



QUANTUM-RESILIENT BANKING: STRATEGIES FOR A SECURE TRANSITION

Authors : Prof. Manish Gangwar, Dr. Shruti Mantri, Dr. Avik Sarkar



The ISB Institute of Data Science is dedicated to driving innovation by fostering partnerships with industry, government, and academia to tackle cutting-edge research challenges and develop digital solutions that enhance competitive advantage. With a mission to be a global leader in data science, the institute empowers organisations and individuals to harness data-driven insights for transformative innovation and sustainable growth. By focusing on collaboration and knowledge exchange, the ISB Institute of Data Science aims to create impactful solutions that not only address current challenges but also anticipate future needs in an increasingly data-centric world.

Authors



Professor Manish Gangwar

Executive Director, ISB Institute of Data Science



Dr. Shruti Mantri

Associate Director, ISB Institute of Data Science



Dr. Avik Sarkar

Senior Research Fellow, ISB Institute of Data Science

IIDS Team



Varalakshmi Peketi

Manager,
ISB Institute of Data Science



Renu Chaturvedi

Content Writer
ISB Institute of Data Science



Rizwan Zhad

Research Associates
ISB Institute of Data Science



Vaibhav Talekar

Research Associates
ISB Institute of Data Science



Raj Tare

Research Associates
ISB Institute of Data Science

Executive Summary

The advancements in the field of technology and telecommunication have also evolved the cyber security threat landscape. Though Quantum computing brings a lot of opportunities, Quantum computers pose a significant risk to currently used Public Key Cryptography (PKC) algorithms (RSA, ECDSA, EdDSA, DH, ECDH), with NIST mandating their deprecation by 2030 and complete removal by 2035. This urgency is heightened by predictions that state actors might possess quantum decryption capabilities as early as 2028, creating a “harvest now, decrypt later” threat. The only way to stay ahead of these attacks is to be aware of security trends, anticipate advanced threats, and build resilient defences. This study investigates the cybersecurity preparedness of India’s Banking, Financial Services, and Insurance (BFSI) sector in response to the emerging quantum computing threat.

The research, which included an analysis of the banking ecosystem, its stakeholders, and supply chains, employed a survey of approximately 118 BFSI CISOs/CTOs to assess current cybersecurity postures, awareness of quantum threats, and readiness for migrating to Post-Quantum Cryptography (PQC). The survey revealed significant vulnerabilities: a substantial portion of respondents demonstrated only moderate understanding of quantum computing and a concerning lack of preparedness for PQC implementation (average score of 2.4 out of 5). While common security measures like access controls and encryption were widely implemented, more advanced techniques and future-proofing strategies were lacking. The most frequent threats in the past year were phishing (65%), DDoS (47.5%), and social engineering (40%) attacks. A majority of respondents (57.5%) believe quantum computing will pose a significant threat within three years. Most respondents rated the potential impact of quantum decryption on stolen data as extremely high.

This study also developed a framework for PQC migration within the BFSI sector, considering data shelf life across the ecosystem. Key advantages of this framework include minimal disruption to existing infrastructure through support for hybrid implementation, straightforward deployment across various environments, and a future-proof architecture designed to counter evolving quantum threats. This framework facilitates the adoption of quantum-safe protocols while minimising disruption.

The study results also highlighted key recommendations for accelerating PQC adoption. Most of the CIOs/CTOs believe that government action needs to prioritise establishing clear guidelines and standards (45%), fund research and development (27.5%), and facilitate stakeholder collaboration (17.5%). Around 42.5% of the CISOs/CTO feel the need for cybersecurity awareness and education, as well as certification programs. Government-funded audits and research grants were equally favored as incentives for financial institutions to prioritise PQC (30% each). Additionally, the respondents highlighted the need for a government-defined migration timeline (45%) and guidance on algorithm selection (27.5%). Finally, for enhancing collaboration, a dedicated forum or working group was strongly recommended (42.5%).

The findings underscore the urgent need for immediate action to mitigate the risks posed by quantum computing. Recommendations include prioritising PQC migration, implementing robust key management practices, enhancing staff training, developing crypto-agile systems, and creating comprehensive data breach response plans. The results emphasise the urgency of developing and implementing a quantum-ready business model within the BFSI sector.

Acknowledgement

We gratefully acknowledge Bank of America for funding this research.

We are grateful to the College of Defence Management for collaborating on the roundtable discussion exploring quantum computing’s impact on the financial and defense sectors. Our thanks also extend to the many cyber and quantum experts who provided invaluable guidance, particularly Lt. Cdr. Karan Kalra (Ret.) and Mr. Rajesh Duddu. We thank Col. Kapil Jaiswal (Ret.), Col. Sai Shankar (Ret.), the Quantum AI Global team, and the QClairvoyance Quantum Labs Pvt. Ltd team for their valuable contributions, guidance, framework review, and model testing.

We gratefully acknowledge the mentorship provided by Mrs. Rohini Priyadarshini (IPS), Mr. Abhinav Biswas, and Major Vineet Kumar to the women leaders participating in the Cybersecurity Workshop, a collaborative effort with WEP. We also thank WEP for their partnership.

Chapter 1

Cyber Crimes: Rising Threats in a Digital World

Introduction

Over the past 15 years, the world has witnessed an unprecedented surge in digitalisation, which is reshaping how businesses and governments operate, function, and engage with digital users. From the advent of smartphones enabling internet access on mobile devices to the emergence of artificial intelligence, the evolution of technology has paved the way for enhanced efficiencies, convenience, and unparalleled connectivity. However, this significant push towards digitalisation has introduced new vulnerabilities, making the system more susceptible to cyber threats and attacks. A key cybersecurity concern is the targeting of critical infrastructure like financial systems, power grids, water supplies, and transportation networks. The rise of quantum computing poses an even greater risk, as it has the potential to break existing encryption methods, making sensitive data and critical systems more vulnerable to sophisticated cyberattacks.

The Surge in Cyber Vulnerabilities

The widespread adoption of the internet in the early 2000s was a pivotal moment, as various industries integrated digital tools to boost productivity and interconnectedness. At the same time, the declining cost of computing power, coupled with the widespread availability of high-speed internet, encouraged both businesses and individuals to embrace a digital-first approach. As organisations increasingly relied on interconnected systems, the attack surface for cyber threats expanded. Traditional cybersecurity measures often focused on a system and network level defences became insufficient. New vulnerabilities arose from integrating digital systems, significantly impacting businesses reliant on extensive supply chains, cloud services, and third-party vendors—all potential points of failure.

By the late 2000s and early 2010s, the sophistication of cyberattacks increased significantly. Hackers began utilising advanced techniques to carry out cyberattacks, such as social engineering, ransomware and distributed denial-of-service (DDoS) attacks. The Internet of Things (IoT), introduced in the early 2010s, made the situation worse; billions of smart devices joined shared networks with insufficient security protocols. Everyday objects—once benign—now became potential entry points for attackers. Critical infrastructure became a focal point for these threats, given its essential role in maintaining public safety and operational continuity.

The cost of cybercrime has surged from \$0.86 trillion in 2018 to a projected \$15.63 trillion by 2029, marking an 18-fold increase. Between 2024 and 2029, it is expected to rise by \$6.4 trillion, a 64.91% increase (<https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>).

Globally, cyberattacks remain a significant challenge for the finance, insurance, and manufacturing sectors. In 2023, the manufacturing sector experienced the highest share of cyberattacks among the leading industries worldwide (<https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/>). Approximately 18% of cyberattacks targeted the finance and insurance sectors, making them the second most targeted industries.

The Threat Landscape: Cyberattacks on Critical Infrastructure

The attack on critical infrastructure is not merely a technology failure but a

complex interplay of security, geo-politics, and economics. Critical infrastructure vulnerabilities are deeply concerning due to the potentially catastrophic societal impact of disruptions to finance, healthcare, transport, and power.

According to Center for Strategic and International Studies (CSIS) there was a 70% surge in Russian cyberattacks on Ukraine in 2024, reaching 4315 incidents and targeting critical infrastructure (government, energy, and defence) as of January 2025. In December 2024, Chinese hackers breached a third-party vendor for the US Treasury Department to gain access to over 3,000 unclassified files. Chinese hackers have breached at least twenty Canadian government networks over the last four years (as of October 2024), according to the Canadian Centre for Cyber Security (CCCS).

In July 2024, a faulty software update for Microsoft Windows issued by cybersecurity firm CrowdStrike caused a global IT outage that disrupted airline and hospital operations. It affected approximately 8.5 million machines and cost Fortune 500 companies \$5.4 billion, according to reports.

One of the most notorious cyber thefts in banking history occurred when hackers infiltrated the Bangladesh Bank, the central bank of Bangladesh, in 2016. The attackers gained access to the bank's systems and used the SWIFT network to send fraudulent requests to transfer \$951 million to accounts across the world, resulting in losses of \$81 million.

The cyber incidents in the financial sector have become more frequent over the past two decades (Fig. 1). Cyberattacks with malicious intent like extortions or malicious data breaches have almost doubled relative to the period of the COVID-19 pandemic. According to the International Monetary Fund (IMF) report, April 2024, direct losses from cyber incidents amounted to almost \$28 billion (Fig. 2). Total direct and indirect costs of these incidents, however, are most likely to be substantially higher (Kamiya and others 2021). Many factors have contributed to the rise in cyberattacks such as growing digitalisation accelerated by the COVID-19 pandemic, financial invocation, especially growth in UPI and geopolitical tensions, considering the surge of cyberattacks after Russia invaded Ukraine in February 2022 and the Gaza-Hamas war (Fig. 3).

The financial sector is especially vulnerable to cyberattacks. According to the International Monetary Fund (IMF) report, one-fifth of the reported cyber incidents in the past two decades have affected the financial sector (Fig 4.). As per the IMF, financial firms have reported around \$12 billion financial losses since 2004 and \$2.5 billion in direct losses (Fig 5). JPMorgan Chase, for example, the largest US bank, recently reported experiencing 45 billion cyber events per day while spending \$15 billion on technology.

In 2019, Capital One, one of the largest banks in the United States, suffered a massive data breach affecting over 100 million customers. A former employee exploited a misconfigured web application firewall to gain access to sensitive data stored by Capital One. The breach exposed personal information, including Social Security Numbers and bank account details. Capital One faced significant reputational damage, regulatory scrutiny, and an eventual settlement of \$80 million with the Office of the Comptroller of the Currency (OCC).

In 2020, the Banking Association of South Africa (BASA) was the target of a significant denial-of-service (DoS) attack. The attack flooded the bank's services with traffic, rendering them unavailable. Hackers claimed responsibility, demanding a ransom to cease the attack.

In 2017, Union Bank of India experienced a significant data breach that exposed sensitive customer information. Hackers reportedly accessed the bank's internal systems through a phishing attack that compromised employee credentials. The breach revealed the personal information of customers, including account numbers and balance information.

The State Bank of India (SBI), one of the largest public sector banks in India, fell victim to a phishing attack in 2016. Cybercriminals set up fake websites mimicking SBI's online banking portal, luring customers to enter sensitive login information. The stolen data was then used to siphon funds from customer accounts. In early 2021, Paytm Payments Bank encountered a cyberattack that affected some of its customer accounts. The bank's systems were targeted by a sophisticated malware attack designed to extract sensitive information and access

payment credentials. Quick action from the bank's IT team contained the breach and prevented a significant impact.

The financial sector's digital ecosystem is exposed to cyber risks from time to time as financial firms handle large amounts of customer data and transactions, potentially making them a target of choice for cybercriminals seeking monetary gains or aiming to disrupt economic activity. The IMF's April 2024 report shows that the financial industry experiences a significant portion of cyberattacks, with banks and other financial institutions bearing roughly half the brunt. Cyberattacks disproportionately affect large banks, even with their robust security measures (Fig. 6). The Bank's digital ecosystem and payment networks are a part of the nation's critical infrastructure. A cyber incident could disrupt the network and severely affect economic activity (Eisenbach, Kovner, and Lee 2022).

Financial market infrastructure, encompassing payments, securities, central depositories, counterparties, and repositories, often exhibits high concentration and limited substitutability, thus making financial institutions vulnerable to cyberattacks (Fig. 10A). Financial institutions depend on third-party vendors for their operations for a variety of tasks, such as software development, hardware, cloud services, etc. Over half of global IT providers serve at least two major international banks, indicating significant market overlap. IT providers of around 20 percent of insurers and 25 percent of assets managers supply services to two or more institutions in their respective groups (Fig. 9D). Interconnectedness and strong dependencies

among the banking processes also lead to a higher probability of cyber incidents. Despite the benefits IT providers offer financial institutions, significant overlap in third-party services increases their cybercrime vulnerability (Financial Stability Report 2023; Duffie and Younger 2019).

Cyber Crimes: Financial Sector in India

According to the National Crime Record Bureau (NCRB) data from 2017 to 2022, in the last 5 years, 1,36,000 cases have been registered. India has seen a 236.6% surge in cyberattacks. The year 2019 witnessed a 78.12% rise in the number of cases, as compared to 2018, and a 23.53% rise in cases in 2022 as compared to 2011. India's cybersecurity landscape underwent an unprecedented evolution throughout 2024, marked by escalating threats and advancements in detection capabilities. The year 2024 witnessed over 369.01 million security incidents across 8.44 million endpoints. This translates to an average of 702 potential security threats every minute (India Cyber Threat 2024, Data Security Council of India). In 2024, the healthcare industry was the most targeted sector, accounting for 21.82% of all attacks, followed by hospitality at 19.57% and banking at 17.38%. This indicates that attackers focus on industries handling large volumes of personal and financial data. Geographically, major tech hubs like Telangana witnessed maximum cyber incidents at 15.03% followed by Tamil Nadu (12%), Surat (14.58%), Bengaluru (11.93%), and Jaipur (11.72%).

Malware continues to be a significant challenge, with various types of malicious software impacting millions of devices.

Ransomware attacks on BFSI (Banking, Financial Services, and Insurance) organisations increased in 2024, with the India Cyber Threat Report noting that ransomware remains a high-impact threat despite accounting for a relatively small percentage of overall malware detections. The attacks often involved double extortion (encrypting data and threatening to release it publicly). The report specifically highlights the RansomEXX group as active in this area, utilising advanced encryption techniques, such as RSA-2048 and AES-256. The attacks also included data exfiltration alongside encryption.

In 2024, phishing and social engineering attacks continued to be prevalent, targeting BFSI employees to obtain credentials with the use of sophisticated techniques, including the use of AI to create highly targeted and personalised phishing attacks. These attacks aim to trick users into revealing sensitive information or downloading malware. The report also points out the emergence of deepfake scams targeting BFSI executives. These attacks involve AI-generated voice and video impersonations to trick individuals into releasing sensitive information or performing fraudulent transactions. 2024 witnessed an increase in threats targeting mobile banking users with Antasa Android Banking Trojan employing techniques such as screen streaming and keylogging to steal banking credentials. In the attack on Brontoo Technology Solutions-a collaborator with C-EDGE (a joint venture between Tata Consultancy Services and the State Bank of India)-attackers exploited a vulnerability (CVE-2024-23897) in a misconfigured Jenkins

server, gaining access to sensitive internal files (including SSH keys) and ultimately deploying ransomware. This showcases the danger of vulnerabilities in software development pipelines and the risk of relying on third-party vendors (India Cyber Threat Report 2025, DSCI).

Macro-Financial Stability: Impact of Cyber Risks

A cyber incident at a financial institution could threaten macro-financial stability through three key factors:

1. **Loss of Confidence and Liquidity Risk:** Data breaches erode public trust, potentially triggering liquidity crises. Deposit withdrawals or bank runs ("cyber runs") can ensue, leading to solvency issues and potentially impacting related institutions.
2. **Disruption of Critical Infrastructure:** Cyberattacks, such as ransomware, can cripple key infrastructure like cloud access, networks, and servers. This operational disruption directly threatens a financial institution's stability.
3. **Systemic Contagion:** The interconnected nature of the financial system—through shared technology (e.g., common software) or financial linkages (e.g., interbank markets, settlement systems, shared assets)—can rapidly spread the impact of a single cyber incident across multiple institutions, creating systemic risk.

Financial stability could also be undermined by cyber incidents at non-financial institutions. For example, a cyberattack on critical

infrastructure (such as electricity grids) could make it difficult for financial institutions to operate normally, with the effects spilling over to the macro-economy. The cyber incidents at non-financial institutions and third-party vendors could raise credit risks for financial institutions. Cyberattacks on public entities, such as those disrupting government debt management, negatively impact the financial sector—either directly or indirectly via increased sovereign risk (Global Financial Stability Report, April 2022) (Fig. 8).

As attackers become more organised and sophisticated, they employ a mix of strategies, including data theft, phishing schemes, and brute-force attacks. For example, they exploit vulnerabilities within the banking ecosystem, launch supply chain attacks, and identify weaknesses in third-party vendor tools to steal bank data. Once they gain access to sensitive customer information, they send phishing emails and SMS messages containing malicious links to lure customers into clicking on them. These links often mimic the bank’s actual website.

Believing they are on a legitimate site, customers enter their login details. Once attackers obtain this information, they can initiate spoofing attacks to transfer funds from the customers’ accounts.

Following data breaches, usernames and passwords are often leaked on the dark web. Attackers take advantage of these stolen credentials to access multiple accounts across different financial institutions, knowing that many customers reuse passwords. Given the

critical role that banks play in the economy, paying ransom to prevent the release of stolen data on the dark web may seem like a more viable option than risking operational downtime and reputational damage.

Losses to Firms from Cyber Incidents

According to the IMF’s report from April 2024, the maximum expected loss has doubled since 2017, reaching \$141 million in 2021, which amounts to 50 percent of an average firm’s operating income (Fig. 9A). Furthermore, it is anticipated that a cyber incident occurring once every decade could lead to a \$2.5 billion loss, representing about 800 percent of an average firm’s operating income, thereby jeopardising the liquidity and solvency of the affected firm. For financial institutions, estimated maximum losses in a median year are around \$152 million, with potential peaks of up to \$2.2 billion occurring once every ten years (Fig. 9D). While firms typically do not report indirect losses such as reputational harm, lost business, or investments in cybersecurity, overall losses—both direct and indirect—can be approximated by analysing stock price reactions to cyber incidents (Kamiya and others, 2011). On average, stock returns decrease by 0.1 to 0.2 percentage points for affected firms, with the most significant losses observed in small firms, ranging from 0.3 to almost 0.6 percentage points (Fig. 9B). This indicates that small firms often lack robust incident response and business continuity plans to mitigate potential losses from cyberattacks (Fig. 9C).

Emerging Technologies and Cyber Attacks

With the advancements in technology and telecommunications, the cyber threat landscape has also evolved over the years and is dominated by AI-driven attacks, with cybercriminals leveraging generative AI, deep learning technologies to create more sophisticated and adaptive threats using AI-powered malware. Social media and generative AI enable highly targeted scams and impersonations, making it harder to distinguish between real and artificial interactions. Deepfakes continue to remain a matter of concern in the BFSI sector.

Polymorphic Malware: Many cybercriminals utilise polymorphic malware, an advanced type of malware that employs artificial intelligence to continuously alter its code. The malware changes its structure each time an antivirus program tries to detect it via its signature. For instance, BlackMamba leverages AI technology to actively avoid detection. Its capability to infiltrate the Android operating system broadens the attack surface, posing threats to a wider array of users and devices. Initially disguised as a basic banking Trojan, it rapidly adapts by integrating new techniques, making detection and removal significantly more challenging.

AI-Enhanced Social Engineering: Modern cybercriminals harness AI techniques to execute social engineering attacks. They analyse the social media profiles of government and banking officials using machine learning models to identify their interests, family members, and professional networks. With this information, attackers tailor highly personalised phishing emails that appear to come from trusted sources, including

specific details from the target’s life, greatly increasing the likelihood of being opened and acted upon. These emails may contain links to highly convincing fake login pages designed to capture user credentials.

Data Poisoning: In a data poisoning attack, a malicious actor gains access to a dataset employed to train fraud detection systems. They subtly manipulate a small portion of the data to introduce biases, resulting in the AI system misclassifying fraudulent transactions as legitimate. This could lead to substantial financial losses for the institution before the issue is detected.

Automated Attacks: Attackers leverage AI technologies to automate various stages of the attack chain, enhancing the speed and efficiency of attacks while enabling large-scale operations with less manpower. For example, an attacker might utilise an AI-powered tool to automatically identify and exploit vulnerabilities across thousands of Indian BFSI (Banking, Financial Services, and Insurance) websites. This rapid, automated method enables a single attacker to compromise multiple systems far more quickly than manual techniques would allow.

Fake ChatGPT App: In this type of attack, a user downloads what appears to be a legitimate ChatGPT app from an unofficial app store. Although the app looks authentic, it contains hidden malware that collects the user’s location data, contacts, and browsing history. This information is then sent to a remote server controlled by the attackers.

AI-Powered Phishing Kit: The India Cyber Incident Report 2025 highlights the rise of fake ChatGPT applications in app stores. These apps disguise themselves as legitimate ChatGPT

applications but secretly incorporate spyware or other malicious components. Once installed, they can collect sensitive user information, steal data, and potentially facilitate broader compromises.

Deepfake Attacks: Cybercriminals are increasingly using deepfake technology to create hyper-realistic audio and video for malicious purposes. These deepfakes can impersonate individuals, such as corporate executives or public figures, convincingly mimicking their voices and appearances. Attackers may use this technology to conduct fraudulent activities, like manipulating video calls to authorise transactions or provide misleading information, potentially causing reputational damage and financial loss to the victims.

Post-Quantum Cryptography Cyber Threats: Quantum computing, while still in its nascent stages, represents a rapidly evolving technology with the potential to revolutionise various fields, including cybersecurity. Its immense computational power poses a significant threat to current cryptographic systems, including those widely used in the BFSI sector. Currently, both symmetric and asymmetric cryptographic algorithms are used across the banking ecosystem to ensure secure and safe banking experience for customers. In the current study, researchers analysed the NCRB data from 2017 to 2022 to identify trends and patterns in cyber threats faced by the banking sector, including the types of attacks that may target the present encryption methods and how the vulnerabilities can be exploited by cyber criminals in the Quantum Era. An analysis of NCRB data revealed that cheating by impersonation using computer resources topped the list with approximately

46,596 cases, followed by identity theft (37,623), online banking fraud (19,226), ATM fraud (10,643), OTP fraud (7,233), credit/debit card fraud (5,554), and ransomware (4,872) (Fig. 11).

1. Cheating by Impersonation (45,596 cases):

The cheating by impersonation cases rose from 2,269 in 2017 to 11,919 in 2020 (243.1% increase from 2017). The COVID-19 pandemic in 2020 saw a notable increase (115.9%) in impersonation cases from 2019. The rise in impersonation cases suggests vulnerabilities in authentication protocols. If the attackers can decrypt communications and impersonate legitimate users, they could initiate fraudulent transactions or gain unauthorised access to sensitive accounts. By exploiting weakness in digital signatures susceptible to quantum attacks, criminals could easily impersonate individuals leading to fraudulent transactions and unauthorised actions.

2. Identity Theft (37,623 cases):

Identity theft saw a sharp increase, from 3,724 cases in 2017 to 6,688 in 2018 (79.6% rise), further escalating to 18,943 in 2019 (183.5% increase from 2018). Quantum computing, with its increasing processing power, can decrypt user data in a fraction of seconds. Using this, cyber criminals could extract personal information, enabling them to impersonate victims and commit frauds on a larger scale. When quantum decryption becomes feasible, cyber criminals could intercept secured communications that contain sensitive identity information, leading to theft.

3. Online Banking Frauds (19,226 cases):

As banks transition to post-quantum algorithms, they may inadvertently expose vulnerabilities, leading to increased online banking fraud during the transition. For example, forging digital signatures could facilitate unauthorised transactions, resulting in direct financial loss through online banking systems.

4. ATM Frauds (10,643 cases):

Quantum-capable threats could capture and decrypt ATM transaction data, potentially allowing hackers to recreate authentication tokens to access accounts illicitly. If an attacker compromises the software used in ATMs (often using weak encryption), they could facilitate unauthorised withdrawals, especially during the transition to newer security standards resulting in supply chain attacks.

5. OTP Fraud (7,233 cases):

If the algorithms securing OTPs are not updated to be quantum-resistant, attackers could exploit these weaknesses to intercept and reuse OTPs, leading to unauthorised access of accounts resulting in digital signature forgery.

6. Credit/Debit Card Fraud (5,554 cases):

Transition vulnerabilities could allow fraudsters to gain access to credit/debit card information, especially if payment systems continue to rely on outdated encryption methods during the switch to post-quantum cryptography. Also, the possibility of quantum decryption enables attackers to intercept payment card

transactions and extract sensitive data for fraudulent purposes.

7. Ransomware (4,872 cases):

Cyber criminals can exploit weak encryption during ransomware attacks, compromising digital signatures. Attackers could exploit these vulnerabilities to access sensitive files, increasing the impact of the attacks.

The onset of quantum computing poses significant cyber risks, especially if organisations do not proactively implement post-quantum cryptographic solutions. Falling behind in this transition not only leaves systems open to attack but also leads to far-reaching consequences across various sectors, particularly in banking and finance, where security and trust are paramount. The transition to post-quantum cryptography (PQC) is a complex undertaking, demanding a meticulous and well-planned migration, not simply a straightforward upgrade. At the heart of this transition lies the critical recognition that cryptographic algorithms underpin the very fabric of our digital world, securing everything from online banking and web authentication to the protection of sensitive data.

As businesses prepare for this monumental shift, they must consider the following:

- **Comprehensive Diagnosis:** A thorough assessment of current cryptographic implementations is crucial to understand vulnerabilities and prioritise areas for change.
- **Strategic Planning:** Organisations need to develop a roadmap outlining their approach to PQC, including the selection

of appropriate algorithms, timelines for implementation, and resource allocation.

- Execution and Adaptation: Moving to PQC will necessitate changes to existing systems and processes, requiring careful execution and adaptation to ensure smooth integration.

The current study aims to understand how well prepared is the BFSI sector from a cybersecurity perspective; Are the financial institutions CISOs (Chief Information Security Officers) fully aware of the risks and threats posed by these techniques? Do the organisations have a well-prepared, quantum-guided model at hand, ready for implementation?

The Aims and Objectives of the current study are:

1. Evaluate Current Cybersecurity Posture:
- Assess the current cybersecurity posture of financial institutions, examining their existing security measures, encryption practices, and data protection policies.
 - Analyse the effectiveness of these measures in mitigating known threats, as well as the potential vulnerabilities to quantum computing attacks.

2. Assess Awareness of Quantum Threats in BFSI Sector:

- Evaluate the level of awareness among the BFSI sector regarding the risks and threats posed by quantum computing.
- Explore their understanding of the potential impact of quantum computing on cryptography, data security, and business operations.
- Identify any gaps in awareness and knowledge, highlighting areas where education and training are needed.

3. Determine Quantum-Guided Business Model Readiness:

- Assess whether financial institutions have developed a quantum-guided business model that incorporates strategies for mitigating quantum-related risks.
- Analyse existing plans, policies, and procedures related to the transition to post-quantum cryptography (PQC).
- Identify any gaps in preparedness and recommend steps that organisations can take to develop a robust and comprehensive quantum-ready business model.

References

1. Adelman, Frank, Jennifer A. Elliott, Ibrahim Ergen, Tamas Gaidosch, Nigel Jenkinson, Tanai Khiaonarong, Anastasiia Morozova, Nadine Schwarz, and Christopher Wilson. 2020.

2. Bibek Das, "Recent Cyber Attacks in Indian Banks," SpringerLink, 2018.

3. Cybersecurity for Indian Banks," NASSCOM, 2022.

4. Duffie, Darrell, and Joshua Younger. 2019. "Cyber Runs." Hutchins Center Working Paper 51, Brookings Institution, Washington, DC

5. Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee. 2022. "Cyber Risk and the US Financial System: A Pre-Mortem Analysis." Journal of Financial Economics 145 3: 802-26.

6. Global Financial Stability Report, The Last Mile: Financial Vulnerabilities and Risks, International Monetary Fund Report April 2024.

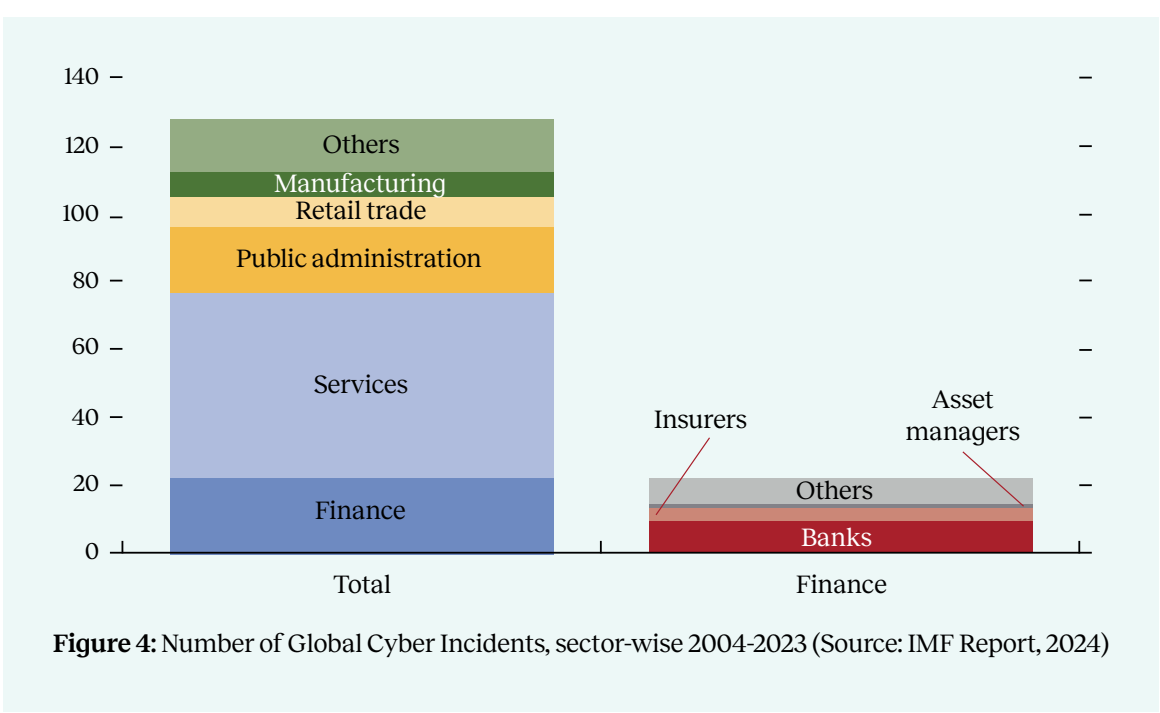
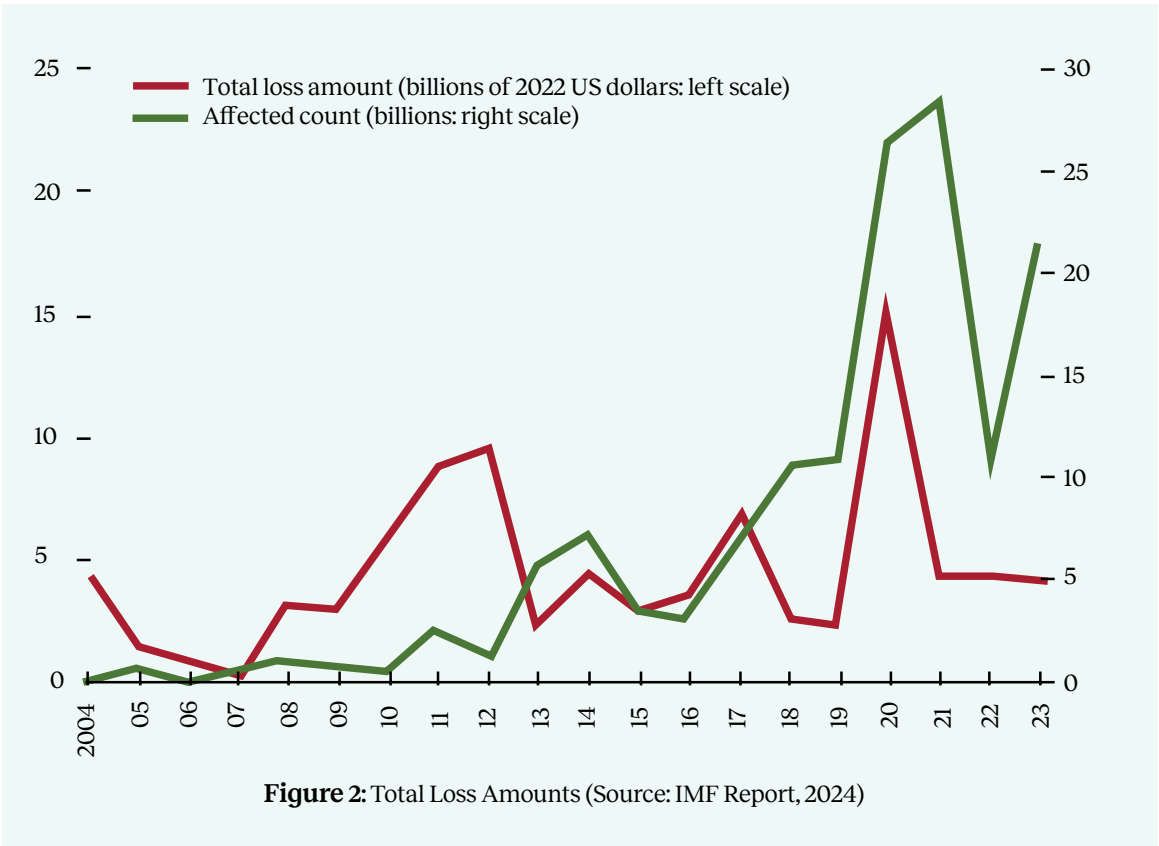
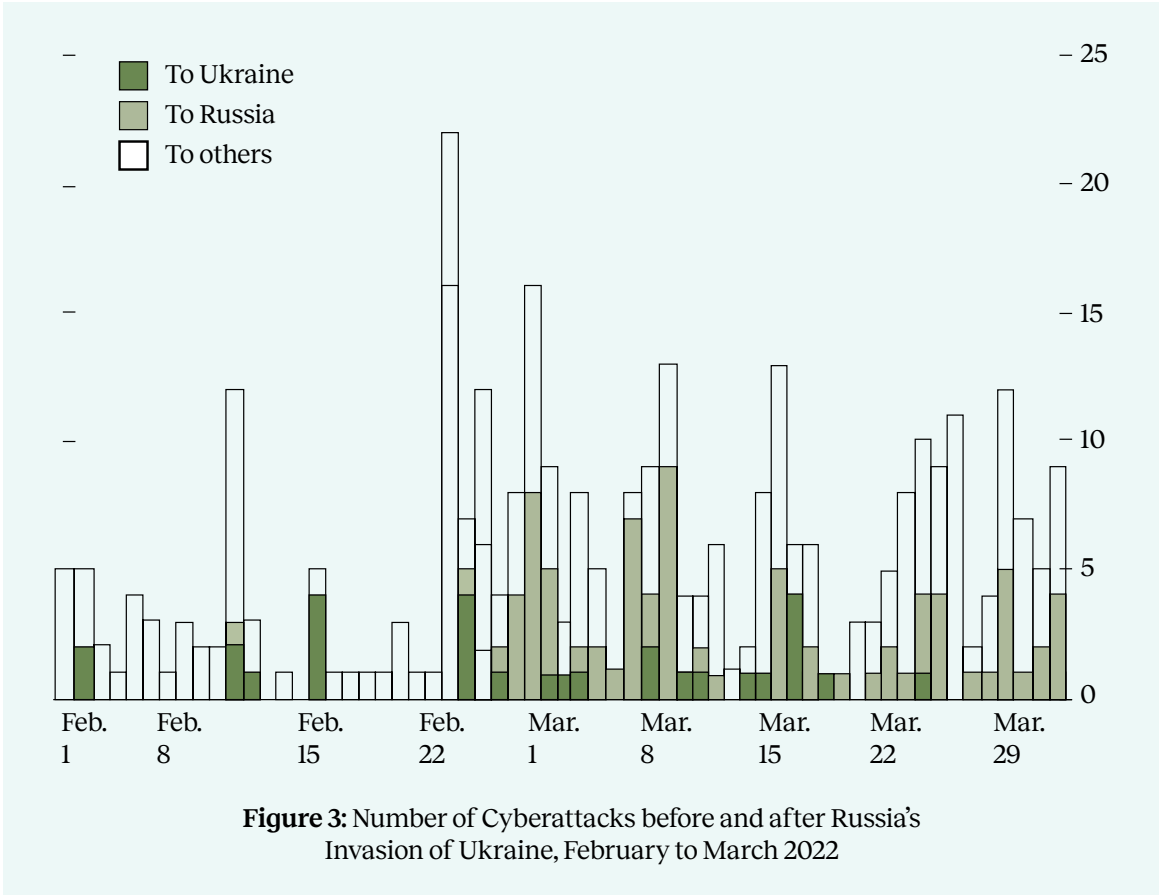
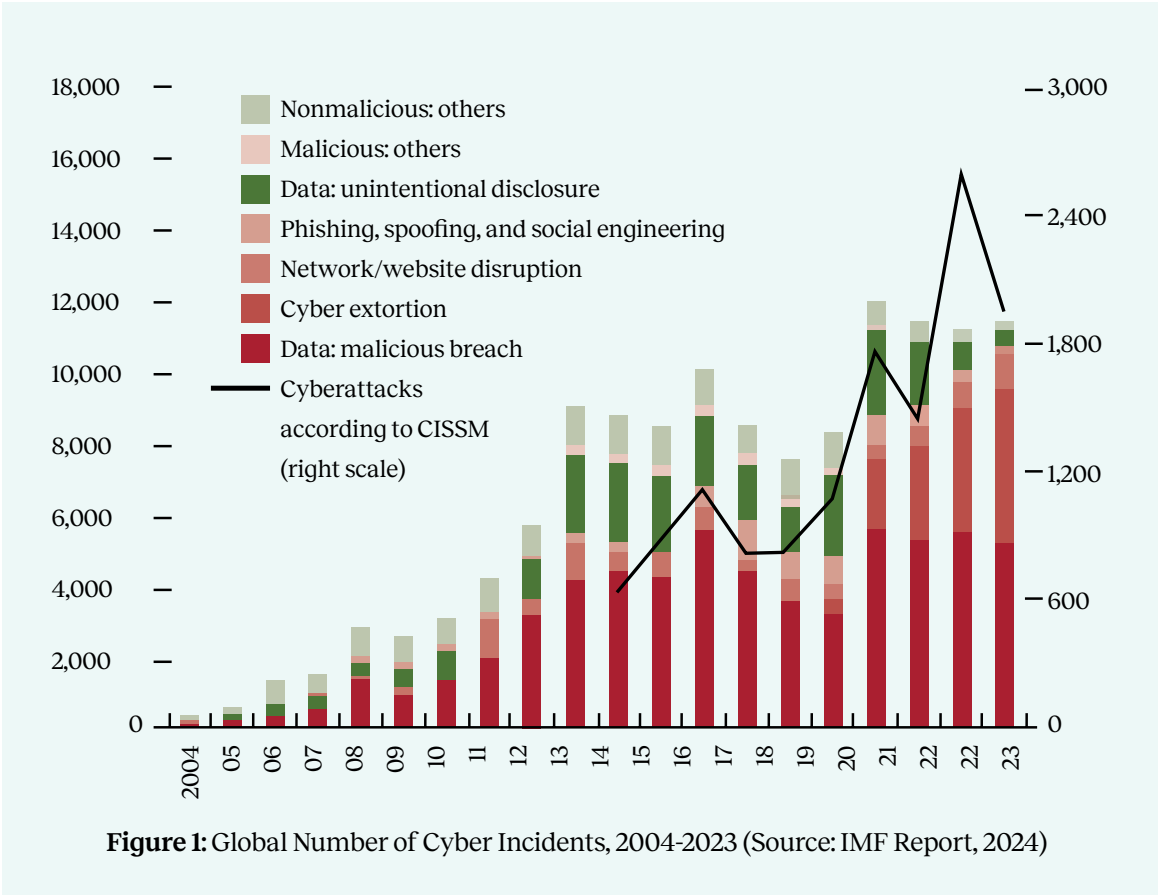
7. Jamilov, Rustam, Hélène Rey, and Ahmed Tahoun. 2023. "The Anatomy of Cyber Risk." NBER Working Paper 28906, National Bureau of Economic Research, Cambridge, MA.

8. Kamiya, Shinichi, Kang Jun-Koo, Kim Jungmin, Andreas Milidonis, and René M Stulz. 2021. "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms." Journal of Financial Economics 139 3: 719-49.

9. Sedik, Tahsin, Majid Malaika, Michel Gorbanyov, and Jose Deodoro. 2021. "Quantum Computing's Possibilities and Perils." IMF Blog, September.

10. Quantum Computing and the Future of Cybersecurity, NASSCOM, 2021





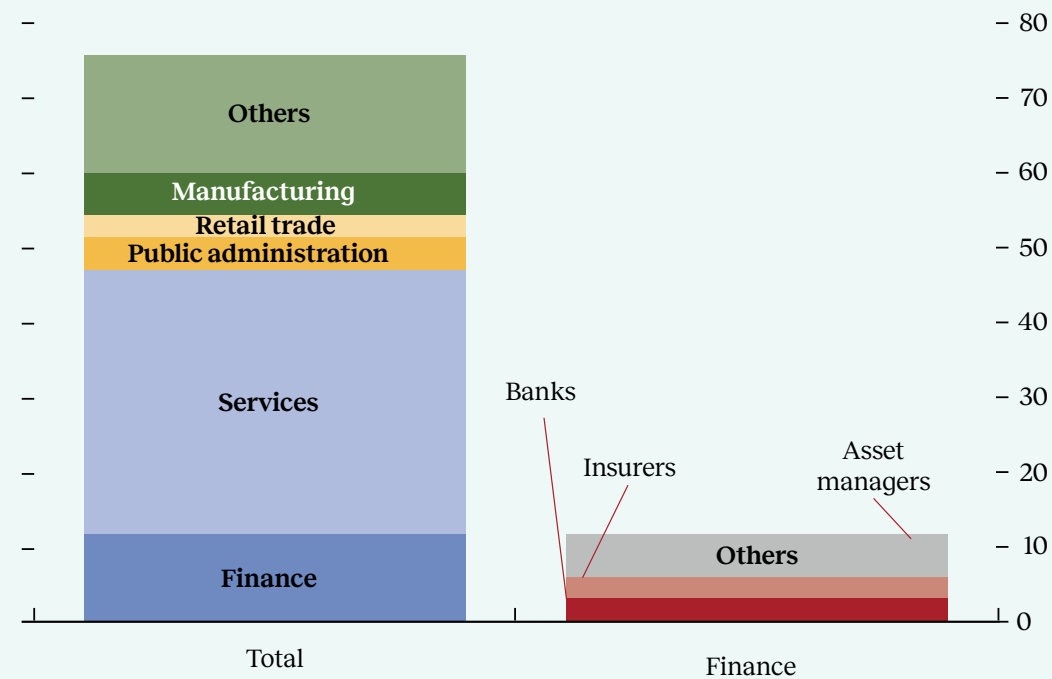


Figure 5: Losses from Global Cyber Incidents sector-wise 2004-2023 (Source: IMF Report, 2024)

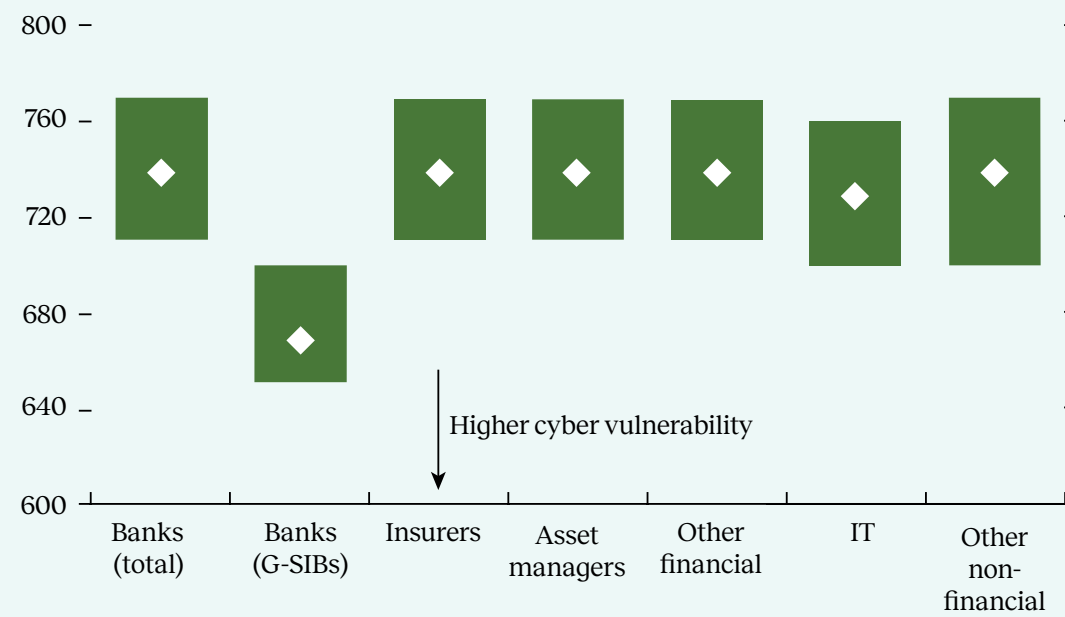


Figure 6: Cyber Risks in Financial Sector (Source: IMF Report, 2024)

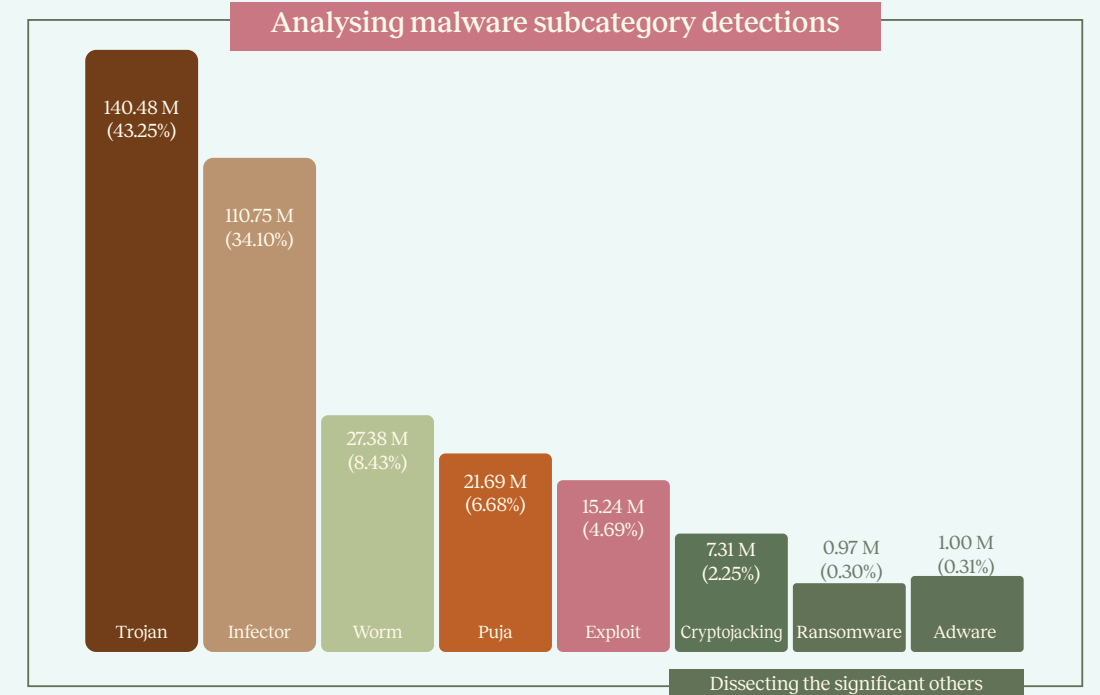


Figure 7: Malware Sub-category Detections
Source: India Cyber Threat 2025 Report, Data Security Council of India

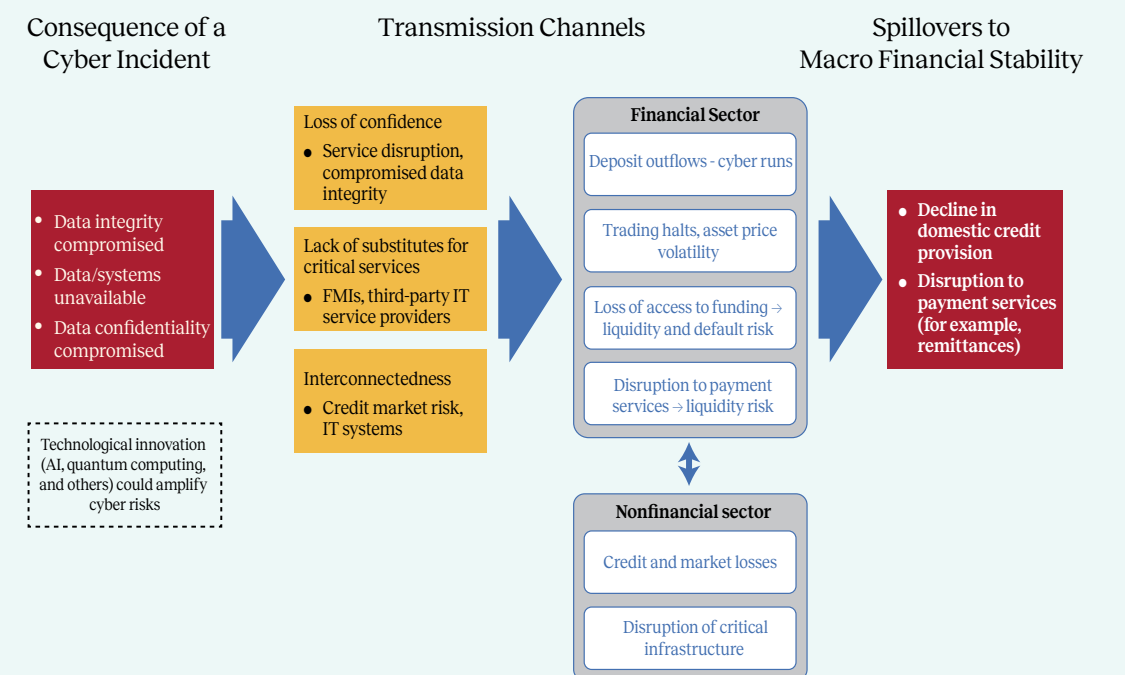


Figure 8: *Cybersecurity and Micro-financial Stability

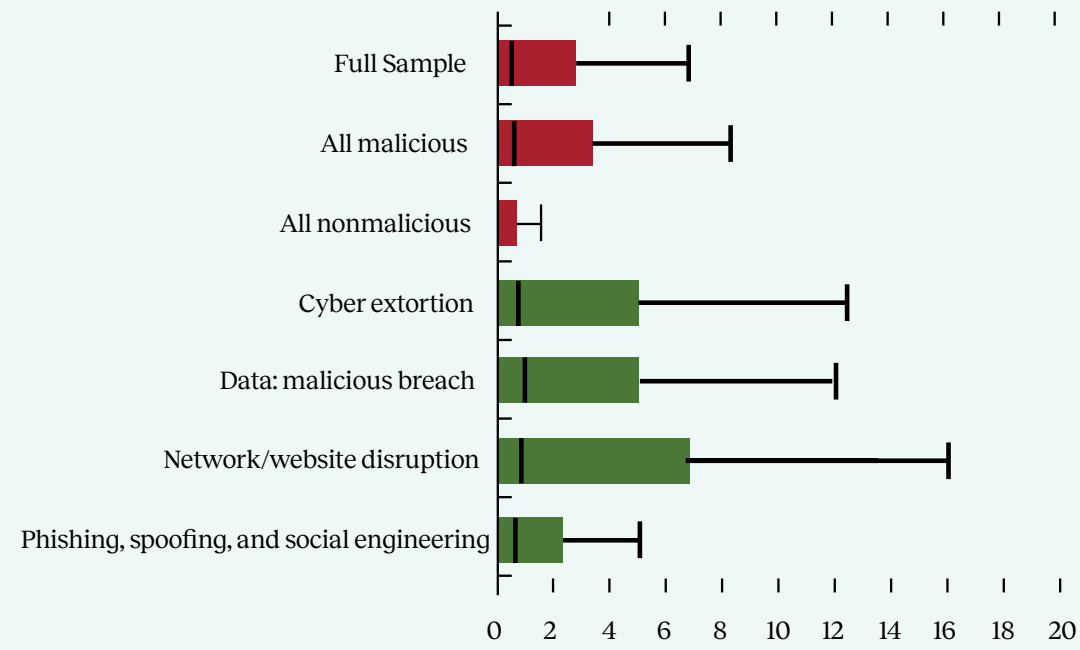


Figure 9A: Reported Direct Losses Resulting from Cyber Incidents (Source: IMF Report, 2024)

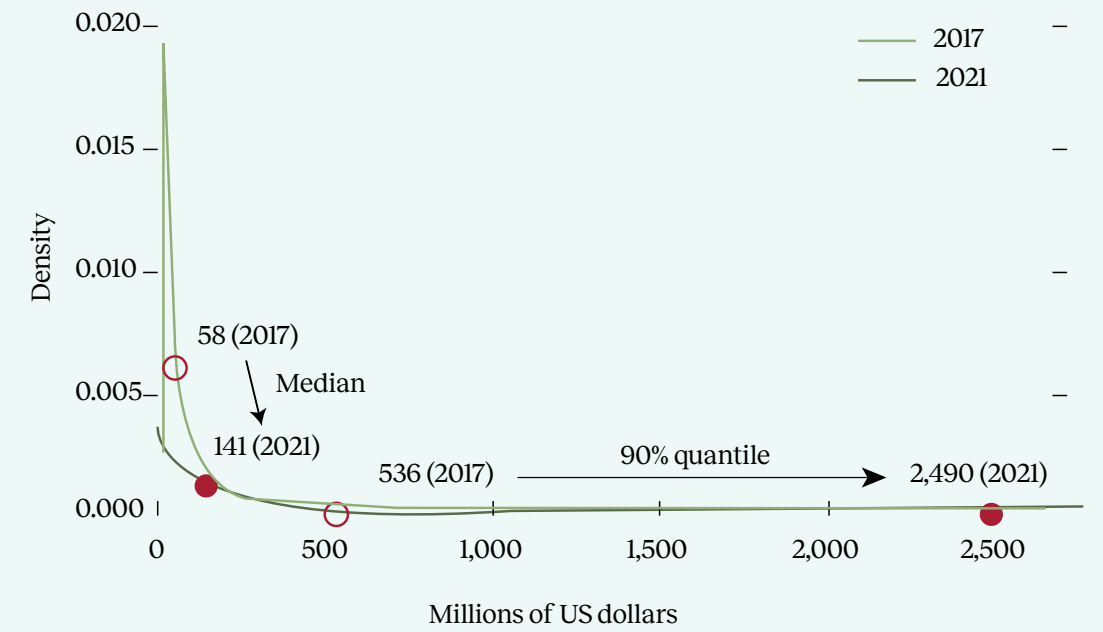


Figure 9C: Estimated Distribution of Maximum Annual Loss (Source: IMF Report, 2024)

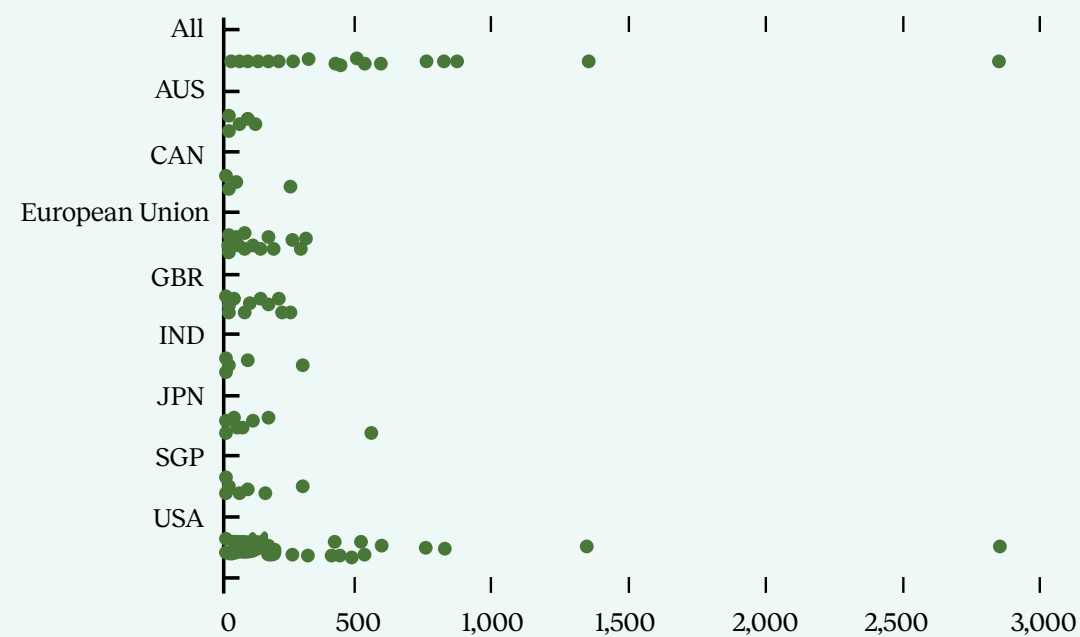


Figure 9B: Losses Resulting from Cyber incidents Globally (Source: IMF Report, 2024)

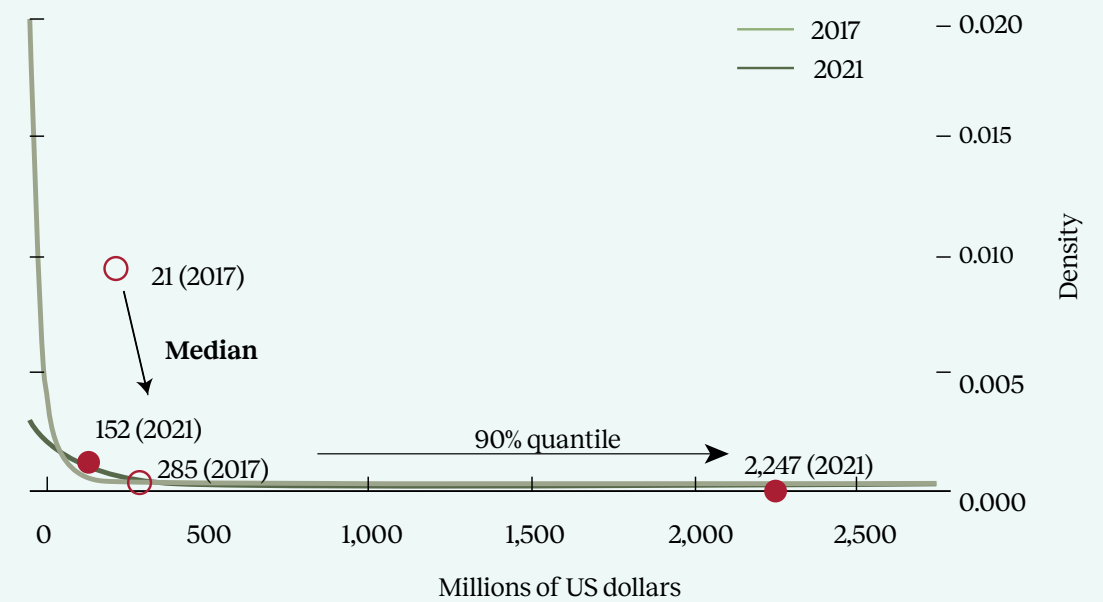
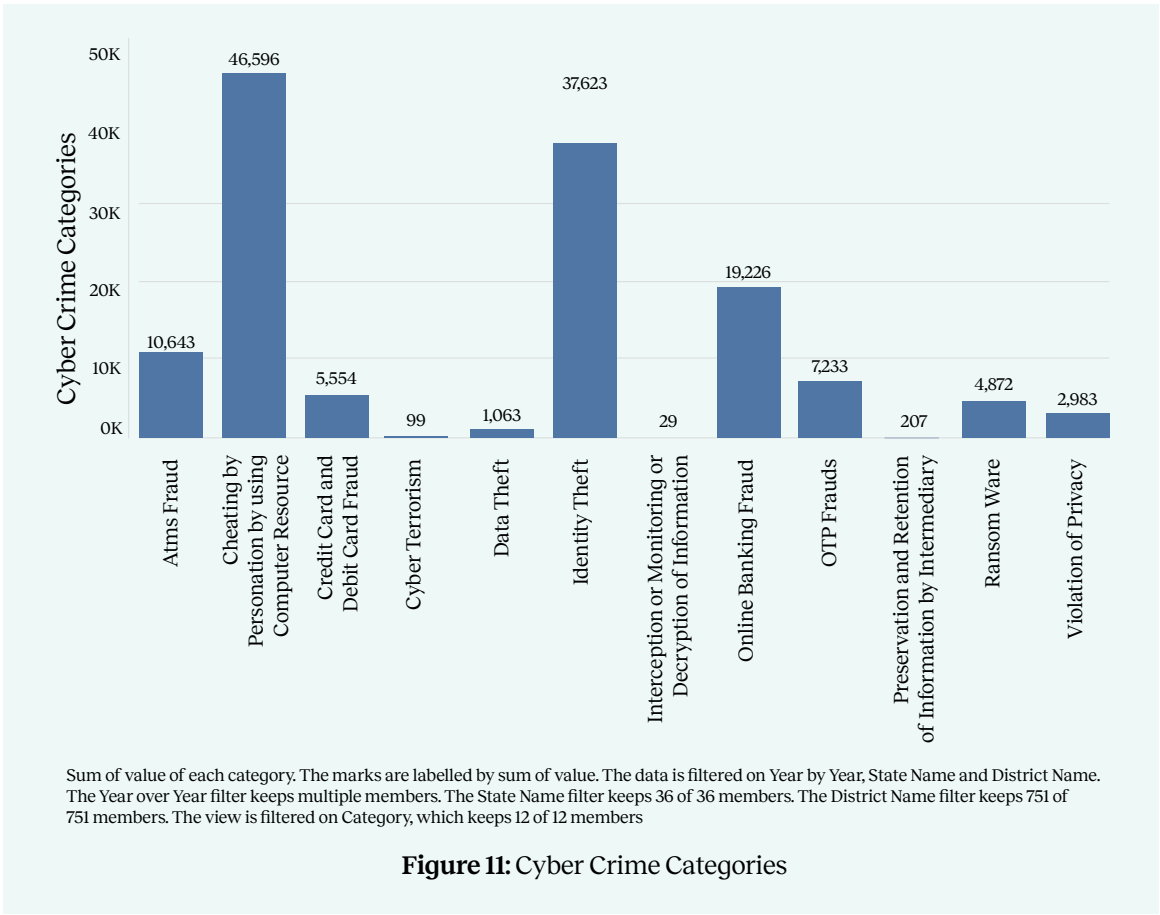
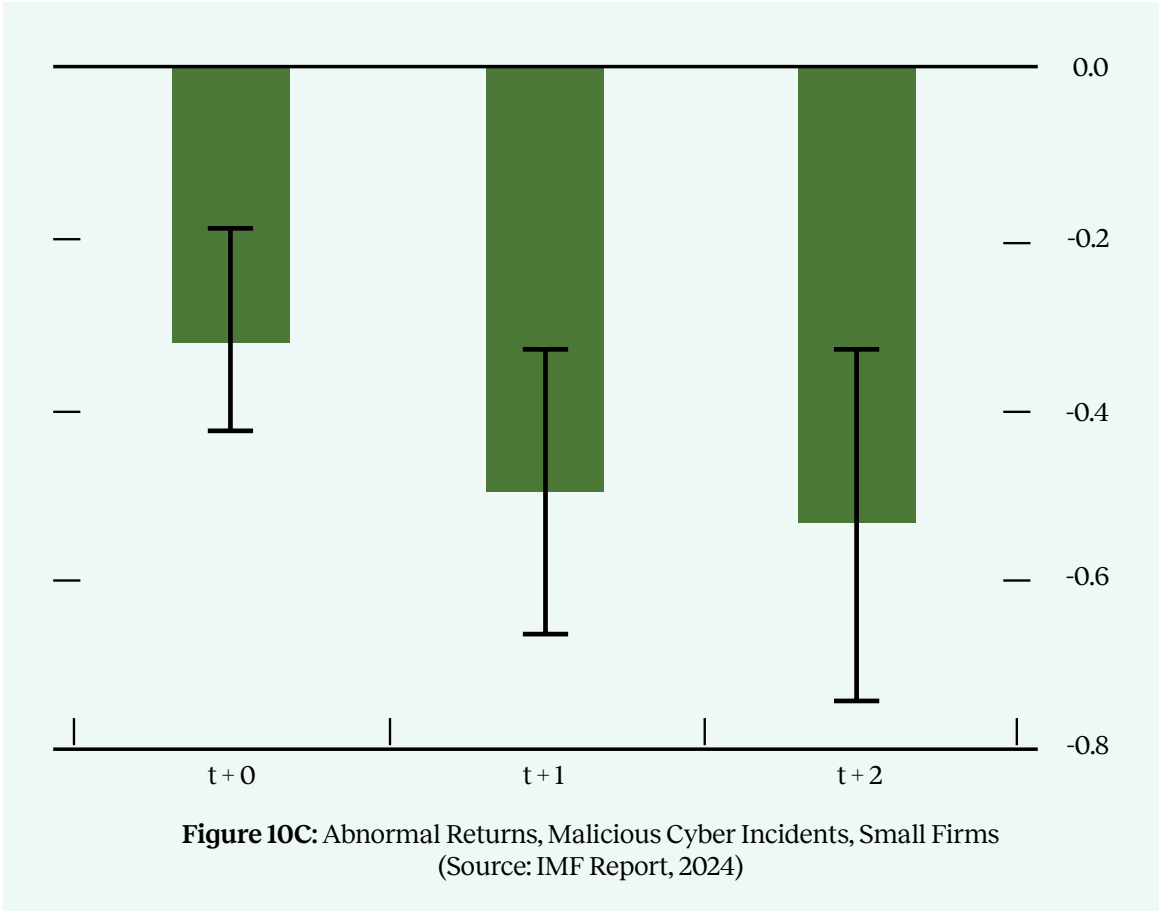
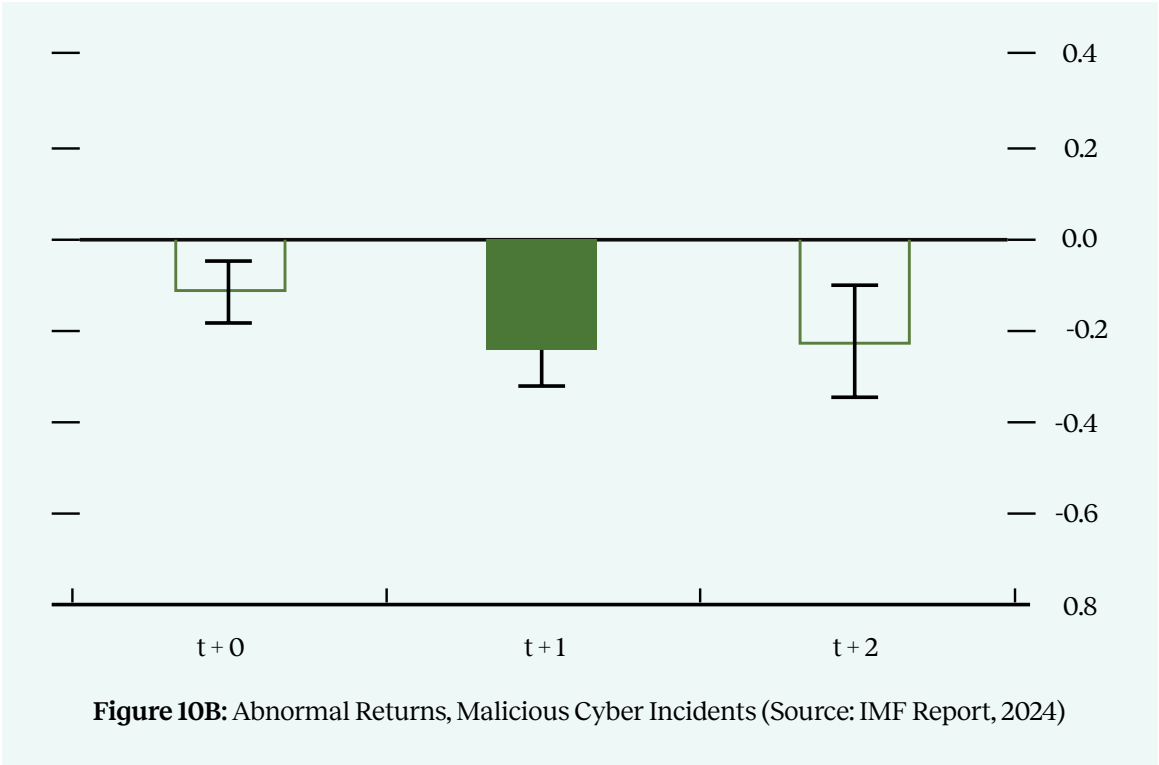
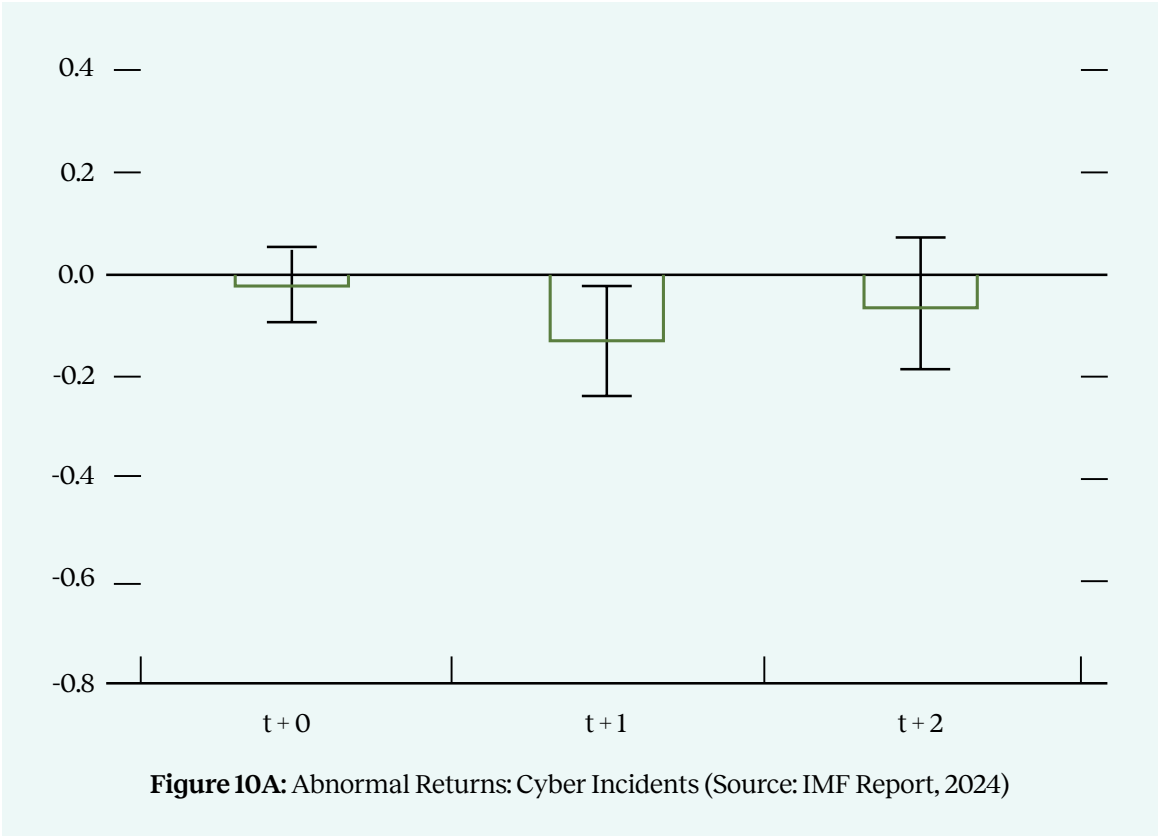


Figure 9D: Estimated Distribution of Maximum Annual Loss for Financial Firms (Source: IMF Report, 2024)



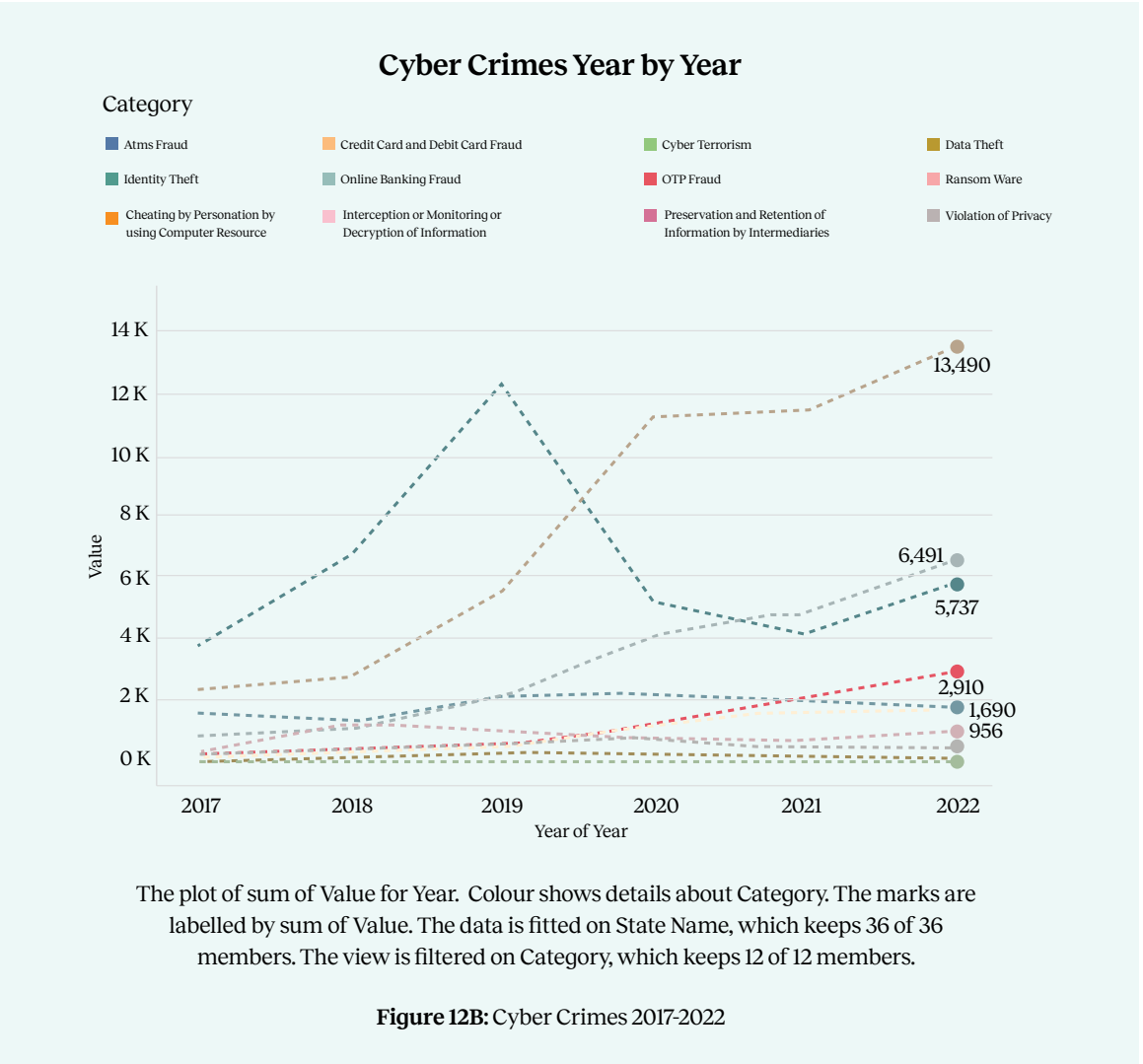
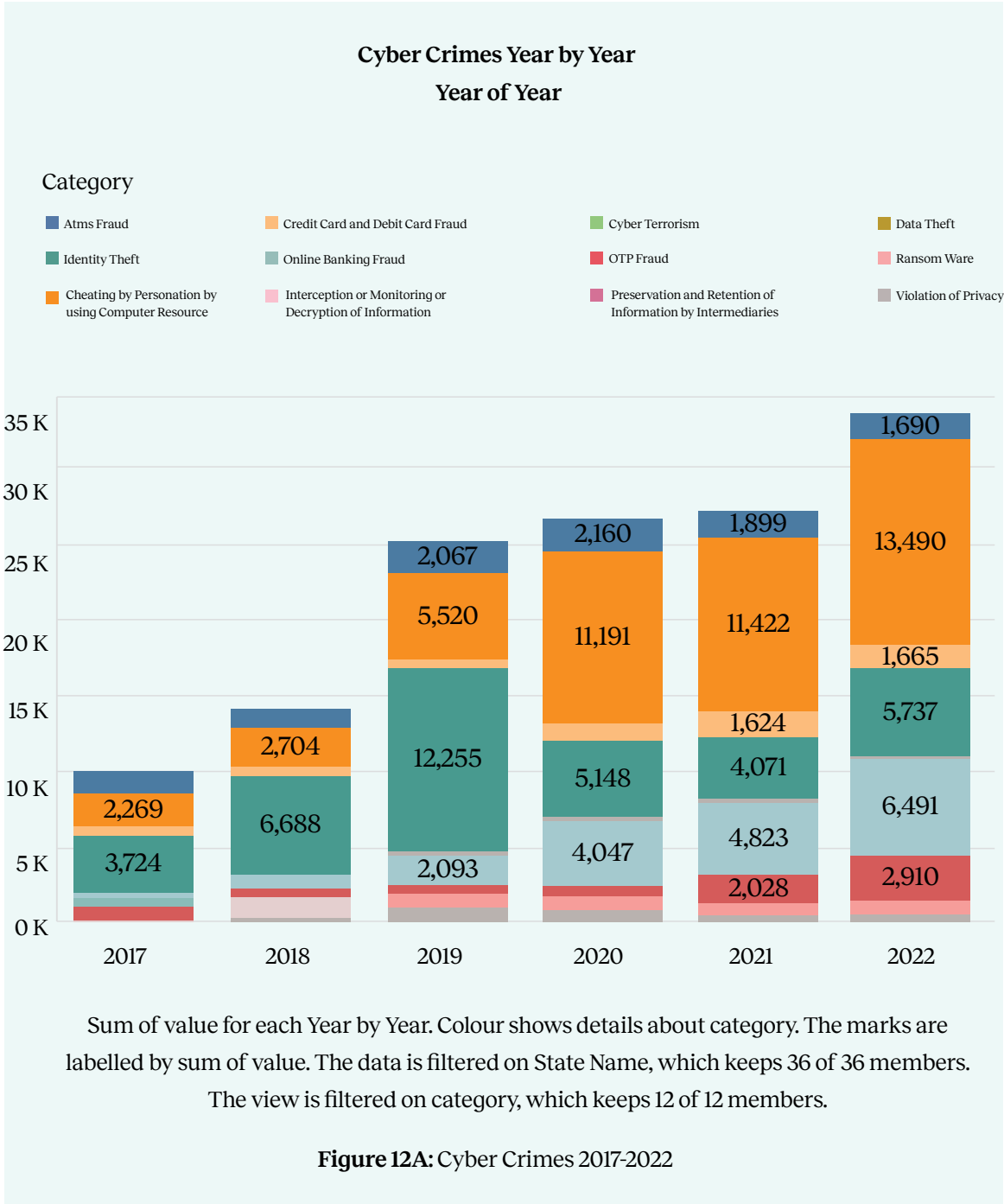


Table 1: Cyber Crime Trends

Yearly Trend of Overall Crimes

Year of Year	Total Crimes	Year Over Year % Change
2017	9,951	
2018	14,039	41.08%
2019	25,006	78.12%
2020	26,494	5.95%
2021	27,127	2.39%
2022	33,511	23.53%

Total Crimes and Year Over Year % Change broken down by Year over Year. The data is filtered on Category, District Name and State Name. The Category filter keeps 12 of 12 members. The District Name filter keeps 12 of 12 members. The state Name filter keeps 36 of 36 members.

Chapter 2

The Banking Ecosystem: Structure, Stakeholders, and Interdependencies

Evolution of the Banking Industry in India

The banking industry has played an indispensable role in developing the Indian economy continuously evolving to meet the changing needs of customers while sustaining itself in the global economy. Dating back to around 1000 BC, banking has undergone significant transformations, incorporating innovations that have streamlined financial transactions and enhanced accessibility.

The Bank of Bombay, set up in 1720, is popularly considered as the first Indian bank, while the Bank of Hindustan, founded in Calcutta in 1770, was among the first modern Indian banks. Several banks established in the mid-1800s merged to form the Imperial Bank of India, which later came to be known as the State Bank of India. This period also saw the formation of several private banks, some of which continue to operate today. Apart from the establishment of the banking system, the emergence of commercial banks and the merger of banks have been significant developments in shaping the Indian banking ecosystem.

During the post-independence era, in 1969, the Indian government nationalised 14 commercial banks, significantly transforming India's post-independence banking industry. This move facilitated the expansion of bank branches and banking services across India. The post-independence era also witnessed the establishment of key financial institutions like NABARD to aid agriculture activities, EXIM to develop imports and exports, National Housing Board to fund housing projects, and SIDBI to finance small-scale Indian industries.

Currently, India has 11 nationalised banks, 21 private banks, one local area bank, 11 small finance banks (SFBs), 6 payment banks (PBs), 34 state cooperative banks, 43 Regional Rural Banks, and 44 foreign banks (<https://rbi.org.in/commonman/english/scripts/banksinindia.aspx>).



Mumbai got its first automated teller machine (ATM) in 1987. Since then, ATMs have steadily increased, giving customers the convenience of withdrawing money anytime. Today, ATMs offer various services, including account balance checks, bill payments, and cash deposits. As of February 2024, there are approximately 2.19 lakh ATMs in India.

The adoption of core banking systems marked a significant milestone in modern banking technology. These advancements have eliminated the need for customers to visit home branches for basic banking tasks. With the rise of digital banking, customers can now access banking services 24/7 from almost anywhere. Mobile and digital banking enable users to manage their accounts, transfer funds, and access various financial services with minimal human intervention.

Introduced in 2016, the Unified Payments Interface (UPI) has revolutionised the way Indians conduct financial transactions, ushering in an era of cashless payments while promoting a more inclusive financial system. UPI, a groundbreaking payment system, has catapulted India into a future powered by effortless digital payments. Today, the scan-and-pay UPI system is ubiquitous, facilitating transactions of all sizes- from high-value luxury purchases to a simple 10-rupee cup of tea. In October 2024 alone, UPI processed a remarkable INR 23.49 lakh crore (approximately USD 285 billion), facilitated by 16.58 billion transactions-a 45% increase from the previous year. With 632 banks connected to the platform; UPI has cemented its position as the dominant payment system in India. The security and convenience sought by individuals and businesses underscores UPI's crucial role in accelerating India's transition to a cashless economy.

Banking Ecosystem: A Holistic View

The banking ecosystem is a dynamic and interconnected network of institutions, individuals, regulations, and technologies that facilitate financial transactions, lending, and investment. Understanding its structure, key stakeholders, and the interplay between its components is essential for assessing its efficiency, resilience, and overall economic impact. This section examines the banking ecosystem’s supply chain, outlining the sequential stages of financial services delivery and identifying the key stakeholders whose actions and interactions shape its functionality and stability. Understanding this system requires an in-depth examination of its key components and their interactions.

Key Stakeholders in the Banking Ecosystem

- Banks: The central actors, offering various financial services.
- Customers (Individuals & Businesses): The end users of banking services.
- Central Banks: Oversee monetary policy, regulate banks, and maintain financial stability.
- Financial Regulators: Implement and enforce regulations (e.g., SEC, FCA).
- Technology Providers: Supply software, hardware, and other technologies.
- Payment Networks: Facilitate electronic payments (Visa, Mastercard, etc.).
- Clearing Houses: Settle transactions between banks.
- Financial Market Infrastructure (FMI): Provide essential services for financial markets.
- Insurance Companies: Provide risk mitigation services.
- Auditors & Consultants: Offer advisory services and conduct audits.
- Investors: Provide capital to banks.



Banking Ecosystem and Supply Chain

The banking ecosystem requires a sophisticated supply chain with diverse stages involved in the ultimate delivery of financial services. These sequential stages begin with customer needs and demand and culminates with technology infrastructure and regulatory compliance.

Customer Needs & Demand

The ‘Customer Needs & Demand’ stage is the foundational element driving the entire banking ecosystem. Customer needs are diverse and vary significantly based on demographics, life stage, financial goals, and risk tolerance. Customers demand various financial services, such as deposits, loans, investments, payments, etc.

Funding & Capital Acquisition

The ‘Funding & Capital Acquisition’ stage is critical for a bank’s operational viability and growth. Banks require a constant inflow of capital to fund their lending activities, operational expenses, and investments in technology and infrastructure. They borrow from other banks (interbank lending), central banks, or issue bonds in capital markets.

Product & Service Development

Based on customer needs, banks develop and refine financial products (e.g., savings accounts, mortgages, credit cards) and services (online banking, mobile payments). This involves extensive market research, product design, and pricing strategies, all subject to regulatory compliance.

Technology & Infrastructure

The ‘Technology & Infrastructure’ stage is paramount for modern banking operations, impacting nearly every aspect of a bank’s activities. It involves the core banking systems (CBS), payment systems integration, cyber security, and data centers, and cloud computing.



Core Banking Systems (CBS): These are the central nervous systems of banks and consist of comprehensive software applications that manage all core banking functions, including:

- **Account Management:** Creating, updating, and managing customer accounts (checking, savings, loans, etc.).
- **Transaction Processing:** Recording and processing all types of transactions (deposits, withdrawals, transfers, payments).
- **Loan Management:** Managing the entire loan lifecycle, from origination to repayment.
- **Customer Relationship Management (CRM):** Storing and managing customer data to personalise service and marketing efforts.
- **Reporting and Analytics:** Generating reports on various aspects of bank operations and performance.

The core banking systems (CBS) are typically complex enterprise-grade systems, often purchased from specialised technology vendors. Implementing and maintaining a CBS requires significant investment in hardware, software, and skilled personnel. Outsourcing the management of these systems to technology providers is common, particularly for smaller banks that lack internal expertise or resources. This outsourcing reduces capital expenditure and allows banks to focus on their core business while relying on specialised vendor expertise.

Payment Systems Integration: Efficient and secure payment processing is a critical aspect of modern banking. Banks integrate their systems with various payment networks like:

- **Visa and Mastercard:** For processing credit and debit card transactions.
- **UPI (Unified Payments Interface):** For processing real-time peer-to-peer (P2P) payments in India.
- **SWIFT (Society for Worldwide Interbank Financial Telecommunication):** For processing international wire transfers.
- **ACH (Automated Clearing House):** For processing electronic payments and direct debits.

Integration with these networks requires specialised software, secure communication protocols, and adherence to industry standards. This ensures that transactions are processed quickly, efficiently, and securely. Disruptions in payment processing can significantly impact a bank's operations and reputation.

Cybersecurity: The banking sector is a prime target for cyberattacks. Robust cybersecurity infrastructure is essential to protect against data breaches, fraud, and system disruptions. This involves:

- **Network Security:** Implementing firewalls, intrusion detection systems, and other security measures to protect the bank's network from unauthorised access.

- **Data Security:** Encrypting sensitive data both at rest and in transit stages to prevent unauthorised disclosure.
- **Application Security:** Securing banking applications from vulnerabilities that attackers could exploit.
- **Identity and Access Management (IAM):** Implementing strong authentication and authorisation controls to restrict access to sensitive systems and data.
- **Incident Response Planning:** Developing and regularly testing procedures to handle security incidents effectively.
- **Vulnerability Management:** Regularly scanning systems for vulnerabilities and patching them promptly.

Cybersecurity is often managed by specialised firms that possess advanced expertise in threat detection, prevention, and response. The continuous evolution of cyber threats necessitates ongoing investment in cybersecurity infrastructure and personnel.

Data Centers & Cloud Computing: Banks and financial institutions manage vast amounts of sensitive customer data, requiring robust data storage and management capabilities that entail using:

- **On-Premise Data Centers:** Maintaining physical data centers to store and manage data internally. This offers greater control but requires significant investment in hardware, software, and personnel.
- **Cloud Computing:** Utilising cloud services from providers like AWS, Azure, or Google Cloud to store and manage data. This can offer cost savings and scalability but requires careful consideration of security and data privacy implications.

Transaction Processing: Transaction processing is a core operational function of banking, encompassing the secure and efficient handling of financial transactions. This includes deposit processing, loan origination, payment settlements, and investment management. The payment processing stage involves managing various payment methods, such as:

1. ATM Transactions
2. Online Banking Transfers
3. Mobile Payments
4. Card Payments
5. Cheque Processing
6. Wire Transfers

The Interconnected Banking Ecosystem: A Landscape of Cybersecurity Risks and Vulnerabilities

The interconnectedness of the banking ecosystem, while fostering efficiency and innovation, significantly amplifies cybersecurity risks. A breach at one point in the system can have cascading effects, affecting numerous stakeholders and potentially destabilising the entire financial ecosystem. It is thus important to identify the cyber risks and vulnerabilities arising in this complex ecosystem, some of which are listed below.

Third-Party Risk: Modern banking relies heavily on third-party vendors for critical services, such as technology infrastructure, payment processing, cloud storage, cybersecurity solutions, etc. While these partnerships enhance efficiency, they also expand the attack surface, creating multiple vulnerabilities.

- **Vendor Vulnerabilities:** A security weakness or breach at a vendor (e.g., a core banking system provider, payment processor, or cloud service provider) can directly impact the bank. Such incidents can expose sensitive customer data, disrupt transactions, and cause reputational damage.
- **Supply Chain Attacks:** Attackers increasingly target third-party vendors to gain indirect entry into larger systems. A compromised vendor can serve as an entry point to the bank’s network and data, often bypassing the bank’s direct security measures. Vendors with less robust security practices are particularly vulnerable to such breaches.

- **Lack of Transparency and Visibility:** Banks often lack complete visibility into their vendors’ security practices, making risk assessment difficult. Contracts may not explicitly define security responsibilities, leaving grey areas and potential liabilities.
- **Contractual Gaps and Liability:** Agreements with vendors may not adequately address liability in the event of a breach. Clearly defining responsibilities for data security, incident response, and financial compensation in the event of a compromise is critical but often overlooked.

Data Exposure from Interconnected Systems: The constant exchange of data between various stakeholders (banks, customers, payment processors, clearing houses, merchants, etc.) creates several vulnerabilities.

- **Data Breaches at Payment Processors:** A breach at a payment processor (e.g., compromise of card details) affects multiple banks and numerous customers. These processors handle vast amounts of sensitive data, making them high-value targets.

- **Cloud Data Breaches:** Banks and vendors store data in cloud environments, which can be compromised if security configurations are inadequate or in case of a security breach. Misconfigured or insufficient access controls at cloud service providers pose significant risks.
- **API Vulnerabilities:** Application Programming Interfaces (APIs) are commonly used for data exchange between different systems. Exploiting vulnerabilities in APIs can provide attackers with unauthorised access to sensitive data or control over systems.

Systemic Risk from Interdependencies: The interconnected nature of the financial system means a cyberattack on one institution can have widespread consequences.

- **Contagion Effect:** A successful attack on one bank can spread rapidly to others through shared systems, payment networks, or interbank transactions, creating a systemic risk, threatening the stability of the entire financial system.
- **Ripple Effects:** Even a seemingly minor disruption (e.g., a temporary outage at a payment processor) can have significant ripple effects, impacting numerous banks, businesses, and individuals. Interruptions in payment flows can have widespread economic consequences.

Human Factors across the Ecosystem: Human error and malicious intent can compromise security at any point in the banking ecosystem’s supply chain.

- **Insider Threats:** Bank or vendor employees may unintentionally expose

data or intentionally engage in data theft or sabotage. Strong internal controls, employee background checks, and security awareness training are crucial.

- **Phishing and Social Engineering:** Cybercriminals can manipulate employees at all levels into divulging credentials or downloading malware. Continuous security awareness training and robust security awareness programs are necessary to mitigate these risks.

Regulatory Compliance Challenges: Banks must navigate a complex regulatory environment across different jurisdictions.

- **Conflicting Regulations:** International Banks face a patchwork of regulations, creating complexities in maintaining consistent security standards across different regions.
- **Keeping Pace with Evolving Threats:** Cybersecurity threats evolve constantly, requiring banks and vendors to continuously update their security measures. Keeping up with the latest threats and vulnerabilities remains an ongoing challenge.
- **Enforcement Challenges:** Regulatory oversight is challenging in a global financial system, requiring international cooperation to ensure effective enforcement.

The interconnected nature of the banking ecosystem necessitates a proactive and collaborative approach to cybersecurity. Ignoring these vulnerabilities can have catastrophic consequences for individual institutions and the stability of the entire financial system. The advent of quantum

computing presents a significant and evolving set of cybersecurity risks to the banking ecosystem, exacerbating many of the existing vulnerabilities described above. Once sufficiently powerful, quantum computers will be able to break widely used public-key cryptography algorithms (like RSA and ECC) that are currently used to secure online banking, transactions, and data storage. This presents a profound threat to the confidentiality, integrity, and authenticity of financial data, impacting numerous stakeholders.

Compromised Confidentiality: Once quantum computers reach sufficient computational power, they can pose a direct threat to the confidentiality of data currently protected by widely used public-key cryptography algorithms like RSA and ECC. This has significant consequences.

- **Customer Data Exposure:** Personal and financial information of millions of customers, such as account numbers, balances, transaction histories, addresses, social security numbers, will become vulnerable to decryption. This could result in large-scale identity theft, financial fraud, and severe reputational damage for financial institutions.
- **Internal Data Breaches:** Confidential information stored by the banks, such as financial statements, strategic plans, and sensitive business information, could be decrypted, leading to financial losses and regulatory penalties.

- **Transaction Data Manipulation:** Attackers could intercept and decrypt ongoing financial communications, allowing them to manipulate transactions or commit fraud. This could range from unauthorised fund transfers to the alteration of transaction records.

Undermined Integrity: The ability of sufficiently advanced quantum computers to break current cryptographic algorithms directly undermines the integrity of financial data.

- **Transaction Tampering:** Malicious actors could alter transaction details (amounts, dates, recipient information) without detection, leading to significant financial losses and no trace of the fraudulent activities. In such a scenario, attackers could alter payment amounts, change transaction recipients, or create false transactions.
- **Data Falsification:** Attackers could alter sensitive information stored in databases without leaving readily detectable traces, leading to inaccurate records and compromising the reliability of financial statements. This could have severe consequences for regulatory compliance, financial reporting, and auditing.
- **Forged Digital Signatures:** Digital signatures, widely used to authenticate documents and transactions, rely on current cryptographic algorithms. Quantum computers could potentially forge these signatures, enabling fraudulent activities and creating legal and financial disputes, undermining the trustworthiness and verifiability of critical documents.

Erosion of Authentication: Current security measures in online banking and other financial services rely heavily on cryptographic authentication methods. Quantum computers pose a serious threat to the integrity of these systems.

- **Mass Identity Theft:** The ability to crack cryptographic algorithms used in authentication protocols could allow attackers to gain unauthorised access to customer accounts en masse. This could lead to widespread identity theft and substantial financial losses.
- **System Intrusions:** Attackers could potentially bypass security mechanisms and gain control of banking systems and networks, allowing them to manipulate data, initiate fraudulent transactions, and cause widespread disruption. This represents a significant threat to operational stability.
- **Compromised Access Controls:** The security of access control systems within banking institutions would be severely compromised, potentially giving attackers unrestricted access to various systems and data.

Increased Systemic Risk: The widespread use of cryptographic algorithms creates a significant systemic risk. A successful quantum attack on one institution would have far-reaching consequences.

- **Contagion via Interconnected Systems:** The interconnected nature of the banking ecosystem means that a successful attack on one bank could quickly spread to others through shared payment networks, data exchange systems, and interbank

transactions. The potential for rapid and widespread disruption is extremely high.

- **Erosion of Public Trust:** A large-scale quantum-driven breach would drastically erode public trust in the financial system, potentially leading to bank runs, reduced investment, and economic instability. The consequences could extend far beyond the immediate victims of an attack.

Impact on Third-Party Vendors: Banks rely on third-party vendors for essential services, but these vendors are also at risk.

- **Supply Chain Vulnerabilities:** Quantum threats could compromise vendors providing payment processing, cloud computing, and cybersecurity solutions, leading to indirect breaches of banks' systems.
- **Vendor Liability:** Vendors who fail to implement robust data security measures will have to face significant legal and financial consequences of breaches caused by quantum computing capabilities.

Addressing the quantum computing threat requires a coordinated response from the banking industry and regulatory bodies. The transition will demand extensive planning, testing, and phased implementation. Investing in quantum-resistant hardware and software is essential, including updating cryptographic libraries, upgrading network infrastructure, and securing cloud environments. Open communication and collaboration between banks, vendors, and government agencies is crucial for effective threat response and coordinated mitigation efforts. Governments and regulatory bodies must establish clear guidelines and standards for the adoption of

PQC (Post-Quantum Cryptography) and the management of quantum-related risks. The quantum computing threat is not a distant concern but a rapidly approaching reality. Proactive and comprehensive strategies are essential to safeguard the integrity, security, and the stability of the global financial system. Failure to address this challenge effectively could have far-reaching and potentially catastrophic economic consequences.

In Chapter three, the authors describe the cryptographic frameworks, identify risks arising from quantum computing, identify the time-lines of banking data and propose a hybrid model for migration to Post-Quantum Cryptography.

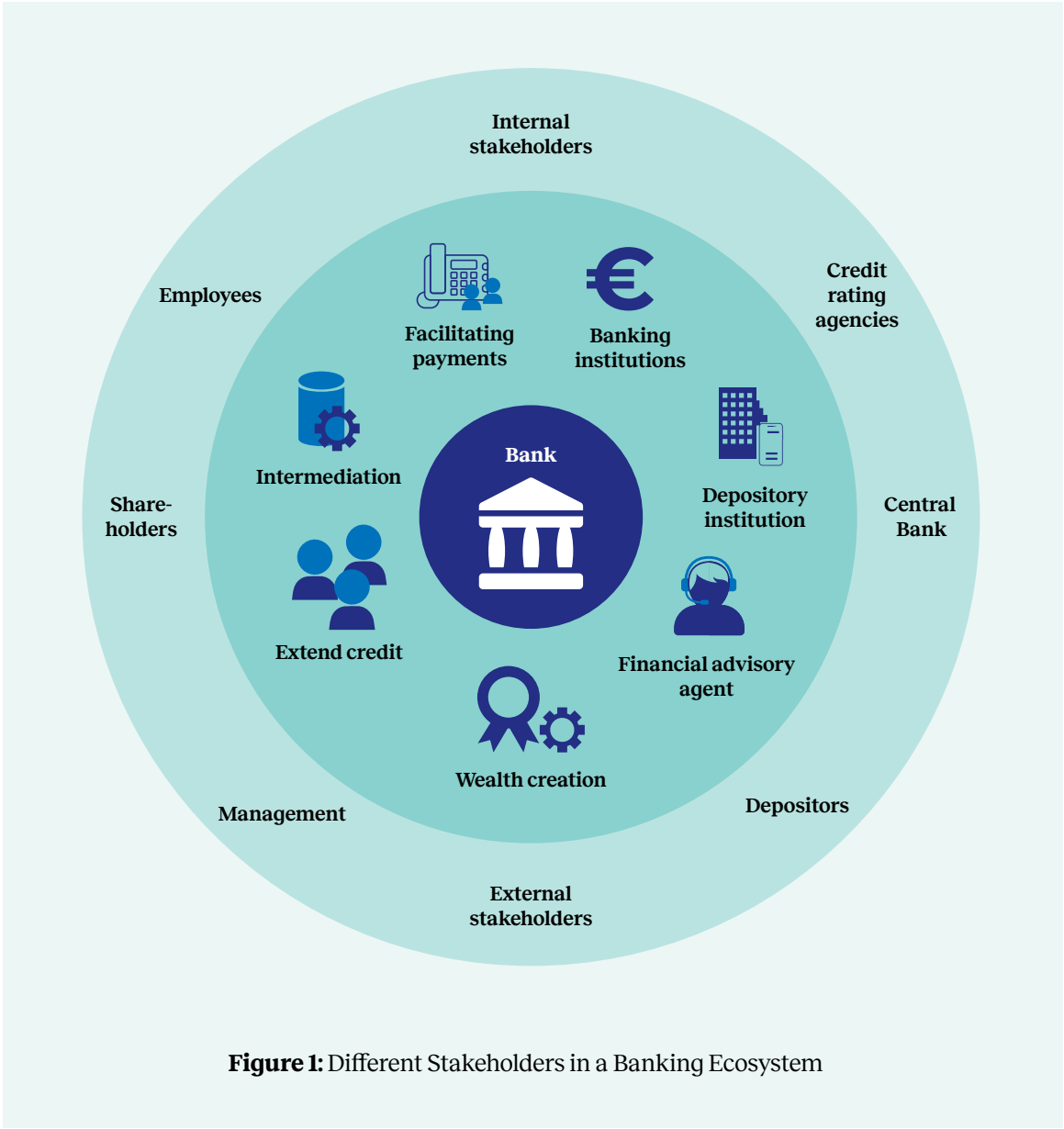


Figure 1: Different Stakeholders in a Banking Ecosystem

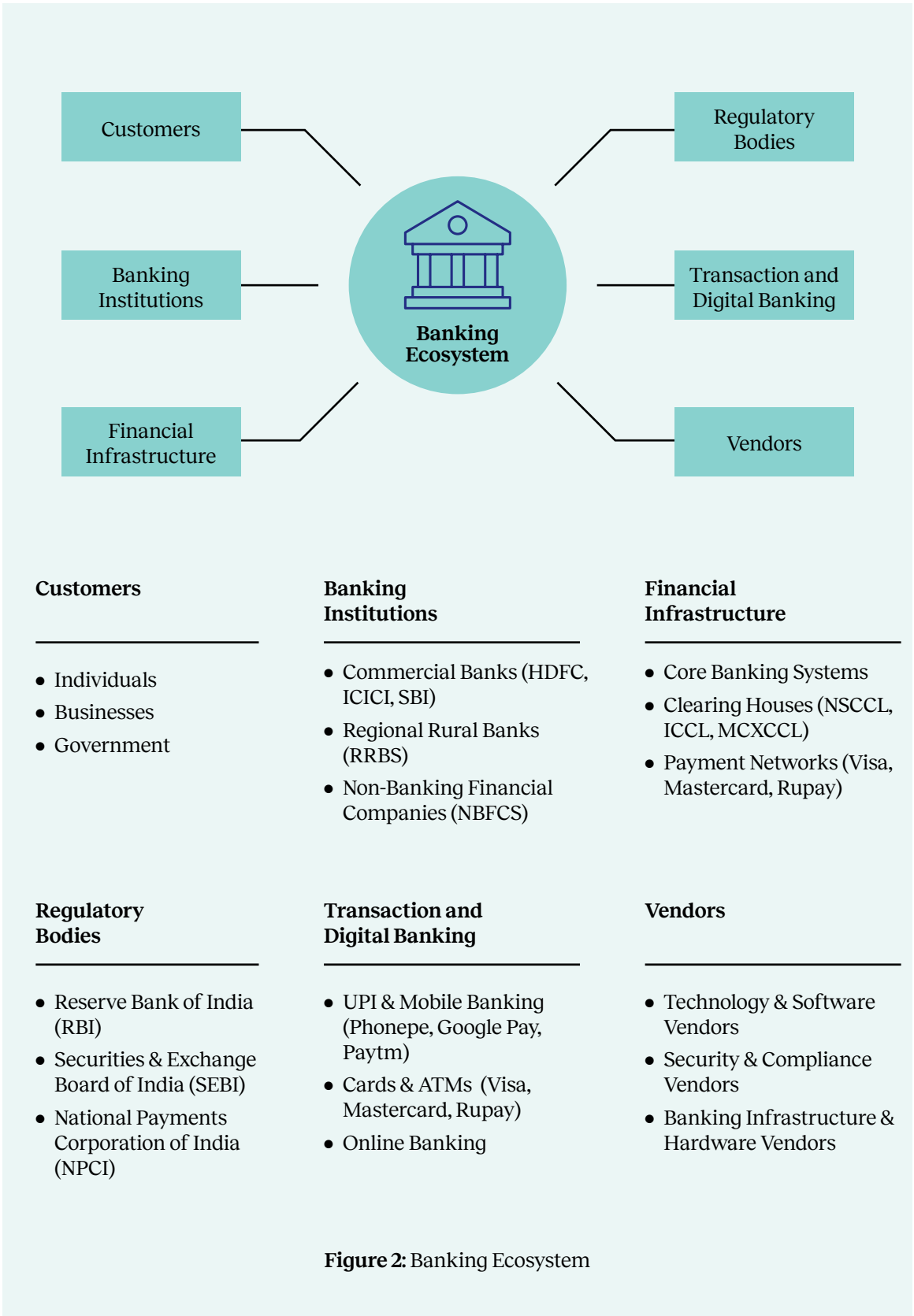


Figure 2: Banking Ecosystem

Chapter 3

Navigating Data Security: Strategies for Quantum Readiness in the Banking and Financial Sector

Strategising for the Future: Preparing for Post-Quantum Cryptography

Quantum computing has the potential to tackle complex problems that surpass the capabilities of current high-performance computers, potentially advancing fields like life-saving drug development and sustainable battery technology. However, this powerful technology also presents serious cybersecurity threats. Highly precise, error-corrected quantum computers are expected to outperform current encryption. According to a McKinsey report (<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography>), experts predict that the first fully error-corrected quantum computers could debut as early as 2030. Once fully error-corrected quantum computers become available, the threat level to existing protocols will transform as these quantum systems will be able to decrypt widely used asymmetric security protocols, such as RSA and elliptic curve algorithms. These existing protocols are primarily utilised to securely distribute messages (or keys) over public networks like the internet, where anyone can encrypt a message, but only the original sender possesses the key needed for decryption. However, quantum computing will enable the decoding of encrypted messages without this key, rendering them vulnerable.

Conversely, symmetric encryption protocols—where the sender and receiver exchange encryption and decryption keys prior to sharing information—are believed to be secure from quantum threats. However, the need to securely transfer cryptographic keys beforehand often renders these protocols impractical for rapid data exchange across public networks. Managing the large number of keys required for exchanging numerous messages also translates into significant computational costs. Hence, the effective distribution of symmetric keys is a critical hurdle to overcome for successful protocol implementation.

The era of post-quantum cryptography (PQC) has already begun for many companies, particularly those in the banking and financial sectors. Banks and financial institutions will be expected to uphold high security standards to ensure user safety and privacy throughout their operational lifespan, which could extend beyond 2040, by which time experts predict that error-corrected quantum computers will be available. Unlike previous cyber threats addressed by simple protocol updates, quantum computing will fundamentally compromise some protocols and cartographic models, requiring companies to invest significant time and resources into substantially upgrading their security measures. While some of the currently used and stored data may remain unaffected, the security of large volumes of data, critical systems, and flagship products remains at risk. Security leaders should start by answering these two crucial questions: (i) When should they initiate mitigation efforts, and (ii) How can they protect their organisational data and systems?

The timing for migration and implementation will vary across industries and within organisations depending on the data shelf life. Recognising the significance of cybersecurity is typically the first step in conventional security assessments, both for overall protection and the safeguarding of specific systems and products. Evaluating the value exposed to risks is crucial for developing effective strategies to combat threats and respond to potential security breaches.

As fully error-corrected quantum computers are not yet available, quantum security strategies must begin with considerations of timing. Risk managers should closely analyse two critical aspects of high-priority assets: (i) Data shelf life and system life and (ii) Development cycles—to decide when to implement quantum mitigation measures.

Data shelf life and system life cycle are two factors banking and financial institutions need to consider while formulating strategies for PQC implementation. If we take data shelf life into consideration, then data produced today—such as long-term life insurance contracts—may already be susceptible to future quantum threats because it could still be active when quantum computers become commercially available. Similarly, customer financial records maintained by banks, especially those containing sensitive personal information, could remain in use for several years and therefore be vulnerable if not secured against quantum decryption (Fig. 2). Historical transaction data kept by financial institutions for auditing and compliance purposes could also be a target for quantum threats, as it may reveal sensitive patterns or insights into customer behaviour years after its generation. Trade secrets held by banks related to proprietary algorithms and trading strategies could also be at risk if these secrets remain accessible through less secure channels. Any current long-term data that is transferred over public channels will be at risk of interception and future decryption (Fig. 3).

The banking ecosystem has diverse types of data, and each data point has a different shelf-life depending on its type, regulatory requirements, and business needs (Fig. 2). There is no single “data shelf life” applicable to all the data. The different types of banking data are:

Transactional Data: Transactional data points are directly related to financial transactions, such as deposits, withdrawals, payments, and transfers. This type of data has a short shelf life, which typically ranges from 5 years to 10 years. The time period after which transactional data can be archived depends on:

- **Regulatory Requirements:** Many jurisdictions have regulations mandating the retention of transactional data (e.g., for tax purposes, audit trails, or fraud investigations) for a specific period. These requirements vary by region and type of transaction.
- **Business Needs:** Banks might keep transactional data beyond the minimum regulatory requirements for internal analysis, fraud detection, and customer service purposes.
- **Data Archival:** After the required retention period, transactional data may be archived to reduce storage costs and improve data management efficiency.

Customer Data: Apart from a variety of personal information, like biometric, KYC, and financial details, customer data can include:

- **Account Information:** This includes details like account numbers, balances, and transaction history. Its shelf life is like transactional data, typically a few years

to seven years, guided by regulations and business needs.

- **Personal Information:** This includes details such as name, address, contact details, date of birth. Retention periods for this data are often extended, sometimes indefinitely, particularly for KYC/AML compliance and potential legal disputes.
- **Loan Application Data:** Requirements like credit history and legal reasons entail the retention of loan application data for extended periods, frequently exceeding the loan repayment timeframe by many years.

Marketing and Sales Data: This data pertains to records of customer interactions, marketing campaigns, and sales activities. Unless legally required, data is typically retained for shorter periods, usually **one to three years**.

Risk Management Data: Data related to credit risk, market risk, operational risk, and regulatory compliance is often kept for longer periods, typically **seven to ten years or longer**, for internal analysis, audits, and potential litigation. The shelf life of this type of data is influenced by specific regulatory requirements and the length of potential legal ramifications.

Audit Data: Data related to internal audits, regulatory audits, and financial audits is usually retained for **seven to ten years or longer**, in compliance with audit trails and regulatory requirements.

Strategic and Business Data: Data used for strategic planning, market analysis, and business decision-making generally has a longer shelf life, sometimes **indefinitely**, based on its ongoing relevance.

The shelf life of data in the banking ecosystem is highly variable, governed by a complex interplay of regulatory requirements, business needs, and data minimisation principles. Responsible and ethical handling of data throughout its lifecycle is crucial for maintaining customer trust, complying with regulations, and mitigating security risks. The Data Shelf Life Table for Banks and Financial Institutions serves as a comprehensive tool for assessing and managing the longevity and relevance of various types of financial data within an organisation. Table 1 categorises different data types commonly handled by banks and financial institutions, such as customer personal information, transaction records, loan documentation, regulatory compliance data, and so on. For each data type, the table provides a brief description to clarify its significance and purpose within the organisation. One of the critical elements of the table is the “Shelf Life” column, which indicates the estimated duration for which each type of data remains relevant and legally required. This helps institutions prioritise data management efforts and ensures compliance with data retention regulations.

The “Risk Assessment” column evaluates the potential risk involved if a particular dataset is compromised, ranging from low to very high. This assessment assists decision-makers in the identification of data that requires enhanced security measures and monitoring. To address

the looming threats posed by quantum computing, the “PQC Mitigation Strategy” column outlines suggested actions and strategies for transitioning to post-quantum cryptography (PQC) readiness. This proactive approach allows organisations to prepare for advancements in quantum technology and ensure the protection of sensitive data against future threats. Last, the “Review Frequency” column specifies how often data should be reviewed for relevance, compliance, and security. Regular reviews are crucial for maintaining data integrity and implementing necessary updates or changes to data management protocols.

Thus, banks and financial institutions must carefully assess the shelf life of their data and implement robust security measures to protect against emerging quantum threats. The decision-makers have three options: (i) migrate to post-quantum cryptography (PQC) solutions immediately, (ii) retrofit existing systems to meet PQC standards in the future, or (iii) focus solely on improving the effectiveness of traditional encryption protocols, while monitoring emerging industry standards and regulations (Fig. 7). The transition decisions will depend on when organisations need to begin mitigation, the performance requirements of cryptography protocols, and the number and distribution of connected devices and systems that require protection.

Option 1: Immediate Transition to Post-Quantum Cryptography

As referenced in Table 1 (Data Shelf-Life Management Table for Banks and Financial Institutions), some high-risk, indefinitely stored data types require immediate adoption of post-quantum cryptography (PQC).

1. **Customer Personal Information:** This type of data is constantly at exposure risk and remains relevant indefinitely. Safeguarding it using PQC is vital because a data breach could have severe repercussions.

2. **Account Information:** Given its indefinite relevance and high risk, it is essential to secure account data against future quantum threats.

3. **Investment Data:** The sensitive nature and indefinite shelf life of investment data necessitates strong protection measures to safeguard customer interests and proprietary information.
4. **Passwords and Security Keys:** The high vulnerability and critical nature of passwords and security keys for authentication demands a shift to PQC solutions.

5. **Loan Documentation:** Given its long-term nature (7-15 years) and high-risk profile, usage of PQC solutions is essential for securing sensitive agreements and collateral information from potential breaches.

Many startups and a handful of established cryptography firms are already offering provisional commercial post-quantum cryptography (PQC) solutions. While these options may seem ideal for organisations needing quick solutions, several trade-offs exist: (i) The first consideration is cost. According to the McKinsey Report, PQC solutions account for only about 2 percent of the global cryptography market as of now. This limitation will severely hamper organisations that need to secure large volumes of data, devices, and systems across their networks and protocols. (ii) Second, since PQC solutions are still in their early stages and cannot be rigorously tested against future quantum computers, their effectiveness in protecting against quantum or even conventional threats has not been definitively established. Therefore, organisations may have to invest in both traditional and PQC solutions to uphold the highest security level if they decide to progress today. Additionally, organisations might face the need to transition to higher-performance PQC solutions that become available over time, especially if options that are available currently are later deemed to be non-compliant with new regulations. (iii) Finally, existing PQC solutions demand significantly more computing power and have higher latency times compared with traditional standards. However, today’s PQC solutions might still be adequate for applications that do not have stringent latency requirements, such as non-urgent bank transfers or the transfer of insurance contracts.

Option 2: Future-proofing: Retrofitting Systems with Post-Quantum Cryptography

As discussed in Table 1., banks and financial Institutions, could consider the following data types when retrofitting systems with post-quantum cryptography (PQC) solutions at a later date due to their moderate risk assessment and defined shelf life.

1. **Transaction Records:** With a shelf life of 5-10 years and a medium risk assessment, organisations can plan to retrofit systems with PQC solutions, when necessary, rather than implementing them immediately.

2. **Regulatory Compliance Data:** This data, required for audits and oversight, has a shelf life of 5-10 years, allowing organisations to transition to PQC when the risks become imminent.

3. **Financial Statements:** Since financial statements are relevant for up to 7 years and carry a medium risk, organisations can choose to retrofit their systems with PQC solutions as the deadline approaches.

4. **Risk Assessment Reports:** As these reports have a shelf life of 5 years and are at moderate risk, organisations can manage retrofitting efforts in anticipation of evolving quantum threats.
- First, they have to ensure that their hardware and software architecture is designed for easy retrofitting. This can involve reserving computational resources for future cryptographic updates or creating a sufficiently modular architecture to facilitate the addition and replacement of cryptographic modules at a later date. In line with traditional security practices, hardware and software should be kept separate, allowing systems to remain adaptable to emerging PQC algorithms.

Second, banks and financial institutions should prepare both operationally and financially for the retrofitting process. They need to ensure that systems remain accessible for updates to post-quantum cryptography (PQC) solutions, even while they are active or widely distributed. While some changes could be implemented remotely through software updates, it is likely that high-performance PQC solutions will require specialised hardware, necessitating physical access to affected devices for retrofitting. Companies with large quantities of devices or systems, such as banks, may encounter operational challenges and high costs with this approach, underscoring the significance of immediate planning.

While these data types are important to secure, their moderate risk assessment and defined shelf life provide organisations the flexibility to implement PQC solutions later, while still maintaining current security measures. Planning for future retrofitting will ensure a smooth transition to quantum-safe security practices when the need arises. Nevertheless, banks and financial institutions have important steps to take now.

Option 3: Strengthening Security:
Emphasising Traditional Encryption Protocols

Banks and financial institutions may choose to only enhance traditional encryption protocols for marketing data and symmetric keys due to their lower risks assessments and shorter or ambiguous shelf life.

- 1. **Marketing Data:** This data type has a low risk assessment since it typically involves customer consent information for communications and is only relevant until consent is withdrawn. Enhancing traditional encryption protocols may be sufficient for its protection.
- 2. **Symmetric Key Lengths:** For specific applications involving symmetric keys, organisations could focus on enhancing current encryption methods to improve security without immediately transitioning to PQC solutions.

Strengthening traditional encryption is enough to secure these data types, delaying the need for PQC. This allows organisations to manage their resources effectively, while monitoring future developments in cryptography and quantum threats.

However, banks should still implement traditional mitigation strategies, particularly by extending asymmetric key lengths and utilising symmetric cryptography where feasible. Longer keys will help them stay ahead of the initial versions of error-corrected quantum computers, as breaking these keys will require significantly more qubits (the fundamental units of quantum computers). For instance, upgrading from RSA-1024 to RSA-2048 encryption can prolong security lifetimes

by one to three years. For added protection, organisations could also consider increasing the lengths of symmetric keys for more sensitive data. It is vital for decision-makers to plan for future updates on long-lasting systems by assessing the modularity of their technological architecture.

Additionally, certain banking systems, such as ATMs, will require ample time to prepare for quantum threats, as they must first be updated. The existing ATM infrastructure, including both hardware and software, does not support quantum computing. Consequently, ATM manufacturers may choose not to transition to post-quantum cryptography (PQC) in the near future. It's important to note that neglecting PQC-specific measures poses some risk to banks and their customers. Without investments in PQC, any application relying on asymmetric encryption will eventually be vulnerable to fully error-corrected quantum systems.

However, as with any risk, organisations must balance the costs of enhancing security against the potential costs of a breach. Thus, it's important for banks and financial institutions to identify the data shelf life and consider a hybrid approach for securing data and its systems. Identifying the data shelf life is crucial for the banks as it will help them understand how long various types of data remain relevant and valuable. By combining established encryption protocols with post-quantum cryptographic solutions, financial institutions can create a robust security framework that addresses current threats

while preparing for future challenges posed by advancements in technology, particularly quantum computing. For instance, while some data may be adequately protected through enhanced traditional encryption methods, other high-risk data may need the advanced protection offered by post-quantum cryptography (PQC).

This approach allows banks to adapt their security measures, acknowledging that some data require long-term protection while other data need only immediate attention. Implementing a hybrid approach allows organisations to balance their resources effectively, ensuring that they are not overly focused on one method of encryption at the expense of another. It leads to better risk management because institutions can concentrate their security efforts based on the assessed risk associated with different data types, thereby optimising their investment

in cybersecurity. As regulatory standards and industry best practices evolve, a hybrid strategy provides the agility needed to adapt to changing compliance requirements. It also prepares institutions for potential future threats associated with quantum computing, ensuring that their data remains protected against new attack vectors that may arise.

Recognising data shelf life and adopting a hybrid approach to security enables banks and financial institutions to create a comprehensive and flexible framework that not only addresses current risks but also positions them to respond proactively to emerging threats in the cybersecurity landscape. This strategic readiness is essential for maintaining customer trust and safeguarding sensitive financial data in an increasingly complex digital environment.

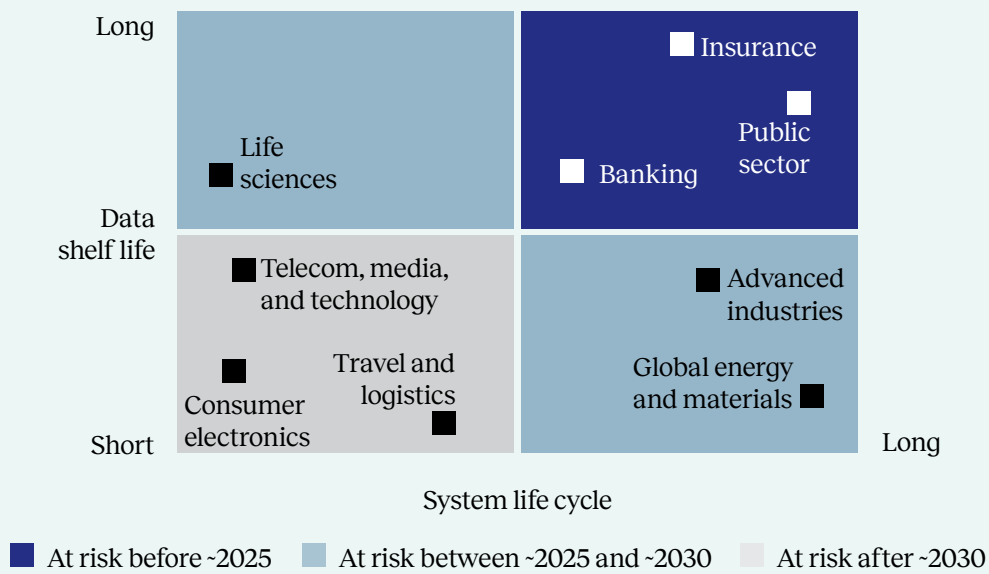


Figure 1: Data Shelf Life and System Lifetime for Different Sectors

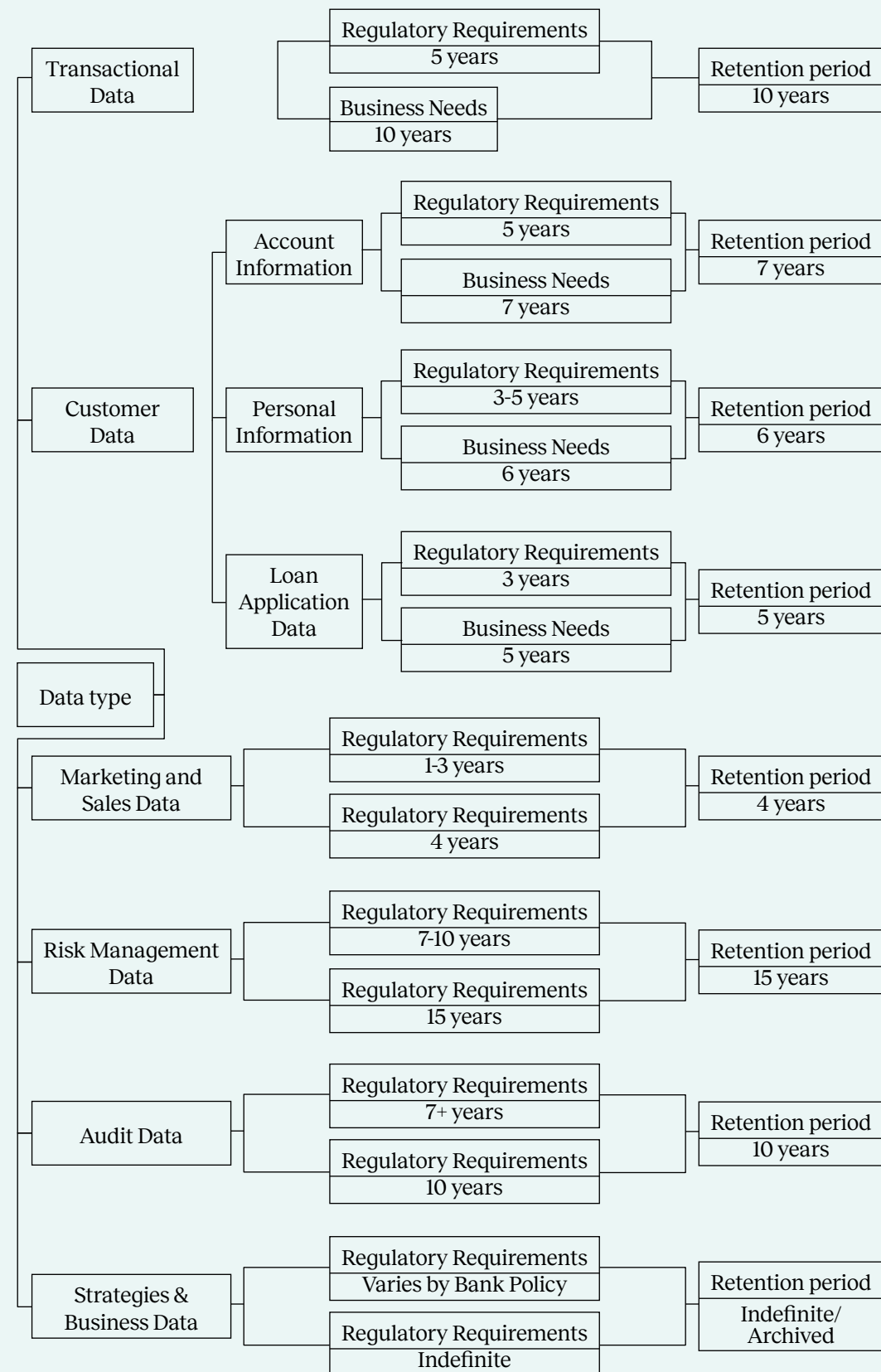


Figure 2: Data Shelf Life in the Banking Ecosystem

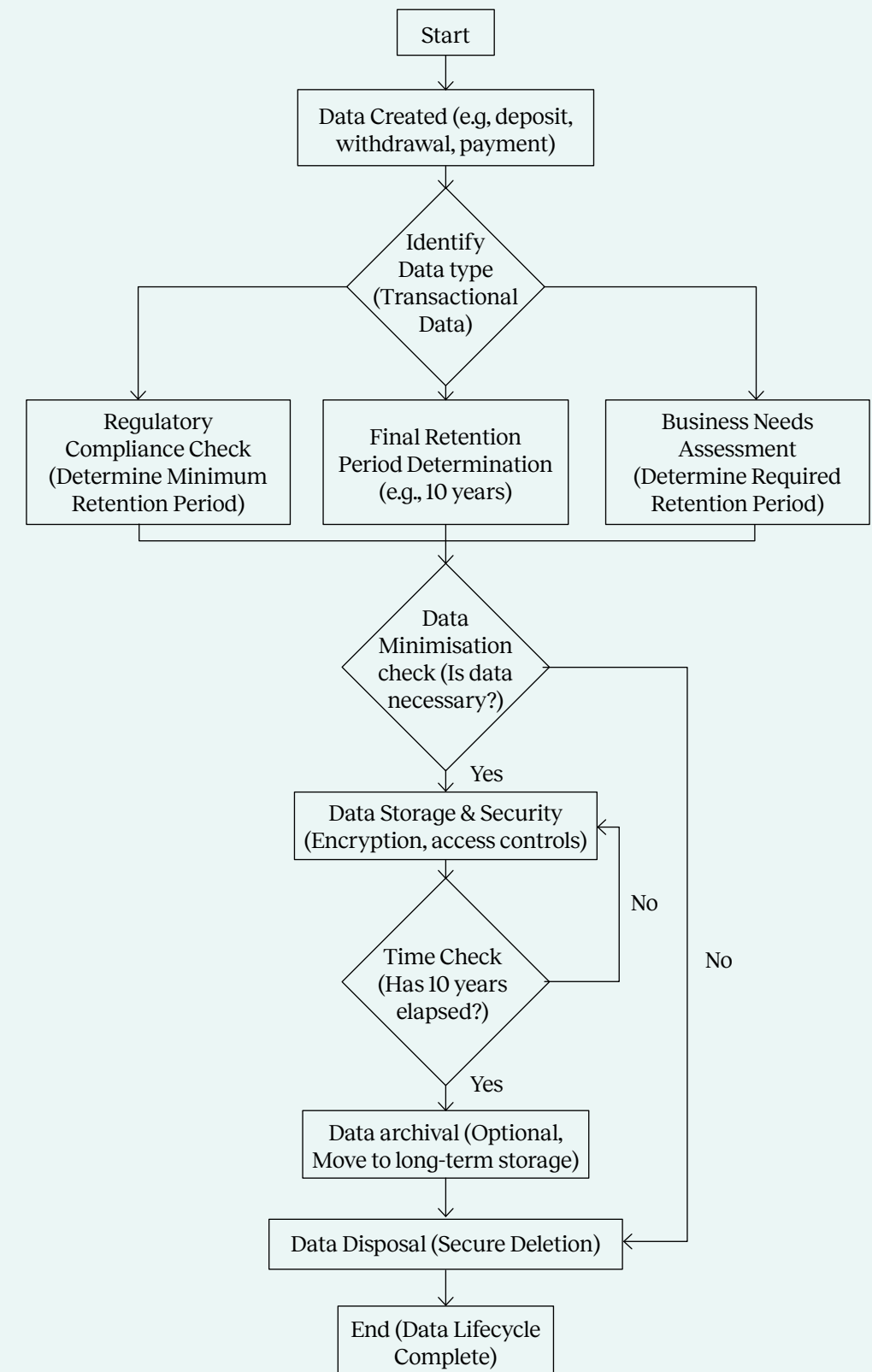


Figure 3: Transactional Data Lifecycle Management Process

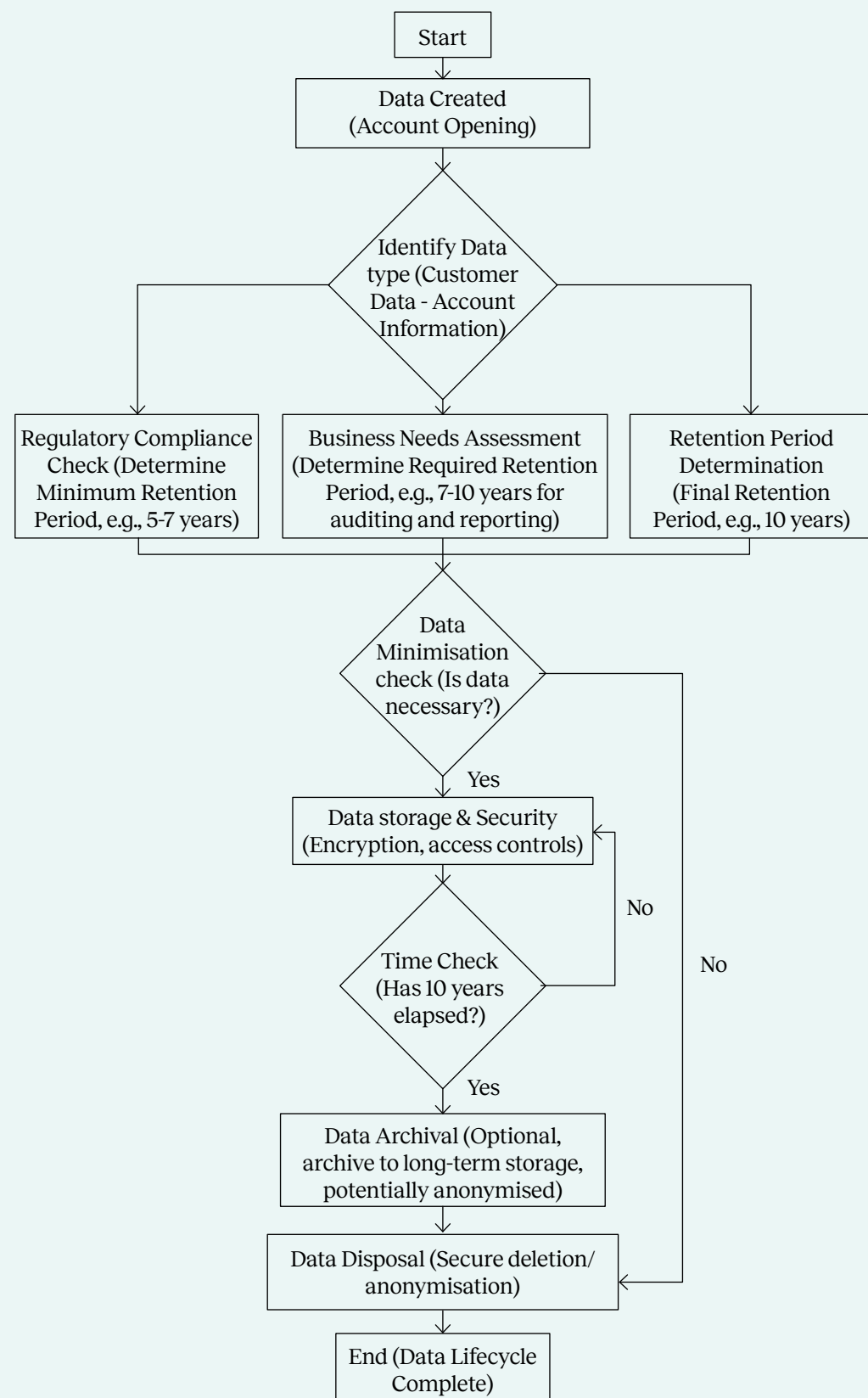


Figure 4: Customer Account Information Data Lifecycle Management Process

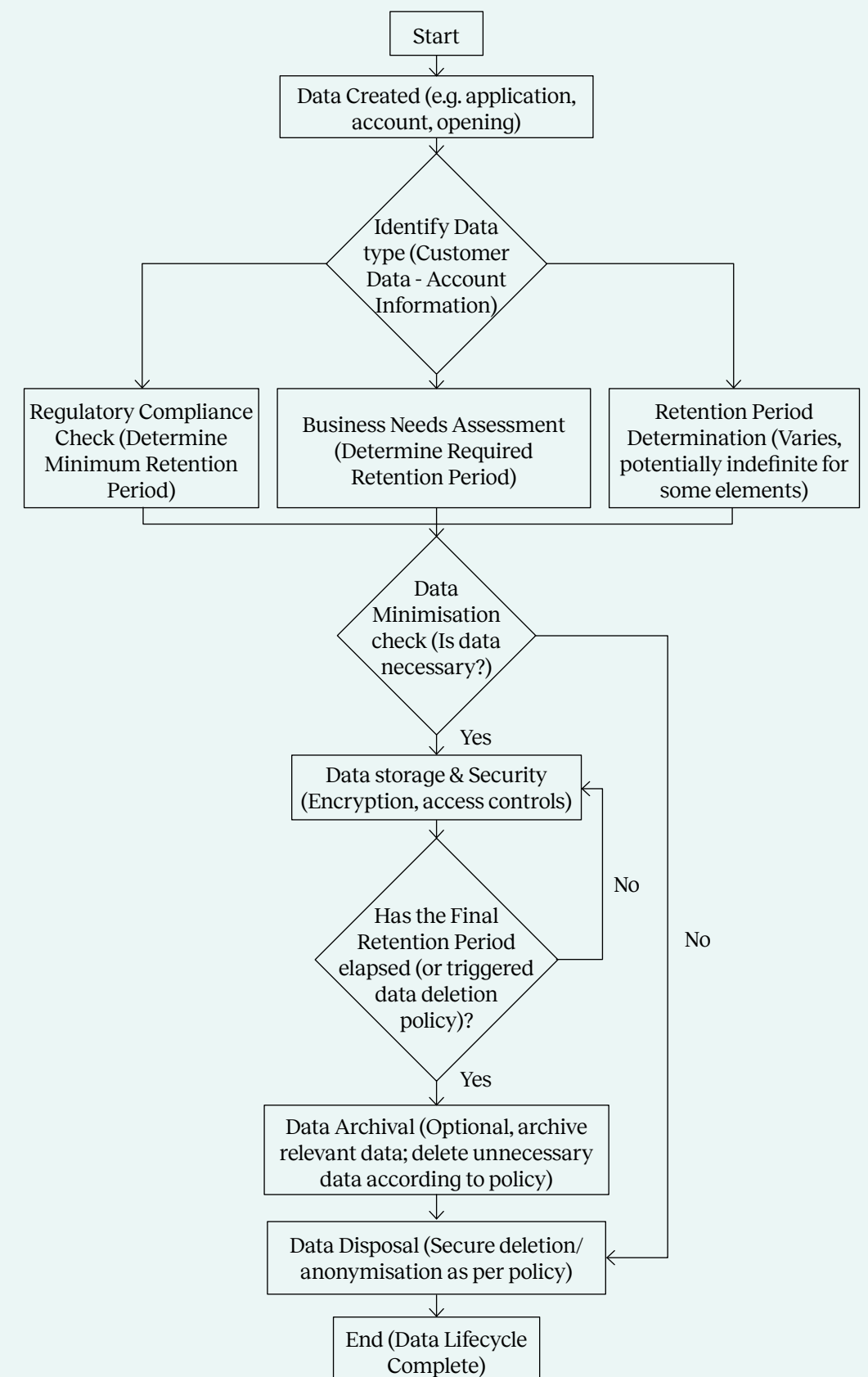


Figure 5: Customer Personal Information Data Lifecycle Management Process

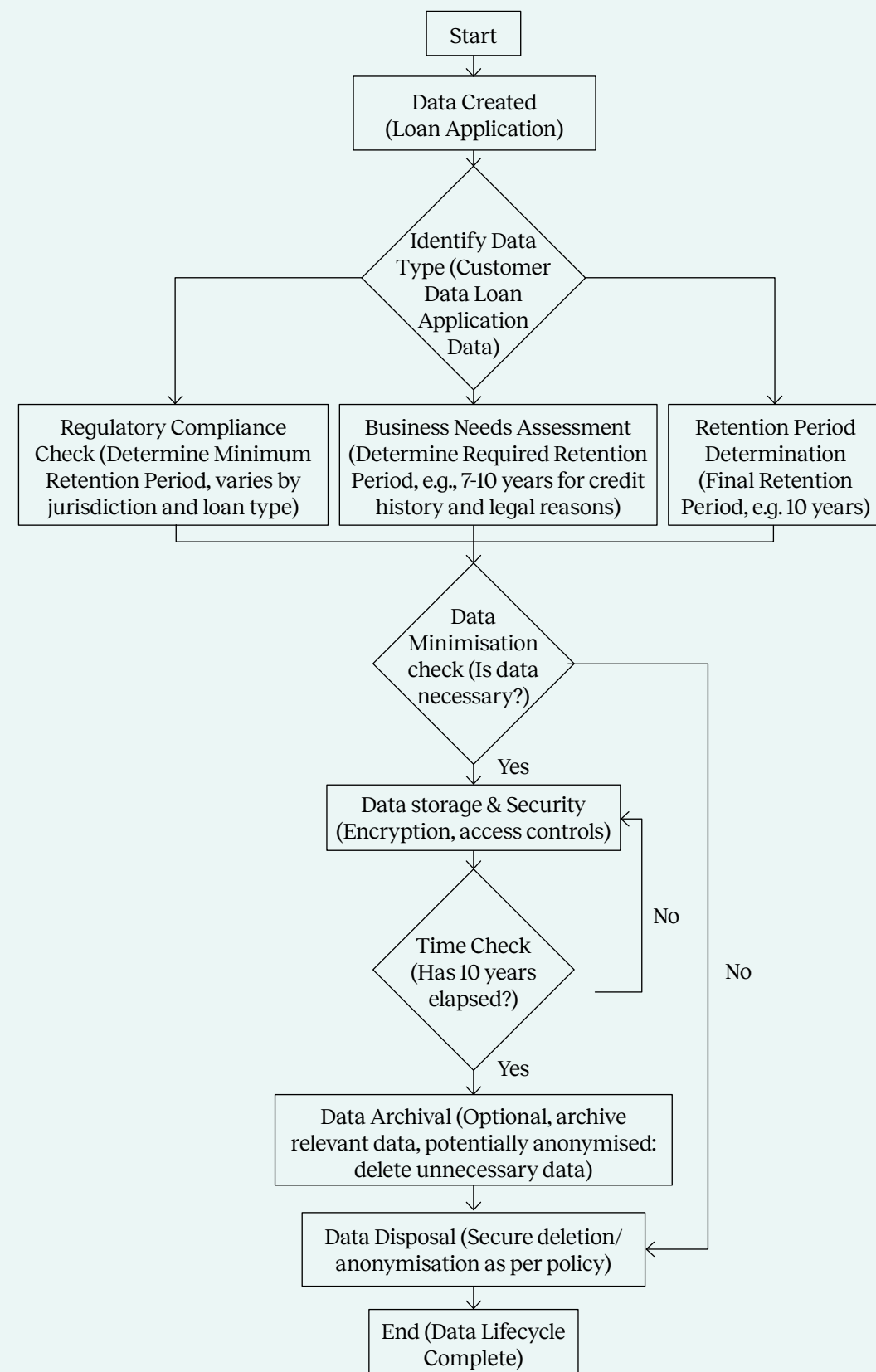


Figure 6: Customer Loan Application Data Lifecycle Management Process

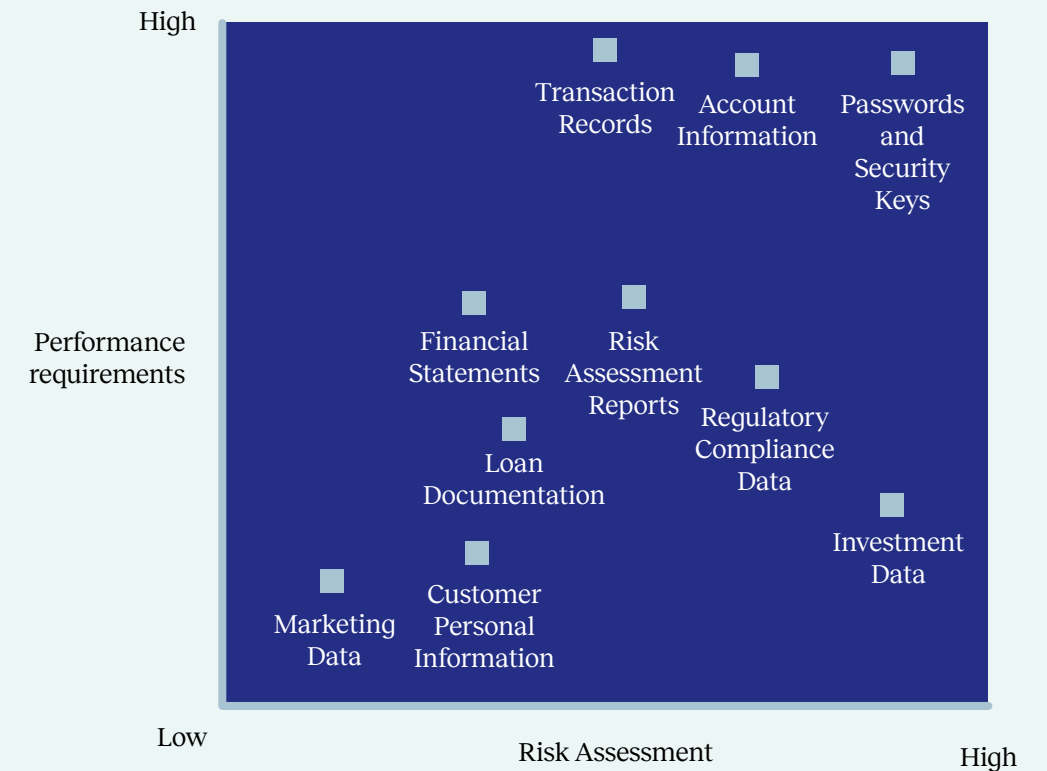


Figure 7: Risk Assessment vs. Performance Requirements for Different Data Types

Timelines for mitigation scenarios

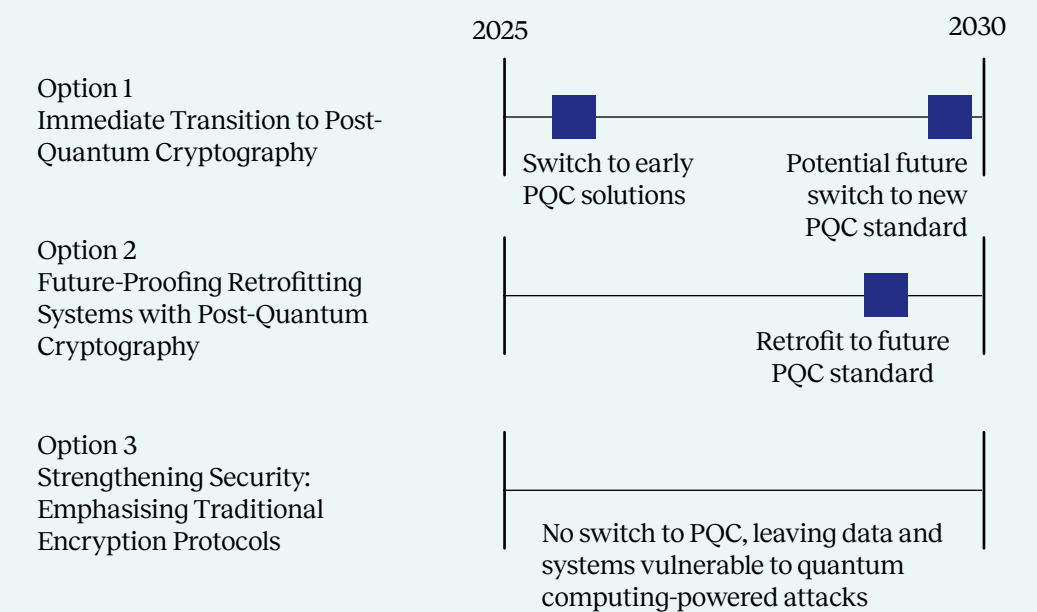


Figure 8: Timelines and Strategies for Post-Quantum Cryptography Mitigation

Table 1: Data Shelf Life Management Table for Banks and Financial Institutions:
Assessing Longevity, Risk, and Quantum Readiness

Data Type	Description	Shelf Life	Risk Assessment	PQC Mitigation	Review Frequency
Customer Personal Information	Names, addresses, dates of birth, KYC, biometric details	Indefinite	High	Upgrade encryption to PQC when available	Annually
Transaction Records	Details of customer transactions	5-10 years	Medium	PQC encryption today	Every 2 years
Account Information	Account numbers, balances, and types	Indefinite	High	Transition to PQC protocols	Annually
Loan Documentation	Contracts, agreements, collateral information	7-15 years	High	Secure storage with PQC considerations	Every 2 years
Regulatory Compliance Data	Data required for audits and regulations	5-10 years	Medium	Maintain secure access; utilize PQC	Quarterly
Marketing Data	Customer consent for communications and preferences	Until consent is revoked	Low	Encrypt with current standards	Annually
Financial Statements	Year-end summaries, audit reports	7 years	Medium	Secured archiving; PQC consideration	Every 5 years
Risk Assessment Reports	Evaluations of financial and operational risk	5 years	Medium	Keep updated; evaluate PQC needs	Every 2 years
Investment Data	Portfolio holdings, investment analysis	Indefinite	High	Potentially migrate to PQC	Annually
Passwords and Security Keys	User passwords and cryptographic keys	Until changed	Very High	Implement PQC-ready systems	Every 6 months



Chapter 4

Quantum Computing— Current Scenario and Future Outlook

Introduction

What is Quantum Computing?

Quantum computing is a revolutionary computing paradigm that harnesses the principles of quantum mechanics to solve problems beyond the reach of classical computers. Traditional computers process information using bits (0 or 1) which limits their ability to process complex information. Quantum computers, on the other hand, use the principles of quantum physics, like superposition, tunneling, entanglement, and interference. These systems rely on probabilities rather than fixed binary states of 0 or 1. Quantum computers use qubits (quantum bits), which can exist as 0, 1, or both simultaneously. This unique property enables quantum computers to perform parallel computations exponentially faster than classical systems.

As the number of qubits increases, the computing power of these machines grows

exponentially, significantly augmenting both the processing speed and volume of data processed by quantum computers. These advancements hold vast potential in financial modeling, cybersecurity, and fintech innovations, with the potential to bridge socio-economic gaps.

To understand quantum computing, it is essential to grasp four key principles of quantum mechanics.

- (i) **Superposition:** In quantum mechanics, particles can exist in multiple states simultaneously. In quantum computing, qubits can be both 0 and 1, unlike classical bits that are either 0 or 1. This allows quantum computers to process vast amounts of data in parallel, exponentially increasing their computational power.

- (ii) **Entanglement:** Quantum entanglement is a phenomenon where the state of one particle becomes dependent on the state of another, even when separated by large distances. In quantum computing, entangled qubits can perform coordinated operations, enabling more efficient computation and communication.
- (iii) **Wave-particle duality:** Quantum mechanics postulates that particles exhibit both wavelike and particle-like properties. This concept plays a crucial role in the development of quantum algorithms that leverage the wavelike nature of qubits to perform complex calculations
- (iv) **Decoherence:** Decoherence is the process in which quantum particles and systems can decay, collapse, or change, converting into single states measurable by classical physics.

Quantum Computing and its Evolution

Quantum computing traces its origins to the early 20th century, when several groundbreaking discoveries by Max Planck, Albert Einstein, and Niels Bohr contributed to the development of quantum mechanics and laid the foundation for the principles of quantum computing.

Quantum mechanics is characterized by several unique features (superposition, entanglement, and wave-particle

duality) that distinguish it from classical mechanics. These features enable quantum computing to perform tasks that are impossible or prohibitively slow on classical computers. With the passage of time, the mathematical framework developed by John von Neumann provided the requisite tools to explore the potential applications of quantum mechanisms in computation.

The period 1994-2000 marked the emergence of quantum computing algorithms. In 1994, Peter Shor, an American mathematician and computer scientist, developed the first quantum algorithm known as the Shor algorithm that poses a risk to the existing cryptographic algorithms by making them vulnerable. In 1996, Lov Grover, an Indian American computer scientist, developed Grover's algorithm. This algorithm searches unsorted databases more efficiently than classical algorithms. Grover's algorithm can search a database of N elements in roughly $\sqrt{N}$ steps, offering a quadratic speedup compared to classical algorithms, which require approximately N steps. Although the speedup provided by Grover's algorithm is less dramatic than Shor's algorithm, it still demonstrates how quantum computing can outperform classical computing in specific tasks (Fig.1). The development of Shor's and Grover's algorithms laid the foundation for research and development in the domain of quantum computing.

Quantum Computing Hardware Development

Quantum computing is a rapidly advancing field poised at the intersection of physics, engineering, materials science, and computer science. Unlike classical computing, which relies on bits (0 or 1) as the fundamental unit of information, quantum computing utilizes quantum bits or qubits for computation and processing. The realization of practical quantum computers hinges on the development of robust and scalable quantum hardware. Currently, research around the world is focused towards addressing quantum hardware challenges, and progressing towards scalable quantum computing systems. There are four key tracks for qubit implementation, with both advantages and limitations.

Superconducting Qubits: They are based on Josephson junctions and operate at cryogenic temperatures. Because of their relatively matured fabrication techniques, and compatibility with the existing semiconductor technologies, IBM, and Google have chosen this track and have invested billions of dollars in superconducting qubits.

Trapped Ions: Ion-based qubits make use of single ions confined in electromagnetic traps. They offer very high-fidelity operations and coherence times, but scaling these systems to large qubit numbers remains a challenge due to the complex laser setups.

Photonic Qubits: Photons as qubits offer room temperature operation and much easier integration into existing communication networks. However, the key challenge in their usage is the need to realize deterministic two-qubit gates for photonic systems.

Topological Qubits: They seek to leverage anyons—particles that exist in two-dimensional spaces—toward error-resistant quantum processing. This approach is being researched by companies like Microsoft due to the potential for very high fault tolerance.

The Quantum Computing Stack

The quantum computing stack is a hierarchical structure that integrates essential components for building quantum computing systems. It comprises many layers, each playing a crucial role in ensuring functionality and scalability for quantum systems. The stack (Fig. 3) comprises:

Physical Layer: This forms the base of the quantum computing stack, which includes the qubits and their physical realization. This also includes hardware for qubit control, like lasers for trapped ions or microwave circuits for superconducting qubits.

Control Layer: The control layer provides precise signals to actuate the qubits. It translates high-level instructions into hardware-level operations. Included in this layer are cryogenic control electronics and signal processors.

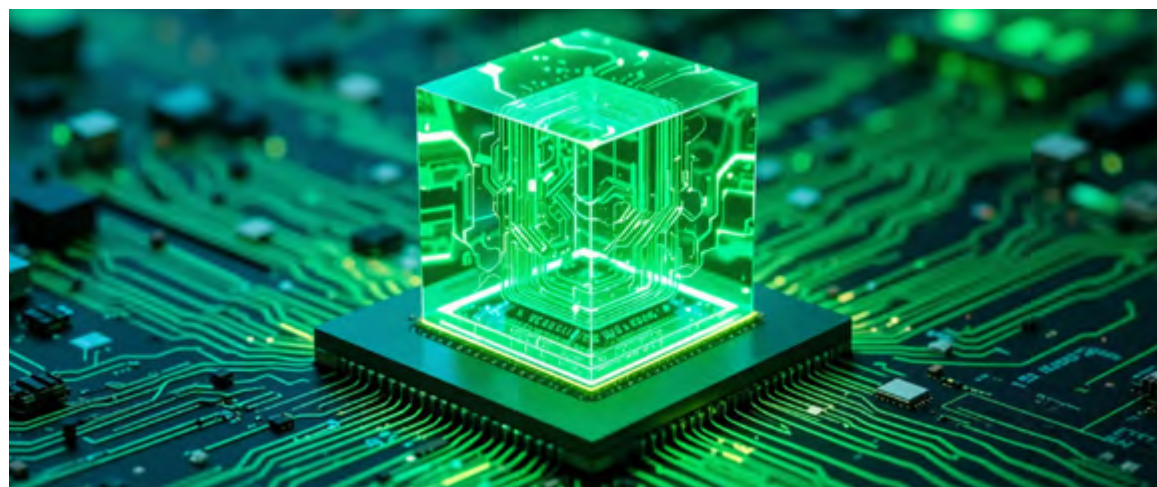
Error Correction Layer: This is a layer comprising quantum error correction algorithms that mitigate the effects of noise and errors in quantum computations. It guarantees reliability by encoding logical qubits into several physical qubits.

Logical Layer: In this layer, logical qubits and gates are defined. On this logical layer, one can implement algorithms independently from specific hardware configurations.

Algorithm Layer: This layer is concerned with the design of quantum algorithms on specific applications; a notable one is Shor's algorithm, which factors integers, whereas Grover's search algorithm sorts out problems.

Application Layer: This is the topmost layer of the stack. It integrates quantum algorithms with real-world applications, including cryptography, optimization, and quantum chemistry, enabling hybrid quantum-classical computing.

Each layer interacts with its neighboring layers to ensure smooth processing, for example, abstraction of user-level instructions into quantum computation, solving errors, and keeping qubit coherence in place.



Quantum Computing Applications and Use-Cases

The applications of quantum computing are still in the research and development phase, however, a few are already available and are also commercially feasible. For instance, a specific type of quantum computer, known as Quantum Annealer, has been developed to solve a certain set of optimization challenges. Similarly, quantum algorithms designed to enhance existing AI and Machine Learning models are already being tested. Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) are being developed to secure quantum communications (some PQC models have been tested, as mentioned in earlier sections). With advancements in quantum sensing and metrology, it is likely that scientists and technologists will already have a fair idea of deploying these technologies as soon as these machines become readily functional (i.e., error-free). Against this backdrop, quantum computing is expected to have a transformative impact across various fields, as discussed below.

Cryptography and Cybersecurity

Quantum computers can factor large integers efficiently and quickly, posing a threat to widely used encryption schemes, including the RSA paradigm. Shor’s algorithm, once fully realized, can be a grave threat to the present-day public-key cryptography systems, necessitating the use of post-quantum cryptography (PQC). For example, lattice-based cryptography (e.g., NTRU) and hash-based signatures (e.g., XMSS) do not rely on mathematical problems that quantum computers can easily solve. Besides PQC, quantum computing enables cryptographic techniques such as quantum key distribution (QKD), which use the principles of quantum mechanics to enable secure communication channels that are theoretically “unhackable” or resistant to eavesdropping, such as the BB84 protocol. For instance, the Micius satellite has already demonstrated long-distance QKD, paving the way for global quantum communication networks.

Drug Discovery and Molecular Simulation

Quantum computing has the potential to significantly impact drug discovery and the pharmaceutical industry. Simulating complex protein structures and their interactions at a molecular level is beyond the ability of classical computing. Quantum computers can model these interactions more effectively by exploiting the concept of quantum parallelism. This capability speeds up the processes of drug discovery, reduces costs and complexity, and advances personalized medicine. For instance, quantum simulations have been used to understand the behavior of the FeMoco molecule in nitrogenase enzymes, a crucial step toward efficient nitrogen fixation (Reiher et al., 2017). Such breakthroughs could lead to sustainable agricultural practices and innovative medical therapies. Startups like Rigetti Computing and companies like Biogen are using quantum computing to explore drug formulations, understand molecular interactions, and simulate reaction pathways, thus reducing trial-and-error approaches in traditional drug discovery.

Optimization Problems

Quantum computing holds immense potential for solving complex optimization problems across logistics, supply chains, and finance. Classical optimization methods often rely on heuristics or approximations, which may not always yield the most optimal solution in a reasonable timeframe. Quantum computers, however, can solve combinatorial optimization problems efficiently using algorithms like QAOA. Quantum computing can optimize decision points like inventory levels and transportation routes, especially in supply chain management. Similarly, portfolio optimization and risk analysis could also benefit from the increased computational power that quantum systems provide, enabling financial institutions to maximize returns while minimizing risks. Rigetti Computing provides access to quantum processors through its Forest platform and Quantum Cloud Services (QCS) and is currently developing quantum algorithms for optimization problems (Rigetti Quantum Cloud Services (QCS): <https://www.rigetti.com/quantum-cloud-services>).

Artificial Intelligence and Machine Learning

Most of the machine learning (ML) algorithms involve optimization problems or matrix computations, which a quantum computer can execute significantly faster than classical computers. For example, quantum-enhanced algorithms for support vector machines and neural networks promise better performance when it comes to applications such as image recognition, natural language processing, and predictive analytics. Google’s Quantum AI Lab has already demonstrated the potential of quantum ML by providing an

exponentially fast solution to kernel-based learning tasks (Biamonte et al., 2017). While these developments are still in their infancy, they have the potential to revolutionize AI applications in various fields, from healthcare and finance to autonomous systems.

Materials Science

Quantum computers naturally simulate quantum systems, offering unprecedented insights into material behavior. This capability is particularly valuable for designing high-performance batteries, superconductors, and catalysts. For example, scientists are using quantum computing to study solid-state materials for better solar panels, and lightweight alloys for aerospace industries. These advancements can contribute towards greener energy solutions and newer technologies in diverse areas. IBM’s Qiskit framework allows users to simulate quantum chemistry, aiding in the prediction of material properties and facilitating materials discovery. Similarly, Rigetti Quantum Cloud Services (QCS) can be used to simulate complex materials and understand their properties.

Financial Services

The financial industry, with its complex mathematical models, is a natural fit for quantum computing applications. Quantum algorithms can accelerate tasks such as derivative pricing, risk assessment, and fraud detection, allowing financial institutions to function more efficiently and securely. Quantum computing can significantly improve Monte Carlo simulations, considered a backbone of financial modeling. For instance, quantum amplitude estimation algorithms decrease computational complexity in Monte

Carlo simulations and increase the speed of results (Egger et al., 2020), that helps improve high-frequency trading applications where every second counts. IBM's quantum capabilities are being used for financial modeling and optimization tasks by firms like Goldman Sachs and JP Morgan. Researchers are using Google's Cirq to develop algorithms for complex problem-solving, including portfolio management and derivative pricing (<https://ai.google/research/teams/applied-science/quantum-ai/>).

Energy Sector

The energy sector has to contend with challenges in resource allocation, grid optimization, and renewable energy integration. Quantum computing can optimize energy distribution networks and improve the efficiency of renewable systems. For instance, it can optimize wind farm layouts or solar panel placements for improved energy generation. Quantum simulations can also aid in the search for better materials for efficient

energy storage, be it in advanced batteries or fuel cells. These advancements support the transition towards sustainable energy systems and address the global challenges around energy. D-Wave is working on using quantum technology for optimizing power generation and the management of resources in smart grids, as well as for scheduling and logistics in energy distribution.

Climate Modeling and Environmental Science

Modeling climate change involves enormous amounts of data and complex simulations. Quantum computing is an important tool in climate modeling because it can handle high-dimensional datasets and solve differential equations efficiently. Quantum algorithms can enhance the accuracy of weather forecasts, model the impact of various interventions, and optimize resource allocation for conservation efforts. These are core applications for solving environmental challenges and achieving sustainable development.

Quantum Computing Ecosystem

In the last few years, both nation-states and the private sector have invested in quantum science and technological development. There have been sizeable budgetary allocations by governments to translate quantum science into tangible technological solutions. According to Market.us, the global quantum computing market is projected to reach \$1.238 billion by 2025 and is expected to grow to \$8.2856 billion by 2032, reflecting a compound annual growth rate (CAGR) of 31.2%. Statista's analysis for the period from 2001 to 2021 reveals that venture capital accounts for 43% of investments in quantum technology, with the private sector contributing 30%, corporations 15%, and the public sector 5%. Notably, private sector investments surged by 39% from 2021 to 2022. As of 2024, data from The Quantum Insider shows that investment in quantum computing declined from \$2.7 billion in 2022 to \$1.4 billion in 2023, followed by a significant rebound to \$2.6 billion in 2024. By early 2025, investments in quantum computing are estimated to be \$0.1 billion.

Most of these investments aim to propel quantum computing, quantum communication, quantum sensing, Quantum Information Theory, and the development of quantum materials. As per the Quantum Insider data, the total investment in quantum space as of 2025 stands at \$12.2 billion, with the funding for December 2024 at \$204.1 million. Apart from government funding, the private sector has also expanded its funding portfolios to support quantum startups. From the national security perspective, analyzing and mapping these investments is crucial to develop an understanding of global quantum

science development and identify which nations stand ahead of others.

The quantum computing ecosystem has experienced significant growth, with numerous hardware and software providers making notable advancements. This expansion is driven by substantial investments from both the private and public sector, aiming to harness the transformative potential of quantum technologies. According to The Quantum Insider data, there are around 1542 companies working in quantum computing, around 1496 investors and 480 enterprises (Figure 6).

Hardware Providers

IBM: A pioneer in quantum computing, IBM has developed quantum processors accessible via the cloud. Its roadmap includes scaling up to a 1,000-qubit processor, with the recent introduction of the "Condor" chip featuring over 1,200 qubits. IBM's commitment is further evidenced by significant investments in research and development to enhance qubit coherence and error rates.

Google: In 2019, Google achieved a milestone by demonstrating its quantum supremacy with the 53-qubit Sycamore processor. Building on this, Google introduced the "Willow" chip in December 2024, a 105-qubit processor capable of solving complex problems in mere minutes, showcasing the rapid progress in its quantum hardware capabilities.

Microsoft: Focusing on topological qubits, Microsoft aims to develop more stable and



error-resistant quantum systems. Their Azure quantum platform integrates quantum computing services into the cloud, facilitating broader accessibility for developers and researchers. In January 2025, Microsoft launched the “Quantum Ready” program, signaling a push towards preparing businesses for quantum advancements.

IonQ: IonQ specializes in trapped-ion quantum computing, which uses ions as qubits for their exceptional stability and coherence times. In 2024, IonQ unveiled a quantum processor with 32 algorithmic qubits, achieving industry-leading performance in terms of error rates and algorithmic depth. IonQ went public in 2021 through a SPAC merger, raising significant capital to accelerate its research and commercialization efforts. Its partnerships include collaborations with Amazon Braket and Google Cloud for cloud-based quantum services.

D-Wave Quantum: D-Wave is a pioneer in quantum annealing, a specialized approach tailored for optimization problems. In 2024, D-Wave introduced the Advantage2 system, featuring over 5,000 qubits, which improved connectivity for solving large-scale optimization challenges. It also expanded its quantum cloud services. D-Wave has secured partnerships with companies like Volkswagen and Lockheed Martin to solve real-world problems, such as supply chain logistics and satellite optimization.

Software Providers

Quantinuum: Quantinuum provides an integrated quantum computing stack, combining Honeywell’s hardware with Cambridge Quantum Computing’s software expertise. In 2024, Quantinuum developed one of the industry’s most powerful quantum processors, the H2 generation, which excels in both speed and fidelity. The company also launched new quantum software tools for cryptography and chemistry simulations. Quantinuum raised over \$300 million in a funding round led by JP Morgan Chase, elevating its valuation to \$5 billion and underscoring confidence in its integrated hardware and software solutions.

Horizon Quantum Computing: Focused on simplifying quantum software development, Horizon Quantum Computing raised \$18.1 million in a Series A funding round. This investment supports the creation of tools that enable developers to build quantum applications more efficiently, bridging the gap between classical and quantum computing paradigms.

Entropica Labs: A Singapore-based company specializing in quantum error correction software, Entropica Labs secured \$5.5 million in a Series A round in 2023, with participation from State Farm Ventures. This investment highlights the growing interest in quantum software solutions that enhance the reliability of quantum computations.

Quantum Computing-Specific Providers

While tech giants like IBM, Google, and Microsoft have been leading quantum computing development, numerous specialized quantum computing providers are emerging as key players. These companies focus exclusively on quantum hardware, software, or integrated solutions, bringing niche expertise and innovative approaches to the industry.

Rigetti Computing

Rigetti focuses on superconducting qubits and hybrid quantum-classical systems to address real-world problems in optimization and machine learning. In 2023, Rigetti launched the “Aspen-M” processor with 80 qubits, featuring advancements in gate fidelity and error correction techniques. The company also announced partnerships with Fortune 500 companies for piloting quantum applications. Rigetti raised \$260 million in funding since its founding, including a \$75 million Series C round to enhance its fabrication capabilities and build a fault-tolerant quantum system.

PsiQuantum

PsiQuantum is developing a photonic quantum computer, leveraging photons as qubits to achieve scalability and error resistance. The company is working towards a million-qubit quantum computer and has already developed key components like silicon photonic chips and quantum error correction codes. PsiQuantum

has raised over \$665 million, including backing from BlackRock and Microsoft’s M12, to build its first commercial-grade quantum computer.

Xanadu

Xanadu focuses on photonic quantum computing and quantum machine learning, offering cloud-based access to its hardware. Xanadu launched “Borealis,” a quantum computer that demonstrated a quantum advantage in solving Gaussian Boson Sampling (GBS) problems in 2023. It has also introduced software like PennyLane, a leading quantum machine learning library. The company secured \$100 million in a Series C round to expand its quantum computing infrastructure and software development.

ColdQuanta

ColdQuanta employs cold atom technology for building scalable quantum processors. In 2024, ColdQuanta introduced “Hilbert,” its first quantum computer available via the cloud. The system demonstrated superior coherence times and gate fidelities. ColdQuanta raised \$110 million in funding to accelerate its R&D and commercialization, making it a key player in cold atom-based quantum systems.

Alpine Quantum Technologies (AQT)

AQT focuses on trapped-ion quantum computing and quantum integration solutions. Based in Austria, AQT has developed modular quantum computing systems for scalable

architectures, aiming to integrate quantum processors seamlessly with classical systems. AQT collaborates with European research institutions and industries to drive innovation in quantum computing applications.

Quantum Machines

The company, Quantum Machines, builds quantum control hardware and software to manage and optimize quantum computers. Its flagship product, the Quantum Orchestration Platform (QOP), is widely used for controlling and scaling quantum systems. Backed by leading investors like Red Dot Capital and Battery Ventures, Quantum Machines raised \$50 million to expand its global reach and develop next-generation control systems.

Zapata Computing

Zapata focuses on quantum software for enterprise applications, offering tools to solve problems in chemistry, logistics, and finance. Its flagship software, Orquestra, integrates quantum and classical workflows to optimize performance across platforms. Zapata has partnered with AWS and Google Cloud to deliver scalable quantum solutions to the pharmaceutical and automotive industries.

These quantum-specific providers are pushing the boundaries of innovation, from novel hardware architectures to advanced software solutions. Their specialized focus and strategic partnerships are essential for the maturation and commercialization of quantum computing.



**Quantum Technology Funding Landscape:
Global and Indian Perspective**

Global Perspective

Role of the public sector: Governments all over the world have invested over \$42 billion in the development of quantum technologies. As compared to the private sector, public investments increased by over 50% in 2022, according to the McKinsey report of April 2024 (Fig. 8). Many countries, such as Germany, the United Kingdom, and South Korea, have announced significant new funding for quantum technology as of April 2024, bringing the global public funding total to about \$42 billion.

Table 4.1 outlines the quantum budget of several national governments. Research suggests that the government spending in China on quantum technology development exceeds that of any other country in the world. China announced in its 13th and 14th Five-Year Plans that quantum science and applications will be key in accelerating scientific progress, improving national security, and enhancing strategic support. To this end, the Chinese government has diverted \$15.3 billion for the duration of the Plan (2021-25). Such large-scale public funding projects have created a conducive environment for dozens of quantum research institutions in China to go ahead of other nation-states and be the first movers in many applications of quantum science. The other major government/ public funding of quantum projects is by the European Union (\$7.3 billion) and the United States (\$1.9 billion).



Table 4.1: Global Quantum Strategies and Investments by National Governments

Country/Region	Mission/Initiative	Budgetary allocation	Time period
United States	The National Quantum Initiative Act, 2018	\$1.2 billion (in government funding). Private organisations and several American universities have also pledged a contribution of \$340 million to research centers that have been setup through the Act.	Five years (2018 - present)
United Kingdom	National Quantum Strategy	£1 billion (\$1.3 billion). The UK has committed £2.5 billion for the next ten years, beginning 2024 towards advanced quantum tech development.	Ten years (2014 - present)
China	China’s 13th and 14th Five-Year Plans outline the importance of quantum science and tech development	\$15.3 billion	2016-present
Canada	National Quantum Strategy	\$360 million	2021-present
India	National Quantum Mission	\$1.1 billion	2020-present
European Union	Quantum Technologies Flagship Programme	€1 billion (cumulatively by the European Commission). Over the years, EU members have invested \$7.3 billion in their national projects.	10 years (2018–present)
France	National R&D Strategy	€1.8 billion	2018-present
Germany	Action Plan for Quantum Technologies	Germany invested €650 million in 2018, followed by €2 billion in 2020. The country’s expected budgetary allocation is €3.1 billion by the end of 2026.	8 years (2018–present)
Australia	National Quantum Strategy	\$670 million (AUD 1 billion)	7 years (2023– present)

Role of the private sector: In recent years, the private sector has also significantly increased its investment in quantum technologies. Both, academia and research labs have conducted quantum experiments, and large tech corporations (like IBM, Google, Microsoft, Intel, D-Wave, Honeywell, etc.) and startups (like Rigetti Computing, PsiQuantum, and IonQ) across the world are actively working towards commercialization of quantum technologies. In most countries, private players have collaborated with universities and research labs to advance quantum computing, develop quantum communication models, and fine-tune quantum sensing.

Venture capital (VC) funds and other investment avenues have also started to mature in the last few years. As per a McKinsey report, funding raised by quantum startups was \$1.7 billion in 2024, a 27% decrease from 2023 (Fig 7). According to The Quantum Insider intelligence platform, venture funding tapered in Q3 2024 compared to Q2 2024. Specifically, there was a ~25% reduction in the number of funding rounds from Q2 to Q3, leading to a 60% decrease in total funding amount.

In recent years, all three key areas ofIn recent years, all three key areas of quantum science—quantum computing, quantum communication, and quantum sensing—have seen a funding boost (there was a drop in private sector investment in 2023), with quantum computing receiving the most significant investment. By the end of 2023, quantum computing had attracted \$6.7 billion, while quantum communication and sensing received \$1.2 billion and \$0.7 billion, respectively.

Big ticket investments in quantum computing underscore the importance of hardware development in the quantum value chain. Approximately 50% of these global private investments are directed towards firms and corporations in the United States, followed by the UK, Canada, and China. This is outlined in Fig. 11.

Over the past decade, Big Tech has been steadily investing in quantum computing. Although specific funding amounts and budgets are not disclosed (and can only be estimated), these corporations have been collaborating and funding research and development projects at US universities. For instance, in May 2023, Alphabet Inc. and IBM partnered with the University of Chicago and funded a \$100 million project to accelerate the development of fault-tolerant quantum computers over a ten-year period.

Companies have made major strides in quantum error correction, paving the way for large-scale, fault-tolerant quantum computing. Recent milestones include record qubit fidelities of 99.5% (achieved by QuEra, MIT, and Harvard) and 99.9% (by Microsoft and Quantinuum), enabled by advanced error correction schemes and innovative logical qubit architectures. By prioritizing software and architecture-based error mitigation over hardware alone, these advancements promise to drastically lower hardware requirements, such as the number of physical qubits per logical qubit, and accelerate progress toward universal quantum computing.

Google's Quantum Supremacy (2019)

Google's Sycamore processor, a 53-qubit quantum computer, solved a specific computational problem in 200 seconds, a task estimated to take the most powerful classical supercomputers 10,000 years. It marked the first demonstration of quantum supremacy, proving quantum computers could outperform classical ones at specific tasks.

IBM's Quantum Roadmap and their Vision of a QC with 1000+ qubits

IBM unveiled an ambitious roadmap aiming to develop quantum processors with over 1,000 qubits by 2023. By 2024, IBM had introduced its "Condor" chip with over 1,200 qubits. IBM's advancements reflect efforts to scale quantum hardware for real-world applications.

Google's Willow Quantum Processor

Google introduced the "Willow" chip, a 105-qubit quantum processor. It solved a problem in 5 minutes that would take classical supercomputers an impractical length of time (trillions of years). It demonstrated a leap in quantum hardware capabilities, bringing quantum computing closer to solving real-world problems.

Advancements in Quantum Error Correction

Significant strides have been made in reducing quantum error rates. By 2024, Microsoft and Quantinuum reported achieving error rates 800 times better than prior benchmarks. Improved error correction is critical for fault-tolerant quantum computers, making them more stable and reliable for complex computations.

Rise of Quantum Cloud Services

IBM, AWS Braket, and Google expanded quantum cloud services, enabling businesses and researchers to access quantum hardware and simulators remotely. This democratizes access to quantum computing, fostering innovation across industries like finance, materials science, and healthcare.

Quantum AI for Drug Discovery

Companies like Quantum Computing Inc. and startups, such as Zapata Computing, have explored quantum algorithms to simulate molecular structures and accelerate drug discovery. Quantum computing could revolutionize healthcare by identifying potential drugs faster and at lower costs.

Quantum Networking Breakthroughs

Research groups have demonstrated entanglement-based quantum communication over increasing distances. In 2023, Chinese researchers achieved a 1,200 km quantum entanglement experiment via satellites. Progress in quantum networking is foundational for building the Quantum Internet, which would offer ultra-secure communications.

Quantum Computing Partnerships in Industry

Collaborations between quantum companies and industries have expanded. For example, in 2025, D-Wave partnered with Carahsoft to integrate quantum solutions in the US federal government. Partnerships accelerate the adoption of quantum technologies in solving optimization, logistics, and defense problems.

Hybrid Quantum-Classical Systems

Companies like Rigetti Computing have pioneered hybrid approaches, combining classical and quantum systems for computational tasks. Hybrid systems leverage the strengths of both paradigms, making quantum solutions more practical and accessible in the near term. Applications include improving supply chain logistics and portfolio optimization.

Indian Perspective

India is actively building a quantum technology ecosystem with the support of the Indian government. The ecosystem focuses on a strategic alliance between industry, government, and academia. Launched in April 2023, India's National Quantum Mission (NQM) marks a significant step forward in the country's commitment to advancing quantum technologies. With a budget of ₹6,003 crores (approximately \$730 million), NQM aims to place India among the global leaders in quantum research and innovation by 2031. It focuses on developing critical quantum computing capabilities by creating a quantum-ready workforce that can transform sectors such as communication, computing, healthcare, and defense. India's private sector is also creating synergies with the government's quantum mission.

The mission has four key verticals: Quantum Computing, Quantum Communication, Quantum Sensing, and Quantum Materials (Fig. 10). One of its primary objectives is to establish a quantum computer with 50-1,000 physical qubits over the next decade, supporting research in quantum algorithms, error correction, and scalable hardware. In quantum communication, the mission aims to secure sensitive information by developing quantum key distribution (QKD) networks for government and defense applications.

Additionally, the NQM emphasizes strong collaboration between academia, industry, and global partners. It supports the establishment of research hubs, promotes quantum workforce development through fellowships, and encourages indigenous development of quantum technologies. This includes advancing quantum sensors for precision measurement in fields such as healthcare, agriculture, and navigation.



Startups in India at the forefront of Quantum Computing:

BosonQ Psi - Founded in 2020, BosonQ Psi specializes in quantum-powered engineering simulation software, enabling high-fidelity simulations in computational fluid dynamics, structural analysis, and heat transfer for aerospace and automotive sectors.

QuLabs - Established in 2017, QuLabs focuses on quantum communication and computing solutions, aiming to deliver secure and efficient quantum software for various applications.

QpiAI - Founded in 2019, QpiAI integrates quantum computing with artificial intelligence, developing platforms that leverage quantum algorithms for optimization and machine learning tasks. Based in Bengaluru, QpiAI focuses on building superconducting quantum computers. They have developed the QpiAISense™ platform for room temperature qubit control, contributing to scalable and high-performance quantum computing solutions.

Qkrishi - Established in 2021, Qkrishi specializes in quantum finance and algorithms, contributing to the development of quantum computing applications in the financial sector.

QRDLab - QRDLab focuses on superconducting quantum computing and offers consulting and educational services in quantum technologies.

QNu Labs: Established in 2016 and headquartered in Bengaluru, QNu Labs is India's first firm to develop commercial cybersecurity products utilizing quantum physics. Their offerings include Armos, a quantum key distributor, and Tropos, a quantum random number generator.

Silicofeller: Founded in 2021 in New Delhi, Silicofeller focuses on superconducting quantum computing technologies, working towards advancing India's capabilities in this domain.

By aligning with global trends, the National Quantum Mission aims to address critical challenges and leverage opportunities in quantum technologies, ensuring India's leadership in this transformative field. It also supports the country's broader goals of self-reliance (Aatmanirbhar Bharat) in emerging technologies.

Toward Scalable Quantum Systems

The pursuit of scalable quantum systems requires a multifaceted approach, encompassing advancements in hardware, software, algorithms, and system integration. Collaborations between academia, industry, and government agencies will be essential for building a robust quantum ecosystem. Further exploration into novel materials like diamond nitrogen-vacancy centers and silicon-based qubits could offer promising alternatives to current limitations. Integrating artificial intelligence and machine learning for optimizing quantum control and error correction could further accelerate progress.

Despite these advancements, significant challenges persist, including managing error rates, addressing scalability to millions of qubits, isolating systems from environmental noise, and ensuring consistent fabrication. Quantum systems face significant challenges from error rates and noise, which stem from their inherent fragility and sensitivity to environmental factors. Decoherence, caused by interactions with the surroundings, results in the loss of quantum information, while operational errors arise from imperfections in executing quantum gates. These issues get amplified as systems scale, with cumulative errors threatening the reliability of computations. Error correction techniques, such as surface codes, aim to mitigate these issues by encoding logical qubits using thousands of physical qubits. Addressing these hurdles is crucial to unlocking the transformative potential of quantum computing in the years ahead.

Risks Arising from Quantum Computing

As the cybersecurity landscape evolves, the advent of quantum computing poses significant threats to existing cryptographic models and frameworks. As quantum computing and AI processing advance, financial institutions must transition to PQC. During this transition, they will encounter a unique set of cybersecurity risks that could compromise their operational integrity and data security. This critical juncture not only necessitates a shift in cryptographic paradigms but also requires a thorough understanding of the challenges associated with implementing new algorithms, ensuring compatibility with existing systems, and maintaining performance levels required for high-volume transactions. As financial institutions navigate the complexities of deploying PQC while managing vendor dependencies, regulatory compliance, and insider threats, they must also anticipate and mitigate a variety of vulnerabilities that could be exploited during the transition phase.

1. Transition Challenges

- a. **Complex Migration:** Identifying the critical data and existing encryption modes that will be affected by PQC is essential. Transitioning from existing systems to PQC involves updating numerous software and hardware components across the organization. This can lead to integration issues where old systems may not be fully compatible with new protocols.
- b. **Temporary Vulnerabilities:** The transition process will have some systems employing a mixed strategy using both classical cryptography and PQC. This hybrid state can create potential points of vulnerability where attackers could exploit weaknesses before both systems are fully updated.

2. Interoperability Issues

- a. **Legacy Systems Compatibility:** Existing systems employed by financial institutions are legacy systems that utilize traditional cryptographic methods. Integrating these systems with new PQC approaches may

lead to incompatibility issues or require complete overhauls, introducing new technical risks.

- b. **Protocols and Standards:** The development of new communication protocols to support PQC could lead to more complexity and potential vulnerabilities if not carefully designed.

3. Supply Chain Risks

Vendor Dependencies: Many financial institutions rely on third-party vendors for implementation, lacking access to the source code of existing banking solutions. The PQC solutions will also depend on third-party vendors for implementation. Hence, the migration will introduce risks that cyber criminals could exploit.

4. Potential New Attack Vectors

New algorithms may introduce unforeseen vulnerabilities, allowing attackers to exploit specific weaknesses unique to quantum-resistant systems.

References

- 1. <https://Quantumpedia.uk/a-brief-history-of-Quantum-computing-e0bbd05893d0>
- 2. <https://theQuantuminsider.com/2023/12/29/Quantum-computing-companies/>

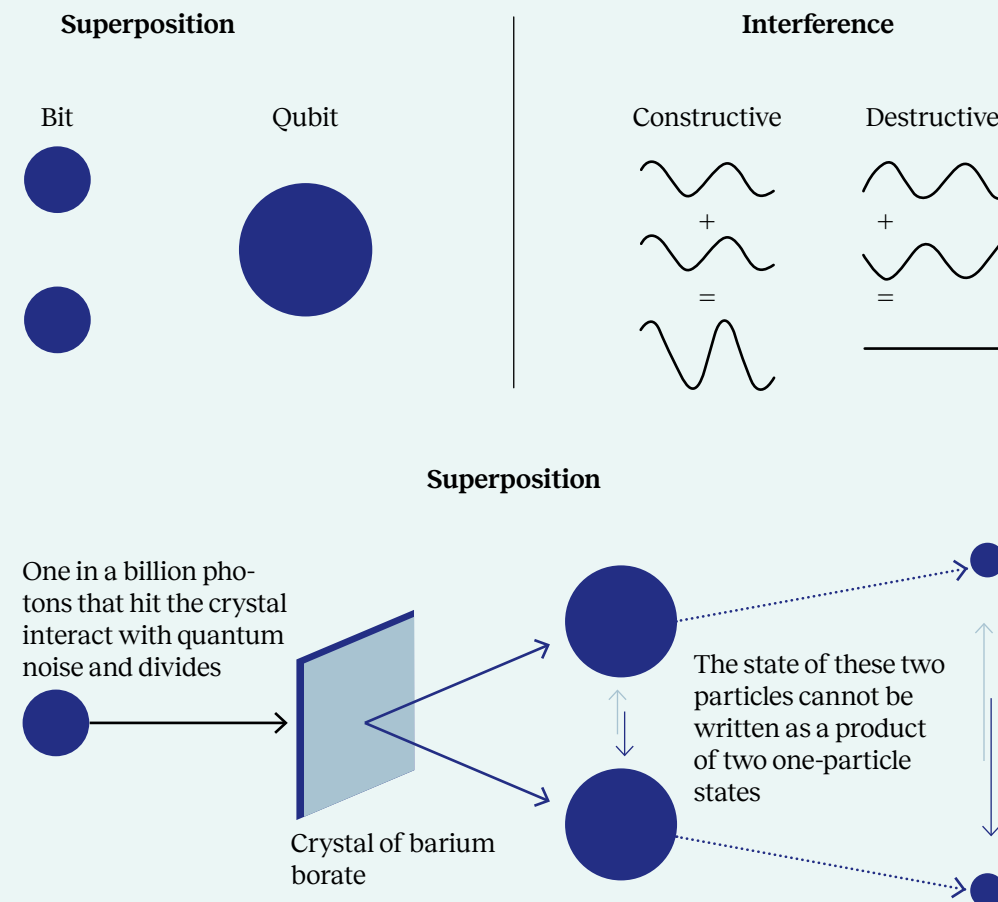


Figure 1: Properties of Quantum Computers (Source: SN Computer Science)

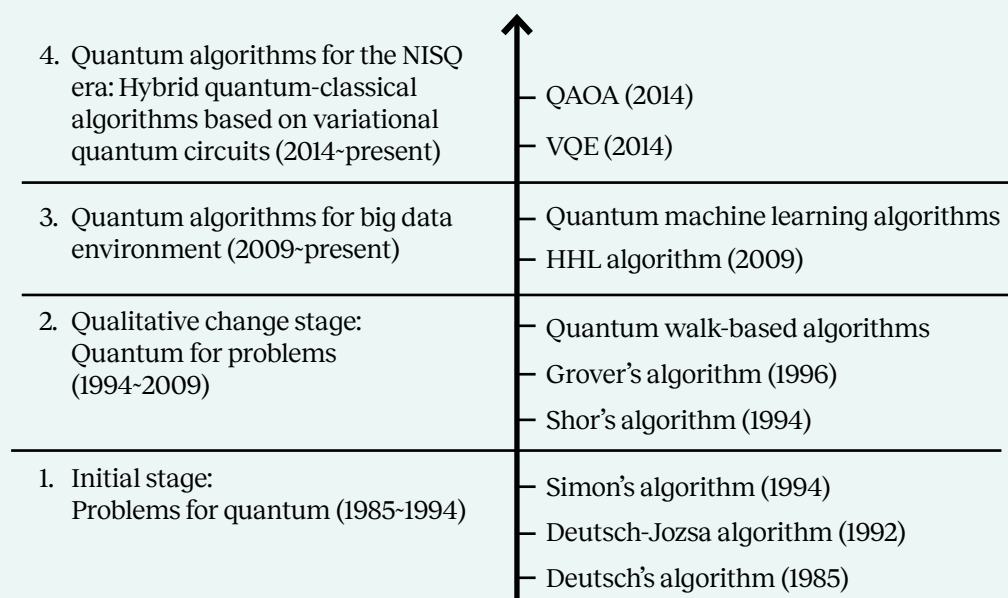


Figure 2: Summary of Quantum Algorithms' development



Physical Layer

This forms the base of the Quantum computing stack, which includes the qubits and their physical realisation. This would also include hardware for qubit control, like lasers for trapped ions or microwave circuits for superconducting qubits.



Control Layer

The control layer provides precise signals to actuate the qubits. It translates high-level instructions into hardware-level operations. Included in this layer are cryogenic control electronics and signal processors.



Error Correction Layer

This is a layer comprising quantum error correction algorithms that mitigates the effects of noise and errors in quantum computations. It guarantees reliability by encoding logical qubits into several physical qubits.



Logical Layer

In this layer, logical qubits and gates are defined. On this logical layer, one can implement algorithms independently from specific hardware configurations.



Algorithm Layer

This layer is concerned with the design of quantum algorithms on specific applications; a notable one is Shor's algorithm, which factors integers, whereas Grover's search algorithm sorts out problems.



Application Layer

This is the topmost layer of the stack. It integrates quantum algorithms with real-world applications, including cryptography, optimisation, and quantum chemistry, enabling hybrid Quantum-classical computing.

Figure 3: Quantum Computing Stack

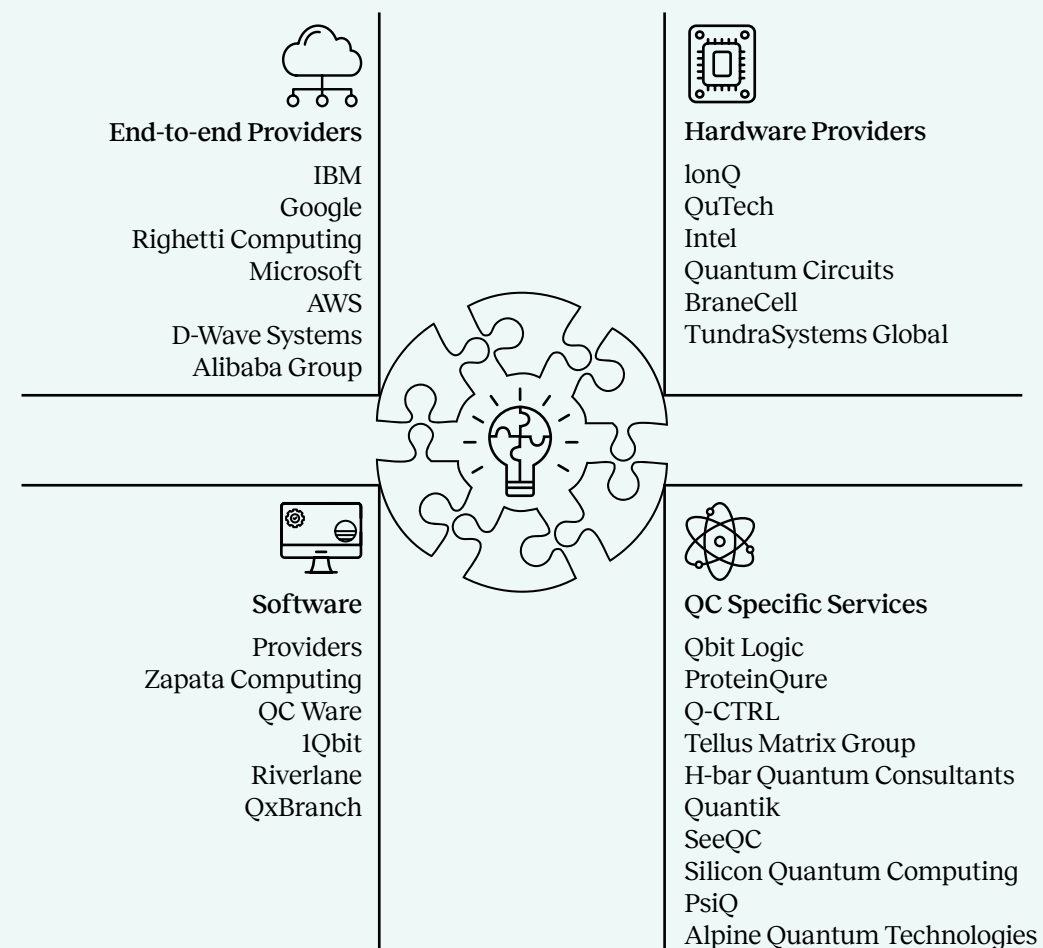


Figure 4: Quantum Computing Ecosystem

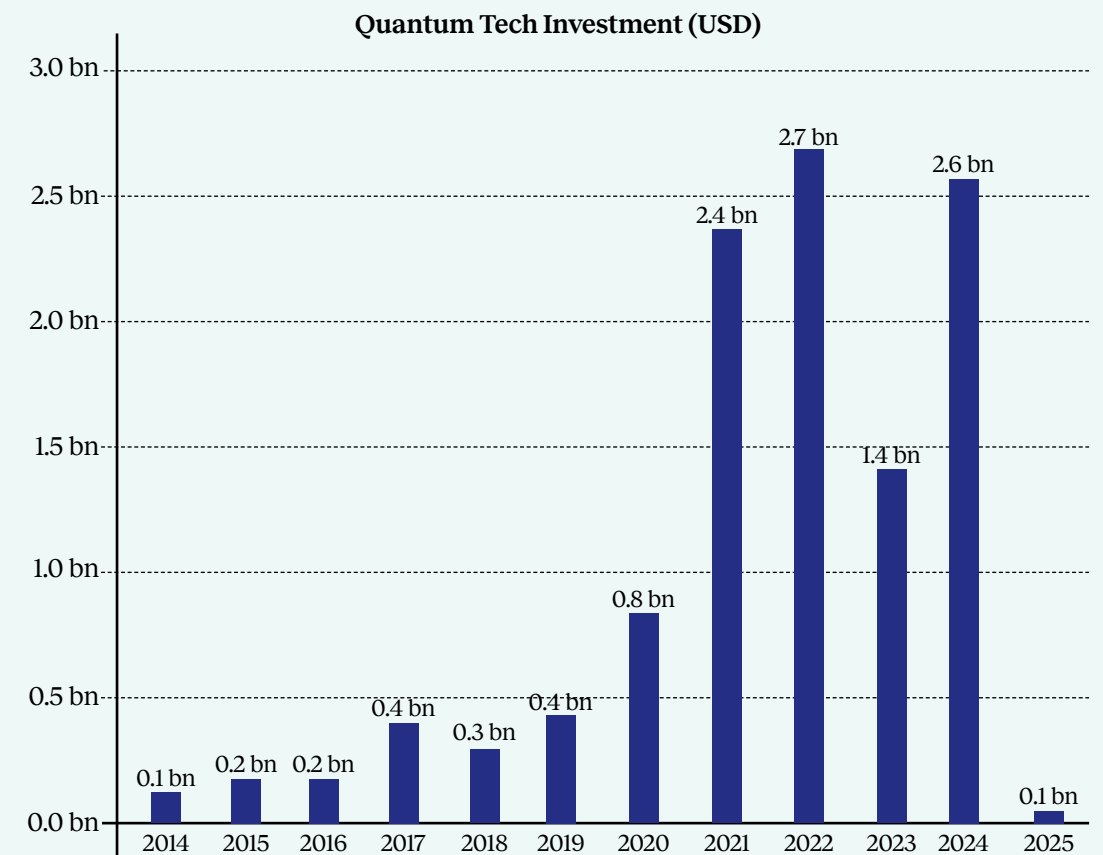


Figure 5: Quantum Tech Investment (source Quantum Insiders)

Data Parameters

Company count 1542	Investors count 1496	Total Funding USD \$12.2 bn
Number of Funding 1095	Last Month Funding \$204.1 mm	Last 12 Months Funding Rounds \$204.1 bn
Data points 229,757	Partnership Count 1459	Enterprise User Count 480

Figure 6: Summary of Quantum Tech (Source: Quantum Insiders)

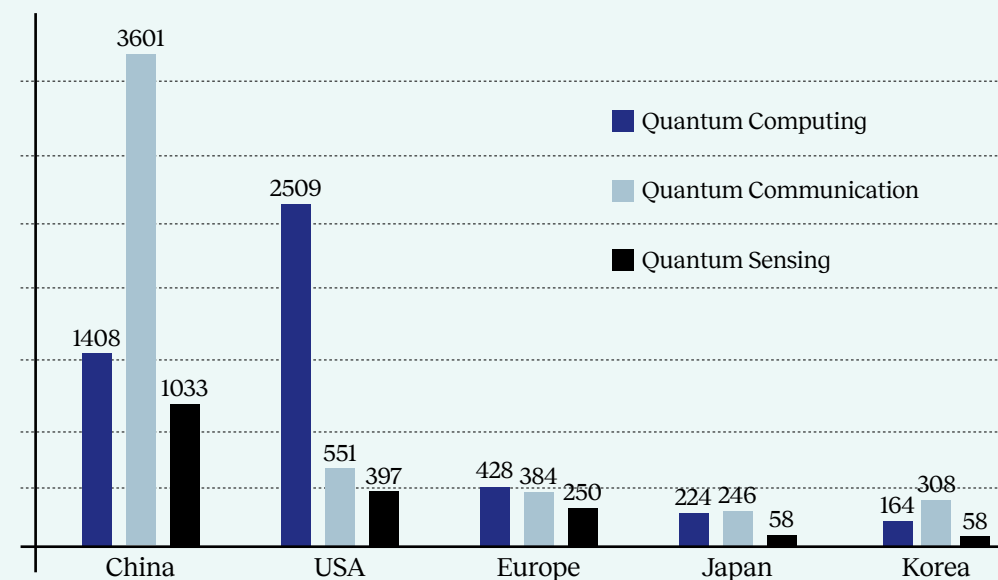


Figure 7: Global Patent Tallies in Quantum Computing, Communications, and Sensing (three core areas of quantum technological development)
(Source: European Quantum Industry Consortium (2024))

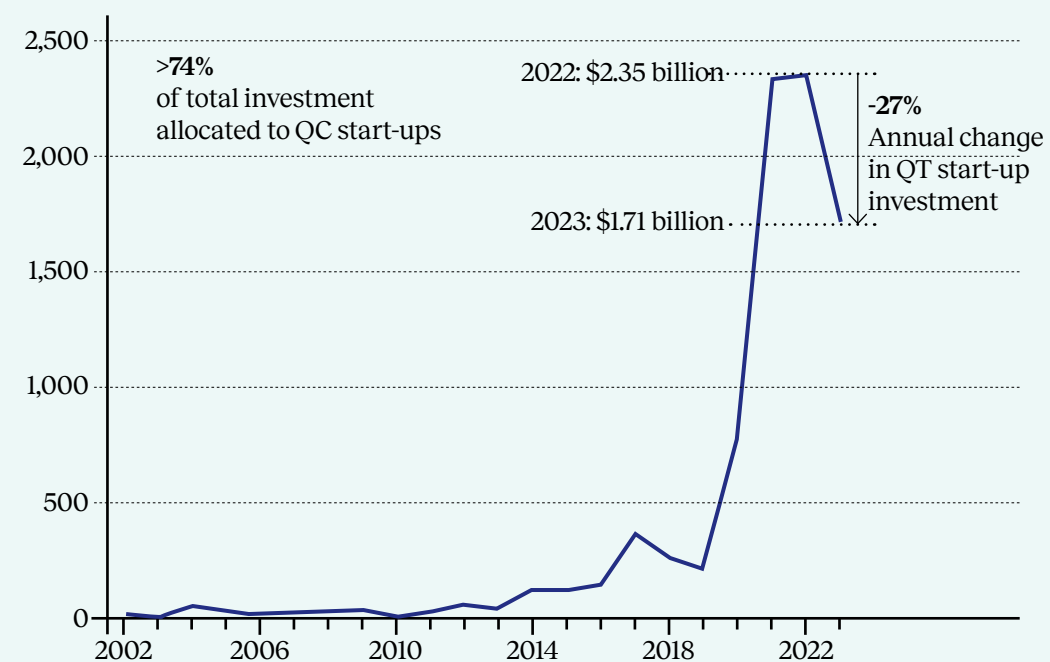


Figure 8: Investments in Quantum Technology Startups (Source: McKinsey)

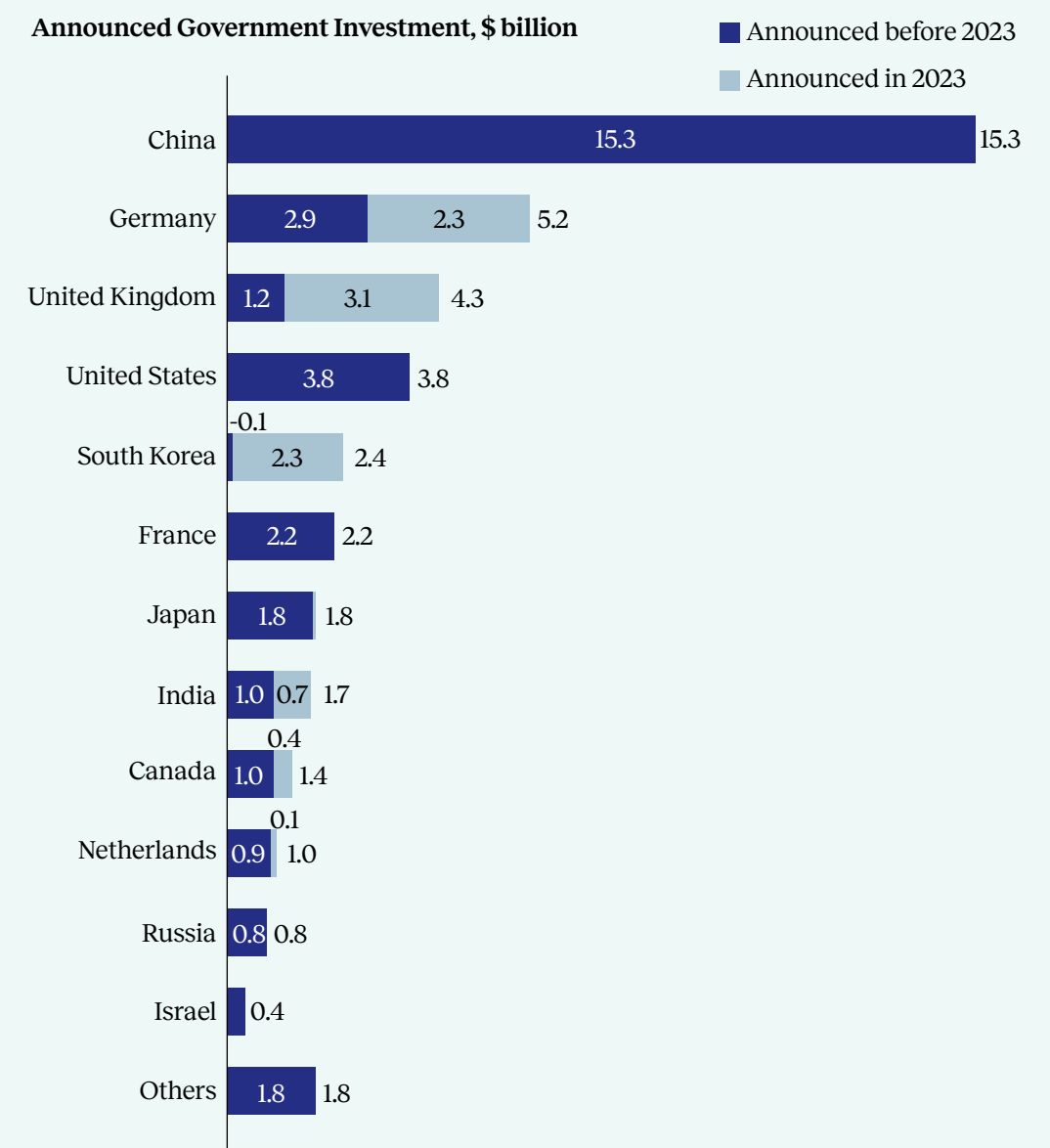


Figure 9: Global Public Investment in Quantum Technologies
(Source: McKinsey Report (April 2024))

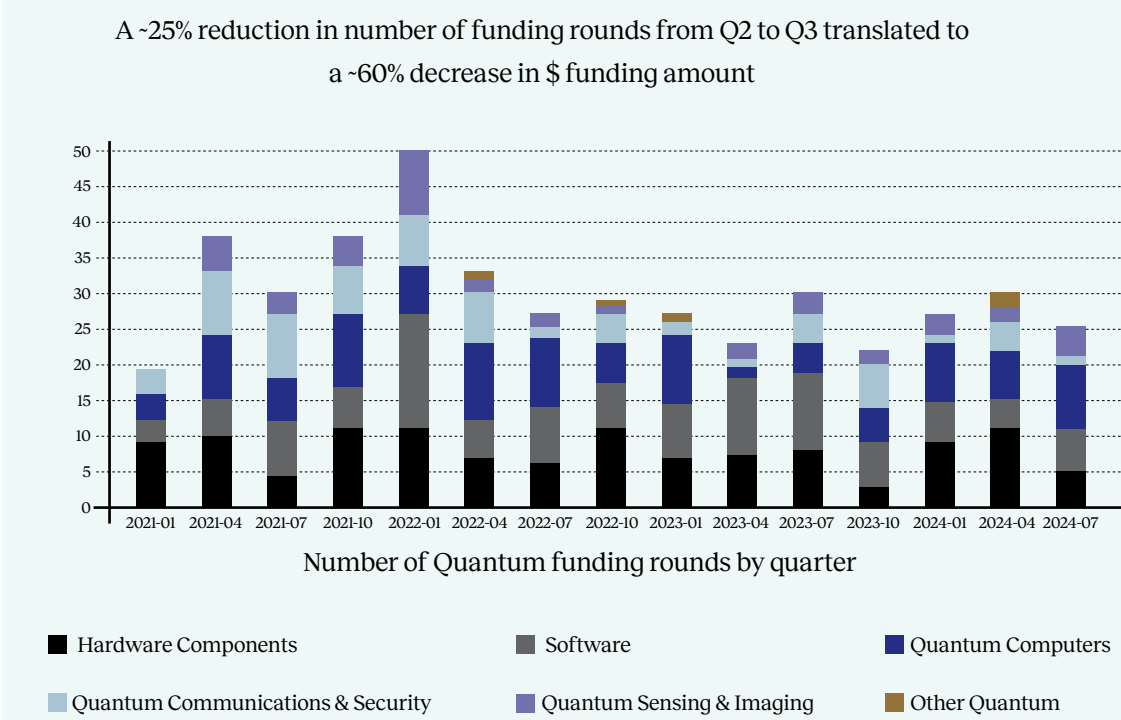
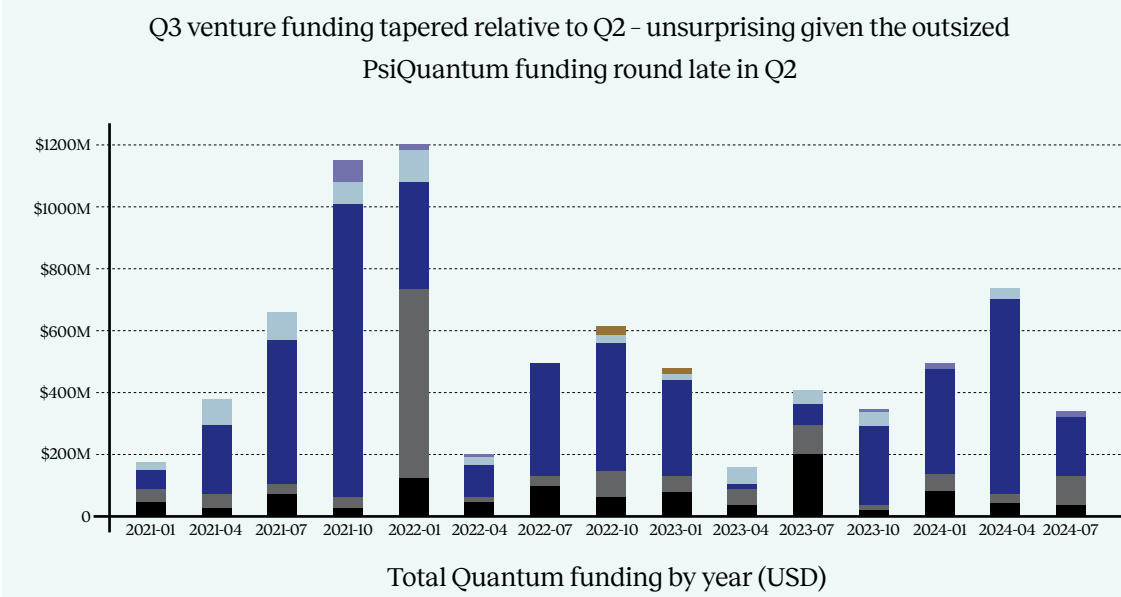


Figure 10: Venture Funding for the year 2024

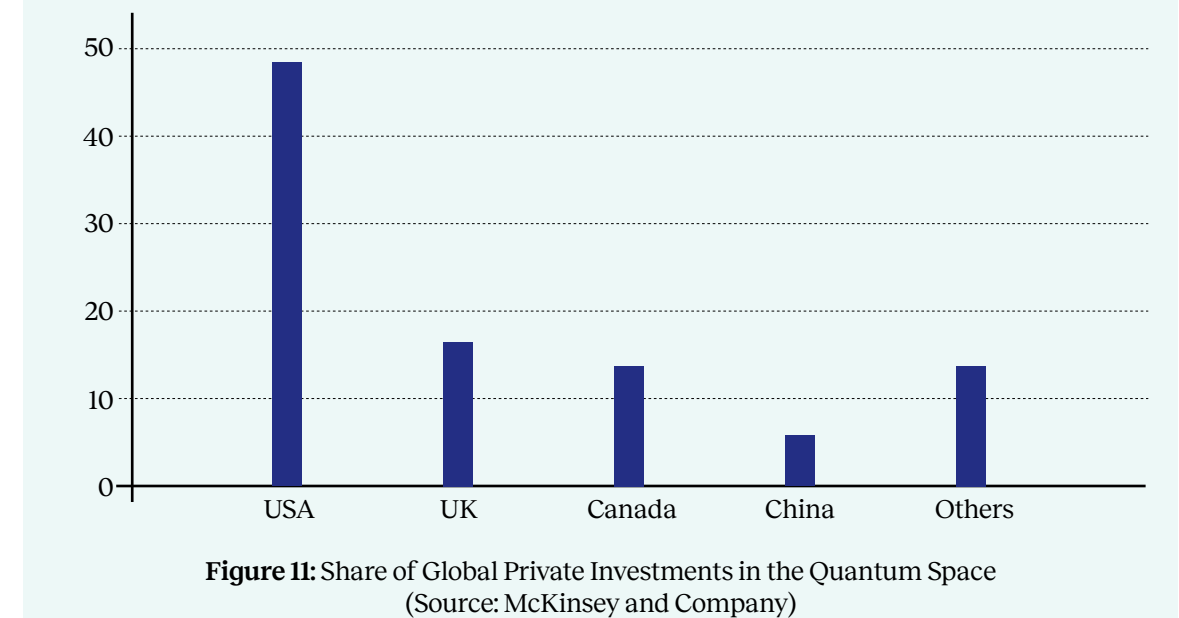
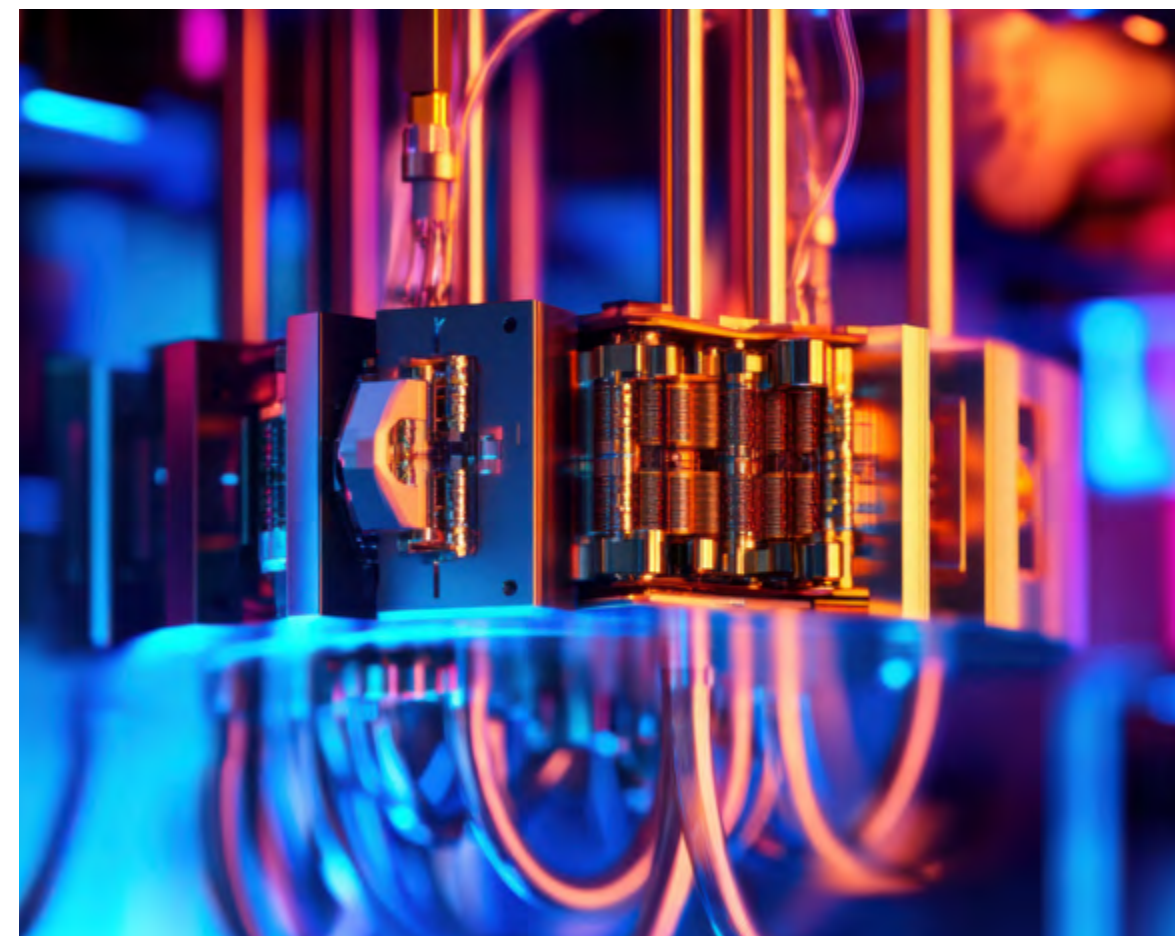


Figure 11: Share of Global Private Investments in the Quantum Space (Source: McKinsey and Company)



Chapter 5

Quantum-Resilient BFSI:
A Framework for Secure Transition to
Post-Quantum Cryptography



What is Cryptography?

Cryptography is the art and science of securing communication and information by converting data into a format that is unreadable to unauthorised users. It involves the use of mathematical algorithms, protocols, and keys to protect data confidentiality, integrity, and authenticity. In today’s digital era, where everyone has a digital footprint, cryptography is a vital tool for safeguarding sensitive information from hackers and cybercriminals (Fig. 1).

Cryptography originates from the Greek term, “Kryptos” which means hidden. Its roots can be traced back to ancient times, notably when Julius Caesar introduced the Caesar Cipher to protect messages from enemies during wartime around 100 BC. Today, the National Institute of Standards and Technology (NIST) is heavily involved in developing cryptographic standards worldwide to ensure data security.

Key Concepts in Cryptography

- 1. **Encryption:** The process of converting plaintext (readable data) into ciphertext (encrypted data) using an algorithm and a key, making it undecipherable for anyone who does not have the appropriate key to decrypt it.
- 2. **Decryption:** The reverse process of encryption, where ciphertext is converted back to plaintext using a decryption algorithm and a key.
- 3. **Keys:** Cryptographic keys are used in the encryption and decryption processes. They can be symmetric (the same key for both encryption and decryption) or asymmetric (using a pair of keys: a public key for encryption and a private key for decryption).

Principles of Cyber Security

Modern day cryptography has evolved over time, but its basic concepts remain the same and have coalesced around the following principles:

- 1. **Confidentiality:** The principle of confidentiality ensures that sensitive information is available only to the authorised senders and receivers (Fig. 2). This is achieved through encryption access controls, and authentication mechanisms.
- 2. **Integrity:** The principle of integrity ensures that information remains accurate, complete and unaltered during storage, transmission, and processing between the sender and the intended receiver without any alterations being detected (Fig. 3).
- 3. **Authentication:** This principle verifies the identity of users, devices, or systems before granting access. Strong authentication methods, including multi-factor authentication (MFA), ensure that only legitimate users can access sensitive resources (Fig. 4).
- 4. **Availability:** The principle of availability ensures that authorised users have access to information and systems when needed. This principle aims to prevent disruptions due to attacks, system failures, or natural disasters, often using redundancy, backups, and disaster recovery plans.
- 5. **Non-repudiation:** This principle provides proof of the origin and integrity of data, ensuring that senders cannot deny sending a message or making a transaction. This can be achieved through digital signatures and logging mechanisms.

Types of Cryptography

There are two main types of cryptography: (i) Symmetric Cryptography and (ii) Asymmetric Cryptography. Both these methods utilise keys for encrypting and decrypting data during transmission. There are also hybrid cryptosystems that combine both.

- 1. **Symmetric Key Cryptography:** Symmetric key cryptography, also known as secret key cryptography, is a type of encryption where the same key is used for both encryption and decryption of data. This method requires that both the sender and the recipient securely share and store the key before they can communicate (Fig. 5).
- 2. **Asymmetric Key Cryptography:** Asymmetric key cryptography, also known as public key cryptography, is a method of encryption that uses a pair of keys for secure data transmission: a public key and a private key. The public key is shared openly and can be used by anyone to encrypt a message, while the private key is kept secret by the owner and is used to decrypt messages that were encrypted with the corresponding public key (Fig. 6).

Key Features of Asymmetric Key Cryptography:

Key Pair: It involves two keys.

- 1. **Public Key:** This key can be shared with anyone. It is used to encrypt data or verify digital signatures.
- 2. **Private Key:** This key must be kept secret. It is used to decrypt data or create digital signatures.

Applications of Cryptography

Cryptography plays a crucial role in ensuring the security and integrity of data used by various applications across different domains. Cryptography has multiple applications, such as:

1. **Secure Communication:** Cryptography is widely used to protect communication over networks. Protocols like HTTPS for secure browsing utilise encryption to safeguard data transmitted between web servers and clients.
2. **Data Protection:** Encryption is employed to secure sensitive data stored in databases, file systems, and cloud storage. This ensures that, even if data is intercepted or accessed without authorisation, it remains unreadable.
3. **Digital Signatures:** Cryptography enables the creation of digital signatures, which verify the authenticity and integrity of electronic documents and messages. This is essential in legal agreements, financial transactions, and software distribution.
4. **Authentication:** Cryptographic techniques are integral to authenticating users and devices. Methods such as password hashing, multi-factor authentication (MFA), and public key infrastructure (PKI) ensure that only authorised individuals have access to systems and data.
5. **Secure Email:** Email encryption protocols (like PGP and S/MIME) protect the contents of emails from unauthorised access and ensure that messages are sent and received securely.
6. **Virtual Private Networks (VPNs):** VPNs rely on cryptography to secure internet connections, safeguarding data sent over unsecured networks by encrypting the link between the user's device and the VPN server.
7. **Blockchain and Cryptocurrencies:** Cryptography secures transactions and controls the creation of new units in cryptocurrencies like Bitcoin. It ensures the integrity of the blockchain, enabling secure peer-to-peer transactions without a central authority.
8. **Secure File Sharing:** Cryptographic techniques are used in applications that enable secure file sharing and collaborative work environments, ensuring that shared documents remain confidential and tamper-proof.
9. **Internet of Things (IoT):** With the proliferation of IoT devices, cryptography becomes essential for securing communication between devices, protecting user data, and ensuring the integrity of information transmitted across networks.
10. **Secure Software Updates:** Cryptography ensures that software updates are authentic and have not been tampered with during transmission, protecting users from malicious code injections.
11. **Health Information Protection:** In the healthcare sector, cryptography is used to secure patient records and ensure compliance with regulations like HIPAA by protecting sensitive health information.

Recent Trends in Cryptography

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a form of public-key cryptography based on the mathematical structure of elliptic curves over finite fields. It offers a method for securing communications and data, providing encryption, digital signatures, and key exchange. One of the most significant advantages of ECC is its efficiency. With its much smaller key sizes, it offers a higher level of security compared to other cryptographic systems, such as RSA. For example, a 256-bit key in ECC provides comparable security to a 3072-bit key in RSA. In ECC, a private key is a randomly selected integer, while the public key is derived from a point on the elliptic curve multiplied by the private key. This one-way function makes it difficult for adversaries to decipher the private key from the public key. ECC is widely used in various applications, including secure communications (such as HTTPS), digital signatures (like ECDSA), and key agreement protocols (such as ECDH). It is especially useful in environments with constrained resources, such as mobile devices and IoT systems.

Given our growing dependence on devices with limited computing power, like mobile phones, ECC offers a refined solution through the complex mathematics of elliptic curves, producing smaller keys that are more resistant to attacks. The benefits of ECC over earlier public-key cryptosystems are clear, and it has already been adopted by entities such as the US government, Bitcoin, and Apple's iMessage service. While first-generation systems like RSA remain effective in many contexts, ECC is set to become the new standard for online privacy and security, especially with the advent of quantum computing.

Quantum Cryptography

Quantum cryptography leverages the principles of quantum mechanics to secure data in a manner that is resistant to the many vulnerabilities found in traditional cryptosystems. Unlike other encryption methods that depend on mathematical principles, quantum cryptography utilises the laws of physics to protect data, making it theoretically immune to hacking. Because it is impossible to observe a quantum state without altering it, any attempts to covertly access quantum-encoded information would be promptly detected.

Originally proposed in 1984, quantum encryption operates by transmitting photon light particles through a fiber-optic cable to establish a private key between the sender and receiver. These photons travel in a single direction, with each one representing a bit of data, either 0 or 1. A polarised filter on the sender's end adjusts the physical orientation of each photon to a specific angle, while the receiver employs two beam splitters to interpret the position of each photon. The sender and receiver then compare the sent photon positions with the decoded ones, determining the key based on the matches.

Quantum cryptography offers several advantages over traditional cryptographic methods, as it does not rely on mathematical equations that could potentially be solved. It inherently prevents eavesdropping, since quantum data cannot be observed without modification, and it can be effectively integrated with other encryption protocols. It allows users to digitally share a private encryption key that remains uncopyable during transmission. Once shared, this key can be utilised to encrypt and decrypt subsequent messages with minimal compromise risk.

However, quantum cryptography faces numerous challenges and limitations that currently hinder its practical application. As quantum computing is still transitioning from theoretical models to practical use, quantum cryptography is susceptible to errors caused by unintended changes in photon polarisation.

Additionally, quantum cryptography requires specialised infrastructure. According to IBM (<https://www.ibm.com/think/topics/cryptography#:~:text=Cryptography%20is%20the%20practice%20of,and%20ability%20to%20decrypt%20it.>), fiber-optic lines are essential for transmitting photons, but they have a limited range of approximately 248 to 310 miles, with ongoing research aimed at extending this distance. Furthermore, quantum cryptography systems are constrained by the number of destinations they can transmit data to, as these systems depend on the specific orientation of unique photons and cannot send signals to more than one intended recipient simultaneously.

The current study presents a comprehensive hybrid framework designed specifically for banks and financial institutions, to address the potential vulnerabilities of financial data during the migration to quantum computing. This framework aims to facilitate a smooth and secure transition into the post-quantum cryptography era, where traditional encryption methods may no longer be sufficient to safeguard sensitive information. The proposed hybrid framework integrates both existing cryptographic techniques and emerging post-quantum solutions, allowing organisations to benefit from the strengths of both approaches while minimising the risks associated with data exposure during this critical transition period. By leveraging traditional encryption methods for less sensitive data and adopting more advanced post-quantum cryptographic techniques for their most critical assets, banks and financial institutions can enhance their overall security posture.

Cryptography Implementation Banking Ecosystem

Encryption algorithms are essential for securing banking transactions. They protect sensitive data such as login credentials, account information, and transaction details from unauthorised access and eavesdropping. During a net banking transaction where an amount is credited to a sender, the encryption process establishes a secure session using asymmetric encryption for authentication and key exchange, followed by symmetric encryption for the secure transmission of transaction details. This process ensures the confidentiality, integrity, and security of sensitive financial information throughout the transaction. In this study, researchers have considered net banking and UPI transactions. Net banking transactions involve cryptographic systems at various levels.

Steps in the Encryption Process for a Net Banking Transaction

1. Secure Session Establishment

- **User Initiates the Transaction:** The user logs into their net banking account and initiates a transaction to credit an amount to a sender’s account.
- **Establishing HTTPS Connection:** The user’s browser requests to connect to the bank’s server over HTTPS, which uses Transport Layer Security (TLS). This establishes an encrypted connection between the user’s device and the bank’s server. TLS is the protocol that ensures an encrypted connection between the user’s device and the bank’s server. It uses a combination of asymmetric encryption for the initial handshake and symmetric encryption for the data exchange afterward (Fig. 7).

2. Asymmetric Encryption for Authentication and Key Exchange

- **Server Sends Digital Certificate:** The bank’s server sends its digital certificate to the user’s browser. The certificate

includes the bank’s public key and is signed by a trusted certification authority (CA), using RSA or ECDSA (Elliptic Curve Digital Signature Algorithm) to sign the certificate.

- **Browser Validates Certificate:** The user’s browser verifies the authenticity of the certificate to ensure it is communicating with the legitimate bank server.
- **Session Key Creation:** The user’s browser generates a session key (symmetric key) for encrypting data for the current session. Advanced Encryption Standards (AES) is commonly used for symmetric encryption.
- **Encrypting Session Key:** The browser encrypts this session key using the bank’s public key (obtained from the digital certificate) and sends it to the bank’s server. RSA (Rivest-Shamir-Adleman) is commonly used for secure key exchange during this phase.
- **Server Decrypts Session Key:** The bank’s server decrypts the session key using its private key, allowing both the user’s device and the bank’s server to use this session key for subsequent encryption (Fig. 8).

3. **Transaction Data Encryption**

- **User Enters Transaction Details:** The user enters the amount to be credited and the recipient's account information in the net banking portal.
- **Encrypting Transaction Details:** Before sending this information over the network, the user's browser encrypts the transaction details (sender's account, recipient's account, amount) using the session key (Fig. 9).
- **Sending Encrypted Data:** The encrypted transaction data is sent to the bank's server.

4. **Bank Processes the Transaction**

- **Decrypting Transaction Details:** Upon receiving the encrypted transaction details, the bank's server uses the session key to decrypt the information using AES algorithm, consistent with what was used for encryption during the previous step.
- **Validation:** The bank verifies the sender's account balance and confirms that the transaction complies with banking regulations and anti-fraud checks.

- **Credit Transaction:** If everything is valid, the bank credits the specified amount to the recipient's account and debits it from the sender's account (Fig. 10).

5. **Acknowledgment and Confirmation**

- **Generating Confirmation:** Once the transaction is completed, the bank prepares a confirmation message, which includes information about the transaction (amount credited, transaction ID, etc.).
- **Encrypting Confirmation:** The bank encrypts this confirmation message using the session key and sends it back to the user's browser.
- **User Receives Confirmation:** The user's browser decrypts the confirmation message using the session key, allowing the user to see the transaction result (Fig. 11).

6. **Session Termination**

- **Closure of Secure Session:** After the transaction process is completed and the confirmation is displayed to the user, the secure session can be terminated. While the session key is deleted from both the client and server sides, the initial asymmetric keys remain unchanged for future secure sessions (Fig. 12).

Cryptography Implementation in UPI Transactions

Unified Payments Interface (UPI) is a real-time payment system that enables users to transfer money between bank accounts using a mobile device. The encryption process plays a crucial role in ensuring the security of UPI transactions, including when an amount is credited to the sender's bank account. It involves multiple layers of encryption for transaction data, user authentication, and secure communication between the user's device and the bank's server. This comprehensive security framework protects users against unauthorised transactions and potential cyber threats, providing a safe and efficient payment experience.

Overview of the UPI Transaction Process

1. **User Authentication**

- **Initiating the UPI Transaction:** The user opens a UPI-enabled application on their mobile device (e.g., a banking app or a payments app) and chooses to make a payment or a transfer.
- **Authentication:** The users must authenticate themselves using a secure method, such as a PIN, biometric authentication (fingerprint or facial recognition), or other secure login processes. This initial authentication ensures that only authorised users can initiate a transaction (Fig. 13).

2. **Secure Connection Establishment**

- **Establishing HTTPS Connection:** The UPI application establishes a secure connection with the bank's server using HTTPS (HyperText Transfer Protocol Secure), employing encryption protocols, to ensure that data transferred between the user's device and the bank's server is secure. The server sends its digital certificate to the client. This certificate includes the server

public key and is issued by a certification authority. After validating the certificate, the client generates a session key (symmetric key) using the AES algorithm. The session key is a random number that ensures unique encryption for that session. The client encrypts the session key using the server's public key (obtained from the digital certificate) and sends it to the server. The server uses its private key to decrypt the session key sent by the client. Now, both the client and the server share the same session key (Fig. 14).

3. **Transaction Details Input**

- **Entering Transaction Information:** The user enters the transaction details, including the recipient's UPI ID or bank account number, the amount to be credited, and potentially a note or reference.
- **Generating a Unique Transaction ID:** The UPI application generates a unique transaction ID for tracking purposes (Fig. 15).

4. Data Encryption

- **Encrypting Transaction Data:** Before sending this transaction data over the network, the UPI application encrypts the sensitive information using AES symmetric encryption (with a session key). RSA (Rivest-Shamir-Adleman) might be used to encrypt the session key itself or certain sensitive elements, allowing secure key exchange without sharing private keys.
- **Encryption Process:** The transaction details include the sender's account information, the recipient's details, the amount, and the transaction ID. Encryption ensures that even if attackers intercept the data, they cannot read it without the appropriate keys.

5. Sending Encrypted Data

- **Transmission:** The encrypted transaction data is transmitted to the bank's server through the secure TLS/HTTPS connection established previously (Fig. 16).

6. Bank Server Processing

- **Receiving the Encrypted Data:** The bank's server receives the encrypted transaction information and uses the appropriate decryption method to decrypt the data, typically using the same symmetric encryption algorithm (e.g., AES) employed during encryption.
- **Validation:** The bank verifies the transaction details, ensuring that the sender has sufficient funds, and that the transaction is legitimate. This may include checking against fraud detection systems (Fig. 17).

7. Crediting the Amount

- **Transaction Execution:** If all checks are successful, the bank executes the transaction by debiting the sender's account and crediting the recipient's account accordingly.
- **Acknowledgment Generation:** After processing the transaction, the bank generates a confirmation message indicating the success or failure of the transaction (Fig. 18).

8. Confirmation and Secure Messaging

- **Encrypting Confirmation Message:** The bank encrypts the confirmation message using the same encryption method applied during the transaction process (Fig. 19).

- **Sending Back Confirmation:** The encrypted confirmation message is sent back to the user's device.

9. User Receives Confirmation

- **Decryption of Confirmation:** The UPI application on the user's device decrypts the confirmation message using the appropriate key, allowing the user to see the result of the transaction (whether it was successful or not).

10. Session Termination

- **End of Secure Session:** Once the transaction is complete, the secure session may be terminated, and session keys can be cleared from memory to ensure no sensitive information remains accessible (Fig. 20).

Quantum Cyber Threats: Compromising Cryptographic System

When the encryption process in net banking is compromised, it opens the door for various cyberattacks that can lead to unauthorised access, data breaches, and financial losses. Robust and up-to-date encryption practices, along with comprehensive security measures, are crucial in mitigating these threats and protecting users' sensitive information. If the encryption process in the banking ecosystem is compromised, it can lead to several types of cyberattacks that specifically target or exploit weaknesses in encryption methods. Here are some of the possible cyberattacks:

Man-in-the-Middle (MitM) Attacks

In a man-in-the-middle (MitM) attack, malicious actors covertly intercept and manipulate the communication occurring between a user and their banking server. This type of attack poses a significant threat, especially in environments where encryption is weak or not properly implemented. When encryption is insufficient, attackers can exploit vulnerabilities to decrypt the data exchanged between the user and the bank's server. This means that they can access sensitive information that is typically protected, such as login credentials, personal identification numbers (PINs), and detailed transaction information. Once they have successfully decrypted the data, attackers can engage in various malicious activities. For instance, they may steal the user's login credentials, allowing them unauthorised access to the user's bank account (Fig. 21). Furthermore, they can not only obtain sensitive information but also alter details of the transactions without either the user or the bank being aware. This could involve changing the amount of money being sent, the recipient's account, or even redirecting funds to the attacker's own account. The implications of such an attack are severe. User accounts might get compromised, resulting in financial loss, while banks may

face liability issues and reputational damage. Therefore, it is crucial for organisations to implement strong encryption techniques, conduct regular security audits, and remain vigilant against potential vulnerabilities to defend against man-in-the-middle attacks effectively.

Ciphertext Manipulation

Ciphertext manipulation attacks occur when malicious individuals gain unauthorised access to encrypted data, known as ciphertext, and attempt to alter it before it is decrypted by the intended recipient. This type of attack becomes possible primarily when the encryption mechanism used does not adequately ensure the integrity of the data. In scenarios where integrity checks are weak or absent, attackers may intercept encrypted messages and modify the ciphertext in a way that avoids detection. For example, they might change transaction amounts, recipient details, or other critical information embedded within the ciphertext. Once altered, the manipulated ciphertext can be sent to the receiver (typically a banking server or application) for decryption. When the recipient decrypts the manipulated ciphertext, they may be led to believe that

they are processing a legitimate transaction. If the receiver fails to detect the unauthorised changes, it may result in fraudulent transfers or payments being executed against a user's account. This can have dire consequences, including financial losses for the user and potential liability for the financial institution involved. To protect against ciphertext manipulation attacks, it is crucial to implement robust integrity verification methods, such as digital signatures or HMAC (Hash-based Message Authentication Code), alongside strong encryption protocols. These measures can help ensure that any unauthorised modifications to the ciphertext are detected prior to decryption, thereby safeguarding the integrity of the transaction data.

Replay Attacks

A replay attack is a type of cyber threat wherein attackers intercept and capture encrypted data from a previous transaction and then resend the same data to the bank at a later time. The intent behind this malicious activity is to deceive the bank into processing the same transaction again, effectively tricking the system into believing that a legitimate transaction is being executed. If the bank does not have adequate safeguards in place, such as timestamps, session identifiers, or unique transaction IDs, the system may unknowingly process the same transaction multiple times. This can lead to serious consequences, such as double transactions, where a user is charged twice for the same payment, or unauthorised payments, where funds are transferred without the account holder's consent or knowledge (Fig. 22).

Weak Key Attacks

If a bank employs weak encryption keys or algorithms that have known vulnerabilities, such as outdated methods like DES (Data Encryption Standard), attackers can execute brute force attacks to uncover the encryption key. Once they successfully obtain the key, attackers can decrypt sensitive information, including account credentials and transaction data, which may result in unauthorised access to users' accounts and data.

Cryptanalysis Attacks

Cryptanalysis attacks involve the use of sophisticated mathematical techniques to examine, analyse, and exploit vulnerabilities inherent in encryption algorithms themselves. Unlike brute force attacks, where an attacker systematically tries every possible key until they find the correct one, cryptanalysis seeks to identify flaws in the algorithm or its implementation that can be exploited to break the encryption without needing to guess the key. Attackers may analyse the structure of the encryption algorithm, studying patterns, weaknesses, and potential shortcuts that allow them to decrypt data more efficiently. They may leverage relationships between plaintext, ciphertext, and keys, employing various strategies such as frequency analysis, known-plaintext attacks, or chosen-ciphertext attacks. For example, if an encryption algorithm exhibits certain statistical patterns or predictable outputs in response to specific inputs, attackers can exploit these inconsistencies to decrypt messages without the decryption key.

Session Hijacking

Session hijacking is a type of cyberattack in which an attacker exploits vulnerabilities within the encryption process to gain unauthorised access to active user sessions. If they succeed in compromising the security measures, they can capture session tokens or cookies that are typically used to authenticate users during online transactions or interactions with web applications. When a user logs into a system, a session is established, often accompanied by a unique session token or cookie that acts as a digital key, granting access to the user's account for the duration of that session. If an attacker can obtain this session token—through techniques like man-in-the-middle attacks, sniffing network traffic, or exploiting security flaws—they can impersonate the legitimate user as if they were logged in. Once the attacker has successfully hijacked the session, they gain the capability to access sensitive account details, conduct unauthorised transactions, change account settings, or even extract personal information. This poses serious risks, including financial loss and potential damage to the user's reputation.

SSL Stripping Attacks

The attackers downgrade secure HTTPS connections to unencrypted HTTP connections, allowing them to intercept data. If the encryption is not properly enforced, users may unknowingly transmit sensitive information over insecure channels. Attackers can capture sensitive data, such as login credentials and personal information, since the data is not encrypted in the downgraded connection.

Phishing for Encryption Keys

Attackers may use social engineering techniques to trick users or bank employees into revealing encryption keys or passwords that protect encrypted data. This could lead to unauthorised access of sensitive accounts and data.

Data Breaches and Exfiltration

If attackers breach a bank's database and obtain encrypted data, they may store this data with the intent of decrypting it offline later, especially if weak encryption algorithms are used. Compromised personal and financial data could be decrypted, leading to fraud and identity theft.

PQC Standards by National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is actively working to develop standards for cryptographic algorithms that can withstand the threats posed by quantum computing. As part of this effort, several Federal Information Processing Standards (FIPS) have been proposed or finalised, focusing on lattice-based and hash-based cryptographic schemes.

CRYSTALS-Kyber

CRYSTALS-Kyber is a key encapsulation mechanism (KEM) that enables secure key exchange and encryption. It is based on lattice cryptography, specifically leveraging the hardness of the Module Learning With Errors (LWE) problem. CRYSTALS-Kyber offers a combination of strong security, efficient performance, and relatively small key sizes, making it suitable for real-world implementation even in resource-constrained environments. Its efficiency in both key generation and encryption/decryption processes makes it a viable alternative to conventional encryption methods amidst the quantum threat landscape.

CRYSTALS-Dilithium

CRYSTALS-Dilithium is a digital signature scheme that provides integrity and authenticity for digital messages. Like CRYSTALS-Kyber, it is also based on lattice cryptography and focuses on achieving robust security against quantum attacks. It is recognised for its strong security guarantees and efficiency, allowing for quicker signing and verification times. Its balance of security and performance makes it a suitable choice for applications requiring digital signatures.

FALCON

FALCON (Fast-Fourier Lattice-based Compact Signatures) is another digital signature scheme but is designed for use cases where CRYSTALS-Dilithium signatures may be too large or inefficient. It also employs a lattice-based approach to offer post-quantum security. FALCON is particularly useful for applications where smaller signature sizes and faster verification times are critical, such as in embedded systems and constrained environments. One of the key advantages of FALCON is its compact signature size, which makes it more suitable for scenarios with limited bandwidth or storage capacity. By offering a smaller footprint while maintaining security, FALCON addresses specific use cases that require optimised performance.

SPHINCS+

SPHINCS+ is a stateless hash-based digital signature scheme that avoids dependence on lattice security. Instead, it relies on the security of cryptographic hash functions, making it distinct from the other algorithms listed. SPHINCS+ is applicable in environments where traditional public key infrastructure (PKI) solutions may be leveraged, and it is particularly well-suited to applications

requiring long-term signature validity, such as blockchain technology or secure archiving. This algorithm's robustness comes from its resistance to quantum attacks while utilising established cryptographic primitives like hash functions. SPHINCS+ provides a unique signing approach that opens alternative paths for securing digital communications without relying solely on lattice security.

Proposed Framework

In the current study, the researchers have proposed a hybrid approach to implement a post- quantum cryptographic framework for banking and financial purposes. In the current study, the proposed framework is designed and developed and tested for two banking operations:

- (i) Net banking/Mobile Banking
- (ii) UPI

The proposed framework used ML-KEM-1024 (1024 key bits) algorithm for encryption and decryption and DSA algorithm for hash/ message digest generation.

In this study, the framework designed by ISB Institute of Data was tested by QClairvoyance Quantum Labs Pvt. Ltd and Quantum AI Global to identify the feasibility of the proposed framework.

QClairvoyance Quantum Labs Pvt. Ltd tested the framework for net banking. They tested the framework using their secure VPN called Quantum Secure VPN. The proposed framework for Unified Payment Interface (UPI) was tested by Quantum AI Global. They have used their QSleeve tool for testing the feasibility of the framework.

The test reports for the net banking and UPI transactions are enclosed in Appendix B. ML-KEM-1024 and ML-DSA, both NIST-approved post-quantum Key Encapsulation Mechanism and digital signature generation algorithms were used. The pseudocode for ML-KEM key generation, encryption, and decryption algorithm and ML-DSA hash generation algorithm are enclosed in Appendix C. The following section explains the working of ML-KEM.



ML-KEM: Multilevel Key Encapsulation Mechanism

ML-KEM, or Multilevel Key Encapsulation Mechanism, is a cryptographic protocol designed primarily for secure key exchange in scenarios involving multiple hierarchical levels of security. It is often used in systems that require different security levels among users or devices, allowing flexible and secure sharing of encryption keys. It is based on the concepts of CRYSTALS-Kyber. ML-KEM consists of three algorithms and a collection of parameter sets. The three algorithms are:

- 1. A probabilistic key generation algorithm denoted by KeyGen
- 2. A probabilistic “encapsulation” algorithm denoted by Encaps
- 3. A deterministic “decapsulation” algorithm denoted by Decaps

ML-KEM algorithm is used to establish a shared secret key between two parties and perform encryption and decryption. For example, if two parties, Alice (customer) and Bob (Bank Server) would like to send confidential message among themselves, the process begins with Alice executing the KeyGen function (refer Appendix A) to generate a public encapsulation key and a private decapsulation key.

After obtaining Alice’s encapsulation key, Bob uses the Encaps algorithm (refer Appendix A), which generates his copy (K) of the shared secret key along with the corresponding ciphertext. Bob transmits the ciphertext back to Alice, who completes the process by applying the Decaps algorithm with her decapsulation key and the ciphertext (refer

Appendix A). This final step yields Alice’s copy (K’) of the shared secret key. Following this procedure, Alice and Bob wish to confirm that their outputs meet the condition ($K' = K$) and that this value represents a secure, randomly shared secret key (refer Appendix A for working of ML-KEM Algorithm)

ML-KEM Key Generation

The key generation algorithm for ML-KEM, denoted as ML-KEM.KeyGen, does not accept any external input; instead, it generates a random number internally and produces both an encapsulation key and a decapsulation key. The encapsulation key is intended for public use, while the decapsulation key must remain confidential. The seed ((d, z)) created in steps 1 and 2 of ML-KEM.KeyGen can be stored for later expansion using the ML-KEM.KeyGen_internal function (refer Appendix A). Since this seed can be utilised to compute the decapsulation key, it is considered sensitive data and should be protected with the same level of safeguards as the decapsulation key.

Working of ML-KEM

1. Key Generation

- Each participant (user or device) generates a public-private key pair. The public key is shared with others, while the private key is kept secret (Fig. 23).

2. Symmetric Key Generation

- The participant who needs to send a message generates a new symmetric session key for each communication session. This key is used for encrypting the actual data (Fig. 24).

3. Key Encapsulation

- The sender encapsulates the symmetric session key using the public key of the recipient. This process creates an encapsulated key (encrypted symmetric key) that can be securely sent over the communication channel. The encapsulation process ensures that even if an attacker intercepts the encapsulated key, they cannot retrieve the symmetric key without the recipient’s private key (Fig. 25).

4. Transmission

- The encapsulated key is transmitted securely to the intended recipient along with any necessary metadata and identifier information (Fig. 26).

5. Decapsulation

- Upon receiving the encapsulated key, the recipient uses their private key to decrypt the encapsulated key. This process retrieves the symmetric session key that was originally generated by the sender. Decapsulation ensures that only the intended recipient can access the symmetric key needed for decryption of the message content (Fig. 27).

6. Data Encryption and Decryption

- The sender then uses the symmetric session key to encrypt the actual message or data that is to be transmitted. The encrypted message is sent to the recipient, who uses the symmetric session key (retrieved during decapsulation) to decrypt the message (Fig. 28).



PQC Migration Framework for Secured Communication: Net Banking

The proposed PQC framework for net banking/mobile banking enhanced with post-quantum cryptography (PQC) aims to safeguard against both classical and quantum computing attacks. This enhanced security protocol operates across multiple stages of the banking ecosystem, such as transactions, balance enquiries, and more. The framework aims to ensure the confidentiality and integrity of sensitive data exchanged between users such as the sender, the sender’s bank, the recipient’s bank, and an intermediary system such as the National Payments Corporation of India (NPCI) for a fund transaction, as well as between the bank server and the bank database.

NIST-approved ML-KEM with key 1024 bytes is incorporated to protect critical infrastructure. The integration of PQC, particularly using these advanced algorithms, strengthens the existing security measures and provides a robust defense against a wider range of potential threats, including those posed by future quantum computing. This enhanced PQC framework for fund transfer incorporates a multi-layer security approach using post-quantum cryptography (PQC), specifically leveraging ML-KEM for key exchange and AES for data encryption. The system is designed to be resilient against both classical and quantum attacks, with security measures implemented at each stage of the transaction. The process involves the user, the sender’s bank, the recipient’s bank, and an intermediary system like NPCI, all employing PQC daemons for localised encryption and decryption. The system also incorporates a hybrid approach, combining established classical cryptographic techniques with PQC algorithms to enhance security and efficiency. The step by step working for the proposed framework is illustrated below.



1. User Login and Authentication

The sender initiates the transaction via their web browser or mobile app, establishing a secure HTTPS connection with the bank server. Simultaneously, an ML-KEM handshake is performed. Both the user device and the bank server generate key pairs (public and private). The user’s public key is shared with the bank, and vice versa. The user computes a shared secret key, E1, using their private key, the bank’s public key, and a random number. The bank server independently computes E2 using its private key, the user’s public key, and a random number (via the ML-KEM-1024 algorithm). E1 and E2 must match for successful authentication. The user’s encrypted login credentials (username, password hash) are then sent to the bank server using AES encryption with a key derived from E1 and E2. The server validates these credentials; and successful authentication results in a login success message being sent to the user. If credentials are not validated, the user receives three login attempts before their account gets locked. The encrypted request is then forwarded to an intermediary system (e.g., NPCI). The intermediary decrypts the request (using a key derived from E1 and E2) and validates the credentials against the bank database. An encrypted authentication response (session token and status), also encrypted with AES, is sent back to the user’s browser (Fig. 29).

2. Transaction Initiation

The user selects “Funds Transfer,” enters recipient details (account number, IFSC

code, amount), and the transaction request is encrypted using AES with the session key established in step I. The encrypted request is sent to the sender’s bank. The sender’s bank performs an ML-KEM handshake with an intermediary (like NPCI). The intermediary decrypts the request and sends an encrypted validation request to the recipient’s bank (using AES) (Fig. 30).

3. Recipient Validation

The intermediary validates the recipient by contacting the recipient’s bank. An ML-KEM handshake is performed, generating shared secret keys E3 (intermediary) and E4 (recipient bank). E3 and E4 must match for successful validation. Upon successful validation, the transaction proceeds to the next step (Fig. 31).

4. OTP Verification and Transaction Processing

After successful recipient validation, the sender’s bank verifies the sufficiency of funds. If sufficient, an encrypted OTP (using AES) is generated and sent for validation. Upon successful OTP validation, the amount is debited from the sender and credited to the recipient (Fig. 32).

5. Transaction Confirmation and Notification

The recipient’s bank sends confirmation to the intermediary, which routes it to the sender’s bank. The sender’s bank then sends an encrypted (AES) transaction status update to the user’s browser (Fig. 33).

Infrastructure Implementation

The framework uses PQC daemons (client, sender bank, intermediary, recipient bank) for local encryption/decryption, eliminating the transmission of decrypted data over insecure channels. Each entity handles encryption/decryption independently, using the session key derived from DH and ML-KEM. ML-KEM facilitates secure key exchange, while AES encryption bolsters protection against both classical and quantum attacks. NPCI plays a crucial role in routing and validating transactions.

QClairvoyance tested the framework using a Quantum Secure VPN, a cutting-edge, enterprise-grade Virtual Private Network (VPN) that incorporates quantum-resistant cryptography. Quantum Secure VPN also used ML-KEM-1024 & QRNG (refer Appendix C for details about QVPN) (Fig. 34).

Proposed Framework for Secured Communication between Bank Server and Data Centers

Quantum Key Distribution (QKD) is a method used to securely transmit encryption keys between two parties, such as bank servers and data centers, mitigating the risks posed by post-quantum computing cyber threats, leveraging the principles of quantum mechanics. This is achieved by encoding key information in quantum states, such as the polarisation of photons, which are inherently susceptible to disturbance upon observation by

an unauthorised party. It allows the generation of a shared secret key that can be used for symmetric encryption, thereby ensuring secure communication. For relatively short distances, a direct point-to-point QKD link using fiber-optics is likely feasible. Current QKD systems using fiber-optics can operate over distances of tens of kilometers without the need for intermediate quantum repeaters (though signal attenuation increases with distance). In this case, a dedicated fiber-optic cable could be installed to create a secure quantum channel between the bank server and the data center. For very long distances, the technological hurdles of QKD implementation become considerable. Fiber-optic cable quality significantly affects QKD performance. High-quality, low-loss fiber is essential for optimal performance, especially over longer distances. While QKD secures the key exchange, classical channels used for data transmission and communication regarding basis selection need to be robustly secured against attacks. Implementing QKD involves considerable costs related to equipment, installation, maintenance, and integration with existing network infrastructure. The economic viability needs careful consideration. The implementation of QKD for mitigating cyber threats heavily depends on distances and current technological advancements. In the current study, the QKD technology is proposed, assuming the distance between the bank's server and its data center is less than 100 kms. The proposed framework leverages Quantum Key Distribution (QKD) and the Multi-Layer Key Encapsulation Mechanism (ML-KEM) to establish a highly secure communication

channel between a bank's server and its data centers, mitigating the risks posed by post-quantum computing cyber threats. The framework combines the security of QKD for initial key generation, the enhanced security of ML-KEM for key encapsulation, and the efficiency of symmetric encryption for data transmission. The proposed framework combines the security of QKD for key exchange with the efficiency of symmetric encryption for data transmission.

Key Distribution and Key Derivation using QKD

1. **Network Infrastructure:** A dedicated, secure quantum communication network is established between the bank server and the data center using fiber-optics or free-space optics, designed to minimise signal loss and interference.
2. **Quantum Key Generation:** The bank server and the data center each utilise QKD devices to generate a series of qubits encoding bits (0s and 1s) using properties like photon polarisation. Qubit transmission occurs over the secure quantum channel.
3. **Measurement and Basis Selection:** The data center (receiver) randomly selects a measurement basis for each incoming qubit and records the results. The bank server (sender) independently communicates its chosen basis over a separate, secure classical channel.
4. **Key Sifting:** Qubits with mismatched measurement bases are discarded. Matching bits form the raw key (K_{QKD}).
5. **Error Correction and Privacy Amplification:** Classical error correction algorithms are applied to correct errors in K_{QKD} . Privacy amplification techniques enhance key security by reducing its size and removing potentially compromised bits. The resulting key is the final shared secret key (K_{QKD}).
6. **Key Derivation Function (KDF):** K_{QKD} serves as an input for a cryptographically secure KDF to generate multiple keys for different purposes:
 - **K_{AES} :** A symmetric key for encrypting transmitted data (using AES).
 - **K_{MLKEM} :** A key specifically for ML-KEM operations.

Data Encryption and Transmission

- 1. **ML-KEM Encapsulation:** K_AES is encapsulated (encrypted) using the ML-KEM algorithm with K_MLKEM. This provides an additional layer of security for the AES encryption key.
- 2. **Data Encryption:** All data transmitted between the bank server and the data center is encrypted using AES with K_AES.
- 3. **Data Transfer:** The encapsulated K_AES and encrypted data are transferred via a secure classical communication channel (e.g., using HTTPS or TLS).
- 4. **ML-KEM Decapsulation and Data Decryption:** The receiving end uses K_QKD (through the KDF) to obtain K_MLKEM, which is then used to decapsulate (decrypt) K_AES. Post this, K_AES is used to decrypt the transmitted data.

Security Monitoring and Key Management

- 1. **Eavesdropping Detection:** QKD’s inherent ability to detect eavesdropping is crucial. If any interference with the quantum channel during key generation is detected, the existing key is discarded, and a new key is generated.
- 2. **Key Management System:** A robust key management system handles key storage, distribution, rotation, and revocation for both K_QKD and K_MLKEM.

This enhanced framework leverages QKD for secure key generation and ML-KEM for additional key encapsulation, offering robust protection against both classical and quantum attacks. The hybrid approach combines the strengths of both technologies for enhanced security and efficiency in securing data transmission between bank servers and data centers.



Proposed PQC Framework for UPI Transaction

Unified Payments Interface (UPI) is a real-time payment system developed by the National Payments Corporation of India (NPCI) that facilitates peer-to-peer and person-to-merchant transactions through mobile devices. The working of UPI involves linking multiple bank accounts to a single mobile application, allowing users to send and receive money seamlessly. When a user initiates a transaction, they select the recipient’s UPI ID, enter the amount, and authenticate the transaction using a secure PIN. The UPI app generates a transaction request, which is transmitted over a secure connection to the bank’s server, where the authenticity is verified. Upon successful verification, the amount is debited from the sender’s account and credited to the recipient’s account instantly, with both parties receiving real-time notifications. UPI supports various features, including the ability to schedule payments, make bill payments, and access a host of services through one platform, all while ensuring high levels of security through encryption and multi-factor authentication. This innovative payment system has transformed the way digital transactions are conducted in India, making them more accessible and convenient for users. The Unified Payments Interface (UPI) ecosystem involves various stakeholders who play crucial roles in its functioning and success. The primary entities in a UPI transaction are:

- | | |
|---|---|
| 1. National Payments Corporation of India (NPCI): The central entity managing the UPI system, ensuring secure routing, validation, and settlement of transactions between banks. | 4. Sender’s DB and Receiver’s DB: Databases at the respective banks, storing transaction details, balances, and validation results. |
| 2. Sender Banks: The bank where the sender’s account is held. | 5. Merchants: Merchants utilise UPI for payment collection from customers via QR codes or payment links. They benefit from instant payments, reduced transaction costs, and enhanced customer convenience. |
| 3. Payment Service Providers (PSPs): Entities that facilitate UPI transactions by offering mobile applications or payment platforms that allow users to perform transactions. These can include digital wallets and fintech companies that enhance the UPI experience. The UPI transaction includes Sender PSP and Receiver PSP. | 6. Consumers/Users: Individual users who utilise UPI to make payments, transfer money to friends or family, pay bills, and make purchases at merchant outlets. They are the end-users driving the adoption of UPI, for example sender and the recipient. |

Implementing post-quantum cryptography (PQC) frameworks, particularly utilising the Multilevel Key Encapsulation Mechanism (ML-KEM) for UPI (Unified Payments Interface) transactions necessitates a well-structured and systematic approach to effectively address the security challenges posed by the advancements in quantum computing technology. The PQC framework needs to be implemented by all entities involved in the transactions to ensure safe and secure transactions. In this study, researchers have used QSleeve to secure UPI transactions. QSleeve integrates ML-KEM-1024 bits for generation of keys and encryption and decryption and ML-DSA (Module-Lattice-Based Digital Signature Algorithm) for the generation of hash/digital signature. The proposed framework allows organisations to integrate quantum-safe protocols seamlessly into their existing infrastructure.

1. User Initiations, Authentication, and Handshake

The PSPs need to integrate a software toolkit that simplifies the integration of post-quantum cryptography algorithms, such as QSleeve SDK library, into their respective UPI applications and systems. Such a toolkit provides developers and users with the necessary tools and libraries to implement quantum-resistant cryptographic algorithms without needing deep expertise in cryptography. QSleeve offers quantum-safe protection by integrating ML-KEM algorithm for key generation, encryption, and decryption, as well as ML-DSA for digital signatures.

To execute a transaction, the user opens their UPI-enabled application, such as GPay or Paytm, on a mobile device and logs in using username and password, and then selects the option to make a payment or a transfer. The app and the bank server initiate a TLS handshake using ML-KEM-1024 bytes. This handshake establishes a secure channel for subsequent communication and a unique session ID is generated.

ML-KEM uses the session ID to generate the symmetric key used for secure

communication. The user credentials are encrypted by ML-KEM using QSleeve tool and are sent to the sender PSP. The sender PSP authenticates and verifies the data with the sender bank. The sender bank decrypts the data using its ML-KEM decryption algorithm and validates with the bank database. The bank database is also secured using PQC Crypto Module, such as QSleeve, developed by Quantum Global AI. It is a hardware security module (HSM) designed to enhance the security of applications and systems by incorporating post-quantum cryptography (PQC).

On successful validation and authentication, a login success or failure message is displayed on the user’s mobile device (Fig. 35).

2. Recipient Information, Validation, and Hash Generation

The user enters the recipient’s UPI ID. The sender PSP encrypts the recipient’s UPI ID by using ML-KEM encryption and generates a hash of the recipient’s UPI ID using ML-DSA and session ID. This hash provides data integrity. The app encrypts the hash using ML-KEM encryption algorithm before sending it to NPCI for validation. NPCI forwards the

encrypted hash to the recipient bank. The recipient bank validates the recipient’s UPI ID with its database and generates its own hash. Both hashes must match for the transaction to proceed (Fig. 36).

3. Transaction Details, ML-KEM, and Encryption

After successful validation, the user confirms the amount and enters their UPI PIN. The sender PSP’s app generates a symmetric session key. The app uses ML-KEM to encapsulate (encrypt) the session key. The bank, using its private key and the corresponding ML-KEM decryption algorithm, retrieves the session key. The app encrypts the transaction details (UPI PIN of the sender, receiver’s UPI ID, amount, and a hash of the entire transaction data, including the session ID) using symmetric key. This ensures data confidentiality during transmission. The sender’s bank validates the UPI PIN, checks the balance with its database and on successful validation, executes the transaction (Fig. 37).

4. Transaction Routing and Processing

The encrypted transaction details and the encapsulated session key are sent to the NPCI. The NPCI routes the transaction to the receiver bank (Fig. 38).

5. Funds Transfer and Confirmation

The receiver bank processes the transaction. It uses the retrieved session key to decrypt the transaction data. It generates and returns a hash of this decrypted data along with a transaction ID. If this hash matches the one included by the user’s app the transfer proceeds (Fig. 39).

6. Notification

The bank sends an encrypted confirmation (including the hash of the transaction) to the user’s app. The app decrypts the confirmation using the session key. The user receives a notification (Fig. 40).

Key Highlights of the Proposed PQC Framework

Quantum Secure Protection

The proposed framework is designed to safeguard data transmission and provide defense against future quantum decryption threats, ensuring a secure transition to post-

- 1. **Post-Quantum Cryptography (PQC)** for banks and financial institutions. This robust protection addresses the evolving cybersecurity risks associated with quantum computing.
- 2. **NIST-Standardised Algorithms:** By integrating NIST-approved algorithms such as ML-KEM and ML-DSA, the framework enhances its capability to deliver quantum resilience. This integration not only strengthens enterprise systems and communications but also ensures compliance with established industry standards for enhanced security.
- 3. **Minimal Changes to Existing Infrastructure:** A key advantage of the framework is its minimal impact on current infrastructure, as it supports hybrid implementation.
- 4. **Seamless Integration Across Platforms:** The framework is easily deployable in various environments—on-premises,

cloud, and hybrid—allowing banks and financial institutions to adopt quantum-safe protocols without disrupting existing infrastructures. This flexibility facilitates a smooth transition while maintaining operational continuity and efficiency.

5. **Comprehensive Security Across Use Cases:** By offering quantum-safe encryption for a wide range of applications, the framework covers essential areas such as remote access, site-to-site connectivity, IoT protection, and sensitive transactions. This holistic approach ensures comprehensive security for all digital interactions, safeguarding critical data in today’s interconnected world.
6. **Future-Ready Architecture:** The framework is built with future-proofing in mind, allowing banks and financial institutions to stay ahead of rapidly evolving quantum threats. By implementing this advanced architecture, businesses can adapt to emerging technologies and maintain a strong security posture.
7. **Performance Metrics:** The framework’s performance is backed by QClairvoyance Quantum Labs Pvt. Ltd. and Quantum Global AI, demonstrating its effectiveness for banks and financial institutions’ infrastructure, showcasing its reliability and efficiency in protecting sensitive information against quantum threats. Users can expect measurable improvements in security measures while maintaining operational speed and performance.

Key Encapsulation Security Considerations

A key encapsulation mechanism requires high-quality of entropy during the key pair generation and ciphertext generation steps.

Key Encapsulation Mechanisms (KEMs), including ML-KEM, do not inherently provide authentication. An adversary could substitute their own public key or ciphertext, establishing a shared secret key with either party. Therefore, any protocol using a KEM must incorporate mechanisms allowing Bob (recipient) to verify Alice’s (sender) public key and Alice to verify Bob’s ciphertext (or at least verify that the ciphertext originates from an authorised entity). This authentication is typically achieved through digital signatures or Message Authentication Codes (MACs) to ensure the integrity of the key exchange. The proposed framework thus integrates digital signatures to provide this essential authentication.

In the ML-KEM algorithm, if an adversary can substitute the copy of the public key for both Alice (sender) and Bob (recipient), an attacker can introduce a malicious public key that allows the same private key to be used for decapsulation, but the probability of decryption failure is marginally higher. As decryption failures can leak information about the secret decapsulation key, it is important that Alice keeps a secure copy of the public key as part of her secret key.

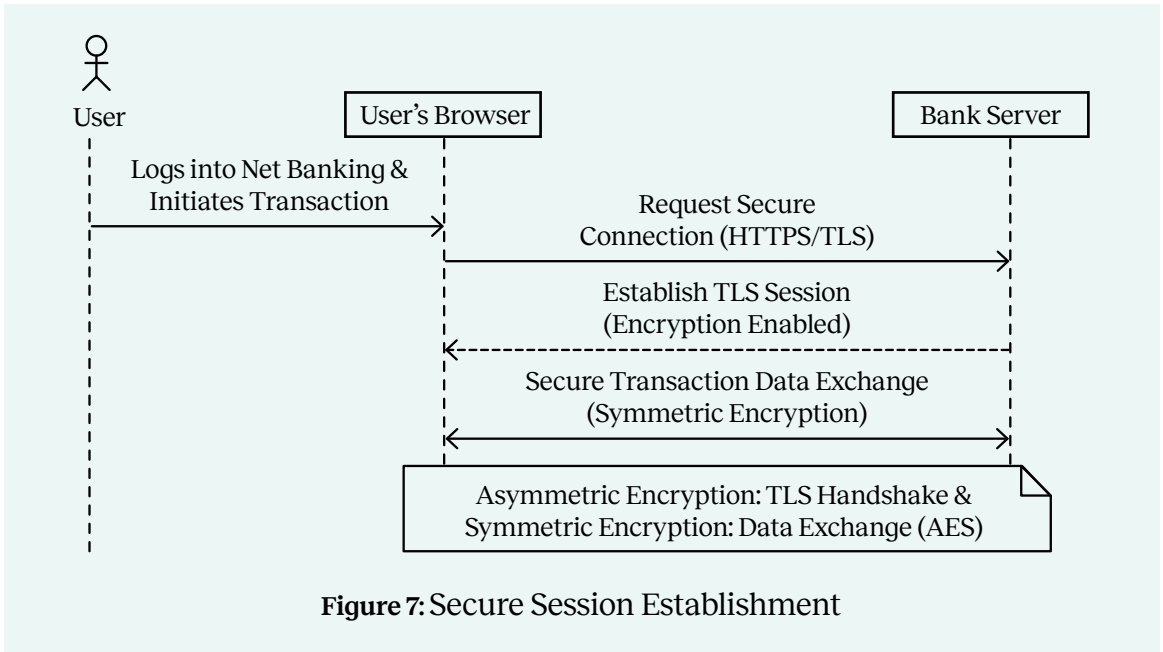
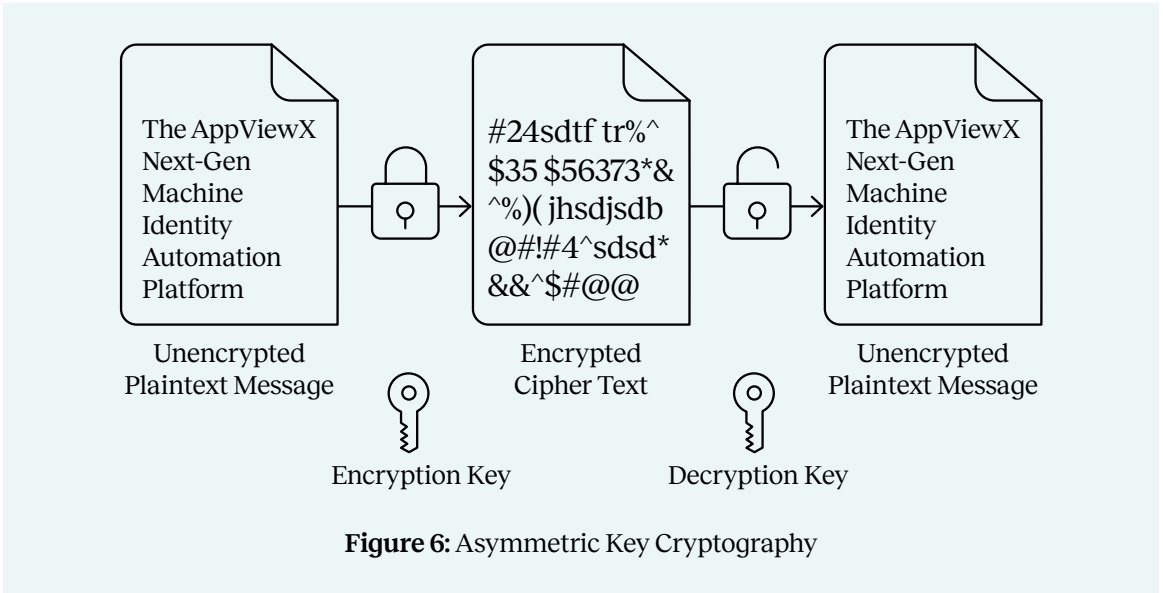
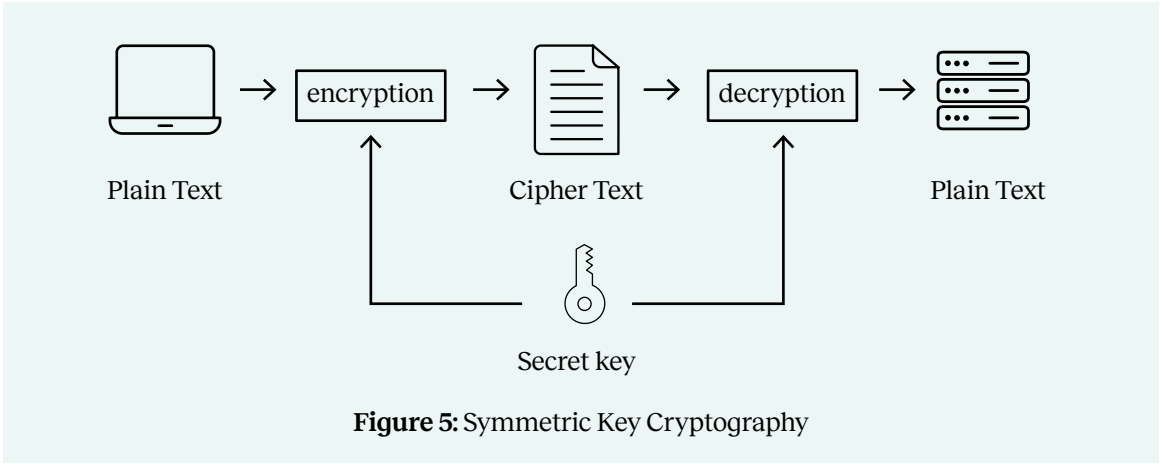
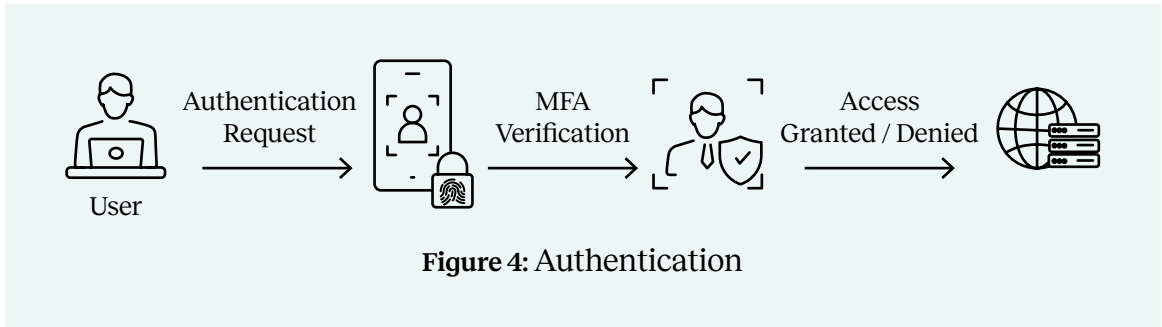
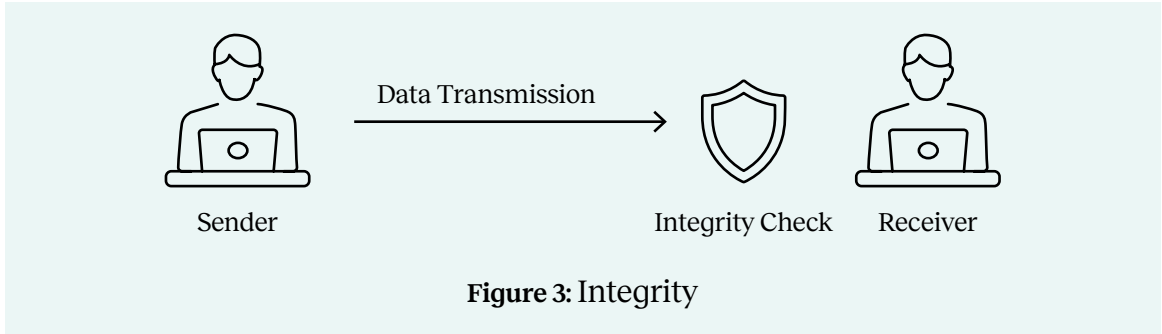
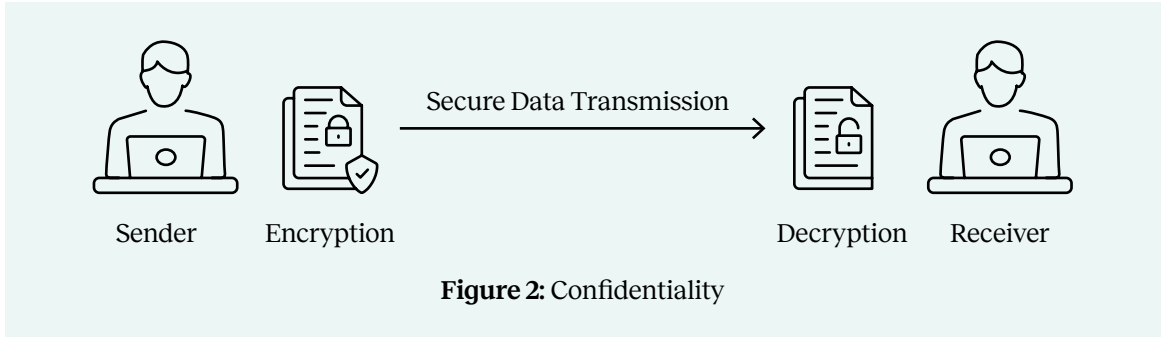
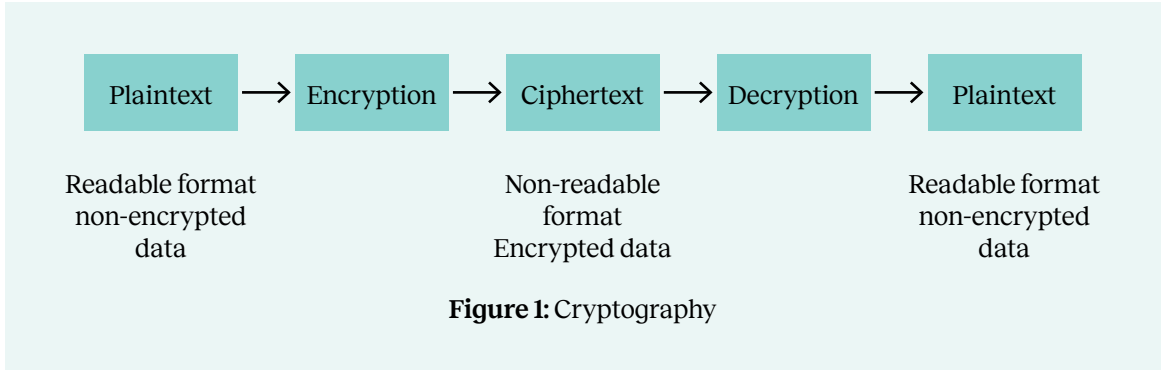


Cyber attackers could compromise the implementation of post-quantum cryptography (PQC) algorithms by targeting the weaknesses in the code, hardware, or system integration. Examples of such weaknesses include:

1. **Bugs or vulnerabilities in the code implementing the PQC algorithm can lead to unexpected behavior or information leaks.** These flaws can be exploited to extract information about the secret keys or to manipulate the system’s operation.
2. **By introducing faults or errors into the computation (e.g., through power glitches, electromagnetic pulses, or clock manipulation), attackers might cause the algorithm to produce incorrect results, potentially revealing information about the secret key.**
3. **If the PQC algorithm is integrated with other systems through application programming interfaces (APIs), vulnerabilities in those APIs could allow attackers to bypass the security offered by the PQC algorithm.**

4. **Weak key management practices, such as improper key generation, storage, or use, can weaken the overall security of the system and make the PQC algorithm ineffective.**

To mitigate these risks, a multi-layered approach to security is essential. This could include careful code review and testing, robust key management practices, secure hardware design and implementation, protection against side-channel and fault-injection attacks, secure API design and implementation, and continuous monitoring and vulnerability assessment. The use of formal methods and independent third-party audits can also increase the security and trustworthiness of PQC implementations. Staying updated on emerging attacks and vulnerabilities through ongoing research and collaboration within the cybersecurity community is crucial for maintaining effective security.



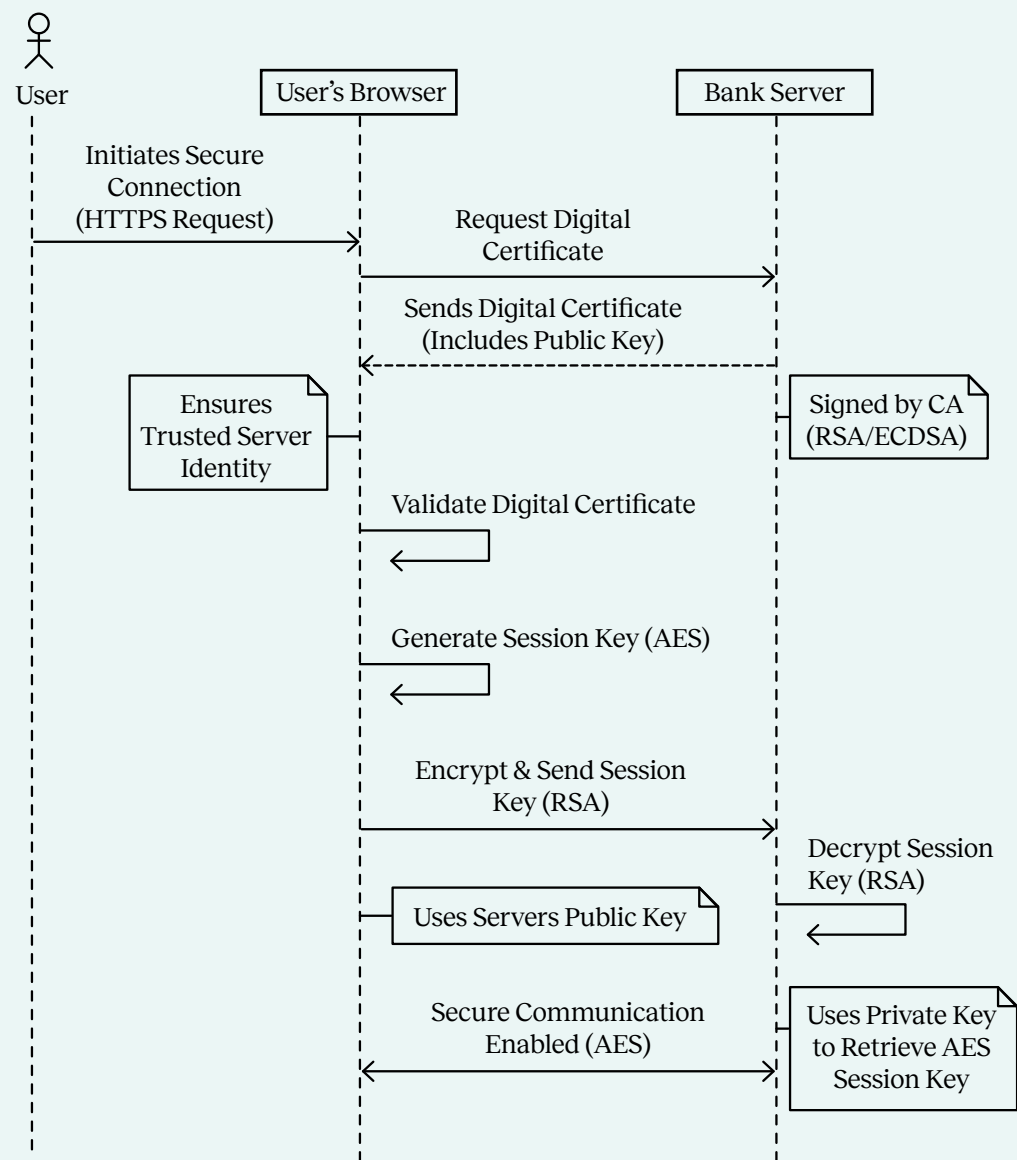


Figure 8: Asymmetric Encryption for Authentication and Key Exchange

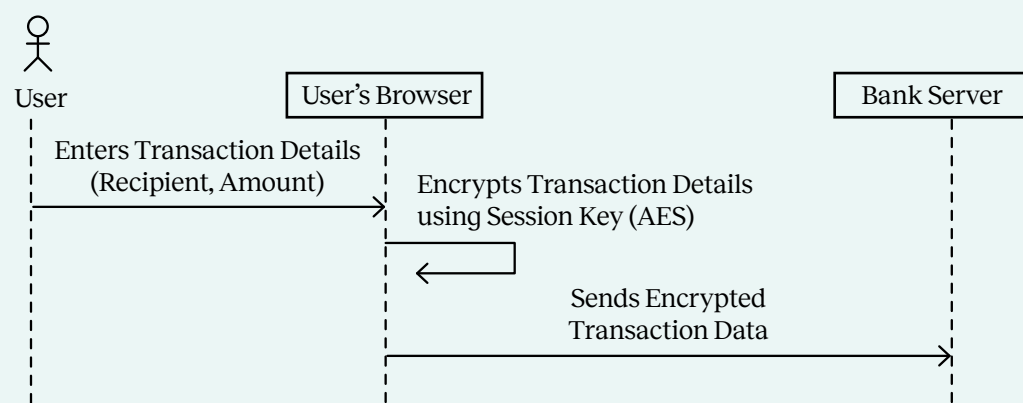


Figure 9: Encrypting and Sending Transaction Details

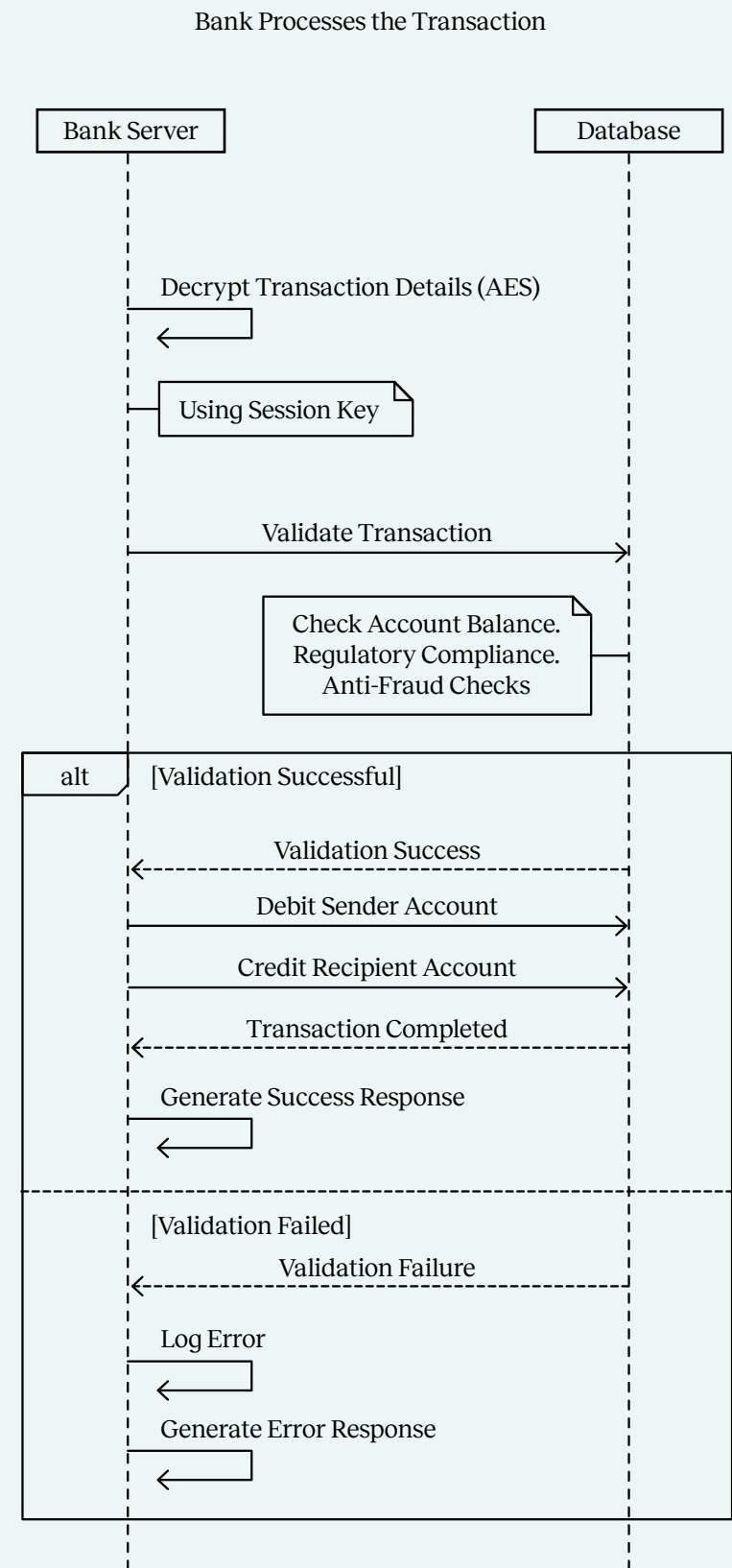


Figure 10: Encrypting and Sending Transaction Details

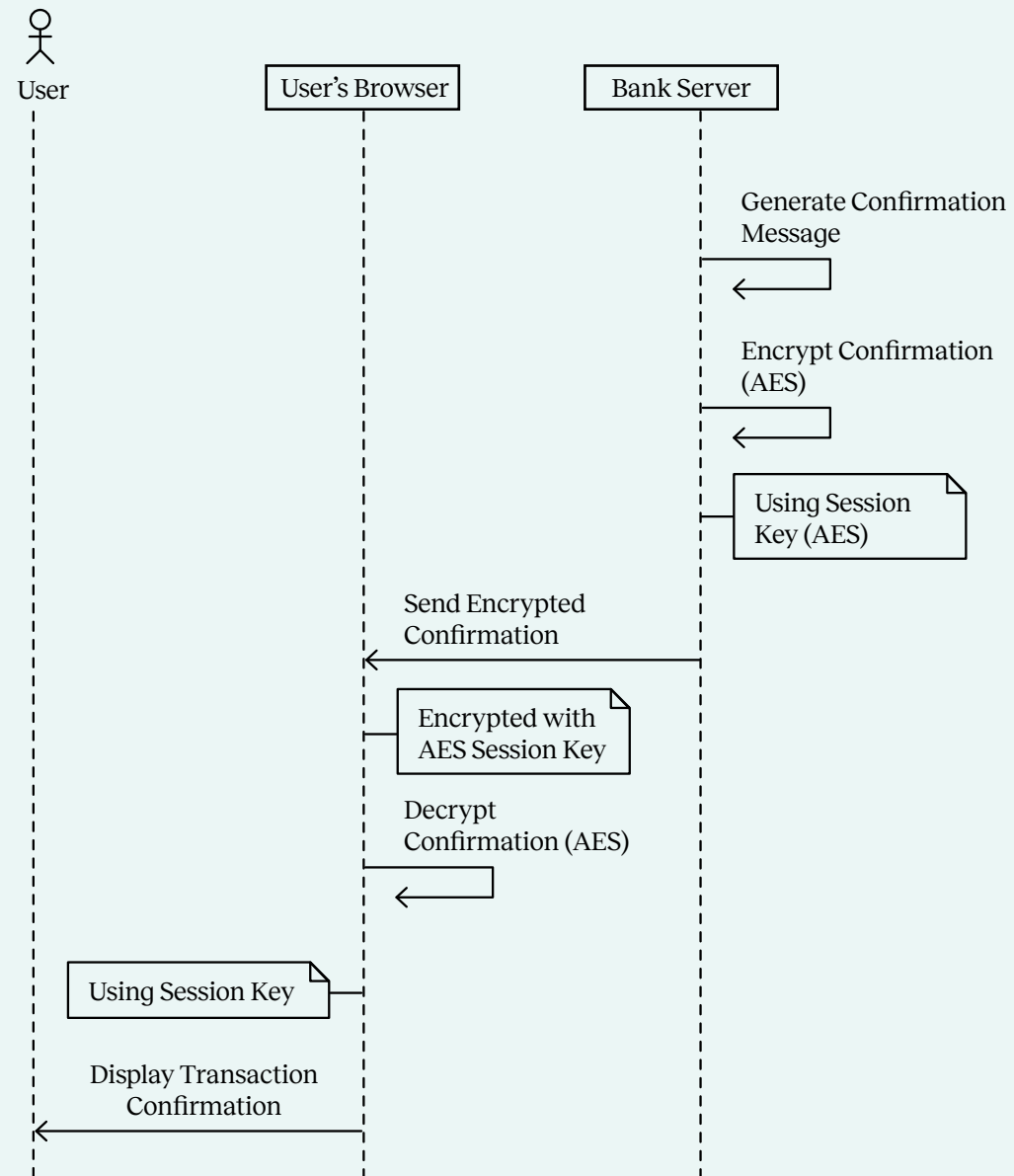


Figure 11: Acknowledgment and Confirmation

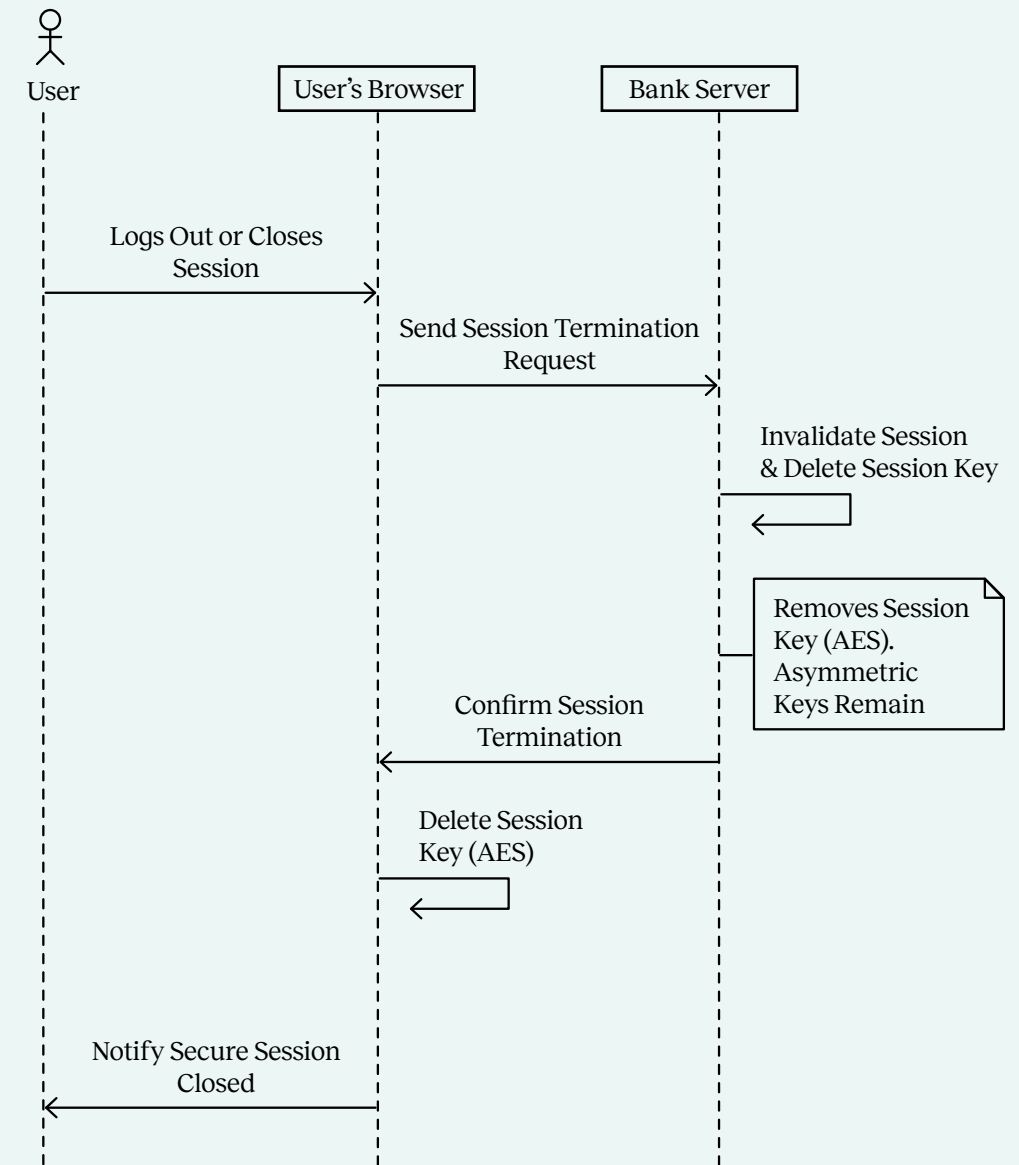
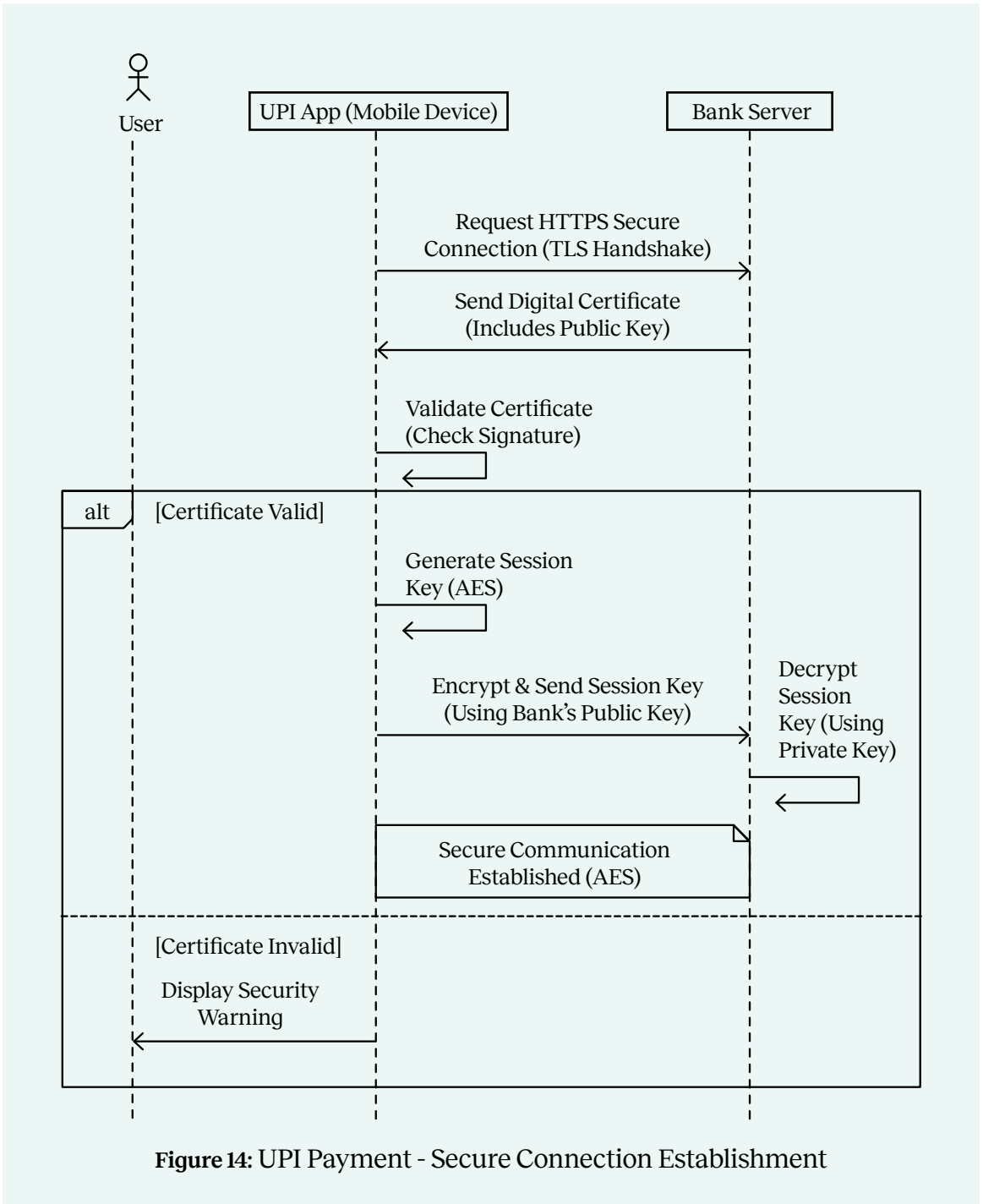
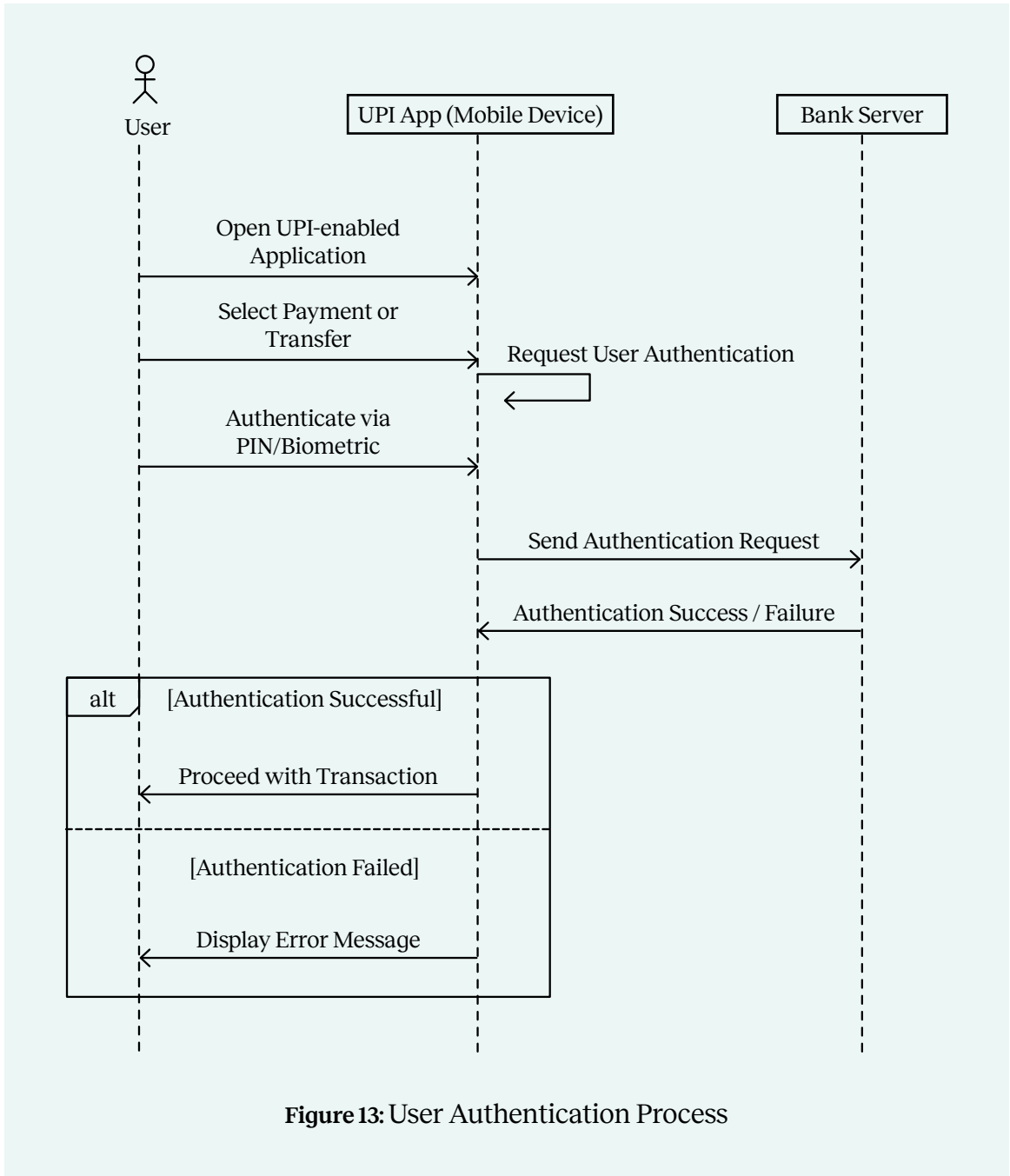


Figure 12: Session Termination



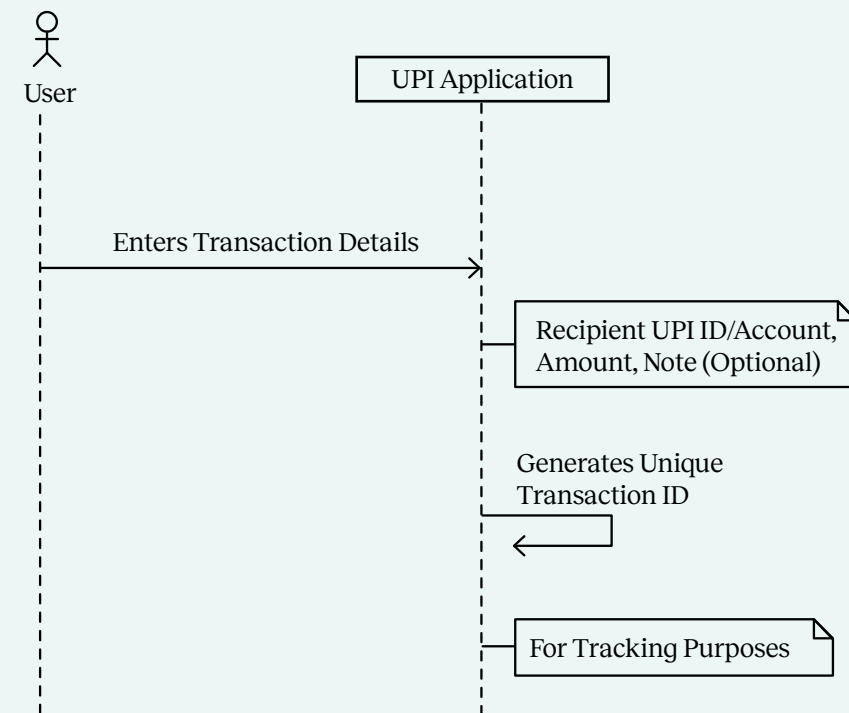


Figure 15: Transaction Details Input

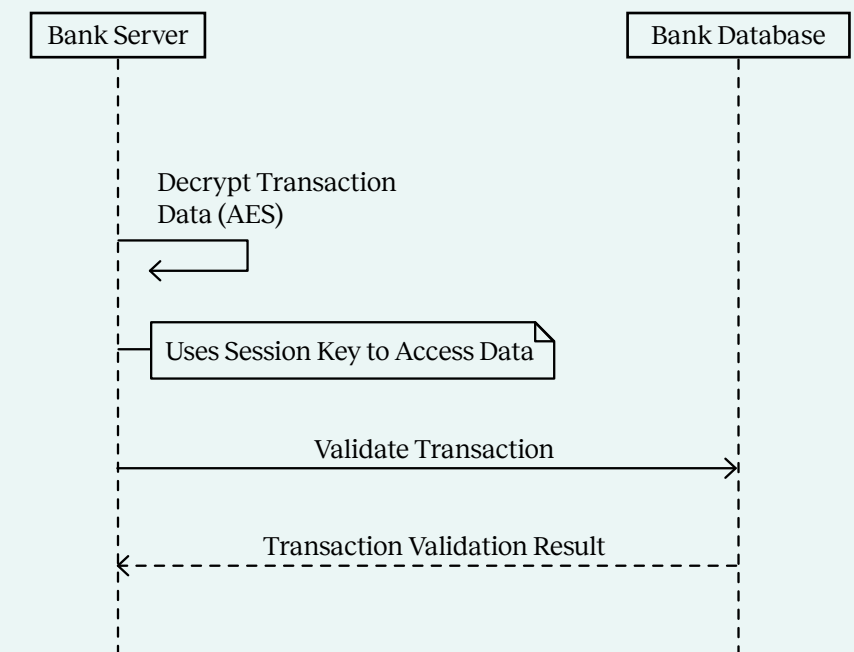


Figure 17: Bank Server Processing

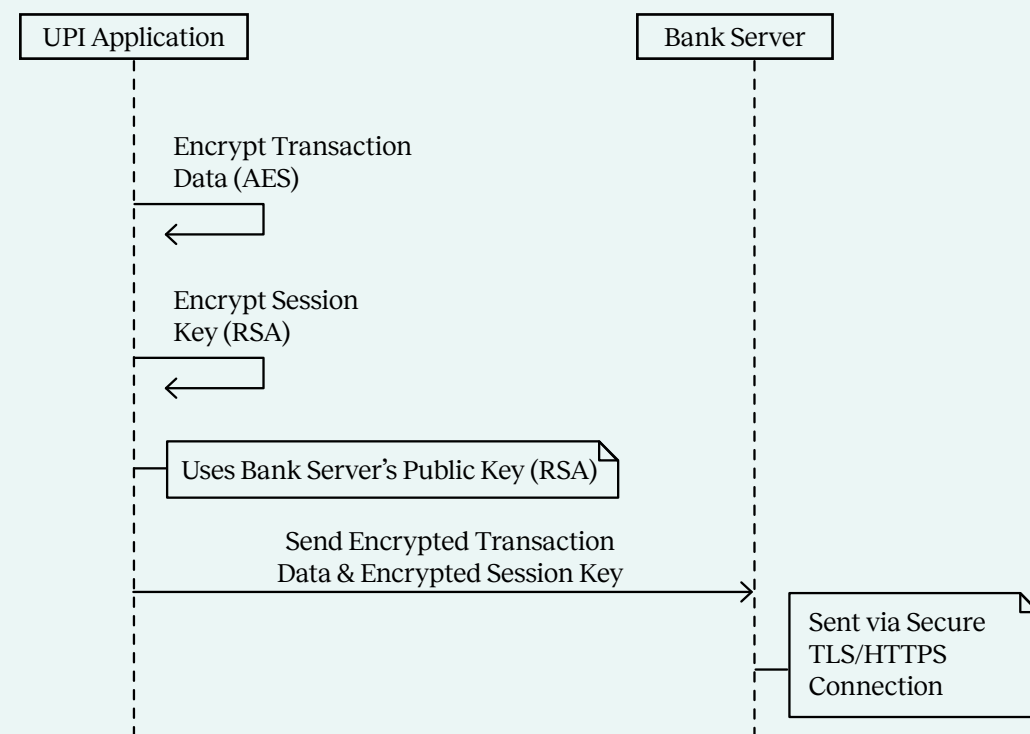


Figure 16: Data Encryption & Secure Transmission in UPI Transaction



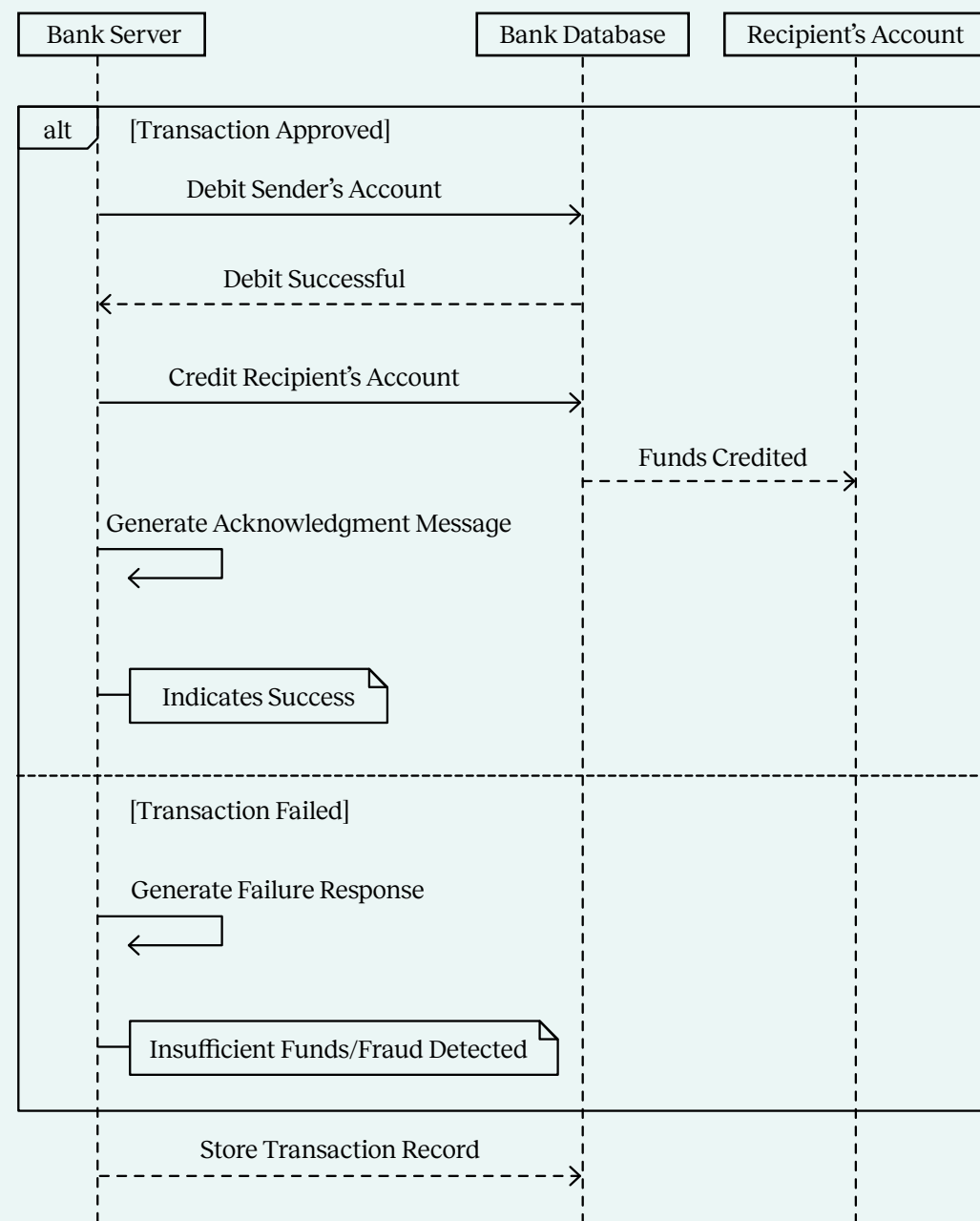


Figure 18: Crediting the Amount

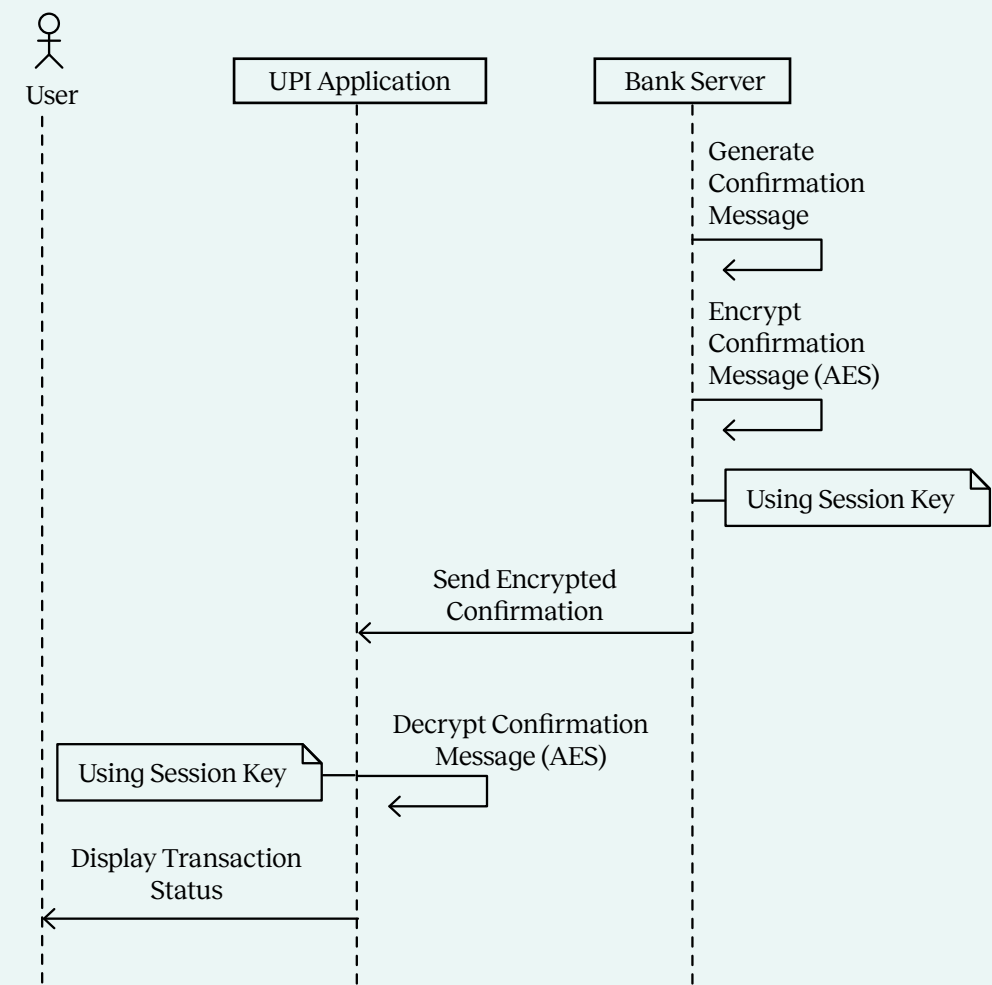
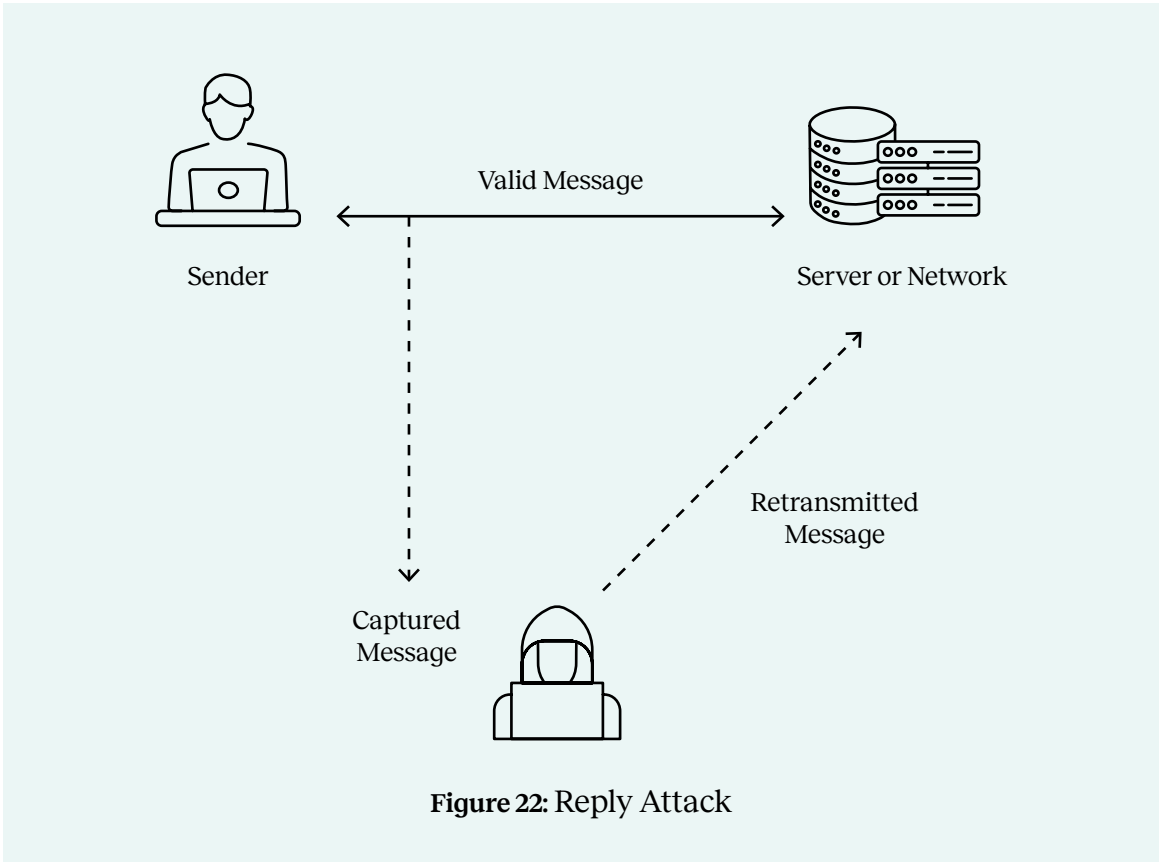
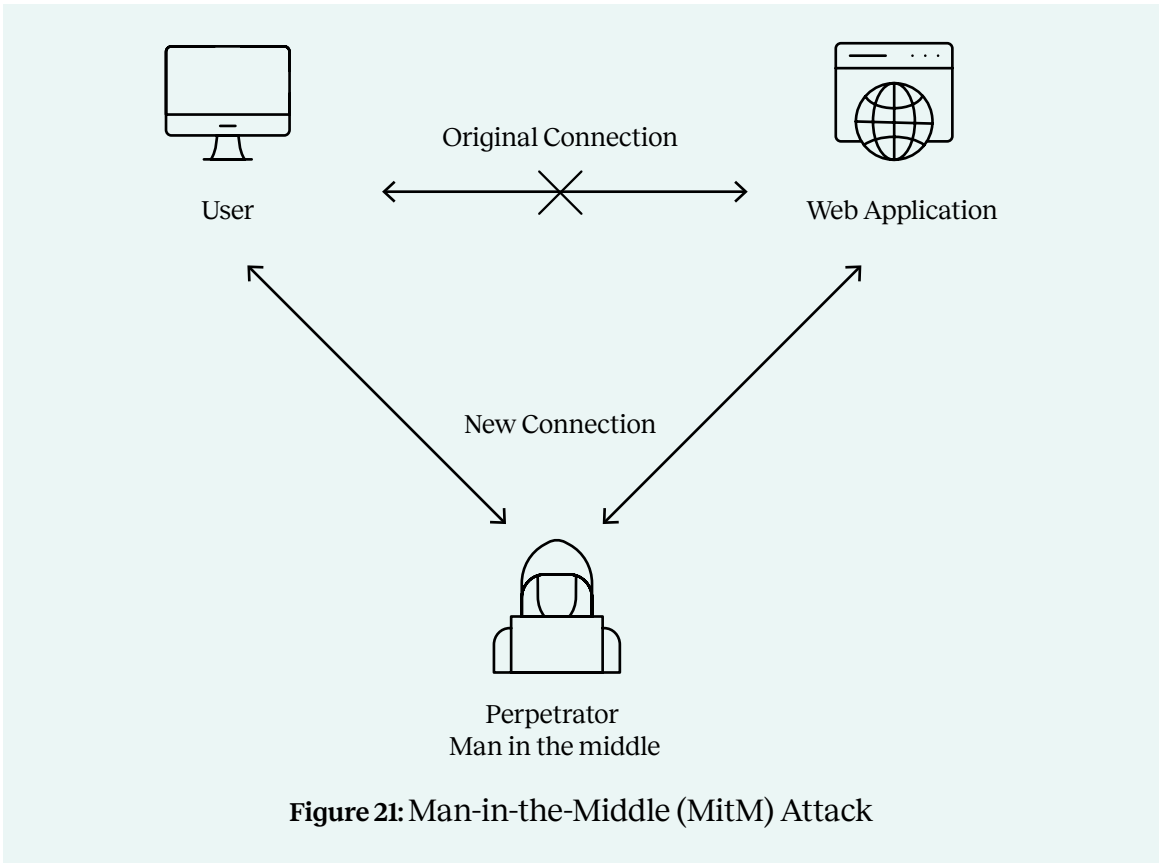
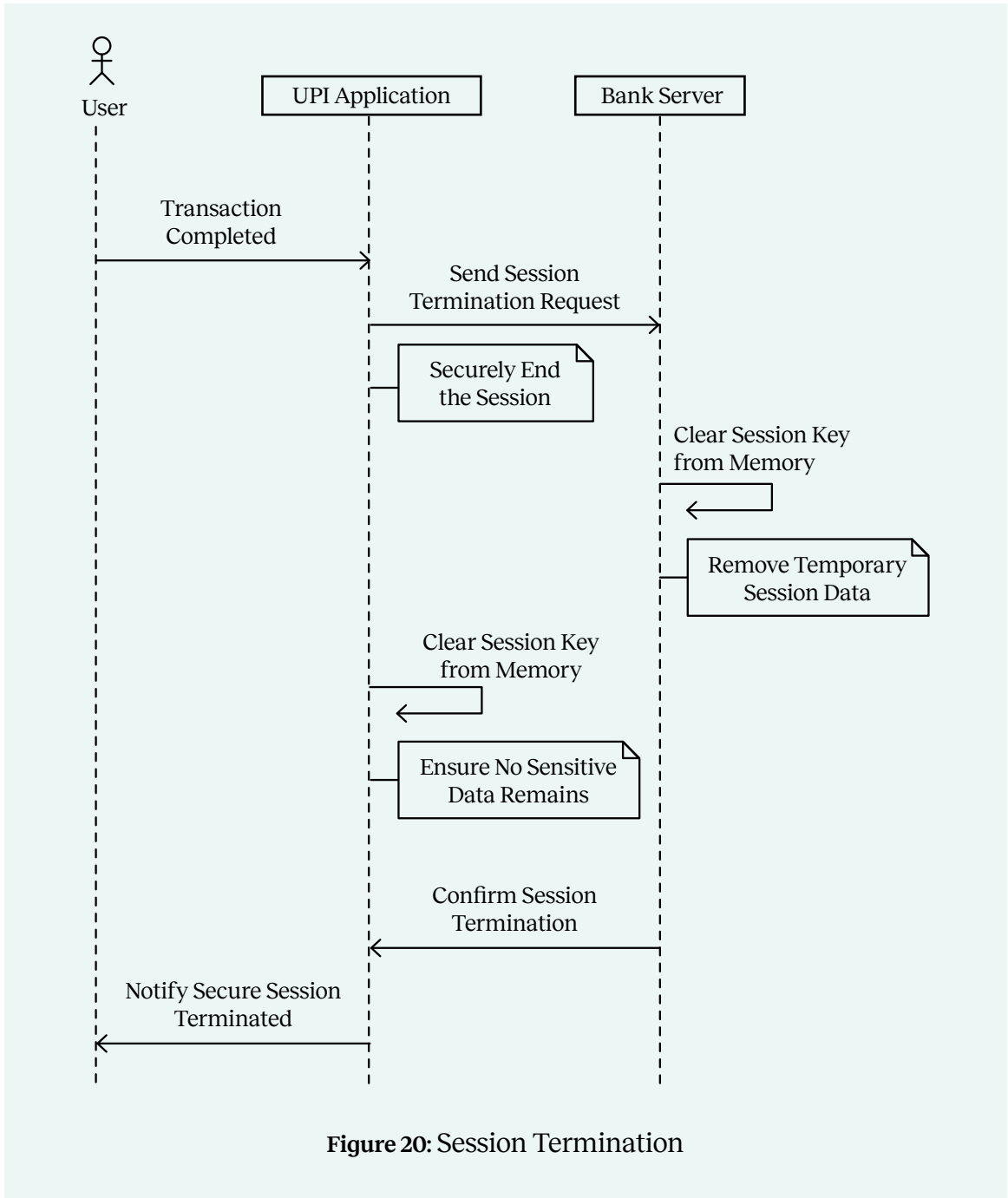


Figure 19: Secure Transaction Confirmation & User Acknowledgment



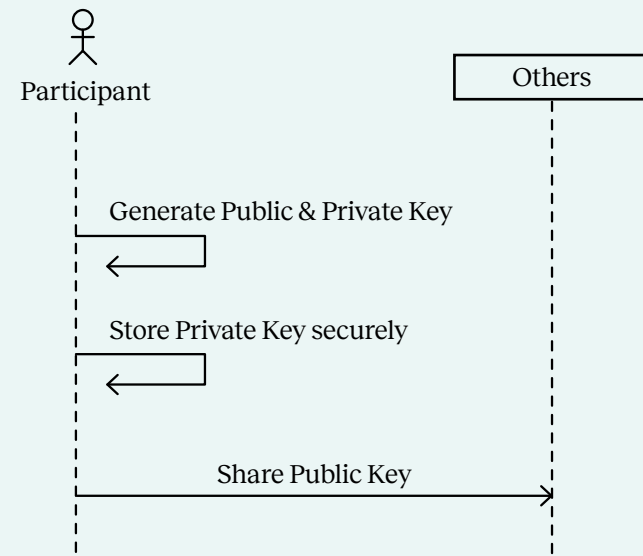


Figure 23: Key Generation

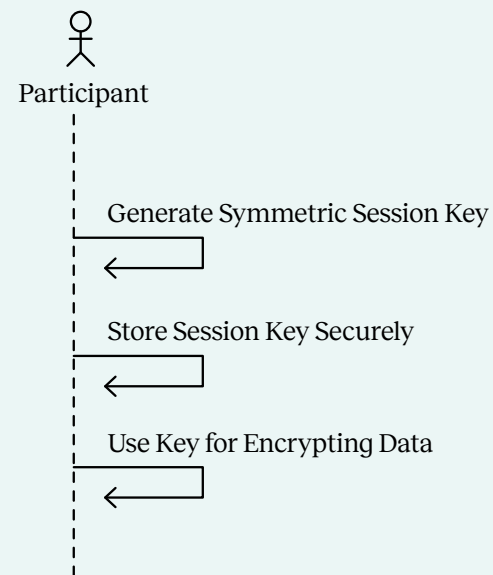


Figure 24: Symmetric Key Generation

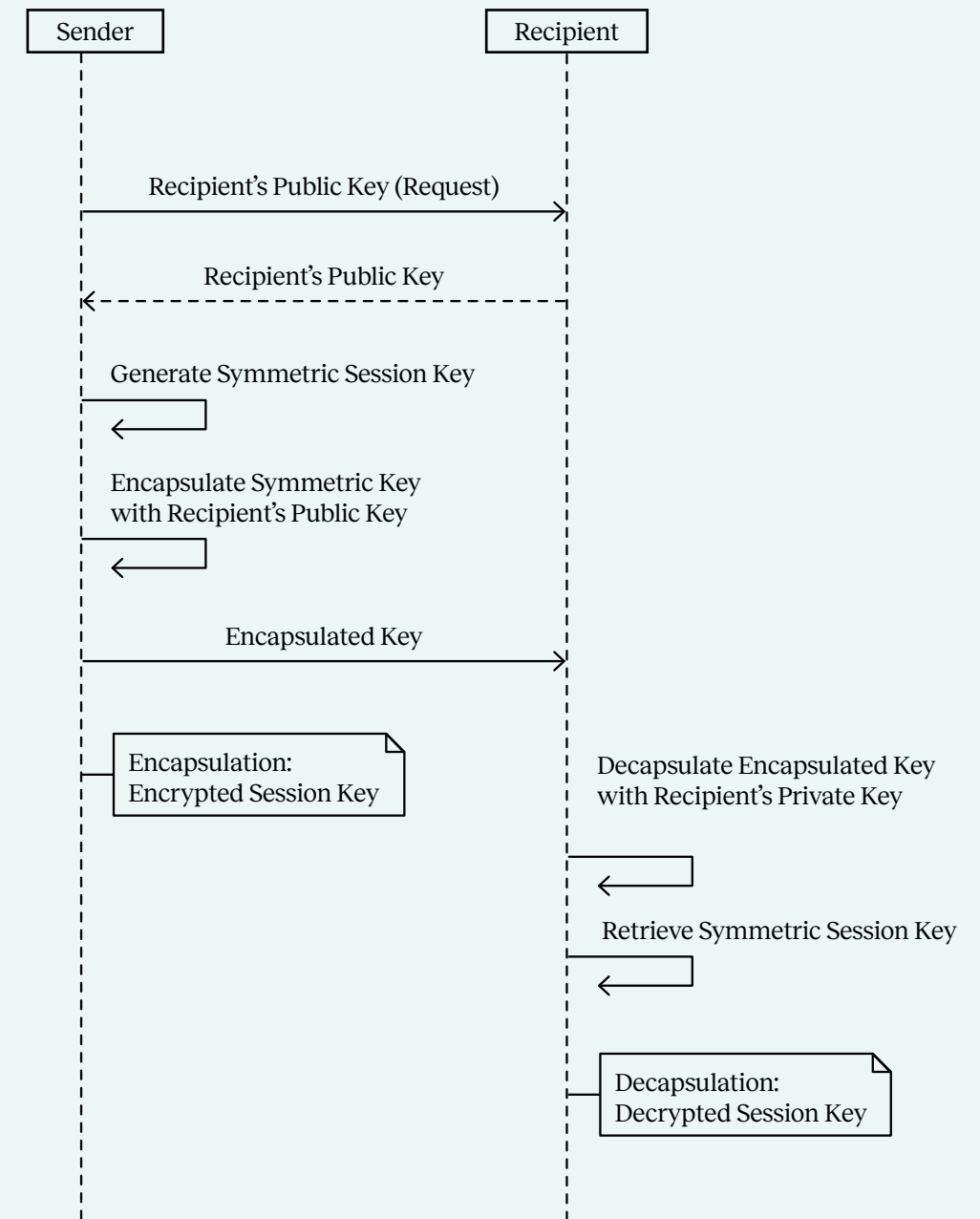


Figure 25: Key Encapsulation

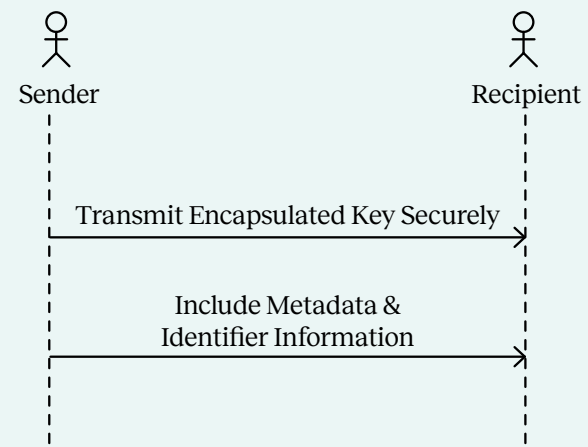


Figure 26: Transmission

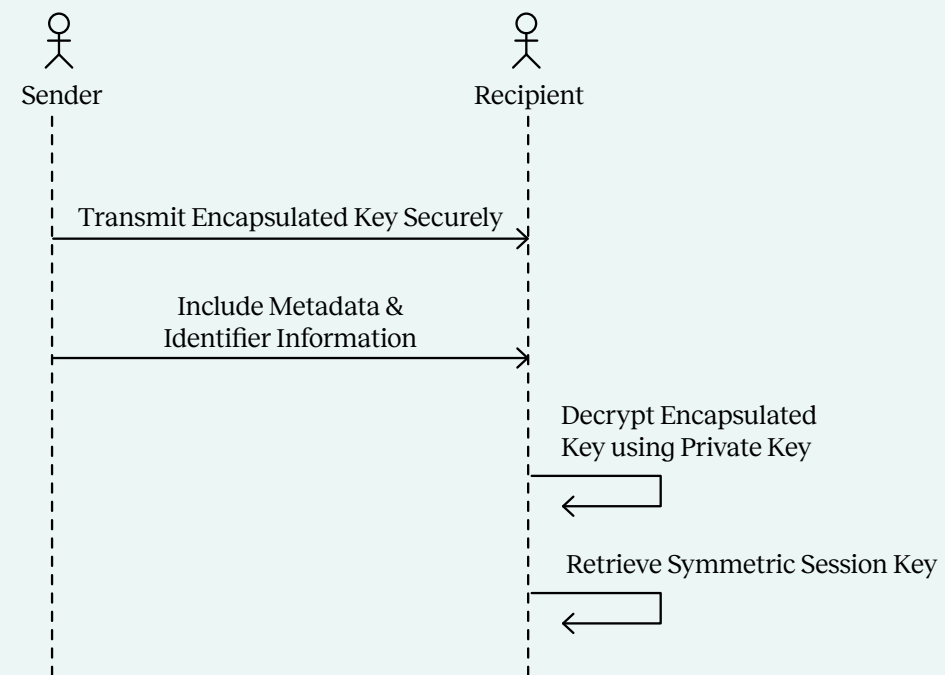


Figure 27: Decapsulation

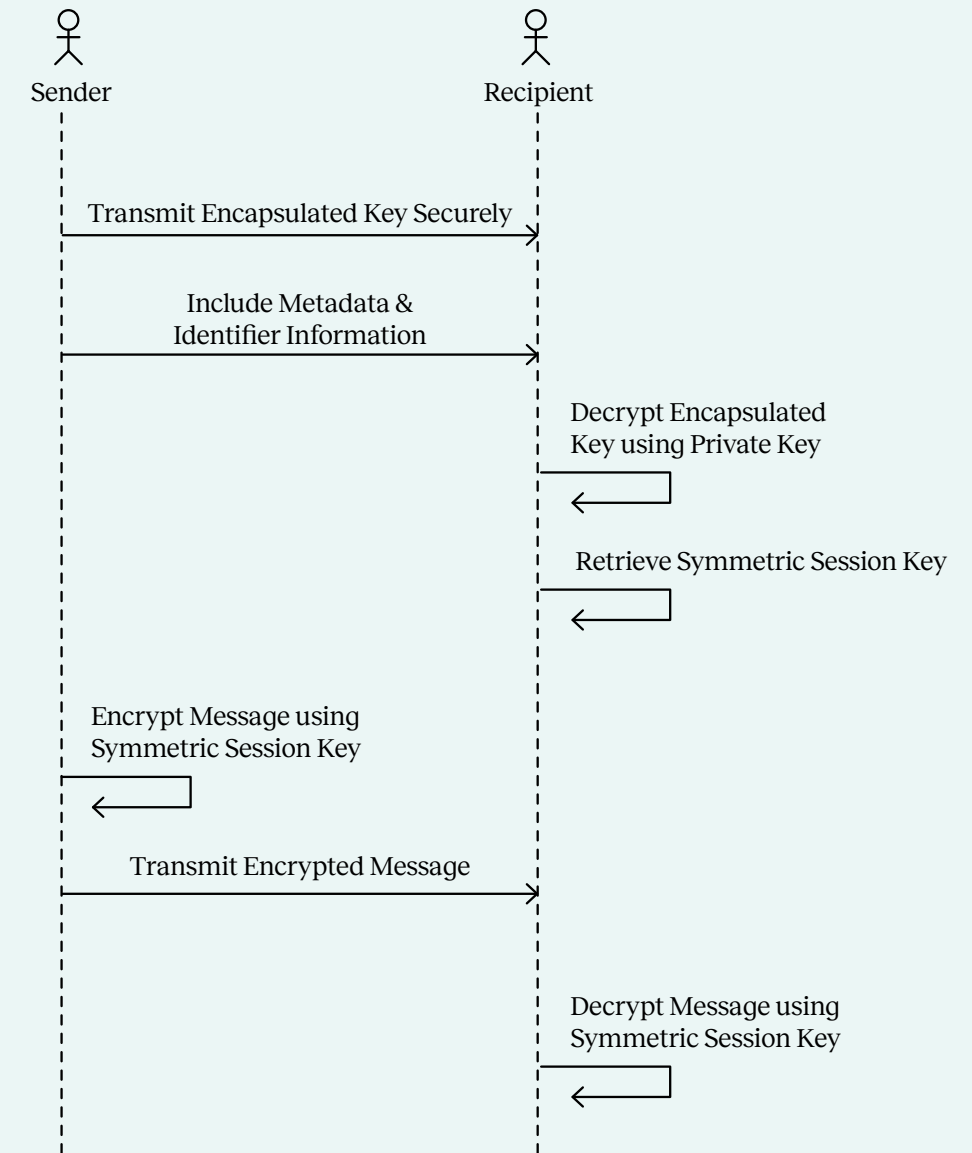


Figure 28: Data Encryption and Decryption

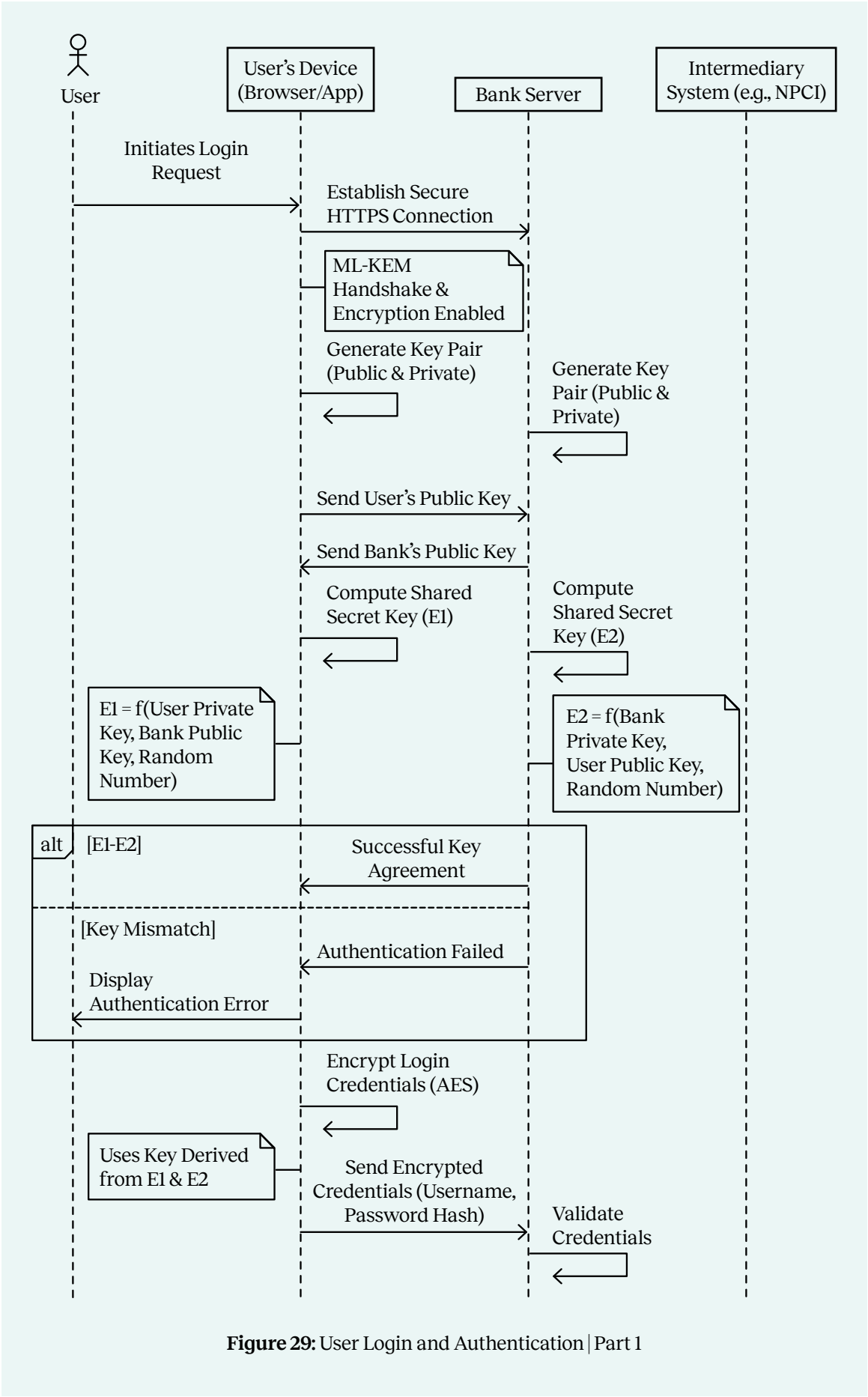


Figure 29: User Login and Authentication | Part 1

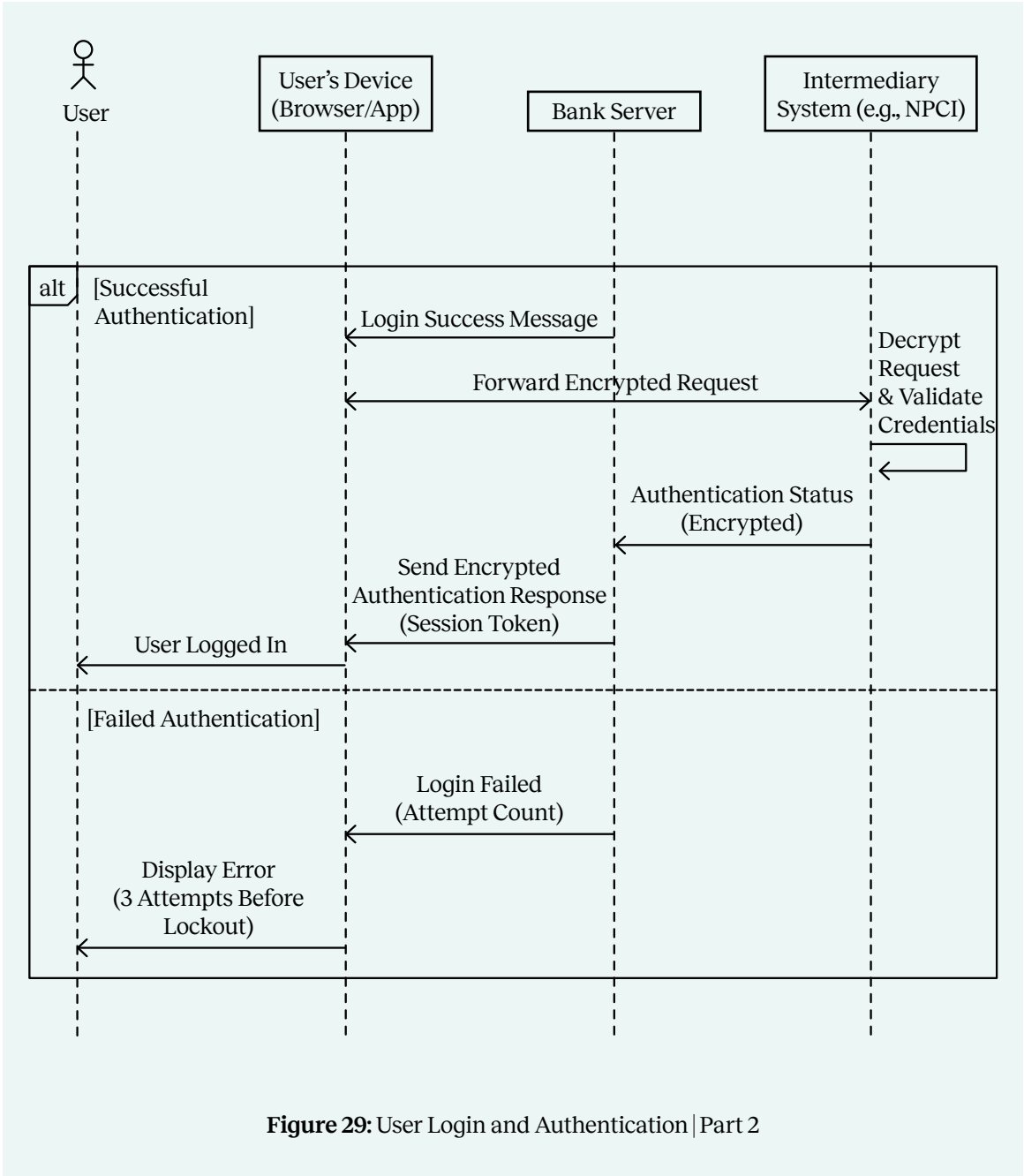


Figure 29: User Login and Authentication | Part 2

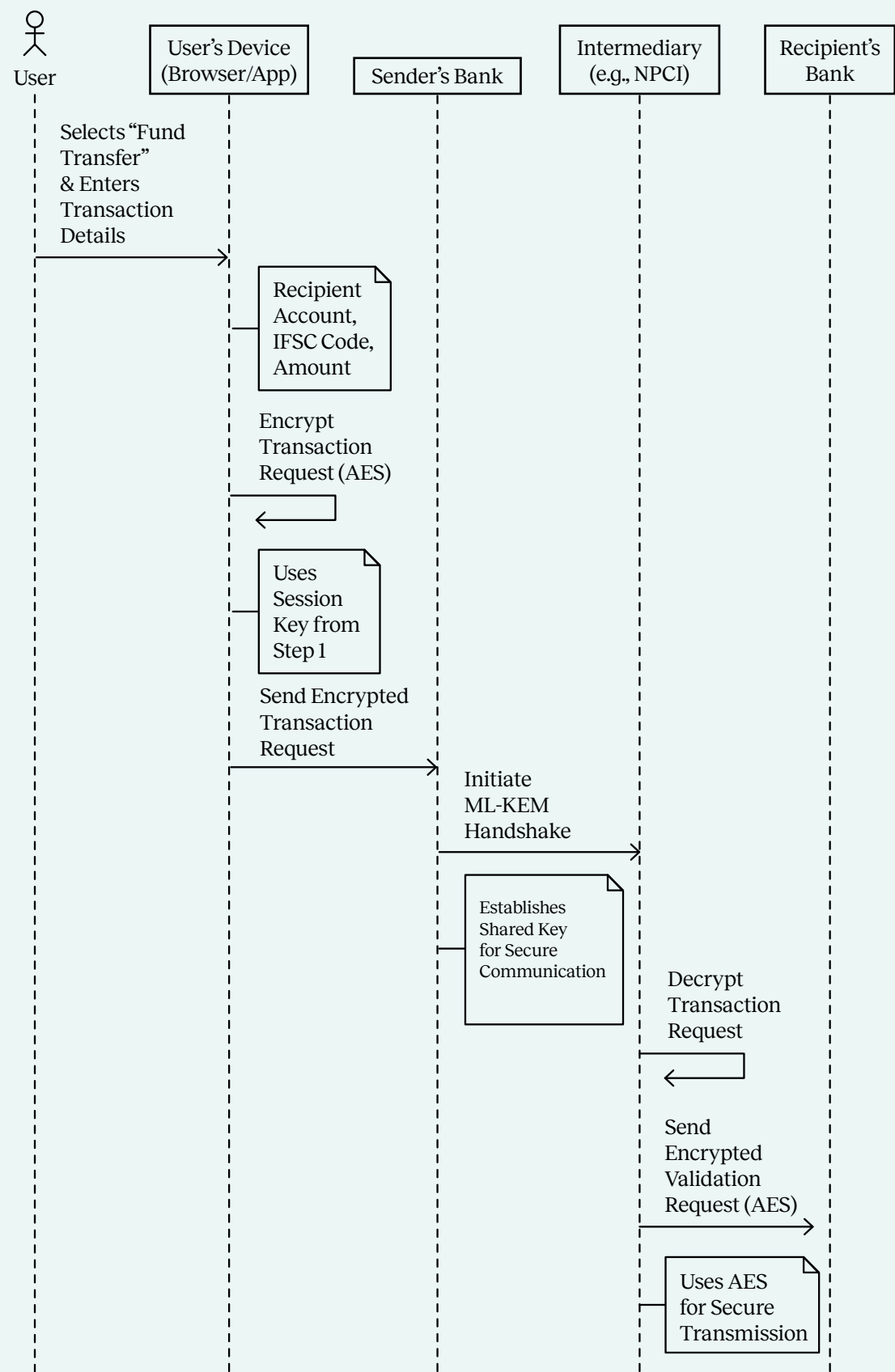


Figure 30: Transaction Initiation

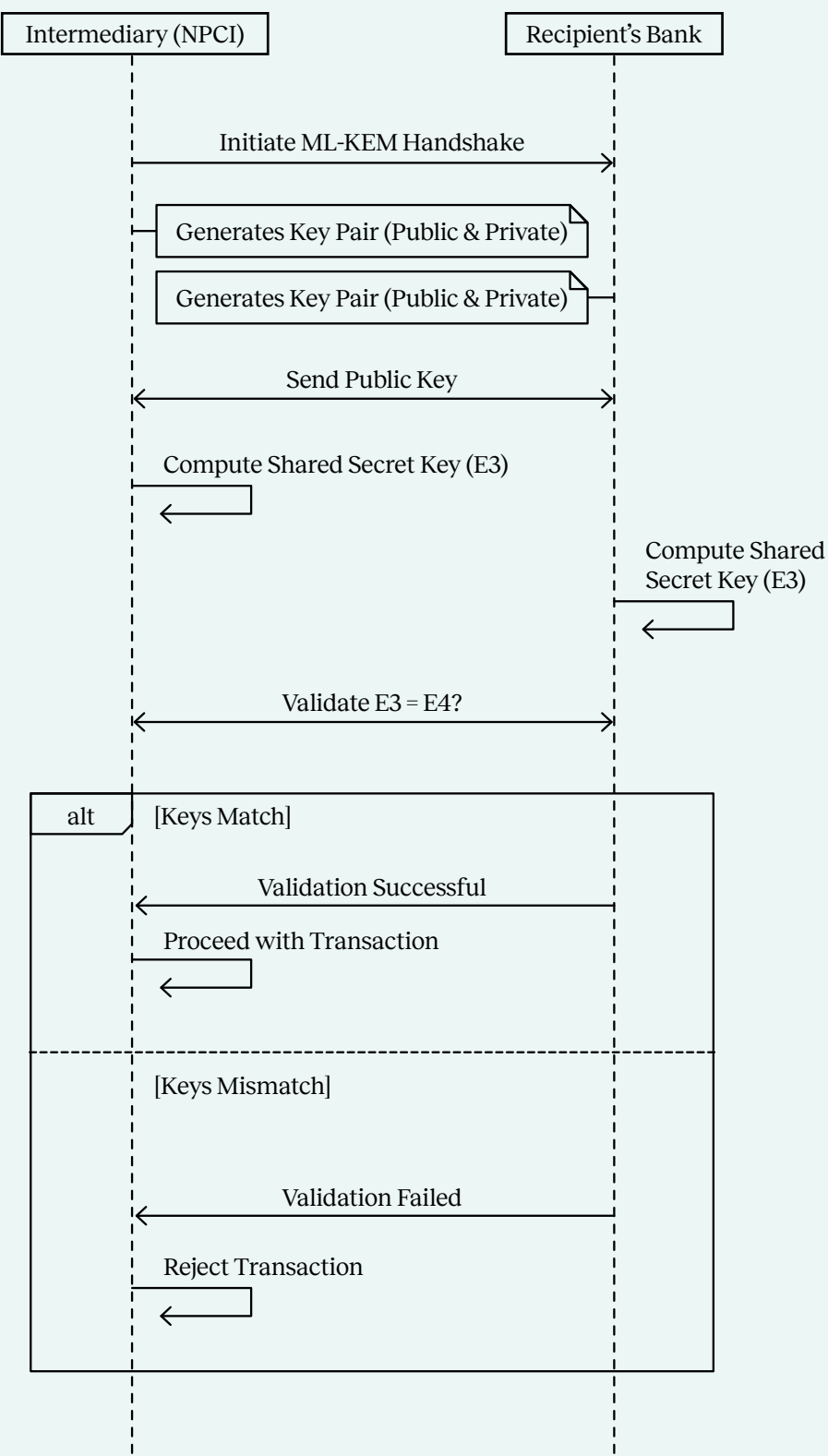


Figure 31: Recipient Validation

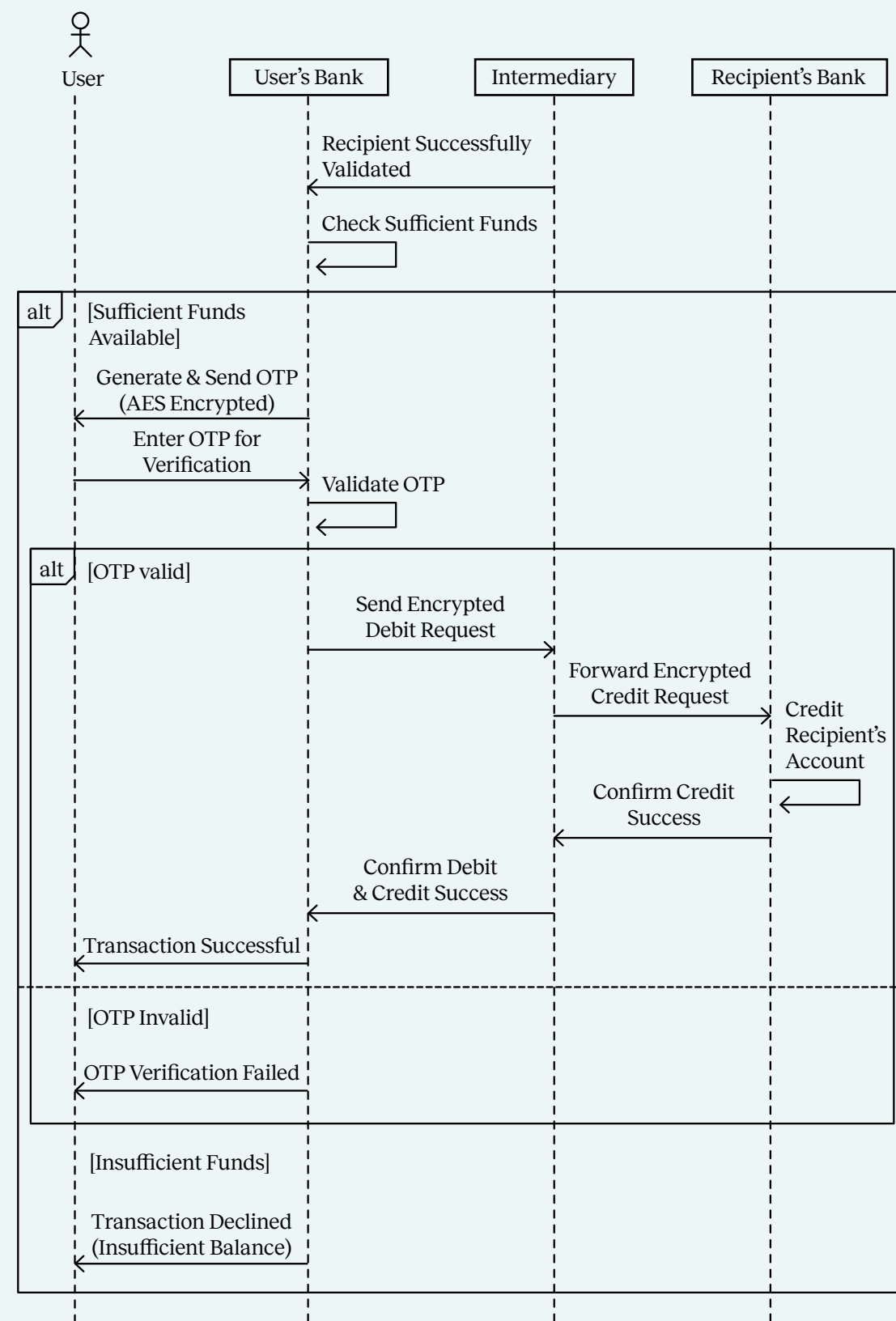


Figure 32: OTP Verification and Transaction Processing

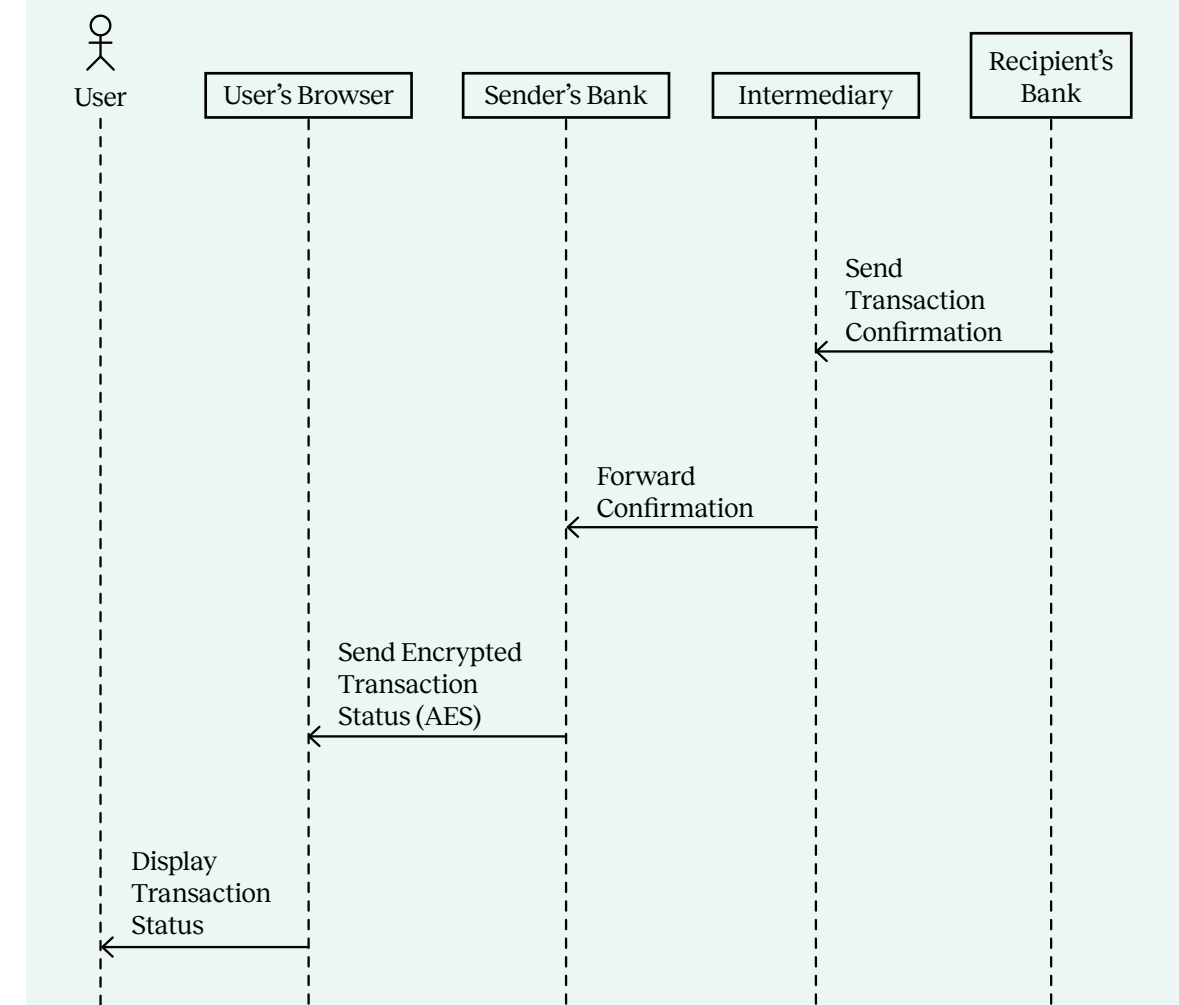
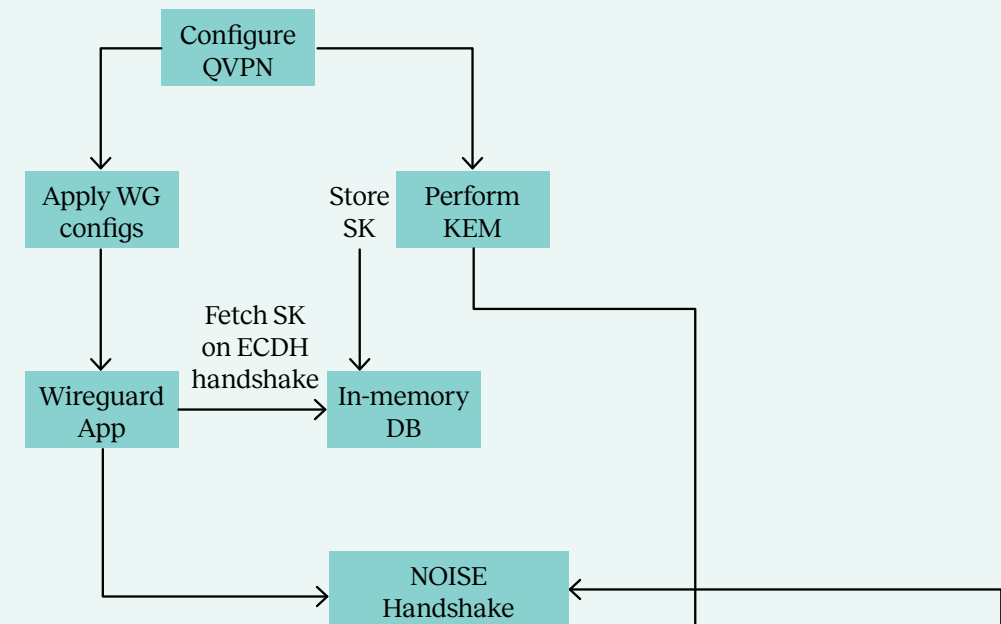


Figure 33: Transaction Confirmation and Notification

QVPN Client



QVPN Server

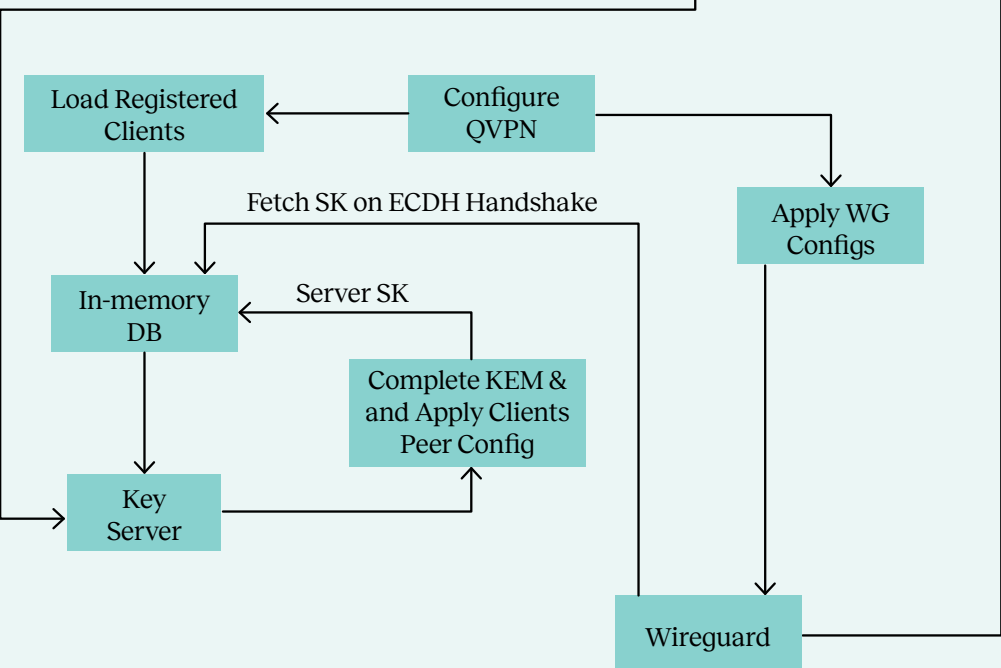


Figure 34: QVPN Client Server Interaction

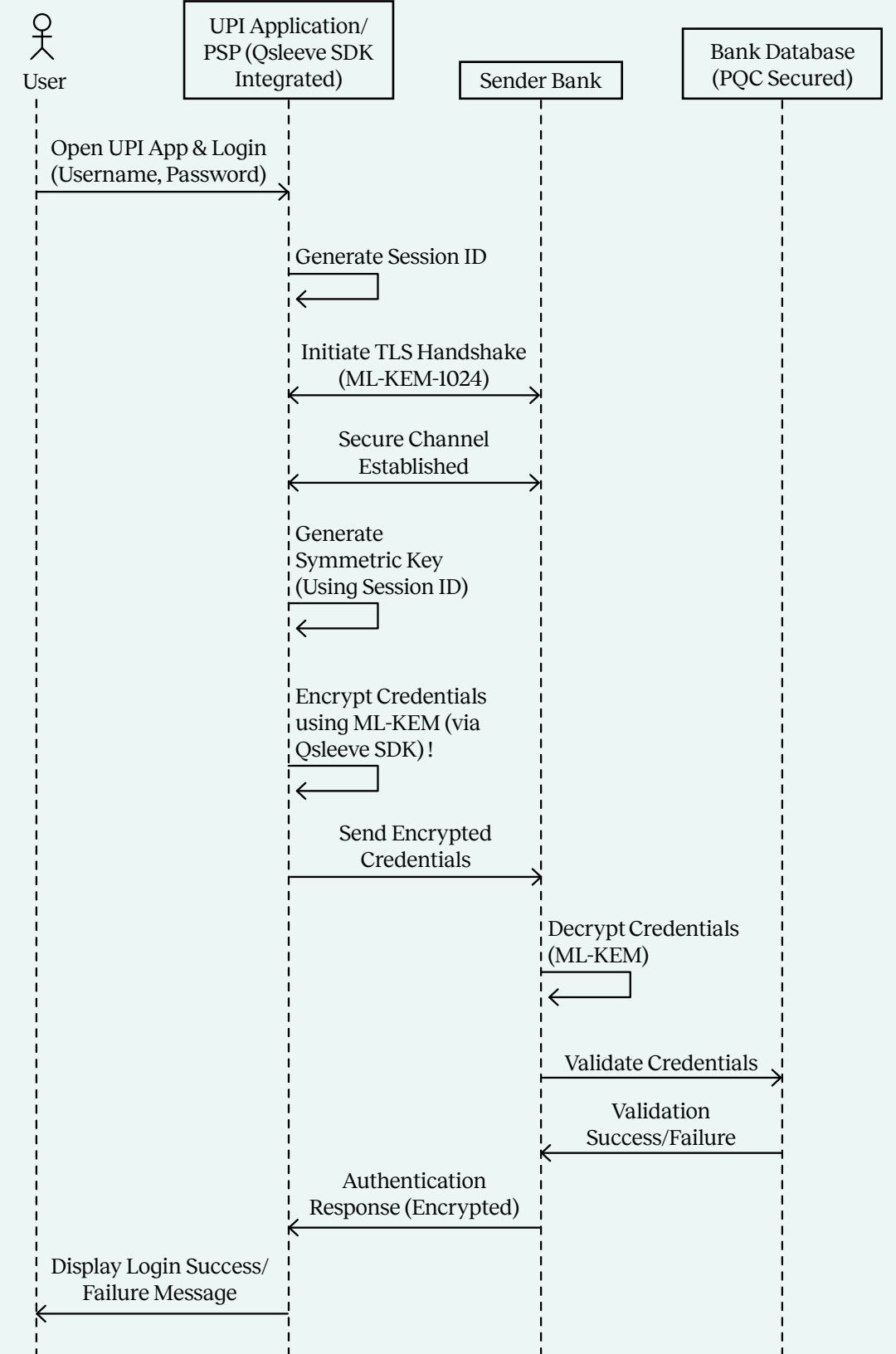


Figure 35: User Initiation, Authentication, and Handshake with QSleeve SDK

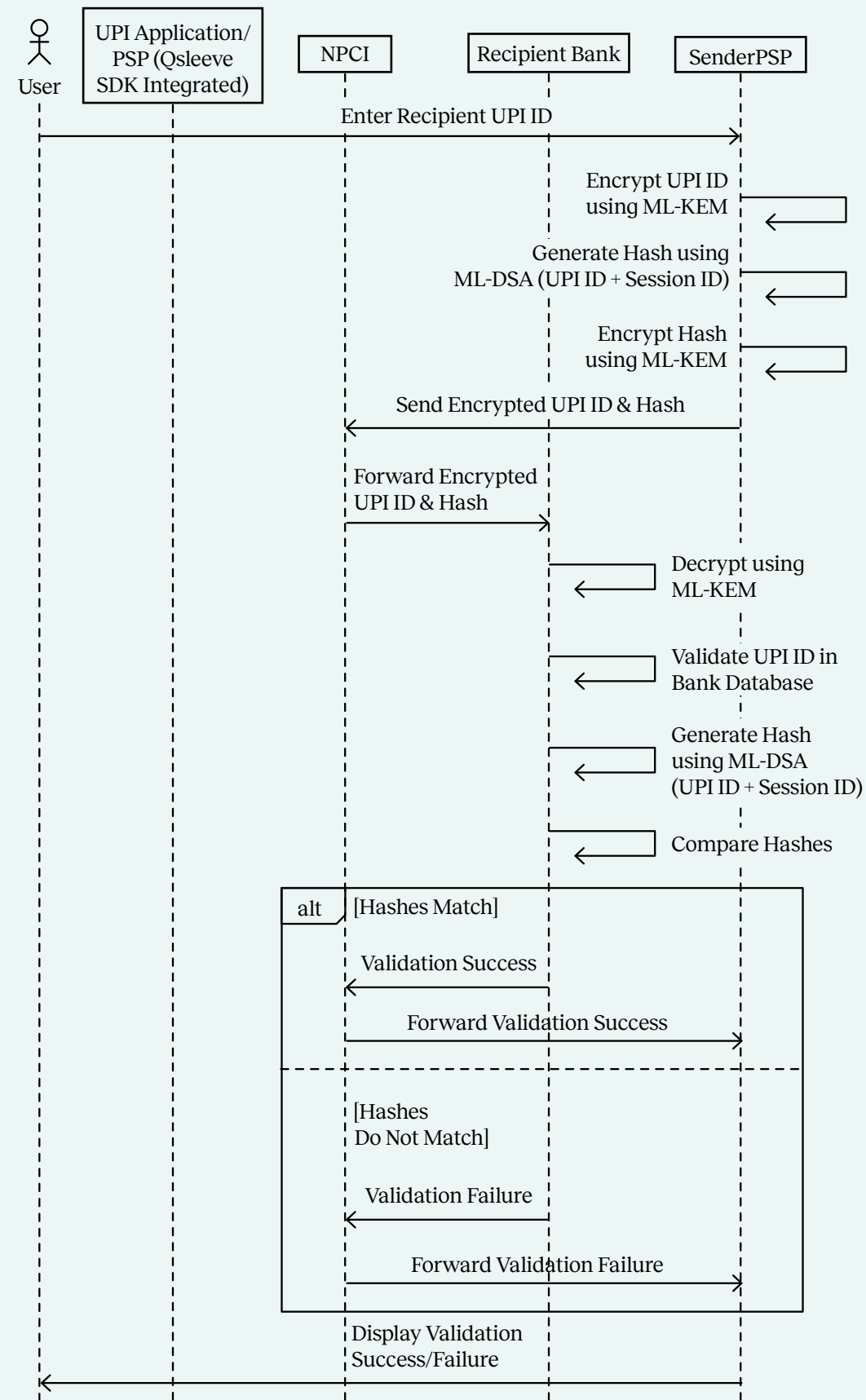


Figure 36: Recipient Information, Validation, and Hash Generation

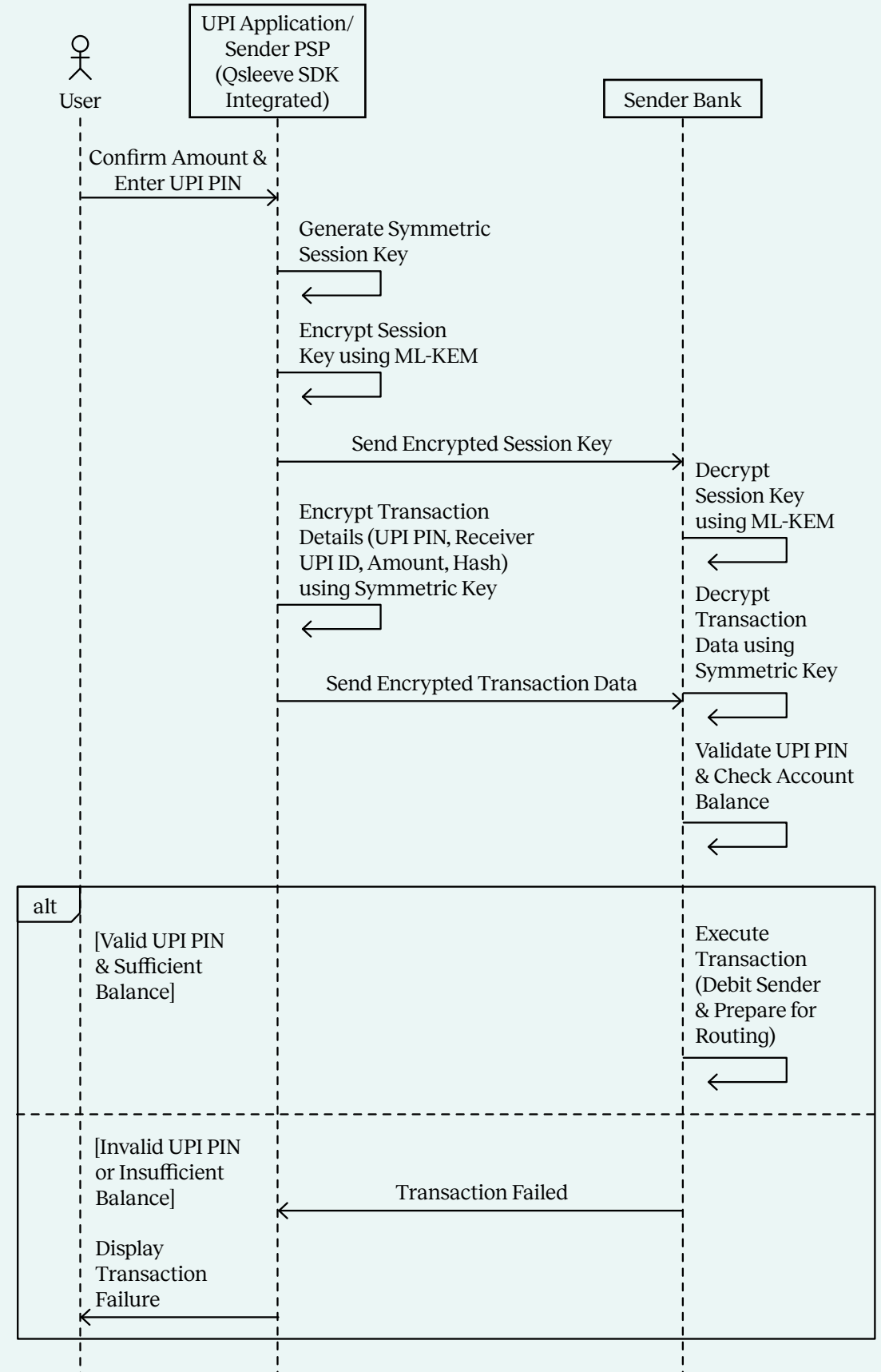
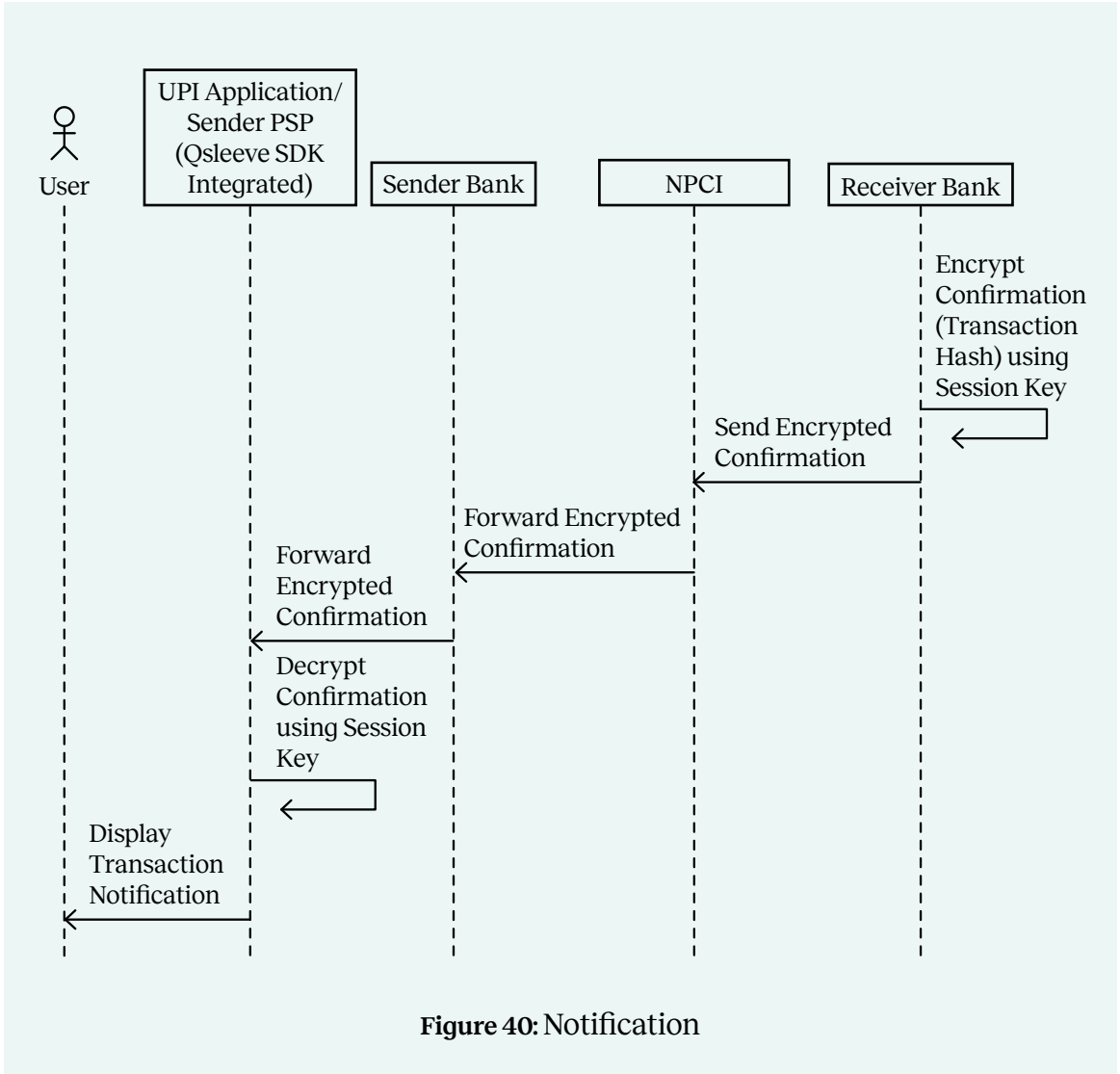
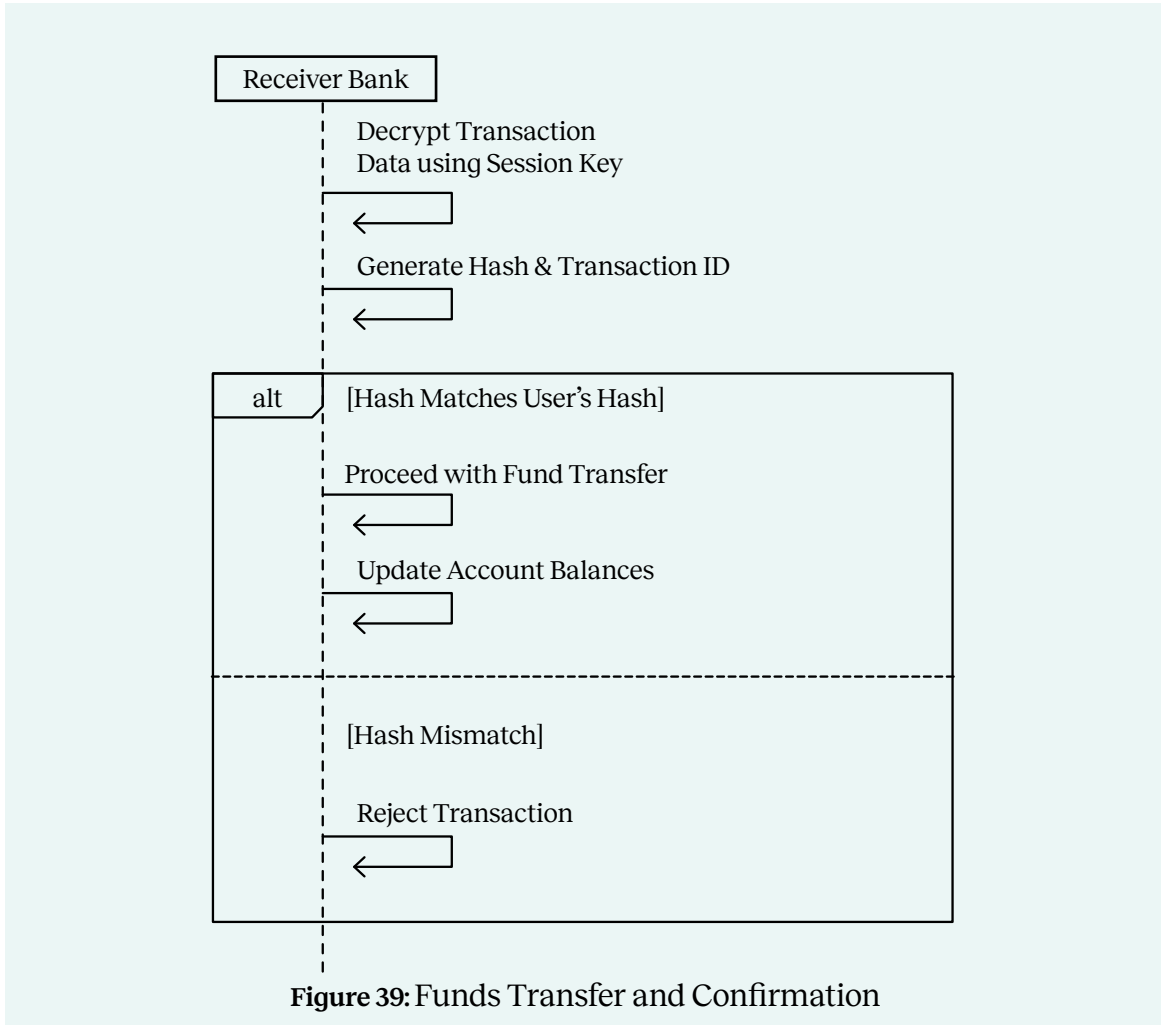
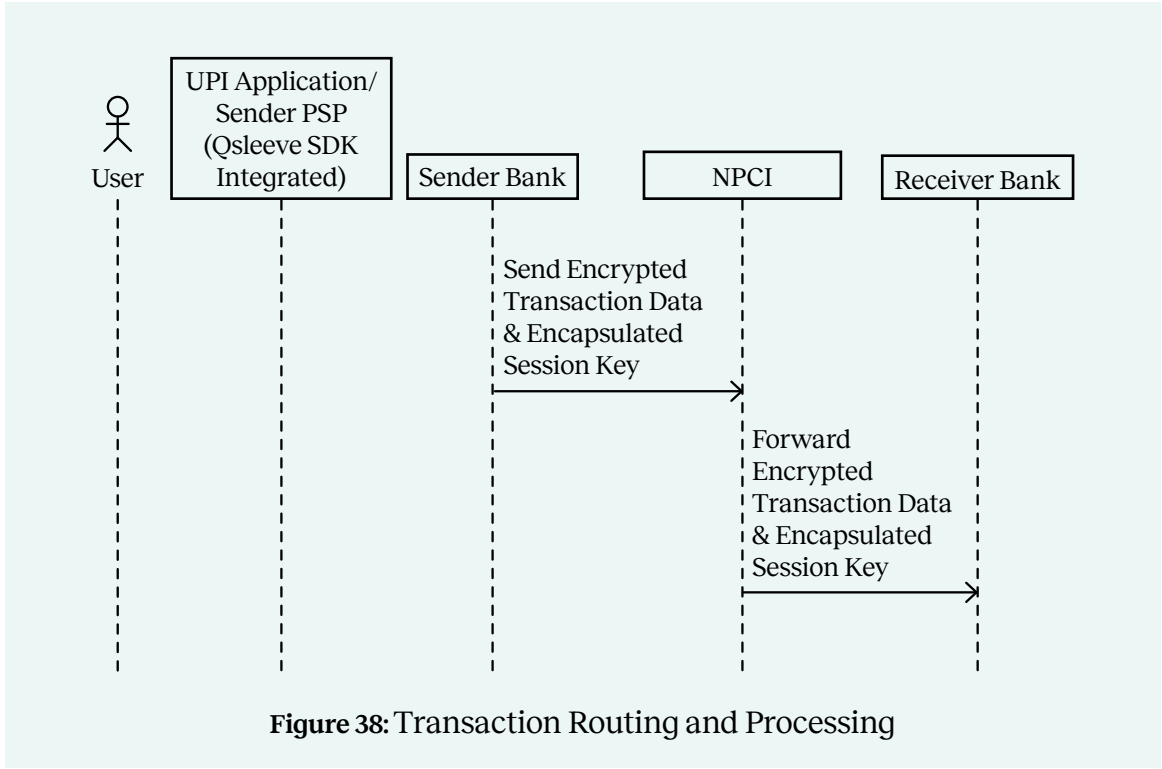


Figure 37: Transaction Details, ML-KEM, and Encryption





Chapter 6

Post-Quantum Security with Multivariate Quadratic (MQ) Cryptography

Multivariate Quadratic (MQ) cryptosystems are a type of public-key cryptography based on the difficulty of solving systems of multivariate quadratic equations over a finite field. Unlike traditional public-key cryptosystems that rely on the difficulty of problems like integer factorisation (RSA) or the discrete logarithm problem (ECC), MQ systems base their security on the NP-hardness of solving systems of multivariate polynomial equations. A basic MQ cryptosystem works as follows:

Key Generation

Secret Key: The secret key consists of two main components. A set of n randomly chosen quadratic polynomials in m variables ($m > n$). These polynomials define the central transformation used in both encryption and decryption. The coefficients of these polynomials are elements of a finite field (often a prime field, like $GF(p)$, where p is a prime number). A linear transformation of the variables, often represented by an invertible matrix, serves as an additional layer to further obfuscate the system of equations.

Public Key: The public key consists of a set of n quadratic polynomials, but after the linear transformation has been applied to the variables. This set of polynomials represents a highly complex and seemingly random set of quadratic equations in m variables. The complexity of this system is what makes solving it difficult without the private key.

Digital Signature

To sign a message, a hash function is applied to the message, generating a hash value (a fixed-size fingerprint of the message). This hash value is then interpreted as a vector of n elements from the finite field. Using the private key (the set of polynomials and the transformation matrix), the signer transforms this hash vector into another vector. This transformation is the computationally easy part of the scheme thanks to the structure of the secret key. The resulting vector is the signature associated with that message.

Signature Verification: The verifier receives the message, the signature, and the public key. The verifier hashes the message to obtain the same hash value as generated by the signer. Again, this is public information based on the message. The verifier applies the public key (the transformed quadratic polynomials) to the hash vector. If the resulting vector matches the signature, the signature is verified as authentic. The security of MQ cryptosystems relies on two primary computational problems: (i) Solving a general system of multivariate quadratic equations is an NP-hard problem. This means there’s no known algorithm to solve it efficiently for large systems. (ii) Finding the original system of quadratic polynomials (the private key) from its transformed version (the public key) is also computationally very hard.

However, the implementation of MQ algorithms for post-quantum cryptography is still evolving, as they have not achieved the same level of prominence or standardisation as lattice-based, code-based, or other types of post-quantum cryptography when it comes to widespread adoption. The field continues to evolve, and new and improved MQ schemes may emerge in the future. The two prominent types of MQ-based cryptographic algorithms are:

- 1. **MQOM (Modified Quadratic Quotient of Multivariate):** MQOM is a signature scheme. Its security relies on the difficulty of solving a system of multivariate quadratic equations. The general principle involves these steps:

Key Generation: A central mapping is generated from a relatively simple polynomial system to a complex

multivariate quadratic system. The structure of this mapping is the private key. The resulting complex quadratic system is the public key.

- **Signature Generation:** To sign a message, a hash function is applied to the message, generating a hash value (a fixed-size fingerprint of the message). This hash value is then interpreted as a vector of n elements from the finite field. The steps involved in signature generation are given below:

Step 1: The message is hashed to produce a hash value.

Step 2: The hash value is transformed using the private key’s mapping into a solution vector in the complex quadratic system. This transformation is computationally efficient using the structure of the private key.

Step 3: The resulting vector is the signature.

- 2. **Signature Verification:** To verify a signature, the following steps are followed:

Step 1: The message is hashed.

Step 2: The hash value is transformed using the public key’s complex quadratic system. This part is computationally hard without the private key.

Step 3: If the result matches the received signature, the signature is valid.

- 2. **UOV (Unbalanced Oil and Vinegar):** UOV is also a signature scheme focused on the difficulty of solving a system of multivariate quadratic equations. Its strategy centers around the concept of "oil" and "vinegar" variables.

- 1. **Key Generation:** The private key consists of a set of quadratic polynomials in m variables partitioned into o "oil" variables and v "vinegar" variables ($m = o + v$, with $o > v$). These polynomials are constructed in a way that allows for relatively easy solution-finding using the structure of the private key. A public key is generated by applying a linear transformation to the private key. This transformation maps the private key’s m variables into n new variables ($n < m$). The resulting n quadratic polynomials form the public key. This is a set of randomly appearing quadratic equations without the structure of the private key.
- 2. **Signature Generation:** The message is first hashed to generate a signature for a message. The hash value (a vector) is treated as the "vinegar" part of the variable vector. The signer solves for the "oil"

variables using the private key’s structure to find a solution vector that satisfies the private key’s polynomial system. This solution vector is then transformed to obtain the signature.

- 3. **Signature Verification:** To verify the signature, the signature is transformed back to a solution vector using the inverse linear transformation from the public key. This vector is then used to verify whether it satisfies the public key’s multivariate quadratic polynomial system.

MQOM-Based Net Banking Encryption

- 1. **Secure Session Establishment:** This step remains unchanged. An HTTPS connection is established using TLS for secure communication between the user’s device and the bank’s server.
- 2. **MQOM-based Authentication and Key Exchange:** This step is significantly altered.

Server Sends Public Key: The bank’s server sends its public key for the MQOM system to the user’s browser. This is a set of multivariate quadratic polynomials (the transformed system in MQOM, representing the public key). There’s no digital certificate at this stage (or a modified certificate would be required).

Session Key Generation: The user’s browser doesn’t explicitly generate a session key. The session key might be implicitly derived within the MQOM signature generation process itself. Some MQ schemes may have implicit key agreement as part of the signature creation.

Transaction Signing (Using MQOM):

Instead of using RSA or ECDSA, the transaction data (sender’s account, receiver’s account, amount) is hashed. This hash value is then used as input for the MQOM signature generation algorithm. The bank’s public key (the underlying, simpler polynomial system and the transformation mapping in MQOM) is used to transform this hash into a digital signature. This signature is then included with the transaction data. This is the core change in this step—the computationally easy part (using the public key) of the MQOM transformation happens here.

Sending Transaction Data and Signature:

The encrypted transaction data (using a session key established via a separate secure channel, or a key implicitly derived in the signing process) and the MQOM digital signature are sent to the bank’s server.

Transaction Data Encryption: Transaction details are encrypted using a session key using AES algorithm.

Bank Processes the Transaction

- **Signature Verification (Using MQOM):**
The bank receives the encrypted transaction data and the digital signature. It decrypts the data using the session key. The bank then verifies the signature using the private key and the MQOM signature verification algorithm. This is the computationally hard part of the process (checking if the signature is valid). If verification fails, the transaction is rejected.
- **Validation:** After successful signature verification, the bank performs its standard validation checks (sufficient funds, valid account numbers, compliance with regulations, fraud detection routines, etc.).
- **Credit Transaction:** If everything is valid, the transaction is processed.
- **Acknowledgment and Confirmation:** The bank generates a confirmation message, encrypts it (using the session key), and sends it to the user’s browser.
- **Session Termination:** Secure session and session keys are terminated once the transaction is complete.

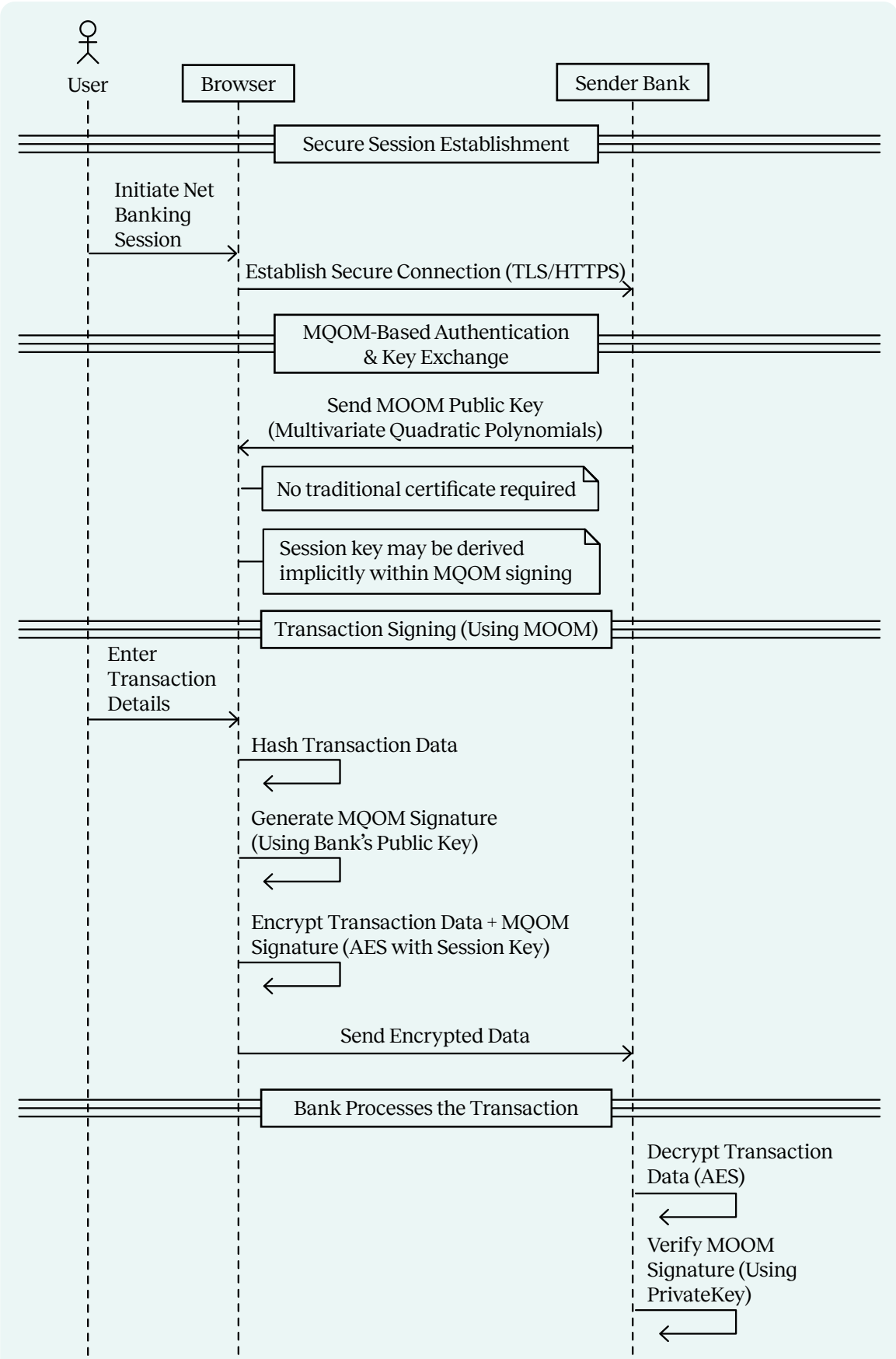


Figure 1. Multivariate Quadratic for Net Banking | Part 1

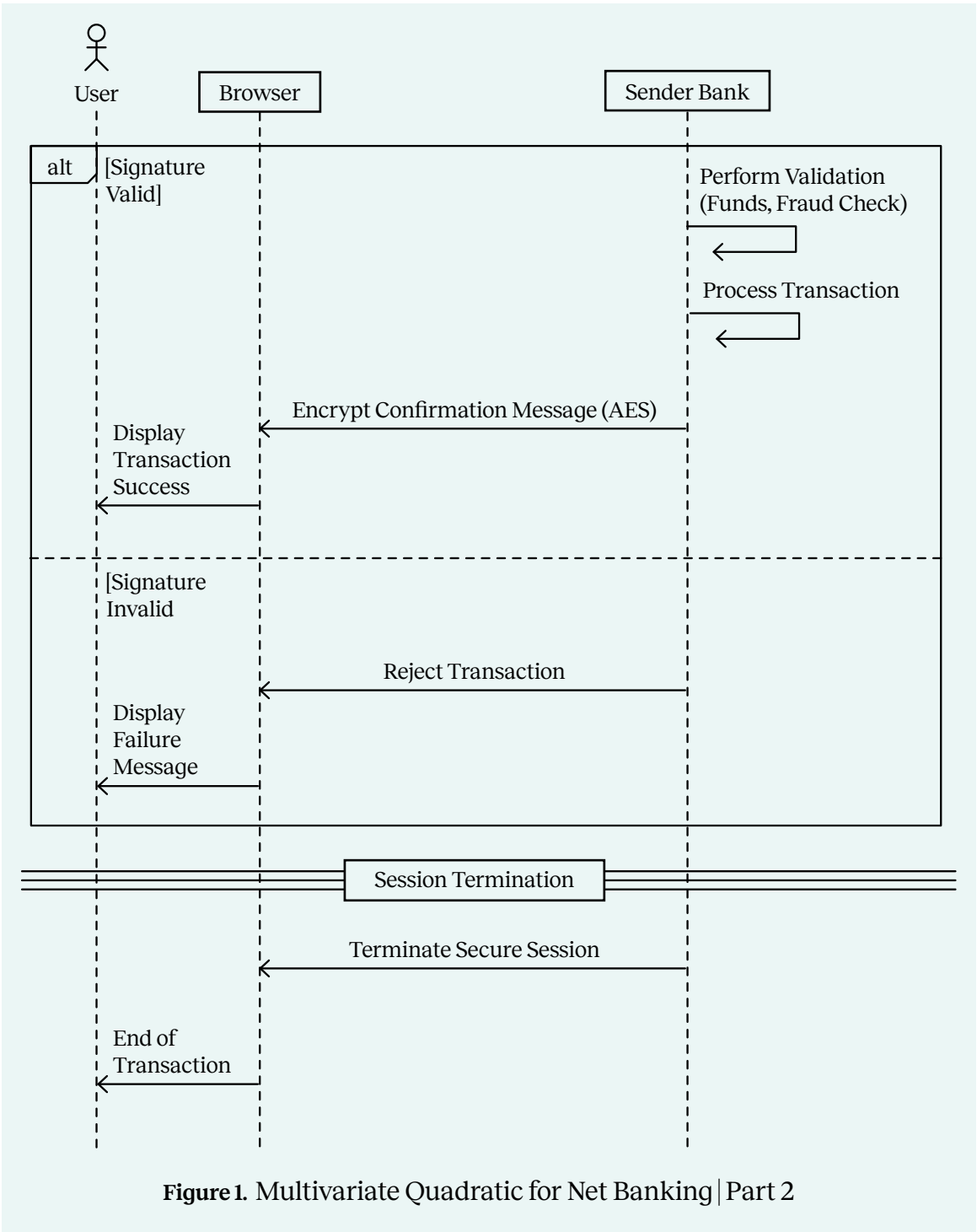
Chapter 7

*Interpretation
of the Cybersecurity
Preparedness Survey*

Methods and Data —
Perception and Experience Study

The "Perceptions and Experience" study assessed the cybersecurity preparedness of Indian banking and financial services organisations. Its primary objectives were to: (1) evaluate current cybersecurity postures by analysing existing security measures, encryption practices, data protection policies, and vulnerabilities to quantum computing attacks; (2) gauge CISOs' awareness of quantum-related threats, including their understanding of quantum computing's impact on cryptography, data security, and operations; and (3) determine the readiness of quantum-guided business models by analysing existing PQC transition plans and identifying preparedness gaps. In this chapter, we present the main findings from the survey.

The survey, conducted from January to February 2025, gathered data from 118 CISOs/CTOs across the BFSI sector. It covered various aspects of cybersecurity maturity, including organisational profiles (firmographics), cyber threat perceptions, understanding of quantum computing, technological and operational readiness, and policy recommendations. The data gathered has informed the development of strategic recommendations for mitigating quantum-related threats within the BFSI sector.



Findings

1. Organisational Profile

The majority of respondents (50%) identified themselves as working in Public Sector Banks, highlighting significant representation from this sector. Other respondents included those from Asset Management Companies, Insurance Companies, National Housing Banks, Private Sector Banks, and Foreign Banks, with a smaller share from Non-Banking Financial Companies (NBFCs), Payment Banks, and Small Finance Banks (Fig. 1).

The survey revealed that a majority of the divisions (60%) operated primarily within India, while 25% had a combined presence in both India and foreign regions, and 15% operated exclusively in foreign markets (Fig. 2).

In terms of revenue, the majority of respondents (30%) belonged to Giant organisations (those with revenue exceeding \$20 billion), followed by Mid-size organisations (27.5%) (revenue between \$500 million and \$5 billion), and Large organisations (17.5%) (revenue between \$5 billion and \$20 billion). Small organisations (25%) (those with revenue less than \$500 million) formed the last segment (Fig. 3).

2. Cybersecurity Maturity

The survey used the CISA Zero Trust Maturity Model to evaluate respondents' Zero Trust maturity. The overall cybersecurity maturity score across divisions averaged 3.65 out of 5, indicating a moderate level of maturity, with room for improvement. The data shows a clear connection between Zero Trust maturity

and cybersecurity performance. Divisions at the "Advanced Level" of Zero Trust maturity achieved the highest cybersecurity maturity, averaging 4.00, with 22.73% reaching Level 5. In contrast, divisions at the "Initial Level" averaged 3.33, mostly remaining at Levels 3 and 4, while divisions in the "Not Adopted" category trailed with an average score of 3.00, struggling to move beyond Level 3. This underscores the importance of advancing Zero Trust adoption to strengthen cybersecurity maturity (Fig. 4).

3. Security Measures and Threat Landscape

The survey assessed the implementation of various security measures within the divisions. While firewalls (92.50%), endpoint protection (90%), and Multi-factor Authentication (90%) were widely adopted, the implementation of more advanced security measures such as intrusion detection systems, vulnerability management tools, and SIEM was less prevalent (Fig. 5).

The most frequently reported cybersecurity threats were phishing attacks (65%), DDoS attacks (47.50%), and social engineering attacks (40%). Other threats, such as ransomware, data breaches, cloud security vulnerabilities, and insider threats were reported but were less prevalent (Fig. 6).

Banks and financial institutions have adopted various data storage methods to enhance security against cyber threats, with around 31.25% of the CISOs/CTOs choosing a hybrid (blending cloud and private servers) approach. Private servers maintained by banks and private institutions are the second

most preferred option at 27.08%, reflecting a preference for direct, in-house oversight. Third-party data centres account for 25%, indicating notable trust in external providers. Utilisation of cloud storage services is less common at 10.42%, while other methods constitute 6.25%, indicating some reliance on alternative solutions. The dominance of hybrid and private models highlights a clear focus on balancing security with operational resilience (Fig. 7).

4. Preparedness for Incidents and Threat Prioritisation

A significant portion (45%) of respondents reported high levels of preparedness for cybersecurity incidents. However, a notable percentage (19%) of the respondents did not regularly test their security processes, highlighting a potential vulnerability in their preparedness strategies (Fig. 8).

When asked to prioritise threats for the next 12 months, the most critical threats identified were compliance and regulatory issues, data breaches, and phishing attacks. (Fig. 9)

The operational presence of the BFSI institutions in the study spans India, combined regions (India and abroad), and foreign-only regions, each displaying varied maturity levels under the CISA Zero Trust Maturity Model. While Indian operations show strong progress with 62.5% operations at an advanced level, around 12.5% remain at the "Not Adopted" stage, indicating potential for further improvement. Combined operations show a balanced spread, but with 30% still at the "Not Adopted" level, progress seems slower. Notably, foreign operations have no presence at the "Not Adopted" level, suggesting a stronger

commitment to at least initial adoption, even if advanced maturity remains a work in progress (Fig. 10).

5. Quantum Computing Preparedness

The majority (45%) of the respondents stated that they had not engaged in any discussions or briefings on the implications of quantum computing on cybersecurity within their divisions (Fig. 11). The survey also revealed that a large number of respondents rated their understanding of quantum computing as moderate, indicating a moderate level of awareness and the need for further education and training (Fig. 12). Concerns regarding quantum computing-related cyber threats were high (average rating of 3.675 out of 5) with 32.5% of respondents rating their concern at level 4, and 27.5% selecting level 5, indicating very high concern (Fig. 13).

A significant percentage (57.5%) of respondents believed that quantum computing would pose a material threat to BFSI cybersecurity frameworks within the next 3 years (Fig. 14). There was also a wide range of opinions regarding the migration timeline related to post-quantum cryptography, although a high percentage had not yet initiated this process (Fig. 15).

Organisations with lower preparedness levels of cyber security reported low crypto-agility thereby indicating low adaptability to new cryptographic standards, with an average score of 1.0 at the lowest level. Adaptability to new cryptographic standards improved progressively alongside preparedness, reaching an average of 3.9 at the highest level. Half of the respondents at the highest preparedness level

also demonstrated the highest adaptability, highlighting a strong connection between robust cybersecurity measures and readiness for cryptographic transitions (Fig. 16).

6. Data Breach: Harvest Now, Decrypt Later

The data on the potential impact of quantum decryption on stolen information highlights a strong sense of urgency and concern. Most respondents (57.5%) considered the impact extremely significant, showing that many recognise the severe damage data breaches could cause. With an average score of 4.13, the results suggest that most respondents view quantum decryption as a critical, high-stakes threat with potentially devastating consequences (Fig. 17).

7. Quantum Readiness: A Critical Business Gap

The data reveals that most organisations are underprepared for implementing quantum-resistant security measures. A striking 60% rated their preparedness as low (1 or 2), while only 17.5% considered themselves highly prepared (4 or 5). The overall average score of 2.4 highlights a significant gap in readiness, signalling an urgent need for stronger, future-proof security strategies (Fig. 18).

Organisational readiness for quantum-resistant security measures varies based on when organisations expect quantum computing to become a cybersecurity threat. Those anticipating the threat within 3 years report the lowest preparedness, averaging 2.35, with most falling between levels 2 and 3. Organisations expecting the threat within 5 years show a slight improvement, averaging 2.43, but still remain in the mid-range scores. In

contrast, those expecting the threat within 10 years report significantly higher confidence, averaging 3.5, with half reaching levels 4 and 5 (Fig. 19).

The data suggests that organisations with lower preparedness may perceive the threat as closer, possibly because they recognise they are not equipped to implement quantum-resistant security measures in time.

8. Post-Quantum Cryptography: Challenges, Strategies, and Future Readiness

The most commonly recognised key management measures include Access Control Measures and Encryption of Keys at Rest and in Transit, highlighting a strong focus on restricting access and ensuring data integrity. Staff Training and Awareness Programs, along with Secure Key Storage, also rank high, underscoring the importance of human factors and secure hardware.

Key Management Policies, Auditing and Monitoring of Key Usage, and Regular Key Rotation reflect procedural and operational best practices. Meanwhile, Backup and Recovery, Adoption of Quantum-Resistant Algorithms, and Vendor Evaluation appear less frequently, suggesting that future readiness and compliance efforts may need greater attention (Fig. 20). Notably, a small but concerning portion of respondents reported having no specific key management measures in place, pointing to a potential gap in awareness or implementation.

Organisations face multiple challenges in addressing quantum readiness, with Technology (22%) being the most cited

concern, reflecting issues of readiness and advancements. Comprehensive Risk Assessment (20%) and Implementing Quantum-Resistant Systems (19%) follow, indicating a strong focus on risk management and practical implementation. Budget and Evaluating Vendors' Quantum Readiness (both 11%) are notable but secondary challenges. Regulatory issues and Staff Education and Training (both 9%) rank lower, suggesting they are important but are not seen as immediate barriers (Fig. 21).

9. Strategic Priorities for Post-Quantum Cryptography Adoption

According to respondents, the most important step the government can take to accelerate the standardisation and adoption of post-quantum cryptography algorithms is establishing guidelines and standards, which emerges as the leading priority at 45%. Funding research and development follows at 27.5%, Emphasising the need for investment in innovation. Stakeholder collaboration (17.5%) is also considered valuable, though to a lesser extent. Financial incentives for adoption rank the lowest at 10%, suggesting that this intervention is not viewed as a primary driver in this process (Fig. 22).

Certification programs for quantum cybersecurity are the most favoured approach for cybersecurity awareness and education, with 42.5% of respondents supporting them. Public awareness campaigns follow at 32.5%, indicating a strong preference for broad outreach efforts. Training programs (15%) and educational resources (10%) receive lower support, suggesting that they are seen as less impactful in driving awareness and preparedness (Fig. 23).

When it comes to incentives and funding mechanisms for financial institutions to prioritise post-quantum cryptography, respondents favour government-funded audits and research grants equally, each receiving 30% support. Tax credits follow closely at 27.5%, indicating a strong preference for financial relief measures. Liability protection for early adopters ranks the lowest at 12.5%, suggesting it is not seen as a primary motivator for investment in post-quantum security (Fig. 24).

To support a smooth and secure transition to post-quantum cryptography in the financial sector, respondents prioritise the development of a clear migration timeline (45%). Guidance on algorithm selection follows at 27.5%, highlighting the need for technical direction. Regulatory harmonisation (15%) and breach notification rules (12.5%) are seen as lower priorities, suggesting that, while important, they are not the most immediate concerns in the transition process (Fig. 25).

To enhance collaboration and information sharing on quantum threats and mitigation strategies, the majority of the respondents (42.5%) favour the establishment of a dedicated forum or working group. Mandatory information sharing follows at 27.5%, reflecting the importance of structured communication. The development of best practices (20%) is also seen as valuable, while international cooperation ranks lowest at 10%, suggesting it is perceived to be a lesser priority compared to domestic efforts (Fig. 26).

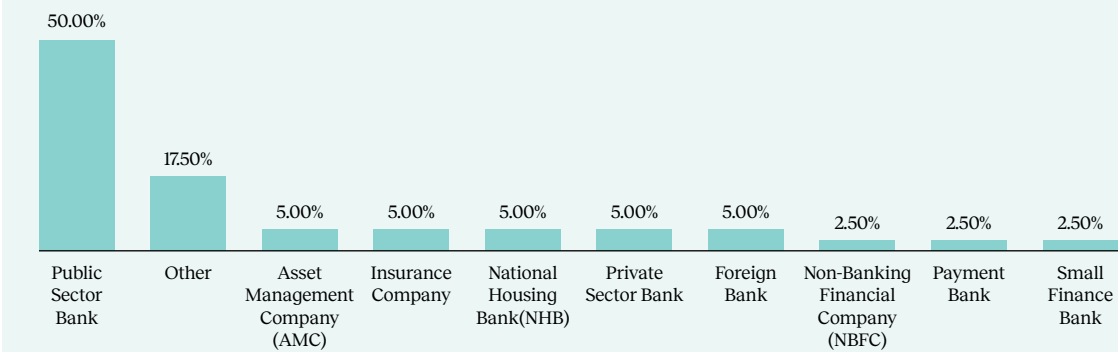


Figure 1: Distribution of Respondents by Financial Institution Type

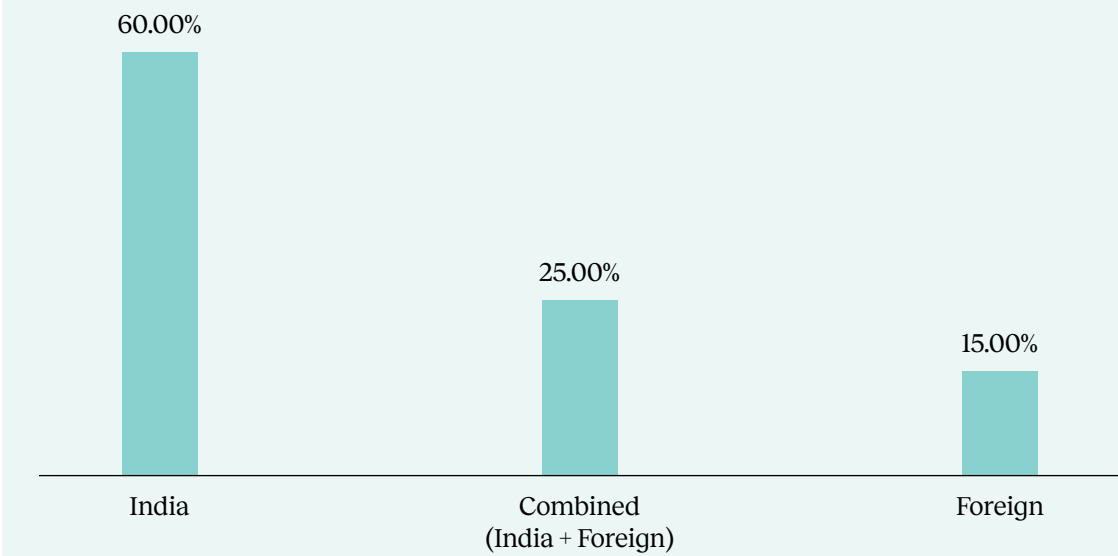


Figure 2: Geographic Distribution of Division's Operational Presence

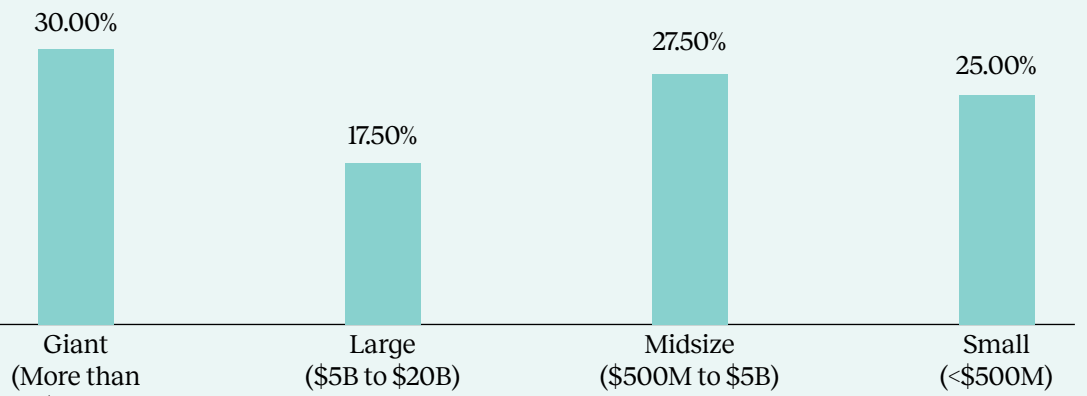
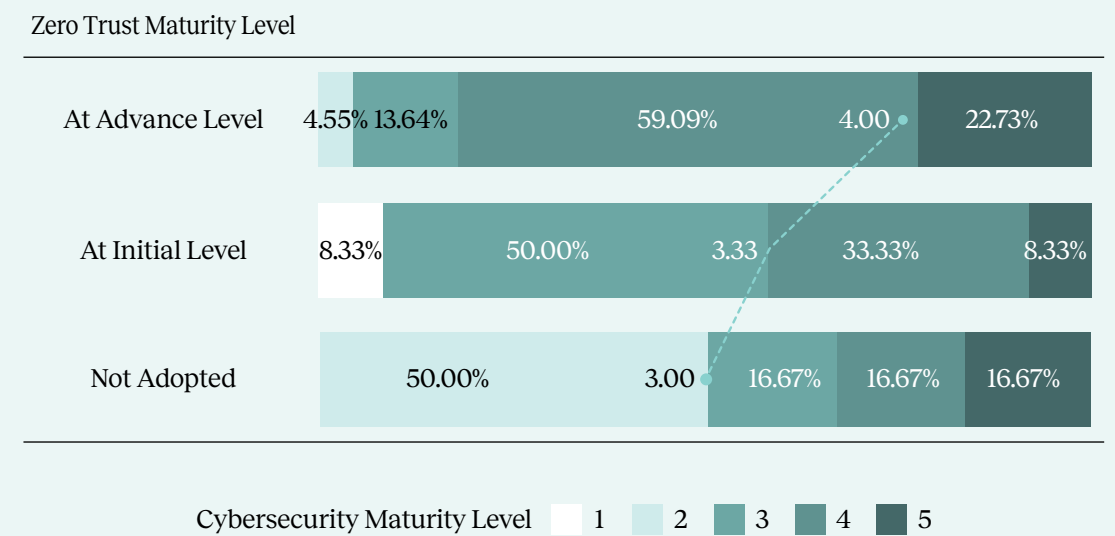


Figure 3: Revenue Classification of Divisions by Size



Cybersecurity Maturity Level 1 2 3 4 5

Figure 4: Relationship Between Zero Trust Maturity Level and Overall Cybersecurity Maturity Rating

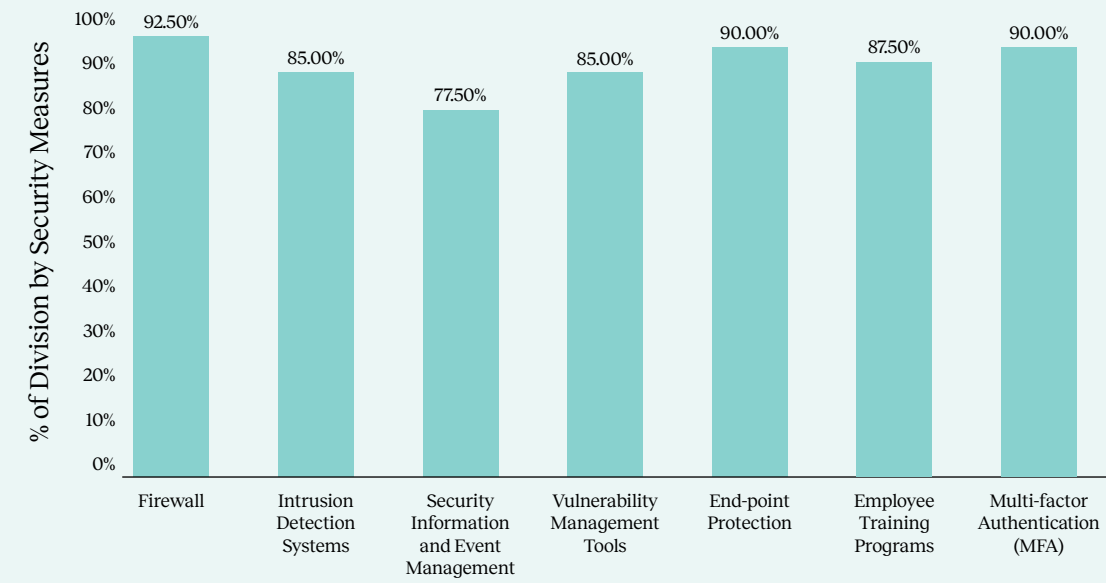


Figure 5: Security Measures Implemented by Divisions

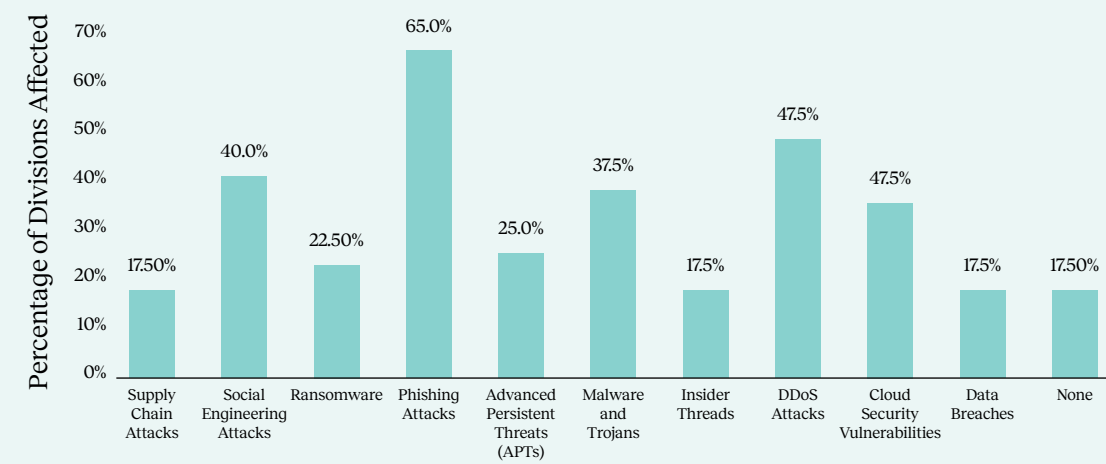


Figure 6: Types of Cybersecurity Threats Experienced by Divisions 2024-2025

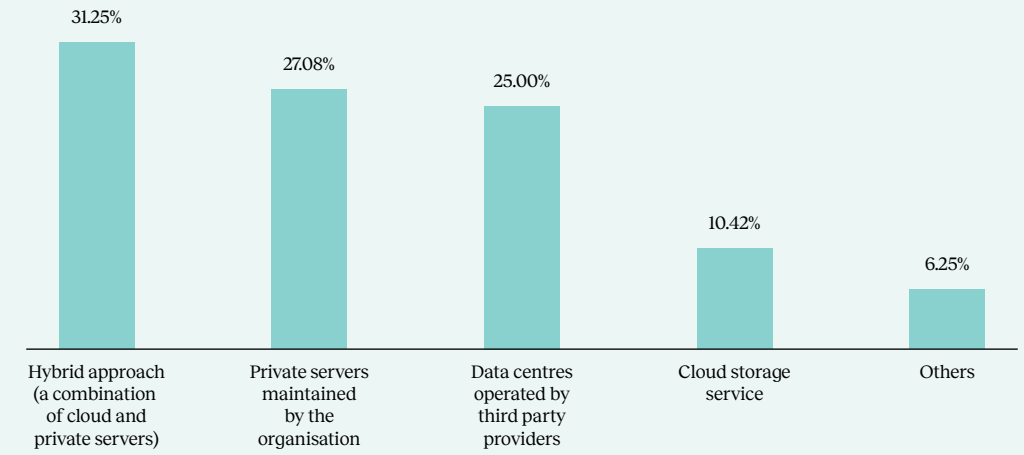


Figure 7: Primary Data Storage Methods for Security

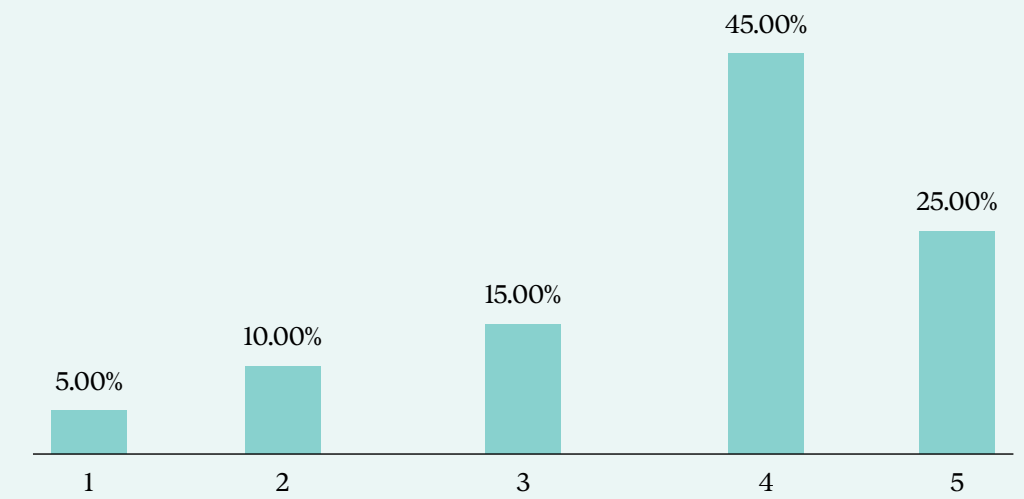


Figure 8: Division's Readiness to Respond to Cybersecurity Incidents (Likert Scale)

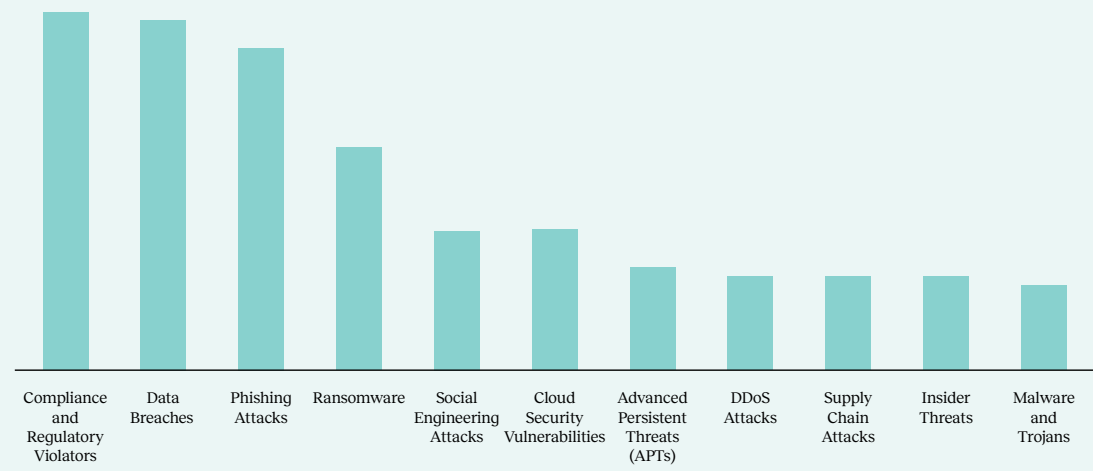


Figure 9: Perceived Biggest Cybersecurity Threats for the Next 12 Months

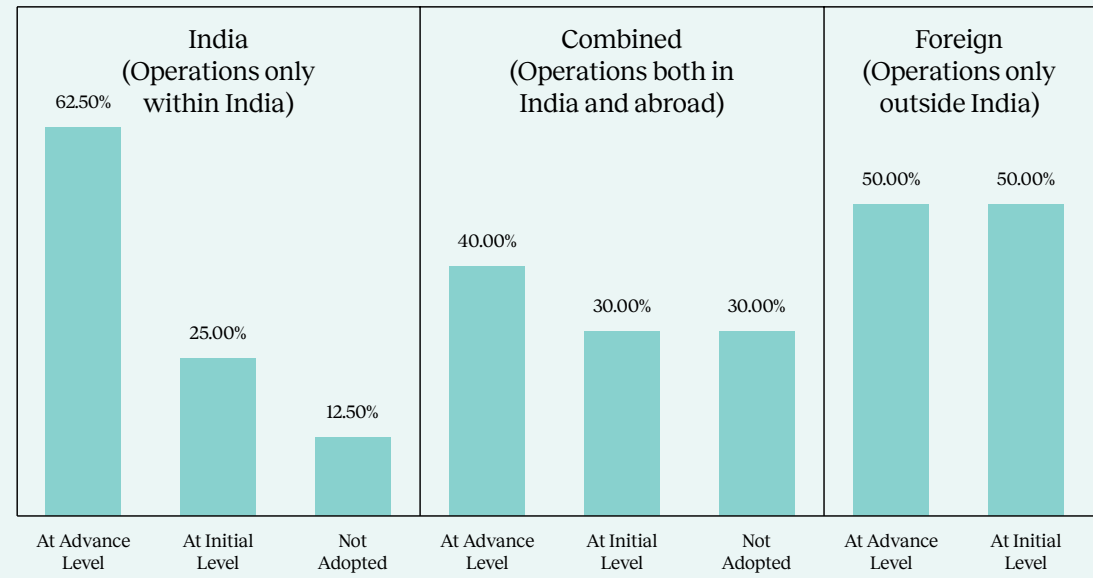


Figure 10: Adoption of Zero Trust Levels Across Different Regions

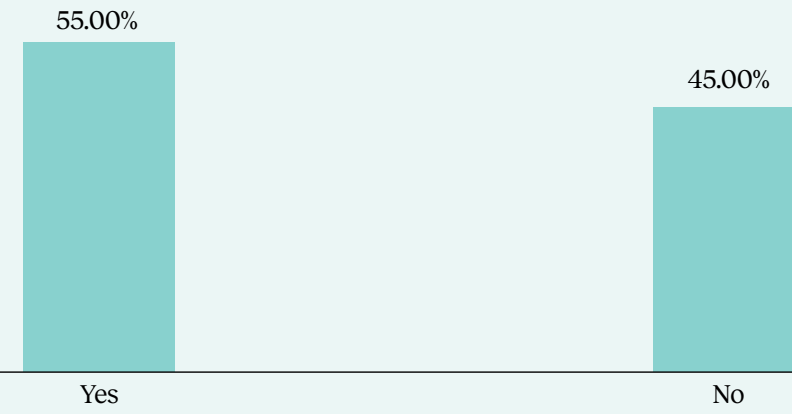


Figure 11: Engagement in Discussions on Quantum Computing Implications for Cybersecurity

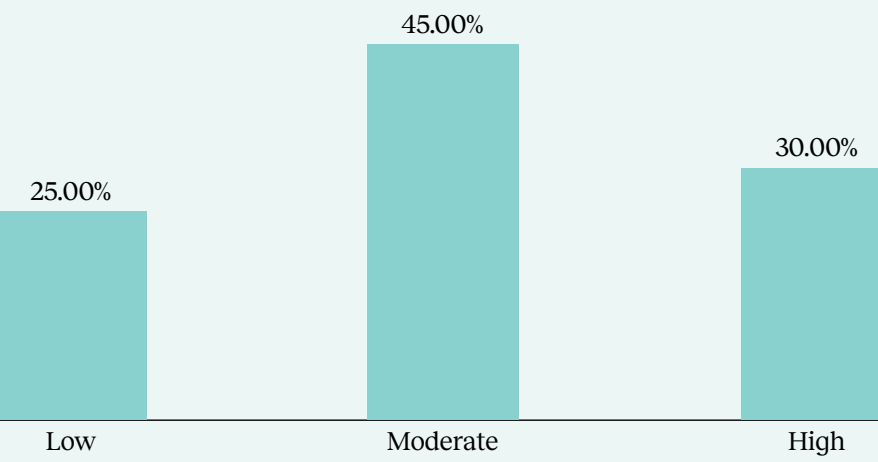
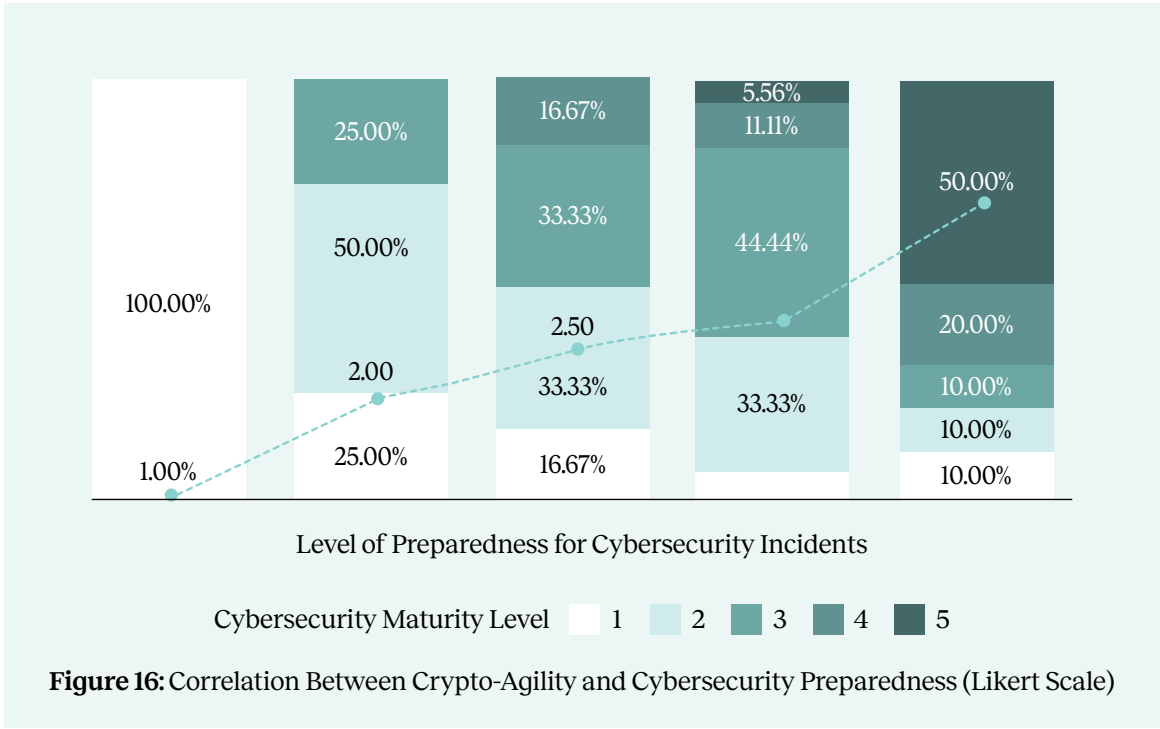
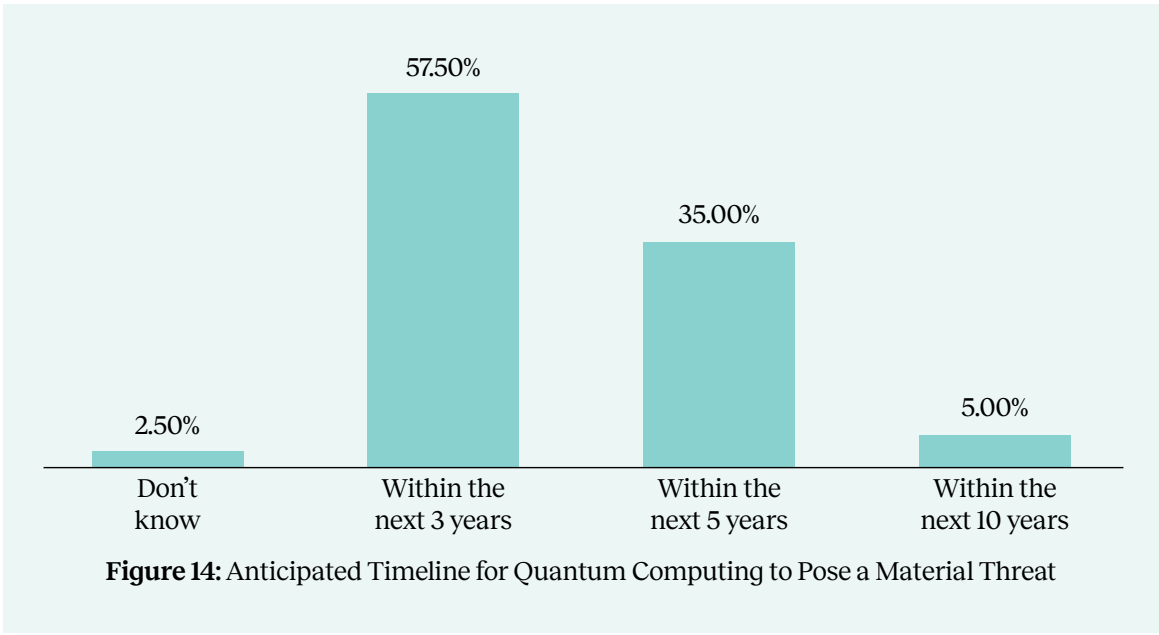
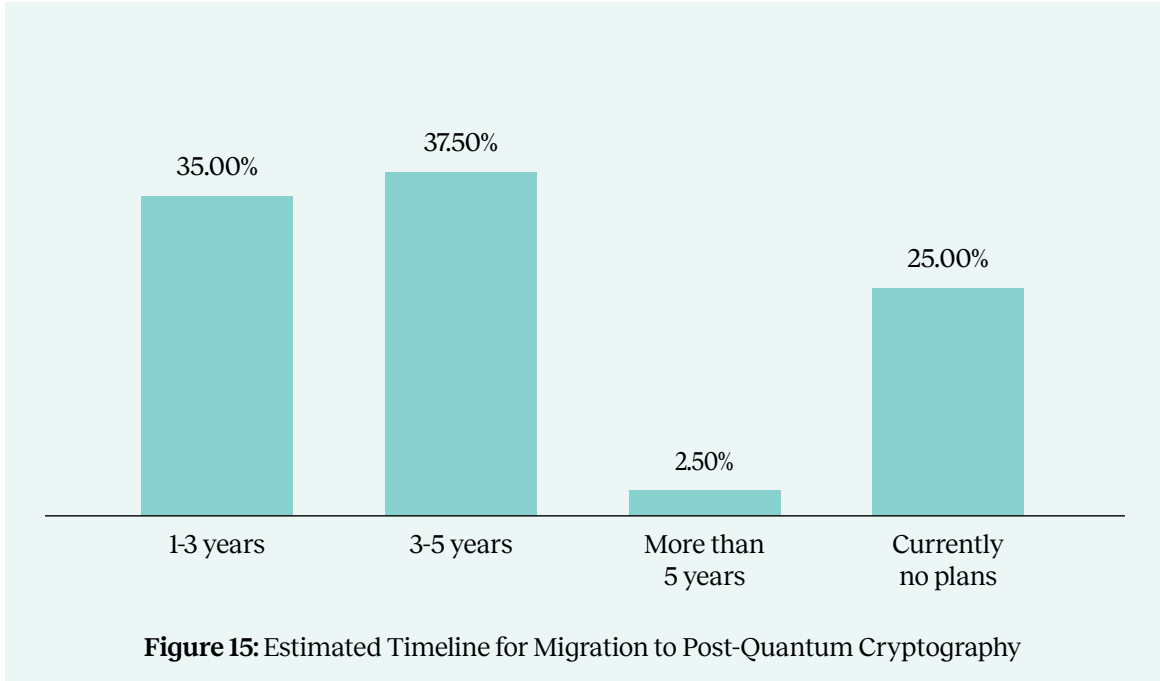
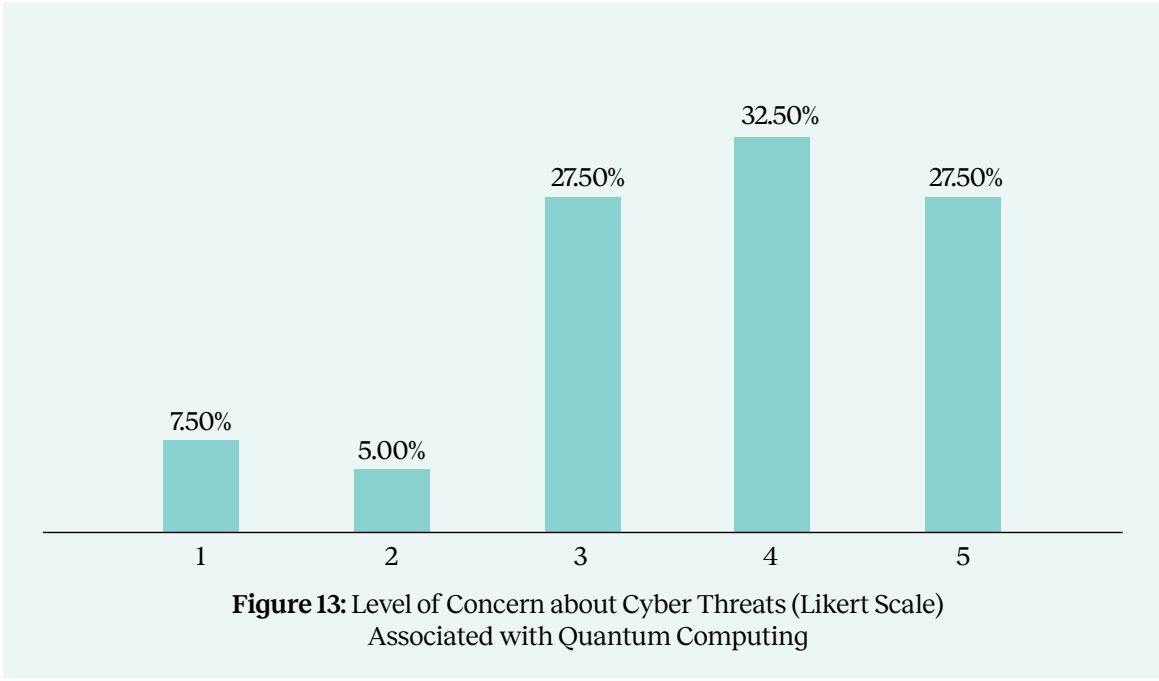


Figure 12: Level of Understanding of Quantum Computing



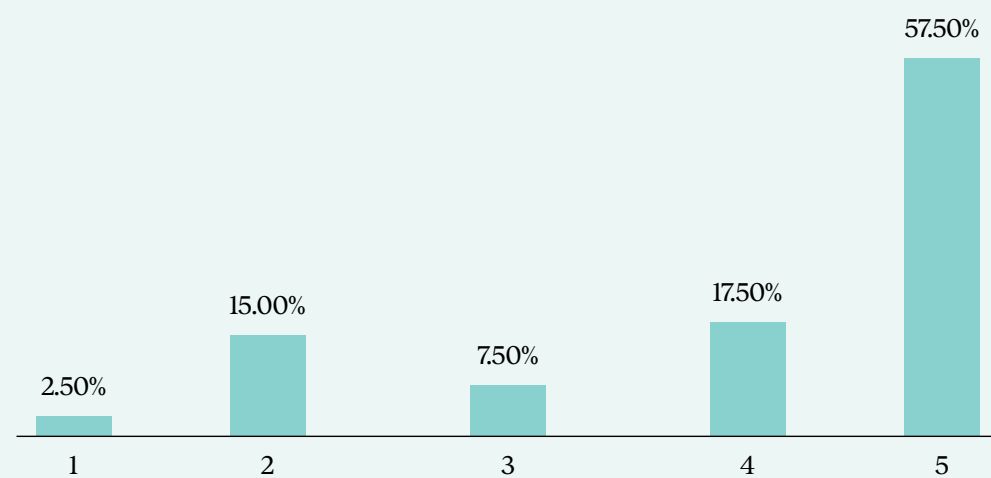


Figure 17: Perceived Impact of Future Quantum Decryption on Data Breach Severity (Likert Scale)

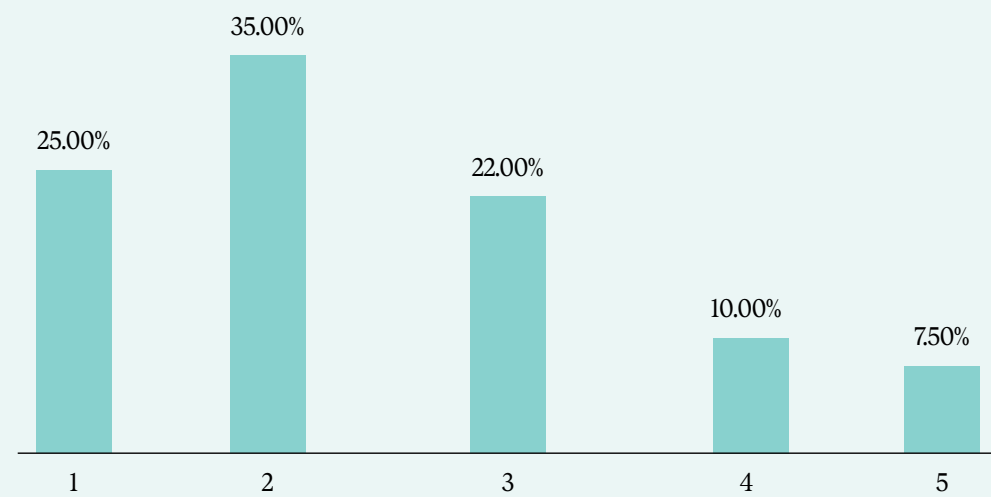
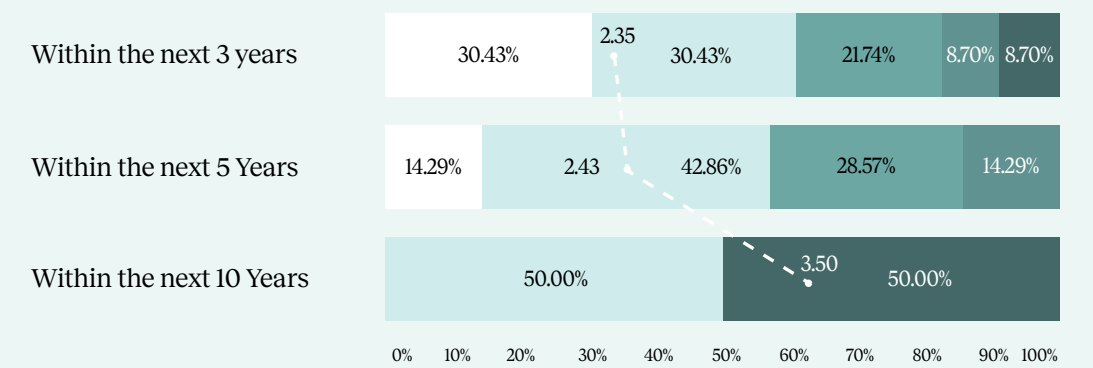


Figure 18: Readiness of Business Models for Implementing Quantum-Resistant Security Measures (Likert Scale)

Quantum Threat Timeline Expectation



Readiness of Business Model for Quantum-Resistant Security

Cybersecurity Maturity Level 1 2 3 4 5

Figure 19: Timeline for Quantum Threats and Business Model Preparedness

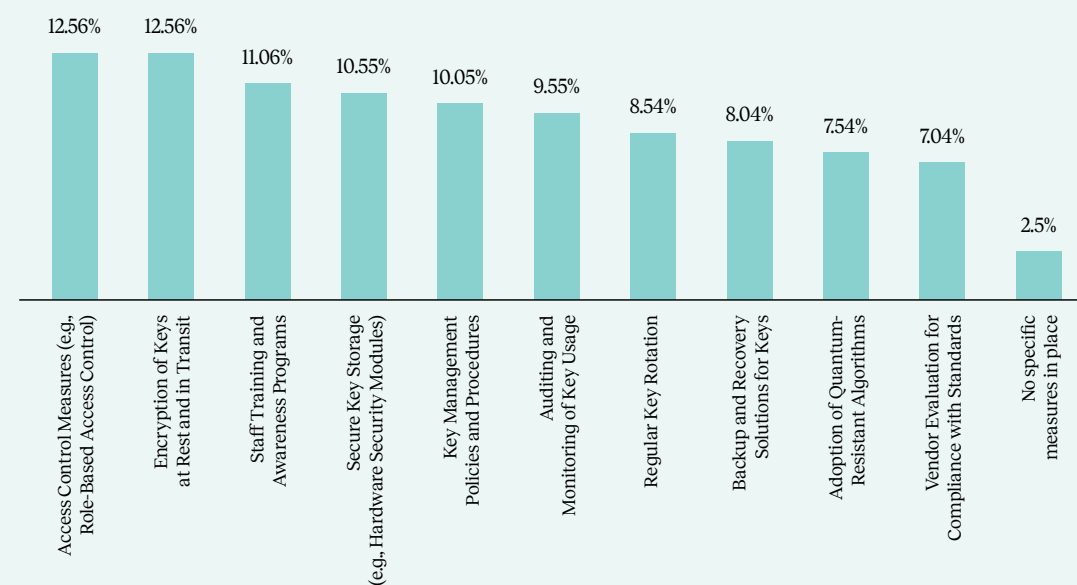
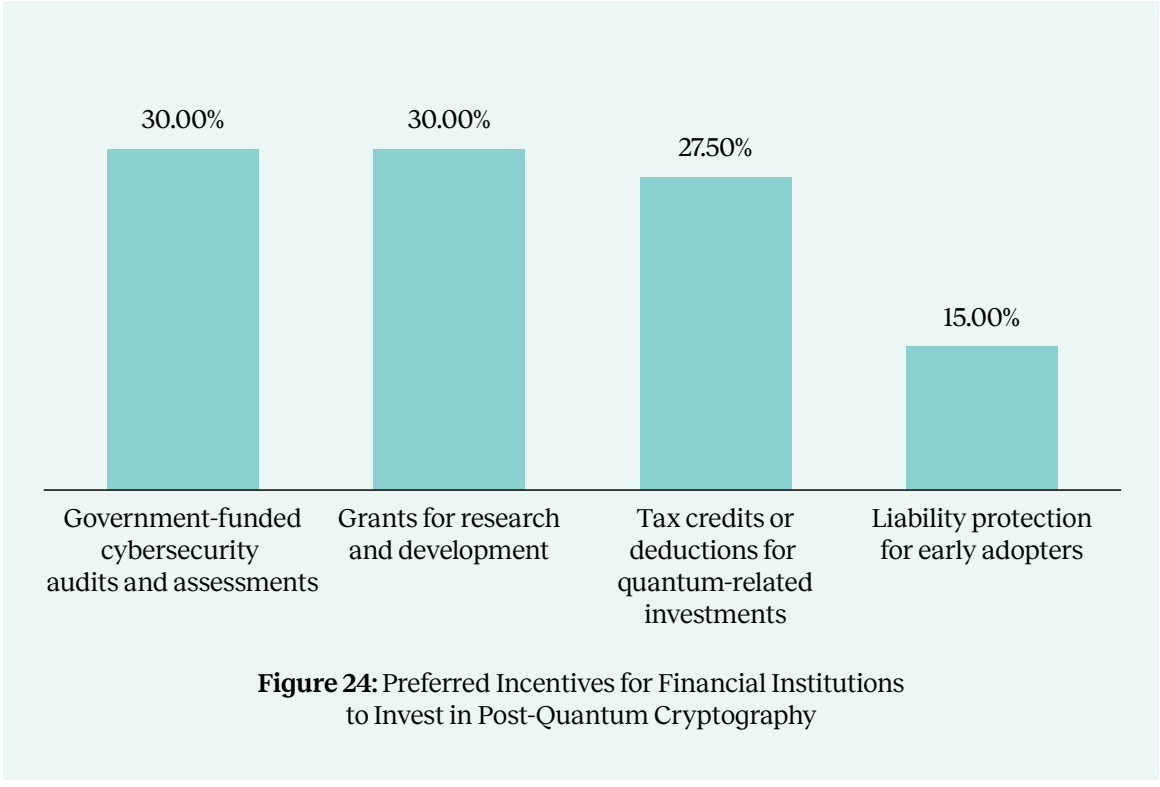
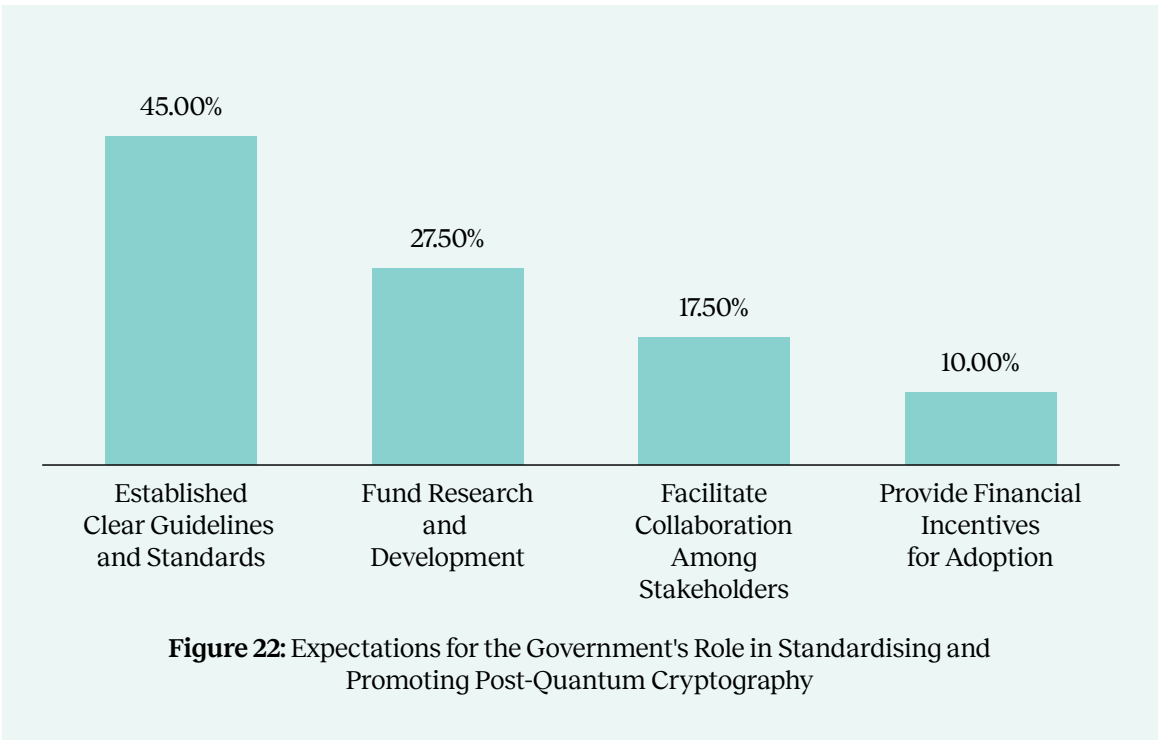
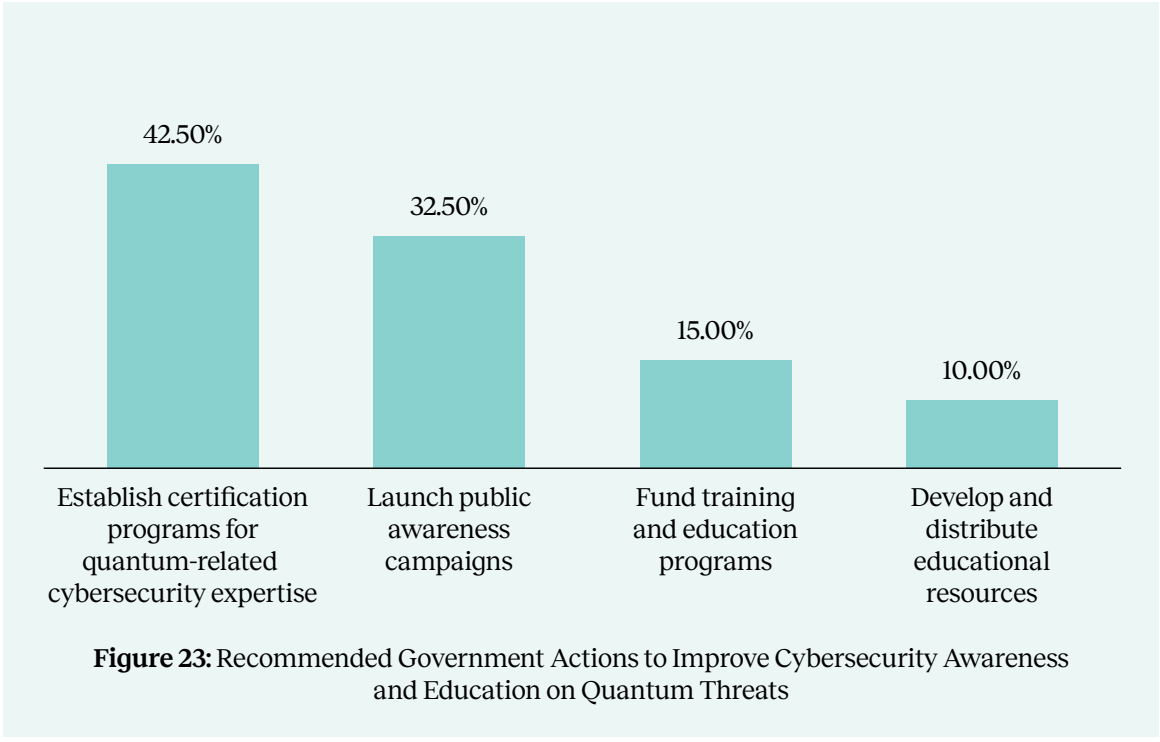
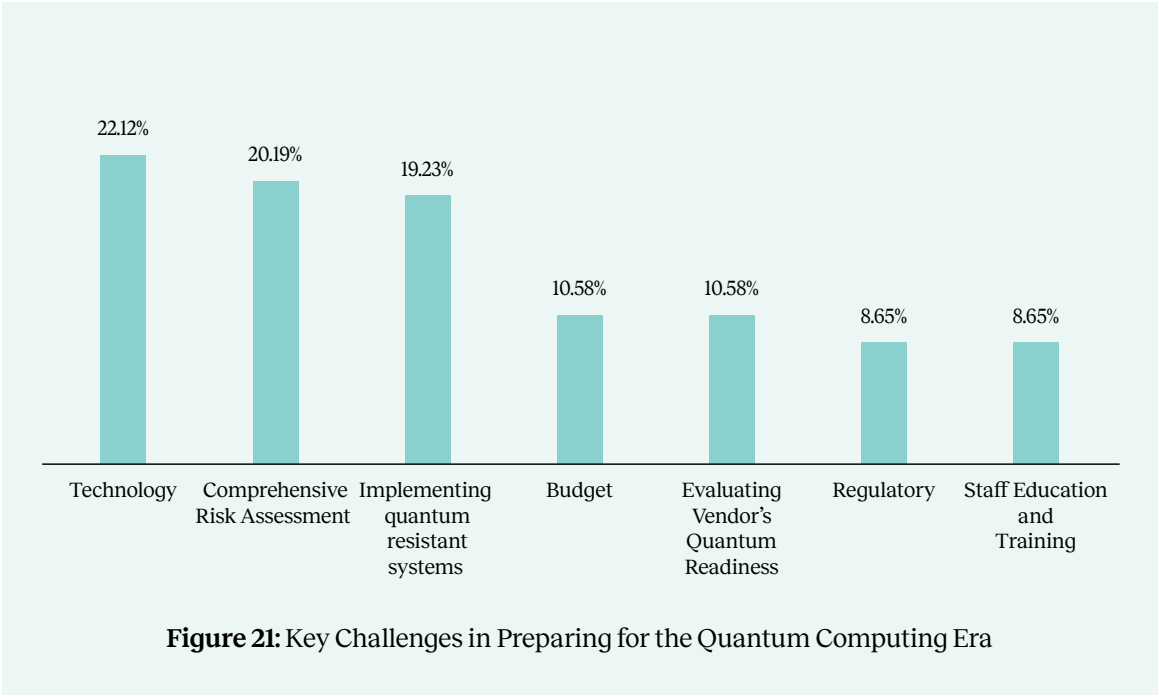
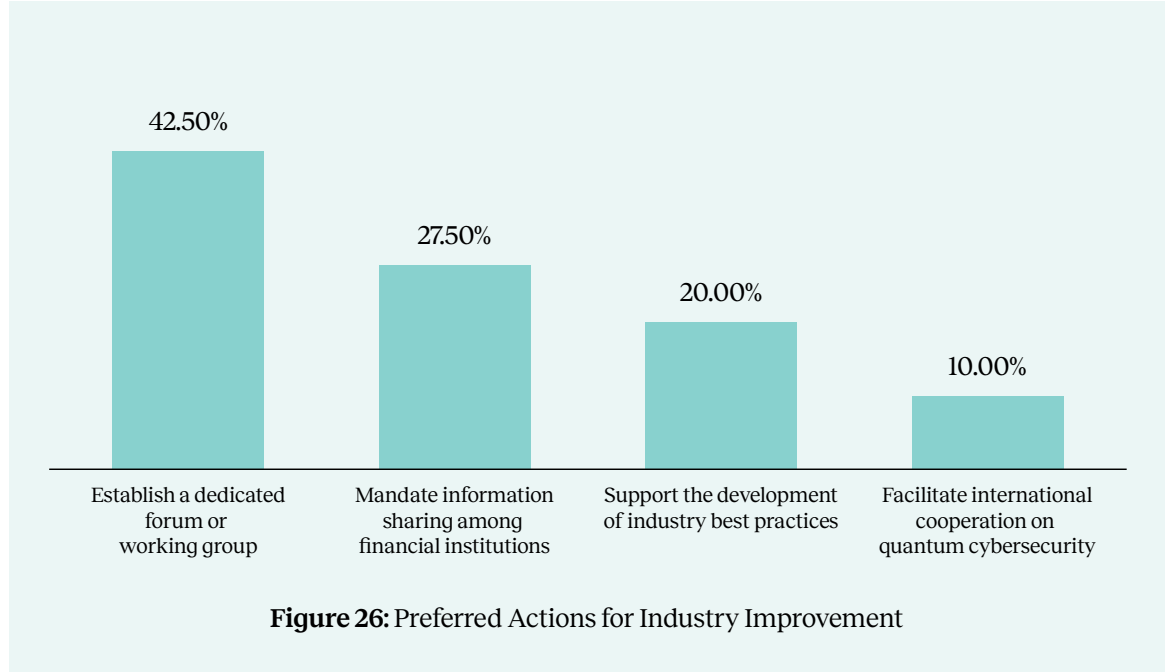
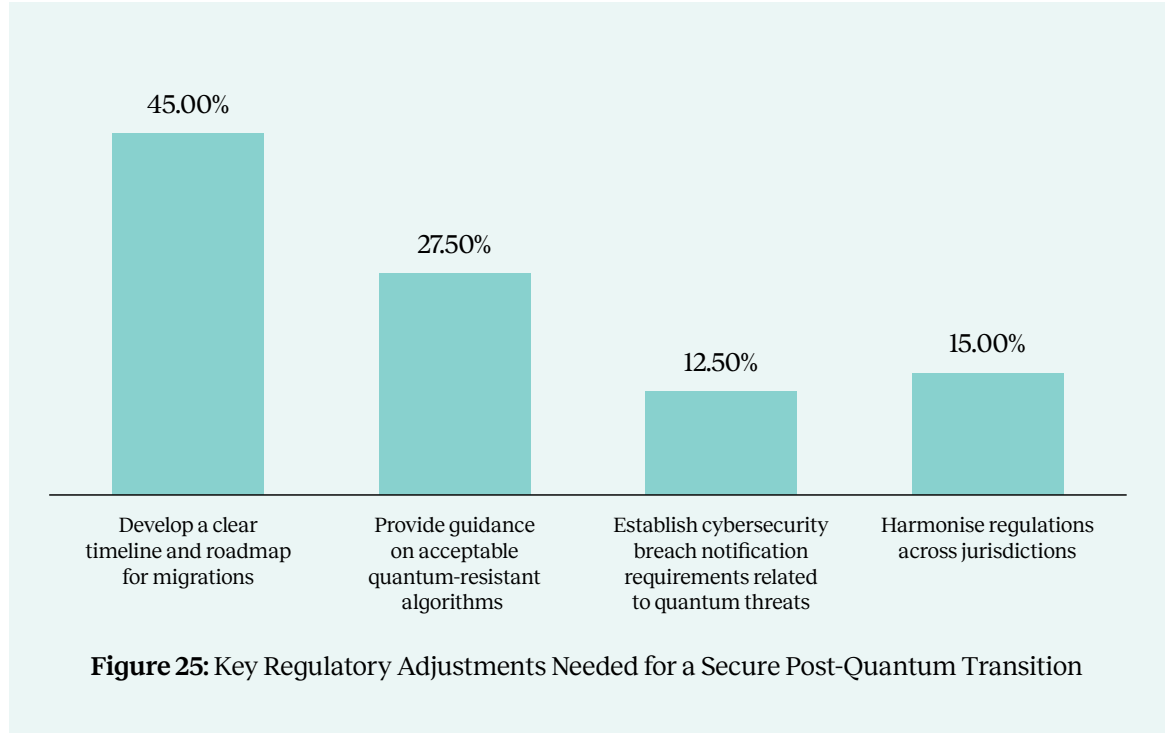


Figure 20: Measures for Managing and Safeguarding Cryptographic Keys





Chapter 8

Policy Recommendations for Banks and Financial Institutions: Preparing for the Post-Quantum Cryptography Era

The rapid advancement of quantum computing presents a significant and evolving threat to existing cryptographic systems, particularly within the financial sector. To mitigate these risks, a timely and well-planned transition to Post-Quantum Cryptography (PQC) is crucial. This requires a multi-faceted approach involving both technological advancements and strategic policy decisions. The following recommendations are based on insights gleaned from a recent survey conducted among the CISOs/CTOs of banks and financial institutions, an assessment of data shelf life, and the PQC framework designed for Net banking and UPI transactions. They outline key steps for banks and financial institutions, as well as crucial policy interventions required from the Indian government, to ensure a smooth and secure migration to PQC, while also addressing the long-term implications of data preservation in the face of future quantum capabilities.

Policy Recommendations for Banks and Financial Institutions

- Prioritise Post-Quantum Cryptography (PQC) Migration:** The survey indicates that banks and financial institutions are aware of the significant threats posed by quantum computing to current cryptographic systems within the BFSI sector. As per the survey, 35% of cybersecurity professionals in banks and financial institutions anticipate that the transition to post-quantum cryptography (PQC) will occur within the next 1-3 years, while 37% expect this shift to happen in the next 3-5 years. Given these findings, banks and financial institutions need to define a timeline for migrating to PQC. This should be a high priority for all BFSI institutions.

2. **Consider Data Shelf Life:** When planning PQC migration, banks must also consider the "shelf life" of their data. Data that needs to remain confidential for an extended period (e.g., certain financial records) needs to be protected using methods resistant to attacks from both current and future (quantum) technologies. Data retention policies should be reviewed to identify which data requires the highest level of long-term protection, and migration strategies should prioritise this data accordingly.

3. **Implement a Phased Hybrid Approach:** A complete overnight switch to PQC is impractical and potentially risky. A phased migration strategy, using both existing and post-quantum cryptographic methods concurrently during the transition period, is strongly recommended. This minimises service disruption and risk. The framework designed and developed in this study acts as a road map for banks and financial institutions to migrate to PQC.

4. **Develop Crypto-Agile Security Protocols:** The existing systems should be designed for flexibility and adaptability to accommodate emerging cryptographic standards. This “crypto-agility” requires a modular system architecture, allowing for the replacement or upgrade of cryptographic components without needing extensive system overhauls.

5. **Strategic Algorithm Selection:** While familiarity may exist with various post-quantum algorithms, banks and financial institutions should prioritise those algorithms and cryptographic models that

are standardised and recommended by NIST to ensure interoperability and long-term security.

6. **Implement ISB’s ML-KEM & ML-DSA Framework for Net Banking and UPI:** To enhance security during the transition to PQC, implementing the Multilinear Map-based Key Encapsulation Mechanism (ML-KEM) framework designed by ISB should be considered. This framework can provide quantum-resistant key exchange for net banking and UPI transactions, strengthening security and safeguarding sensitive financial data.

7. **Robust Quantum-Resistant Key Management:** The security of any cryptographic system depends on proper key management. BFSI institutions should implement stringent key management practices, including secure key storage using a Quantum Random Number Generator (QRNG), regular key rotation, access control mechanisms, and well-defined procedures for key backups and recovery. Particular attention should be given to quantum-resistant key management techniques.

8. **Enhance Cybersecurity Awareness and Training:** While the survey shows that many security measures are in place, investments in comprehensive training programs are still needed. Employees must be educated on both current and emerging quantum-related cyber threats, as well as best practices for implementing quantum-resistant security. This training should be integrated into the overall cybersecurity strategy.

9. **Data-Breach Response Planning for the Post-Quantum World:** The BFSI sector needs to develop comprehensive plans to address the potential consequences of a data breach where sensitive information, encrypted using current algorithms, is subsequently decrypted using quantum computing. This requires developing robust recovery strategies, incident response protocols, regulatory compliance procedures, and clear communication plans for stakeholders.

10. **Third-Party Vendor Risk Management:** BFSI institutions must conduct thorough due diligence on all third-party vendors involved in their technology infrastructure, particularly those providing cryptographic services or security solutions. Contracts should include specific clauses addressing PQC migration, outlining vendor responsibilities, ensuring the security and reliability of services provided by them throughout the transition. Regular audits and assessments of third-party vendors are vital.

Recommendations for Banks Regarding Third-Party Vendor Management in the Context of PQC Migration

The transition to Post-Quantum Cryptography (PQC) requires a comprehensive approach to cybersecurity risk management, extending to all aspects of a bank’s technology infrastructure, including its reliance on third-party vendors. To mitigate the risks associated with third-party vendors during this transition, banks should implement the following measures:

1. **Due Diligence and Vendor Selection:** Conduct thorough due diligence on all third-party vendors involved in providing cryptographic services or security solutions. This due diligence should extend beyond basic security assessments to include a detailed evaluation of the vendor’s plans for PQC migration, their experience with post-quantum algorithms, and their capacity to meet the bank’s security requirements. The selection process should prioritise vendors with proven experience in PQC implementation and a strong track record of security.

2. **Contractual Agreements:** Include specific clauses in contracts with third-party vendors that address PQC migration. These clauses should clearly outline:
 - The vendor’s responsibilities for supporting the bank’s PQC migration.
 - The timeline for implementing PQC-compliant solutions.
 - The vendor’s commitment to providing regular updates and security patches.
 - The mechanisms for addressing any vulnerabilities or security breaches.

- The vendor’s compliance with relevant industry standards and regulations.
 - The processes for termination of contracts if the vendor fails to meet security standards.
3. Ongoing Monitoring and Audits: Implement a robust program for ongoing monitoring and regular security audits of third-party vendors. These audits should evaluate the vendor’s security posture, their PQC implementation, and their adherence to contractual obligations. The findings of these audits should be carefully reviewed, and any necessary corrective actions should be implemented promptly.
 4. Security Information and Event Management (SIEM) Integration: Integrate third-party vendor security systems with the bank’s SIEM system. This integration enables centralised monitoring and analysis of security events across the bank’s entire technology infrastructure, allowing for faster detection and response to potential threats originating from third-party systems.
 5. Regular Communication and Collaboration: Establish clear communication channels and have regular meetings with third-party vendors to discuss PQC migration progress, address challenges, and ensure effective collaboration. Open communication promotes early detection and mitigation of potential risks.
 6. Phased Migration Approach: The transition to PQC should have a phased approach. The bank and its vendors should collaborate to create a timeline for

upgrading systems and gradually integrate PQC-compliant solutions while ensuring uninterrupted services. This reduces the overall risk of disruption.

7. Training and Awareness: Banks and financial institutions can take initiatives to provide training and run awareness programs for both bank employees and third-party vendor’s personnel on the importance of PQC and the best practices for implementing quantum-resistant security measures. This ensures that all stakeholders are aware of the security implications and the steps necessary to protect sensitive data.

Policy Recommendations for the Government and the Reserve Bank of India (RBI): Facilitating a Smooth Transition to PQC

Governmental action and RBI oversight are vital in guiding and supporting India’s transition to post-quantum cryptography.

1. Establish Clear Guidelines and Standards: Provide clear, concise guidelines, timelines, and best practices for PQC adoption and implementation within the financial sector. This standardisation is essential to ensure consistency and interoperability across the BFSI industry. The RBI should play a leading role in defining these standards.
2. Invest in Research and Development: Significantly increase funding for research and development of quantum-resistant cryptographic algorithms and technologies. This requires collaboration

between government agencies, academia, and private sector organisations to develop effective and efficient PQC solutions tailored to India’s unique needs. The RBI can incentivise this research through grants and collaborations.

3. Foster Collaboration and Information Sharing: Create a collaborative environment to encourage information sharing, joint research projects, and the development of best practices. A dedicated government forum bringing together financial institutions, cybersecurity experts, and researchers would greatly facilitate this. The RBI can promote this collaboration by creating a central platform for information exchange and best practice dissemination.
4. Provide Incentives for PQC Adoption: Implement financial incentives (such as tax credits or grants) and liability protection for early adopters of PQC. This would help offset the costs of implementation and encourage rapid adoption across the BFSI sector. The RBI can influence this through its regulatory powers and policy recommendations.
5. Enhance Cybersecurity Awareness and Education: Launch comprehensive public awareness campaigns and training programs to educate financial

institutions about the implications of quantum computing and the importance of transitioning to PQC. Establish certification programs to formally recognise and reward individuals with expertise in quantum-resistant cybersecurity. The RBI can mandate or incentivise this training within the BFSI sector.

6. Harmonise Regulations and Notification Requirements: Create a consistent regulatory framework to ensure that cybersecurity regulations, particularly concerning breach notification requirements related to quantum threats, are aligned across various jurisdictions within India. This consistency would greatly simplify the process for financial institutions. The RBI should take a lead in coordinating these regulatory efforts.
7. RBI Oversight and Guidance: The RBI should provide specific guidance and oversight on the implementation of PQC within the banking and financial sector. This would include setting timelines for migration, recommending specific algorithms, and ensuring compliance with regulatory requirements. The RBI could also conduct periodic audits to assess the preparedness of financial institutions for the quantum computing era.

Conclusion

This research project comprehensively assesses the cybersecurity risks posed by the advent of quantum computing to India's Banking, Financial Services, and Insurance (BFSI) sector. Our findings highlight the immediate necessity of pre-emptively adopting Post-Quantum Cryptography (PQC), given NIST's planned deprecation of current algorithms and the anticipated emergence of quantum decryption by state actors. The survey of BFSI CISOs/CTOs revealed a concerning lack of preparedness for this transition, underscoring the critical need for immediate action. The framework developed for PQC migration addresses these concerns by offering minimal disruption to existing infrastructure through a hybrid implementation approach, facilitating easy adoption of quantum-safe protocols, and providing a future-proof architecture capable of adapting to evolving threats. The framework's design incorporates strategies to address data shelf-life considerations, ensuring long-term data protection. Our recommendations highlight the need for strong key management, robust staff training, and enhanced cybersecurity awareness programs. The importance of collaborative initiatives and government support for research and development, along with appropriate regulatory frameworks and financial incentives to encourage PQC adoption, has also been emphasised.

Future Work

This research serves as a foundation for future work in several key areas:

- Refinement of the PQC Framework:** Further research is needed to refine the proposed PQC framework for the BFSI sector. This could involve exploring additional quantum-resistant algorithms, optimising the framework's performance, and enhancing its resilience against various attack vectors. Real-world pilot programs with BFSI organisations should be conducted to thoroughly evaluate the framework's effectiveness and usability in diverse operational settings.
- Deepening the Analysis of Quantum Threats:** Ongoing research is needed to further understand the specific quantum-related threats impacting the BFSI sector. This involves analysing emerging attack

vectors and developing more sophisticated risk assessment models to evaluate the likelihood and potential impact of these threats. This will require continuous monitoring and analysis of the evolving quantum computing landscape.

- Exploring International Policy Harmonisation:** The international policy landscape surrounding PQC adoption is dynamic. Future research should focus on analysing and comparing international policies and standards related to PQC implementation and data protection to provide a comparative analysis of best practices. This will inform the development of India-specific regulations that align with global standards and maintain international interoperability while ensuring the integrity of financial systems and data.

- Addressing Human Factors:** The human element remains a critical aspect of cybersecurity. Future work should focus on developing effective training programs and creating robust awareness campaigns for financial institutions and government agencies to ensure widespread adoption and secure use of PQC technologies.
 - Development of Quantum-Resistant Key Management Systems:** Secure key management is vital for PQC implementation. Future research should focus on developing robust, quantum-resistant key management systems that provide strong protection against various types of attacks while ensuring the efficient and effective use of cryptographic keys.
 - Targeted Research and Development Funding:** Increased investment in research and development is crucial for advancing PQC technologies and building India's quantum-resistant cybersecurity capabilities. This includes funding for the development of new PQC frameworks, efficient implementation strategies, and robust testing methodologies. Specific funding should be directed toward addressing the unique challenges of the BFSI sector.
- By addressing these areas of future research, we can further enhance the cybersecurity preparedness of India's BFSI sector and promote the secure adoption of PQC, ensuring the long-term protection of sensitive financial data in the evolving quantum landscape and contributing to international best practices in this critical domain.





Chapter 8A

Steps for Successful Migration to Post-Quantum Cryptography in the BFSI Sector

As the landscape of cybersecurity evolves with the advancements in quantum computing, banks and financial institutions must plan for the transition from traditional cryptographic methods to post-quantum cryptography (PQC). This migration is essential for safeguarding sensitive financial data and maintaining trust in an increasingly digital and interconnected financial environment. The adoption of PQC will not only enhance the resilience of cryptographic systems against quantum threats but also ensure compliance with emerging regulatory requirements. In this section, we outline a structured, step-by-step approach for banks and financial entities to effectively migrate to PQC, ensuring a smooth transition while minimising disruption to existing operations. Each step is designed to address specific challenges and considerations unique to the financial sector, providing a comprehensive roadmap for securing the future of financial transactions and communications.

Step 1: Assessment and Planning

This first step in migrating to post-quantum cryptography (PQC) is crucial for ensuring a smooth and secure transition. This phase involves a thorough assessment of current cryptographic systems, data, data shelf life, and strategic planning for the implementation of PQC. The BFSI sector needs to identify various transactions within the banking ecosystem, including its diverse stakeholders and the banking supply chain. This involves understanding the technology infrastructure, such as core banking systems, payment system integration, and data storage patterns (whether hybrid, bank servers, or cloud computing). It's essential to assess data exposure, system and data interdependencies, and transmission channels among different stakeholders. Additionally, maintaining comprehensive records is crucial for understanding where and how encryption is utilised to protect data throughout the institution—covering data at rest, in transit, and during processing. This includes the use of cryptographic models, both symmetric and asymmetric, along with their algorithm implementations within the banking ecosystem. Furthermore, a thorough evaluation of cryptographic systems, including the algorithms, protocols, and key management practices currently employed across the organisation (as detailed in Chapter 2), is necessary. Finally, it is also essential to perform a risk assessment to determine the data shelf life, as described in Chapter 3.

Step 2: Risks Evaluation

- Threat Analysis: The BFSI sector must assess the potential threats that future quantum computing capabilities pose to the existing ecosystem, which could lead to compromised confidentiality, diminished integrity, weakened authentication, increased systemic risks, and supply chain vulnerabilities, as outlined in Chapter 2.
- Vulnerability Analysis: Identify weaknesses within current cryptographic systems and evaluate how quantum attacks may exploit these vulnerabilities, as discussed in Chapter 5.
- Prioritisation: Rank data according to its shelf life (chapter 3, Table 1), sensitivity and vulnerability to quantum threats in order to highlight areas that need immediate focus.

Step 3: Migration Strategy Creation

The transition to post-quantum cryptography (PQC) is a complex endeavour that requires meticulous planning. Depending on the findings of the risk assessment, the BFSI sector can select from one of the three options presented in Chapter 3.

- Option 1: Immediate Transition to Post-Quantum Cryptography
- Option 2: Futureproofing by Retrofitting Systems with Post-Quantum Cryptography
- Option 3: Enhancing Security by Focusing on Traditional Encryption Protocols

Additionally, users can utilise the mitigation framework developed in this study as a risk management strategy, as outlined in Chapter 5.

Step 4: Regulatory and Compliance Considerations

- Understanding Requirements: Stakeholders within the BFSI sector must examine pertinent regulatory requirements and industry standards, including NIST-approved post-quantum cryptography algorithms like ML-KEM and ML-DSA (as outlined in Chapter 5). This review ensures that the migration plan meets all compliance obligations related to cryptographic security.
- Document Compliance Plans: Incorporate compliance checks and maintain comprehensive documentation throughout the migration process to enable smooth audits and verifications.

Step5: Develop a Communication Plan

- Internal Communication: Set up communication channels to keep all stakeholders informed on the progress of the migration, including updates on any challenges encountered and key milestones achieved.
- External Communication: Strategise how to communicate about the transition to clients and partners, highlighting the benefits and security enhancements that PQC provides.

By completing this comprehensive assessment and planning phase, banks and financial institutions can lay a solid foundation for a successful transition to post-quantum cryptography, ensuring a proactive approach to securing data against future quantum threats.





Appendix A1

Expert Interview: Rajesh Duddu

The study, conducted by the ISB Institute of Data Science, aims to assess organisations' readiness, particularly within the financial sector, to address the emerging cybersecurity threats posed by the advancement of quantum computing.

Quantum computing has the potential to revolutionise various fields, but it also presents significant challenges to existing cybersecurity infrastructure. Current cryptographic algorithms, widely used to secure sensitive data, are vulnerable to attacks from sufficiently powerful quantum computers. This necessitates a transition to post-quantum cryptography (PQC), which employs algorithms resistant to these attacks.

This questionnaire seeks to understand views of some cyber experts on the current cybersecurity practices followed by financial institutions, their perceptions of quantum-related risks, their plans for transitioning to PQC, and their views on the role of government in fostering this transition.

Interview with Mr. Rajesh Dhuddu, Partner Emerging Tech, PwC

Interviewer: Dr. Shruti Mantri, Associate Director, ISB Institute of Data Science

Date of the Interview: February 12, 2024

When we talk about quantum computing, we often discuss its impact on cybersecurity. Specifically, are we saying that encryption and decryption will be compromised? Apart from this, what advantages do you see for quantum computing in the cybersecurity domain?

At this point, many people claim that cybersecurity will be compromised due to quantum computing. However, this is not yet proven; it is merely an anticipation. The most widely used encryption method today is asymmetric cryptography, commonly known as RSA cryptography. This method relies on a public key and a private key. The public key is used to transmit information, while the private key is used to read the transmitted information.

This encryption method is based on a mathematical concept called a trapdoor function, which involves prime numbers. Classical computers can verify the results of these functions but cannot easily determine the prime numbers used, due to the enormous number of possible combinations. The current computational power available is not sufficient to decipher which prime numbers were used in the encryption, making RSA cryptography secure.

To illustrate, let's take a simple example. Suppose I send you the number 16 and tell you that you can only verify my message if

you arrive at the same number. Now, 16 can be derived from multiple factor combinations: 4×4 , $2 \times 2 \times 2 \times 2$, 8×2 , etc. You can confirm that the output is 16, but you cannot determine which combination was actually used.

Quantum computing, on the other hand, is expected to perform multiple calculations simultaneously. This has led to speculation that quantum computers will be able to crack RSA encryption by identifying the prime factors quickly. However, based on my analysis, breaking RSA encryption would require a quantum computer with at least 5000 to 7000 qubits. We are nowhere near that capability today.

If we project the current development rate of quantum computing, RSA encryption is expected to remain secure until at least 2074—another 50 years. Of course, if an unforeseen breakthrough occurs, this timeline could change. Some believe quantum decryption could happen by 2070, 2050, or even 2040, which is why the industry is proactively preparing for potential risks.

Right now, we are in a speculative phase. It's like assuming India and Pakistan will face off in the World Cup final before they have even reached the semi-finals. Everyone is making predictions and discussing strategies when the actual qualifying rounds haven't even taken place. This is where we stand in the quantum computing debate today.

So now, in line with what you just mentioned—once quantum computing becomes a reality, and we reach around 5000 to 7000 qubits, though this is still far away—what do you think will be the primary risks associated with this development?

Well, what has been demonstrated now is how cryptographic keys can be distributed using quantum computers themselves. The emerging focus is on making encryption quantum-secure. Researchers are exploring ways to ensure cybersecurity keys remain protected, even against quantum computing threats. It has already been shown that once a key is encrypted using quantum computing, even another quantum computer will struggle to break it.

For every potential breach, there is also a solution, and that solution lies within quantum computing itself. A critical area of research is private key distribution using quantum computing. Numerous research articles discuss this, indicating that even after quantum computers become more advanced, securely distributed quantum-encrypted keys will remain unbreakable.

If we look at past cybersecurity developments, we see a similar pattern. For instance, the MD5 cryptographic standard was once widely used, but researchers at Google successfully demonstrated its vulnerability, leading to what is known as MD5 collision. If you search for MD5 collision or MD5 compromise, you'll find how it was broken. Since its compromise, no one relies on it anymore.

This is similar to using navigation on Google Maps. If a road is shown as flooded, would you take it? No, you would find an alternative route, even if it takes longer, because reaching safely is the priority. The same principle applies to cybersecurity: when one method is compromised, people adopt an alternative.

Currently, the strongest alternatives include RSA cryptography and ECC (Elliptic Curve Cryptography). These methods remain secure, and based on my research, both RSA and ECC cryptography will not be compromised for at least the next 30 to 40 years.

Now, when we talk about quantum computing, there is still time before financial institutions need to fully adapt to it. However, do you think that, starting today, financial institutions should consider a hybrid model when upgrading their systems? Should they prepare for quantum while still relying on classical methods?

Even before quantum computing becomes a reality, there are multiple cybersecurity advancements available today. For example, self-sovereign identity (SSI) is a blockchain-based protocol that enhances authentication. Another blockchain-driven protocol is password-less authentication, which utilises zero-knowledge proofs to verify identities securely.

A great example is Verizon ID, a password-less authentication system used in the United States. Cybersecurity breaches today are largely due to poor password hygiene rather

than failures in the underlying technology. Many users fail to secure their credentials properly, leading to account compromises. For instance, if someone's banking password is stolen and their account is hacked, it does not mean the bank's entire security system is compromised—it simply indicates poor password management by the user.

To address this, financial institutions can adopt password-less authentication, which operates efficiently on classical computers without requiring quantum computing. A strong real-world example of SSI is DigiYatra. Despite being used widely at airports and interacting with multiple stakeholders—CIS, airline staff, and third-party providers—it remains highly secure. This demonstrates the strength of decentralised identity systems.

It is not necessary for banks to immediately overhaul their systems for quantum computing. While research and innovation departments within banks may explore future-proofing technologies, immediate large-scale upgrades are not required. Instead, institutions can focus on self-sovereign identity, password-less authentication, and zero-knowledge proofs, which are already available and provide strong cybersecurity defence without needing quantum computing.

Though you have mentioned that the possibility of quantum computing becoming a significant threat is still 50-70 years away, what obstacles do you think financial institutions might

encounter when they start considering the adoption of post-quantum cryptographic solutions?

The primary obstacles include:

1. Lack of Awareness: Many organisations are not yet fully aware of the potential impact of quantum computing on cybersecurity.
2. Lack of Planning and Forecasting: Companies often fail to plan ahead for such long-term risks.

Consider this analogy—countries around the world invest heavily in nuclear defence despite the low probability of a nuclear attack, as seen post-World War II after Hiroshima and Nagasaki. Governments continue to allocate substantial budgets for nuclear preparedness because the risk, though small, has catastrophic potential.

Now, replace nuclear threats with quantum-based cyberattacks. The key question for financial institutions is: Are they at least considering quantum risks?

You don't need to over-invest and build an entire workforce dedicated to quantum cybersecurity today. However, you also cannot ignore it completely just because it may take decades to materialise. The best approach is a balanced risk mitigation strategy:

- Are organisations thinking about quantum threats?
- If so, what early measures can be taken?

- Should they start integrating post-quantum cryptographic solutions into their risk framework?
- Is there a contingency plan in place for potential threats?

That being said, many CISOs and CXOs are so occupied with daily operations that they rarely prioritise quantum-related risks. Often, they only engage with these topics when attending an ISB program or an industry event, but once the event is over, the urgency fades, and they return to their routine responsibilities without concrete follow-ups.

Even though the industry knows that we are still far from fully realising quantum computing, there is a lot of hype surrounding it. Governments are investing heavily in quantum research, computing, and communication. Why do you think there is so much hype? Is it because major companies like Google, Microsoft, and IBM are investing in quantum for cloud technology, or is there another reason?

The hype is not just because of cloud technology or corporate investments. Companies are investing in quantum computing because it represents the future. Take Elon Musk, for example—he continues to invest in SpaceX, even though space tourism is not yet mainstream. Someone has to take a futuristic approach and invest in long-term technological advancements.

This is similar to what happened when computers were not yet mainstream. IBM, which stands for International Business Machines, invested in business computing because they foresaw its eventual importance. Companies like Apple, Microsoft, and IBM spent significant amounts on research and development long before personal computers became widespread. Initially, perhaps one in 10,000 people had access to such technology, whereas today, nearly one in ten people own a computer or a smart device.

These investments are about taking a forward-looking perspective, guiding industries toward a future state where quantum computing becomes an integral part of technology. That is why companies and governments are making these substantial investments today.

When do you think will be the right time for organisations to start integrating certain quantum measures or PQC into their existing systems? As you mentioned, we still have other effective measures in place, like password-less authentication and blockchain-based zero-knowledge proofs. However, considering the long timeline you mentioned, when do you think, organisations should start preparing?

In some areas, companies are already making significant financial investments. For example, airlines implementing the hub-and-spoke model, like Indigo or Air India, need to

optimise flight allocations efficiently. When expanding into Tier 3 and Tier 4 cities, airlines must carefully decide where to station planes overnight. Indigo, for instance, prefers flying 200 kilometres to a regional airport with lower parking fees rather than paying higher fees in major airports like Hyderabad, Mumbai, or Delhi. The complex calculations involved in optimising such operations could benefit from quantum computing.

Similarly, financial institutions engaged in asset allocation and wealth management can leverage quantum computing. Companies like D.E. Shaw use advanced quantitative finance techniques to identify arbitrage opportunities—buying a stock at a lower price in one country and selling it at a higher price in another. These processes require enormous computing power and sophisticated algorithms, making them ideal candidates for early quantum adoption.

Drug discovery is another area where quantum computing can be transformative. Typically, it takes years to develop and test new drugs, ensuring minimal risk to human life. During the COVID-19 pandemic, however, decisions had to be made under unprecedented urgency. Authorities had to weigh the risk of losing thousands of lives against the greater threat of the pandemic itself. While classical computers helped accelerate vaccine development, quantum computing could further enhance precision in such life-critical scenarios.

In summary, industries with high computational demands—such as airlines optimising routes, financial firms managing global investments, and pharmaceutical companies conducting complex drug research—should be the first to explore

quantum computing. While widespread adoption may still be decades away, strategic investments in quantum research and preparation should begin now in these sectors.

For banks, financial institutions, asset management firms, and data centres, transaction security is crucial. Retail companies also handle sensitive data. Since there are various security alternatives available, such as post-quantum cryptography (PQC) and quantum key distribution (QKD), do you think the right approach is to first identify what data could be compromised? Should organisations assess the importance and lifespan of their data before deciding on a security solution, rather than immediately transitioning to quantum computing or PQC?

Yes, a mass movement to quantum computing is not a practical solution at this stage due to the high cost of quantum computers. From an India-specific perspective, we do not yet have a sovereign quantum computer. Without a sovereign quantum infrastructure, mission-critical data—such as defence and security information—cannot be transferred to quantum systems. There is no clear understanding of how the data would be processed or integrated into other systems, which presents significant security risks.

In such scenarios, organisations must ensure the highest level of security for sensitive data transfers. This is where quantum routers come

into play. Today, a \$40 packet sniffer from eBay can be used to tap into fibre-optic networks and intercept data packets. Cybercriminals exploit this method to gather sensitive information.

Companies like Nu Labs and others are addressing this issue by developing highly secure solutions. If the information pertains to sovereign security or homeland security, quantum networks are essential. In highly sensitive areas—such as military communications across borders—data interception is a real threat. This is why the military is actively involved in developing and deploying quantum-secure communication networks to protect classified transmissions.





Appendix A2
Expert Interview:
Col. Kapil Jaiswal
(Retired)

*** * * * ***

Name of the Company: Quantum AI Global

Affiliation of the Person Interviewed: Col. Kapil Jaiswal, Quantum AI Global, CTO

Details about the Company: Quantum AI Global is at the forefront of the quantum revolution, merging quantum technology with AI innovation to solve complex challenges and transform industries. The company specialises in Quantum Technology, Quantum AI Integration, and Post-Quantum Cryptography. For more information, visit <https://thequantum.ai/>.

Interviewer: Dr. Shruti Mantri

Date of the Interview: December 17, 2024

Section 1: Organisation Profile and Firmographics

Describe your organisation's primary business focus and its specific role within the cybersecurity landscape.

At Quantum AI Global, we lead the quantum revolution by merging quantum technology with AI innovation. Our mission is to solve complex challenges and transform industries. We are currently a deep-tech startup focusing on three key areas: Quantum Technology, Quantum AI Integration, and Post-Quantum Cryptography. These are the primary business areas where we are directing our efforts.

Our focus translates into three key products within the cybersecurity domain

1. QSleeve
- Core product that enables seamless integration of Post-Quantum Cryptography (PQC) into existing networks.
 - Ensures all communications are quantum-secure by overlaying them with a quantum encryption layer.
 - Provides quantum-enhanced Virtual Private Network (VPN) capabilities with secure key exchange mechanisms.
 - Simplifies network and client management while ensuring easy integration and adherence to industry standards.
 - It is highly customisable to meet user-specific requirements, providing advanced protection against quantum threats.

2. ChecQ
- A comprehensive tool for auditing and maintaining PQC readiness in existing systems.
 - Detects cryptographic vulnerabilities in websites and software, proactively addressing quantum computing threats.
 - Assesses hardware and software for vulnerabilities and ensures compatibility with quantum-secure standards.
 - Monitors encrypted sessions and data flow to maintain optimal performance and identify potential issues post-migration.
3. Quantum Random Number Generator (QRNG)
- Overcomes traditional pseudo-random number generators' limitations by generating truly random numbers using quantum phenomena.
 - Ensures the highest level of encryption security for sensitive data transmissions.
 - Provides centralised, scalable quantum key management, reducing hardware dependency while enhancing security.

These tools position us as pioneers in quantum-driven cybersecurity solutions and in ensuring that our clients are equipped to face emerging quantum-era challenges.

What are the main regions that your organisation currently operates out of?

We are a company registered in India, with offices in the US (New Jersey) and Dubai. While we have a global presence in these three regions, we are primarily an Indian company. Our aim is to develop technology in India,

under the Atmanirbhar Bharat (Made in India) initiative and then expand globally as an Indian technology provider.

Section 2: Cybersecurity Threat Perception (Post-Quantum Cryptography)

What cybersecurity threats do you foresee arising from the commercial availability of post-quantum cryptography (PQC) to digital users?

The cybersecurity threats that will arise stem from the computing capacities capable of breaking current key exchange mechanisms. This will primarily impact banking, finance, and the security of web sessions. Web browsing will become vulnerable as someone could intercept and monitor user activities.

Email security and secure transactions, which rely on encryption, will also be under threat. Applications like WhatsApp, which currently provide end-to-end encryption, could be compromised in the future. Additionally, data stored on platforms like Google Cloud—which typically update encryption keys annually—will become susceptible to breaches.

In the long run, businesses and individuals may lose confidence in cloud storage and start moving critical data to offline storage, such as hard drives disconnected from networks, to ensure its security.

Does your organisation develop: (a) both software and hardware for quantum/post-quantum computing; (b) only software; (c) only hardware?

We work on both hardware and software. For quantum cryptography infrastructure, we focus on building user interfaces and enterprise solutions, particularly in post-quantum cryptography. However, for strategic areas like defence systems, financial institutions, and critical power infrastructure—where security is of national importance—we provide hardware solutions for quantum cryptography.

Could you describe the implementation of the QSleeve Tool, and the cryptographic algorithms embedded into it?

Currently, we are working on NIST-approved cryptographic algorithms. NIST has introduced three cryptographic algorithms, and we have included all three in our QSleeve Tool. They are:

- ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism): This is used for key exchange and encapsulation.
- ML-DSA (Module-Lattice Digital Signature Algorithm): A digital signature algorithm.
- SLD-DSA (Stateless Digital Signature Algorithm): A hashless digital signature standard.

So how do you rate the performance of your tool 'QSleeve' in comparison with non-cryptography encryption decryption?

We have conducted simulations to assess the impact of post-quantum cryptographic protocols. One challenge is the increased key length and digital signature sizes in PQC. While there are no widely published comparative studies due to the differing scenarios, we have made some observations. One is that when comparing the same key length (e.g., RSA 2048 vs. ML-KEM), ML-KEM performs faster. However, because PQC algorithms require larger key sizes, ML-KEM is slightly slower overall. This introduces some overhead, but for regular user traffic—where key exchange constitutes only 5-7% of the data—the impact is negligible.

However, for financial institutions and banking sectors, where key exchange and authentication are central to transactions, there will be a noticeable impact.

How well does your product prepare organisations, particularly in the financial sector, to respond to cybersecurity incidents in a post-quantum world?

Our product is currently targeted primarily towards the fintech and banking sectors. Initially, we are focusing on fintech companies, as they are more agile and open to adopting solutions from startups. Banks, being highly regulated, take longer to integrate such technologies. Our solution is designed specifically to help fintech and banking organisations prepare for post-quantum cybersecurity challenges.

Section 3: Quantum Computing Threat Perception

Has your organisation participated in discussions or briefings regarding the implications of quantum computing for cybersecurity?

Yes, I am an ex-government official and have previously served as Director of Research, InfoSec. My core research area involved estimating the impact of quantum threats and aligning them with the expected development timelines for quantum computing.

As an organisation, we have a clear understanding of where we currently stand and the potential timelines for quantum computing threats. However, we must also prepare for unforeseen developments, such as the discovery of a new algorithm capable of breaking existing systems. Given the threat perception, it is better to be proactive and ready for any "Black Swan" event.

On a scale of 1-5(1=not at all concerned, 5=extremely concerned), how concerned are you about cyber threats associated with quantum computing?

I would rate it 3-4

On a Scale of 1-5(1=minimal impact, 5=catastrophic impact), how significant would the effect be on industry/government if sensitive information were stolen and later decrypted using quantum computing?

The impact would be tremendous. Today, if someone compromises a user, it often happens through phishing emails where the digital certificate is flagged as invalid, stopping the user from proceeding. However, with quantum computers, digital certificates can be duplicated.

In this scenario, if a malicious link is clicked, the browser will validate the digital certificate, and a fake web page will appear legitimate. Users will have no way of identifying whether it is a genuine or malicious site. This would threaten the entire interface of the Internet, which depends on current cryptographic technologies for security and verification.

Section 4: Quantum-Guided Business Model Readiness

As per you, what is the estimated timeline for the migration of an organisation and critical infrastructure (e.g., Banking Systems) to post-quantum cryptography? What are the main challenges or roadblocks you anticipate?

For small organisations, the migration timeline is approximately 3 months. Larger organisations with more complex infrastructures will require 6-9 months. Financial institutions, due to their scale, regulatory requirements, and critical nature, may require several years for complete migration.



Section 5: Challenges and Policy Recommendations

What role should the government play in accelerating the standardisation and adoption of post-quantum cryptography algorithms?

The government has two key roles to play. Governments like the US have already provided timelines for when critical sectors (e.g., financial institutions, and government bodies) need to shift to PQC standards. Similarly, our government should analyse the threat perception, engage with academia and industry, and define a timeline for adoption.

Encryption is not just a technical tool; in the long run, it is a matter of national power projection. Currently, we rely heavily on foreign standards. As a country of 1.4 billion people, we must start developing our own post-quantum cryptography standards.

This requires creating a system similar to NIST, where a transparent process allows researchers and industry experts to propose, test, and validate cryptographic standards. We must foster a community that continually revisits and updates these standards year after year to ensure they remain robust and reliable.

What specific actions could the government take to improve cyber security awareness and education regarding quantum computing threats?

Cybersecurity policy groups currently exist at a conventional level, but there is no dedicated effort for post-quantum cryptography (PQC). It would be beneficial for the Ministry of Electronics and IT (MeitY), the Ministry of Communications, or the Department of Science and Technology (DST) to take the lead and establish a dedicated central body for PQC. This central body should bring together the academia, industry, and government to create a joint working group. This group would focus on research, education, and policy discussions specific to quantum computing and PQC threats. Initiating awareness programs, workshops, and training sessions at national and institutional levels will help improve understanding of quantum computing threats and the urgency of transitioning to PQC standards.

What incentives or funding mechanisms would encourage startups and institutions to prioritise and invest in post-quantum cryptography?

For the banking sector, direct incentives are challenging due to their highly regulated nature. Instead, regulatory directions, similar to those in the US, could encourage adoption.

For startups and institutions, there is significant potential for further research and development (R&D) in this area. While we have developed our initial set of products, there remains a lot of scope to refine these solutions and explore deeper tech opportunities. The government can play a critical role here by:

- I. Funding R&D Initiatives: The government should provide grants or funding mechanisms to support deep-tech research. For example, initiatives like the challenge launched by the Department of Science and Technology (DST) last year are a good step. We had submitted our application, but progress on that front has been slow. Timely and well-funded challenges would help startups accelerate product development.
- II. Promoting Business Opportunities: India has a chance to become a powerhouse in post-quantum cryptography. The market opportunity is vast, as solutions must be tailored to different organisations and industries—one-size-fits-all approach will not work. By supporting multiple companies now, the government can prepare Indian startups to lead this emerging market when global demand surges.

What adjustments to existing regulations or frameworks would best facilitate a secure transition to post-quantum cryptography?

Currently, India lacks dedicated cryptography regulations. While some frameworks exist, such as Department of Telecommunications (DoT) regulations for telecom networks, these are limited in scope.

To ensure a smooth and secure transition to post-quantum cryptography, we need:

1. A Dedicated Indian Cryptography Act: Similar to the IT Act or other sector-specific regulations, India should establish comprehensive crypto regulations. A dedicated framework would define standards, compliance requirements, and security protocols for the adoption of post-quantum cryptography across industries.
2. Cross-Sectoral Guidelines: Regulations must apply across sectors, including finance, telecommunications, critical infrastructure, and government systems, ensuring a unified and secure adoption process.
3. Collaboration with Industry and Academia: Regulatory frameworks should be developed in consultation with industry experts, startups, and academia to address practical implementation challenges and foster innovation.

Having strong regulations in place will not only secure critical infrastructure but also position India as a leader in post-quantum cryptography standards globally.



Appendix A3
Expert Interview:
Col. Sai Shankar
(Retired)

Interview with Col. Sai Shankar, Founder, QClairvoyance Quantum Labs Pvt. Ltd.

Name of the Company: QClairvoyance Quantum Labs Pvt. Ltd.

Affiliation of the Person Interviewed: Col. Sai Shankar

Details about the Company: QClairvoyance Quantum Labs Pvt. Ltd. is a deep-tech startup working on developing next-generation applications that leverage post-Moore computing architectures, specifically in the form of quantum computing hardware.

Interviewer: Mrs. Renu Chaturvedi

Date of the Interview: 16th December 2024

Section I: Organisation Profile and Firmographics

Describe your organisation's primary business focus and its specific role within the cybersecurity landscape.

Our organisation's primary focus is on developing applications based on quantum technologies. From a cybersecurity perspective, we are particularly concerned with the imminent reality of quantum computers. Once quantum computing becomes fully operational, all existing encryption protocols, especially public asymmetric encryption, will be vulnerable. Our mission is to safeguard against this threat. By implementing our applications, organisations can ensure that their systems remain secure in the age of quantum computing. This is the core of our work.

What are the main regions your organisation currently operates out of?

Our main operational base is currently in Secunderabad. While we are exploring the possibility of establishing subsidiaries in the United States, the Netherlands, and Germany, these discussions are still at a very preliminary stage. As a relatively new organisation, having started just three months ago, these expansions are part of our long-term vision rather than immediate plans. For at least the next year, our focus will remain firmly on Secunderabad as our primary location.

Section II: Cybersecurity Threat Perception (Post-Quantum Cryptography)

What cybersecurity threats do you foresee arising from the commercial availability of post-quantum cryptography (PQC) to digital users?

The commercial availability of post-quantum cryptography (PQC) to digital users introduces several cybersecurity threats. While the mathematical foundations of PQC are robust and difficult to break, the primary vulnerabilities lie in implementation. Users cannot rely on simply downloading libraries from open-source platforms without validation. These libraries must be rigorously assessed to ensure they are free from flaws or backdoors, as errors in implementation can compromise security.

At all levels—national, organisational, or individual—it is critical to establish strict checks and balances before deploying PQC tools. Without these precautions, the adoption of PQC could inadvertently introduce significant risks, undermining its intended purpose of safeguarding against quantum-era cyber threats.

Does your organisation develop: (a) both software and hardware for quantum/post-quantum computing; (b) only software; (c) only hardware.

Our organisation focuses solely on software development. To clarify, there is no such term as "post-quantum computing"; the correct term is "post-quantum cryptography" (PQC). Quantum computing and PQC are distinct fields.

In PQC, we work exclusively on software and are not involved in hardware development. Quantum secure communication, which encompasses PQC and quantum key distribution (QKD), highlights their differences. PQC, based purely on mathematics, requires only software updates, making it highly scalable without hardware upgrades.

In contrast, QKD, grounded in quantum physics, depends on specialised hardware and media, which limits scalability. Each has specific applications, but our focus remains on PQC due to its seamless integration into existing systems through software alone.

Which specific post-quantum cryptographic algorithms, are you focusing on, and why? (Specify algorithm types: lattice-based, code-based, multivariate, hash-based, isogeny-based, etc. Explain your selection criteria and any trade-offs considered.)

We are focusing on Kyber for key exchange and Dilithium for digital signatures, both recommended by NIST. These algorithms are well-tested and reliable.

Instead of directly using pre-existing libraries, we develop custom libraries to ensure better security and adaptability. Kyber and Dilithium are applied across all applications,

including VPNs, messengers, and other secure communication tools.

Additionally, we are working on an India-specific cryptographic suite to address the absence of a national standard. This suite integrates encryption algorithms developed by Indian universities, key exchange protocols and quantum random number generators from reputed Indian entities.

Our strategy combines the proven security of the NIST standards with indigenous algorithms, allowing time for rigorous testing and validation. Over the next few years, if the India-specific suite proves secure, it could evolve into a national standard. In the meantime, the foundational NIST algorithms ensure robust security. This approach balances innovation with reliability.

Describe your implementation of PQC tools/algorithms/ software. Detail its performance characteristics (speed, memory usage, latency, resource requirements), and security features. How does it compare to pre-quantum algorithms?

Our implementation of post-quantum cryptographic (PQC) tools is in progress, and we have yet to establish benchmarks against pre-quantum algorithms. Once fully implemented, we will assess key performance parameters such as latency, speed, memory usage, and resource requirements.

Globally, several companies have already tested PQC algorithms as part of compliance

with initiatives like the US mandate to upgrade systems by 2035. Early implementations suggest that while latency issues are unlikely to be significant, the primary challenges lie in ensuring robust cybersecurity. The effectiveness of PQC tools depends heavily on the proper implementation of libraries.

As we proceed with our development, our focus remains on ensuring secure and efficient execution, aligning with global standards, and addressing any vulnerabilities that may arise during implementation.

How does your product address post-quantum key management challenges?

By implementing post quantum cryptography we are addressing the key address, key management challenge. In a traditional encryption, Public Key Infrastructure (PKI) is used for key transfer, while symmetric encryption is employed for bulk encryption. We address post-quantum challenges by replacing PKI with post-quantum cryptography, specifically lattice-based cryptography, for key transfer. Symmetric encryption remains secure against quantum attacks, as no algorithms currently exist to break it.

The threat posed by quantum computers is their ability to break asymmetric encryption. Once asymmetric encryption is compromised, the symmetric key is exposed. However, instead of breaking symmetric encryption directly, quantum computers would simply unlock it through the weakened asymmetric key. Therefore, our focus is on upgrading

asymmetric encryption to post-quantum standards, while symmetric encryption remains intact.

Which security measures best describe your organisation's developed hardware or software?

We follow the software development life cycle (SDLC) and adhere to established standards. In addition, we implement a concept known as DevSecOps, which integrates security into the entire development process. Unlike traditional DevOps, which focuses primarily on development and operations, DevSecOps ensures that cybersecurity is considered from the very beginning of the product lifecycle.

As a cybersecurity company, we recognise the importance of incorporating security measures right from the development stage. This includes utilising practices such as SSL pinning, rate limiters, and other relevant security protocols and best practices. We also rely on open-source software, and within that context, we ensure security is embedded in the development pipeline, minimising vulnerabilities before they arise.

Could you share the product details and the description of its working model so that we can include them in the study?

Currently, I can provide details for two products: the Quantum Secure Wrapper and Quantum Secure VPN.

In essence, our Quantum Secure VPN is very similar to traditional VPNs, with one key distinction—it is quantum-safe. To achieve this, we have upgraded the key exchange protocol from PKI to post-quantum cryptography (PQC). Additionally, for random number generation, we use quantum random number generators (QRNGs), which enhance security against quantum computing threats.

This same cryptographic suite is applied to our other products as well.

Does your organisation utilise any third-party infrastructure (e.g., cloud services) in its development process?

Yes, we do utilise third-party infrastructure. However, our applications are designed to be flexible and can operate in three scenarios: cloud-based, on-premises, and air-gapped (standalone) environments. The standalone, air-gapped setup is particularly important because it ensures that we are not dependent on any third-party libraries, providing a higher level of security and control.

How well does your product prepare organisations, particularly in the financial sector, to respond to cybersecurity incidents in a post-quantum world?

By implementing post-quantum cryptographic suites, we are confident that the financial sector will be safeguarded from potential quantum computing threats. Our approach aims to ensure comprehensive protection across the sector. Additionally, we plan to introduce an ethical hacking competition, accompanied by a bug bounty program worth 5 to 10 lakh rupees. We believe that post-quantum cryptography itself will remain secure, but the real risk lies in how it is implemented. This competition will help identify potential vulnerabilities, which we will address through ongoing patches, creating a continuous improvement cycle for our product's security.

Section III: Quantum Computing Threat Perception

Has your organisation participated in discussions or briefings regarding the implications of quantum computing for cybersecurity?

Yes, we are actively part of several online forums where we closely monitor discussions on quantum computing's implications for cybersecurity. While we may not yet have the expertise to contribute directly, our team includes highly qualified mathematicians with PhDs in post-quantum cryptography from prestigious institutions like IIT Kharagpur. We are confident that our approach is on the right path, adhering to global standards followed worldwide.

On a scale of 1-5 (1=not at all concerned, 5=extremely concerned), how concerned are you about cyber threats associated with quantum computing?

I would rate it as a 4. The reason for this is that while there are papers discussing the potential risks, no one has yet broken any algorithms. However, about a month ago, China published a paper claiming they could break certain aspects of encryption. While we should take such claims with caution, if we consider even 50% of their findings to be accurate, it suggests that the threat is real and imminent. Hence, my concern is significant, but not at the highest level.

What specific quantum-related threats are you aware of? What steps is your organisation taking to prepare for them?

There are well-established papers that indicate once quantum computers become a reality, all asymmetric encryption methods, such as PKI and elliptic curve cryptography, will be vulnerable and could be broken in a matter of days. Our organisation is focusing specifically on this issue. To address it, we are implementing post-quantum cryptography to ensure that online communication remains secure, even in a world where quantum computers are operational.

On a scale of 1-5 (1=minimal impact, 5=catastrophic impact), how significant would the effect be on industry/government if sensitive information were stolen and later decrypted using quantum computing?

It would be catastrophic. Consider this: critical organisations such as DRDO or those in the nuclear sector have secure networks, but a vast amount of sensitive information flows over the internet. For example, if I am collaborating with a foreign university on building a nuclear reactor, even before the information becomes confidential, significant data is exchanged. Hackers could decrypt this data at a later stage. In the banking sector, while transaction information can be vulnerable to brute force attacks, much of the sensitive customer information is stored in log files. If quantum computing becomes a reality, this

information would be at risk and cyberattacks could increase. Specifically, ransomware and data breaches would become more prevalent. If sensitive data isn't stored securely with symmetric encryption, it would be exposed.

Section IV: Quantum-Guided Business Model Readiness

What is your estimated timeline for the migration of an organisation and critical infrastructure (e.g., banking systems) to post-quantum cryptography? What are the main challenges or roadblocks you anticipate?

First, let me address the roadblocks. One of the major challenges is the education and awareness of systems. Leaders must fully understand quantum computing and the threats it poses. Without this knowledge, they may not take the necessary steps to mitigate the risks. Awareness programs are crucial, and they should be designed in a way that even non-technical individuals can comprehend the potential threats and the need to address them.

The first step is to educate and inform, and this awareness must be widespread across all levels of an organisation. As for the timeline, it will depend on how quickly these educational efforts are made and how soon the necessary technologies can be deployed to support a migration to post-quantum cryptography. To be specific companies should start now. It is not so easy to upgrade crypto suites as it takes time, therefore sooner the better.

Section VI: Challenges and Policy Recommendations

What role should governments play in accelerating the standardisation and adoption of post-quantum cryptography algorithms?

Firstly, the governments need to introduce policy guidelines on PQC as soon as possible. These guidelines should be robust and comprehensive, offering a clear framework for its implementation. Following that, governments should consider enacting legislation on similar lines to other countries to ensure its widespread adoption.

Critical area where governments can help, because of their wide reach; is increasing awareness. Awareness should not only target technical experts but also non-technical individuals, particularly leaders and decision-makers at all levels. Awareness programs should aim to reach decision-makers at every level, from senior executives to mid-level and lower-level staff. The key is ensuring that everyone in the organisation recognises the importance of transitioning to PQC for it to be effective. Only when this mindset is shared across the entire workforce will meaningful progress be made.

What specific actions could governments take to improve cybersecurity awareness and education regarding quantum computing threats?

To enhance cybersecurity awareness and education regarding quantum computing threats, I believe governments should initiate a state-level framework similar to national initiatives. While the National Quantum Mission is a good starting point, it is essential for each state to have its own focused approach. In addition to the national program, state-level initiatives should be introduced to address local needs and engage regional expertise.

Given India’s vast pool of energy and knowledge, one national initiative alone is not enough. There should be more widespread participation across various states, ensuring that universities, research institutions, and other stakeholders are actively involved. This state-level approach would foster more localised efforts to tackle the quantum computing threat and improve overall cybersecurity education.

Other initiatives could be running awareness programs at various levels, introducing Quantum Technologies as subjects/degrees at UG, PG levels in various universities. It should also be made part of the AICTE curriculum.

What incentives or funding mechanisms would encourage startups and institutions to prioritise and invest in post-quantum cryptography?

To encourage startups and institutions to invest in post-quantum cryptography (PQC), the government could implement incentives similar to those used in other sectors, like electric vehicles (EVs). For instance, providing

subsidies or offering advantages like tax benefits in government tenders for those implementing PQC could be effective.

One example could be the Reserve Bank of India (RBI) recognising PQC implementation in its guidelines and offering rewards or preferences to organisations that adopt these technologies. In the finance sector, similar mechanisms could be explored.

The key is a balanced approach — offering both incentives (the "carrot") and regulatory requirements (the "stick"). Without such mechanisms, adoption would be slow, as organisations are unlikely to prioritise PQC unless there are tangible benefits.

What adjustments to existing regulations or frameworks would best facilitate a secure transition to post-quantum cryptography?

Awareness, inventory management, incentives, regulations. Give guidelines and ensure they are followed like the IBRT Act.

How can governments foster better collaboration and information sharing between financial institutions and cybersecurity experts on quantum threats?

Last three questions are inter-related, answers given for those are equally applicable for this question also. I would like to mention one more point that institutions like UGC should, at an academic level, introduce quantum computing and quantum cryptography at the university level to create awareness.

Appendix B

Pseudo Code for ML-KEM.KeyGen Algorithm

Generates an encapsulation key and a corresponding decapsulation key.

Output: encapsulation key $ek \in \mathbb{B}^{384k+32}$

Output: decapsulation key $dk \in \mathbb{B}^{768k+96}$

Step 1: $d \xleftarrow{\$} \mathbb{B}^{32}$ ▷ Where d is 32 random by

Step 2: $z \xleftarrow{\$} \mathbb{B}^{32}$ ▷ Where z is 32 random bytes

Step 3: if $d == \text{NULL}$ or $z == \text{NULL}$ then

Step 4: return $\perp$ ▷ Where return an error indication if random bit generation failed

Step 5: end if

Step 6: $(ek, dk) \leftarrow \text{ML-KEM.KeyGen_internal}(d, z)$ ▷ run internal key generation algorithm

Step 7: return (ek, dk)

ML-KEM Encapsulation

The encapsulation algorithm **ML-KEM.Encaps** of **ML-KEM** accepts an encapsulation key as input, generates randomness internally, and outputs a ciphertext and a shared key.

Pseudo Code for **ML-KEM.Encaps** Algorithm

Uses the encapsulation key to generate a shared secret key and an associated ciphertext.

Checked input:

encapsulation key $ek \in \mathbb{B}^{384k+32}$

Output: shared secret key $K \in \mathbb{B}^{32}$

Output: ciphertext $c \in \mathbb{B}^{32(d_u k + d_v)}$

Step 1: $m \xleftarrow{\$} \mathbb{B}^{32}$

Step 2: if $m == \text{NULL}$ then

▷ m is 32 random bytes

Step 3: return $\perp$ ▷ return an error indication if random bit generation failed

Step 4: end if

Step 5: $(K, c) \leftarrow \text{ML-KEM.Encaps_internal}(ek, m)$
▷ run internal encapsulation algorithm

Step 6: return (K, c)

The algorithm **ML-KEM.Encaps_internal** accepts an encapsulation key and a random byte array as input and outputs a ciphertext and a shared key.

Pseudo Code for **ML-KEM.Encaps_internal** Algorithm

Uses the encapsulation key and randomness to generate a key and an associated ciphertext.

Input: encapsulation key $ek \in \mathbb{B}^{384k+32}$

Input: randomness $m \in \mathbb{B}^{32}$

Output: shared secret key $K \in \mathbb{B}^{32}$

Output: ciphertext $c \in \mathbb{B}^{32(d_u k + d_v)}$

Step 1: $(K, r) \leftarrow G(\text{mlH}(ek))$

▷ derive shared secret key K and randomness r

Step 2: $c \leftarrow \text{K-PKE.Encrypt}(ek, m, r)$

▷ encrypt m using **K-PKE** with randomness r

Step 3: return (K, c)

K-PKE Encryption

The encryption algorithm **K-PKE.Encrypt** of **K-PKE** takes an encryption key ek_{PKE} , a 32-byte plaintext m , and randomness r as input and produces a single output: a ciphertext c .

Pseudo Code for **K-PKE.Encrypt** Algorithm

Uses the encryption key to encrypt a plaintext message using the randomness r .

Input: encryption key $ek_{\text{PKE}} \in \mathbb{B}^{384k+32}$

Input: message $m \in \mathbb{B}^{32}$

Input: randomness $r \in \mathbb{B}^{32}$

Output: ciphertext $c \in \mathbb{B}^{32(d_u k + d_v)}$

Step 1: $N \leftarrow 0$

Step 2: $\hat{t} \leftarrow \text{ByteDecode}_{12}(ek_{\text{PKE}}[0 : 384k])$

▷ run ByteDecode_{12} k times to decode $\hat{t} \in \mathbb{Z}_q^{256})^k$

Step 3: $\rho \leftarrow ek_{\text{PKE}}[384k : 384k + 32]$

▷ extract 32-byte seed from ek_{PKE}

Step 4: for $(i \leftarrow 0, i < k, i++)$

▷ re-generate matrix $\hat{A} \in (\mathbb{Z}_q^{256})^{k * k}$

Step 5: for $(j \leftarrow 0, j < k, j++)$

Step 6: $\hat{A}[i, j] \leftarrow \text{SampleNTT}(\rho[j]i)$ j and i are bytes 33 and 34 of the input

Step 7: end for

Step 8: end for

Step 9: for $(i \leftarrow 0; i < k; i++)$

▷ generate $\mathbf{y} \in (\mathbb{Z}_q^{256})^k$

Step 10: $\mathbf{y}[i] \leftarrow \text{SamplePolyCBD}_{\eta_1}(\text{PRF}_{\eta_1}(r, N))$ ▷ $\mathbf{y}[i] \in (\mathbb{Z}_q^{256})$ sampled from CBD

Step 11: $N \leftarrow N + 1$

Step 12: end for

Step 13: for $(i \leftarrow 0; i < k; i++)$

▷ generate $\mathbf{e}_1 \in (\mathbb{Z}_q^{256})^k$

Step 14: $e_1[i] \leftarrow \text{SamplePolyCBD}_{\eta_2}(\text{PRF}_{\eta_2}(r, N))$ ▷ $e_1[i] \in \mathbb{Z}_q^{256}$ sampled from CBD

Step 15: $N \leftarrow N + 1$

Step 16: end for

Step 17: $e_2 \leftarrow \text{SamplePolyCBD}_{\eta_2}(\text{PRF}_{\eta_2}(r, N))$

▷ sample $e_2 \in (\mathbb{Z}_q^{256})^k$ from CBD

Step 18: $\mathbf{\bar{y}} \leftarrow \text{NTT}(\mathbf{y})$ ▷ run NTT k times

Step 19: $\mathbf{u} \leftarrow \text{NTT}^{-1}(\hat{A}^T \circ \mathbf{\bar{y}}) + e_1$

▷ run NTT⁻¹ k times

Step 20: $\mu \leftarrow \text{Decompress}_1(\text{ByteDecode}_1(m))$

Step 21: $v \leftarrow \text{NTT}^{-1}(\hat{A}^T \circ \mathbf{\bar{y}}) + e_2 + \mu$

Step 22: $c_1 \leftarrow \text{ByteEncode}_{du}(\text{Compress}_{du}(\mathbf{u}))$
▷ run ByteEncode_{du} and compress_{du} k times

Step 23: $c_2 \leftarrow \text{ByteEncode}_{du}(\text{Compress}_{du}(v$

Step 24: return $c \leftarrow (c_1 || c_2)$

K-PKE Decryption

The decryption algorithm **K-PKE.Decrypt** of **K-PKE** takes a decryption key dk_{PKE} and a ciphertext c as input, requires no randomness, and outputs a plaintext m .

Pseudo Code of **K-PKE.Decrypt**

Uses the decryption key to decrypt a ciphertext.

Input: decryption key $dk_{\text{PKE}} \in \mathbb{B}^{384k}$

Input: ciphertext $c \in \mathbb{B}^{32(d_u k + d_v)}$

Output: message $m \in \mathbb{B}^{32}$

Step 1: $c_1 \leftarrow c[0 : 32d_u k]$

Step 2: $c_2 \leftarrow c[32d_u k : 32(d_u k + d_v)]$

Step 3: $\mathbf{u}' \leftarrow \text{Decompress}_{d_u}(\text{ByteDecode}_{d_u}(c_1))$
▷ run Decompress_{d_u} and ByteDecode_{d_u} k times

Step 4: $v' \leftarrow \text{Decompress}_{d_v}(\text{ByteDecode}_{d_v}(c_2))$

Step 5: $\hat{s} \leftarrow \text{ByteDecode}_{12}(dk_{\text{PKE}})$
▷ run ByteDecode_{12} k times

Step 6: $w \leftarrow v' - \text{NTT}^{-1}(\hat{s}^T \circ \text{NTT}(\mathbf{u}'))$
▷ run NTT k times; run NTT⁻¹ once

Step 7: $m \leftarrow \text{ByteEncode}_1(\text{Compress}_1(w))$
▷ decode plaintext m from polynomial v

Step 8: return m

ML-KEM.Decaps_internal

The algorithm **ML-KEM.Decaps_internal** accepts a decapsulation key and a cipher-text as input, does not use any randomness, and outputs a shared secret key.

Pseudo Code of ML-KEM.Decaps_internal

Uses the decapsulation key to produce a shared secret key from a ciphertext.

Input: decapsulation key $dk \in \mathbb{B}^{768k+96}$

Input: ciphertext $c \in \mathbb{B}^{32(d_u k+d_v)}$

Output: shared secret key $K \in \mathbb{B}^{32}$

Step 1: $dk_{PKE} \leftarrow dk[0 : 384k]$
▷ extract (from **KEM decaps** key) the **PKE decryption** key

Step 2: $ek_{PKE} \leftarrow dk[384k : 768k+32]$
▷ extract **PKE encryption** key

Step 3: $h \leftarrow dk[768k+32 : 768k+64]$
▷ extract hash of **PKE encryption** key

Step 4: $z \leftarrow dk[768k+64 : 768k+96]$
▷ extract implicit rejection value

Step 5: $m' \leftarrow \text{K-PKE.Decrypt}(dk_{PKE}, c)$
▷ decrypt ciphertext

Step 6: $(K', r') \leftarrow G(m' || h)$

Step 7: $K \leftarrow J(Z || c)$

Step 8: $c' \leftarrow \text{K-PKE.Encrypt}(ek_{PKE}, m', r')$
▷ re-encrypt using the derived randomness r'

Step 9: if $c \neq c'$ then

Step 10: $K' \leftarrow \emptyset$
▷ if ciphertexts do not match, “implicitly reject”

Step 11: end if

Step 12: return K'

ML-KEM.Decaps

The decapsulation algorithm **ML-KEM.Decaps** of **ML-KEM** accepts a decapsulation

key and an **ML-KEM** ciphertext as input, does not use any randomness, and outputs a shared secret.

Pseudo Code of ML-KEM.Decaps

Uses the decapsulation key to produce a shared secret key from a ciphertext.

Checked input: decapsulation key $dk \in \mathbb{B}^{768k+96}$

Checked input: ciphertext $c \in \mathbb{B}^{32(d_u k+d_v)}$

Output: shared secret key $K \in \mathbb{B}^{32}$

Step 1: $K' \leftarrow \text{ML-KEM.Decaps_internal}(dk, c)$
▷ run internal decapsulation algorithm

Step 2: return K

Module-Lattice-Based Digital Signature Standard (ML-DSA)

ML-DSA, a digital signature scheme based on CRYSTALS-Dilithium, is designed for multi-key environments. Its key strength lies in its resistance to quantum computing threats, leveraging the quantum-resistant security of its underlying cryptographic structure. The scheme comprises three main algorithms:

ML-DSA.KeyGen (Algorithm 1),
ML-DSA.Sign (Algorithm 2), and
ML-DSA.Verify (Algorithm 3)

Working of the ML-DSA Algorithm

1. Key Generation

- Multi-Key Pairs: Each participant involved in the signature process generates their own public-private key pair. For example, if three parties (Alice, Bob, and Carol) are involved, each will create a private key ((SK_A), (SK_B), (SK_C)) and a corresponding public key ((PK_A), (PK_B), (PK_C)).
- Key Distribution: The public keys are distributed to all parties involved, while the private keys are kept secret.

2. Signature Generation

- Message Preparation: The party that wants to sign a message (let's say, Alice) prepares the message (M) that needs to be signed.
- Hashing the Message: Alice computes a hash of the message using a secure hash function to produce a message digest (H(M)).

- Signature Creation (Using Multiple Keys):
 - Alice creates a signature for the message digest (H(M)) using her private key ((SK_A)):
 - This may involve mathematical operations related to the underlying lattice-based or multivariate algorithms.
 - Alice then includes the signatures generated by the other participants who are also signing the message. This allows for a joint signature that requires validation against all involved public keys.

3. Output the Digital Signature

- The final output will be a composite signature consisting of Alice's signature along with additional signatures from Bob and Carol. This combined signature ensures that all parties have agreed to the validity of the message.

4. Signature Verification

- Signature Verification Process: When a recipient receives the signed message, they can verify the signature against the corresponding public keys:
 - The recipient checks Alice's signature using (PK_A), Bob's using (PK_B), and Carol's using (PK_C).
 - Each signature is verified by correlating it with the message digest (H(M)) computed from the original message.
- Validation Outcome: If all signatures are validated successfully, the recipient can trust that the message was signed by all parties and has not been altered.

ML-DSA Key Generation

The key generation algorithm **ML-DSA.KeyGen** takes no input and outputs a public key and a private key, which are both encoded as byte strings.

Pseudo Code of ML-DSA Key Generation

Generates a public-private key pair.

Output: Public key $pk \in \mathbb{B}^{32+32k(\text{bitlen } (q-1)-d)}$ and private key $sk \in \mathbb{B}^{32+32+64+32 \cdot ((\ell+k) \text{ bitlen } (2\eta)+dk)}$

Step 1: $\xi \leftarrow \mathbb{B}^{32}$
▷ choose random seed

Step 2: if $\xi = \text{NULL}$ then

Step 3: return $\perp$ ▷ return an error indication if random bit generation failed

Step 4: end if

Step 5: return **ML-DSA.KeyGen_internal**(ξ)

ML-DSA Signing

The signing algorithm **ML-DSA.Sign** takes a private key, a message, and a context string as input. It outputs a signature that is encoded as a byte string.

Pseudo Code of ML-DSA Singing

Generates an **ML-DSA signature**.

Input: Private key $sk \in \mathbb{B}^{32+32+64+32 \cdot ((\ell+k) \text{ bitlen } (2\eta)+dk)}$, message $M \in \{0, 1\}^*$, context string ctx (a byte string of 255 or fewer bytes).

Output: Signature $\sigma \in \mathbb{B}^{\lambda/4+\ell \cdot 32 \cdot (1+\text{bitlen } (\gamma 1-1))+\omega+k}$.

Step 1: if $|ctx| > 255$ then

Step 2: return $\perp$ ▷ return an error indication if the context string is too long

Step 3: end if

Step 4:

Step 5: $rnd \leftarrow \mathbb{B}^{32}$ ▷ for the optional deterministic variant, substitute $rnd \leftarrow \{0\}^{32}$

Step 6: if $rnd = \text{NULL}$ then

Step 7: return $\perp$ ▷return an error indication if random bit generation failed

Step 8: end if

Step 9:

Step 10: $M' \leftarrow \text{BytesToBits}(\text{IntegerToBytes}(0, 1) \parallel \text{IntegerToBytes}(\langle ctx \rangle, 1) \parallel ctx) \parallel M$

Step 11: $\sigma \leftarrow \text{ML-DSA.Sign_internal}(sk, M', rnd)$

Step 12: return σ

ML-DSA Verifying

The verification algorithm **ML-DSA.Verify** takes a public key, a message, a signature, and a context string as input. The public key, signature, and context string are all encoded as byte strings, while the message is a bit string.

Pseudo Code of ML-DSA Verifying

Verifies a signature σ for a message M .

Input: Public key $pk \in \mathbb{B}^{32+32k(\text{bitlen } (q-1)-d)}$, message $M \in \{0, 1\}^*$,

signature $\sigma \in \mathbb{B}^{\lambda/4+\ell \cdot 32 \cdot (1+\text{bitlen } (\gamma 1-1))+\omega+k}$,

context string ctx
(a byte string of 255 or fewer bytes).

Output: Boolean.

Step 1: if $|ctx| > 255$ then

Step 2: return $\perp$ ▷ return an error indication if the context string is too long

Step 3: end if

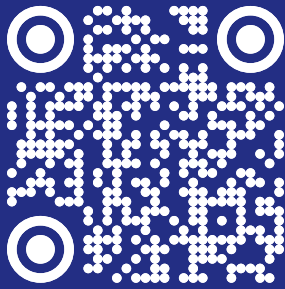
Step 4:

Step 5: $M' \leftarrow \text{BytesToBits}(\text{IntegerToBytes}(0, 1) \parallel \text{IntegerToBytes}(\langle ctx \rangle, 1) \parallel ctx) \parallel M$

Step 6: return **ML-DSA.Verify_internal**(pk, M', σ)



View Digital Report



Indian School of Business
Hyderabad | Mohali

Hyderabad Campus: Gachibowli, Hyderabad - 500 111.

Mohali Campus: Knowledge City, Sector 81, SAS Nagar, Mohali - 140 306.