Factors influencing the Adoption of Quantum Cryptography in the Cybersecurity Industry

Juliette van Mil

Delft University of Technology

TU Delft

Factors influencing the Adoption of Quantum Cryptography in the Cybersecurity Industry

by

Juliette van Mil

to obtain the degree of Master of Science in Communication Design for Innovation
at the Delft University of Technology,

Student number:	4775899	
Project duration:	October 1, 2024 – October 9, 2025	
Thesis committee:	Caroline Wehrmann,	TU Delft, supervisor
	Éva Kalmár,	TU Delft
	Julia Cramer,	Leiden University (assistant professor)
	Hanno van Keulen,	TU Delft

Preface

This thesis project concludes my Master's in Communication Design for Innovation at the TU Delft. It is a double degree master programme, which means that part of this thesis is a technical master thesis in applied physics, that was done in parallel. This applied physics thesis is on the topic of Quantum Secure Function Evaluations, a class of quantum cryptographic schemes and forms the context of this thesis for Communication Design for Innovation. The abstract of the applied physics thesis is included after the Executive Summary. The combination of these two theses resulted in the largest, most interesting and most challenging project I have ever done. I got the opportunity to work on my time-management skills, planning, designing and executing an exploratory research and applying the findings in a communication tool.

I would like to thank Caroline, for her guidance and advice during this project. Our conversations were really helpful and made me feel encouraged to get absolutely everything out my research. Thanks to Julia for her support and for welcoming me in her research group in Leiden. Thanks to the Quantum & Society group for making me feel at home. I really enjoyed the meetings and being able to present and discuss my ideas with the group. I want to thank Éva for her support, and for pushing me to turn the green light version of my thesis into the version it is now, with her feedback. Thanks also to Francisco for our helpful conversations and for your contacts in the quantum and cybersecurity field. I want to thank Leonne for using her amazing skills to design custom images for my communication tool. Thanks to my parents for their support over the past years. Lastly, I want to thank Jasper for his truly unwavering patience and support. Thank you for always being ready to listen, think along, pick up my slack during the last stress-filled weeks, and provide feedback on my chapters.

Juliette van Mil
Delft, October 2025

Executive summary

Encryption is central to securing communication and information exchange in today's digital society. The rapid progress of quantum computing poses a major threat to this. Once cryptographically relevant quantum computers become available, widely used cryptographic systems could be broken. Quantum cryptography, with protocols such as Quantum Key Distribution (QKD) and newer foundations of protocols such as Quantum Secure Function Evaluations, is being developed as a possible solution. Yet, an open question remains whether industry is ready and willing to adopt these technologies once they move beyond research. This adoption challenge is further complicated by the dynamics of technological hype. The excitement around quantum technologies has attracted investment and media attention, and inspired national strategies. However, it also risks inflating expectations and shaping priorities in ways that may not align with practical realities, as has happened with technologies like blockchain. Against this backdrop, it becomes essential to examine how experts in cybersecurity and quantum research perceive quantum cryptography, navigating between justified optimism and potentially misleading expectations.

Research aim and approach

This thesis explores the factors influencing the adoption of quantum cryptography in the Dutch cybersecurity industry and presents a communication tool for those who promote quantum cryptography, to help enhance future narratives surrounding adoption.

How can the opportunities and challenges of adopting quantum cryptography in the Dutch cybersecurity industry be understood through insights into stakeholder perceptions and adoption dynamics?

This is further broken down into four subquestions:

1. How is quantum cryptography perceived in the cybersecurity industry in the Netherlands?
2. Which theoretical perspectives can help explain the dynamics of innovation and technology adoption relevant to quantum cryptography?
3. What insights from adoption models of other security technologies can inform a tailored adoption model for quantum cryptography?
4. How do experts from cybersecurity and quantum cryptography assess the adoption of quantum cryptography in the cybersecurity industry, and which factors do they identify as most influential?

The findings to these research questions are applied in the design of a communication tool to conclude this research.

To answer these questions and apply them in a design, the research followed a triple diamond model (Discover–Define × 2 – Develop–Deliver). The first two diamonds focused on research and analysis, while the third translated findings into a communication design. The methodology combined:

1. A background study of perceptions of quantum cryptography in the cybersecurity industry;
2. The construction of a theoretical framework, drawing on adoption and innovation models;
3. A systematic literature review of adoption models for comparable disruptive security technologies (AI, blockchain, IoT);
4. Expert interviews with professionals in cybersecurity and quantum cryptography;
5. A design phase producing a communication tool to address narrative challenges.

Findings

Perceptions in the Dutch cybersecurity industry

The Dutch cybersecurity field is aware of the quantum threat but demonstrates little urgency or coordination in its response. Awareness is largely concentrated on QKD, with limited recognition of other

quantum cryptographic protocols. Quantum cryptography is often viewed as a far future solution rather than an imminent opportunity.

Theoretical framework

Three dimensions help explain adoption dynamics:

- Why innovation is necessary: framed through the Red Queen hypothesis, cybersecurity is seen as a continuous race between attackers and defenders, with quantum computing as a disruptive shift.
- What drives or constrains adoption: Protection Motivation Theory highlights the role of perceived threats and coping abilities, while security economics reveals systemic disincentives for adoption.
- How adoption unfolds: models such as TAM, UTAUT, TOE, and DOI provide insights into processes of acceptance, diffusion, and integration. Together, these perspectives contextualise adoption of quantum cryptography as both a behavioural and systemic phenomenon.

Insights from adoption models of other technologies

Adoption studies of AI, blockchain, and IoT show that effective models are built by combining different theoretical frameworks and adding technology-specific factors. For quantum cryptography, a hypothetical adoption model is proposed that integrates TAM and TOE, supplemented by DOI innovation characteristics (e.g. relative advantage, complexity, compatibility). Additional factors such as perceived trust and perceived security are highlighted, given their critical importance in the context of data security technologies.

Expert assessments and influential factors

Interviews revealed that adoption of quantum cryptography will depend most strongly on

- A convincing business case (marketing and relative advantage);
- Environmental drivers (standards, certifications, and government regulations);
- Social influence, including hype and lobbying.

Barriers are predominantly technological (complexity, immaturity, fragility of infrastructure, comparison with capabilities of classical cryptography) and organisational (knowledge gaps in both cybersecurity and quantum communities, cost considerations). Importantly, many factors interact: for example, complexity undermines perceived ease of use and trust, while immaturity diminishes relative advantage.

To capture these interdependencies, an infographic synthesis was developed, mapping adoption factors, their relationships, and stakeholder perspectives. This visualisation serves both as an analytical synthesis and a decision-support tool, highlighting factors that have greater or more direct impacts on adoption intention and how their effects are viewed by stakeholders.

Design contribution

Building on the findings, a communication tool was designed to address the issue of fragmented narratives. Stakeholders often rely on a single narrative, such as the hype of absolute security. This oversimplifies the reality of quantum cryptography and risks undermining trust.

The design introduces the ”Dice of Narratives of Quantum Cryptography”, a metaphorical cube with six narrative perspectives. Just as one cannot see all faces of a dice at once, stakeholders rarely perceive all narratives simultaneously. Rolling the dice becomes a way to encounter multiple perspectives, emphasising that only by combining narratives one can make a more balanced and trustworthy story.

The tool is intended for use in policy workshops on conferences (e.g. Quantum Meets), engaging stakeholders such as policymakers, industry leaders, and advocates. By encouraging participants to combine and compare narratives, the tool promotes more nuanced discussions between stakeholder, so future users can make better informed decisions.

Future research directions

This exploratory study of quantum cryptography adoption in the Dutch cybersecurity industry suggests several avenues for further research. First, the proposed hypothetical adoption model could be validated through larger-scale surveys to assess the relative weight and interactions of factors across stakeholders. Longitudinal studies could track how perceptions evolve alongside technical developments and pilot projects. Comparative research across countries would reveal how adoption dynamics differ under varying levels of investment, regulation, and infrastructure readiness. The influence of hype, lobbying, and narratives needs deeper investigation, starting with systematic mapping of currently circulating narratives in industry, policy, and media. The role of standards and certifications on trust, investment decisions, and experimentation should also be explored. Finally, the adoption dynamics infographic that resulted from this research, provides additional paths for design-oriented studies, investigating how different lines of influence can be visualised, communicated, and tested in practice.

Abstract of van Mil, 2025

Cryptographic primitives such as Bit Commitment (BC) and Oblivious Transfer (OT) are foundational building blocks for two-party Secure Function Evaluations. While unconditional security for BC is impossible in the quantum setting, it can be realised under additional physical assumptions. In particular, the bounded- and noisy-storage models provide a framework where security is guaranteed against adversaries with limited quantum memory. Recent work by Ribeiro and Wehner (2020) introduced the first Measurement-Device-Independent (MDI) protocols for BC and OT in the bounded storage model. For the BC protocols, they consider a variant of BC that is called Randomised String Commitment (RSC). They give two MDI-RSC protocols using polarisation-encoded photon sources: one with perfect single-photon emission and another with multi-photon emissions. They also give an MDI-OT protocol using sources with perfect single-photon emission. However, the MDI security for OT using sources with multi-photon emissions remains an open problem.

This thesis investigates the feasibility of MDI-RSC protocols using sources with multi-photon emissions, such as weak coherent pulses (WCP) and spontaneous parametric down-conversion (SPDC) sources. First, we correct a practical error in the existing MDI-RSC protocol by bounding the relevant parameters, ensuring the validity of the original security claims. Second, we analyse the achievable committed string rates while using WCP and SPDC sources. We further consider heralded SPDC sources, which in principle enable single-photon emission, and discuss the impact of imperfect local detectors on their performance and the consequences that has on the protocol implementation.

Finally, motivated by techniques from Twin-Field Quantum Key Distribution (TF-QKD), we give a phase-encoded MDI-RSC protocol using coherent states and provide a sketch of the security proof in the bounded-storage model. We also investigate extending the approach to OT. However, this is still a challenge due to the basis-dependent information leakage inherent in phase-encoded coherent states.

Contents

1 Introduction

In today's digital society, almost all communication and information exchange relies on encryption to ensure confidentiality, integrity, and trust. Classical cryptographic protocols are incorporated in activities as diverse as online banking, secure messaging and the protection of critical government systems. However, the rapid development of quantum computing introduces a fundamental challenge: once sufficiently powerful quantum computers become available, many widely used classical cryptographic systems could be broken. This so-called quantum threat places the future of secure digital communication at risk (AIVD, 2021; Vaishnavi & Pillai, 2021).

One response to this threat is quantum cryptography, which uses the principles of quantum mechanics to secure information and communication in new ways. The most well-known example is Quantum Key Distribution (QKD), but there are other promising approaches, such as two-party protocols. In the parallel applied physics thesis (van Mil, 2025), we investigate protocols in this category, specifically quantum bit commitment, which is a functionality that can be a foundation to enable a wide range of quantum cryptographic applications. This work naturally raises a central question: if new quantum cryptographic protocols are developed in research institutions, is the industry ready and willing to adopt them?

At the same time, it is important to situate this research within the broader discourse of technological hype. The dawn of quantum computing and quantum communication has been accompanied by significant public and private investments, ambitious national strategies, and frequent media attention, often presented in highly expectant or even exaggerated terms (Roberson et al., 2021; Smith, 2020). Such hype can be productive in mobilising resources, raising awareness, and accelerating innovation, but it also risks distorting priorities and inflating expectations. In the field of national security, hype around quantum computers, communication, and sensing technologies has already influenced decision-making (McKinsey, 2024), even as experts caution that timelines and practical applications remain uncertain. This dynamic is not unique to quantum technologies: blockchain, for example, was once heralded as a revolutionary solution across sectors, yet its trajectory illustrates how inflated expectations, coupled with a limited understanding of practical constraints, can lead to disappointment or opportunistic implementations that ultimately hinder adoption (Agustini & Mustakini, 2025). Against this background, examining how experts in cybersecurity and quantum research perceive quantum cryptography is not only a matter of technical feasibility, but also of navigating between justified optimism and potentially misleading expectations.

1.1. Research goal

The current discussion around quantum cryptography is largely dominated by technical development. Yet, the success of any new cryptographic technology depends not only on its theoretical soundness or technical feasibility, but also on whether it is perceived as valuable, relevant, and practical by potential adopters. At present, little is known about how quantum cryptography is viewed outside research environments, particularly within the cybersecurity industry, which is a likely early adopter of such technologies given its role in securing digital infrastructures. The aim of this research is therefore to explore and analyse the key factors influencing the adoption of quantum cryptography in the cybersecurity industry and present a communication tool for those who promote quantum cryptography, to help enhance future narratives surrounding adoption.

This thesis focuses on the intersection of quantum cryptography and the cybersecurity industry. By quantum cryptography, we refer to protocols that use quantum mechanical principles to secure communication or information. By cybersecurity industry, we refer to organisations, companies, and government bodies that are responsible for securing digital communication and data, including large IT companies, dedicated cybersecurity providers, and in-house cybersecurity departments. The scope of the research is limited to companies and organisations in the Dutch cybersecurity industry and field of quantum cryptography.

1.1.1. Research objectives

This project has the following research objectives:

1. To investigate how quantum cryptography is currently perceived in the Dutch cybersecurity industry;
2. To analyse relevant theoretical perspectives on innovation and technology adoption that can explain the dynamics surrounding quantum cryptography;
3. To extract insights from adoption models for other technologies applicable to quantum cryptography via a systematic literature review;
4. To identify and analyse expert perspectives on the opportunities, challenges, and adoption factors of quantum cryptography in the cybersecurity industry.

At the end of the research, a design is proposed that focuses on a communication challenge surrounding the adoption of quantum cryptography that lies in different narratives. We formulate the following design objective:

5. To develop a communication tool that reveals the multiple narratives surrounding quantum cryptography and shows how combining them creates a more balanced and trustworthy story for informed stakeholder decision-making.

1.1.2. Research questions

From the research aim, scope and objectives follows the following main research question.

How can the opportunities and challenges of adopting quantum cryptography in the Dutch cybersecurity industry be understood through insights into stakeholder perceptions and adoption dynamics?

This is further broken down into the following subquestions:

1. How is quantum cryptography perceived in the cybersecurity industry in the Netherlands?
2. Which theoretical perspectives can help explain the dynamics of innovation and technology adoption relevant to quantum cryptography?
3. What insights from adoption models of other security technologies can inform a tailored adoption model for quantum cryptography?
4. How do experts from cybersecurity and quantum cryptography assess the adoption of quantum cryptography in the cybersecurity industry and which factors do they identify as most influential?

The findings to these research questions are applied in the design of a communication tool to conclude this research.

1.2. Approach and methodology

This project follows a triple diamond model (Discover–Define x2 – Develop–Deliver), which structures the process as three iterative cycles of divergence and convergence. The first two diamonds focus on the research objectives, while the third diamond addresses the design objective. Together, these cycles move from exploring and defining the problem space, to analysing adoption dynamics, and finally to producing a communication-oriented design output.

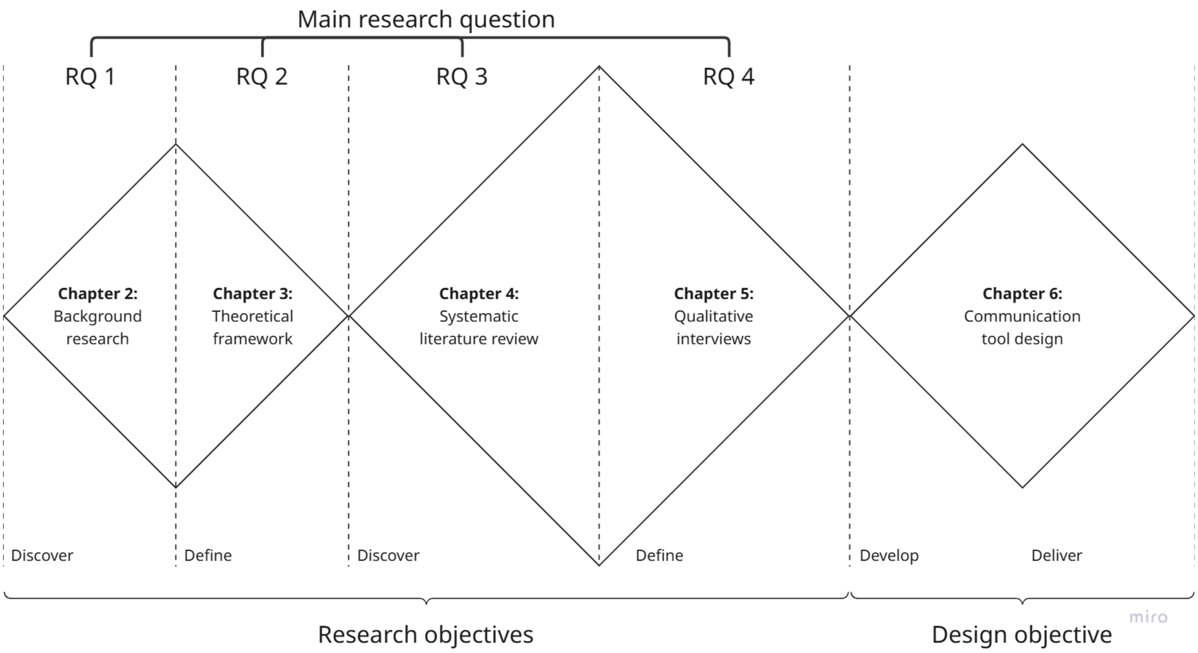
Main research question
RQ 1
RQ 2
RQ 3
RQ 4
Chapter 2: Background research
Chapter 3: Theoretical framework
Chapter 4: Systematic literature review
Chapter 5: Qualitative interviews
Chapter 6: Communication tool design
Discover
Define
Discover
Define
Develop
Deliver
Research objectives
Design objective
miro

Figure 1.1: Visualisation of the triple diamond structure of this thesis. The first two diamonds cover the research part and the last diamond the design. For each diverging or converging phase, it is indicated which research question is answered in which chapter of the thesis.

The research part of the project consists of two diamonds, each combining exploratory and validating activities:

1. **Discover (Background exploration):** An initial literature scan and exploratory interviews with a cybersecurity professor and representatives of the Dutch security cluster HSD are conducted. The aim is to understand how cybersecurity professionals and researchers perceive quantum cryptography, and to gauge current awareness of its potential benefits and limitations.
2. **Define (Theoretical grounding):** Insights from the discovery phase inform the construction of a theoretical framework. This framework combines perspectives on innovation in cryptography with established technology adoption models.
3. **Discover (Systematic review):** A systematic literature review is conducted on adoption models of other disruptive security technologies (e.g., AI, blockchain, IoT). The purpose is to extract transferable insights that could inform an adoption model for quantum cryptography.
4. **Define (Expert validation):** Qualitative, exploratory interviews are carried out with experts in both cybersecurity and quantum cryptography. These interviews helped refine and validate a hypothetical adoption model, that was established from the previous steps, while also providing additional perspectives on opportunities and challenges.

The design component is presented as a distinct third diamond, building on the insights generated in the research phase. It does not function as a separate research question, but rather as a translation of the findings into a practical output:

5. **Develop & Deliver (Communication design):** In this final phase, one focal point of the research outcomes is taken as the starting point for a design exploration. The design translates theoretical and empirical insights into a practical communication tool that conveys stakeholder narratives and supports knowledge exchange on the opportunities and challenges of quantum cryptography adoption.

The triple diamond structure with the corresponding chapters of each part, is visualised in Figure 1.1.

Taken together with the applied physics thesis on primitives for new quantum cryptographic protocols, this project offers a dual contribution: while the physics research advances the technical foundations of quantum cryptography, the communication research explores the conditions under which such innovations might be received, evaluated, and eventually implemented. This combination highlights not only the technical possibilities of quantum-secured communication, but also the communicative and organisational dynamics that determine whether those possibilities become reality.

1.3. Thesis outline

Chapter 2 provides an overview of the quantum computing threat to current cryptography and introduces quantum cryptography as a potential solution. The chapter also explores the current awareness and perceptions of quantum technologies in the cybersecurity industry. In Chapter 3, the theoretical framework for this study is created. Chapter 4 outlines the methodology and results of a systematic review of adoption models from other disruptive security technologies. Insights from these models are analysed for their relevance to quantum cryptography adoption. Chapter 5 presents the methodology, results, and discussion of qualitative interviews with experts in cybersecurity and quantum cryptography. Then, Chapter 6 builds on the research findings to develop a communication tool that illustrates narratives around quantum cryptography adoption. In Chapter 7 conclusions of the research and design are presented, together with recommendations for future research. Lastly, Chapter 8 reflects on the thesis, discussing the research design, methodology, and limitations.

2

Background: Quantum cryptography and cybersecurity

Future quantum computers pose a significant threat to modern cryptographic systems. Fault-tolerant quantum computers could break widely used encryption schemes, exposing sensitive data such as government secrets, medical records, and financial information (Salem et al., 2023). Even though the exact timeline for quantum computers to break conventional cryptography remains uncertain, national security services are encouraging proactive preparation for a post-quantum world (AIVD, 2021; NIST Computer Security Resource Center, 2024).

Concerns about the disruptive potential of quantum computing are not new and have circulated since Shor's publication of his factoring algorithm in 1994. In response, two broad solution paths have emerged: post-quantum cryptography, which seeks to design new classical algorithms resistant to quantum attacks, and quantum cryptography, which uses the laws of quantum mechanics to secure communication.

While post-quantum cryptography is actively being researched by the cybersecurity community (NIST Computer Security Resource Center, 2024), the role of quantum cryptography is more uncertain. Its adoption not only depends on technical feasibility, but also on stakeholder perceptions. This chapter addresses the first research question, *how quantum cryptography is perceived in the cybersecurity field in the Netherlands*, through an exploratory literature study and a set of interviews.

2.1. Quantum computers and cryptography

Cryptography is the ancient art of transmitting a message securely between parties, ensuring that it cannot be read or modified by third parties. In modern practice, two broad categories are distinguished. In symmetric cryptography the same key is used to encrypt and decrypt a message. These kinds of schemes are used, for example, to encrypt stored data, like that on hard drives, or secure VPN connections once a session key has been established. In asymmetric (public-key) cryptography, different keys are used for encryption and decryption. These schemes secure for example HTTPS connections, digital signatures and blockchain wallets. Many secure systems combine both types of cryptography. Asymmetric cryptography establishes a secure channel or exchanges a symmetric session key, and then symmetric cryptography handles the bulk data encryption.

Symmetric cryptography relies on the secrecy of the shared key. Breaking it typically requires brute-force searching through all possible keys, which is computationally infeasible for strong encryption schemes. Asymmetric cryptography, on the other hand, is built on families of mathematically hard problems, such as factoring large primes (RSA) or solving discrete logarithms (ECC). Its security depends on the assumption that these problems cannot be solved efficiently. Attacks against asymmetric schemes can therefore target either the underlying hard problem or weaknesses in implementation (e.g. poor randomness, weak parameters).

Cryptographic Algorithm	Type	Purpose	Impact from Quantum Computing
AES-256	Symmetric key	Encryption	Secure
SHA-256, SHA-3	-	Hash functions	Secure
RSA	Asymmetric key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography (ECC))	Asymmetric key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Asymmetric key	Signatures, key exchange	No longer secure

Table 2.1: Impact analysis of quantum computing on encryption schemes (Mavroeidis et al., 2018)

Quantum computers change this landscape because they enable algorithms that cannot run efficiently on classical computers. Grover's algorithm speeds up brute-force search, effectively halving the security of symmetric key lengths. While significant, this does not fundamentally break symmetric cryptography: doubling the key size restores security. Shor's algorithm, however, is far more disruptive. It is a very specific application of the quantum computer, but it targets exactly the mathematically hard problems underlying widely used asymmetric encryption schemes. It allows efficient factoring and discrete logarithm solving, thereby breaking RSA, ECC, and related schemes. Once cryptographically relevant quantum computers (CRQCs) are built, today's widely deployed public-key infrastructure would become insecure.

Mavroeidis et al. (2018) provide an overview of current algorithms and their vulnerabilities, summarised in Table 2.1.

Cybersecurity has always evolved as a cat-and-mouse game between attackers and defenders, with each innovation provoking a countermeasure. Quantum computing represents the next offensive move in this cycle. Defenders are responding in two directions:

- Post-quantum cryptography (PQC) are new classical algorithms designed to withstand quantum attacks. It explores new families of mathematical problems that are hard to solve even for a predicted quantum computer.
- Quantum cryptography describes protocols that use quantum mechanical principles to achieve security, in some cases with information-theoretic guarantees (unbreakable by any type of computational power).

Neither approach ends the evolutionary cycle. PQC could still be challenged by future algorithmic or hardware breakthroughs, while quantum cryptographic protocols, despite strong theoretical security, may be undermined by flaws in implementation or deployment.

Quantum cryptography has attracted significant attention as an emerging, potentially disruptive technology in cybersecurity. Its promise of information-theoretic security and fundamentally new capabilities has led to widespread hype in both academic and industry circles (Pirandola et al., 2019; Smith, 2020). However, like many new technologies, its current practical applications are limited, the infrastructure is costly, and its adoption faces many barriers. Presenting it as a transformative solution while simultaneously acknowledging these limitations, provides a realistic lens through which to assess its potential impact and adoption.

2.2. What is quantum cryptography?

Quantum cryptography is broadly defined as the study of cryptographic tasks that can be implemented using quantum hardware (Vidick & Wehner, 2023). IBM describes it as a set of methods for encrypting and transmitting secure data based on the principles of quantum mechanics (IBM, 2023). It belongs to the wider field of quantum communication, where information is transmitted using quantum bits (qubits). This gives quantum communication the power to implement applications beyond the reach of classical systems, including:

- **Quantum Key Distribution (QKD)**: protocols to securely distribute a shared key between two trusted users, with the feature that eavesdropping on this exchange can be detected.
- **Quantum secret sharing**: distributing a secret among multiple parties such that only a subset can reconstruct it, with added quantum security guarantees.

- **Delegated quantum computing**: protocols that allow a client with limited quantum capability to delegate computations to a powerful quantum server while maintaining privacy and security.
- **Blind quantum computing**: a stronger form of delegated quantum computing where the server performing the computation learns nothing about the client's data, algorithm, or result.
- **Distributed quantum sensing**: linking sensors across large distances through entanglement distribution to achieve higher precision measurements than possible classically.

To realize such applications, three elements are essential.(Vidick & Wehner, 2023):

- **End nodes**: devices on which a user can manipulate quantum information. At least one end node with one qubit already makes it possible to observe some quantum properties that are needed for cryptography such as the no-cloning theorem and uncertainty relations. With two end nodes with qubits, one for each user, you can have quantum entanglement between the two. More nodes implies more complex quantum functionality.
- **Transmission**: the means to transmit quantum states from one end node to the other. These can be physical media that are able to transmit light (e.g. glassfiber cables), as quantum states can be encoded in light.
- **Cost-effective and reliable connections**: making quantum cryptographic technologies broadly available relates to the cost and reliability of quantum communication technology. Costs can be lowered by making a network that users can share, like the classical internet, but this brings complications. Building a network makes the technology more complex, because of the delicate nature of qubits. Distance scaling is hard as qubits tend to get lost over large distance transmissions. It is also hard to amplify the information as they cannot be copied without information being lost.

Quantum cryptography uses the core quantum principles of superposition, measurement disturbance, no-cloning, and entanglement. These properties make some protocols theoretically unbreakable (Pirandola et al., 2019). Unlike classical schemes, which rely on computational assumptions, quantum cryptographic protocols can offer statistical (information-theoretic) security, meaning security holds regardless of an adversary's computational power. Moreover, for some protocols, even with relatively modest resources, quantum communication can outperform classical communication, as Wehner et al. (2018) point out in their review on the road to the future quantum internet. This is because the quantum properties can already be exploited with very few qubits.

At the same time, the field rests on a chain of assumptions. Most advanced quantum protocols are still only in the research and design phase, with security based on theoretical proofs, disregarding the flaws of practical implementations. Furthermore, the quantum threat itself is still hypothetical (large-scale CRQCs do not yet exist), and quantum cryptography as a solution assumes that this threat will materialise. Adoption therefore requires organisations to act under uncertainty, investing in solutions for a problem whose timeline and form remain unclear.

2.3. The quantum network

During a private conversation on 9 January 2025, in Delft, a cybersecurity professor of TU Delft shared his perspective on quantum cryptography. He described quantum cryptographic protocols as building blocks, comparable to Lego bricks, rather than complete systems. Classical cryptography already provides a full, functioning structure, whereas quantum protocols currently exist as isolated pieces whose eventual integration remains uncertain. It is still unclear whether these quantum ”bricks” will replace some classical components, supplement them, or eventually contribute to an entirely new structure.

Among these building blocks, QKD is by far the most widely recognized and deployed. It is highlighted in industry reports such as McKinsey's Quantum Technology Monitor (McKinsey, 2024), reviewed comprehensively in Pirandola et al. (2019), and already piloted in practice, for example at the Port of Rotterdam (Port of Rotterdam - News Overview, 2024). The reason that QKD is most well known, is because it can be implemented with relatively modest hardware requirements, placing it at the earliest stage of Wehner et al.'s quantum internet roadmap (Figure 2.1).

However, later stages in the roadmap include functionalities such as secure identification and advanced two-party protocols that could more directly replace vulnerable classical primitives like signatures. The

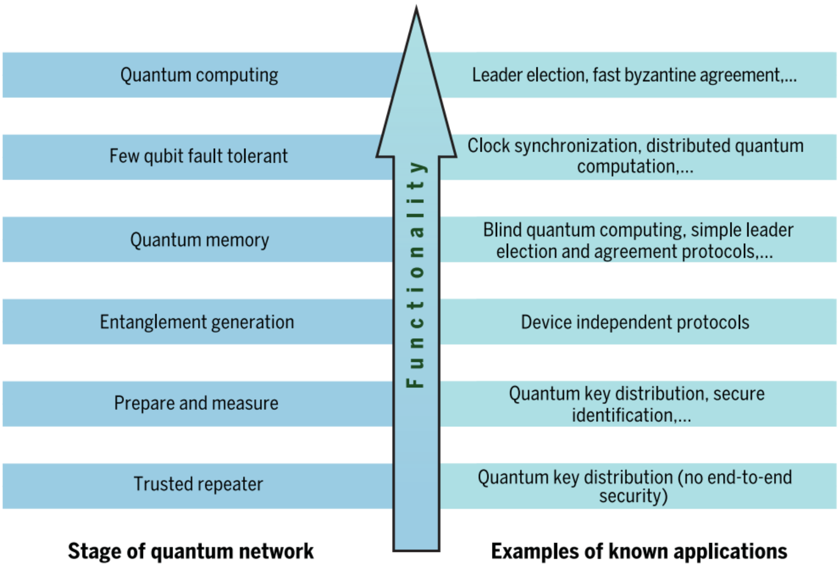
Quantum computing
Few qubit fault tolerant
Quantum memory
Entanglement generation
Prepare and measure
Trusted repeater
Leader election, fast byzantine agreement,...
Clock synchronization, distributed quantum computation,...
Blind quantum computing, simple leader election and agreement protocols,...
Device independent protocols
Quantum key distribution, secure identification,...
Quantum key distribution (no end-to-end security)
Functionality
Stage of quantum network
Examples of known applications

Figure 2.1: Stages in the development of a quantum internet from Wehner et al. (2018). Each stage is characterised by an increase of functionality at the expense of greater technological difficulty.

strong association of quantum cryptography with QKD may therefore narrow industry perceptions. Complicating matters, QKD is still costly and technically challenging, leading organisations like the AIVD to discourage its adoption (AIVD, 2021). As a result, some security companies may refrain from exploring the broader potential of quantum cryptography.

2.4. Awareness and perception in the cybersecurity field

To assess awareness of quantum cryptography in the Dutch cybersecurity field, we combined an interview with an industry stakeholder and an analysis of publications aimed at practitioners.

On 5 February 2025, in The Hague, we conducted an interview with The Hague Security Delta (HSD), a Dutch cybersecurity umbrella organisation. The conversation revealed that quantum cryptography remains largely unfamiliar. Beyond QKD, most quantum protocols are virtually unknown. Companies in their network do not perceive urgency: other threats are more immediate, and the unclear timeline for CRQCs contributes to a lack of prioritisation. HSD currently focuses on raising awareness, often framing the quantum threat in terms of geopolitical adversaries such as China or the U.S. This resonates with their members, but the abstract and distant nature of the risk hampers engagement.

The interview further highlighted the complexity of the cybersecurity ecosystem as a barrier. Before responding to the quantum threat, organisations need to map which systems are at risk and what replacements are feasible. Yet the novelty of quantum technologies makes this difficult, and there is little coordination across the ecosystem. Responsibilities and first steps remain ambiguous, leading to a sense that ”everyone is waiting for each other.”

This findings are also represented in broader industry perspectives. Deloitte (Raskovich et al., 2024) contrasts the quantum risk with Y2K. While Y2K had a fixed deadline, the quantum threat’s fuzzy timeline encourages procrastination and focus on immediate problems. Publications directed at industry audiences likewise emphasise the threat of quantum computing and the promise of PQC and QKD (AIVD, 2021; McKinsey, 2024; Verhagen et al., 2019), but rarely highlight the broader spectrum of quantum cryptography.

To conclude, the Dutch cybersecurity field is aware of the quantum threat but lacks urgency and coordination in its response. Awareness is mainly focused toward QKD, with limited recognition of other quantum cryptographic possibilities. Greater education and cross-sector collaboration could help expand the focus from quantum as merely a threat to quantum as an opportunity, fostering more balanced preparation for the sizeable impact of CRQCs (Raskovich et al., 2024).

3 Theoretical Framework

To analyse the adoption of quantum cryptography, this chapter brings together several theoretical perspectives that explain the interaction between technological change, organisational decision-making, and user behaviour. These perspectives collectively provide a theoretical framework for the study and answer the second research question: *Which theoretical perspectives can help explain the dynamics of innovation and technology adoption relevant to quantum cryptography?*

The discussion is structured around three guiding dimensions: *why*, *what*, and *how*. At the evolutionary level, we ask *why* innovation in cybersecurity, and specifically quantum cryptography, is necessary. The Red Queen hypothesis, introduced in Section 3.1, frames cybersecurity as a perpetual race between attackers and defenders, with quantum computing representing a potentially disruptive turn in this dynamic. At the behavioural level, we consider *what* factors drive or constrain adoption in Section 3.2. Protection Motivation Theory highlights how perceptions of threat and coping ability influence security choices, while insights from security economics show the systemic pressures influencing adoption. Finally, at the adoption level, we turn to *how* new technologies become integrated. In Section 3.3 we look at how established models of technology acceptance and diffusion explain the processes through which individuals and organisations evaluate and integrate new technologies such as quantum cryptography.

3.1. The Red Queen hypothesis and disruptive innovation theory

The Red Queen hypothesis, first proposed by Van Valen (1973), describes systems in evolutionary biology in which species must continually adapt simply to maintain their relative fitness in an environment where others (predators, parasites) are also evolving. The name is borrowed from Lewis Carroll's Through the Looking-Glass, in which the Red Queen tells Alice that it takes continuously running, just to stay in place (see Figure 3.1).

Applied to cybersecurity, this perspective frames the field as a co-evolutionary arms race in which defenders and attackers continuously adapt to each other's moves. The emergence of quantum computing and the corresponding development of PQC and quantum cryptography illustrate this dynamic. The Red Queen hypothesis provides a theoretical foundation to understand why cybersecurity innovation cannot be a one-time response but must be ongoing. It also provides an argument to keep working on quantum cryptography next to PQC, even if they are not needed yet for the current security threats.

Alternatively, quantum cryptography can be framed by disruptive innovation theory (Christensen, 1997) as a potential paradigm-shifting technology that can fundamentally alter the landscape of secure communications. This relates mainly to quantum cryptography in the broader context of quantum communication, which promises more applications than what is described by cryptography and may create new markets dedicated to quantum communication. In this sense, organisations are not only deciding whether to keep pace with the Red Queen but also whether to adapt to a disruptive set of new innovations with more elaborate implications. In this thesis, the broad context of quantum communication is outside the scope, and this perspective will be disregarded.

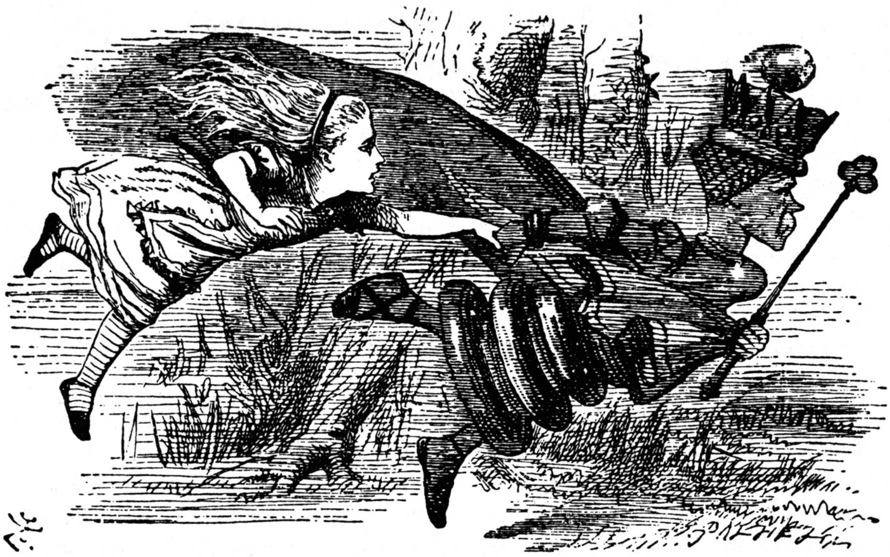

Figure 3.1: ”Now, here, you see, it takes all the running you can do, to keep in the same place.” - Lewis Carroll (Carroll, 2010)

3.2. Protection Motivation Theory and security economics

While the Red Queen hypothesis frames cybersecurity as an endless evolutionary race, it does not explain how individuals or organisations actually make decisions to adopt new protective measures. To address this, Protection Motivation Theory (PMT) (E. M. Rogers, 1983; R. W. Rogers, 1975) provides a useful framework. Originally developed in health psychology to explain how people respond to threats, PMT has since been applied in information security research (Ifinedo, 2012; Lee & Larsen, 2009).

PMT proposes that protective behaviour is based on two factors:

- Threat appraisal, which considers perceived severity and vulnerability, and
- Coping appraisal, which weighs the efficacy of the response, self-efficacy, and response costs.

In the cybersecurity context, PMT helps explain why organisations may choose to invest (or not invest) in new security solutions. For example, as the quantum threat becomes more visible, organisations with a high perception of vulnerability and belief in the effectiveness of PQC or QKD will be more motivated to adopt. Conversely, if response costs are too high, motivation may be reduced despite the evolutionary need highlighted by the Red Queen hypothesis.

This connects to the standpoint of security economics, that security is not only a technical challenge but also an economic one (Anderson, 2001). Organisations face a cost–benefit dilemma: investing in stronger cryptographic solutions gives immediate costs, while the benefits are probabilistic and often only expresses in the prevention of bad events.

3.3. Technology acceptance and adoption in the case of quantum cryptography

To understand the adoption of quantum cryptography, it is useful to draw on established theories of technology acceptance and adoption at both the individual and organisational levels. While adoption refers to the organisational or societal decision to integrate a technology into existing practices, acceptance captures the individual end-user’s willingness and intention to use it (Davis, 1989).

3.3.1. Foundational behavioural theories

Individual acceptance theories highlight how attitudes, norms, and perceived control shape technology use. The Theory of Reasoned Action (TRA), developed by Fishbein and Ajzen (1975) explains behaviour as a function of intention, which is itself shaped by attitudes and subjective norms. The Theory of Planned Behaviour (TPB) extends TRA by adding perceived behavioural control, acknowledging that intentions may not translate into action when individuals feel constrained (Dainton & Zelley, 2010).

3.3.2. Technology acceptance models

Building on TRA and TPB, the Technology Acceptance Model (TAM) (Davis, 1989) identifies two key beliefs influencing acceptance: perceived usefulness (PU) and perceived ease of use (PEOU). Both shape attitudes and behavioural intentions, with PU having a strong direct influence. A visual representation of TAM is given in Figure 3.2.

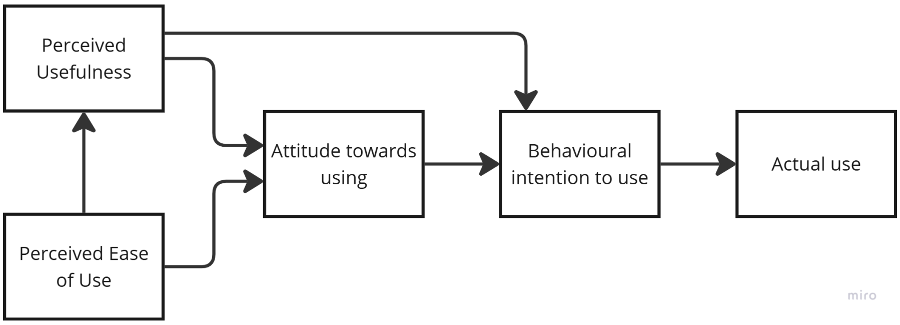

Figure 3.2: Diagram of the Technology Acceptance Model of Davis (1989).

The Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003) integrates TAM and other frameworks, emphasising performance expectancy, effort expectancy, social influence, and facilitating conditions, with effects moderated by demographic and situational variables. These models are particularly useful for understanding end-user acceptance of new technologies such as quantum cryptography.

3.3.3. Organisational adoption frameworks

At the organisational level, the Technology–Organization–Environment (TOE) framework (Tornatzky & Fleischer, 1990) highlights three contexts shaping adoption: technological (e.g., feasibility, compatibility), organisational (e.g., size, resources, culture), and environmental (e.g., competition, regulation). Complementing this, Diffusion of Innovations (DOI) theory (E. M. Rogers, 1983) emphasises how the characteristics of an innovation itself influence its rate of adoption across a population. These five characteristics are relative advantage, compatibility, complexity, trialability, and observability.

4 Systematic literature review: adoption models of security technologies

This chapter addresses the third research question: *What insights from adoption models of other security technologies can inform a tailored adoption model for quantum cryptography?*

While the previous chapter introduced general theories of innovation and technology adoption, this chapter extends that foundation by examining how such models have been applied to other emerging, security-relevant technologies. Specifically, blockchain, artificial intelligence (AI), and the Internet of Things (IoT) are considered. They share important features with quantum cryptography, such as high technical complexity, security and trust concerns, dependency on infrastructure, regulatory uncertainty, and being surrounded by hype. By comparing adoption research across these domains, this chapter identifies relevant extensions and contextual factors for the theoretical models that can inform a model tailored to quantum cryptography.

First, the review method and search strategy are explained. Second, the selected studies are presented. Third, the findings are discussed in terms of their implications for quantum cryptography adoption. Finally, the chapter concludes by proposing a hypothetical adoption model that integrates these insights and provides a basis for further validation in later stages of this research.

4.1. Methodology

This systematic literature review examines how technology adoption models have been applied in the context of blockchain, AI, and IoT security. The goal is to identify adoption factors and theoretical extensions that may also be relevant for quantum cryptography.

Blockchain shares similarities with quantum cryptography, particularly regarding its emphasis on security and the high technical complexity that can act as a barrier to understanding and adoption. While both technologies aim to secure data, their core purposes differ: blockchain emphasizes decentralisation and transparency, whereas quantum cryptography is concerned with unbreakable encryption and secure communication based on quantum mechanical principles. Despite differences in application, existing blockchain adoption studies offer valuable insights into how users perceive security, trust, and technological usefulness, which are equally important concepts for quantum technologies.

The use of AI in security applications introduces another set of relevant adoption challenges. Trust in autonomous decision-making, high complexity, and the need for transparency are central concerns in both AI and quantum cryptographic systems. Both quantum cryptography and AI can seem to operate as a ”black box,” requiring users to place confidence in a system they may not fully understand. As such, adoption models for AI incorporate constructs like perceived trust and perceived risk which may also be relevant for quantum cryptography.

Lastly, IoT security is included due to its deployment context. Like quantum cryptography, it is often adopted by large organisations rather than individual consumers.

Search Strategy

The review was conducted using two databases: Web of Science and Scopus. For each technology, search queries combined the term *”technology acceptance model”* with *adoption* and *security*, alongside the name of the technology. The following queries were used:

- `"technology acceptance model" AND blockchain AND adoption AND security`
- `"technology acceptance model" AND ("artificial intelligence" OR AI) AND adoption AND security`
- `"technology acceptance model" AND ("internet of things" OR IoT) AND adoption AND security`

Inclusion and Exclusion Criteria

The following criteria guided the selection of studies:

- **Inclusion:** Peer-reviewed articles published within the last five years up to March 2025, focusing on adoption factors for blockchain, AI, or IoT in a cybersecurity context.
- **Exclusion:** Studies indexed under unrelated domains (e.g., hospitality, medicine, food sciences), studies focused on end-consumer rather than organisational adoption, cross-cultural comparisons, voice assistants (for AI), articles written in languages other than English or Dutch, unavailable articles, and duplicates across the two databases.

After applying the criteria, the search gave 8 blockchain studies, 8 AI studies, and 3 IoT studies, of which one overlapped with blockchain. This resulted in a total of 18 articles for the review.

4.2. Findings from the literature

The articles that were found included two systematic literature reviews on blockchain adoption. Alshamsi et al. (2022) revealed that in the articles they collected, TAM was by far the most common model for studying blockchain adoption, followed by the TOE model, then UTAUT and IDT. They also analysed the collected articles, to find the most common external factors that influence the adoption of blockchain. The first four of these factors are trust, perceived cost, social influence and facilitating conditions. The authors of this review do not give descriptions of these factors.

In a systematic review of research on the adoption of blockchain Norbu et al., 2024 focus on trust and UTAUT as the main influencers for blockchain adoption. The results from their literature review indeed support that the four factors of UTAUT influence consumer acceptance of the adoption of blockchain in digital payment systems. They also find that the adoption of blockchain-based systems is influenced by trust, going so far even to say that trust is the foundation for user acceptance. Trust is in turn built on regulation, security, privacy and transparency.

The other 16 articles we found are summarised in Table 4.1. Most of the articles that were found use TAM as the basis of their research into the adoption of blockchain, AI or IoT, and augment this with extra factors.

4.2.1. Extending TAM

The article by Kuberkar and Singhal (2021) looks into both blockchain and IoT. They add two extra factors to TAM acting on the behavioural intention towards the adoption of blockchain and IoT, besides perceived ease of use and perceived usefulness.

- Perceived Security, the perception of technology being secure from external unauthorized access, and
- Government Support, government’s policies and regulations, formulation of standards, incentivising stakeholders.

These two additions were suggested by experts, and tested through survey in their research. They also propose and test the task-technology fit (TTF), described as a measure of how the technology characteristics fit with the task characteristics to determine the performance impact of technology, as preceding factors before perceived usefulness and perceived ease of use. They found that the hypothesised influence of all factors were supported.

In a research exploring blockchain adoption in real estate, Yang et al. (2025) also hypothesises task-technology fit as influencing factor for perceived usefulness and perceived ease of use. Next to that they propose

- *Perceived compatibility*, which refers to the degree to which a technology or innovation aligns with users' existing values, needs, and experiences, and
- *Data privacy and security*, which represent the protection of users' personal and sensitive information during technology use,

to extend TAM, based on previous literature. The proposed model was tested via a field survey among real estate buyers and sellers in China. They found that task-technology fit and data privacy and security were significant factors.

The study by Shrestha et al. (2021) adds trust, privacy and security dimensions to classic TAM for analysing the adoption of blockchain based systems. Based on previous literature they add the factors

- *Quality of System*, the technical details of the system interface and system's quality that produces output response;
- *Trust*, the user's belief in the reliability of a system or service provider, especially in contexts where the user becomes vulnerable during transactions;
- *Perceived Privacy*, the user's concern over unauthorized access and misuse of their personal and financial information;
- *Perceived Security*, the degree to which a user believes the technology has no predisposition to risk.

The effects that these factors, besides perceived usefulness and perceived ease of use have on the attitude towards blockchain based systems and the intention to use, were validated through survey questionnaire among participants recruited through the university website. Quality of system and trust were found to be significant factors influencing the intention to use and the attitude towards blockchain based systems respectively.

Sciarelli et al. (2022) extend TAM with perceived benefits of *reduced cost* and *efficiency and security*. These hypotheses were tested via survey questionnaire spread among their target segment. They find that efficiency and security has a significant effect on attitude towards adoption and perceived usefulness. Reduced cost does not have a significant effect on either.

Koyluoglu and Acar (2023) add *perceived security* to TAM, defined as the perception of loss of control over sensitive information. They hypothesise its influence on attitudes towards AI and intention to use AI in mobile banking, next to the usual factors perceived usefulness and perceived ease of use. The hypotheses are tested through survey and it was found that all three have significant influence on the attitude. Park and Jones-Jang (2023) also adds *security and surveillance concerns* to TAM, after suggestions from experts, in the examination of adoption of AI systems. They do not include explicit descriptions of these factors. From their survey they found support for the indirect influence of security concerns on the intention to use AI, and no support for the influence of surveillance concerns.

Also for the adoption of AI in banking services, Rahman et al. (2023) extends TAM with the factors

- *Awareness*, the user's level of knowledge about the technology;
- *Perceived risk*, the user's subjective expectation of suffering a loss by using the technology in the quest of obtaining the desired outcome;
- *Perceived trust*, A multifaceted and dynamic belief held by users, particularly in uncertain or risky environments, that a system, service, or provider will act reliably, securely, and in their best interest;
- *Subjective norms*, the belief that a person or group of people will approve and support a particular behaviour, the influence and opinion of other people

that influence the intention to adopt AI in banking. They gathered their hypothesised factors form semi-structured face-to-face interviews with bank officers and validated them through structured questionnaires among bank clients. They found significant support for the influencing factors perceived usefulness, perceived risk, perceived trust and subjective norms.

Majrashi (2024) creates an augmented TAM from factors found in literature. Next to perceived usefulness and perceived ease of use, they add

- *Perceived trust*, the extent to which individuals believe that a technology or system is reliable and will act in their best interest.
- *Social/subjective norms*, the perceived social pressure individuals feel to engage or not engage in a specific behaviour.
- *Perceived tolerance*, an organisation's openness to learning from failures during innovation.
- *Perceived impact*, the expected organisational, social, and environmental benefits of adopting a technology.
- *Isomorphic pressure*, external and internal influences that drive organisations to conform to established norms or practices.

This model was validated through a survey and it was found that all of the hypothesised relationships between the factors and the attitude toward AI and intention to adopt AI were supported.

Zhang et al. (2023) adds four extra factors to TAM besides perceived usefulness, perceived ease of use:

- *Support system* refers to the level of support from the organisation and other and other basic resources to use the technology;
- *Perceived security* refers to the users' belief or impression that their personal data is adequately protected when using an application or technology;
- *Individual innovation* refers to a personal trait that reflects a person's willingness and ability to embrace and adopt new technologies;
- *Perceived enjoyment* is the degree to which a user experiences pleasure or fun from using a system or technology, independent of its performance or utility outcomes.

They test the hypotheses that these factors influence the constructs of TAM via a questionnaire among a very broad group of IoT users in their target audience. Perceived security, individual innovation and support system were found to have a significant effect on the behavioural intention to use.

To assess the adoption of IoT, Picoto et al. (2023) use UTAUT2, which includes the following factors, besides perceived usefulness, perceived ease of use and social influence.

- *Perceived enjoyment* is the level of pleasure and fun derived from using a technology, regardless of its performance benefits.
- *Habit* refers to the automatic tendency to perform behaviours due to prior learning and repetition.

They combine this with a trust model including the factors

- *Trust* refers to the expectation that others will not behave opportunistically in a given context.
- *Privacy* is defined as the rules governing access to personal user data.
- *Data confidentiality concerns* refers to ensuring that personal data is accessible only to authorised individuals or systems.

They validated the influence factors have on the intention to use IoT in e-commerce via a questionnaire and found that only data confidentiality concerns, perceived ease of use and social influence were not significant.

4.2.2. Other adoption models

In the research on the adoption of blockchain done by Bhardwaj et al. (2021) TAM is integrated with TOE and DOI. The factors that are included in the hypothesised model are *perceived usefulness* and *perceived ease of use* from TAM, *technology readiness, top management support, security concerns, cost concerns, government policy* and *vendor support* from TOE, and *relative advantage, technology compatibility* and *complexity* from DOI. These hypotheses were tested via an online questionnaire among companies in India and it was found that relative advantage, technology compatibility, complexity, perceived usefulness and top management support were significant factors. For these results in relation to the current research for quantum cryptography, it should be noted that there are cultural differences between India and the Netherlands, that might influence the outcomes of the questionnaires.

Chittipaka et al. (2023) examine the adoption of blockchain in supply chains in India through the TOE framework. From literature, they identify the following 11 factors: *relative advantage, trust, compatibility* and *security* in the technological perspective, *firm't IT resources, higher authority support, firm size* and *monetary resources* in the organisational perspective, and *rivalry pressure, business partner's pressure* and *regulatory support* in the environmental perspective. The hypothesised influencing factors are tested via an online survey among professionals in their target group. All 11 factors having significant influence on the adoption of blockchain were supported by the results of the survey.

In assessing the acceptance of AI Assaf et al. (2024) use a combination of TOE and TAM with *Relative advantage, complexity, compatibility* and *observability* in the technological perspective, *top management support, managerial capability* and *organisational readiness* in the organisational perspective, and *legal framework* and *competitive pressure* in the environmental perspective. In their model, these TOE-factors are hypothesised to have effect on either *perceived usefulness* or *perceived ease of use* and this is validated with a survey among the target group.

Rana et al. (2024) study the factors influencing the adoption of AI in developing countries. For this they use an extended UTAUT that includes *trust* and *privacy* besides the standard *performance expectancy, effort expectancy, social influence* and *facilitating conditions*. These factors and their influence on the intention to adopt AI were validated through questionnaires. Facilitating conditions and privacy were found to only have significant influence on the actual use behaviour, the other four factors were found to have significant influence on the intention to adopt.

New models

Two articles create their own, new adoption models. Russo (2024) investigated the adoption of AI tools in software engineering through an open-ended question survey among software engineers, based on TAM, DOI and Social Cognitive Theory (SCT). The factors included in the survey were perceived usefulness, perceived ease of use, compatibility, relative advantage, complexity, social influence, environmental factors and self-efficacy. They propose a new model to understand and predict the adoption of AI in software engineering: the Human-AI Collaboration and Adaptation Framework (HACAF), which is based on TAM, DOI, SCT and UTAUT, and claim that it is a more tailored and nuanced model. HACAF includes four factors that influence the intention to use AI: *personal and environmental factors, perceptions about technology, compatibility factors and social factors*. These were validated through a survey, in which all factors proved to be significant, and perceptions about technology and social factors were the most significant influencers of the intention to use AI.

After an elaborate literature study Vorm and Combs (2022) introduce the intelligent systems technology acceptance model (ISTAM), with the added factor of *transparency* next to perceived usefulness and perceived ease of use influencing the behavioural intention of acceptance. The model is based on an elaborate analysis of the effect of trust on intelligent systems acceptance. Transparency is in this model defined as a multidimensional entity consisting of transparency for monitoring, transparency for process visibility, transparency for surveillance, and transparency for disclosure. They found that transparency is essential for trust in intelligent systems. Their model ISTAM is only conjectured, not tested through, for example, surveys.

Table 4.1: Overview of adoption models and factors used in literature results

Reference	Title	Model(s) used	Factors used	Empirical Validation
		Blockchain		
Bhardwaj et al. (2021)	Determinants of Blockchain Technology Adoption in Supply Chains by Small and Medium Enterprises (SMEs) in India	TAM, TOE, DOI	RA, CP, CX, PU, PEOU, technology readiness, top management support, security concerns, cost concerns, government policy, vendor support	Online surveys
Kuberkar and Singhal (2021)	Factors Influencing the Adoption Intention of Blockchain and Internet-of-Things Technologies for Sustainable Blood Bank Management	TAM	TTF, PU, PEOU security concerns, government support	Online and offline survey questionnaire
Shrestha et al. (2021)	Augmenting the technology acceptance model with trust model for the initial adoption of a blockchain-based system	TAM	PU, PEOU, security, trust, perceived privacy, quality of the system	Online survey questionnaire
Sciarelli et al. (2022)	Factors affecting the adoption of blockchain technology in innovative Italian companies: an extended TAM approach	TAM	PU, PEOU, reduced cost, efficiency and security	Survey questionnaire
Chittipaka et al. (2023)	Blockchain Technology for Supply Chains operating in emerging markets: an empirical examination of technology-organization-environment (TOE) framework	TOE	RA, CP, trust, security, firm's IT resources, higher authority support, firm size, monetary resource, rivalry pressure, business partner's pressure, regulatory support	Survey
Yang et al. (2025)	Exploring real estate blockchain adoption: An empirical study based on an integrated task-technology fit and technology acceptance model	TAM	PU, PEOU, TTF, Data privacy and security, Perceived compatibility	Field survey
		Artificial Intelligence		

Continued on next page

Reference	Title	Model(s) used	Factors used	Empirical Validation
Vorm and Combs (2022)	Integrating Transparency, Trust, and Acceptance: The Intelligent Systems Technology Acceptance Model (ISTAM)	ISTAM	PU, PEOU, transparency	Literature study
Koyluoglu and Acar (2023)	A study on adoption of artificial intelligence use in mobile banking	TAM	PU, PEOU, perceived security	survey
Park and Jones-Jang (2023)	Surveillance, security, and AI as technological acceptance	TAM	PU, PEOU, security concerns, surveillance concerns	Survey
Rahman et al. (2023)	Adoption of artificial intelligence in banking services: an empirical analysis	TAM	PU, PEOU, awareness, perceived risk, perceived trust, subjective norms	structured questionnaire
Assaf et al. (2024)	Assessing the Acceptance for Implementing Artificial Intelligence Technologies in the Governmental Sector	TAM, TOE	PU, PEOU, RA, CP, CX, OB, top management support, managerial capability, organisational readiness, legal framework, competitive pressure	survey
Majrashi (2024)	Determinants of Public Sector Managers' Intentions to Adopt AI in the Workplace	TAM	PU, PEOU, perceived trust, social/subject norms, perceived tolerance, perceived impact, isomorphic pressure	survey
Rana et al. (2024)	Assessing AI adoption in developing country academia: A trust and privacy-augmented UTAUT framework	UTAUT	Perf Exp, Eff Exp, Soc Inf, Fac Con, trust, privacy	Survey
Russo (2024)	Navigating the Complexity of Generative AI Adoption in Software Engineering	HACAF	personal and environmental factors, perceptions about technology, compatibility factors, social factors	Survey
		Internet of Things		

Continued on next page

Reference	Title	Model(s) used	Factors used	Empirical Validation
Picoto et al. (2023)	Integrating the Internet of Things Into E-Commerce: The Role of Trust, Privacy, and Data Confidentiality Concerns in Consumer Adoption	UTAUT2	PU, PEOU, Soc Inf, perceived enjoyment, habit, trust, privacy, data confidentiality concerns	questionnaire
Zhang et al. (2023)	A research on users' behavioral intention to adopt Internet of Things (IoT) technology in the logistics industry: the case of Cainiao Logistics Network	TAM	PU, PEOU, support system, perceived security, individual innovation, perceived enjoyment	Questionnaire

4.2.3. Summary of key empirical findings

Across the reviewed studies, several empirical patterns emerge. Perceived usefulness and perceived ease of use, the core constructs of TAM, are consistently found to be significant in influencing attitudes and intentions toward adopting emerging technologies like blockchain, AI, and IoT. However, many studies combined multiple theoretical frameworks, such as TAM, UTAUT, TOE, DOI, and SCT, to better capture the complex interplay of technological, organisational, and environmental factors. This trend suggests that traditional models alone may not sufficiently explain adoption behaviours for emerging technologies. Studies also add new factors to the theory that are derived from the characteristics of the technology itself, like security, trust and transparency. Trust appears frequently as an external factor (Chittipaka et al., 2023; Majrashi, 2024; Picoto et al., 2023; Rahman et al., 2023; Rana et al., 2024; Shrestha et al., 2021; Vorm & Combs, 2022). This trust is often grounded in related concerns such as security, privacy, and transparency, which are themselves often significant in shaping user perceptions.

Other external factors that show frequent significance include task-technology fit, perceived risk, social influence, subjective norms, and top management support. These findings highlight the importance of contextual and organisational elements in adoption decisions, especially when technologies are complex or unfamiliar.

Conversely, some factors were often found to be insignificant. For instance, perceived cost and surveillance concerns were hypothesised as potential barriers but failed to show a consistent or strong influence across multiple studies. (Bhardwaj et al., 2021; Park & Jones-Jang, 2023; Sciarelli et al., 2022)

4.3. Implications for a proposed adoption model for quantum cryptography

While the results of adoption studies of blockchain, AI and IoT provide valuable guidance, they mainly show that models are created by combining different theories and adding extra factors depending on the unique characteristics of the technologies. We can adopt the same approach for quantum cryptography, where we combine the acceptance and adoption models we introduced in Section 3.3 and add extra factors. A hypothetical adoption model is therefore proposed that is informed by, but not strictly bound to, the empirical findings from the literature review, with extra consideration of the characteristics of quantum cryptography.

The proposed model will be built on the foundations of TAM and TOE, selected for their flexibility and demonstrated relevance to emerging technologies. In line with recommendations from Sciarelli et al. (2022) and Kuberkar and Singhal (2021), external factors were derived from the defining characteristics of the innovation itself, consistent with the DOI model. Note that innovation characteristics such as complexity, relative advantage, and compatibility are especially relevant. Quantum cryptography is inherently complex and difficult to communicate outside the physics community. As we found in the background study, its relative advantage lies in its potential to provide provable security against future quantum adversaries. However, compatibility is a contested issue, since integration with existing fibre networks is possible, but technologically fragile. To not limit the hypothetical adoption model, all five technological characteristics of DOI will be taken into account.

Notably, perceived trust will be included as a key factor due to its frequent presence in prior models and its particular relevance to data security technologies. Similarly, perceived security is emphasized, not in terms of the technology's ability to secure information, but the extent to which users feel the technology itself is secure from unauthorized access. This nuance is particularly relevant in the context of quantum technologies, where new security paradigms are being introduced and quantum security technology is being developed by new organisations and enterprises other than the ones conventionally developing cybersecurity systems.

This brings to the following seventeen factors to be included in the proposed model in Figure 4.1. These are factors from the theoretical models in Section 3.3 and security technology specific factors from the literature review. We add

- from DOI: *Relative Advantage, Complexity, Compatibility, Trialability, Observability*;
- from UTAUT/TOE: *Costs, Organisation Size, Cultural Readiness for Change, Government Regulations, Facilitating Conditions, Social Influence, Vendor Support*;
- from TAM: *Perceived Usefulness, Perceived Ease of Use*;
- from the literature: *Perceived Trust, Perceived Security*;
- and from expert feedback (in a private conversation): *Lobbying Group*, reflecting the influence of national-level policy dynamics in the Dutch quantum ecosystem.

To provide structure and clarity, these factors are organised into four contexts: technical, organisational, environmental, and personal. These contexts reflect the theories from which the factors originate. DOI factors are in the technological context. Factors from UTAUT/TOE and the lobbying group from expert feedback further fill the organisational and environmental context. The personal context has the TAM factors and perceived trust and security that we got from the literature review. Organising into contexts avoids presenting them as an arbitrary list and instead shows how they are grounded in established models.

The finer structure of their influence on adoption behaviour, i.e. whether they affect attitudes or intentions, as in TAM, cannot be concluded from the reviewed studies. This is because the studies that are examined focus on different technologies and use empirical validation (e.g., surveys) that is outside the scope of the present work. To keep the model open while still theoretically grounded, the approach loosely follows Bhardwaj et al. (2021). We draw dotted links only between the contexts and the intention to adopt, signalling hypothetical relationships that require empirical testing. These gaps motivate the next stage of the research, where expert interviews in the Dutch cybersecurity and quantum cryptography communities will be used to validate and refine the proposed model.

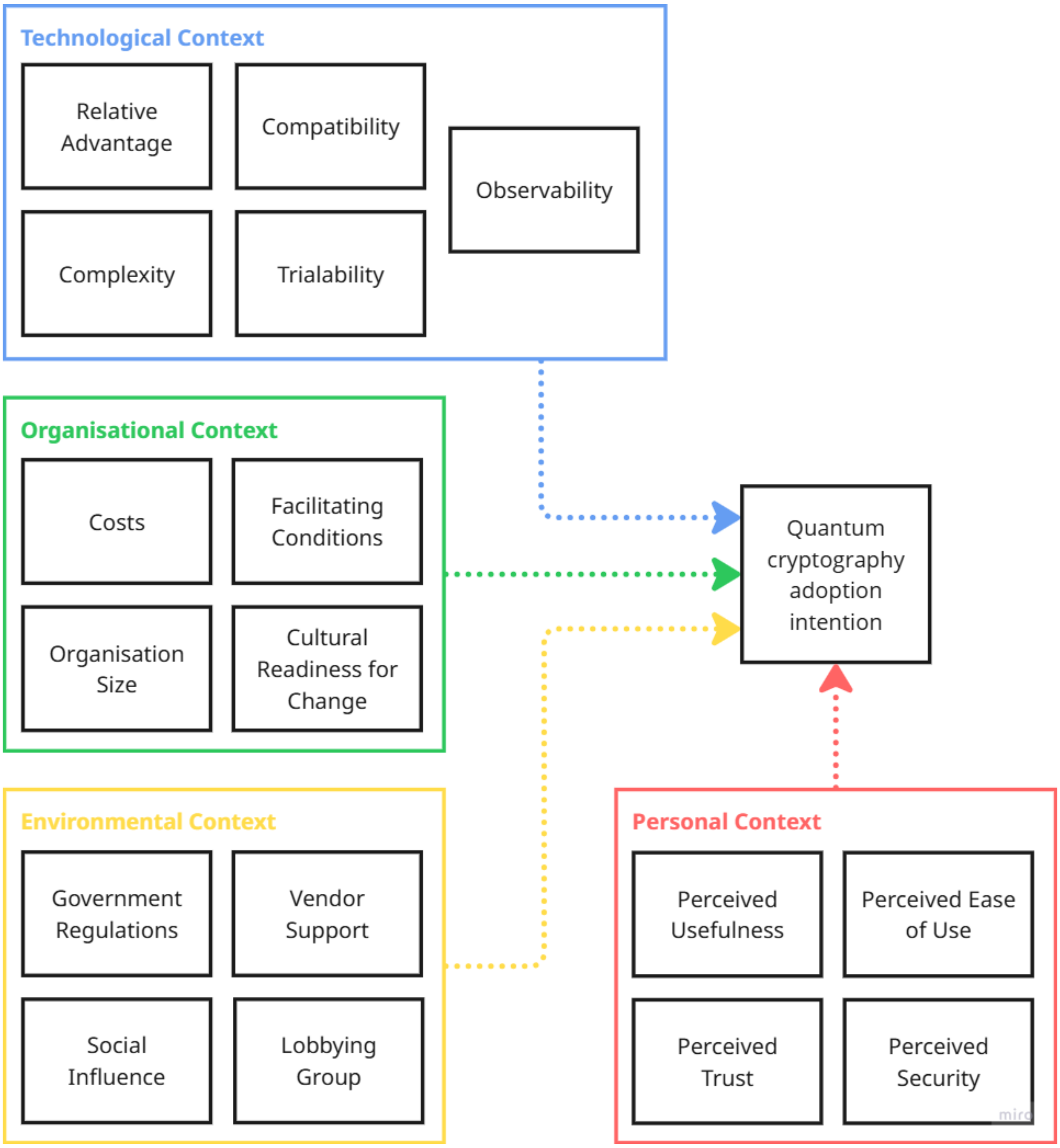

Figure 4.1: Hypothetical adoption model for quantum cryptography, synthesised from TAM, TOE, DOI, UTAUT, and prior empirical studies into blockchain, AI and IoT. Seventeen adoption factors are grouped into four contexts: technical, organisational, environmental, and personal. Dotted links indicate hypothesised relationships between contexts and adoption behaviours that remain to be validated.

5

Expert interviews: influencing factors in the adoption of quantum cryptography

In this chapter, the fourth research question is addressed through structured interviews. The question asks: *How do experts from cybersecurity and quantum cryptography assess the adoption of quantum cryptography in the cybersecurity industry, and which factors do they identify as most influential?* These interviews provide the framework for guided discussions, where participants can elaborate on their insights, experiences, and concerns regarding quantum cryptography. These insight are used to validate and improve the hypothetical adoption model from the previous chapter.

Given the complexity and emerging nature of quantum cryptography, a qualitative approach allows for the collection of in-depth perspectives from experts across both cybersecurity and quantum research domains. In this approach, the exploration and understanding of views on adoption in the context of the participants' perceptions is central.

5.1. Methodology

To capture a wide range of expert insights, participants were selected from two main domains: cybersecurity and quantum cryptography. Within each domain, participants were further distinguished by their level of involvement:

- **Operational experts**: involved in the design, implementation, and development of cryptographic protocols.
- **Strategic experts**: involved in higher-level system decisions, including cryptographic policy and evaluation.

This results in four distinct participant categories:

1. Quantum cryptography – strategic
2. Quantum cryptography – operational
3. Cybersecurity – strategic
4. Cybersecurity – operational

This structure is visualised as a two-dimensional spectrum (Figure 5.1). Participants are then placed along this spectrum, which maps their domain expertise (cybersecurity vs. quantum) against their focus level (technical vs. strategic). The aim was to recruit eight participants in total, two from each category. Initial categorisation was based on publicly available information, such as LinkedIn profiles, publications, and company websites, while the final positioning was refined through the interviews themselves.

All participants were asked to sign an informed consent form (example included in Appendix A). The

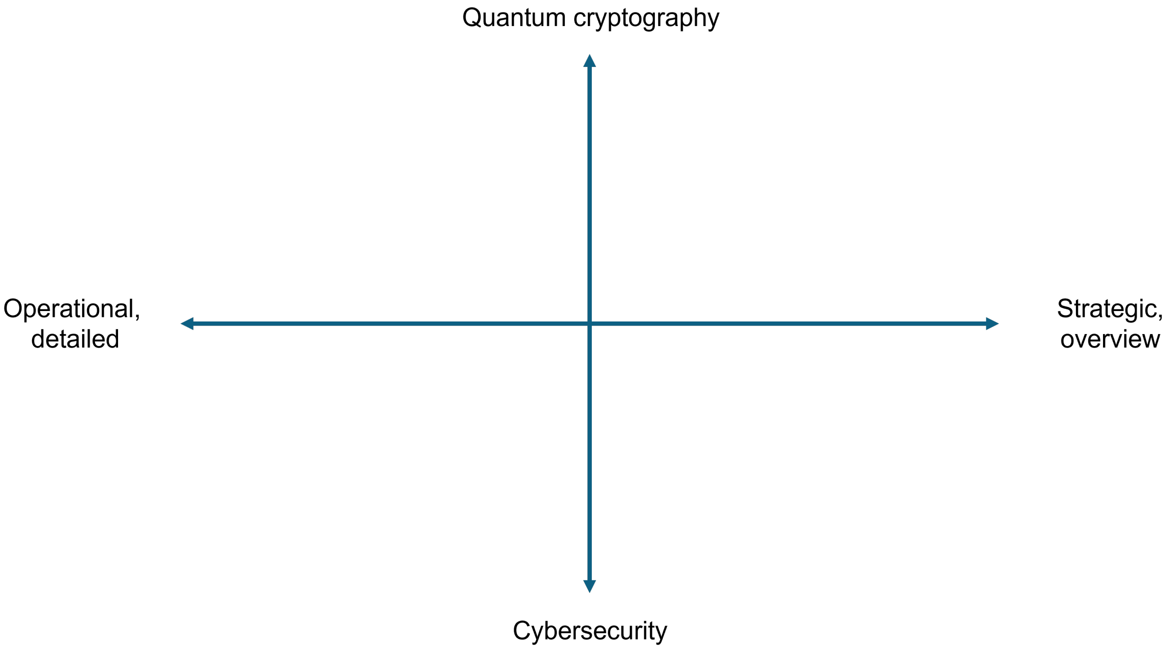

Figure 5.1: Expertise spectrum used during the interviews. Note that quantum cryptography is a subdomain of cybersecurity, and not its opposite.

study protocol was reviewed and approved by the Human Research Ethics Committee of TU Delft.

The interviews were primarily designed for in-person sessions with interactive elements. For logistical reasons, one interview was conducted online. The format proved adaptable, and no substantive differences were observed between online and offline sessions. While in-person interviews remained preferable, both approaches were effective in generating rich qualitative insights.

Each interview was scheduled for approximately 45 minutes, with actual durations ranging between 35 and 60 minutes. The interviews are recorded with a mobile phone app in the case of an offline interview, and with MS Teams in the case of an online interview. The audio recordings are stored on a private hard drive and online in OneDrive. Both storage locations are protected with passwords. The audio recordings are transcribed with MS Word and mistakes in the transcripts are corrected with the audio. The transcripts are stored in OneDrive and uploaded to ATLAS.ti, where they are also stored in the cloud files. The interview guide and supplementary materials are provided in Appendix A.

Question design process

The goal of the interviews is to get the factors for adoption of quantum cryptography in the cybersecurity industry as they are perceived by the interviewed experts. However, all experts that are being interviewed have different backgrounds and levels of expertise, which will influence their opinions. Therefore, a part of the interview needs to be used to create context for the participants insights into adoption by gauging their knowledge and perception of quantum cryptography and the cybersecurity industry.

The interviews thus focus on:

- Context creation: The perception of quantum cryptography from the perspective of the expert's own field.
- Main objective: The factors that influence the attitude of cybersecurity organisations to adopt quantum cryptography.
- The interrelationships: how different expert backgrounds and perceptions of quantum cryptography shape the perceived importance of identified adoption factors.

The first two aspects will be asked explicitly in the interviews, whereas the interrelationships will follow from the analysis of the interview transcripts.

The context creation is done in the introductory part of the interview and in part 1. In the introductory part of the interview, the participant is asked to describe their job. To be able to compare answers of participants, they are also asked to place themselves on the spectrum in Figure 5.1.

Besides the background of the participant, also their perception of quantum cryptography is mapped out to create context for their answers. This is done in the first part of the interview.

Part 1: Perception mapping of quantum cryptography

The first part of the interview aims to map the participant's perception of quantum cryptography. Since the second part of the interview is more in-depth and time-consuming, this section is designed to be efficient yet insightful. To achieve this, three statements about quantum cryptography are presented, each with a 5-point Likert scale (from ”strongly disagree” to ”strongly agree”). After selecting their level of agreement, participants are asked to elaborate on their choice.

Using the Likert scale allows for a structured, standardized way to capture the participants responses and compare them. A 5-point scale specifically provides enough gradation to capture differences in opinion while avoiding the cognitive overload or ambiguity that can occur with longer scales. It also includes a neutral midpoint, covering the possibility of lack of opinion.

This design choice is grounded in Uncertainty Reduction Theory (URT, Berger and Calabrese, 1975). Rather than beginning with open-ended questions, the use of structured statements helps participants anchor their thoughts and reduce initial ambiguity, especially when dealing with a complex and technical topic such as quantum cryptography. The statements serve as cognitive prompts that guide participants toward articulating their perspectives more clearly.

Each of the three statements serves a distinct purpose:

- **Definition of Quantum Cryptography**
  Quantum cryptography is the study and implementation of cryptographic tasks with quantum hardware.
  Adapted from Vidick and Wehner (2023), this statement presents a basic definition of quantum cryptography. It is used to explore whether the participant has an accurate or personally adapted understanding of the concept, whether consciously or unconsciously.
- **Relevance to the Cybersecurity Industry**
  Quantum cryptography is an addition to the field of cybersecurity
  This statement addresses the perceived relevance of quantum cryptography to the cybersecurity sector. Since the rest of the interview focuses on factors influencing adoption in this industry, this serves as a baseline measure of perceived value.
- **Complexity as a barrier for use**
  You have to understand quantum mechanics to implement quantum cryptography.
  This statement probes a hypothesis from the background research: that the technical complexity of quantum mechanics may hinder the adoption of quantum cryptography. It explores whether perceived complexity is seen as a barrier.

The combination of Likert scale and open elaboration is also informed by Cognitive Dissonance Theory. When participants are asked to make a definitive choice on the Likert scale, they may experience a mild form of dissonance, especially if their opinion is not fully formed. The follow-up prompt to explain their choice allows them to resolve this dissonance through reflection and justification, leading to deeper insight into their reasoning.

Part 2: Factors influencing the attitude of cybersecurity companies to adopt quantum cryptography

In the second part of the expert interview, we aim to explore which factors professionals believe will influence the adoption of quantum cryptography in the cybersecurity industry. Rather than asking one complex question, we split the discussion into two more accessible questions:

- What do you think are the main drivers or factors that positively influence the attitude of cybersecurity companies to adopt quantum cryptography?
- And what are the main barriers or factors that negatively influence the attitude of cybersecurity companies to adopt quantum cryptography?

This separation makes it easier for participants to reflect and provide more structured responses.

After this open discussion, we connect the interview back to the literature review. The 17 factors identified from prior studies on emerging technologies are introduced on individual cards. Participants are asked to sort these cards into three categories:

- Positive influence (drivers),
- Negative influence (barriers), or
- Not important (neutral or irrelevant in their view).

Next, we revisit the earlier responses about drivers and barriers. Participants check whether the factors they mentioned are already represented in the cards. If not, they write additional cards for any new or missing factors they believe are important.

The factors and their descriptions as they are presented on the cards are given in Appendix A.

5.2. Data Analysis

The collected data from the interviews consists of

- transcripts of the interview recordings;
- pictures of the factor cards that are picked, ordered into positive and negative influences, and sorted by importance, by the participant;
- pictures of the job description spectrum with the position of the participant indicated with a button.

The interview transcripts were analysed using thematic analysis in ATLAS.ti, conducted in two stages. Thematic analysis was chosen because it allows for the systematic identification of patterns across the different expert perspectives, while remaining flexible enough to incorporate both expected and unexpected insights. The coding process combined a set of predefined codes, derived from the theoretical framework and literature review, with in vivo coding to capture concepts introduced by the participants.

In the first stage, all participant responses were coded to capture recurring themes. In the second stage, the analysis focused on the relationships between participants' backgrounds and the context established in the introduction and Part 1 of the interview, and their insights from Part 2. A detailed description of the coding process, along with the complete code tree, is provided in Appendix A.

The pictures of the ordered factor cards are converted into lists of positive and negative factors, per participant. The position of each factor is paired with a score in the following way

$$\begin{gathered}\#1 \to 1\\ \#2 \to \tfrac{1}{2}\\ \#3 \to \tfrac{1}{3}\\ \#4 \to \tfrac{1}{4}\\ \#5 \to \tfrac{1}{5}\\ \text{et cetera,}\end{gathered}$$

where factors that are tied are given the same score. These results are analysed in MS Excel.

5.3. Participants

A total of 12 participants were interviewed in 11 sessions (one interview included two participants at the same time). This is 50% more respondents than expected. During the interview they placed a marker on a physical copy of the spectrum in Figure 5.1 indicating where they saw themselves. These marker indications were photographed and the placements of all participants are documented in Figure 5.2. These results were used to group the participant into groups, along with the descriptions they gave of themselves during the interviews.

The participants are divided into two groups based on their expertise: quantum cryptography (5 participants) and cybersecurity (7 participants). Within the cybersecurity group, a subcategory of post-quantum cryptography experts (2 participants) was identified. These are specialists in classical cryp-

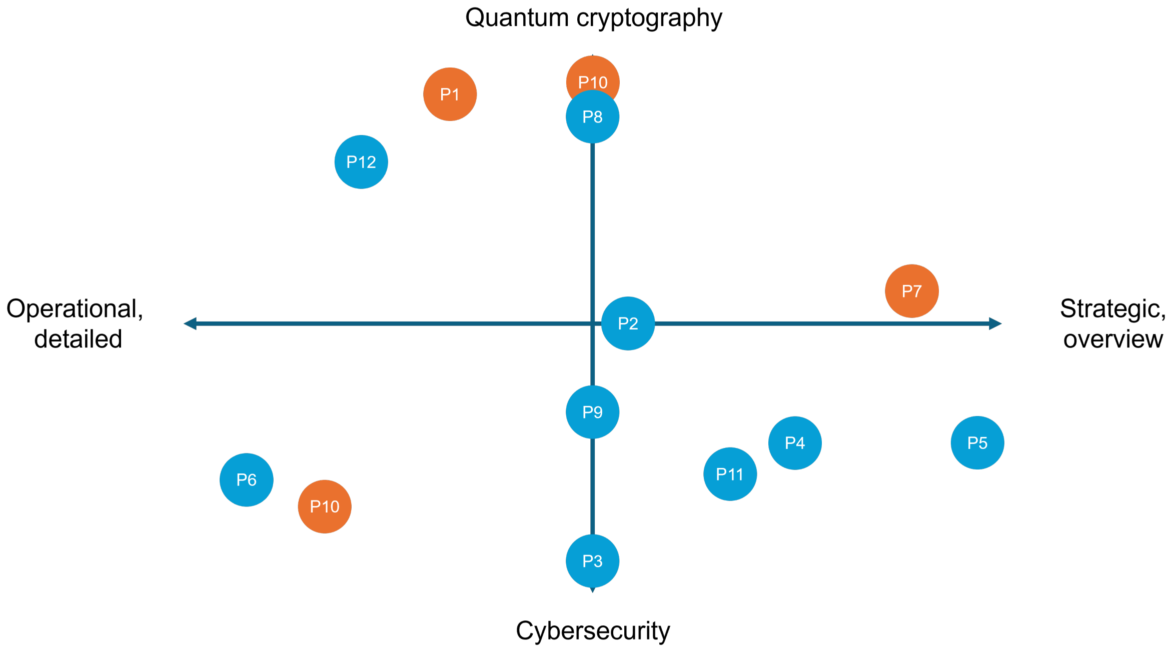

Figure 5.2: Placements of the 12 participants on the job description chart. Participants 1, 7 and 10 were excluded from the analysis, as they either did not do, misunderstood the assignment or withdrew their action.

tography who are more aware of the quantum treat and quantum cryptography, because of their professional expertise.

A division over the other axis, their focus level, was less clear. The participants could, however, be grouped according to their professional roles. The first group consists of professionals working in cybersecurity organisations or in the security divisions of IT and IT-intensive organisations. The second group are civil servants, professionals who work for the government, specifically a quantum expert of the Chief Science and Technology Office (CSTO) of the General Intelligence and Security Service of the Netherlands (AIVD) and two cybersecurity professionals from the Dutch Tax Authority (Belastingdienst). This group overlaps with the first. The third group is composed of executives, all of whom described themselves as part of the ”C-suite” of their organisations, including CTOs and a CEO of cybersecurity companies and a CFO of a QKD startup. The final group includes researchers: two from QuTech and one from TNO.

A Venn diagram of the four participant groups and how they are divided by expertise, is given in Figure 5.3, and a full description of the participants can be found in Appendix **??**.

5.4. Perceptions of the participants

The participants that were interviewed approached quantum cryptography from very different backgrounds, which shaped how they perceived its role, value, and limitations. To capture these perspectives, the first part of the interviews presented three statements. The discussions that followed revealed both areas of agreement and clear divides in how the participants view quantum cryptography.

Defining quantum cryptography

When presented with the definition *quantum cryptography is the study and implementation of cryptographic tasks using quantum hardware*, most participants agreed in principle, though nearly all raised important caveats. Their critiques centred on three aspects: the scope of ’study and implementation’, the vagueness of ’cryptographic tasks’, and the reliance on ’quantum hardware’.

Executives tended to argue that the phrasing was either too narrow or too broad. Some felt that activities such as design and validation should be included, while others believed that calling it a ’study’ was misleading, as they saw it primarily as an applied technology. Several executives also challenged the

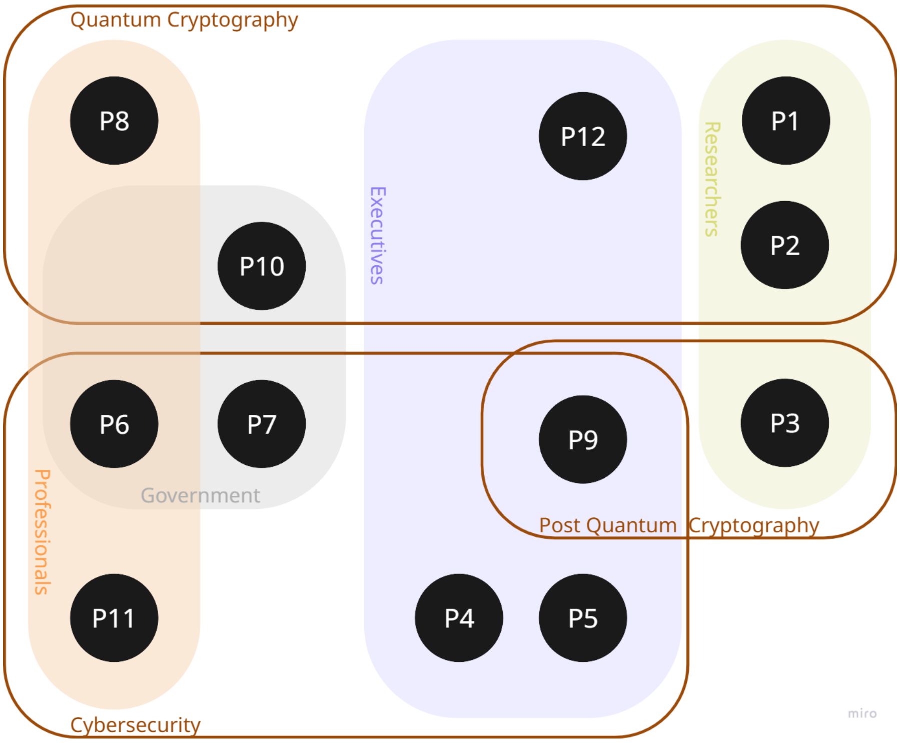

Figure 5.3: Venn diagram of the participants of the interviews, grouped by their role (coloured fields) or expertise (outlined).

breadth of ’cryptographic tasks’, stressing that quantum cryptography is not a full system but rather a set of highly specific protocols, such as QKD.

Participants with a quantum background focused on the phrase ’using quantum hardware’. They emphasised that quantum cryptography is not simply classical cryptography running on a quantum computer. Instead, it exploits the principles of quantum mechanics, such as entanglement and uncertainty, to deliver security guarantees that go beyond classical approaches. From this perspective, quantum cryptography belongs as much to the field of quantum information science as to cybersecurity.

Across groups, several recurring views emerged. First, quantum cryptography is widely seen as a niche technology: valuable in specific applications but unlikely to replace classical cryptography. Second, many participants stressed that the field remains immature, lacking standardisation and real-world testing. This uncertainty leads some to frame quantum cryptography as a ”black box”, or a technology that is poorly understood by non-specialists and not yet ready for broad adoption. Finally, some saw it as a stepping stone toward a larger vision, namely the development of a quantum internet, where its role would extend beyond security alone.

Use cases in cybersecurity

Despite these disagreements about definitions, there was broader consensus on use cases. Most participants described quantum cryptography as a useful addition to the cybersecurity toolbox, though one post-quantum cryptography researcher strongly rejected this view, arguing that, for now, anything quantum cryptography can do, post-quantum methods can also achieve. Even so, there was cautious optimism that quantum methods may eventually offer unique advantages.

For the majority, the real value of quantum cryptography lies in highly specific scenarios. They consistently highlighted two areas: protection against ’store now, decrypt later’ attacks enabled by future quantum computers, and the provision of information-theoretic security that surpasses the mathematical hardness assumptions of classical protocols. Researchers, as well as some executives, further noted that its applications would likely remain concentrated in environments where extremely high-value or long-lived data must be protected. Quantum researchers also pointed to privacy-preserving applications as an emerging area of interest.

Understanding and implementation

The final statement, *you have to understand quantum mechanics to implement quantum cryptography*, provoked the most division.

Researchers and cybersecurity professionals generally rejected this claim, treating quantum cryptography as a 'black box' that can be integrated into existing infrastructures without specialist knowledge of quantum mechanics. However, others argued that at least some level of expertise is required within an implementation team. Without it, they warned, organisations risk misusing or misunderstanding the technology.

Executives and civil servants were typically more cautious and non-committal, acknowledging that while users of quantum cryptography do not need to grasp its physics, awareness of its risks, advantages, and limitations is essential for informed decision-making. A few researchers took this further, stressing that certain core concepts, such as entanglement, are too central to ignore, especially for those developing new cryptographic products.

In practice, the disagreement often came down to how one interprets the word 'implement'. From an end-user perspective, plugging in a device requires no quantum expertise. But for those designing, validating, or deploying the technology at scale, a deeper understanding of quantum mechanics was considered indispensable.

Summary

Participants across groups agree that quantum cryptography offers unique capabilities, particularly for protecting high-risk or long-term data, but they also stress its immaturity, lack of standards, and limited scope. Some frame it as a niche technology, others as a building block toward the quantum internet, and many see it as a 'black box' that will be difficult for end-users to evaluate or trust. These differing perspectives suggest that adoption will depend not only on technical progress but also on clarifying use cases and bridging the gap between expert understanding and practical implementation. Table 5.1 gives an overview of the perspectives the participants regarding the three statements.

Theme	Executives	Professionals	Researchers
Definition of QC	– Too narrow or too broad (debate over ”study and implementation”) – QC is not a full system, but a set of specific protocols – Viewed as a black box	– Generally pragmatic view – QC is more than ”cryptography on quantum hardware” – Some concerns over maturity	– Emphasise link to quantum mechanics and information theory – Stress immaturity and lack of standardisation – QC is a step toward quantum internet
Use cases	– QC is an addition to cybersecurity – Value mainly in very high-risk data scenarios – Stronger guarantees than classical	– QC adds value but only in specific niches – Highlight protection against ”store now, decrypt later” attacks	– Add privacy as a possible use case – Emphasise high-risk, long-term data as key domain
Understanding vs. Implementation	– Users don't need physics, but awareness of risks/benefits essential – Understanding may increase trust	– QC is a plug-and-play black box – Minimal need for quantum expertise	– End-users don't need deep knowledge, but developers/implementers must grasp concepts (e.g. entanglement)

Table 5.1: Overview of expert perspectives on quantum cryptography by role. QC stands for quantum cryptography.

5.5. Influencing factors for the adoption of quantum cryptography

The second part of the interviews focused on identifying the factors that play a role in the adoption of quantum cryptography within the cybersecurity industry.

5.5.1. Categories of factors and emerging additions

The participants were presented with 17 predefined factors on cards and were invited to discuss and expand them. Collectively, they added 20 new factors and even proposed a new overarching category: the business case context. This was introduced alongside the existing technological, environmental, organisational, and personal contexts. Notably, some factors originally placed in other categories were reassigned: *relative advantage* was moved from the technological context, and *costs* from the organisational context, to better fit within the business case category.

During the discussions, the participants repeatedly emphasised the interconnectedness of factors. These links, illustrated in Figure 5.5, were used to refine the adoption model hypothesis. The revised model highlights that technological and environmental factors rarely exert a direct influence on attitudes or intentions to adopt. Instead, they typically act indirectly through the personal context, which consistently emerged as the most immediate driver of adoption attitudes and intentions. All of the newly mentioned factors and the links that were noted between the contexts are incorporated in Figure 5.6.

In the final assignment, the participants had to rank which factors they thought were the most important influences on the attitude towards adoption of quantum cryptography. An overview of these results of importance ranking is given in Figure 5.4.

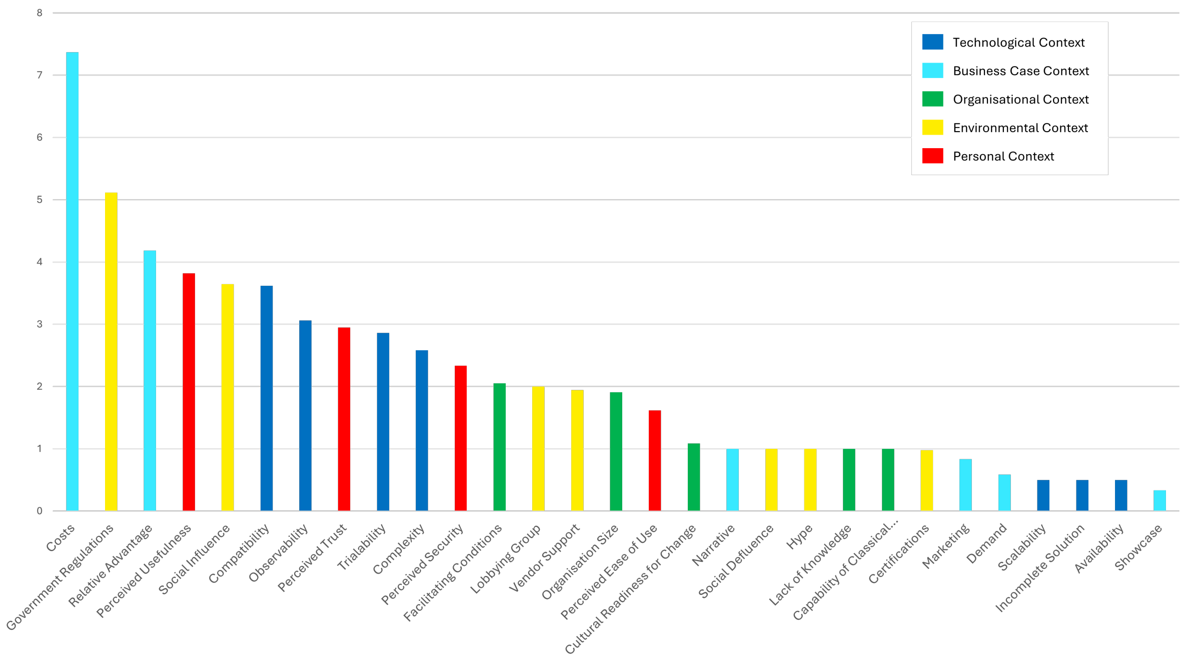

Figure 5.4: Histogram of the factors ranked by importance by the participants. The colours of the bars are according to the contexts the factors belong to.

5.5.2. Drivers and barriers

Before discussing individual factors, participants were asked to consider them as either *drivers* (positively supporting adoption) or *barriers* (hindering adoption). To avoid hypothetical speculation, they were instructed to assess the current status of each factor in relation to quantum cryptography.

Factors perceived as both drivers and barriers

Several factors, particularly from the technological context, were categorised differently by different participants, highlighting their ambiguous role.

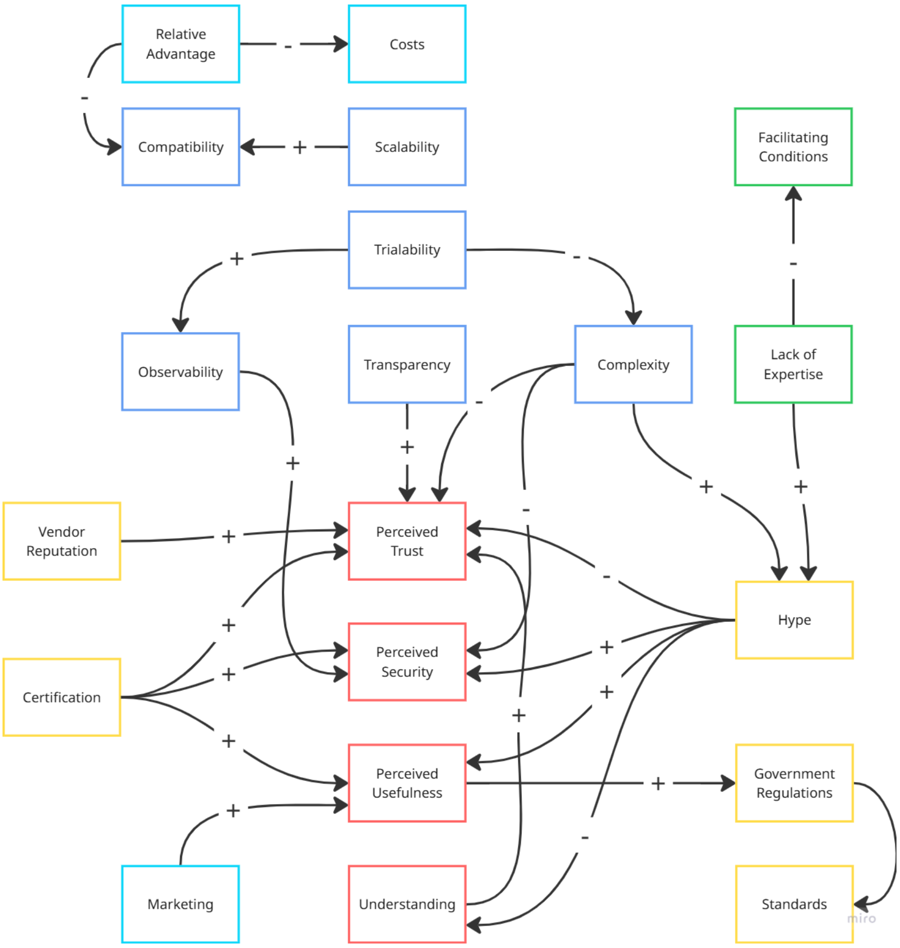

Figure 5.5: Links between factors that were mentioned by the participants during the interviews. Arrows with a '+' mean an enhancing effect and arrows with a '-' mean a mitigating effect.

Compatibility, defined as the degree to which quantum cryptography aligns with existing needs, practices, and values, was a key point of disagreement. Cybersecurity professionals, executives and civil servants often described it as incompatible with current practices, as it relies on fundamentally different security principles than conventional protocols. By contrast, quantum-focused executives and civil servants argued that it directly addresses pressing needs such as the quantum threat and the protection of sensitive data. Researchers, however, questioned its relevance to end-users, pointing out that in a culture where privacy is undervalued (e.g., in the age of social media), compatibility with user values is weak. It appears that the groups may have had different end-users in mind. Interestingly, the civil servants and some professionals dismissed compatibility with current practices altogether, noting that compliance with standards, rather than alignment with practices, drives adoption in cybersecurity.

Observability also produced divergent opinions. Some argued that cybersecurity in general is not observable unless it fails, and that quantum cryptography will face the same limitation, making this factor largely neutral. Others linked observability to the visible benefits of using quantum cryptography, such as provable information-theoretic security, which could be leveraged in marketing as a driver for adoption. However, demonstrating such advantages requires a minimum level of technical understanding from the target audience, which in itself is a challenge.

Trialability was widely seen as problematic. Cybersecurity experts stressed that unlike post-quantum cryptography, quantum cryptography requires specialised hardware and cannot simply be downloaded and tested in existing systems. Although testbeds exist, they are limited in scope and rarely persuasive for large-scale adoption. For this reason, several participants characterised trialability as a barrier. Nevertheless, experts from the quantum community, saw test runs in universities or small-scale pilots as

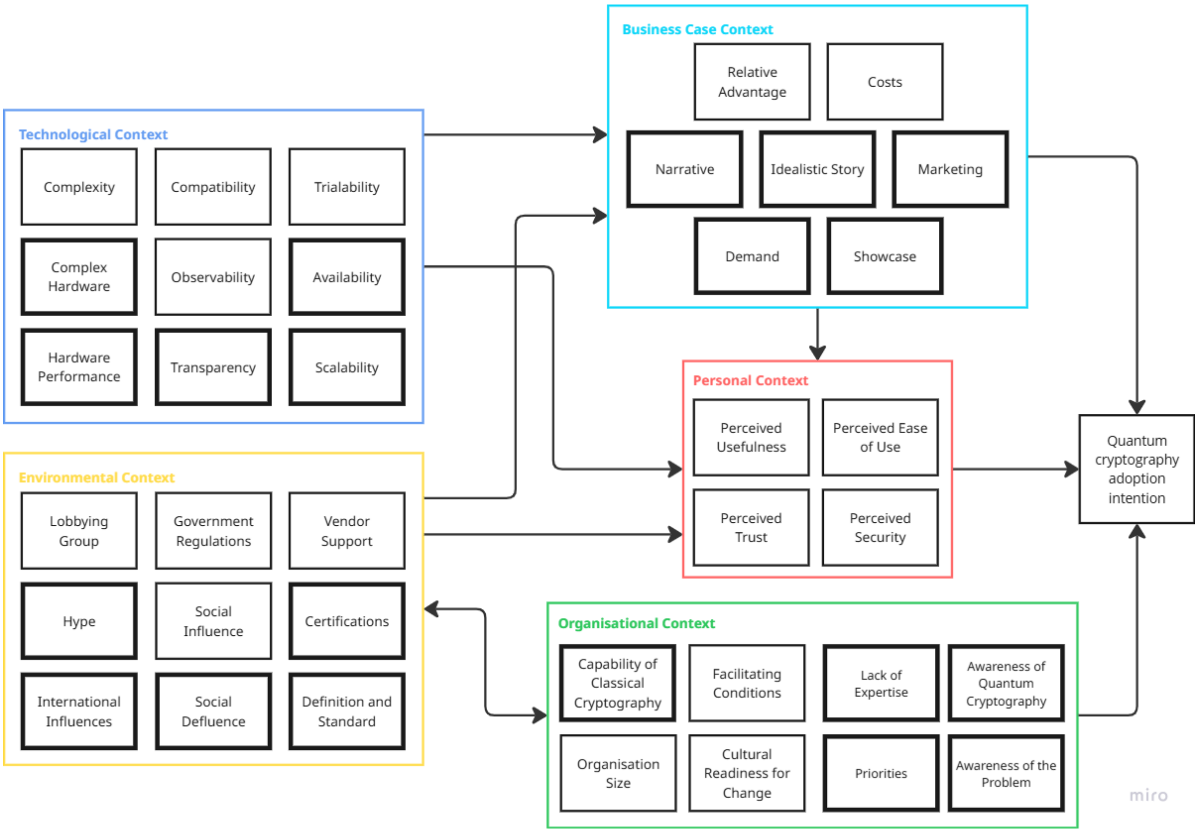

Figure 5.6: Hypothetical adoption model for quantum cryptography, extended with results from the interviews. The factors with bold outlines were added by the participants of the interviews. Note also that the business case context was added.

potential drivers, especially when they increase the visibility and observability of quantum cryptography in practice.

Personal perception factors

The personal context factors, perceived usefulness, ease of use, security, and trust, were consistently highlighted as central to shaping adoption attitudes. Yet, they were also the most contested, with participants offering both positive and negative assessments depending on perspective.

A recurring observation was the overlap between usefulness, security, and trust in the case of cryptography. Many researchers and executives noted that these perceptions are often inseparable: for a cryptographic system to be seen as useful, it must also be considered secure and trustworthy.

At the same time, differences emerged between academic and industry perspectives. Executives and professionals emphasised that what is considered useful in a scientific context does not always translate to practical relevance in industry. Similarly, researchers and executives noted that trust is undermined by the gap between laboratory demonstrations and real-world deployment. From an industry viewpoint, a protocol proven in a lab does not automatically inspire confidence once implemented at scale.

The participants also linked perceptions to two concrete aspects:

- Perceived ease of use is strongly shaped by the complexity of quantum cryptography. The more complex it appears, the less directly useful it is judged to be.
- Perceived security and trust are tied to certifications and standards, which currently do not exist for quantum cryptography. Until such frameworks are developed, doubts will continue to undermine trust.

Taken together, the personal context factors emerged as the most immediate and decisive influences on adoption attitudes. However, their subjective nature and dependence on individual experience, background, and expectations, makes them both the most critical and the most difficult to address. For this reason it was decided to not categorise these four factors as either drivers or barriers, but consider them as direct drivers of adoption and judge their effect by the drivers that in turn positively influence them.

5.5.3. Drivers

The drivers for the adoption of quantum cryptography come mainly from the business case and the environmental context.

Business case drivers: Selling quantum's advantage

Across the interviews, relative advantage emerged as the most important business case driver for adoption. Almost all quantum experts emphasised that quantum cryptography's technical potential benefits should form the cornerstone of any adoption narrative. One cybersecurity executive also stressed that relative advantage can mitigate negative perceptions of costs and compatibility, making it a decisive factor.

Beyond relative advantage, participants highlighted several additional business case drivers. These include showcasing the quantum threat and its solutions, effective marketing, and demand from end-users (i.e., the clients of cybersecurity organisations). Executives and civil servants warned, however, that much of the current marketing around quantum cryptography is overly idealistic and risks undermining credibility. A more balanced narrative is needed, one that acknowledges both the opportunities and the challenges.

As the founder and CEO of an organisation that helps companies become quantum safe argued:

> ”There needs to be a better narrative, not only around quantum cryptography but quantum technology in general. I have been telling organisations like Quantum Delta NL for years: do not be afraid to include the quantum threat in your narrative. If you avoid it, people will quickly doubt whether you really understand the field. But if you acknowledge the threat and explain it well, you will be seen as the expert. It does not hurt adoption, it builds trust, strengthens the investment climate, and shows that you have a complete picture.”

From this perspective, a successful business case rests on honesty and authority: quantum cryptography should not be framed as a complete solution, but as a valuable tool that addresses pressing security concerns.

Environmental drivers: Hype and social influence

Social influence was identified by most participants as a positive driver. When influential organisations adopt quantum cryptography, others are likely to follow. Related to this are international influences. The quantum expert from the AIVD noted that technological progress of influential nations such as China or the US can be a real driver for European countries to work hard on staying ahead in the field of quantum cryptography. For some, this effect of social influence is amplified by the hype surrounding quantum technology, which attracts attention, investment, and research. A cybersecurity professional even noted that hype can play a constructive role in accelerating interest and experimentation.

Others were more sceptical. Several executives warned that hype can also lead to premature adoption, followed by disillusionment, drawing parallels with the blockchain boom. As the CTO of one cybersecurity company explained:

> ”Think of blockchain: there was enormous social influence until people realised it had little practical value in many cases. Social influence can create a kind of herd behaviour. If expertise is lacking, there is a risk that the most hyped technology gets adopted, instead of the most suitable technology for solving the actual problem, which ultimately leads to a waste of money and time.”

Lobbying was discussed as another form of social influence. Most executives and professionals were sceptical, associating lobbying groups with superficial messaging and internal echo chambers. They worried that such groups might exploit the lack of expertise among decision-makers. Researchers, however, saw lobbying as a potentially useful mechanism to connect academia with government. One executive suggested lobbying could indeed support adoption, but only if the narrative is improved and includes a stronger acknowledgement of the quantum threat.

Finally, government regulation was seen as a powerful but double-edged factor. At present, the absence of standards is a barrier, but once established, regulations and certifications could strongly drive adoption, as has been the case for conventional cryptography. Executives cautioned, however, that regulation should not prescribe specific protocols but instead require quantum-safe solutions more generally. The quantum expert of the AIVD also warned that governments may resist quantum cryptography as it is not widely considered mature on the short term from a security perspective. At the same time, the AIVD has concerns with regard to legal aspects and is interested in quantum cryptography, citing Dutch intelligence legislation:

> ”The WIV (Intelligence and Security Services Act) states, for example, that in specific cases, telecommunications companies and providers of communication services must be able to provide specific data. Is that possible when it comes to quantum cryptography?”

Drivers within organisations: Secondary enablers

Within cybersecurity organisations, several secondary drivers were discussed.

Cultural readiness for change was generally seen as positive: most professionals and quantum researchers argued that IT and cybersecurity sectors are accustomed to rapid technological change and therefore open to new tools. One CEO, however, disagreed based on experience, noting that clients often resist change.

Organisation size was described as a mixed factor. Small organisations lack the resources and relevant use cases, while very large organisations may adopt prematurely without a clear need. Adoption is most likely in medium-to-large organisations with sufficient resources and a concrete security demand.

Finally, vendor support was universally acknowledged as a necessary driver. The participants considered it a basic expectation rather than a decisive reason to adopt: without vendor support, adoption is impossible, but with it, adoption is merely enabled rather than guaranteed.

5.5.4. Barriers

Costs are the most important negative factor for the adoption of quantum cryptography in the cybersecurity industry. Both a quantum executive and a quantum professional link high costs to limited availability: the technology is scarce, and this scarcity drives up expenses even more at the moment.

Barriers in the technological factors of quantum cryptography

Professionals, civil servants and executives emphasise that cybersecurity experts will find quantum cryptography complex, since its foundations in quantum mechanics differ greatly from the familiar rules of classical cryptography. The involvement of new and unfamiliar hardware further complicates matters. Moreover, given that classical cryptography is already complex, identifying which components require updates becomes an additional challenge. As the CTO of a large cybersecurity organisation says:

> ”The issue at hand [of the quantum threat to cybersecurity] is already complex for most organisations. So it is not only the complexity of quantum cryptography that deters, but also the complexity in the preliminary phase, where they have to figure out what kind of cryptography needs to be used in which cases.”

In contrast, researchers and some executives consider complexity irrelevant. Their arguments are that quantum cryptography could ultimately be delivered as a ’plug-and-play’ solution, where complexity is hidden from the user. For some, the complexity even adds to the hype, making the technology more intriguing without negatively affecting adoption. They also point out that conventional cryptography is highly complex too, yet indispensable. By that reasoning, complexity alone does not influence adoption.

Both researchers and executives point out that quantum cryptography is not yet a full cryptographic system. At best, it can act as an additional layer of quantum security within an existing cybersecurity framework, bringing with it compatibility challenges. But realistically, looking at what quantum cryptography currently offers, it can only protect against very specific cyber attacks and full security relies on the full system around it being secure and well-maintained. This has also been pointed out in an earlier study by Lindsay (2020).

The fragile and complex hardware is another barrier: it makes the technology difficult to scale, and current performance is insufficient for most practical applications.

Barriers from the environment: The novelty of quantum cryptography

The immaturity of quantum cryptography also creates environmental barriers.

Participants across all groups noted that no certifications currently exist for quantum cryptography, given its early stage of development. Yet certifications are essential in cybersecurity: organisations usually define requirements in terms of standards and certifications, and will only adopt protocols that comply.

One executive linked this absence of certification to social influence, calling it a form of social ”defluence”. They highlighted that reports from influential cybersecurity bodies actively discourage the use of quantum cryptography because of the novelty, uncertainty, and lack of certification of its protocols. While this scepticism may fade as the technology matures, it risks creating a lasting reputation problem.

Some professionals and executives also mentioned vendor reputation as a barrier. When acquiring security, the reputation of the vendor is important. As quantum cryptography is mostly brought to the market by startups at the moment, this is expected to be a barrier.

Barriers from the cybersecurity industry: No knowledge, no interest, no facilities

Professionals and two executives stressed a basic barrier within the cybersecurity field: a lack of awareness, and therefore expertise, regarding quantum cryptography. Many organisations are not even aware of the quantum threat. This challenge is compounded by the inherent complexity of cybersecurity systems, which are themselves becoming more complicated in the era of artificial intelligence.

This lack of knowledge leads directly to a lack of interest. One executive observed that quantum security is at the bottom of most organisations' priority lists. A professional with a quantum background working for an information and communication technology organisation argued that the capabilities of classical cryptography should not be underestimated:

> ”There are decades of work in classical cryptography. [...] And now, post quantum cryptography just shows that you can actually solve the problem to a large extent without any quantum involvement. And I think that really cannot be understated. That might actually be the biggest barrier.”

Participants from all groups also noted that the scepticism of cybersecurity professionals toward unfamiliar technology creates an additional barrier, dampening perceived usefulness even when relative advantage is acknowledged.

This scepticism also negatively shapes perceptions of facilitating conditions. Participants across groups agree that the necessary conditions for adoption, such as infrastructure, support, and expertise, are largely absent, making this a barrier in itself.

Finally, two participants pointed out that the lack of awareness and expertise goes both ways: quantum researchers often lack sufficient understanding of the cybersecurity industry and its actual problems. As a result, there is a tendency to design quantum solutions for problems that do not exist, while the real challenges faced by cybersecurity practitioners remain unaddressed.

5.6. Discussion of the results

The results of this study provide an exploratory view of how participants from different backgrounds perceive the adoption of quantum cryptography in the cybersecurity industry. In this section, the findings are interpreted in light of the research objectives, connected to the literature, and critically examined in terms of scope and implications.

5.6.1. Interpretation of the findings

The analysis revealed a number of recurring themes across the expert groups. Cost was most frequently mentioned as a barrier and relative advantage and social influence most frequently as drivers. Interestingly, both quantum and post-quantum researchers considered complexity to be irrelevant, whereas participants closer to industry regarded it as a significant obstacle. Similarly, there was surprising divergence around the role of lobbying groups: researchers saw them as potential drivers, while other participants considered them irrelevant.

The initial aim was to determine whether participants with a quantum background held different opinions from those with cybersecurity backgrounds. This was indeed noticeable for factors such as trialability, compatibility, hype, and barriers related to the lack of expertise in the cybersecurity industry, where participants with similar backgrounds tended to agree. However, beyond these cases, more agreement appeared within groups defined by role rather than by background. This is likely a result of the interview sample: all participants were already familiar with both cybersecurity and quantum cryptography, given that they agreed to take part. Their opinions and knowledge may therefore have been closer than expected.

Still, the results showed clear differences between groups of participants. Researchers and executives tended to highlight mainly technological barriers, whereas cybersecurity professionals pointed to barriers within their industry and organisations instead. These contrasts can be explained by the experiences and organisational responsibilities of the participants. Overall, the findings highlight that adoption cannot be understood in isolation from the perspectives and incentives of the stakeholders involved.

5.6.2. Relation to the literature

Several results confirmed expectations from the literature. For example, perceived trust and security emerged as factors that are distinct from traditional adoption theories, although some participants regarded them as aspects of perceived usefulness.

The findings also align with the literature in showing that environmental and organisational factors play a central role in the adoption of complex and unfamiliar technologies.

At the same time, the results diverged from earlier work on the role of cost. In prior studies, cost was often hypothesised as important but failed to show statistical significance in surveys. In this study cost was named as the most important expected barrier. If tested in a larger survey, it will be interesting to see whether this factor again proves statistically insignificant, or whether it emerges more strongly than in previous work.

Also the context of the business case was added, which has not explicitly been used in the theory or literature. The business case can be seen as lying in between the technological and organisational context, as it also incorporates the factors relative advantage and costs from these contexts, respectively.

5.6.3. Broader implications

Looking more broadly at the factors identified, the most important drivers appear in the business case, specifically the relative advantage, which is heavily influenced by technological factors, and in the environmental context, through social influence and government. For the latter, however, government is a driver only once standards and certifications are in place to promote quantum cryptography.

The most important barriers, apart from cost, were found in the technological and organisational contexts. Several links between factors also became apparent. Complexity is a barrier mainly for perceived ease of use, trust and security, yet it was also associated with hype. Immaturity negatively influenced the relative advantage in the business case. Relative advantage, in turn, positively influenced perceived usefulness, but perceived usefulness was diminished by the strong capabilities of classical cryptography, an organisational barrier. Organisational barriers were reinforced by a lack of knowledge about quantum in the cybersecurity industry, which was enforced by social defluence. This social defluence comes from environmental barriers: the novelty and immaturity of quantum cryptography, and the absence of standards or certifications. The resulting knowledge gaps leave the field vulnerable to hype and lobbying, which in turn negatively impact perceived trust.

Government and social influence were named as potential strong drivers, but only if they are explicitly positive about quantum cryptography.

These insights suggest that adoption of quantum cryptography will depend above all on environmental factors and a convincing business case, both of which are closely tied to the immaturity of the technology. Although the technological factors currently act mainly as indirect barriers, they deserve attention because of their cascading influence on many other aspects. Organisational barriers are equally important, as they are less directly affected by technological progress. Particularly concerning is the lack of quantum knowledge in the cybersecurity industry. But even more critical is the lack of cybersecurity knowledge within the quantum field. If this gap is not addressed, the two communities risk continuing to develop in parallel without convergence.

The lack of knowledge about quantum could be addressed through environmental drivers, provided that these are accompanied by a carefully framed narrative. Still, there remains a danger that the quantum cryptography community will develop solutions to problems that do not exist.

For theory, the study provides a first exploratory model of how quantum cryptography may be assessed through the lens of technology adoption frameworks. The proposed acceptance model is given in Figure 5.7 and this could be validated through survey in a next study. The factors that are selected for this hypothesis are those that the participants found most important (see Figure 5.4), disregarding whether it would be a driver or a barrier. Based on the discussion of the factors in the interviews, only the factors with a score of 2 or higher are included, making that vendor support, and factors deemed less important than that, are not included in the hypothesis of the adoption model for quantum cryptography.

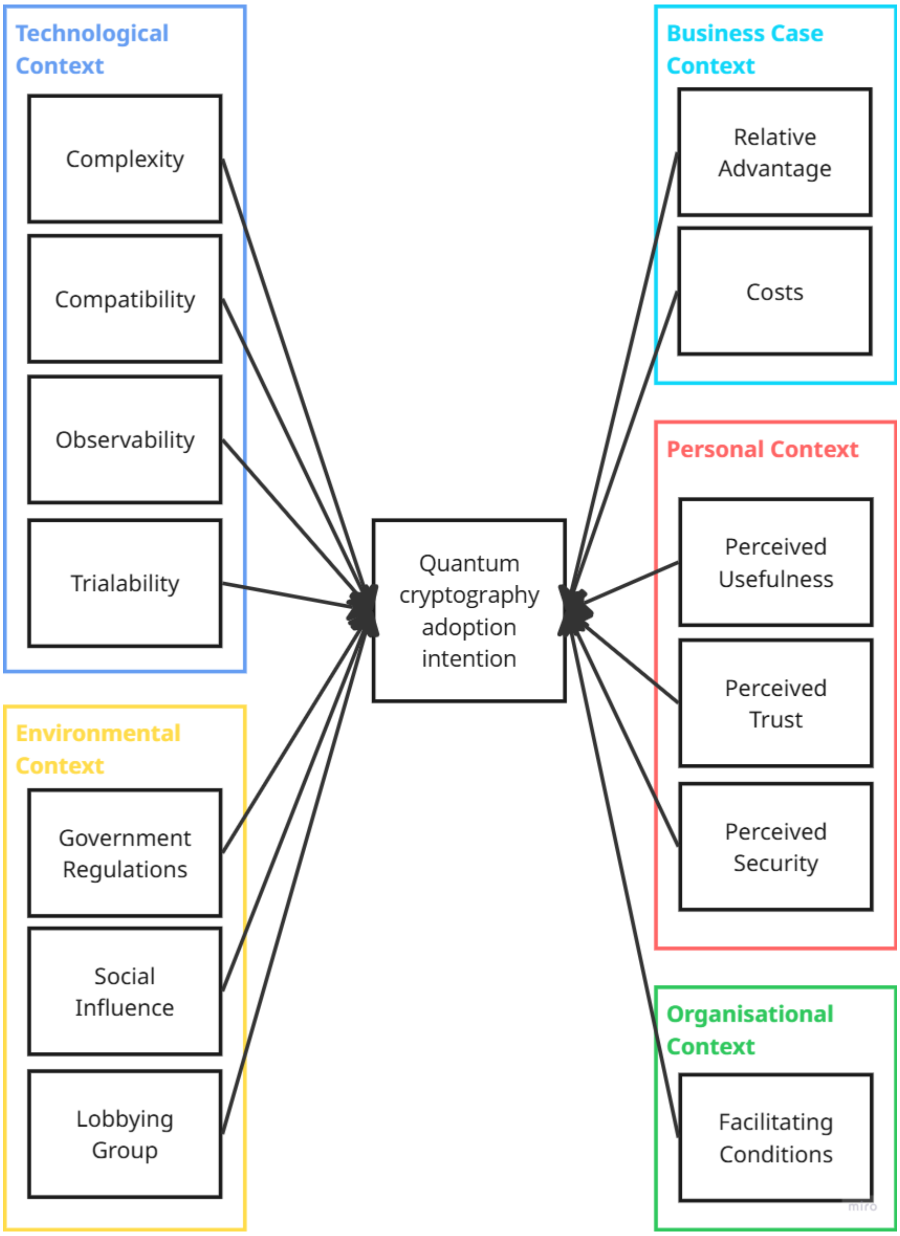

Figure 5.7: Hypothesis for an adoption model for quantum cryptography in the cybersecurity industry based on the inputs of the participants that were interviewed.

5.7. Synthesis: adoption factors of quantum cryptography and their interactions

While Figure 5.7 addresses which factors the participants consider most influential for the adoption of quantum cryptography, the question of how adoption is assessed within the cybersecurity industry requires a more nuanced synthesis. To capture this complexity, Appendix B presents an infographic titled ”Adoption Factors of Quantum Cryptography and their Interactions”, that brings together all identified factors, their interrelationships, and the diversity of perspectives expressed by the participants.

The infographic visualises adoption factors as nodes connected by arrows that indicate influence. Factors are grouped into clusters, represented by coloured shapes. For example, lobbying group, social influence, international influences, and hype form a cluster labelled *Hype and Social Influence*, whereas single factors such as government regulations or compatibility stand alone as clusters of their own. Five cluster colours correspond to the five contexts used in the hypothetical adoption model (Figure 5.7): technological, organisational, environmental, personal, and business case. Each cluster is marked with a ”+” (positive influence), ”–” (negative influence), or both, depending on how the participants evaluated its role.

The perspectives of the participants are represented through speech bubbles that capture explanations and nuances. Icons indicate which stakeholder group the view belongs to: government, professionals, executives, or researchers (see Figure 5.3). An additional icon distinguishes whether the participants have a background in quantum cryptography or cybersecurity, since this sometimes shaped their assessment of specific factors.

The infographic can be used as both a synthesis and a decision-support tool. By showing which factors apply direct and indirect influence, it highlights potential leverage points for supporting the adoption of quantum cryptography. For instance, addressing factors that strongly affect multiple others may have more effect on the adoption process. At the same time, the stakeholder-specific speech bubbles reveal how perceptions diverge, offering insight into communication challenges and opportunities. Together, these layers allow the infographic to serve not just as a descriptive map, but also as a practical guide for identifying priorities in promoting and communicating about quantum cryptography adoption. The key message is that adoption is shaped by a wide range of interdependent factors, and these need to be recognised and addressed in order for quantum cryptography to become a meaningful innovation in the Dutch cybersecurity industry.

6 Design

This chapter translates the findings from the research in this thesis into the design of a communication tool. The starting point for this design is the infographic in Appendix B, which maps out the complex interplay of factors influencing the adoption of quantum cryptography in the cybersecurity industry. Within this map, the factors situated in the personal context stand out as direct drivers of the adoption intention, themselves shaped by influences from other contexts. Among these, we see perceived trust as a particularly critical factor.

First, the literature review highlighted trust as a recurring theme in adoption studies of other security technologies. Second, expert interviews confirmed its importance: after perceived usefulness, perceived trust was ranked as the most influential personal factor (Figure 5.4). Perceived usefulness also emerged from the literature review as an influential factor for the adoption of other security technologies. When we look at direct influencers of perceived usefulness in Appendix B, we see that they are factors from the organisational and business-case context context, which are in turn influenced by the technological context and the clusters *immature technology* and *complexity*. Perceived trust, on the other hand, is directly influenced by environmental factors, such as legislation, lobbying, and hype. These environmental factors are all then influenced by one factor from the business case: *narratives*. These factors and influences are illustrated in Figures 6.1 and 6.2, which are details of the infographic in Appendix B. Thus, whereas perceived usefulness is ultimately influenced by technological factors, perceived trust comes back to the kind of narrative that is used.

This connection is significant. Executives and civil servants in the interviews commented on how quantum cryptography is framed. One participant even explicitly emphasised that the narratives surrounding quantum cryptography, how it is promoted and explained to stakeholders, need improvement. The main problem with there being diverging narratives is that a potential user might hear one story about quantum cryptography from a promoter, but read something else in the news, for example. Not fully aligning or even conflicting narratives will then create confusion and decrease trust.

Across the interviews and background explorations in this research, a wide range of narratives also emerged. Quantum cryptography was framed as a response to the quantum threat or as a set of building blocks for future systems, a step towards a quantum internet. It was also linked to geopolitical competition and the need to stay ahead. At the same time, it was described as a hyped, uncertain, or ”black box” technology, while others highlighted its purely technical promises, such as information-theoretic security and protection against ”store now, decrypt later” attacks.

Building on these insights, the design presented in this chapter focuses on the different narratives around quantum cryptography and their role in shaping communication between stakeholders. The communication tool aims to make these narratives explicit, helping stakeholders to better understand, compare, and reflect on the stories that shape perceptions of trust and adoption.

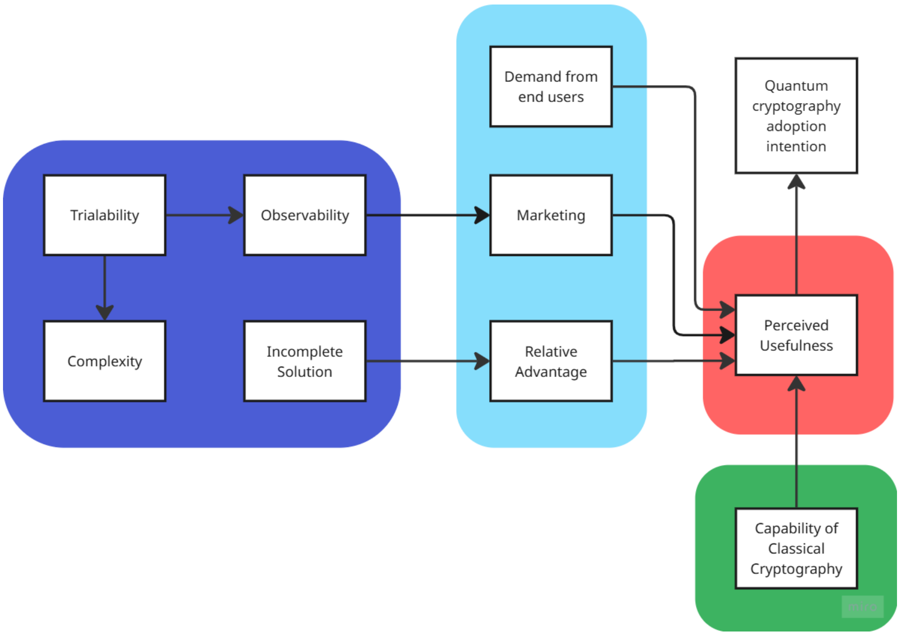

Figure 6.1: Line of influencing factors working through perceived usefulness on the adoption intention. Simplified detail of Appendix B.

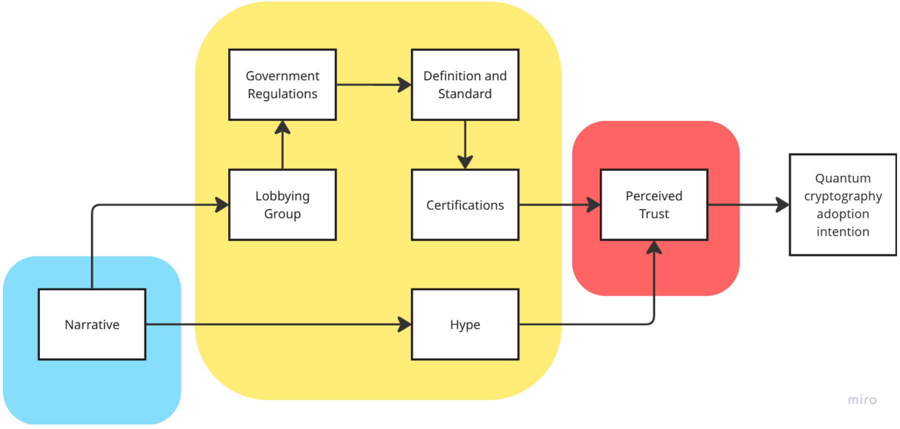

Figure 6.2: Line of influencing factors working through perceived trust on the adoption intention. Simplified detail of Appendix B.

6.1. Problem statement

Current promotion of quantum cryptography often relies on a single narrative. From the interviews, we found that executives and civil servants recognised the hype narrative, which tends to present quantum cryptography in an idealised and exaggerated way. While this approach can capture attention, it risks oversimplifying the technology and undermining trust. To support adoption, communication strategies need to reflect the diversity of narratives, which acknowledge both opportunities and challenges. Different narratives have varying effects of different stakeholders. When different narratives are present, the credibility of the claims decreases.

6.2. Design objective

The goal is to create a communication tool that reveals the multiple narratives surrounding quantum cryptography and shows how combining narratives creates a more balanced, trustworthy story. A more honest and nuanced story helps stakeholder to form informed opinions on the adoption of quantum cryptography.

6.3. Narratives of quantum cryptography

To translate the discussions into recognisable perspectives, six distinct narratives about quantum cryptography are introduced in the form of characters from *Alice in Wonderland*. Each character embodies a symbolic role: urgency, curiosity, confusion, scepticism, authority or realism. They provide a persona for the different narratives. Each narrative connects with different audiences and emphasises different aspects of the technology. The six narratives are based on perspectives that have come up during the research. However, it is possible that there exist more different narratives. To find the full spectrum of different narratives that exist, we recommend more in-depth research that is focused on uncovering this.

The **White Rabbit** embodies the quantum threat narrative. Like the rabbit anxiously checking his pocket watch, this perspective conveys urgency: quantum computers are advancing rapidly, and the security of today's encryption may collapse sooner than expected. This narrative reflects the fear of ”store now, decrypt later” attacks. The urgency makes policymakers, intelligence agencies, and critical infrastructure operators aware of looming deadlines. The effect is to stimulate migration planning and accelerate funding for quantum-resistant solutions, often framed around the arrival of ”Q-day”. We saw this narrative in the background research, mainly in official reports aimed at the security industry (AIVD, 2021; NIST Computer Security Resource Center, 2024; Salem et al., 2023).

The **Caterpillar** represents the technology narrative. Sitting on his mushroom, he keeps asking curious questions. This perspective is about the technical depths of quantum mechanics, how protocols of e.g. Quantum Key Distribution offer provably secure communication, and how hybrid systems might integrate classical and quantum techniques. This narrative appeals to research funders, telecom operators, and technically minded policymakers. If this narrative reaches the right targets who have enough prior knowledge, it can help shaping investments in pilot infrastructures and encouraging debates in standards-setting bodies. This narrative is present closer to the research community. The technical advantages of quantum cryptography, such as possible information-theoretic security, were brought up by the interview participants who are researchers, or who have a quantum background. This narrative is also present in leading review papers about quantum cryptography, such as Pirandola et al. (2019).

The **Mad Hatter** represents the hype narrative, where curiosity tips into exaggeration and confusion. Here, quantum cryptography is promised as a silver bullet: a future where all communications are made absolutely secure through the power of quantum. Grand claims attract media attention, exaggerated headlines and enthusiasm from venture capital investors. The risk is inevitable disappointment when such promises fail to materialise. Confusion about the claims made can result in policy overreaction that makes further development difficult. In the interviews it was noted by executives and civil servants that the current marketing around quantum cryptography uses too much of this narrative, and that the idealism undermines credibility.

The **Cheshire Cat**, appearing and dissolving into thin air again, captures the uncertainty narrative. This perspective stresses ambiguity: no one knows when, or even if, a CRQC will emerge. Predictions range from imminent breakthroughs to a future that may never arrive. For cautious policymakers, auditors, and risk managers, this uncertainty justifies restraint, delaying major investments and encouraging scenario planning over immediate action. We saw this hesitation and uncertainty in the background research into the perspective of the cybersecurity industry on quantum cryptography. The fuzzy deadline of ”Q-day” that was highlighted by e.g. Raskovich et al. (2024) really downplays the urgency narrative.

The **Red Queen** embodies the geopolitics and arms race narrative. This perspective is less about technical feasibility and more about power. Falling behind the US or China in quantum-secure communication is framed as a threat to national sovereignty. For governments and defence ministries, quantum cryptography becomes part of a global race. This justifies large-scale national programmes, alliances, and strategies driven by urgency and prestige. This narrative was brought up by HSD in the exploratory interview for the background study. They said that this narrative resonated with their members. Also the interviewed quantum expert of the AIVD brought up this narrative as a driver for European countries to invest in quantum.

Finally, there is **Alice**, who represents the future and use cases narrative. Through her eyes, quantum cryptography becomes a gateway to new worlds, much like the looking glass in Lewis Carroll's story. Quantum cryptography is a foundation for a future quantum internet connecting quantum computers across continents, enabling applications like blind quantum computing or secure distributed sensing. This vision inspires innovators and research communities. It fuels exploratory funding programmes and shapes policy documents that imagine infrastructures not yet built. This narrative was already brought up in the background study in the interview with the cybersecurity professor, who called quantum cryptographic protocols the ”building blocks” for a future quantum internet. This point was repeated by interview participants from all groups in the interview question about the definition of quantum cryptography.

6.4. Different sides of the story: the dice of quantum cryptography narratives

To illustrate the multiplicity of narratives surrounding quantum cryptography, the design object is a cube, or dice. When observing a dice, one typically sees only a single face, or at most two or three from a certain angle, but never all six at the same time. In the same way, stakeholders rarely perceive the full spectrum of narratives simultaneously. Each viewpoint reveals only part of the whole picture.

Rolling the dice becomes a metaphor for exploring these perspectives. To understand the full story, one must engage with the cube from multiple angles, encountering different narratives in turn. In this design, all six sides have an equal chance of appearing, but in reality, some narratives dominate the public and professional discussion, as was noted by the interviewed executives and civil servants about the hype narrative (Mad Hatter narrative). Likewise, there may be more than six narratives in circulation, but for the sake of clarity and accessibility, the model is distilled into the six characters that are discussed.

6.5. Use as a communication tool

The dice and its narratives form the basis of an interactive communication tool for workshops. The intended setting for this workshop is at conferences where diverse stakeholder groups naturally come together to discuss the future of quantum technologies. A good example is *Quantum Meets* (see quantummeets.com). A conference like this attracts quantum end-users to discover new technologies, quantum businesses to connect with industry and investors, and policymakers to stay informed about industry advancements. This is the right mix of participants to explore how different narratives around quantum cryptography shape perceptions and decisions.

The target audience for the workshop is then those promoting the adoption of quantum cryptography, members of lobbying groups, organisations like Quantum Delta NL, and even quantum cryptography startups. These are the relevant participants for the workshop, as we saw from our problem statement that they are the ones who need to improve their marketing, and to do that improve the framing and narrative. If the workshop is simply present at such a conference, that means that the participants will join voluntarily, based on an interest in the purpose of the workshop.

Workshop "The Dice of Quantum Cryptography Narratives"

Purpose

To make participants aware of the different narratives surrounding quantum cryptography and explore how these narratives affect stakeholders differently. By the end, participants will have a better idea of which narratives are useful, risky, or underused in their own work and how narratives should be combined to create a nuanced and complete story.

Materials

- **Narrative dice**, the six sides are the six Alice-in-Wonderland characters/narratives.
- **Six narratives**, a visual information sheet that explains the six narratives, much like they are explained in Section 6.3. This sheet is included in Appendix C.
- **Prompt cards**, news or paper headlines that function as examples for each narrative, sorted into six piles.
- **Sticky notes**.

Preparation

One participant is chosen to act as a facilitator, but the workshop is simple enough that it can be self-guided with these written instructions.

The participants write stakeholders on the sticky notes that they target with their promotion of quantum cryptography. Recommended is to use the following four categories (just as categories of targets or to come up with stakeholders within the categories):

1. Policymakers and regulators (e.g. intelligence organisations)
2. Industry and infrastructure (e.g. executives, telecommunications companies)
3. Research and innovation (e.g. research funders)
4. Public and media (e.g. general audience, journalists, investors)

Find a surface to put up the sticky notes (table or wall) and choose one side of the surface to represent positive attitude towards adoption and the other side the negative.

Structure (45-60 minutes)

1. Introduction (5 min)
The facilitator explains the idea of the workshop and the dice. Quantum cryptography is surrounded by multiple narratives. Like a dice, you only ever see one side at a time, but one side does not tell the whole story. This may undermine the credibility. Also the six narratives (characters) are introduced. If there is no facilitator, the participants read the information sheet.

2. Discover the narratives (5-10 min)
One participant rolls the dice and comes up with a statement or claim that fits with the narrative of the side of the dice that lands on top. If the participant cannot think of anything they may take a prompt card of the corresponding pile and read it out. Then follows a quick discussion: “Which stakeholder groups would this claim resonate with most? Who might react negatively?” Based on the discussion, the participants move the sticky notes with the stakeholder to a more positive or a more negative attitude towards adoption of quantum cryptography.

For example, the narrative/character that lands on top of the dice is Alice, the future and use cases narrative. The participant comes with the following claim: ”Quantum cryptography will form the foundation of a quantum internet, enabling new applications like blind quantum computing and secure distributed sensing.” This claim will resonate most with the research funders, as it aligns with their long term plans. Policymakers may find this inspiring, but too abstract for immediate decisions. The industry may be encouraged to consider long-term preparations, but may also put the claim aside and focus on more urgent topics. For the media and general public, this claim may be too technical for them to interact. The participants will move the sticky notes to positive and negative attitudes accordingly

Repeat this for 3 rounds.

3. Combine and balance (20-25 min)
Now it is time to combine narratives into a more complete and nuanced story. Participants take turns to roll the dice until two different narratives have landed on top. The participants who rolled the dice will now combine the two narratives to create a joint message. Again it is allowed to use the prompt cards for inspiration. Discuss with the group again how the stakeholders will react to this new message.

Repeat this for 3 or 4 rounds where the amount of times the dice is rolled increases. Thus, the next round the participants need to combine three narratives, then four, five, up to all six.

4. Reflection (15 min)
If the group is larger than four participants, they split up into pairs or trios to reflect. The participants discuss the following questions:

1. Which combination of narratives are most effective for building trust in your context?
2. Which narratives are risky or counterproductive?
3. Were there narratives you had not yet consciously encountered? Which ones?
4. Which narratives and combinations of narratives are worth exploring in your context? Why?

6.6. Validation of the Design

The design has unfortunately not been validated with a test group, because of time constraints.

To validate the design, ideally the workshop should be tested in the intended setting, on a conference, with the intended target audience. For the test workshop, the facilitator should be one of the participants, in order to also test this option of the workshop. For the evaluation, the test workshop is observed and afterwards the participants are asked a set of questions. They are given the questions on a paper questionnaire. After they have filled in the questionnaire, the questions are discussed in the group. This way, the participant will not influence each others answers to the validation questions, but there is still room for discussion afterwards.

There are two sets of questions. The first is about the workshop experience and the second about the validation and if the communication tool achieved its intended purpose.

Questions about the workshop experience:

- Were the rules and purpose of the workshop clear?
- Did you understand the narratives on the information sheet, the role of the dice and the prompt cards?
- How was the pacing? Was the workshop too long, too short, just right?
- Did the use of stakeholder categories make sense, or would you prefer a different grouping?
- To what extent did the game stimulate discussion between participants?
- Did you find the workshop enjoyable?
- Do you think this tool could be useful as workshop in the setting of a conference like Quantum Meets, where participants join the workshop voluntarily? Why or why not?

Questions about the workshop purpose:

- Did you recognise some of the narratives from your
- Do you feel more aware of the different narratives surrounding quantum cryptography after the workshop?
- Did you gain a better understanding of how different narratives affect different stakeholders?
- Did combining two narratives help you see quantum cryptography from a new perspective?
- Were there moments where you felt surprised, challenged, or gained a new insight?
- What do you take away from this workshop?
- What would you change to make it more effective for its intended audience?

7 Conclusion

This thesis set out to explore how the opportunities and challenges of adopting quantum cryptography in the Dutch cybersecurity industry can be understood through insights into stakeholder perceptions and adoption dynamics. While much of the current discourse on quantum cryptography is dominated by technical development, this study has shown that adoption depends on a far broader set of factors, ranging from organisational readiness and business incentives to narratives, perceptions, and drivers and barriers from the industry environment.

The Dutch cybersecurity field is aware of the quantum threat but does not yet treat it with urgency. Perceptions are concentrated on Quantum Key Distribution, with little recognition of other quantum cryptographic possibilities. Quantum is primarily framed as a looming risk rather than an opportunity. In terms of future adoption of quantum cryptography in this industry, this shows that is need for more education and balanced communication.

Adoption dynamics can be understood at three levels: evolutionary, behavioural, and organisational. The Red Queen hypothesis frames cybersecurity innovation as a constant race between attackers and defenders, with quantum computing as a disruptive force in this race. At the behavioural level, Protection Motivation Theory highlights the role of perceived threat and coping ability. At the organisational level, frameworks such as Technology Acceptance Models (TAM), Technology–Organisation–Environment (TOE), and Diffusion of Innovations (DOI) explain how technologies are evaluated, integrated, and diffused. Together, these perspectives emphasise that adoption is not purely technical but shaped by perception, motivation, and context.

Adoption studies of blockchain, AI, and IoT show that no single framework is enough to describe the adoption dynamics around these technologies. The models are instead constructed by combining multiple theories and tailoring them to the specific characteristics of a technology. Following this approach, this thesis proposed a hypothetical adoption model for quantum cryptography built on TAM and TOE, enriched by DOI's technological characteristics. Perceived trust and perceived security are explicitly included given their significance in the other studies and relevance to quantum cryptography.

Interviews with experts revealed that adoption is driven most by the strength of the business case (particularly relative advantage) and by environmental factors such as social influence and government support. Barriers include technological immaturity, cost, compatibility challenges, and organisational knowledge gaps. These factors are deeply interconnected: for instance, technological immaturity undermines relative advantage, which in turn reduces perceived usefulness, while lack of knowledge reinforces scepticism and vulnerability to hype. Experts stressed that adoption will depend on building trust through standards, certifications, and balanced narratives. Crucially, the interviews also revealed a disconnect between the quantum and cybersecurity communities, with each lacking sufficient understanding of the other's domain.

Synthesising these findings, adoption is best understood as a complex interplay of technological, organisational, environmental, business, and personal factors. This complexity is captured in the infographic presented in Appendix B, which visualises interdependencies and stakeholder perspectives, and serves as both a synthesis and a decision-support tool.

Practical implications

The findings have concrete implications for practice:

- For developers of quantum cryptography, future adoption requires more than technical depth and strength. More attention must be given to usability, compatibility, business incentives, and the trust of end-users. Bridging knowledge gaps with the cybersecurity industry is essential and most importantly, goes both ways. More education about the opportunities of quantum cryptography for the cybersecurity industry is needed, but also more true understanding of the cybersecurity industry and the complexity of security systems is needed in order to make fitting quantum solutions.
- For advocates and policymakers, standards, certifications, and balanced narratives are crucial to encouraging adoption. Narratives should highlight both opportunities and limitations, avoiding moving into hype and unrealistic claims.
- For the broader discussion on emerging technologies, the case of quantum cryptography reinforces that adoption dynamics depend on organisational and environmental factors as much as on technological progress.

The proposed design, the Dice of Quantum Cryptography Narratives, directly addresses these communication challenges. By making visible the multiplicity of narratives and encouraging stakeholders to explore them in combination, it helps to correct the current one-sided storytelling and supports more informed, trustworthy decision-making.

Directions for future research

This thesis contained an exploratory study of the adoption of quantum cryptography in the Dutch cybersecurity industry and opens up several directions for further work. One clear path is the quantitative validation of the proposed adoption model through larger-scale surveys, which would allow testing the relative weight and interactions of the identified factors across a broader set of stakeholders.

Beyond validation, another direction can be longitudinal studies that track how perceptions of quantum cryptography evolve over time as quantum computing progresses and quantum cryptography pilot projects are implemented. This will be interesting, as quantum cryptography is still relatively unknown, but developing rapidly. A study like this will track perceptions alongside technical developments.

Since this thesis only focused on the Dutch cybersecurity industry, An international comparison would also be valuable, as adoption dynamics are likely to differ between national contexts with varying levels of quantum investment, regulation, and infrastructure readiness.

The role of hype and lobbying, and the effect of narratives on policy and investment deserves further investigation. Before this can be studied in depth, more research is needed to identify which narratives are currently circulating in industry, policy, and media spheres, since the narratives proposed in this research and design are only informed by patterns that emerged during the research. A dedicated research into these narratives to group and classify them, is recommended.

The impact of standards and certification on adoption is another important area. Questions remain about how the timing, content, and enforcement of standards affect trust, investment decisions, and the willingness of organisations to experiment with quantum technologies.

Finally, the adoption dynamics infographic in Appendix B contains more starting points for designs and further research. In the design in this thesis, only one path of the infographic was explored, but many more paths are possible to explore how different lines of influence can be mapped, communicated, and tested in practice. Such research would help bridge the gap between theoretical adoption models and actionable tools for stakeholders.

8 Discussion

This chapter reflects on the findings and limitations of the study, as well as the methodological choices that shaped its outcomes. As this research aimed to provide an exploratory perspective on the adoption of quantum cryptography in the cybersecurity industry, it is important to consider both the strengths and the boundaries of what can be concluded from the results.

Reliability, generality, and validity

The most important limitation of this research is the small and heterogeneous dataset of the interviews: twelve experts with different backgrounds participated. In comparison, most studies that aim to build adoption models for a given technology, formulate a hypothesis based on literature and expert insights, and then test it with large-scale surveys. This thesis covers primarily the first step: hypothesis-building. As such, the model proposed here should be regarded as exploratory rather than definitive. Repeating this research with a new group of experts could well produce different factors or factor weightings. Nevertheless, in the absence of other studies attempting an adoption model for quantum cryptography, the exploratory nature of this project is a valuable first step.

The generality of the findings is also limited by the scope of the sample. The participants were all based in the Netherlands and, once divided into groups, consisted of only three to four experts per group. This is not sufficient for broad generalisation, but the sample did represent a meaningful cross-section of professionals, researchers, executives, and civil servants. For an exploratory study, this was enough to identify relevant adoption factors and stimulate discussion, though future work would benefit from a larger dataset. It also has to be noted that the outcomes in the final design are very bound the Netherlands and the Dutch landscape of cybersecurity. Repeating this study in a different county will give different results.

In terms of validity, several results were consistent with expectations drawn from existing literature. Factors such as trust, complexity, and transparency were highlighted, as well as cost, which emerged as the strongest negative driver. This role of costs was also visible in the hypotheses of the studies in the literature, although most of them found costs to be insignificant in later validation through surveys. The differences between groups also aligned with anticipated patterns: participants with a quantum background tended to focus more on technical factors and downplay complexity, while cybersecurity experts emphasised organisational and environmental barriers. These findings suggest that the research captured some real and meaningful distinctions. However, it must be noted that because of the limited existing literature and small dataset, the expectations were necessarily open-ended.

Scope of the research

The decision to focus on the cybersecurity industry shaped the project in important ways. Although cybersecurity organisations are logical potential adopters, they are not the only ones. Some participants pointed out that end users, such as critical infrastructure providers, may ultimately procure quantum cryptography systems directly from vendors rather than via established cybersecurity firms. At the same time, the results from study also suggests that adoption through existing cybersecurity providers may offer advantages, since these organisations already have reputational trust with their clients. A more detailed mapping of the cybersecurity landscape, including vendors and end users, could have strengthened the justification of the chosen scope. Nonetheless, the focus on cybersecurity was useful for narrowing the project and engaging with a sector likely to play a central role in future adoption.

The research, and mainly the interviews, focus broadly quantum cryptography, even though this term is used for a collection of different technologies. We could have focused on QKD, but there are already a lot of publications about QKD. We could have focused two party quantum protocols, to align with the applied physics thesis, but from the background interviews it was clear that this was so unknown, it would be useless to ask about it.

In formulating the narratives in the design, we again deviated a bit from the scope of quantum cryptography in the White Rabbit narrative, which is actually about the threat from quantum computers, and in the Alice narrative, which is more broadly about quantum communication and quantum internet. These deviations show exactly the point of having a complete narrative. They show that only talking about quantum cryptography and its pure security-based opportunities is too limiting. To give an honest and complete narrative we had to include the context of quantum cryptography, the quantum threat and quantum communication as well.

Reflections on methodology

A systematic literature review on the adoption models of technologies that are comparable to quantum cryptography is not ideal, since the results will not fully align with the research objective. This meant that there was need for interpretations, which inevitably impacts the reliability. However, since there is no prior research into adoption models for quantum cryptography, this was chosen as the best option for a systematic literature review. We would like to add here some insights from a paper published after the completion of the literature review. Panteli (2025) advocates that organisations should not wait for quantum technologies to fully mature but must already start on ”quantum readiness”. By this they mean preparing not technically for a new innovation, but also on organisational, governance and ecosystem (environmental) contexts. This aligns well with what we concluded from the literature review regarding adoption of quantum cryptography.

Then to expand and validate the adoption model, we interviewed experts. The use of qualitative interviews gave rich and detailed insights that allowed for a nuance which a survey would not have captured. Several participants commented that they had never thought about the questions posed before, and many appreciated the opportunity to reflect on them. This indicates that the interview design not only gathered data but also stimulated reflection among experts themselves. A focus group could have enabled further discussion between experts, as one participant suggested, but coordinating such a session would have been logistically difficult. The interviews did, however, serve as effective conversation starters. This purpose can be continued with the final design of this study.

The interview design evolved over the course of the study. After the first interview, several changes were made.

- The descriptions on the factor cards were tailored more specifically to quantum cryptography and cybersecurity professionals, to eliminate general formulations and to take away one step from the thought process of the participants.
- The background question about the job description and expertise of the participants was made more structured by introducing a two-dimensional chart.
- A new factor, ”lobbying group,” was added, according to the suggestion of the first interview participant.
- the categories ”neutral” and ”not important” were distinguished to capture more nuance, when dividing the factor cards into piles of driver and barrier or other.

These adjustments improved clarity and reduced ambiguity for participants.

Even so, some challenges remained. For instance, the two-dimensional spectrum asking participants to position themselves between quantum and cybersecurity, and between strategic and operational focus, often resulted in placements along the axes, reflecting their interdisciplinary work. This made grouping participants for analysis more interpretative than intended. In the end, I categorised participants into researchers, professionals, executives, and civil servants, with roughly equal numbers from quantum and cybersecurity backgrounds. In hindsight, it might have been easier to ask participants to indicate, for example, what proportion of their time is spent on quantum cryptography, thereby producing a clearer division.

The task of ranking adoption factors also raised difficulties. Participants were asked to order factors by importance, but this produced lists of varying lengths that were challenging to compare. A point-allocation method, such as distributing ten points among the factors, would have generated more consistent results, even if still only relative per participant. Furthermore, while I interpreted links between factors from the interview conversations, explicitly asking about such relationships could have given richer insights and reduced the reliance on interpretation.

Finally, some participants found it difficult to distinguish between drivers and barriers, despite explanations. This sometimes led to factors being placed in the ”wrong” pile. The interview transcripts then provided enough context to recover their intended meaning. Overall, the qualitative format proved its worth here: such nuances would likely have been lost in a purely quantitative approach.

The findings of the research resulted ultimately in an infographic that maps the adoption factors, their relations and interactions, and the expect perspectives on them. It is presented as both a synthesis of findings and a decision-support tool. A pitfall of this infographic, however, that it is still very complicated to read and will therefore not be easy to use.

Reflections on the design outcome

To focus the overwhelming information of the infographic, the design revolves in essence around only one of the factors, narrative. This is however a critical factor that has come up during the research multiple times, often in combination with hype, marketing and knowledge gaps.

In the design we formulated six narratives. This number and these narratives are merely based on observations during the research. A more thorough foundation for grouping and categorising narratives would have been better. For example, Meinsma et al. (2024) did do a similar research into the effect of frames on engagement with quantum technology. The method by which they establish the tested frames, could be used here as well to formulate narratives.

The workshop outline mentions four stakeholder groups, including research and public/media. It should be noted that these groups are not considered as potential adopters of quantum cryptography in the rest of this thesis. Still, they are included as stakeholder groups, since their perceptions on the adoption of quantum cryptography will contribute to the full ecosystem. Including a wide variety of stakeholders in the workshop that the participants can use to sympathise with, will help with understanding the impacts that narratives and combinations of narratives have.

Concluding remarks

In this thesis we presented a comprehensive infographic that reflects the complex interplay of technological, organisational, environmental, business, and personal factors that shape the adoption dynamics of quantum cryptography. These factors and relations are annotated by the perceptions of the interviewed experts. We also designed a communication tool that focuses on one aspect of this infographic, the narratives that ultimately influence perceived trust, which impacts the adoption intention. This communication tool is targeted at those who promote the adoption of quantum cryptography. It has to be noted that the author of this thesis is actually a part target group.

In the applied physics thesis (van Mil, 2025) we investigated a class of quantum cryptographic protocols and the motivation for this thesis was to explore how these would be perceived and ultimately adopted in the cybersecurity industry. For that reason, there is a significant risk of bias in the way the findings are presented and which aspects are highlighted in the design. On the other hand can it be argued that the resulting tool has a high chance of being relevant and usable for its intended audience.

Apart from that, the results of this thesis gave some valuable takeaways regarding the motivation with which we started. It has really helped to put the technical thesis into context. We can conclude, for example, that the technical thesis is framed from the Caterpillar and Alice narratives, focusing on technical depth and building foundations for future applications and protocols. Since most of the interviewed experts adopted an Alice narrative when defining quantum cryptography, we can say that this framing is justified for the technical thesis.

References

Agustini, A. T., & Mustakini, J. H. (2025). A systematic literature review of blockchain technology and accounting issues: Is it a hype or hope? *South African Journal of Accounting Research*, *39*(1), 73–107. https://doi.org/10.1080/10291954.2024.2371616

AIVD. (2021). *Bereid je voor op de dreiging van quantum-computers* (tech. rep.). Algemene Inlichtingen- en Veiligheidsdienst, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers

Alshamsi, M., Al-Emran, M., & Shaalan, K. (2022, May). A systematic review on blockchain adoption [n = 30 quantitative systematic reviewPrevailing theories/models TAM > TOE > UTAUT > IDT/-DOImost frequent external factors in paper, but without description. identifies three different concepts within the technology adoption domain: adoption, acceptance, post-adoption/continuous intention.]. https://doi.org/10.3390/app12094245

Anderson, R. (2001). Why information security is hard - an economic perspective. *Seventeenth Annual Computer Security Applications Conference*, 358–365. https://doi.org/10.1109/ACSAC.2001.991552

Assaf, R., Omar, M., Saleh, Y., Attar, H., Alaqra, N. T., & Kanan, M. (2024). Assessing the acceptance for implementing artificial intelligence technologies in the governmental sector an empirical study. *Engineering, Technology and Applied Science Research*, *14*, 18160–18170. https://doi.org/10.48084/etasr.8711

Berger, C. R., & Calabrese, R. J. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research*, *1*(2), 99–112. https://doi.org/10.1111/j.1468-2958.1975.tb00258.x

Bhardwaj, A. K., Garg, A., & Gajpal, Y. (2021). Determinants of blockchain technology adoption in supply chains by small and medium enterprises (smes) in india. *Mathematical Problems in Engineering*, *2021*. https://doi.org/10.1155/2021/5537395

Carroll, L. (2010). Through the looking-glass. In *Alice's adventures in wonderland & other stories* (pp. 151–152). Barnes & Noble / Sterling Publishing (Leatherbound Classics).

Chittipaka, V., Kumar, S., Sivarajah, U., Bowden, J. L. H., & Baral, M. M. (2023). Blockchain technology for supply chains operating in emerging markets: An empirical examination of technology-organization-environment (toe) framework. *Annals of Operations Research*, *327*, 465–492. https://doi.org/10.1007/s10479-022-04801-5

Christensen, C. M. (1997). *The innovator's dilemma*. Harvard Business Review Press.

Dainton, M., & Zelley, E. D. (2010, April). Theory of planned behaviour. In *Applying communication theory for professional life; a practical introduction* (4th ed., pp. 127–129). SAGE Publications.

Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information* (tech. rep.).

IBM. (2023, December 1). *What is quantum cryptography?* Retrieved December 17, 2024, from https://www.ibm.com/topics/quantum-cryptography

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/https://doi.org/10.1016/j.cose.2011.10.007

Koyluoglu, A. S., & Acar, O. E. (2023). A study on adoption of artificial intelligence use in mobile banking. *EMC Review - Časopis za ekonomiju - APEIRON*, *26*. https://doi.org/10.7251/emc2302344k

Kuberkar, S., & Singhal, T. K. (2021). Factors influencing the adoption intention of blockchain and internet-of-things technologies for sustainable blood bank management. *International Journal of Healthcare Information Systems and Informatics*, *16*. https://doi.org/10.4018/IJHISI.20211001.oa15

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of smb executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Lindsay, J. R. (2020). Demystifying the quantum threat: Infrastructure, institutions, and intelligence advantage. *Security Studies*, *29*, 335–361. https://doi.org/10.1080/09636412.2020.1722853

Majrashi, K. (2024). Determinants of public sector managers' intentions to adopt ai in the workplace. *International Journal of Public Administration in the Digital Age*, *11*, 1–26. https://doi.org/10.4018/ijpada.342849

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. https://doi.org/10.14569/IJACSA.2018.090354

McKinsey. (2024, April). Quantum technology monitor.

Meinsma, A. L., Albers, C. J., Vermaas, P., Smeets, I., & Cramer, J. (2024). The effect of frames on engagement with quantum technology [recommended by Julia. reached the participants through kieskompas.nl].

NIST Computer Security Resource Center. (2024). *Post quantum cryptography*. Retrieved December 17, 2024, from https://csrc.nist.gov/projects/post-quantum-cryptography

Norbu, T., Park, J. Y., Wong, K. W., & Cui, H. (2024, March). Factors affecting trust and acceptance for blockchain adoption in digital payment systems: A systematic review. https://doi.org/10.3390/fi16030106

Panteli, A. (2025). White paper: Quantum readiness—strategic imperatives for enterprise organisations. *European Journal of Business and Management Research*, *10*(3), 144–151. https://doi.org/10.24018/ejbmr.2025.10.3.2705

Park, Y. J., & Jones-Jang, S. M. (2023). Surveillance, security, and ai as technological acceptance. *AI and Society*, *38*, 2667–2678. https://doi.org/10.1007/s00146-021-01331-9

Picoto, W. N., Abreu, J. C., & Martins, P. (2023). Integrating the internet of things into e-commerce: The role of trust, privacy, and data confidentiality concerns in consumer adoption. *International Journal of e-Business Research*, *19*. https://doi.org/10.4018/IJEBR.321647

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2019). Advances in quantum cryptography. *arXiv*, 1–118. https://doi.org/10.1364/aop.361502

Port of Rotterdam - News Overview. (2024, May). https://www.portofrotterdam.com/en/news-and-press-releases/consortium-parties-first-world-build-scalable-quantum-internet-connection

Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2023). Adoption of artificial intelligence in banking services: An empirical analysis. *International Journal of Emerging Markets*, *18*, 4270–4300. https://doi.org/10.1108/IJOEM-06-2020-0724

Rana, M. M., Siddiqee, M. S., Sakib, M. N., & Ahamed, M. R. (2024). Assessing ai adoption in developing country academia: A trust and privacy-augmented utaut framework. *Heliyon*, *10*. https://doi.org/10.1016/j.heliyon.2024.e37569

Raskovich, K., Briggs, B., Bechtel, M., & Burns, E. (2024, December). *Quantum computing and cybersecurity* (D. Insights, Ed.). https://www2.deloitte.com/us/en/insights/focus/tech-trends/2025/tech-trends-quantum-computing-and-cybersecurity.html

Ribeiro, J., & Wehner, S. (2020, April). On bit commitment and oblivious transfer in measurement-device independent settings [Use of Bell measurements for MDI communications].

Roberson, T., Leach, J., & Raman, S. (2021). Talking about public good for the second quantum revolution: Analysing quantum technology narratives in the context of national strategies. *Quantum Science and Technology*, *6*. https://doi.org/10.1088/2058-9565/abc5ab

Rogers, E. M. (1983). *Diffusion of innovations* (3rd ed.). The Free Press; A Division of Macmillan Publishing.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change [PMID: 28136248]. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Russo, D. (2024). Navigating the complexity of generative ai adoption in software engineering. *ACM Transactions on Software Engineering and Methodology*, *33*. https://doi.org/10.1145/3652154

Salem, E., Ojha, S., & Meyers, A. (2023, July). *Security in a post-quantum world* (B. C. Ventures, Ed.). https://baincapitalventures.com/insight/security-in-a-post-quantum-world/

Sciarelli, M., Prisco, A., Gheith, M. H., & Muto, V. (2022). Factors affecting the adoption of blockchain technology in innovative italian companies: An extended tam approach. *Journal of Strategy and Management*, *15*, 495–507. https://doi.org/10.1108/JSMA-02-2021-0054

Shrestha, A. K., Vassileva, J., Joshi, S., & Just, J. (2021). Augmenting the technology acceptance model with trust model for the initial adoption of a blockchain-based system. *PeerJ Computer Science*, *7*, 1–38. https://doi.org/10.7717/PEERJ-CS.502

Smith, F. L. (2020). Quantum technology hype and national security [Has the quantum hype reached national security? Is national security influenced by hype?]. *Security Dialogue*, *51*, 499–516. https://doi.org/10.1177/0967010620904922

Tornatzky, L. G., & Fleischer, M. (1990). *The process of technological innovation*. Lexington Books.

Vaishnavi, A., & Pillai, S. (2021, July). Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. https://doi.org/10.1088/1742-6596/1964/4/042002

van Mil, J. (2025). *Quantum secure function evaluations with real-world devices* [MSc thesis]. TU Delft. https://resolver.tudelft.nl/uuid:b3bd61ad-8fba-4c7b-9327-d53490514ae8

Van Valen, L. (1973). A new evolutionary law. *Evolutionary Theory*, *1*, 1–30.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Quarterly*, *27*, 425–478.

Verhagen, P., Frinking, E., Kattenbroek, L., & Attema, T. (2019, September). Understanding the strategic and technical significance of technology for security.

Vidick, T., & Wehner, S. (2023, September). *Introduction to quantum cryptography*. Cambridge University Press. https://doi.org/10.1017/9781009026208

Vorm, E. S., & Combs, D. J. (2022). Integrating transparency, trust, and acceptance: The intelligent systems technology acceptance model (istam). *International Journal of Human-Computer Interaction*, *38*, 1828–1845. https://doi.org/10.1080/10447318.2022.2070107

Wehner, S., Elkouss, D., & Hanson, R. (2018, October). Quantum internet: A vision for the road ahead. https://doi.org/10.1126/science.aam9288

Yang, H., Zhang, Z., Jian, C., & Ahmad, N. (2025). Exploring real estate blockchain adoption: An empirical study based on an integrated task-technology fit and technology acceptance model. *PLoS ONE*, *20*. https://doi.org/10.1371/journal.pone.0317993

Zhang, X., Yue, ; & Lee, S. Y. (2023). A research on users' behavioral intention to adopt internet of things (iot) technology in the logistics industry: The case of cainiao logistics network. *Journal of International Logistics and Trade*.

A

Supplementary materials for the interviews

This appendix is a guide to the supplementary materials regarding the interviews. These include:

- Informed consent form
- Interview script
- Picture of example interview outcome
- Code tree

The informed consent form and interview script are self explanatory. The picture of an example interview outcome shows an example of how the factor cards might be arranged at the end of an interview. These pictures are used as data outcomes from the interviews.

The analysis and coding of the interview transcripts was based on a hybrid process of thematic coding combined with in vivo coding. See the code tree for the codes and code families that were used in the thematic coding. Coding of the interviews was done in two stages. For each stage the entire transcript was covered. The first stage is to code all of the content of the participants responses. Codes from the A, B and C branches are used. The second stage investigates the interrelationships between the backgrounds of the experts, the context that has been created in the introduction and part 1, and the answers they give in part 2. This is done with codes from branch D. Codes from the stem are meta comments on the interview itself and elements of the interview that are coded in the first or second pass.

The 17 factors and their descriptions on the cards are:

(Personal context, red cards)

- **Perceived Usefulness** How much a cybersecurity professional believes that using quantum cryptography will improve the way they protect sensitive information.
- **Perceived Ease of Use** How much a cybersecurity professional believes that implementing and using quantum cryptography will be straightforward and not overly complicated.
- **Perceived Trust** How much a cybersecurity professional trusts that quantum cryptography and its providers are reliable, ethical, and will perform as expected.
- **Perceived Security** How much a cybersecurity professional believes that quantum cryptography is protected against unauthorised access or attacks.

(Technical context, blue cards)

- **Relative Advantage** How much quantum cryptography is seen as an improvement over existing encryption and security methods.
- **Compatibility** How well quantum cryptography fits with the current needs, practices and values of organisations and security teams.
- **Complexity** How hard or easy it is to understand, implement and use quantum cryptography.

- **Trialability** How easily quantum cryptography can be tested or experimented with on a small scale before full adoption.
- **Observability** How clearly the benefits and results of using quantum cryptography can be seen by others.

(Environmental context, yellow cards)

- **Social Influence** How much a cybersecurity professional feels encouraged by colleagues, managers or industry leaders to use quantum cryptography.
- **Government Regulations** How much laws and official rules affect the decision to adopt and use quantum cryptography.
- **Vendor Support** How much help, training and maintenance technology providers offer to make sure quantum cryptography is used successfully.
- **Lobbying Group** How much groups that bridge academia, industry and government affect the decision to adopt and promote quantum cryptography

(Organisational context, green cards)

- **Facilitating Conditions** How much a cybersecurity professional believes their organisation has the systems and support needed to use quantum cryptography.
- **Cost** How much money is believed to be needed to buy, set up and keep using quantum cryptography.
- **Organisation Size** How the size and resources of an organisation affect its ability to adopt and manage quantum cryptography.
- **Cultural Readiness for Change** How open and supportive an organisation's culture is toward trying new technologies like quantum cryptography.

B

Infographic: Adoption Factors of Quantum Cryptography and their Interactions

See supplementary materials for the infographic synthesising expert perspectives on adoption factors for quantum cryptography in the Dutch cybersecurity industry. Factors are shown as nodes connected by arrows that indicate influence, and grouped into coloured clusters representing five analytical contexts: technological, organisational, environmental, personal, and business case. Each cluster is marked as positive, negative, or mixed depending on expert views. Stakeholder perspectives are represented through speech bubbles, with icons indicating the role (government, professionals, executives, researchers) and background (quantum cryptography or cybersecurity) of the speaker. Legends provide explanations for the cluster colours and stakeholder icons.

C

The Dice of Quantum Cryptography Narratives

See supplementary materials for the information sheet that specifies the six narratives on the sides of the Dice of Quantum Cryptography Narratives. This sheet visualises the communication design and functions as a tool for the workshop described in Chapter 6.