Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Michaela Králová

Post-Quantum Password-Authenticated Key Exchange

Master's thesis in Digital Infrastructure and Cyber Security
Supervisor: Tjerand Silde
January 2026

NTNU
Norwegian University of Science and Technology

Michaela Královú

Post-Quantum Password-Authenticated Key Exchange

Master's thesis in Digital Infrastructure and Cyber Security
Supervisor: Tjerand Silde
January 2026

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Norwegian University of
Science and Technology

Post-Quantum Password-Authenticated Key Exchange

Michaela Královová

Submission date: January 2026
Main supervisor: Associate Professor Tjerand Silde, NTNU

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Problem description

Most online services require a username and password to authenticate users when logging in. This is usually handled in the following way:

1. The user creates a fresh TLS connection with the server
2. The user sends their password to the server over TLS
3. The server checks if it matches the password in the database

This approach has several weaknesses, such as the server seeing all passwords in plaintext sent from the user whenever someone tries to log in. While alternatives such as FIDO exist, which rely on public key cryptography and trusted devices, passwords are here to stay, and we need better ways to protect the authentication process.

A promising solution is password-authenticated key exchange (PAKE), where the user never sends the password to the server but instead performs a key exchange with the server using a mapping of the password as input. If the password is correct, the key exchange is successful, and the parties have consequently derived a shared key for secure communication. However, there are various PAKE protocols in the literature, with many different properties and tradeoffs, and several implementations are available online. A survey is available [HV22].

This project concerns post-quantum PAKE protocols. The goal is to classify the current quantum-resistant constructions with respect to the properties achieved by the classical protocol, which are not secure against quantum computers. Furthermore, the goal is to compare the security and efficiency of the currently available post-quantum PAKE protocols in the literature and present open problems requiring further research.

Approved: 2025-08-20 – Associate Professor Tjerand Silde, NTNU (Main supervisor)

Abstract

Most online services require a password when users log in. While alternatives exist, password-authenticated key exchange (PAKE) protocols enable secure authentication and key establishment based on shared passwords without ever transmitting them in plaintext. However, the advent of quantum computing threatens classical cryptographic schemes, including existing PAKEs, requiring the development of quantum-resistant alternatives.

This work presents a systematic literature review of post-quantum password-authenticated key exchange protocols. We identified and analyzed 29 protocols from 23 papers published between 2017 and 2025, categorizing them by cryptographic foundations, security properties, performance characteristics, and implementation status. Our analysis reveals that lattice-based cryptography dominates the field, with 18 protocols relying on variants of the Learning with Errors problem. Code-based and isogeny-based approaches represent smaller but important alternatives for cryptographic diversity. Furthermore, when picking out important existing post-quantum PAKEs, the Compact Half-Ideal Cipher (Arriaga et al., ASIACRYPT 2024) emerged as the most efficient construction with microsecond-level execution times, while protocols like Ouroboros-based PAKE (Wang et al., Security and Communication Networks 2022) and a PAKE based on Module Learning with Errors (Ren and Gu, ICISC 2021), offer strong quantum security guarantees.

We also identified significant challenges facing the field, including inconsistent reporting, lack of standardized benchmarking, continued reliance on classical security models, and a substantial gap between theoretical proposals and practical implementations. The review highlights several critical directions for future research: diversifying cryptographic foundations beyond lattice-based approaches, establishing standardized evaluation methodologies, extending security proofs to quantum adversary models, developing protocols for resource-constrained environments, and exploring hybrid constructions. Our findings provide a baseline for future research in the field and enable a smoother adoption process for post-quantum password-authenticated key exchange protocols.

Preface

This Master's thesis was written under the Department of Information Security and Communication Technology at the Norwegian University of Science and Technology as a part of the study program Digital Infrastructure and Cyber Security during the autumn semester of 2025. The idea for this thesis originated from my supervisor, Tjerand Silde, and the intended audience comprises cryptography researchers and experts, as well as readers with a keen interest in post-quantum cybersecurity.

I would especially like to thank Associate Professor Tjerand Silde for his expertise, advice, and patience throughout the writing of this thesis. His support for my interest in the field, including the invitation to the Cryptology and Social Life Workshop 2025, was invaluable for both the completion of this thesis and my growing interest in cryptography and cybersecurity.

Contents

List of Figures

List of Tables

List of Acronyms

EKE Encrypted Key Exchange.

IoT Internet of Things.

KEM Key Encapsulation Mechanism.

KEX Key Exchange Mechanism.

NIST National Institute of Standards and Technology.

OPRF Oblivious Psuedorandom Function.

PAKE Password-Authenticated Key Exchange.

PQC Post-Quantum Cryptography.

SoK Systematization of Knowledge.

Chapter 1
Introduction

Today, secure communication forms the backbone of modern society. From online banking to healthcare records, from private messaging to critical infrastructure, cryptographic protocols protect our society's most sensitive information. However, this foundation faces a new challenge: the advent of quantum computing which may render many of our current cryptographic schemes obsolete.

In practice, Password-Authenticated Key Exchange (PAKE) protocols are used in modern authentication and secure communication, enabling key establishment based on low-entropy passwords. PAKE is deployed at scale in systems supporting credential recovery, end-to-end secure channel establishment, and device pairing on widely used platforms such as WhatsApp and iCloud [HV22]. As a result, there is a clear need for the development and identification of quantum-safe PAKE protocols suitable for secure deployment.

Our work addresses a gap in our preparation for the quantum future by conducting a comprehensive literature review of post-quantum PAKE protocols. As organizations and governments worldwide begin transitioning to quantum-resistant cryptography, understanding the landscape of available solutions becomes even more important. This work aims to provide other researchers with a structured overview of post-quantum PAKE schemes, their security properties, and their practical applicability.

1.1 What is the Quantum Threat?

In 1970, the New York Times published an article [Por70] on the advent of computers and their ability to solve problems which were previously impossible to tackle for humans alone. The author, Dr. Porter, says: "The computer today holds enormous potential for people determined to find solutions to mankind's most pressing problems - an exploding world population, hunger, disease, urban misery, crime, environmental pollution, natural disasters, inflationary economies and mass education." While expectations were high regarding what this breakthrough encompassed, the path to

making it truly useful for humanity was far less clear. The challenges that would inevitably arise in integrating computers into both research and daily life were not even acknowledged in the column. As we now know, many of the world's problems described are still present and have been fundamentally transformed due to the rapid growth of technology, beyond the computer. That is to say, Dr. Porter was halfway correct - the opportunities were great, but so were the threats.

Just about half a century later, in 2019, the New York Times posted an online article [Gor19] on quantum computing. Naturally, technology had evolved quite a bit by then, though the words used to describe it were no different in terms of level of grandiose: "The achievement[1], if real, could presage a revolution in how we think, compute, guard our data and interrogate the most subtle aspects of nature." While the article, in many ways, resembled Dr. Porter's, the tone surrounding opportunities and threats of a potential quantum computer was more sober. The article dedicated a few paragraphs to the discussion of how a powerful enough quantum computer could be potentially used to break classical cryptographic schemes but also mentioned that the further development of such a computer is still hazy and uncertain. Despite the speculations, the message was clear: we might be close to a big change.

Almost half a decade later, a group of Chinese researchers claimed to have broken 50-bit RSA encryption [All24]. While this claim has yet to be replicated by others and should not cause immediate panic, it does constitute a proof-of-concept confirming that brand new cybersecurity threats are incoming. Meanwhile, other researchers have now produced estimates for the timeline at which quantum computers will become powerful enough to compromise cryptographic schemes currently in use, such as 2048-bit RSA [Jaq25]. It seems that the big change may be coming soon.

Taking a short diversion away from the news, it is important to explain why quantum computers are surrounded by high expectations as well as some fear and mystery. The cryptographic threat that the 2019 article alludes to is not merely speculative but stems from a concrete mathematical breakthrough achieved decades earlier. In 1994, mathematician Peter Shor published an algorithm [Sho97] that could efficiently solve the integer factorization problem and the discrete logarithm problem using a quantum computer. These problems form the mathematical foundation of virtually all public-key cryptography used today, including RSA encryption [RSA78] and the Diffie-Hellman key exchange [DH76] that underlies today's secure communication over the internet. Even if large-scale quantum computers are not available just yet, adversaries could collect encrypted data today and store it until quantum computers become available to decrypt it, the so-called "Harvest Now, Decrypt Later" strategy. For information requiring long-term confidentiality, like medical or financial

[1]Referring to a (later-removed) paper published on NASA's website on an execution run on a quantum computer.

data, this means that quantum-resistant protection must be implemented as soon as possible.

Recognizing the importance of this challenge, the National Institute of Standards and Technology (NIST) began developing and standardizing quantum-resistant cryptographic algorithms [Nat24b] in 2016. While this process is still ongoing, in August 2024 the first post-quantum cryptographic algorithms were published. As of June 2025, the European Commission published an implementation roadmap [Eur25] for transitioning Member States to post-quantum cryptography, with the beginning already scheduled for the end of 2026. The goal is for all high-risk systems, like critical infrastructure, to have been transitioned to post-quantum cryptography by 2030 and the remaining infrastructure undergoing the same transition by 2035.

All in all, if there was ever a time to coordinate knowledge and review existing literature in order to aid the upcoming (and already ongoing) transition as well as research into post-quantum cryptography, it would be now. As such, we position our work as research which aims to improve the future resistance to quantum computing and allows other researchers to build their work off of our findings.

1.2 Password-Based Authentication

In the digital age, passwords are everywhere. Despite the rise of biometrics, hardware tokens, and password managers, many online systems still rely on a shared low-entropy password between clients and servers. Humans like passwords because they are easy to remember and universally understood. But from a cryptographic point of view, passwords are often short, reused, and vulnerable to brute-force attacks. Worse yet, if sent directly over the network or stored improperly on a server, they can become an easy entry point for attackers.

There are a number of ways passwords can be used to authenticate users. The Password Authentication Protocol [Sim92], PAP, relies on a client sending their password to a server, which accepts or rejects it. In PAP, passwords are sent in plaintext and have no proper security measures against replay attacks or similar threats. The more complex version, Challenge-Handshake Authentication Protocol [Sim92], CHAP, is based on a three-way handshake in which a “challenge” is sent to the client by the server. The client then calculates a hash function and sends back the result, which is then matched against the expected value by the server. CHAP protects the password in transit and is overall more complex than PAP, though both protocols are mainly used in legacy systems at this point.

That is where Password-Authenticated Key Exchange (PAKE) steps in. PAKE protocols allow two parties to establish a shared cryptographic key over an insecure

channel, using only a password [HV22]. In some variants this can be done without ever transmitting the password itself or relying on external public-key infrastructure. At the same time, some instantiations of PAKE can provide mutual authentication between the server and client, where PAP, for example, only authenticates the client to the server. This makes PAKE incredibly valuable, not just for user-facing systems like cloud logins and secure messaging, where it is already used, but also for more constrained use cases like the Internet of Things (IoT) [RG21]. With PAKE, authentication and secure key exchange can happen based on something as lightweight as a pre-installed password or PIN, without the need for digital certificates or trusted third parties.

That being said, PAKE has so far not been utilized as widely as might be expected, partially because of missing elegant implementations on hand and other methods of establishing shared keys simply being more straightforward while offering similar security guarantees [Gre18]. At the same time, very few PAKEs have been standardized by the Internet Engineering Task Force (IETF), which has further prevented wide usage.

Nevertheless, the advent of quantum computers will mean that widely used cryptographic schemes have to get replaced with post-quantum variants and, perhaps, now would be time to give PAKE another chance. Therefore, this work presents a literature review that will discuss and compare the potential post-quantum PAKE solutions that can guarantee a secure quantum future.

1.3 Our Contributions

With our work, we make the following contributions to the field of post-quantum cryptography and password-authenticated key exchange:

- **Comprehensive and Comparative Literature Review**: We provide a systematic review of existing post-quantum PAKE protocols. The results of the review are used to compare different post-quantum PAKE schemes based on their security properties, computational efficiency, and practical applicability.
- **Protocol Readiness and Deployment**: We select the most promising of the identified protocols and provide details of their readiness for real-world deployment, considering details like implementation complexity and performance.
- **Research Gap Identification**: We identify open problems in the field and provide clear directions for future research in post-quantum PAKE.

These contributions meant to be a consolidated resource for understanding the current state of the post-quantum PAKE research and advancing it.

1.4 Thesis Organization

Our work is organized into chapters that closely follow the structure of a standard literature review. We begin by placing the thesis within a broader context, outlining its objectives and linking them to current sustainability goals as well as providing an overview of related works in Chapter 1. Next, we introduce the field of post-quantum cryptography and various security models, providing all relevant details in Chapter 2, followed by Chapter 3, which details the methodology used to conduct our literature review. The results of the review are presented comprehensively in Chapter 4 and discussed in depth in Chapter 5. Drawing on these findings, Chapter 6 outlines potential areas for future research. Finally, Chapter 7 concludes both the literature review and the thesis as a whole.

1.5 Sustainability

This thesis contributes to the UN Sustainability Development Goals (SDGs) [UD15] in a variety of ways. We highlight the the most impacted sub-goal/target in this section, though it must be noted that this work may have broader societal impact given the importance of cryptographic research and online privacy in an increasingly digital world.

Target 9.1 emphasizes developing "quality, reliable, sustainable and resilient infrastructure," which directly encompasses the cryptographic protocols that secure digital communications. Current cryptographic schemes form a critical component of the global digital infrastructure, protecting banking systems, medical information and private communication, among many other use cases. The advent of powerful quantum computers would render existing classical cryptographic protocols obsolete, potentially causing adversaries, whether hostile governments, organizations or even individuals, to have direct access to personal or private information. By researching quantum-resistant PAKE protocols, this thesis contributes to ensuring the resilience of digital infrastructure by providing a comprehensive review of existing schemes. The work addresses the proactive replacement of vulnerable cryptographic primitives before quantum threats even exist, thereby preventing potential disruptions to critical services and maintaining continuity of secure communications.

1.6 Related Works

As a first step in examining previous works in post-quantum PAKE research, it is essential to consider the foundational developments in classical PAKEs. As such, it is invaluable to introduce the key Systematization of Knowledge (SoK) paper on classical PAKEs [HV22] that assembles the history and analysis of PAKE research, up to 2021. This work systematically reviews major PAKE proposals, establishes a comprehensive

domain taxonomy, and critically evaluates real-world PAKE applications. The paper also conducts comparative analysis of selected protocols based on various metrics, including performance considerations. It concludes by presenting five crucial lessons, highlighting challenges such as incomplete specifications, unrealistic assumptions, the need to adapt protocols for emerging threats and deployment scenarios, and the complexity of protocol comparison. For our work, the paper's five-type taxonomy and key insights are particularly relevant, as our contribution aims to address new threats, specifically those posed by quantum computers.

The transition from pre-quantum to post-quantum cryptography represents a significant research gap, which [Fer20] comprehensively addresses. This work looks at Internet of Things (IoT) security challenges in the context of quantum computing emergence and provides a detailed mapping of post-quantum cryptosystems. The survey presents comparative analyses of various algorithms, including CRYSTALS Kyber [Nat24a], specifically within the IoT context. While the paper focuses primarily on IoT systems, emphasizing efficiency and optimization considerations, it does not directly address PAKE protocols. Nevertheless, it discusses related algorithms and presents an interesting framework for analyzing quantum computing's impact across different security domains.

Table 1.1: Comparison of related literature (✓: included, -: not included)

Paper	Systematic Review	PQ	PAKE	Topics addressed
[HV22]	✓	-	✓	PAKE Taxonomy, Fundamental Protocols Highlighted
[Fer20]	-	✓	-	PQ Field Mapped, Fundamental Protocols Highlighted
[AHMW25]	-	✓	✓	PQ PAKE Systematization, Introducing Each Protocol
This work	✓	✓	✓	PQ PAKE Systematization, Fundamental Protocols Highlighted

Finally, we present an unpublished related paper by Alnahawi et al. [AHMW25], from 2025, which presents a contemporary SoK on post-quantum PAKEs, built upon earlier works. The authors provide an overview of the fundamental post-quantum concepts, including hardness assumptions and security notions, while adopting Hao and van Oorschot's [HV22] classification scheme for PAKE categorization. It presents detailed performance and security analyses, alongside real-world use cases, ending with key observations about the field. Although this SoK effectively captures the current

state of post-quantum PAKE research, its descriptive approach primarily covers categorization. The paper's limitations lie in its non-replicable and non-systematic literature review methodology and limited comparative analysis, particularly toward classical PAKE protocols.

As such, this context makes it both attractive and valuable to conduct a systematic, replicable literature review of post-quantum PAKEs that bridges pre- and post-quantum domains through comprehensive comparative analysis, building upon the foundational work done for classical PAKEs [HV22].

Chapter 2
Background

In order to properly discuss the reviewed literature, we must establish the key concepts, definitions and intuition needed for proper understanding of the topic as a whole. This chapter presents both classical and post-quantum PAKE as well as some key security models, providing the core competencies needed to understand the remainder of this work. Curious readers are invited to consult the references for further information on the concepts we introduce.

2.1 Classical Password-Authenticated Key Exchange

In 1992, Encrypted Key Exchange (EKE) became the first example of a Password-Authenticated Key Exchange (PAKE) protocol [BM92]. The core idea behind PAKE has remained the same since. According to Hao and van Oorschot [HV22], each party uses a common secret, typically a password (called a *balanced* PAKE) or a derivation of a password, to output a session key, based on some messages between the parties. For *augmented* PAKE, the server stores a one-way transformation of the secret. This version of PAKE offers additional security protections, including lowering the chance of impersonation in case of server data leaks or dictionary attacks.

Simply put, PAKEs rely on the password as a foundation of security and typically do not require a separate public key infrastructure. That being said, we form the basis of our exploration of the topic through a SoK on classical PAKE [HV22]. The authors create a 5-type taxonomy of PAKEs which are differentiated by the various ways in which the password can be used within PAKEs:

1. C1 **Password used as encryption key.** The password is directly used during key exchange as an encryption key. Depending on the associated cryptosystem it is used with (e.g. RSA, DH) the password may need to be padded and is often also hashed.

2. C2 **Password-derived generator.** The password is passed through a (set of) functions which map the password to a group generator or element. This can be done through Hash-to-Group or Hash-to-(Elliptic)- Curve functions, for example.

3. C3 **Trusted setup.** This type requires pre-defined parameters which are agreed on, typically by depending on a trusted third-party. One example can be a set of generators, where no one knows the discrete log of any of these generators with respect to any of the others.

4. C4 **Secure two-party computation.** This type is based on a two-party secure computation problem where a session key is derived once a test of two passwords being equal is passed. The protocol utilizes a non-interactive zero-knowledge proof (ZKP).

5. C5 **Password-derived exponent.** The password is used as the exponent in g^w for a Diffie-Hellman key exchange as a verifier, hence why all protocols that fall into this category are augmented.

While not all these types may be relevant in the domain of post-quantum PAKE, this taxonomy allows us to approach the topic with a clear mapping of the field.

2.2 Key Exchange and Key Encapsulation Mechanisms

In cryptographic protocols, two fundamental approaches exist for establishing shared secret keys between parties: Key Exchange Mechanism (KEX) and Key Encapsulation Mechanism (KEM). Both serve the purpose of enabling secure communication and can be used in the context of post-quantum PAKEs.

Definition 2.1. Key Exchange A Key Exchange (KEX) [DH76] protocol is an interactive cryptographic protocol that allows two or more parties to jointly establish a shared secret key over an insecure communication channel. Each party contributes information to the protocol execution, and upon completion, all honest participants obtain the same shared secret, which can subsequently be used for secure communication.

PAKE-based key exchange protocols are typically organized into a small number of phases or subroutines, though the exact structure varies. In the setup phase, the shared parameters are defined, including the password. The client initiates the protocol, typically exchanging a message with the server with information about herself and proof that she knows the shared password. The server response phase follows, in which the server responds with its own message, computed using the

shared password and some local randomness. In the client finish and server finish phases, both parties complete the key derivation and optionally exchange confirmation messages, concluding the key exchange.

Definition 2.2. Key Encapsulation Mechanism A Key Encapsulation Mechanism (KEM) [CS98] is a public-key cryptographic primitive that enables a sender to securely establish a shared secret key with a recipient. A KEM consists of three algorithms: KeyGen, which generates a public-private key pair; Encaps, which takes a public key and outputs a ciphertext and a shared secret; and Decaps, which takes the corresponding private key and the ciphertext to recover the shared secret.

KEX is typically interactive, requiring multiple messages exchanged between participants who then jointly build the shared secret. On the other hand, a KEM can be a non-interactive primitive in which one party encapsulates a shared secret under the other party's public key and transmits a ciphertext that allows the recipient to recover the same secret. Both classic and post-quantum PAKEs used to use KEX as the underlying approach, though this has changed in the past few years.

2.3 Post-Quantum Cryptography

Post-quantum cryptography is a subset of cryptography that a quantum computer cannot, as far as we know, efficiently break. There is nuance to this, as there is ongoing research both on algorithms that can use quantum computers' features to break encryption, such as Shor's [Sho97], as well as new defenses in the form of Post-Quantum Cryptography (PQC) [Nat24b].

Generally speaking, there are 6 ways to achieve quantum resistance [AGMS21], showcased in Figure 2.1. We will be covering lattice-based cryptography in detail in Section 2.4.1, isogeny-based cryptography in Section 2.4.2 and code-based schemes are discussed in Section 2.4.3. These types of PQC appeared in the literature which we reviewed and hence are considered relevant to our work.

On the other hand, the remaining types of quantum-safe cryptography do not appear in this thesis for several reasons. Beginning with symmetric key quantum resistance, this approach is essentially classical cryptography using key sizes large enough to be considered quantum-safe. Naturally, this format does not lend itself to the development of PAKEs. Hash-based schemes are also popular. Indeed, one of the initially standardized post-quantum algorithms published by NIST was hash-based [Nat24b]. However, these schemes typically appear in signature applications and lack efficient KEM constructions upon which a PAKE could be built. Multivariate cryptography faces similar limitations. Since the core structures of these cryptographic

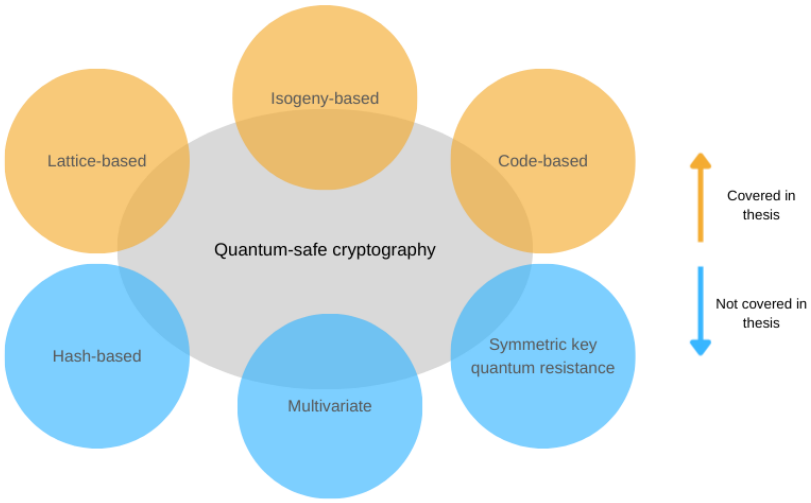


Figure 2.1: Figure showcasing different types of post-quantum cryptography

approaches are not currently suitable for PAKE construction, it is natural that these types of cryptography did not appear in the literature review for this thesis.

2.4 PQC Toolbox for Post-Quantum PAKE

In this work, we will be primarily discussing the quantum resistant variants of PAKE. Nevertheless, the characterization of classical PAKE still applies, as the primary distinction lies in the mathematics behind the hard problems used in the schemes. Therefore, we introduce lattice-based, isogeny-based, and code-based cryptography, as these approaches appear as the most prominent both in our literature review and in the broader post-quantum cryptographic field.

2.4.1 Lattice-Based Cryptography

Lattice-based cryptography forms one of the most promising foundations for the field of post-quantum cryptography. Its security relies on the assumed hardness of computational problems defined over high-dimensional lattices which quantum computers cannot break, at least for now. This section introduces the key definitions, computational assumptions, and hardness problems that form the basis for modern lattice-based schemes used by the papers which we reviewed in the literature review. This section is based on findings from Chi et al. [CCKK15] as well as the research

into relevant background material which was carried out in the project preceding this thesis [Kra24].

Mathematical Preliminaries

A *lattice* is a discrete, periodic set of points in a n-dimensional space, defined as the set of all integer linear combinations of basis vectors.

Definition 2.3. Lattice Let $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m\} \subset \mathbb{R}^n$ be a set of m linearly independent vectors. The lattice denoted either by $\mathcal{L}(\mathbf{B})$ or $\Lambda(\mathbf{B})$ and generated by $\mathbf{B}$ is:

$$\Lambda(\mathbf{B}) = \mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^{m} z_i \mathbf{b}_i \ : \ z_i \in \mathbb{Z}^m \right\}.$$

Equivalently, using matrix notation, let $\mathbf{B} \in \mathbb{R}^{n \times m}$ be a matrix whose columns are the vectors $\mathbf{b}_i$. Then the lattice is:

$$\mathcal{L}(\mathbf{B}) = \{\mathbf{B}z \mid z \in \mathbb{Z}^m\}.$$

A lattice is said to be *full-rank* if $m = n$. Note that any lattice of dimension 2 or higher can have infinitely many bases, but any basis of a given lattice generates the same underlying lattice point set.

Computational Problems in Lattices

Two fundamental hard problems in lattices underpin lattice-based cryptography:

Definition 2.4. Shortest Vector Problem (SVP) Let $\|\cdot\|$ be the norm of a vector and $\lambda(\Lambda)$ be the length of the shortest non-zero vector in a given lattice. Given a basis $\mathbf{B}$ of a lattice $\Lambda(\mathbf{B})$, find a non-zero lattice vector $\mathbf{x} \in \Lambda(\mathbf{B})$ such that

$$\lambda(\Lambda(\mathbf{B})) = \min_{\mathbf{x} \neq 0 \in \Lambda} \|\mathbf{x}\|.$$

Definition 2.5. Closest Vector Problem (CVP) Given a basis $\mathbf{B}$ of a lattice $\Lambda(\mathbf{B})$ and a target point $t \in \mathbb{R}^n$, find the lattice vector $\mathbf{v} \in \Lambda(\mathbf{B})$ that minimizes $\|v - t\|$.

Intuitively, the SVP asks for the shortest non-zero vector in a lattice, while the CVP concerns finding the lattice vector closest to a given target point. These two problems are closely related and, as such, the ability to efficiently solve one implies the ability to solve the other. Both SVP and CVP are known to be NP-hard under certain norms, and their approximations are hard in high dimensions. Importantly, there currently exist no efficient solutions to these problems even with access to quantum computers, making them an interesting basis for further post-quantum cryptographic research.

Learning with Errors (LWE) and Short Integer Solution (SIS)

The Learning With Errors (LWE) problem was introduced by Regev [Reg05] and provides a worst-case security reduction from lattice problems.

Definition 2.6. Search LWE Let $q \in \mathbb{N}$ be a modulus, n be the dimension, and χ be a probability distribution over $\mathbb{Z}_q$. Let $\mathbf{s} \in \mathbb{Z}_q^n$ be a secret vector and $\mathbf{A} \in \mathbb{Z}_q^{n \times n}$ be a uniform matrix. Given access to $(\mathbf{A}, \mathbf{b})$ such that:

$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \mod q, \quad e \leftarrow \chi,$$

the goal is to recover $\mathbf{s}$.

Definition 2.7. Decision LWE Let $u \in \mathbb{Z}_q^n$ be drawn from some uniform distribution. The goal is to distinguish between samples drawn from the distribution:

$$(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \mod q), \quad e \leftarrow \chi,$$

and samples drawn from the uniform distribution:

$$(\mathbf{A}, \mathbf{u})$$

In the decision LWE, the goal is to be able to distinguish uniformly random samples, $\mathbf{u}$, from $\mathbf{b}$ which is noisy due to the error term. This should only be consistently possible for a participant who knows the value of $\mathbf{s}$. Indeed, the trick to LWEs is in this error term $\mathbf{e}$, which transforms the problems from a solvable system of linear equations to hard problems that rely on an adversary not being able to find the secret vector s.

Another central lattice problem is the **Short Integer Solution (SIS)** problem introduced by Ajtai [Ajt96].

Definition 2.8. Short Integer Solution (SIS) Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find a non-zero integer vector $\mathbf{z} \in \mathbb{Z}^m$ such that:

$$\mathbf{A}\mathbf{z} = 0 \mod q \quad \text{and} \quad \|\mathbf{z}\| \leq \beta,$$

for some norm bound β.

The norm bound β is meant to restrict the solutions to short integer vectors, excluding trivial or excessively large solutions. The hardness of the SIS problem increases as β decreases. SIS is provably as hard as approximating worst-case lattice problems such as the SVP under certain parameters.

The security of both LWE and SIS increases with the dimension, which can in turn reduce the efficiency of the schemes relying on these problems. To optimize

performance and size, there exist structured variants of LWE and SIS which are commonly used [Bal21]:

- **Ring:** RLWE or RSIS operate on polynomial rings over finite fields, such as $R_q = \mathbb{Z}_q[X]/(f(x))$. The linear equations get replaced with noisy ring products which allows for improved computational performance.
- **Module:** MLWE and MSIS generalize their respective ring variants to modules, which are vector spaces over rings. These module-based problems are considered better-performing alternatives while maintaining at least the same hardness guarantees.

The CRYSTALS Kyber Key Encapsulation Mechanism

CRYSTALS Kyber is a Module-Lattice-based KEM and one of the three post-quantum schemes standardized by NIST in 2024 [Nat24a]. KEMs are the basis of establishing shared secret keys established over insecure, public channels. Kyber was the only KEM standardized by NIST, until March 2025, when the Hamming Quasi-Cyclic (HQC) was selected as a backup for Kyber [Nat25]. That being said, we chose to briefly describe Kyber to outline the basic functionality of a post-quantum cryptographic scheme.

Kyber operates over the ring $R_q = \mathbb{Z}_q[X]/(X^{256}+1)$ with $q = 3329$ and $n = 256$. The core hardness assumption is MLWE.

With this established, we present the Chosen-Plaintext Attack secure (CPA) version of Kyber:

1. Create uniform matrix $\mathbf{A} \leftarrow R^{k\times k}_{3329,X^{256}+1}$. This matrix is generated pseudo-randomly using a seed which may be shared across multiple key pairs for efficiency but is usually refreshed when used as a KEM. Sample secret and error vectors $(\mathbf{s},\ \mathbf{e}) \leftarrow \psi$ from $R^k_{X^{256}+1}$, where ψ denotes the centered binomial distribution $\mathcal{B}_\eta$. Similarly to LWE, we now compute:

$$\mathbf{t} = \mathbf{A}\cdot\mathbf{s} + \mathbf{e}$$

   The public key is $(\mathbf{A}, \mathbf{t})$ and the private key is $\mathbf{s}$. The binomial distribution $\mathcal{B}_\eta$ is used instead of discrete Gaussian distributions for practical implementation reasons, while maintaining statistical closeness to the ideal LWE error distribution.

2. Sample ephemeral randomness and noise vectors $(\mathbf{r}, \mathbf{e}_1, \mathbf{e}_2) \leftarrow \psi$ from $R^k_{X^{256}+1}$. Create a ciphertext made up of two elements:

$$(\mathbf{u}, v) = (\mathbf{r}^T\mathbf{A} + \mathbf{e}_1^T, \mathbf{r}^T\mathbf{t} + e_2 + \frac{q-1}{2}\mathbf{m})$$

where $\mathbf{m}$ is the binary message to be encrypted and q is the prime modulus, 3329, in this case. The factor $\frac{q-1}{2}$ scales the binary message to use the high-order bits of the polynomial coefficients. The ciphertexts $(\mathbf{u}, v)$ also undergo compression, the result of which is denoted as $(\mathbf{u}', v')$. This compression removes low-order bits while preserving enough information for correct decryption.

3. Decompress $(\mathbf{u}', v')$ to recover approximate versions of the original ciphertext components. Then, the decryption is simply:

$$\mathbf{m}' = v - \mathbf{u}^T\mathbf{s}$$

We note that the decrypted message is an approximation, since:

$$\mathbf{m}' = \frac{q-1}{2}\mathbf{m} + e_3$$

where e_3 is an error formed due to decryption as well as compression and decompression. Specifically:

$$e_3 = e_2 + \mathbf{e}_1^T\mathbf{s} - \mathbf{e}^T\mathbf{r} + \text{compression errors}$$

The decrypted message $\mathbf{m}'$ needs to undergo error correction such that the receiving party is able to round $\mathbf{m}'$ to $\mathbf{m}$. This is typically achieved through nearest-neighbor rounding, provided the total noise remains below $q/4$.

There are three security levels of Kyber, with Kyber768 being the currently-recommended default to use:

- Kyber512 NIST Security Level 1, $k = 2$, Security level equivalent to AES-128
- Kyber768 NIST Security Level 3, $k = 3$, Security level equivalent to AES-192
- Kyber1024 NIST Security Level 5, $k = 4$, Security level equivalent to AES-256

2.4.2 Isogeny-Based Cryptography

Isogeny-based cryptography is an alternative approach to building quantum-resistant solutions and is based on the algebraic structure of elliptic curves, known from classical cryptography, and their relationships. Unlike lattice-based schemes, isogeny-based cryptography utilizes the difficulty of finding isogenies between elliptic curves defined over finite fields. In this section, we briefly introduce the mathematical foundations relevant for isogeny-based cryptography, the well-known Supersingular Isogeny Diffie-Hellman (SIDH) construction, and the Castryck-Decru attack which re-oriented research to look into alternative isogeny-based constructions. This section is based on the findings from [Tai18; CLM+18; Gus24].

Mathematical Preliminaries

An elliptic curve over a finite field $\mathbb{F}_q$ is typically given in Weierstrass form as:

$$E : y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{F}_q$. The points on E, together with a point at infinity $\mathcal{O}$, form an abelian group under a well-defined addition operation.

Definition 2.9. Isogeny An isogeny $\Phi : E_1 \to E_2$ is a non-constant rational map between elliptic curves that preserves the group structure and maps the identity element, $\mathcal{O}_1$, of E_1 to the identity element, $\mathcal{O}_2$, of E_2. The degree of an isogeny is defined as its degree as a rational map.

Definition 2.10. Endomorphism Ring The endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E is the set of all endomorphisms $\Phi : E \to E$ (isogenies from E to itself) under addition and composition. For supersingular elliptic curves over $\mathbb{F}_{p^2}$, this ring is isomorphic to a maximal order in a quaternion algebra.

The security of isogeny-based cryptography fundamentally relies on the difficulty of the following computational problem:

Definition 2.11. Isogeny Finding Problem Given two elliptic curves E_1 and E_2 over $\mathbb{F}_q$ that are known to be isogenous, find an isogeny $\Phi : E_1 \to E_2$ of minimal degree.

In other words, if there is a known fixed base curve E and a known curve E', then it is assumed that finding an isogeny between $\Phi : E \to E'$ is as hard as computing $\mathrm{End}(E')$ which is as hard as computing the corresponding maximal order in a quaternion algebra.

For general elliptic curves, this problem is believed to be exponentially hard, even for quantum computers, making it an attractive foundation for post-quantum schemes.

Supersingular Isogeny Diffie-Hellman

The Supersingular Isogeny Diffie-Hellman (SIDH) protocol, introduced by Jao and De Feo [JD11], represented the most prominent isogeny-based key exchange mechanism, which was even submitted for approval by NIST. However, this was prior to its cryptanalysis in 2022, which ended up breaking SIDH [CD23].

SIDH operates over a supersingular elliptic curve E_0 defined over $\mathbb{F}_{p^2}$ where $p = 2^a \cdot 3^b - 1$ for some a and b. The protocol exploits the rich structure of the

supersingular isogeny graph, where vertices represent supersingular elliptic curves and edges represent isogenies of a fixed prime degree.

The protocol proceeds as follows:

1. **Setup**: Choose a supersingular curve E_0 over $\mathbb{F}_{p^2}$ and torsion bases $\{P_A, Q_A\}$ for $E_0[2^a]$ and $\{P_B, Q_B\}$ for $E_0[3^b]$, where $E_0[n]$ denotes the n-torsion subgroup of E_0.
2. **Key Generation**:
   - Alice samples a random secret key $s_A \in \mathbb{Z}/(2^a)\mathbb{Z}$ and computes the secret isogeny $\Phi_A : E_0 \to E_A$ with kernel $\langle P_A + s_A Q_A \rangle$.
   - Bob samples a random secret key $s_B \in \mathbb{Z}/(3^b)\mathbb{Z}$ and computes the secret isogeny $\Phi_B : E_0 \to E_B$ with kernel $\langle P_B + s_B Q_B \rangle$.
3. **Public Key Exchange**:
   - Alice publishes $(E_A, \Phi_A(P_B), \Phi_A(Q_B))$
   - Bob publishes $(E_B, \Phi_B(P_A), \Phi_B(Q_A))$
4. **Shared Secret**: Both parties can compute isogenous curves E_{AB} via their respective secret isogenies, yielding the shared j-invariant $j(E_{AB})$.

The security of SIDH relied on the difficulty of recovering the secret isogeny from the public information, which appeared to resist both classical and quantum attacks.

The Castryck-Decru Attack

In July 2022, Castryck and Decru [CD23] published a polynomial-time attack against SIDH, effectively breaking all practical parameter sets. The attack exploits the auxiliary torsion point information that SIDH requires for the key exchange to function.

The core issue is that the additional torsion point images $\Phi_A(P_B), \Phi_A(Q_B)$ provide sufficient information to construct what the authors term a "torsion point attack." Specifically, the attack utilizes the fact that the pushed-forward torsion points create a linear system that can be solved efficiently using standard techniques, while also reducing the exponential search space to a polynomial one. Researchers continued to work on this attack, demonstrating its general applicability to SIDH-based constructions, which was also reflected in the literature review presented later in this work.

While the Castryck-Decru attack effectively disqualified SIDH from the post-quantum race, note that not all isogeny-based cryptography has been broken. Importantly, Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) remains

unbroken by the attack, as it does not rely on auxiliary torsion point information. However, CSIDH faces other efficiency challenges, and its viability is still being investigated by researchers.

We note that SIDH constructions released prior to 2022 will be included in the literature review, but will be labelled as not quantum-safe and broken in general, even under classical cryptography.

2.4.3 Code-Based Cryptography

Code-based cryptography is the final type of quantum-safe cryptography we introduce. It is based on structures, called codes, which use redundancy to introduce some desirable properties. This type of cryptography was represented the least in the reviewed literature, despite being historically invaluable. The descriptions in this chapter are based on information from a thesis [Per20].

Mathematical preliminaries

Error-correcting codes are mathematical structures designed to detect and correct errors in transmitted data. The fundamental objects in code-based cryptography are linear codes over finite fields.

Definition 2.12. Linear Code A linear code C of length n and dimension k over a finite field $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The *minimum distance* of C is defined as

$$d := \min_{\mathbf{c}_1 \neq \mathbf{c}_2 \in C} d_H(\mathbf{c}_1, \mathbf{c}_2),$$

where $d_H(\cdot, \cdot)$ denotes the Hamming distance. Such a code is denoted by an $[n, k, d]_q$ code. A generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ is a matrix whose rows form a basis of C.

Definition 2.13. Hamming Weight and Distance The *Hamming weight* of a vector $\mathbf{v} \in \mathbb{F}_q^n$, denoted by $\mathrm{wt}(\mathbf{v})$, is the number of non-zero coordinates in $\mathbf{v}$. The *Hamming distance* between two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ is defined as

$$d_H(\mathbf{u}, \mathbf{v}) := \mathrm{wt}(\mathbf{u} - \mathbf{v}).$$

The minimum distance element is important to the error correcting capabilities of a particular code, as it denotes the smallest number of non-zero coordinates where two distinct codes differ.

Definition 2.14. Parity-Check Matrix Let $C \subseteq \mathbb{F}_q^n$ be a linear code. A matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ is called a parity-check matrix of C if

$$C = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{H}\mathbf{c}^T = \mathbf{0}\}.$$

Definition 2.15. Syndrome Given a received word $\mathbf{r} \in \mathbb{F}_q^n$ and a parity-check matrix $\mathbf{H}$, the *syndrome* of $\mathbf{r}$ is defined as

$$\mathbf{s} := \mathbf{H}\mathbf{r}^T \in \mathbb{F}_q^{n-k}.$$

If $\mathbf{r} = \mathbf{c} + \mathbf{e}$ for some codeword $\mathbf{c} \in C$, then $\mathbf{s} = \mathbf{H}\mathbf{e}^T$.

We can observe that the syndrome is directly correlated to the error of a received code, that is, a zero syndrome implies there is no error in the codeword. The syndrome relies on the parity-check matrix which defines valid codewords for a particular linear code. In a similar fashion to lattice-based cryptography, the security of code-based cryptography relies on several computationally hard problems related to errors:

Definition 2.16. Syndrome Decoding Problem Given a parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, a syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$, and a weight bound $t \in \mathbb{N}$, find a vector $\mathbf{e} \in \mathbb{F}_q^n$ such that

$$\mathbf{H}\mathbf{e}^T = \mathbf{s} \quad \text{and} \quad \mathrm{wt}(\mathbf{e}) \leq t.$$

Definition 2.17. Code Distinguishing Problem Given a matrix $G \in \mathbb{F}_q^{k\times n}$, distinguish whether G is the generator matrix of a uniformly random linear code or the generator matrix of a code drawn from a specific family of structured codes.

The hardness of the Syndrome Decoding Problem increases as the weight bound t decreases, and it forms the basis of security for many code-based cryptographic constructions. Nevertheless, both problems are known to be NP-complete in their general forms, and no efficient quantum algorithms are known for solving them. In practice, code-based cryptosystems often employ structured codes such as Goppa codes [Gop70] to achieve efficient key sizes and operations, while relying on the computational difficulty of distinguishing these structured codes from random ones.

The McEliece Cryptosystem

The McEliece cryptosystem was introduced by Robert McEliece in 1978 [McE78]. It is among the most known code-based cryptographic algorithms. The McEliece system is based on binary Goppa codes, which are a family of algebraic codes with efficient decoding algorithms. We note that the papers, which were reviewed for the literature review section of our work utilized more complex code-based cryptosystems (eg. quasi-cyclic), though we chose to present the McEliece for illustrative purposes.

The system operates [Weg18] as follows:

1. **Key Generation**:
   - Choose a binary irreducible Goppa code C with parameters $[n, k, d]$ capable of correcting t errors, with generator matrix $\mathbf{G}$.
   - Select a random $k \times k$ invertible matrix $\mathbf{S}$ and a random $n \times n$ permutation matrix $\mathbf{P}$.
   - Compute the public generator matrix $\hat{\mathbf{G}} = \mathbf{SGP}$.
   - The public key is $(\hat{\mathbf{G}}, t)$ and the private key is $(\mathbf{S, G, P})$.

2. **Encryption**:
   - To encrypt a message $m \in \mathbb{F}_2^k$, compute $c = m\hat{\mathbf{G}} + \mathbf{e}$, where $\mathbf{e}$ is a random error vector of weight $\leq t$.

3. **Decryption**:
   - Compute $c' = c\mathbf{P}^{-1} = m\mathbf{SG} + \mathbf{eP}^{-1}$.
   - Use the efficient Goppa decoding algorithm to recover mS from c'.
   - Compute $m = (m\mathbf{S})\mathbf{S}^{-1}$ to recover the original message.

The security of the McEliece system relies on the indistinguishability of the public generator matrix $\hat{\mathbf{G}}$ from a random matrix, as well as the hardness of decoding the resulting linear code without knowledge of its structure.

2.5 Oblivious Pseudorandom Functions

Oblivious Pseudorandom Functions (OPRFs) are a family of deterministic functions which output a value that is indistinguishable from a random output [CHL22]. They are based on pseudorandom functions, PRFs, which are essentially instantiations of random oracles, covered in Section 2.6.1. The oblivious element relates to the idea that the two parties participating in the protocol, can securely compute a PRF without learning certain information from each other. More formally:

Definition 2.18. Oblivious Pseudorandom Function An Oblivious Pseudorandom Function (OPRF) is a two-party cryptographic protocol between a client and a server holding a secret key k for a pseudorandom function $\mathrm{PRF}_k(\cdot)$. On input x, the client obtains the value $\mathrm{PRF}_k(x)$, while the protocol ensures that the client learns nothing about the key k beyond what is implied by the output, and the server learns nothing about the client's input x.

While Oblivious Psuedorandom Function (OPRF)s are not PAKEs, they are valuable building blocks that do make up an important security element in many of the PAKEs discussed in both in our and other's research. Furthermore, one paper utilizing OPRFs even repeatedly appeared appeared in the literature search for PAKEs, and OPRFs have been mentioned in a number of papers reviewed during

the literature review. As such, we decided to extend this thesis by a minor literature search on post-quantum OPRFs to better understand their current state.

2.6 Security Models

Establishing the security of cryptographic schemes has been a fundamental challenge. As has been widely discussed by cryptographers [Abd05], previously, cryptographic protocol design followed an ad hoc approach, where designers developed schemes, and adversaries - sometimes real-world attackers - attempted to break them. Eventually, one side would run out of ideas, temporarily concluding development, until a new advancement came. Naturally, this approach had significant limitations, particularly in terms of provability and standardization.

Thus, the field of provable security emerged. By formally defining both an adversary's capabilities and a scheme's security goals, provable security models provide assurances about the security of cryptographic primitives based on well-defined hardness assumptions. This approach moves the focus from designing ad hoc attacks against individual protocols to analyzing the soundness of their underlying foundations. It should be noted, however, that provable security offers primarily *theoretical* guarantees. Practical implementations may still be vulnerable due to side channels, incorrect assumptions, or deployment issues, and may therefore fall short of the *ideal* security notion. Nevertheless, we present the provable security models most commonly referenced and applied in the context of (post-quantum) PAKE.

2.6.1 Idealized Models

Idealized models are used to simplify imperfect implementations of certain core concepts into more elegant and convenient theoretical constructions. This was done, for the first time, in the formalization of the Random Oracle Model (**ROM**) [BR93] which was intended to be an idealized model of a hash function. In this case, the hash function is defined as a function in which each input query generates a uniformly random output. If the query is repeated, it will generate the same output, but two different input queries should never generate the same output (this property is also called collision-resistance.) The ROM is a purely theoretical model of the hash function, as it has been shown by Bellare and Rogaway that practical random oracle implementations do not exist in practice. As such, when security proofs rely on the ROM, any concrete hash function used in an actual implementation will deviate from the idealized model and therefore may fail to satisfy all the theoretical properties. Yet, relying on the ROM or any other idealized model is convenient when constructing cryptographic schemes or security proofs.

That being said, another commonly used model is the Ideal Cipher (**IC**) [BPR00]. The IC assumes that every input will yield a truly random and independent permutation for every key. This model, in principle, means that an attacker cannot infer any information by reusing the same key on different inputs, nor the same input with different keys. This model used to be considered to be stronger than the ROM, but [CPS08] proved these models to be equivalent.

The Common Reference String (**CRS**) [Pas03] is another model, which is based on a public string generated in a trusted manner and shared with all parties involved. The generation of the CRS is particularly complex when there is limited trust among the participants in the system. If a scheme is able to be proven secure under the CRS model, it is assumed to be so, as long as the setup (primarily the generation) was done correctly. As such, this model has wider potential for practical implementation than the ROM.

2.6.2 Game-Based Models

Game-based models are generally used as one of the ways to achieve a security proof of a cryptographic protocol. According to Bellare and Rogaway [BR06], a game-based security model starts off by building two games that can mimic two "worlds". We represent these games to ensure that they are *syntactically identical*, apart for a single flag. This flag is essentially a marker that notifies of an undesirable event which would mean that an attacker has broken a cryptographic scheme. Then, the so-called "fundamental lemma of game playing" is invoked, which is that the upper bound of the probability that the attacker manages to activate the flag in either of the games. There is a chain of games in which we change one of the games slightly and the probability remains unchanged or increases, or decreases by a bounded amount. Finally, we reach some *terminal game*, where we can bound the probability of the flag being set by conventional methods. The goal of this game is to demonstrate that if the probability is low, then the scheme is secure and that the attacker gains a minimal advantage to distinguish between the two games.

The Bellare-Pointcheval-Rogaway (**BPR**) model [BPR00] is a game-based model typically used to prove that a key exchange protocol is secure against dictionary attacks. Initially, BPR modeling establishes a game between an adversary $\mathcal{A}$ and an honest set of participants, U, running the protocol. Each protocol instance, or session, is denoted as Π_U^i, where i is the session index. $\mathcal{A}$ is able to interact with the session oracles and can query session participants. There are 6 types of queries:

1. Send (U, i, M) - the adversary can send an arbitrary message M to the oracle Π_U^i. This requires the oracle to process the message M and respond in accordance with the protocol, potentially even establishing the session key.

2. Reveal (U, i) - if a session key exists for a particular Π_U^i, it will be revealed to the adversary.
3. Corrupt (U, pw) - this models the adversary getting the password of a user U. It could also replace the password pw of the user used by the server.
4. Execute (A, i, B, j) - the adversary eavesdrops on an entire execution of the protocol and gains a full transcript of the execution between a client A and a server B.
5. Test (U, i) - this tests the adversary on the central premise of the game. Based on a coin flip, either a secret key sk or a random session key drawn from the distribution of session keys is returned. $\mathcal{A}$ must then attempt distinguish the session key from the randomly drawn one. The protocol is considered secure if the adversary's advantage in distinguishing real from random keys is negligible.
6. Oracle (M) - gives the adversary access to a function h on the which the key generation or protocol may depend. The choice of h then dictates the strength and practicality of the proof, for example ROM.

The security proof is developed through a series of games, each slightly modified from the previous one, in which the adversary can execute (some of) the queries. The idea is that unless a "bad" event occurs, the adversary cannot identify a participant's key from a set of remaining keys and that the set of remaining keys shrinks by at most one per run query. Typically, this "bad" event would entail the adversary needing to break a hard problem, like DH or LWE. The proof is completed by showing that the adversary gains no bigger advantage in distinguishing real keys from random ones than if the adversary was to just randomly guess and this advantage is bound by a concrete value.

2.6.3 Simulation-Based Models

The simulation-based security model uses a simulator for the real execution to become indistinguishable from an ideal world scenario to an adversary. These models rely on clearly defining trusted parties under ideal functionality, then simulating this world to an adversary, who cannot computationally distinguish the real world from the simulated world.

In the context of our work, the most important simulation-based model is the Universal Composability (**UC**) framework, introduced by Canetti [Can01]. This model simulates an environment $\mathcal{Z}$ with an adversary $\mathcal{A}$ and ideal trusted functionality, i.e. the idealized version of the protocol $\mathcal{F}$. If $\mathcal{Z}$ interacts with both the adversary and honest parties, and is unable to distinguish if its interacting with the real protocol or a simulated execution, the protocol is considered to be UC-safe.

Importantly, the composition theorem from UC proves a particularly interesting property. This theorem guarantees that any protocol which securely realizes a given UC functionality remains secure under composition, even in environments where multiple known or unknown protocols execute concurrently and interact with one another, as is typical in real-world systems. As such, a protocol proven UC-secure can be safely composed with other protocols without compromising its security - that is to say that this protocol is *universally composable* with other protocols.

Generally speaking, UC is considered the superior security model due to its applicability in modern systems, in particular due to the composition assurances. On the other hand, proving a protocol to be UC-safe is significantly more complex and tedious than using the BPR model.

2.6.4 Other Models

The erasure model, occasionally mentioned both explicitly and implicitly, assumes that any internal information ceases to exist once it no longer has a use [BCP+23]. This is practical because retaining such information can be harmful during leaks or aid attackers in accessing other sensitive information.

The real-or-random (RoR) model assumes that an attacker cannot distinguish the encryption of some text from the encryption of a random string of the same length [BDJR97].

Chapter 3
Methodology

As standard, when conducting the review of existing literature, we will describe the full search strategies, including the inclusion and exclusion criteria, the searched databases and registers, as well as the results of the search. In this section, we discuss the choices made and the motivations behind them in relation to the literature search, and we present the final outline of the methodology used.

We divide the methodology into the main section, which covers post-quantum PAKE and should be considered the core research output for our work. We also include a smaller, follow-up methodology on the literature review on OPRFs, which we found to be valuable in the context of the works discussed in the main literature review on PAKEs.

3.1 Methodology for Post-Quantum PAKE

We first discuss the option of using the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) [PRI], as a standard framework to conduct literature reviews in our work. While PRISMA is a useful guide to conducting reviews, it also has a number of criteria that have to be strictly fulfilled which are suitable for publishing. As the goal for this thesis is not to directly produce a conference paper or publishable article, we find following PRISMA to be limiting in the learning and writing process necessary for conducting our research. That being said, the general guidance of this framework will be used as inspiration for conducting the search. Therefore, we first present the chosen database tools to search, along with the query, including the inclusion and exclusion criteria. The number of results is presented throughout the process, and the adopted search strategies are described and justified. Lastly, the final set of found papers is presented and listed.

The searched databases were The Cryptology ePrint Archive [Int], Web of Science [Cla] and Scopus [Els]. For the ePrint Archive, the search criteria was simply "post-quantum PAKE" and the search yielded 24 unique results. This simple search query

was chosen as there were no apparent advanced search tools available on this site. The search term for Web of Science was more complex, including title, abstract or keywords: “post-quantum” AND “PAKE”, which also yielded 23 results. Finally, Scopus yielded 48 results with the same search query as Web of Science. We use Zotero, a research assistant to keep track of and organize the found literature.

Out of the total 95 hits, a number of search results were discarded. First, 5 papers were excluded due to being written in Chinese, and 4 entries were removed because they referred to entire conference proceedings or book series rather than standalone papers. All duplicated papers were also merged, resulting in 45 unique papers to review. These were then manually screened based on their abstracts to assess their relevance to the scope of this study.

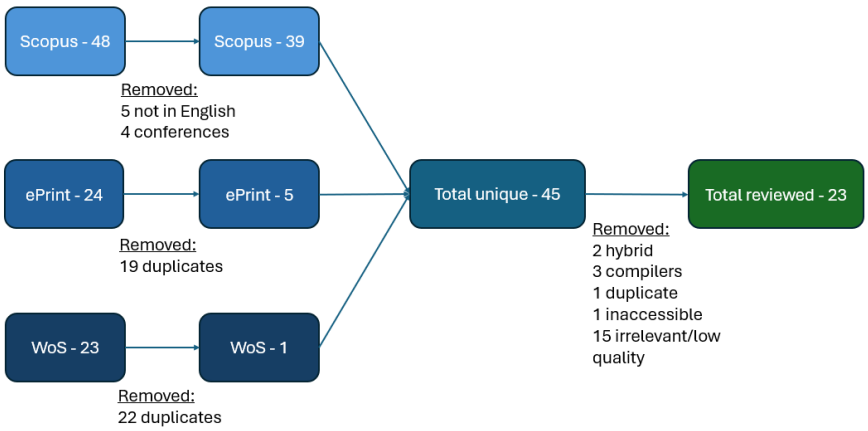


Figure 3.1: Figure showcasing the process of excluding literature

Following this review, 23 papers were retained for further analysis. The remaining 22 were excluded for various reasons: 15 were out of scope, focusing on specific instantiations, like on energy grids or a PAKE mail or low quality, like [PG19]; 1 was not publicly accessible; 1 was an extension of a previously included paper; 3 were on compilers; and 2 presented hybrid implementations of PAKEs. The final set of 23 papers are the basis for the subsequent literature reviews and analysis.

Once this process was finalized, we worked through every paper individually, noting down key details. We were inspired by the process Hao’s SoK utilized [HV22], which extracted information, such as number of rounds, number of flows, key confirmation (implicit/explicit), and whether the scheme requires a trusted setup. Similarly to other work in the field [AHMW25], we also built out a number of tables with information that categorizes the papers by the hardness assumption and balanced/augmented, for example.

Throughout this process, we also identified a number of stand-out papers which we chose to present in detail. This is also based on Hao's work [HV22], who also described exemplary protocols from the 5 types of classical PAKE which the SoK identified. In particular, we get inspired by their criteria for choosing these protocols described as: "academic interest and industrial use, plus simplicity, maturity and efficiency within classes."

3.2 Methodology for Post-Quantum OPRF

During our search for post-quantum PAKEs, we encountered a number of papers discussing OPRFs as a core component of the schemes we discuss. However, OPRFs are inherently different in their structure and therefore do not fit into the core literature review, as they are not categorizable the same way as PAKEs are. As such, we decided to perform a small, secondary review on The Cryptology ePrint Archive with the search criteria "post-quantum OPRF", yielding 13 results. Of these, 3 were not accessible and officially published. One of the discarded results described an attack instead of an instantiation and another was on combining OPRFs. Hence, we were left with 8 papers on post-quantum OPRFs and one was added from the post-quantum PAKE literature review, ending up with 9 in total.

As for the information we looked for, we were inspired by a SoK on the topic [CHL22] and extracted the most relevant information for the purposes of this thesis, including the underlying pseudo-random function the OPRF is built on, the method of evaluation or hardness assumption used, whether the scheme is committed and verifiable, and which security model was used.

Chapter 4
Literature Review

In this chapter, we present the findings of our literature review, organized across 6 tables. Within each table, protocols are listed chronologically by publication date. Our analysis categorizes the research by fundamental properties, performance characteristics, security guarantees, and implementation status. The data presented reflects values reported by the original authors. As such, some variance, in particular in implementation metrics, should be expected due to differences in hardware and design choices. We have also included later-compromised protocols in the tables for illustrative purposes, which we mark in red. Table entries marked with a dash mean that we did not find information about the particular property of the protocol in the original paper.

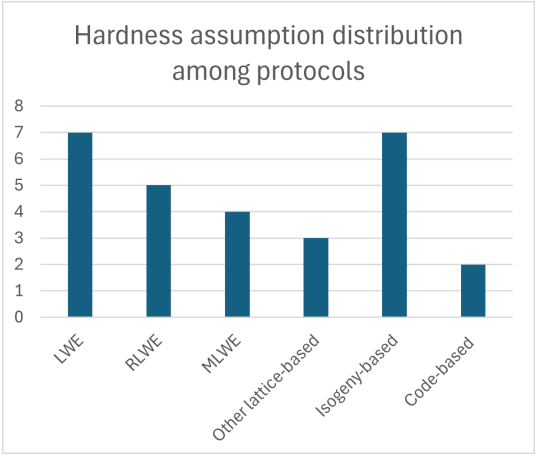


Figure 4.1: Overview of the hardness assumptions used among the reviewed protocols

Table 4.1 provides a comprehensive overview of all 29 post-quantum PAKE protocols from the 23 papers identified in the literature review. The table categorizes

each protocol according to several key dimensions discussed in research on classical PAKEs. Namely, we begin by identifying which of the five categories [HV22] the protocol falls into, as described in Section 2. Notably, no representatives of C4 and C5 in the post-quantum variety exist so far.

The hardness assumptions which these protocols are based span the post-quantum cryptographic families described in this project. Specifically, lattice-based approaches dominate the field, as can be seen in Figure 4.1, with 19 protocols relying on various lattice problems including LWE (7 protocols), RLWE (5 protocols), MLWE (4 protocols), as well as MLWR, SIS and a generic construction which can be instantiated with either MLWE or LWE (each 1 protocol). Isogeny-based constructions account for 7 protocols, though these include the now-broken SIDH constructions. Code-based schemes represent the smallest category with only 2 protocols identified.

Furthermore, we distinguish between balanced and augmented protocols. For the sake of consistency with current literature, we consider protocols in which servers store a hash transform of a password, without a salt or other prevention mechanisms for attacks based on pre-computation, as balanced. We also distinguish between implicit and explicit mutual authentication. While in implicit mutual authentication, the parties assume the agreed-upon key is the same, in explicit mutual authentication, the protocol confirms this. We note that protocols can generally achieve explicit mutual authentication by adding a key confirmation flow after the agreement, if this is not already present in the protocol.

Finally, of the 29 protocols, 17 exist only as theoretical constructions, as far as our literature review found. This distribution highlights the gap between theoretical development and practical deployment in the post-quantum PAKE field and is particularly important for future protocol standardization.

In Table 4.2 we present performance metrics for the 12 protocols that include implementations. Notably, two papers did not provide any relevant testing data about the performance of the protocol, despite it being implemented. In the remaining papers, the key exchange times varied dramatically, ranging from 0.25 milliseconds to 589 milliseconds. This variance stems from multiple factors, including differing hardness assumptions, applications and architectures behind the protocols. Perhaps the most important factor, however, is what the authors include in the key exchange timing itself, which varied between the reviewed papers. In some cases [ABJŠ], we included the time it took for the protocol instantiation and set up in the total, as this was detailed in the paper. In other work [SA24], we added up the total time the communication took both from the server to client and client to server. Many papers, however, only report a single aggregate value without specifying which steps and operations are included in the total time.

Table 4.1: Comprehensive Password-Authenticated Key Exchange Protocol Overview

Protocol	Citation	Classical Type	Hardness Assumption	Type (Bal/Aug)	Authen-tication	Impl. Status
RLWE-PAK	[DAL+17]	C2	RLWE	Balanced	Explicit	×
RLWE-PPK	[DAL+17]	C2	RLWE	Balanced	Implicit	×
RLWE-SRP	[GDLL18]	C2	RLWE	Augmented	Explicit	✓
SPHF	[LW19]	C3	LWE	Balanced	Implicit	×
SIDH-EKE	[TY19]	C1	Isogeny (SIDH)	Balanced	Implicit	✓
CSIDH-EKE	[TY19]	C1	Isogeny (CSIDH)	Balanced	Implicit	✓
PAKE	[YGWX20]	C2	RLWE	Balanced	Explicit	✓
SIDH	[TSJL21]	C2	Isogeny (SIDH)	Balanced	Explicit	✓
MLWE	[RG21]	C2	MLWE	Augmented	Explicit	✓
X-GA-PAKE	[AEK+22]	C3	Isogeny	Augmented	Implicit	×
COM-GA-PAK	[AEK+22]	C3	Isogeny	Augmented	Implicit	×
SRP	[LW22a]	C3	LWE	Augmented	Implicit	×
PHF	[LWM22]	C3	LWE	Augmented	Explicit	✓
One-round-SPHF	[LW22b]	C3	LWE	Balanced	Implicit	×
OPAKE	[WLW22]	C2	Code-based	Balanced	Explicit	✓
GeT a CAKE	[BCP+23]	C1	LWE	Balanced	Explicit	×
Saber.PAKE	[SA23]	C2	MLWR	Balanced	Explicit	✓
NICE	[AAA+24]	C2	MLWE	Balanced	Implicit	×
PAKE_QRO_LWE	[LLH24]	C3	LWE	Balanced	Explicit	×
PAKE_RO_LWE	[LLH24]	C3	LWE	Balanced	Explicit	×
PAKE_RO_GA	[LLH24]	C3	Isogeny	Balanced	Explicit	×
PAKE_QRO_GA	[LLH24]	C3	Isogeny	Balanced	Explicit	×
BiGISIS	[SA24]	C2	SIS	Augmented	Explicit	✓
CHIC	[ABJŠ]	C2	MLWE	Balanced	Implicit	✓
NoIC	[ABJ25]	C1	-	Balanced	Implicit	×
CPAKE	[JD25]	C3	Code-based	Balanced	Implicit	×
GenPAKE	[PZ23]	C1	LWE/MLWE	Balanced	Explicit	×
LPAKE	[JDZ25]	C3	MLWE	Augmented	Implicit	×
KPAKE	[YZYW25]	C3	RLWE	Augmented	Explicit	✓

Similarly, communication overhead, measured as total data exchanged, shows substantial variation across protocols. Here the clear outlier is a PAKE to be used on satellites [YZYW25], which may contribute to higher resource needs. Nevertheless, the reason for the large variance in results is also that many papers do not explicitly specify what is included in their reported values.

For this project, we chose to note the number of flows rather than rounds, as they provide more granular information about the found protocols. We define a flow as unidirectional communication from the client to the server (or vice versa), whereas the round is a back-and-forth, with two messages. The majority of protocols required

Table 4.2: Performance Metrics of Implemented Password-Authenticated Key Exchange Protocols

Protocol	Citation	Key Exchange Time (ms)	Number of Flows	Total Data Exchanged (bytes)	C→S (bytes)	S→C (bytes)
RLWE-SRP	[GDLL18]	–	2	–	–	–
SIDH-EKE	[TY19]	5	2	330	–	–
CSIDH-EKE	[TY19]	80.6	2	64	–	–
PAKE	[YGWX20]	–	3	4456	1864	2592
SIDH	[TSJL21]	–	3	–	–	–
MLWE (rec.)	[RG21]	252.76	3	2816	1344	1472
PHF (asym,clas)	[LWM22]	477	2	7414	3295.25	4118.75
OPAKE	[WLW22]	7.53	4	–	–	–
Saber.PAKE	[SA23]	0.41	3	4928	1760	3168
BiGISIS	[SA24]	256.8	3	–	–	–
CHIC	[ABJŠ]	0.253	2	–	–	–
KPAKE	[YZYW25]	–	3	918496	459504	458992

2 or 3 flows, though the authors often noted that additional flows or rounds may add desirable properties to the given protocol.

Table 4.3 provides a detailed analysis of the security properties and proof techniques employed across the reviewed protocols. We list all protocols with their flows, proof standards and security models, as described in detail in Section 2. We further compare these in a different format in Table 4.4 to showcase the wide range and distribution of the different models used. Finally, we also include the claimed security level of the protocols we found. We note that in some cases, the authors chose to implement multiple versions of their protocol at different security levels, hence multiple values may be listed. If this is the case, the value in bold is the recommended security level of this protocol, as listed by the authors or, if this is not specified, the highest security level.

When we discuss classical security levels, we mean the number of operations a classical computer would need to perform to break the cryptographic scheme, expressed as a power of 2 e.g., 128-bit security requires approximately 2^{128} operations. On the other hand, quantum security levels account for the speedup that quantum algorithms provide against certain mathematical problems. For example, for symmetric cryptography, Grover's algorithm [Gro96] provides a quadratic speedup, effectively halving the security level e.g. AES-256 provides 128-bit quantum security. We note that we did not investigate how exactly the authors came to the security levels presented in their papers.

Finally for the PAKE-focused portion of the literature review, in Table 4.5 we provide a comparative ranking of the implemented protocols based on multiple performance and security criteria. The ranking considers key exchange time, total

Table 4.3: Security Analysis

Protocol	Citation	Flows	Proof Standard	Security Model	Security Level (bits) Classical	Quantum
RLWE-PAK	[DAL+17]	3	BPR	ROM	84	76
RLWE-PPK	[DAL+17]	3	BPR	ROM	84	76
RLWE-SRP	[GDLL18]	2	UC	–	209	–
SPHF	[LW22b]	2	BPR	CRS	–	–
SIDH-EKE	[TY19]	2	BPR	ROM, IC	128	–
CSIDH-EKE	[TY19]	2	BPR	ROM, IC	128	–
PAKE	[YGWX20]	3	BPR	ROM	282/229	253/206
SIDH	[TSJL21]	3	BPR	ROM	–	–
MLWE	[RG21]	3	BPR	ROM	128/**195**/263	116/**177**/239
X-GA-PAKE	[AEK+22]	2	BPR	CRS	–	–
COM-GA-PAK	[AEK+22]	3	BPR	CRS	–	–
SRP	[LW22a]	3	BPR	CRS	–	–
PHF	[LWM22]	2	BPR	CRS	128	128
One-round-SPHF	[LW22b]	2	BPR	CRS	–	–
OPAKE	[WLW22]	4	BPR	ROM	80/**128**/256	–
GeT a CAKE	[BCP+23]	2	UC	ROM, IC	–	102/162
Saber.PAKE	[SA23]	3	Hybrid	ROM	–	128/192/**256**
NICE	[AHHR24]	2	BPR	ROM	–	–
PAKE_QRO_LWE	[LLH24]	3	UC	CRS, QROM	–	–
PAKE_RO_LWE	[LLH24]	3	UC	CRS, ROM	–	–
PAKE_RO_GA	[LLH24]	3	UC	CRS, ROM	–	–
PAKE_QRO_GA	[LLH24]	3	UC	CRS, QROM	–	–
BiGISIS	[SA24]	3	RoR	–	–	–
CHIC	[ABJŠ]	2	UC	ROM, IC	128/**192**/256	–
NoIC	[ABJ25]	2	UC	ROM	–	–
CPAKE	[JD25]	3	BPR	CRS, ROM	–	–
GenPAKE	[PZ23]	2	BPR	ROM, IC	-	-
LPAKE	[JDZ25]	3	BPR	CRS, ROM	–	–
KPAKE	[YZYW25]	3	UC	ROM	–	–

data exchanged, number of flows, security level and proof standard. We note the column on security level includes both classical and quantum security (in the format classical/quantum.) We will naturally include the highest rated protocols in our more thorough discussions to come.

In Table 4.6, we present the literature on post-quantum OPRF constructions identified during the review. These 9 protocols present auxiliary cryptographic primitives often used in PAKE constructions, as multiple of their authors note themselves. The underlying pseudorandom functions span the standard approaches, including Diffie-Hellman based constructions adapted to post-quantum settings and the Naor-Reingold construction [NR04].

Table 4.4: Security Model and Proof Technique Overview

Security Model	Protocols	Count
Random Oracle Model (ROM)	RLWE-PAK, RLWE-PPK, SIDH-EKE, CSIDH-EKE, PAKE, SIDH, MLWE, OPAKE, GeT a CAKE, Saber.PAKE, PAKE_RO_LWE, PAKE_RO_GA, CPAKE, LPAKE NICE, CHIC, NoIC, GenPAKE, KPAKE	19
Common Reference String (CRS)	SPHF, X-GA-PAKE, COM-GA-PAK, SRP, PHF PAKE_QRO_GA, PAKE_RO_LWE, PAKE_RO_GA, CPAKE LPAKE, One-round-SPHF, PAKE_QRO_LWE	12
Quantum ROM (QROM)	PAKE_QRO_LWE, PAKE_QRO_GA	2
Ideal Cipher (IC)	SIDH-EKE, CSIDH-EKE, GeT a CAKE, CHIC, GenPAKE	5
Real-or-Random (RoR)	BiGISIS	1
Other/Unspecified	RLWE-SRP	1

Table 4.5: Performance Comparison of High-Performance Password-Authenticated Key Exchange Protocols

Protocol	Key Exchange Time (ms)	Total Data Exchanged (bytes)	Number of Flows	Security Level (bits)	Proof Standard	Overall Rating
CHIC	0.253	–	2	192/-	UC	**Excellent**
Saber.PAKE	0.41	4,928	3	-/256	Hybrid	**Excellent**
SIDH-EKE	5.0	330	2	128/-	BPR	**Good**
OPAKE	7.53	–	4	128/-	BPR	**Good**
MLWE	252.76	2,816	3	195/177	BPR	**Good**
CSIDH-EKE	80.6	64	2	128/-	BPR	**Moderate**
BiGISIS	256.8	–	3	–	RoR	**Poor**
PHF	477	7414	2	128/128	BPR	**Poor**
KPAKE	–	918496	3	–	UC	**Poor**

The evaluation methods employed in these OPRFs include oblivious transfer (OT) [Rab81], homomorphic encryption, and various zero-knowledge proof techniques [GMR89]. Several protocols offer additional features such as verifiability and output commitment, which provide enhanced security properties for specific application scenarios. The security models employed are, similarly to PAKEs, predominantly UC with ROM assumptions. One construction [FOO23] notably has an additional property, the programmable ROM, which is implemented by dynamically selecting return values of the model, while still ensuring uniform distribution of the outputs.

While some reviewed papers included comparative analyses of related works (including other protocols also covered in this work), we chose not to incorporate their performance data or assessments of other protocols into our findings. Ideally, a comprehensive comparative analysis would involve implementing and testing all protocols on the same system under identical conditions. However, such a task is beyond the scope of this thesis and was not performed by any other paper that we

Table 4.6: Comparison of Oblivious Pseudorandom Function Constructions

Source	Citation	Underlying PRF	Evaluation Method	Features	Model
Boneh (SIDH)	[BKW20]	DH-Isogenies (SIDH)	OT	Augmentable	UC, ROM
Boneh (CSIDH)	[BKW20]	Naor-Reingold CSIDH	OT	Augmentable	UC, ROM
Faller	[FOO23]	Garbled Circuits	OT + Symmetric	-	UC, pROM
Albrecht	[ADDG24]	LWE	Homomorphic Encryption	Output Commitment	ROM
Basso	[Bas24]	SIDH	OT	Verifiable (Key)	UC, ROM
Heimberger (2024)	[HHM+24]	NR-CSIDH	CSIDH Hardness	-	-
Beullens	[BDFH25]	2Hash	OT + ZKP + Legendre	Ver. + Commitment	UC, ROM
Heimberger (2025)	[HKL+25]	Spring (LWR)	OT + OLE	Standard	UC, ROM
Yang	[YBH+25]	Power Residue	Legendre + VOLE	Ver. + Committed	UC, ROM

found. Instead, we have relied exclusively on the performance metrics and security claims reported by each protocol's original authors. This way, we try to keep our data sources fair across all reviewed papers.

Chapter 5
Discussion

Our work, representing a review of the current published literature in the field, requires additional discussion beyond the presentation of relevant information in tables. Throughout the process of gathering, organizing and systematizing information, we noted a number of key findings, challenges and papers, which have truly shaped the research in post-quantum PAKE. As such, in this chapter we discuss the findings from Chapter 4, present some of the representative protocols in detail and compare our work to that of other authors on classical PAKEs.

5.1 Findings from the Literature Review

This section serves as a place to introduce or re-iterate some of the most important findings from the literature review. The following subsections are broadly arranged from the most general findings to the most specific. We note that this organization is not meant to imply any hierarchy of their importance.

5.1.1 Lacking and Inconsistent Reporting of Protocol Properties

Throughout our work, we found inconsistent use of terminology across the literature, particularly regarding the distinction between "balanced" and "augmented" PAKE protocols (also referred to as symmetric and asymmetric PAKEs, respectively.) According to the original definition [HV22], a balanced protocol involves both parties holding the same password, while an augmented protocol allows the server to store a derivative of the password (typically a hash) rather than the password itself. However, some more recent work [AHMW25; Gjø24] has put these terms into question. The argument is that protocols where the server stores only a password hash may still be classified as "balanced" if the hash lacks additional protections like salting, because such schemes remain vulnerable to pre-computed attacks using rainbow tables or similar techniques. Only protocols providing both hashing and salt-based protection, or more sophisticated password verification mechanisms, would qualify as truly augmented. Furthermore, we note that, under the traditional definition, many

balanced PAKEs could be turned into augmented PAKEs by partially revising the protocol inputs, without changing any of the foundational or underlying building blocks of the scheme. Hence, for our work, we operated with the revised definition, as we found this to provide the reader with more granular information about the protocol.

However, there has been an attempt to resolve the aforementioned issues of balanced and augmented PAKEs. As a part of their work, Jarecki, Krawczyk, and Xu [JKX18] proposed an alternative approach, distinguishing asymmetric (meaning augmented) PAKEs and so-called *strong* asymmetric PAKEs. Strong asymmetric PAKEs (SaPAKEs) require the password to be hashed and salted on the server's side or perform further transformations to avoid pre-computation attacks. In our search, we did not find the notion of SaPAKE to be widely adopted in the literature. As many protocols often do not explicitly distinguish even between balanced and augmented PAKEs, we chose to not pursue adopting the SaPAKE definition in our review. We note that the authors of OPAQUE [JKX18] also present a compiler that transforms asymmetric PAKEs into Strong asymmetric PAKEs, allowing other constructions to gain higher security guarantees.

Beyond these inconsistencies, many papers fail to provide comprehensive information about their proposed protocols at all. This resulted in us working through the protocols manually and, on occasion, making assumptions about how the protocol is intended to operate, if this information was omitted by the authors. For example, the authors of KPAKE [YZYW25] do not clarify the number formatting convention used in their implementation, leading to ambiguity of the resulting computational overhead. We were able to infer the authors' intentions by cross-referencing other literature, but this is not an ideal solution.

Before beginning this work, we were under the assumption that most of the published papers would clearly include the information we searched for within our tables, such as if the protocol is built based on implicit or explicit mutual authentication, its implementation details, general performance metrics or security level information. One re-occurring example was that when papers specified the security level of their protocol, the authors would not clearly state if they were talking about the classical or quantum security level, which can make an impact on the security assurances the protocol provides, as in nearly all cases, the quantum security level is lower. This lack of standardized reporting makes it extremely difficult to properly evaluate and compare protocols.

The problem extends to computational analysis, where round optimality and total computational cost are often conflated or incompletely reported. These properties are not necessarily correlated as a protocol achieving round optimality (typically two

or three rounds for PAKE) may impose significant computational burdens on one or both parties, while a protocol with additional rounds might distribute computation more efficiently. At the same time, we found no consistency in what authors actually reported when it comes to key exchange times and data exchanged. For example, some papers would report the time individual operations took [SA23], including the setup, while others just present one bulk number, as was the case for KPAKE [YZYW25], the total number of bytes between the client and server (and vice versa.)

5.1.2 Benchmarking the Implementation

Similar to the issue of inconsistent reporting of information, the absence of standardized benchmarking criteria and testing environments was another challenge when comparing the PAKE protocols we found. Researchers evaluate their protocols using different hardware and parameter choices, among other key differences. This heterogeneity presents multiple challenges. For one, it becomes difficult to meaningfully compare protocols between one another, as the particular system testing is conducted on may make an impact on the reported performance values. Furthermore, some authors opted to solve this issue by implementing their own protocol and either running or implementing other publications' protocols, and testing everything on one system. While this does allow the author to meaningfully compare their results to others, this solution is not scalable and inconsistencies may still arise, especially if the code used for testing is not publicly accessible and the parameters which were used are not clearly described in the paper itself.

5.1.3 Lattice-Based Approaches

As noted, while code-based and isogeny-based approaches appear in the literature, they represent a small minority of proposed protocols and most protocols focus on lattice-based cryptography. This concentration likely reflects several factors: the NIST standardization process has validated other lattice-based schemes, LWE and its variants offer favorable performance characteristics compared to other post-quantum primitives, and since it the most developed of the primitives, at least in the context of this field, there are many publications for researchers to draw from and build upon. Furthermore, we observe that the highest performing protocols tend to utilize computationally less expensive LWE variants, particularly Module Learning With Errors (MLWE) in [ABJŠ] and Learning With Rounding (MLWR) [SA23]. This relationship is not bidirectional, that is, using MLWE, MLWR or other variants does not automatically guarantee the protocol to be efficient.

5.1.4 Protocol Security Developing Throughout Time

In terms of security analysis, we found an evolution in proof standards throughout time. The Bellare-Pointcheval-Rogaway (BPR) model served as the predominant

framework for proving PAKE security in earlier works, however, more recent protocols increasingly adopt the Universal Composability (UC) framework, which offers stronger security guarantees. This shift toward UC proofs represents a maturation of the field, though it comes with increased proof complexity. We also note that some of the earlier-published papers did not include a security proof whatsoever and left this as future work, though this practice also disappeared and most recent papers include a full security proof.

Security levels have also evolved significantly, with newer protocols introducing increasingly high security parameters in both the quantum and classical security levels, while retaining high efficiency guarantees. Naturally, higher security parameters typically result in a trade-off in efficiency. Furthermore, there is growing recognition of the need for parameter flexibility, with some recent works providing multiple parameter sets tailored to different contexts: from high-security scenarios requiring 256-bit security to resource-constrained environments where 128-bit security is preferred. These security levels are referred to as paranoid, recommended and light, referring to the 256-, 192- and 128-bit security respectively. Nevertheless, only 12 of the protocols actually listed the security level their scheme achieves and only half of those provided multiple parameter choices, though some authors did note that the security level of their protocol can be easily adjust during implementation, based on the specific security needs.

5.1.5 Quantum Security

Perhaps the most common gap we found in security models for current post-quantum PAKE research is the continued reliance on classical security models despite developing protocols intended to resist quantum adversaries. The majority of reviewed papers prove security in the classical Random Oracle Model (ROM) or Ideal Cipher (IC) model, with many authors acknowledging that extension to Quantum Random Oracle Model (QROM) or Quantum Ideal Cipher (QIC) proofs should come as future work. These quantum models take into consideration that a potential adversary could use the beneficial properties of a quantum computer in their attack.

While positioning proofs in QIC as future work makes sense, as it remains (to our knowledge) a theoretical security model, without an accepted definition, the QROM has been defined [BDF+11]. NIST defines QROM [Nat20] as: “The quantum random oracle model (QROM) is similar to the ROM, except that it is additionally assumed that all parties (in particular, the adversary) have quantum computers and can query the random oracle H in superposition. [...] While this complicates security claims as compared to the ROM, it more accurately models the power of an adversary that has access to a large-scale quantum device for its cryptanalysis when attacking a real-world scheme.” We further note that there seems to be consensus that proving

security in QROM is more difficult than in ROM, further highlighting the potential vulnerabilities and missing security assurances the found PAKE constructions may have.

Related to this issue is the concept of quantum annoying properties, which were discussed in a paper we found during our initial search but it was not included in the literature review itself [ES21]. PAKEs are considered quantum annoying if a quantum computer can solve a discrete logarithm problem for one singular password guess for a particular scheme, that is, the security of the scheme is compromised but it would take a quantum computer a long time to actually find the correct password because it would still have perform many computationally-challenging password guesses. The idea would be that quantum annoying PAKEs could delay the need for quantum-safe PAKEs to be implemented and deployed, serving as a bridge between classical and post-quantum PAKEs. While we did find references to this property in our research, it seems to be unclear what the practical value of quantum annoyance would be. As of now, there seems to be only one paper published with the explicit goal of the PAKE being quantum annoying [TES23], making it another potentially under-explored territory in this field.

5.1.6 Transition to Key Encapsulation Mechanisms

The standardization of CRYSTALS-Kyber in 2024 by NIST [Nat24b] shaped the functioning and process of the proposed protocols we found. While previously key exchange was the common format for PAKEs, recently, black-box constructions relying on a key encapsulation mechanism (KEM) have grown more popular [AAA+24; ABJŠ; YZYW25] and importantly, a generic transformation from KEMs to PAKEs has also been introduced [BCP+23]. While researchers are increasingly choosing to base their PAKEs on a standardized KEM, allowing them to claim their protocol has certain security guarantees as well as more desirable computational and communication efficiency, it also means that some of the relevant properties we looked for in our review transformed throughout time.

This shift toward KEM-based constructions offers clear advantages: protocols can leverage the established security guarantees of standardized primitives like Kyber while improving certain desirable properties in PAKEs. Performance-wise, the efficiency of KEM-based PAKEs depends primarily on minimizing the overhead introduced on top of the base KEM which makes the ones based on Kyber relatively efficient. However, it also introduces new challenges and considerations. All Kyber-based PAKEs are lattice-based, further concentrating the field on a single cryptographic foundation. Nearly all such protocols rely on the Ideal Cipher (IC) model or its variants [ABJŠ] for their security proofs, with NICE [AAA+24] as a notable exception. Alnahawi et al. raise concerns about IC-based approaches,

arguing that invalid cipher outputs could enable easier password guessing attacks and that the lack of a well-defined Quantum Ideal Cipher (QIC) model leaves these security proofs inadequate against quantum adversaries.

Furthermore, the classical PAKE categorization taxonomy (C1-C5) and some of the authentication steps do not naturally translate in KEM-based constructions, which operate under different assumptions than traditional key exchange protocols. This presented us with some challenges when identifying the key properties from the KEM-based PAKEs for our literature review.

5.1.7 The Incorporation of Oblivious Pseudorandom Functions

OPRFs were mentioned throughout the literature we reviewed as a building block which have allowed some PAKEs to take on desirable properties. Perhaps the most notable among these is the OPAQUE protocol [JKX18], which is a classical PAKE, built in a modular fashion. One of its building blocks is a UC OPRF which provides OPAQUE with the aforementioned Strong asymmetric properties, making it secure against pre-computation attacks. At the time of publishing, there were only sparse discussions of post-quantum OPRF variants, though the authors proposed a generic OPRF + AKE construction of which OPAQUE was one concrete instantiation. This implies that any of the post-quantum OPRFs listed in Table 4.6 could be used in hybrid or post-quantum instantiations. We note that the proposed compiler [JKX18] also relies on both the OPRF and AKE having certain properties (for OPAQUE the OPRF was UC and ROM, and the AKE was also UC, among others.)

On the note of hybrid[1] PAKEs, which were disregarded in the context of this work, it must be noted that the proposed OPAQUE combiner [JKX18] is seen as a potential way to achieve a hybrid Strong asymmetric PAKE [HR25]. Nevertheless, as of 2025, there were no hybrid OPRF + AKE constructions published and uncertainty remains about how much the strength of the overall construction relies on the OPRF, that is, whether plugging a quantum-safe OPRF necessarily implies a hybrid or post-quantum PAKE can be constructed. As of our work on this topic, we also found no post-quantum OPAQUE-like instantiation, in spite of the existing quantum-safe OPRFs and AKEs.

5.2 Highlighted Protocols

We will now present three papers which we identified to have been broadly influential or unique in this field, as far as our research goes. We note that all three are

[1]Hybrid PAKEs are schemes which rely on the hardness of a post-quantum assumption as well as a classical assumption. The idea is to combine two PAKEs with mild assumptions to produce a PAKE with a more desirable combination of the original assumptions.

present and ranked highly in Table 4.5. Beyond this table, we also selected these protocols based on our literature review, during which we also found a number of associated papers to the papers we selected that, for example, build out the work through extending security proofs. This is the case for CHIC [ABJŠ] and OPAKE [WLW22]. We aimed to include PAKEs built on all major post-quantum hardness assumptions, that is lattice-based, isogeny-based, and code-based variants. However, we were unable to find any implemented isogeny-based PAKEs. The most prominent candidate [TY19], which presented both SIDH and CSIDH PAKE constructions, was shown to be vulnerable to offline dictionary attacks in a subsequent analysis [AJK+20]. This flaw was discovered even before the Castryck-Decru attack that broke SIDH itself. As such, we instead present one of the protocols based on the key encapsulation mechanism (KEM) approach [ABJŠ].

5.2.1 CHIC [ABJŠ]

This paper by Afonso Arriaga, Manuel Barbosa, Stanislaw Jarecki, and Marjan Škrobot, published at ASIACRYPT 2024, introduces the Compact Half-Ideal Cipher (CHIC) which is a UC-secure PAKE protocol built from lattice-based KEMs. The work is motivated by NIST's standardization of Kyber and aims to create a practical and efficient PAKE that uses the post-quantum KEM in a black-box manner.

The security proof for CHIC is based on the UC framework and a security notion called the Half-Ideal Cipher (HIC) which relaxes the standard Ideal Cipher (IC.) CHIC focused on achieving efficiency by splitting the KEM public key into two components and using one of them, the seed, directly in the modified 2-Feistel (m2F) construction. As such, the HIC fully removes the overhead in the first flow and reduces the overhead to just a 32-byte MAC tag in the second flow.

Being the highest performing protocol among our literature review, the practical contribution is obvious. The authors report execution times in the order of tens of microseconds on a regular laptop, with computational overhead of approximately 25% for initiators and 50% for responders compared to the basic chosen-ciphertext attack-KEM key exchange for Kyber768. This makes CHIC the most efficient UC-secure PAKE from black-box KEM to date and, on top of this, the best-performing post-quantum PAKE we found.

The protocol achieves security through the m2F construction combined with KEM encapsulation, also assuming the erasure model and requiring only one password-based encryption operation on the client's side rather than two as in some earlier KEM designs. The authors emphasize that CHIC is secure against the "Harvest now, decrypt later" threat thanks to Kyber's quantum resistance.

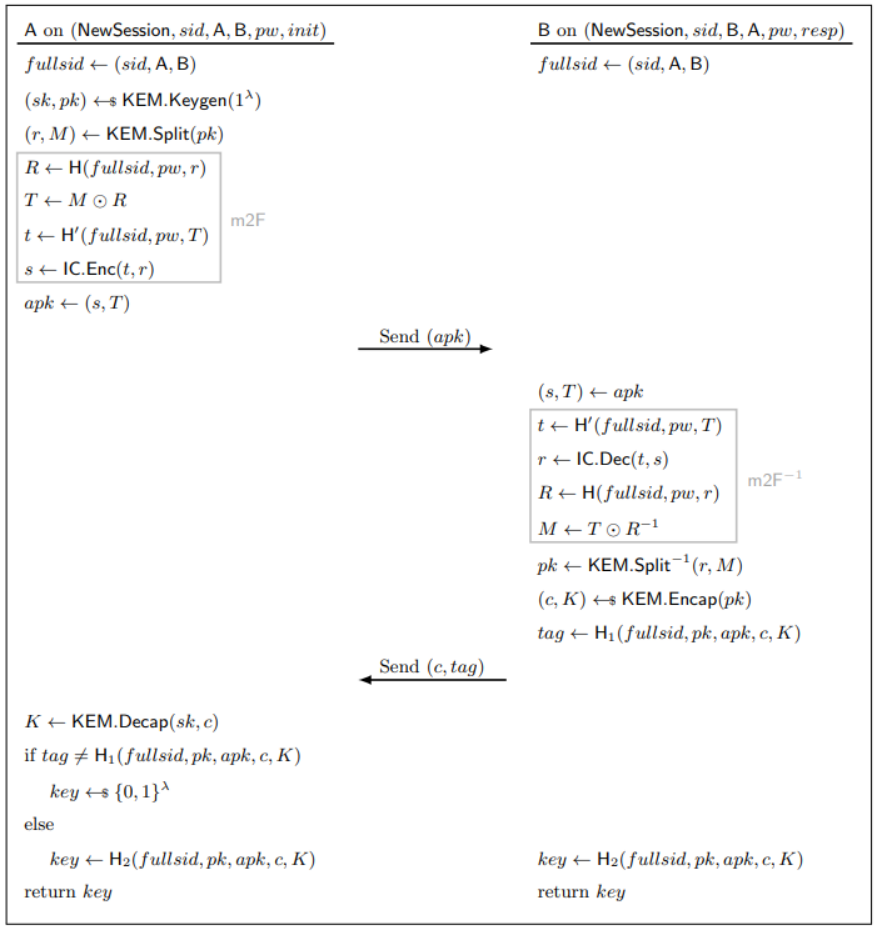


Figure 5.1: CHIC protocol description from [ABJŠ]

We describe the protocol at a high level; readers interested in full details should consult the original paper [ABJŠ].

- **Setup**: The client and server share a common password. Both parties agree on public parameters including the KEM scheme, four hash functions, and an ideal cipher IC operating on 256-bit blocks.
- **Client initiation**: The client generates a KEM key pair (sk, pk) and splits the public key into two parts: a seed r and a group element M, which are encrypted and masked, respectively. The encrypted seed and the masked group element is transmitted to the server.
- **Server response**: The server recovers both the original seed r and group element M. Then by reversing the KEM split algorithm, the server recovers

the public key. Using the KEM encapsulation algorithm on the public key, the server gets a secret key K and a ciphertext c, and calculates a tag from one of the hash functions. The server derives the session key and sends the ciphertext as well as the tag to the client.
- **Client finish**: The client decapsulates the secret key K and verifies the tag. If valid, the client computes the session key; otherwise, outputs a random key to maintain implicit authentication.

5.2.2 OPAKE [WLW22]

This paper by Hao Wang, Yu Li, and Li-Ping Wang, published in Security and Communication Networks 2022, proposes OPAKE (Ouroboros-based PAKE) which is the first code-based PAKE protocol among the literature we reviewed. More importantly, OPAKE is the first provably secure PAKE based on error-correcting codes published in the field. The name, OPAKE, is based on an efficient code-based key exchange protocol called Ouroboros which the authors use as a basis for their protocol.

The security of OPAKE is proven in the BPR model and is reduced to the hardness of the quasi-cyclic syndrome decoding (QCSD) problem in the random oracle model. Low-entropy passwords have to be adapted to the algebraic structure required by the original construction, as such, the authors introduce a so-called weight-restricted hash function, which maps passwords to fixed-weight binary vectors while preserving collision resistance.

From a implementation perspective, OPAKE shows that code-based PAKEs can achieve reasonable efficiency despite operating over large binary vectors. The authors evaluate three parameter sets and report runtimes below 10 ms. While the communication overhead seems to be larger than that of lattice-based PAKEs, the information provided by the authors is not directly comparable to the other literature. However, the results show that code-based approaches are not purely theoretical and may still be viable in practice.

We describe the protocol at a high level and refer the interested reader to the original paper [WLW22] for full definitions, parameter choices, and proofs.

- **Setup**: The client and server share a common low-entropy password. Public parameters include the quasi-cyclic code dimensions, decoding thresholds, and four hash functions, including a weight-restricted hash function used to encode the password.
- **Client initiation**: The client samples random vectors (x, y) and a public value h, and computes a password-dependent masking value using the weight-

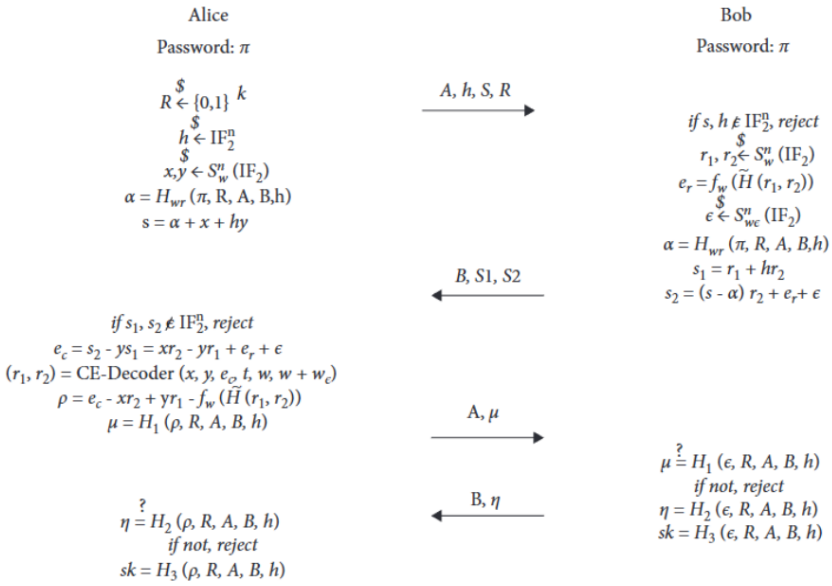


Figure 5.2: OPAKE protocol description from [WLW22]

restricted hash function. These components are combined singular value and sent to the server together with a nonce.

- **Server response**: The server verifies the rationality of the received values and samples its own secret vectors along with an ephemeral error vector. Using the Ouroboros construction, the server embeds a fresh secret into its response and returns two messages.
- **Client authentication**: The client decodes the received messages using the Ouroboros decoding algorithm to recover the server's ephemeral secret. It then computes a confirmation hash to explicitly authenticate itself to the server.
- **Server finish**: The server verifies the client's confirmation value and responds with its own authentication tag. Upon successful verification, both parties derive the final session key using a key derivation hash function.

5.2.3 MLWE [RG21]

This paper by Peixin Ren and Xiaozhuo Gu, published at ICISC 2021, proposes a practical three-flow asymmetric PAKE based on MLWE. Up until this point, researchers predominantly used RLWE, but the authors note that MLWE offers flexibility in parameter selection while retaining the computational advantages of ring polynomials.

The security proof for this PAKE is based on BPR, however the authors use some

assumptions to aid in their proof. In particular, the authors define the Pairing with Errors (PWE) assumption, alongside with its reduction to decision MLWE, showing that the underlying assumption is hard. PWE is then used to simplify the security proof. Similarly, the authors note using the CDF-Zipf model to define the adversarial capabilities in the proof, with respect to assumptions on online dictionary attacks.

What distinguishes this paper is its strong practical approach to developing this PAKE. The authors note the importance of TLS usage in web traffic and hence built the parameter tests for the implementation phase with such applications in mind. In particular, this paper defines three levels: lightweight, recommended and paranoid. Notably, the authors discuss the important of building quantum-resistant PAKEs for resource-constrained IoT devices, which typically do not rely on a PKI. In most other papers, the consideration for IoT devices is missing, despite this application being quite widespread.

Client C		**Server** S
Input S, pw_c		$\mathbf{\Gamma}' = -H_1(pw_c)$
$\rho \sim \{0,1\}^{256}$		
$\mathbf{A} \sim R_q^{d \times d} := Sam(\rho)$		Abort if $\mathbf{m} \notin R_q^d$
$(\mathbf{s}_c, \mathbf{e}_c) \leftarrow \beta_\eta^d \times \beta_\eta^d$	$\xrightarrow{C, \mathbf{m}, \rho}$	$\mathbf{A} \sim R_q^{d \times d} := Sam(\rho)$
$\mathbf{y}_c = \mathbf{A}\mathbf{s}_c + \mathbf{e}_c$		$(\mathbf{s}_s, \mathbf{e}_s) \leftarrow \beta_\eta^d \times \beta_\eta^d$
$\mathbf{\Gamma} = H_1(pw_c)$		$\mathbf{y}_s = \mathbf{A}^T\mathbf{s}_s + \mathbf{e}_s$
$\mathbf{m} = \mathbf{y}_c + \mathbf{\Gamma}$		$\mathbf{y}_c = \mathbf{m} + \mathbf{\Gamma}'$
		$e_\sigma \leftarrow \beta_\eta$
		$\sigma_s = \mathbf{y}_c{}^T\mathbf{s}_s + e_\sigma$
Abort if $\mathbf{y}_s \notin R_q^d$	$\xleftarrow{\mathbf{y}_s, v, k}$	$(k_\sigma, v) = \mathsf{Con}(\sigma_s)$
$\sigma_c = \mathbf{s}_c^T\mathbf{y}_s$		$k = H_2(C, S, \mathbf{m}, \mathbf{y}_s, k_\sigma, \mathbf{\Gamma}')$
$k_\sigma = \mathsf{Rec}(\sigma_c, v)$		$k'' = H_3(C, S, \mathbf{m}, \mathbf{y}_s, k_\sigma, \mathbf{\Gamma}')$
Abort if $k \neq H_2(C, S, \mathbf{m}, \mathbf{y}_s, k_\sigma, \mathbf{\Gamma}')$		
$k' = H_3(C, S, \mathbf{m}, \mathbf{y}_s, k_\sigma, \mathbf{\Gamma}')$	$\xrightarrow{k'}$	Abort if $k' \neq k''$
$sk_c = H_4(C, S, \mathbf{m}, \mathbf{y}_s, k_\sigma, \mathbf{\Gamma}')$		$sk_s = H_4(C, S, \mathbf{m}, \mathbf{y}_s, k_\sigma, \mathbf{\Gamma}')$

Figure 5.3: MLWE PAKE protocol description from [RG21]

We describe the protocol in a general manner and advise a curious reader to consult the original paper [RG21] for further details and definitions.

- **Setup**: The client and server share a common password, where the server holds a hashed version of it. Both parties also agree on public system parameters including the lattice dimensions, modulus values, and four hash functions.
- **Client initiation**: In addition to the lattice matrix, secret and error vectors, as we discuss in Section 2.4.1, the client also samples a seed ρ and masks vector $\mathbf{y}_c$ with a hash of the password. The client identity, seed and masked message $(C, \mathbf{m}, \rho)$ is then transmitted to the server.
- **Server response**: The server checks the rationality of $\mathbf{m}$ and computes its own $\mathbf{y}_s$. Then the server recovers $\mathbf{y}_c$ and uses a standard conciliate function to

produce a key k_σ and a hint v, used due to small errors being introduced in this step. Finally, k is hash function calculated to prove the server's identity to the client and k' is a challenge for the client. The vector $\mathbf{y}_s$, hint v and identity verification hash k is transmitted.
- **Client finish**: The client does her own rationality checks and uses her $\mathbf{y}_c$ to build the reconciliation function and retrieve k_σ. Finally, it calculates its own identity verification k' and uses the key derivation function to arrive at sk_c. k' is sent to the server.
- **Server finish**: The server verifies the client's identity and calculates its own sk_s.

5.3 Comparing Post-Quantum PAKE to Classical

Looking back at our work, we are now able to discuss our findings in relation to the SoK on classical PAKEs [HV22], which we will refer to just as the "SoK" in this section. We will focus on the core outcomes of the SoK, and discuss the parallels that we have found relevant information on. That is to say, as this work is not intended to be one-to-one post-quantum replacement, we look to present the field as it stands currently.

Overall, some of the foundations and principles underlying classical PAKE protocols translate naturally to post-quantum constructions, as would be expected. For example, PAKEs in category C1 rely on ideal cipher models in both classical and post-quantum constructions, and the real-world use cases for PAKEs remain largely the same. Moreover, security considerations continue to be a central issue across the reviewed protocols, with some protocols being broken upon more thorough analysis by researchers. Characteristics such as these which are more closely tied to PAKE protocols themselves, rather than their underlying hardness assumption, therefore carry over directly from classical to post-quantum PAKEs.

On the other hand, the field has matured in several important ways. Universal Composability (UC) was not even mentioned by the SoK on classical PAKEs, while today, it is a widely used proof model among the post-quantum PAKEs we found. Furthermore, aforementioned issues related to balanced and augmented PAKEs have been addressed through proposed fixes, though these approaches have not seen widespread adoption. In addition, the increased reliance on Key Encapsulation Mechanisms (KEMs) in the design of PAKE protocols is also completely novel and was not discussed as a possible construction in the SoK.

One of the main contributions of the SoK was the five class taxonomy presented in 2.1. In our work, we found only the first three classes represented, that is, C1 through C3. On top of that, C1 was clearly the least represented as using the

password as an encryption key introduces a number of offline attack risks due to passwords generally being low-entropy and pre-computable. In addition, for both classical and post-quantum PAKEs, protocols falling under C1 generally required the assumption of an ideal cipher which is difficult to instantiate and prevents broad use. Furthermore, C4 was a small category in the original paper, with only one representative, J-PAKE [HR11], which has yet to have a post-quantum alternative presented. Finally, C5 in its original form refers to the use of a password-derived exponent given the group-based structure of classical Diffie-Hellman (DH) PAKEs. Since post-quantum PAKEs are not built on on primitives using exponentiation, like DH, this category becomes obsolete in its original meaning.

On the note of J-PAKE, this protocol was among the few which were highlighted by SoK authors as important for the field. The others include OPAQUE [JKX18], SRP [Wu02] and CPACE [AHH25]. Of these only SRP has a post-quantum variant published [LW22a], meaning that most of the popular classical PAKEs still do not have post-quantum versions. Similarly, we also could not rely on standardization efforts of PAKE protocols to the same degree the previous work on classical PAKEs could, which limited the availability of well-vetted protocol specifications. While the work was ongoing for the SoK on classical PAKEs, standards bodies were trying to encourage the deployment of PAKEs, which resulted in a number of classical protocols undergoing more thorough formalization and standardization, though with mixed results. Unfortunately, this trend has not yet followed through to post-quantum PAKEs.

The SoK concludes with five learnings (in *italics*) which we chose to highlight and contrast with our own:

- *PAKEs should be accompanied with complete specifications to enable analysis and open implementations.* Our research has revealed the same insight, in that, as has been discussed in this chapter, many authors do not present their work with all the necessarily detail creating research and adoption barriers.
- *Security proofs should specify both the underlying model and realistic assumptions.* Unlike the SoK, our work did not focus as much on implementation details and analysis of security proofs, meaning that this learning may not be fully applicable to our work. However, we did find that many authors note the importance of realistic assumptions in their protocol designs, such as operating based on the Zipf's law for passwords [WW16].
- *PAKE standards must be regularly revisited to address new attacks and correct previous flaws.* While we did find some protocols in which the security proofs were missing, overall it seems that the field has matured in this direction, with the exception of missing a quantum version of the IC and the underwhelming use of QROM.
- *Use cases for new protocols emerge or evolve with deployment environments.*

This learning has widely remained true, though most use cases are not novel or specific for post-quantum PAKEs.

– *PAKE protocols are rarely directly comparable and have various trade-offs.* As is repeated throughout our literature review, especially when discussing the performance evaluation metrics, it is very difficult to directly compare PAKEs to each other and their individual feasibility depends on a variety of criteria and specific use case.

Chapter 6
Future Research

The literature review we conducted in this work has revealed several promising directions for future research in post-quantum PAKE. As such, in this chapter, we outline the most pressing research gaps and opportunities that emerged from our systematic analysis, which can be used by researchers to further develop the field.

Perhaps most importantly, the heavy concentration on LWE-based protocols is a weak point of current post-quantum cryptography efforts. In case a breakthrough in lattice cryptanalysis occurs, the same way SIDH was broken some years ago, the vast majority of post-quantum PAKE protocols could simultaneously become vulnerable. Future research should actively explore PAKE constructions based on alternative post-quantum hardness assumptions, including code- and isogeny-based cryptography. While these alternatives may not currently achieve the performance characteristics of optimized lattice-based protocols, developing a diverse portfolio of post-quantum PAKE protocols ensures that fall-back options exist. The current communication from NIST [Nat24b] has the same tone: the standardized schemes are secure, but we will continue to look for alternatives in case an attack is found.

As was highlighted in similar works for classical PAKEs [HV22], future research should establish agreed-upon benchmarking criteria and standardized testing environments. Researchers currently evaluate protocols using different hardware configurations, parameter choices, and measurement methodologies, making cross-protocol comparisons nearly impossible. Standardized benchmark suites, similar to those used in other cryptographic domains [BL], would enable meaningful performance comparisons and help identify the most promising protocols for different use cases. This benchmark should include specifications for various security levels across different application contexts like IoT.

The classical PAKE taxonomy (C1-C5) introduced by the SoK on classical PAKEs [HV22] requires an update to better accommodate post-quantum constructions. The emergence of KEM-based PAKEs, which do not fit elegantly into the existing

framework, further highlights this need. More specifically for C5, which identifies the "PAKEs based on password-derived *exponents*" should be reformulated to be relevant to post-quantum constructions, such as to "PAKEs based on password-derived *secrets*." This would better reflect the current trends in PAKE constructions.

In relation to security models, we must highlight the need to extend existing protocol proofs in the Quantum Random Oracle Model (QROM) or Quantum Ideal Cipher (QIC). This requires the field for a dual contribution: developing QROM security proofs for existing and future protocols, and to come up with a formalization for the QIC. The need for a well-defined, yet accessible standard for researchers to base their work on, similarly to ROM, is vital to ensuring post-quantum cryptography is ready for quantum adversaries.

Furthermore, the development of post-quantum PAKEs can be supported by underlying primitives such as OPRFs, which already play a central role in several widely deployed classical PAKEs. While quantum-safe OPRF constructions exist, as well as compilers that transform OPRFs and AKE protocols into PAKEs, no post-quantum PAKEs currently make use of both of these approaches, making this an interesting direction for future work. Investigating such constructions could provide a practical pathway toward post-quantum PAKEs that rely on existing UC-secure and quantum-safe primitives, while also improving our understanding of hybrid PAKEs. Similarly, future research could explore quantum-annoying security properties, what they might offer the field, and whether they are even needed, given the current developemnt of the field.

Of the 29 protocols identified in our review, only 12 included implementations, and even fewer provided comprehensive performance evaluations with detailed specifications. This gap between theory and practice hinders real-world adoption and prevents researchers from identifying practical vulnerabilities that may not appear in theoretical analysis. Future work should prioritize developing implementations of promising protocols, complete with thorough security and performance testing across diverse hardware platforms. Open-source implementations with clear documentation would accelerate adoption and enable independent verification of security and performance claims.

The field would also benefit from standardization efforts similar to those undertaken for classical PAKEs, though this may be premature given the rapid evolution of post-quantum cryptography. With respect to the implemented protocols, future work should develop lightweight post-quantum PAKEs optimized for IoT device pairing and authentication. These protocols must balance security guarantees with strict constraints on computation, communication, and energy consumption. Similarly, protocols tailored for satellite communications, mobile devices, and other specific

contexts would expand the practical applicability of post-quantum PAKEs.

Chapter 7
Conclusion

This work can be classified as the only comprehensive, systematic literature review in the field of post-quantum PAKE, to our knowledge. We identified 29 protocols across 23 published papers, which we analyzed in depth and categorized using criteria drawn from prior work in the field and identified within our research goal. Beyond finding existing constructions, we also evaluated the most ambitious and deployment-ready post-quantum PAKEs in greater detail. This was done to give readers from different backgrounds a more concrete understanding of how such protocols work in practice while also highlighting the protocols with high potential in the field.

By considering not only the papers included in the review but also the 22 works that were excluded, we were able to form a holistic view of the current state of post-quantum PAKE research. From this perspective, we identified several key areas where further attention and development are needed, while also tying these learnings back to existing research on classical PAKEs. These insights reflect both the individual contributions of the reviewed papers and a broader synthesis of the field as a whole. Based on this analysis, we conclude that the original research goal, namely, to classify quantum-resistant PAKE constructions with respect to the properties of their classical counterparts, compare their security and efficiency, and identify open research problems, was achieved.

In addition to the core review, we also examined important building blocks related to PAKEs, such as OPRFs. For this component, we conducted a dedicated literature review and connected the results back to PAKE constructions more broadly. This additional context helps clarify not only the maturity of PAKE protocols but also how they relate to their underlying primitives, highlighting important interdependencies within the field.

At the same time, it is important to acknowledge the scope limitations of this work. Certain categories of information that may be relevant to researchers or practitioners were intentionally left out. For example, we did not systematically

analyze fine-grained security notions such as ciphertext indistinguishability, nor did we classify protocols according to specific application scenarios. We also excluded hybrid constructions and compiler-based approaches from the core literature review, despite them forming an interesting and closely related line of research. These omissions were made to keep the scope manageable, but they also form possible extensions for future work.

Overall, as quantum computing continues to move from theory toward practical reality, the need for quantum-resistant cryptography becomes increasingly pressing. This work contributes to that transition by offering a structured overview of post-quantum PAKE field. Researchers can use it as a foundation for further study and comparison, while developers may consult the highlighted protocols as a starting point for practical PAKE implementations.

References

[AAA+24] N. Alnahawi, J. Alperin-Sheriff, *et al.*, "NICE-PAKE: On the Security of KEM-Based PAKE Constructions without Ideal Ciphers", 2024, Publication info: Preprint. [Online]. Available: https://eprint.iacr.org/2024/1957.

[Abd05] M. Abdalla, *Provable security*, https://www.di.ens.fr/~mabdalla/coursedocs/provablesecurity.pdf, Course Notes, 2005.

[ABJ25] A. Arriaga, M. Barbosa, and S. Jarecki, *NoIC: PAKE from KEM without ideal ciphers*, Cryptology ePrint Archive, Report 2025/231, 2025. [Online]. Available: https://eprint.iacr.org/2025/231.

[ABJŠ] A. Arriaga, M. Barbosa, *et al.*, "C'est Très CHIC: A Compact Password-Authenticated Key Exchange from Lattice-Based KEM", in *Advances in Cryptology – ASIACRYPT 2024, Part V*, K.-M. Chung and Y. Sasaki, Eds., ser. Lecture Notes in Computer Science, vol. 15488, Kolkata, India: Springer, Singapore, Singapore, pp. 3–33. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85213350061&doi=10.1007%2f978-981-96-0935-2_1&partnerID=40&md5=689ea6e4dd32602fd4a1c8cd56ca009d.

[ADDG24] M. R. Albrecht, A. Davidson, *et al.*, "Crypto dark matter on the torus - oblivious PRFs from shallow PRFs and TFHE", in *Advances in Cryptology – EUROCRYPT 2024, Part VI*, M. Joye and G. Leander, Eds., ser. Lecture Notes in Computer Science, vol. 14656, Zurich, Switzerland: Springer, Cham, Switzerland, May 2024, pp. 447–476.

[AEK+22] M. Abdalla, T. Eisenhofer, *et al.*, "Password-Authenticated Key Exchange from Group Actions", en, in *Advances in Cryptology – CRYPTO 2022*, Y. Dodis and T. Shrimpton, Eds., vol. 13508, Cham: Springer Nature Switzerland, 2022, pp. 699–728. [Online]. Available: https://link.springer.com/10.1007/978-3-031-15979-4_24.

[AGMS21] T. Attema, N. Gervasoni, *et al.*, *Post-quantum cryptography: Computational-hardness assumptions and beyond*, Cryptology ePrint Archive, Report 2021/571, 2021. [Online]. Available: https://eprint.iacr.org/2021/571.

[AHH25] M. Abdalla, B. Haase, and J. Hesse, "CPace, a balanced composable PAKE", Internet Engineering Task Force, Internet-Draft draft-irtf-cfrg-cpace-17, Dec. 2025, Work in Progress, 98 pp. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/17/.

[AHHR24] N. Alnahawi, K. Hövelmanns, *et al.*, "Towards post-quantum secure PAKE - A tight security proof for OCAKE in the BPR model", in *CANS 2024: 23rd International Conference on Cryptology and Network Security, Part II*, M. Kohlweiss, R. Di Pietro, and A. R. Beresford, Eds., ser. Lecture Notes in Computer Science, vol. 14906, Cambridge, UK: Springer, Singapore, Singapore, Sep. 2024, pp. 191–212.

[AHMW25] N. Alnahawi, D. Haas, *et al.*, *SoK: PQC PAKEs - cryptographic primitives, design and security*, Cryptology ePrint Archive, Paper 2025/119, 2025. [Online]. Available: https://eprint.iacr.org/2025/119.

[AJK+20] R. Azarderakhsh, D. Jao, *et al.*, "How not to create an isogeny-based PAKE", in *ACNS 2020: 18th International Conference on Applied Cryptography and Network Security, Part I*, M. Conti, J. Zhou, *et al.*, Eds., ser. Lecture Notes in Computer Science, vol. 12146, Rome, Italy: Springer, Cham, Switzerland, Oct. 2020, pp. 169–186.

[Ajt96] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)", in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '96, Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 99–108. [Online]. Available: https://doi.org/10.1145/237814.237838.

[All24] P. R. Allison, "Chinese scientists claim they broke RSA encryption with a quantum computer — but there's a catch", *Live Science*, Oct. 22, 2024. [Online]. Available: https://www.livescience.com/technology/computing/chinese-scientists-claim-they-broke-rsa-encryption-with-a-quantum-computer-but-theres-a-catch.

[Bal21] D. Balbás, *The hardness of LWE and ring-LWE: A survey*, Cryptology ePrint Archive, Report 2021/1358, 2021. [Online]. Available: https://eprint.iacr.org/2021/1358.

[Bas24] A. Basso, "A Post-Quantum Round-Optimal Oblivious PRF from Isogenies", en, in *Selected Areas in Cryptography – SAC 2023*, C. Carlet, K. Mandal, and V. Rijmen, Eds., vol. 14201, Series Title: Lecture Notes in Computer Science, Cham: Springer Nature Switzerland, 2024, pp. 147–168. [Online]. Available: https://link.springer.com/10.1007/978-3-031-53368-6_8.

[BCP+23] H. Beguinet, C. Chevalier, *et al.*, "GeT a CAKE: Generic transformations from key encaspulation mechanisms to password authenticated key exchanges", in *ACNS 2023: 21st International Conference on Applied Cryptography and Network Security, Part II*, M. Tibouchi and X. Wang, Eds., ser. Lecture Notes in Computer Science, vol. 13906, Kyoto, Japan: Springer, Cham, Switzerland, Jun. 2023, pp. 516–538.

[BDF+11] D. Boneh, Ö. Dagdelen, *et al.*, "Random oracles in a quantum world", in *Advances in Cryptology – ASIACRYPT 2011*, D. H. Lee and X. Wang, Eds., ser. Lecture Notes in Computer Science, vol. 7073, Seoul, South Korea: Springer Berlin Heidelberg, Germany, Dec. 2011, pp. 41–69.

[BDFH25] W. Beullens, L. Dodgson, *et al.*, "The 2Hash OPRF Framework and Efficient Post-quantum Instantiations", en, in *Advances in Cryptology – EUROCRYPT 2025*, S. Fehr and P.-A. Fouque, Eds., vol. 15608, Series Title: Lecture Notes in Computer Science, Cham: Springer Nature Switzerland, 2025, pp. 332–362. [Online]. Available: https://link.springer.com/10.1007/978-3-031-91101-9_12.

[BDJR97] M. Bellare, A. Desai, *et al.*, "A concrete security treatment of symmetric encryption", in *Proceedings 38th Annual Symposium on Foundations of Computer Science*, Miami Beach, Florida: IEEE Computer Society Press, Oct. 1997, pp. 394–403.

[BKW20] D. Boneh, D. Kogan, and K. Woo, "Oblivious Pseudorandom Functions from Isogenies", en, in *Advances in Cryptology – ASIACRYPT 2020*, S. Moriai and H. Wang, Eds., vol. 12492, Series Title: Lecture Notes in Computer Science, Cham: Springer International Publishing, 2020, pp. 520–550. [Online]. Available: https://link.springer.com/10.1007/978-3-030-64834-3_18.

[BL] D. J. Bernstein and T. Lange, *Ebacs: Ecrypt benchmarking of cryptographic systems*, https://bench.cr.yp.to, Editors.

[BM92] S. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks", in *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, IEEE Computer Society Press, May 1992, pp. 72–84.

[BPR00] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks", in *Advances in Cryptology — EUROCRYPT 2000*, B. Preneel, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 139–155.

[BR06] M. Bellare and P. Rogaway, "The security of triple encryption and a framework for code-based game-playing proofs", in *Advances in Cryptology – EUROCRYPT 2006*, S. Vaudenay, Ed., ser. Lecture Notes in Computer Science, vol. 4004, St. Petersburg, Russia: Springer Berlin Heidelberg, Germany, May 2006, pp. 409–426.

[BR93] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols", in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, ser. CCS '93, Fairfax, Virginia, USA: Association for Computing Machinery, 1993, pp. 62–73. [Online]. Available: https://doi.org/10.1145/168588.168596.

[Can01] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols", in *42nd Annual Symposium on Foundations of Computer Science*, Las Vegas, NV, USA: IEEE Computer Society Press, Oct. 2001, pp. 136–145.

[CCKK15] D. P. Chi, J. W. Choi, *et al.*, "Lattice based cryptography for beginners", Cryptology ePrint Archive, Report 2015/938, Tech. Rep., 2015, Accessed: 2025-07-30. [Online]. Available: https://eprint.iacr.org/2015/938.pdf.

[CD23] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH", in *Advances in Cryptology – EUROCRYPT 2023, Part V*, C. Hazay and M. Stam, Eds., ser. Lecture Notes in Computer Science, vol. 14008, Lyon, France: Springer, Cham, Switzerland, Apr. 2023, pp. 423–447.

[CHL22] S. Casacuberta, J. Hesse, and A. Lehmann, "SoK: Oblivious Pseudorandom Functions", in *2022 IEEE European Symposium on Security and Privacy (EuroSP)*, IEEE, 2022, pp. 529–546. [Online]. Available: https://doi.org/10.1109/EUROSP53844.2022.00045.

[Cla] Clarivate, *Web of science*, https://clarivate.com/products/web-of-science/.

[CLM+18] W. Castryck, T. Lange, *et al.*, "Csidh: An efficient post-quantum commutative group action", in *Advances in Cryptology – ASIACRYPT 2018*, T. Peyrin and S. Galbraith, Eds., Cham: Springer International Publishing, 2018, pp. 395–427.

[CPS08] J.-S. Coron, J. Patarin, and Y. Seurin, "The random oracle model and the ideal cipher model are equivalent", in *Advances in Cryptology – CRYPTO 2008*, D. Wagner, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1–20.

[CS98] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", in *Advances in Cryptology – CRYPTO'98*, H. Krawczyk, Ed., ser. Lecture Notes in Computer Science, vol. 1462, Santa Barbara, CA, USA: Springer Berlin Heidelberg, Germany, Aug. 1998, pp. 13–25.

[DAL+17] J. Ding, S. Alsayigh, *et al.*, "Provably secure password authenticated key exchange based on rlwe for the post-quantum world", in *Topics in Cryptology – CT-RSA 2017*, H. Handschuh, Ed., Cham: Springer International Publishing, 2017, pp. 183–204.

[DH76] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[Els] Elsevier, *Scopus*, https://www.scopus.com/.

[ES21] E. Eaton and D. Stebila, "The "quantum annoying" property of password-authenticated key exchange protocols", in *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021*, J. H. Cheon and J.-P. Tillich, Eds., Daejeon, South Korea: Springer, Cham, Switzerland, Jul. 2021, pp. 154–173.

[Eur25] European Commission, *A coordinated implementation roadmap for the transition to post-quantum cryptography*, Jun. 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[Fer20] T. M. Fernandez-Carames, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things", *IEEE INTERNET OF THINGS JOURNAL*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020.

[FOO23] S. Faller, A. Ottenhues, and J. Ottenhues, "Composable Oblivious Pseudorandom Functions via Garbled Circuits", en, in *Progress in Cryptology – LATINCRYPT 2023*, A. Aly and M. Tibouchi, Eds., vol. 14168, Series Title: Lecture Notes in Computer Science, Cham: Springer Nature Switzerland, 2023, pp. 249–270. [Online]. Available: https://link.springer.com/10.1007/978-3-031-44469-2_13.

[GDLL18] X. Gao, J. Ding, *et al.*, "Post-Quantum Secure Remote Password Protocol from RLWE Problem", vol. 10726 LNCS, 2018, pp. 99–116. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85042232274&doi=10.1007%2f978-3-319-75160-3_8&partnerID=40&md5=d4c8d739f4a76dbb1a5d8446ce163196.

[Gjø24] K. Gjøsteen, *Password-authenticated key exchange and applications*, Cryptology ePrint Archive, Report 2024/1057, 2024. [Online]. Available: https://eprint.iacr.org/2024/1057.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems", *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–208, 1989.

[Gop70] V. D. Goppa, "A New Class of Linear Error-Correcting Codes", *Problemy Peredachi Informatsii*, vol. 6, no. 3, pp. 24–30, 1970, In Russian.

[Gor19] J. Gorman, "Quantum computing is coming, bit by qubit", *The New York Times*, Oct. 21, 2019. [Online]. Available: https://www.nytimes.com/2019/10/21/science/quantum-computer-physics-qubits.html.

[Gre18] M. Green, *Let's talk about pake*, Oct. 2018. [Online]. Available: https://blog.cryptographyengineering.com/2018/10/19/lets-talk-about-pake/.

[Gro96] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '96, Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219. [Online]. Available: https://doi.org/10.1145/237814.237866.

[Gus24] E. Gusak, *A friendly intro to isogeny crypto*, YouTube video, Apr. 2024. [Online]. Available: https://www.youtube.com/watch?v=pIHLTJBEHOQ.

[HHM+24] L. Heimberger, T. Hennerbichler, *et al.*, "OPRFs from Isogenies: Designs and Analysis", en, in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, Singapore Singapore: ACM, Jul. 2024, pp. 575–588. [Online]. Available: https://dl.acm.org/doi/10.1145/3634737.3645010.

[HKL+25] L. Heimberger, D. Kales, *et al.*, "Leap: A Fast, Lattice-Based OPRF with Application to Private Set Intersection", en, in *Advances in Cryptology – EUROCRYPT 2025*, S. Fehr and P.-A. Fouque, Eds., vol. 15607, Series Title: Lecture Notes in Computer Science, Cham: Springer Nature Switzerland, 2025, pp. 254–283. [Online]. Available: https://link.springer.com/10.1007/978-3-031-91098-2_10.

[HR11] F. Hao and P. Y. A. Ryan, "Password authenticated key exchange by juggling", in *Security Protocols XVI*, B. Christianson, J. A. Malcolm, *et al.*, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 159–171.

[HR25] J. Hesse and M. Rosenberg, "PAKE combiners and efficient post-quantum instantiations", in *Advances in Cryptology – EUROCRYPT 2025, Part II*, S. Fehr and P.-A. Fouque, Eds., ser. Lecture Notes in Computer Science, vol. 15602, Madrid, Spain: Springer, Cham, Switzerland, May 2025, pp. 395–420.

[HV22] F. Hao and P. C. Van Oorschot, "Sok: Password-authenticated key exchange theory, practice, standardization and real-world lessons", in *ASIA CCS 2022 - Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security*, 2022, pp. 697–711.

[Int] International Association for Cryptologic Research, *IACR Cryptology ePrint Archive*, https://eprint.iacr.org/.

[Jaq25] S. Jaques, *Expected and unexpected developments in quantum computing*, https://pqcrypto2025.iis.sinica.edu.tw/slides/Invited3.pdf, Invited Talk, PQCrypto 2025, University of Waterloo, 2025.

[JD11] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", in *Post-Quantum Cryptography*, B.-Y. Yang, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[JD25] P. Jana and R. Dutta, "CPAKE: An Identity-Binding Password Authenticated Key Exchange from Quasi-cyclic Codes", vol. 15496 LNCS, 2025, pp. 180–200. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85213379749&doi=10.1007%2f978-3-031-80311-6_9&partnerID=40&md5=a98aee583393414028b490e6325df47a.

[JDZ25] P. Jana, R. Dutta, and C. Zuo, "Quantum Safe Computation-Friendly Identity-Binding Password Authenticated Key Exchange", vol. 14904 LNCS, 2025, pp. 298–309.

[JKX18] S. Jarecki, H. Krawczyk, and J. Xu, "OPAQUE: An asymmetric PAKE protocol secure against pre-computation attacks", in *Advances in Cryptology – EUROCRYPT 2018, Part III*, J. B. Nielsen and V. Rijmen, Eds., ser. Lecture Notes in Computer Science, vol. 10822, Tel Aviv, Israel: Springer, Cham, Switzerland, Apr. 2018, pp. 456–486.

[Kra24] M. Kralova, "Post-quantum password-authenticated key exchange", Department of Information Security, Communication NTNU – Norwegian University of Science, and Technology, Project report in TTM4502, Dec. 2024.

[LLH24] Y. Lyu, S. Liu, and S. Han, "Universal Composable Password Authenticated Key Exchange for the Post-Quantum World", vol. 14657 LNCS, 2024, pp. 120–150.

[LW19] Z. Li and D. Wang, “Two-round PAKE protocol over lattices without NIZK”, vol. 11449 LNCS, 2019, pp. 138–159. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85064122906&doi=10.1007%2f978-3-030-14234-6_8&partnerID=40&md5=1fd08da9b9bc30185b29ebea7ac1e9f4.

[LW22a] H. Li and B. Wang, “A Secure Remote Password Protocol From The Learning With Errors Problem”, in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE, 2022, pp. 1084–1090.

[LW22b] Z. Li and D. Wang, “Achieving One-Round Password-Based Authenticated Key Exchange over Lattices”, English, *IEEE TRANSACTIONS ON SERVICES COMPUTING*, vol. 15, no. 1, pp. 308–321, Jan. 2022.

[LWM22] Z. Li, D. Wang, and E. Morais, “Quantum-safe round-optimal password authentication for mobile devices”, *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1885–1899, 2022.

[McE78] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory”, Jet Propulsion Laboratory, California Institute of Technology, The Deep Space Network Progress Report 42-44, Jan. 1978, https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF, pp. 114–116.

[Nat20] National Institute of Standards and Technology, “Recommendation for Stateful Hash-Based Signature Schemes”, National Institute of Standards and Technology, Tech. Rep. NIST SP 800-208, Oct. 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf.

[Nat24a] National Institute of Standards and Technology, “NIST FIPS 203: Cryptographic Key Management”, Tech. Rep. FIPS 203, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf.

[Nat24b] National Institute of Standards and Technology, *NIST Post-Quantum Cryptography Project*, https://csrc.nist.gov/projects/post-quantum-cryptography, Accessed: 2024-11-02, 2024.

[Nat25] National Institute of Standards and Technology, “NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption”, Tech. Rep., Mar. 2025, Accessed: 2025-07-12. [Online]. Available: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption.

[NR04] M. Naor and O. Reingold, “Number-theoretic constructions of efficient pseudo-random functions”, *J. ACM*, vol. 51, no. 2, pp. 231–262, Mar. 2004. [Online]. Available: https://doi.org/10.1145/972639.972643.

[Pas03] R. Pass, “On deniability in the common reference string and random oracle model”, in *Advances in Cryptology - CRYPTO 2003*, D. Boneh, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 316–337.

[Per20] J. C. S. Perez, "Introduction to code-based post-quantum cryptography", Proyecto de grado para obtener el título de Matemático, Bachelor's thesis, Universidad de los Andes, Bogotá D.C., Colombia, Dec. 2020. [Online]. Available: https://repositorio.uniandes.edu.co/server/api/core/bitstreams/16df48d1-bc35-4fb2-86a9-f995f69c159c/content.

[PG19] H. Parmar and A. Gosai, "Improve end-to-end security using s-aepake", in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2019, pp. 333–338.

[Por70] J. C. Porter, "Computers take step to maturity", *The New York Times*, Jan. 11, 1970. [Online]. Available: https://www.nytimes.com/1970/01/11/archives/computers-take-step-to-maturity.html.

[PRI] PRISMA Executive Group, *Preferred reporting items for systematic reviews and meta-analyses (prisma) website*, https://www.prisma-statement.org/.

[PZ23] J. Pan and R. Zeng, "A generic construction of tightly secure password-based authenticated key exchange", in *Advances in Cryptology – ASIACRYPT 2023, Part VIII*, J. Guo and R. Steinfeld, Eds., ser. Lecture Notes in Computer Science, vol. 14445, Guangzhou, China: Springer, Singapore, Singapore, Dec. 2023, pp. 143–175.

[Rab81] M. O. Rabin, "How to exchange secrets with oblivious transfer", Aiken Computation Laboratory, Harvard University, Tech. Rep. TR-81, 1981.

[Reg05] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography", in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing (STOC)*, Baltimore, MD, USA: ACM, 2005, pp. 84–93. [Online]. Available: http://portal.acm.org/citation.cfm?id=1060590.1060603.

[RG21] P. Ren and X. Gu, "Practical post-quantum password-authenticated key exchange based-on module-lattice", in *ICISC 21: 24th International Conference on Information Security and Cryptology*, J. H. Park and S.-H. Seo, Eds., ser. Lecture Notes in Computer Science, vol. 13218, Seoul, Korea: Springer, Cham, Switzerland, Dec. 2021, pp. 137–156.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: https://doi.org/10.1145/359340.359342.

[SA23] K. Seyhan and S. Akleylek, "A new password-authenticated module learning with rounding-based key exchange protocol: Saber.PAKE", *JOURNAL OF SUPERCOMPUTING*, vol. 79, no. 16, pp. 17 859–17 896, Nov. 2023.

[SA24] K. Seyhan and S. Akleylek, "A new lattice-based password authenticated key exchange scheme with anonymity and reusable key", *PEERJ COMPUTER SCIENCE*, vol. 10, Jan. 2024.

[Sho97] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997. [Online]. Available: http://dx.doi.org/10.1137/S0097539795293172.

[Sim92] W. A. Simpson, *PPP Authentication Protocols*, RFC 1334, Oct. 1992. [Online]. Available: https://www.rfc-editor.org/info/rfc1334.

[Tai18] E. Tairi, "Isogenies for post-quantum cryptography", Master's thesis, Johannes Kepler University Linz, 2018. [Online]. Available: https://epub.jku.at/download/pdf/2581853?name=Isogenies%20for%20Post-Quantum%20Cryptography.

[TES23] M. Tiepelt, E. Eaton, and D. Stebila, "Making an asymmetric PAKE quantum-annoying by hiding group elements", in *ESORICS 2023: 28th European Symposium on Research in Computer Security, Part I*, G. Tsudik, M. Conti, *et al.*, Eds., ser. Lecture Notes in Computer Science, vol. 14344, The Hague, The Netherlands: Springer, Cham, Switzerland, Sep. 2023, pp. 168–188.

[TSJL21] O. Taraskin, V. Soukharev, *et al.*, "Towards Isogeny-Based Password-Authenticated Key Establishment", *Journal of Mathematical Cryptology*, vol. 15, no. 1, pp. 18–30, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097180194&doi=10.1515%2fjmc-2020-0071&partnerID=40&md5=fe91dd7ff8bf39928aedf267f013460c.

[TY19] S. Terada and K. Yoneyama, "Password-Based Authenticated Key Exchange from Standard Isogeny Assumptions", vol. 11821 LNCS, 2019, pp. 41–56. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075732888&doi=10.1007%2f978-3-030-31919-9_3&partnerID=40&md5=339ea1770fc098d124d358959d668959.

[UD15] D. o. E. United Nations and S. A. .-. S. Development, *Transforming our world: The 2030 agenda for sustainable development*, General Assembly, 2015. [Online]. Available: https://sdgs.un.org/2030agenda.

[Weg18] V. Weger, *What is... the McEliece system?*, Zurich Graduate Colloquium, University of Zurich, Presentation, Nov. 2018. [Online]. Available: https://user.math.uzh.ch/weger/slides/ZGC.pdf.

[WLW22] H. Wang, Y. Li, and L.-P. Wang, "Post-Quantum Secure Password-Authenticated Key Exchange Based on Ouroboros", *Security and Communication Networks*, vol. 2022, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85144100406&doi=10.1155%2f2022%2f9257443&partnerID=40&md5=ff2b3ca9268833b0eaa1aa90cd4cbf15.

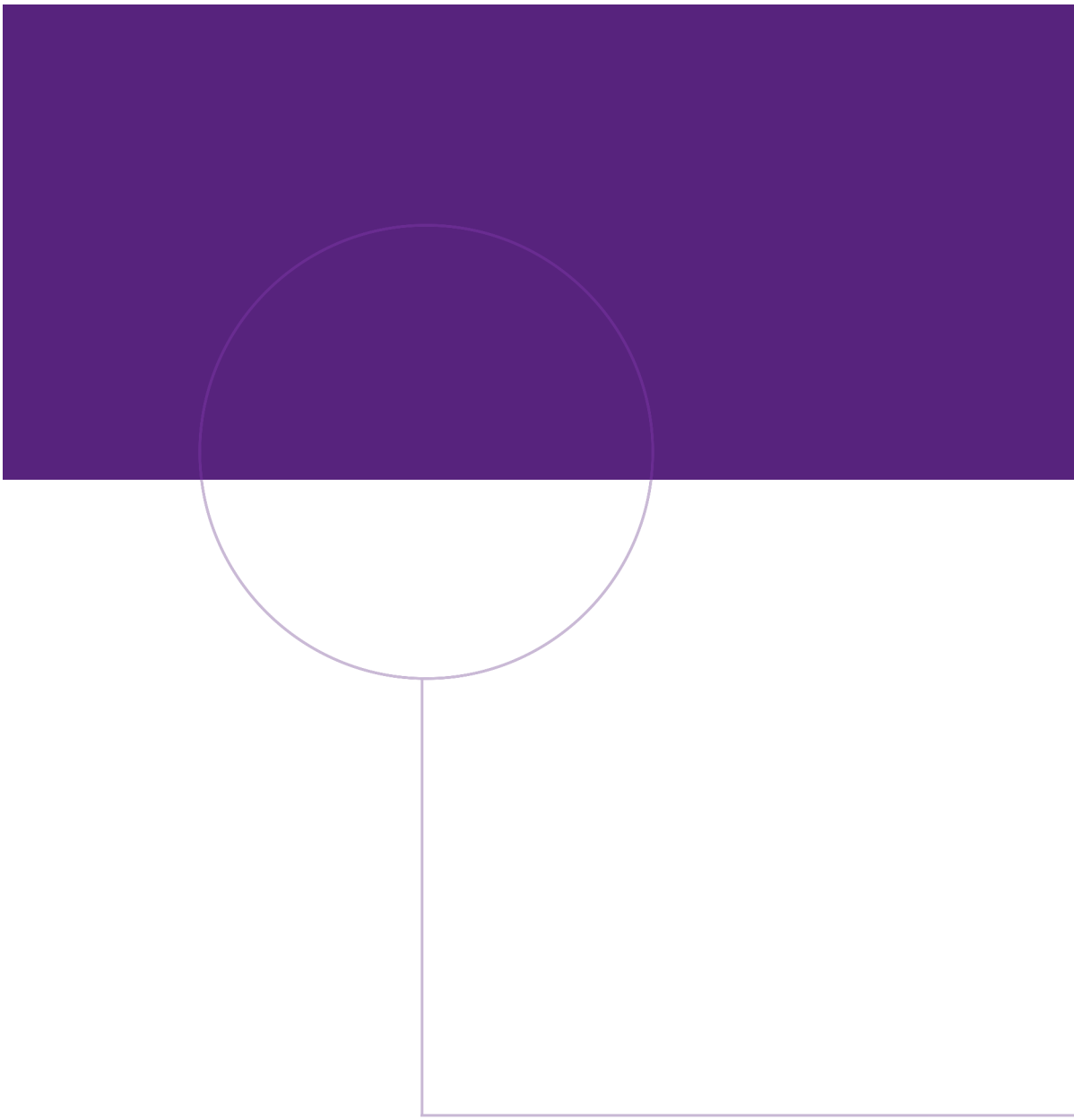
[Wu02] T. Wu, *SRP-6: Improvements and Refinements to the Secure Remote Password Protocol*, http://srp.stanford.edu/srp6.ps, Technical Note, 2002.

[WW16] D. Wang and P. Wang, "On the implications of Zipf's law in passwords", in *ESORICS 2016: 21st European Symposium on Research in Computer Security, Part I*, I. G. Askoxylakis, S. Ioannidis, *et al.*, Eds., ser. Lecture Notes in Computer Science, vol. 9878, Heraklion, Greece: Springer, Cham, Switzerland, Sep. 2016, pp. 111–131.

[YBH+25] Y. Yang, F. Benhamouda, *et al.*, "Gold OPRF: Post-Quantum Oblivious Power-Residue PRF", in *2025 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA: IEEE, May 2025, pp. 259–278. [Online]. Available: https://ieeexplore.ieee.org/document/11023512/.

[YGWX20] Y. Yang, X. Gu, *et al.*, "Efficient Password-Authenticated Key Exchange from RLWE Based on Asymmetric Key Consensus", vol. 12020 LNCS, 2020, pp. 31–49. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085246925&doi=10.1007%2f978-3-030-42921-8_2&partnerID=40&md5=3e16c7d2f653e16cb420cc79372f3763.

[YZYW25] Y. Yang, R. Zhao, *et al.*, "K-pake: Post quantum password authentication key exchange protocol for satellite networks", *Cluster Computing*, vol. 28, no. 4, Feb. 2025. [Online]. Available: https://doi.org/10.1007/s10586-024-04942-1.



NTNU

Norwegian University of
Science and Technology