SoK: Post-Quantum PAKEs

Cryptographic Primitives, Design and Security

Nouri Alnahawi[1,3] ⓘ ⧉, David Haas[2], Erik Mauß[1] and
Alexander Wiesmaier[1,3] ⓘ ⧉

[1] University of Applied Sciences, Darmstadt, Germany
[2] Technical University, Darmstadt, Germany
[3] National Research Center for Applied Cybersecurity ATHENE, Darmstadt, Germany

Abstract. PAKE protocols are used to establish secure communication channels using a relatively short, often human memorable, password for authentication. The currently standardized PAKEs however rely on classical asymmetric (public key) cryptography. Thus, these classical PAKEs may no longer maintain their security, should the expected quantum threat become a reality. Unlike prominent security protocols such as TLS, IKEv2 and VPN, quantum-safe PAKEs did not receive much attention from the ongoing PQC integration efforts. Thus, there is a significant gap in awareness compared to PQC schemes that are subject to the official governmental and institutional standardization processes. In the work at hand, we provide a comprehensive overview of the existing PQC PAKEs focusing on their design rationales, authentication methods and used asymmetric key agreement primitives. We highlight their performance and properties as per their assumed security assurances and practical usage in applications. Moreover, we address PAKE designs that are still non-present in the PQC realm and discuss the possibility of their adaptation. Thus, we offer a detailed reference and derive future work for quantum-safe PAKEs.

Keywords: Systematization of Knowledge · Password Authenticated Key Exchange · Post-Quantum Cryptography · Public-Key Cryptography

1 Introduction

Ever since their emergence in the early nineties [BM92], Password Authenticated Key Exchange (PAKE) protocols became of great importance in the world of (applied) cryptography. According to [HvO22], PAKE applications can be be found in several scenarios such as credential recovery (e.g., ICloud and ProtonMail), device pairing (e.g., E-Passport, bluetooth and WLAN), and E2E secure communication (e.g., Thread and Blackberry Messenger). As the name suggests, PAKEs are used to carry out a key exchange combined with password based authentication. In other words, they allow for establishing secure communication over an insecure channel, where a communication party can prove their identity using a (often human memorable) password or a PIN (Personal Identification Number). The original idea proposed by Bellovin and Merritt was to combine a symmetric encryption scheme with a public-key crypto-system [BM92]. Basically, one encrypts a crucial part of the asymmetric key agreement with a password (or a password-derived value), so that attackers can neither trace the outcome of the agreement back to a possible password, nor actively manipulate the asymmetric key agreement. According to Jablon [Jab96], this can be achieved through a low entropy password if the small password

---

size space is multiplied by the size of the key space of an asymmetric primitive. This concept is seen in protocols such as Encrypted Key Exchange (EKE) [BM92], Password Authenticated Key Agreement (PAK) [Mac02], and Simple Password Exponential Key Exchange (SPEKE) [Jab96], all of which can be instantiated with the Diffie-Hellman (DH) scheme to realize key agreement. Over the last decade, the advances in quantum computing and its threat to (classical) asymmetric cryptography attracted many studies towards realizing PAKEs based on Post-Quantum Cryptography (PQC) primitives.

1.1 Motivation and Contribution

Currently, none of the PAKE schemes selected by IEEE (P1363.2 [IEE09]), ISO/IEC (11770-4 [ISO17]) or IETF (CFRG 104 [For19]) in the recent standardization processes[1] are quantum resistant. Further, and to the best of our knowledge, there does not exist any surveys concerned with PQC PAKEs. In this paper, we address PQC PAKEs (PAKEs built from or on top of PQC primitives), and provide a complete and comprehensive overview of works identified in the literature. These include PQC PAKEs built from lattices and isogenies, in addition to generic Key Encapsualtion Mechanisms (KEM). We investigate the current PQC PAKE proposals and point out the aspects we deem necessary to grasp the differences and issues of constructing PAKEs from PQC schemes. We build upon the systematic review in [HvO22] and adapt their classification of classical PAKEs to PQC ones. Moreover, we extend their categorization to incorporate generic design approaches and thus provide a thorough overview of the current PQC PAKEs. Considering the performance and security of said PAKEs, we collect their respective analysis and benchmarks, and offer a comparison as per their proposed instantiations, parameters, and security models in similar manner to the works in [Jar22] and [HvO22]. Further, we address PAKE designs that are currently non-present in the PQC realm and discuss the possibility of their adaptations and instantiations. Finally, we highlight open issues and future research questions, and summarize the main takeaways from the conducted review.

1.2 Methodology

The presented literature review is a result of an extensive study in the form of a systematization of knowledge (SoK). The reviewed proposals were collected through an exhaustive key-word search (e.g., PQC PAKE, LWE Post-Quantum PAKE, SIDH PAKE etc.) conducted on online database and digital libraries platforms such as *Scholar, ACM, IEEE, CiteSeer,* and *Research Gate*, as well as using the preliminary search results as seed for a forward/backward search using online tools such as *Litmaps* and *Citation Gecko*.

1.3 Related Work

Azarderakhsh et al. [AJK+20] discuss PAKEs from isogeny assumptions, and show the difficulty or even the impossibility of translating DH-based PAKEs to isogenies. To the best of our knowledge, no other works in the literature directly survey PQC PAKEs. The following related work focuses only on classical PAKEs, but has nonetheless provided a valuable foundation for our own overview. For instance, the PAKE overview by Abdalla [Abd14] is one of the earliest works concerned with the design and security goals of PAKE protocols. This work describes the beginnings of PAKE design studies sufficiently (e.g., EKE [BM92] and its variants) and classifies following proposals based on their construction approach. In [Jar22], Jarecki provides a detailed overview on the methods used for constructing PAKEs from classical asymmetric cryptography. The overview offers a thorough analysis on the design and security of PAKEs in different security frameworks, as well as on their

---

[1]We refer the reader to [HvO22] for a complete overview of *classical* PAKEs and more details on the official PAKE standardization processes.

strengths and shortcomings. Hao and van Oorschot [HvO22] present a review of the state-of-the-art of classical PAKEs and provide practical information on their real-world applications. More importantly, the authors offer a complete classification of all reviewed PAKEs in a similar, yet more extensive, manner to [Abd14].

2   Post-Quantum Cryptography

Nowadays, the term classical cryptography is often used in reference to public key crypto-systems based on the hardness assumptions obtained from the integer factorization and discrete logarithm problems. The most prominent classical algorithms and schemes are the *Rivest-Shamir-Adleman* (RSA) crypto-system [RSA78], the renowned *Diffie-Hellman* (DH) asymmetric key agreement scheme [DH76], as well as variants using Elliptic Curve Cryptography (ECC) such as as *Elliptic Curve Diffie-Hellman* (ECDH) and the *Elliptic Curve Digital Signature Algorithm* (ECDSA) [JMV01]. However, these public-key encryption (PKE) and digital signature schemes are expected to be broken by quantum computers utilizing Grover's and Shor's [Gro96, Sho97] algorithms in the near future [CCJ$^+$16, KNW18]. Hence, Post-Quantum Cryptography (PQC) became an established term following the start of the NIST PQC standardization process [CCJ$^+$16] in 2016. Unlike classical cryptography, PQC is based on mathematical problems that presumably can neither be solved efficiently using quantum computers, nor by classical computers for that matter [Ber09, BL17].

2.1   Hardness Assumptions

Including generic KEMs, all of the proposed PQC PAKEs come from two PQC algorithm families. These are *Supersingular Isogenies* (SI) e.g., *Supersingular Isogeny Diffie–Hellman* (SIDH) or *Commutative Supersingular Isogeny DH* (CSIDH), and the lattice *Learning-with-Errors* (LWE) problem and its *Ring Learning-with-Errors* (RLWE), *Module Learning-with-Errors* (MLWE), and *Module Learning-with-Rounding* (MLWR) variants.

SIDH and CSIDH   Generally speaking, isogenies are non-zero homomorphisms of elliptic curves (EC) [Smi18]. One may imagine that they resemble a mapping between ECs yielding a specific mathematical relation (isomorphism). SIs and CSIs are more or less special cases of isogenies. Mainly, they rely on the difficulty of identifying isogenies between ECs, i.e. curves that have the same j-invariants. Finding such mappings is considered a hard problem, since there can be infinitely many of them. Their attractiveness in asymmetric cryptography lies within their striking similarities to the DH scheme. They are hence used to construct the computational and decisional problems similar to DH and ECDH. However, we refrain from elaborate explanation due to a complexity beyond the scope of this paper. That being said, we refer to [Smi18] for further reading. Nonetheless, we note that the SIKE [CCH$^+$19] algorithm, which builds on SIDH, was a NIST round four candidate until its withdrawal due to its sudden break[2]. CSIDH [CLM$^+$18] on the other hand is still deemed secure, and was not effected by the recent break of SIKE.

LWE   A lattice is a discrete subgroup of a multidimensional vector space over real numbers under addition and can be described as a set of points in an n-dimensional space with a periodic structure. There are several classical computational problems in lattices, upon which crypto-systems are based [RHCB21], such as the Shortest Vector Problem (SVP) and the Smallest Integer Solution (SIS). The most relevant problem for PQC PAKEs is LWE (cf. Tab. 1), which was first introduced by Regev in [Reg05, Reg06]. The decisional LWE problem is basically to distinguish between random linear equations (called samples)

---

[2] https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf

from uniform equations, after applying a small amount of noise (called errors), as found in the Regev plain LWE crypto-system [Reg10]. Although lattice LWE is defined in the Euclidean vector space, it is defined on integral lattices from a computational viewpoint, where its representation is a matrix of integers (e.g., modular lattices). Moreover, a lattice base can be replaced by an irreducible polynomial and thus a lattice can be defined as a special subset where all vectors form an ideal in a certain ring (e.g., ideal lattices), which was introduced in the Lyubashevsky-Peikert-Regev ideal RLWE crypto-system [LPR10]. The MLWE crypto-system was defined by Brakerski et al. [BGV14] and further studied by Langlois and Stehlé [LS15]. It takes the construction idea of RLWE a step further to replace the integers by a ring of algebraic integers of a number field. Hence, the MLWE problem generalizes both LWE and RLWE using module lattices. The most notable LWE schemes are the NIST standardization finalist CRYSTALS-Kyber [BDK+18] (MLWE), the round three candidates FrodoKEM [BCD+16] (LWE) and SABER [DKSRV18] (MLWR), and the RLWE key exchange scheme (not a NIST KEM) of Ding et al. [DXL12].

2.2   Key Agreement

Current PQC PAKEs make use of two types of asymmetric key agreement schemes:

1) *Key Exchange (KEX):* Protocol parties combine the exchanged key materials from their respective ephemeral public keys to create a session key utilizing the mathematical properties of the used asymmetric scheme. This method can be found in the classical DH key agreement scheme (Fig. 1a), SIDH (Fig. 1b), and LWE (Fig. 1c).

2) *Key Encapsulation Mechanism (KEM):* Regardless of the used primitive, the protocol receiver (generically) encapsulates a session key based on the public key of the initiator into a ciphertext, and then sends it to the initiator, who in turn (generically) decapsualtes the session key from the ciphertext using their secret key (Fig. 1d).

Alice   **Bob**

a, g, p b

$A = g^a \bmod p$ $\xrightarrow{A,g,p}$

                    $\xleftarrow{B}$ $B = g^b \bmod p$

$K = B^a \bmod p$ $K = A^b \bmod p$

(a) Classical DH Key Agreement

Alice   **Bob**

$k_A \in_R SK_A$ $k_A \in_R SK_A$

$R_A = P_A + k_A Q_A$ $\xrightarrow{E_A, \phi_A(P_B), \phi_A(Q_B)}$ $R_B = P_B + k_B Q_B$

$\phi_A : E \to E_A = E/\langle R_A \rangle$ $\xleftarrow{E_B, \phi_B(P_A), \phi_B(Q_A)}$ $\phi_B : E \to E_B = E/\langle R_B \rangle$

$R_{BA} = \phi_B(P_A) + k_A \phi_B(Q_A)$ $R_{AB} = \phi_A(P_B) + k_B \phi_A(Q_B)$

$K_{\text{Alice}} = j(E_B/\langle R_{BA} \rangle)$ $K_{\text{Bob}} = j(E_A/\langle R_{AB} \rangle)$

(b) SIDH Key Agreement [FTTY19]

Alice   **Bob**

                    $\mathbf{A} \in R_q^{k \times k}$

$s_a, e_a \in R_q$ $s_b, e_b \in R_q$

$\mathbf{b}_a = \mathbf{A}s_a + e_a$ $\xleftrightarrow{\mathbf{b}_b, \mathbf{b}_a}$ $\mathbf{b}_b = \mathbf{A}s_b + e_b$

$K = s_a^t \cdot \mathbf{b}_b$ $K = \mathbf{b}_a \cdot s_b$

$s_a^t(\mathbf{A}s_b + e_b)$ $\approx$ $(s_a^t \mathbf{A} + e_a^t)s_b$

(c) LWE Key Agreement

Alice   **Bob**

                    KEM Parameters

$(pk, sk) \leftarrow \text{KGen}(1^\kappa)$

                    $\xrightarrow{pk}$

                                          $(c, K) \leftarrow \text{Encap}(pk)$

                    $\xleftarrow{c}$

key := Decap(sk, c)   key := K

(d) Abstract KEM Algorithm

Figure 1: High level description of key exchange and encapsulation algorithms

Whereas key agreement from isogenies works (almost) exactly the same as in the case of DH or ECDH over cyclic groups, their security is less mature and rather questionable due to the recent break of SIKE. Key agreement from (noisy) lattices does not produce identical shared keys and requires a so-called reconciliation step through signaling (or hinting) [HPA21]. Lattice-based KEM constructions rather act as a key transport scheme and thus do produce identical shared keys with a negligible margin of error [Pei14] (decryption failures). Whereas a DH-like KEX allows relying on the hardness assumptions of cryptographic

primitives, using KEMs in a black-box manner does not (cf. Sec. 10), and thus requires fulfilling abstract security properties, which we address in the following.

2.3 Security Properties (Notions)

The design of PAKEs, and especially generic constructions, takes several security properties (goals) into account, which the underlying asymmetric scheme must fulfill. These properties mainly address the semantics of a KEX regarding the security of the shared key, the public key, and the ciphertext. For a KEM, similar notions also define the security of the encapsulated (or decapsulated) key, the public (encapsulating) key, and the (decapsulation) ciphertext. Here we note that the exact definitions and security assurances of the following notions differ across the existing literature. In this work, they solely serve the purpose of understanding their usage in PAKE designs. Hence, they are not to be viewed as formal definitions or a comparison of such, which is out of the scope of this paper[3].

Encryption (Key) Security: The *Indistinguishability (IND)* notion expresses the core security of key security in a KEX or a KEM. In general, this property indicates the infeasibility for an attacker to differentiate (distinguish) real, honestly generated values, from random ones [GM84]. This property is present in all PAKE constructions and is considered as the minimum degree required for the security of the final key. The *One-wayness (OW)* property plays a similar role, and denotes the irreversibility of an encryption, i.e., the infeasibility of recovering a value from its corresponding encryption [ABP15].

Public Key Security: Public key *Uniformity or Fuzziness (PKU):* denotes the indistinguishability of real generated public keys from uniform ones, i.e., honestly generated public keys have an equal probability distribution to random ones from the same public key space [BCP+23, AHHR24]. Further, public key *Anonymity (ANO)* expresses the public key privacy, i.e., the difficulty of utilizing information from a ciphertext to reveal which public key was used to create it [GMP22, CDM23]. Note that some works refer to the anonymity of a ciphertext, and not of a public key (e.g., [BCP+23, ABJS24]).

Ciphertext Security: The ciphertext *Robustness (ROB)* notion denotes the binding property of a ciphertext / secret key relationship, i.e., a ciphertext does not decrypt to a valid plaintext for two distinct secret keys [GMP22, CDM23]. Further, ciphertext *Pseudo Randomness (PR)* denotes the indistinguishability of ciphertext and shared key pairs from random ones. i.e., it is infeasible to distinguish between said pairs under knowledge of the plaintext message and the public key used for encryption [Xag22, CDM23]. Finally, the ciphertext *Non-malleability (NM)* expresses the infeasibility to construct ciphertexts that are meaningfully related to a known ciphertext and its initailly corresponding plaintext [DDN91].

Applicable Attacks (Related Security Experiments): Multiple variants of the afore mentioned properties can be obtained under a variety of attacks, which define the capabilities of an adversary interacting with challenges constructed from said notions, and hence provide different degrees of security:

- *Plaintext Checking Attack (PCA):* Adversaries have access to a plaintext-checking oracle that answers queries as to whether given plaintext-ciphertext pairs correspond to each other [OP01].

- *Chosen Plaintext Attack (CPA):* Adversaries can generate arbitrary valid ciphertexts from plaintexts of their own choosing using an honest public key [GM84].

---

[3]We refer to [Poi22] for more details on formal definitions of security notions in asymmetric cryptography.

- *Non-adaptive Chosen Ciphertext Attack (CCA1):* Adveraries have access to a decryption oracle before accessing the challenge ciphertext, i.e., adversaries may choose a set of ciphertexts distinct from the challenge ciphertext and query the decryption oracle to obtain the corresponding plaintexts [NY90].

- *Adaptive Chosen Ciphertext Attack (CCA2):* Adversaries have permanent access to a decryption oracle with the only restriction of not being able to query the challenge ciphertext itself to directly obtain the corresponding plaintext [RS91].

On this basis, it is possible to obtain different notions of security by combining goals with attack models. Ostensibly, there exist a multitude of pathways in which these notions relate to each other (i.e., implications and separations) as shown in [BDPR98, OP01, ABP15, CDM23]. For instance, *IND-CPA* provides a weaker, yet more efficient alternative to *IND-CCA* for scenarios where the ability to check plaintexts is sufficient for the application's security requirements, and *OW* offer security guarantees on a lower level. As a result, *IND-CCA* implies *IND-CPA*. Further, a crypto-system may exhibit semantic security against *CPA*, or even *CCA1*, yet it may remain malleable. However, achieving complete semantic security, and therefore *CCA2* is equivalent to achieving non-malleability against *CCA2*. In consequence, it is widely accepted in the cryptographic research community that the *IND-CCA2* model is the preferable notion of security for a general purpose PKE scheme.

That being said, unlike PAKEs built directly from PQC primitives in white-box manner (e.g., [KV09, DAL$^+$17]), the emphasis on the security properties is mostly found in generic PAKE constructions. This is due to the impossibility of involving the hardness assumptions of the chosen primitives for proof reductions in a black-box design. In this case, the generic construction defines a set of required properties, and utilize a KEM that fulfill them in concrete instantiations and implementations. According to [Jar22], the chosen PKE for a PAKE has to be at least *IND-CPA* secure. Since all KEMs fulfill this property, most recent works focus on finding PQC KEMs that also fulfill properties such as *OW*, *PKU* and *ANO*. It is also worth mentioning that NIST PQC KEMs are considered *IND-CCA* secure, since they apply the generic Fujisaki-Okamoto (FO) transform [FO99] to lift the underlying PKEs from *CPA* to *CCA2* security [Unr20]. This transformation was a requirement for all NIST PQC KEMs throughout the standardization process.

2.4   SPHF, OPRF and NIZK Systems

Generally speaking, *Smooth Projective Hash Functions* (SPHF), *Oblivious Pseudo Random Functions* (OPRF), and *Non-Interactive Zero-Knowledge* proofs (NIZK) in PAKEs mainly serve as supporting components for either establishing a trusted setup or realizing commitment schemes mainly w.r.t. users and their public keys.

SPHF   Originally, Cramer and Shoup introduced the *Smooth Projective Hash Function* (SPHF) [CS02] in order to obtain hash proof systems with IND-CCA security. Gennaro and Lindell proposed a generalized SPHF [GL03] for its many attractive properties and purposes such as implicit designated verifier proofs of membership. The use of SPHFs in PAKEs was presented by Katz, Ostrovsky, and Yung [KOY01] and also Gennaro and Lindell [GL03], which is known as the KOY-GL paradigm. The basic idea is that an SPHF defined over a language allows to hash a value (word) in two different ways, with the hashing key (secret key), or with the associated projection key (public key). If the word is in the language, both ways of hashing will yield the same hash value. However, if it is outside the language, the hash obtained using the secret must be statistically indistinguishable from a random value, even with knowledge of the public key. One of the earliest PQC PAKEs levering these properties is the use of Approximate Smooth Projective Hash systems (ASPH) by Katz and Vaikuntanathan [KV09] (cf. Sec. 4).

OPRF The first *Pseudo Random Function* (PRF) as demonstrated by Goldreich et al. [GGM86] dates back to 1986, and 18 years later, Naor and Reingold introduced the idea of interactive and oblivious evaluation of such functions [NR04]. Based on the Naor-Reingold PRF, Freedman et al. formalized the definition of the first two-party protocol known as an Oblivious PRF [FIPR05]. The general idea of an OPRF is to associate a keyed PRF with a protocol execution between a server and a user. The server holds the key for the function and the user provides an input to that function. The main catch is that the user can learn the output of the PRF at the end of the execution, whereas the server does not learn anything about the input of the user. We refer the reader to [CHL22] for a complete overview on the evolution, applications and different types of OPRFs. That being said, the most notable example of the usage of OPRF in PAKE constructions is the augmented OPAQUE protocol [JKX18], which utilizes the verifiable hash DH-OPRF as proven secure by Jarecki et al. in [JKK14, JKKX16]. As far as post-quantum security is concerned, almost all practical OPRF instantiations rely on classical hardness assumptions [CHL22], with the exception of ones based on symmetric primitives and garbled circuit (e.g., [FOO23]). Only a few recent works provide OPRF constructions based on PQC, more precisely from lattices [ADDS21, ADDG24] and isogenies [BKW20, HHM$^+$24, DdSGP24]. Currently, there are still no PQC PAKE construction utilizing quantum-secure OPRFs.

NIZK *Zero-Knowledge Proofs* (ZKP), first introduced by Goldwasser et al. [GMR85], are cryptographic constructions that enable one party (a prover) to exhibit its knowledge of a certain property to another party (a verifier), without revealing the property itself. In other words, ZKPs allow sharing a proof of holding a specific secret without sharing the actual secret. In PAKEs, this property or secret could be the long lived key (e.g., the password) or an honest public key pair. While interactive proofs require multiple rounds of interaction, Non-Interactive Zero-Knowledge Proofs (NIZK), first introduced by Blum et al. [BFM88], require only one message from a prover to a verifier, as they make use of a Common Reference String (CRS) for an initial setup. NIZKs have already seen use in some classical PAKE applications such as J-PAKE [HR10], which employs the Schnorr protocol [Sch91]. Benhamouda et al. [BBDQ18] discuss how to construct 3, 2, and 1-round PAKEs using ASPHs and NIZKs, which we recommend for further reading.

3 PAKE Classification and Security Models

Equipped with basic knowledge regarding cryptographic building blocks and security assumptions relevant to (PQC) PAKE designs, we can now establish an understanding for the following classification system and concrete constructions. Nonetheless, first we recall that unlike key negotiation and agreement found in protocols such as TLS and IKEv2, Password Authenticated Key Exchange (PAKE) protocols, as the name suggests, aim at establishing a session key between communication parties over insecure (not-trusted) channels, and usually without static public keys or certificates. Formally, a PAKE protocol is a key exchange mechanisms that provides authentication and secure (ephemeral) symmetric shared secretes based solely on a low entropy *long-lived-key* (i.e., password), and a secure asymmetric cryptographic primitive [BM92]. Depending on the actual usage of the password and the way it is stored, and the underlying hardness assumptions, PAKEs can be categorized into several classes and types, as explained in the following sections.

3.1 Classification

We adopt the classification system in [HvO22] based on the authentication method and password usage, and slightly adapt it for our PQC PAKE classification:

C1) *Password Encrypted Public Key*, aka **EKE-style** PAKE, where the password is used directly to encrypt a public key using a symmetric encryption scheme based on an ideal cipher (e.g., CAKE [BCP+23]).

C2) *Password Modified Public Key*, aka **PAK-style** PAKE, where the password is used to modify the public key while preserving the underlying hardness assumption in hash to group (H2G) manner (e.g., RLWE-PAK [DAL+17]).

C3) *Trusted Setup*, multiple approaches, where predefined trusted parameters are required to achieve authentication (e.g., KV-PAKE [KV09] and GA-PAKE [AEK+22a]).

Although [HvO22] introduced five design classes for classical PAKEs, only classes C1, C2, and C3 apply to the current PQC PAKEs, as classes C4 and C5 do not (yet) have any representatives in the PQC realm (cf. Sec. 8). Moreover, some works could be categorized into more than one class at the same time (e.g., a password modified public key combined with a trusted setup). Arguably, generic PAKE constructions may also be considered a class of their own. However, these PAKEs also fall into the same design classes regarding their password usage methods. They differ only in the underlying crypto-systems used for concrete instantiations. Therefore, we opted to summarize the reviewed PQC PAKEs in this paper (cf. Sec. 4) according to: 1. the underlying PQC family (i.e., lattices, isogenies or generic), 2. the adapted classification into C1, C2 and C3 from [HvO22], 3. whether balanced or augmented, and 4. chronological order. An overview of all surveyed PAKE protocols with their respective properties is presented in Tab. 1. The landscape table consists mainly of two parts: The first half contains balanced PAKEs, while the other half contains augmented ones. In each part we group PAKEs into said classes, within which they are listed in chronological order. The columns indicating the security model and underlying assumptions allow more than one value, as many constructions require multiple models and include instantiations using different primitives. We deem a PAKE fully quantum-safe provided that its formal analysis does not involve classical security models (e.g., IC or ROM), nor classical hardness assumptions (e.g., DDH or ECDH).

3.2   Balanced and Augmented PAKEs

The most important security characteristics of PAKEs are resisting *offline dictionary attacks*, surviving *online dictionary attacks* targeting the used password, and preventing *Man-in-the-Middle (MitM) attacks* targeting the cryptographic key agreement [Jab96]. Moreover, PAKEs should preferably provide *session-key security* and *perfect forward secrecy* (PFS) [HvO22]. PAKEs fulfilling these requirements are referred to as *Balanced* [HvO22]. Since online attacks are relatively easy to deal with through limiting the number of password entry trials (usually three), the security of a PAKE protocol heavily relies on its resistance to offline-dictionary attacks. In other words, even an attacker with substantial resources and enough time should not be able to guess the password from the public transcript of a protocol execution. However, a stolen or pre-computed password could be used directly in impersonation attacks. PAKEs that also protect against *server compromise* and *pre-computation attacks* are thus referred to as *Augmented* [HvO22], where the value of the pre-shared password or PIN is stored only as a one-way transformation on the server.

3.3   Security Models and Idealized Objects

Arguably whenever possible, security proofs should be given in the standard model. This is due to the fact that the standard model allows for security proofs based solely on complexity (hardness) assumptions, which state that an attacker cannot solve a certain complex problem in polynomial time (e.g., integer factorizing). That is where the attacker's

Table 1: PQC PAKE Overview / Landscape

Class	Scheme	Year	Security Model	Assumptions	Proof Method	Generic-Safed²	Quantum-Safe³	Peer-Reviewed	2-Party	3-Party	Provide Impl.	Benchmarks	Recomm. Param.
Balanced													
C1	Terada, Yoneyama [TY19] ((C)SIDH-EKE)	2019	IC, ROM	SIDH, CSIDH	BPR			✓	○		✓		
	Dos Santos et al. [DGJ23] (HIC-EKE)	2023	IC, ROM	MLWE, MLWR	UC	✓		✓	○				
	Beguinet et al. [BCP+23] ((O)CAKE)	2023	IC, ROM	MLWE	UC	✓		✓	○				
	Alnahawi [AHHR24] (OCAKE)	2023	IC, ROM	MLWE, LWE	BPR	✓			○		✓		
	Pan, Zeng [PZ23] (CAKE)	2023	IC, ROM	LWE	BPR	✓		✓	○				
	Arriaga et al. [ABJS24] (CHIC)	2024	IC, ROM	MLWE	UC	✓			○		✓	✓	✓
	Alnahawi et al. [AASAW24] (NICE-PAKE)	2024	ROM	NLWE / whLWE	BPR	✓	✓?		○				✓
C2	Zhu, Geng [ZG15]	2015	-	SIDH/CSIDH	CK				○				
	Alsayigh [Als16]	2016	ROM	RLWE	BPR				○				✓
	Ding et al. [DAL+17, Din17] (RLWE-PAK-PPK)	2017	ROM	RLWE	BPR			✓	○		✓		
	Gao et al. [GDL+17] (RLWE-PAK-PPK)	2017	ROM	RLWE	BPR				○		✓		
	Taraskin et al. [TSJL20] (SIDH-PAK)	2019	ROM	SIDH	BPR				○		✓		✓
	Yang et al. [YGWX19] (RLWE-PAK)	2019	ROM	RLWE	BPR	✓			○		✓		✓
	Jiang et al. [JGH+20] (PAKEs)	2020	ROM	LWE, RLWE	BPR	✓			○		✓		✓
	Ren et al. [RGW23]([RG22]) (MLWE-PAK)	2022	-	MLWE	Hybrid	✓			○		✓	✓	✓
	Seyhan, Akleylek [SA23]	2023	ROM	MLWR	Hybrid				○		✓	✓	✓
	Basu et al. [BSIA23] (MLWR-2PAKA)	2023	ROM	MLWR	DY	✓			○				✓
C3	Katz, Vaikuntanathan [KV09]	2009	CRS	LWE	BPR	✓	✓		○				
	Xu et al. [XHCC17] (RLWE-3PAKE)	2017	ROM	RLWE	BPR					○	✓		✓
	Zhang, Yu [ZY17]	2017	CRS, ROM	LWE	BPR				○				
	Choi et al. [CAK+18] (AtLast)	2018	ROM	RLWE	BPR			✓		○			
	Li, Wang [LW18]	2018	CRS	LWE	BPR	✓	✓		○				
	Li, Wang [LW19]	2019	CRS	LWE	BPR	✓	✓		○				
	Karbasi et al. [KAA19] (Ring-PAKE)	2019	CRS	RLWE	BPR	✓	✓		○				
	Yin et al. [YGS+20]	2020	ROM	LWE	BPR		✓		○	○			
	Lyu et al. [LLH24]	2024	(Q)ROM	LWE, GA-DDH	UC	✓	✓	✓	○				
Augmented													
C2	Gao et al. [GDLL17]	2018	-	RLWE	UC			✓	○		✓		✓
C3	Zhu et al. [ZHS14]	2014	-	SIDH	CK			✓		○			
	Feng et al. [FHZ+18]	2018	ROM	RLWE	BPR			✓	○		✓		✓
	Liu et al. [LZJY19]	2019	ROM	RLWE	Hybrid					○	✓	✓	✓
	Dabra et al. [DBK20] (LBA-PAKE)	2020	ROM	RLWE	FTG			✓	○		✓		✓
	Li et al. [LWM22]	2020	CRS	LWE, LWR	BPR	✓	✓	✓	○		✓		✓
	Tang et al. [TLZ+21]	2021	ROM	RLWE	BPR			✓		○	✓		✓
	Islam, Basu [IB21] (BP-3PAKA)	2021	ROM	RLWE	BPR			✓		○	✓		
	Ding et al. [DCQ22]	2022	RoR	RLWE	FTG			✓	○		✓	✓	✓
	Abdalla et al. [AEK+22a] (X-GA-PAKE)	2022	CRS	CSIDH	BPR	✓			○				
	Wang et al. [WCL+23] (LB-ID-2PAKA)	2023	ROM	MLWE	BPR			✓	○				
	Dharminder et al. [DRD+23]	2023	Standard	RLWE	Hybrid			✓	○		✓		✓
	Dadsena et al. [DJRD23]	2023	ROM	RLWE	BPR			✓	○		✓		✓
	Kumar et al. [KGKD23]	2023	ROM	RLWE	BPR			✓	○		✓		✓
	Guo et al. [GSG+23]	2023	ROM	MLWE	BPR			✓		○	✓		✓
	Chaudhary et al. [CKS23]	2023	ROM	RLWE	BPR			✓		○	✓		✓

[1] Properties with a question mark denote claims that we were not able to verify.

[2] Denotes whether a PAKE follows a generic design without relying on a specific scheme (e.g., using KEMs opposed to using PKEs).

[3] Denotes whether a PAKE relies only on quantum-safe building blocks (e.g., proofs in the QROM opposed to proofs in the ROM).

capabilities are only limited by their computational power, i.e., an arbitrary polynomial-time machine [CGH04]. Nevertheless, the following models are often used in PAKE security proofs, since they allow for additional complexity-theoretic hardness assumptions [Bla06], which make proving the security less difficult than in the standard model.

ROM   A *Random Oracle* (RO) is an ideal primitive that models a random hash function that responds to each query to a given fixed-length input value with a corresponding random output [BR93]. Additionally, a RO keeps a record of all placed queries, and responds with the same value for a previously queried input. To prove security in the ROM means constructing a convincing argument by first replacing some function in the actual protocol, by an idealized one that returns a random value as described. Hence, the ROM is basically present in almost all PAKE design classes, since its usage is required to model hash and key derivation functions. Nearly all ROM-based PAKE constructions surveyed in

this paper are proven in classical settings (cf. Tab. 1), and are mostly instanstiated using a secure hash function (e.g., *Hash-to-group (H2G)* as in [DAL$^+$17]).

QROM   Boneh et al. [BDF$^+$11] proposed the *Quantum RO Model* (QROM) and addressed the issues with the classical ROM in the presence of adversaries with quantum capabilities, who may evaluate hash functions on superpositions. Although it was not clear, whether proofs in the ROM also hold in the QROM, new proof techniques clarified that many ROM constructions remain secure in the QROM [YZ21]. However, despite the existence of certain types of ROM to QROM lifting theorems, a fully general lifting theorem for all ROM security reductions seems yet impossible [YZ21]. Among the works surveyed in this paper, only one PQC PAKE provides a security proof in the QROM (cf. Tab. 1).

IC Model   An *Ideal Cipher* (IC) serves modeling block ciphers (e.g., AES) as idealized objects similar to hash functions in the ROM with some exceptions [Bla06]. Its main advantage is defining the behavior of a cipher, where each encryption maps to an independently random permutation that belongs to the same set of possible input values. In other words, it models a random block cipher as being chosen uniformly from the set of all possible block ciphers [Bla06]. Similar to a ROM, the IC provides oracle access for forward queries on encryption, which are kept record of. However, an IC provides oracle access for backward queries on decryption as well. Nonetheless, unlike instantiations using DH over finite fields, applying an IC to e.g., LWE samples is non-trivial and could result in values that do not exist in the key space (i.e., invalid keys). Considering adversaries with quantum capabilities, it is not possible to keep record of queries due to the quantum no-cloning theorem. Very few works in the literature [AR17, HY18, SS19] address the notion of the *Quantum* IC model (QICM), yet do not show how to fully obtain the capabilities of a classical IC. The work by Unruh [Unr23] builds upon the idea of compressed function oracles (CFO) and takes a step forward in modeling keyed invertible permutations (i.e., IC) in quantum settings by introducing compressed permutation oracles (CPO). Nevertheless, and despite the novelty of the proposed approach, it is not yet formally proven that a CPO is indistinguishable from a truly random permutation [Unr23]. We note that using an IC in PAKE construction is mostly found in the design class C1 (cf. Tab. 1).

HIC   To avoid the afore mentioned issues, Dos Santos et al. [DGJK22] introduced a relaxation of the IC model called *Half Ideal Cipher* (HIC), which is realized through a modified 2-Feistel construction (m2f) using a block cipher and hash functions. This construction also inspired the work by Arriaga et al. [ABJS24], where a compact m2f is used over uniform bit-strings from so-called KEMs with splittable public keys. The usage of HIC in PAKEs is also found in the design class C1.

CRS Model   The *Common Reference String* (CRS) model was introduced by Blum et al. [BFM88] as a way to realize non-interactive zero-knowledge proof systems (NIZK) by providing a shared string accessible to and trusted by all protocol parties. Usually, the CRS is drawn from a pre-defined uniform distribution (randomness source) that does not reveal any information about the way the string is generated. A Structured Reference String (SRS) is a variant of a CRS where the string is structured, which is mainly used in NIZK design. In the context of PAKEs in general, and PQC PAKEs in particular, a pre-shared public key of the protocol initiator is used as a CRS in a trusted-setup (mostly with a prior registration phase), and thus serving as means for authentication. Since a public key is (theoretically) indistinguishable from a random string taken from a uniform distribution, a PAKE in the CRS model is widely accepted in the community. That being said, most PQC PAKEs constructions in the CRS model make use of SPHFs and ASPHs or NIZKs such as [KV09, ZY17, BBDQ18, KAA19], and belong to the design class C3.

Here we note that using a CRS (very often) implies security proofs in the standard model, except for RLWE-PAK-like PAKEs relying on the H2G mechanism in the ROM.

CoR Setup (Multi-Setups)   In 2008, Groth and Ostrovsky [GO14] introduced the *Multi-String* (Multi-CRS) model to mitigate the risks of having only one trusted authority generating a random string. Following this work, other methods and ideas were developed to distribute trust among multiple setups as discussed in [XZZ24]. The *CRS-or-RO-Setup* (CoR) was unified in 2014 by Katz et al. [KKZZ14], who showed the impossibility of obtaining a secure construction from a straightforward setup combining one CRS and one RO [XZZ24]. While this result also holds for PAKEs, Xiao et al. [XZZ24] showed how to maximize the utility of a such setup by extending the model to a so called *Fine Grained* CoR-Setup, where either the CRS or the RO may fail, yet it remains possible to build a secure PAKE. Still, this type of setup has no representatives in the PQC realm.

3.4   Adversarial (Threat) Models and Frameworks

The security of key agreement protocols is most commonly proven in one of the following frameworks, which model the capabilities of an adversary in a *simulation* of a cryptographic protocol: 1) *Bellare-Pointcheval-Rogaway (BPR)* model [BPR00] and the extended eBPR [AFP05] variant. 2) *Universal Composability (UC)* model [Can01]. The BPR model defines a set of *queries* that an adversary may submit throughout a series of so-called games. The adversary's goal is to either guess the correct password or distinguish real session keys from random ones by outputting a test bit. Hence, the BPR and eBPR models are often referred to as *Find-then-Guess* (FTG), and *Real-or-Random* (RoR) respectively for single and multiple test queries. The UC model on the other hand, defines *ideal* functionalities emulating a protocol, and and environment acting as a distinguisher interacting with honest parties and adversaries. The environment outputs a bit at the end of an execution indicating whether it was interacting with the real protocol or its ideal emulation. Nonetheless, both models include changes in behavior through steps (i.e., game hops). In each game the protocol is changed in a way that an adversary's advantage in breaking the original protocol remains statistically negligible. These changes are defined based on the protocol interface (i.e., exchanged messages) and the idealized objects or functionalities. Although the UC model is claimed to provide better security proofs, almost all of the current PQC PAKEs are proven in the BPR model (cf. Tab. 1). This is most likely since the UC framework is supposedly yet to be shown suitable for lifting security proofs from classical to quantum settings. Other less common frameworks in the context of PAKEs are the *Dolev-Yao (DY)* [DY83], *Canetti-Krawczyk (CK)* [CK01] and *Benhamouda-Blazy-Ducas-Quach (BBDQ)* [BBDQ18] models.

4   PQC PAKEs

Despite the novelty and to a certain extent the immaturity of some PQC schemes, the work on PQC PAKEs dates back to even before the start of the NIST PQC standardization process. The LWE PAKE by Katz and Vaikuntanathan [KV09] in 2009 and the isogeny-based PAKE by Zhu et al. [ZHS14] in 2014 may therefore, and to the best of our knowledge, be considered the very first PQC PAKEs. However, the RLWE PAKE by Ding et al. [DAL+17] in 2017 marks the emergence of many other PQC PAKEs, as shown in the timeline in Fig. 2.
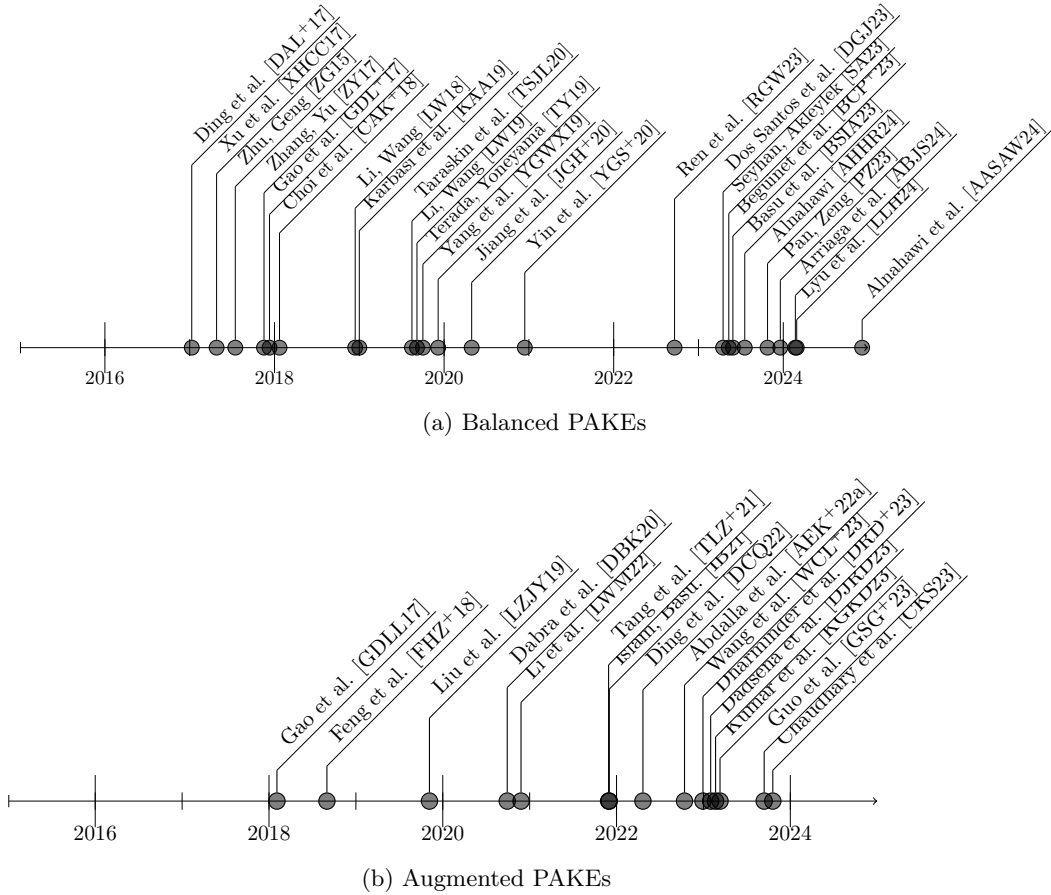
(a) Balanced PAKEs

(b) Augmented PAKEs

Figure 2: Timeline of a) Balanced and b) Augmented PQC PAKE Publications

4.1   Overview

Up to date, we collected roughly 50 PQC PAKEs, which were thoroughly reviewed except for eight papers[4]. These works consist of over 30 PAKEs based on lattice LWE and variants. Whereas the remaining works consist of five SIDH and CSIDH isogeny PAKEs, and seven generic KEM PAKEs almost entirely instantiated using LWE. In the following we categorize said works according to their underlying PQC assumptions, and whether balanced or augmented within their respective design classes. For each class, and before diving into the high-level review, we take a closer look at a respective representative PAKE (Tab. 2) with a technical description in comparison to the corresponding classical design.

Table 2: PQC PAKE Representatives for each Class and Corresponding Classical Designs

Class	PQC PAKE(s)	Classical PAKE(s)
C1	CAKE [BCP+23]	EKE2 [BPR00]
C2	RLWE-PAK [DAL+17]	PAK [Mac02]
C3	KV-PAKE [KV09] / GA-PAKE [AEK+22b]	KOY-PAKE [KOY01] / SPEKE [Jab96]

---

[4]Ye et al. [YHL13] (full-text unavailable), Ding and Fang [DF11] and Jheng et al. [JTCW18] (incomplete works), Yu et al. [YLZ+21] and Rewal et al. [RSM+23] (paid access), Zi-chen et al. [ZTJ21] and Shu et al. [SWL+21] (written in Chinese), and Seyhan and Akleylek [SA24] (unknown assumption).

4.2 Lattice-Based

Class C2: PAK-Style with LWE and Variants in the ROM

As previously noted, Ding et al. [DAL$^+$17] proposed the first RLWE PAKE based on Ding's RLWE KEX and reconciliation mechanism [DXL12]. The PAKE construction is inspired by MacKenzie's classical PAK and PKK [Mac02] and follows a very similar security analysis. The variant following PAK is a 3-pass PAKE (consists of 3 messages) and provides mutual explicit authentication. The other variant following PPK is a 2-pass PAKE and provides implicit authentication. The security proof is given in the ROM and the BPR model. The authors also introduce the *Pairing with Errors* (PWE) and the decisional (D)PWE problems relying mainly on the H2G method for the public key authentication, which can be reduced to the RLWE problem. In other words, the hash value of the password is added to the public key, which results in shifting (masking) the RLWE sample to a new one within the same lattice. A previous version of this PAKE exists as a PhD thesis [Als16], and the first author of [DAL$^+$17], Jintai Ding, submitted a patent later on for this construction [Din17].

Technical Description: The 3-pass RLWE-PAK protocol (Fig. 3) resembles the original DH-based PAK protocol (Fig. 4). The client initiates the protocol by randomly sampling s_C, e_C (the RLWE secret and error terms) and computing α (the RLWE public key), γ (the hashed password), $m = \alpha + \gamma$ (the shifted RLWE sample i.e., public key), and finally sending $< C, m >$ to the Server. The server verifies if $m \in R_q$, aborting if the check fails. It then similarly samples s_S, e_S, computes μ and recovers $\alpha = m + \gamma'$. In the following steps, the server computes k_S (DH-like key agreement) to finally compute $w = \text{Cha}(k_S) \in \{0,1\}^n$ and $\sigma = \text{Mod}_2(k_S, w)$. The server sends μ, w and k to the client, who in turn checks if $\mu \in R_q$, aborting if the check fails. Else, the client computes k_C and σ. Both client and server check if the pre-keys match using two hash functions. Finally, they can derive the session key $sk_C = sk_S = H_4(C, S, m, \mu, \sigma, \gamma')$.

Client $\mathcal{C}$		Server $\mathcal{S}$
Input $\mathcal{S}, pw$		$\gamma' = -\text{H}_1(pw_\mathcal{C})$
Sample $s_\mathcal{C}, e_\mathcal{C} \leftarrow \mathcal{X}_\beta$		Sample $s_\mathcal{S}, e_\mathcal{S} \leftarrow \mathcal{X}_\beta$
$\alpha = as_\mathcal{C} + 2e_\mathcal{C} \in R_q$		$\mu = as_\mathcal{S} + 2e_\mathcal{S} \in R_q$
$\gamma = \text{H}_1(pw_\mathcal{C})$		Abort if $m \notin R_q$
$m = \alpha + \gamma$	$\xrightarrow{<\mathcal{C},m>}$	$\alpha = m + \gamma'$
Abort if $\mu \notin R_q$		$k_\mathcal{S} = \alpha s_\mathcal{S}$
$k_\mathcal{C} = s_\mathcal{C}\mu$		$w = \textbf{Cha}(k_\mathcal{S}) \in \{0,1\}^n$
$\sigma = \textbf{Mod}_2(k_\mathcal{C}, w)$	$\xleftarrow{\mu,w,k}$	$\sigma = \textbf{Mod}_2(k_\mathcal{S}, w)$
$\gamma' = -\gamma$		$k = \text{H}_2(\mathcal{C}, \mathcal{S}, m, \mu, \sigma, \gamma')$
		$k'' = \text{H}_3(\mathcal{C}, \mathcal{S}, m, \mu, \sigma, \gamma')$
Abort if $k \neq \text{H}_2(\mathcal{C}, \mathcal{S}, m, \mu, \sigma, \gamma')$		
else $k' = \text{H}_3(\mathcal{C}, \mathcal{S}, m, \mu, \sigma, \gamma')$	$\xrightarrow{k'}$	Abort if $k' \neq k''$
$sk_\mathcal{C} = \text{H}_4(\mathcal{C}, \mathcal{S}, m, \mu, \sigma, \gamma')$		$sk_\mathcal{S} = \text{H}_4(\mathcal{C}, \mathcal{S}, m, \mu, \sigma, \gamma')$

Figure 3: RLWE-PAK [Din17]

Client		**Server**
Input: S, π		$\pi_S[C] = \langle (H_1(\pi_C))^{-1} \rangle$

$x \xleftarrow{R} \mathbb{Z}_q$

$\alpha \leftarrow g^x$

$\gamma \leftarrow H_1(\pi)$

$m \leftarrow \alpha \cdot \gamma$

$$\xrightarrow{\langle C, m \rangle}$$

$$\text{Abort if } \neg ACCEPTABLE(m)$$

$$y \xleftarrow{R} \mathbb{Z}_q$$

$$\mu \leftarrow g^y$$

$$\gamma' \leftarrow \pi_S[C]$$

$$\alpha \leftarrow m \cdot \gamma'$$

$$\sigma \leftarrow \alpha^y$$

$$k \leftarrow H_2(\langle C, S, m, \mu, \sigma, \gamma' \rangle)$$

$\sigma \leftarrow \mu^x$ $\qquad \xleftarrow{\langle \mu, k \rangle} \qquad k'' \leftarrow H_3(\langle C, S, m, \mu, \sigma, \gamma' \rangle)$

$\gamma' \leftarrow (\gamma)^{-1}$

Abort if $k \neq H_2(\langle C, S, m, \mu, \sigma, \gamma' \rangle)$

$k' \leftarrow H_3(\langle C, S, m, \mu, \sigma, \gamma' \rangle) \qquad \xrightarrow{k'} \qquad \text{Abort if } k' \neq k''$
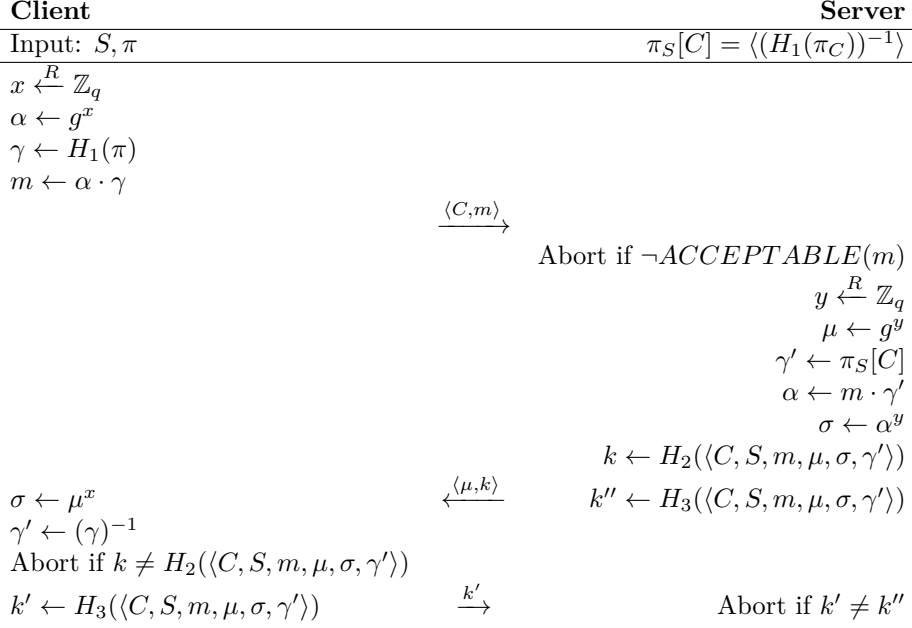
Figure 4: The PAK Protocol [Mac02]

In 2017, Gao et al. [GDL$^+$17] proposed an integration of RLWE-PPK in the TLS library and provided a C++ implementation in the NFLlib library, improving the performance of the original construction in Alsayigh's PhD thesis. Yang et al. [YGWX19] modified this construction using a new reconciliation mechanism based on asymmetric key consensus [JZ16]. The authors claim higher bit-security levels, and provide an optimized implementation in C, stating that their construction is 12x faster than RLWE-PAK. Ren et al. [RGW23] (preliminary version in [RG22]) also proposed a modification of the RLWE-PAK construction using MLWE and the CDF-Zipf [WCW$^+$17] model within a similar BPR security proof in the ROM, in order to model the adversary's ability of using the PWE assumption. The authors also provide a thorough comparison to previous constructions showing that their PAKE is more advantageous in both bit security and performance, most likely due to the use of their own optimally-balanced key consensus with noise error reconciliation mechanism over MLWE. Seyhan and Akleylek [SA23] proposed the first Learning-with-Rounding (LWR) PAKE protocol SABER.PAKE. As the name suggests, the construction is based on module LWR (MLWR), yet the construction idea is the same as in RLWE-PAK. The authors give a security proof in the ROM and a hybrid model from BPR and MacKenzie [Mac02]. They provide thorough benchmarks and claim smaller key sizes and CPU cycles than other lattice constructions. However, roughly a year later, Cao and Liu [CL24] showed that Saber.PAKE is vulnerable against offline dictionary attack and impersonation attack by, where an impersonating adversary can utilize publicly transmitted hash values to test passwords at will, and thus compute the corresponding session key. Basu et al. [BSIA23] proposed a hybrid construction from MLWR in the ROM combined with user certificates. The authors claim that using a new reconciliation mechanisms (modified HiHo) makes session keys unbiased and that their construction provides resistance against key compromise attacks. They provide a security proof in the DY threat model and provide benchmarks for key sizes, failure probability, and bandwidth.

Class C2: Outlier

Jiang et al. [JGH+20] proposed new techniques to construct a PQC PAKE in the standard model based on LWE and RLWE, and associated ASPH systems over a commitment scheme. The authors suggest a new reconciliation mechanism for the LWE key agreement and a new key-fuzzy Message Authentication Code (KF-MAC) for the final key verification. The security proof is provided in the BPR model and does not rely on the ROM. This 3-pass construction interestingly differs from other ASPH-based PAKEs (cf. Class C3 in the following) through its approximate key establishment, which is reconciliated later on, and verified via a commitment scheme. We note here that most (R)LWE PAKEs with reconciliation follow the previously described RLWE-PAK [DAL+17] approach without using ASPHs or NIZKs. However, although this construction is more similar to those described in the following subsection (Class C3), strictly speaking it belongs to Class C2. Gao et al. [GDLL17] proposed an *augmented* PAKE in the form of a secure remote password (SPR) protocol based on the RLWE KEX scheme of Ding [DXL12] and the previously mentioned RLWE-PAK. The authors claim security in the UC model, but do not provide a full proof. They implement the protocol in C++ using NFLlib. Benchmarks for 209-bit security are compared to the classical SRP showing a 3x speed-up using RLWE.

Class C3: KOY-GL-Style with ASPHs and NIZKs (mostly in the CRS Model)

As already mentioned, the lattice-based PAKE by Katz and Vaikuntanathan [KV09] is most likely the first PQC PAKE built from an LWE PKE. The authors showed how a modification of the Genarro-Lindell framework [GL03] is used to construct a PAKE from an IND-CCA encryption scheme and an associated ASPH. The protocol consists of three messages and relies on a CRS for a trusted setup using an LWE public key combined with said ASPH. Mainly, the protocol parties exchange CCA secure ciphertexts, from which they attempt to compute ASPH values and execute a reconciliation to derive a final session key. This reconciliation first extracts a bit from the noisy ASPH value and then applies an error-correcting code (ECC) to finish the reconciliation [JGH+20].

Technical Description: The 3-pass KV-LWE-PAKE (Fig. 5) employs an SPHF in similar manner to the KOY-PAKE [KOY01] (Fig. 6). First, the client runs a key generation algorithm to generate the verification key and secret (signing) key pair (VK, SK). They proceed by setting a label and encrypting the password w to obtain the ciphertext $C := \mathrm{Enc}_{pk}(\mathrm{label}, w; r)$. After receiving the message (Client|VK|C), the server computes its own encryption of the password to obtain the ciphertext C'. It continues by choosing a random hash key and computing the projection $s' := \alpha(k', \mathrm{label}, C)$, sending both C' and s' to the client. Upon receiving the server's ciphertext and projection, the client chooses it's own random hash key to compute the projection $s := \alpha(k, \mathrm{label}', C')$. At this point, the client computes a temporary session key $tk := H_k(\mathrm{label}', C'.w) \oplus H_{k'}(\mathrm{label}, C, w)$ and a random session key sk. Using $\mathbf{ECC} : \{0,1\}^l \to \{0,1\}^n$, an error-correcting code that corrects 2ϵ-fraction of errors, the client computes $c := \mathbf{ECC}(sk)$ to finally set $\Delta := tk \oplus c$ and signs σ, sending s, Δ and σ to the server. To finalize the exchange, the server verifies σ and similarly computes a temporary session key tk' and the following final session key $sk := \mathbf{ECC}^{-1}(tk' \oplus \Delta)$.

Client	CRS: pk	**Server**
w		w

$(\mathrm{VK}, \mathrm{SK}) \leftarrow \mathcal{K}(1^\kappa)$
$r \leftarrow \{0,1\}^*$
label $:= \mathrm{VK}|\mathrm{Client}|\mathrm{Server}$

$C := \mathrm{Enc}_{pk}(\mathrm{label}, w; r)$ $\xrightarrow{\mathrm{Client}|\mathrm{VK}|C}$ $r' \leftarrow \{0,1\}^*$
$\mathrm{label}' := \varepsilon$
$C' := \mathrm{Enc}_{pk}(\mathrm{label}', w; r')$
$\mathrm{label} := \mathrm{VK}|\mathrm{Client}|\mathrm{Server}$

$\mathrm{label}' := \varepsilon$ $\xleftarrow{\mathrm{Server}|C'|s'}$ $k' \leftarrow K; \; s' := \alpha(k', \mathrm{label}, C)$
$k \leftarrow K; \; s := \alpha(k, \mathrm{label}', C')$
$\mathrm{tk} := \mathrm{H}_k(\mathrm{label}', C', w) \oplus \mathrm{H}_{k'}(\mathrm{label}, C, w)$
$\mathrm{sk} \leftarrow \{0,1\}^\ell; c := \mathrm{ECC}(\mathrm{sk})$
$\Delta := \mathrm{tk} \oplus c$

$\sigma \leftarrow \mathrm{Sign}_{\mathrm{SK}}(C|C'|s'|s|\Delta)$ $\xrightarrow{s|\Delta|\sigma}$ if $\mathrm{Vrfy}_{\mathrm{VK}}(C|C'|s'|s|\Delta, \sigma) = 1:$
$\mathrm{tk}' := \mathrm{H}_k(\mathrm{label}', C', w) \oplus \mathrm{H}_{k'}(\mathrm{label}, C, w)$

$\mathrm{sk} := \mathrm{ECC}^{-1}(\mathrm{tk}' \oplus \Delta)$

Figure 5: Katz and Vaikuntanathan [KV09]

Client	$p, q, g_1, g_2, h, c, d, \mathcal{H}$	**Server**

$(\mathrm{VK}, \mathrm{SK}) \leftarrow \mathrm{SigGen}(1^\kappa)$
$r_1 \leftarrow \mathbb{Z}_q$
$A = g_1^{r_1}; B = g_2^{r_1}$
$C = h^{r_1} g_1^{pw_C}$
$\alpha = \mathcal{H}(Client|\mathrm{VK}|A|B|C)$
$D = (cd^\alpha)^{r_1}$ $\xrightarrow{Client|\mathrm{VK}|A|B|C|D}$ $x_2, y_2, z_2, w_2, r_2 \leftarrow \mathbb{Z}_q$
$\alpha' = \mathcal{H}(Client|\mathrm{VK}|A|B|C)$
$E = g_1^{x_2} g_2^{y_2} h^{z_2} (cd^{\alpha'})^{w_2}$
$F = g_1^{r_2}; G = g_2^{r_2}$
$I = h^{r_2} g_1^{pw_C}$
$\beta = \mathcal{H}(Server|E|F|G|I)$

$x_1, y_1, z_1, w_1 \leftarrow \mathbb{Z}_q$ $\xleftarrow{Server|E|F|G|I|J}$ $J = (cd^\beta)^{r_2}$
$\beta' = \mathcal{H}(Server|E|F|G|I)$
$K = g_1^{x_1} g_2^{y_1} h^{z_1} (cd^{\beta'})^{w_1}$
$\mathrm{Sig} = \mathrm{Sign}_{\mathrm{SK}}(\beta'|K)$ $\xrightarrow{K|\mathrm{Sig}}$ if $\mathrm{Verify}_{\mathrm{VK}}((\beta|K), \mathrm{Sig}) = 1$
$C' = C/g_1^{pw_C}$
$I' = I/g_1^{pw_C}$ $sk_S = K^{r_2} A^{x_2} B^{y_2} (C')^{z_2} D^{w_2}$
$sk_C = E^{r_1} F^{x_1} G^{y_1} (I')^{z_1} J^{w_1}$ else $sk_S \leftarrow \mathcal{G}$

Figure 6: The KOY PAKE [KOY01]

Following this construction, a lot of CRS and ASPH PQC PAKEs were published, most of which inspired by the same idea. Zhang and Yu [ZY17] built upon the previous work to obtain a generic 2-pass PAKE based on a splittable IND-CCA PKE and non-adaptive ASPH. Further, the PKE construction relies on simulation-sound NIZK proofs from

lattices, and the concrete instantiation is also done with a splittable lattice PKE. Karbasi et al. [KAA19] constructed the first ring-based SPHF PAKE (Ring-PAKE) building upon the Lyubashevsky-Peikert-Regev (LPR) dual-style RLWE cryptosystem. Apart from using RLWE instead of LWE, the construction resembles the one by Katz and Vaikuntanathan. However neither a security proof, nor an evaluation are provided. Li and Wang [LW18] showed how to construct a 2-round PAKE over an LWE SPHF without a NIZK in the standard model using a CRS. They integrate the Micciancio-Peikert and Regev schemes to design two lattice-based SPHFs. CCA-secure encryption is required on the client side, and CPA-secure encryption on the server side, thus reducing the required weakness assumptions for the protocol. In the following year, Li and Wang [LW19] claimed achieving a one-round PAKE based on the same simulation-sound NIZK approach also using LWE. However, the supposedly 1-round construction consists of two message flows, which we deem confusing, as the previous one also had two messages and was referred to as a 2-round PAKE (cf. Sec. 5). The authors integrate a lattice-based ASPH with adaptive smoothness into the classical PAKE construction by Katz and Vaikuntananthan [KV13], and the ASPH scheme is built from the IND-CCA Miccianio-Peikert Scheme [MP12] and inspired by Benhamouda et al. [BBDQ18]. The authors present a performance comparison to [KV09] and [ZY17], and discuss the potential applications in IoT device authentication. An updated yet similar construction was presented by Li, Wang, and Morias in 2022 [LWM22], and the publication also features an augmented 3-party PAKE described in a following section. Building upon the same construction ideas, Yin et al. [YGS+20] proposed a two-round 3PAKE with mutual authentication, however from a splittable labeled IND-CCA PKE (SPKE) and a non-adaptive ASPH (NA-ASPH). The authors also present a 2PAKE version and compare the security properties to other PAKEs.

Class C3: 3-Party RLWE-PAK and RLWE-PPK

Xu et al. [XHCC17] presented the first LWE 3PAKE construction using the PWE and DPWE problems introduced by Ding et al. [DAL+17]. They build upon the RLWE-PAK protocol to create a 3-party PAKE with mutual authentication, using the server for a trusted setup. The authors provide a very similar security analysis in the BPR model and an implementation using similar parameters to NewHope using the C library *LatticCrypto*. They compare their work to a previous classical 3PAKE construction based on ECDH, which they also implemented using the MIRACL library. However, we question the applicability of the benchmarking results, as the total runtime for the PQC 3PAKE is only 0.25 ms compared to 53.3 ms using ECDH. Choi et al. [CAK+18] extend RLWE-PPK to 3-party setting constructing a 3PAKE protocol with implicit mutual authentication. The authors claim ROM security based on RLWE-PPK, but do not provide a formal proof.

Class C3: Augmented 3-Party RLWE-PAK

Liu et al. [LZJY19] proposed an augmented 3PAKE based on the RLWE-PAK protocol and refer to it as RLWE-3PAK, however using the Peikert reconciliation mechanism. The authors rely on the ROM and provide a security proof in a modified BPR model following a proof strategy by MacKenzie [Mac02]. They also present benchmarking results for a proof of concept implementation in C. Guo et al. [GSG+23] proposed an augmented 2-round 3PAKE with a registration phase. The security proof is given in the ROM and the BPR model, and the authors rely on the decisional module PWE (DMPWE) assumption over MLWE and use the Peikert error reconciliation mechanism. Still, the protocol does not need to send a signal in plain text, and thus mitigates the risk of signal leakage attacks. They suggest their protocol is suitable for large networks as it has smaller key sizes.

Class C3: Augmented KOY-GL-Style with SPHFs and ASPHs

Tang et al. [TLZ+21] constructed a 3-round 3PAKE protocol based an ASPH over ideal lattices (RLWE). Further, the authors claim to reduce the size of ciphertexts and achieve lower computational overhead by using the Fast Fourier Transformation (FFT). Li et al. [LWM22] presented a 3-round PAKE based on LWE and LWR for mobile devices. They use a CRS with an SPHF and a commitment-based Password-Hashing Scheme (PHS) over lattices for the registration phase, and provide a security proof in the standard model. The authors claim their construction eliminates costly NIZK methods and bypasses ROM assumptions and provide thorough performance measurements and security parameters.

Class C3: Anonymous Augmented RLWE-PAK (Mostly 3-Party)

Feng et al. [FHZ+18] proposed the first anonymous augmented PAKE based on the RLWE problem with a security proof in the BPR model. The construction consists of a user registration phase, a login and authentication phase, and also allows for a password update phase. Dabra et al. [DBK20] addressed vulnerabilities discovered in a conducted cryptanalysis of the former protocol and proposed LBA-PAKE, an improved lattice-based anonymous PAKE for mobile devices with key reuse. The authors use a similar construction to Feng et al. based on RLWE. However, Ding et al. [DCQ22] discovered a signal leakage attack in LBA-PAKE and claimed to break the protocol in less than two minutes. Ding et al. thus propose an improved protocol and provide a new security analysis. Islam and Basu [IB21] proposed a similar 3PAKE for mobile devices with a registration phase called BP-3PAKA. Similar to previous constructions, the authors build their PAKE form RLWE with reconciliation. They implement their PAKE using the LatticeCrypto library and compare their protocol efficiency to previous constructions based on chaotic maps[5] and one time keys. Chaudhary et al. [CKS23] addressed the security vulnerabilities in the construction of Islam and Basu and propose a new protocol following the same approach. The authors suggest a registration method using ECC and key agreement using RLWE, and provide a security proof in the ROM and the BPR model. They also provide thorough performance and security comparison to other 3PAKEs based on chaotic maps, which are not included in our survey[6]. In the same year, two more works were proposed to address signal leakage attacks including Kumar et al. [KGKD23] and Dadsena [DJRD23]. Finally, Dharminder et al. [DRD+23] addressed the same issue with another augmented RLWE 3PAKE in the standard model providing a hybrid security proof. Both works provide similar evaluation benchmarks and comparison to the previous constructions.

Class C3: Outlier

Moving in a slightly different direction, Wang et al. [WCL+23] combined identity based signatures with Kyber MLWE key exchange and Peikert's reconciliation mechanism to construct an augmented 2-round PAKE, without the registration phase. The authors refer to their protocol as LB-ID-2PAKA and provide a security proof in the ROM. Lastly, earlier this year Seyhan and Akleylek [SA24] proposed a new augmented PAKE based on the BiGISIS problem over lattices. However we were not able to review this construction due to our insufficient knowledge regarding this specific harndess assumption.

---

[5]Chaotic maps are used as pseudo-random number generators given a seed value and have applications in encryption. Source: https://www.sciencedirect.com/topics/computer-science/chaotic-map

[6]We opted to only consider PAKEs based on PQC primitives, even if chaotic maps are, strictly speaking, quantum-resistant.

4.3 Generic Constructions

Class C1: EKE-Style with IC

In 2023, Beguinet et al. [BCP+23] proposed the first construction to transform a black-box KEM into a PAKE in generic manner, i.e., relying on KEM properties rather than on PQC hardness assumptions. Inspired by EKE and OEKE [BM92], the authors proposed the CAKE and OCAKE protocols respectively and provided a security proof in the UC framework utilizing the IC and ROM models. The idea is to encrypt the the public key and the ciphertext using the password to provide explicit mutual authentication in the CAKE variant. Alternatively, the ciphertext is authenticated with a key confirmation tag in OCAKE, which provides explicit authentication for the receiver. Additionally, mutual explicit authentication can be achieved via a key confirmation round. CAKE and OCAKE both require KEMs that fulfill IND-CPA, public key fuzziness (Fuzzy KEM), and ciphertext anonymity, which arguably differ from the prevailing recent KEM notions in the literature. The authors also suggest an instantiation of the IC for CRYSTALS-Kyber public keys and provide preliminary bit security estimations using Kyber as well. Following Beguinet et al., Pan and Zeng [PZ23] and Alnahawi et al. [AHHR24] presented further security analysis for CAKE and OCAKE respectively. The two additional security proofs were presented in the eBPR model. Pan and Zeng [PZ23] suggested the notion of ANO-PCA for the chosen KEM and extended the security proof to handle multi-user challenges. The authors in [AHHR24] also adapted similar anonymity and multi-user notions and formulated the notion of KEM-PKU as a replacement for the Fuzzy-KEM property. Additionally, they show how to formally handle password guesses in a detailed game-based proof and provide an implementations with run-time and memory benchmarks.

Technical Description: The CAKE protocol (Fig. 7) is built similar to the classical EKE2 protocol (Fig. 8), however using an KEM in a black-box manner instead of DH. CAKE relies on two pairs of ICs, denoted by (E_1, D_1) and (E_2, D_2), which resemble ε_w in EKE. Both parties share knowledge of the password pw. Alice starts by generating a key-pair (pk, sk) and encrypts the public key using the ideal cipher $\mathbf{Epk} \leftarrow E_1(\text{ssid}||\text{pw}, pk)$. After receiving $\mathbf{Epk}$, Bob can decrypt Alice's message to obtain her public key, plugging it into the encapsulation function to receive (c, K). Bob uses E_2 to encrypt the ciphertext, sending it back to Alice. After decrypting the message E_c to receive c', Alice decapsulates it to get $K' \leftarrow \text{KEM.Decaps}(sk, c')$. If Alice and Bob use matching passwords, the pre-keys match too, i.e., $K = K'$, and both parties obtain a matching session key SK via hashing.

Alice		**Bob**
A, pw	ssid	B, pw
$(pk, sk) \leftarrow \text{KEM.KeyGen}(1^K)$		
$\mathbf{Epk} \leftarrow E_1(\text{ssid}||\text{pw}, pw)$	$\xrightarrow{A, \mathbf{Epk}}$	$pk \leftarrow D_1(\text{ssid}||\text{pw}, \mathbf{Epk})$
		$(c, K) \leftarrow \text{KEM.Encaps}(pk)$
$c' \leftarrow D_2(\text{ssid}||\text{pw}, \mathbf{Ec})$	$\xleftarrow{B, \mathbf{Ec}}$	$\mathbf{Ec} \leftarrow E_2(\text{ssid}||\text{pw}, c)$
$K' \leftarrow \text{KEM.Decaps}(sk, c')$		
$\text{SK} \leftarrow \text{H}(\text{ssid}, A, B, \mathbf{Epk}, \mathbf{Ec}, K')$		$\text{SK} \leftarrow \text{H}(\text{ssid}, A, B, \mathbf{Epk}, \mathbf{Ec}, K')$

Figure 7: The CAKE Protocol [BCP+23]

Alice	Bob
A	B

$x \in_R [0, p-1]$

$$\xrightarrow{A, \varepsilon_w(g^x \bmod p)}$$

$y \in_R [0, p-1]$

$$\xleftarrow{B, \varepsilon_w(g^x \bmod p)}$$

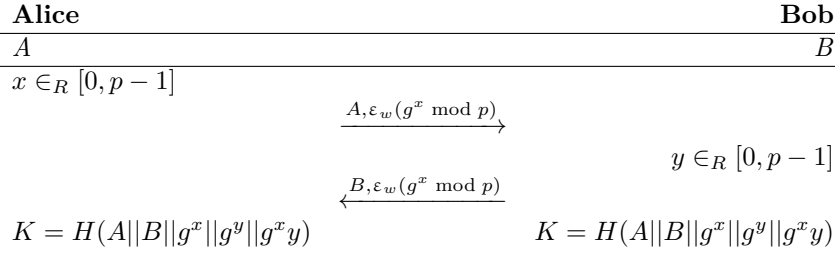$K = H(A||B||g^x||g^y||g^x y)$ $K = H(A||B||g^x||g^y||g^x y)$

Figure 8: The EKE2 Protocol [BPR00] - adopted from [HvO22]

Class C1: EKE-Style with HIC

Dos Santos et al. [DGJ23] introduced an IC relaxation called the randomized *Half-Ideal Cipher* (HIC) on a group utilizing a modified 2-round Feistel (m2f). Also based on EKE [BM92], the authors propose a 2-round PAKE and provide a security proof relying on the ROM in the UC framework. By extending the IC domain to bit strings, the authors suggest instantiating their constructions with a generic KEM satisfying the security notions IND-CPA, ANO-CCA and UNI-PK. A concrete instantiation is benchamrked with the MLWR SABER-KEM, showing a decrease of approximately 85% in bandwidth usage compared to Ding's RLWE-PAK [DAL+17]. Building upon the HIC idea of Dos Santos et al. [DGJ23], Arriaga et al. [ABJS24] proposed the Compact Half-Ideal Cipher (CHIC) protocol. The authors utilize the m2f construction of Dos Santos et al. in white-box manner and use a randomized value taken from the PKE public key as input. Their main contribution is a compact m2F and bandwidth-minimal KEM-to-PAKE compiler, where they also establish security requirements for KEM with splittable public keys. These requirements include OW-CPA, ANO-PCA, UNI-PK, and ciphertext anonymity. The authors extend their findings to generic EKE-KEM constructions in the BPR model and the UC framework, claiming that IND-CPA is not sufficient for tight security proofs. The authors instantiate the proposed protocol using CRYSTALS-Kyber (also proving the pseudo-randomness of its public keys) and provide a C implementation with respective performance benchmarks. The analysis of the runtime and communication overhead indicates a 25% overahead in the initation phase, and 50% in response. Still, the authors state that the execution times are only in the order of tens of microseconds, and that the overhead decreases when the security parameters of the KEM are raised.

Class C1: EKE-Style without IC

Inspired by the idea of splitting a KEM public key in CHIC [ABJS24], Alnahawi et al. [AASAW24] claim a new approach to construct a secure PAKE in the BPR framework, completely eliminating the usage of IC. The authors use a RO to model a hash function used to extend the password to the same length as the uniform string part of the public key (the seed used to sample a lattice base i.e., a matrix) in LWE, RLWE, and MLWE KEMs. While the authors rely on well studied KEM properties such as IND-CCA and ANO-CCA, they also introduce the notions of *A-Part-Secrecy* (A-SEC-CCA), *Splittable Collision Freeness* (A-CFR-CCA) and *Public Key Uniformity* (SPLIT-PKU) for splittable LWE KEMs, which rely on the Non-Uniform LWE (NLWE) and the Weak-Hint LWE (whLWE) assumptions. However, the authors also demonstrate several attacks on instantiations using NIST KEM parameters, some of which lead to a complete break in security. Therefore, they suggest several remedies to obtain secure instantiations from ML-KEM and FrodoKEM.

Class C3: Outlier

Recently, Lyu et al. [LLH24] proposed the first UC PAKEs in the QROM, with three passes and mutual authentication. They rely on a trusted setup using a CRS, and four hash functions. Applying concrete LWE and isogeny group action instantiations for the PKE and LPKE schemes yields four PQC PAKEs, of which two are in the ROM, and two in the QROM. The ROM construction makes use of Lossy Public Key Encryption (LPKE) on IND-CCA PKEs, and the QROM construction uses a variant called extractable Lossy PKE (eLPKE) and utilizes some of the hash functions as PRFs. Although this PAKE allows for the use of multiple IND-CCA PKE schemes, it is questionable whether it can be considered a fully generic construction. This is due to the fact that the FO transformation is used directly to lift the PKE security from IND-CPA to IND-CCA in white-box manner. Additionally, the use of LPKE or eLPKE schemes poses further restrictions on the possible choices for this PAKE. Nevertheless, we opted to include this work in this category, since it is instantiated from both lattice and isogeny assumptions, and could be observed as a semi-generic construction in that sense. Notably, Lyu et al. [LLH25] also proposed a new PAKE compiler to transform a symmetric PAKE into an asymmetric one making use of generic KEMs and Authenticated Encryption (AE) in the ROM. The authors claim that their construction can be efficiently instantiated using lattice-based KEMs (e.g., ML-KEM) and show how to apply their compiler to the previously discussed generic PAKEs, as well as their own. Further, they provide performance benchmarks using ML-KEM and compare their results to the aPAKE compiler of Gentry et al. [GMR06].

4.4   Isogeny-Based

Class C1: EKE-Style

Terada and Yoneyama [TY19] proposed the only EKE-like PAKE based on SIDH and CSIDH. Hence, the authors refer to their constructions as SIDH-EKE and CSIDH-EKE respectively. As in all EKE-style PAKEs, the protocol relies on the ROM and the IC model. The authors provide a security proof in the BPR model with tight security bounds. A performance comparison to the SIDH PAKE of Taraskin et al. [TSJL20] with the same security levels (i.e., NIST lvl. 1) shows no differences when using SIDH. However, the communication overhead drops from 2640 to 512 bits using CSIDH. On the other hand, the computation time drastically increases from approximately 5 to 80 ms. Azarderakhsh et al. [AJK$^+$20] address problems regarding the indistinguishability of isogeny public keys and illustrate possible MitM and offline dictionary attacks on [TY19], which may lead to explicit breaks in security (cf. Sec. 10).

Class C2: PAK-Style

Taraskin et al. [TSJL20] proposed a PAK-similar PAKE based on SIDH and group action. They rely on the ROM for their security proof in the BPR model. The protocol is instantiated with SIDH parameter sets p434 and p503 and its performance is measured based on total clock cycles for running SIDH and the additional PAKE overhead. Nevertheless, the authors address the issue of the message distribution being dependent of the used password (cf. Sec. 10), which is also found in RLWE-PAK and RLWE-PPK constructions.

Class C3: SPEKE-Style

A more recent work by Abdalla et al. [AEK$^+$22a] builds upon the H2G idea from the classical SPEKE protocol [Jab96]. The authors proposed two constructions, the 1-round (2-pass) X-GA-PAKE and the 3-pass Com-GA-PAKE. Both protocols are based on restricted effective group actions with the ability of computing the so-called quadratic twist, which

implies the same hardness assumptions as in CSIDH. The PAKEs rely on the CRS model and provide a security proof in the eBPR model. The authors make use of a CRS to fix two set elements and use the password to map a tuple of elements. The protocols can also be modified to construct other variants, e.g., by increasing the number of public parameters in the CRS, or by using quadratic twists in the setup phase.

Technical Description: The SPEKE protocol (Fig. 10) relies on DH, where the password is hashed into a group generator using the function f. The GA-PAKE (Fig. 9) resembles this construction in the group action setting by mapping the password to an ℓ-tuple of elements in $\mathcal{X}$, instead of one element. It utilizes a CRS with two elements $(x_0, x_1) \in \mathcal{X}^2$ as a trusted setup, and a password $pw := (b_1, \ldots, b_\ell) \in \{0,1\}^\ell$ that is mapped to the tuple $(x_{b1}, \ldots, x_{b\ell}) \in \mathcal{X}^\ell$. Afterwards, a DH key agreement is done using the basis x_{bi} for each $i \in [\ell]$. Both user and server generate random group elements and compute a set of new elements using the DH basis, which they can exchange simultaneously. Then both compute new elements using the exchanged sets to hash into a final session key, along with previously generated values, the password, and their IDs. We note that this version of the protocol is not secure, but serves illustration only. The secure protocol X-GA-PAKE doubles the message length in the first round and triples it in the key derivation, relying on a new assumption called SqInv-StCDH, where an adversary has to compute the square and the inverse of its input at the same time. The Com-GA-PAKE adds a commitment from the server before the first message, and security is reduced to standard isogeny assumptions.
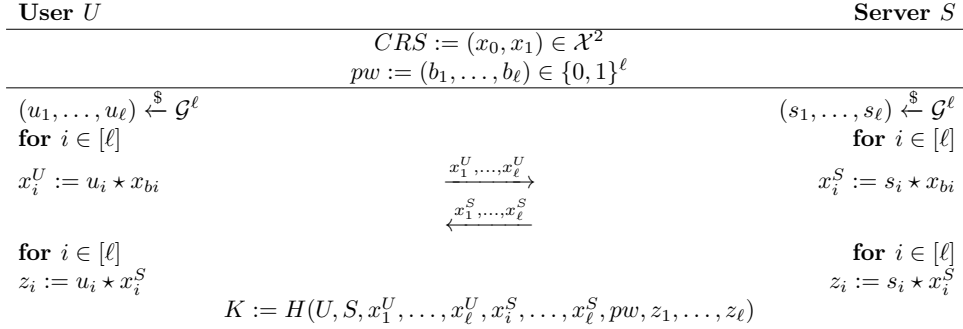
User U		**Server S**
	$CRS := (x_0, x_1) \in \mathcal{X}^2$	
	$pw := (b_1, \ldots, b_\ell) \in \{0,1\}^\ell$	
$(u_1, \ldots, u_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(s_1, \ldots, s_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$		**for** $i \in [\ell]$
$x_i^U := u_i \star x_{bi}$	$\xrightarrow{x_1^U, \ldots, x_\ell^U}$	$x_i^S := s_i \star x_{bi}$
	$\xleftarrow{x_1^S, \ldots, x_\ell^S}$	
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := u_i \star x_i^S$		$z_i := s_i \star x_i^S$
	$K := H(U, S, x_1^U, \ldots, x_\ell^U, x_i^S, \ldots, x_\ell^S, pw, z_1, \ldots, z_\ell)$	

Figure 9: The GA-PAKE Protocol [AEK$^+$22b]

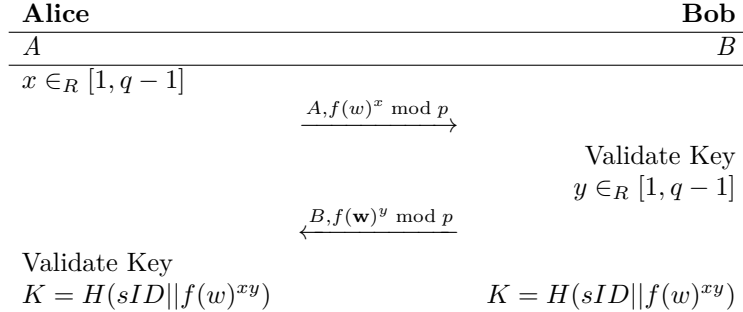| **Alice**		**Bob**
A		B
$x \in_R [1, q-1]$		
	$\xrightarrow{A, f(w)^x \bmod p}$	
		Validate Key
		$y \in_R [1, q-1]$
	$\xleftarrow{B, f(\mathbf{w})^y \bmod p}$	
Validate Key		
$K = H(sID \| f(w)^{xy})$		$K = H(sID \| f(w)^{xy})$

Figure 10: The Patched SPEKE protocol [HS14] - adopted from [HvO22]

Class C3: DH-Style

In 2014, Zhu et al. [ZHS14] introduced an *augmented* 3PAKE without timestamps based on the SI problem and its computational (SSCDH) and desicional (SSDDH) DH variants, and secure one-way hash functions. The protocol consists of five messages in total, and the authors prove its security in the CK model. They claim to achieve several security goals including mutual authentication and PFS, as well as resisting impersonation and replay attacks. However, their efficiency claims are based solely on the number of hashing, symmetric encryption/decryption, and isogeny operations. In 2015 (and revised in 2017), Zhu and Geng [ZG15] proposed a new version of their protocol building upon the same assumptions and also providing a security proof in the CK model. However, this protocol is a 2-party PAKE, and does not require a trusted setup.

5 Security Overview

Tab. 3 offers an overview of security properties applicable only to generic KEM-based PAKE constructions. Since such PAKEs make use of PQC PAKEs in black-box manner, they rely on properties that need to be satisfied by the used PQC KEM. The indistinguishability (IND-) and anonymity (ANO-) are suffixed with a hyphen to indicate the attached attack model (i.e., -CPA or -CCA). However, the authors in CHIC [ABJS24] opted for the notion of OW-CPA for session key security and for ANO-PCA for anonymity, the latter of which is also used in the CAKE and OCAKE versions of Pan and Zeng [PZ23], and Alnahawi et al. [AHHR24] respectively. While the afore mentioned properties are well known and sufficiently studied in the literature, some authors propose new notions to support their formal analysis, which are, casually put, less famous. This can be seen in properties concerning the uniformity of public keys, which are prefixed (-PK) to indicate the applied notion. The CHIC construction defines UNI-PK as in HIC-EKE [DGJ23], which is defined as Fuzzy-KEM in the original CAKE paper [BCP+23] and the follow-up work in [PZ23]. In contrast, the OCAKE follow-up in [AHHR24] and NICE-PAKE [AASAW24] refer to this property as PKU and SPLIT-PKU respectively.

Table 3: Security Properties of KEM-Based Generic PQC PAKEs

Protocol	IND-	ANO	-PK	Other
HIC-EKE [DGJ23]	CPA	CCA	UNI	-
CAKE [BCP+23]	CPA	CPA	Fuzzy	-
OCAKE [BCP+23]	CPA	CPA	Fuzzy	-
Pan and Zeng (CAKE) [PZ23]	CPA	PCA	Fuzzy	Multi-User
Alnahawi et al. (OCAKE) [AHHR24]	CPA	PCA	PKU	Multi-User
CHIC [ABJS24]	-	PCA	UNI	OW-CPA
NICE-PAKE [AASAW24]	CCA	CCA	SPLIT-PKU	A-SEC / A-CFR

In Tab. 4, we present an overview of the security assurances of PQC PAKEs regarding their design classes and properties. These are the number of rounds, security of the session key (IND-), forward secrecy (FS), and mutual authentication (MA) for both implicit and explicit authentication variants. The session key security is denoted by either IND-CPA or IND-CCA depending on the underlying key agreement scheme. Forward secrecy can either be weak (FS) or perfect (PFS). Mutual authentication is either checked or not, regardless of the fact whether it is done explicitly or implicitly. The number of rounds indicates how many messages are sent from one protocol participant to another (e.g., one round equals one message). However we note that, and to the best of our knowledge, one round in a cryptographic protocol should actually indicate one back and forth message exchange between two parties. That is, one round consists of two messages (or passes). Nonetheless

we opted for this presentation due to the extreme inconsistency in the usage of this term in the surveyed papers. The reader may thus feel free to simply divide the presented number of rounds by two, should it better suit their understanding of the term.

Table 4: Security Properties of PQC PAKE Protocols

Class	Protocol	Rounds	IND-	FS	MA
Balanced					
C1	Terada and Yoneyama (SIDH-EKE) [TY19]	2	CPA	PFS	✓
	Terada and Yoneyama (CSIDH-EKE) [TY19]	2	CPA	PFS	✓
	Dos Santos et al. (HIC-EKE) [DGJ23]	2	CPA	PFS	✓
	Beguinet et al. (CAKE) [BCP+23][1]	2	CPA	PFS	✗
	Beguinet et al. (OCAKE) [BCP+23]	2	CPA	PFS	✓
	Pan and Zeng (CAKE) [PZ23]	2	CPA	PFS	✗
	Alnahawi et al. (OCAKE) [AHHR24]	2	CPA	PFS	✓
	Arriaga et al. (CHIC) [ABJS24]	2	OW-CPA	PFS	✓
	Alnahawi et al. (NICE-PAKE) [AASAW24][1]	2	CCA	PFS	✗
C2	Zhu, Geng [ZG15]	2	CPA	PFS	✗
	Ding et al. (RLWE-PAK) [DAL+17]	3	CPA	FS	✓
	Ding et al. (RLWE-PPK) [DAL+17]	2	CPA	FS	✗
	Gao et al. (RLWE-PAK) [GDL+17]	3	CPA	FS	✓
	Gao et al. (RLWE-PPK) [GDL+17]	2	CPA	FS	✗
	Taraskin et al. (SIDH-PAK) [TSJL20]	3	CPA	FS	✓
	Yang et al. (RLWE-PAK) [YGWX19]	3	CPA	FS	✓
	Jiang et al. (PAKEs) [JGH+20]	3	CPA	PFS	✓
	Ren et al. (MLWE-PAK)[RGW23] ([RG22])	3	CPA	FS	✓
	Seyhan, Akleylek [SA23]	3	CCA	PFS	✓
	Basu et al. (MLWR-2PAKA) [BSIA23][2]	4	CPA	PFS	✓
C3	Katz, Vaikuntanathan [KV09]	3	CCA	PFS	✗
	Xu et al. (RLWE-3PAKE) [XHCC17]	6	CPA	PFS	✓
	Zhang, Yu [ZY17]	2	CCA	PFS	✗
	Choi et al. (AtLast) [CAK+18][3]	5	CPA	FS	✓
	Li, Wang [LW18]	2	CPA / CCA	FS	✗
	Li, Wang [LW19]	2	CCA	FS	✗
	Karbasi et al. (Ring-PAKE) [KAA19]	3	CCA	PFS	✗
	Yin et al. [YGS+20][4]	2	CCA	FS	✓
	Lyu et al. [LLH24]	3	CCA	?	✓
Augmented					
C2	Gao et al. [GDLL17]	2	CPA	FS	✓
C3	Zhu et al. [ZHS14]	5	?	PFS	✓
	Feng et al. [FHZ+18][†5]	3	CPA	FS	✓
	Liu et al. [LZJY19]	?	CPA	FS	✓
	Dabra et al. (LBA-PAKE) [DBK20][†5]	3	CPA	FS	✓
	Tang et al. [TLZ+21]	3	CCA	FS	✓
	Li et al. [LWM22][7]	3	CCA	PFS	✓
	Islam, Basu (BP-3PAKA) [IB21][†5]	4	CPA	PFS	✓
	Abdalla et al. (X-GA-PAKE) [AEK+22a]	2	CPA	PFS	✓
	Abdalla et al. (Com-GA-PAKE) [AEK+22a]	3	CPA	PFS	✓
	Wang et al. (LB-ID-2PAKA) [WCL+23][5]	2	CCA	PFS	✓
	Guo et al. [GSG+23]	2	CCA	FS	✓
	Chaudhary et al. [CKS23][†5]	4	?	PFS	✓

[1] Mutual authentication requires an additional key confirmation round.
[2] Number of rounds excluding the initialization phase.
[3] No explicit authentication with the server, only between users.
[4] Applies to both 2PAKE and 3PAKE variants.
[5] Excluding the registration phase.
[†] Anonymous PAKEs.

6 Performance Overview

In Tab. 5 and Tab. 6 we compile information on bit-security, communication cost and computation cost for two-party and three-party PAKEs respectively. Any values for communication and computation cost given are rounded to three decimal places where appropriate, otherwise values are adopted exactly as provided in their original publications. Some publications yield multiple table rows for specific security or implementation variants of a PAKE. Such cases may include the variant of an underlying KEM, the variant of a security parameter set (where the values n, p and q denote the security parameter of the underlying hardness assumption), a slight variation in the implementation of a protocol or two different protocols within the same publication. Communication cost describes the total size of outgoing messages of a given party and is either given in bits (b), bytes (B) or kilobytes (kB) while computation costs are either given in microseconds (μs), milliseconds (ms), seconds (s) or cycles (c).

Table 5: Comparison of Bit Security and Performance for 2-Party PAKEs

Class	PAKE Publication	Variant	Security Classic	Quantum	Computational Cost Client	Server	Total	Communication Cost Client	Server	Total
Balanced										
C1	Terada and Yoneyama [TY19]	SIDH	NIST lvl 1	NIST lvl 1	-	-	80.6ms	64B	64B	128B
		CSIDH	NIST lvl 1	NIST lvl 1	-	-	5.0ms	330B	330B	660B
	Beguinet et al. [BCP+23]	CAKE	-	102bit	-	-	-	-	-	-
		OCAKE		162bit	-	-	-	-	-	-
	Alnahawi [AHHR24]	Kyber512	-	-	-	-	0.995s	-	-	-
		Kyber1024	-	-	-	-	2.039s	-	-	-
		frodokem640shake	-	-	-	-	73.057s	-	-	-
		bikel1	-	-	-	-	26.519s	-	-	-
	Arriaga et al. [ABJS24]	Kyber512	128bit	-	84μs	74μs	158μs	800B	800B	1600B
		Kyber768	128bit	-	168μs	85μs	253μs	1,184B	1,120B	2,304B
		Kyber1024	128bit	-	206μs	123μs	329μs	1,568B	1,600B	3,168B
C2	Ding et al. [DAL+17]	RLWE-PAK	-	76bit	2,981.251μs	2,884.243μs	6,702.656μs	4,136B	4,256B	8,392B
		RLWE-PPK	-	76bit						
	Gao et al. [GDL+17]	RLWE-PAK	≥200bit	82bit	0.176ms	0.175ms	0.351ms	3,904B	4,000B	7,904B
		RLWE-PPK	≥200bit	82bit	0.203ms	0.203ms	0.406ms	3.75kB	3.875kB	7.625kB
	Taraskin et al. [TSJL20]	p434	-	-	-	-	142×10⁶c	-	-	-
		p503	-	-	-	-	228×10⁶c	-	-	-
	Yang et al. [YGWX19]	avx2	228bit	206bit	145,964c	137,313c	283,277c	1,864B	2,592B	4456B
		portable C	228bit	206bit	294,460c	270,227c	564,687c	1,864B	2,592B	4456B
	Jiang et al. [JGH+20]	-	-	-	0.2s	0.71s	0.91s	39,990B	167,090B	207,080B
	Ren et al. [RGW23]([RG22])	Lightweight-PAK	128bit	116bit	89.76ms	93.35ms	183.11ms	928B	1,056B	1,984B
		Recommended-PAK	195bit	177bit	126.71ms	126.05ms	252.76ms	1,344B	1,472B	2,816B
		Paranoid-PAK	263bit	239bit	174.97ms	169.52ms	344.49ms	1,760B	1,888B	3,648B
	Seyhan, Akleylek [SA23]	Lightsaber	-	128bit	104,824μs	60,632μs	165,456μs	896B	1,600B	2,496B
		Saber	-	192bit	172,427μs	97,758μs	270,185μs	1,344B	2,368B	3,712B
		Firesaber	-	256bit	257,756μs	152,232μs	409,988μs	1,760B	3,168B	4,928B
	Basu et al. [BSIA23]	$p=2^{10}$, $q=2^{13}$	127bit	116bit	-	-	-	-	-	2816B
		$p=2^9$, $q=2^{15}$	140bit	127bit	-	-	-	-	-	2560B
Augmented										
C2	Gao et al. [GDLL17]	-	209bit	-	0.286ms	0.257ms	0.543ms	3,963B	4,032B	7,995B
C3	Feng et al. [FHZ+18]	Without Precomputation	-	-	2.307μs	0.222μs	2.529μs	5,121b	4,609b	9,730b
		With Precomputation	-	-	1.184μs	0.075μs	1.259μs	5,121b	4,609b	9,730b
	Dabra et al. [DBK20]	n=128	-	-	6.501ms	33.298ms	39.799ms	3528b	3296b	6824b
		n=256	-	-	17.372ms	66.094ms	83.466ms	6600b	6368b	12,968b
		n=512	100bit	75bit	26.271ms	136.442ms	162.713ms	12,744b	12,512b	25,256b
	Li et al. [LWM22]	Classical	-	-	116ms	361ms	477ms	26,326b	32,950b	59,312b
		Quantum	-	-	116ms	473ms	589ms	29,602b	40,320b	69,922b
	Ding et al. [DCQ22]	n=128	-	-	-	-	-	4496b	4224b	8720b
		n=256	-	-	-	-	-	8,464b	8,192b	16,656b
		n=512	-	-	39.22ms	12.65ms	51.87ms	16,400b	16,128b	32,528b
	Dharminder et al. [DRD+23]	-	-	-	2.297μs	0.229μs	2.526μs	-	-	9,790b
	Dadsena et al. [DJRD23]	-	-	-	-	-	2.826μs	-	-	9,725b
	Kumar et al. [KGKD23]	-	-	-	2.297μs	0.229μs	2.526μs	-	-	9,726b

Table 6: Comparison of Bit Security and Performance for 3-Party PAKEs

Class	PAKE Publication	Implementation	Security Classic	Quantum	Runtime Client$_A$	Client$_B$	Server	Total	Message Sizes Client$_A$	Client$_B$	Server	Total
Balanced												
C3	Xu et al. [XHCC17]	-	-	-	0.067ms	0.071ms	0.122ms	0.259ms	-	-	-	-
Augmented												
C3	Liu et al. [LZJY19]	-	-	-	3.267ms	4.155ms	2.195ms	9.617ms	-	-	-	-
	Tang et al. [TLZ+21]	n=32	-	-	2.27ms	0.38ms	20.52ms	23.17ms	-	-	-	7kB
		n=64	-	-	4.44ms	0.63ms	63.10ms	68.17ms	-	-	-	13kB
		n=128	-	-	10.38ms	1.07ms	353.49ms	364.91ms	-	-	-	24kB
		n=256	-	-	24.31ms	3.39ms	3,373.06ms	3,400.76ms	-	-	-	48kB
		n=512	-	-	82.11ms	4.62ms	45,802.87ms	45,889.60ms	-	-	-	79kB
	Islam, Basu [IB21]	-	-	-	-	-	-	6,315.553×10⁶ms	5,249b	5,249b	9,408b	19,906b
	Guo et al. [GSG+23]	-	-	222bit	-	-	-	0.788ms	-	-	-	10,080B
	Chaudhary et al. [CKS23]	-	-	-	4.999μs	-	0.215μs	5.214μs	-	-	-	19,226b

7   Honorable Mentions

Strictly speaking, the following categories cannot be directly viewed as PQC PAKEs. Nevertheless, they may be viewed as quantum-safe or at least quantum annoying due to the inherent nature of the primitives used in their constructions.

Symmetric (Fuzzy) PAKEs

This special type of PAKEs focuses on use cases where the shared password (or credentials) of two parties in a protocol instance are not necessarily identical, yet close enough up to a predefined threshold. This method is mainly utilized to amend the shortcomings of balanced and augmented PAKEs in dealing with frequent typing errors in passwords, but more importantly when using biometric data as authentication credentials [Ott24] (e.g., iris scans and fingerprints). Since Fuzzy PAKEs are mostly built from inherently quantum-safe primitives (e.g. garbled circuits), they can be considered relevant in quantum-resilient PAKE research. A recent work by Ottenhues [Ott24] presents and overview of such symmetric Fuzzy PAKE protocols and compares their security both in theory and practice. This overview includes one protocol built from garbled circuits [DHP+18] and two from error correcting codes [DHP+18, BFH+23]. Other Fuzzy PAKEs include the work of Erwig et al. [EHOR20], which relies on oblivious transfer and robust secret sharing to obtain two asymmetric Fuzzy PAKEs in the UC model. Further, Bauspieß et al. [BSP+24] present a modification of unlinkable fuzzy vault schemes combined with OPRFs, which can be instantiated with lattices, to construct a protocol for biometrics-based authenticated key exchange. The authors also provide a comparison to similar constructions including the previously mentioned PAKEs, in addition to the works of Wang et al. [WHC+21], Han et al. [HXL+23] (ttPAKE), and Zhang et al. [ZYL+23] (BAKA).

Quantum-Annoying PAKEs

Although quantum annoying properties do not promise full quantum-resilience, they do provide a certain degree of resistance against quantum computers by making some classical operations more expensive for quantum adversaries. The main idea, in the context of PAKEs, is to make offline dictionary attacks more expensive by hiding group elements, so that an adversary needs to compute the discrete logarithm for each offline password guess [TES23]. That is, even if they succeeds in computing the discrete logarithm (i.e., essentially break DH) in an online protocol session, they cannot directly relate the computed value to a certain single password. To the best of our knowledge, the notion of quantum annoying PAKEs is mainly found in the generic group model for discrete logarithm-based PAKEs, and was formalized by Eaton and Stebila [ES21] based on the classical symmetric CPace protocol, which was shown to inherently satisfy this property. Following that, Tiepelt et al. [TES23] presented a simple modification to the classical asymmetric KHAPE-HMQV [GJK21] PAKE protocol by adding an IC-based encryption to one protocol message, which also makes KHAPE quantum annoying.

8   Unexplored Territory

Considering the fact that almost all of the PQC PAKEs surveyed in this paper are more or less an adaptation of classical PAKE designs, and following the classification system of Hao and van Oorschot [HvO22], we observe that a few designs are still unrepresented or not fully explored in the PQC realm. However, we observe that a few classical PAKEs can still be adapted to PQC, and had not yet been addressed in the literature. Such constructions include, strictly speaking, PAKEs that make use of cryptographic building blocks that can

be replaced by PQC primitives and schemes, where the password usage is not dependent on a mathematical properties inherent to classical cryptography (e.g., password-derived generators as in PACE or password-derived exponents as in SPR-6). Additionally, we address some special PAKE designs, which are not inlcuded in [HvO22]. In the following we shed some light on these designs and discuss the possibility of their PQC instantiation.

Augmented OPAQUE-Style with OPRFs

The augmented PAKE protocol OPAQUE was proposed by Jarecki et al. [JKX18] defining the strong aPAKE functionality, primarily addressing the vulnerabilities of pre-computation attacks. While there is still no PQ OPAQUE proposal in the literature, the original authors did provide two general frameworks to obtain a strong aPAKE in the UC model. The first framework is based on an authenticated key exchange (AKE) scheme and an OPRF, whereas the second requires an authenticated encryption scheme (AE) and a key exchange scheme in addition to the OPRF. Both versions of OPAQUE consist of a registration and a login phase, where the OPRF is meant to hide the values associated with the password usage during the registration. In other words, a user runs an OPRF on their password with a server to obtain an ephemeral random secret, which they later on use as a private key for a key exchange in the login phase. In the AKE variant, both user and server already provide their (static) public keys during registration for later usage in the login phase. Since an AKE with either unilateral or bilateral authentication can easily be constructed using a PQC KEM (as shown by Bos et al. with CRYSTALS-Kyber [BDK$^+$18]), and there exists a number of PQ OPRFs (cf. Sec. 2), we suggest obtaining a PQC OPAQUE adaptation for a user U and a server S as in the following outline:

Registration (with bilateral static keys):

- S chooses a fresh OPRF key $k \xleftarrow{\$} \{0,1\}^n$, a static KEM key pair (sk_s, pk_s), and sends pk_s to U.

- U executes the OPRF $\mathcal{F}$ with S using the password π as input to obtain a secret $s = \mathcal{F}_k(\pi)$. U derives a KEM key pair (sk_u, pk_u) from s, computes an authentication key $K_{MAC} = HMAC_s(pk_s)$, and sends K_{MAC} to S.

- S stores the values (sk_s, pk_s, pk_u), the OPRF key k, and K_{MAC}.

Login (with session key establishment):

- U executes the OPRF $\mathcal{F}$ with S using the password π as input to obtain a secret $s = \mathcal{F}_k(\pi)$. U derives an ephemeral KEM key pair (sk, pk) from s then receives pk_s and K_{MAC} from S and verifies K_{MAC}.

- U encapsulates pk_s into (K_s, C_s) and sends thei pk along with C_s to S.

- S decapsulates C_s with their secret key sk_s to obtain K_s and encapsulates pk, pk_u into $(K, C), (K_u, C_u)$ respectively, and then send C, C_u to U.

- U decapsulates C, C_u to obtain K, K_u respectively.

- Both U and S set their final keys (session key) to $\overline{K} = \mathcal{H}(K, K_u, K_s)$.

Remarks: We note, and stress, that the above outline is neither verified nor formally analyzed, and thus serves only as a rough sketch for a possible instantiation of OPAQUE using a PQC KEM and a PQC OPRF. That being said, other variants without static public keys (i.e., without an AKE), or using a PQC KEX (e.g., Ding's RLWE scheme) are very likely to be possible as well. Further, and as noted in the original OPAQUE paper, the UC aPAKE functionality requires a non-black-box hardness assumption on the ROM in order to extract password guesses, which automatically implies the need for re-programming in the QROM. Last but not least, the used KEX or KEM must provide forward secrecy (FS) and key-compromise impersonation (KCI) security. Nevertheless, an open question remains in finding a mechanism to to derive a valid key pair from the random secret obtained via the OPRF execution between the user and the server. Since OPAQUE originally relies on a H2C function to map a password to an EC base generator, it seems intuitive to resort to its adaptation to H2G settings, which is mainly found in C2 PQC PAKE constructions (e.g., RLWE-PAK), and rightfully so, since OPAQUE belongs to class C2 according to [HvO22]. While this might answer the question of instantiating OPAQUE directly with a PQC primitive (e.g., an RLWE KEX), it is not clear how to realize this in combination with generic KEMs. So far, the only existing method to construct generic KEM-based PQC PAKEs relies mainly on an IC encryption, which differs drastically from the public key modification (PAK-style) method. As the key generation routine in a KEM does not usually allow for any input values, a rather uncomfortable approach would be to use the OPRF obtained secret directly as the secret key, and apply it to the key generation base (e.g., a lattice base matrix) to generate a public key. Another approach might be found in using a PQC Non-Interactive Key Exchange (NIKE), e.g., SWOOSH [GdKQ+24], that enables a white-box key generation routine, while also maintaining the non-interactive key agreement characteristics of a KEM. Considering the scope of this paper, we deem finding a solution an open question for future work.

J-PAKE-Style with NIZKs

The J-PAKE protocol proposed by Hao and Ryan [HR10] can be considered the first PAKE to make use NIZKs (namely the Schnorr protocol [Sch91]) and achieve a relatively efficient construction. The balanced J-PAKE essentially aims at providing a proof of knowledge of the password without actually revealing it. It relies on a the juggling technique using NIZKs, where random public keys are combined in order to achieve a vanishing effect when both parties supply exactly the same passwords. Other variants and adaptations of J-PAKE include RO-J-PAKE and CRS-J-PAKE proposed by Lencrenon et al. [LST16], and sJ-PAKE proposed by Abdalla et at. [ABR+21] (sJ-PAKE replaces two NIZK proofs by two exponentiations). Recently, Hao et al. [HBCvO23] proposed the augmented Owl protocol addressing the limitations of SPR-6a and OPAQUE, however inspired by J-PAKE and elevating it to an augmented PAKE. Considering the ongoing progress on realizing secure and efficient PQ ZKP systems (including variants such as NIZKs, SNARKs etc.), it is quite reasonable to assume that a PQC version of J-PAKE can be realized while maintaining the original design. Intuitively, replacing the underlying KEX in J-PAKE by a PQC scheme, and providing PQC NIZK proofs for the secrets of the used scheme might very well yield a PQC instantiations of J-PAKE and similarly of Owl. An open question remains as to finding a suitable mechanisms for replacing the password exponentiations used to derive a shared key in J-PAKE, which is very likely to be coupled to the used PQC-based NIZK system and KEX. For a generic KEM, a similar issue to OPAQUE arises considering how to integrate said mechanism in black-box routines.

Threshold PAKEs

In order to mitigate the risks of offline dictionary attacks following server compromise, *Multi-Party Computation* (MPC) can be utilized to distribute a stored password among multiple servers. By doing so, an attacker needs to compromise more than one server instance bound by some threshold t to reconstruct server data, and hence the name Threshold PAKE, aka tPAKE [GJK+25]. There already exist many approaches to realize symmetric tPAKEs from (t, n)-MPC protocols as in [Jab01, DRG03, ACFP05]. This idea underwent further development and became known as *Password-Protected Secret Sharing* (PPSS) or *Password-Authenticated Secret Sharing* (PASS) as in [BJSL11, CLN12, JKK14, JKKX16]. Recently, Gu et al. [GJK+25] extended this approach to asymmetric settings and formalized the notion of (augmented) atPAKEs, where the password hash value is distributed among multiple servers using a secret-sharing scheme. Whereas tPAKEs are still non-present in PQ-settings, it is worth considering for a straight-forward adaptation as in the case of OPAQUE. This is mainly due to the fact that the construction in [GJK+25] can be considered a threshold version of OPAQUE, as it mainly relies on a threshold OPRF (tOPRF). Nevertheless, we suffice with this short overview, as this specific type of PAKEs is clearly beyond the scope of this paper.

Decoy, Honey and Oblivious PAKEs

In line with the previously mentioned PAKE designs, another approach to reducing the threats of server compromise and credential leakage can be found in utilizing decoy accounts or decoy passwords [ARS24]. Interestingly, this type of PAKEs addresses the issues of password leakage in different manner than the previously mentioned designs (e.g., OPAQUE, J-PAKE, and tPAKEs). The original idea of Honey PAKEs, introduced by Becerra et al. [BRRS18], introduces decoy passwords (honeywords) that are utilized to detect password guesses. The real password is hence called the sugarword, and the set of all decoy passwords with the real one are the sweetwords [ARS24]. Similar approaches can also be found in the oblivious O-PAKE proposed by Kiefer and Manulis [KM15], as well as the HPAKE (as in honey) proposed by Li et al. [LWL22]. In a very recent publication, Arriaga et al. [ARS24] propose the SweetPAKE and BeePAKE (as in a honey producing buzzing bee) protocols building upon the afore mentioned works and comparing their results. Nonetheless, and again considering the scope of this paper, we suffice to mentioning the prior constructions as possible candidates for PQC adaptation, as they mostly provide generalized protocol frameworks in black-box manner.

9   Real World Use Cases

In the following, we establish a mapping between current PQC PAKEs and existing real world applications, where classical PAKEs are already used. We adopt the PAKE use cases from [HvO22], in addition to one new use case [DFG+23]. That being said, we disregard a discussion on non-PAKE alternatives, i.e., cryptographic solutions without using PAKEs, since it is sufficiently covered in [HvO22].

Credential Recovery

Several well-known commercial IT systems including Apple iCloud, 1Password manager, ProtonMail, and Blizzard incorporate classical PAKE protocols such as the Secure Remote Password protocol (SRP-6a) [Wu98, Wu02] for general account access, user authentication, or credential recovery [HvO22].

PQC Replacement: For a straight-forward PQC replacement, such use cases arguably require a ***C3 2-party PAKE with a trusted setup and a prior registration phase***.

Discussion: We recall the previous observations related to the risks of pre-computation attacks and server compromise. Thus, an augmented PAKE is especially preferable, as it is highly recommended to register users without storing the actual password on the server. However, ***most of the proposed C3 augmented PQC PAKEs are 3-party PAKEs, whereas most C3 2-party PAKEs are balanced***. Therefore, it is difficult to name specific candidates for this use case. ***Gao et al. [GDLL17] explicitly state that their PQC PAKE is an SRP-similar protocol*** and provide reasonable security margins and benchamrking values for the well-studied RLWE problem. Hence, this PAKE could be a candidate for replacing SRP-6a, should a full proof be provided for the construction.

Device Pairing

The most common applications of PAKE-based device pairing are found in situations where it is not possible to rely on a Public Key Infrastructure (PKI). This especially the case for relatively small devices and e-cards equipped with smart chips (i.e., embedded and IoT), or in the context of Wi-Fi connection[ASWZ24]. For instance PACE [BFK09] is used in electronic IDs and eMRTDs (Machine Readable Travel Document) for secure connection establishment with terminals and e-card readers; and Dragonfly [Har08] is used in WPA3 for establishing a Wi-Fi connection between an access point and a client [HvO22].

PQC Replacement: Several PQC PAKE proposals claim constructions tailored for embedded and IoT devices (e.g., [FHZ+18, DBK21, LWM22, DRD+23, RGW23, RSM+23]). On the design level, we believe that ***balanced 2-party PQC PAKEs in classes C1 and C2*** are the most suitable for ad-hoc device pairing (e.g., [TY19, BCP+23, ABJS24]), ***where no registration is possible nor needed*** (e.g., Wi-Fi and eMRTDs). However, in other use cases (e.g., smart-gadgets, smart-meters, e-mobility etc.), ***light weight C3 PAKEs with prior registration may also be a valid option***.

Discussion: The ***low computational power and resource constraints of such small devices inherently infer restrictions*** on the choice of a suitable PAKE. Further, ***embedded and IoT devices are more prone to physical attacks such as Side-Channel Analysis (SCA) and Fault Injections (FI)***, the mitigation of which comes with additional costs both in memory and run time [ASWZ24]. Considering the already existing extra costs of PQC schemes, the need for ***light weight PAKEs with fast execution times*** is an absolute must.

End-to-End (E2E) Secure Channel

E2E encryption is usually found in chat applications that mostly utilize an AKE using static keys from a connected PKI (e.g., Signal's X3DH). Nevertheless, some applications involving embedded and IoT devices cannot rely on a PKI. For instance, the J-PAKE protocol is used in Thread IoT products, Palemoon web browser, and the Smoke Chat application for android; whereas EC-SPEKE is used in Blackberry Messenger (BBM) [HvO22].

PQC Replacement: Since this use applciation may rule out a trusted setup in the client-client case, we believe that ***balanced PQC PAKEs in C1 and C2 with PFS and mutual authentication*** (e.g., [JGH+20, SA23, BCP+23, BSIA23]) are most suitable. That being said, use cases with a possible trusted third-party would enable the use of augmented 3-party PAKEs (e.g., [LZJY19, IB21, RSM+23, GSG+23]).

Discussion: Similar to device pairing, small devices require PAKEs with **light weight implementations and resistance to physical attacks**. Considering the ever increasing computational power of personal portable devices, **this requirement does not necessarily apply to smart-phones and tablets** etc.. Still, E2E session key establishment in both the client-server and the client-client models imposes the requirement of PFS.

End-to-End (E2E) Encrypted Backups

To the best of our knowledge, the only E2E encrypted backup application relying on a PAKE is found in the WhatsApp Backup Protocol (WBP), which was released in 2021 [DFG⁺23]. WBP allows users to recover their backup keys using a password and ultimately retrieve their chat histories from lost or broken devices. Under the hood, OPAQUE serves as the main cryptographic protocol related to password usage. Being an aPAKE, it enables a key exchange between a user and a server[7] without revealing the actual password to the server. Apparently, **directly elevating the security of WBP to PQ-settings requires the employment of a PQ-version of OPAQUE, or an augmented C3 PQC 2-party PAKE** (e.g., Gao et al [GDL⁺17]). Similar to credential recovery, we were unable to identify other suitable candidates for this use case.

10 Observations and Discussion

Based on the conducted review, we present the most important observations and discuss the issues related to PQC PAKE design, security, and performance.

Design Paradigms and Schemes

Evidently, finding the holy grail for PQC PAKE design is not an easy question to answer. Especially since each design may or may not be suitable for some specific application or on some specific platform. Further, some designs may not be attainable depending on the choice of the PQC scheme used in the construction.

Observation 1: There are three mainstream trends in PQC PAKE design with strong focus on LWE, RLWE and MLWE schemes (cf. Tab. 1):

- PAKEs following the (O)EKE paradigm with focus on generic NIST PQC KEMs, and especially ML-KEM (C1).

- PAKEs following the PAK-suite paradigm using LWE and its variants directly and relying on different reconciliation mechanisms (C2 and C3).

- PAKEs following the KOY-GL paradigm using SPHF, APSH, and NIZK constructions from LWE and its variants (C2 and C3).

Observation 2: Other prominent classical PAKE designs such as in SPEKE (except for isogeny-based GA-PAKE), SPR-6, SPAKE, (Au)CPace, OPAQUE, and J-PAKE are currently non-present in the PQC realm, some of which we had already addressed in Sec. 8.

Observation 3: Save for a few exceptions (e.g., PAKEs based on splittable KEMs), we are yet to witness the birth of a new paradigm in PQC PAKE design that is more than a mere adoption or adaptation of classical ones.

---

[7]Precisely, the server only relays user messages to a HSM (Hardware Security Module), with which a user establishes a secure session.

Observation 4: As seen in lattice PAKEs from the classes C2 and C3, There exists a plethora of either RLWE-PAK, or LWE ASPH PAKEs, but the main contribution is more or less restricted to performance or security improvements. Ultimately, it appears that the prevailing tendency is set on the lattices, especially because of the standardization of CRYSTALS-Kyber as ML-KEM.

Observation 4: Isogeny-based PAKEs are remarkably under-represented and there are no code-based PAKEs at all. Thus, it is worth investigating, whether other more isogeny PAKEs are attainable; and whether code-based PQC primitives are also a viable option.

Discussion: Mainly, the lack of diversity in PQC PAKE design paradigms can be traced back to the fact that many classical PAKE designs are tightly coupled to password usage within the DH paradigm. ***This can be clearly seen in the absence of approaches relying on secret key exponentiation or base generator modification (H2G and H2C) using the password or a password derived value.*** Here, we differentiate between multiple cases w.r.t the chosen PQC scheme in a PAKE construction.

KEMs: Briefly put, and regardless of the underlying primitive, generic KEMs cannot support any design operating (mathematically speaking) on the underlying PKE level. These designs include base mapping subroutines, password-derived generators and password-derived secrets. This is clearly due to the fact that the ***KEM algorithms are used as a black-box interface within the PAKE protocol, and should not be utilized in white-box manner***. For instance, utilizing the password within the ML-KEM key generation routine to obtain a new lattice base defeats the purpose of a black-box design, and ultimately restricts the PAKE to concrete hardness assumptions.

Splittable KEMs: In this case, the only KEMs available are those based on lattice LWE primitives and variants (e.g., RLWE and MLWE), where the lattice base is a bit-string seed appended (or prepended) to the public key. Still, splittable KEMs do maintain the provided algorithm interface in black-box manner, and thus do not support operations within the underlying PKE. That being said, ***designs of splittable lattice-based KEM-PAKEs do not seem to apply to KEMs from other hardness assumptions***.

Lattices: Using PQC primitives directly does indeed offer more flexibility in PAKE design, as observed in PAK-style LWE and RLWE PAKEs, where the H2G method is used to shift the public key. Nevertheless, other approaches remain difficult to obtain from LWE and variants, ***as they do not support the exact operations as in discrete logarithm DH or ECDH***. Another obstacle is that ***most RLWE schemes still require a reconciliation mechanism***. Thus, it is worth investigating, whether NIKE PQC schemes like SWOOSH [GdKQ+24] can be utilized for a DH-like PAKE design.

Isogenies: While isogenies strongly resemble ECC, classical approaches cannot be directly translated to SIDH and CSIDH, as sufficiently discussed in [AJK+20]. According to Azarderakhsh et al. [AJK+20], and unlike their classical DH-based counterparts, ***EKE-style, PAK-style, and J-PAKE style isogeny-based PAKEs are not secure***. Further, ***the secuirty of SPEKE-style and Dragonfly-like isogeny PAKEs is rather questionable***, since they are difficult to realize when hashing into public keys.

Design Simplicity (or Complexity)

The construction of cryptographic schemes as such is a very delicate endeavor surrounded by many obstacles and pitfalls. This task is equally difficult, if not more, for quantum-resistant asymmetric key exchange schemes and PAKEs in particular.

Observation 1: Direct designs from lattices and isogenies are already of very complex nature stemming from the underlying harndess assumptions. This is especially the case for many LWE schemes and variants that require key reconciliation via signaling.

Observation 2: Design complexity becomes even more entangled when adding idealized objects with sophisticated oracles such as the (Q)ROM and the IC. To a certain degree, this complexity becomes overwhelming when SPHFs and NIZKs are thrown into the equation as well, which makes the peer-review process extremely difficult.

Discussion: We argue that generic constructions relying on ***proven abstract security properties rather than direct hardness assumptions*** (as discussed in Barbosa et al. [BGHJ24] and Januzelli et al. [JRX24]) may reduce the overall complexity, and even make the peer-reviewing process easier and more reliable. That is especially the case for PQC schemes and protocols, as their security has not matured to the level of classical cryptography yet. Further, ***generic designs enable realizing frameworks that support interchangeability and adaptability*** in the case of sudden breaks and the emergence of new threats.

Hybrid Schemes and Crypto-Agility

Several governmental bodies and institutions (e.g., NIST, BSI, and ETSI) recommend a transition to PQC in the near future. Nevertheless, they also recommend applying hybrid schemes (PQC combined with classical cryptography) due to the skepticism still surrounding the new PQC KEMs and digital signatures. In line with this recommendation, several hybrid KEMs were proposed (e.g., KEM Combiners [GHP18] and X-Wing [BCD⁺24]).

Observation 1: There is still no clear answer to the question of finding a generic approach to construct a hybrid PAKE [KR24].

Observation 2: Very recently, both Hesse and Rosenberg [HR24], and Lyu and Liu [LL24] (almost simultaneously) addressed this issue and proposed a PQC PAKE combiner and a hybrid PAKE framework respectively.

Discussion: While these works claim to have obtained ***a generic recipe for hybrid PAKEs using parallel and sequential (or serial) combiners in the UC model, both are still not peer reviewed***, which makes verifying their results to the time of writing this paper rather difficult. This questions becomes even more difficult, since ***Hesse and Rosenberg show the impossibility of achieving a parallel combiner with minimal overhead using the existing PQC PAKEs***. Similarly, ***Lyu and Liu claim that a parallel combiner requires both used PAKEs to satisfy the properties of a full DH-type PAKE***, which so far can only by obtained from group action isogenies in the PQC realm. Thus, it is worth investigating, how generic KEM PAKEs can be optimized to support hybrid PAKE designs. Optimally, such designs should also allow for an interchangeable KEM usage in plug-and-play manner and consequentially enable crypto-agility in sophisticated manner [ASW⁺22].

Semantic Security

Regarding the semantic security in PAKEs, many questions still surround the properties needed from PQC schemes to realize secure PAKEs. Most efforts, although not exclusively, address the analysis of generic designs.

Observation 1: It was usually believed that schemes fulfilling CPA security are sufficient for building secure PAKEs [Jar22]. However, it was recently argued that CCA security is required for tighter proofs [ABJS24]. Therefore, it is still an open question, whether it is possible to achieve a secure PAKE solely from IND-CPA security.

Observation 2: Generic KEM constructions need to additionally address novel notions such as public key uniformity, anonymity, and robustness. Although these notions are increasingly reaching a rather stable state in the literature (e.g., [Xag22, GMP22, MX23, CDM23, Sch24, BCD+24]), it is yet to be seen how their potential can be fully leveraged in generic PQC PAKE design.

Observation 3: Almost all PAKE designs still need to address the issues arising from classical IC and ROM usage.

Observation 4: Efficient designs and proofs in the standard model are strongly wished for. This might however be extremely difficult to achieve with many schemes relying mainly on hashing and permutations.

Discussion: Based on the attained level of maturity in PQC PAKE design, it is not audacious to suggest that future constructions should not rely on non-quantum-safe models or assumptions. Surprisingly, the overwhelming majority of the PAKEs reviewed in this paper rely on the classical ROM, and only a few make use of abstract security notions (cf. Tab. 1 and Tab. 3). Whereas QROM proofs are starting to emerge, it is still not foreseeable when, and if the QIC is something that can be considered in the future.

Public Keys and Passwords

The relation between public keys and password in PAKEs is indeed long-lasting, yet delicate and fragile at the same time. Almost all authentication methods in PAKEs involve applying the password to the public key in some shape or form.

Observation 1: C1 EKE-like constructions encrypting the public key with an IC may suffer from vulnerability to offline dictionary attacks [AJK+20].

Observation 3: In C2 PAK-like constructions, the modified public key message distribution is directly dependent of the password due to the H2G password usage [AJK+20].

Discussion: Essentially, public keys need to be indistinguishable from random bit strings, which may not be the case for PQC keys yielding a certain structure [AJK+20] such as, say a Kyber public key [AASAW24]. The public key uniformity notion is meant to address this issue in theory, however practical instantiations and implementations need to either work around this problem, or find a way to make the public keys unstructured in some sense. Further, extracting information about the password from the public key message is assumed to be infeasible, yet it may still be possible to obtain partial information about the used keys, as discussed in the following for leakage attacks.

Tight Bounds and Reductions

Following the previous discussion, security bounds in formal proofs usually provide an average estimation of the expected success probability for attacks targeting a scheme. Therefore, tight bounds and better reductions are obviously of great importance.

Observation 1: Reducing the need for idealized objects, or providing proofs in QROM and QICM is a future work for almost all PQC PAKEs (cf. Tab. 1).

Observation 2: In the absence of an IC, it is not possible to prove knowledge of any information about an adversary's interactions with public keys in security proofs [AASAW24].

Observation 3: It might be hard to enumerate the number of passwords that can be ruled-out through active password guessing [AASAW24]. In cases where the key pairs are generated honestly, it is rather easy to deal with guesses targeting key derivations or hashing on the final key. However, ***password guesses under unknown secret keys are difficult to handle, where the initiator's key pair was generated maliciously.***

Observation 4: It is hard to formulate a hardness assumption bound to the number of password guessing queries for an unknown number of malicious key pairs [AASAW24].

Discussion: PQC KEMs mainly differ from bare primitives in the fact that they cannot yet apply self-reducible [KTAT20] properties to remove multiplicative factors in multiple-queries for certain security properties [ACH+24]. ***Random self-reducibility allows for independent instances of a property to be reduced to one, thus leading to tighter reductions.*** For instance, the multiplicative factor for the number of queries on an IC directly affects the bounds on public key encryptions [PZ23, AHHR24]. That being said, a PQC KEM with a tight proof of multi-instance security would solve this problem. For a RO, ***one should consider how to deal with queries on public key modifying or masking operations that allow for offline dictionary attacks***. Lastly, RO reprogramming is probably not necessary, but ***the QROM still needs to simulate real session keys using a decision oracle***. Some authors argue that classical output transfer is acceptable if the extraction is possible using recent online extractability techniques. An open question is also if quantum rewinding is applicable in PAKE proofs that rely on rewinding.

Sufficient Analysis and Unknown Attack Surfaces

As observed in the case of LBA-PAKE [DBK20], the authors attempted fixing vulnerabilities in a previous construction [FHZ+18], yet introduced a signal leakage attack on the PWE assumption that lead to full key recovery [DCQ22]. This can also be seen in the case of BP-3PAKA [IB21], which was addressed in follow-up works by Chaudhary et al. [CKS23], Kumar et al. [KGKD23], Dadsena et al. [DJRD23], and Dharminder et al. [DRD+23]. The common denominator among these examples is that they all suffered from signal leakage attacks.

Observation 1: Constructing complex PAKEs from relatively new hardness assumption may introduce new attack services.

Observation 2: New attacks are not restricted to the used security models, but can also target the underlying schemes cryptographically and physically.

Observation 3: Most anonymous PQC PAKE proposals suffer from vulnerabilities against impersonation attacks, stolen smart-card attack, password guessing attack, and sometimes even fail to provide user anonymity or non-traceability (cf. Sec. 4).

Observation 4: Many augmented PAKEs do not explicitly address the possibility of pre-computation attacks, where an attacker can leverage the password dictionary for an

offline pre-computation attack before compromising the server (cf. Sec. 4).

Discussion: Assuming the soundness of a certain hardness assumption and its usage in proof reductions (e.g., PWE to LWE via H2G), works building upon it need to pay special attention to practical threats, and not only theoretical assumptions. Moreover, since anonymous communication is required in real world use cases such as eIDs and e-healthcare [ASWZ24], we believe that the work on constructions with more rigorous formal and physical analysis, as well as weaker assumptions is highly required.

Implementations, Performance and Standardization

Since research surrounding PQC PAKEs is still in its early stages, there are not sufficient driving factors such as the NIST PQC standardization etc.. Thus, comparing performance and finding a baseline for the different styles of PQC PAKEs is an open problem.

Observation 1: Testing and benchmarking projects are missing in PQC PAKE research.

Observation 2: Many works do not provide clear experimental results and do not directly address the security guarantees and assumptions of their constructions (cf. Sec. 6).

Observation 3: Different papers providing performance indicators widely differ in the measurement setup and used units (e.g., clock cycles, milliseconds or computational cost etc.), and the benchmarking environments also differ in their computational capabilities (cf. Sec. 6). Hence, ***it is extremely difficult to make any accurate statements regarding which constructions is more secure or can perform better under which circumstances.***

Observation 4: Many experimental results and benchmarks, especially for LWE and RLWE PAKEs seem unreasonable or rather unconvincing (cf. Sec. 4).

Discussion: Similar to projects aimed at PQC KEMs such as the Open Quantum Safe (OQS) project [SM16] and pqm4 [KRSS19], there is an urgent need to make an effort to provide reproducible performance benchmarks for different PQC PAKEs on various platforms, making them also comparable and comprehensive. Moreover, governmental bodies and institutions should aim at standardizing PQC PAKEs, and ultimately provide a guideline for security and performance evaluations.

11   Conclusion and Future Work

In this paper, we extensively reviewed and systematized nearly 50 PAKE proposals based on PQC hardness assumptions and PQC KEMs. Conclusively, only a small percentage of these works offer ground-breaking novelty in terms of design paradigms, as the major contributions are focused on optimizations of existing ones. Further, most PQC PAKEs heavily rely on the RO and the IC models, and need to either address these models in quantum settings, or eliminate their usage completely to achieve real post-quantum security. Nevertheless, some works were able to shed some light on undiscovered security issues or unknown attack surfaces. Compared to direct approaches, generic PAKEs utilizing PQC KEMs seem more attractive, due to their simpler designs and manageable interfaces. However, they often pose more requirements w.r.t. the security notions of the used KEMs.

Considering the discussion and summary of our review, a pressing order of business for future work would be an offical project providing a unified hardware and software

framework for PQC PAKE implementation and benchmarking. Further, a such project can actively integrate and test PQC PAKEs in real world applications in order to evaluate their claimed suitability for certain use cases, and investigate their physical security. Moreover, hybrid schemes can also be considered in such evaluations to assess their applicability and feasibility for future cryptographic migrations. On the theoretical side, future PQC PAKEs have to consciously aim at designs with crypto-agility, where building blocks are at least interchangeable, if not updateable. That being said, the most urgent future work concerns these very building blocks. As previously observed, we believe that KEM security properties and idealized objects should get special attention. That is on the one hand to actively involve abstract security notions in PAKEs for tighter reductions and simpler designs. On the other hand, to follow up on quantum lifting techniques for the IC and the ROM. A slightly different approach could be found in designing PAKEs that are non-reliant on such models, which could be the more difficult path, yet the one bearing the most fruit.

References

[AASAW24] Nouri Alnahawi, Jacob Alperin-Sheriff, Daniel Apon, and Alexander Wiesmaier. NICE-PAKE: On the security of KEM-based PAKE constructions without ideal ciphers. Cryptology ePrint Archive, Paper 2024/1957, 2024.

[Abd14] Michel Abdalla. Password-based authenticated key exchange: An overview. In *Provable Security: 8th International Conference, ProvSec 2014*, 2014.

[ABJS24] Afonso Arriaga, Manuel Barbosa, Stanislaw Jarecki, and Marjan Skrobot. C'est très chic: A compact password-authenticated key exchange from lattice-based kem, 2024.

[ABP15] Michel Abdalla, Fabrice Benhamouda, and David Pointcheval. Public-key encryption indistinguishable under plaintext-checkable attacks. In *Public-Key Cryptography – PKC 2015*, 2015.

[ABR+21] Michel Abdalla, Manuel Barbosa, Peter B. Rønne, Peter Y. A. Ryan, and Petra Šala. Security Characterization of J-PAKE and its Variants, 2021.

[ACFP05] Michel Abdalla, Olivier Chevassut, Pierre-Alain Fouque, and David Pointcheval. A simple threshold authenticated key exchange from short secrets. In *Advances in Cryptology-ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005. Proceedings 11*, pages 566–584. Springer, 2005.

[ACH+24] Joël Alwen, Matthew Campagna, Dominik Hartmann, Shuichi Katsumata, Eike Kiltz, Jake Massimo, Marta Mularczyk, Guillermo Pascual-Perez, Thomas Prest, and Peter Schwabe. How multi-recipient kems can help the deployment of post-quantum cryptography. *Fifth PQC Standardization Conference*, 2024.

[ADDG24] Martin R Albrecht, Alex Davidson, Amit Deo, and Daniel Gardham. Crypto dark matter on the torus: Oblivious prfs from shallow prfs and tfhe. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2024.

[ADDS21] Martin R Albrecht, Alex Davidson, Amit Deo, and Nigel P Smart. Round-optimal verifiable oblivious pseudorandom functions from ideal lattices. In *IACR International Conference on Public-Key Cryptography*, 2021.

[AEK+22a] Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, and Doreen Riepel. Password-authenticated key exchange from group actions. In *Annual International Cryptology Conference*, 2022.

[AEK+22b] Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, and Doreen Riepel. Password-Authenticated Key Exchange from Group Actions. In *Advances in Cryptology – CRYPTO 2022*, 2022.

[AFP05] Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval. Password-Based Authenticated Key Exchange in the Three-Party Setting. In *Public Key Cryptography - PKC 2005*, 2005.

[AHHR24] Nouri Alnahawi, Kathrin Hövelmanns, Andreas Hülsing, and Silvia Ritsch. Towards post-quantum secure pake-a tight security proof for ocake in the bpr model. In *International Conference on Cryptology and Network Security*, pages 191–212. Springer, 2024.

[AJK+20] Reza Azarderakhsh, David Jao, Brian Koziel, Jason T. LeGrow, Vladimir Soukharev, and Oleg Taraskin. How Not to Create an Isogeny-Based PAKE. In *Applied Cryptography and Network Security*, 2020.

[Als16] Saed A Alsayigh. *New Password Authenticated Key Exchange Based on the Ring Learning with Errors*. PhD thesis, University of Cincinnati, 2016.

[AR17] Gorjan Alagic and Alexander Russell. Quantum-secure symmetric-key cryptography based on hidden shifts. In *Annual international conference on the theory and applications of cryptographic techniques*, 2017.

[ARS24] Afonso Arriaga, Peter YA Ryan, and Marjan Skrobot. Sweetpake: Key exchange with decoy passwords. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, pages 1017–1033, 2024.

[ASW+22] N. Alnahawi, N. Schmitt, A. Wiesmaier, A. Heinemann, and T. Graßmeyer. On the State of Crypto-Agility. In *18. Deutscher IT-Sicherheitskongress*. SecuMedia Verlags-GmbH, February 2022. Preprint: https://ia.cr/2023/4 87.

[ASWZ24] Nouri Alnahawi, Nicolai Schmitt, Alexander Wiesmaier, and Chiara-Marie Zok. Toward next generation quantum-safe eids and emrtds: A survey. *ACM Trans. Embed. Comput. Syst.*, 23, 2024.

[BBDQ18] Fabrice Benhamouda, Olivier Blazy, Léo Ducas, and Willy Quach. Hash proof systems over lattices revisited. In *IACR International Workshop on Public Key Cryptography*, 2018.

[BCD+16] Joppe Bos, Craig Costello, Leo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[BCD+24] Manuel Barbosa, Deirdre Connolly, João Diogo Duarte, Aaron Kaiser, Peter Schwabe, Karolin Varner, and Bas Westerbaan. X-wing. *IACR Communications in Cryptology*, 1(1), 2024.

[BCP+23] Hugo Beguinet, Céline Chevalier, David Pointcheval, Thomas Ricosset, and Mélissa Rossi. Get a cake: Generic transformations from key encapsulation mechanisms to password authenticated key exchanges. In *International Conference on Applied Cryptography and Network Security*, 2023.

[BDF+11]   Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Advances in Cryptology–ASIACRYPT 2011*, 2011.

[BDK+18]   Joppe Bos, Leo Ducas, Eike Kiltz, T Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehle. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018.

[BDPR98]   Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology — CRYPTO '98*, 1998.

[Ber09]   Daniel J. Bernstein. Introduction to post-quantum cryptography. In *Post-Quantum Cryptography*, 2009.

[BFH+23]   Jonathan Bootle, Sebastian Faller, Julia Hesse, Kristina Hostáková, and Johannes Ottenhues. Generalized fuzzy password-authenticated key exchange from error correcting codes. In *Asiacrypt*, 2023.

[BFK09]   Jens Bender, Marc Fischlin, and Dennis Kügler. Security Analysis of the PACE Key-Agreement Protocol. In *Information Security*, 2009.

[BFM88]   Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, New York, NY, USA, 1988. Association for Computing Machinery.

[BGHJ24]   Manuel Barbosa, Kai Gellert, Julia Hesse, and Stanislaw Jarecki. Bare pake: universally composable key exchange from just passwords. In *Annual International Cryptology Conference*, pages 183–217. Springer, 2024.

[BGV14]   Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1–36, 2014.

[BJSL11]   Ali Bagherzandi, Stanislaw Jarecki, Nitesh Saxena, and Yanbin Lu. Password-protected secret sharing. In *Proceedings of the 18th ACM conference on Computer and Communications Security*, pages 433–444, 2011.

[BKW20]   Dan Boneh, Dmitry Kogan, and Katharine Woo. Oblivious pseudorandom functions from isogenies. In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26*, pages 520–550. Springer, 2020.

[BL17]   Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549, 2017.

[Bla06]   John Black. The ideal-cipher model, revisited: An uninstantiable blockcipher-based hash function. In *Fast Software Encryption: 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers 13*, 2006.

[BM92]   S.M. 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*, 1992.

[BPR00]   Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated Key Exchange Secure against Dictionary Attacks. In *Advances in Cryptology — EUROCRYPT 2000*, 2000.

[BR93]   Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm
             for designing efficient protocols. In *Proceedings of the 1st ACM Conference on
             Computer and Communications Security*, 1993.

[BRRS18]   José Becerra, Peter B Rønne, Peter YA Ryan, and Petra Sala. Honeypakes. In
             *Security Protocols XXVI: 26th International Workshop, Cambridge, UK, March
             19–21, 2018, Revised Selected Papers 26*, pages 63–77. Springer, 2018.

[BSIA23]   Swagatam Basu, Kübra Seyhan, SK Hafizul Islam, and Sedat Akleylek. Mlwr-
             2paka: A hybrid module learning with rounding-based authenticated key agreement
             protocol for two-party communication. *IEEE Systems Journal*, 2023.

[BSP$^+$24] Pia Bauspieß, Tjerand Silde, Matej Poljuha, Alexandre Tullot, Anamaria Costache,
             Christian Rathgeb, Jascha Kolberg, and Christoph Busch. Brake: Biometric resilient
             authenticated key exchange. *IEEE Access*, 2024. doi:10.1109/ACCESS.2024.3380
             915.

[CAK$^+$18] Rakyong Choi, Hyeongcheol An, Kwangjo Kim, et al. AtLast: another three-party
             lattice-based PAKE scheme. In *Proceedings of the 2018 Symposium on Cryptography
             and Information Security (SCIS 2018)*, 2018.

[Can01]   Ran Canetti. Universally composable security: A new paradigm for cryptographic
             protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer
             Science*, 2001.

[CCH$^+$19] Matthew Campagna, Craig Costello, Basil Hess, Amir Jalali, Brian Koziel, Brian
             LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, David Urbanik, et al.
             Supersingular isogeny key encapsulation. https://www.sike.org/files/SIDH-s
             pec.pdf, 2019.

[CCJ$^+$16] Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta,
             Ray Perlner, and Daniel Smith-Tone. Report on Post-Quantum Cryptography. US
             Department of Commerce, National Institute of Standards and Technology, 2016.

[CDM23]   Cas Cremers, Alexander Dax, and Niklas Medinger. Keeping up with the kems:
             Stronger security notions for kems and automated analysis of kem-based protocols.
             2023.

[CGH04]   Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology,
             revisited. *Journal of the ACM (JACM)*, 51(4), 2004.

[CHL22]   Sílvia Casacuberta, Julia Hesse, and Anja Lehmann. Sok: oblivious pseudoran-
             dom functions. In *2022 IEEE 7th European Symposium on Security and Privacy
             (EuroS&P)*, pages 625–646. IEEE, 2022.

[CK01]   Ran Canetti and Hugo Krawczyk. Analysis of Key-Exchange Protocols and Their
             Use for Building Secure Channels. In *Advances in Cryptology – EUROCRYPT
             2001*, 2001.

[CKS23]   Dharminder Chaudhary, Uddeshaya Kumar, and Kashif Saleem. A Construction
             of Three Party Post Quantum Secure Authenticated Key Exchange Using Ring
             Learning with Errors and ECC Cryptography. *IEEE Access*, 2023.

[CL24]   Zhengjun Cao and Lihua Liu. A note on "a new password-authenticated module
             learning with rounding-based key exchange protocol: Saber.PAKE". Cryptology
             ePrint Archive, Paper 2024/683, 2024. URL: https://eprint.iacr.org/2024/683.

[CLM$^+$18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes.
             Csidh: an efficient post-quantum commutative group action. In *Advances in
             Cryptology–ASIACRYPT 2018*, 2018.

[CLN12]   Jan Camenisch, Anna Lysyanskaya, and Gregory Neven. Practical yet universally composable two-server password-authenticated secret sharing. In *Proceedings of the 2012 ACM conference on Computer and Communications Security*, pages 525–536, 2012.

[CS02]   Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *International Conference on the Theory and Applications of Cryptographic Techniques*, 2002.

[DAL+17]   Jintai Ding, Saed Alsayigh, Jean Lancrenon, Saraswathy RV, and Michael Snook. Provably Secure Password Authenticated Key Exchange Based on RLWE for the Post-Quantum World. In *Topics in Cryptology – CT-RSA 2017*, 2017.

[DBK20]   Vivek Dabra, Anju Bala, and Saru Kumari. LBA-PAKE: Lattice-based anonymous password authenticated key exchange for mobile devices. *IEEE Systems Journal*, 2020.

[DBK21]   Vivek Dabra, Anju Bala, and Saru Kumari. LBA-PAKE: Lattice-Based Anonymous Password Authenticated Key Exchange for Mobile Devices. *IEEE Systems Journal*, 2021.

[DCQ22]   Ruoyu Ding, Chi Cheng, and Yue Qin. Further analysis and improvements of a lattice-based anonymous PAKE scheme. *IEEE Systems Journal*, 2022.

[DDN91]   Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In *Symposium on the Theory of Computing*, 1991.

[DdSGP24]   Cyprien Delpech de Saint Guilhem and Robi Pedersen. New proof systems and an oprf from csidh. In *IACR International Conference on Public-Key Cryptography*, pages 217–251. Springer, 2024.

[DF11]   Yi Ding and Lei Fan. Efficient password-based authenticated key exchange from lattices. In *2011 Seventh International Conference on Computational Intelligence and Security*, 2011.

[DFG+23]   Gareth T Davies, Sebastian Faller, Kai Gellert, Tobias Handirk, Julia Hesse, Máté Horváth, and Tibor Jager. Security analysis of the whatsapp end-to-end encrypted backup protocol. In *Annual International Cryptology Conference*, pages 330–361. Springer, 2023.

[DGJ23]   Bruno F. Dos Santos, Yanqi Gu, and Stanislaw Jarecki. Randomized half-ideal cipher on groups with applications to uc (a)pake. In *Advances in Cryptology – EUROCRYPT 2023*. Springer Nature Switzerland, 2023.

[DGJK22]   Bruno F. Dos Santos, Yanqi Gu, Stanislaw Jarecki, and Hugo Krawczyk. Asymmetric PAKE with Low Computation and communication. In *Advances in Cryptology – EUROCRYPT 2022*, 2022.

[DH76]   Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 1976.

[DHP+18]   Pierre-Alain Dupont, Julia Hesse, David Pointcheval, Leonid Reyzin, and Sophia Yakoubov. Fuzzy password-authenticated key exchange. In *Eurocrypt*, 2018.

[Din17]   Jintai Ding. Password based key exchange from ring learning with errors, 2017. URL: https://patents.google.com/patent/WO2017041669A1/en.

[DJRD23]   Pradeep Kumar Dadsena, Jainendra Jain, Saurabh Rana, and Dharminder Dharminder. A construction of post quantum secure authenticated key agreement design for mobile digital rights management system. *Multimedia Tools and Applications*, 82, 2023.

[DKSRV18]   Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Ver-cauteren. Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure kem. In *Progress in Cryptology–AFRICACRYPT 2018*, 2018.

[DRD⁺23]   Dharminder Dharminder, Challa Bhageeratha Reddy, Ashok Kumar Das, Youngho Park, and Sajjad Shaukat Jamal. Post-quantum lattice-based secure reconciliation enabled key agreement protocol for iot. *IEEE Internet of Things Journal*, 2023.

[DRG03]   Mario Di Raimondo and Rosario Gennaro. Provably secure threshold password-authenticated key exchange. In *Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings 22*, pages 507–523. Springer, 2003.

[DXL12]   Jintai Ding, Xiang Xie, and Xiaodong Lin. A simple provably secure key exchange scheme based on the learning with errors problem. *IACR Cryptol. ePrint Arch. 2012/688*, 2012.

[DY83]   Danny Dolev and Andrew Yao. On the security of public key protocols. *IEEE Transactions on information theory*, 1983.

[EHOR20]   Andreas Erwig, Julia Hesse, Maximilian Orlt, and Siavash Riahi. Fuzzy asymmetric password-authenticated key exchange. In *Asiacrypt*, 2020.

[ES21]   Edward Eaton and Douglas Stebila. The "quantum annoying" property of password-authenticated key exchange protocols. In *Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12*, pages 154–173. Springer, 2021.

[FHZ⁺18]   Qi Feng, Debiao He, Sherali Zeadally, Neeraj Kumar, and Kaitai Liang. Ideal lattice-based anonymous authentication protocol for mobile devices. *IEEE Systems Journal*, 2018.

[FIPR05]   Michael J. Freedman, Yuval Ishai, Benny Pinkas, and Omer Reingold. Keyword search and oblivious pseudorandom functions. In *Proceedings of the Second International Conference on Theory of Cryptography*, TCC'05, page 303–324, Berlin, Heidelberg, 2005. Springer-Verlag.

[FO99]   Eiichiro Fujisaki and Tatsuaki Okamoto. How to enhance the security of public-key encryption at minimum cost. In *Public Key Cryptography*, Lecture Notes in Computer Science, 1999.

[FOO23]   Sebastian Faller, Astrid Ottenhues, and Johannes Ottenhues. Composable oblivious pseudo-random functions via garbled circuits. In *International Conference on Cryptology and Information Security in Latin America*, 2023.

[For19]   Internet Engineering Task Force. PAKE Selection Process. IETF, 2019. URL: https://github.com/cfrg/pake-selection.

[FTTY19]   Atsushi Fujioka, Katsuyuki Takashima, Shintaro Terada, and Kazuki Yoneyama. Supersingular isogeny diffie–hellman authenticated key exchange. In *Information Security and Cryptology–ICISC 2018*, 2019.

[GdKQ⁺24]   Phillip Gajland, Bor de Kock, Miguel Quaresma, Giulio Malavolta, and Peter Schwabe. {SWOOSH}: Efficient {Lattice-Based}{Non-Interactive} key exchange. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 487–504, 2024.

[GDL⁺17]   Xinwei Gao, Jintai Ding, Lin Li, RV Saraswathy, and Jiqiang Liu. Efficient implementation of password-based authenticated key exchange from RLWE and post-quantum TLS. *IACR Cryptol. ePrint Arch. 2017/1192*, 2017.

[GDLL17]   Xinwei Gao, Jintai Ding, Jiqiang Liu, and Lin Li. Post-Quantum Secure Remote Password Protocol from RLWE Problem. In *Information Security and Cryptology*, 2017.

[GGM86]   Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, 1986.

[GHP18]   Federico Giacon, Felix Heuer, and Bertram Poettering. Kem combiners. In *Public-Key Cryptography–PKC 2018: 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part I 21*, pages 190–218. Springer, 2018.

[GJK21]   Yanqi Gu, Stanislaw Jarecki, and Hugo Krawczyk. KHAPE: Asymmetric PAKE from Key-Hiding Key Exchange. In *Advances in Cryptology – CRYPTO 2021*, 2021.

[GJK+25]   Yanqi Gu, Stanislaw Jarecki, Pawel Kedzior, Phillip Nazarian, and Jiayu Xu. Threshold pake with security against compromise of all servers. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 66–100. Springer, 2025.

[GL03]   Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. In *International Conference on the Theory and Applications of Cryptographic Techniques*, 2003.

[GM84]   Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 1984.

[GMP22]   Paul Grubbs, Varun Maram, and Kenneth G Paterson. Anonymous, robust post-quantum public key encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2022.

[GMR85]   S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, New York, NY, USA, 1985. Association for Computing Machinery.

[GMR06]   Craig Gentry, Philip MacKenzie, and Zulfikar Ramzan. A method for making password-based key exchange resilient to server compromise. In *Annual International Cryptology Conference*, pages 142–159. Springer, 2006.

[GO14]   Jens Groth and Rafail Ostrovsky. Cryptography in the multi-string model. *Journal of cryptology*, 27(3):506–543, 2014.

[Gro96]   Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, Philadelphia, Pennsylvania, United States, 1996.

[GSG+23]   Songhui Guo, Yunfan Song, Song Guo, Yeming Yang, and Shuaichao Song. Three-Party Password Authentication and Key Exchange Protocol Based on MLWE. *Symmetry*, 2023.

[Har08]   Dan Harkins. Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks. In *2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008)*, 2008.

[HBCvO23]   Feng Hao, Samiran Bag, Liqun Chen, and Paul C. van Oorschot. Owl: An augmented password-authenticated key exchange scheme. Cryptology ePrint Archive, Paper 2023/768, 2023.

[HHM+24]   Lena Heimberger, Tobias Hennerbichler, Fredrik Meisingseth, Sebastian Ramacher, and Christian Rechberger. Oprfs from isogenies: designs and analysis. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, pages 575–588, 2024.

[HPA21]   James Howe, Thomas Prest, and Daniel Apon. Sok: How (not) to design and implement post-quantum cryptography. In *Cryptographers' Track at the RSA Conference*, 2021.

[HR10]   Feng Hao and Peter Ryan. J-pake: authenticated key exchange without pki. *Transactions on Computational Science XI: Special Issue on Security in Computing, Part II*, 2010.

[HR24]   Julia Hesse and Michael Rosenberg. PAKE combiners and efficient post-quantum instantiations. Cryptology ePrint Archive, Paper 2024/1621, 2024. URL: https://eprint.iacr.org/2024/1621.

[HS14]   Feng Hao and Siamak F Shahandashti. The speke protocol revisited. In *International Conference on Research in Security Standardisation*, 2014.

[HvO22]   Feng Hao and Paul C van Oorschot. Sok: Password-authenticated key exchange–theory, practice, standardization and real-world lessons. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022.

[HXL⁺23]   Yunxia Han, Chunxiang Xu, Shanshan Li, Changsong Jiang, and Kefei Chen. ttpake: Typo tolerance password-authenticated key exchange. *Journal of Information Security and Applications*, 79:103658, 2023.

[HY18]   Akinori Hosoyamada and Kan Yasuda. Building quantum-one-way functions from block ciphers: Davies-meyer and merkle-damgård constructions. In *Advances in Cryptology–ASIACRYPT 2018*, 2018.

[IB21]   SK Hafizul Islam and Swagatam Basu. PB-3PAKA: Password-based three-party authenticated key agreement protocol for mobile devices in post-quantum environments. *Journal of Information Security and Applications*, 2021.

[IEE09]   IEEE. IEEE Standard Specification for Password-Based Public-Key Cryptographic Techniques. *IEEE Std 1363.2-2008*, 2009.

[ISO17]   ISO/IEC. Part 4: Mechanisms based on weak secrets. volume 11770-4. Standard, International Organization for Standardization, Geneva, CH, 2017. URL: https://www.iso.org/standard/67933.html.

[Jab96]   David P. Jablon. Strong password-only authenticated key exchange. *ACM SIGCOMM Computer Communication Review*, 1996.

[Jab01]   David P Jablon. Password authentication using multiple servers. In *Cryptographers' Track at the RSA Conference*, pages 344–360. Springer, 2001.

[Jar22]   Stanislaw Jarecki. Password Authenticated Key Exchange: Protocols and Security Models. *Asymmetric Cryptography: Primitives and Protocols*, 2022.

[JGH⁺20]   Shaoquan Jiang, Guang Gong, Jingnan He, Khoa Nguyen, and Huaxiong Wang. PAKEs: new framework, new techniques and more efficient lattice-based constructions in the standard model. In *IACR International Conference on Public-Key Cryptography*, 2020.

[JKK14]   Stanislaw Jarecki, Aggelos Kiayias, and Hugo Krawczyk. Round-optimal password-protected secret sharing and t-pake in the password-only model. In *Advances in Cryptology–ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, ROC, December 7-11, 2014, Proceedings, Part II 20*, pages 233–253. Springer, 2014.

[JKKX16]   Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk, and Jiayu Xu. Highly-efficient and composable password-protected secret sharing (or: How to protect your bitcoin wallet online). In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 276–291. IEEE, 2016.

[JKX18]   Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu. OPAQUE: An Asymmetric PAKE
            Protocol Secure Against Pre-computation Attacks. In *Advances in Cryptology –
            EUROCRYPT 2018*, 2018.

[JMV01]   Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital
            signature algorithm (ecdsa). *International journal of information security*, 1:36–63,
            2001.

[JRX24]   Jake Januzelli, Lawrence Roy, and Jiayu Xu. Under what conditions is encrypted
            key exchange actually secure? Cryptology ePrint Archive, Paper 2024/324, 2024.

[JTCW18]   Yi-Siou Jheng, Raylin Tso, Chien-Ming Chen, and Mu-En Wu. Password-Based
            Authenticated Key Exchange from Lattices for Client/Server Model. In *Advances
            in Computer Science and Ubiquitous Computing*, 2018.

[JZ16]   Zhengzhong Jin and Yunlei Zhao. Optimal key consensus in presence of noise.
            arXiv preprint arXiv:1611.06150, 2016.

[KAA19]   Amir Hassani Karbasi, Reza Ebrahimi Atani, and Shahabaddin Ebrahimi Atani. A
            New Ring-Based SPHF and PAKE Protocol on Ideal Lattices. *ISeCure*, 2019.

[KGKD23]   Uddeshaya Kumar, Manish Garg, Saru Kumari, and Dharminder Dharminder. A
            construction of post quantum secure and signal leakage resistant authenticated
            key agreement protocol for mobile communication. *Transactions on Emerging
            Telecommunications Technologies*, 34(1), 2023.

[KKZZ14]   Jonathan Katz, Aggelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas. Distributing
            the setup in universally composable multi-party computation. In *Proceedings of the
            2014 ACM Symposium on Principles of Distributed Computing*, PODC '14, page
            20–29, New York, NY, USA, 2014. Association for Computing Machinery.

[KM15]   Franziskus Kiefer and Mark Manulis. Oblivious pake: Efficient handling of password
            trials. In *International Conference on Information Security*, pages 191–208. Springer,
            2015.

[KNW18]   Michael Kreutzer, Ruben Niederhagen, and Michael Waidner. Eberbacher Gespräch
            on Next Generation Crypto. *Fraunhofer SIT*, 2018.

[KOY01]   Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient password-authenticated
            key exchange using human-memorable passwords. In *International Conference on
            the Theory and Applications of Cryptographic Techniques*, 2001.

[KR24]   Jonathan Katz and Michael Rosenberg. Latke: a framework for constructing
            identity-binding pakes. In *Annual International Cryptology Conference*, pages
            218–250. Springer, 2024.

[KRSS19]   Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. pqm4:
            Testing and benchmarking NIST PQC on ARM cortex-m4. Cryptology ePrint
            Archive, Paper 2019/844, 2019. URL: https://eprint.iacr.org/2019/844.

[KTAT20]   Tomoki Kawashima, Katsuyuki Takashima, Yusuke Aikawa, and Tsuyoshi Takagi.
            An efficient authenticated key exchange from random self-reducibility on CSIDH.
            Cryptology ePrint Archive, Paper 2020/1178, 2020.

[KV09]   Jonathan Katz and Vinod Vaikuntanathan. Smooth projective hashing and
            password-based authenticated key exchange from lattices. In *International Con-
            ference on the Theory and Application of Cryptology and Information Security*,
            2009.

[KV13]   Jonathan Katz and Vinod Vaikuntanathan. Round-optimal password-based au-
            thenticated key exchange. *Journal of Cryptology*, 2013.

[LL24]   You Lyu and Shengli Liu. Hybrid password authentication key exchange in the
            UC framework. Cryptology ePrint Archive, Paper 2024/1630, 2024. URL: https:
            //eprint.iacr.org/2024/1630.

[LLH24]   You Lyu, Shengli Liu, and Shuai Han. Universal composable password authenticated
            key exchange for the post-quantum world. In *Annual International Conference on
            the Theory and Applications of Cryptographic Techniques*, 2024.

[LLH25]   You Lyu, Shengli Liu, and Shuai Han. Efficient asymmetric pake compiler from kem
            and ae. In *International Conference on the Theory and Application of Cryptology
            and Information Security*, pages 34–65. Springer, 2025.

[LPR10]   Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning
            with errors over rings. In *Advances in Cryptology–EUROCRYPT 2010: 29th
            Annual International Conference on the Theory and Applications of Cryptographic
            Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*, pages 1–23.
            Springer, 2010.

[LS15]   Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for
            module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015. doi:
            10.1007/s10623-014-9938-4.

[LST16]   Jean Lancrenon, Marjan Skrobot, and Qiang Tang. Two more efficient variants of
            the J-PAKE protocol. In *Applied Cryptography and Network Security - 14th Inter-
            national Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings*,
            volume 9696 of *Lecture Notes in Computer Science*, pages 58–76. Springer, 2016.

[LW18]   Zengpeng Li and Ding Wang. Two-Round PAKE Protocol over Lattices With-
            out NIZK. In *International Conference on Information Security and Cryptology*.
            Springer, 2018.

[LW19]   Zengpeng Li and Ding Wang. Achieving One-Round Password-based Authenticated
            Key Exchange over Lattices. *IEEE Transactions on Services Computing*, 2019.

[LWL22]   Wenting Li, Ping Wang, and Kaitai Liang. Hpake: Honey password-authenticated
            key exchange for fast and safer online authentication. *IEEE Transactions on
            Information Forensics and Security*, 18:1596–1609, 2022.

[LWM22]   Zengpeng Li, Ding Wang, and Eduardo Morais. Quantum-Safe Round-Optimal
            Password Authentication for Mobile Devices. *IEEE Transactions on Dependable
            and Secure Computing*, 2022.

[LZJY19]   Chao Liu, Zhongxiang Zheng, Keting Jia, and Qidi You. Provably secure three-party
            password-based authenticated key exchange from rlwe. In *Information Security
            Practice and Experience: 15th International Conference, ISPEC 2019*, 2019.

[Mac02]   Philip MacKenzie. The PAK suite: Protocols for Password-Authenticated Key
            Exchange. In *Ieee P1363.2*, 2002.

[MP12]   Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter,
            faster, smaller. In *Annual International Conference on the Theory and Applications
            of Cryptographic Techniques*, 2012.

[MX23]   Varun Maram and Keita Xagawa. Post-quantum anonymity of kyber. In *IACR
            International Conference on Public-Key Cryptography*. Springer, 2023.

[NR04]   Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-
            random functions. *J. ACM*, 51(2):231–262, 2004.

[NY90]   M Naor and M Yung. Public-key cryptosystems provably secure against chosen
            ciphertext attacks. In *Proceedings of the twenty-second annual ACM symposium on
            Theory of computing - STOC '90*, 1990.

[OP01]   Tatsuaki Okamoto and David Pointcheval. React: Rapid enhanced-security asymmetric cryptosystem transform. In *Topics in Cryptology — CT-RSA 2001*, 2001.

[Ott24]   Johannes Ottenhues. An overview of symmetric fuzzy pake protocols. *Sicherheit 2024*, 2024.

[Pei14]   Chris Peikert. Lattice Cryptography for the Internet. In *Post-Quantum Cryptography*, 2014.

[Poi22]   David Pointcheval. *Asymmetric Cryptography: Primitives and Protocols*. John Wiley & Sons, Inc. Hoboken, NJ, USA, 2022.

[PZ23]   Jiaxin Pan and Runzhi Zeng. A generic construction of tightly secure password-based authenticated key exchange. In *International Conference on the Theory and Application of Cryptology and Information Security*, 2023.

[Reg05]   Oded 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 '05, page 84–93, New York, NY, USA, 2005. Association for Computing Machinery. doi:10.1145/1060590.1060603.

[Reg06]   Oded Regev. Lattice-based cryptography. In *Annual International Cryptology Conference*. Springer, 2006.

[Reg10]   Oded Regev. The learning with errors problem. *Invited survey in CCC*, 7(30):11, 2010.

[RG22]   Peixin Ren and Xiaozhuo Gu. Practical Post-quantum Password-Authenticated Key Exchange Based-on Module-Lattice. In *Information Security and Cryptology – ICISC 2021*, 2022.

[RGW23]   Peixin Ren, Xiaozhuo Gu, and Ziliang Wang. Efficient module learning with errors-based post-quantum password-authenticated key exchange. *IET Information Security*, 2023.

[RHCB21]   Prasanna Ravi, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. Lattice-Based Key-Sharing Schemes: A Survey. *ACM Comput. Surv.*, 2021.

[RS91]   Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Annual international cryptology conference*, 1991.

[RSA78]   Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[RSM+23]   Purva Rewal, Mrityunjay Singh, Dheerendra Mishra, Komal Pursharthi, and Ankita Mishra. Quantum-safe three-party lattice based authenticated key agreement protocol for mobile devices. *Journal of Information Security and Applications*, 2023.

[SA23]   Kübra Seyhan and Sedat Akleylek. A new password-authenticated module learning with rounding-based key exchange protocol: Saber.PAKE. *The Journal of Supercomputing*, 2023.

[SA24]   Kübra Seyhan and Sedat Akleylek. A new lattice-based password authenticated key exchange scheme with anonymity and reusable key. *PeerJ Computer Science*, 2024.

[Sch91]   Claus-Peter Schnorr. Efficient signature generation by smart cards. J. Cryptology 4, 1991.

[Sch24]   Sophie Schmieg. Unbindable kemmy schmidt: Ml-kem is neither mal-bind-k-ct nor mal-bind-k-pk. 2024.

[Sho97]   Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 1997.

[SM16]   Douglas Stebila and Michele Mosca. Post-quantum key exchange for the internet and the open quantum safe project. In *International Conference on Selected Areas in Cryptography*, pages 14–37. Springer, 2016.

[Smi18]   Benjamin Smith. Pre-and post-quantum diffie–hellman from groups, actions, and isogenies. In *Arithmetic of Finite Fields: 7th International Workshop, WAIFI 2018*, 2018.

[SS19]   Shingo Sato and Junji Shikata. So-cca secure pke in the quantum random oracle model or the quantum ideal cipher model. In *Cryptography and Coding: 17th IMA International Conference*, 2019.

[SWL$^+$21]   Qin SHU, Shengbao WANG, Fanyi LU, Lidong HAN, and Xiao TAN. Universally Composable Two-Party Password-Based Authenticated Key Exchange from Ideal Lattices. *Journal of Electronics & Information Technology*, 43, 2021.

[TES23]   Marcel Tiepelt, Edward Eaton, and Douglas Stebila. Making an asymmetric pake quantum-annoying by hiding group elements. In *European Symposium on Research in Computer Security*, pages 168–188. Springer, 2023.

[TLZ$^+$21]   Yongli Tang, Ying Li, Zongqu Zhao, Jing Zhang, Lina Ren, and Yuanhong Li. Improved verifier-based three-party password-authenticated key exchange protocol from ideal lattices. *Security and Communication Networks*, 2021.

[TSJL20]   Oleg Taraskin, Vladimir Soukharev, David Jao, and Jason T LeGrow. Towards isogeny-based password-authenticated key establishment. *Journal of Mathematical Cryptology*, 2020.

[TY19]   Shintaro Terada and Kazuki Yoneyama. Password-Based Authenticated Key Exchange from Standard Isogeny Assumptions. In *Provable Security*, 2019.

[Unr20]   Dominique Unruh. Post-quantum verification of fujisaki-okamoto. In *Advances in Cryptology – ASIACRYPT 2020*, 2020.

[Unr23]   Dominique Unruh. Towards compressed permutation oracles. In *International Conference on the Theory and Application of Cryptology and Information Security*, 2023.

[WCL$^+$23]   Jinhua Wang, Ting Chen, Yanyan Liu, Yu Zhou, and XinFeng Dong. Efficient Two-Party Authentication Key Agreement Protocol Using Reconciliation Mechanism from Lattice. In *International Conference on Security and Privacy in New Computing Environments*, 2023.

[WCW$^+$17]   Ding Wang, Haibo Cheng, Ping Wang, Xinyi Huang, and Gaopeng Jian. Zipf's law in passwords. *IEEE Transactions on Information Forensics and Security*, 2017.

[WHC$^+$21]   Mei Wang, Kun He, Jing Chen, Zengpeng Li, Wei Zhao, and Ruiying Du. Biometrics-authenticated key exchange for secure messaging. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 2618–2631, 2021.

[Wu98]   Thomas D. Wu. The secure remote password protocol. In *Network and Distributed System Security Symposium*, 1998.

[Wu02]   Thomas D. Wu. Srp-6: Improvements and refinements to the secure remote password protocol, 2002. URL: http://srp.stanford.edu.

[Xag22]   Keita Xagawa. Anonymity of nist pqc round 3 kems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2022.

[XHCC17]   Dongqing Xu, Debiao He, Kim-Kwang Raymond Choo, and Jianhua Chen. Provably
            Secure Three-party Password Authenticated Key Exchange Protocol Based On
            Ring Learning With Error. *IACR Cryptol. ePrint Arch. 2017/360*, 2017.

[XZZ24]   Yuting Xiao, Rui Zhang, and Hong-Sheng Zhou. Maximizing the utility of crypto-
            graphic setups: Secure PAKEs, with either functional RO or CRS. Cryptology ePrint
            Archive, Paper 2024/1640, 2024. URL: https://eprint.iacr.org/2024/1640.

[YGS+20]   Anqi Yin, Yuanbo Guo, Yuanming Song, Tongzhou Qu, and Chen Fang. Two-
            Round Password-Based Authenticated Key Exchange from Lattices. *Wireless
            Communications and Mobile Computing*, 2020.

[YGWX19]   Yingshan Yang, Xiaozhuo Gu, Bin Wang, and Taizhong Xu. Efficient password-
            authenticated key exchange from RLWE based on asymmetric key consensus. In
            International Conference on Information Security and Cryptology, 2019.

[YHL13]   Mao Ye, Xue-xian Hu, and Wen-fen Liu. Password authenticated key exchange
            protocol in the three party setting based on lattices. *Journal of Electronics &
            Information Technology*, 2013.

[YLZ+21]   Jinxia Yu, Huanhuan Lian, Zongqu Zhao, Yongli Tang, and Xiaojun Wang. Chapter
            Four - Provably secure verifier-based password authenticated key exchange based
            on lattices. In *Advances in Computers*, 2021.

[YZ21]   Takashi Yamakawa and Mark Zhandry. Classical vs quantum random oracles. In
            *Annual International Conference on the Theory and Applications of Cryptographic
            Techniques*, 2021.

[ZG15]   Hongfeng Zhu and Shuai Geng. Simple and Universal Construction for Round-
            Optimal Password Authenticated Key Exchange towards Quantum-Resistant. *Jour-
            nal of Information Hiding and Multimedia Signal Processing*, 2015.

[ZHS14]   Hongfeng Zhu, Xin Hao, and Yang Sun. Elliptic Curve Isogenies-Based Three-party
            Password Authenticated Key Agreement Scheme towards Quantum-Resistant. *J.
            Inf. Hiding Multim. Signal Process.*, 2014.

[ZTJ21]   Li Zi-chen, Xie Ting, and Zhang Juan-mei. Post Quantum Password-Based Au-
            thentication Key Exchange Protocol Based on Ring Learning with Errors Problem.
            ACTA ELECTONICA SINICA, 2021.

[ZY17]   Jiang Zhang and Yu Yu. Two-round PAKE from approximate SPH and instantiations
            from lattices. In *Advances in Cryptology–ASIACRYPT 2017*, 2017.

[ZYL+23]   Shiwen Zhang, Ziwei Yan, Wei Liang, Kuan-Ching Li, and Ciprian Dobre. Baka:
            Biometric authentication and key agreement scheme based on fuzzy extractor for
            wireless body area networks. *IEEE Internet of Things Journal*, 2023.