SoK: PQC PAKEs
Design, Security and Performance

Nouri Alnahawi[1,4], David Haas[2], Erik Mauß[1,4] and Alexander Wiesmaier[1,3,4]

[1] Hochschule Darmstadt, Germany
[2] Technical University, Darmstadt, Germany
[3] National Research Center for Applied Cybersecurity ATHENE, Germany
[4] European University of Technology, European Union

Abstract. Password Authenticated Key Exchange (PAKE) establishes secure communication channels using passwords for authentication. Currently, standardized PAKEs rely on classical asymmetric cryptography. However, these PAKEs may become insecure should the expected quantum threat become a reality. Despite the growing interest in realizing quantum-safe PAKEs, they did not receive much attention from the ongoing Post-Quantum Cryptography (PQC) integration efforts. Hence, there is a significant awareness gap compared to PQC primitives subject to the official standardization processes. We provide a comprehensive overview of existing PQC PAKEs, classify their design rationales and authentication methods, and address aspects related to their security and performance. We identify PAKE designs that are still unexplored in the PQC realm and discuss the possibility of their adaptation. Thus, we offer a detailed reference for future work on PQC PAKEs.

Keywords: SoK · PAKE · PQC · Key Agreement · KEM

1 Introduction

Ever since their emergence in the early 1990s [BM92], *Password Authenticated Key Exchange* (PAKE) protocols have been a subject of numerous studies [HvO22]. According to [HvO22], PAKEs are present in applications such as credential recovery (e.g., *iCloud* and *ProtonMail*), device pairing (e.g., *E-Passport*, *Bluetooth*, and *WLAN WPA3 i.e., Dragonfly*), and E2E secure communication (e.g., *Thread*[1]). Over the last decade, advances in quantum computing and its threat to (classical) asymmetric cryptography have attracted studies towards realizing PAKEs based on Post-Quantum Cryptography (PQC). We present an overview of PQC PAKEs in the literature and classify them according to their design paradigms and cryptographic building blocks.

1.1 Password Authenticated Key Exchange

PAKE is a special form of key agreement that adds password authentication to key exchange [Jar22]. They establish secure communication over an insecure channel, where authentication is done using a password or a PIN. Hence, they pose the question of how password authentication can be achieved combined with a passively secure key

E-mail: nouri.alnahawi@h-da.de (Nouri Alnahawi), david.haas1@stud.tu-darmstadt.de (David Haas), erik.mauss@stud.h-da.de (Erik Mauß), alexander.wiesmaier@h-da.de (Alexander Wiesmaier)

[1]Thread is an IPv6 network protocol for IoT, mesh, and Wireless Personal Area Networks (WPAN). Further information available at https://threadgroup.org/ and https://openthread.io/

This work is licensed under a "CC BY 4.0" license.
Date of this document: 2026-09-11.

agreement [Jar22]. The first PAKE protocol by Bellovin and Merritt, *Encrypted Key Exchange* (EKE), combines symmetric encryption with asymmetric key agreement [BM92]. By encrypting the public key with a password (or a value derived from it), an attacker cannot manipulate the key agreement [Jar22]. Similar approaches are also found in *Password Authenticated Key Agreement* (PAK) [Mac02], *Simple Password Exponential Key Exchange* (SPEKE) [Jab96], and *Password Authenticated Connection Establishment* (PACE) [BFK09]; typically instantiated with (EC)DH[2].

1.2 Motivation and Contribution

Recently, the hybrid PAKE protocol CPaceOQUAKE+ was proposed to IETF as an internet draft [VJW25a]. However, none of the PAKE schemes selected in previous standardizations by IEEE (P1363.2 [IEE09]), ISO/IEC (11770-4 [ISO17]) or IETF (CFRG 104 [For19]) are quantum safe. To the best of our knowledge, there are no dedicated peer-reviewed surveys on PQC PAKEs. We provide an extensive and comprehensive overview of PQC PAKE proposals identified in the literature addressing PAKEs built directly from PQC primitives or on top of PQC *Key Encapsulation Mechanisms* (KEM). This includes PAKEs from lattice and isogeny assumptions and generic and semi-generic PQC KEMs. We investigate said PAKEs and point out aspects we deem necessary to grasp the differences and issues of constructing PAKEs from PQC schemes. We build on the systematic review in [HvO22] and adapt their classification of classical PAKEs to PQC ones. By doing so, we enable a direct comparison to classical designs, show the tight relations between classical and PQC PAKEs, and incorporate generic designs. Considering performance and security aspects, we collect available benchmarks and provide an overview as per the proposed instantiations, parameters, and security models. Further, we address PAKE designs that are currently non-present in the PQC realm and discuss the possibility of their instantiations. Finally, we highlight open issues, takeaways, and future work.

1.3 Methodology

This SoK follows a structured Systematic Literature Review (SLR) methodology [KC07, CROLL22]. Its main objective is to systematically identify, classify, and compare existing PQC PAKEs, thereby providing a comprehensive overview of the current state of the field. The review protocol was defined prior to the analysis and specifies the research questions, search strategy, study selection criteria, and data extraction process.

Research Questions. This work is guided by the following research questions addressing the landscape of PQC PAKEs. 1) Which PQC PAKEs have been proposed in the literature? 2) Which PQC hardness assumptions underlie these proposals? 3) Which authentication paradigms (e.g., balanced vs. augmented) are employed? 4) Which PQC families (e.g., lattice- or code-based etc.) and generic KEMs are used? 5) Which formal models and proof techniques are used to establish security? 6) How do the proposed PAKEs compare in terms of complexity? 7) What limitations, research gaps, and open problems remain?

Search Strategy. Relevant papers were identified via a structured keyword search across scientific databases, including IACR ePrint, ACM Digital Library, IEEE Xplore, SpringerLink, ScienceDirect, DBLP, Scholar, and ResearchGate. The search mainly employed combinations of terms related to PAKE and PQC (e.g., PQC PAKE or quantum-safe PAKE etc.). To improve completeness, initial seed works (Ding et al. [DAL+17] and Beguinet et al. [BCP+23]) were used in a backward and forward snowballing search. The

[2]We refer to [HvO22] for a complete overview of *classical* PAKEs and their real-world applications, as well as more details on the past official PAKE standardization processes.

literature search was finalized on the 18th of July 2025. Publications appearing after this date are not considered in this version of the document.

Inclusion and Exclusion Criteria. Candidate publications were screened using predefined inclusion and exclusion criteria. Only publications written in English proposing, extending, or analyzing post-quantum PAKE protocols with sufficient technical detail were considered. Both peer-reviewed publications and publicly available ePrints were included. Duplicate publications, non-PQC PAKEs, incomplete protocol descriptions, protocols with no formal analysis and publications without publicly accessible full texts were excluded.

Data Extraction. For each included study, a common set of protocol characteristics was extracted to facilitate consistent comparison (cf. Tab. 1). These include the authentication paradigm, underlying computational assumption, PQC family, generic KEM (where applicable), security model, proof model and implementation or experimental evaluation. Further aspects and details also include communication complexity, computational complexity and round complexity (cf. Sec. 7).

Data Synthesis. The extracted information is synthesized through qualitative comparison and thematic classification. Protocols are grouped according to their cryptographic construction, security assumptions, and design methodology, enabling the identification of common design patterns, trade-offs, limitations, and open research problems.

1.4 How to Read this Paper

Due to the immense number of PQC PAKEs in the literature and the involved building blocks, we opted for a (bottom-up) SoK that enables researchers and scholars to navigate relevant aspects from A to Z in one paper. Fig. 1 illustrates the methodology and structure of this paper. In order to facilitate an optimal reading experience, we recommend one of the following reading approaches depending on the expertise and interest of the reader.

1) Readers unfamiliar with PAKEs can start with the basic concepts in Sec. 2. Here, we provide a formal definition of PAKE and describe the rationale for PAKE security and variants thereof (e.g., PAKE security frameworks).

2) Readers new to PQC can explore the primitives and building blocks in Sec. 3. While we focus on bare PQC primitives (i.e., asymmetric crypto-systems from lattices) in Sec. 3.1, we also address more complex (supporting) constructions in Sec. 3.2, which can be obtained from the former (e.g., zero-knowledge from lattices).

3) Readers interested in KEM research and abstract properties may consult Sec. 4. Since a PAKE is a key agreement protocol at its core, we address the subtleties of key exchange (and key encapsulation) security properties, which play an essential role in all PAKE designs and especially in generic ones.

4) Readers new to idealized models (objects) may refer to Sec. 5. This section covers the state-of-the-art in cryptographic idealized models used in PAKEs and their applicability in the presence of quantum adversaries (e.g., ROM vs. QROM).

5) Ultimate experts may skip directly to Sec. 6. Here, we (technically) describe the reviewed PQC PAKEs within their respective classes, and derive relevant observations.

The rest of the paper is organized as follows. Sec. 7 reviews the security and performance of the surveyed PQC PAKEs. Real world use cases are reviewed in Sec. 8 and discussed respectively. Sec. 9 deals with unexplored classical designs and non-PQC quantum-safe PAKEs. Finally, Sec. 10 provides an elaborate discussion on the identified observations, takeaways, open questions, and future directions.

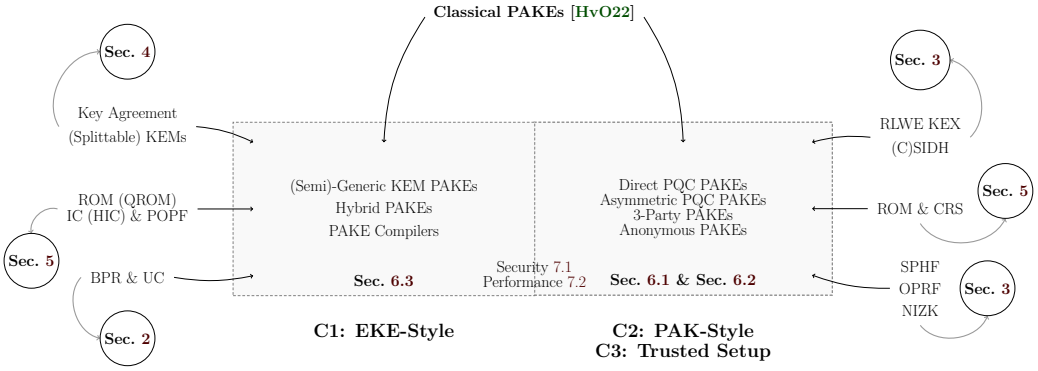


Figure 1: Overview of PQC PAKE Design Classes, Primitives and Security Models.

1.5 PAKE Classification by Hao and van Oorschot [HvO22]

Hao and van Oorschot [HvO22] presented a classification and review of the state-of-the-art of classical PAKEs and provided practical insights on real-world applications and standardization. The authors defined five classes w.r.t. password usage, which is referred to as the design paradigm. The key aspect here is the password representation and how it is (cryptographically) applied to protect the asymmetric key agreement. Generally, the password is rarely used in its bare form, but rather as input to an Extended Output Function (XOF) to obtain a fixed-length value (e.g., obtaining an AES key using a Key Derivation Function (KDF)) or as a group element (e.g., a generator or exponent) in an operation on the underlying number-theoretic assumptions. Additionally, it can be used within more complex primitives (cf. Sec. 3), where a trusted set-up is required. Intuitively, almost all classical PAKEs are based on the hardness of some variant of (EC)DH such as the Computational (C)DH or Decision (D)DH problems.

1.6 Adapted Classification System

We adapt the classification of [HvO22] to PQC PAKEs w.r.t. password usage as follows.

C1) **Password Encrypted Public Key** (aka *EKE-style*): The password (or a password-derived symmetric key) is used directly to encrypt or hide the public key, e.g., *(O)CAKE* [BCP+23]. Encryption is done using a symmetric key (e.g. AES), where the block cipher is modeled as an IC and hash functions as ROs. The PQC CAKE protocol is built similar to the classical EKE [BM92], however using a KEM instead of DH for the key agreement (cf. Fig. 11). Hence, overall PAKE security is mainly realized on the basis of the underlying KEM properties.

C2) **Password Modified Public Key** (aka *PAK-style*): The password is used to modify the public key while preserving the underlying hardness assumption of the KEX primitive, e.g., *RLWE-PAK* [DAL+17]. As in the classical version [Mac02], the PAK and PPK designs change the value of a public key by combining it (mathematically) with the hash of the password. The RO-modeled hash value is interpreted as a group element and hence it is called Hash-to-Group (H2G). The modified public key is also a valid group element. Hence, security is based on the hardness of the underlying KEX. RLWE-PAK utilizes a lattice RLWE crypto-system to realize this design by adding the password hash to an RLWE sample (cf. Fig. 8).

C3) **Trusted Setup**: Multiple approaches, where predefined trusted parameters are required to achieve authentication, e.g., *KV-PAKE* [KV09] and *GA-PAKE* [AEK+22a]. The classical variants assumed parameters such as two or more related group generators, as introduced in the KOY [KOY01] and SPAKE2 [AP05] protocols. However, group generators are not really applicable to PQC. Hence, a PQC PKE or KEX are combined with previously established parameters known only to honest parties to realize a trusted setup. Such PAKEs often rely on additional (complex) supporting cryptographic building blocks (cf. Sec. 3) to verify the authentication using said pre-established values as in *KV-PAKE* [KV09]. Security is usually in the standard model (i.e., no idealized assumptions), but may require a Common Reference String (CRS) to model the trusted parameters as in *GA-PAKE* [AEK+22a].

Although [HvO22] introduced five design classes, only classes C1, C2, and C3 apply to current PQC PAKEs, as classes C4 and C5 do not (yet) have any representatives in the PQC realm (cf. Sec. 9). Some works could be categorized into more than one class at the same time (e.g., RLWE-PAK in a trusted setup). Generic PAKEs may be considered a class of their own; however, they also adhere to the same classes w.r.t. password usage. For instance, both CAKE and NoIC are generic, yet CAKE relies on block ciphers (IC) to encrypt public keys, and NoIC utilizes an H2G in the ROM to modify them.

1.7 Related Work

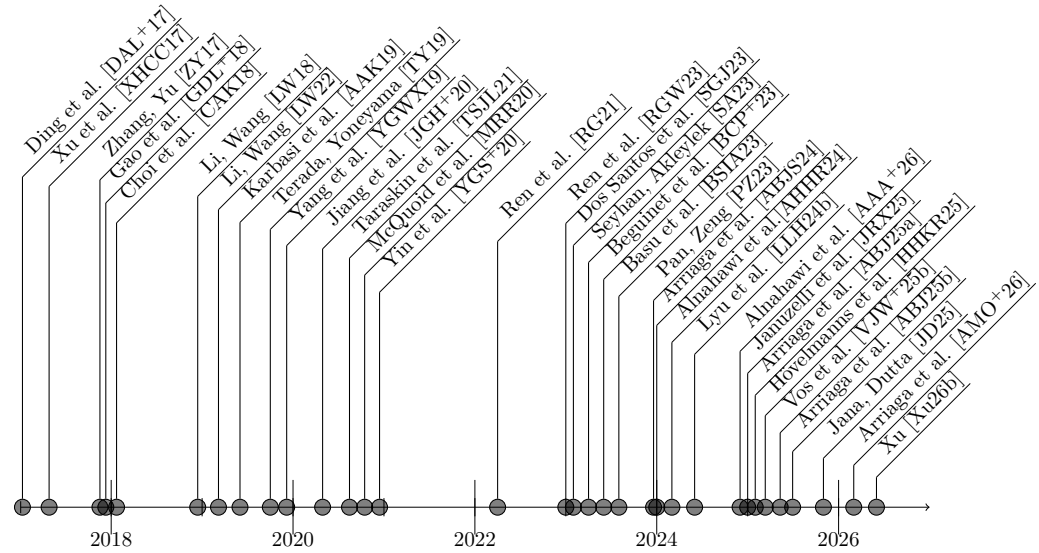
Azarderakhsh et al. [AJK+20] discuss isogeny PAKEs and show the difficulty of obtaining them from DH-based designs. To our knowledge, no other works in the literature address PQC PAKEs particularly. The rest of related work focus on classical PAKEs, but nevertheless prove valuable for our own overview. The work of Abdalla [Abd14] is one of the first papers to address the design and security of PAKE protocols. It sufficiently describes the beginnings of PAKE design studies (e.g., EKE [BM92] and its variants) and classifies follow-up PAKEs based on their construction approach. In [Jar22], Jarecki provides a detailed overview of the methods used to construct PAKEs from classical asymmetric cryptography. It offers a thorough analysis of the design and security of PAKEs in different security frameworks, as well as their strengths and shortcomings.

1.8 Overview

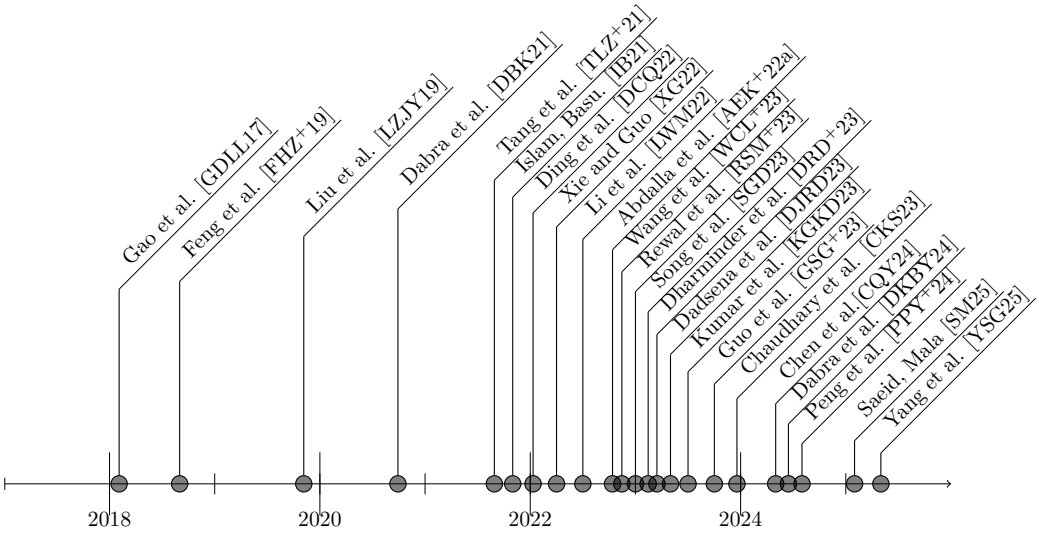
PQC PAKEs date before the start of the NIST PQC standardization process. The LWE PAKE by Katz and Vaikuntanathan [KV09] in 2009 and the isogeny-based PAKE by Zhu et al. [ZHS14] in 2014 may therefore, and to the best of our knowledge, be considered the very first PQC PAKEs. However, the RLWE PAKE by Ding et al. [DAL+17] in 2017 marks the emergence of many other PQC PAKE proposals (cf. Timeline in Fig. 2).

An overview of all surveyed PAKEs and their properties is presented in Tab. 1, which consists of two parts dividing *balanced* and *augmented* PAKEs. In each part, we group PAKEs into their respective design classes. We collected over 50 papers, all but eight were taken into account in this SoK[3]. These include more than 30 PAKEs based on lattice LWE and variants. The remaining works consist of six (C)SIDH isogeny PAKEs and thirteen generic PAKEs.

[3]Ye et al. [YHL13] (full-text unavailable), Ding and Fang [DF11] and Jheng et al. [JTCW17] (incomplete works), Yu et al. [YLZ+21] and Zhu et al. [ZWCW22] (paid access), Zi-chen et al. [ZTJ21] and Shu et al. [SWL+21] (written in Chinese), and Seyhan and Akleylek [SA24] (unknown assumption).



(a) Balanced PAKEs



(b) Augmented PAKEs

Figure 2: Timeline of Balanced and Augmented PQC PAKE Publications - Not Including Hybrid and Asymmetric Compiler Frameworks.

Table 1: PQC PAKE Overview / Landscape - Hybrid and aPAKE Compilers Excluded.

Class	Scheme	Year	Security Model	Assumptions	Proof Framework	Properties					
						Generic[1]	Quantum-Safe[2]	Peer-Reviewed	2-Party	3-Party	Benchmarks	Provide Impl.	Recomm. Param.
Balanced													
C1	Terada, Yoneyama [TY19] ((C)SIDH-EKE)	2019	IC, ROM	(C)SIDH†	BPR			✓	✓		✓		
	McQuoid et al. [MRR20] (sPAKE)	2020	ROM	-	UC	✓		✓	✓				
	Beguinet et al. [BCP+23] ((O)CAKE)	2023	IC, ROM	(M)LWE	UC	✓		✓	✓				
	Dos Santos et al. [SGJ23] (HIC-EKE/KEM)	2023	IC, ROM	MLWE(R)[3]	UC	✓		✓	✓				
	Pan, Zeng [PZ23] (CAKE)	2023	IC, ROM	(M)LWE	BPR	✓		✓	✓				
	Alnahawi et al. [AHHR24] (OCAKE)	2023	IC, ROM	(M)LWE	BPR	✓		✓	✓		✓	✓	
	Arriaga et al. [ABJS24] (CHIC)	2024	IC, ROM	(M)LWE	UC	✓		✓	✓		✓	✓	✓
	Alnahawi et al. [AAA+26] (NICE-PAKE)	2024	ROM	(M)LWE	BPR	✓	✓		✓				✓
	Januzelli et al. [JRX25] ((O)EKE/(O)CAKE)	2025	ROM	-	UC	✓		✓	✓				
	Arriaga et al. [ABJ25a] (NoIC-PAKE)	2025	ROM	-	UC	✓			✓				
	Hövelmanns et al. [HHKR25] ((O)CAKE)	2025	(IC), QROM	(M)LWE	BPR	✓			✓				
	Vos et al. [VJW+25b] (OQUAKE)	2025	ROM	MLWE	UC	✓			✓				
	Arriaga et al. [ABJ25b] (TEMPO)	2025	ROM	MLWE	BPR	✓			✓				
	Arriaga et al. [AMO+26] (PAPKE-HIC)	2026	IC,ROM	-	UC	✓		✓	✓		✓	✓	✓
	Xu [Xu26b] (OEKE-2F)	2026	ROM	-	UC	✓			✓				
C2	Zhu, Geng [ZG17]	2015	-	(C)SIDH†	CK				✓				
	Alsayigh [Als16]	2016	ROM	RLWE	BPR				✓				✓
	Ding et al. [DAL+17] (RLWE-PAK-PPK)	2017	ROM	RLWE	BPR			✓	✓		✓		
	Gao et al. [GDL+18] (RLWE-PAK-PPK)	2017	ROM	RLWE	BPR				✓		✓		
	Taraskin et al. [TSJL21] (SIDH-PAK)	2019	ROM	SIDH	BPR				✓		✓		✓
	Yang et al. [YGWX19] (RLWE-PAK)	2019	ROM	RLWE	BPR			✓	✓		✓		✓
	Jiang et al. [JGH+20] (PAKEs)	2020	ROM	(R)LWE	BPR			✓	✓		✓		✓
	Ren et al. [RGW23]([RG21]) (MLWE-PAK)	2022	-	MLWE	Multiple			✓	✓		✓	✓	✓
	~~Seyhan, Akleylek~~ [SA23]*	2023	ROM	MLWR	Multiple				✓		✓	✓	✓
	Basu et al. [BSIA23] (MLWR-2PAKA)	2023	ROM	MLWR	DY			✓	✓				✓
	Jana, Dutta [JD25] (iPAKE)	2025	ROM	RLWR[4]	BPR				✓				
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. [CAK18] (AtLast)	2018	ROM	RLWE	BPR			✓		✓			
	Li, Wang [LW18]	2018	CRS	LWE	BPR	✓		✓	✓				
	Li, Wang [LW22]	2019	CRS	LWE	BPR	✓		✓	✓				
	Karbasi et al. [AAK19] (Ring-PAKE)	2019	CRS	RLWE	BPR	✓		✓	✓				
	Yin et al. [YGS+20]	2020	ROM	LWE	BPR			✓	✓	✓			
	Lyu et al. [LLH24b] ((e)LPKE-PAKE)	2024	(Q)ROM	(M)LWE[5]	UC	✓	✓	✓	✓				
Augmented													
C2	Gao et al. [GDLL17]	2018	-	RLWE	UC			✓	✓		✓		✓
C3	Zhu et al. [ZHS14]	2014	-	SIDH†	CK			✓		✓			
	Feng et al. [FHZ+19]	2018	ROM	RLWE	BPR			✓	✓		✓		✓
	Liu et al. [LZJY19]	2019	ROM	RLWE	Multiple					✓	✓	✓	✓
	Dabra et al. [DBK21] (LBA-PAKE)	2020	ROM	RLWE	FTG			✓	✓		✓		✓
	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			✓	✓		✓	✓	✓
	Xie and Guo [XG22]	2022	CRS,ROM	RLWE	BPR			✓		✓			
	Li et al. [LWM22]	2022	CRS	LWE(R)[3]	BPR	✓		✓	✓		✓		✓
	Abdalla et al. [AEK+22a] (X-GA-PAKE)	2022	CRS	CSIDH	BPR			✓	✓				
	Wang et al. [WCL+23] (LB-ID-2PAKA)	2023	ROM	MLWE	BPR			✓	✓				
	Rewal et al. [RSM+23]	2023	ROM	RLWE	BPR			✓		✓	✓		✓
	Song et al. [SGD23]	2023	CRS,ROM	RLWE	BPR			✓	✓				
	Dharminder et al. [DRD+23]	2023	Standard	RLWE	Multiple			✓	✓		✓		✓
	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			✓		✓	✓		✓
	Chen et al.[CQY24] (Multi-PAKE)	2024	CRS	LWE	BPR			✓	✓		✓		✓
	Dabra et al. [DKBY24] (SL3PAKE)	2024	ROM	RLWE	BPR			✓		✓	✓		✓
	Peng et al. [PPY+24] (R-GA-PAKE)	2024	CRS	CSIDH	BPR			✓	✓				✓
	Yang et al. [YZYW25] (K-PAKE)	2025	ROM	MLWE	UC			✓	✓		✓		
	Saeid, Mala [SM25] (APAKE)	2025	ROM	RLWE	BPR			✓	✓		✓		✓
	Yang et al. [YSG25] (2-Server-PAKE)	2025	ROM	MLWE	BPR			✓		✓	✓		✓

[1] Generic: Follows a generic design without relying on a specific primitive.
[2] Quantum-Safe: Security analysis in a quantum or in the standard model, regardless of the primitives.
[3] (R): Denotes the (M)LWR variant of (M)LWE as in Learning with Rounding.
[4] Provides a variant based on the commutative supersingular DH (CSSDH) assumption.
[5] Provides an instantiation based on the GA-DDH assumption.
* Insecure (broken) construction.
† Insecure instantiation using SIDH (cf. Sec. 3.1).

2 PAKE Definition and Security

At its core, a PAKE protocol involves two parties sharing a password π, who intend to establish a session key for secure communication over an unauthenticated channel. In other words, a PAKE assigns the communicating parties with a session key if and only if they use the same password. Based on [Gjö24], we can formally define a PAKE as follows.

Definition 1 (Password Authenticated Key Exchange [Gjö24])**.** A PAKE is a cryptographic protocol, $\mathsf{PAKE} = (\mathcal{I}, \mathcal{R}, \mathcal{K}, \mathcal{D}, AD)$ that consists of a session key space $\mathcal{K}$, a password dictionary $\mathcal{D}$, associated data AD, and is executed between two algorithms, an Initiator $\mathcal{I}$ and a Receiver $\mathcal{R}$ defined as follows:

- $\mathcal{I}$: Takes as input the associated data $ad \in AD$ and a password $\pi \in \mathcal{D}$. It sends and receives messages and outputs a session key $K \in \mathcal{K}$ or $\perp$ signaling rejection.
- $\mathcal{R}$: Takes as input the associated data $ad \in AD$ and a password $\pi \in \mathcal{D}$. It sends and receives messages and outputs a session key $K \in \mathcal{K}$ or $\perp$ signaling rejection.

2.1 PAKE Security

Fundamentally, PAKE security asks the question whether a low entropy password suffices to protect a key exchange (KEX) [Jar22]. Nevertheless, practical security involves other aspects such as implementation correctness, safe parameter sets, password choices, and compositions within larger security protocols and mechanisms.

Provable Security. According to Jablon [Jab96], PAKE security can be achieved if the small password size space is multiplied by the size of the key space of the asymmetric primitive. It follows that a PAKE should have the following security properties.

- Provide session key security (indistinguishability) against attacks targeting a transcript of a protocol execution (i.e. a session) [Jar22].
- Resist *offline dictionary attacks* passively targeting the password and a transcript of a protocol execution [Jab96, Jar22].
- Survive *online dictionary attacks* actively targeting the password [Jab96].
- Prevent *Man-in-the-Middle* (MitM) attacks actively targeting the KEX [Jab96].
- Provide explicit mutual authentication (MA), or at least implicit MA [Jar22].
- Provide *Perfect Forward Secrecy* (PFS), or at least weak PFS (FS) [Jar22].

Online Dictionary Attacks. According to [Jar22], and similar to KEX, the security of the session key in PAKEs is defined in terms of indistinguishability in the real-or-random model; that is, for passive (eavesdropping) adversaries. Intuitively, this property implies that the passive security of a PAKE must not be worse than that of the underlying KEX in the sense that it does not leak information regarding the final key. However, KEX are usually used in authenticated settings (e.g. in TLS). Hence, PAKE adversarial models assume authentication using a password with min-entropy t, such that the success probability of password guessing is upper bounded by 2^{-t}, which prevents active MitM adversaries from successfully impersonating any of the honest parties. This so-called online dictionary attack must be an adversary's best chance at deceiving an honest party to agree on a session key with them.

Offline Dictionary Attacks. Since online attacks are relatively easy to deal with through limiting the number of password entry trials, the security of a PAKE protocol heavily relies on its resistance to offline dictionary attacks. Therefore, even if honest parties reuse the same password across multiple sessions, an attacker with substantial resources and enough time must not be able to determine the correct password.

Example Toy PAKE. We consider a simple (naive) implementation of a simple EKE protocol to explain the baseline security of PAKE (Fig. 3). Alice and Bob share a low-entropy password pw and want to establish a high-entropy session key K. Since the exchanged public keys are directly encrypted with the password, the security of the protocol relies entirely on the password entropy. Thus, an attacker may intercept the exchanged messages and guess many passwords in order to compute many $(g^a)^b$. Later, Alice and Bob eventually exchange payload messages encrypted with K (ignoring explicit authentication upon successful key agreement). The attacker can then trial decrypt using the computed possible final keys, and determine the correct password by evaluating the meaningfulness of a decrypted message.

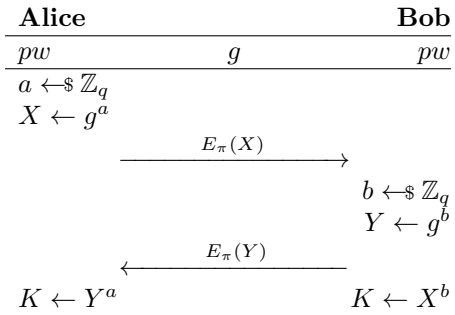


Figure 3: Toy Example: Insecure implementation of DH-EKE.

(Perfect) Forward Secrecy. Additionally, PAKEs requires protecting past executions, should the password get leaked or compromised in the following sessions. This requirement is referred to as *Perfect Forward Secrecy* (PFS). Restricting PFS to protect only passively observed previous executions is called weak PFS. Leaking the ephemeral secrets (or internal state) of honest parties is referred to as *adaptive compromise* (corruption) and withstanding such attacks is called adaptive security, which implies PFS. That is, since the password is part of an honest user's state [Jar22]. However, the concrete security that can be achieved depends on the proof framework in which the formal analysis is conducted (cf. Sec. 2.3).

Practical Security. Even if a PAKE is cryptographically secure, other practical and human-related aspects may jeopardize its effective security. For example, consider users who choose very weak passwords (e.g., 1234567890 or *password*). Obviously, all cryptographic security guarantees become meaningless if an attacker can guess the correct password so easily. Therefore, issues related to user compromise through social engineering and phishing are only partially modeled in PAKE security (cf. Sec. 2.3 for modeling password distributions).

According to [HvO22], PAKE-based applications need to provide a trusted interface and a trusted channel for both entering and sharing the password, respectively. Another

important aspect is how PAKEs are actually implemented (i.e., instantiated) and according to which specifications. That is, some idealized assumptions in proofs cannot be instantiated in practice, or implementation aspects are missing in theoretical constructions (cf. [HvO22, Sec. 6]). Last but not least, PAKEs can also be susceptible to Denial-of-Service (DoS), downgrade, and authentication bypass attacks [VR20] (Dragonfly in WPA3 and EAP), as well as Side-Channel-Analysis (SCA) and Fault Injection (FI) [ASWZ24].

Post-Quantum (In-)Security. Primarily, quantum computers (QC) threaten the asymmetric schemes used in classical PAKEs. This applies both to sessions executed in the presence of cryptographically relevant QCs (CRQC), or to past ones, where an attacker may leverage their ability to break a key agreement (e.g., DH) and therefore nullify the hardness assumptions utilized in formal analysis (e.g., CDH or DDH). To illustrate this threat, we consider a passive adversary with access to a (simplified) PAKE session transcript (cf. Fig. 3). The attacker can mount an offline password dictionary attack on the first message (cf. Sec. 9), compute all possible public keys (since all possible passwords can be obtained through a prepared brute-force dictionary attack), and then simply compute d-log for each one afterwards. By doing so, the attacker can compute the same session key as the honest parties since they can compute the initiator's secret key. This enables the attacker to either impersonate one party or compromise any following encrypted communication between honest users. In other words, QRQCs will not only endanger active future PAKE security, but also pose the risk of the so-called Harvest-Now-Decrypt-Later (HNDL) attacks.

2.2 Balanced and Augmented PAKEs

PAKEs that fulfill the provable security properties mentioned above are referred to as *Balanced* or symmetric PAKEs [HvO22]. The symmetry lies within the fact that two honest parties share the same password in its raw form. This usually applies to a so-called user-user or client-client setting, where no server is involved that holds many passwords from different clients. However, in the client-server setting, the passwords are threatened by server compromise, even if users keep them safe. PAKEs that protect against server compromise and pre-computation attacks are thus referred to as *Augmented* or asymmetric (aPAKE) and strong asymmetric (saPAKE) respectively [HvO22], where the value of the pre-shared password is stored only as a one-way transformation on the server.

Def. 1 does not reflect the asymmetry [Gjö24]. Hence, an additional algorithm is required that takes a password and associated data as input and outputs a password representation and some client-related data. Then, the initiator can use these parameters as input and the responder can take the associated data and the password representation as input [Gjö24]. Also, an aPAKE can be extended to three-party setting, where two users run a PAKE with a "mediating" server, with whom they each share a password, but not with themselves. This type can be balanced or augmented, depending on how the passwords are stored.

2.3 Adversarial (Threat) Models and Frameworks

The security of PAKEs is commonly shown in one of the following frameworks, which model cryptographic protocols and adversaries w.r.t. their capabilities.

1) *Bellare-Pointcheval-Rogaway* (BPR) model [BPR00] and extended eBPR [AFP05].

2) *Universal Composability* (UC) model [Can01, CHK+05].

Other frameworks less used in the context of PAKEs are the *Boyko-MacKenzie-Patel* (BMP) model [BMP00], *Dolev-Yao* (DY) [DY83], *Canetti-Krawczyk* (CK) [CK01] and *Benhamouda-Blazy-Ducas-Quach* (BBDQ) [BBDQ18] models (cf. Tab. 1).

BPR. The BPR model defines a game in which an adversary $\mathcal{A}$ interacts with honest parties running multiple instances of the protocol. The PAKE provides so-called oracles that implement the protocol on behalf of the parties, and the interaction is carried out via a set of *queries* that an adversary may submit throughout a series of game changes. The adversary's goal is to break the protocol through distinguishing real session keys from random ones. At the end of $\mathcal{A}$'s interaction with the protocol, they test a chosen session by outputing a test bit b, which determines if they receive the real session key or a random one from the protocol oracle. $\mathcal{A}$'s advantage in succeeding is defined as $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PAKE}} = (\Pr[b' = b] - \frac{1}{2})$, bounding $\mathcal{A}$'s chances at being better than random guessing. 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.

Definition 2 (PAKE Security in the BPR Model [Jar22])**.** A PAKE protocol is secure in the Bellare-Pointcheval-Rogaway (BPR) model if, for all password dictionaries $\mathcal{D}$ and all efficient algorithms (adversaries) $\mathcal{A}$,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PAKE}}(1^{\kappa}) \leq \frac{q_s}{|\mathcal{D}|} + \mathsf{negl}(1^{\kappa})$$

where q_s is the number of sessions that $\mathcal{A}$ actively interacts with, and negl is a negligible function for some security parameter κ.

UC. The UC model defines two distinct executions (modeling both honest and malicious adversarial behavior) called the *real-world* and the *ideal-world*. It also defines *ideal* functionalities emulating a protocol and an environment acting as a distinguisher through observing honest parties and adversaries and interacting with them. The environment outputs a bit at the end of an execution, indicating whether it was interacting with the real protocol or its ideal emulation. This modular approach allows using a UC secure PAKE as an ideal subroutine (blackbox) within other cryptographic compositions [Jar22]. However, UC also includes changes in behavior through steps (i.e., game hops) the goal of which is to (gradually) move the execution from the *real-world* to the *ideal-world*. In each game, the protocol is changed so that an adversary's advantage in breaking the original protocol remains statistically negligible. These changes are usually defined on the basis of the protocol interface (i.e., exchanged messages) and the ideal functionalities. Follow-up works proposed variants of the original UC PAKE functionality such as Implicit-Only UC [DHP+18], Relaxed UC [ABB+20, HTTY24], and Subversion-Resilient UC [LWC+25].

Definition 3 (UC Security [Tue13])**.** Let $\mathcal{P}$ be a real protocol and $\mathcal{F}$ be an ideal protocol. $\mathcal{P}$ realizes $\mathcal{F}$ ($\mathcal{P} \leq \mathcal{F}$) only if there exists a simulator $\mathcal{S} \in \mathsf{Sim}^{\mathcal{P}}(\mathcal{F})$ (an ideal adversary) s.t. $\mathcal{E}|\mathcal{P} \equiv \mathcal{E}|\mathcal{S}|\mathcal{F}$ for every environment in $\mathcal{E} \in \mathsf{Env}(\mathcal{P})$.

UC vs. BPR. Generally, both models define PAKE security based on two key principles. First, an adversary can only make one online password guess in an attacked session. Second, the final PAKE output keys are independent unless a correct password guess was made [Xu26a]. However, there are subtle differences in adversarial capabilities, and consequently in the degree of security captured within each model.

UC definitions are deemed stronger than game-based ones, since the former ensures security under arbitrary compositions with (or within) other secure constructions. Additionally, UC allows for arbitrary password correlations, and thus captures real-world scenarios such as password reuse and related or mistyped passwords. Evidently, all classical PAKEs that made it to the second round of the previously mentioned IETF standardization were analyzed in the UC framework [KX25].

UC security was shown to imply BPR security for PAKE, but not the other way around [Xu26a]. Presumably, due to one or both of the following differences. First, UC requires the simulator to always be able to extract adversarial password guesses, whereas BPR does not (even though many BPR proofs actually do perform explicit password extraction). Second, the UC simulator must resume the simulation even in the presence of a successful attack (i.e., a correct password guess). However, the BPR definition declares that an adversary wins the security game simply by guessing the correct password, regardless of the final result of the execution [KX25]. Hence, not all BPR protocols can necessarily be proven in UC. We note that almost all current PQC PAKEs are analyzed in BPR. Apparently, BPR has regained popularity partially because it is believed that security proofs in BPR are more likely to be liftable to quantum idealized models (e.g., simulating in the QROM). That being said, we were not able to identify any formal proof of this proclaimed gap of simulating quantum adversaries in the UC framework.

3 Post-Quantum Cryptography

The term classical cryptography is used in reference to public key crypto-systems based on the hardness assumptions from the integer factorization and discrete logarithm problems. The most prominent classical asymmetric algorithms and schemes are the *Rivest-Shamir-Adleman* (RSA) crypto-system [RSA78], the renowned *Diffie-Hellman* (DH) key agreement scheme [DH76], as well as variants using *Elliptic Curve Cryptography* such as *Elliptic Curve Diffie-Hellman* (ECDH) and the *EC Digital Signature Algorithm* (ECDSA) [JMV01]. However, these public-key encryption (PKE) and digital signature schemes are expected to be broken by QCs utilizing Grover's [Gro96] and Shor's [Sho97] algorithms in the near future [Ber09, CCJ+16, KNW18]. Hence, PQC became of interest even before the start of the NIST PQC standardization process [CCJ+16] in 2016. Unlike classical cryptography, PQC is based on mathematical problems that presumably cannot be efficiently solved using QCs, nor classical ones for that matter [Ber09, BL17].

3.1 Simple Primitives

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

SIDH and CSIDH. Generally speaking, an isogeny is a surjective morphism of elliptic curves defined over an algebraically closed field that induces a group homomorphism between these curves (e.g., $\varphi : E_1 \to E_2$) [Smi18]. One may imagine that they resemble a structure-preserving map between ECs yielding a specific mathematical relation (non-constant morphism) [MW25]. SIs and Commutative SIs (CSI) are more or less special cases of isogenies defined over supersingular ECs. Supersingular means that there is only one point on a curve (its identity element) over a field with positive characteristic p that is eliminated through multiplication by p. SIs and CSIs rely on the difficulty of identifying isogenies between these supersingular ECs because finding such mappings is considered a hard problem, as there can be infinitely many of them [Smi18].

Their attractiveness in asymmetric cryptography comes from the fact that they enable the construction of key agreement schemes that are very similar to the classical DH. They are therefore also used to construct computational and decisional problems. However, we refrain from an elaborate explanation because of complexity beyond the scope of this paper. That being said, we refer to [Smi18, MW25] for further reading. Note that *SIKE* [ACC+19],

which builds on *SIDH*, was a NIST round four candidate until its withdrawal due to sudden breakdown[4], while *CSIDH* [CLM+18] is still deemed secure.

Definition 4 (Problems on Isogenies [HPA21])**.** Given two elliptic curves E, E_A the SIDH and CSIDH problems are defined as follows:

- **SIDH:** Given the isogeny value $\varphi : E \to E_A$ on $E[\ell^e]$, find φ.
- **CSIDH:** Find an efficiently computable isogeny $\varphi \in \mathcal{C}\ell(\mathcal{O})$ s.t. $E_A = \varphi \cdot E$, where $\mathcal{C}\ell(\mathcal{O})$ is the class group of $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

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 [RHCB22], 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) and uniform equations, after applying a small amount of noise (called errors), as found in the Regev plain LWE crypto-system [Reg10]. LWE can also be defined on integral lattices, where the lattice basis is a matrix of integers (e.g., modular lattices). Moreover, a base can be replaced by an irreducible polynomial and thus 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]. MLWE was defined by Brakerski et al. [BGV14] and was further studied by Langlois and Stehlé [LS15]. It takes the construction idea of RLWE a step further to replace integers by a ring of algebraic integers of a number field.

The most notable LWE schemes are the recent NIST standard *ML-KEM (CRYSTALS-Kyber)* [BDK+18] (MLWE), the NIST round three candidates *FrodoKEM* [BCD+16] (LWE) and *SABER* [DKRV18] (MLWR), and the Ding et al. RLWE key exchange scheme [DXL12] (was not a NIST submission).

Definition 5 (Problems on LWE [HPA21])**.** Given a monic polynomial $\varphi \in \mathbb{Z}[x]$ and an integer modulus q, let $\mathcal{R} = \mathbb{Z}_q[x]/(\varphi(x))$ be a ring, and $\mathbf{A} \in \mathcal{R}^{n \times m}$ be uniformly random. Further, let $\mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, where $\mathbf{s} \in \mathcal{R}^n$ and $\mathbf{e} \in \mathcal{R}^m$ are sampled from secret and error distribution respectively. The **decision** LWE problem is to distinguish $(\mathbf{A}, \mathbf{b})$ from uniform, and **search** LWE is to find $\mathbf{s}$.

3.2 Complex (Supporting) Primitives

Mainly, *Smooth Projective Hash Functions* (SPHF), *Oblivious Pseudo Random Functions* (OPRF), and *Non-Interactive Zero-Knowledge* proofs (NIZK) serve as supporting components in PAKEs. That is, either in establishing a trusted setup or in realizing commitment schemes w.r.t. users and public keys. For instance, one of the earliest PQC PAKEs leveraging such building blocks is the LWE PAKE by Katz and Vaikuntanathan [KV09], which adapts classical *KOY-GL* PAKEs (Katz, Ostrovsky, and Yung [KOY01], and Gennaro and Lindell [GL03]), however using *Approximate* SPHs (ASPH) from LWE (cf. Sec. 6.1). An example of the usage of OPRF in PAKEs is the augmented *OPAQUE* protocol [JKX18], which was implemented using an isogeny-based OPRF in [HHM+24] (no formal proof provided). Last but not least, NIZKs have also appeared in classical PAKEs such as

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

J-PAKE [HR10], which employs the Schnorr protocol [Sch91]. Nevertheless, there have been no attempts at realizing J-PAKE using PQC primitives or KEMs.

Smooth Projective Hash Functions. Cramer and Shoup introduced SPHFs [CS02] 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 hashing 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. Hence, computing the projection key via hashing a value in the language does not reveal any information about the hash of a random value.

Definition 6 (Projective Hash Function [GL03])**.** The family $(\mathcal{H}, K, X, L, G, S, \alpha)$ is a projective hash family if for all $k \in K$ and $x \in L$, it holds that the value of $H_k(x)$ is uniquely determined by $\alpha(k)$ and x.

Definition 7 (Smooth Projective Hash Function [GL03])**.** Let $(\mathcal{H}, K, X, L, G, S, \alpha)$ be a projective hash family. Then let $V(x, \alpha(k), H_k(x))$ be the following random variable: choose $x \in X \setminus L$ according to $D(X \setminus L)$, $k \in_R K$ and output $(x, \alpha(k), H_k(x))$. Similarly, define $V(x, \alpha(k), g)$ as follows: choose $x \in X \setminus L$ according to $D(X \setminus L)$, $k \in_R K$, $g \in_R G$ and output $(x, \alpha(k), g)$. Then the projective hash family $(\mathcal{H}, K, X, L, G, S, \alpha)$ is smooth if

$$\Big\{V(x, \alpha(k), H_k(x))\Big\}_{n\in\mathsf{N}} \overset{s}{\equiv} \Big\{V(x, \alpha(k), g)\Big\}_{n\in\mathsf{N}}$$

Definition 8 (Approximate Smooth Projective Hash Function [KV09])**.** An approximate smooth projective hash function is a collection of keyed functions $H_k : X \to \{0,1\}^n{}_{k\in K}$, along with a projection function $\alpha : K \times (\{0,1\}^* \times \mathcal{C}) \to S$, satisfying notions of (approximate) correctness and smoothness:

- **Approximate correctness:** If $x = (\text{label}, C, m) \in \overline{L}$, then the value of $H_k(x)$ is approximately determined by $\alpha(k, \text{label}, C)$ and x.
- **Smoothness:** If $x \in X \setminus L$ then the value of $H_k(x)$ is statistically close to uniform given $\alpha(k, label, C)$ and x (assuming k was chosen uniformly in K).

Oblivious Pseudo-Random Functions. The first *Pseudo-Random Function* (PRF) 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. For example, *OPAQUE* [JKX18] is an saPAKE that utilizes the verifiable hash DH-OPRF proven secure by Jarecki et al. [JKK14, JKKX16], and OneTwoPAKE [KMM+26] realizes an saPAKE based on the Dodis-Yampolskiy (DY) OPRF [DY05]. The majority of practical (efficient) OPRF instantiations rely on classical hardness assumptions [CHL22], with the exception of ones based on symmetric primitives

and garbled circuits. Nevertheless, many recent works provide OPRF constructions based on PQC such as oblivious transder (OT) and NIZKs [FOO23, BDFH25], Legendre PRFs [SHB25, KCM25, YBH+25], lattices [ADDS21, ADDG24] and isogenies [BKW20, Bas23, HHM+24, dSGP24, BM25]. We refer to [HHM+24] for a comprehensive and thorough overview on PQC OPRFs[5]. Currently, there are no PQC PAKE constructions utilizing quantum-secure OPRFs that provide a full formal proof.

Definition 9 (Pseudorandom Function [HHM+24])**.** A Pseudorandom Function is a deterministic and polynomial time function $F : \{0,1\}^k \times \{0,1\}^x \to \{0,1\}^n$ such that there is no probabilistic polynomial-time algorithm to distinguish any output N from a randomly chosen element from $\{0,1\}^n$.

Definition 10 (Oblivious Pseudorandom Function [HHM+24])**.** An Oblivious Pseudorandom Function is a protocol between two parties. One holds the secret key K and the other holds their secret input X. The OPRF privately realizes the joint computation outputting $F(K, X)$ for a PRF F to the party holding X, and nothing to the party holding K.

Non-Interactive Zero-Knowledge Proofs. *Zero-Knowledge Proofs* (ZKP), first introduced by Goldwasser et al. [GMR85], are cryptographic constructions that enable one party (a prover) to exhibit the truth of a statement to another party (a verifier), without revealing any information other than the validity of that statement. However, since the statement is public, the secret part of the proof (the witness) can assess the validity of the statement without being actually revealed itself. In other words, ZKPs allow the sharing of a proof of holding a specific secret without sharing the actual secret. While interactive proofs require multiple rounds of interaction, NIZKs, 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. In PAKEs, this property or secret could be the long-lived key (e.g., the password) or an honest public key pair. Benhamouda et al. [BBDQ18] provide an overview of lattice-based hash proof systems and discuss how to construct 3, 2, and 1-round PAKEs using ASPHs and NIZKs.

Definition 11 (Non-Interactive Zero-Knowledge Proof System [WW14])**.** A Non-Interactive Zero-Knowledge Proof System for language L consists of a pair of probabilistic algorithms (P, V), where the following conditions hold:

- **Completeness:** $\forall x \in L$ and polynomial $p(.)$,

$$Pr[V(x, CRS, P(x, CRS)) = 1] \geq 1 - \frac{1}{p(|x|)}$$

  i.e., an honest prover and verifier should cause the verifier to accept with overwhelming probability if the statement is true.

- **Soundness:** $\forall x \notin L$, any P', and polynomial $p(.)$,

$$Pr[V(x, CRS, P'(x, R)) = 1] < 1 - \frac{1}{p(|x|)}$$

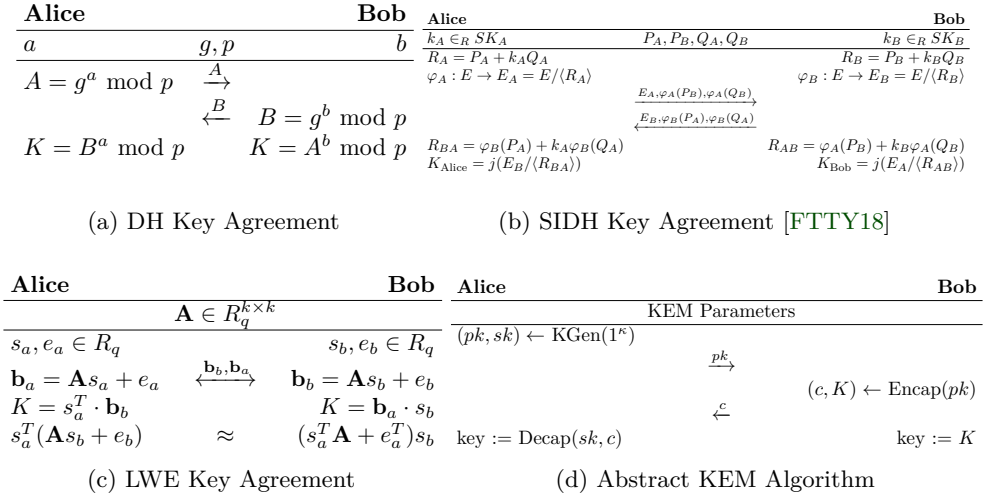
  i.e., a malicious provers can only trick an honest verifier that a statement is true with negligible probability.

- **Zero knowledge:** $\forall x \in L$, there is a probabilistic algorithm M (a simulator) s.t.,

$$\{(x, CRS \in \{0,1\}^{p(|x|)}, P(x, CRS))\} \approx \{M(x)_{x \in L}\}$$

  i.e., an efficient simulator should be able to generate the transcript of the protocol without knowledge regarding the truth of the statement, and the computation performed by the simulator is indistinguishable from the real algorithm.

[5] https://heimberger.xyz/oprfs.html provides a regularly updated list of PQ friendly OPRFs.



(a) DH Key Agreement

(b) SIDH Key Agreement [FTTY18]

(c) LWE Key Agreement

(d) Abstract KEM Algorithm

Figure 4: High level description of key exchange and encapsulation algorithms.

4 Key Exchange and Key Encapsulation

Ever since the seminal publication of the renowned DH key agreement [DH76], many new directions in modern cryptography have indeed emerged, resulting in a plethora of terms and definitions concerned with key exchange and its multiple variants (e.g., key establishment, agreement, transport, or distribution)[6]. Here, we refer to key agreement schemes with the understanding that KEX relies on direct (white-box) hardness assumptions. In contrast, a KEM utilizes black-box assumptions regardless of the underlying hard problem used in concrete instantiations. For ease of exposition, we first unify the terminology used to describe the schemes, their components, and their security properties.

4.1 PKE, KEX and KEM Syntax

While a Public-Key Encryption (PKE) system is not (per se) a key agreement protocol, it may be utilized within a PAKE (e.g., KV-LWE PAKE [KV09]) and is also found inside KEMs. KEX and KEM serve the sole purpose of key establishment and consist of three steps. These are *Key Generation*, *Message Exchange*, and *Key Derivation* [Boy22].

Key Exchange (KEX). Exchanged key material is combined from (ephemeral) public keys to create a final key. This method is found in DH (Fig. 4a), SIDH (Fig. 4b), and LWE (Fig. 4c). Isogenies and lattices follows a concept similar to DH, where both parties provide key shares through their public keys, which are (mathematically) combined to obtain the same final key [HPA21]. However, this relation is not very straightforward on isogenies due to some extra information required to agree on a common curve [Smi18, HPA21]. Furthermore, (noisy) lattices do not produce identical final keys in non-interactive settings, as the error terms produce noisy secrets that differ in their lower bits [HPA21]. Thus, they require a so-called (interactive) reconciliation step through signaling (or hinting), where Bob tells Alice how to round the noisy secrets [HPA21]. However, reconciliation can be eliminated in LWE by relying on a rounding technique instead. This can be realized in the form of a Non-Interactive Key Agreement (NIKE) or an abstract KEM algorithm. NIKE proceeds similarly to KEX without reconciliation and can thus be viewed as a KEX.

[6] We refer to the definitions of Boyd [Boy22] for further reading.

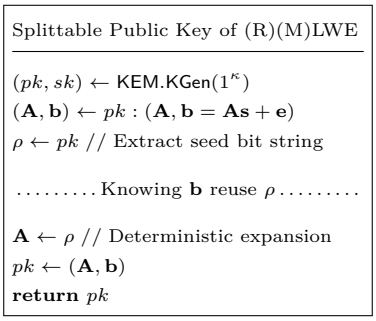


Figure 5: Splitting the public key of an (R)(M)LWE KEM to obtain the fixed-length seed ρ appended (or prepended) to the public key pk [AAA+26].

Key Encapsulation Mechanism (KEM). KEM acts as a key transport scheme, where the parties do not proceed symmetrically. Regardless of the primitive used, a receiver 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 decapsulates the session key from the ciphertext using their secret key (Fig. 4d). For instance, lattice-based KEMs utilize PKEs that allow a KEM to produce identical final keys with a negligible error margin (decryption failures [HPA21]) without reconciliation [Pei14].

Splittable KEM. Arriaga et al. [ABJS24, ABJ25b], followed by Alnahawi et al. [AAA+26] introduced the idea of lattice-based KEMs with splittable public keys (*splittable KEM*[7]). Recall the decision LWE problem (Def. 5, Sec. 3). Essentially, the component $\mathbf{b}$ is the LWE public key (also RLWE and MLWE), and $\mathbf{A}$ is the public matrix representation of the lattice. Here (Fig. 5), $\mathbf{A}$ is deterministically expanded from a fixed-length random seed (i.e. a bitstring), which is appended (or prepended) to $\mathbf{b}$ to form a complete public key representation, and an encapsualtor expands this seed to obtain the same $\mathbf{A}$. Although this concept was applied to reduce the size of the public key, it allowed the idea of splitting the public key to prove rather useful in PAKE design (cf. Sec. 6).

Lossy (L)PKE. Lossy Public-Key Encryption (LPKE) and its extractable variant (eLPKE) were introduced by Lyu et al. [LLH24b]. Here, key generation takes as input a label that binds a key pair to the label, which is used in encryption and decryption to determine whether a key matches its real label (via a trapdoor function). Both LPKE and eLPKE can be used to obtain a KEM through applying the FO transform (cf. Sec. 6).

4.2 KEX and KEM Semantics

A PKE simply defines a shared key, a plaintext, and a ciphertext, which is very straightforward. However, both KEX and KEM define their own semantics to explain the exchanged messages and the resulting output. In Tab. 2, we illustrate the differences based on the definitions in the literature, ignoring 3-party settings. While the output is (obviously) always the final key, the initiator and responder messages are not necessarily semantically equivalent. Conventionally, DH-like KEX consists of two messages that represent the respective public keys of the key agreement participants (cf. Fig. 4). For a KEM, we have the public (encapsulating) key, the (decapsulation) ciphertext, and the encapsulated (or decapsulated) final key [Boy22]. McQuoid et al. [MRR20] use the terms *First Message* and *Second Message* w.r.t. any key agreement (KA) and generalize both KEX and KEM into

[7] Not to be confused with Split-KEM as in hybrid key encapsulation [BBF+19].

one concept regardless of the mechanisms used to establish the final key. We use the terms public key and ciphertext with the understanding that they imply the generalized terms.

Table 2: Components of KEX and KEM Schemes.

Role	(DH-Like or PQC) KEX [Boy22]	(PQC) KEM [Boy22]	Generalized KA [MRR20]	Unified Term
Initiator / Alice / $\mathcal{P}$	Public Key	Public Key Splittable PK [ABJS24]	First Message	Public Key
Receiver / Bob / $\mathcal{P}'$	Public Key	Ciphertext	Second Message	Ciphertext
Both	Final Key / Shared Key	KEM Key	KA Key	Final Key

4.3 Security Properties

Now, we attempt to define the meaning of the (abstract) security properties related to the previously introduced components. However, we note that the exact definitions and security guarantees of cryptographic notions differ widely across the non-PAKE literature. In this work, they serve solely to understand their usage in PAKE designs[8]. Hence, we shall consistently refer to a final key with the implication that it could also be a plaintext message in the context of PKE schemes. We collect the varying notions from recent generic PAKE proposals in Tab. 3, provide a mapping between them, and unify some where applicable. For ease of exposition, we only cite the paper that used a notion for the first time and refer to Sec. 7.1 for a detailed overview in generic PAKEs[9].

Table 3: Notions used in KEX, KEM, Splittable KEM and KA. * indicates that the concrete property depends on the underlying hardness assumption (e.g., LWE), and † indicates properties applicable only to splittable KEM.

Aspect	KEX	(Splittable) KEM	Generalized KA	Unified Notion
Final Key	IND	IND [SGJK22] OW [ABJS24]	KA Security [MRR20]	IND OW
Public Key	*	Uniformity [SGJK22] Fuzinness [BCP+23] UNI-PK [ABJS24]† SPLIT-PKU [AAA+26]†	First Pseudo-Randomness [JRX25] KA Pseudo-Randomness [MRR20] KA Random Message [SGJK22]	PKU [AHHR24]
Ciphertext	*	-	Pseudo-Random Non-Malleability [JRX25]	SPR [Xag22]
Public Key / Ciphertext	*	ANO [SGJK22] A-SEC [AAA+26]†	Second Pseudo-Randomness [JRX25] Strong Random Response [MRR20] KA Random Message [SGJK22]	(w)ANO [GMP22]
Ciphertext / Final Key	*	A-CFR [AAA+26]†	Robustness [MRR20] Collision Resistance [JRX25]	SROB [GMP22] SCFR [GMP22]
All	-	-	Strong Pseudo-Randomness [JRX25]	SPR/SMT [Xag22]

Final Key Security. The *Indistinguishability* (IND) notion expresses the core security of the established key. Basically, it indicates the infeasibility for an attacker to distinguish real (honestly computed) final keys from random ones [Jar22]. The *One-Wayness* (OW) property plays a similar role and denotes the irreversibility of a ciphertext, i.e., the infeasibility of recovering the final key from its corresponding ciphertext [ABJS24].

Public Key Security. Public key *Uniformity* (PKU), *Fuzziness*, and *First Pseudo-Randomness* (PR) all denote the indistinguishability of real generated public keys from uniform ones, i.e., honestly generated public keys have an equal probability distribution to

[8]We refer to [AM22] for more details on the formal definitions of security notions in asymmetric cryptography and public-key encryption.

[9]We explicitly acknowledge the immensely valuable insights gained from [JRX25] in writing this section and refer to [Xu26b] for newly introduced properties not covered in our overview.

random ones from the same public key space [BCP+23, AHHR24, JRX25]. For splittable KEMs, similar notions were introduced as *Splittable and Pseudo-Uniform Public Keys* (UNI-PK) [ABJS24] and *Splittable Public Key Uniformity* (SPLIT-PKU) [AAA+26].

Ciphertext Security. *Non-malleability* (NM) is the infeasibility to construct a meaningfully related ciphertext to a known one and its corresponding final key [DDN91, JRX25]. *Strong Pseudo Randomness* (SPR) denotes the indistinguishability of the pair ciphertext / final key from a random one, i.e., it is infeasible to distinguish between such pairs knowing the public key used to compute the real one [Xag22, CDM24]. *Smoothness* (SMT) means the ability to provide pseudo-random ciphertexts without using a public key.

Ciphertext / Final Key Relation. *Strong Collision Freeness* (SCFR) and *Collision Resistance* (CR) denote the binding property of a ciphertext / secret key relationship, i.e., a ciphertext does not decapsulate the same final key under two distinct secret keys. Similarly, *Strong Robustness* (ROB) means that a ciphertext does not successfully decapsulate two valid final keys under two distinct secret keys [GMP22, CDM24]. For splittable KEMs, a variant called *A-Part-Collision-Freeness* (A-CFR) was introduced in [AAA+26].

Public Key / Ciphertext Relation. *Anonymity* (ANO) expresses the privacy of public keys, i.e., the difficulty of utilizing information from a ciphertext and a final key to reveal which public key was used to compute them [GMP22, MX23a, CDM24]. Some works refer to the anonymity of a ciphertext, and not of a public key (e.g., [BCP+23, ABJS24, JRX25]) and it was shown that ANO is implied through SPR [Xag22, MX23a]. Similarly, weak *Anonymity* (wANO) and *Second Pseudo-Randomness* define the same property but without involving the final key. According to [JRX25], *Strong Pseudo-Randomness* is a stronger form of anonymity as a combination of SPR and SMT. For splittable KEMs, a variant called *A-Part-Secrecy* (A-SEC) was introduced in [AAA+26].

5 Idealized Models

5.1 Standard Model

The standard model enables proofs to be based solely on complexity (hardness) assumptions. That is, the attacker's capabilities are only limited by their computational power, i.e., an arbitrary polynomial-time machine [CGH04]. However, idealized models are often used, as they allow for additional complexity-theoretic hardness assumptions [Bla06].

5.2 Random Oracle Model

A *Random Oracle* (RO) is an ideal primitive that models a random hash function that responds to each query (a given fixed-length input value) with a corresponding random output [BR93]. Additionally, a RO keeps a record of all queries placed and responds with the same value for a previously queried input. Basically, ROM is present in almost all PAKEs, since its usage is required to model hash and key derivation functions. Almost all ROM-based PAKEs are analyzed in classical settings (cf. Tab. 1), and only two constructions provide security proofs in the *Quantum* ROM (QROM).

Definition 12 (Random Oracle)**.** *RO* is a function f that maps elements over the function space $\{0,1\}^* \to \{0,1\}^{poly(1^\kappa)}$, where:

$$\textbf{if } f(x) \neq \perp \textbf{ return } f(x) \textbf{ else return } y \leftarrow\$ \{0,1\}^{poly(1^\kappa)}$$

QROM. Boneh et al. [BDF+11] proposed the QROM and addressed issues of the classical ROM in the presence of adversaries with quantum capabilities, who can evaluate hash functions in superposition [BCMR19].

Definition 13 (Quantum(-Accessible) Random Oracle [BDF+11])**.** Evaluating a RO in superposition by submitting a quantum state s.t. $|\varphi\rangle = \sum \alpha_x |x\rangle$ to an oracle $\mathcal{O}$ an receiving the evaluated state $\sum \alpha_x |\mathcal{O}(x)\rangle$ is called a quantum-accessible random oracle.

Many ROM techniques were not directly applicable in the QROM according to the fundamental concepts of quantum information; such as adaptive programmability, extractability, and rewinding [BDF+11, BCMR19]. Thus, it was not clear whether the classical proof techniques in ROM [BDF+11, BCMR19] also hold in QROM. Nevertheless, recent work clarified that many ROM constructions can also be shown to be secure in QROM [Zha19, YZ21, DFMS22, HM24].

In the context of formal analysis of PAKE, the most important QROM proof techniques relate to collision bounds on search queries and extracting inputs to hash functions [LLH24b, HHKR25]. For instance, and considering the *no-cloning principle*, it was not possible to keep record of query transcripts (also called the *recording barrier*), which renders searching for a certain query input to a RO infeasible [DFMS22]. However, *Compressed Oracles* (CO) [Zha19] overcame the recording barrier by allowing efficient on-the-fly simulation of random oracles, similar to classical simulations [Zha19]. This technique was shown to enable proofs for applications involving pre-image search and collision finding [Zha19]. The *Extractable* CO (eCO) [DFMS22] takes this idea a step further by giving a form of observable QROM, where one can check for queries that satisfy some function [HHKR25]. Hence, the eCO allows the extraction of RO based commitments and simulating routines involving RO queries (e.g., decapsulation in an FO-KEM or hash functions in PAKEs [DFMS22, HM24, HHKR25]).

5.3 Ideal Cipher Model

An *Ideal Cipher* (IC) models block ciphers 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. An IC provides oracle access for forward queries on encryption, and for backward queries on decryption as well, all of which are recorded. That being said, IC in PAKEs is mostly found in the design class C1 (cf. Tab. 1), most of which also address the absence of a *Quantum* IC model.

Definition 14 (Ideal Cipher)**.** *IC* is an invertible permutation function $\mathcal{C} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$, where each key $k \in \{0,1\}^\kappa$ defines a unique and independent random permutation $\mathcal{C}_k = \mathcal{C}(k,.)$ on $\{0,1\}^n$.

QIC. Many works in the literature [AR17, HY18, CMSZ19, SS19, Unr21, Ros21, ABPS24, Unr23, MMW25, ACMT25, CHL+25] 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 of Unruh [Unr23] builds on the idea of COs and takes a step forward in modeling keyed invertible permutations (i.e., IC) in quantum settings by introducing the *Compressed Permutation Oracle* (CPO). However, 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]. A recent breakthrough in realizing QIC is the *Permutation Superposition Oracle* (PSO) introduced by Majenz et al. [MMW25]. The PSO can be considered similar to Zhandry's CO, but additionally allowing to (approximately) determine queried inputs

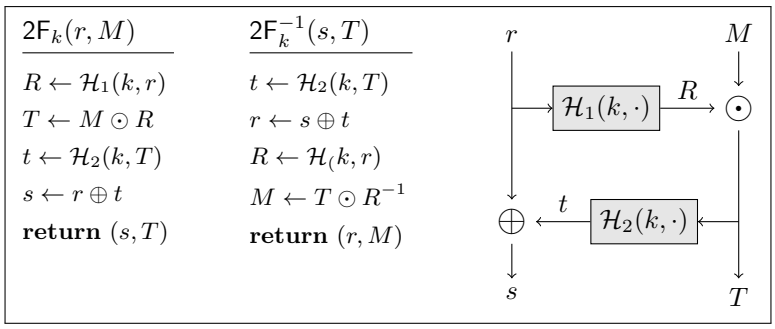


Figure 6: The 2-Round Feistel (2F), where $\oplus$ is an XOR operation on bit strings, $\odot$ is a group operation in G, and $(.)^{-1}$ computes the inverse of a group element [ABJ25a].

to permutation based on the output [MMW25]. Nevertheless, these works aid only in bounding collisions on search queries, yet do not enable programming and extraction.

Definition 15 (Quantum(-Accessible) Random Permutation [MMW25])**.** For a group of elements $[N] = \{1, 2, ..., N\}$, the permutation (bijection) group on N elements S_N, a permutation $\pi \in S_N$, and the corresponding unitary permutation operator $U^\pi|x, y\rangle = |x, y \oplus \pi(x)\rangle : \forall x, y \in [N]$ for the quantum space $\mathbb{C}^N \otimes \mathbb{C}^N$, a Quantum-Accessible Random Permutation consists of query access to U^π and to $U^{-\pi}$, for a permutation $\pi \in S_N$ chosen uniformly at random.

5.4 Programmable-Once Public Function

McQuoid et al. [MRR20] introduced an adaptation of an Oblivious Programmable Pseudo-Random Function (OPPRF) [KMP+17] called the Programmable-Once Public Function (POPF). An initiator can generate a value based on a keyed function and make the evaluation of the function public for any input in a non-interactive manner. Unlike IC, which is defined over invertible and equal input/output domains, POPF defines the forward direction to be randomized on (possibly) larger output domains than the input (as in RO-modeled hash functions). This means that a simulator can program outputs for any (RO) query in the forward direction and make use of these queries again in the reverse direction. Hence, POPF serves as an alternative to an IC on keyed (mostly random) permutations relying on hash functions [ABJ25a].

McQuoid et al. [MRR20] showed that a 2-Fesitel (2F) construction realizes POPF in the ROM. Here, 2F has two wires (Fig. 6). The first holds uniform randomness, and the second holds a group element. The randomness is used to obtain a fresh group element using a hash function (H2G), which is then combined with the element on the second wire to compute a new (shifted) element. Hashing the new element together with a key and combining the output with the randomness again results in a keyed permutation of the original element. Therefore, 2F realizes POPF in the ROM.

Definition 16 (Programmable-Once Public Function [ABJ25a])**.** For a keyed function family $F_\varphi : X \to Y$ a Programmable-Once Public Function (POPF) is a pair of efficient algorithms $\mathsf{Program}$ and Eval s.t.:

- $\mathsf{Program}$ is a randomized algorithm s.t. $\varphi \leftarrow\$ \mathsf{Program}(\mathsf{x}, \mathsf{y})$ fixes a POPF isntance F_φ, a random function constrained by $F_\varphi(x) = y$.
- Eval is a deterministic algorithm that evaluates the POPF instance on arbitrary inputs, i.e., $\mathsf{Eval}(\varphi, x) = F_\varphi(x)$.

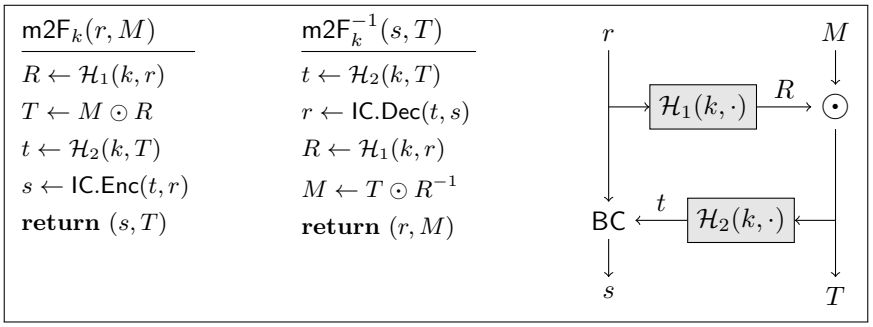


Figure 7: The modified 2-Round Fiestel (m2F), where $\odot$ is a group operation in G, and $(.)^{-1}$ is an inverse in G [SGJK22, ABJS24].

Definition 17 (2-Round Feistel Network [ABJ25a])**.** A 2-Feistel (2F) is constructed from: 1. A hash function $\mathcal{H}_1$ whose output space is an algebraic group G, 2. a hash function $\mathcal{H}_2$ whose output space is a set N of fixed-length bit strings used in sampling the randomness r, 3. and two efficiently computable functions $\mathsf{2F}_k : N \times G \to N \times G$ and its inverses $\mathsf{2F}_k^{-1}$.

Januzelli et al. [JRX25] identified some flaws in the original construction, mainly w.r.t. malleability, and reformulated POPF in a UC PAKE, which was again reformulated by Arriaga et al. [ABJ25a] in UC as well (cf. Sec. 6 and Sec. 10).

5.5 Half Ideal Cipher

Dos Santos et al. [SGJK22] also argued that POPF is susceptible to malleability (actually before [JRX25] and [ABJ25a]) and therefore introduced a relaxation of the IC model called *Half Ideal Cipher* (HIC), which is realized using a modified 2-Feistel construction (m2F) (Fig. 7). Compared to 2F, the left wire in m2F combines the hashed output of the right wire with the randomness using a block cipher. Hence, m2F extends the IC domain to bit strings using both a block cipher and a pair of hash functions. This also inspired the work of Arriaga et al. [ABJS24], where a compact m2F is used on uniform bit strings.

Definition 18 (Modified 2-Round Feistel Construction [ABJS24])**.** A modified 2-round Feistel (m2f) is constructed from: 1. A block cipher denoted by the tuple $(\mathsf{IC.Enc}, \mathsf{IC.Dec})$, with key space $\mathcal{K}$ and input/output space N, 2. a hash function $\mathcal{H}_1$ with output space G, 3. a hash function $\mathcal{H}_2$, with output space $\mathcal{K}$, 4. and two efficiently computable functions $\mathsf{m2F}_k : N \times G \to N \times G$ and its inverse $\mathsf{m2F}_k^{-1}$ (cf. Sec. 6.3 Fig.7).

5.6 Common Reference String

The *Common Reference String* (CRS) was introduced by Blum et al. [BFM88] to realize NIZKs by providing a shared string accessible to and trusted by all protocol parties. Usually, a CRS is drawn from a pre-defined uniform distribution 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, a pre-shared public key of the protocol initiator is used as a CRS in a trusted setup (with a prior registration phase). Most CRS PQC PAKEs imply security in the standard model and make use of SPHFs and ASPHs or NIZKs such as [KV09, ZY17, BBDQ18, AAK19], and belong to the design class C3.

5.7 RO or CRS

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 between multiple set-ups, 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 such a 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.

6 PQC PAKEs

We categorize the collected PAKEs according to their underlying PQC assumptions, and whether balanced or augmented within their respective design classes (cf. Tab. 1).

6.1 Lattice PAKEs

C2: PAK-Style with (R)LWE and Variants in the ROM

Ding et al. [DAL+17] proposed the first RLWE PAKE based on Ding's RLWE KEX and reconciliation mechanism [DXL12]. The PAKE is inspired by MacKenzie's classical PAK and PPK [Mac02] and follows a similar security analysis. The variant following PAK is a 3-pass (i.e., 3 messages) and provides explicit MA. The other variant following PPK is a 2-flow and provides implicit MA. The authors also introduced the *Pairing with Errors* (PWE) and the decisional (D)PWE problems relying mainly on the H2G method for 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. The RLWE-PAK design witnessed numerous adaptations and modifications in follow-up works in the literature [GDL+18, JZ17, GDLL17, JGH+20, RGW23, BSIA23, SA23, YZYW25].

- *Observation 1:* Ding's RLWE KEX strongly resembles the classic DH, which enables a high level of flexibility in its usage in almost any PAKE design.
- *Observation 2:* Ding's RLWE KEX requires signaling for key reconciliation, which is a critical attack surface (e.g., offline dictionary and impersonation attacks, and key re-use attacks), if the signal is sent in plaintext [DCQ22, CL24].
- *Observation 3:* The modified public key message distribution is directly dependent of the used password in RLWE-PAK (RLWE-PPK) and adaptations [TSJL21], which may lead to successful offline guessing attacks.

C3 Adaptations

RLWE-PAK (also RLWE-PPK) was also adapted to the *3-party setting* (i.e., client-server-client) in [XHCC17, CAK18], and to *augmented 3-party* in [LZJY19, GSG+23, YSG25] with prior registration. Another adaptation is to the *anonymous-augmented* setting, focusing on user registration, login, and password updates with key reuse [FHZ+19, DBK21, IB21, RSM+23, CKS23, KGKD23, DJRD23, DRD+23, DKBY24, SM25, JD25].

- *Observation 4:* Many of the augmented RLWE PAKEs are vulnerable to signal-leakage, key-reuse, and pre-computation attacks [DCQ22, CKS23, DRD+23, CL24].

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

Figure 8: The RLWE-PAK protocol [Din17] with the key reconciliation trough signaling using the functions **Cha** and $\mathbf{Mod}_2$ as originally defined in [DXL12].

- *Observation 5:* Using reconciliation without signaling mitigates the risk of signal-leakage attacks but may induce decryption failures [LZJY19, GSG+23].
- *Observation 6:* RLWE-PAK and adaptations do not provide proofs in the QROM, although all of these PAKEs rely mainly on a RO-modeled H2G function.

Technical Description. The 3-pass RLWE-PAK protocol (Fig. 8) resembles the original DH-based PAK protocol [Mac02]. The client initiates the protocol by randomly sampling s_C, e_C (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. Then it 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 $w = \mathrm{Cha}(k_S) \in \{0,1\}^n$ and $\sigma = \mathrm{Mod}_2(k_S, w)$. The server sends μ, w and k to the client, who in turn checks if $\mu \in R_q$, aborting if the check fails. Otherwise, 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 $sk_C = sk_S = H_4(C, S, m, \mu, \sigma, \gamma')$.

C3: KOY-GL-Style with (A)SPHFs and NIZKs (mostly with CRS)

The 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 *Gennaro-Lindell* (GL) 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 an ASPH. The protocol parties exchange CCA secure ciphertexts, from which they attempt to compute ASPH values and execute a reconciliation to derive a final key. The reconciliation first extracts a bit from the noisy ASPH value and then applies an *Error-Correcting Code* (ECC) to finish the reconciliation. This PAKE inspired several CRS adaptations using different variations of

Client		**Server**
w	CRS: pk	w
$(\mathrm{VK}, \mathrm{SK}) \leftarrow \mathcal{K}(1^\kappa)$		
$r \leftarrow \{0,1\}^*$		
label := VK|Client|Server		
$C := \mathrm{Enc}_{pk}(\mathrm{label}, w; r)$	$\xrightarrow{\text{Client}\|\text{VK}\|C}$	$r' \leftarrow \{0,1\}^*$
		label$'$ $:= \varepsilon$
		$C' := \mathrm{Enc}_{pk}(\mathrm{label}', w; r')$
		label := VK|Client|Server
label$'$ $:= \varepsilon$	$\xleftarrow{\text{Server}\|C'\|s'}$	$k' \leftarrow K;\ s' := \alpha(k', \mathrm{label}, C)$
$k \leftarrow K;\ s := \alpha(k, \mathrm{label}', C')$		
$\mathrm{tk} := \mathrm{H}_k(\mathrm{label}', C', w) \oplus \mathrm{H}_{k'}(\mathrm{label}, C, w)$		
$\mathrm{sk} \leftarrow \{0,1\}^\ell; c := \mathrm{ECC}(\mathrm{sk})$		
$\Delta := \mathrm{tk} \oplus c$		
$\sigma \leftarrow \mathrm{Sign}_{\mathrm{SK}}(C\|C'\|s'\|s\|\Delta)$	$\xrightarrow{s\|\Delta\|\sigma}$	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 9: The Katz and Vaikuntanathan KV-LWE-PAKE protocol [KV09]

LWE crypto-systems, (A)SPHFs [ZY17, AAK19, LW18, LW22, YGS+20, LWM22, CQY24] and in *augmented* and 3-party settings [TLZ+21, LWM22, XG22, SGD23].

- *Observation 1:* Most KOY-GL-style PAKEs provide security proofs in the CRS model, and do not require additional idealized assumptions.
- *Observation 2:* Additional supporting cryptographic building blocks (e.g., SPHFs and ASPHs) infer more design complexity and practical inefficiency.
- *Observation 3:* PQC primitives are used in their PKE form and the resulting PAKE is tightly coupled to the PKE routines and its IND-CPA or IND-CCA security.

Technical Description. The 3-pass KV-LWE-PAKE (Fig. 9) employs an SPHF similar to the KOY-PAKE [KOY01]. 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 $sk := \mathbf{ECC}^{-1}(tk' \oplus \Delta)$.

6.2 Isogeny PAKEs

C1: EKE-Style

Terada and Yoneyama [TY19] proposed the only EKE-style PAKE based on (C)SIDH. The authors refer to their constructions as SIDH-EKE and CSIDH-EKE respectively.

C2: PAK-Style

Taraskin et al. [TSJL21] proposed a PAK-similar PAKE based on SIDH and group actions.

- *Observation 1:* Isogeny EKE and isogeny PAK follow the blueprint of their classical predecessors. Therefore, we refer the reader to Fig. 11 and Fig. 8, respectively, for equally applicable high level diagram illustrations.
- *Observation 2:* Evidently, SIDH and SIKE based PAKEs are not secure due to the irreparable break of SIDH and SIKE.
- *Observation 3:* Isogeny EKE is vulnerable to possible MitM and offline dictionary attacks, due to the distinguishability of valid isogeny public keys from invalid ones upon decrypting them with a wrong password [AJK+20].
- *Observation 4:* The modified public key message distribution depends on the password [TSJL21], which may lead to successful offline guessing attacks.

C3: SPEKE-Style

Abdalla et al. [AEK+22a] build on the idea of H2G from the classical SPEKE protocol [Jab96], however, with a CRS. 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 to compute the so-called quadratic twist, which implies the same hardness assumptions as in CSIDH. The CRS is used 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. Peng et al. [PPY+24] proposed R-GA-PAKE, an improvement to X-GA-PAKE using the shuffle algorithm to reduce the number of group actions required in an execution.

Technical Description. The DH-based SPEKE protocol [HS14] hashes the password into a group generator using a function f. The GA-PAKE (Fig. 10) 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 uses 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 assigned 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 as an 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.

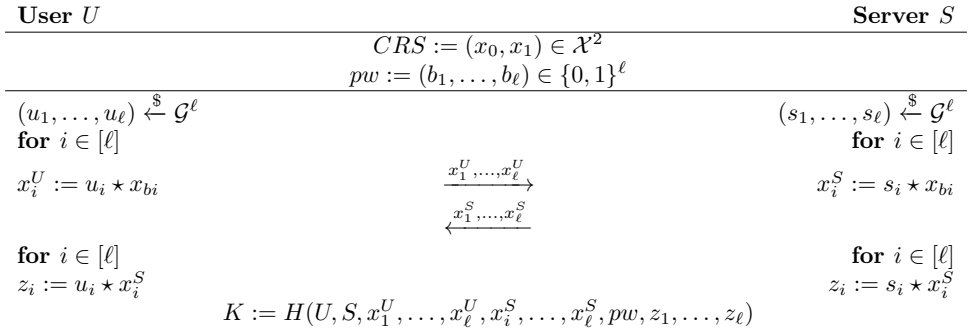


Figure 10: The GA-PAKE protocol with $\star$ denoting a commutative group action [AEK+22b].

6.3 Generic PAKEs

A recent publication by Januzelli, Roy and Xu [JRX25] called *"under What Conditions Is Encrypted Key Exchange Actually Secure?"* extensively analyzed the security of many of the following (O)EKE-style PAKEs, which we highly recommend for further reading.

C1: EKE-Style with IC

Beguinet et al. [BCP+23] proposed the first construction to generically transform a black-box KEM into a PAKE, 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 in the ROM and IC model. While CAKE encrypts both the public key and the ciphertext, the ciphertext is authenticated with a key confirmation tag in OCAKE, and hence "O" as in "one encryption". Following Beguinet et al., Pan and Zeng [PZ23] and Alnahawi et al. [AHHR24] presented further security analysis for CAKE and OCAKE with tighter bounds, respectively, and identified flaws w.r.t. multi-user security notions and the anonymity of the underlying KEM. Hövelmanns et al. revisited the formal analysis of OCAKE in [HHKR25] and extended the proof to a quantum setting with concrete bounds in the QROM. The authors also provide a construction for a (theoretical) simulator, which could be used to program a QIC in a proof should a QIC be realized in the future. Januzelli et al. [JRX25] identified two flaws in the (O)CAKE analysis of [BCP+23]. The first is a subtle miscalculation in a proof step reduction. However, the second is more complex and indicates an overlooked property needed to meet the proposed security (cf. Sec.10).

- *Observation 1:* KEM-based PAKEs, especially (O)EKE-style, appear to be of greater interest, as they enable instantiations with any KEMs, including (standardized) NIST PQC KEMs, that satisfy certain properties utilizing black-box reductions. However, some subtle details were overlooked in initial proposals [JRX25].
- *Observation 2:* KEM black-box reductions are very useful, but need to be programmed carefully to achieve sound simulation-based proofs [JRX25, HHKR25]. However, aspects related to the inner workings of PQC KEMs (e.g., FO and explicit vs. implicit rejection) are not, or cannot be captured in black-box PAKE constructions, and may lead to unavoidable impossibilities [HHKR25].
- *Observation 3:* (O)CAKE is yet to be shown fully quantum-safe due to the lack of the QIC model. Considering the difficulty of (re)programming in the QROM, it is

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

Figure 11: The CAKE protocol [BCP+23].

unclear if a formal analysis in UC can be achieved [MX23b, LLH24a]. However, the recording barrier in the QROM was shown to be adequately manageable with tight results, at least in the BPR model [HHKR25].

Technical Description. CAKE relies on two pairs of ICs, denoted by (E_1, D_1) and (E_2, D_2), which maintain the original DH-EKE design [BPR00]. 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 **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.

C1: EKE-Style with HIC

Dos Santos et al. [SGJ23] proposed a similar generic PAKE in ROM, however, utilizing HIC with m2F, as opposed to the IC used in CAKE. Their HIC-EKE (also HIC-KEM) also relies on abstract KEM security properties, but mainly addresses the lack of QIC and issues with the unconditional uniformity of KEM public keys. Building on the idea of HIC of Dos Santos et al. [SGJ23], Arriaga et al. [ABJS24] proposed the Compact Half-Ideal Cipher (CHIC) protocol. The authors utilize said m2F construction in a white-box manner and use the matrix expansion seed from the public key as randomness. Their main contribution is a compact m2F and bandwidth-minimal KEM-to-PAKE compiler, where they also establish security requirements for generic KEM PAKEs. Further, Arriaga et al. [AMO+26] combined the m2F-based HIC with the classical Password Authenticated Public Key Encryption (PAPKE) protocol presenting PAPKE-HIC. This extension follows a similar design and security rationale as CHIC, however requiring additional KEM properties for secure instantiations from PQC PKEs and KEMs.

- *Observation 4:* KEMs with structured public keys (e.g., ML-KEM) do not satisfy statistical public key uniformity, and are thus vulnerable to detecting invalid keys upon decrypting with a wrong password [SGJ23, ABJS24, AAA+26, ABJ25a].
- *Observation 5:* Reductions from IND-CPA might not be sufficient for tight security proofs in generic PAKE constructions [ABJS24, ABJ25a].
- *Observation 6:* The IC can be applied to PQC when instantiated with domain extenders or for uniform bitstrings over domains with suitable size [SGJ23, ABJS24].

C1: EKE-Style without IC

Although McQuoid et al. [MRR20] did not provide a concrete PQC instantiation, they introduced a generalization of EKE using POPF instantiated as 2F called sPAKE. sPAKE does not rely on an IC and can also accommodate PQC KEMs with certain properties. To encrypt a public key, a password-derived key is used to hash the public key into an algebraic group, and thus shifting its value within the the same group. Since 2F can also be queried in the reverse direction, it enables programming in simulation-based proofs. Januzelli et al. [JRX25] fixed a MitM vulnerability in the said POPF and provided a comprehensive analysis on the UC security of EKE-style PAKEs, especially with respect to the security properties required from the underlying KEM and the flaws in previous proofs. Based also on 2F, Arriaga et al. [ABJ25a] introduced NoIC-PAKE and addressed issues regarding modular vs. monolithic proof techniques and provided a detailed analysis for POPF-based UC PAKE. The authors specified KEM security properties similar to their previous CHIC construction but did not instantiate the PAKE with a concrete KEM. Nevertheless, Vos et al. [VJW+25b] showed how a variant of NoIC called OQUAKE can be instantiated using ML-KEM, where the 2F is applied to an obfuscated public key instead of a group element. Thus, the undefined NoIC group operation is implemented as an XOR of a uniform bitstring with a password derived randomness of the same length.

- *Observation 7:* Many proposals avoid the IC model. It is believed that lifting proofs to the QROM is easier than to the QIC. Also, it is still not known how to directly instantiate an IC over larger domains, which is the case for PQC keys and ciphertexts.
- *Observation 8:* Although abstract KEM security properties are well studied, many details were initially overlooked in PAKE formal analysis [JRX25], some of which may render a PAKE partially or entirely insecure.
- *Observation 9:* In addition to key security (IND or OW), (O)CAKE requires KEMs with public key uniformity and public key/ciphertext anonymity (cf. Sec. 7.1).
- *Observation 10:* Collision resistance for OCAKE, and (strong) pseudo-randomness of ciphertexts for both variants were overlooked in almost all proposals [JRX25]. However, it is argued that including the password along with the PAKE transcript in a final KDF removes the need for collision resistance [ABJ25a, VJW+25b, Xu26b].
- *Observation 11:* According to Xu [Xu26b][10], excluding certain values from the RO input in the second protocol message yields sixteen variants of NoIC, each of which requires certain KEM properties to obtain sound UC proofs (cf. [Xu26b, Tab. 3-4]). The key takeaway is that variants not hashing everything at the end require specific KEM properties w.r.t. its components and the relation between them.
- *Observation 12:* Some works start from KEMs while others from KAs, which makes a direct comparison of the same design rather difficult (cf. Sec. 4).
- *Observation 13:* Programmability can be achieved without an IC but needs careful handling to prevent guessing attacks on malleable messages [ABJ25a, JRX25].

C1: Semi-Generic EKE-Style without IC

Inspired by the idea of splittable KEMs, Alnahawi et al. [AAA+26] proposed a new approach to construct a secure PAKE without IC called NICE-PAKE. This PAKE relies on a RO-modeled hash function used to extend the password to the same length as the

[10] Xu [Xu26b] extensively analyzed the required KEM properties for the OEKE-2F construction (aka NoIC [ABJ25a]) focusing and the RO-modeled tag in the second protocol message.

uniform string part of the public key (the seed used to sample a lattice basis) in LWE, RLWE, and MLWE KEMs. The authors also use similar KEM properties and introduce new notions for LWE KEMs with splittable public keys. Building on the same idea, but using it the other way around, Arriaga et al. [ABJ25b] address issues related to timing attacks on the seed expansion routine in lattice KEMs (e.g., ML-KEM rejection sampling used in the matrix expansion). The authors present a solution to prevent such attacks and call it the ML-KEM-to-PAKE compiler, which is a modification of their previously discussed NoIC-PAKE protocol. The protocol dubbed TEMPO splits the public key as in NICE-PAKE, but instead of hiding the seed, it encrypts the **b**-part using 2F and sends the seed in the clear. We note that Arriaga et al. [ABJ25b] also presented two constant-time algorithms to protect seed expansion, but they are not directly related to PAKE design.

- *Observation 14:* Additional assumptions from primitives (e.g., LWE) can be acquired, but may require parameter changes to remedy decreased security or complete breaks [AAA+26], which may lead to additional computational costs.
- *Observation 15:* Exploring non-standard usage of KEMs with abstract properties may enable new PAKE designs with reasonable trade-offs [AAA+26, ABJ25b].
- *Observation 16:* Splittable KEMs from lattices are becoming of interest in generic PAKE design, and seem to offer more flexibility and also avert multiple side effects that accompany PQC KEM usage.
- *Observation 17:* Timing attacks (i.e., implementation security) is often overlooked in new PAKE constructions [ABJ25b].

C3: Semi-Generic with CRS (No Specific Style)

Lyu et al. [LLH24b] proposed the first UC PAKEs in the QROM, with three passes and MA in the CRS model. Their PAKEs use one CCA PKE and one CCA KEM simultaneously, where the former is used to provide a static public key modeled as a CRS. Lossy Public Key Encryption (LPKE) is utilized to enable password extraction based on the label in the ROM. For the QROM construction, the extractable LPKE (eLPKE) variant is used, with additional hash functions as PRFs. The protocol flow is similar to CAKE, where the first message is a public key and the second is a ciphertext. However, the public key is never encrypted. Instead, a password-derived label is used to extract password guesses. Also, the second message contains two ciphertexts, one of which is computed using the static public key. In both variants, a standard explicitly rejecting KEM FO is used to lift the PKE security from IND-CPA to IND-CCA in a white-box manner. Remarkably, the authors avoid online QROM extraction for adversarial password guesses from hash functions by explicitly using the bare password as a public key label in the QROM variant. Thus, the UC simulator can still extract such guesses and proceed accordingly.

- *Observation 18:* QROM collision query bounds can be obtained from the Oneway-to-Hiding (O2H) lemma for RO-modeled elements [LLH24b, HHKR25].
- *Observation 19:* Online QROM extraction is also possible to a certain extent, where a simulator is able to determine the input randomness to a RO query. [LLH24b].
- *Observation 20:* UC simulation in the QROM is doable if the simulator can extract password guesses consistently [LLH24b].

6.4 PAKE Combiners and Compilers

Usually, a PAKE is a standalone protocol that provides complete functionality (depending on the use case). However, it can also be composed into more complex constructions such

as a hybrid PAKE or a (strong) asymmetric PAKE. We only introduce recent progress on such constructions obtained from PQC PAKEs, and we refer to the respective work for further reading, as these specific types of PAKEs are out of the scope of our paper.

6.4.1 Hybrid PAKE Combiners

Hybrid schemes utilize two (or more) functionally equivalent schemes to provide security guarantees that hold as long as at least one of the schemes used remains secure [ABK27]. In light of the increasing interest in hybrids, this concept has recently begun to appear in PAKEs as well. Hesse and Rosenberg [HR25] and Lyu and Liu [LL25] (almost simultaneously) proposed two black-box methods to realize hybrid PAKEs in UC. These are generic recipes based on parallel and sequential (or serial) combiners, where two PAKEs with certain properties are executed in parallel or one after the other.

Vos et al. [VJW+25b] provided a concrete instantiation in UC building on a variant of the sequential combiner in [HR25]. The resulting protocol (also appeared as an IETF draft in [VJW25a]), CPaceOQUAKE is a hybrid PAKE obtained from the classical CPace protocol, and the previously mentioned NoIC-PAKE instantiation, OQUAKE. Günther et al. [GRSV25] suggested a different hybrid instantiation method relying on Obfuscated KEMs [GSV24] (OKEM) to realize hybrid IND-CCA security and unconditional public key obfuscation for LWE-based OKEMs, which they utilized to construct a hybrid PAKE secure against adaptive corruption in UC based on CAKE.

Vazirinejad et al. [VHLL26] build upon the parallel composition framework of Lyu and Liu [LL25] and present a UC secure hybrid compiler secure against HNDL attacks. The construction combines the classical J-PAKE protocol with a KEM in modular manner, where the KEM is only used to encapsulate messages computed within the classical PAKE. The resulting protocol is shown to provide session key security and PQ forward secrecy without relying on idealized assumptions or a trusted setup.

6.4.2 aPAKE Compilers (Symmetric to Asymmetric Transformation)

Basically, an aPAKE compiler provides a (generic) recipe to obtain a secure asymmetric PAKE from another secure symmetric PAKE, in order to protect against server compromise attacks. This is done through composition, where the symmetric PAKE is augmented with some additional steps (usually a registration phase and defining behavior for stolen passwords), and hence it is usually analyzed in UC.

The compiler of Gentry et al. [GMR06] is the first one instantiated from quantum-safe primitives (lattices) and signatures. Nearly a decade later, McQuoid and Xu [MX23b] proposed a UC aPAKE compiler based on isogeny group action. Recently, Lyu et al. [LLH24a] also proposed a generic compiler based on KEMs and Authenticated Encryption (AE) and compared their construction to the aforementioned ones. The authors of the hybrid CPaceOQUAKE [VJW+25b] also showed how to obtain the first hybrid aPAKE instantiation using a variant of the black-box compiler in [LLH24a] relying on a relaxed lazy-extraction PAKE. The resulting aPAKE is called CPaceOQUAKE+, and also appeared in the aforementioned IETF draft in [VJW25a]. We refer to [Gu24, VJW+25b] for a more detailed overview of existing aPAKE compilers and their respective methods.

Table 4: Security Properties of KEM-Based Generic PQC PAKEs.

Protocol	K	PK	PK / C	C	C / K
sPAKE [MRR20]	IND-CPA	PKU	wANO-(?)	-	SROB-(?)
(O)CAKE [BCP+23]	IND-CPA	PKU	ANO-CPA	-	-
HIC-EKE (HIC-KEM) [SGJ23]	IND-CPA	PKU	ANO-CCA	-	-
Pan and Zeng (CAKE) [PZ23]	IND-CPA	PKU	ANO-PCA	-	-
Alnahawi et al. (OCAKE) [AHHR24]	IND-CPA	PKU	ANO-PCA	-	-
Januzelli et al. (EKE/CAKE) [JRX25]	IND-(CCA)	PKU	ANO-(CCA)	SPR-1CCA	SPR-1CCA SMT-CCA
Januzelli et al. (OEKE/OCAKE) [JRX25]	IND-(CCA)	PKU	wANO-(CCA)	SPR-1CCA	SCFR-CPA
CHIC [ABJS24]	OW-CPA	PKU	ANO-PCA	-	-
NICE-PAKE [AAA+26]	IND-CCA	PKU	ANO-CCA A-SEC-CCA	-	A-CFR-CCA
NoIC-PAKE [ABJ25a]	OW-CPA	PKU	ANO-PCA	-	-
Hövelmanns et al. (CAKE) [HHKR25]	IND-CPA	PKU	ANO-PCA	-	-
Hövelmanns et al. (OCAKE) [HHKR25]	IND-CPA	PKU	ANO-PCA	-	-
OQUAKE [VJW+25b]	OW-CPA	PKU	ANO-PCA	-	-
TEMPO [ABJ25b]	OW-CPA	PKU	ANO-PCA	-	-
PAPKE-HIC [AMO+26]	IND-CCA	PKU	ANO-CCA	-	SROB-CCA DROB-CCA
OEKE-2F (Hash Everything)[1] [Xu26b]	OW-1PCA	PKU	ANO-1PCA	-	-

[1] Refer to [Xu26b] for the properties required in the other variants.

7 Security and Performance

7.1 Security Overview

The emphasis on abstract notions is found in generic designs, due to the impossibility of involving white-box hardness assumptions in black-box reductions (cf. Sec. 10). Hence, PAKEs built from abstract notions can be viewed as a secure template, which can be instantiated using any KEM that fulfills the utilized properties (cf. Sec. 10). Since IND-CCA implies IND-CPA, which in turn also implies OW; and all NIST PQC KEMs realize IND-CCA, recent works focus more on additional notions.

Tab. 4 offers an overview of the properties found in KEM-based PAKEs and uses the unified notations established in Sec. 4. Values in parentheses indicate properties that we were unable to completely identify in the work in which they appear. Clearly, all constructions require public key uniformity. However, CHIC and NoIC opt for OW-CPA for key security and ANO-PCA for anonymity, the latter of which is also used in the CAKE and OCAKE versions of Pan and Zeng, and Alnahawi et al., respectively. For POPF-EKE, we were unable to identify whether ANO-CPA or ANO-CCA is implied, and hence the question mark. Januzelli suggested additional requirements especially regarding the ciphertext and the final key / ciphertext relationship. Although the authors did not explicitly mention IND-CCA or ANO-CCA, they argued that SPR-CCA and SMT-CCA are required, which automatically implies ANO-CCA and IND-CCA. NICE-PAKE and TEMPO adopt PKU in its splittable form, but NICE-PAKE additionally derives properties specific to splittable KEMs w.r.t. anonymity (A-SEC) and Collision-Freeness (A-CFR).

Tab. 5 and Tab. 6 present an overview of the basic security properties of all surveyed PAKEs. These are number of flows, final key security (IND-), and forward secrecy (FS). Final key security is denoted by OW-CPA, IND-CPA, or IND-CCA, depending on the underlying key agreement scheme. Forward secrecy can either be weak (FS) or perfect (PFS), as no authors state that their constructions do not provide any at all. Mutual authentication is not included, as any PAKE could support explicit MA simply by adding a key confirmation flow at the end. The number of flows indicates how many messages are sent from one protocol participant to another (i.e., one flow equals one message).

Table 5: Security Properties of Balanced PQC PAKE Protocols. One round in a cryptographic protocol indicates one back and forth message exchange between two parties. That is, one round consists of two flows (or passes).

Class	Protocol	Flows	IND-	FS
C1	Terada and Yoneyama ((C)SIDH-EKE) [TY19]†	2	CPA	PFS
	McQuoid et al. (sPAKE) [MRR20]	2	CPA	PFS
	Dos Santos et al. (HIC-EKE / HIC-KEM) [SGJ23]	2	CPA	PFS
	Beguinet et al. (CAKE) [BCP+23]	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]	3	CPA	PFS
	Januzelli et al. (POPF-EKE) [JRX25]	2	CPA	PFS
	Januzelli et al. (POPF-OEKE) [JRX25]	2	CPA	PFS
	Arriaga et al. (CHIC) [ABJS24]	2	OW-CPA	PFS
	Alnahawi et al. (NICE-PAKE) [AAA+26]	2	CCA	PFS
	Arriaga et al. (NoIC-PAKE) [ABJ25a]	2	OW-CPA	PFS
	Hövelmanns et al. (OCAKE) [HHKR25]	3	CPA	PFS
	Vos et al. (OQUAKE) [VJW+25b]	2	OW-CPA	PFS
	Arriaga et al. (TEMPO) [ABJ25b]	2	OW-CPA	PFS
	Arriaga et al. (PAPKE-HIC) [AMO+26]	2	CCA	?
	Xu (OEKE-2F) [Xu26b]	2	OW-1PCA	PFS
C2	Zhu, Geng [ZG17]	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+18]	3	CPA	FS
	Gao et al. (RLWE-PPK) [GDL+18]	2	CPA	FS
	Taraskin et al. (SIDH-PAK) [TSJL21]	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] ([RG21])	3	CPA	FS
	Seyhan, Akleylek [SA23]	3	CCA	PFS
	Basu et al. (MLWR-2PAKA) [BSIA23][1]	4	CPA	PFS
	Jana, Dutta (iPAKE) [JD25]	3	CCA	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) [CAK18][2]	5	CPA	FS
	Li, Wang [LW18]	2	CPA / CCA	FS
	Li, Wang [LW22]	2	CCA	FS
	Karbasi et al. (Ring-PAKE) [AAK19]	3	CCA	PFS
	Yin et al. [YGS+20][3]	2	CCA	FS
	Song et al. [SGD23]	2	CPA	?
	Lyu et al. [LLH24b]	3	CCA	?

[1] Number of rounds excluding initialization or registration.
[2] No explicit authentication with the server, only between users.
[3] Applies to both 2PAKE and 3PAKE variants.
† Broken underlying hardness assumption.

7.2 Performance Overview

In Tab. 7 and Tab. 8 we compile information on bit-security, communication cost, and computation cost for 2-party and 3-party PAKEs, respectively. Any values for communication and computation cost given are rounded to three decimal places where appropriate. 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), or a slight variation in the implementation of a one or two different protocols within the same publication.

The communication cost describes the total size of the outgoing messages of a given party and is given in bytes (B), whereas the computation costs are given in milliseconds (ms). We note that some of the original values were converted for ease of exposition. These are indicated as such in both tables.

Table 6: Security Properties of Augmented PQC PAKE Protocols.

Class	Protocol	Flows	IND-	FS
C2	Gao et al. [GDLL17]	2	CPA	FS
C3	Zhu et al. [ZHS14]	5	?	PFS
	Feng et al. [FHZ+19]†[1]	3	CPA	FS
	Liu et al. [LZJY19]	?	CPA	FS
	Dabra et al. (LBA-PAKE) [DBK21]†[1]	3	CPA	FS
	Tang et al. [TLZ+21]	3	CCA	FS
	Li et al. [LWM22][1]	3	CCA	PFS
	Islam, Basu (BP-3PAKA) [IB21]†[1]	4	CPA	PFS
	Xie and Guo [XG22]	?	CPA	?
	Abdalla et al. (Com-GA-PAKE) [AEK+22a]	3	CPA	PFS
	Abdalla et al. (X-GA-PAKE) [AEK+22a]	2	CPA	PFS
	Wang et al. (LB-ID-2PAKA) [WCL+23][1]	2	CCA	PFS
	Rewal et al. [RSM+23]†[1]	4	CPA	FS
	Guo et al. [GSG+23]	2	CCA	FS
	Chaudhary et al. [CKS23]†[1]	4	?	PFS
	Chen et al. (Multi-PAKE) [CQY24]	2/4	CCA	?
	Dabra et al. (SL3PAKE) [DKBY24]†[1]	4	CPA	FS
	Peng et al. (R-GA-PAKE) [PPY+24]	2	CPA	PFS
	Yang et al. (K-PAKE) [YZYW25]	1	CCA	PFS
	Saeid and Mala (APAKE) [SM25]†[1]	2	CPA	FS
	Yang et al. (2-Server-PAKE) [YSG25][1]	4	CPA	FS

[1] Number of rounds excluding initialization or registration.
† Anonymous PAKE.

Generic PAKEs. Only four constructions provided performance estimates. These are isogeny-EKE [TY19], CHIC [ABJS24], Alnahawi et al. [ASWZ24], and PAPKE-HIC [AMO+26]. In general, isogeny PAKEs are slower than lattice ones. However, larger message sizes in lattices induce a higher communication cost. Comparing Kyber-based instantiations of OCAKE and CHIC yields closer results for all parameters, but at first glance it appears that CHIC is evidently faster, whereas PAPKE-HIC is somewhere in between. Nevertheless, this is not a precise statement since OCAKE was tested on a 1.8 GHz i7, CHIC on a 2.3 GHz i5, and PAPKE-HIC on a 2,8 GHz AMD EPYC (ignoring details such as DRAM and cache etc.). Arriaga et al. [AMO+26] also compare their results to PAPKE-IC and Kameleon showing that the HIC variant is clearly more efficient in terms of runtime.

Alnahawi et al. also tested OCAKE with arm Cortex m4 optimized KEMs on an STM32-NUCLEO-L4R5ZI board running at 20 MHz (same setup as the pqm4 project), but their results are not comparable to standard laptop benchmarks. A recent work by Alnahawi et al. [AAB+25] evaluated the feasibility of OCAKE using ML-KEM on NXP micro-controller chips both as initiator and responder (in Tab. 7 only as responder) and compared the results to ECDH.

RLWE-PAK and Adaptations. RLWE-PAK (PPK) have the largest number of adaptations and implementations. Gao et al. [GDL+18] proposed a TLS integration using C++ in the NFLlib library to improve the performance of Ding et al. [DAL+17]. The modification based on asymmetric key consensus by Yang et al. [YGWX19] claimed higher bit security levels and a 12x speedup over [DAL+17] using an optimized implementation in C. Ren et al. [RGW23], and Seyhan and Aklyelek [SA24] also proposed a modification using MLWE and MLWR respectively, claiming an advantage in both bit security and performance, which is true for communication, but untrue for computational cost. Taraskin et al. [TSJL21] instantiated the only PAK-similar isogeny PAKE with parameter sets p434 and p503 and measured its performance based on total clock cycles.

Augmented RLWE-PAK Adaptations. Gao et al. [GDLL17] implemented their SPR adaptation using RLWE in C++ using NFLlib and claim a 3x speed-up compared to the classical SRP for 209 bit security. Feng et al. [FHZ+19], Rewal et al. [RSM+23], Dharminder et al. [DRD+23], Dadsena et al. [DJRD23], Kumar et al. [KGKD23], and Chaudhary et al. [CKS23] showed almost identical results, all based on [DAL+17]. Dabra et al. [DBK21, DKBY24] and Saeidi and Mala [SM25] analyzed a very similar construction, but their results differ drastically from the former group.

Xu et al. [XHCC17] provided an implementation for a 3-party PAKE using parameters similar to NewHope using the LatticeCrypto C library. Although they compare their work to ECDH-PAKE, we question the applicability of the benchmarks, as the total runtime for the PQC variant is only 0.25 ms compared to 53.3 ms using ECDH. Liu et al. [LZJY19] also adapted RLWE-PAK, however, to a 3-party aPAKE using the Peikert reconciliation mechanism, and presented benchmarks for a proof of concept implementation in C. Guo et al. [GSG+23] and Yang et al. [YSG25] built similar PAKEs based on MLWE and the Peikert reconciliation, but they appear to be much faster..

KOY-GL Adaptations. SPHF and ASPH RLWE PAKEs saw fewer adaptations. Li et al. [LWM22] claimed that their construction eliminates costly NIZK operations and provide detailed performance measurements for classical and quantum security parameters. Tang et al. [TLZ+21] (3-party) claimed to reduce the size of ciphertexts and achieve lower computational overhead by using the Fast Fourier Transformation (FFT) over RLWE. Chen et al. [CQY24] presented results for two variants of 2-Server-PAKEs. However, they stated a security parameter $n = 12$, which is not comprehensible, and their total execution times are much slower than other LWE SPHF PAKEs.

8 Real World Use Cases

The most important PAKE applications are device pairing, credential recovery, E2E secure channel establishment [HvO22], and E2E encrypted backups [DFG+23]. Based on the security and performance data collected previously, we conclude that it is extremely difficult to assess the suitability of current PQC PAKEs to real world applications. Still, it is at least possible to evaluate the applicability on the design level.

Device Pairing. PAKE-based device pairing is found in situations where it is not possible to rely on a Public Key Infrastructure (PKI) or a trusted setup. This applies to Wi-Fi connection, small devices (i.e., embedded and IoT), and e-cards equipped with smart chips [ASWZ24]. For example, PACE [BFK09] is used in electronic IDs and eMRTDs (Machine Readable Travel Document) to establish a secure connection with terminals and e-card readers; and Dragonfly [Har08] is used in WPA3 for Wi-Fi connection between an access point and a client [HvO22].

Although several works claim constructions tailored for embedded and IoT devices (e.g., [FHZ+19, DBK21, LWM22, DRD+23, RGW23, RSM+23]), good candidates can mostly be found in generic balanced PAKEs. In other use cases (e.g., smart-gadgets, smart-meters, e-mobility etc.), lightweight PAKEs with a registration phase may also be a valid option. Nevertheless, the low computational power and resource constraints of such small devices inherently enact restrictions on the choice of a suitable PAKE. Embedded and IoT devices are also more prone to SCA and FI, the mitigation of which comes with additional costs in both memory and run time [ASWZ24]

Table 7: Comparison of Bit Security and Performance for 2-Party PAKEs.

Class	PAKE			Security		Computational Cost			Communication Cost		
	Publication	Platform	Variant	Classic	Quantum	Client	Server	Total	Client	Server	Total
Balanced											
C1	Terada and Yoneyama [TY19]	Intel Core i7-6700 @ 3.4GHz Intel Core i5 @ 3.5GHz	SIDH	NIST I	NIST I	-	-	80.6ms	64B	64B	128B
			CSIDH	NIST I	NIST I	-	-	5.0ms	330B	330B	660B
	Beguinet et al. [BCP+23]	-	CAKE	-	102bit	-	-	-	-	-	-
			OCAKE	-	162bit	-	-	-	-	-	-
	Alnahawi et al.[AHHR24]	Intel Core i7-8565U @1.80GHz	Kyber512	NIST I	NIST I	0.331ms	0.275ms	0.570ms	-	-	-
			kyber768	NIST II	NIST II	0.517ms	0.340ms	0.798ms	-	-	-
			Kyber1024	NIST III	NIST III	0.718ms	0.398ms	1.048ms	-	-	-
	Arriaga et al. [ABJS24]	Intel Core i5 @ 2.3GHz	Kyber512	NIST I	NIST I	0.084ms	0.074ms	0.158ms	800B	800B	1,600B
			Kyber768	NIST II	NIST II	0.168ms	0.085ms	0.253ms	1,184B	1,120B	2,304B
			Kyber1024	NIST III	NIST III	0.206ms	0.123ms	0.329ms	1,568B	1,600B	3,168B
	Alnahawi et al. [AAB+25]	NXP SmartMX3 P71D600	Kyber512	NIST I	NIST I	-	-	652ms	-	-	-
			kyber768	NIST II	NIST II	-	-	995ms	-	-	-
			Kyber1024	NIST III	NIST III	-	-	1.406ms	-	-	-
	Arriaga et al. [AMO+26] [1]	AMD EPYC 7543 @ 2,8 GHz	Kyber512	NIST I	NIST I	0.214ms	0.116ms	0.330ms			
			Kyber768	NIST II	NIST II	0.333ms	0.163ms	0.496ms			
			Kyber1024	NIST III	NIST III	0.484ms	0.222ms	0.706ms			
C2	Ding et al. [DAL+17] [2]	Intel Core i7-4790 CPU @ 3.60GHz	RLWE-PAK	-	76bit	2.981251ms	2.884243ms	6.702656ms	4,136B	4,256B	8,392B
			RLWE-PPK	-	76bit	-	-	-	-	-	-
	Gao et al. [GDL+18]	Intel Xeon E5-2687W v2 @ 3.4GHz	RLWE-PAK[3]	≥200bit	82bit	0.176ms	0.175ms	0.351ms	3,904B	4,000B	7,904B
			RLWE-PPK	≥200bit	82bit	0.203ms	0.203ms	0.406ms	3,750B[4]	3,875B[4]	7,625B[4]
	Taraskin et al. [TSJL21]	Intel Core i5-8250U @ 1.6GHz	p434	-	-	-	-	88.75ms[5]	-	-	-
			p503	-	-	-	-	142.5ms[5]	-	-	-
	Yang et al. [YGWX19]	Intel Core i7-8550U @ 1.8GHz	avx2	228bit	206bit	0.081ms[5]	0.076ms[5]	0.157ms[5]	1,864B	2,592B	4,456B
			portable C	228bit	206bit	0.164ms[5]	0.150ms[5]	0.314ms[5]	1,864B	2,592B	4,456B
	Jiang et al. [JGH+20]	Intel Core i7-7700HQ @ 2.80GHz	-	-	-	200ms	710ms	910ms	39,990B	167,090B	207,080B
	Ren et al. [RG21, RGW23][6]	Intel Core i7-4790 CPU @ 3.60GHz	Light	128bit	116bit	89.76ms	93.35ms	183.11ms	928B	1,056B	1,984B
			Recomm.	195bit	177bit	126.71ms	126.05ms	252.76ms	1,344B	1,472B	2,816B
			Paranoid	263bit	239bit	174.97ms	169.52ms	344.49ms	1,760B	1,888B	3,648B
	Seyhan, Akleylek [SA23]	Intel Core i5 @ 2.50 GHz	Lightsaber	-	128bit	104.824ms	60.632ms	165.456ms	896B	1,600B	2,496B
			Saber	-	192bit	172.427ms	97.758ms	270.185ms	1,344B	2,368B	3,712B
			Firesaber	-	256bit	57.756ms	152.232ms	409.988ms	1,760B	3,168B	4,928B
	Basu et al. [BSIA23]	Intel Core i3-4030U @ 1.90-GHz	$p=2^{10}$, $q=2^{13}$	127bit	116bit	-	-	-	-	-	2,816B
			$p=2^{9}$, $q=2^{15}$	140bit	127bit	-	-	-	-	-	2,560B
Augmented											
C2	Gao et al. [GDLL17]	Intel Xeon E5-2687W v2 @ 3.40 GHz	-	209bit	-	0.286ms	0.257ms	0.543ms	3,963B	4,032B	7,995B
C3	Feng et al. [FHZ+19]	Server: Intel Core i7-6700 @ 3.40 GHz Client: Samsung Exynos 4412 @ 1.40 GHz	w/out Precomp.	-	-	0.002307ms	0.000222ms	0.002529ms	641B[7]	577B[7]	1,217B[7]
			w/ Precomp.	-	-	0.001184ms	0.000075ms	0.001259ms	641B[7]	577B[7]	1,217B[7]
	Dabra et al. [DBK21]	Server: Intel Core i5-7200U @ 2.50 GHz Client: CPU @ 1.80 GHz	n=128	-	-	6.501ms	33.298ms	39.799ms	441B	412B	853B
			n=256	-	-	17.372ms	66.094ms	83.466ms	825B	796B	1,621B
			n=512	100bit	75bit	26.271ms	136.442ms	162.713ms	1593B	1,564B	3,157B
	Li et al. [LWM22]	Intel Core i7-8750H @ 2.20 GHz	Classical	-	-	116ms	361ms	477ms	3,291B[7]	4,119B[7]	7,414B[7]
			Quantum	-	-	116ms	473ms	589ms	3,701B[7]	5,040B[7]	8,741B[7]
	Ding et al. [DCQ22]	Server: Intel Xeon E5-2620 @ 3.00 GHz Client: Qualcomm MSM8996 @ 1.50 GHz	n=128	-	-	-	-	-	562B	528B	1,090B
			n=256	-	-	-	-		1,058B	1,024B	2,082B
			n=512	-	-	39.22ms	12.65ms	51.87ms	2,050B	2,016B	4,066B
	Dharminder et al. [DRD+23]	Server: Intel Core i7 @ 3.40 GHz Client: Samsung Exynos 4412 @ 1.40 GHz	-	-	-	0.002297ms	0.000229ms	0.002526ms	-	-	1,224B[7]
	Dadsena et al. [DJRD23]	Server: Intel Core i7 @ 3.40 GHz Client: Samsung Exynos 4412 @ 1.40 GHz	-	-	-	-	-	0.002826ms	-	-	1,216B[7]
	Kumar et al. [KGKD23]	Server: Intel Core i7 @ 3.40 GHz Client: Samsung Exynos 4412 @ 1.40 GHz	-	-	-	0.002297ms	0.000229ms	0.002526ms	-	-	1216B[7]
	Yang et al. [YZYW25]	-	Kyber	-	-	-	-	-	459.5B	459B	918.5B
	Saeidi and Mala [SM25]	Server: Intel Core i7-8700 @ 3.20 GHz Client: Samsung Exynos 9611 @ 1.70/2.30 GHz	n = 512	-	-	25.301527ms	6.300295ms	31.601822ms	-	-	4,428B

[1] Client runtime is the sum of key generation and decryption as presented in original work. Similarly, total runtime is the sum of all operations. The authors also provide benchmarks for FrodoKEM and Classic McEliece in all NIST security levels.

[2] Computational Cost and Communication Cost taken from [RGW23].

[3] Communication Cost taken from [RGW23].

[4] Converted from kilobytes to bytes. May be inaccurate within $\frac{1}{100}kB$.

[5] Measurement converted from cycle counts to milliseconds based on clock frequency provided in the respective paper.

[6] Measurements taken from [RGW23]. Different measurements are provided in [RG21] on an Intel Core i7-4790 @ 3.60 GHz.

[7] Converted from bits to bytes and rounded up to the next highest byte.

Table 8: Comparison of Bit Security and Performance for 3-Party PAKEs.

Class	PAKE			Security		Runtime				Message Sizes			
	Publication	Platform	Implementation	Classic	Quantum	Client$_A$	Client$_B$	Server	Total	Client$_A$	Client$_B$	Server	Total
Balanced													
C3	Xu et al. [XHCC17]	Intel Core i5-3340M @ 2.70 GHz	-	-	-	0.067ms	0.071ms	0.122ms	0.259ms	-	-	-	-
Augmented													
C3	Liu et al. [LZJY19]	Intel Core i7-4770K @ 3.50 GHz	-	-	-	3.267ms	4.155ms	2.195ms	9.617ms	-	-	-	-
	Tang et al. [TLZ+21]	Intel Core i5-1135g7 @ 2.40 GHz	n=32	-	-	2.27ms	0.38ms	20.52ms	23.17ms	-	-	-	7,000B[2]
			n=64	-	-	4.44ms	0.63ms	63.1ms	68.17ms	-	-	-	13,000B[2]
			n=128	-	-	10.38ms	1.07ms	353.49ms	364.91ms	-	-	-	24,000B[2]
			n=256	-	-	24.31ms	3.39ms	3,373.06ms	3,400.76ms	-	-	-	48,000B[2]
			n=512	-	-	82.11ms	4.62ms	45,802.87ms	45,889.6ms	-	-	-	79,000B[2]
	Islam, Basu [IB21]	Server: Intel Core i7-6700 @ 3.40 GHz Client: Samsung Exynos 4412 @ 1.40 GHz	-	-	-	-	-	-	-	657B[1]	657B[1]	1,176B	2,489B[1]
	Rewal et al. [RSM+23]	Server: Intel Core i7-6700 @ 3.4 GHz Client: Samsung Exynos 4412 @ 1.40 GHz	-	-	-		-		0.00491ms[3]	-	-	-	2,452B[1]
	Guo et al. [GSG+23]	Intel Core i7-11800H @ 2.30 GHz	-	-	222bit	-	-	-	0.788ms	-	-	-	10,080B
	Chaudhary et al. [CKS23]	Server: Intel Core i7 @ 3.40 GHz Client: Samsung Exynos 4412 @ 1.40 GHz	-	-	-	0.0049ms	-	0.000215ms	0.005214ms	-	-	-	2,404B[1]
	Chen et al. [CQY24]	Intel Core i5-4590 @ 3.30 GHz	t-Multi-PAKE n=12	-	-	-	-	-	103.7ms[4]	-	-	-	13,000B[1]
			nt-Multi-PAKE n=12	-	-	-	-	-	1,037.142ms[4]	-	-	-	719,200B[1]
	Dabra et al. [DKBY24]	Intel Core i5-7200U	n=128	-	-	3.603ms	4.368ms	7.028ms	14.999ms	-	-	-	4,691B[1]
			n=256	-	-	7.024ms	7.494ms	12.153ms	26.671ms	-	-	-	9,197B[1]
			n=512	-	-	15.113ms	16.236ms	26.211ms	57.56ms	-	-	-	18,210B[1]
	Yang et al. [YSG25]	Intel Core i7-10700 @ 2.90 GHz	-	n=256		-	-	-	0.8937ms	-	-	-	9,792B[1]

[1] Converted from bits to bytes and rounded up to the next highest byte.
[2] Converted from kilobytes to bytes. May be inaccurate within a kB.
[3] Converted from nanoseconds to milliseconds.
[4] Converted from seconds to milliseconds.

Credential Recovery. Several commercial IT systems, e.g., Apple iCloud, 1Password manager, ProtonMail, and Blizzard incorporate PAKEs such as the Secure Remote Password protocol (SRP-6a) [Wu98, Wu02] for general account access, user authentication, or credential recovery [HvO22]. Since all these scenarios assume prior registration, an augmented PAKE is required. The only viable replacement candidate so far is they hybrid CPaceOQUAKE+ [VJW+25b]. However, no concrete performance indicators exist for it at the moment.

End-to-End (E2E) Secure Channel. E2E encryption is usually found in applications that can utilize static keys from a connected PKI (e.g., Signal's X3DH). That is, in addition to the ephemeral keys used in a key agreement. Nevertheless, some embedded and IoT applications cannot rely on a PKI. For instance, J-PAKE is used in Thread IoT products, Pale Moon web browser, and Android Smoke Chat; whereas EC-SPEKE is used in Blackberry Messenger (BBM) [HvO22]. Similarly, small devices require PAKEs with light weight implementations and resistance to implementation attacks.

End-to-End (E2E) Encrypted Backups. To our knowledge, the only E2E encrypted backup application relying on a PAKE is 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. Since OPAQUE is an saPAKE, there are no direct replacement candidates, as there are no PQC saPAKEs at the moment. However, CPaceOQUAKE+ [VJW+25b] could be the best next options at the moment.

9 Unexplored Territory and Honorable Mentions

We observe that a few designs are still unrepresented or not fully explored in the PQC realm, which can still be adapted to PQC, and have not yet been addressed in the literature. Such constructions include PAKEs that make use of supporting building blocks that have PQC replacements (e.g., OPRFs and NIZKs), and where the password usage is not dependent on mathematical properties inherent to classical cryptography. Additionally, we mention other quantum-resistant PAKEs that are however not built from PQC primitives or KEMs.

9.1 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 with a formal proof in the literature, the original authors provided two general frameworks to obtain an saPAKE in UC. The first framework is based on an AKE scheme and an OPRF, whereas the second requires an authenticated encryption scheme (AE) and a KEX in addition to the OPRF. Both versions of OPAQUE consist of a registration phase and a login phase, where the OPRF is meant to hide the values associated with the password. 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.

Heimberger et al. [HHM+24] gave an instantiation of a PQC OPAQUE from isogeny-based OPRFs. However, it is drastically inefficient compared to classical instantiations, and no formal proof was provided. In [BDFH25], Beullens et al. presented a secure OPRF from PQ multi-party computation in UC, and suggested that their OPRF can be, composed, or plugged-in an OPAQUE instantiation.

Considering an AKE with unilateral or bilateral authentication can easily be constructed using a PQC KEM (cf. [BDK+18]), and there exist a number of PQ OPRFs, it should be theoretically feasible to realize a PQC variant. Nevertheless, an open question remains in finding a mechanism 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 Hash to Curve (H2C) function to map a password to an EC base generator, it seems intuitive to resort to its adaptation to H2G settings. While this might answer the question of instantiating OPAQUE directly with a PQC primitive, 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 (or similar), which differs 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 basis matrix) to generate a public key. A more suitable solution would be to use the OPRF secret as the deterministic seed that is otherwise usually sampled within the KEM key generation routine. Another approach might be found in using a PQC NIKE, e.g., SWOOSH [GdKQ+24], which enables a white-box key generation routine, while also maintaining the non-interactive characteristics of a KEM.

9.2 J-PAKE-Style with NIZKs

The J-PAKE protocol proposed by Hao and Ryan [HR10] can be considered the first PAKE to make use of 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 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 al. [ABR+21] (sJ-PAKE replaces two NIZK proofs by two exponentiations). Recently, Hao et al. [HBCvO24] 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 PQC instantiations of J-PAKE and similarly of Owl. An open question remains as to finding 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 the said mechanism into black-box routines.

9.3 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, hence the name Threshold PAKE, aka tPAKE [GJK+24]. There already exist many approaches to realize symmetric tPAKEs from (t, n)-MPC protocols as in [Jab01, RG03, 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+24] 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 because the construction in [GJK+24] can be considered a threshold version of OPAQUE, as it relies mainly on a threshold OPRF (tOPRF).

9.4 Decoy, Honey and Oblivious PAKEs

In line with the PAKE designs mentioned above, another approach to reducing the threat of server compromise and credential leakage can be found in using decoy accounts or decoy passwords [ARS24]. Interestingly, this type of PAKEs addresses the issues of password leakage differently 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. [LWL23]. In a very recent publication, Arriaga et al. [ARS24] propose the SweetPAKE and BeePAKE (as in a honey producing buzzing bee) protocols, based on the aforementioned works and comparing their results.

9.5 Symmetric (Fuzzy) PAKEs

This 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 used mainly to rectify the deficiencies 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 an overview of such symmetric Fuzzy PAKE protocols and compares their security both in theory and practice. This overview includes a protocol built from garbled circuits [DHP+18] and two from ECC [DHP+18, BFH+23].

Other Fuzzy PAKEs include the work of Erwig et al. [EHOR20], which relies on OT and robust secret sharing to obtain two asymmetric Fuzzy PAKEs in the UC model. In addition, 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 AKE. They also compare to similar constructions including the previously mentioned PAKEs, and to the works of Wang et al. [WHC+21], Han et al. [HXL+23] (ttPAKE), and Zhang et al. [ZYL+24] (BAKA). Recently, McQuoid et al. [MRX25] presented a new design that "tolerates typos" in PAKEs through a combination of fuzzy and strong asymmetric PAKEs, which they call safPAKE. Last but not least, Richardson et al. [RRX26] showed how to obtain an efficient Fuzzy PAKE from garbled circuits utilizing a conditionally input revealing (CIR) 2-party computation protocol, which involves an OT, a commitment protocol and a garbling scheme.

9.6 Quantum-Annoying PAKEs

A PAKE is considered quantum-annoying, if a quantum adversary can break the PAKE, but only by solving a specific mathematical problem (e.g., discrete logarithm) for each password they try [ES21]. Thus, quantum-annoying PAKEs do not promise full quantum-resilience, but they do provide some resistance against QCs by making certain classical operations more expensive for quantum adversaries. The main idea is to make offline dictionary attacks harder 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 succeed in computing d-log (i.e., break DH) in an online protocol session, they cannot directly relate the computed value to a certain single password. To 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. Subsequently, 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.

10 Observations and Discussion

10.1 Design Paradigms and Schemes

Save for a few exceptions, 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. Furthermore, other prominent classical PAKE designs such as in SPEKE (except isogeny-based GA-PAKE [AEK+22a]), SPR-6 (except Gao et al. [GDLL17]), SPAKE, (Au)CPace, OPAQUE, and J-PAKE are currently non-present in the PQC realm (previously addressed in Sec. 9).

10.1.1 Design Paradigms

There are three main trends in PQC PAKE design with a strong focus on LWE, RLWE, and MLWE schemes (cf. Tab. 1). 1) PAKEs following the (O)EKE paradigm with focus on generic NIST PQC KEMs, and especially ML-KEM (C1), 2) PAKEs following

the PAK-suite paradigm using LWE and its variants directly and relying on different reconciliation mechanisms (C2 and C3), and 3) PAKEs following the KOY-GL paradigm using SPHF, ASPH, and NIZK constructions from LWE and its variants (C2 and C3).

10.1.2 PQC Schemes

As observed in classes C2 and C3, There exists a plethora of RLWE-PAK and LWE ASPH PAKEs, but the main contribution is more or less restricted to performance or security improvements. Ultimately, it appears that the prevailing trend is set on the lattices, especially because of the standardization of CRYSTALS-Kyber as ML-KEM. However, isogeny-based PAKEs are remarkably under-represented, and there are no code-based PAKEs at all. Thus, it is worth investigating whether more isogeny PAKEs are attainable; and whether code-based primitives are also a viable option.

10.1.3 Design Simplicity (or Complexity)

Generic constructions from abstract security properties can reduce overall complexity and even make peer reviews easier and more reliable [BGHJ24, JRX25]. In addition, generic designs enable the realization of (hybrid) frameworks (cf. Sec. 6.4) supporting interchangeability in the case of sudden breaks and the emergence of new threats.

10.1.4 Discussion

The lack of diversity can be mainly traced back to the fact that many classical PAKE designs are tightly coupled to password usage within the DH paradigm. This is 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. Regardless of the underlying primitive, generic KEMs provide limited support to designs operating (mathematically speaking) at the PKE level. Such designs include base mapping subroutines, password-derived generators, and password-derived secrets. KEMs are essentially used as a black-box interface within the PAKE, and should preferably not be used as a white-box. For instance, using the password within the ML-KEM key generation to obtain a new lattice basis defeats the purpose of a generic design and ultimately restricts the PAKE to concrete hardness assumptions. However, it may enable unexplored designs.

Splittable KEMs. This design had only been explored for KEMs based on lattice LWE primitives and variants (e.g., RLWE and MLWE). Still, splittable KEMs do maintain the provided algorithm interface in a black-box manner and may not directly support operations within the underlying PKE. Designs of splittable lattice-based KEM-PAKEs might also apply to KEMs from other primitives, which has not been addressed yet.

Lattices. Using PQC primitives directly offers more flexibility in, e.g., PAK-style LWE and RLWE PAKEs, where the H2G is used to hide the real 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 PQC NIKEs (e.g., SWOOSH [GdKQ+24]) can be used for a DH-like PAKE design.

Isogenies. While isogenies strongly resemble ECDH, classical approaches cannot be directly translated to SIDH and CSIDH, as adequately 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. Furthermore, the security of SPEKE-style and Dragonfly-like isogeny PAKEs is questionable, since they are difficult to realize when hashing into public keys. Last but not least, we recall that SIDH and SIKE were broken, which led to less interest in isogenies in general.

10.2 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 the application of hybrid schemes. Due to the skepticism that still surrounds the new PQC KEMs and digital signatures, hybrids can be either classical combined with PQC, or multiple PQC schemes together. In line with this recommendation, several hybrid KEMs were proposed, such as KEM Combiners [GHP18], X-Wing [BCD+24], and [ABK27].

Hybrids PAKEs. According to [KR24], there was no clear answer to the question of finding a generic approach to construct a hybrid PAKE. However, as seen in Sec. 6.4, new provably secure recipes have recently emerged, and a better understanding of the requirements and security guarantees of hybrid PAKEs is being established. For example, Hesse and Rosenberg [HR25] claimed the impossibility of obtaining a parallel combiner with adaptive security for hybrid PQC PAKEs, and Lyu and Liu [LL25] claimed that a parallel combiner requires both used PAKEs to satisfy the properties of a full DH-type PAKE. However, Günther et al. [GRSV25] found a method to do so using hybrid obfuscated KEMs. Moreover, Vos et al. [VJW+25b] showed how to obtain the password hiding property required in sequential combiners as presented in [HR25]. In [VJW+25b], this property is realized from information-theoretic assumptions on statistically uniform bitstrings, similar to [AAA+26] and [GRSV25].

Discussion. Optimally, hybrid PAKEs should also allow for interchangeable KEM usage in a plug-and-play manner and consequently enable crypto-agility in a sophisticated manner [ASW+22]. Nevertheless, such a state is yet to be achieved as hybrid designs are still in their early stages. Considering security, the most important question is whether a hybrid PAKE succeeds in (unconditionally) protecting the password, even if only one of the underlying schemes is broken, which is the focus of all recent proposals. Last but not least, it is also necessary to weigh in the performance of each proposed approach. As noted in [VJW+25b], realizing a parallel PAKE combiner using FrodoKEM in [GRSV25] improves runtime but results in much larger key sizes. Similarly, obfuscating ML-KEM and using a serial combiner results in a noticeable slowdown but reduces key sizes significantly.

10.3 Semantic Security and KEM Properties

Although abstract KEM properties are increasingly reaching a rather stable state in the literature (e.g., [Xag22, GMP22, MX23a, CDM24, Sch24, BCD+24, JRX25, Xu26b]), some questions still surround the properties needed to realize secure KEM PAKEs, and some results have been shown to be incomplete or even incorrect. Clearly, IND (or at least OW), PKU and ANO are present in all PAKEs [Xu26b]. Regardless of the used names, Fuzziness, PKU, and UNI-PK describe the distribution of the public key and are essentially the same property, which can also be observed in their almost identical security experiments.

OW-PCA, IND-CPA and IND-CCA. CPA security was believed to be sufficient to build secure PAKEs [Jar22]. However, it was recently argued that PCA provides a better alternative [ABJS24, ABJ25a, Xu26b]. Furthermore, recent work suggested the notions of SPR and SMT that imply key security and ciphertext pseudo-randomness as well [MRR20, JRX25]. Ultimately, SPR translates to both IND-CCA and ANO-CCA at the same time.

ANO. Regarding anonymity, it is agreed that it is necessary to hide the relationship between a ciphertext and the public key used to compute it. However, it is not clear which variant is considered sufficient. This applies for wANO and ANO, as well as PCA, CPA, and CCA. Usually, PAKE adversaries have no access to decryption or decapsulation oracles, which means that ANO-CPA should suffice. However, having SPR and SMT as a requirement makes it difficult to determine whether CCA security is also a must for ANO.

Ciphertexts and Final Keys. Januzelli et al. [JRX25] identified several flaws or overlooked aspects in prior constructions and suggested additional requirements, especially regarding the ciphertext and the final key/ciphertext relation. This applies to all CAKE (or EKE) proposals, where the ciphertext is also encrypted using an IC or a similarly programmable function. For example, it was shown in [JRX25] that both sPAKE [MRR20] and HIC-KEM [SGJK22] only realize a weaker UC functionality called " *TestSamePassword*", which can be traced back to the absence of IC properties that ensure non-malleability of randomized ciphertexts. In the case of CAKE, a similar attack was also shown when the final key derivation is not a PRF or does not include the password. These subtle findings led the authors in [JRX25] to state that many variants of EKE or CAKE require ciphertext collision freeness (SCFR), pseudo-randomness (SPR), and smoothness (SMT).

Proof Techniques. In contrast, Arriaga et al. [ABJ25a] argued in NoIC-PAKE that different proof methods are the reason behind these discrepancies. According to the authors, their monolithic proof exposes the required KEM properties and the RO behavior directly. On the other hand, Januzelli et al. [JRX25] construct their proof in a modular way, where the almost-UC POPF functionality is composed into the PAKE. As a result, the conditional composability notion makes it harder to identify exact bounds on the distinguishing advantage of the UC environment.

Encrypting Messages with Passwords. PAKEs that encrypt the public key may be vulnerable to offline dictionary attacks [AJK+20, AAA+26]. According to [ABJ25a], poor IC instantiation can lead to a mismatch between the domain of a block cipher and PAKE messages. An IC is usually instantiated with block ciphers over 128 bit domains (e.g., AES), which is infeasible for larger domains as in PQC public keys and ciphertexts. Although an 8-round Feistel was shown to be indifferentiable from an IC [DS16], it incurs four RO queries onto a group per cipher operation. This, in addition to the immaturity of the QIC model, can be viewed as the main motivation to either use domain extenders, which are extremely inefficient for very large domains, or avoid the IC all together. In C2 PAK-like constructions, the modified public key message distribution is directly dependent on the password due to the H2G password usage [AJK+20], which is also often overlooked.

Additional Properties. Recent work concerned with the FO [HV22, JMZ23, CWC+24] and validation of KEM public keys and ciphertexts [HK25, HHMS25] shows the possibility to obtain KEMs with new properties, which have not been observed in PAKE design so far. Moreover, there are constructions outside the NIST competition (e.g., POLKA [HLM+23], SPLIT-KEMs [Nio25], and Subversion-Resilient KEMs [DFJ+25]), which may revive other classical designs. NICE-PAKE [AAA+26] and TEMPO [ABJ25b] seem to deviate from the

ongoing trend in generic PAKEs as they apply additional KEM properties for adversarially chosen values. Xu [Xu26b] also addresses additional KEM properties such as ciphertext and key binding, and unpredictability.

Discussion. Evidently, incorrect results are an extremely sensitive matter and cannot be resolved with an educated guess. Nevertheless, it is clear that earlier constructions suffered from more flaws (or worse), and logically so, since PAKE design is tightly coupled to the progress made in PQC analysis. Essentially, public keys must be indistinguishable from random bit strings, which may not be the case for PQC keys yielding a certain structure [AJK+20, GRSV25] such as ML-KEM keys [AAA+26, GRSV25]. Public key uniformity 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 keys unstructured in some sense (e.g., splitting [ABJS24, AAA+26] or obfuscation [AAA+26]).

Intuitively, and similar to public keys, defining a random permutation over the cipheretxt domain requires a tangible assumption on the ciphertext distribution, otherwise it may lead to distinguishing attacks following wrong password guesses or offline dictionary attacks, which we view as a factual statement. The difficult question remains in identifying the gap between (additional) KEM assumptions without an IC, which was recently addressed in [Xu26b]. Further, extracting information about the password from randomized message is assumed to be infeasible, yet it may still be possible to obtain partial information about the used keys, as discussed below for leakage attacks.

10.4 Quantum Idealized Models

Two works [LLH24b, HHKR25] showed great progress with QROM bounds and it is safe to assume that QROM will not remain an issue for long. Considering IC, there are three main issues. First, there is still no known quantum equivalent for IC that is equally capable of defining a programmable behavior in the presence of quantum adversaries [AAA+26, HHKR25]. Second, it is not known how to instantiate an IC over domains much larger than 128 bits without inefficient domain extenders [ABJS24] or using a less efficient 8-round Feistel alternative [DS16]. Finally, there is an assumption (folklore) that proofs in IC are harder to lift to QIC in UC, which was also believed for the QROM.

Discussion. Almost all PAKE designs still need to address the issues arising from classical IC and ROM usage. Moreover, efficient designs and proofs in the standard model are strongly desired. However, this might be extremely difficult to achieve with many schemes relying mainly on hashing and permutations. Moreover, based on the attained level of maturity in PQC, 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. 4). 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. Nevertheless, the simulator of Hövelmanns et al. [HHKR25] at least demonstrates which capabilities are required to simulate a QIC. Still, the focus is on working around the IC or completely eliminating it.

10.5 Tight Bounds and Reductions

In the absence of an IC, it is difficult to prove knowledge of any information about an adversary's interactions with public keys in security proofs [AAA+26, ABJ25a, HHKR25]. Thus, it might be hard to enumerate passwords that can be ruled-out through active password guessing. For honest key generation, 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. Hence, it is difficult to formulate a hardness assumption bound to the number of password guessing queries for an unknown number of malicious key pairs [AAA+26, HHKR25].

Discussion. PQC KEMs differ mainly from bare primitives in the fact that they cannot yet apply self-reducible [KTAT20] properties to remove multiplicative factors in multiple-queries for certain 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]. A 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. As for QROM, allowing adversaries to perform superposition queries makes it hard for a simulator to extract pre-images or reprogram [LLH24a]. Still, RO reprogramming is probably not necessary (at least not in UC proofs [Hes20, MX23b, LLH24a]), but the QROM still needs to simulate real session keys using a decision oracle. Some works argue that classical output transfer is acceptable if extraction is possible using recent online extractability techniques [HHKR25]. However, an open question is whether quantum rewinding is applicable in PAKE proofs that rely on rewinding or back-patching [ABB+20, HTTY24].

10.6 Sufficient Analysis and Unknown Attack Surfaces

As observed in LBA-PAKE [DBK21], the authors attempted to fix vulnerabilities in a previous construction [FHZ+19], yet introduced a signal leakage attack on the PWE assumption that lead to full key recovery [DCQ22]. This is also seen in 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.

Old and New Attacks. Most (proclaimed) privacy preserving PQC PAKEs suffer from vulnerabilities against impersonation, stolen credentials (digitally or physically), and password guessing attacks; and sometimes even fail to provide user privacy or non-traceability. Furthermore, there are several aPAKE proposals, but no saPAKEs, as aPAKEs do not 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. Also, new attacks are not restricted to design, but can also target the underlying schemes cryptographically and also physically (cf. Dragonblood [VR20]).

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 privacy preserving communication is required in real world use cases such as eIDs and e-healthcare [ASWZ24], we believe that work on constructions with more rigorous formal and physical analysis is required. Finally, PQC saPAKEs are required to deal with pre-computation attacks. However, these are currently missing in the literature.

10.7 Implementations, Performance and Standardization

Since PQC PAKE research is still in its early stages, there are not sufficient driving factors (e.g., official standardization). Thus, comparing performance and finding a common

benchmarking baseline is an open problem. Based solely on our survey, we conclude that a meaningful comparison is not entirely possible. Essentially, this is due to the following reasons. 1) The absence of a unified benchmarking platform with the same HW capabilities and HW/SW optimizations, 2) the lack of comparison to classical predecessors, 3) the different security levels used in these implementations, and 4) the varying costs of password usage methods (e.g., H2G) and supporting cryptographic components (e.g., SPHFs).

Classical vs. PQC Primitives. PQC PAKEs are mainly based on lattice primitives (including KEMs), which inherently suffer from slower execution times and larger key sizes compared to DH and ECDH. This leads to an inescapable overhead in both computation and communication costs. Among more than 50 papers, only three compare their results to classical counterparts, two of which claim unreasonable speed-ups [XHCC17, GDLL17], while the third show a slowdown varying between a factor 3 and 10 depending on the parameters chosen for OCAKE with ML-KEM compared to PACE with p256 [AAB+25].

Realistic and Reliable Evaluation. Many works do not provide clear experimental results and do not directly address the security guarantees of their constructions. Moreover, some experimental results and benchmarks, especially for LWE and RLWE, seem unconvincing or rather unreasonable. Moreover, the performance indicators of the reviewed works differ in the measurement setup, used units (e.g., clock cycles, milliseconds, or computational cost, etc.), and the benchmarking environments also differ in their computational capabilities. Hence, it is extremely difficult to make accurate statements about which constructions are more secure or can perform better under which circumstances.

Impact of Design and Performance. The underlying primitive in is indeed the overwhelming factor in overall performance, which is especially true for generic KEM-based PAKEs. However, different use-cases impose different security and design requirements; therefore, trade-offs are probably inevitable. For example, ID cards are subject to regulations that define how fast and how secure a micro-chip must be. Other use cases impose other requirements, and by any means, finding the proper balance between security, computational complexity, and communication costs is not an easy task.

Discussion. Ideally, we would like to assess performance by assuming that the same primitive will require the same resources using the same platform and the same implementation (or optimization). 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. Assuming a unified platform, the question is to compare the efficiency of designs for the most suitable use case; preferably also compared to similar classical designs.

11 Conclusion and Future Work

Based on our review, a pressing order of business for future work would be an official project providing a unified hardware and software framework for PQC PAKE implementation and benchmarking. Further, such a 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 implementation security. In addition, 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 the security properties of KEM and idealized objects should receive 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.

12 Epilogue: Limitations of (*Short-Lived*) SoKs

In this work, we reviewed over 50 PQC PAKE proposals identified in the literature; and presented a thorough taxonomy and analysis of their design paradigms. Still, other taxonomies are also found in PAKE proposals and formal analysis papers that provide brief overviews of prior and concurrent (related) work. For example, Kumar and Xu [KX25] discuss the security of the KOY protocol built from SPHFs and define two design paradigms, which they refer to as EKE-type and SPHF-based. However, their classification is more related to the framework and security model used in analysis. Indeed, the authors pose very important questions considering the implications of the chosen design on the provable security of a PAKE, or better said the attained degree of security. Still, attempting to classify PAKEs based on security models ultimately fails to encompass all relevant constructions, since almost all PQC PAKEs (and classical ones for that matter) rely on one or more models independent of the proof framework used in their analysis (cf. Tab 1). Another example can be found in the recent hybrid PAKE proposal of Vos et al. [VJW+25b], who describe existing PAKEs that can be instantiated using PQC primitives (including KEMs). However, the authors choose a method to classify these PAKEs, which is too fine-grained and makes a type dependent on the underlying primitive rather than on the way the password is used. Our (adapted) classification is also an attempt, and is subject to continuous change. Hence it is only transient and destined to become obsolete at some point in the future[11]. Nevertheless, we believe that providing a snapshot of research progress is of great benefit to cryptographers and practitioners alike.

References

[AAA+26] Nouri Alnahawi, Jacob Alperin-Sheriff, Daniel Apon, Gareth T. Davies, and Alexander Wiesmaier. NICE-PAKE: on the security of kem-based PAKE constructions without ideal ciphers, 2026. URL: https://doi.org/10.62056/abksr-iuc, doi:10.62056/ABKSR-IUC.

[AAB+25] Nouri Alnahawi, Melissa Azouaoui, Joppe W. Bos, Gareth T. Davies, SeoJeong Moon, Christine van Vredendaal, and Alexander Wiesmaier. Post-quantum cryptography in emrtds evaluating PAKE and PKI for travel documents. In Henrich C. Pöhls and Chris J. Mitchell, editors, *Security Standardisation Research - 10th International Conference, SSR 2025, Passau, Germany, December 4-5, 2025, Proceedings*, volume 16466 of *Lecture Notes in Computer Science*, pages 181–201. Springer, 2025. doi:10.1007/978-3-032-19567-8_9.

[AAK19] Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, and Amir Hassani Karbasi. A new ring-based SPHF and PAKE protocol on ideal lattices. *ISC Int. J. Inf. Secur.*, 11(1):75–86, 2019. URL: https://doi.org/10.22042/isecure.2018.109810.398, doi:10.22042/ISECURE.2018.109810.398.

[11] We deliberately express this thought in the section title using the term *Short-Lived* as opposed to *Long-Lived* Secrets, which are the passwords in PAKEs.

[ABB+20] Michel Abdalla, Manuel Barbosa, Tatiana Bradley, Stanislaw Jarecki, Jonathan Katz, and Jiayu Xu. Universally composable relaxed password authenticated key exchange. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part I*, volume 12170 of *Lecture Notes in Computer Science*, pages 278–307. Springer, 2020. doi:10.1007/978-3-030-56784-2_10.

[Abd14] Michel Abdalla. Password-based authenticated key exchange: An overview. In Sherman S. M. Chow, Joseph K. Liu, Lucas Chi Kwong Hui, and Siu-Ming Yiu, editors, *Provable Security - 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014. Proceedings*, volume 8782 of *Lecture Notes in Computer Science*, pages 1–9. Springer, 2014. doi:10.1007/978-3-319-12475-9_1.

[ABJ25a] Afonso Arriaga, Manuel Barbosa, and Stanislaw Jarecki. NoIC: PAKE from KEM without ideal ciphers. Cryptology ePrint Archive, Paper 2025/231, 2025. URL: https://eprint.iacr.org/2025/231.

[ABJ25b] Afonso Arriaga, Manuel Barbosa, and Stanislaw Jarecki. Tempo: ML-KEM to PAKE compiler resilient to timing attacks. Cryptology ePrint Archive, Paper 2025/1399, 2025. URL: https://eprint.iacr.org/2025/1399.

[ABJS24] Afonso Arriaga, Manuel Barbosa, Stanislaw Jarecki, and Marjan Skrobot. C'est très CHIC: A compact password-authenticated key exchange from lattice-based KEM. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part V*, volume 15488 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2024. doi:10.1007/978-981-96-0935-2_1.

[ABK27] Gorjan Alagic, Fahran Bajaj, and Aybars Kocoglu. The best of both KEMs: Securely combining KEMs in post-quantum hybrid schemes, 2027. doi:10.1007/978-3-032-32560-0_2.

[ABPS24] Gorjan Alagic, Chen Bai, Alexander Poremba, and Kaiyan Shi. On the two-sided permutation inversion problem. *IACR Commun. Cryptol.*, 1(1):27, 2024. URL: https://doi.org/10.62056/a0qj89n4e, doi:10.62056/A0QJ89N4E.

[ABR+21] Michel Abdalla, Manuel Barbosa, Peter B. Rønne, Peter Y. A. Ryan, and Petra Sala. Security characterization of J-PAKE and its variants. *IACR Cryptol. ePrint Arch.*, 2021:824, 2021. URL: https://eprint.iacr.org/2021/824.

[ACC+19] Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Aaron Hutchinson, Amir Jalali, Koray Karabina, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersingular isogeny key encapsulation. https://www.sike.org/files/SIDH-spec.pdf, 2019.

[ACFP05] Michel Abdalla, Olivier Chevassut, Pierre-Alain Fouque, and David Pointcheval. A simple threshold authenticated key exchange from short secrets. In Bimal K. Roy, editor, *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*, volume 3788 of *Lecture Notes in Computer Science*, pages 566–584. Springer, 2005. doi:10.1007/11593447_31.

[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.

[ACMT25] Gorjan Alagic, Joseph Carolan, Christian Majenz, and Saliha Tokat. The sponge is quantum indifferentiable. In *66th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2025, Sydney, Australia, December 14-17, 2025*, pages 2591–2630. IEEE, 2025. doi:10.1109/FOCS63196.2025.00135.

[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 Marc Joye and Gregor Leander, editors, *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*, volume 14656 of *Lecture Notes in Computer Science*, pages 447–476. Springer, 2024. doi:10.1007/978-3-031-58751-1_16.

[ADDS21] Martin R. Albrecht, Alex Davidson, Amit Deo, and Nigel P. Smart. Round-optimal verifiable oblivious pseudorandom functions from ideal lattices. In Juan A. Garay, editor, *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part II*, volume 12711 of *Lecture Notes in Computer Science*, pages 261–289. Springer, 2021. doi:10.1007/978-3-030-75248-4_10.

[AEK+22a] Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, and Doreen Riepel. Password-authenticated key exchange from group actions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*, volume 13508 of *Lecture Notes in Computer Science*, pages 699–728. Springer, 2022. doi:10.1007/978-3-031-15979-4_24.

[AEK+22b] Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, and Doreen Riepel. Password-authenticated key exchange from group actions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*, volume 13508 of *Lecture Notes in Computer Science*, pages 699–728. Springer, 2022. doi:10.1007/978-3-031-15979-4_24.

[AFP05] Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval. Password-based authenticated key exchange in the three-party setting. In Serge Vaudenay, editor, *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings*, volume 3386 of *Lecture Notes in Computer Science*, pages 65–84. Springer, 2005. doi:10.1007/978-3-540-30580-4_6.

[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 Markulf Kohlweiss, Roberto Di Pietro, and Alastair R. Beresford, editors, *Cryptology and Network Security - 23rd International*

Conference, CANS 2024, Cambridge, UK, September 24-27, 2024, Proceedings, Part II, volume 14906 of *Lecture Notes in Computer Science*, pages 191–212. Springer, 2024. doi:10.1007/978-981-97-8016-7_9.

[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 Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *Applied Cryptography and Network Security - 18th International Conference, ACNS 2020, Rome, Italy, October 19-22, 2020, Proceedings, Part I*, volume 12146 of *Lecture Notes in Computer Science*, pages 169–186. Springer, 2020. doi:10.1007/978-3-030-57808-4_9.

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

[AM22] Nuttapong Attrapadung and Takahiro Matsuda. Public-Key Encryption and Security Notions. *Asymmetric Cryptography: Primitives and Protocols*, 2022.

[AMO+26] Afonso Arriaga, David Mestel, Jan Oupickỳ, Peter Browne Rønne, and Marjan Škrobot. Hic is all you need: Practical post-quantum password-authenticated public-key encryption. In *Cryptographers' Track at the RSAC Conference*, pages 127–154. Springer, 2026. URL: http://dx.doi.org/10.1007/978-3-032-22931-1_5, doi:10.1007/978-3-032-22931-1_5.

[AP05] Michel Abdalla and David Pointcheval. Simple password-based encrypted key exchange protocols. In Alfred Menezes, editor, *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, volume 3376 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2005. doi:10.1007/978-3-540-30574-3_14.

[AR17] Gorjan Alagic and Alexander Russell. Quantum-secure symmetric-key cryptography based on hidden shifts. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 65–93, 2017. doi:10.1007/978-3-319-56617-7_3.

[ARS24] Afonso Arriaga, Peter Y. A. Ryan, and Marjan Skrobot. Sweetpake: Key exchange with decoy passwords. In Jianying Zhou, Tony Q. S. Quek, Debin Gao, and Alvaro A. Cárdenas, editors, *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2024, Singapore, July 1-5, 2024*. ACM, 2024. doi:10.1145/3634737.3645009.

[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/2023/487.

[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(2):34:1–34:28, 2024. doi:10.1145/3585517.

[Bas23] Andrea Basso. A post-quantum round-optimal oblivious PRF from isogenies. In Claude Carlet, Kalikinkar Mandal, and Vincent Rijmen, editors, *Selected Areas in Cryptography - SAC 2023 - 30th International Conference,*

Fredericton, Canada, August 14-18, 2023, Revised Selected Papers, volume 14201 of *Lecture Notes in Computer Science*, pages 147–168. Springer, 2023. doi:10.1007/978-3-031-53368-6_8.

[BBDQ18] Fabrice Benhamouda, Olivier Blazy, Léo Ducas, and Willy Quach. Hash proof systems over lattices revisited. In Michel Abdalla and Ricardo Dahab, editors, *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 II*, volume 10770 of *Lecture Notes in Computer Science*, pages 644–674. Springer, 2018. doi:10.1007/978-3-319-76581-5_22.

[BBF+19] Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. Hybrid key encapsulation mechanisms and authenticated key exchange. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 206–226. Springer, 2019. doi:10.1007/978-3-030-25510-7_12.

[BCD+16] Joppe W. Bos, Craig Costello, Léo 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 Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 1006–1018. ACM, 2016. doi:10.1145/2976749.2978425.

[BCD+24] Manuel Barbosa, Deirdre Connolly, João Diogo Duarte, Aaron Kaiser, Peter Schwabe, Karoline Varner, and Bas Westerbaan. X-wing. *IACR Commun. Cryptol.*, 1(1):21, 2024. URL: https://doi.org/10.62056/a3qj89n4e, doi:10.62056/A3QJ89N4E.

[BCMR19] Erica Blum, Makana Castillo-Martin, and Michael Rosenberg. Survey on the security of the quantum rom. https://www.cs.umd.edu/class/fall2019/cmsc657/projects/group_2.pdf, 2019.

[BCP+23] Hugo Beguinet, Céline Chevalier, David Pointcheval, Thomas Ricosset, and Mélissa Rossi. Get a CAKE: generic transformations from key encaspulation mechanisms to password authenticated key exchanges. In Mehdi Tibouchi and Xiaofeng Wang, editors, *Applied Cryptography and Network Security - 21st International Conference, ACNS 2023, Kyoto, Japan, June 19-22, 2023, Proceedings, Part II*, volume 13906 of *Lecture Notes in Computer Science*, pages 516–538. Springer, 2023. doi:10.1007/978-3-031-33491-7_19.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011. doi:10.1007/978-3-642-25385-0_3.

[BDFH25] Ward Beullens, Lucas Dodgson, Sebastian H. Faller, and Julia Hesse. The 2hash OPRF framework and efficient post-quantum instantiations. In Serge

Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques Madrid, Spain, May 4-8, 2025, Proceedings, Part VIII*, volume 15608 of *Lecture Notes in Computer Science*, pages 332–362. Springer, 2025. doi:10.1007/978-3-031-91101-9_12.

[BDK+18] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS - kyber: A cca-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018*, pages 353–367. IEEE, 2018. URL: https://doi.org/10.1109/EuroSP.2018.00032, doi:10.1109/EUROSP.2018.00032.

[Ber09] Daniel J Bernstein. *Introduction to post-quantum cryptography*, volume 1, pages 1–14. Springer Berlin/Heidelberg, Germany, 2009. URL: http://dx.doi.org/10.1007/978-3-540-88702-7_1, doi:10.1007/978-3-540-88702-7_1.

[BFH+23] Jonathan Bootle, Sebastian H. Faller, Julia Hesse, Kristina Hostáková, and Johannes Ottenhues. Generalized fuzzy password-authenticated key exchange from error correcting codes. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part VIII*, volume 14445 of *Lecture Notes in Computer Science*, pages 110–142. Springer, 2023. doi:10.1007/978-981-99-8742-9_4.

[BFK09] Jens Bender, Marc Fischlin, and Dennis Kügler. Security analysis of the PACE key-agreement protocol. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio A. Ardagna, editors, *Information Security, 12th International Conference, ISC 2009, Pisa, Italy, September 7-9, 2009. Proceedings*, volume 5735 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 2009. doi:10.1007/978-3-642-04474-8_3.

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). In Janos Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 103–112. ACM, 1988. doi:10.1145/62212.62222.

[BGHJ24] Manuel Barbosa, Kai Gellert, Julia Hesse, and Stanislaw Jarecki. Bare PAKE: universally composable key exchange from just passwords. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part II*, volume 14921 of *Lecture Notes in Computer Science*, pages 183–217. Springer, 2024. doi:10.1007/978-3-031-68379-4_6.

[BGV14] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Trans. Comput. Theory*, 6(3):13:1–13:36, 2014. doi:10.1145/2633600.

[BJSL11] Ali Bagherzandi, Stanislaw Jarecki, Nitesh Saxena, and Yanbin Lu. Password-protected secret sharing. In Yan Chen, George Danezis, and Vitaly Shmatikov,

editors, *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011*, pages 433–444. ACM, 2011. doi:10.1145/2046707.2046758.

[BKW20] Dan Boneh, Dmitry Kogan, and Katharine Woo. Oblivious pseudorandom functions from isogenies. In Shiho Moriai and Huaxiong Wang, editors, *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*, volume 12492 of *Lecture Notes in Computer Science*, pages 520–550. Springer, 2020. doi:10.1007/978-3-030-64834-3_18.

[BL17] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nat.*, 549(7671):188–194, 2017. URL: https://doi.org/10.1038/nature23461, doi:10.1038/NATURE23461.

[Bla06] John Black. The ideal-cipher model, revisited: An uninstantiable blockcipher-based hash function. In Matthew J. B. Robshaw, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*, pages 328–340. Springer, 2006. doi:10.1007/11799313_21.

[BM92] Steven M. Bellovin and Michael Merritt. Encrypted key exchange: password-based protocols secure against dictionary attacks. In *1992 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, May 4-6, 1992*, pages 72–84. IEEE Computer Society, 1992. doi:10.1109/RISP.1992.213269.

[BM25] Andrea Basso and Luciano Maino. Poké: A compact and efficient PKE from higher-dimensional isogenies. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 94–123. Springer, 2025. doi:10.1007/978-3-031-91124-8_4.

[BMP00] Victor Boyko, Philip D. MacKenzie, and Sarvar Patel. Provably secure password-authenticated key exchange using diffie-hellman. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 156–171. Springer, 2000. doi:10.1007/3-540-45539-6_12.

[Boy22] Colin Boyd. Key Exchange. *Asymmetric Cryptography: Primitives and Protocols*, 2022.

[BPR00] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 139–155. Springer, 2000. doi:10.1007/3-540-45539-6_11.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *CCS '93, Proceedings*

of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993, pages 62–73. ACM, 1993. doi:10.1145/168588.168596.

[BRRS18] José Becerra, Peter B. Rønne, Peter Y. A. Ryan, and Petra Sala. Honeypakes. In Vashek Matyás, Petr Svenda, Frank Stajano, Bruce Christianson, and Jonathan Anderson, editors, *Security Protocols XXVI - 26th International Workshop, Cambridge, UK, March 19-21, 2018, Revised Selected Papers*, volume 11286 of *Lecture Notes in Computer Science*, pages 63–77. Springer, 2018. doi:10.1007/978-3-030-03251-7_7.

[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 Syst. J.*, 17(4):6093–6103, 2023. doi:10.1109/JSYST.2023.3288629.

[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*, 12:46596–46615, 2024. doi:10.1109/ACCESS.2024.3380915.

[CAK18] Rakyong Choi, Hyeongcheol An, and Kwangjo Kim. 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 *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, Las Vegas, Nevada, USA, October 14-17, 2001*, pages 136–145. IEEE Computer Society, 2001. doi:10.1109/SFCS.2001.959888.

[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.

[CDM24] Cas Cremers, Alexander Dax, and Niklas Medinger. Keeping up with the kems: Stronger security notions for kems and automated analysis of kem-based protocols. In Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie, editors, *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS 2024, Salt Lake City, UT, USA, October 14-18, 2024*, pages 1046–1060. ACM, 2024. doi:10.1145/3658644.3670283.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, 2004. doi:10.1145/1008731.1008734.

[CHK+05] Ran Canetti, Shai Halevi, Jonathan Katz, Yehuda Lindell, and Philip D. MacKenzie. Universally composable password-based key exchange. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 404–421. Springer, 2005. doi:10.1007/11426639_24.

[CHL22] Sílvia Casacuberta, Julia Hesse, and Anja Lehmann. Sok: Oblivious pseudorandom functions. In *7th IEEE European Symposium on Security and*

Privacy, EuroS&P 2022, Genoa, Italy, June 6-10, 2022, pages 625–646. IEEE, 2022. URL: https://doi.org/10.1109/EuroSP53844.2022.00045, doi:10.1109/EUROSP53844.2022.00045.

[CHL+25] Alexandru Cojocaru, Minki Hhan, Qipeng Liu, Takashi Yamakawa, and Aaram Yun. Quantum lifting for invertible permutations and ideal ciphers. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part II*, volume 16001 of *Lecture Notes in Computer Science*, pages 481–512. Springer, 2025. doi:10.1007/978-3-032-01878-6_16.

[CK01] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*, pages 453–474. Springer, 2001. doi:10.1007/3-540-44987-6_28.

[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*, 11:136947–136957, 2023. doi:10.1109/ACCESS.2023.3325886.

[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 Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018. doi:10.1007/978-3-030-03332-3_15.

[CLN12] Jan Camenisch, Anna Lysyanskaya, and Gregory Neven. Practical yet universally composable two-server password-authenticated secret sharing. In Ting Yu, George Danezis, and Virgil D. Gligor, editors, *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*, pages 525–536. ACM, 2012. doi:10.1145/2382196.2382252.

[CMSZ19] Jan Czajkowski, Christian Majenz, Christian Schaffner, and Sebastian Zur. Quantum lazy sampling and game-playing proofs for quantum indifferentiability. Cryptology ePrint Archive, Paper 2019/428, 2019. URL: https://eprint.iacr.org/2019/428.

[CQY24] Lin Chen, Tongzhou Qu, and Anqi Yin. Quantum-safe multi-server password-based authenticated key exchange protocol. *Multim. Tools Appl.*, 83(24):65011–65038, 2024. URL: https://doi.org/10.1007/s11042-023-17984-1, doi:10.1007/S11042-023-17984-1.

[CROLL22] Angela Carrera-Rivera, William Ochoa, Felix Larrinaga, and Ganix Lasa. How-to conduct a systematic literature review: A quick guide for computer

science research. *MethodsX*, 9:101895, 2022. URL: http://dx.doi.org/10.1016/j.mex.2022.101895, doi:10.1016/j.mex.2022.101895.

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64. Springer, 2002. doi:10.1007/3-540-46035-7_4.

[CWC+24] Jinrong Chen, Yi Wang, Rongmao Chen, Xinyi Huang, and Wei Peng. Tighter proofs for pke-to-kem transformation in the quantum random oracle model. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part IV*, volume 15487 of *Lecture Notes in Computer Science*, pages 101–133. Springer, 2024. doi:10.1007/978-981-96-0894-2_4.

[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 Helena Handschuh, editor, *Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings*, volume 10159 of *Lecture Notes in Computer Science*, pages 183–204. Springer, 2017. doi:10.1007/978-3-319-52153-4_11.

[DBK21] Vivek Dabra, Anju Bala, and Saru Kumari. LBA-PAKE: lattice-based anonymous password authenticated key exchange for mobile devices. *IEEE Syst. J.*, 15(4):5067–5077, 2021. doi:10.1109/JSYST.2020.3023808.

[DCQ22] Ruoyu Ding, Chi Cheng, and Yue Qin. Further analysis and improvements of a lattice-based anonymous PAKE scheme. *IEEE Syst. J.*, 16(3):5035–5043, 2022. doi:10.1109/JSYST.2022.3161264.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In Cris Koutsougeras and Jeffrey Scott Vitter, editors, *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 542–552. ACM, 1991. doi:10.1145/103418.103474.

[DF11] Yi Ding and Lei Fan. Efficient password-based authenticated key exchange from lattices. In Yuping Wang, Yiu-ming Cheung, Ping Guo, and Yingbin Wei, editors, *Seventh International Conference on Computational Intelligence and Security, CIS 2011, Sanya, Hainan, China, December 3-4, 2011*, pages 934–938. IEEE Computer Society, 2011. doi:10.1109/CIS.2011.210.

[DFG+23] Gareth T. Davies, Sebastian H. Faller, Kai Gellert, Tobias Handirk, Julia Hesse, Máté Horváth, and Tibor Jager. Security analysis of the whatsapp end-to-end encrypted backup protocol. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part IV*, volume 14084 of *Lecture Notes in Computer Science*, pages 330–361. Springer, 2023. doi:10.1007/978-3-031-38551-3_11.

[DFJ+25] Kévin Duverger, Pierre-Alain Fouque, Charlie Jacomme, Guilhem Niot, and Cristina Onete. Subversion-resilient key-exchange in the post-quantum world. In Chun-Ying Huang, Jyh-Cheng Chen, Shiuh-Pyng Shieh, David Lie, and Véronique Cortier, editors, *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, CCS 2025, Taipei, Taiwan, October 13-17, 2025*, pages 1200–1214. ACM, 2025. doi:10.1145/3719027.3765165.

[DFMS22] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Online-extractability in the quantum random-oracle model. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 677–706. Springer, 2022. doi:10.1007/978-3-031-07082-2_24.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976. doi:10.1109/TIT.1976.1055638.

[DHP+18] Pierre-Alain Dupont, Julia Hesse, David Pointcheval, Leonid Reyzin, and Sophia Yakoubov. Fuzzy password-authenticated key exchange. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 393–424. Springer, 2018. doi:10.1007/978-3-319-78372-7_13.

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

[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. *Multim. Tools Appl.*, 82(17):26643–26660, 2023. URL: https://doi.org/10.1007/s11042-023-14937-6, doi:10.1007/S11042-023-14937-6.

[DKBY24] Vivek Dabra, Saru Kumari, Anju Bala, and Sonam Yadav. SL3PAKE: simple lattice-based three-party password authenticated key exchange for post-quantum world. *J. Inf. Secur. Appl.*, 84:103826, 2024. URL: https://doi.org/10.1016/j.jisa.2024.103826, doi:10.1016/J.JISA.2024.103826.

[DKRV18] Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure KEM. In Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings*, volume 10831 of *Lecture Notes in Computer Science*, pages 282–305. Springer, 2018. doi:10.1007/978-3-319-89339-6_16.

[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 Things J.*, 10(3):2680–2692, 2023. doi:10.1109/JIOT.2022.3213990.

[DS16] Yuanxi Dai and John P. Steinberger. Indifferentiability of 8-round feistel networks. In Matthew Robshaw and Jonathan Katz, editors, *Advances in*

Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I, volume 9814 of *Lecture Notes in Computer Science*, pages 95–120. Springer, 2016. doi:10.1007/978-3-662-53018-4_4.

[dSGP24] Cyprien Delpech de Saint Guilhem and Robi Pedersen. New proof systems and an OPRF from CSIDH. In Qiang Tang and Vanessa Teague, editors, *Public-Key Cryptography - PKC 2024 - 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia, April 15-17, 2024, Proceedings, Part III*, volume 14603 of *Lecture Notes in Computer Science*, pages 217–251. Springer, 2024. doi:10.1007/978-3-031-57725-3_8.

[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 Chi-Chih Yao. On the security of public key protocols. *IEEE Trans. Inf. Theory*, 29(2):198–207, 1983. doi:10.1109/TIT.1983.1056650.

[DY05] Yevgeniy Dodis and Aleksandr Yampolskiy. A verifiable random function with short proofs and keys. In Serge Vaudenay, editor, *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings*, volume 3386 of *Lecture Notes in Computer Science*, pages 416–431. Springer, 2005. doi:10.1007/978-3-540-30580-4_28.

[EHOR20] Andreas Erwig, Julia Hesse, Maximilian Orlt, and Siavash Riahi. Fuzzy asymmetric password-authenticated key exchange. In Shiho Moriai and Huaxiong Wang, editors, *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*, volume 12492 of *Lecture Notes in Computer Science*, pages 761–784. Springer, 2020. doi:10.1007/978-3-030-64834-3_26.

[ES21] Edward Eaton and Douglas Stebila. The "quantum annoying" property of password-authenticated key exchange protocols. In Jung Hee Cheon and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20-22, 2021, Proceedings*, volume 12841 of *Lecture Notes in Computer Science*, pages 154–173. Springer, 2021. doi:10.1007/978-3-030-81293-5_9.

[FHZ+19] Qi Feng, Debiao He, Sherali Zeadally, Neeraj Kumar, and Kaitai Liang. Ideal lattice-based anonymous authentication protocol for mobile devices. *IEEE Syst. J.*, 13(3):2775–2785, 2019. doi:10.1109/JSYST.2018.2851295.

[FIPR05] Michael J. Freedman, Yuval Ishai, Benny Pinkas, and Omer Reingold. Keyword search and oblivious pseudorandom functions. In Joe Kilian, editor, *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, volume 3378 of *Lecture Notes in Computer Science*, pages 303–324. Springer, 2005. doi:10.1007/978-3-540-30576-7_17.

[FOO23] Sebastian H. Faller, Astrid Ottenhues, and Johannes Ottenhues. Composable oblivious pseudo-random functions via garbled circuits. In Abdelrahaman

Aly and Mehdi Tibouchi, editors, *Progress in Cryptology - LATINCRYPT 2023 - 8th International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2023, Quito, Ecuador, October 3-6, 2023, Proceedings*, volume 14168 of *Lecture Notes in Computer Science*, pages 249–270. Springer, 2023. doi:10.1007/978-3-031-44469-2_13.

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

[FTTY18] Atsushi Fujioka, Katsuyuki Takashima, Shintaro Terada, and Kazuki Yoneyama. Supersingular isogeny diffie-hellman authenticated key exchange. In Kwangsu Lee, editor, *Information Security and Cryptology - ICISC 2018 - 21st International Conference, Seoul, South Korea, November 28-30, 2018, Revised Selected Papers*, volume 11396 of *Lecture Notes in Computer Science*, pages 177–195. Springer, 2018. doi:10.1007/978-3-030-12146-4_12.

[GdKQ+24] Phillip Gajland, Bor de Kock, Miguel Quaresma, Giulio Malavolta, and Peter Schwabe. SWOOSH: efficient lattice-based non-interactive key exchange. In Davide Balzarotti and Wenyuan Xu, editors, *33rd USENIX Security Symposium, USENIX Security 2024, Philadelphia, PA, USA, August 14-16, 2024*. USENIX Association, 2024. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/gajland.

[GDL+18] Xinwei Gao, Jintai Ding, Lin Li, Saraswathy RV, and Jiqiang Liu. Efficient implementation of password-based authenticated key exchange from RLWE and post-quantum TLS. *Int. J. Netw. Secur.*, 20(5):923–930, 2018. URL: http://ijns.jalaxy.com.tw/contents/ijns-v20-n5/ijns-2018-v20-n5-p923-930.pdf.

[GDLL17] Xinwei Gao, Jintai Ding, Jiqiang Liu, and Lin Li. Post-quantum secure remote password protocol from RLWE problem. In Xiaofeng Chen, Dongdai Lin, and Moti Yung, editors, *Information Security and Cryptology - 13th International Conference, Inscrypt 2017, Xi'an, China, November 3-5, 2017, Revised Selected Papers*, volume 10726 of *Lecture Notes in Computer Science*, pages 99–116. Springer, 2017. doi:10.1007/978-3-319-75160-3_8.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, 1986. doi:10.1145/6490.6503.

[GHP18] Federico Giacon, Felix Heuer, and Bertram Poettering. KEM combiners. In Michel Abdalla and Ricardo Dahab, editors, *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*, volume 10769 of *Lecture Notes in Computer Science*, pages 190–218. Springer, 2018. doi:10.1007/978-3-319-76578-5_7.

[GJK21] Yanqi Gu, Stanislaw Jarecki, and Hugo Krawczyk. KHAPE: asymmetric PAKE from key-hiding key exchange. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part IV*, volume 12828 of *Lecture Notes in Computer Science*, pages 701–730. Springer, 2021. doi:10.1007/978-3-030-84259-8_24.

[GJK+24] Yanqi Gu, Stanislaw Jarecki, Pawel Kedzior, Phillip Nazarian, and Jiayu Xu. Threshold PAKE with security against compromise of all servers. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 -*

30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part V, volume 15488 of *Lecture Notes in Computer Science*, pages 66–100. Springer, 2024. doi:10.1007/978-981-96-0935-2_3.

[Gjö24] Kristian Gjösteen. Password-authenticated key exchange and applications. Cryptology ePrint Archive, Paper 2024/1057, 2024. URL: https://eprint.iacr.org/2024/1057.

[GL03] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 524–543. Springer, 2003. doi:10.1007/3-540-39200-9_33.

[GMP22] Paul Grubbs, Varun Maram, and Kenneth G. Paterson. Anonymous, robust post-quantum public key encryption. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 402–432. Springer, 2022. doi:10.1007/978-3-031-07082-2_15.

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In Robert Sedgewick, editor, *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 291–304. ACM, 1985. doi:10.1145/22145.22178.

[GMR06] Craig Gentry, Philip D. MacKenzie, and Zulfikar Ramzan. A method for making password-based key exchange resilient to server compromise. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 142–159. Springer, 2006. doi:10.1007/11818175_9.

[GO14] Jens Groth and Rafail Ostrovsky. Cryptography in the multi-string model. *J. Cryptol.*, 27(3):506–543, 2014. URL: https://doi.org/10.1007/s00145-013-9152-y, doi:10.1007/S00145-013-9152-Y.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996. doi:10.1145/237814.237866.

[GRSV25] Felix Günther, Michael Rosenberg, Douglas Stebila, and Shannon Veitch. Hybrid obfuscated key exchange and kems. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part III*, volume 16002 of *Lecture Notes in Computer Science*, pages 575–609. Springer, 2025. doi:10.1007/978-3-032-01881-6_18.

[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*, 15(9):1750, 2023. URL: https://doi.org/10.3390/sym15091750, doi:10.3390/SYM15091750.

[GSV24] Felix Günther, Douglas Stebila, and Shannon Veitch. Obfuscated key exchange. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS 2024, Salt Lake City, UT, USA, October 14-18, 2024*, pages 2385–2399. ACM, 2024. doi:10.1145/3658644.3690220.

[Gu24] Yanqi Gu. *New Paradigms For Efficient Password Authentication Protocols*. PhD thesis, University of California, Irvine, 2024. URL: https://escholarship.org/uc/item/7qm0220s.

[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. URL: http://dx.doi.org/10.1109/sensorcomm.2008.131, doi:10.1109/sensorcomm.2008.131.

[HBCvO24] Feng Hao, Samiran Bag, Liqun Chen, and Paul C. van Oorschot. Owl: An augmented password-authenticated key exchange scheme. In Jeremy Clark and Elaine Shi, editors, *Financial Cryptography and Data Security - 28th International Conference, FC 2024, Willemstad, Curaçao, March 4-8, 2024, Revised Selected Papers, Part II*, volume 14745 of *Lecture Notes in Computer Science*, pages 227–244. Springer, 2024. doi:10.1007/978-3-031-78679-2_12.

[Hes20] Julia Hesse. Separating symmetric and asymmetric password-authenticated key exchange. In Clemente Galdi and Vladimir Kolesnikov, editors, *Security and Cryptography for Networks - 12th International Conference, SCN 2020, Amalfi, Italy, September 14-16, 2020, Proceedings*, volume 12238 of *Lecture Notes in Computer Science*, pages 579–599. Springer, 2020. doi:10.1007/978-3-030-57990-6_29.

[HHKR25] Kathrin Hövelmanns, Andreas Hülsing, Mikhail Kudinov, and Silvia Ritsch. CAKE requires programming - on the provable post-quantum security of (o)CAKE. Cryptology ePrint Archive, Paper 2025/458, 2025. URL: https://eprint.iacr.org/2025/458.

[HHM+24] Lena Heimberger, Tobias Hennerbichler, Fredrik Meisingseth, Sebastian Ramacher, and Christian Rechberger. Oprfs from isogenies: Designs and analysis. In Jianying Zhou, Tony Q. S. Quek, Debin Gao, and Alvaro A. Cárdenas, editors, *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2024, Singapore, July 1-5, 2024*. ACM, 2024. doi:10.1145/3634737.3645010.

[HHMS25] Kathrin Hövelmanns, Andreas Hülsing, Christian Majenz, and Fabrizio Sisinni. (un)breakable curses - re-encryption in the fujisaki-okamoto transform. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 245–274. Springer, 2025. doi:10.1007/978-3-031-91124-8_9.

[HK25] Kathrin Hövelmanns and Mikhail A. Kudinov. Treating dishonest ciphertexts in post-quantum kems - explicit vs. implicit rejection in the FO transform. In Ruben Niederhagen and Markku-Juhani O. Saarinen, editors, *Post-Quantum*

Cryptography - 16th International Workshop, PQCrypto 2025, Taipei, Taiwan, April 8-10, 2025, Proceedings, Part II, volume 15578 of *Lecture Notes in Computer Science*, pages 325–350. Springer, 2025. doi:10.1007/978-3-031-86602-9_12.

[HLM+23] Clément Hoffmann, Benoît Libert, Charles Momin, Thomas Peters, and François-Xavier Standaert. POLKA: towards leakage-resistant post-quantum cca-secure public key encryption. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *Public-Key Cryptography - PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7-10, 2023, Proceedings, Part I*, volume 13940 of *Lecture Notes in Computer Science*, pages 114–144. Springer, 2023. doi:10.1007/978-3-031-31368-4_5.

[HM24] Kathrin Hövelmanns and Christian Majenz. A note on failing gracefully: Completing the picture for explicitly rejecting fujisaki-okamoto transforms using worst-case correctness. In Markku-Juhani O. Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part II*, volume 14772 of *Lecture Notes in Computer Science*, pages 245–265. Springer, 2024. doi:10.1007/978-3-031-62746-0_11.

[HPA21] James Howe, Thomas Prest, and Daniel Apon. Sok: How (not) to design and implement post-quantum cryptography. In Kenneth G. Paterson, editor, *Topics in Cryptology - CT-RSA 2021 - Cryptographers' Track at the RSA Conference 2021, Virtual Event, May 17-20, 2021, Proceedings*, volume 12704 of *Lecture Notes in Computer Science*, pages 444–477. Springer, 2021. doi:10.1007/978-3-030-75539-3_19.

[HR10] Feng Hao and Peter Y. A. Ryan. J-PAKE: authenticated key exchange without PKI. *Trans. Comput. Sci.*, 11:192–206, 2010. doi:10.1007/978-3-642-17697-5_10.

[HR25] Julia Hesse and Michael Rosenberg. PAKE combiners and efficient post-quantum instantiations. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 395–420. Springer, 2025. doi:10.1007/978-3-031-91124-8_14.

[HS14] Feng Hao and Siamak Fayyaz Shahandashti. The SPEKE protocol revisited. In Liqun Chen and Chris J. Mitchell, editors, *Security Standardisation Research - First International Conference, SSR 2014, London, UK, December 16-17, 2014. Proceedings*, volume 8893 of *Lecture Notes in Computer Science*, pages 26–38. Springer, 2014. doi:10.1007/978-3-319-14054-4_2.

[HTTY24] Shuya Hanai, Keisuke Tanaka, Masayuki Tezuka, and Yusuke Yoshida. Universally composable relaxed asymmetric password-authenticated key exchange. In Clemente Galdi and Duong Hieu Phan, editors, *Security and Cryptography for Networks - 14th International Conference, SCN 2024, Amalfi, Italy, September 11-13, 2024, Proceedings, Part II*, volume 14974 of *Lecture Notes in Computer Science*, pages 272–293. Springer, 2024. doi:10.1007/978-3-031-71073-5_13.

[HV22] Loïs Huguenin-Dumittan and Serge Vaudenay. On ind-qcca security in the ROM and its applications - CPA security is sufficient for TLS 1.3. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 613–642. Springer, 2022. doi:10.1007/978-3-031-07082-2_22.

[HvO22] Feng Hao and Paul C. van Oorschot. Sok: Password-authenticated key exchange - theory, practice, standardization and real-world lessons. In Yuji Suga, Kouichi Sakurai, Xuhua Ding, and Kazue Sako, editors, *ASIA CCS '22: ACM Asia Conference on Computer and Communications Security, Nagasaki, Japan, 30 May 2022 - 3 June 2022*, pages 697–711. ACM, 2022. doi:10.1145/3488932.3523256.

[HXL+23] Yunxia Han, Chunxiang Xu, Shanshan Li, Changsong Jiang, and Kefei Chen. ttpake: Typo tolerance password-authenticated key exchange. *J. Inf. Secur. Appl.*, 79:103658, 2023. URL: https://doi.org/10.1016/j.jisa.2023.103658, doi:10.1016/J.JISA.2023.103658.

[HY18] Akinori Hosoyamada and Kan Yasuda. Building quantum-one-way functions from block ciphers: Davies-meyer and merkle-damgård constructions. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 275–304. Springer, 2018. doi:10.1007/978-3-030-03326-2_10.

[IB21] SK Hafizul Islam and Swagatam Basu. PB-3PAKA: password-based three-party authenticated key agreement protocol for mobile devices in post-quantum environments. *J. Inf. Secur. Appl.*, 63:103026, 2021. URL: https://doi.org/10.1016/j.jisa.2021.103026, doi:10.1016/J.JISA.2021.103026.

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

[ISO17] ISO/IEC. Part 4: Mechanisms based on weak secrets, 2017. URL: https://www.iso.org/standard/67933.html.

[Jab96] David P. Jablon. Strong password-only authenticated key exchange. *Comput. Commun. Rev.*, 26(5):5–26, 1996. doi:10.1145/242896.242897.

[Jab01] David P. Jablon. Password authentication using multiple servers. In David Naccache, editor, *Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings*, volume 2020 of *Lecture Notes in Computer Science*, pages 344–360. Springer, 2001. doi:10.1007/3-540-45353-9_26.

[Jar22] Stanislaw Jarecki. Password Authenticated Key Exchange: Protocols and Security Models. *Asymmetric Cryptography: Primitives and Protocols*, 2022. URL: http://dx.doi.org/10.1002/9781394188369.ch10, doi:10.1002/9781394188369.ch10.

[JD25] Pratima Jana and Ratna Dutta. Quantum-safe identity-binding password authenticated key exchange protocols. Cryptology ePrint Archive, Paper 2025/2107, 2025. URL: https://eprint.iacr.org/2025/2107.

[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 Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part I*, volume 12110 of *Lecture Notes in Computer Science*, pages 396–427. Springer, 2020. doi:10.1007/978-3-030-45374-9_14.

[JKK14] Stanislaw Jarecki, Aggelos Kiayias, and Hugo Krawczyk. Round-optimal password-protected secret sharing and T-PAKE in the password-only model. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 233–253. Springer, 2014. doi:10.1007/978-3-662-45608-8_13.

[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 *IEEE European Symposium on Security and Privacy, EuroS&P 2016, Saarbrücken, Germany, March 21-24, 2016*, pages 276–291. IEEE, 2016. URL: https://doi.org/10.1109/EuroSP.2016.30, doi:10.1109/EUROSP.2016.30.

[JKX18] Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu. OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 456–486. Springer, 2018. doi:10.1007/978-3-319-78372-7_15.

[JMV01] Don Johnson, Alfred Menezes, and Scott A. Vanstone. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Sec.*, 1(1):36–63, 2001. URL: https://doi.org/10.1007/s102070100002, doi:10.1007/S102070100002.

[JMZ23] Haodong Jiang, Zhi Ma, and Zhenfeng Zhang. Post-quantum security of key encapsulation mechanism against CCA attacks with a single decapsulation query. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part IV*, volume 14441 of *Lecture Notes in Computer Science*, pages 434–468. Springer, 2023. doi:10.1007/978-981-99-8730-6_14.

[JRX25] Jake Januzelli, Lawrence Roy, and Jiayu Xu. Under what conditions is encrypted key exchange actually secure? In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 451–481. Springer, 2025. doi:10.1007/978-3-031-91124-8_16.

[JTCW17] Yi-Siou Jheng, Raylin Tso, Chien-Ming Chen, and Mu-En Wu. Password-based authenticated key exchange from lattices for client/server model. In James J. Park, Vincenzo Loia, Gangman Yi, and Yunsick Sung, editors, *Advances in Computer Science and Ubiquitous Computing - CSA/CUTE 2017, Taichung, Taiwan, 18-20 December*, volume 474 of *Lecture Notes in Electrical Engineering*, pages 315–319. Springer, 2017. doi:10.1007/978-981-10-7605-3_52.

[JZ17] Zhengzhong Jin and Yunlei Zhao. Optimal key consensus in presence of noise. *IACR Cryptol. ePrint Arch.*, 2017:1058, 2017. URL: http://eprint.iacr.org/2017/1058.

[KC07] Barbara Kitchenham and Stuart Charters. Guidelines for performing systematic literature reviews in software engineering, 2007.

[KCM25] Novak Kaluderovic, Nan Cheng, and Aikaterini Mitrokotsa. A post-quantum distributed OPRF from the legendre PRF. In Vincent Nicomette, Abdelmalek Benzekri, Nora Boulahia-Cuppens, and Jaideep Vaidya, editors, *Computer Security - ESORICS 2025 - 30th European Symposium on Research in Computer Security, Toulouse, France, September 22-24, 2025, Proceedings, Part II*, volume 16054 of *Lecture Notes in Computer Science*, pages 205–225. Springer, 2025. doi:10.1007/978-3-032-07891-9_11.

[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. *Trans. Emerg. Telecommun. Technol.*, 34(1), 2023. URL: https://doi.org/10.1002/ett.4660, doi:10.1002/ETT.4660.

[KKZZ14] Jonathan Katz, Aggelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas. Distributing the setup in universally composable multi-party computation. In Magnús M. Halldórsson and Shlomi Dolev, editors, *ACM Symposium on Principles of Distributed Computing, PODC '14, Paris, France, July 15-18, 2014*, pages 20–29. ACM, 2014. doi:10.1145/2611462.2611480.

[KM15] Franziskus Kiefer and Mark Manulis. Oblivious PAKE: efficient handling of password trials. In Javier López and Chris J. Mitchell, editors, *Information Security - 18th International Conference, ISC 2015, Trondheim, Norway, September 9-11, 2015, Proceedings*, volume 9290 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2015. doi:10.1007/978-3-319-23318-5_11.

[KMM+26] Yashvanth Kondi, Ian McQuoid, Kelsey Melissaris, Claudio Orlandi, Lawrence Roy, and LaKyah Tyner. Onetwopake: Two-round strong asymmetric PAKE with ideal security, 2026. doi:10.1007/978-3-032-25317-0_10.

[KMP+17] Vladimir Kolesnikov, Naor Matania, Benny Pinkas, Mike Rosulek, and Ni Trieu. Practical multi-party private set intersection from symmetric-key techniques. In Bhavani Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1257–1272. ACM, 2017. doi:10.1145/3133956.3134065.

[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 Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*, pages 475–494. Springer, 2001. doi:10.1007/3-540-44987-6_29.

[KR24] Jonathan Katz and Michael Rosenberg. LATKE: A framework for constructing identity-binding pakes. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part II*, volume 14921 of *Lecture Notes in Computer Science*, pages 218–250. Springer, 2024. doi:10.1007/978-3-031-68379-4_7.

[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. In Deukjo Hong, editor, *Information Security and Cryptology - ICISC 2020 - 23rd International Conference, Seoul, South Korea, December 2-4, 2020, Proceedings*, volume 12593 of *Lecture Notes in Computer Science*, pages 58–84. Springer, 2020. doi:10.1007/978-3-030-68890-5_4.

[KV09] Jonathan Katz and Vinod Vaikuntanathan. Smooth projective hashing and password-based authenticated key exchange from lattices. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *Lecture Notes in Computer Science*, pages 636–652. Springer, 2009. doi:10.1007/978-3-642-10366-7_37.

[KX25] Naman Kumar and Jiayu Xu. On the UC-(in)security of PAKE protocols without the random oracle model. Cryptology ePrint Archive, Paper 2025/998, 2025. URL: https://eprint.iacr.org/2025/998.

[LL25] You Lyu and Shengli Liu. Hybrid password authentication key exchange in the UC framework. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 421–450. Springer, 2025. doi:10.1007/978-3-031-91124-8_15.

[LLH24a] You Lyu, Shengli Liu, and Shuai Han. Efficient asymmetric PAKE compiler from KEM and AE. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part V*, volume 15488 of *Lecture Notes in Computer Science*, pages 34–65. Springer, 2024. doi:10.1007/978-981-96-0935-2_2.

[LLH24b] You Lyu, Shengli Liu, and Shuai Han. Universal composable password authenticated key exchange for the post-quantum world. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*, volume 14656 of *Lecture Notes in Computer Science*, pages 120–150. Springer, 2024. doi:10.1007/978-3-031-58754-2_5.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010. doi:10.1007/978-3-642-13190-5_1.

[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 Mark Manulis, Ahmad-Reza Sadeghi, and Steve A. Schneider, editors, *Applied Cryptography and Network Security - 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings*, volume 9696 of *Lecture Notes in Computer Science*, pages 58–76. Springer, 2016. doi:10.1007/978-3-319-39555-5_4.

[LW18] Zengpeng Li and Ding Wang. Two-round PAKE protocol over lattices without NIZK. In Fuchun Guo, Xinyi Huang, and Moti Yung, editors, *Information Security and Cryptology - 14th International Conference, Inscrypt 2018, Fuzhou, China, December 14-17, 2018, Revised Selected Papers*, volume 11449 of *Lecture Notes in Computer Science*, pages 138–159. Springer, 2018. doi:10.1007/978-3-030-14234-6_8.

[LW22] Zengpeng Li and Ding Wang. Achieving one-round password-based authenticated key exchange over lattices. *IEEE Trans. Serv. Comput.*, 15(1):308–321, 2022. doi:10.1109/TSC.2019.2939836.

[LWC+25] Jiahao Liu, Yi Wang, Rongmao Chen, Xinyi Huang, Jinshu Su, and Moti Yung. Universally composable subversion-resilient authenticated key exchange. In Goichiro Hanaoka and Bo-Yin Yang, editors, *Advances in Cryptology - ASIACRYPT 2025 - 31st International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, VIC, Australia, December 8-12, 2025, Proceedings, Part II*, volume 16246 of *Lecture Notes in Computer Science*, pages 103–136. Springer, 2025. doi:10.1007/978-981-95-5096-8_4.

[LWL23] Wenting Li, Ping Wang, and Kaitai Liang. HPAKE: honey password-authenticated key exchange for fast and safer online authentication. *IEEE Trans. Inf. Forensics Secur.*, 18:1596–1609, 2023. doi:10.1109/TIFS.2022.3214729.

[LWM22] Zengpeng Li, Ding Wang, and Eduardo Morais. Quantum-safe round-optimal password authentication for mobile devices. *IEEE Trans. Dependable Secur. Comput.*, 19(3):1885–1899, 2022. doi:10.1109/TDSC.2020.3040776.

[LZJY19] Chao Liu, Zhongxiang Zheng, Keting Jia, and Qidi You. Provably secure three-party password-based authenticated key exchange from RLWE. In Swee-Huay Heng and Javier López, editors, *Information Security Practice and Experience - 15th International Conference, ISPEC 2019, Kuala Lumpur, Malaysia, November 26-28, 2019, Proceedings*, volume 11879 of *Lecture Notes in Computer Science*, pages 56–72. Springer, 2019. doi:10.1007/978-3-030-34339-2_4.

[Mac02] Philip D. MacKenzie. The PAK suite: Protocols for password-authenticated key exchange. Contributions to IEEE P1363.2, 2002.

[MMW25] Christian Majenz, Giulio Malavolta, and Michael Walter. Permutation superposition oracles for quantum query lower bounds. In Michal Koucký and Nikhil Bansal, editors, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 1508–1519. ACM, 2025. doi:10.1145/3717823.3718266.

[MRR20] Ian McQuoid, Mike Rosulek, and Lawrence Roy. Minimal symmetric PAKE and 1-out-of-n OT from programmable-once public functions. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*, pages 425–442. ACM, 2020. doi:10.1145/3372297.3417870.

[MRX25] Ian McQuoid, Mike Rosulek, and Jiayu Xu. How to tolerate typos in strong asymmetric PAKE. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part III*, volume 16002 of *Lecture Notes in Computer Science*, pages 610–641. Springer, 2025. doi:10.1007/978-3-032-01881-6_19.

[MW25] Arthur Herlédan Le Merdy and Benjamin Wesolowski. Unconditional foundations for supersingular isogeny-based cryptography. In Benny Applebaum and Huijia (Rachel) Lin, editors, *Theory of Cryptography - 23rd International Conference, TCC 2025, Aarhus, Denmark, December 1-5, 2025, Proceedings, Part III*, volume 16270 of *Lecture Notes in Computer Science*, pages 266–297. Springer, 2025. doi:10.1007/978-3-032-12296-4_9.

[MX23a] Varun Maram and Keita Xagawa. Post-quantum anonymity of kyber. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *Public-Key Cryptography - PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7-10, 2023, Proceedings, Part I*, volume 13940 of *Lecture Notes in Computer Science*, pages 3–35. Springer, 2023. doi:10.1007/978-3-031-31368-4_1.

[MX23b] Ian McQuoid and Jiayu Xu. An efficient strong asymmetric PAKE compiler instantiable from group actions. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part VIII*, volume 14445 of *Lecture Notes in Computer Science*, pages 176–207. Springer, 2023. doi:10.1007/978-981-99-8742-9_6.

[Nio25] Guilhem Niot. Practical deniable post-quantum X3DH: A lightweight split-kem for k-waay. In *Proceedings of the 20th ACM Asia Conference on Computer*

and Communications Security, ASIA CCS 2025, Hanoi, Vietnam, August 25-29, 2025, pages 298–312. ACM, 2025. doi:10.1145/3708821.3736192.

[NR04] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM*, 51(2):231–262, 2004. doi:10.1145/972639.972643.

[Ott24] Johannes Ottenhues. An overview of symmetric fuzzy PAKE protocols. In Steffen Wendzel, Christian Wressnegger, Laura Hartmann, Felix C. Freiling, Frederik Armknecht, and Lena Reinfelder, editors, *Sicherheit, Schutz und Zuverlässigkeit: Konferenzband der 12. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Sicherheit 2024, Worms, Germany, April 9-11, 2024*, volume P-345 of *LNI*, pages 75–89. Gesellschaft für Informatik e.V., 2024. URL: https://doi.org/10.18420/sicherheit2024_005, doi:10.18420/SICHERHEIT2024_005.

[Pei14] Chris Peikert. Lattice cryptography for the internet. In Michele Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings*, volume 8772 of *Lecture Notes in Computer Science*, pages 197–219. Springer, 2014. doi:10.1007/978-3-319-11659-4_12.

[PPY+24] Congrong Peng, Cong Peng, Xiaolin Yang, Qingcai Luo, and Min Luo. Isogeny-based password-authenticated key exchange based on shuffle algorithm. In Zhe Xia and Jiageng Chen, editors, *Information Security Practice and Experience - 19th International Conference, ISPEC 2024, Wuhan, China, October 25-27, 2024, Proceedings*, volume 15053 of *Lecture Notes in Computer Science*, pages 112–132. Springer, 2024. doi:10.1007/978-981-97-9053-1_7.

[PZ23] Jiaxin Pan and Runzhi Zeng. A generic construction of tightly secure password-based authenticated key exchange. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part VIII*, volume 14445 of *Lecture Notes in Computer Science*, pages 143–175. Springer, 2023. doi:10.1007/978-981-99-8742-9_5.

[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 Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 131–141. Springer, 2006. doi:10.1007/11818175_8.

[Reg10] Oded Regev. The learning with errors problem (invited survey). In *Proceedings of the 25th Annual IEEE Conference on Computational Complexity, CCC 2010, Cambridge, Massachusetts, USA, June 9-12, 2010*, pages 191–204. IEEE Computer Society, 2010. doi:10.1109/CCC.2010.26.

[RG03] Mario Di Raimondo and Rosario Gennaro. Provably secure threshold password-authenticated key exchange. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications*

of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings, volume 2656 of *Lecture Notes in Computer Science*, pages 507–523. Springer, 2003. doi:10.1007/3-540-39200-9_32.

[RG21] Peixin Ren and Xiaozhuo Gu. Practical post-quantum password-authenticated key exchange based-on module-lattice. In Jong Hwan Park and Seung-Hyun Seo, editors, *Information Security and Cryptology - ICISC 2021 - 24th International Conference, Seoul, South Korea, December 1-3, 2021, Revised Selected Papers*, volume 13218 of *Lecture Notes in Computer Science*, pages 137–156. Springer, 2021. doi:10.1007/978-3-031-08896-4_7.

[RGW23] Peixin Ren, Xiaozhuo Gu, and Ziliang Wang. Efficient module learning with errors-based post-quantum password-authenticated key exchange. *IET Inf. Secur.*, 17(1):3–17, 2023. URL: https://doi.org/10.1049/ise2.12094, doi:10.1049/ISE2.12094.

[RHCB22] Prasanna Ravi, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. Lattice-based key-sharing schemes: A survey. *ACM Comput. Surv.*, 54(1):9:1–9:39, 2022. doi:10.1145/3422178.

[Ros21] Ansis Rosmanis. Tight bounds for inverting permutations via compressed oracle arguments. *arXiv preprint arXiv:2103.08975*, 2021.

[RRX26] David Richardson, Mike Rosulek, and Jiayu Xu. Conditionally input-revealing 2pc and fuzzy password-authenticated key exchange. In *Advances in Cryptology - EUROCRYPT 2026 - 45th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Rome, Italy, May 10-14, 2026, Proceedings, Part II*, volume 16542 of *Lecture Notes in Computer Science*, pages 468–498. Springer, 2026. doi:10.1007/978-3-032-25317-0_16.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978. doi:10.1145/359340.359342.

[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. *J. Inf. Secur. Appl.*, 75:103505, 2023. URL: https://doi.org/10.1016/j.jisa.2023.103505, doi:10.1016/J.JISA.2023.103505.

[SA23] Kübra Seyhan and Sedat Akleylek. A new password-authenticated module learning with rounding-based key exchange protocol: Saber.pake. *J. Supercomput.*, 79(16):17859–17896, 2023. URL: https://doi.org/10.1007/s11227-023-05251-x, doi:10.1007/S11227-023-05251-X.

[SA24] Kübra Seyhan and Sedat Akleylek. A new lattice-based password authenticated key exchange scheme with anonymity and reusable key. *PeerJ Comput. Sci.*, 10:e1791, 2024. URL: https://doi.org/10.7717/peerj-cs.1791, doi:10.7717/PEERJ-CS.1791.

[Sch91] Claus-Peter Schnorr. Efficient signature generation by smart cards. *J. Cryptol.*, 4(3):161–174, 1991. doi:10.1007/BF00196725.

[Sch24] Sophie Schmieg. Unbindable kemmy schmidt: ML-KEM is neither MAL-BIND-k-CT nor MAL-BIND-k-PK. Cryptology ePrint Archive, Paper 2024/523, 2024. URL: https://eprint.iacr.org/2024/523.

[SGD23] Yunfan Song, Songhui Guo, and Ruiyang Ding. Anonymous password-authenticated key exchange protocol based on lattice. In *2023 2nd International Conference on Big Data, Information and Computer Network (BDICN)*, 2023. doi:10.1109/BDICN58493.2023.00078.

[SGJ23] Bruno Freitas Dos Santos, Yanqi Gu, and Stanislaw Jarecki. Randomized half-ideal cipher on groups with applications to UC (a)pake. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 128–156. Springer, 2023. doi:10.1007/978-3-031-30589-4_5.

[SGJK22] Bruno Freitas Dos Santos, Yanqi Gu, Stanislaw Jarecki, and Hugo Krawczyk. Asymmetric PAKE with low computation and communication. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part II*, volume 13276 of *Lecture Notes in Computer Science*, pages 127–156. Springer, 2022. doi:10.1007/978-3-031-07085-3_5.

[SHB25] István András Seres, Máté Horváth, and Péter Burcsi. The legendre pseudorandom function as a multivariate quadratic cryptosystem: security and applications. *Appl. Algebra Eng. Commun. Comput.*, 36(2):223–253, 2025. URL: https://doi.org/10.1007/s00200-023-00599-2, doi:10.1007/S00200-023-00599-2.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. doi:10.1137/S0097539795293172.

[SM16] Douglas Stebila and Michele Mosca. Post-quantum key exchange for the internet and the open quantum safe project. In Roberto Avanzi and Howard M. Heys, editors, *Selected Areas in Cryptography - SAC 2016 - 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers*, volume 10532 of *Lecture Notes in Computer Science*, pages 14–37. Springer, 2016. doi:10.1007/978-3-319-69453-5_2.

[SM25] Mohammad Reza Saeidi and Hamid Mala. Post-quantum anonymous password authenticated key exchange with indirect public key validation. *J. Supercomput.*, 81(14):1325, 2025. URL: https://doi.org/10.1007/s11227-025-07793-8, doi:10.1007/S11227-025-07793-8.

[Smi18] Benjamin Smith. Pre- and post-quantum diffie-hellman from groups, actions, and isogenies. In Lilya Budaghyan and Francisco Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields - 7th International Workshop, WAIFI 2018, Bergen, Norway, June 14-16, 2018, Revised Selected Papers*, volume 11321 of *Lecture Notes in Computer Science*, pages 3–40. Springer, 2018. doi:10.1007/978-3-030-05153-2_1.

[SS19] Shingo Sato and Junji Shikata. SO-CCA secure PKE in the quantum random oracle model or the quantum ideal cipher model. In Martin Albrecht, editor, *Cryptography and Coding - 17th IMA International Conference, IMACC 2019, Oxford, UK, December 16-18, 2019, Proceedings*, volume 11929 of *Lecture Notes in Computer Science*, pages 317–341. Springer, 2019. doi:10.1007/978-3-030-35199-1_16.

[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 Gene Tsudik, Mauro Conti, Kaitai Liang, and Georgios Smaragdakis, editors, *Computer Security - ESORICS 2023 - 28th European Symposium on Research in Computer Security, The Hague, The Netherlands, September 25-29, 2023, Proceedings, Part I*, volume 14344 of *Lecture Notes in Computer Science*, pages 168–188. Springer, 2023. doi:10.1007/978-3-031-50594-2_9.

[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. URL: http://dx.doi.org/10.1155/2021/6952869, doi:10.1155/2021/6952869.

[TSJL21] Oleg Taraskin, Vladimir Soukharev, David Jao, and Jason T. LeGrow. Towards isogeny-based password-authenticated key establishment. *J. Math. Cryptol.*, 15(1):18–30, 2021. URL: https://doi.org/10.1515/jmc-2020-0071, doi:10.1515/JMC-2020-0071.

[Tue13] Max Tuengerthal. *Analysis of real-world security protocols in a universal composability framework*. Berlin : Logos-Verl., 2013. URL: https://d-nb.info/1037219570.

[TY19] Shintaro Terada and Kazuki Yoneyama. Password-based authenticated key exchange from standard isogeny assumptions. In Ron Steinfeld and Tsz Hon Yuen, editors, *Provable Security - 13th International Conference, ProvSec 2019, Cairns, QLD, Australia, October 1-4, 2019, Proceedings*, volume 11821 of *Lecture Notes in Computer Science*, pages 41–56. Springer, 2019. doi:10.1007/978-3-030-31919-9_3.

[Unr21] Dominique Unruh. Compressed permutation oracles (and the collision-resistance of sponge/SHA3). Cryptology ePrint Archive, Paper 2021/062, 2021. URL: https://eprint.iacr.org/2021/062.

[Unr23] Dominique Unruh. Towards compressed permutation oracles. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part IV*, volume 14441 of *Lecture Notes in Computer Science*, pages 369–400. Springer, 2023. doi:10.1007/978-981-99-8730-6_12.

[VHLL26] Yasmine Vazirinejad, Feng Hao, You Lyu, and Shengli Liu. Universally composable hybrid PAKE secure against harvest-now-decrypt-later attacks. Cryptology ePrint Archive, Paper 2026/1832, 2026. URL: https://eprint.iacr.org/2026/1832.

[VJW25a] Jelle Vos, Stanislaw Jarecki, and Christopher A. Wood. Hybrid post-quantum password authenticated key exchange. Internet-Draft: draft-vos-cfrg-pqpake-00, 2025. https://datatracker.ietf.org/doc/draft-vos-cfrg-pqpake/.

[VJW+25b] Jelle Vos, Stanislaw Jarecki, Christopher A. Wood, Cathie Yun, Steve Myers, and Yannick Sierra. A hybrid asymmetric password-authenticated key exchange in the random oracle model. Cryptology ePrint Archive, Paper 2025/1343, 2025. URL: https://eprint.iacr.org/2025/1343.

[VR20] Mathy Vanhoef and Eyal Ronen. Dragonblood: Analyzing the dragonfly handshake of WPA3 and eap-pwd. In *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*, pages 517–533. IEEE, 2020. doi:10.1109/SP40000.2020.00031.

[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. URL: http://dx.doi.org/10.1007/978-3-031-30623-5_3, doi:10.1007/978-3-031-30623-5_3.

[WHC+21] Mei Wang, Kun He, Jing Chen, Zengpeng Li, Wei Zhao, and Ruiying Du. Biometrics-authenticated key exchange for secure messaging. In Yongdae Kim, Jong Kim, Giovanni Vigna, and Elaine Shi, editors, *CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*, pages 2618–2631. ACM, 2021. doi:10.1145/3460120.3484746.

[Wu98] Thomas D. Wu. The secure remote password protocol, 1998. URL: https://www.ndss-symposium.org/ndss1998/secure-remote-password-protocol/.

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

[WW14] Huixin Wu and Feng Wang. A survey of noninteractive zero knowledge proof system and its applications. *The scientific world journal*, 2014(1):1–7, 2014. URL: http://dx.doi.org/10.1155/2014/560484, doi:10.1155/2014/560484.

[Xag22] Keita Xagawa. Anonymity of NIST PQC round 3 kems. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 551–581. Springer, 2022. doi:10.1007/978-3-031-07082-2_20.

[XG22] Haodong Xie and Yuanbo Guo. Two-round three-party pake protocol over lattices. In *EMIE 2022; The 2nd International Conference on Electronic Materials and Information Engineering*, 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.

[Xu26a] Jiayu Xu. Does the uc-security notion for PAKE imply game-based security?, 2026. URL: https://doi.org/10.62056/anjby76bm, doi:10.62056/ANJBY76BM.

[Xu26b] Jiayu Xu. The most efficient protocol for PAKE: What exact stuff do you need to hash at the end? Cryptology ePrint Archive, Paper 2026/1331, 2026. URL: https://eprint.iacr.org/2026/1331.

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

[YBH+25] Yibin Yang, Fabrice Benhamouda, Shai Halevi, Hugo Krawczyk, and Tal Rabin. Gold OPRF: post-quantum oblivious power-residue PRF. In Marina Blanton, William Enck, and Cristina Nita-Rotaru, editors, *IEEE Symposium on Security and Privacy, SP 2025, San Francisco, CA, USA, May 12-15, 2025*, pages 259–278. IEEE, 2025. doi:10.1109/SP61157.2025.00116.

[YGS+20] Anqi Yin, Yuanbo Guo, Yuanming Song, Tongzhou Qu, and Chen Fang. Two-round password-based authenticated key exchange from lattices. *Wirel. Commun. Mob. Comput.*, 2020:8893628:1–8893628:13, 2020. doi:10.1155/2020/8893628.

[YGWX19] Yingshan Yang, Xiaozhuo Gu, Bin Wang, and Taizhong Xu. Efficient password-authenticated key exchange from RLWE based on asymmetric key consensus. In Zhe Liu and Moti Yung, editors, *Information Security and Cryptology - 15th International Conference, Inscrypt 2019, Nanjing, China, December 6-8, 2019, Revised Selected Papers*, volume 12020 of *Lecture Notes in Computer Science*, pages 31–49. Springer, 2019. doi:10.1007/978-3-030-42921-8_2.

[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*, 6, 2013. URL: http://dx.doi.org/10.3724/sp.j.1146.2012.01135, doi:10.3724/sp.j.1146.2012.01135.

[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, 2021. URL: https://doi.org/10.1016/bs.adcom.2020.09.003, doi:10.1016/BS.ADCOM.2020.09.003.

[YSG25] Yeming Yang, Shuaichao Song, and Songhui Guo. Two-server password authenticated key exchange protocol based on mlwe. In *Proceedings of the 2025 4th International Conference on Cryptography, Network Security and Communication Technology*, CNSCT '25, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3723890.3723901.

[YZ21] Takashi Yamakawa and Mark Zhandry. Classical vs quantum random oracles. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 568–597. Springer, 2021. doi:10.1007/978-3-030-77886-6_20.

[YZYW25] Yatao Yang, Ruoyan Zhao, Fangrui Yin, and Ke Wang. K-PAKE: post quantum password authentication key exchange protocol for satellite networks. *Clust. Comput.*, 28(4):223, 2025. URL: https://doi.org/10.1007/s10586-024-04942-1, doi:10.1007/S10586-024-04942-1.

[ZG17] Hongfeng Zhu and Shuai Geng. Simple and universal construction for round-optimal password authenticated key exchange towards quantum-resistant. *J. Inf. Hiding Multim. Signal Process.*, 8(4):798–807, 2017. URL: http://bit.kuas.edu.tw/%7Ejihmsp/2017/vol8/JIH-MSP-2017-04-005.pdf.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 239–268. Springer, 2019. doi:10.1007/978-3-030-26951-7_9.

[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.*, 5(4):672–689, 2014. URL: http://bit.kuas.edu.tw/%7Ejihmsp/2014/vol5/JIH-MSP-2014-04-009.pdf.

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

[ZWCW22] Hongfeng Zhu, Xintong Wang, Yeh-Cheng Chen, and Xueying Wang. Security analysis and improvements of a universal construction for a round-optimal password authenticated key exchange protocol. *Int. J. Inf. Comput. Secur.*, 17(1/2):104–118, 2022. doi:10.1504/IJICS.2022.121293.

[ZY17] Jiang Zhang and Yu Yu. Two-round PAKE from approximate SPH and instantiations from lattices. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*, volume 10626 of *Lecture Notes in Computer Science*, pages 37–67. Springer, 2017. doi:10.1007/978-3-319-70700-6_2.

[ZYL+24] 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 Things J.*, 11(3):5118–5128, 2024. doi:10.1109/JIOT.2023.3302620.

A Converted Benchmarking Results

Table 9: Original Cycle Counts of [TSJL21] and [YGWX19]

Class	PAKE			Security		Computational Cost			Communication Cost		
	Publication	Platform	Variant	Classic	Quantum	Client	Server	Total	Client	Server	Total
Balanced											
C2	Taraskin et al. [TSJL21]	Intel Core i5-8250U @ 1.6GHz	p434	-	-	-	-	142×10^6c	-	-	-
			p503	-	-	-	-	228×10^6c	-	-	-
	Yang et al. [YGWX19]	Intel Core i7-8550U @ 1.8GHz	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

B PQC OPAQUE Adaptation Draft (Not Verified)

We suggest implementing a KEM-based PQC OPAQUE adaptation for a user U and a server S as follows.

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 PQC OPAQUE 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., with an AE), 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 programming in the QROM. Last but not least, the used KEX or KEM must provide PFS and key-compromise impersonation (KCI) security. Nevertheless, an open question remains in finding a mechanism 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 Hash to Curve (H2C) function to map a password to an EC base generator, it seems intuitive to resort to its adaptation to H2G settings, which can be directly obtained from isogenies (cf. [HHM+24]) or 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, 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 (or similar), which differs 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 basis matrix) to generate a public key. A more suitable solution would be to use the OPRF secret as the deterministic seed that is otherwise usually sampled within the KEM key generation routine. Another approach might be found in using a PQC NIKE, e.g., SWOOSH [GdKQ+24], which enables a white-box key generation routine, while also maintaining the non-interactive characteristics of a KEM. We consider finding a solution an open question for future work.