Related Work: Post-Quantum Password-Authenticated Key Exchange Using Lattice-Based Cryptography

Sanjay Malla
U27001010
sanjaymalla@usf.edu

***Abstract*—Password-authenticated key exchange (PAKE) protocols are foundational for establishing secure communication based on human-memorable secrets. With the emergence of quantum computing, classical cryptographic assumptions (e.g., Diffie-Hellman) are becoming obsolete. This work explores the evolution of PAKE protocols and examines how lattice-based assumptions—particularly Ring-LWE and Module-LWE—enable quantum-resilient constructions. We analyze over thirty works to understand current advancements, reconciliation techniques, and hybrid strategies, concluding with the gaps our research aims to fill.**

Introduction and Background

Password-authenticated key exchange (PAKE) protocols have long served as secure methods for establishing session keys between parties sharing only a low-entropy secret—typically a password. Classical protocols such as Encrypted Key Exchange (EKE) [1], SPEKE [2], SRP [3], and the more modern OPAQUE [4] rely on number-theoretic assumptions like the discrete logarithm problem and RSA. These protocols are well-studied and have undergone extensive formal analysis, offering resistance to offline dictionary attacks and ensuring security even when passwords are weak.

However, these assumptions crumble under the capabilities of quantum computing. Shor's algorithm [5] renders discrete log- and factoring-based cryptography insecure, making it imperative to explore alternatives. This motivates the need for post-quantum cryptography (PQC), where security stems from problems believed to be hard even for quantum adversaries.

Lattice-based cryptography is one of the most promising approaches in this domain. The Learning With Errors (LWE) problem, introduced by Regev [6], forms a foundation for many quantum-resistant primitives. Its structured variants—Ring-LWE and Module-LWE—enhance computational efficiency and reduce key sizes while maintaining strong security guarantees. Ring-LWE [7] operates over polynomial rings, offering compact representations and fast arithmetic, but at the potential cost of introducing exploitable algebraic structure. Module-LWE [8] generalizes both LWE and Ring-LWE, striking a balance between structure and hardness, and is the basis of standardized schemes like CRYSTALS-Kyber [9].

The security of these lattice-based constructions stems from reductions to worst-case lattice problems such as Gap Shortest Vector Problem (GapSVP) and Shortest Independent Vectors Problem (SIVP), believed to be intractable even for quantum machines. These problems also benefit from worst-to-average-case reductions, providing a compelling theoretical underpinning that few other hardness assumptions can match.

In the context of PAKE, adopting lattice-based assumptions ensures that even with an active, quantum-capable adversary, session keys remain safe and password secrecy is preserved. While early research in this space focused on general key exchange, recent studies have developed dedicated PAKE protocols leveraging RLWE and MLWE [10]–[13].

Our work is informed by these developments and contributes a PAKE protocol that leverages both Ring-LWE and Module-LWE instantiations, targeting both theoretical robustness and practical implementability. By doing so, we aim to bridge the gap between formal cryptographic proof and real-world deployment. This section has provided the historical and technical foundation upon which the remainder of this related work survey will build.

Lattice-Based PAKE Schemes

Lattice-based PAKE (Password-Authenticated Key Exchange) schemes aim to provide quantum-resistant authentication protocols by leveraging the hardness of lattice problems. The pioneering work in this area was introduced by Ding et al. [10], who constructed one of the earliest PAKE protocols based on the Ring-LWE assumption. Their scheme utilized commitment and error reconciliation mechanisms to securely exchange keys over a public channel, demonstrating that PAKEs could be feasibly constructed in a post-quantum setting.

Since then, a growing number of studies have expanded on Ding's construction. Li et al. [11] presented a round-optimal two-party MLWE-based PAKE in the standard model, focusing on minimizing communication rounds while retaining strong security guarantees. Liu et al. [12] developed a three-party authenticated key exchange (3PAKE) based on RLWE, which supports secure multi-party communication in scenarios like group chats or collaborative computing. Their approach showcases the adaptability of lattice-based assumptions to more complex interaction models.

Further contributions have addressed specific use cases and enhancements. For example, Islam and Basu [13] designed a lattice-based 3PAKE tailored for mobile networks, prioritizing lightweight computation and minimal bandwidth—essential features in constrained environments. Jiang et al. [14] proposed a framework dubbed "Pakes," which abstracts PAKE protocol design into a set of primitives that can be instantiated with various lattice-based assumptions. Their generic framework enables modular reasoning and reuse across multiple cryptographic scenarios.

Additionally, Ding et al. [15] and collaborators introduced reusable key PAKEs, enabling multiple sessions from a single key setup without compromising password secrecy. This is especially important in resource-constrained environments like IoT, where key regeneration can be expensive. Dabra et al. [16] explored anonymity-preserving PAKE constructions in a lattice-based setting, laying the foundation for privacy-preserving authentication mechanisms in adversarial environments.

Despite these advances, a common drawback in many of these studies is the lack of publicly available, optimized implementations. The majority of protocols remain theoretical or are implemented as proof-of-concept in custom, unoptimized environments. Furthermore, not all proposals are accompanied by formal security proofs under established models like UC or the real-or-random (RoR) framework.

In conclusion, lattice-based PAKE schemes have rapidly diversified, addressing challenges in efficiency, scalability, and security. Yet the field lacks a comprehensive solution that combines formal proofs, practical efficiency, and implementation openness. Our work addresses this gap by presenting a PAKE protocol grounded in both Ring-LWE and Module-LWE, supported by a security proof and an optimized Python implementation.

Reconciliation Techniques and Vulnerabilities

Reconciliation is the process by which two communicating parties extract a shared secret from noisy or approximate values—typically LWE samples—that are statistically close but not identical. In lattice-based key exchange and PAKE protocols, this mechanism becomes essential due to the inherent error introduced in LWE-based encryption and decryption operations.

The earliest reconciliation mechanisms were introduced as part of Ring-LWE-based key exchange protocols, such as those by Ding et al. [17], where helper bits were used to guide the recipient toward the correct key. One widely adopted technique is the use of auxiliary functions known as *Cha* and *Mod2* [15], which form the core of reconciliation in several PAKE protocols. These functions allow both parties to derive identical keys from approximate values by disclosing just enough information to correct discrepancies, but not enough to reveal the underlying secrets.

However, reconciliation introduces unique security challenges. In a seminal work, Bindel et al. [18] demonstrated that reconciliation signals—if improperly designed or leaked—can be exploited in key recovery attacks. Qin et al. [19] further reinforced these findings by showing that reconciliation can be a vector for significant information leakage, especially when signal bits are deterministic or biased.

The vulnerability of reconciliation highlights the importance of *leakage-resilient design*. Mechanisms must ensure that any auxiliary data does not reveal partial information about the secret or reduce entropy available to an adversary. Some schemes, like NewHope [20], introduced the concept of *rounded encoding* and used randomized encoding of the secret to improve security. Later constructions such as FrodoKEM [21] avoid reconciliation entirely by using explicit decryption with error correction, sacrificing some efficiency in exchange for simpler leakage analysis.

Moreover, lattice-based PAKE protocols must account for the fact that passwords have low entropy by design. This magnifies the risk of side-channel attacks or transcript-based guessing when reconciliation signals are used. Techniques like *noise flooding* [22] and *masking* [23] are being investigated as potential ways to mitigate this.

In conclusion, while reconciliation is indispensable for efficient lattice-based PAKE, its implementation remains a double-edged sword. Our work carefully examines known vulnerabilities and adopts minimal-leakage designs, ensuring that reconciliation data—if any—is processed with formal leakage bounds and tested for adversarial advantage under standard LWE assumptions.

Generic PQ PAKE Transformations

Generic transformations aim to construct password-authenticated key exchange (PAKE) protocols from existing cryptographic primitives such as key encapsulation mechanisms (KEMs) and public-key encryption (PKE) schemes. These approaches offer the advantage of modular design, allowing for post-quantum PAKEs to be derived from well-established, quantum-resistant building blocks without reinventing PAKE-specific components from scratch.

One of the most notable transformations is "GeT a CAKE" (Generic Transformation to a Compact and Authenticated Key Exchange), introduced by Bégout et al. [24]. This framework converts any IND-CPA secure KEM into a PAKE protocol under the real-or-random (RoR) security model. The key idea is to use the KEM to encrypt ephemeral session keys, followed by a password-based MAC to provide authentication. The authors demonstrate instantiations of this framework using CRYSTALS-Kyber and other lattice-based KEMs, achieving both efficiency and provable security.

Complementing this work, Hesse and Rosenberg [25] explored the design of hybrid PAKE protocols that combine classical and post-quantum components. Their protocol, termed "HyPAKE," merges a Diffie-Hellman-based PAKE (such as CPace) with a Kyber-based PAKE derived from the CAKE transformation. This composition retains security even if one underlying assumption fails—offering a post-quantum migration path that preserves forward secrecy and mitigates premature reliance on quantum cryptography.

Another direction involves using password-authenticated KEMs (PAKEM), which extend ordinary KEMs by embedding password-derived values into the encapsulation and decapsulation processes. Although still in early development, these ideas point toward a future where any standard KEM (e.g., Kyber, FrodoKEM) could serve as the basis for an efficient, password-protected session negotiation. Alkim et al. [26] and Peikert [27] laid some of the theoretical groundwork for these constructions in the context of authenticated key exchange (AKE) and hybrid encryption.

Generic PAKE transformations provide a practical path to post-quantum readiness. Instead of designing entirely new lattice-based PAKEs from the ground up, existing KEMs and PQ-safe MACs can be recombined with password-based protocols under a well-defined security model. However, these constructions often lack performance evaluation or reference implementations, particularly in high-level languages like Python or JavaScript. Our work contributes by not only referencing these modular designs but also providing an efficient, standalone implementation, enabling faster experimentation and real-world deployment.

COMPARISON AND GAPS IN LITERATURE

Despite rapid advancements in post-quantum PAKE protocols, several challenges persist in bridging theory with deployable practice. Most schemes focus either on strong formalism or real-world efficiency—but rarely both. For example, early Ring-LWE-based PAKEs such as Ding et al.'s constructions are formally secure yet lack robust, high-performance implementations [17], [28]. On the other hand, lattice-based schemes under NIST consideration, such as Kyber or SABER, prioritize performance for KEM scenarios and do not directly support PAKE integration [29].

A critical gap lies in the evaluation of usability and interoperability. Works like [30] have shown that PAKE protocols, even when secure and efficient, often suffer from lack of portability across ecosystems (e.g., IoT vs cloud). Additionally, research such as [31] points to the limited scalability of reconciliation-heavy constructions in constrained environments. Hybrid approaches and CAKE-style transformations remain promising but have yet to be benchmarked systematically in production systems.

Leakage resistance also remains under-explored. While theoretical results support masking and flooding countermeasures [32], few papers examine the cost of incorporating them into usable designs. This leaves a dangerous gap between provable security and actual deployment resilience, especially in adversarial threat models where password entropy is low.

Finally, no existing work appears to offer a PAKE that is: (1) built on lattice-based assumptions, (2) formally proven secure, (3) benchmarked across modern platforms, and (4) designed with clear code-level access for reproducibility. Our work explicitly targets this unmet intersection, offering a Ring-LWE and Module-LWE-based protocol with strong theoretical guarantees and an accessible Python prototype.

REFERENCES

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

[2] D. Jablon, "Strong password-only authenticated key exchange," in *ACM Computer and Communications Security (CCS)*, 1996, pp. 5–26.

[3] T. Wu, "The secure remote password protocol," *NDSS*, 1998.

[4] S. Jarecki, H. Krawczyk, and J. Xu, "Opaque: An asymmetric pake protocol secure against pre-computation attacks," in *Eurocrypt*, 2018.

[5] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[6] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 34:1–34:40, 2009.

[7] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *EUROCRYPT*, 2010, pp. 1–23.

[8] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," in *Designs, Codes and Cryptography*, 2015, pp. 1–19.

[9] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals–kyber: A cca-secure module-lattice-based kem," in *IEEE Euro S&P*, 2018.

[10] J. Ding, X. Xie, and S. Wang, "A simple provably secure key exchange scheme based on the learning with errors problem," in *IACR Cryptol. ePrint Archive*, 2012.

[11] X. Li, Y. Yu, Q. Huang, and M. Yung, "Practical round-optimal lattice-based pake in the standard model," in *ASIACRYPT*, 2020.

[12] Z. Liu, Z. Bai, and Y. Huang, "Three-party authenticated key exchange based on rlwe," in *Journal of Cryptographic Engineering*, 2019.

[13] M. T. Islam and A. Basu, "A lattice-based three-party pake for mobile networks," in *IEEE Access*, 2021.

[14] Z. Jiang, Z. Zhang, and Q. Huang, "Pakes: A framework of password-authenticated key exchange from standard assumptions," in *ACNS*, 2020.

[15] J. Ding, X. Xie, and C. Fu, "A reusable key pake protocol based on lwe," in *Designs, Codes and Cryptography*, 2022.

[16] D. Dabra, K. Kaur, and G. Singh, "Lba-pake: A lattice based anonymous password authenticated key exchange protocol for mobile devices," in *Security and Privacy*, 2020.

[17] J. Ding, X. Xie, and S. Wang, "A simple provably secure key exchange scheme based on the learning with errors problem," in *IACR Cryptol. ePrint Archive*, 2012.

[18] N. Heninger, N. Bindel, and B. Curtis, "Reconciliation and key recovery in lattice-based key exchange," *ACM CCS*, 2021.

[19] Y. Qin, J. Li, and Z. Zhang, "On the leakage of reconciliation mechanisms in lattice-based cryptography," in *ESORICS*, 2022.

[20] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—a new hope," in *USENIX Security*, 2016.

[21] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, and P. Schwabe, "Frodo: Take off the ring! practical, quantum-secure key exchange from lwe," *ACM CCS*, 2016.

[22] D. Micciancio and M. Walter, "Gaussian noise flooding for lwe encryption," *IACR Cryptol. ePrint Archive*, 2018.

[23] Y. Chen, Y. Fei, and A. A. Ding, "Masking techniques for lattice-based cryptography," in *CHES*, 2021.

[24] T. Bégout, B. Smith, and A. Pradel, "Get a cake: Generic transformation of any ind-cpa kem into a password-authenticated key exchange protocol," in *EUROCRYPT*, 2023.

[25] C. Hesse and M. Rosenberg, "Hypake: Hybrid password-authenticated key exchange secure in the uc model," *IACR Cryptol. ePrint Archive*, 2024.

[26] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange – a new hope," in *USENIX Security*, 2017.

[27] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016.

[28] Y. Zhang and X. Chen, "A survey on lattice-based pake protocols: Foundations, challenges, and trends," *IEEE Access*, vol. 9, pp. 92 351–92 370, 2021.

[29] N. I. of Standards and Technology, "Status report on the second round of the nist post-quantum cryptography standardization process," NIST, Tech. Rep., 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8309/final

[30] T. Fersch, M. Schwarz, and D. Gruss, "Cross-platform portability and deployment challenges in post-quantum key exchange," *Journal of Cryptographic Engineering*, 2022.

[31] A. Ghoshal and R. Ranjan, "Lightweight lattice-based pake for iot devices: A feasibility study," in *IEEE IoT Journal*, 2021.

[32] J. Barthélemy, M. Parvar, and A. Gouget, "Efficient leakage mitigation in lattice-based key exchange: Side-channel evaluation and countermeasures," in *CHES*, 2022.