Security Proofs for Module-LWE PAKE Protocol

Artifact Appendix

May 6, 2025

1 IND-PAKE Security under LWE

Theorem 2. (IND-PAKE Security)
Let $\mathcal{A}$ be a probabilistic polynomial-time adversary that interacts with the PAKE protocol in a secure authenticated model. Suppose $\mathcal{A}$ succeeds in distinguishing the session key from random with non-negligible probability ϵ. Then there exists an algorithm that solves the Module-LWE problem with non-negligible advantage ϵ'.

Proof Sketch.
We prove this via a sequence of game hops that gradually move the real protocol toward a simulated environment, each change being indistinguishable under standard assumptions.

Game 1. Real Game: $\mathcal{A}$ engages in a real PAKE session between two honest parties. One party embeds the password into their noise via a commitment or key derivation function. The adversary observes (A, B_A, B_B) and receives the session key or a random string.

Game 2. Game 1 (Replace Public Key): The challenger replaces the public key $B = A \cdot s + e$ of one party with a uniformly random vector. If $\mathcal{A}$ distinguishes this modification with advantage ϵ_1, we construct an algorithm that solves the Module-LWE problem.

Game 3. Game 2 (Replace Shared Key): Instead of computing the session key via reconciliation and hashing, the challenger replaces the key with a uniformly random string. If $\mathcal{A}$ distinguishes this with advantage ϵ_2, then either the reconciliation function leaks entropy, or SHA-256 is distinguishable from a random oracle.

Game 4. Final Game: The adversary now interacts entirely with random values. At this point, no adversary should have more than negligible advantage (ϵ_3) in guessing the bit.

Conclusion. The overall advantage of the adversary is:

$$\epsilon \leq \epsilon_1 + \epsilon_2 + \epsilon_3,$$

which is negligible under the assumption that Module-LWE is hard and that reconciliation and hash are secure. Hence, the protocol satisfies IND-PAKE security.

□