Security Proofs for Module-LWE PAKE Protocol

Artifact Appendix

April 11, 2025

1 Offline Dictionary Attack Resistance

Theorem (Resistance to Offline Dictionary Attacks)
Suppose the underlying Module-LWE assumption holds and the password is embedded securely within the protocol via a salted commitment or derivation. Then any adversary $\mathcal{A}$ attempting to perform an offline dictionary attack on the PAKE protocol cannot succeed with non-negligible probability unless they guess the password correctly in a bounded number of attempts.

Proof Sketch.
In an offline dictionary attack, the adversary $\mathcal{A}$ captures transcript data (e.g., (A, B_A, B_B)) from a session and attempts to test password guesses against the derived session key offline, without interacting with honest parties.

Let pwd denote the true password and pwd' be a guessed password.

1. In the Module-LWE PAKE protocol, the password is either used to derive the secret vector (e.g., $\mathbf{s} = \mathsf{KDF}(\mathsf{pwd})$) or to influence a commitment within the noise term.

2. For each guess pwd', the adversary must simulate a fresh LWE instance and derive the session key $K_{\mathsf{pwd}'}$ from it.

3. Since the reconciliation function and hash function are pre-image resistant, and the LWE samples appear pseudorandom, the adversary cannot verify $K_{\mathsf{pwd}'}$ without knowing the correct password.

4. Thus, $\mathcal{A}$ must iterate over the password space and simulate a new LWE instance per guess, which is computationally expensive.

5. No efficient test (e.g., MAC verification or key comparison) exists without deriving the exact shared key, which is infeasible under the LWE assumption.

Conclusion. Any adversary performing an offline dictionary attack must perform one LWE inversion per guess and still cannot verify correctness without side information. Therefore, the PAKE protocol resists offline dictionary attacks under the Module-LWE assumption.

□