Security Proofs for Module-LWE PAKE Protocol

Artifact Appendix

April 19, 2025

1 Forward Secrecy and Replay Attack Resistance

Theorem I (Forward Secrecy of PAKE Protocol)
If the ephemeral secrets $\mathbf{s}_A$ and $\mathbf{s}_B$ are independently generated for every session and never reused, then compromise of long-term secrets or passwords after session termination does not compromise the confidentiality of previous session keys.

Proof Sketch.
Forward secrecy ensures that even if the adversary obtains full access to secret material at time $t > t_0$, all session keys established prior to t_0 remain secure. We argue this under the Module-LWE hardness assumption:

- The session key is derived from ephemeral secrets and public values:

$$K = \mathsf{H}(\mathsf{Rec}(\langle \mathbf{s}_A, B_B \rangle)) = \mathsf{H}(\mathsf{Rec}(\langle \mathbf{s}_A, A \cdot \mathbf{s}_B + \mathbf{e}_B \rangle)).$$

- These ephemeral secrets $\mathbf{s}_A$ and $\mathbf{s}_B$ are freshly sampled for each session and never reused.
- Thus, even if an adversary compromises a device and learns passwords or long-term keys after a session has completed, they cannot reconstruct past ephemeral values.
- Due to the LWE assumption, it is computationally infeasible to recover $\mathbf{s}_A$ or $\mathbf{s}_B$ from (A, B_A, B_B).
- The reconciliation and hashing functions further obfuscate any structure that could help in key inversion.

Conclusion. Since the derivation of each session key relies on ephemeral secrets that are not stored, and recovering those secrets is as hard as solving Module-LWE, the PAKE protocol provides forward secrecy.

□

Theorem II. (Replay Attack Resistance)
If the PAKE protocol incorporates unique session identifiers and fresh randomness per session (e.g., nonce or ephemeral keys), then it is resistant to replay attacks under the Module-LWE assumption.

Proof Sketch.
Replay attacks occur when an adversary captures a transcript of a valid protocol execution and reuses it in an attempt to trick a party into accepting an old session key.

1. In the PAKE protocol, fresh randomness in the form of ephemeral secrets $\mathbf{s}_A, \mathbf{s}_B$ is sampled every session.

2. As a result, public values $B_A = A \cdot \mathbf{s}_A + \mathbf{e}_A$ and $B_B = A \cdot \mathbf{s}_B + \mathbf{e}_B$ are different for every session.

3. A replayed transcript (A, B_A, B_B) from an earlier session will not match any current ephemeral secret, resulting in a mismatched key.

4. Further, inclusion of session identifiers or nonces in key derivation ensures that keys derived from the same password but different sessions are not equal.

5. Under the Module-LWE assumption, the adversary cannot forge new values that yield the same key without solving a hard problem.

Conclusion. The protocol achieves replay attack resistance by relying on fresh randomness and unique key derivation, making transcript reuse ineffective.

□