Security Proofs for Module-LWE PAKE Protocol

Artifact Appendix

May 6, 2025

1 Correctness of Key Exchange

Theorem 1. (Correctness)
Let $A \in \mathbb{Z}_q^{k\times k}[x]/(x^n+1)$ be a public matrix sampled uniformly at random. Let $\mathbf{s}_A, \mathbf{s}_B \in (\mathbb{Z}_q^n)^k$ be secret vectors and $\mathbf{e}_A, \mathbf{e}_B$ be noise vectors with small coefficients. Suppose the reconciliation function $\mathsf{Rec} : \mathbb{Z}_q^n \to \{0,1\}^n$ is used with proper thresholds. Then the derived keys $\mathsf{K}_A = \mathsf{H}(\mathsf{Rec}(\langle \mathbf{s}_A, B_B\rangle))$ and $\mathsf{K}_B = \mathsf{H}(\mathsf{Rec}(\langle \mathbf{s}_B, B_A\rangle))$ are equal with overwhelming probability:

$$\Pr[\mathsf{K}_A = \mathsf{K}_B] \geq 1 - \epsilon,$$

for negligible ϵ, assuming **bounded noise magnitude** and correct reconciliation.

Proof Sketch.

Let Alice and Bob independently compute:

- Alice samples $\mathbf{s}_A$, $\mathbf{e}_A$ and computes $B_A = A \cdot \mathbf{s}_A + \mathbf{e}_A$.
- Bob samples $\mathbf{s}_B$, $\mathbf{e}_B$ and computes $B_B = A \cdot \mathbf{s}_B + \mathbf{e}_B$.

To derive the shared key:

$$\begin{aligned}
u_A &= \langle \mathbf{s}_A, B_B\rangle = \langle \mathbf{s}_A, A\cdot\mathbf{s}_B + \mathbf{e}_B\rangle \\
&= \langle \mathbf{s}_A, A\cdot\mathbf{s}_B\rangle + \langle \mathbf{s}_A, \mathbf{e}_B\rangle \\
u_B &= \langle \mathbf{s}_B, B_A\rangle = \langle \mathbf{s}_B, A\cdot\mathbf{s}_A + \mathbf{e}_A\rangle \\
&= \langle \mathbf{s}_B, A\cdot\mathbf{s}_A\rangle + \langle \mathbf{s}_B, \mathbf{e}_A\rangle
\end{aligned}$$

Though u_A and u_B differ due to independent noise terms, their difference is small:

$$|u_A - u_B| \leq \|\langle \mathbf{s}_A, \mathbf{e}_B\rangle - \langle \mathbf{s}_B, \mathbf{e}_A\rangle\|.$$

The reconciliation function Rec is designed to handle such bounded errors. Hence, both parties derive the same bitstring $\mathbf{b}$:

$$\mathsf{Rec}(u_A) = \mathsf{Rec}(u_B) \Rightarrow \mathsf{H}(\mathbf{b}) = \mathsf{K}.$$

Thus, the PAKE protocol is **correct** with high probability.

□