Formal Methods in Post-Quantum Cryptography – CRYSTALS-Kyber

Katharina Kreuzer  
k.kreuzer@tum.de  

Supervisors: Tobias Nipkow & Javier Esparza  
Collaborators: Manuel Barbosa (Porto, PRT), Dominique Unruh (Tartu, EST)

---

**Motivation**

- Progress on quantum computers will eventually break RSA & Diffie-Hellman  
- Development of post-quantum crypto also for cyber-physical systems  
- Kyber winner of NIST standardisation

**Goal**

Formalize CRYSTALS-Kyber’s public key encryption (PKE) algorithms, and formally verify their correctness and security properties.

**Tool**

- Interactive theorem prover  
- Isabelle is foundational  
- Huge libraries in Archive of Formal Proofs (AFP)

---

**CRYSTALS-Kyber**

**Definition:** A PKE is $\delta$-correct iff  

$$E[\max_{m \in M} P[ decrypt(sk, encrypt(pk, m)) \neq m ]] \leq \delta$$

where the expectation is taken over $(pk, sk) \in R$ key_gen.

**Problem:** Use of centred mod operation implies $\| \cdot \|_\infty$ is only pseudo-norm $\Rightarrow$ Error in pen-and-paper proof

**Solution:** Additional property $q \equiv 1 \mod 4$  
  $\Rightarrow$ Alternative proof without homogeneity  
  $\Rightarrow$ Fulfilled by properties of parameters for NTT

**Problem:** Decryption is dependent on secret key  
  $\Rightarrow$ Original $\delta$ cannot be reduced using the mLWE hardness assumption as claimed in [1]

**Solution:** Modification of $\delta$ wrt. original claim  
  $\Rightarrow$ $\delta'$ dependent on worst case message and keys

---

**Correctness**

**Definition:** Module Learning with Errors (mLWE)

Given $A \in R_{q_n}^{n \times m}$, an error $e \in R_{q_n}$ chosen according to the centered binomial distribution and a target $b \in R_{q_n}$. Then find a solution $z \in R_{q_n}$ such that $A z + e = b$.

Avantage against mLWE:  

$$\text{Adv}^{mLWE} = |P[\text{guess mLWE}] - P[\text{guess coin flip}]|$$

**theorem concrete_security_kyber:**  
  **assumes** lossless: ind_cpa.lossless $A$  
  **shows** ind_cpa.adv oracle $A \leq$ mlwe.adv (red1 $A$) + mlwe.adv (red2 $A$)

---

**IND-CPA Security**

**Future work**

- Formalization of security proofs against quantum attackers (eg. One-Way-to-Hiding Lemma)  
- Formalization of Kyber KEM and $\delta/\delta'$ relation  
- Formalization of hardness assumptions (@ CADE29)

---

**References**


