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)

ConVeY

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

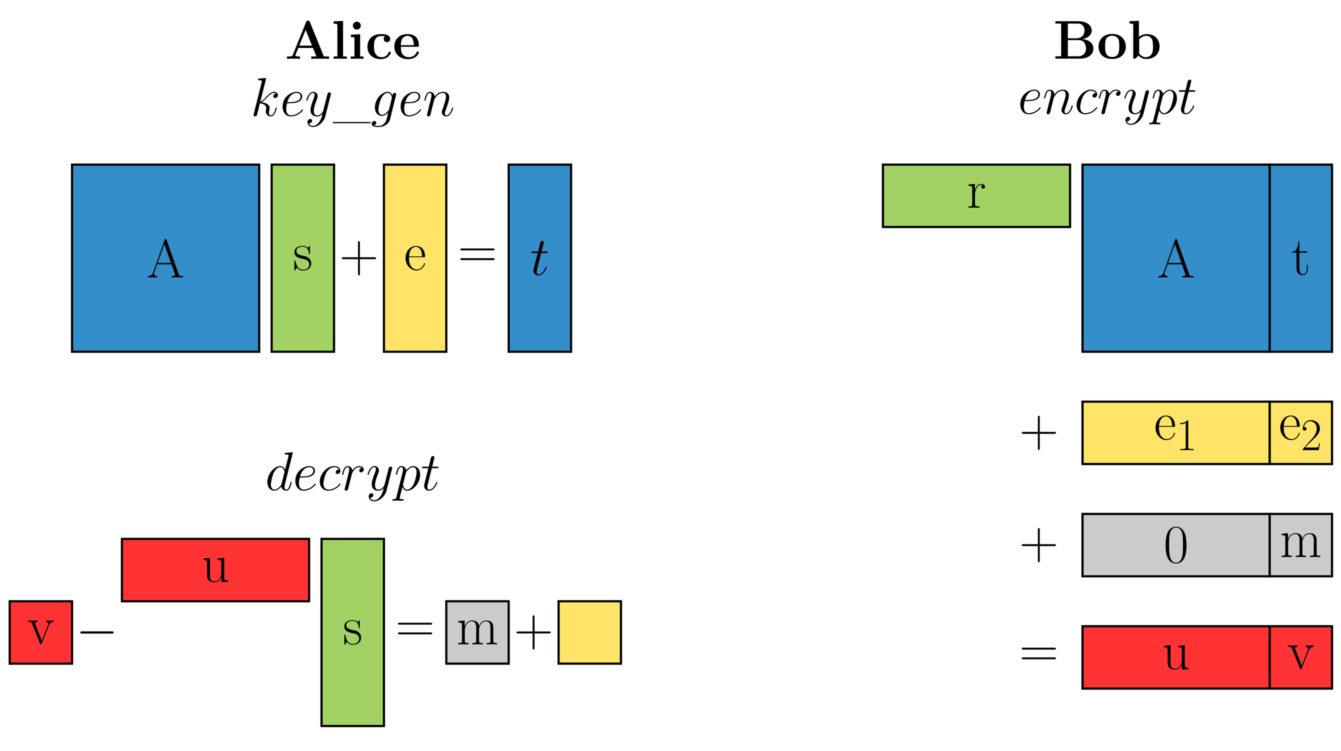
Goal

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



public key private key errors plaintext ciphertext

Underlying Module $\mathbb{Z}_q[x]/(x^n+1)$

q prime, n = power of 2

```
class qr_spec = prime_card +
  fixes qr_poly' :: 'a itself ⇒ int poly
  assumes ¬ int CARD('a) dvd
    lead_coeff (qr_poly' TYPE('a))
  and degree (qr_poly' TYPE('a)) > 0

definition qr_rel where
  qr_rel P Q ↔ [P = Q] (mod qr_poly)

quotient_type 'a qr =
  'a :: qr_spec mod_ring poly / qr_rel
```

Correctness

Definition: A PKE is δ-correct iff

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

where the expectation is taken over $(pk, sk) \xleftarrow{R} key\_gen$.

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

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

Problem: Decryption is dependent on secret key
⇒ Original δ cannot be reduced using the mLWE hardness assumption as claimed in [1]

Solution: Modification of δ wrt. original claim
⇒ δ' dependent on worst case message and keys

IND-CPA Security

Definition: Module Learning with Errors (mLWE)
Given $A \in R_q^{n\times m}$, 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 $z \in R_q^m$ such that $Az + e = b$.
Avantage against mLWE:

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

```
theorem concrete_security_kyber:
assumes lossless: ind_cpa.lossless 𝒜
shows ind_cpa.adv oracle 𝒜 ≤
  mlwe.adv (red1 𝒜) + mlwe.adv (red2 𝒜)
```

Future work

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

References

[1] J. Bos et al. "CRYSTALS — Kyber: A CCA-Secure Module-Lattice-Based KEM". In: *2018 IEEE European Symposium on Security and Privacy*. 2018, pp. 353–367.
[2] K. Kreuzer. "CRYSTALS-Kyber". In: *Archive of Formal Proofs* (2022). https://isa-afp.org/entries/CRYSTALS-Kyber.html, Formal proof development.
[3] K. Kreuzer. *Verification of Correctness and Security Properties for CRYSTALS-KYBER*. Cryptology ePrint Archive, Paper 2023/087. https://eprint.iacr.org/2023/087. 2023.
[4] K. Kreuzer. *Verification of the (1–δ)-Correctness Proof of CRYSTALS-KYBER with Number Theoretic Transform*. Cryptology ePrint Archive, Paper 2023/027. https://eprint.iacr.org/2023/027. 2023.