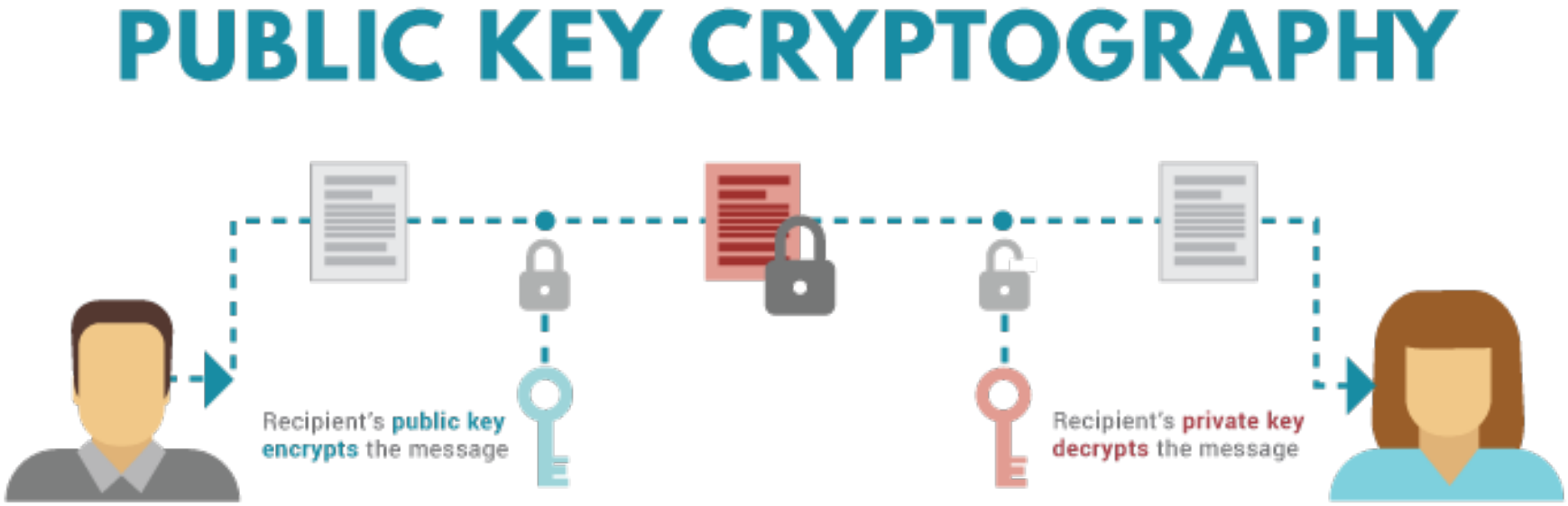
Formalization and Verification of CRYSTALS-KYBER

Katharina Kreuzer

Technische Universität München, ConVeY

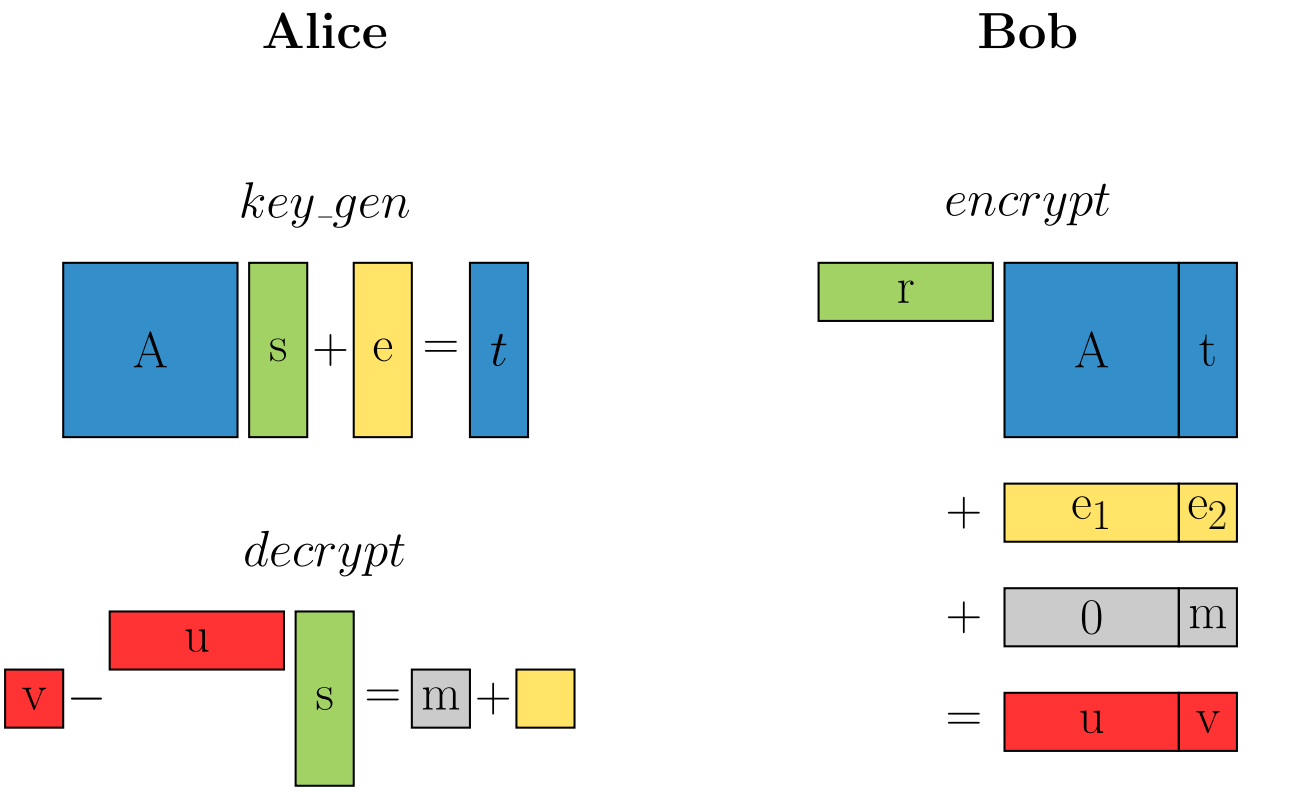
13/10/2022

Public Key Cryptography



Picture taken from
https://baloian.medium.com/how-to-generate-public-and-private-keys-for-the-blockchain-db6d057432fb

Kyber - a post-quantum crypto system



public key private key errors

message (plaintext) encrypted message (ciphertext)

Correctness of Kyber

$(1-\delta)$-correct

A cryptographic scheme is $(1-\delta)$-correct if and only if for all messages m it holds:

$$\mathbb{P}[m = \mathit{decrypt}(sk, \mathit{encrypt}(pk, m)) \mid (sk, pk) \leftarrow \mathit{key\_gen}] \geq 1 - \delta$$

Correctness of Kyber

$(1-\delta)$-correct

A cryptographic scheme is $(1-\delta)$-correct if and only if for all messages m it holds:

$$\mathbb{P}[m = \mathit{decrypt}(sk, \mathit{encrypt}(pk, m)) \mid (sk, pk) \leftarrow \mathit{key\_gen}] \geq 1 - \delta$$

Correctness of Kyber

Define $\delta := \mathbb{P}[\|e^T r + e_2 - s^T e_1\|_\infty \geq \lceil q/4 \rfloor]$. Then Kyber is $(1-\delta)$-correct.

Formalization Project

- Formalization of Kyber crypto scheme, $(1-\delta)$-correctness, and fast multiplication used in Kyber
- Formalizations in theorem prover Isabelle
- approx. 4000 lines of code
- uses mathematical libraries of algebra, number theory, analysis,...
- future projects: security proof, CRYSTALS-DILITHIUM

Questions

Thank you for your attention!