Formal Verification of Post-Quantum Cryptography

Third NIST PQC Standardization Conference

Manuel Barbosa Andreas Hülsing Matthias Meijers Peter Schwabe

Formal Verification of Cryptography: Motivation

- Cryptographic schemes and their proofs are (increasingly) complex
  - As a consequence, verification is difficult and error-prone
  - In turn, faulty scheme designs, proofs and/or implementations go unnoticed

- Examples:
  - OCB2
  - Kyber key-compression
  - MQDSS instantiation

- Formal verification techniques:
  - Reduce the complexity of the manual verification effort
  - Enforce a consistently high level of rigorousness

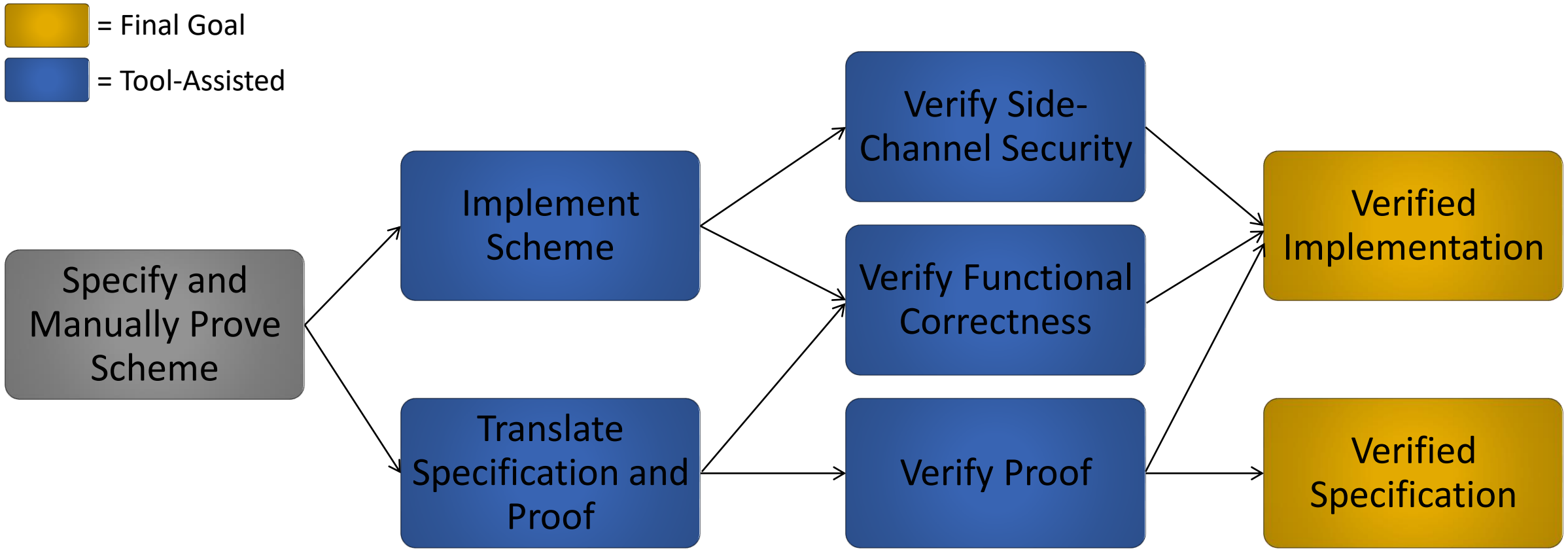
Formal Verification of Cryptography: Approach

- Computer-verifiable approach to cryptography

- Employ frameworks and tools at different levels:
  - Design/specification
    - Verify desired properties of scheme
  - Implementation
    - Verify correctness/correspondence to specification
    - Verify side-channel security

- Reduces manual verification effort to verifying relatively small part of the proofs (e.g., definitions, statements)
- Introduces Trusted Computing Base (TCB)

General Formal Verification Process



EasyCrypt

- Adopts code-based approach to provable security
- Focus on game-based proofs
- Allows for extensive mathematical reasoning

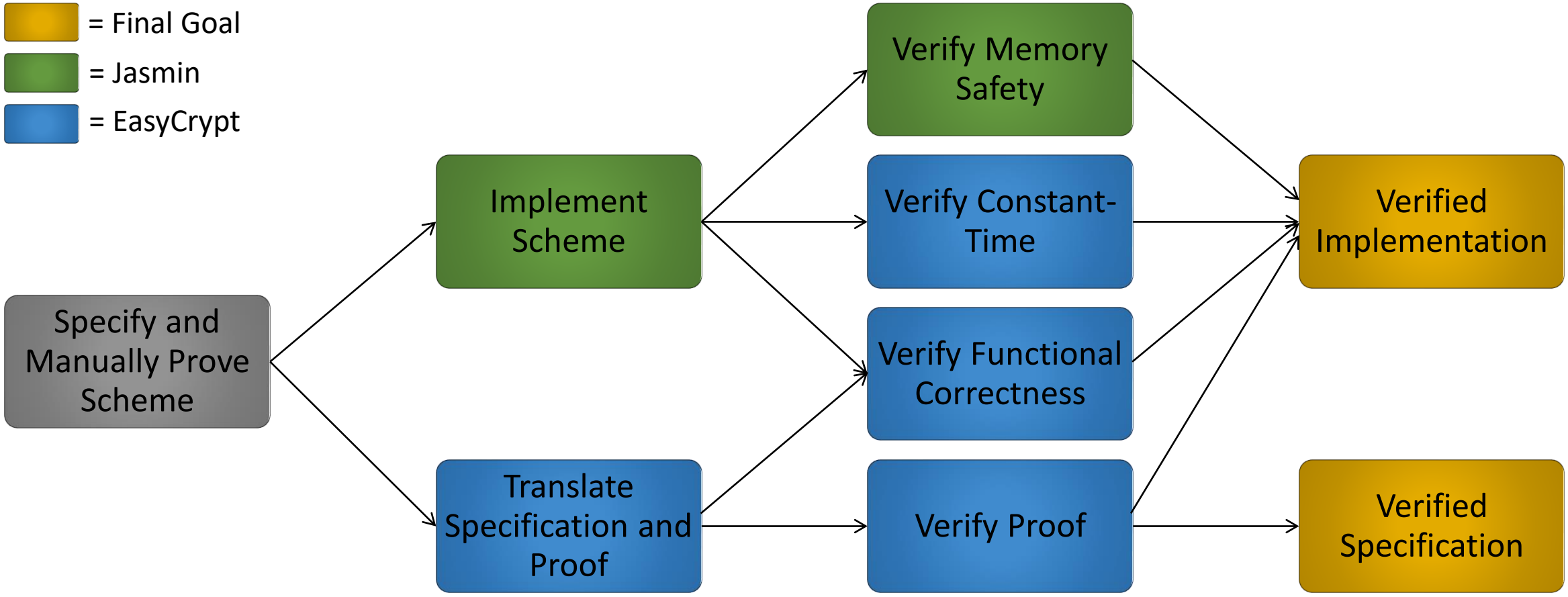
- Applicable at design and implementation level

- Currently not yet suited for analysis considering quantum adversaries
  - However, ongoing project that tries to implement support for this

Jasmin

- Designed for high-speed and high-assurance cryptography
- Programming language
- Certified Compiler
- Tools:
  - Memory-safety
  - Constant-time
  - Functional correctness
- Closely linked to EasyCrypt

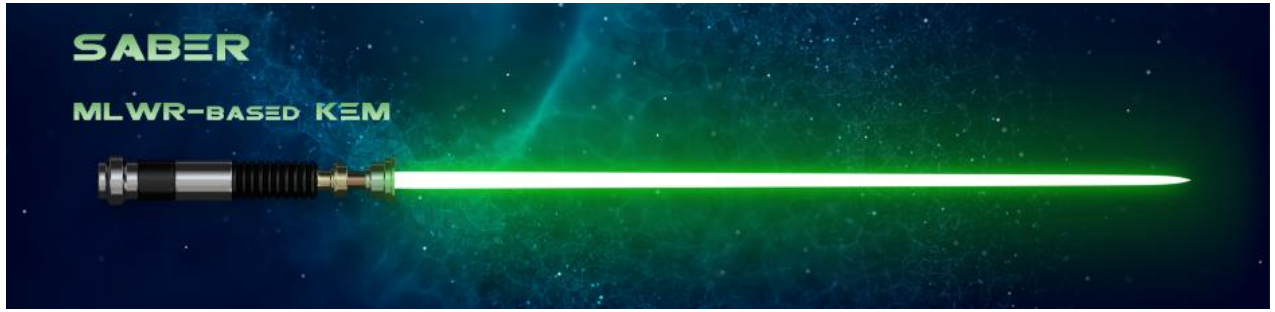
General Formal Verification Process: Jasmin and EasyCrypt



Projects: PQC Finalists

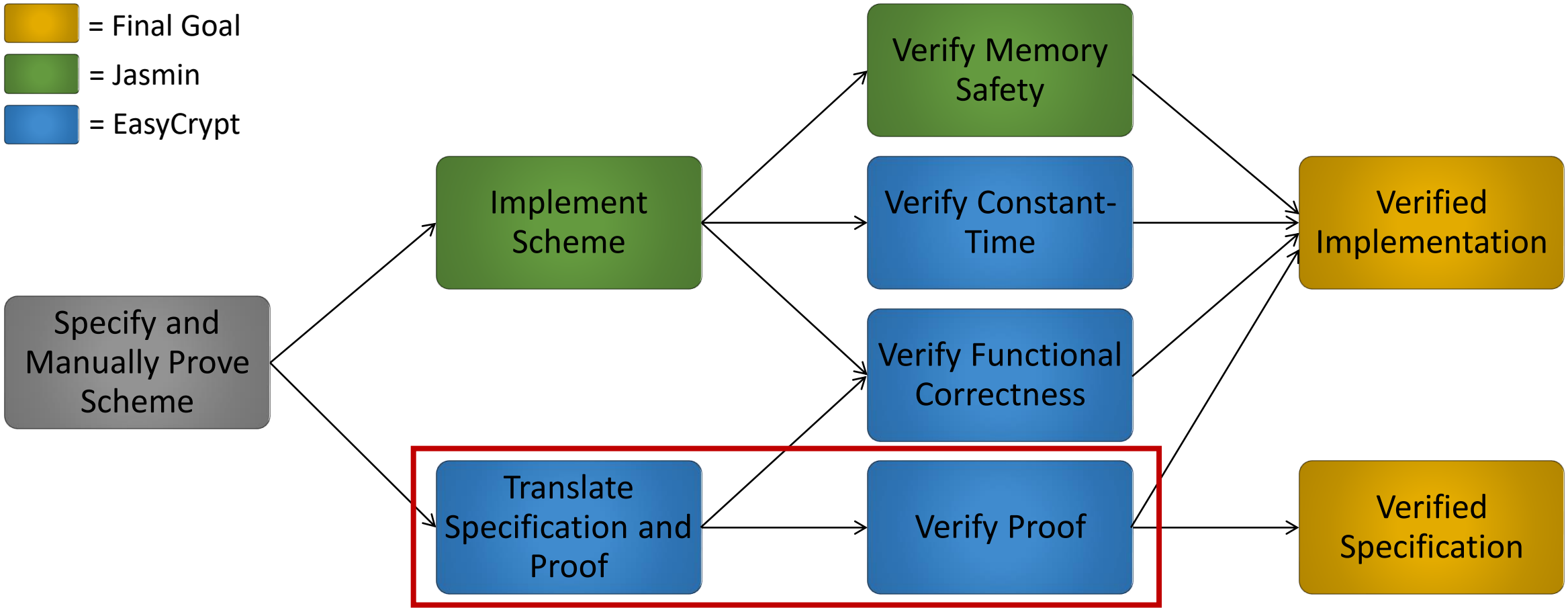
- Kyber

- Saber

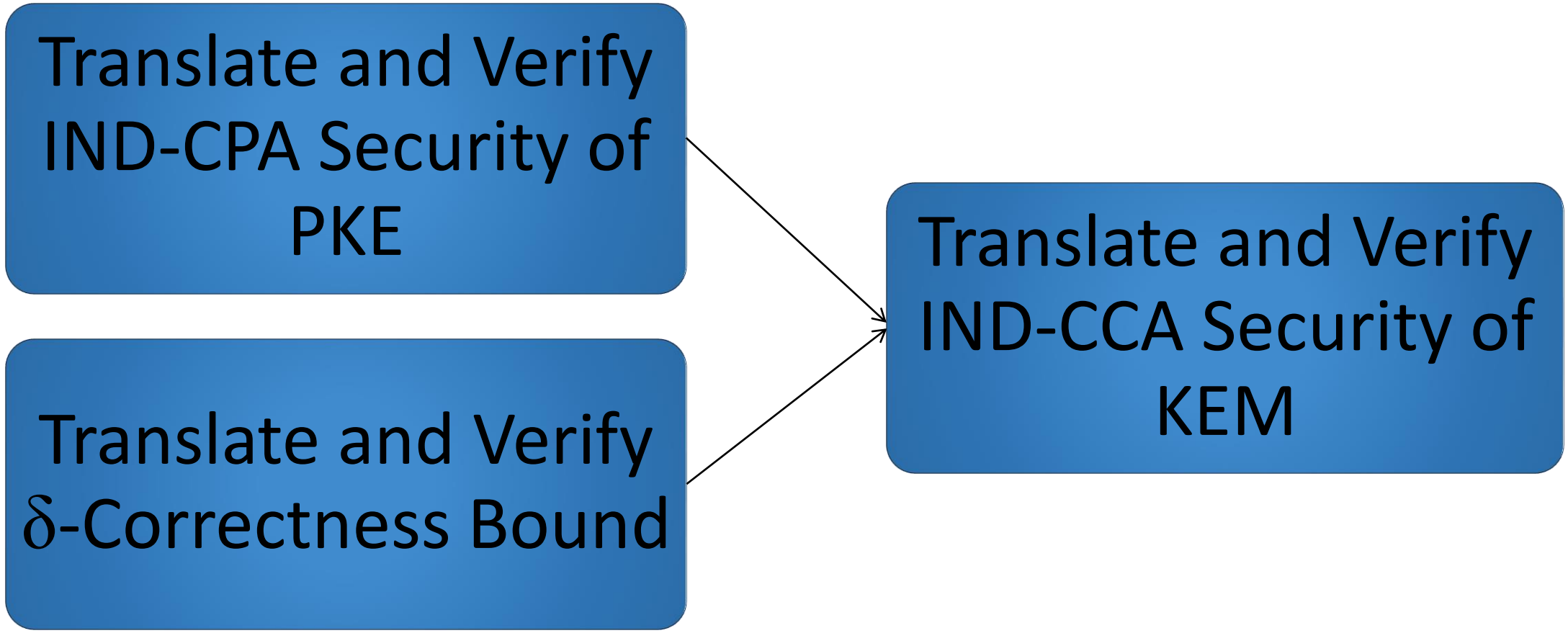


Source Kyber Image: https://pq-crystals.org/kyber/index.shtml
Source Saber Image: https://www.esat.kuleuven.be/cosic/pqcrypto/saber

Specification Verification: Kyber and Saber (1)



Specification Verification: Kyber and Saber (2)



Projects Progress: Specification

= Completed

= Not Started

Goal	Kyber	Saber
Verify IND-CPA Security of PKE		
Verify δ-Correctness Bound		
Verify IND-CCA Security of KEM		

Projects Progress: Implementation

= Completed

= In Progress

= Not Started

Goal	Kyber	Saber
Construct Reference Implementation		
Construct Optimized Implementation		
Verify Memory Safety Reference/Optimized		
Verify Functional Correctness Reference/Optimized		
Verify Constant-Time Reference/Optimized		

List of Contributors

Saber

- Andreas Hülsing
- Matthias Meijers
- Peter Schwabe
- Pierre-Yves Strub

Kyber

- José Bacelar Almeida
- Manuel Barbosa
- Gilles Barthe
- Benjamin Grégoire
- Vincent Laporte
- Miguel Quaresma
- Peter Schwabe
- Pierre-Yves Strub

Questions?