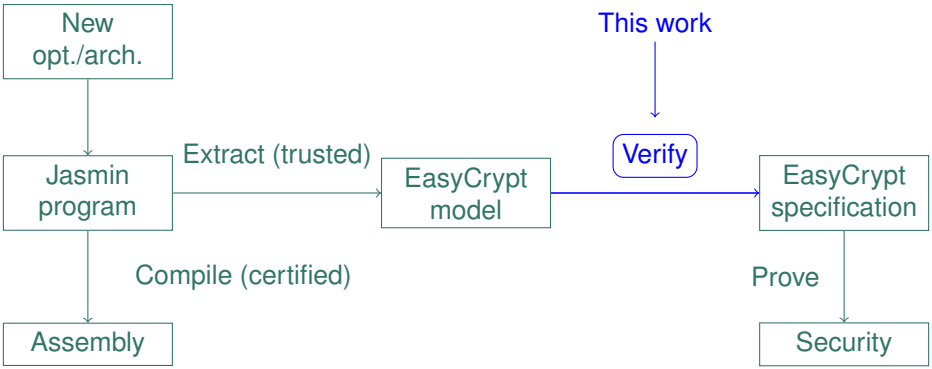
Universidade do Minho, Universidade do Porto (FCUP), INESC TEC, PQShield,
Max Planck Institute for Security and Privacy, SandboxAQ

Faster Verification of Faster Implementations: Combining Deductive and Circuit-Based Reasoning in EasyCrypt

José Bacelar Almeida, Gustavo Marinho Alves, Manuel Barbosa, Gilles Barthe, Luís Esquível, Vincent Hwang, Tiago Oliveira, Hugo Pacheco, Peter Schwabe, Pierre-Yves Strub

May 14, 2025

Verifying Cryptographic Implementations



Hybrid Verification

Blending deductive reasoning and circuit-based reasoning.

- Modularity:
  - New opt./arch. $\rightarrow$ new circuits.
  - Equivalence of old and new circuits $\rightarrow$ same proof afterwards.
- Scalability.
  - Reduce human effort with circuit-based reasoning.

Applications to optimized ML-KEM (NIST PQC standard for KEM).

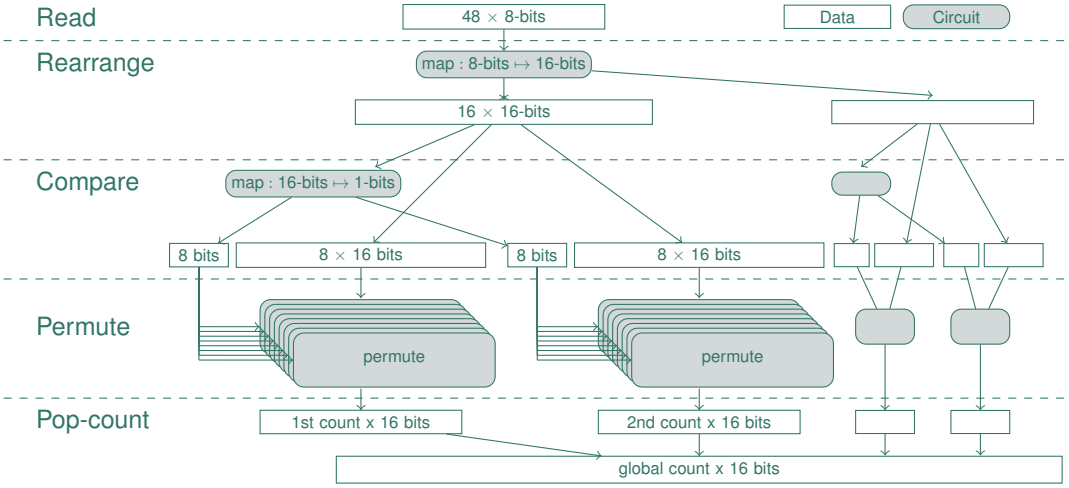
- Rejection sampling for the public matrix (first verified in this work).
- Compression of ciphertext.
- Keccak permutation.

Hybrid Verification for Rejection Sampling

For a 12-bit a, we reject it if $a \geq q$. Repeat until we have a matrix with $256k^2$ elements, $k \in \{2, 3, 4\}$ depending on security level.

- Large problem $\rightarrow$ smaller problems.
  - Read.
  - Rearrange.
  - Compare.
  - Input-dependent vector permutation.
  - Pop-count.
- Input-dependent vector permutation.
  - Input-dependent (256 cases).
  - Restate as table access.
  - Verify table access with circuit.

Overview


Read
Rearrange
Compare
Permute
Pop-count
48 × 8-bits
Data
Circuit
map : 8-bits ↦ 16-bits
16 × 16-bits
map : 16-bits ↦ 1-bits
8 bits
8 × 16 bits
8 bits
8 × 16 bits
permute
permute
1st count x 16 bits
2nd count x 16 bits
global count x 16 bits

Scalability and Modularity with Circuit-Based Reasoning

- Modularity.
  - Circuit equivalence are suitable for verifying some computations.
  - New optimization $\rightarrow$ new circuit $\rightarrow$ circuit equivalence.
  - New architecture $\rightarrow$ new circuit $\rightarrow$ circuit equivalence.
- Scalability.
  - Offload some computations to circuit equivalence when it makes sense.
  - Call circuit equivalence for different circuits implementing the same function.

Compressions on Different Platforms

Ciphertext compression in ML-KEM:

$$\texttt{Compress}_d : a \mapsto \left\lfloor a2^d/q \right\rceil \bmod 2^d.$$

Apply $\texttt{Compress}_d$ to an array of 256 elements.

- Lane-wise dependency (exhaustive):
  - Circuit for $\texttt{Compress}_d$ instead of $\texttt{Compress}_d^{256}$.
- Relational:
  - Lane-wise equivalence $\rightarrow$ equivalence for $\texttt{Compress}_d^{256}$.
  - Equivalence of $\texttt{Compress}_d^{256}$ on different architectures.

Takeaway

- EasyCrypt now comes with circuit-based reasoning.
- Verifying computations in AVX2-optimized ML-KEM.
  - Rejection sampling for public matrix (first verified in this work).
  - Compression of ciphertext.
  - Keccak permutation.

Thank you for listening