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

Specify and Manually Prove Scheme

Implement Scheme

Translate Specification and Proof

Verify Functional Correctness

Verify Side-Channel Security

Verify Proof

Verified Specification

Verified Implementation

= Final Goal

= Tool-Assisted
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

Specify and Manually Prove Scheme

Implement Scheme

Translate Specification and Proof

Verify Memory Safety

Verify Constant-Time

Verify Functional Correctness

Verify Proof

Verified Specification

Verified Implementation

= Final Goal

= Jasmin

= EasyCrypt
Projects: PQC Finalists

- Kyber

- Saber
Specification Verification: Kyber and Saber (1)

= Final Goal
= Jasmin
= EasyCrypt

Specify and Manually Prove Scheme

Implement Scheme

Verify Memory Safety

Verify Constant-Time

Verify Functional Correctness

Verify Proof

Verified Specification

Verified Implementation
Specification Verification: Kyber and Saber (2)

Translate and Verify IND-CPA Security of PKE

Translate and Verify $\delta$-Correctness Bound

Translate and Verify IND-CCA Security of KEM
### Projects Progress: Specification

<table>
<thead>
<tr>
<th>Goal</th>
<th>Kyber</th>
<th>Saber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify IND-CPA Security of PKE</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Verify $\delta$-Correctness Bound</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Verify IND-CCA Security of KEM</td>
<td>Red</td>
<td>Red</td>
</tr>
</tbody>
</table>

- Green = Completed
- Red = Not Started
## Projects Progress: Implementation

<table>
<thead>
<tr>
<th>Goal</th>
<th>Kyber</th>
<th>Saber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Construct Reference Implementation</td>
<td>Complete</td>
<td>Complete</td>
</tr>
<tr>
<td>Construct Optimized Implementation</td>
<td>Complete</td>
<td>Complete</td>
</tr>
<tr>
<td>Verify Memory Safety Reference/Optimized</td>
<td>Complete</td>
<td>Complete</td>
</tr>
<tr>
<td>Verify Functional Correctness Reference/Optimized</td>
<td>In Progress</td>
<td>Not Started</td>
</tr>
<tr>
<td>Verify Constant-Time Reference/Optimized</td>
<td>Not Started</td>
<td>Not Started</td>
</tr>
</tbody>
</table>

- **Green** = Completed
- **Yellow** = In Progress
- **Red** = Not Started
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?