Formally Verified Post-Quantum Cryptography at Scale

HCSS 2026

DUSAN KOSTIC AND ROD CHAPMAN
AMAZON WEB SERVICES

Agenda

- Post-Quantum Cryptography (PQC)
- AWS-LC and friends
- Formal verification of PQC
- AI and Formal Reasoning

Post-Quantum Cryptography

- Cryptography
- Quantum Computers + Shor’s algorithm
- Cryptography → Classical Cryptography
- Post-Quantum Cryptography
- Cryptographically Relevant Quantum Computer (CRQC)

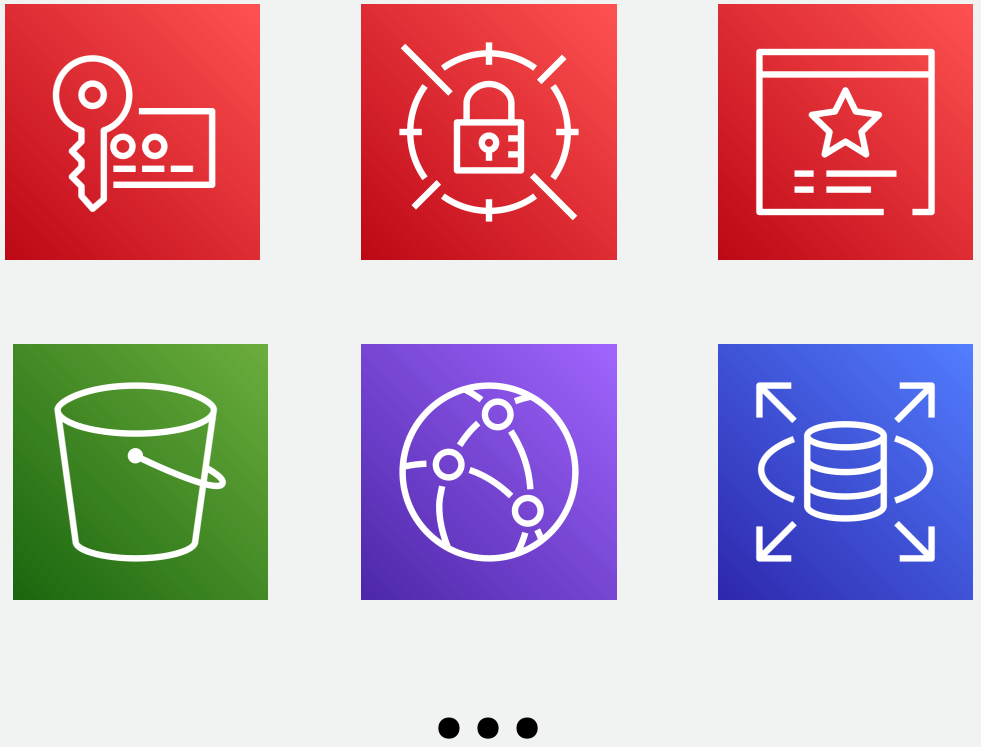
Post-Quantum Cryptography

- Key Exchange
  - ML-KEM (FIPS 203)
- Digital Signatures
  - ML-DSA (FIPS 204)
- CNSA 2.0

AWS-LC

- Open-source cryptographic library
- Fork of BoringSSL
- Powers trillions of crypto operations daily across AWS
- https://github.com/aws/aws-lc/

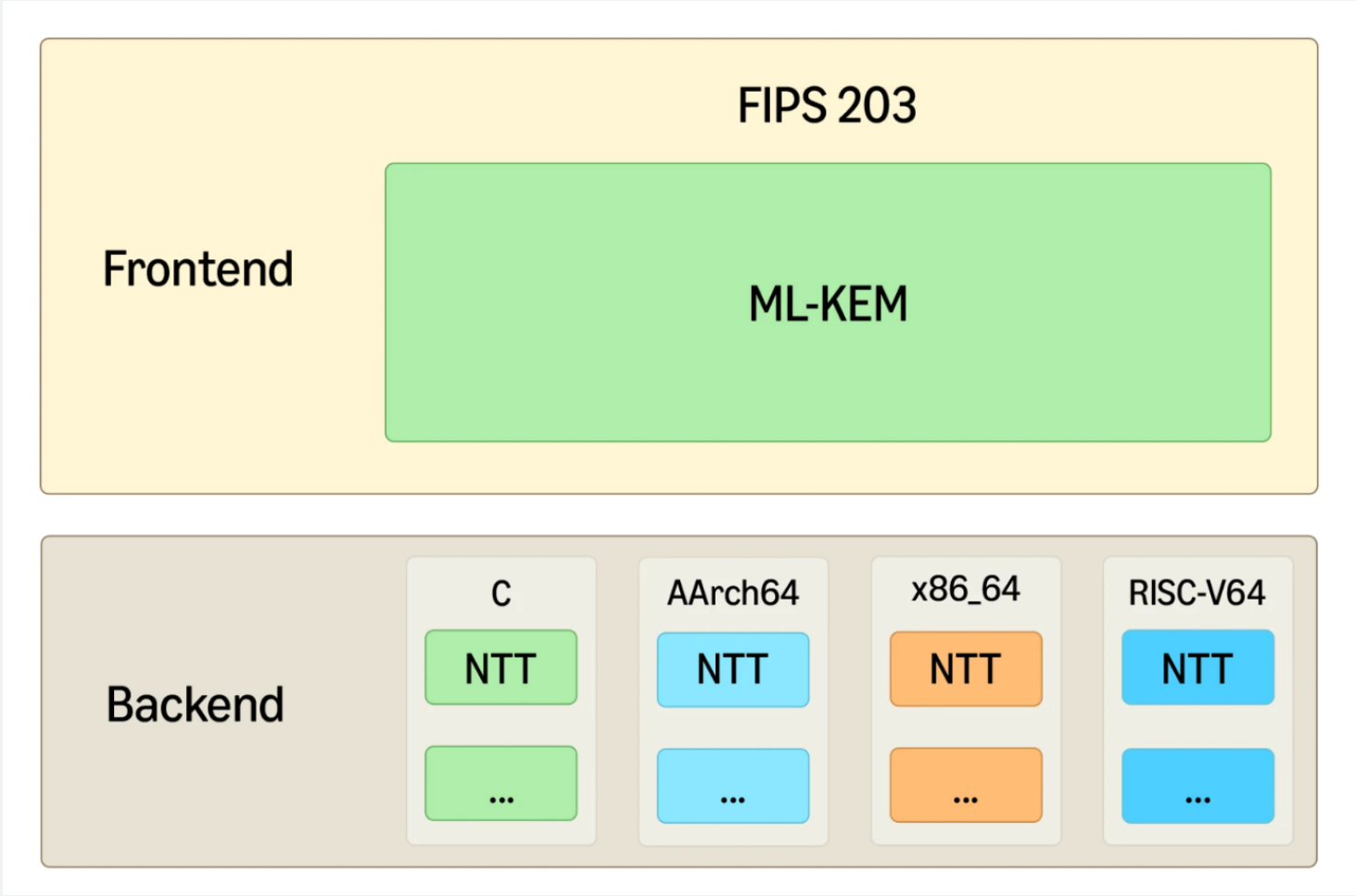
AWS-LC: Fast and Formal



ML-KEM and ML-DSA in AWS-LC

- mlkem-native and mldsa-native
- Post-Quantum Cryptography Alliance (PQCA)
- Linux Foundation
- https://github.com/pq-code-package/mlkem-native
- https://github.com/pq-code-package/mldsa-native

mlkem-native



mlkem/mldsa-native

- C Bounded Model Checker (CBMC) for C
- Memory safety
- Type safety
- 191 ML-KEM and 193 ML-DSA proofs

mlkem/mldsa-native

- HOL Light interactive theorem prover for assembly
- Functional correctness
- Memory safety
- Constant-time
- 36 ML-KEM and 27 ML-DSA proofs

HOL Light proofs of implementation correctness

- HOL Light: https://github.com/jrh13/hol-light
- s2n-bignum: https://github.com/awslabs/s2n-bignum
- aarch64 and x86_64 ISA models
- Symbolic simulation machinery and tactics

SOUNDNESS.md

- Do the specs match the requirements?
- Do the formal models match the real systems?
- Is the proof infrastructure sound?

AI and Formal Reasoning

AI and Formal Reasoning

BC/AD

AI and Formal Reasoning

BC/AD

Claude Opus 4.6

AI and Formal Reasoning (BC)

- Before Claude Opus 4.6
- aarch64 and x86_64
- Wrote all ML-KEM HOL Light proofs by hand
- Used AI for better documentation for existing tactics

AI and Formal Reasoning (AD)

- ML-KEM and ML-DSA are “siblings”, but
- 12-bit vs. 23-bit polynomial coefficients
- 16-bit vs. 32-bit machine words
- Algorithmic differences

AI and Formal Reasoning (AD)

- Claude Opus 4.6 (Act 1)
- ML-KEM and ML-DSA aarch64
- [inverse] Number Theoretic Transform, [i]NTT
- ML-KEM: 500 LoC and 300-400 LoP

AI and Formal Reasoning (AD)

- Claude Opus 4.6 (Act 1)
- Here is the implementation of ML-KEM NTT
- Here is the proof of ML-KEM NTT
- Here is the implementation of ML-DSA NTT
- Here is the _____ of ML-DSA NTT

AI and Formal Reasoning (AD)

- Claude Opus 4.6 (Act 1)
- Fill-in-the-blanks
- Claude wrote the draft of the proof
- I debugged and corrected it (with Claude’s help)
- ML-DSA NTT and iNTT proven in two weeks

AI and Formal Reasoning (AD)

- Claude Opus 4.6 (Act 2)
- ML-KEM and ML-DSA aarch64
- Rejection Sampling algorithm
- ML-KEM: 150 LoC and 2800 LoP

AI and Formal Reasoning (AD)

- Claude Opus 4.6 (Act 2)
- Fill-in-the-blanks
- Gave Claude access to the HOL Light server
- I was still involved in steering Claude
- ML-DSA Rejection Sampling proved in a week

AI and Formal Reasoning (AD)

- Act 3 and beyond
- Proofs from scratch (without existing reference)
- Less human, more AI agent
- Prove → Optimize → Prove → Optimize → Prove

We prove it.

While others test and hope, Automated Reasoning at Amazon delivers mathematical certainty.

Our tools verify the correctness of systems that millions of people depend on every day — across security, storage, networking, identity, and more.

Join Us — Hiring Now

amazon

Scan to Apply

Amazon Automated Reasoning

Open-source cryptography @ AWS

https://aws.amazon.com/security/opensource/cryptography

Thank you!

Dusan Kostic

dkostic@amazon.com