Assembly-Level Formal Verification of HQC

Polynomial Multiplication and Reed-Muller Decoding

Research Proposal • 6-Month Timeline

Background and Motivation

In March 2025, NIST selected HQC (Hamming Quasi-Cyclic) as a post-quantum key encapsulation mechanism (KEM) to complement the lattice-based ML-KEM, providing algorithmic diversity in the post-quantum cryptographic standard portfolio. Unlike ML-KEM, HQC's security rests on the hardness of decoding random quasi-cyclic binary linear codes, and its implementation profile is dominated by two computationally distinct primitives: dense binary polynomial multiplication over GF(2)[x]/(x^n − 1), and a concatenated Reed-Muller/Reed-Solomon error correcting decoder. Together, these two components account for over 85% of total decapsulation latency and, critically, have been the target of multiple published side-channel attacks—including a 2026 single-trace Simple Power Analysis attack achieving a 99.69% key recovery success rate by exploiting data-dependent power consumption during polynomial multiplication.

The s2n-bignum project (AWS Labs) has established a mature infrastructure for formally verifying cryptographic assembly code at the object-code level using the HOL Light interactive theorem prover. Its verification of ML-KEM's NTT-based polynomial arithmetic demonstrates that assembly-level proofs of functional correctness and secret-independence (constant-time execution) are achievable for post-quantum primitives within the HOL Light framework. However, no such verification exists for any HQC component. This proposal targets that gap.

Research Goals

This project will produce the following formally verified artifacts, building on the s2n-bignum HOL Light infrastructure:

- A HOL Light formalization of binary polynomial arithmetic over GF(2)[x]/(x^n − 1), establishing the algebraic foundation for HQC's ring operations.
- Optimized x86_64 assembly implementing constant-time dense–dense polynomial multiplication for all three HQC parameter sets (HQC-128/192/256), leveraging the PCLMULQDQ carry-less multiplication instruction.
- HOL Light proofs of functional correctness and secret independence for the polynomial multiplication assembly, directly addressing the attack surface exploited by published power analysis attacks.
- HOL Light proofs of functional correctness and constant-time execution for the Fast Walsh–Hadamard Transform (FWHT) used in HQC's first-order Reed-Muller decoder.
- A formally stated HOL Light specification of the GF(2^8) syndrome computation in the Reed-Solomon decoder, serving as a foundation for future verification work.

Technical Approach

HQC's binary arithmetic is natively well-suited to the HOL Light bit vector model underlying s2n-bignum: all polynomial operations reduce to XOR, AND, and shift instructions, with no modular integer arithmetic, Montgomery representations, or floating-point semantics. This removes the primary sources of foundational complexity encountered in other post-quantum schemes such as FN-DSA (Falcon). The PCLMULQDQ instruction on x86_64 directly implements carry-less polynomial

multiplication over 128-bit words, enabling highly efficient schoolbook or Karatsuba decompositions whose correctness can be mechanically verified against the polynomial ring specification. The constant-time proof for the dense–dense multiplication is largely structural: because no branch or memory address depends on input polynomial coefficients, the s2n-bignum secret-independence model applies without the case-splitting complexity seen in secret-sparse algorithms.

The Reed-Muller decoder's FWHT consists of butterfly operations over binary vectors of length 128, structurally analogous to an NTT butterfly but with simpler arithmetic (XOR additions). The proof of correctness proceeds by induction over the butterfly stages, and constant-time follows from the absence of data-dependent control flow. Together, the verified polynomial multiplication and FWHT cover the dominant performance and attack surface of HQC decapsulation.

Expected Contributions

This work makes the following novel contributions to the field:

- First assembly-level formally verified implementation of any HQC component, filling a critical gap ahead of the anticipated FIPS standard finalization in 2027.
- First HOL Light mechanization of binary quasi-cyclic polynomial arithmetic, reusable for future code-based cryptography verification efforts.
- A formal, machine-checked proof that the polynomial multiplication implementation is free from secret-dependent branching and memory access patterns, directly invalidating the attack model of all published HQC power analysis attacks.
- Open-source proof artifacts integrated with the s2n-bignum infrastructure, enabling community auditing and extension.

Target Publication Venue

IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), with its quarterly submission windows and focus on implementation security, is the primary target venue. IEEE S&P and USENIX Security are secondary targets if the scope is broadened to include the Reed-Solomon decoder.