StealthPQ

ML-KEM and ML-DSA Post-Quantum Engine With Side-Channel and Glitch Countermeasures

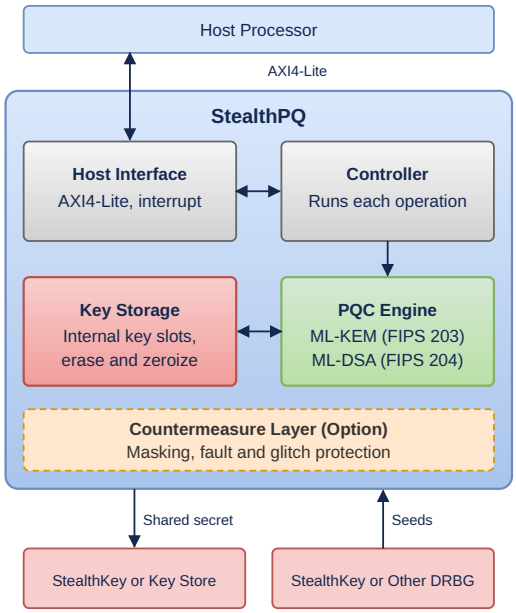
Full offload of ML-KEM and ML-DSA, the NIST post-quantum standards. Private keys remain in secure internal key slots behind a single AXI4-Lite interface, with an optional countermeasure configuration providing side-channel, fault and glitch attack protection.

Up to 12,400/s	Up to 5,190/s	FIPS 203 · 204
ML-KEM-768 Encapsulations	ML-DSA-65 Verifications	All Six Parameter Sets

All major FPGAs and ASICs. **AMD** Versal, UltraScale+, UltraScale and 7 Series · **Microchip** PolarFire, PolarFire SoC, SmartFusion 2 and IGLOO2 · **Altera** Agilex, Arria 10, Stratix 10 and Cyclone 10 · RTL optimized for ASIC implementation

Key Features

- **ML-KEM-512, -768 and -1024 (FIPS 203)**
  Key generation, encapsulation and decapsulation
- **ML-DSA-44, -65 and -87 (FIPS 204)**
  Key generation, signing and verification
- **Advanced Side-Channel Countermeasures**
  Masking of all secret-dependent operations
- **Fault and Glitch Attack Protection**
  Dual-lockstep controller and layered detection
- **Secure Key Storage**
  Private keys generated and held in internal key slots
- **Dedicated Shared-Secret Output**
  Direct key delivery to StealthKey or another key store
- **Random Number Input**
  Connects to StealthKey or another DRBG
- **Simple Integration**
  AXI4-Lite host interface with completion interrupt



Applications

Key Establishment
- TLS 1.3 hybrid key exchange
- IPsec IKEv2
- MACsec key agreement
- Symmetric key delivery

Digital Signatures
- Firmware and code signing
- Secure boot verification
- Signing servers and HSMs
- Post-quantum certificates

Post-Quantum Transition
- CNSA 2.0 compliant algorithms
- Device identity and provisioning
- Firmware update verification
- Defense and aerospace systems

StealthPQ Product Overview

Technical Specifications

Standards	FIPS 203 ML-KEM-512, -768 and -1024, and FIPS 204 ML-DSA-44, -65 and -87
Host interface	AXI4-Lite with completion interrupt
Key storage	Internal key slots with zeroization
Configurations	Standard and Fast, ML-KEM or ML-DSA only, and countermeasure
Software	StealthAPI library, Linux driver and wolfSSL integration
Validation	NIST ACVTS Ready
Deliverables	Verilog or VHDL RTL, test suite with NIST ACVP vectors, C header and documentation

Countermeasure Configuration

The countermeasure configuration offers the same standards and host interface, with additional protection for high-assurance applications.

Side-Channel Countermeasures
Masking of all secret-dependent operations

Fault and Glitch Attack Protection
Over 30 specific protections, including a dual-lockstep controller

Secure Fault Response
Detected faults lock the core until all keys are erased

Area and performance figures for the countermeasure configuration are available on request.

Area and Performance

	AMD Versal AI Edge		Microchip PolarFire SoC		Altera Agilex 5	
	Standard	Fast	Standard	Fast	Standard	Fast
Max frequency	200 MHz	200 MHz	120 MHz	120 MHz	155 MHz	155 MHz
Logic	17.0K LUT6	22.6K LUT6	34.4K 4LUT	45.6K 4LUT	15.5K ALM	19.0K ALM
Flip-flops	10.4K	13.2K	15.6K	22.5K	20.0K	24.2K
Block RAM	43 RAMB36 + 5 RAMB18	73 RAMB36 + 5 RAMB18	80 LSRAM + 6 uSRAM	140 LSRAM + 6 uSRAM	90 M20K	150 M20K
Multipliers	13 DSP58	26 DSP58	27 Math	54 Math	13 DSP	25 DSP

Post-place-and-route results for the core alone on a mid-range device of each family; results vary with device, tools and design.

	Standard			Fast		
ML-KEM	Key generation	Encapsulation	Decapsulation	Key generation	Encapsulation	Decapsulation
ML-KEM-512	11.9 k (16,800)	16.0 k (12,400)	23.4 k (8,550)	9.0 k (22,200)	11.6 k (17,200)	16.7 k (12,000)
ML-KEM-768	18.4 k (10,800)	23.2 k (8,610)	33.1 k (6,040)	13.3 k (15,000)	16.1 k (12,400)	22.9 k (8,730)
ML-KEM-1024	26.3 k (7,600)	31.7 k (6,300)	44.4 k (4,500)	18.4 k (10,800)	21.6 k (9,270)	30.3 k (6,600)
ML-DSA	Key generation	Signing	Verification	Key generation	Signing	Verification
ML-DSA-44	26.9 k (7,420)	169 k (1,180)	36.9 k (5,420)	21.5 k (9,310)	103 k (1,950)	27.6 k (7,250)
ML-DSA-65	40.7 k (4,910)	284 k (703)	51.4 k (3,890)	33.0 k (6,050)	167 k (1,190)	38.5 k (5,190)
ML-DSA-87	57.8 k (3,460)	326 k (613)	72.0 k (2,770)	47.2 k (4,230)	196 k (1,010)	54.9 k (3,640)

Standard and Fast configurations without the countermeasure option. Cycles per operation, with operations per second at 200 MHz shown in gray. Rates scale with the clock frequency of each family. Signing figures are averaged over the expected number of attempts.

Ready to Move to Post-Quantum Cryptography?

info@stealthcores.com | www.stealthcores.com | © 2026 StealthCores

Rev. 2026.1.0