Overview

With quantum computing posing a threat to many of today's standard cryptographic algorithms, new solutions will be required to provide lasting security. Especially vulnerable are public key algorithms. The Cryptographic Suite for Algebraic Lattices (CRYSTALS) encompasses a cryptographic primitive called Dilithium, a digital signature scheme, as well as Kyber, a key encapsulation mechanism. These are based on the module learning with errors (M-LWE) lattice problem known to be quantum-resistant.

The two algorithms are both included in the NIST post-quantum cryptography standardization process and have their own FIPS (Federal Information Processing Standards) documents [1,2]. They are also endorsed by the NSA under the CNSA Suite 2.0 for national defense applications [3].

PQSecure has developed secure hardware intellectual property (IP) cores for these CRYSTALS algorithms [1,2]. These pre-designed and pre-verified circuits can be used for implementation in any hardware silicon including SoCs, FPGAs and ASICs.

Product Description

PQSecure™-CRYSTALS from PQSecure Technologies, LLC. is a set of hardware IP cores designed for various target applications of digital signatures and key encapsulation based on Dilithium and Kyber algorithms. PQSecure™-CRYSTALS supports parameters for all three FIPS recommended security levels with countermeasures (optional) against various side-channel and known fault attacks. It can be used in various security protocols to replace or augment the traditional elliptic curve based key exchange and digital signatures (ECDH and ECDSA) such as TLS, which are potentially compromised by quantum computing.

PQSecure™-CRYSTALS has several variations that operate at different levels of performance and security levels. The lowest area (tiny) design is **PQSecure™-CRYSTALS-1000T**, the compact design is designated **PQSecure™-CRYSTALS-1000C**, the balanced-performance design is **PQSecure™-CRYSTALS-1000B**, and the highest-performance design is **PQSecure™-CRYSTALS-1000H** (as illustrated in Figure 1).

PQSecure™-CRYSTALS-1000 series have been designed in a flexible manner to be platform independent and is available to be integrated to both FPGA- and ASIC-based solutions without relying on specific embedded resources of the platforms [3,4].

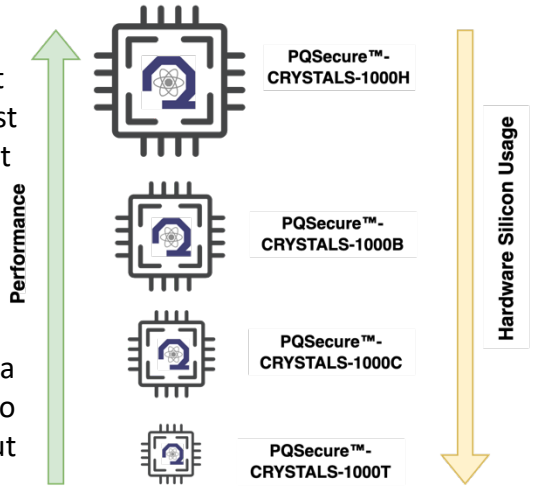

Figure 1. PQSecure™ product series

PQSecure™-CRYSTALS-1000 series are secure against timing attacks and can optionally provide power side-channel countermeasures (to address FIPS 140-3 non-invasive attack requirements) for all three security levels. For instance, PQSecure™-CRYSTALS-1000B-SCA-FI is a balanced performance

implementation that provides basic fault injection (FI) countermeasures and uses masking, shuffling, and other techniques to protect against Simple Power Analysis (SPA) attacks as well as first order Differential Power Analysis (DPA) attacks for all NIST/FIPS security levels.

Applications

- Microcontroller and Microprocessor acceleration for IoTs
- Secure networking protocols such as SSL/TLS, and IPSec
- Secure car-to-car communications
- Secure boot and root of trust for HSMs

Features

- Turn-key implementations of the NIST FIPS recommended CRYSTALS post-quantum for key encapsulation (KEM) and digital signature algorithm (DSA)
- Complete CPU offload of cryptographic operations
- Highly silicon customizable design with optional hash accelerator, memory, and control unit to support customer's requirements.
- Ease of integration into various RISC-V, SoC, and FPGA architectures and development flow
- Support for multiple interface standards including AXI, APB, and AHB.
- Choice of several performance grades versus silicon footprint trade-offs
- Substantial power reductions in comparison to software implementations
- Optional and secure-by-design support for side-channel attack countermeasures
- Protection against known fault injection attacks

Architecture

The internal high-level architecture of PQSecure™-CRYSTALS-1000 is illustrated in Figure 1 with options for SCA and FI countermeasures. The architecture is composed of several accelerators for the CRYSTAL lattice operations, a set of memories, and an optional hash accelerator. The implementation contains patented-technology to provide unsurpassed performance with very low power and gate-count requirements.

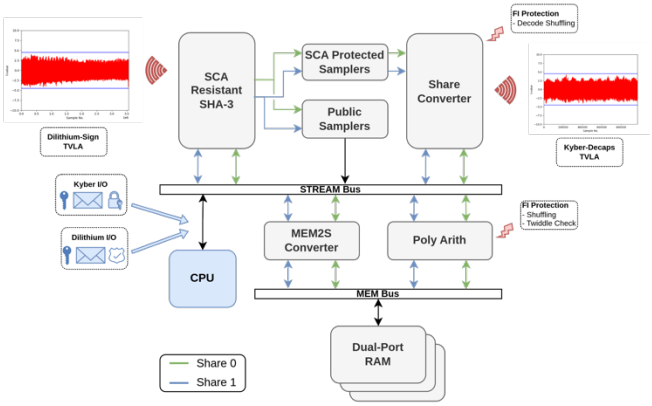

Figure 2. High-level architecture for PQSecure™-CRYSTALS-1000-SCA-FI

Performance

In the below figures, the performance numbers (in terms of cycles) that are independent of type of FPGA are reported. Other results for resource utilization are available upon request. The performance numbers are compared to the software implementations in an ARM Cortex-M4 device with deeply hand optimized assembly results for security level V for illustration. Comparison for all security levels are also available.

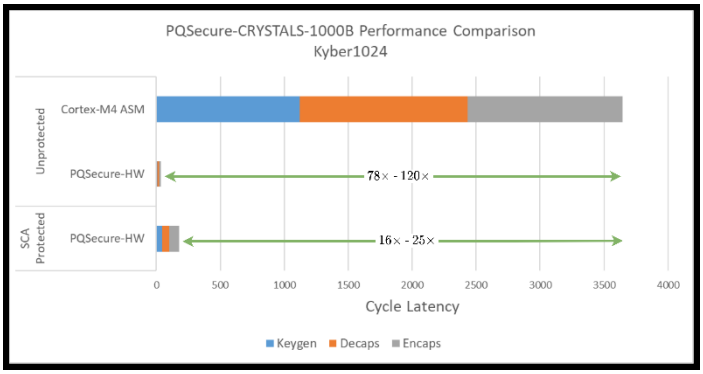

Figure 3. Performance comparisons of PQSecure™-HW with Kyber SW.

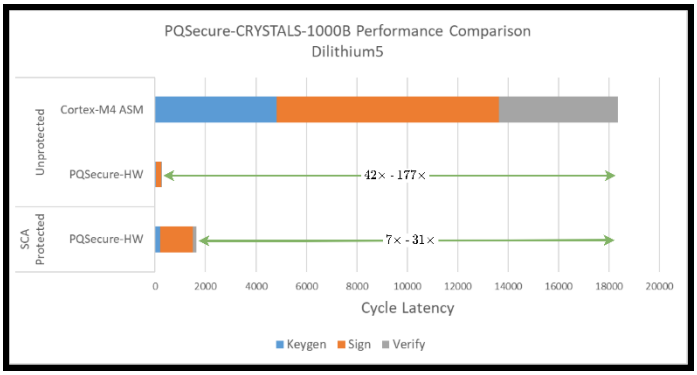

Figure 4. Performance comparison of PQSecure™- HW to Dilithium SW

Deliverables

PQS-CRYSTALS-1000 is available in several formats including netlist, source code (plain and encrypted) with a complete testbench in SystemVerilog with known answer tests (KATs) as per [1,2] for verification, with UVM testbenches, as well as integration data, simulation results and synthesis scripts.

Prototyping Licenses and Support Services

PQSecure™ Technologies offers prototyping licenses for its IPs to be deployed in both software and hardware platforms as well as extensive support services for integration, testing, and validation.

PQSecure

PQSecure™ Technologies, LLC is a leading provider of quantum-safe cryptographic solutions including symmetric and asymmetric algorithms for embedded devices. PQSecure products enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle security (V2V and V2X), networking and communications, cellular base stations (5G and LoRa), satellites, handheld devices, Internet of Things (IoT) and more. PQSecure's hardware and software IP solutions offer various levels of recommended security, size, and performance configurability in numerous markets and applications. PQSecure's post-quantum public key crypto processors enable designers to offload all asymmetric cryptographic operations to hardware and provide support for efficient execution

of various algorithms. PQSecure's innovative and experienced team architects best-in-class products: classical and quantum-safe security coprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators, a comprehensive set of tamper-resistant cryptographic cores with SCA/DPA countermeasures developed internally and patented [7,8,9,10]. Our solutions are available in individual IPs as well as combination of IPs known as PQSecure™ Suite-Q™.

Contact Information

PQSecure Technologies, LLC.
3651 FAU Blvd, #400. Boca Raton, FL 33431 USA, Phone: (201) 844-5743 email: sales@pqsecurity.com

References

[1] Module-Lattice-based Key-Encapsulation Mechanism Standard, Federal Information Processing Standards Publication, FIPS PUB 203, 2023.

[2] Module-Lattice-Based Digital Signature Standard, Federal Information Processing Standards Publication, FIPS PUB 204, 2023.

[3] CNSA Suite 2.0, Commercial national Security Algorithms, Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems, National Securit Agency (NSA), 2022.

[4] Luke Beckwith, Abubakr Abdulgadir, Reza Azarderakhsh, "A Flexible Shared Hardware Accelerator for NIST-Recommended Algorithms CRYSTALS-Kyber and CRYSTALS-Dilithium with SCA Protection", CT-RSA 2023, pp. 469-490, 2023.

[5] Junhao Huang, Jipeng Zhang, Haosong Zhao, Zhe Liu, Ray C. C. Cheung, Çetin Kaya Koç, Donglong Chen: Improved Plantard Arithmetic for Lattice-based Cryptography. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022(4): 614-636 (2022).

[6] Amin Abdulrahman, Vincent Hwang, Matthias J. Kannwischer, Amber Sprenkels: Faster Kyber and Dilithium on the Cortex-M4. ACNS 2022: 853-871, 2022.

[7] US Patent: An area efficient architecture for lattice based key encapsulation and digital signature generation, US17/779,051, 2021, PQSecure Technologies, LLC.

[8] US Patent: A low footprint hardware architecture for Dilithium digital signature scheme, PCT/US2021/029009, 2021, PQSecure Technologies, LLC.

[9] US Patent: Low footprint resource sharing hardware architecture for CRYSTALS-Dilithium and CRYSTALS-Kyber, US11,496,297, 2021, PQSecure Technologies, LLC.

[10] US Patent: Low footprint hardware architecture for Kyber-KEM, US11,632,242, 2020, PQSecure Technologies, LLC.