Synopsys Agile PQC Public Key Accelerators

Highlights

- Agile IP comprised of HW/FW/SW, adaptable to future standards' evolution
- Highly configurable IP can be tuned for specific applications with most optimal PPA
- Scalable PQC PKA IP complies with latest NIST PQC algorithms
  - CRYSTALS-Kyber (FIPS 203)
  - CRYSTALS-Dilithium (FIPS 204)
  - FALCON
  - SPHINCS+ (FIPS 205)
  - XMSS and LMS (SP 800-208)
- Traditional ECC and RSA algorithms support
  - RSA (up to 8192-bit)
  - ECC (up to 1024-bit; NIST, Brainpool, Montgomery, Edwards, SM2, generic Weierstrass)
- Full PQC digital signatures, key encapsulation, key exchange, and encrypt/decrypt functions support
- FIPS 140-3 certification support
- Secure key interface
- Option for DPA/TA and fault injection countermeasures

Target Applications

- NSA quantum resistant CNSA v2.0 suite
- Networking infrastructure
- Industrial control
- Data Centers
- Aerospace & Defense
- Storage
- Automotive
- Consumer, IoT
- Payment card industry
- Secure manufacturing

Overview

The impending development of sufficiently powerful quantum computers will break all ECC and RSA public key cryptographic schemes that are deployed in today's cybersecurity systems. To mitigate this risk, various organizations, including the National Institute of Standards and Technology (NIST), are standardizing cryptographic algorithms that are considered to be secure against both quantum and classical computers, commonly known as post-quantum cryptography (PQC).

Synopsys Agile PQC Public Key Accelerators (PKAs) are quantum safe security IPs that support the computationally intensive operations required for public key infrastructure / asymmetric cryptography, including the latest quantum resistant algorithms selected NIST.

They can adapt to the standards' evolution by efficiently incorporating hardware and embedded firmware, where the hardware accelerates the main cryptographic primitives for performance and power benefits, but the higher-level algorithms are implemented in firmware to provide flexibility for algorithm updates.

Synopsys Agile PQC PKA IP enables designers to protect sensitive data and systems from attacks in the quantum computing era for government, enterprises, and consumers across a wide range of applications from the edge to the cloud.

Synopsys Agile PQC Public Key Accelerator

The high-level block diagram and system level view for Synopsys' Agile PQC PKA IP are depicted in the figure below.

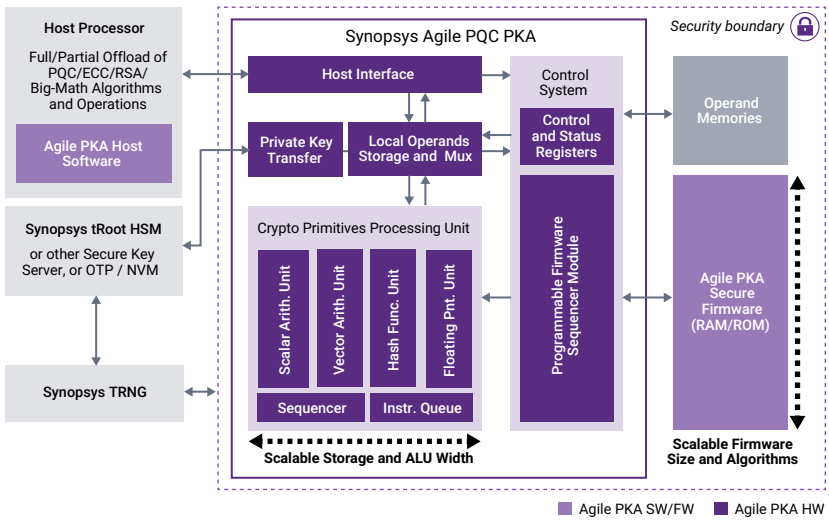

Figure 1: Synopsys Agile PQC PKA Block Diagram and System Level View

Agile PQC PKA Key Features

- Highly configurable PKA supporting fine grain tuning of performance, area, and power for most optimal implementations
- Agile IP, adaptable to future PQC algorithms updates
  - Firmware driven control engine allows for field update of public key algorithms
  - Firmware can be stored in RAM, ROM or be accessible via system initiator interface; combinations may also be selected
- Full support of select key-pair generation, encryption/decryption, digital signatures, key exchange, key encapsulation, and encrypt/decrypt functions
- Scalable PQC PKA supports the latest quantum ready NIST PQC algorithms
  - CRYSTALS—Kyber (FIPS 203; ML-KEM), Lattice based Key Encapsulation Mechanism
    - KYBER512 (ML-KEM-512)
    - KYBER768 (ML-KEM-768)
    - KYBER1024 (ML-KEM-1024)
  - CRYSTALS—Dilithium (FIPS 204; ML-DSA), Lattice based Digital Signature Algorithm
    - Dilithium2 (ML-DSA-44)
    - Dilithium3 (ML-DSA-65)
    - Dilithium5 (ML-DSA-87)
  - SPHINCS+ (FIPS 205; SLH-DSA), Hash based Digital Signature Algorithm
    - SPHINCS+SHA2-128s (SLH-DSA-SHA2-128s)
    - SPHINCS+SHAKE-128s (SLH-DSA-SHAKE-128s)
    - SPHINCS+-SHA2-128f (SLH-DSA-SHA2-128f)
    - SPHINCS+-SHAKE-128f (SLH-DSA-SHAKE-128f)
    - SPHINCS+SHA2-192s (SLH-DSA-SHA2-192s)
    - SPHINCS+SHAKE-192s (SLH-DSA-SHAKE-192s)
    - SPHINCS+SHA2-192f (SLH-DSA-SHA2-192f)
    - SPHINCS+SHAKE-192f (SLH-DSA-SHAKE-192f)
    - SPHINCS+-SHA2-256s (SLH-DSA-SHA2-256s)
    - SPHINCS+-SHAKE-256s (SLH-DSA-SHAKE-256s)
    - SPHINCS+-SHA2-256f (SLH-DSA-SHA2-256f)
    - SPHINCS+-SHAKE-256f (SLH-DSA-SHAKE-256)
  - XMSS and LMS (SP 800-208), Hash based Digital Signature Algorithms
  - FALCON, (FIPS draft planned for 2024), Lattice based Digital Signature Algorithm
- Support for NSA CNSA v2.0 Quantum Resistant Commercial National Security Algorithm suite
  - CRYSTALS-Kyber and CRYSTALS-Dilithium (asymmetric algorithms for key establishment)
  - XMSS and LMS (asymmetric algorithms for digitally signing firmware, software, others)
- Support for traditional RSA and prime ECC algorithms
  - RSA 2048/3072/4096/8192-bit
  - ECC
    - NIST: fips186p244, fips186p256, fips186p384, fips186p521
    - Brainpool: brainpool256r1, brainpool384r1, brainpool512r1
    - SM2
    - Montgomery: C25519, C448
    - Edwards: Ed25519, Ed448
    - Generic Weierstrass: 160/192/224/256/320/384/512/521/1024-bit modulus

- FIPS 140-3 security certification support
- Secure private key handling for import and export of private keys to an external Secure Key Server
- Secure configuration via bus security signal (e.g. arm TrustZone support)
- Protection against physical attacks
  - Option for DPA/TA and Fault Injection countermeasures

The area and performance of the Synopsys Agile PQC PKAs are highly dependent on the configuration selected. For specific benchmarks, contact Synopsys.

Deliverables

- Verilog HDL
- Firmware and host software
- Testbench and sample simulation script
- Sample synthesis script and constraints
- Documentation

About Synopsys IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad Synopsys IP portfolio includes logic libraries, embedded memories, PVT sensors, embedded test, analog IP, wired and wireless interface IP, security IP, embedded processors, and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP software development kits, and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support and robust IP development methodology enable designers to reduce integration risk and accelerate time-to-market.

For more information on Synopsys IP, visit synopsys.com/ip.