Device and Data Security IP

EnSilica provide a comprehensive range of encryption and authentication IP for ASIC and FPGA targets, that offer a range of throughput and resource usage trade-offs, in order to meet different system requirements. IP development and testing has been based on widely accepted cryptographic standards published by NIST, FIPS and IEEE.

The IP has a proven record in production silicon System level functionality of the IP has also been proven through integration in popular open source SSL/TLS software libraries and the IP available as stand-alone or as AMBA APB/AHB/AXI peripherals. The algorithms include:

- CRYSTALS Kyber
- ECC / ECDSA
- RSA
- AES
- TRNG
- CRYSTAL Dilithium
- SHA
- CHACHA20 & POLY1305
- TDES

CRYSTALS

Cryptographic Suite for Algebraic Lattices (CRYSTALS) encompasses two cryptographic primitives, Kyber, a secure KEM, and Dilithium, a strongly EUF-CMA-secure digital signature algorithm both selected by NIST as part their Post-Quantum Cryptography (PQC) standards. PQC are algorithms built to withstand attacks from quantum computers. As quantum computers advance, there is a real threat they will break the current public key-based cryptography used in today's secure communications and financial transactions.

RSA

RSA is a public key cryptography standard that is widely used in smartcards, certificate authority servers, gateways and handheld devices.

EnSilica offers a low gate count RSA IP for accelerating all modular arithmetic operations that are used within RSA based cryptographic protocols.

ECC & ECDSA

ECC is a public key cryptography approach that benefits from the same level of security as RSA but using smaller key sizes. Elliptic curves are commonly used in digital signatures for signing and verification (ECDSA) and establishing a shared secret (key) between communicating parties. 3 variants are offered providing the same functionality but with different splits between software and hardware. ECC-lite and ECDSA also include high throughput implementation options, in order to cover a wider range of application requirements.

Feature	ECC - Micro	ECC-Lite	ECDSA
Supported Curves	All commonly used GF(p) curves (NIST, SEC2, Brainpool		
Key sizes supported	Any key size upto 521		
RAM requirements	No		
CPU Interface	APB with Independent APB & processing clocks		
Basic GF(p) Op. support	HW	HW	HW
EC Op. support (ECD, ECA,ECSM)	SW	HW	HW
ECDH support (ECSM)	SW	HW	HW
ECDSA sign and verify	SW	SW	HW
Public key validation	SW	SW	HW

AES

The Advanced Encryption Standard (AES) is an encryption algorithm originally intended for securing sensitive but unclassified material. Since the publication of FIPS-197, it has been widely adopted by commercial and private organization.

EnSilica offers configurable AES IP that allows for different selections between functionality and silicon area.

The IP supports commonly used AES chaining modes, uch as CBC, CTR, CMAC, CCM, GCM, and also an optional DMA interface. The IP performs a raw encryption/ decryption operation in 14 to 18 clock cycles, depending on the selected key size. A high throughput fully pipelined AES-ECB architecture is also available.

TRNG

An essential part of any cryptographic solution is a high quality True Random Number Generator (TRNG). TRNG provides the raw entropy source for generating private keys used by encryption and authentication protocols.

Ensilica offers a ring-oscillator based TRNG IP that generates blocks of 256 random bits. The IP is compliant with NIST 800-22 for verifying the randomness of the generated data. A CPU can interface to the IP through an AMBA APB or AHB interface. The ring-oscillator component of the IP is supplied as hard macro in the target technology.

SHA

SHA is a family of hash algorithms designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) under FIPS-180-4 and FIPS-202. It was originally designed to be a part of the Digital Signature Algorithm (DSA). SHA1 operates on 512-bit message blocks to update a 190-bit hash value. This was enhanced under SHA2 for 224, 256 and higher hash lengths. A new SHA3 algorithm has also be recently introduced covers by FIPS-202 standard.

EnSilica provides a sophisticated range of SHA related IP for use in ASIC or FPGA target technologies. There are variants of each SHA family with either APB or AHB interfaces.

CHACHA20 & POLY1305

CHACHA20 & POLY105 are two new high speed stream cipher and authentication algorithms that can be used as an alternative to more traditional algorithms, for authentication. CHACHA20 & POLY105 have also been specified for use in the TLS protocol as a new ciphersuite within RFC7905.

EnSilica offers several different options for CHACHA20 & POLY1305, either as individual IP or combined into a single IP. Different configuration options are also provided which allow selecting the most suitable resource/ performance balance for the intended application:

- CHACHA20 High Throughput - 13 cycles per 64 bytes of data
- CHACHA20 Low Area - 23 cycles per 64 bytes of data.
- POLY1305 High Throughput - 4 cycles per 16 bytes of data
- POLY1305 Balanced - 8 cycles per 16 bytes of data
- POLY1305 Low Area - 20 cycles per 16 bytes of data

TDES

Triple Data Encryption Algorithm block cipher. This applies the DES cipher algorithm three times to each data block to overcome key size restrictions in the original DES cipher. Although DES and specifically TDES are secure in practical applications the more modern AES is now commonly used instead. For legacy systems and backwards compatibility, the DES and TDES are still commonplace and require hardware support for efficient calculation.

SNOW3G

The SNOW 3G algorithm which is at the core of 3GPP confidentiality and integrity algorithms UEA2 and UIA2, and specified in ETSI/SAGE Version 1.1.

SNOW 3G is a word oriented stream cipher that generates a sequence of 32-bit words under the control of a 128-bit key and a 128-bit initialization vector. The words are used to mask Plaintext. First a key initialization is performed, and then with every clock tick it produces a new 32-bit output word. The implementation is very efficient in both FPGA and ASIC, being a combination of an LFSR and a finite state machine. Target applications include LTE/3GPP.

© 2023 EnSilica All Rights Reserved. EnSilica and the EnSilica logos are trademarks or registered trademarks of EnSilica. This material is subject to change without notice.