Ultra High-Performance AES-XTS/ECB Cryptographic Cores

Highlights

- Scalable high-performance & low latency AES-XTS/ECB cores with efficient support for varied networking traffic
- Standards compliant: NIST SP800-90-38E and IEEE Std 1619-2018
- Two customer configurable IP cores with scalable throughput
  - 64 bits/cycle, 128 bits/cycle (up to 128 Gbps @ 1 GHz)
  - 256 to 4096 bits/cycle (up to 4 Tbps @ 1 GHz)
- Encrypt/Decrypt/Bypass
- Modes: AES-XTS, AES-ECB
- 128 & 256-bit AES key sizes
- NIST FIPS 140-3 security certification ready. Passed NIST CAVP validation.
- One tweak/cycle precomputation
- Latency as low as 4 cycles
- Up to 64K crypto contexts
- Message interleaving
- Secure key port
- Multi-clock domain
- Configurable CipherText Stealing (CTS) support
- Random memory block sequence access
- Optional support for OSCCA SM4-XTS

Target Applications

- Memory and storage security for High-Performance Computing (HPC), Data Centers, Mobile, and IoT
- DDR/LPDDR, HBM
- SSD, HDD, UFS

Overview

Memory and storage security involves protecting storage resources and the data stored on them, both on-premises and in external data centers and the cloud.

With the tremendous data and bandwidth growth in our connected world, security is essential to protect private and sensitive data as it moves across systems to storage, including memory. While the volume and variety of data are growing, so is the need for higher capacity, faster access, and accelerated processing. Designers are turning to high-performance, low-latency memory encryption solutions to preserve performance while protecting data over the latest generations of DDR, LPDDR, GDDR, and HBM memory interfaces.

AES-XTS, or as it is sometimes referred XTS-AES, is the de-facto cryptographic algorithm for protecting the confidentiality of data-at-rest on storage devices. It is a standards-based symmetric algorithm defined by NIST SP800-38E and IEEE Std 1619-2018 specifications. It allows for pipelined architectures that can scale in performance to Terabits per second (Tbps) bandwidth.

Synopsys Ultra High-Performance AES-XTS/ECB Cores

Synopsys offers two high performance configurable AES-XTS IP cores to give customers options to configure and tune the optimal solution for their application (Figure 1 and Figure 2):

- Synopsys High-Performance AES-XTS/ECB Core supporting up to 128 bits/cycle throughput (e.g., 128 Gbps @ 1 GHz; scales linearly with the maximum frequency achievable in a particular process)
- Synopsys Ultra High-Performance AES-XTS/ECB Core supporting from 256 bits/cycle to 4096 bits/cycle throughput, in 128 bits/cycle increments throughput (e.g., 4 Tbps @ 1 GHz; scales linearly with the maximum frequency achievable in a particular process)

The Ultra High-Performance AES XTS/ECB Cores are based on a pipelined architecture that allows the performance to scale efficiently to Tbps throughput for various data traffic patterns, while keeping the latency and area as low as possible even for multiple cryptographic contexts in flight, and to achieve high operating frequencies in advanced process nodes.

In addition to being standards compliant, Synopsys' Ultra High-Performance AES-XTS Cores support encryption and decryption for all key sizes, allow for seamless context switching for a high number of contexts, support efficient keys setup/refresh, are FIPS 140-3 certification ready and passed NIST CAVP validation.

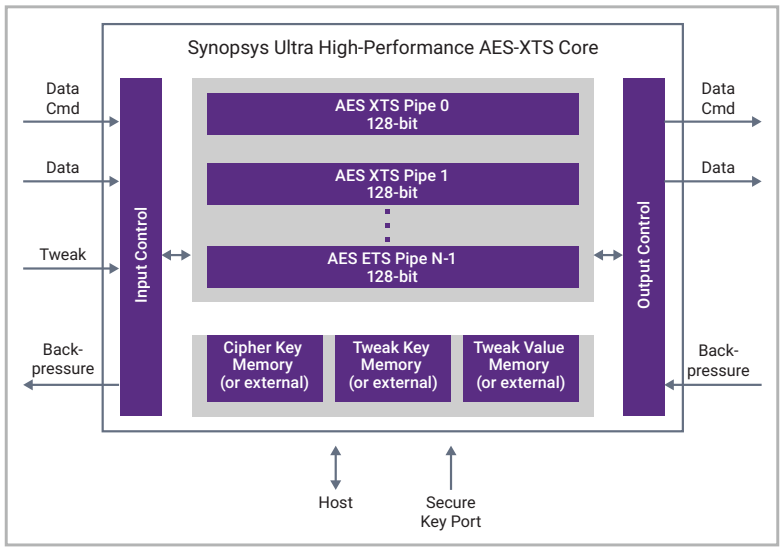

Figure 1: Synopsys Ultra High-Performance AES-XTS Crypto IP Block Diagram

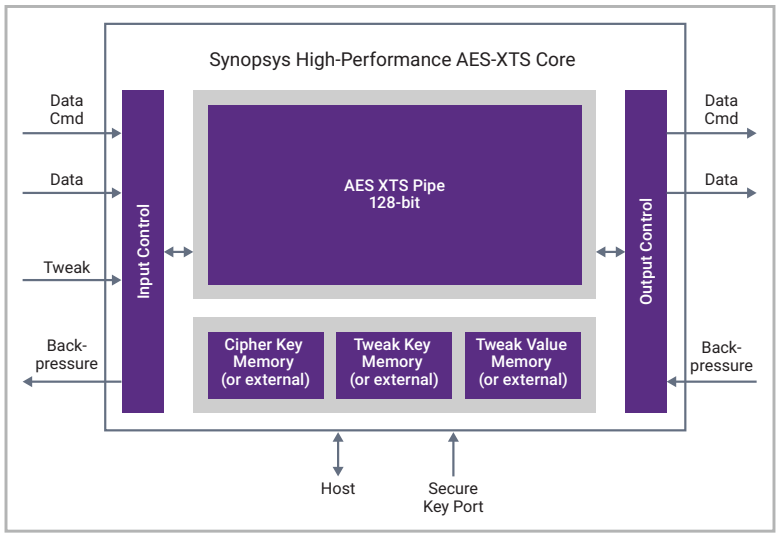

Figure 2: Synopsys High-Performance AES-XTS Crypto IP Block Diagram

Synopsys' Ultra High-Performance AES-XTS Cryptographic Cores provide designers the configurability needed to adjust to the SoC designs' specific use cases and performance requirements, taking advantage of key features including:

- Efficient unidirectional and bidirectional encryption and/or decryption modes of operation for AES-XTS and AES-ECB
- Support for 256-bit key length (NIST SP 800-38E XTS-AES-128) and 512-bit key length (NIST SP 800-38E XTS-AES-256)
- Bypass mode
- Optimal latency by architecture design and options to further reduce it via parametrizable number of AES rounds per cycle
- Secure key loading via a dedicated secure key port
- Data unit size support of up to 16MiB
- 1 tweak per cycle maximum precomputation tweak rate

- Two-port and single-port memories to support multiple applications requirements
- Parametrizable memory access latency for ECC support
- Support for up to 64k interleaved data streams
- Support for Inline Memory Encryption and other applications with random block sequence accesses
- Support for FIPS 140-3 security certification. Passed NIST CAVP validation
- Multiple clock domains support: host, secure key port, core
- Area, performance, and maximum frequency optimization options
- Configurable CipherText Stealing (CTS) support
- Path for seamless full duplex inline memory encryption integration with memory interface controllers, including latest generations DDR4/LPDDR4, DDR5/LPDDR5, and HBM
- Optional support for OSCCA SM4-XTS

Size and Performance

The Ultra AES-XTS/ECB cores deliver an optimized gate count for the required performance level, size, and frequency of the target application. The performance can scale up to 4096 bit/cycle with a minimum latency of 4 cycles. The gate count is dependent on the selected configuration and specific process parameters and can range from hundreds to thousands of kgates.

Synopsys Security IP

Synopsys offers a broad portfolio of silicon-proven Cryptography IP solutions, including symmetric and hash cryptographic engines, Public Key Accelerators (PKAs), and True Random Number Generators (TRNGs). The hardware and software security implementations are highly configurable, cover a broad spectrum of size and performance combinations, and are available in different architectures, such as look-aside or flow-through.

Synopsys' other Cryptography AES products are:

- Ultra High-Performance AES-GCM/CTR Core
- High-Performance AES-GCM/CTR Core
- Multipurpose Security Protocol Accelerator (SPAcc)

Deliverables

- Verilog HDL
- Testbench
- Sample synthesis script & constraints
- Sample simulation script
- 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 prototyping kits, 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.

SYNOPSYS®

03/10/23.CS1065231729-UHP-AES-XTS-ECB-DS.