EMBEDDED
SECURITY IP
& SOFTWARE

SafeXcel-IP-38

Semiconductor IP for High-speed AES, AES-GCM and AES-XTS encryption and decryption

→ INSIDE Solutions

Key Features

- High throughput AES-based encryption/decryption datapath
- AES 128/192/256 key size
- AES modes ECB, CBC, CFB (1-8-128), OFB (128), CTR, ICM, GCM, LRW, XTS
- Optimized AES-XTS (with CTS) only configuration with efficient key switching
- Targeting storage and networking devices
- Easily integrated into SoCs
- Flexible layered design
- Wide range of performance configurations
- Optional Data Path Integrity feature protecting against single bit faults

Cryptographic Acceleration for Storage and Networking Devices

The SafeXcel-IP-38 AES/GCM/XTS Accelerators are specifically suited for next generation processors deployed in storage and networking appliances that need to support combinations of AES (with its regular feedback modes), AES-GCM, and AES-XTS. The SafeXcel-IP AES/GCM/XTS Accelerators not only meet challenging requirements for very high throughput, but also for fast integration and cost effectiveness.

Get to Market Faster with Security IP that Fits Your Design

Get to market quickly with security IP that is optimized for your design, providing the features you need without the expense and schedule impact of special development work. INSIDE Secure has AES encryption/decryption choices for low gate count, low power designs, as well as configurations for very high performance requirements. Designed for full scalability and an optimal performance over gate count ratio, these choices address a range of needs for semiconductor OEMs and provide a reliable and cost-effective IP solution that is easy to integrate into SoC designs. INSIDE's experts in cryptographic IP will work with your design team to help you select the optimal set of modules for your unique requirements.

All of INSIDE Secure's semiconductor IP modules are delivered as synthesizable Verilog RTL source code, with self-checking RTL test bench, including test vectors and expected result vectors, as well as simulation scripts and synthesis scripts.

High Performance Algorithms Exploiting Parallelism

While the AES algorithm was designed for high-speed implementations, its regular feedback modes such as CBC, CFB, and OFB are not ideal in very high-speed storage and networking applications. The AES-GCM and AES-XTS algorithms do not use these regular AES feedback modes. They support very high-speed encryption and authentication by enabling implementations that use of parallelism.

Typical uses cases for AES-GCM and AES-XTS are high-speed transmission (virtual private networking) and disk storage (protection of data at rest). For transmission protection, AES-GCM can implement authenticated encryption at the network layer (IPsec) or at the data link layer (MACsec IEEE 802.1ae). AES-XTS has been adopted by IEEE P1619 for protection of data at rest.

In the optimized AES-XTS only cores for storage solutions, the tweak key generation as well as the Cipher Text Stealing functionality is implemented to comply with disk based storage solutions where the plain text data block cannot be expanded with additional bytes during the encryption process (due to fixed block sizes). The implementation of multiple AES engines (1-5-8-14 AES cores) inside one single EIP-38 AES-XTS core saves a significant number of gates compared to regular duplication of AES-XTS logic.

driving trust™ inside SECURE

www.insidesecure.com

Configuration Flexibility

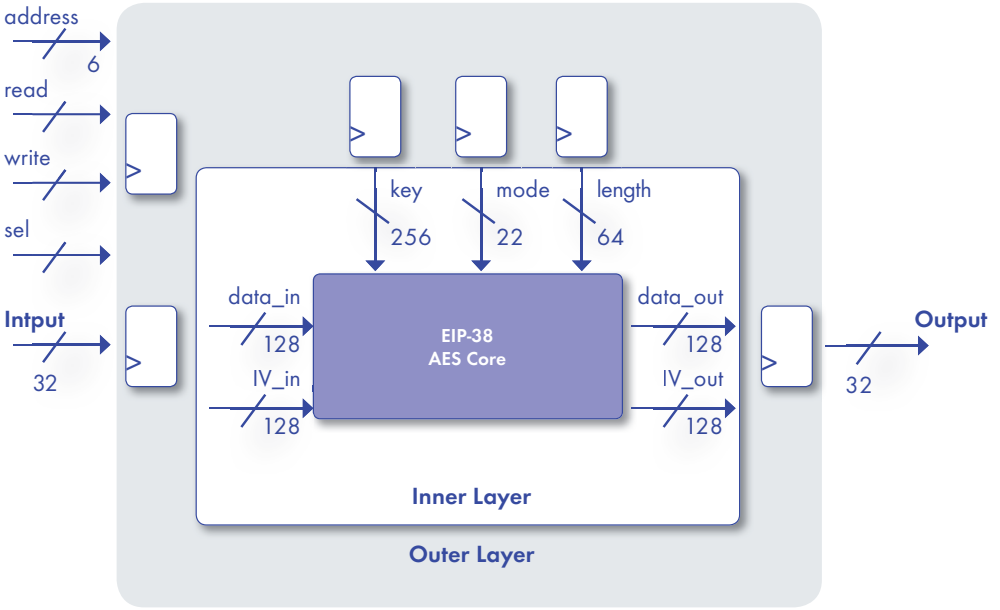
The SafeXcel-IP-38 is available in different configurations, suitable for different applications, and for meeting different gate count and throughput objectives. There are single IP core configurations and multiple IP core configurations using parallelism for higher throughput. Inside also provides various other SafeXcel-IP AES accelerators that do not support AES-GCM and AES-XTS.

Configuration	AES Modes	# of AES cores	Max Freq. (MHz)	Gate Count (K Gates)	AES-128 Bits/cycle	AES-128 At Max Freq (Gbits/s)
EIP-38b	All	1	900	125	12.8	11.5
EIP-38f	All	5	950	290	64	60.8
EIP-38o	All	14	850	664	128	109
EIP-38b-gcm	GCM/CTR/ OFB/CFB	1	900	90	12.8	11.5
EIP-38x-1	XTS/ECB	1	900	135	12.8	11.5
EIP-38x-5	XTS/ECB	5	950	280	64	60.8
EIP-38x-6	XTS/ECB	8	850	395	102	86.7
EIP-38x-14	XTS/ECB	14	850	630	128	109
EIP-38x-8-DI	XTS/ ECB+Integrity	8	900	474	12.8	11.5

SafeXcel-IP-38 Configuration Information (for TSMC 28 nm technology)

Flexible, Layered Design

In order to provide full flexibility and ease of use, the AES/GCM/XTS accelerators feature a layered design. The "inner layer", the Engine, provides "wide bus interfaces" for Mode, Initialization Vector (128 bit IVs), Keys (256 bit), and Data (128 bit). These "wide bus interfaces" allow optimal data throughput and extremely fast context switching (that is, use of new Mode, IV, and Key values). For the non-high speed cores (EIP-38b, EIP38b-gcm, and EIP-38x-1) an "outer layer" is available. This "outer layer" has a 32- bit wide register interface. The input and output buffer registers inside the "outer layer" allow for pipelining. Input data and context information can be written and output data can be read while the Engine is performing an AES/GCM/XTS operation at the same time. This way, optimal throughput is achieved using a 32-bit register interface. The lower speed cores provide customers with the flexibility to be used with or without the without the "outer layer" to achieve the optimal performance. The high-speed cores (EIP- 38f, EIP-38o, EIP-38x-5, EIP-38x-8, and EIP-38x-14) that only have the "inner layer" should be integrated inside a customer data path for an optimized performance.



SafeXcel-IP-38 LayeredDesign

Data Integrity Protection

On request, the AES-XTS only configurations are available with a Data Integrity Protection option. In storage solutions where data is committed to solid state disks or hard disk drives for long term Data-at-Rest storage, assurance of the integrity of the committed data is paramount. In SATA, SAS or RAID controllers this feature is already available in the regular non encrypted data paths. Adding a crypto core in this data path breaks the integrity scheme.

Inserting the EIP-38 with DI protection builds on top of the existing integrity implementation and extends it, with protection similar to regular byte parity, through the AES data and key paths. Since the AES implementation does not work with regular parity logic, a dedicated solution is offered, with significant gate count savings compared to a redundant AES implementation. This implementation includes observation and control logic to test the integrity logic.