

**EIP-38: Silicon-proven  
Intellectual Property (IP)  
for high-speed AES, AES-GCM, and  
AES-XTS encryption and decryption**

### BENEFITS

- High-speed AES-XTS/AES-LRW/AES-GCM solution
- Silicon-proven implementation
- Fast and easy to integrate into SoCs
- Flexible layered design
- Complete range of configurations
- World-class technical support

Even though the Advanced Encryption Standard (AES) algorithm was designed to allow high-speed implementations, its regular feedback modes such as CBC, CFB, and OFB are not ideal for supporting very high-speed networking applications. The AES-GCM and AES-XTS algorithms do not use these regular AES feedback modes and allow very high-speed encryption and authentication by enabling an implementation to make 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 for instance implement authenticated encryption at the network layer (IPsec) or at the data link layer (MACsec).

As part of AuthenTec's award-winning silicon Intellectual Property (IP) product portfolio, the SafeXcel™ IP AES/GCM/XTS Accelerators are specifically suited for next generation processors deployed in networking and storage 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 do not only meet vendor requirements for very high throughputs, but also for fast integration and cost-effectiveness.

### Ease of Integration

Years of experience in designing silicon security products made AuthenTec the leading vendor of complete, reliable, and high-quality IP products, featuring cost-efficient designs and user-friendly product interfaces. This allows integrators to optimally utilize the product's capabilities and performance. In addition, AuthenTec's global presence and expertise in security and silicon design enables AuthenTec to provide our customers with world-class on-site support, ensuring the success of your project.

### AES-GCM and AES-XTS Acceleration

The AES-GCM (Galois Counter Mode) has, since its publication in 2005, been used in many IPsec and MACsec applications. It is a very efficient algorithm, suitable to achieve very high performances. AES-XTS has been adopted by IEEE P1619 for protection of data at rest.

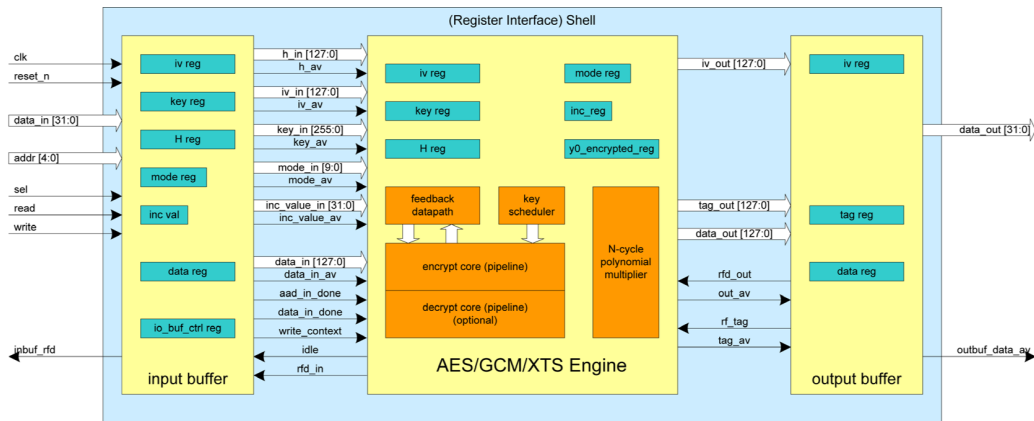
### Flexible, layered design

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 (IVs), Keys, and Data. 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-38a up to EIP-38e) an outer layer is available. This outer layer has a 32-bit wide register interface. The input and output buffer registers inside the Shell 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, maximum 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 Shell. The high-speed cores (EIP-38f up to EIP-38i) must be integrated without the Shell to achieve the optimal performance. Customers can also use the Shell logic as a basis for building a customized, width-constrained interface.

### Configuration flexibility

The SafeXcel IP AES/GCM/XTS Accelerators are available in different configurations, suitable for different applications, and for meeting different gate count and throughput objectives. AuthenTec also provides various SafeXcel IP AES accelerators that do not support AES-GCM and AES-XTS. A separate Product Brief is available for these AES-only accelerators.



SafeXcel IP AES/GCM/XTS Accelerator Architecture

NAME	CONFIGURATION <sup>3</sup>	MAX CLOCK FREQUENCY <sup>1</sup>	THROUGHPUT WITH 128 BIT KEY <sup>2</sup>		APPROXIMATE ENGINE GATE COUNT <sup>1</sup> AT 250 MHZ CLOCK FREQUENCY
			AT ANY CLOCKFREQUENCY (IN BITS/CYCLE)	AT MAX CLOCK FREQUENCY	
EIP-38a	AES/GCM/LRW/XTS encrypt/decrypt	330 MHz	2.46	812 Mbit/s	86 kGates
EIP-38b	AES/GCM/LRW/XTS encrypt/decrypt	330 MHz	12.8	4.2 Gbit/s	125 kGates
EIP-38c	AES/GCM encrypt-only	330 MHz	12.8	4.2 Gbit/s	97 kGates
EIP-38d	AES/GCM/LRW/XTS encrypt/decrypt	366 MHz	25.6	9.4 Gbit/s	215 kGates
EIP-38e	AES/GCM encrypt-only	366 MHz	25.6	9.4 Gbit/s	190 kGates
EIP-38f	AES/GCM/LRW/XTS encrypt/decrypt	366 MHz	64	23 Gbit/s	375 kGates
EIP-38g	AES/GCM encrypt-only	366 MHz	64	23 Gbit/s	240 kGates
EIP-38h	AES/GCM/LRW/XTS encrypt/decrypt	328 MHz	128	42 Gbit/s	595 kGates
EIP-38i	AES/GCM encrypt-only	328 MHz	128	42 Gbit/s	355 kGates

<sup>1</sup> Technology and synthesis dependent; based on the use of a basic design compiler and a 0.13m technology.

<sup>2</sup> ECB, CTR, GCM, CBC-decrypt and CFB-decrypt throughputs (where supported). XTS, LRW, CBC-encrypt, and CFB-encrypt (where supported) have a throughput of 1.75 bits/cycles (EIP-38a) and 11.6 bits/cycle (EIP-38b/c).

<sup>3</sup> Next to the AES-XTS functionality, AES-LRW is included as defined in draft 5 of the IEEE P1619 standard for reasons of backwards compatibility

<sup>4</sup> 'encrypt only', only applies for the basic ECB and CBC mode of operation, the other modes can always be performed in both directions

SPECIFICATIONS

Features

- Supported key sizes: 128, 192, 256 bits
- Includes feedback mode logic
- Various configurations available with support for:
  - Electronic Code Book (ECB), Cipher Block Chaining (CBC), 128-bit Output Feedback (OFB), 1-bit, 8-bit, and 128-bit Cipher Feedback (CFB), Counter (CTR)
  - AES Galois Counter Mode (AES-GCM), using AES-CTR mode and GHASH
  - Basic GHASH
  - Liskov Rivest Wagner (AESLRW)
  - AES-XTS
- Fully synchronous design
- Includes key scheduling hardware

Deliverables

- Synthesizable Verilog RTL source code
- Various pre-compute options are available for GCM and XTS
- Self-checking RTL test bench, including test vectors and expected result vectors
- Simulation script
- Synthesis script
- User's Manual with technical specifications, including the programmer's interface
- Developer's Manual with step-by-step descriptions that allows developers to easily install, verify, and synthesize the design

HEADQUARTERS

AuthenTec, Inc.  
100 Rialto Place, Suite 100  
Melbourne, FL 32901 USA  
Phone: +1-321-308-1300

For more information on Embedded Security Solutions Email us at: [embedded@authentec.com](mailto:embedded@authentec.com)

WORLDWIDE REPRESENTATIVES NETWORK  
A complete listing of AuthenTec's network of representatives is available at our web site.

[www.authentec.com](http://www.authentec.com)