Security IP Product Selection Guide

Common Features

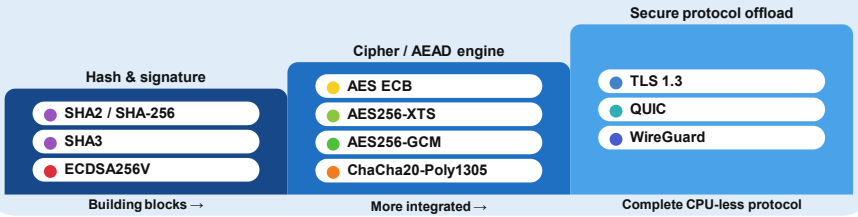
- Standards-based (RFC / NIST / FIPS)
- High throughput
- Free evaluation demo
- Rich document

Supported FPGA Devices

AMD

Versal HBM / Versal Premium /
Versal AI Core / Zynq UltraScale+ /
Kintex UltraScale+ / Virtex UltraScale+ /
Kintex UltraScale / Artix-7

Security Layer Guide



Application-Based Security IP Core Selection

Application	Key Feature	Suitable IP Core	Available Demo	Link
Secure Web & Cloud Connection (HTTPS, TLS 1.3, CPU-less)	**HW fully TLS 1.3 Server** • AES256-GCM, X25519, RSA	*TLS1.3 Server 10G* **IP Core**	• HTTPS server with web browser: upload / download • Speed test with PC client application	AMD Click for AMD
	HW fully TLS 1.3 Client • AES256-GCM, X25519, RSA / ECDSA • External handshake support	*TLS1.3 Client 10G / 1G* **IP Core**	• HTTPS client with node.js server: upload / download • Speed test • Accelerated Lynx web browsing	AMD Click for AMD
Secure Transport over Lossy Networks (QUIC, 5G/6G, drone, tele-surgery)	**HW fully QUIC Client** • 0-RTT, customizable multi-stream • TLS 1.3 + UDP/IP + ARP built in	*QUIC Client 10G / 1G* **IP Core**	• HTTP/3 client with aioquic server • Custom app protocol client with MsQuic server: upload / download	AMD Click for AMD
	HW fully QUIC Server • RFC 9000 • Customizable multi-stream	*QUIC Server 10G* **IP Core**	• Custom app protocol server with MsQuic client: upload / download	AMD Click for AMD
Secure Data Storage (NVMe / SATA SSD, AES-XTS)	**HW fully AES256-XTS, NVMe speed** • Gen3 / Gen4 / Gen5 (1X / 2X / 4X) • Auto IV every 512 byte (LBA)	*AES256-XTS-STG* **IP Core (1X / 2X / 4X)**	• Encrypt / decrypt between two memories • With NVMe IP: encrypted write / decrypted read of NVMe SSD	AMD Click for AMD
	HW fully AES256-XTS, ciphertext stealing • Up to 51.2 Gbps • Any length ≥ 16 byte	*AES256-XTS* **IP Core**	• Encrypt / decrypt between two memories	AMD Click for AMD
Network & Link Encryption (AEAD & VPN: GCM, ChaCha20, WireGuard)	**HW fully AES256-GCM AEAD** • Up to 138.24 Gbps (100G) • 1G / 10G / 25G / 100G Ethernet	*AES256-GCM 1G / 10G25G / 100G* **IP Core**	• Encrypt / decrypt between two memories with authentication tag • NIST test-vector validation	AMD Click for AMD
	HW fully ChaCha20-Poly1305 AEAD • RFC 8439; 128 Mbits/MHz • Lite: smaller (4.5K vs 11.4K LUTs)	*ChaCha20-Poly1305 / Lite* **IP Core**	• Encrypt / decrypt between two memories with authentication tag	AMD Click for AMD
	HW fully WireGuard VPN • ChaCha20-Poly1305, X25519, BLAKE2s • 10G / 1G, internal handshake	*WireGuard10G / 1G* **IP Core**	• Point-to-point tunnel with PC WireGuard software • Selective encapsulation via GUI • PC-to-PC throughput test	AMD Click for AMD
Custom Mode of Operation (ECB core; CTR / CBC by extension)	**HW fully AES ECB, highest throughput** • 51.2 Gbps @400 MHz • 128-bit per clock	*AES256-SS* **IP Core**	• Encrypt / decrypt between two memories	AMD Click for AMD
	HW fully AES ECB, compact • AES256 (15 clk) / AES128 (11 clk) • Up to 5.8 Gbps	*AES256 / AES128* **IP Core**	• Encrypt / decrypt between two memories	AMD Click for AMD
Authentication & Integrity (signature verify, hash)	**HW fully ECDSA P-256 verify** • FIPS 186-4	*ECDSA256V* **IP Core**	• Verify P-256 signature from user inputs • NIST test-vector compliance test • SSL certificate verification example	AMD Click for AMD
	HW fully SHA-2 hash • SHA-224 to SHA-512 • SHA-256 IP: smallest footprint	*SHA2 / SHA-256* **IP Core**	• Hash custom input messages with performance measurement	AMD Click for AMD
	HW fully SHA-3 hash • FIPS 202: SHA3-224/256/384/512, SHAKE128/256 • Over 17.5 Gbps @316 MHz	*SHA3* **IP Core**	• SHA-3 / SHAKE hashing of custom messages with performance test	AMD Click for AMD

Device lists show families with free evaluation demos; other devices on request – please contact Design Gateway. Key Feature: engine / spec / support. Details: see each datasheet.

AES256-GCM vs ChaCha20-Poly1305 IP Selection Guide

AES256-GCM

Pros

- **FIPS / NIST-approved** (SP 800-38D); AES-256 meets CNSA-grade requirements
- **Highest throughput**: up to 138.24 Gbps, 512 Mbits/MHz at 100G
- **Default suite** in TLS 1.3, MACsec, IPsec: widest peer interoperability

Cons

- **Area grows with line rate**: parallel AES rounds plus GHASH multipliers
- **Needs AES instructions on peers** for speed; slow on CPUs without them

ChaCha20-Poly1305

Pros

- **ARX-only design**: no S-box or lookup tables, simple datapath
- **Compact**: Lite 4.5K LUTs, 14.22 Mbits/MHz (3.4 Gbps @240 MHz)
- **The WireGuard cipher**: mandatory in WireGuard VPN; IETF standard (RFC 8439)

Cons

- **Not FIPS-approved**: unusable where FIPS 140 / CNSA is mandatory
- **Lower ceiling**: 25.6 Gbps @200 MHz; no 100G variant in DG lineup

How to Choose

1	FIPS 140 / CNSA compliance required?	AES256-GCM
2	Need more than 25 Gbps?	AES256-GCM (10G25G / 100G)
3	Protocol fixed by peer?	WireGuard → ChaCha20-Poly1305 TLS / MACsec / IPsec → GCM
4	Tight area, 1G-class, IoT / mobile peers?	ChaCha20-Poly1305 (Lite)
5	None of the above	AES256-GCM (widest interop)

Both: 256-bit key, 96-bit IV, zero-length AAD / data. Never reuse a key + IV pair.

Selection Criteria: AES256-GCM vs ChaCha20-Poly1305

Selection Criterion	AES256-GCM	ChaCha20-Poly1305	Choose
Compliance (FIPS 140 / CNSA, finance, gov.)	Approved: NIST SP 800-38D, AES-256	Not FIPS-approved (check your scheme)	**AES256-GCM**
Peak throughput (DG IP)	138.24 Gbps (100G); 512 Mbits/MHz	25.6 Gbps @200 MHz; 128 Mbits/MHz	**AES256-GCM above ~25 Gbps**
Low-rate link (1G class)	3.2 Gbps	Lite: 3.4 Gbps	**Either: decide by area / compliance**
FPGA area (AMD Zynq US+ datasheets)	1G: 6.8K LUTs; 10G25G: 19.2K LUTs	Lite: 4.5K LUTs; standard: 11.4K LUTs	**ChaCha20 Lite at 1G class**
Protocol / ecosystem	TLS 1.3, MACsec, IPsec: default suite	WireGuard (mandatory); optional suite in TLS / QUIC / SSH	**Follow the protocol**
Peers without AES instructions	Slow in software on such peers	Fast in software on any CPU	**ChaCha20-Poly1305**
Key / IV / authentication	256-bit, 96-bit IV, GHASH tag	256-bit, 96-bit IV, Poly1305 tag	**Equal security level**

Design Gateway IP Cores by Algorithm

Application	Key Feature	Suitable IP Core	Available Demo	Link
AES256-GCM Family (compliance, 1G – 100G) 	**High performance**: 512 Mbits/MHz, up to 138.24 Gbps (100G) • FIPS-approved AES-256 GCM; NIST SP 800-38D verified	***AES256-GCM 10G25G / 100G IP Core***	• Encrypt / decrypt between two memories with authentication tag • NIST test-vector validation	AMD Click for AMD
	Compact: 3.2 Gbps • 1G Ethernet class; 6.8K LUTs	***AES256-GCM 1G IP Core***	• Encrypt / decrypt between two memories with authentication tag • NIST test-vector validation	AMD Click for AMD
ChaCha20-Poly1305 Family (compact, WireGuard-ready) 	**High performance**: 128 Mbits/MHz, 25.6 Gbps @200 MHz • RFC 8439; 11.4K LUTs	***ChaCha20-Poly1305 IP Core***	• Encrypt / decrypt between two memories with authentication tag	AMD Click for AMD
	Compact: Lite version, 14.22 Mbits/MHz (3.4 Gbps @240 MHz) • 4.5K LUTs vs 11.4K (standard)	***ChaCha20-Poly1305 Lite IP Core***	• Encrypt / decrypt between two memories with authentication tag	AMD Click for AMD
Ready-made Protocol (cipher already integrated) 	**TLS 1.3 with AES256-GCM inside** • X25519, RSA / ECDSA; server and client, no CPU / DDR	***TLS1.3 Server / Client IP Core***	• HTTPS server with web browser: upload / download • HTTPS client with node.js server: upload / download • Speed test with PC application	AMD Click for AMD
	WireGuard VPN with ChaCha20-Poly1305 inside • X25519, BLAKE2s; 10G / 1G, no CPU / DDR	***WireGuard10G / 1G IP Core***	• Point-to-point tunnel with PC WireGuard software • Selective encapsulation via GUI • PC-to-PC throughput test	AMD Click for AMD

Compliance statements reflect general NIST status; confirm against your certification scheme. ChaCha20-Poly1305 Gbps = datasheet Mbits/MHz x example Fmax; LUTs from example implementation tables (xczu7ev). Device support, demos and details: see each product page and datasheet.