Security IP Product Selection Guide

Common Features

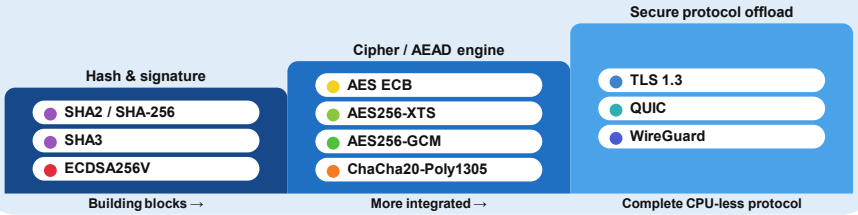
- Standards-based (RFC / NIST / FIPS)
- High throughput
- Free evaluation demo
- Rich document

Supported FPGA Devices

altera

Agilex7 I-Series /
Agilex7 F-Series /
Agilex5 E-Series /
Arria10 SX (SoC)

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) IoT → TLS 1.3 → Server	**HW fully TLS 1.3 Server** • AES256-GCM, X25519, RSA	*TLS1.3 Server 10G* ***IP Core***	• Contact us	Click for Altera
	HW fully TLS 1.3 Client • AES256-GCM, X25519, RSA / ECDSA • External handshake support	*TLS1.3 Client 10G / 1G* ***IP Core***	• Contact us	Click for Altera
Secure Transport over Lossy Networks (QUIC, 5G/6G, drone, tele-surgery) Edge → QUIC 0-RTT → Lossy net	**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	Click for Altera
	HW fully QUIC Server • RFC 9000 • Customizable multi-stream	*QUIC Server 10G* ***IP Core***	• Contact us	Click for Altera
Secure Data Storage (N → AES256 XTS → S) Host, SSD	**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	Click for Altera
	HW fully AES256-XTS, ciphertext stealing • Up to 44.8 Gbps • Any length ≥ 16 byte	*AES256-XTS* ***IP Core***	• Encrypt / decrypt between two memories	Click for Altera
Network & Link Encryption (AEAD & → AES256 GCM → ireGuard) TCP/IP, Network	**HW fully AES256-GCM AEAD** • Up to 112.64 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	Click for Altera
	HW fully ChaCha20-Poly1305 AEAD • RFC 8439; 128 Mbits/MHz • Lite: smaller (3.2K vs 7.4K ALMs)	*ChaCha20-Poly1305 / Lite* ***IP Core***	• Encrypt / decrypt between two memories with authentication tag	Click for Altera
	HW fully WireGuard VPN • ChaCha20-Poly1305, X25519, BLAKE2s • 1G, internal handshake	*WireGuard1G* ***IP Core***	• Point-to-point tunnel with PC WireGuard software • Selective encapsulation via GUI • PC-to-PC throughput test	Click for Altera
Custom Mode of Operation (ECE → AES SS → sion) PlainText, CipherText	**HW fully AES ECB, highest throughput** • 51.2 Gbps @400 MHz • 128-bit per clock	*AES256-SS* ***IP Core***	• Encrypt / decrypt between two memories	Click for Altera
	HW fully AES ECB, compact • AES256 (15 clk) / AES128 (11 clk) • Up to 4.65 Gbps	*AES256 / AES128* ***IP Core***	• Encrypt / decrypt between two memories	Click for Altera
Authentication & Integrity Data → SHA2 ECDSA → Verified	**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	Click for Altera
	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	Click for Altera
	HW fully SHA-3 hash • FIPS 202: SHA3-224/256/384/512, SHAKE128/256	*SHA3* ***IP Core***	• Contact us	Click for Altera

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 112.64 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 3.2K ALMs, 10.67 Mbits/MHz (1.6 Gbps @150 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**: 11.5 Gbps @90 MHz (Arria 10); no 100G variant in DG lineup

How to Choose

1	FIPS 140 / CNSA compliance required?	AES256-GCM
2	Need more than 11 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)	112.64 Gbps (100G); 512 Mbits/MHz	11.5 Gbps @90 MHz (Arria 10); 128 Mbits/MHz	**AES256-GCM above ~11 Gbps**
Low-rate link (1G class)	2.285 Gbps	Lite: 1.6 Gbps	**Either: decide by area / compliance**
FPGA area (Altera example devices)	1G: 4.8K ALMs; 10G25G: 16.4K ALMs	Lite: 3.2K ALMs; standard: 7.4K ALMs	**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 112.64 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	altera Click for Altera
	Compact: 2.285 Gbps • 1G Ethernet class; 4.8K ALMs	***AES256-GCM 1G*** ***IP Core***	• Encrypt / decrypt between two memories with authentication tag • NIST test-vector validation	altera Click for Altera
ChaCha20-Poly1305 Family (compact, WireGuard-ready) 	**High performance**: 128 Mbits/MHz, 11.5 Gbps @90 MHz (Arria 10) • RFC 8439; 7.4K ALMs	***ChaCha20-Poly1305*** ***IP Core***	• Encrypt / decrypt between two memories with authentication tag	altera Click for Altera
	Compact: Lite version, 10.67 Mbits/MHz (1.6 Gbps @150 MHz) • 3.2K ALMs vs 7.4K (standard)	***ChaCha20-Poly1305 Lite*** ***IP Core***	• Encrypt / decrypt between two memories with authentication tag	altera Click for Altera
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***	• Contact us	altera Click for Altera
	WireGuard VPN with ChaCha20-Poly1305 inside • X25519, BLAKE2s; 1G, no CPU / DDR	***WireGuard1G*** ***IP Core***	• Point-to-point tunnel with PC WireGuard software • Selective encapsulation via GUI • PC-to-PC throughput test	altera Click for Altera

Compliance statements reflect general NIST status; confirm against your certification scheme. ChaCha20-Poly1305 Gbps = datasheet Mbits/MHz x example Fmax (Arria 10 SX: 128 x 90, Lite 10.67 x 150 MHz); ALMs from example implementation tables. Device support, demos and details: see each product page and datasheet.