CRYPTOGRAPHY UNDER THE HOOD WEBINAR SERIES

Cryptography at Work: Securing Device Communications

Tommi Lampila

Director,
Business Development
Xiphera

Agenda

I. Security challenges

II. Building blocks: OSI model, AES-GCM

III. Security Protocols: MACsec, IPsec, TLS

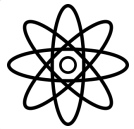
IV. Protocol comparison

V. Xiphera partner solutions

VI. Conclusion

Today's Security Challenges

Data confidentiality, integrity & authenticity



The Quantum Computer Threat

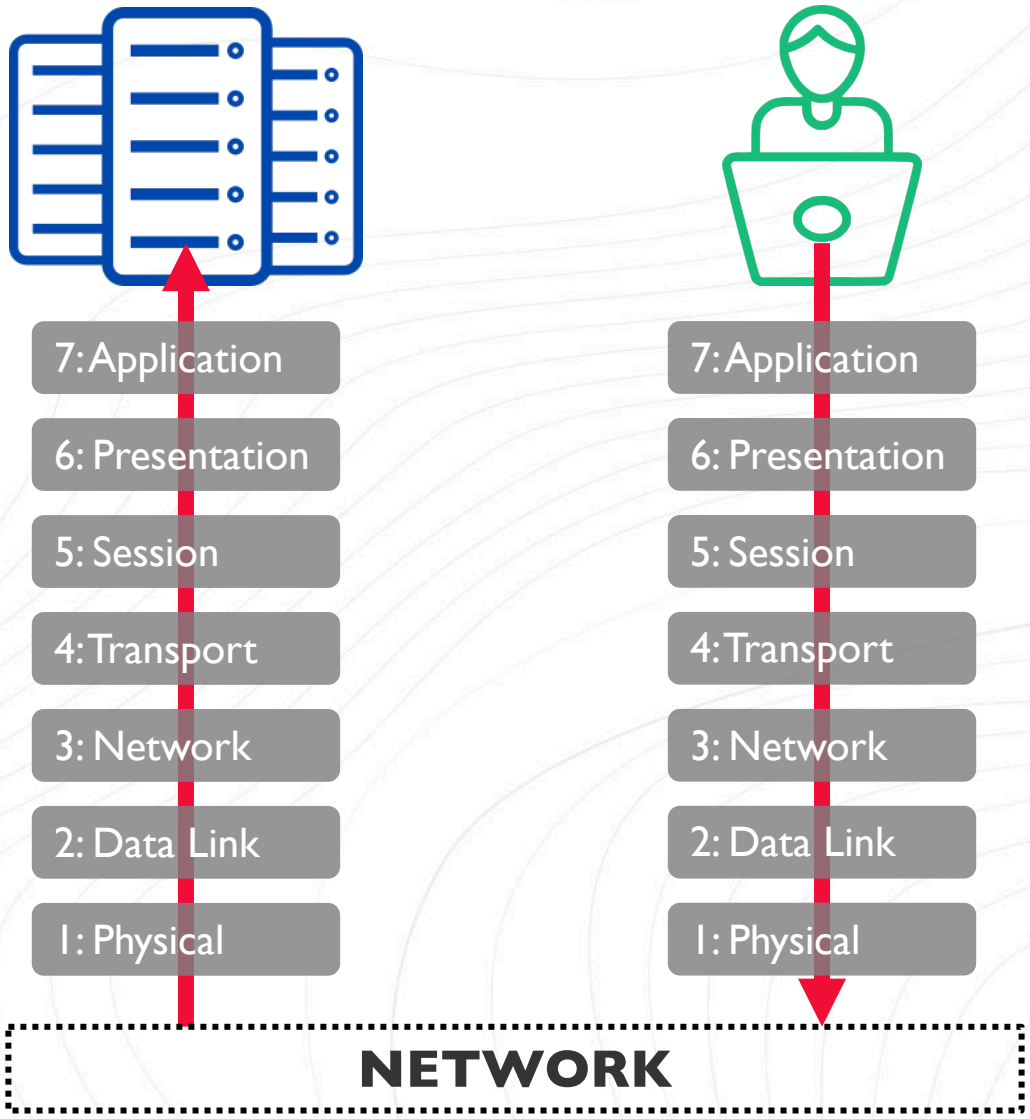
Securing IoT connectivity to edge, cloud, AI environments

Compliance with legislation and mandates

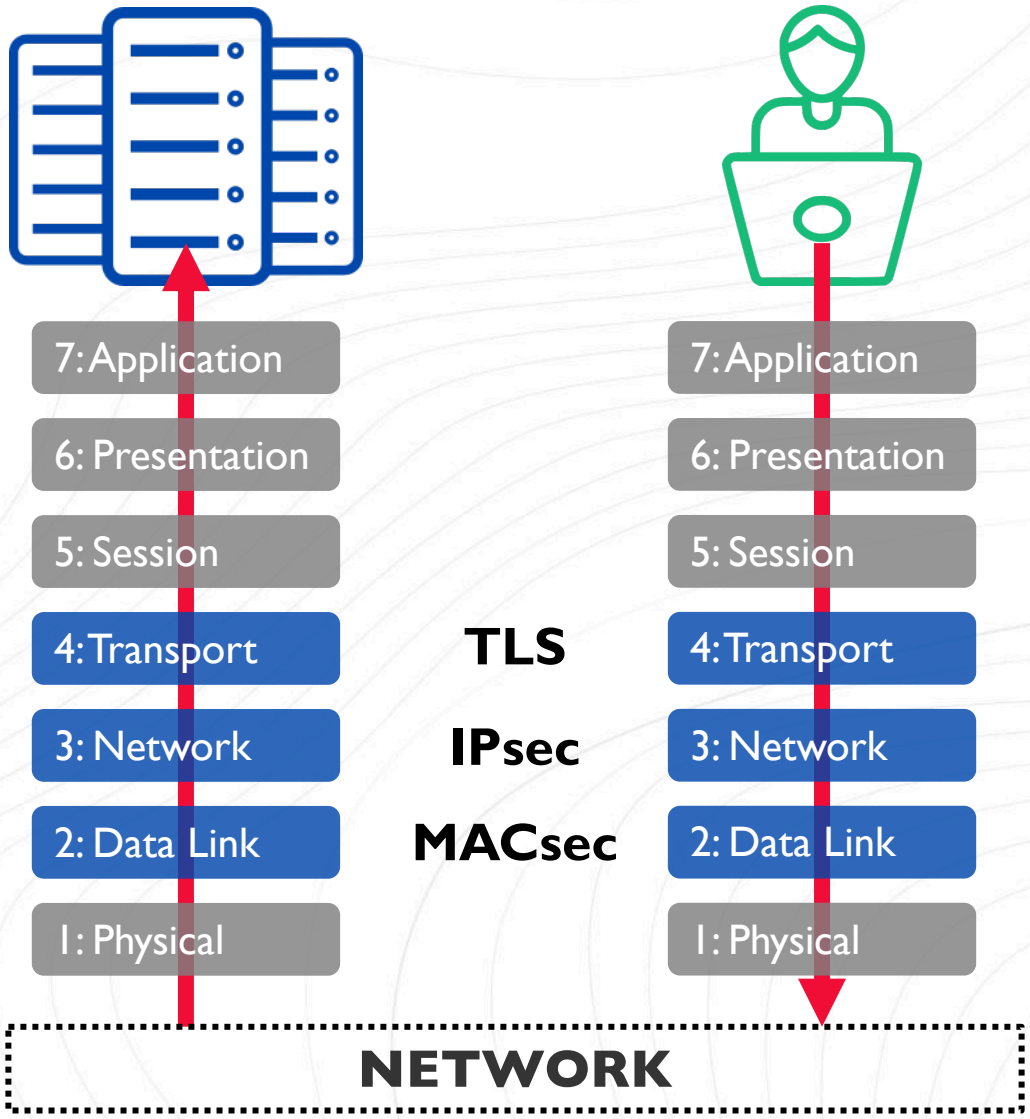
II

Security Protocol Building Blocks

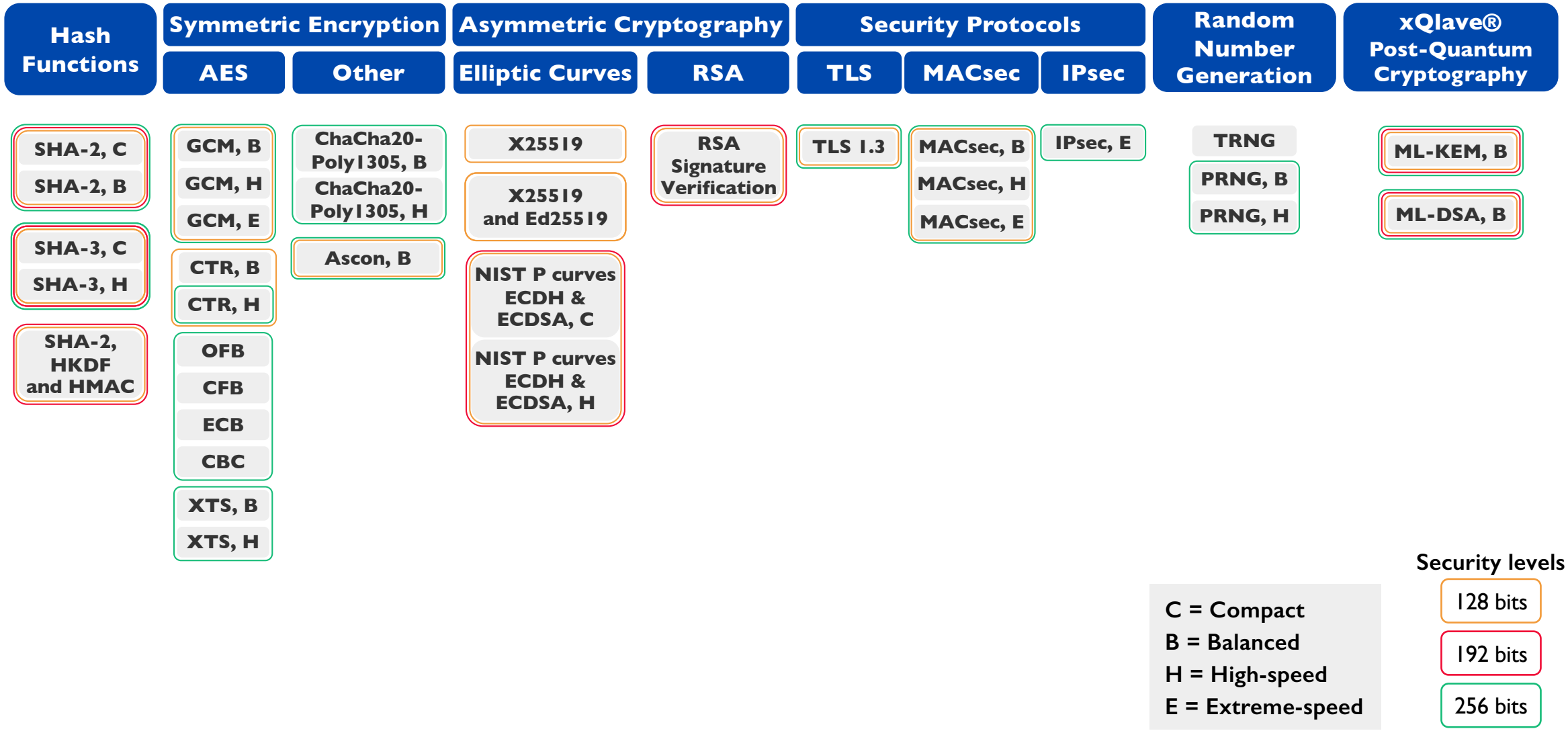
OSI Model



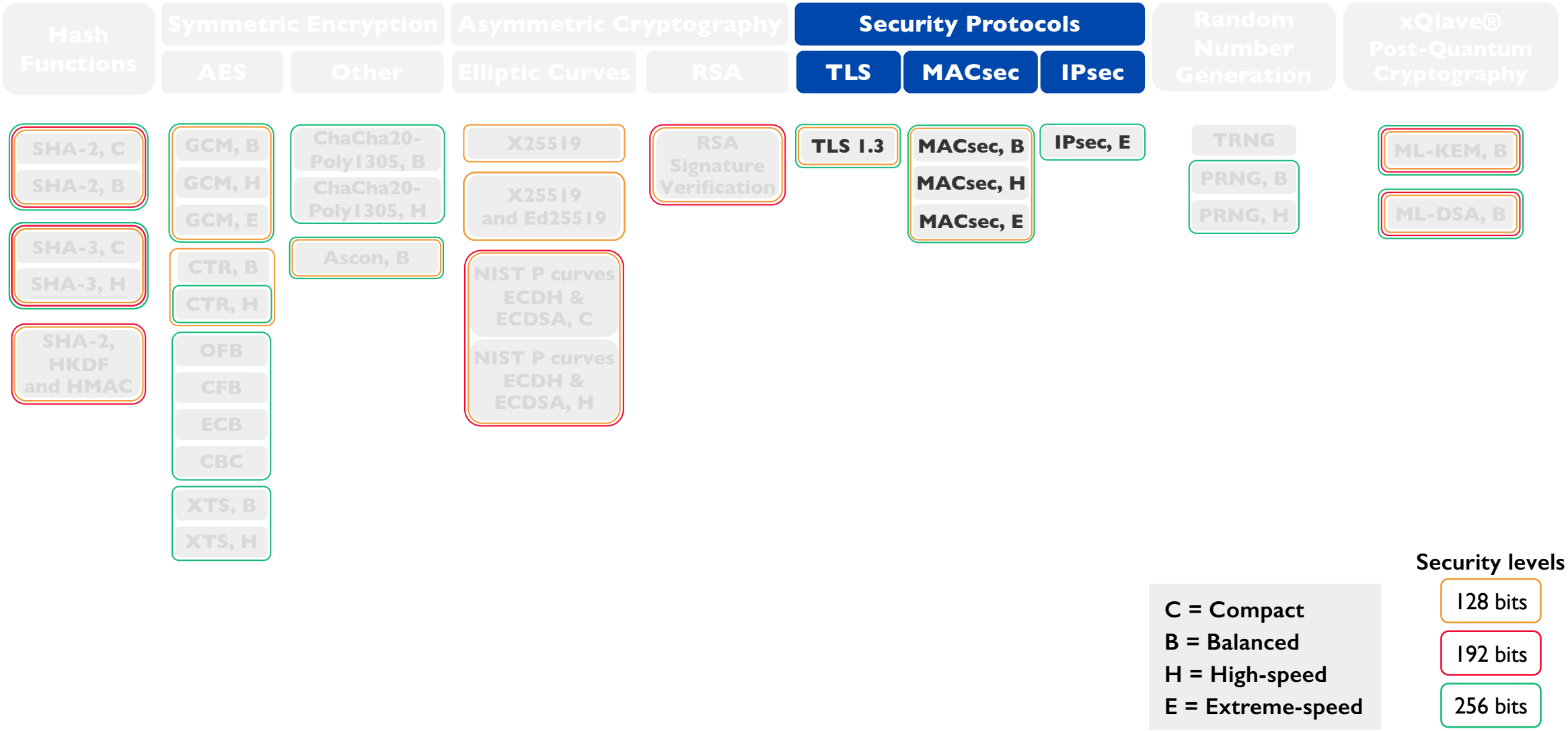
OSI Model



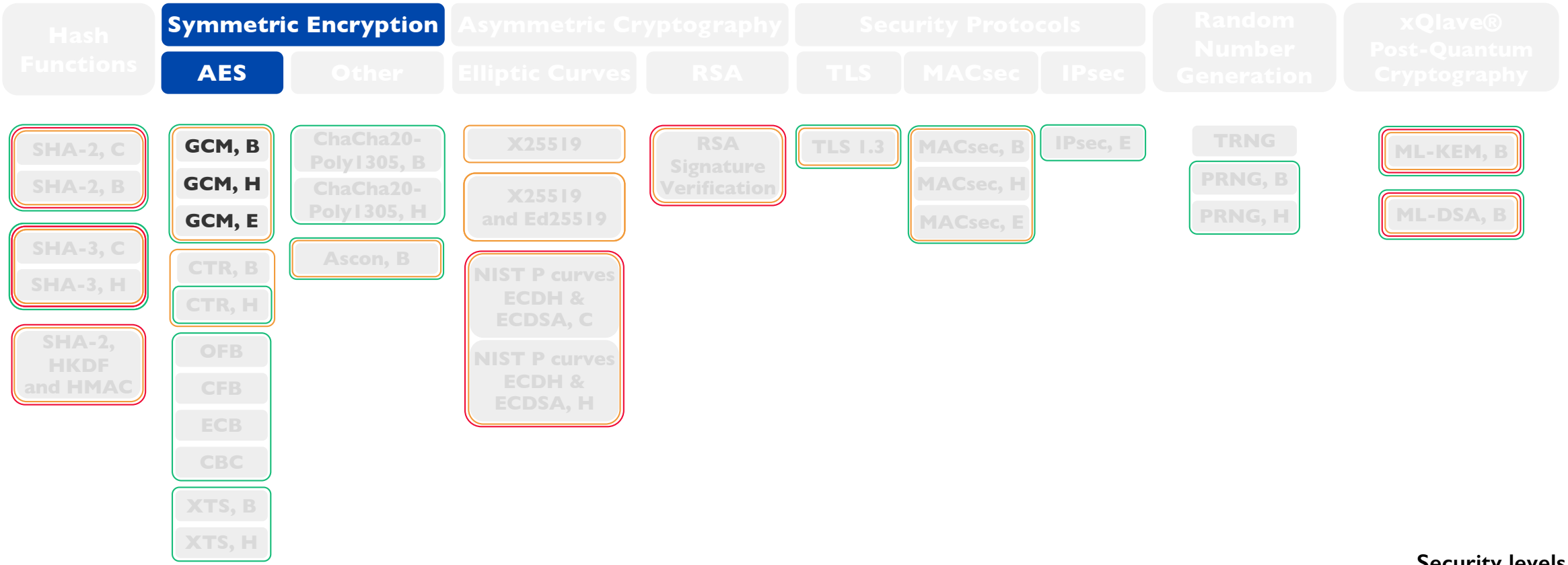
Xiphera Product Portfolio

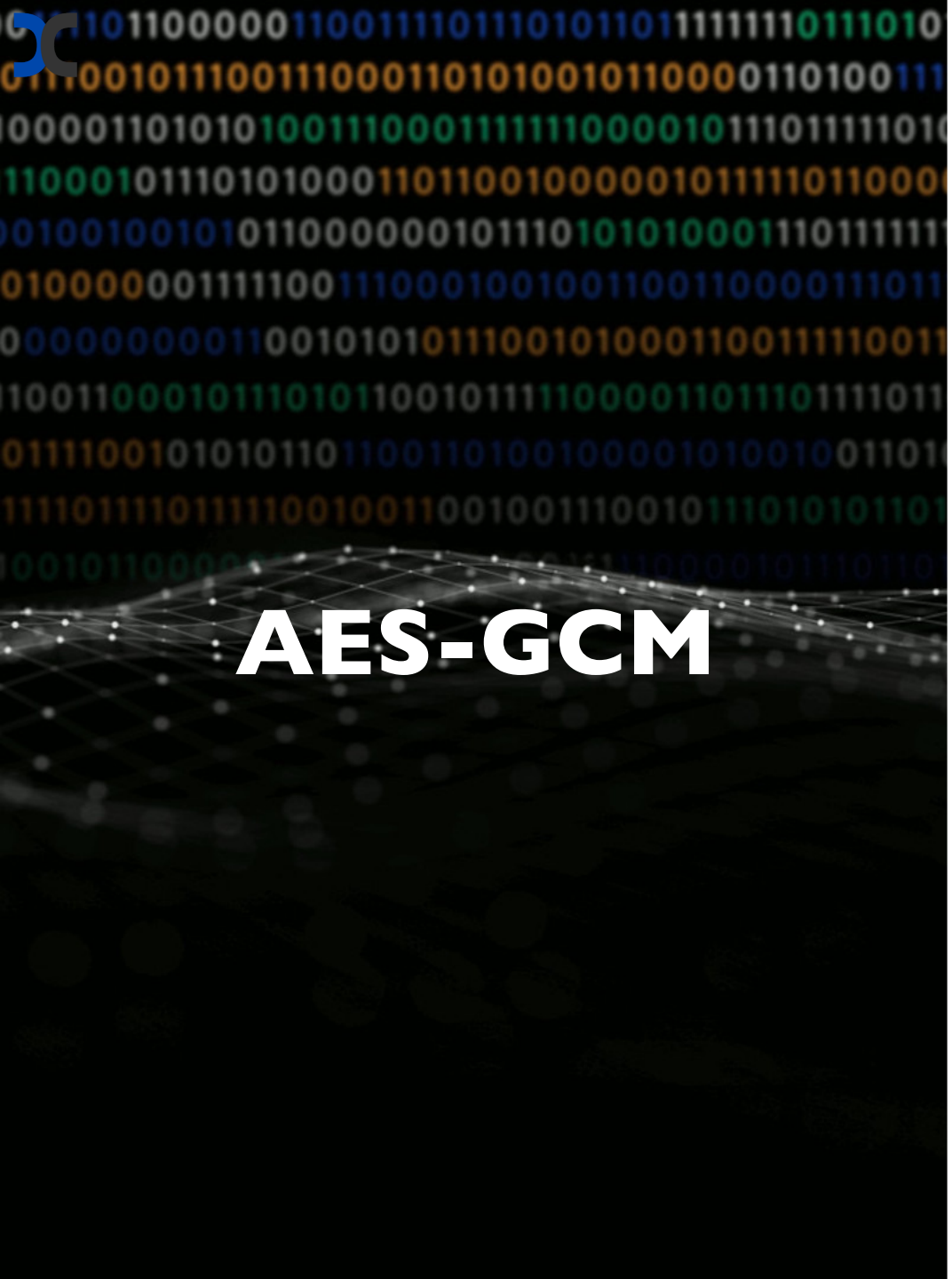


Xiphera Product Portfolio



Xiphera Product Portfolio



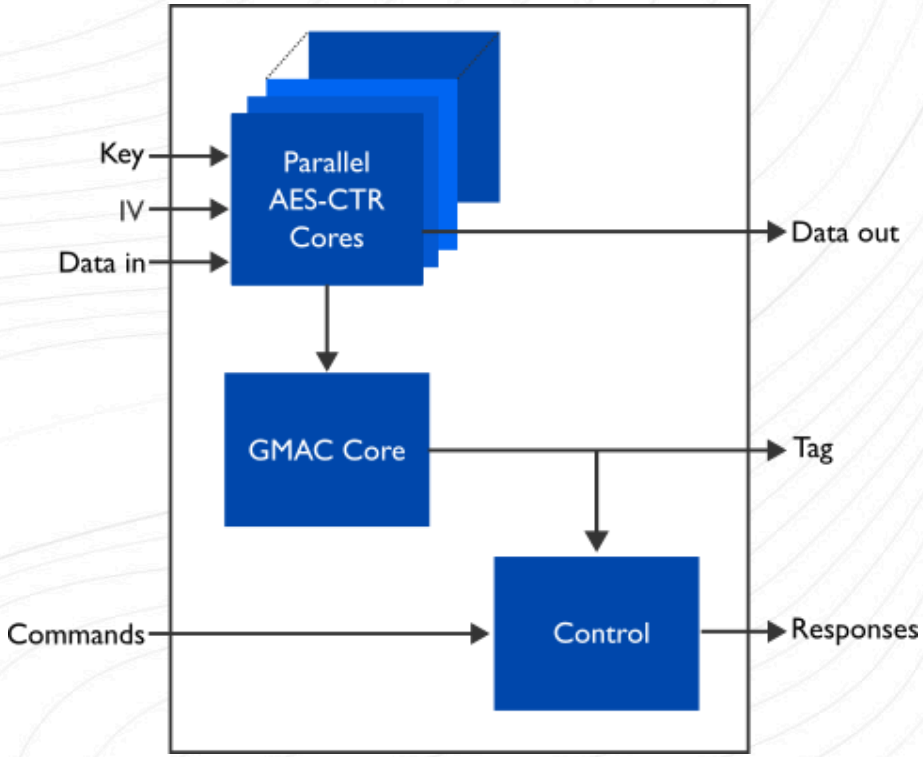


AES-GCM

- Advanced Encryption Standard – Galois Counter Mode
- Block Cipher (128-bit block size)
- Efficient method to guarantee confidentiality, authenticity, and integrity of data
- Authenticated Encryption with Associated Data (AEAD)
- Adds data integrity & authenticity to AES
  - Combines AES-CTR with GMAC
- Offers security at high performance
- 256-bit keys recommended for Quantum Resilience

Xiphera AES-GCM IP cores

- Extreme-speed
  - Parallel and fully pipelined architecture
  - Maximized throughput with no idle cycles
- Ease of design and integration
  - Fixed latency
- Used in security protocol implementations (TLS, IPsec, MACsec) as the default crypto engine



xiphera.com/symmetric-encryption/aes-gcm

III

Security Protocols

Example Applications

MACsec:

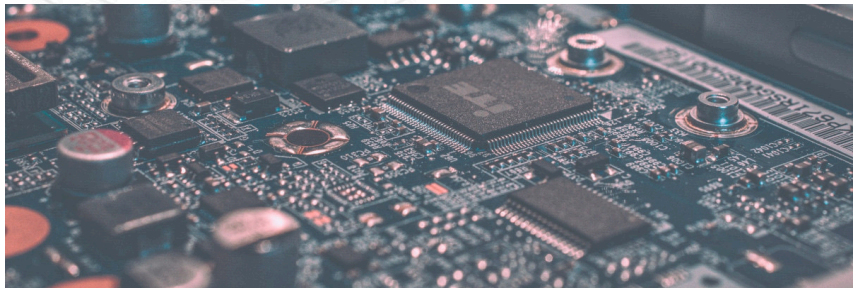
- Automotive backbone connectivity
- Open RAN architectures in 5G
- Mission-critical environments

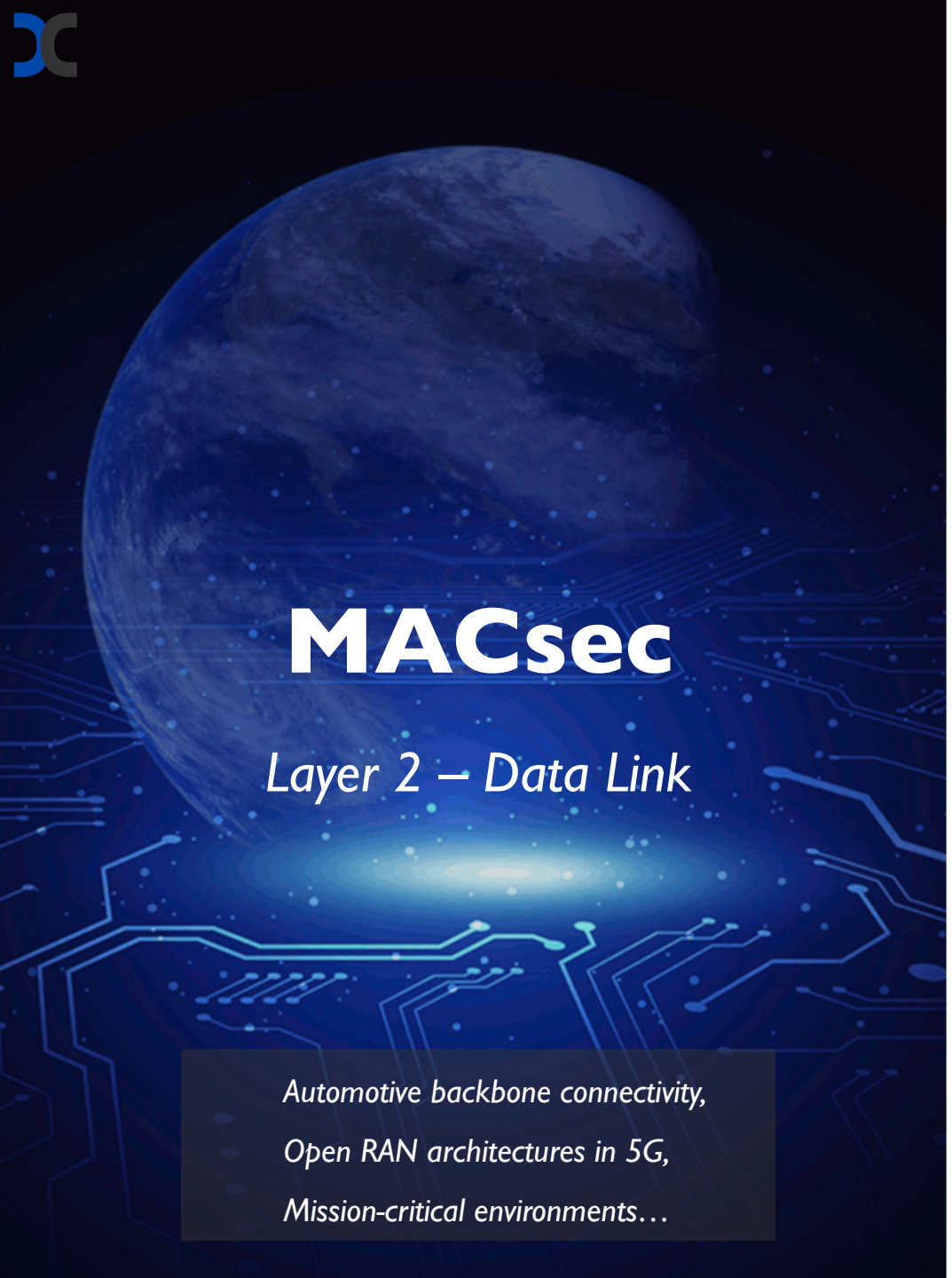
IPsec:

- Virtual Private Networks (VPN)
- FPGA-based SmartNICs

TLS:

- Remote management and configuration interfaces
- System-of-Systems communication
- Test & Measurement connectivity
- Networked storage, such as iSCSI





MACsec

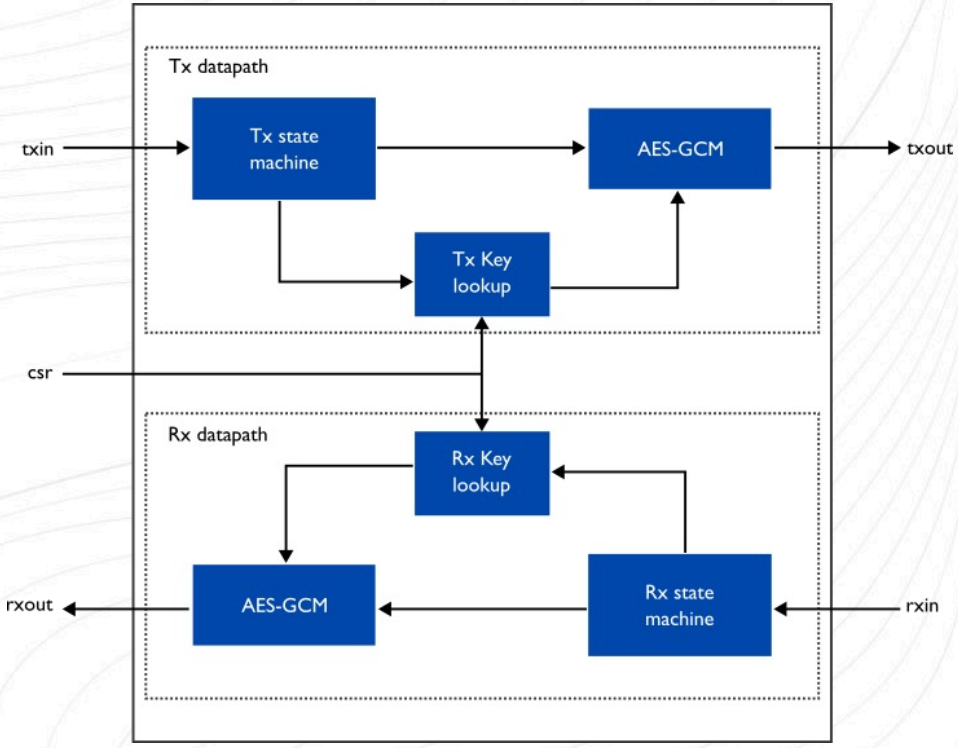
Layer 2 – Data Link

Automotive backbone connectivity,
Open RAN architectures in 5G,
Mission-critical environments…

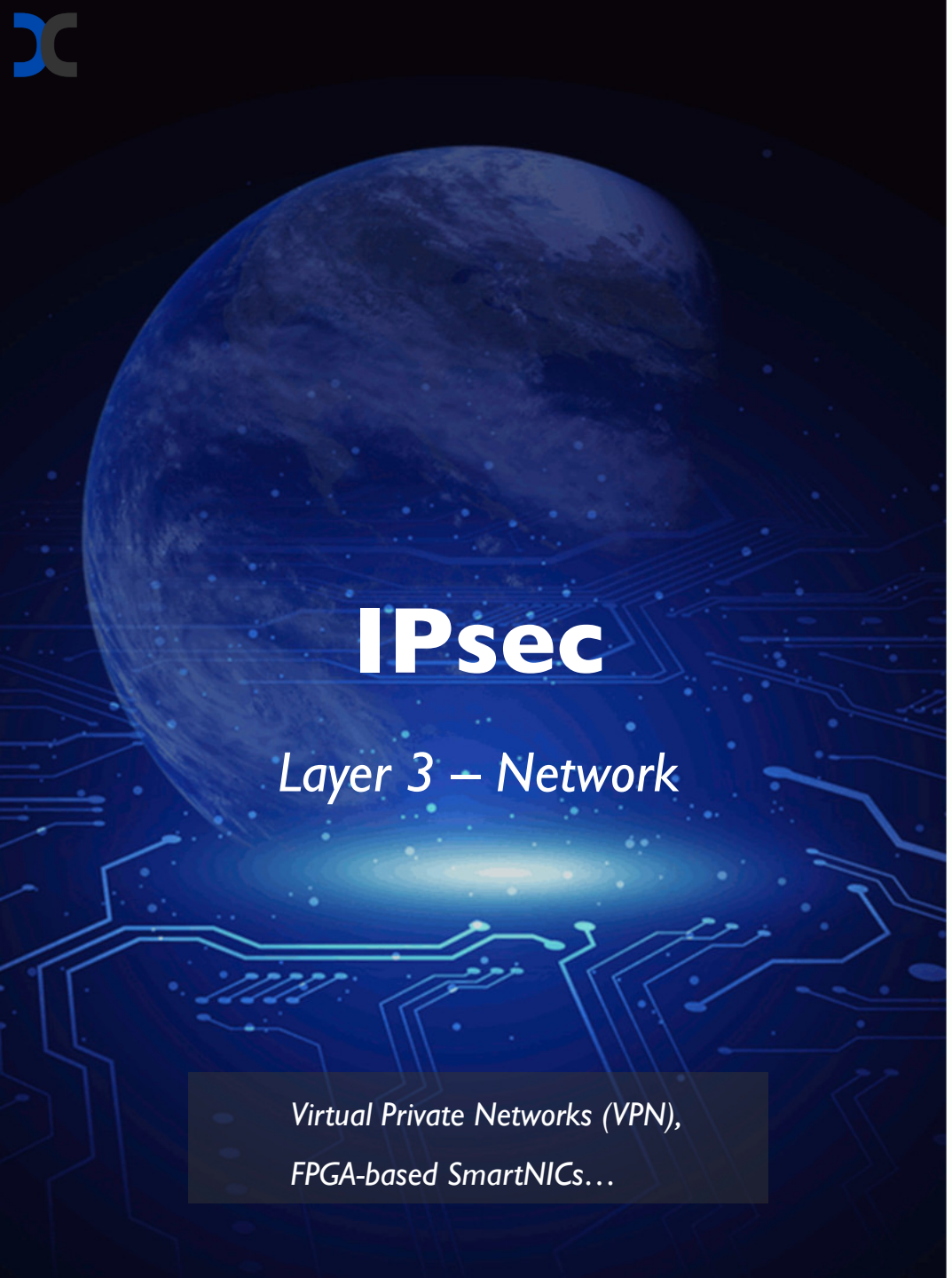
- Medium Access Control security
- Latest standard version IEEE Std 802.1AE-2018
- Ethernet port-to-port security with AES-GCM
  - Confidentiality = AES-CTR
  - Integrity = GMAC
- Multihop extension
- Protocol supports 128-bit and 256-bit keys
  - 256-bit key strength recommended
- Key management defined in IEEE Std 802.1X-2010

Xiphera MACsec IP cores
MACsec AES256-GCM

- **Balanced** variants for single Gbps
- **High-speed** variants for tens of Gbps
- **Extreme-speed** variant up to hundreds of Gbps
  - Parallel streaming architecture with fixed latency
  - Full-duplex – independent send and receive paths
  - No idle cycles regardless of packet size



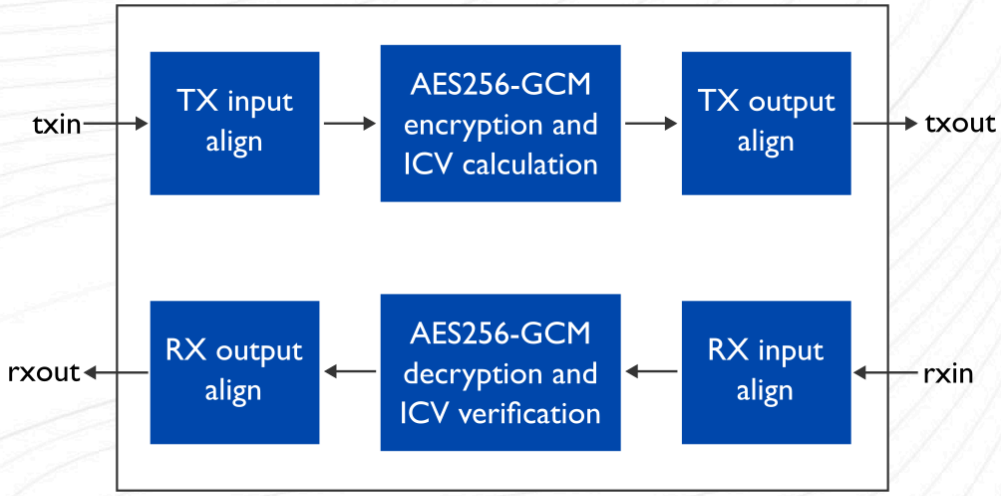
xiphera.com/security-protocols/macsec



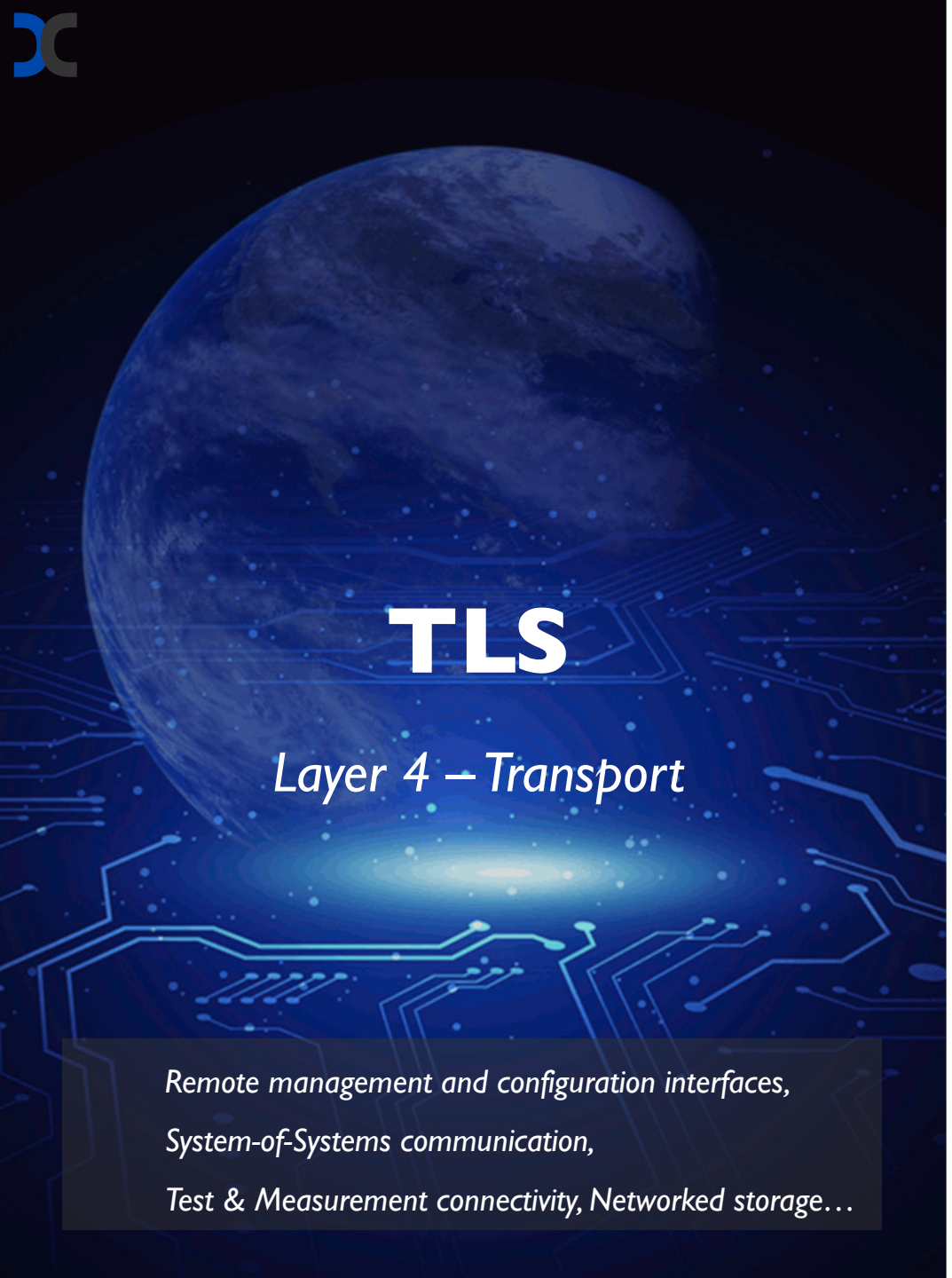
- Internet Protocol Security
- Defined in 70+ RFCs during two decades
- Multiple algorithms for key exchange and data traffic
  - Both encryption and authentication
- Converging on AES-GCM
- IKEv2 protocol for key negotiation
  - Almost always in software

Xiphera Scalable IPsec IP core

- ***Released on March 5th, 2024***
- Designed for scalability
- Best suited for 10 Gbps to 200 Gbps throughput with high-end FPGAs
- Implements ESP (Encapsulating Security Payload) frame processing using AES256-GCM
- Streaming interface for payload data and side-channel signalling for ESP frame parameters



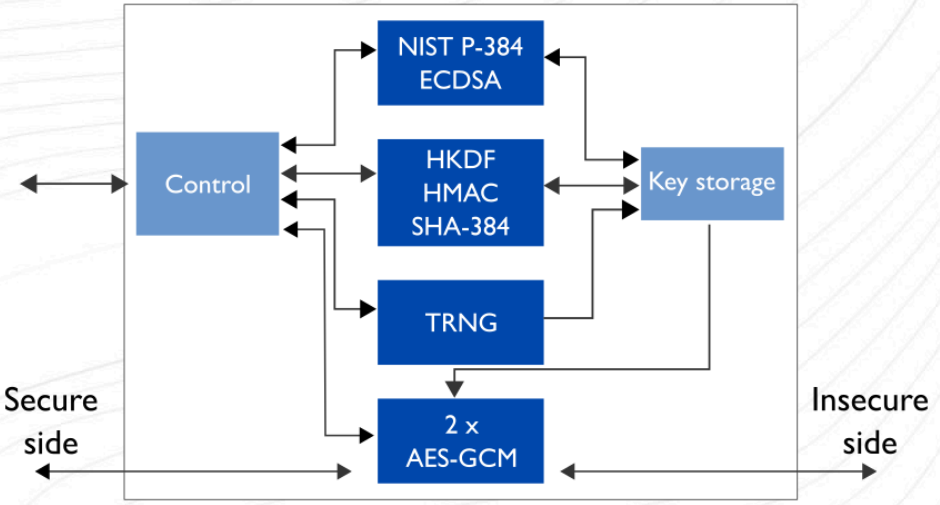
xiphera.com/security-protocols/ipsec



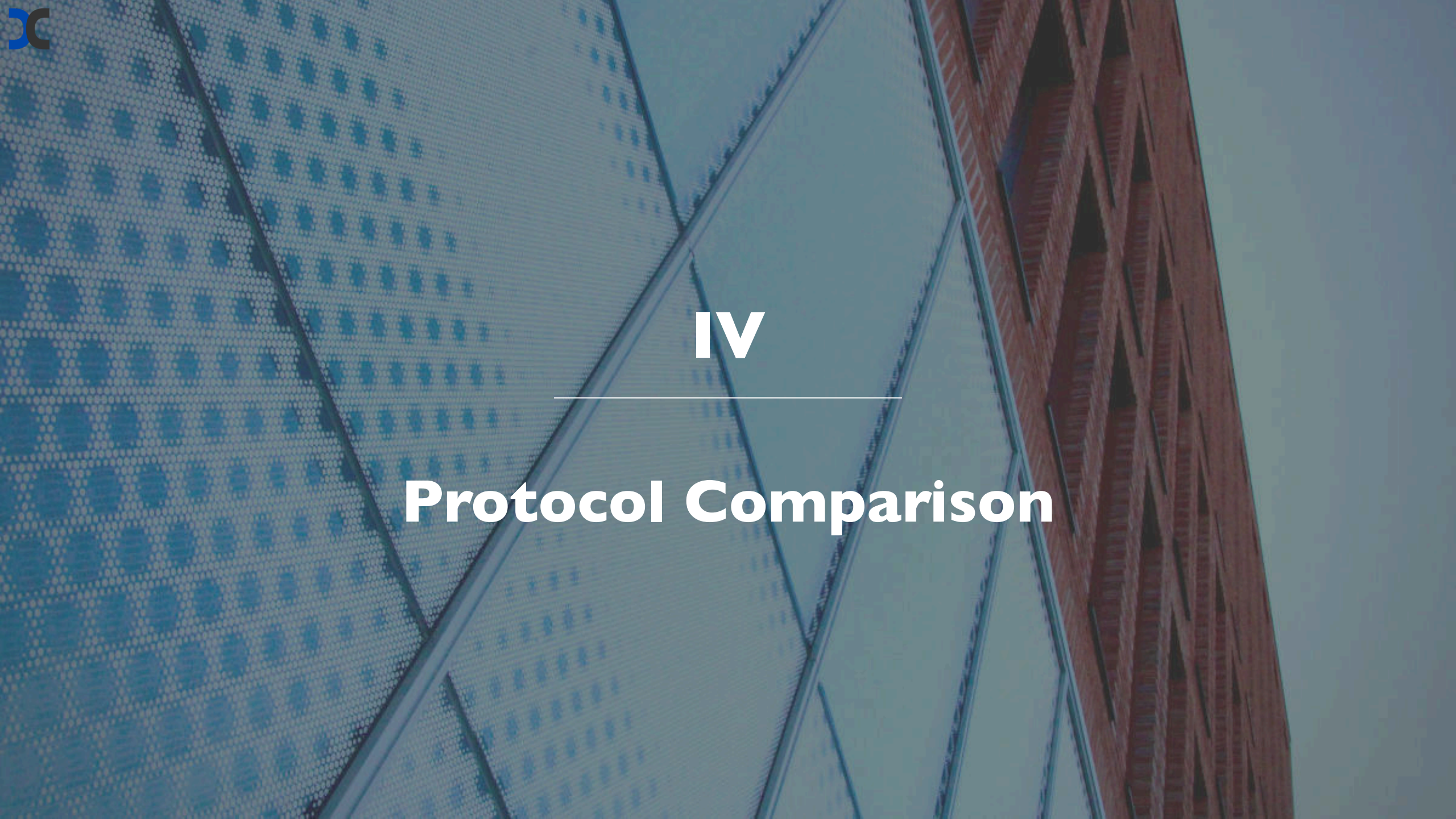
- Transport Layer Security
- Latest version 1.3 defined in RFC 8446
- TLS 1.3 is everywhere on the Internet
  - The “s” in https (secure browsing)
- Handshake protocol for session establishment
- Record protocol for bulk communication
- AES-GCM by default

Xiphera's TLS 1.3 IP core

- Implements TLS 1.3 client/server
- Entirely hardware-based cryptographic operations and key management
- Full independence from software for critical operations
- Optimised for low-area footprint
  - Ideally suited for high-volume applications
- 10k+ LUTs for compact TLS 1.3 client



xiphera.com/security-protocols/tls



IV

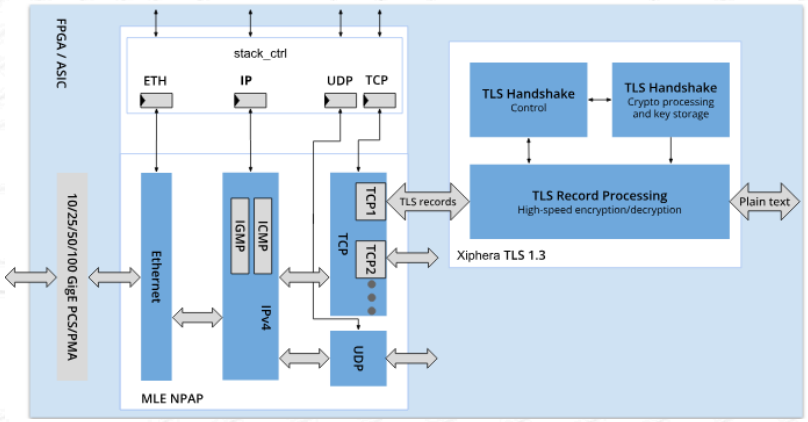
Protocol Comparison

	MACsec	IPsec	TLS 1.3
Definitive standards	IEEE Std 802.1AE-2018	70+ RFCs	RFC 8446
Key management	Refers to 802.1X standard	IKEv2, almost always in software	Included
Multihop	EDE modes enable multi-hop	Yes	Yes
Crypto engine	Only AES-GCM	Converging on AES-GCM	AES-GCM dominant
Interoperability	Reasonable	Challenging	Good
TCP/IP stack	Below IP layer	Between IP and TCP layer	On top of TCP layer, requires TCP/UDP/IP stack on hardware
Sizing from	14k LUT	50k LUT / 100Gbps	10k LUT (compact client)
Typical use	Closed System, Industrial	Network to Network	Open System, Application Security, Human interaction

V

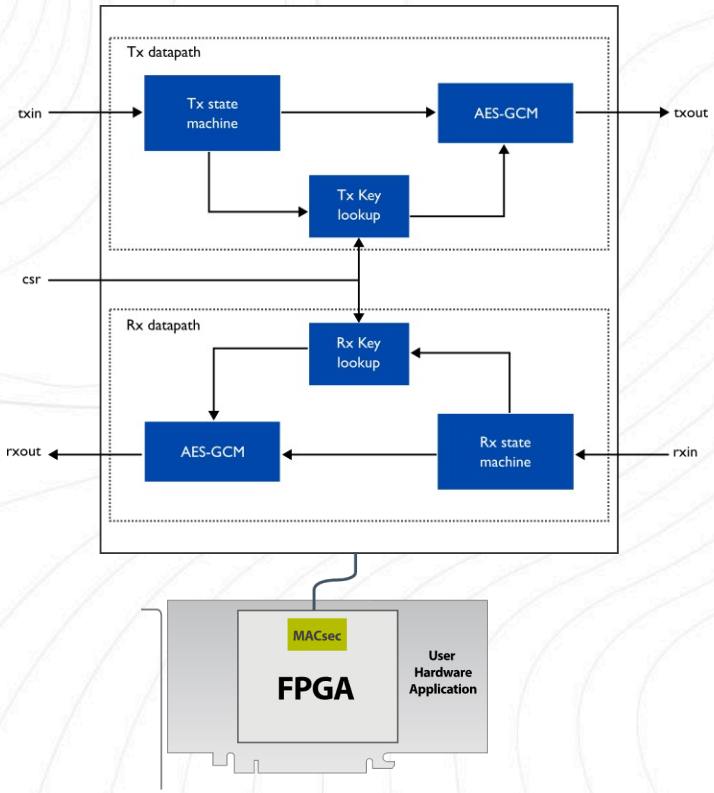
Partner Solutions

Xiphera and MLE –
Embedded Network Accelerator Solution



- Implements TLS on top of the Transmission Control Protocol (TCP) layer
- Highly modular TCP/UDP/IP stack
  - Multiple parallel TCP engines with line rate up to 70Gbps in FPGAs
- Compact TLS 1.3 implementation
- Hardware-based key management
  - IEC 62443 SL 3 compliance
- More information at [the Xiphera solution page] or [missinglinkelectronics.com]

Xiphera and BittWare –
Security Protocols on PCIe Cards



- Xiphera MACsec and IPsec IP implementations run on BittWare PCIe cards with Altera FPGAs
- Example IPsec throughput:

  200+ Gbps on high-end card
- More information at Xiphera partner page or bittware.com

Post-Quantum Cryptography (PQC) and Security Protocols

- Hybrid key exchange with PQC and classical ECC
  - Countermeasure against "Harvest now, decrypt later"
- TLS 1.3:
  - draft-ietf-tls-hybrid-design-09
  - draft-tls-westerbaan-xyber768d00-03
  - draft-kwiatkowski-tls-ecdhe-kyber-01
- IKEv2:
  - RFC 9370
  - draft-kampanakis-ml-kem-ikev2-01
- MACsec:
  - Does not implement asymmetric cryptography
- Always use only 256-bit symmetric encryption!

https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc

To Summarise...

Hardware-based cryptography brings multiple advantages.

Choose the protocol based on your use case scenario.

Xiphera is here to help you on your way to a secure future!


XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD
Thank you!
www.xiphera.com
info@xiphera.com
tommi.lampila@xiphera.com

Thursday, March 14

Xiphera & Flex Logix: Enabling Long Lasting Security for Semiconductors

https://register.gotowebinar.com/register/4870159188814078037

www.xiphera.com

info@xiphera.com

tommi.lampila@xiphera.com