ARTESYN™
EMBEDDED TECHNOLOGIES

Securing Tactical Systems TODAY

Robert Persons
Sr. Sales Architect
Artesyn Embedded Technologies

Evolution of Tactical System Computing

TRANSITION TO COMMERCIAL OFF THE SHELF

YK-43B

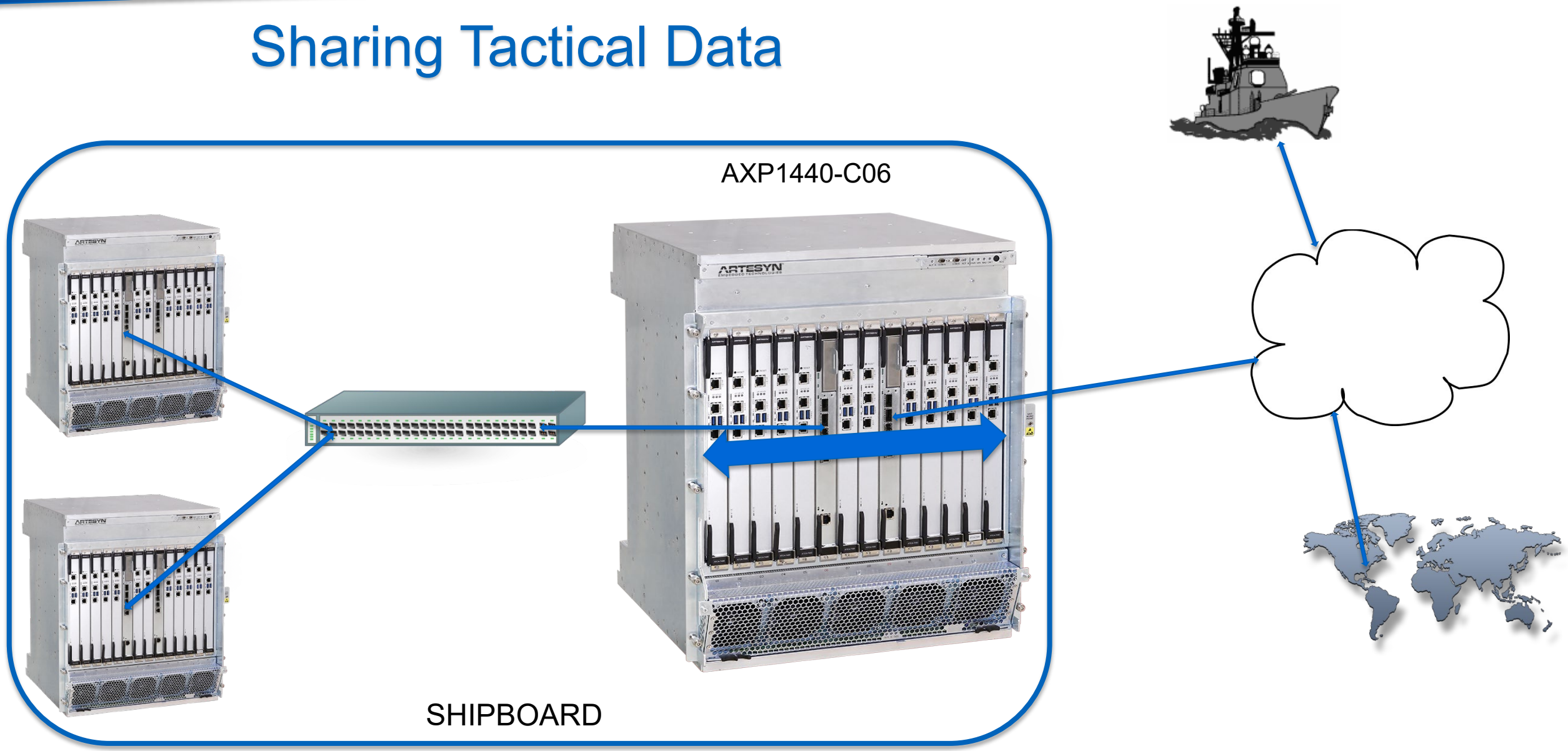
MIGRATION TO VMEBUS

MVME2604

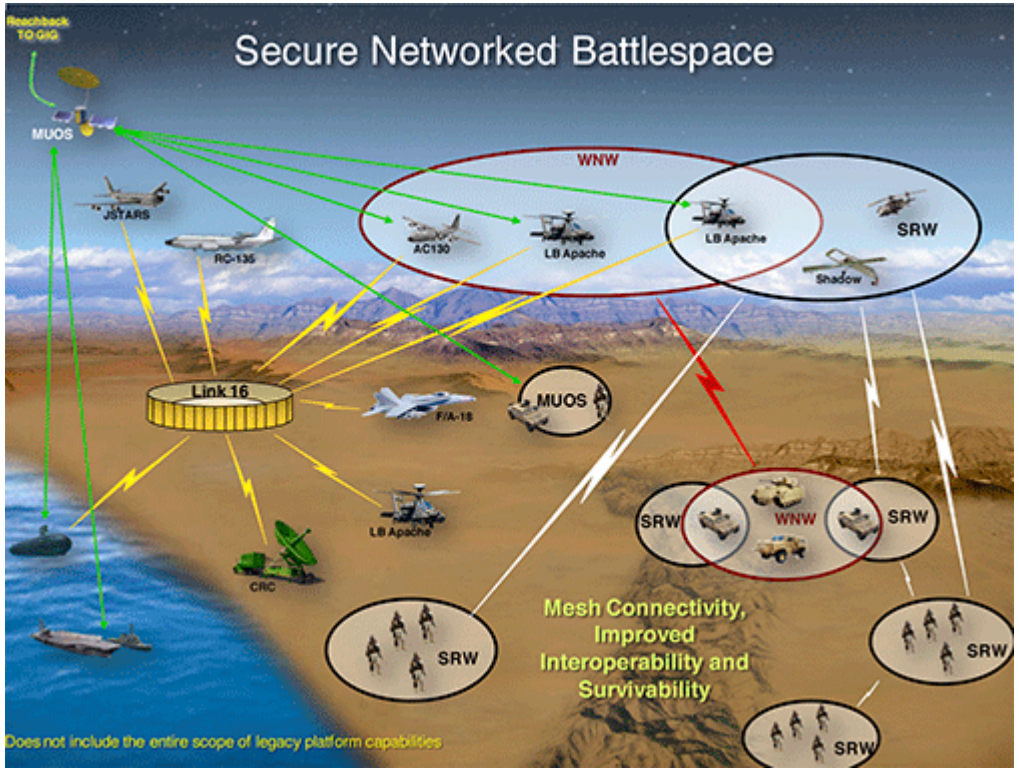
MIGRATION TO NETWORK CENTRIC COMPUTING

AXP1440-C06

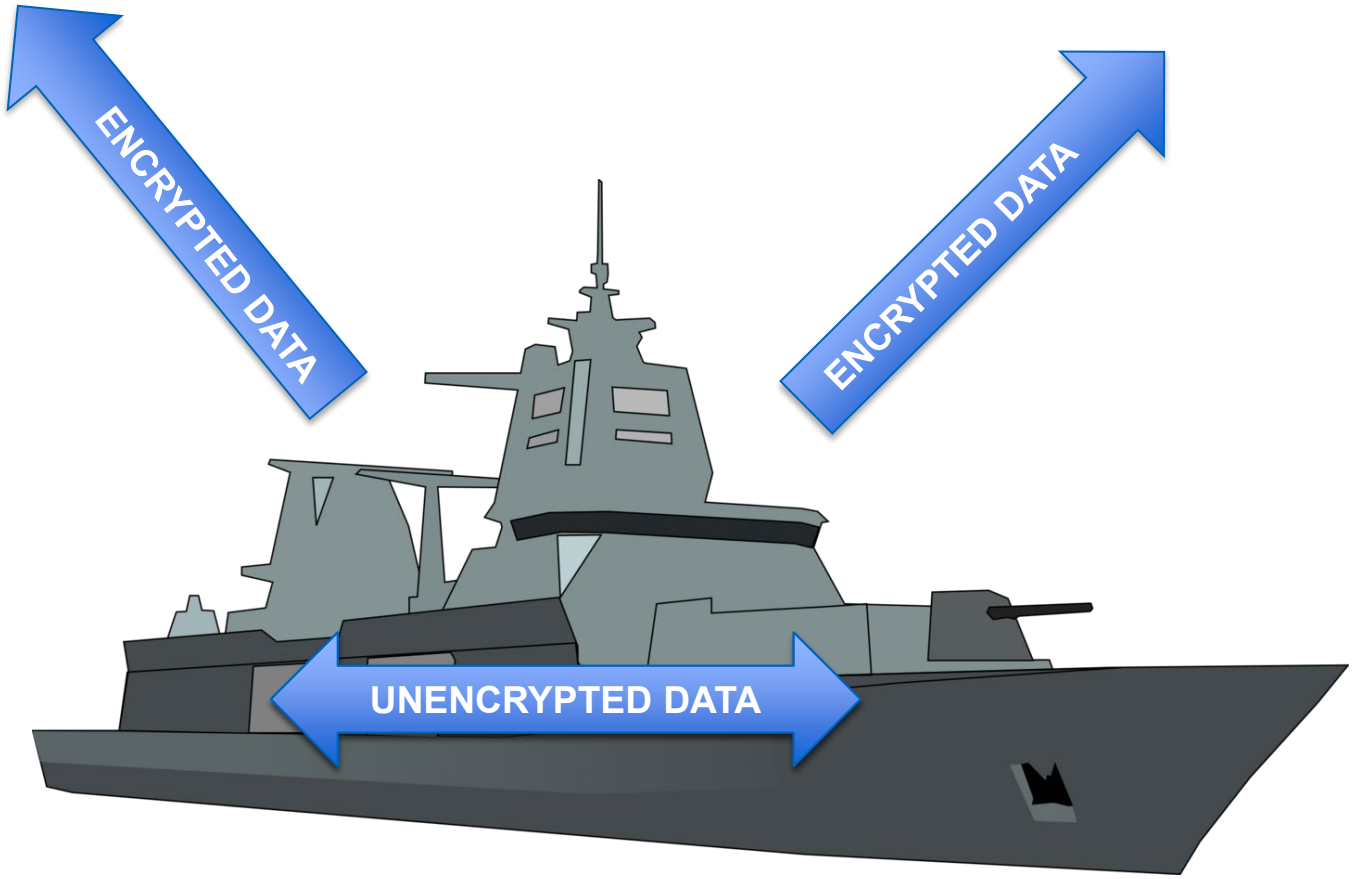
Sharing Tactical Data



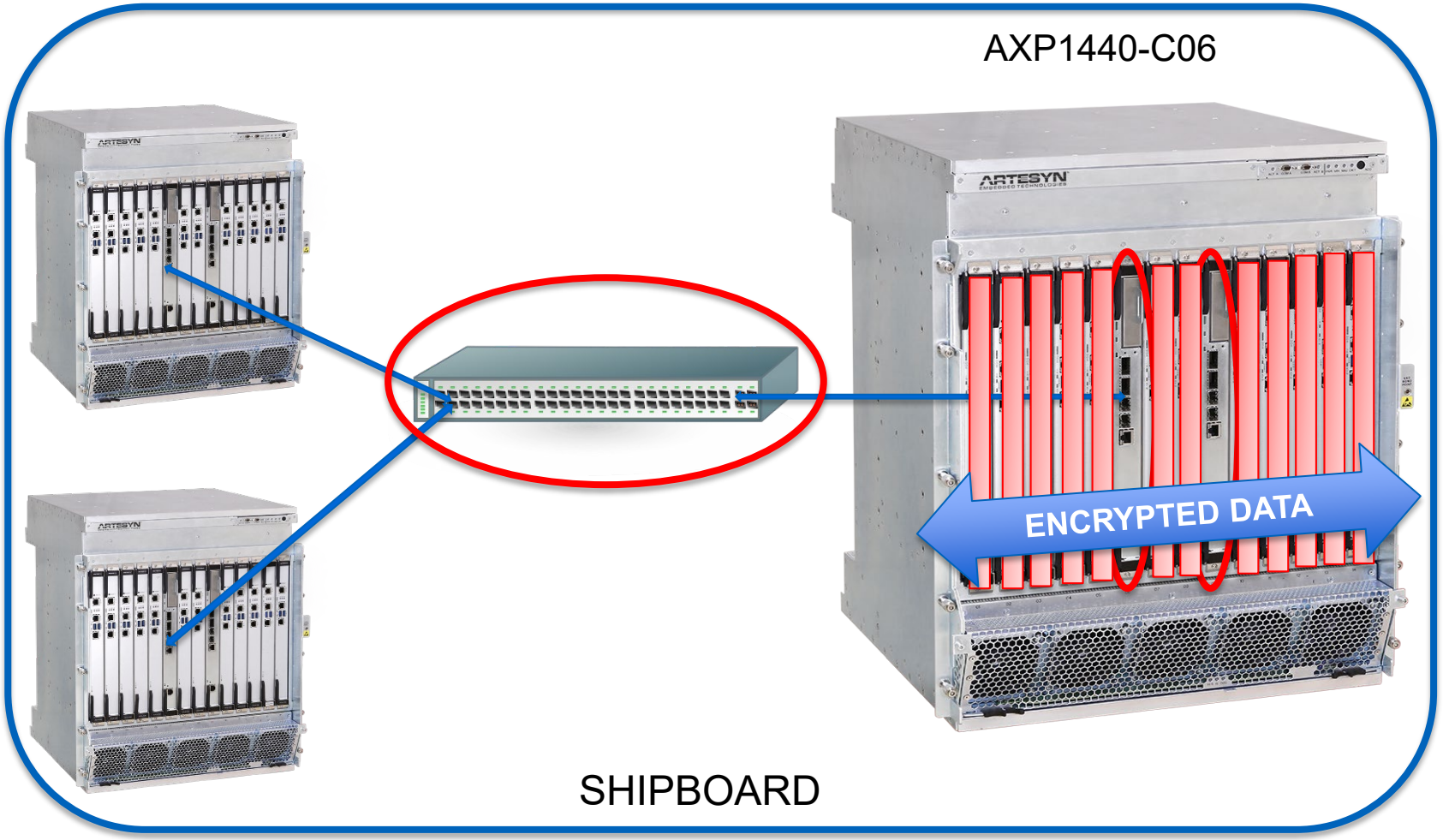
Encrypted Tactical Data



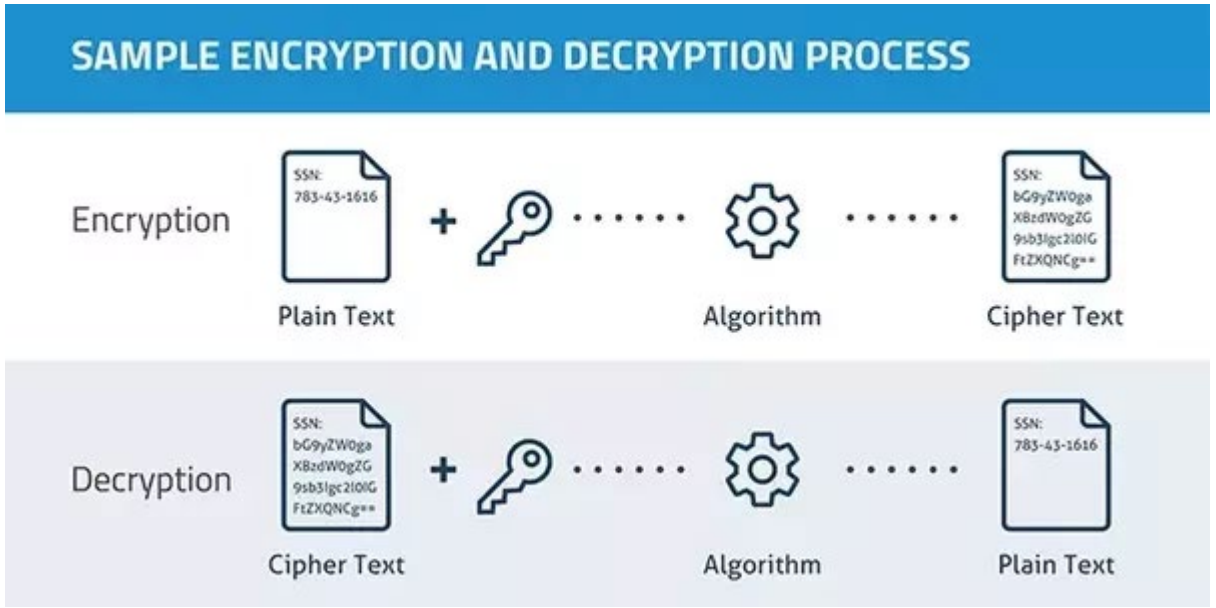
Ship Based Tactical Data



Encrypting Shipboard Tactical Data



Encryption Algorithm Methods



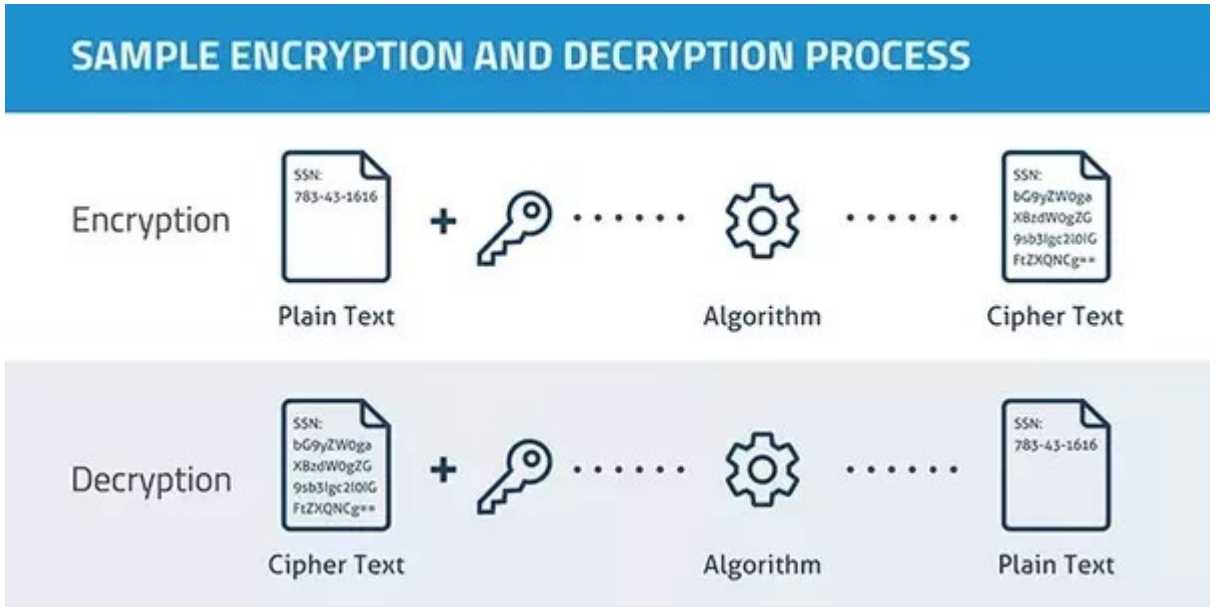
Encryption Keys

Private ***Public***

Cipher Method

Block ***Stream***

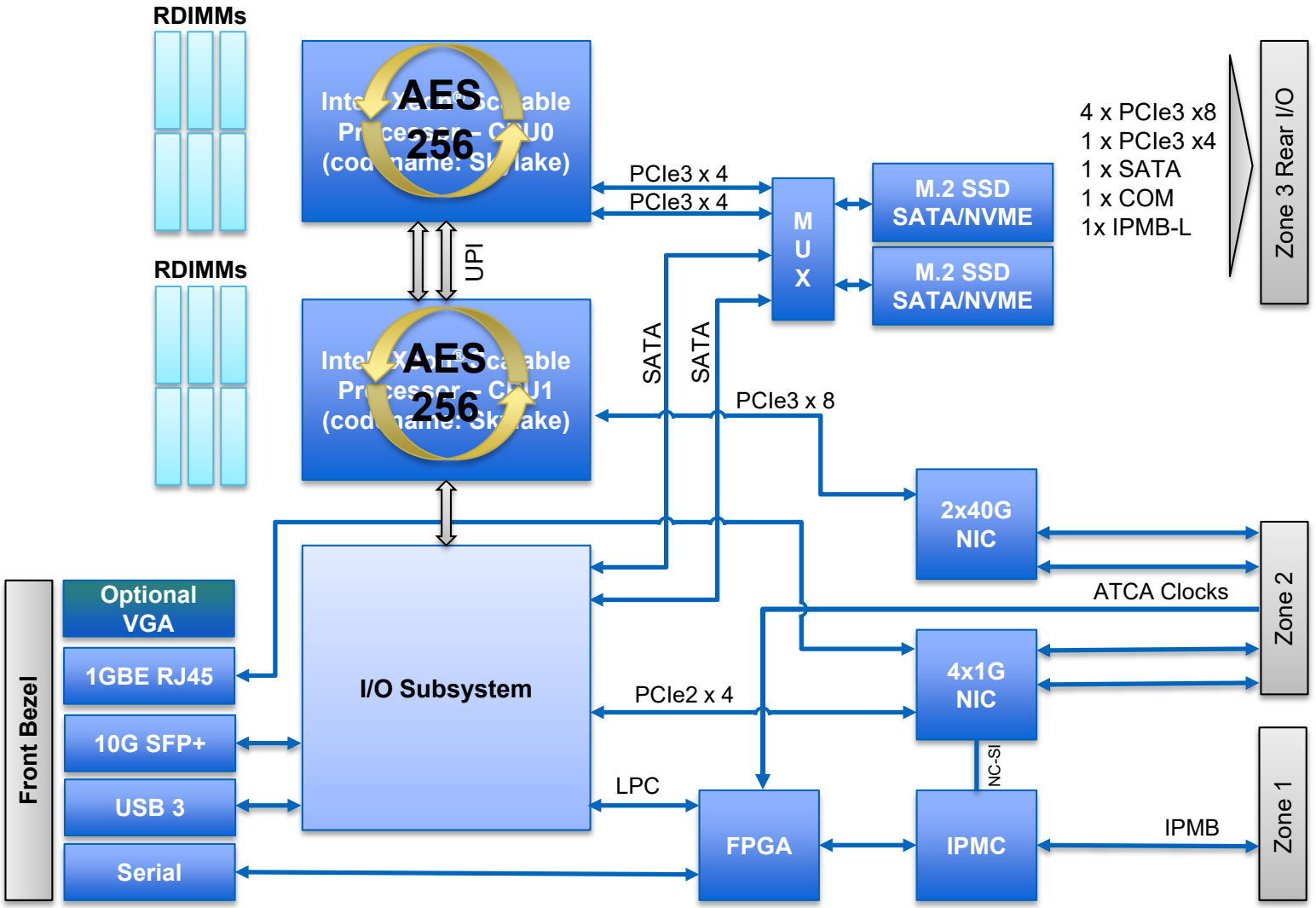
Encryption Algorithm Methods

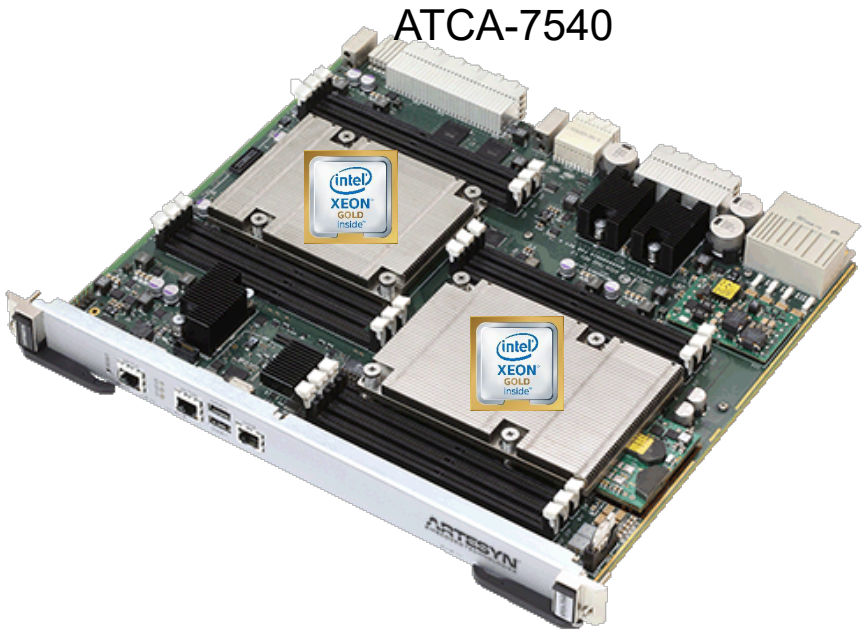


Advanced Encryption Standard

AES-256

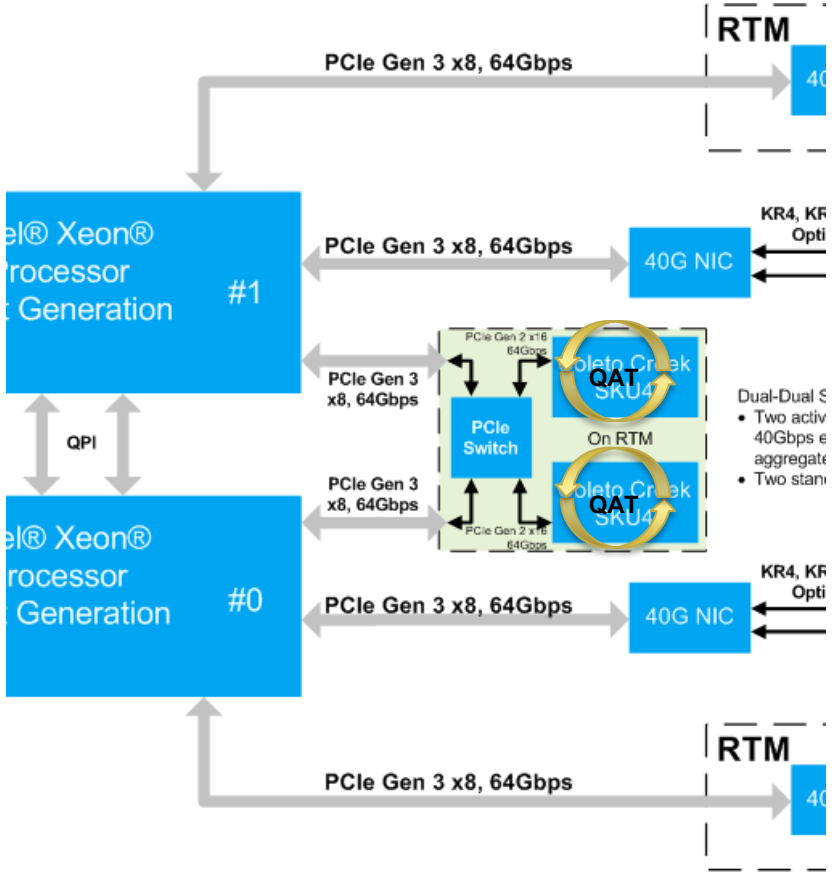
Approaches to Encrypting Tactical Data



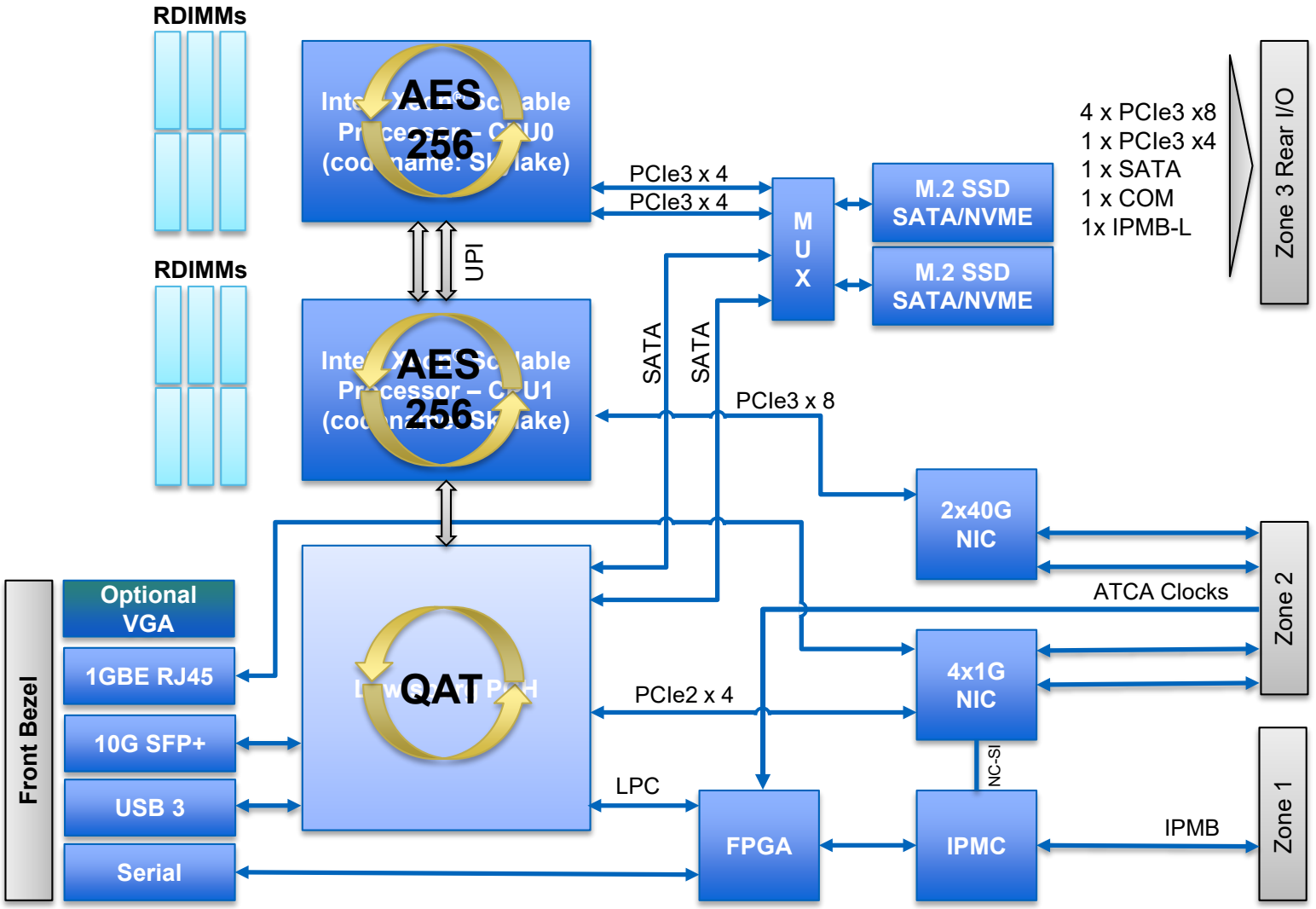


Intel® Quick Assist Technology

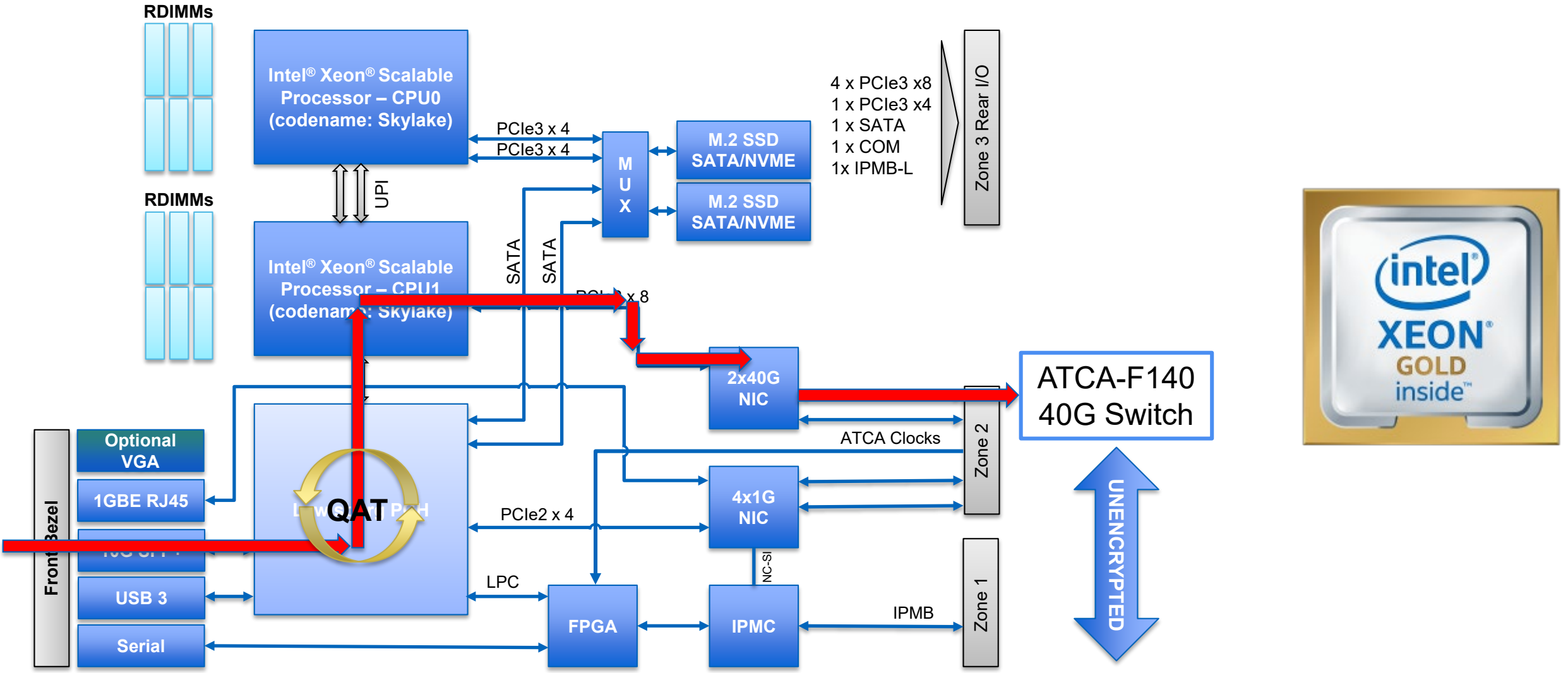
- Symmetric cryptography functions
  - Cipher operations (AES, DES, 3DES, ARC4)
  - Wireless (Kasumi, Snow 3G)
  - Hash/authenticate operations (SHA-1, MD5; SHA-2 [SHA-224, SHA-256, SHA-384, SHA-512])
  - Authentication (HMAC, AES-XCBC, AES-CCM); AES-XTS (8925, 8950 and 8955 only)
  - Random number generation.
- Public Key functions
  - RSA operation
  - Diffie-Hellman operation
  - Digital signature standard operation
  - Key derivation operation
  - Elliptic curve cryptography (ECDSA and ECDH)
  - Random number generation
  - Prime number testing
- Compression/decompression
  - DEFLATE (Lempel-Ziv 77)
  - LZS (Lempel-Ziv-Stac)



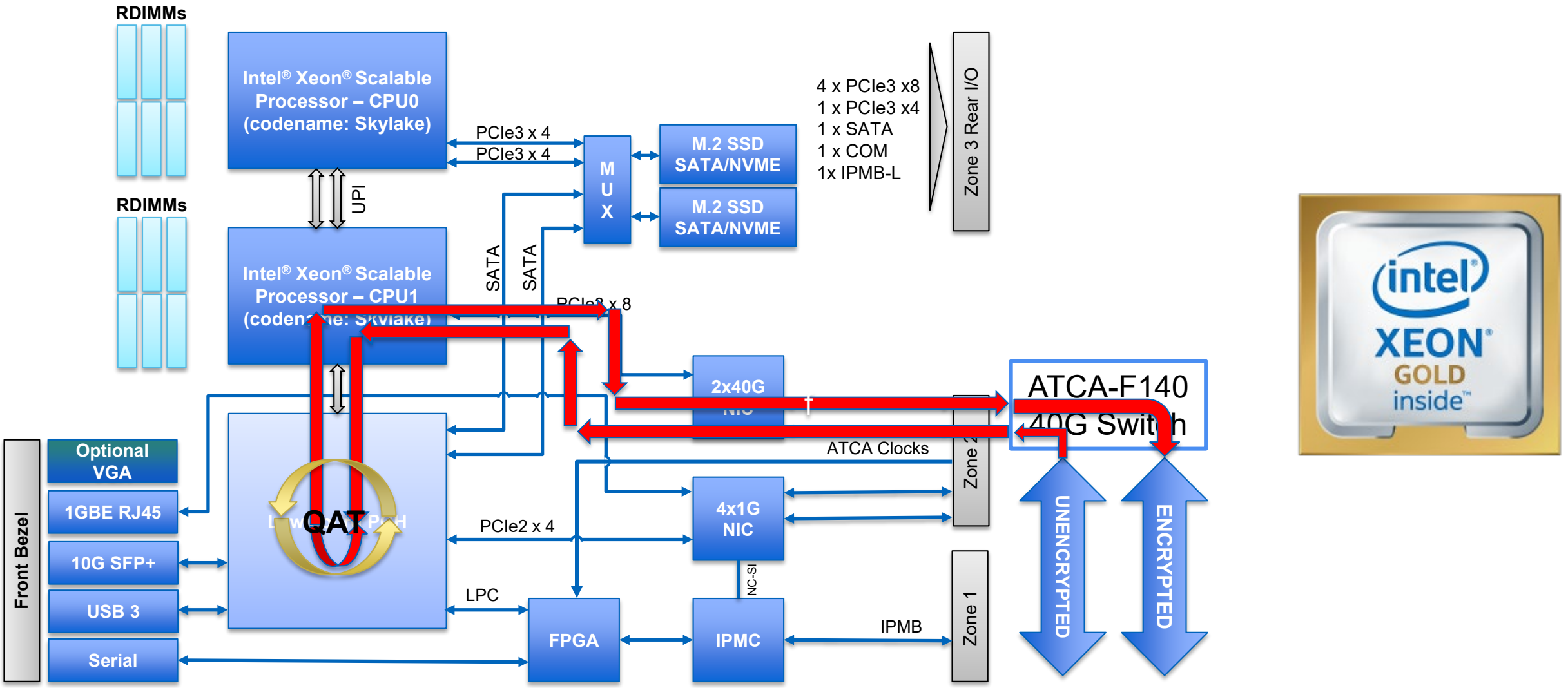
ATCA-7540 with QAT



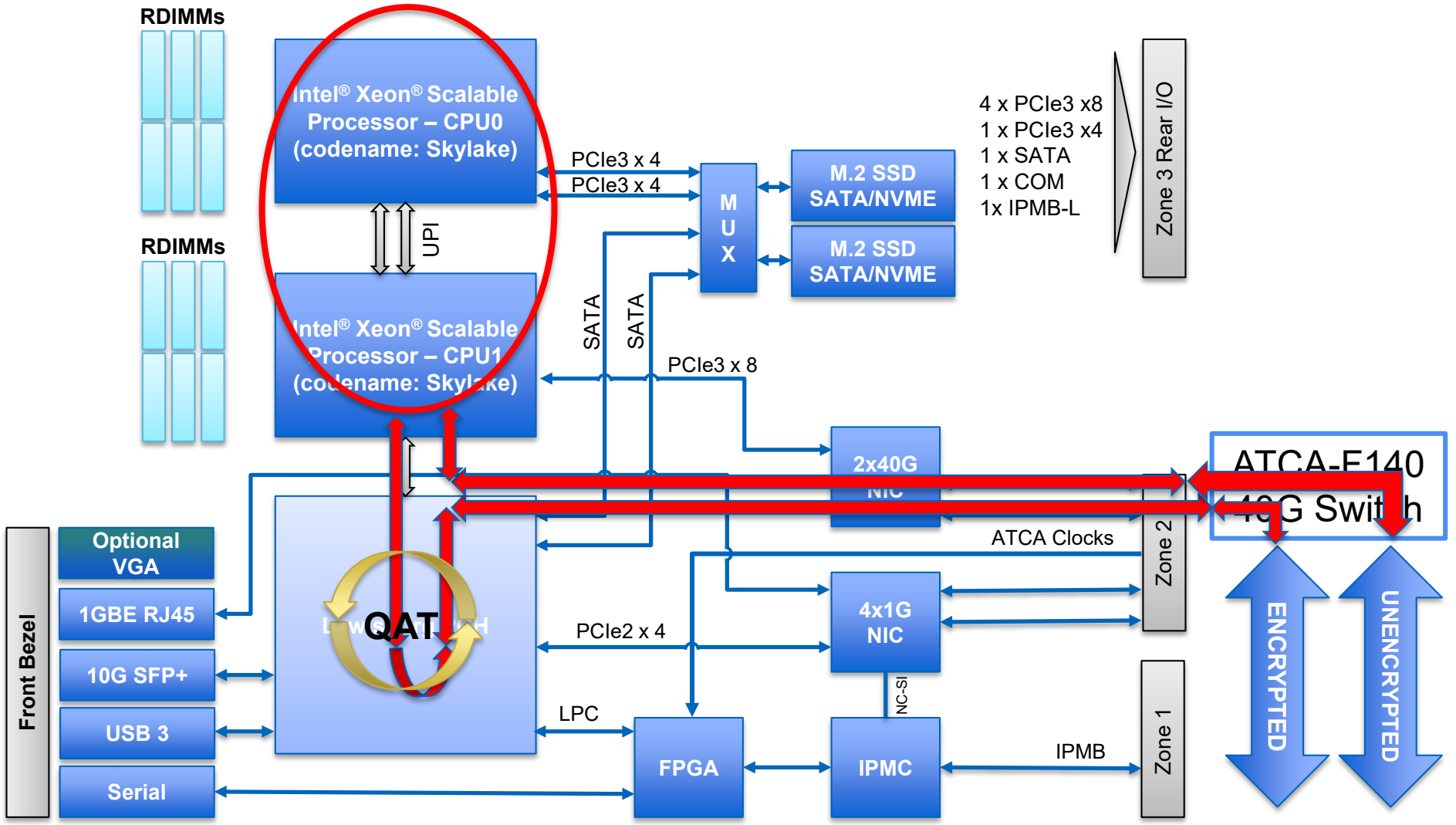
External Secure Gateway



Internal Secure Gateway



Completely Secure System



Data Size	Protocol	OpenSSL Test	QAT	Software/CPU	Magnitude Improvement
			Async	Software/CPU	
	Sign/s	RSA2048	20707	1485	13.9
	Verify/s	RSA2048	160306	52914	3.0
				Average Improvement	8.5

Data Size	Protocol	OpenSSL Test	QAT	Software/CPU	Magnitude Improvement
160 bits	ecdh	(secp160r1)	42773	4529.3	9.4
192 bits	ecdh	(nistp192)	37878	3842.6	9.9
224 bits	ecdh	(nistp224)	31580.2	2650.6	11.9
256 bits	ecdh	(nistp256)	30075.1	18459.3	1.6
384 bits	ecdh	(brainpoolP384r1)	16516.2	1001.7	16.5
384 bits	ecdh	(brainpoolP384t1)	16570.5	1016.2	16.3
512 bits	ecdh	(brainpoolP512r1)	12863.3	685.1	18.8
512 bits	ecdh	(brainpoolP512t1)	12823.4	666.8	19.2
253 bits	ecdh	(X25519)	24414.7	26265.4	0.9
448 bits	ecdh	(X448)	1681.4	1678.1	1.0
				Average Improvement	12.27482669

Quick Assist Improvement over CPU

Protocol	Average Magnitude Improvement
RSA2048	8.5X
ECDH	10.2X

But Why Bother??