Challenges in Data Security In High speed Networks (IB) Perspective

Security issues to resolve?

Secure transactions in Infiniband Protocol:

- Secure SRP(SCSI RDMA Protocol) transactions
- Identify appropriate layer for Security i.e. SSL, IPSec etc.
  - SSL being at TCP layer (host/server to client)
  - IPSec being at IP layer (peer to peer)
- Identify appropriate Security protocol i.e.
  - AES-128/256/?, DES Or other?
  - Security strength over Speed/silicon/cost
- Many more software and Hardware issues relating to functionality, performance, portability etc need to be resolved.
  - What is critical in the order of priority?
  - Do them in stages?

Other issues

- Software Performance considerations:
  - Open-IB: How well tested and performance bench marked are SRP Host drivers and key middleware, supporting SCSI RDMA Protocol (SRP) for block storage applications?
  - Where do you terminate SRP internally at the InfiniBand interface (into fiber channel) for maximum Performance ?

Comparison DES vs AES

Keys technology and their vulnerability comparison:

	DES	AES
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128, 192, or 256 bits
Developed	1977	2000
Cryptanalysis resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and Square attacks
Security	Proven inadequate	Considered secure
Possible Keys	2^{56}	2^{128}, 2^{192}, or 2^{256}
Possible ASCII printable character keys*	95^{7}	95^{16}, 95^{24}, or 95^{32}
Time required to check all possible keys at 50 billion keys per second**	For a 56-bit key: 400 days	For a 128-bit key: 5 x 10^{21} years

ECC/RSA bit sizes in 3DES, AES

Algorithms used in different Keys for varying security levels
Comparative ECC and RSA bit size requirements for five different symmetric algorithms in order to achieve different bit-security levels.

Symmetric key Algorithm	**Skipjack**	**3-DES**	**AES-128 small**	**AES-192 Medium**	**AES-256 Large**
Hash algorithm	**SHA-1**	**SHA-256**	**SHA-256**	**SHA-384**	**SHA-512**
Bit-security level	80	112	128	192	256
ECC size (prime)	192	224	256	384	512
ECC size (binary)	163	239	283	409	571
RSA modulus size	1024	2048	3072	7680	15360

•ECC takes significantly less processing, smaller Chip size, Less software overhead

•RSA-1204, gate count= 150,000, in 2.60 ms
Vs
•ECC-163, gate count= 48,400, in 0.35 ms. Each sides sends one 41 byte payload data

sources: FIPS 186-2. NIST SP 800-57. ANSI X9.30.1 – 2002

Software driver tasks

Very lean/thin-layer driver Model for highest performance.

- **OS Allocates ‘Crypto_buffers’**
- **Allign Buffers to be Encrypted.**
- **Handover to the Hardware accelerator.**
- **Free up the buffer for more data**
- **SSL functions are performed/completed e.g.**
- **Handshaking, record handling, Cryptography.**

Reverse happens during ‘Decryption’

Intelop Encryption/Decryption Solution
Key Features

- **Processes 128-bit data in 32-B blocks**
- **Employs user-defined, 128, 192 or 256 bits Key**
- **Smallest version supports a single block cipher mode, Electronic Codebook (ECB).**
- **Modes can be added as needed:**
  - **Cipher Block Chaining (CBC)**
  - **Cipher Feedback (CFB**
  - **Output Feedback (OFB)**
  - **Counter (CTR)**
  - **Counter with CBC-MAC (CCM)**

- **Satisfies (FIPS) Publication 197 from the US Technology (NIST)**

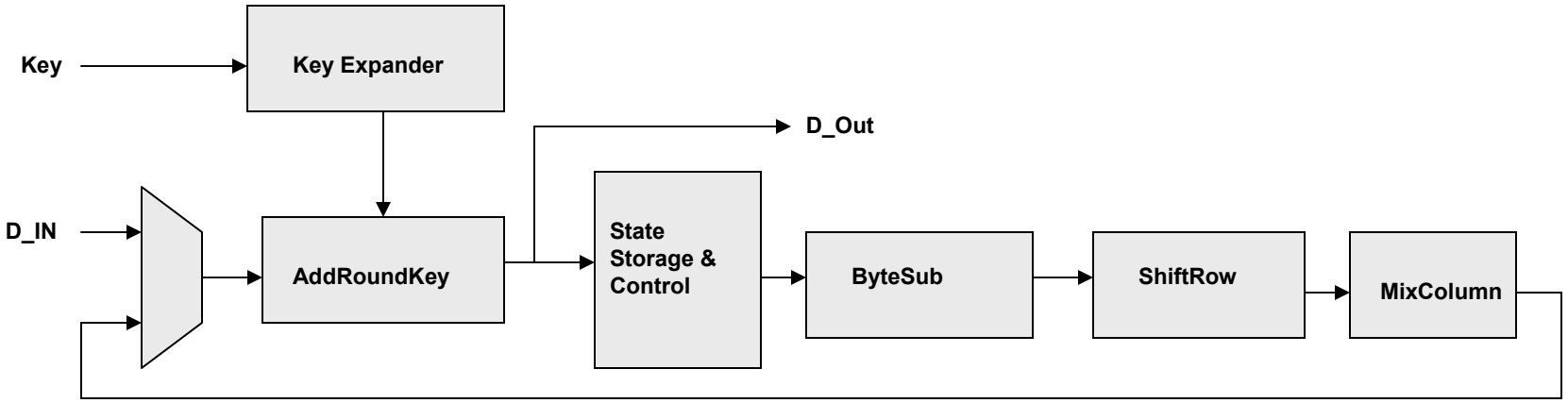
AES-128 Used In Products:

System Application: Storage Server, ‘SecureRAID with 2 G-bit Ethernet ports

AES-128 implemented in Xilinx FPGA, V2P-7
Internal Clock rate 250 MHz
External I/O Clock rate at 125 MHz.

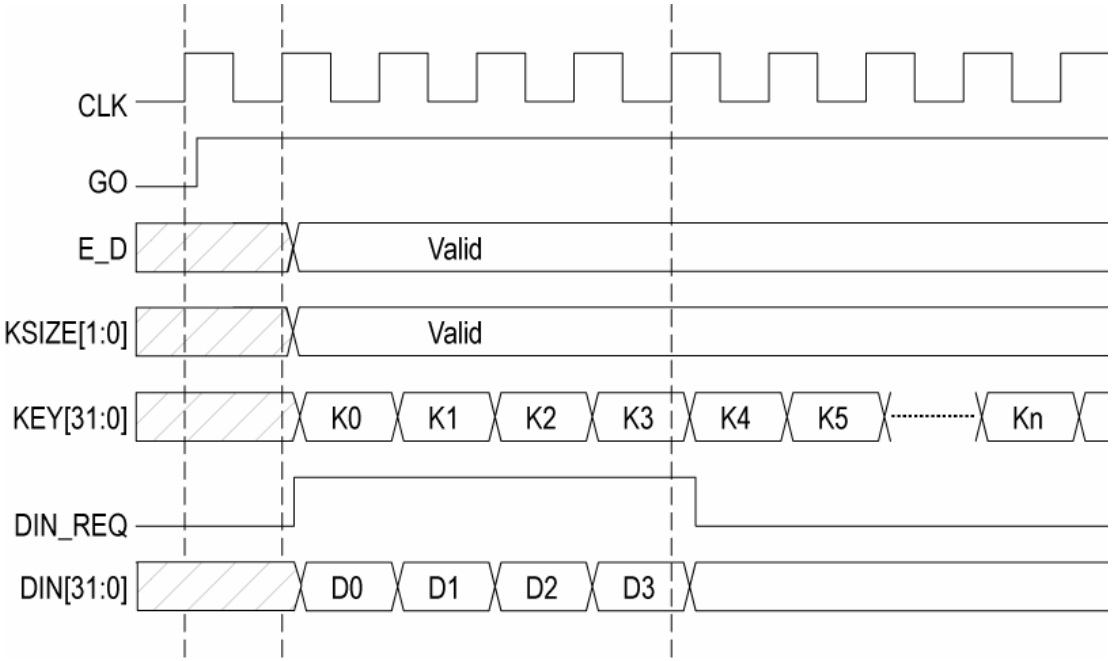
Throughput: 550Mbps

AES Architecture



- Data_In and the key are added together in the AddRoundKey module
- Result is stored in the State Storage area
- State information is then retrieved and the ByteSub, Shiftrow, MixColumn and AddRoundKey functions are performed on it in the specified order
- At the end of each round, the new state is stored in the State Storage
- operations are repeated according to the number of rounds
- final round is anomalous as the MixColumn step is skipped. The cipher is output after the final round

Key Operation's timing



The KSIZE parameter is passed to the core when GO signal is raised.
Input of the KEY data continues for the duration of the cryptographic operation.
Both the data and the key are input serially, 32 bits at a time.
Diagram above shows the case where the input data is 128 bits.

Key Operation Performance

KeySIZE = 128	KeySIZE = 192	Key SIZE = 256
Cycles 44	52	60

During Encryption, the key expander generates expanded key on the fly while the AES core takes it.

For decryption, key is pre-expanded and stored in memory before being used by the AES core.

Core uses the expanded key backwards during decryption.

In cases, key expander is not required, when the key does not need to be changed and so it can be stored in its expanded form or when the key does not change very often, it can be expanded in software

Implementation Results

Device Utilization and Performance numbers

AES 128-bit	TSMC 0.13 u	17.5 Kgates	151 MHz	~1.75 Gbit/s	area
AES 128-bit	UMC 0.18 u	16 Kgates	144 MHz	~1.67 Gbit/s	area
AES 128-bit	TSMC 0.13 u	36.8 Kgates	400 MHz	~4.64 Gbit/s	speed
AES 128-bit	UMC 0.18 u	34.6 Kgates	344 MHz	~3.99 Gbit/s	speed

Study of different Algorithms and Keys

Legacy Keys: (DES) Briefs

DES Modes of Operation

-FIPS 81
-Four modes defined
– Electronic Code Book (ECB)
– Cipher Block Chaining (CBC)
• *Can be used for Message Authentication Code (MAC)*
– Cipher Feedback (CFB)
– Output Feedback (OFB)
-Uses 64-bit blocks
-56 bit keys

Proven to be vulnerable to attack by key exhaustion, was replaced by Triple-DES

NIST National Institute of Standards and Technology

Legacy Keys: (Triple DES) Briefs

Triple DES Modes of Operation

-FIPS 46-3 and ANSI X9.52
-64 bit block size
-112 and 168 bit keys
– DES repeated 3 times with 2 or 3 different keys
-Strong protection
-Easy substitution for DES
– Main difference is bigger key size & slower performance
-Expands 4 DES modes into 7 modes

Proven to be vulnerable to attack by key exhaustion, being replaced by AES

NIST National Institute of Standards and Technology

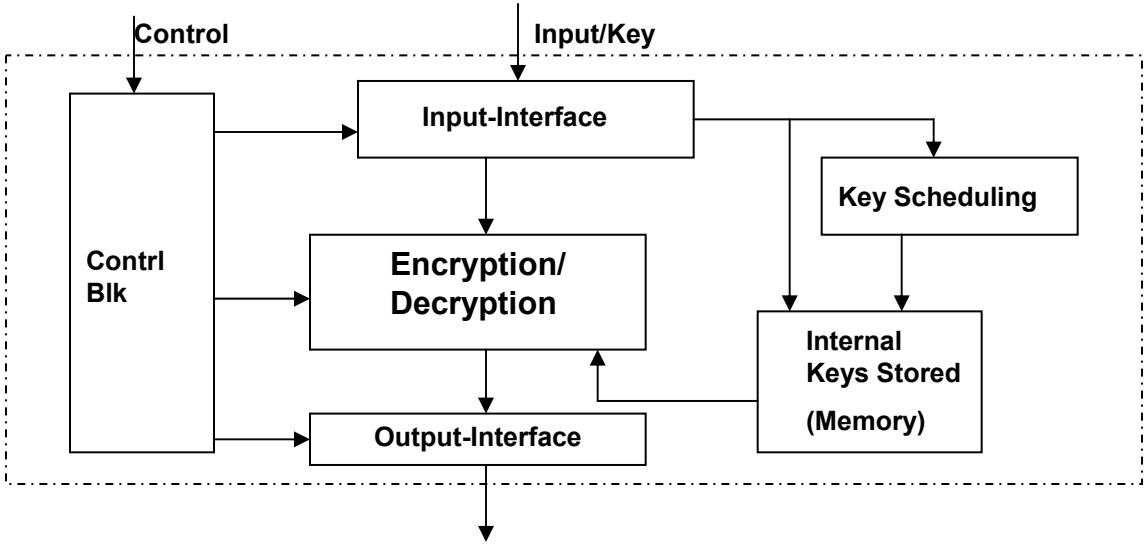
Legacy Keys: (AES) Briefs

-DES and Triple DES replacement
- Selected through open competition run by NIST
– Public evaluation and analysis
– 21 original submissions, 5 “finalists”
– Final selection of ***Rijndael*** announced Oct. 2, 2000
– http://www.nist.gov/aes
- Strong encryption with long expected life
– 128 bit block size
– 128, 192, & 256 bit key sizes

May be royalty free worldwide

NIST National Institute of Standards and Technology

Block diagram: Hardware implementation of a symmetric-block cipher



Rijendael Being the most promising of the 5 AES algorithms selected by the NIST-FIP-197.
(Others being MARS, RC6, Serpent and TwoFish)

The basic organization of the hardware implementation of a symmetric block cipher is shown in Fig. 2. AES can be implemented in blocks shown:

a. *Encryption/decryption unit*, used to encipher and decipher input blocks of data.

b. *Key scheduling unit*, used to compute a set of internal cipher keys based on a single external key.

c. Internal *keys*, used to store internal keys computed by the key scheduling unit, or loaded to the integrated circuit through the input interface.

d. *Input interface*, used to load blocks of input data and internal keys to the circuit, and to store input blocks awaiting encryption/decryption.

e. *Output interface*, used to temporarily store output from the encryption/decryption unit and send it to the external memory.

f. *Control unit*, used to generate control signals for all other units.

Feedback vs. non-feedback operating modes

Symmetric block ciphers are used in several operating modes. From the point of view of hardware implementations, these modes can be divided into two major categories:

a. *Non-feedback modes*, such as **Electronic Code Book mode (ECB**), and counter mode.
b. *Feedback modes*, such as **Cipher Block Chaining mode (CBC), Cipher Feedback Mode (CFB**), and **Output Feedback Mode (OFB).**

In the non-feedback modes, encryption of each subsequent block of data can be performed independently from processing other blocks. In particular, all blocks can be encrypted in parallel. In the feedback modes, it is not possible to start encrypting the next block of data until encryption of the previous block is completed. As a result, all blocks must be encrypted sequentially, with no capability for parallel processing.
According to current security standards, the encryption of data is performed primarily using feedback modes, such as CBC and CFB. Non-feedback modes, such as ECB, are used primarily to encrypt session keys during key distribution. As a result, using current standards does not permit to fully utilize the performance advantage of the hardware implementations of secret key cryptosystems, based on parallel processing of multiple blocks of data.

Key Sizes/Time-to-break

Comparison of Key Size:

Time to break in MIPS years	*RSA/DSA key size*	*ECC key size*	*RSA/ECC key size ratio*
10^4	*512*	*106*	*5 : 1*
10^8	*768*	*132*	*6 : 1*
10^{11}	*1,024*	*160*	*7 : 1*
10^{20}	*2,048*	*210*	*10 : 1*
10^{78}	*21,000*	*600*	*35 : 1*

**MIPS year represents a computing time of one year on a machine capable of performing one million instructions per second.*

SHA-nnn/Comparison

-Secure Hash Algorithm SHA-1
- -FIPS 180-1; ANSI X9.30 Part 2
- -160 bit message digest
- -Wide current use
- -Used with DSA, RSA or ECDSA

-"Birthday" attacks against a hash make *n*-bit AES and a 2*n*-bit hash roughly equivalent

– 128-bit AES » SHA-256
– 192-bit AES » SHA-384
– 256-bit AES » SHA-512

– DSA limited to 1024 bits
– 128-bit AES roughly as strong as 3000 bit DSA
– 1024 bit DSA roughly as strong as 160-bit SHA-1

Available at http://www.nist.gov/sha

NIST National Institute of Standards and Technology

OSI-Layer Implementation: IPSEC OVERVIEW

• IPSEC

-Strong confidentiality, integrity, and authentication at the IP (Network) layer.

• Two architectural elements:
1— *IKE* - does session key management
– Key exchange with either RSA or D-H
– Session protected with DES or 3DES
2— *AH* and *ESP* transforms - carries user data, protected under keys/algorithms negotiated during *IKE*
– Integrity provided by either HMAC-MD5 or HMAC-SHA1
– Confidentiality provided by either DES or 3DES
• Moving to AES and SHA-2
— (NIST) has produced an Internet-Draft describing the use of AES.

NIST National Institute of Standards and Technology

OSI-Layer Implementation TLS
(RFC2246,2712)

Provides Transport Layer Security--usually between application and TCP

• Originated external to IETF, as SSLV3. Most WEB browsers today implement SSLV3, TLS could be next.

• Growth of the WEB has driven growth in deployment of SSLV3, and TLS.

• SSLV3 has almost completely obliterated SET (MasterCard/VISA secure transaction initiative).

• Other application protocols starting to be secured with SSLV3/TLS:

— IMAP

— POP3

— TELNET

— FTP

• Flexible with respect to “crypto suites”.

Replacing current DES/3DES-based suites with AES-based suites.

What is the direction?

- AES-256 Nearly impossible to crack, Very Very strong.

- Implemented in Hardware.
  - For faster Key generation/higher performance and depending upon application, AES-128 can be considered.

- Most of the important protocols will be mandating AES over the next year, while the rest will phase it in over the next two or three years.

- Most IETF protocols that use encryption are naturally "AES Ready"

- DES and Triple DES will remain for backwards compatibility for some Time.

NIST National Institute of Standards and Technology