Security Applications

Abhyudaya Chodisetti
Paul Wang Lee
Garrett Smith

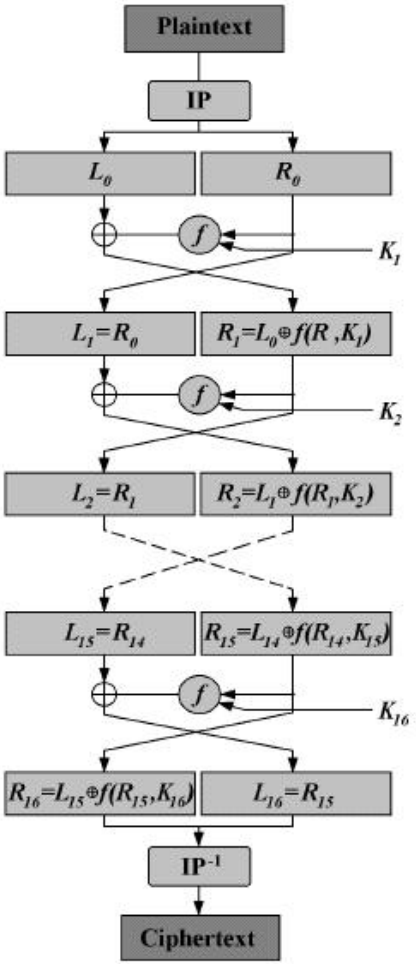
Cryptography

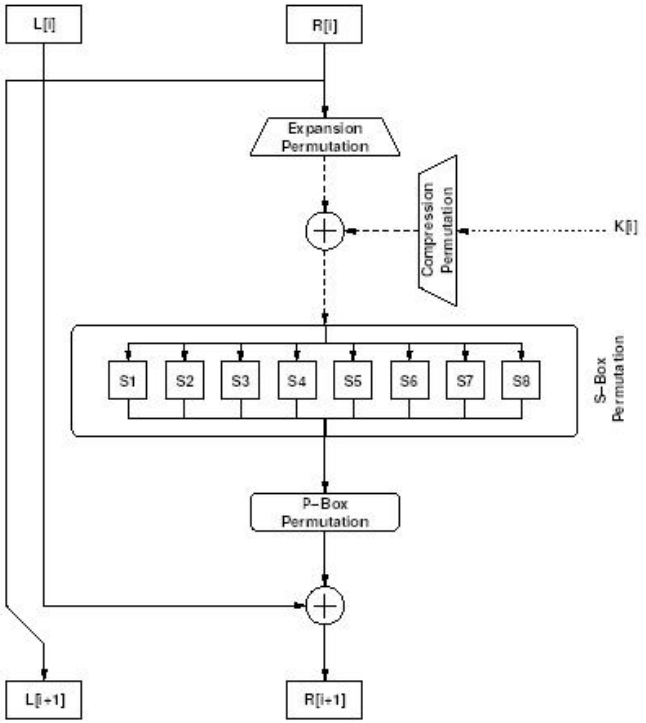
- Encryption
- Integrity : MAC(message authentication code)
- Digital signatures
- Authentication
- Extended applications
  - Electronic cash
  - Electronic voting
  - Secure auctions
  - Copyright protection

Major Components

- Block Ciphers
  - DES, AES
- Secure hash functions
  - SHA-1
- Public key encryption
  - RSA

DES


Plaintext
IP
L_0
R_0
f
K_1
$L_1=R_0$
$R_1=L_0 \oplus f(R_0,K_1)$
f
K_2
$L_2=R_1$
$R_2=L_1 \oplus f(R_1,K_2)$
$L_{15}=R_{14}$
$R_{15}=L_{14} \oplus f(R_{14},K_{15})$
f
K_{16}
$R_{16}=L_{15} \oplus f(R_{15},K_{16})$
$L_{16}=R_{15}$
IP^{-1}
Ciphertext


L[i]
R[i]
Expansion Permutation
Compression Permutation
K[i]
S1
S2
S3
S4
S5
S6
S7
S8
S-Box Permutation
P-Box Permutation
L[i+1]
R[i+1]

Chaining

- DES and AES both work on data blocks, 64 and 128bits respectively
- Most commonly used way of encrypting longer messages is CBC(Cipher Block Chaining), due to security properties
- Introduces serial dependency, limiting parallelism

Properties of DES/AES

- Data size / access patterns
  - Relatively small lookup tables (2K for DES)
  - For encryption, data size is arbitrarily large
  - Working set is small
    - Intermediate values are only used once and then discarded
- Input data is used in a streaming pattern
- Algorithm complexity is constant w.r.t. data
- Constant workload distribution over time

Software implementations

- Ratio of arithmetic to memory operations
  - Per block # of alu/memory operations :
    520/192 for DES, 507/111 for AES
  - Ratios are 2.7 for DES, 4.56 for AES

- DES is inefficient in software due to extensive use of bit-level permutation
- AES is designed to be more amenable to software implementations

Hashing functions

- SHA-1
  - 232 memory operations
  - 2879 other operations
  - Ratio of 12 alu/mem operations
- Reasonable amount of ILP compared to block ciphers

RSA (Public Key Encryption)

- Based on properties of modular arithmetic
- Two keys : private key d, public key e
- Encryption : $C = P^e \bmod M$
- Decryption : $P = C^d \bmod M$
- Uses property that d and e are chosen such that $x^{de} = x \bmod M$

RSA properties

- Key sizes : two 2048 bit integers
- Message size : 2048 bit integer
- Scales with $O(k^3)$ with efficient implementation (k: # key bits)
- Fast modular exponentiation required : multiplication and division
- In one software implementation, ratio of alu to memory operations is 1

Scaling trends

- Small number of very conservative standards
- Rate of change is slow (AES targeted for use during next 20 years)
  - Makes sense to embed special purpose hardware if performance is important
- Available scaling comes from :

  Number of requests per time and data size will increase

Custom hardware

- Custom ASIC's for DES/AES
- Cryptography coprocessors
  - Includes HW implementation of DES/AES
  - Modular arithmetic modules for RSA

Conclusion

- Special purpose modules are a good idea for cryptography applications
- Major scaling direction for cryptographic applications will be independent thread level