Brief Review of Cryptography Basics and Presentation of Crypto System Sample Design

Crypto Algorithm Rundown

- Symmetric (secret key cryptography)

· Encrypt and decrypt using same key

- DES
- 3DES
- AES

- Asymmetric (public key cryptography)

· Two related keys: one public, the other private

· Mainly used for signatures & key establishments

- DSA
- RSA

- Hashing

· Compute a "cryptographic checksum" or "message digest " of messages of files.

· Used for integrity, authentication and signatures

- SHA - 1
- SHA - 256

The Who's Who Of Symmetric Algorithms

- Data Encryption Standard (DES)

  - 64 bit block size
  - 56 bit keys
  - more than 2 decades old (vulnerable to attack by key exhaustion)

- Triple Data Encryption Standard (3DES)

  - 64 bit block size
  - 112 and 168 bits keys
  - DES repeated 3 times with 2 or 3 different keys

- Advanced Encryption Standard (AES)

  - developed and submitted by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen
  - 128 bit block size
  - 128, 192 and 256 bit key sizes

How AES Operates

byte	byte	byte	byte
byte	byte	byte	byte
byte	byte	byte	byte
byte	byte	byte	byte

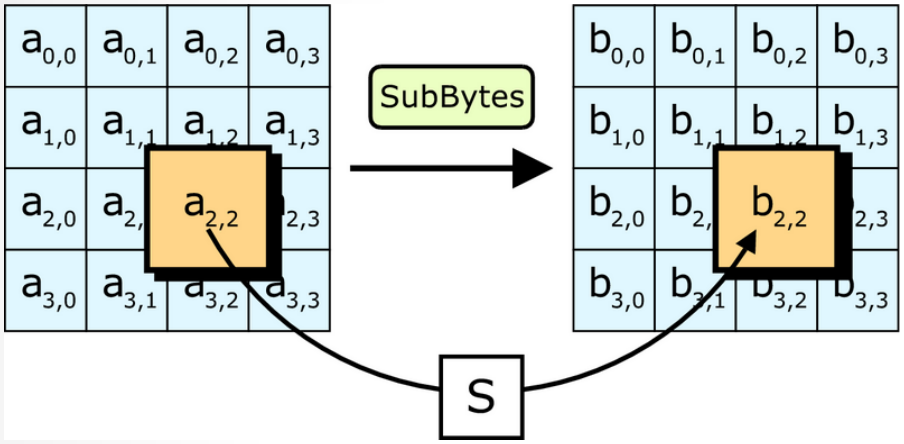
operates on a 4x4 array of bytes, termed *state*

four steps make up a *round* :

- substitution
- shift
- mix
- add key

the final round omits the *mix* step

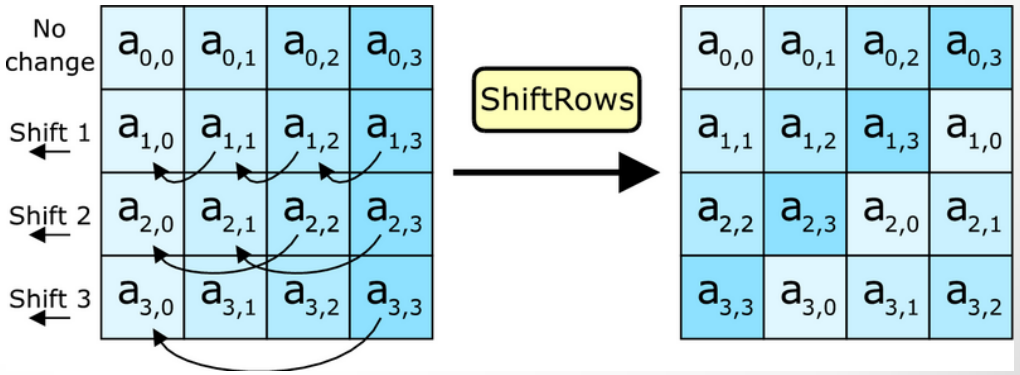
Steps 1 and 2: SubBytes and ShiftRows



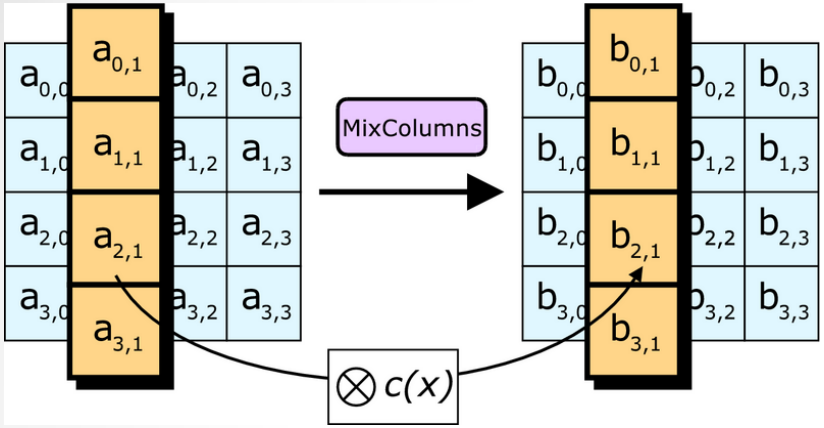
Each byte in the array is updated using an 8-bit S-box, which provides the non-linearity in the cipher.

The S-box is derived from the inverse function over GF(2^8)

Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively.



Steps 3 and 4: MixColumns and AddRoundKey

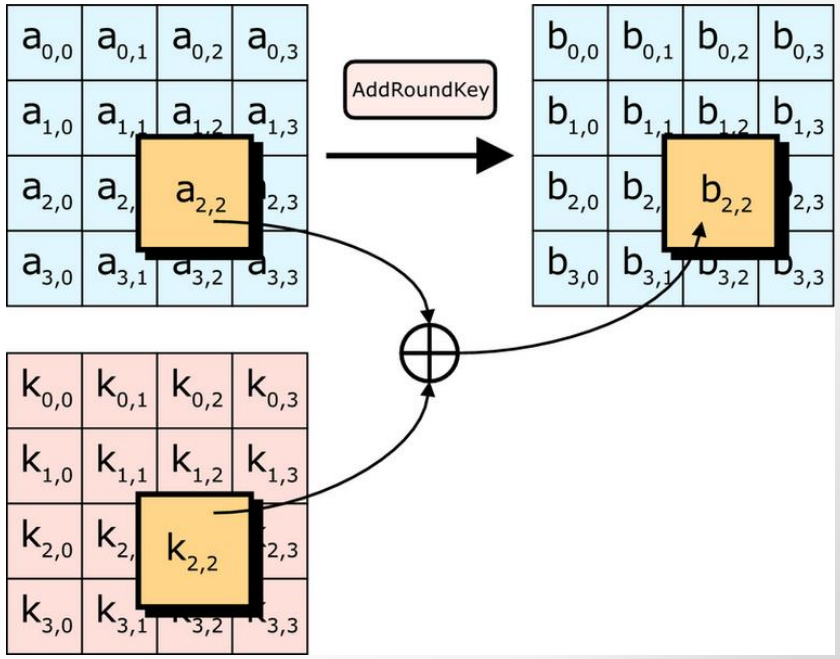


The four bytes of each column of the state are combined using an invertible linear transformation.

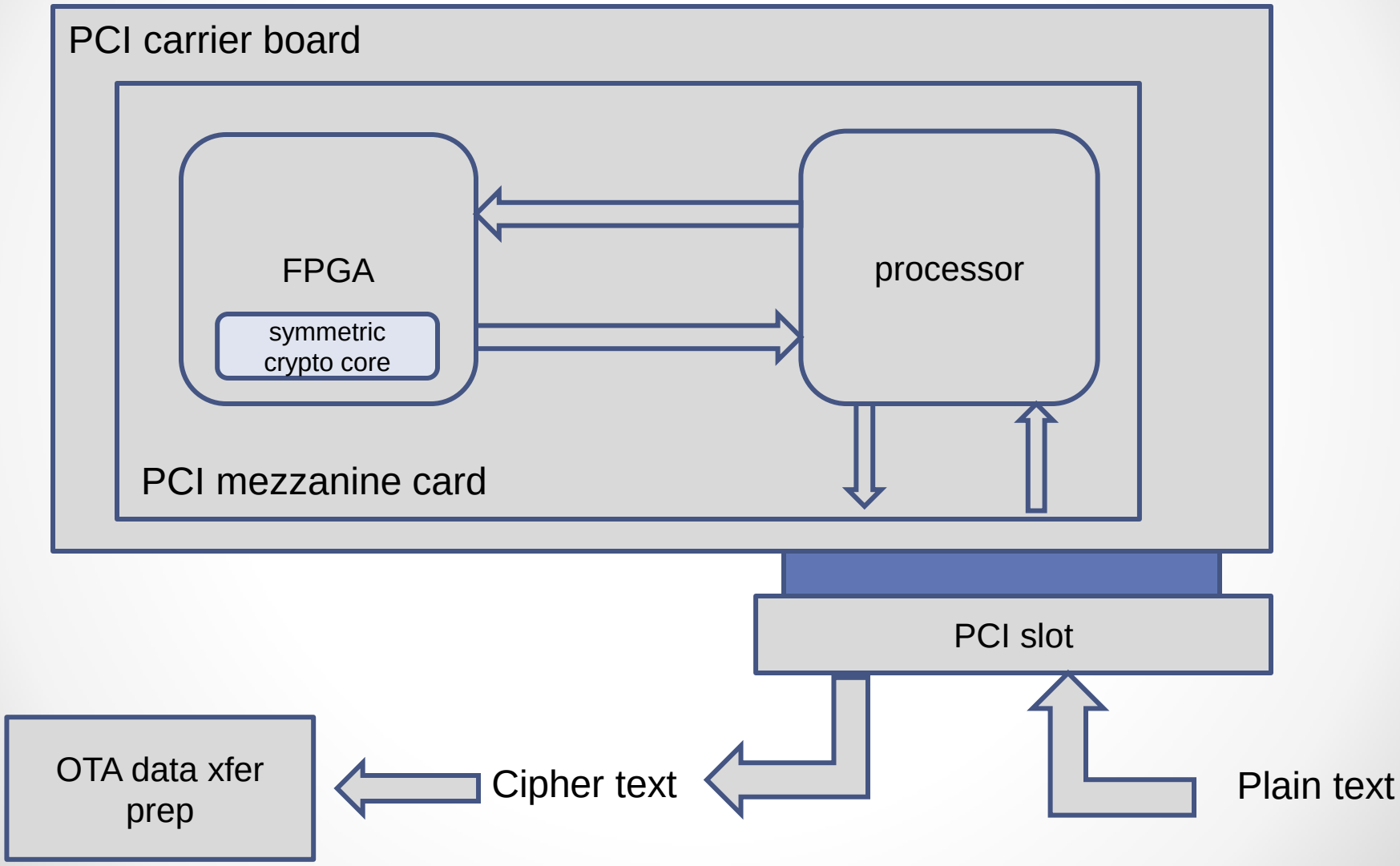
Each column is treated as a polynomial over GF(2^8) and is then multiplied modulo $x^4 + 1$ with a fixed polynomial $c(x) = 3x^3 + x^2 + x + 2$.

For each round, a subkey is derived from the main key using the key schedule; each subkey is the same size as the state.

The subkey is combined with the state via bitwise XOR.



Sample Crypto Card Concept



Loopback Test System