T-79.159
Cryptography and Data Security

Lecture 3:
3.1 Introduction to block ciphers
3.2 DES
3.3 IDEA
3.4 AES
Kaufman et al: Chapter 3
Stallings: Chapters 3, 5

1

Block ciphers

Confidentiality primitive

- Threat: recover the plaintext from the ciphertext without the knowledge of the key.
- Security goal: protect against this threat.

Plaintext P: strings of bits of fixed length n

Ciphertext C: strings of bits of the same length n

Key K: string of bits of fixed length k

Encryption transformations: For each fixed key the encryption operation E_K is one-to-one (invertible) function from the set of plaintexts to the set of ciphertext. That is, there exist an inverse transformation, decryption transformation D_K such that for each P and K we have: $D_K (E_K (P)) = P$

2

Block ciphers, design principles

- The ultimate design goal of a block cipher is to use the secret key as efficiently as possible.
- Confusion and diffusion (Shannon)
- New design criteria are being discovered as response to new attacks.
- A state-of-the-art block cipher is constructed taking into account all known attacks and design principles.
- But no such block cipher can become provably secure, it may remain open to some new, unforeseen attacks.
- Common constructions with iterated round function
  - Substitution permutation network (SPN)
  - Feistel network

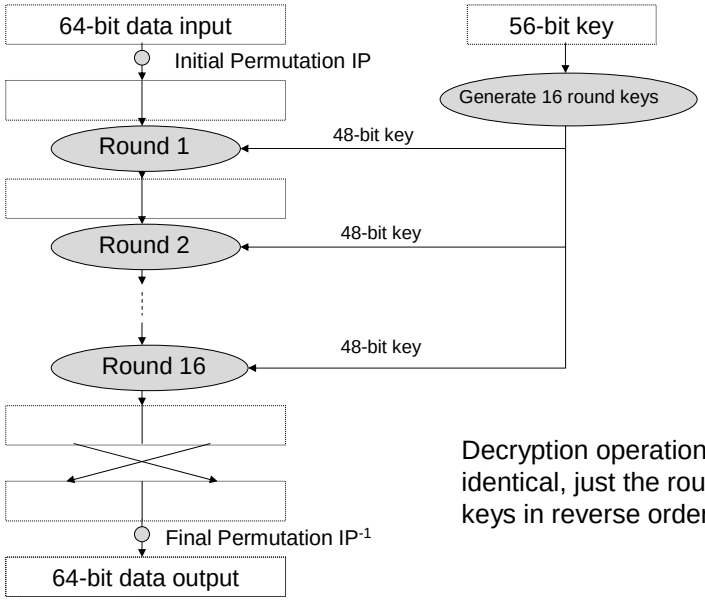
3

DES Data Encryption Standard 1977 - 2002

- Standard for 25 years
- Finally found to be too small. DES key is only 56 bits, that is, there are about 10^{16} different keys. By manufacturing one million chips, such that, each chip can test one million keys in a second, then one can find the key in about one minute.
- The EFF DES Cracker built in 1998 can search for a key in about 4,5 days. The cost of the machine is $250 000.
- DES has greately contributed to the development of cryptologic research on block ciphers.
- The design was a joint effort by CIA and IBM. The design principles were not published until little-by-little. The complete set of design criteria is still unknown.
- Differential cryptanalysis 1989
- Linear cryptanalysis 1993

4

DES encryption operation overview

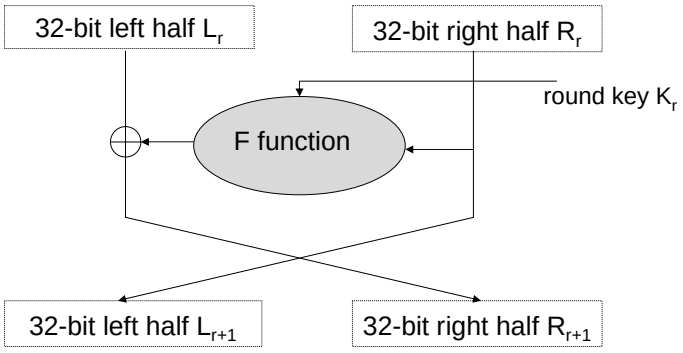


Decryption operation is identical, just the round keys in reverse order

5

DES round function

Round function is its own inverse (involution):



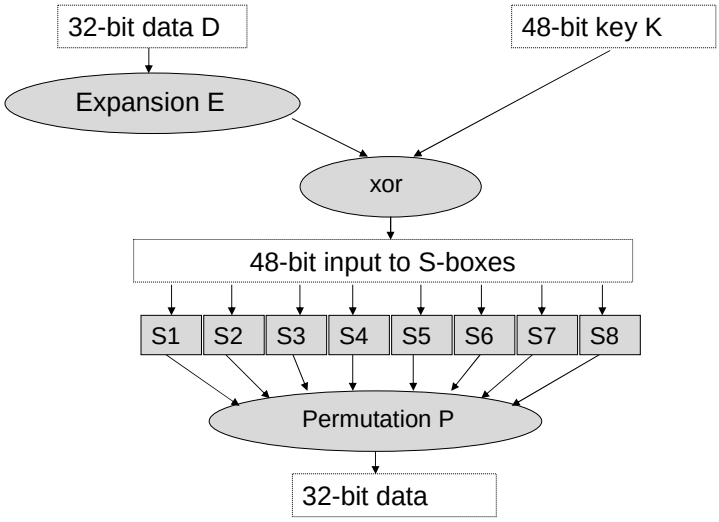
$L_{r+1} = R_r$

$R_{r+1} = L_r \text{ xor } F(R_r, K_r)$

6

The F-function of DES

F(D;K) = P(S(E(D) xor K)



7

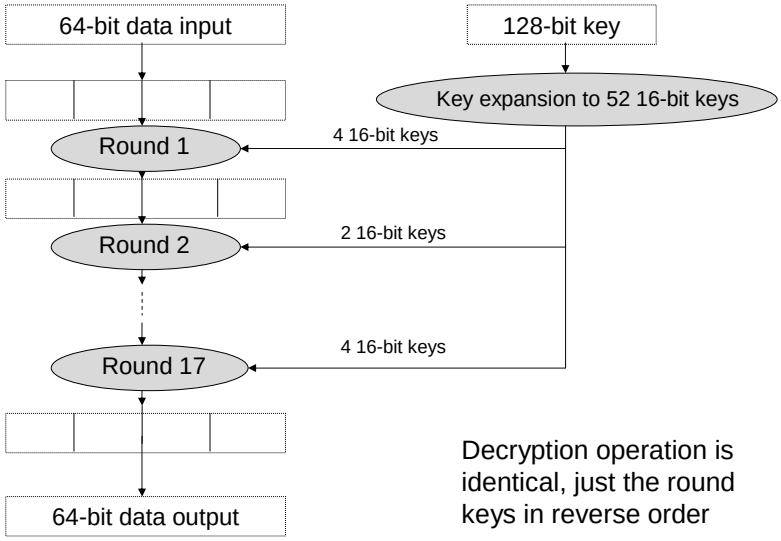
The DES S-boxes

- Small 6-to-4-bit functions
- Given in tables with four rows and 16 columns
- Input data a1,a2,a3,a4,a5,a6
- The pair of bits a1,a6 point to a row in the S-box
- Given the row, the middle four bits point to a position from where the output data is taken.

- S-boxes are the only source of nonlinearity in DES. Their nonlinearity properties are extensively studied.

8

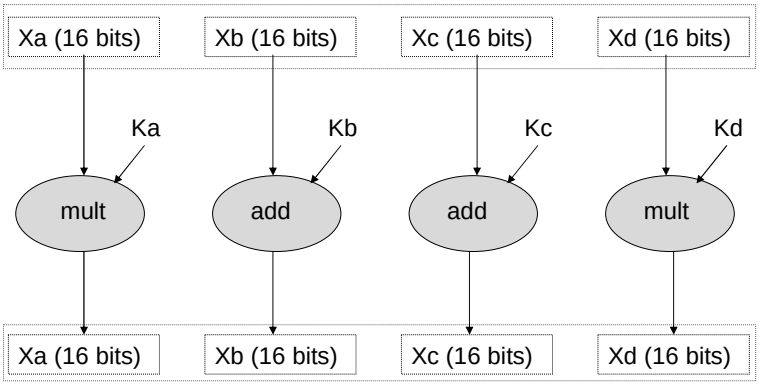
IDEA encryption operation overview



Decryption operation is identical, just the round keys in reverse order

9

One round of IDEA: odd round



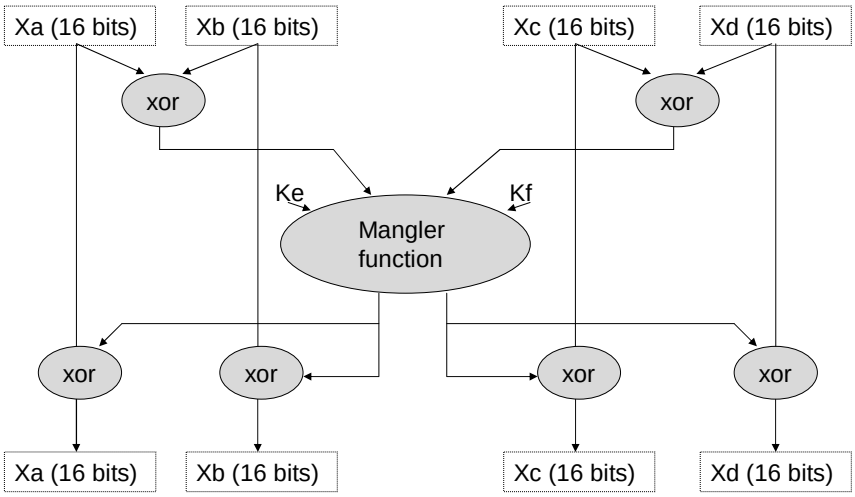
Legend:

mult — Multiplication modulo $2^{16}+1$, where input 0 is replaced by 2^{16}, and result 2^{16} is encoded as 0

add — Addition modulo 2^{16}

10

One round of IDEA: even round

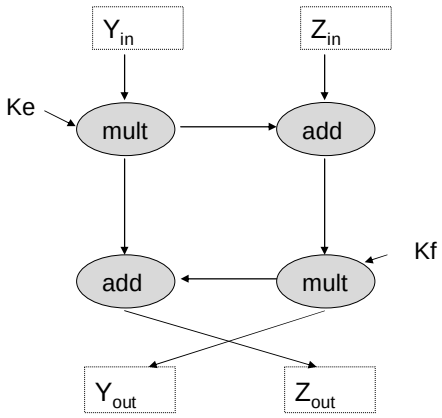


11

The mangler function

Y_{out} = (Ke mult Y_{in}) add Z_{in}) mult Kf

Z_{out} = (Ke mult Y_{in}) add Y_{out}



12

The Security of IDEA

- IDEA has been around almost 15 years
- Designed by Xuejia Lai and Jim Massey
- Its only problem so far is its small block size
- Numerous analysis has been published, but nothing substantial
- It is not available in public domain, except for research purposes
- It is available under licence
- It is widely used, e.g in PGP (see Lecture 11)

13

AES

AES

- Candidates due June 15, 1998: 21 submissions, 15 met the criteria
- 5 finalists August 1999: MARS, RC6, Rijndael, Serpent, and Twofish, (along with regrets for E2)
- October 3, 2000, NIST announces the winner: Rijndael
- FIPS 197, November 26, 2001

  Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES)

14

Rijndael - Internal Structure

Rijndael is an iterated block cipher with variable length block and variable key size. The number of rounds is defined by the table:

	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

AES

Nb = length of data block in 32-bit words

Nk = length of key in 32-bit words

15

Rijndael - Internal Structure

- First Initial Round Key Addition
- 9 rounds, numbered 1-9, each consisting of
  - Byte Substitution transformation
  - Shift Row transformation
  - Mix Column transformation
  - Round Key Addition
- A final round (round 10) consisting of
  - Byte Substitution transformation
  - Shift Row transformation
  - Final Round Key Addition

16

Rijndael - Inverse Structure

ENCRYPT (2 rounds)	DECRYPT (2 rounds)	INV ENCRYPT (2 rounds)
Initial Round Key Add	Final Round Key Add	Inv Initial Round Key Add
Byte Substitution	Inv Shift Row	Inv Byte Substitution
Shift Row	Inv Byte Substitution	Inv Shift Row
Mix Column	Round Key Addition	Inv Mix Column
Round Key Addition	Inv Mix Column	Inv Round Key Addition
Byte Substitution	Inv Shift Row	Inv Byte Substitution
Shift Row	Inv Byte Substitution	Inv Shift Row
Final Round Key Add	Initial Round Key Add	Inv Final Round Key Add

17

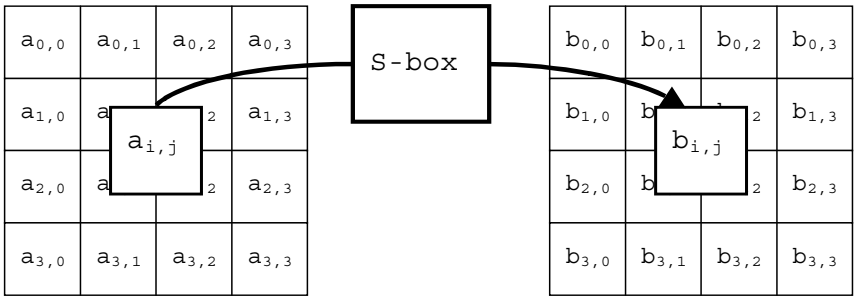
Rijndael-128 State and 128 Cipher Key

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

18

Byte Substitution



19

Rijndael S-box

Sbox[256] = {

```
 99,124,119,123,242,107,111,197, 48,  1,103, 43,254,215,171,118,
202,130,201,125,250, 89, 71,240,173,212,162,175,156,164,114,192,
183,253,147, 38, 54, 63,247,204, 52,165,229,241,113,216, 49, 21,
  4,199, 35,195, 24,150,  5,154,  7, 18,128,226,235, 39,178,117,
  9,131, 44, 26, 27,110, 90,160, 82, 59,214,179, 41,227, 47,132,
 83,209,  0,237, 32,252,177, 91,106,203,190, 57, 74, 76, 88,207,
208,239,170,251, 67, 77, 51,133, 69,249,  2,127, 80, 60,159,168,
 81,163, 64,143,146,157, 56,245,188,182,218, 33, 16,255,243,210,
 96,129, 79,220, 34, 42,144,136, 70,238,184, 20,222, 94, 11,219,
224, 50, 58, 10, 73,  6, 36, 92,194,211,172, 98,145,149,228,121,
231,200, 55,109,141,213, 78,169,108, 86,244,234,101,122,174,  8,
186,120, 37, 46, 28,166,180,198,232,221,116, 31, 75,189,139,138,
112, 62,181,102, 72,  3,246, 14, 97, 53, 87,185,134,193, 29,158,
225,248,152, 17,105,217,142,148,155, 30,135,233,206, 85, 40,223,
140,161,137, 13,191,230, 66,104, 65,153, 45, 15,176, 84,187, 22};
```

20

Rijndael S-box Design View

Galois field GF(2^8) with polynomial

$m(x) = x^8 + x^4 + x^3 + x + 1$

The Rijndael S-box is the composition $f \circ g$ where

$g(x) = x^{-1}$, $x \in GF(2^8)$, $x \neq 0$, and

$g(0) = 0$

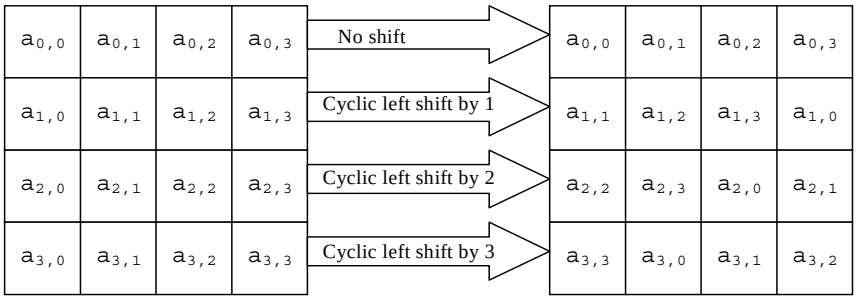
and f is the affine transformation defined by $y = f(x)$

Inv ($f \circ g$) = $g \circ$ (Inv f)

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

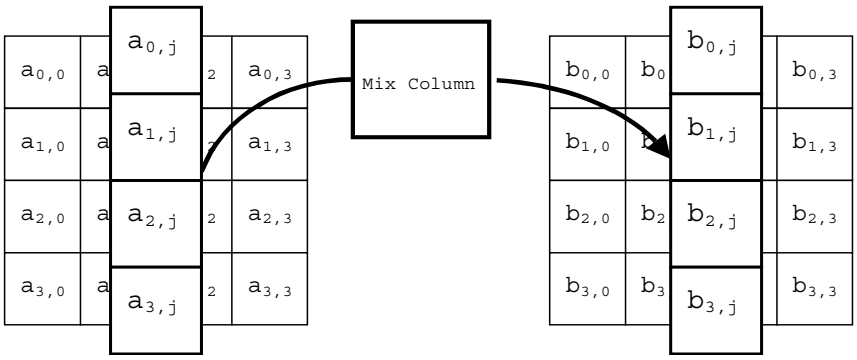
21

Shift Row



22

Mix Column



23

Mix Column - Implemented

The mix column transformation mixes one column of the state at a time.

Column j:

$$b_{0,j} = T_2(a_{0,j}) \oplus T_3(a_{1,j}) \oplus a_{2,j} \oplus a_{3,j}$$
$$b_{1,j} = a_{0,j} \oplus T_2(a_{1,j}) \oplus T_3(a_{2,j}) \oplus a_{3,j}$$
$$b_{2,j} = a_{0,j} \oplus a_{1,j} \oplus T_2(a_{2,j}) \oplus T_3(a_{3,j})$$
$$b_{3,j} = T_3(a_{0,j}) \oplus a_{1,j} \oplus a_{2,j} \oplus T_2(a_{3,j})$$

where:

$$T_2(a) = 2*a \quad \text{if } a < 128$$
$$T_2(a) = (2*a) \oplus 283 \quad \text{if } a \geq 128$$
$$T_3(a) = T_2(a) \oplus a.$$

24

Mix Column - Design view

The columns of the State are considered as polynomials over GF(2^8).

They are multiplied by a fixed polynomial c(x) given by

$$c(x) = \text{'03'}\ x^3 + \text{'01'}\ x^2 + \text{'01'}\ x + \text{'02'}$$

The product is reduced modulo $x^4 + \text{'01'}$.

Matrix form

$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix}$$

The Inverse Mix Column polynomial is $c(x)^{-1} \bmod (x^4 + \text{'01'}) = d(x)$ given by

$$d(x) = \text{'0B'}\ x^3 + \text{'0D'}\ x^2 + \text{'09'}\ x + \text{'0E'}$$

25

Round Key Addition

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

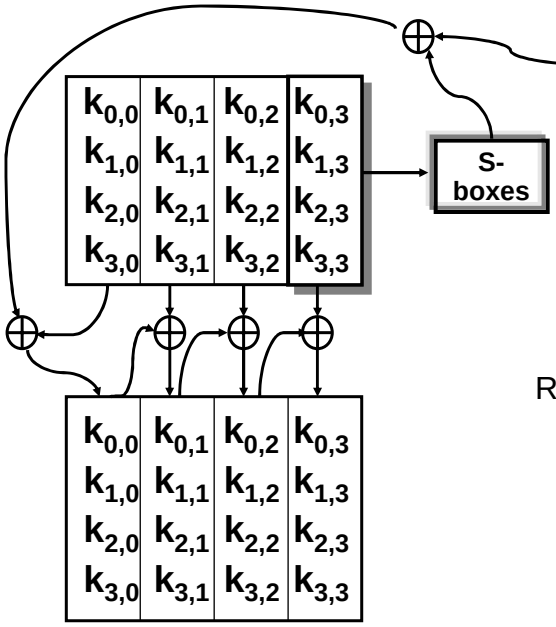
$\oplus$

$rk_{0,0}$	$rk_{0,1}$	$rk_{0,2}$	$rk_{0,3}$
$rk_{1,0}$	$rk_{1,1}$	$rk_{1,2}$	$rk_{1,3}$
$rk_{2,0}$	$rk_{2,1}$	$rk_{2,2}$	$rk_{2,3}$
$rk_{3,0}$	$rk_{3,1}$	$rk_{3,2}$	$rk_{3,3}$

=

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

26



Round Key Derivation

(128 bits)

27

The Security of AES

- Designed to be resistant against differential and linear cryptanalysis
  - S-boxes optimal
  - Wide Trail Strategy
- Has quite an amazing algebraic structure (see the next slide)
- Algebraic cryptanalysis tried but not yet (!) successful
- Algebraic cryptanalysis: given known plaintext – ciphertext pairs construct algebraic systems of equations, and try to solve them.

28

AES encryption

state $x^{(r)} = (x_{ij}^{(r)}), \quad i,j = 0,1,2,3, \quad r = 1,2,...,10, \quad x_{ij}^{(r)} \in GF(2^8)$

key $k^{(r)} = (k_{ij}^{(r)}), \quad i,j = 0,1,2,3, \quad r = 0,1,2,...,10, \quad k_{ij}^{(r)} \in GF(2^8)$

AES encryption:

$$x^{(1)} = p \oplus k^{(0)}$$

$$x^{(r+1)} = M(S(F(G(x^{(r)}))) \oplus k^{(r)}, \; r = 1,2,...,9$$

$$c = S(F(G(x^{(10)}))) \oplus k^{(10)}$$

where

M, S are linear functions over $GF(2^8)$

$G = (g)$ where $g : GF(2^8) \to GF(2^8), \; g(x) = x^{-1}, \; g(0) = 0$

$F = (f)$ where $f - \lambda_0$ is additive over $GF(2^8)$

29