A design of block cipher

周之恒、郭超年、周雷

zzhitter@gmail.com

Introduction

This cipher is also a special type of iterated cipher called a Feistel cipher.

This is a 8-round Feistel cipher having a block length of 32 bits and a key length of 32 bits.

Permutation

Prior to the 8 rounds of encryption, there is a fixed initial permutation IP that is applied to the plaintext. We denote

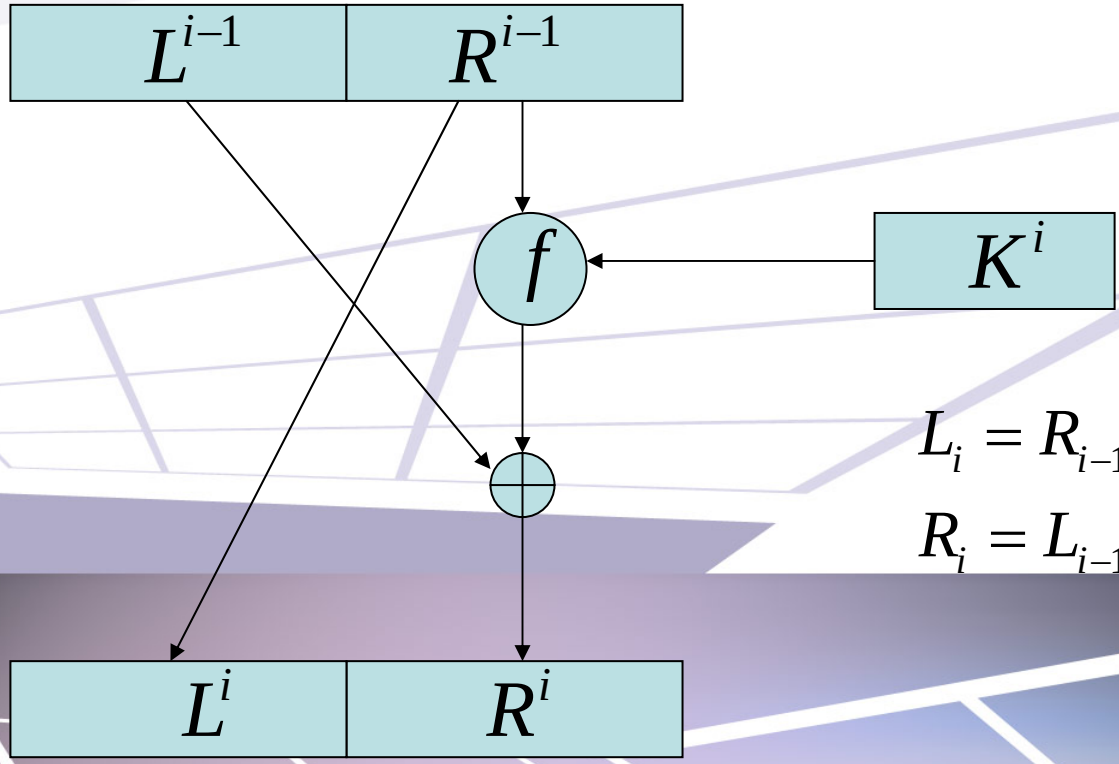
$$IP(x) = L^0 R^0$$

After the 8 rounds of encryption, the inverse permutation IP^{-1} is applied to the bitstring $R^8 L^8$, yielding the ciphertext y . That is,

$$y = IP^{-1}(R^8 L^8)$$

The structure of Feistel cipher

We use this strcuture to do both encryption and decryption.



$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

The structure of Feistel cipher

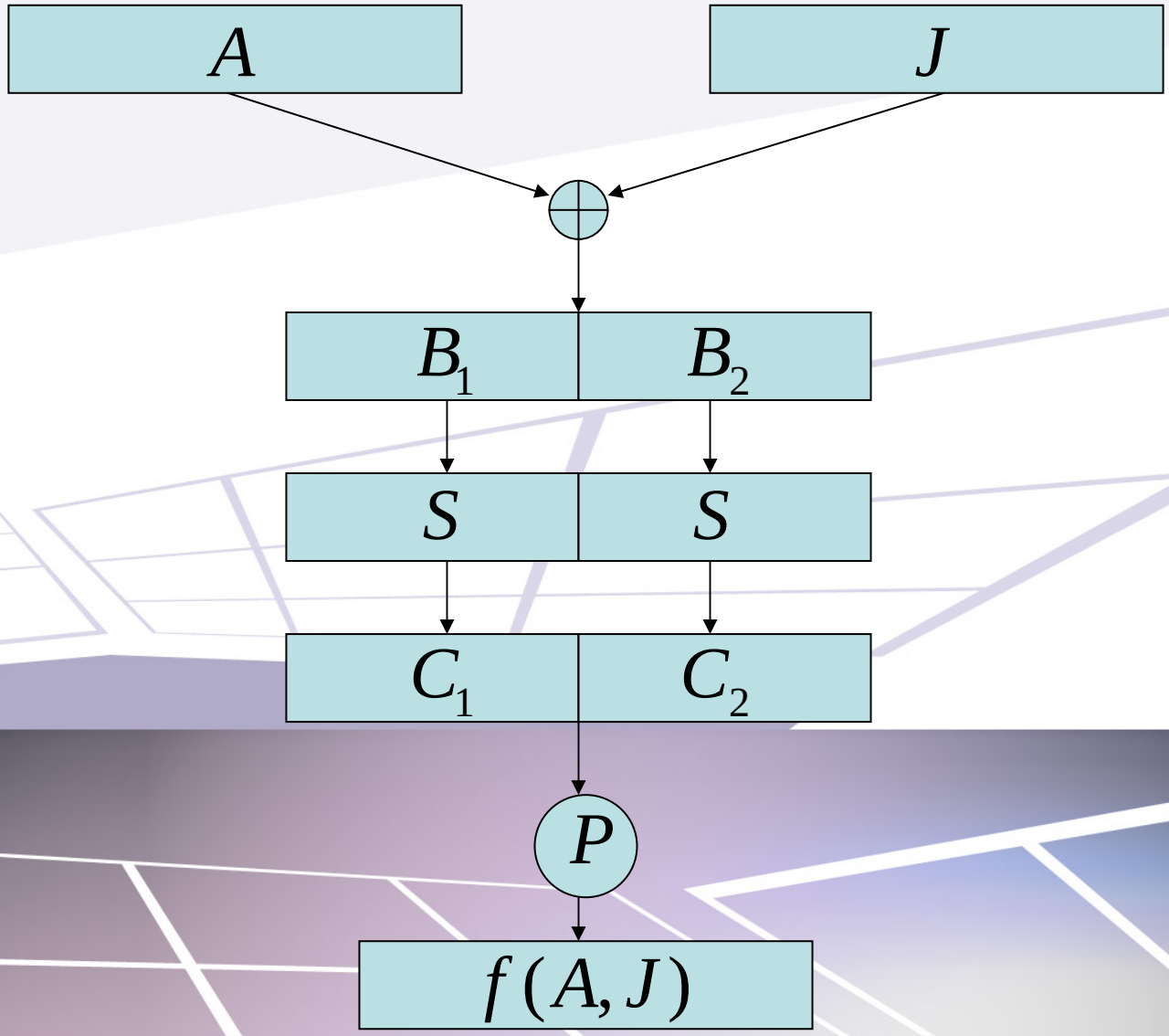
Each L^i and R^i is 16 bits in length. The function

$$f : \{0,1\}^{16} \times \{0,1\}^{16} \rightarrow \{0,1\}^{16}$$

Takes as input a 16-bit string and a round key.

The key schedule, $(K^1, K^2, ..., K^8)$, consists of 16-bit round keys that are derived from the 32-bit key.

The structure of f function



The S function

Since a number mod $2^n + 1$ is invertiable if n=1,2,4,8,16.(Fermat primes)

We can define the S function as follow:

$$c_i = az_i^{-1} + b(\mathrm{mod}\, 2^8 + 1)$$

in which z_i denotes the value of 8-bit string B_i

We define 0=256 to make sure “0” also have an inverse.

The S function

We can use the Low-high algorithm of IDEA to compute this S function.

$$az_i^{-1} + b(\mathrm{mod}\, 2^8 + 1) = (az_i^{-1} + b \bmod 2^8) - (az_i^{-1} + b\ div 2^8)$$

$$if\ \ (az_i^{-1} + b \bmod 2^8) \geq (az_i^{-1} + b\ div 2^8)$$

$$az_i^{-1} + b(\mathrm{mod}\, 2^8 + 1) = (az_i^{-1} + b \bmod 2^8)$$

$$-(az_i^{-1} + b\ div 2^8) + 2^8 + 1$$

$$if\ \ (az_i^{-1} + b \bmod 2^8) < (az_i^{-1} + b\ div 2^8)$$

Permutation

We define IP and IP^{-1} as follow:

IP

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

IP^{-1}

9	17	23	31
13	28	2	18
24	16	30	6
26	20	10	1
8	14	25	3
4	29	11	19
32	12	22	7
5	27	15	21

Permutation

And the permutation in f function is as follows:

$$P$$

9	5	3	2
13	7	4	14
11	6	15	8
16	12	10	1

key schedule

Just simply derive 8 round keys by shifting the 32-bit key.

K_1 : 1~16 bits K_2 : 5~20 bits

K_3 : 9~24 bits K_4 : 13~28 bits

K_5 : 17~32 bits K_6 : 21~32 and 1~4 bits

K_7 : 25~32 and 1~8 bits

K_8 : 29~32 and 1~12 bits

More thinking

1. Is 8 rounds of iteration enough?

2. How to choose “a” and “b” for S function?

   Use different “b” in different round?

3. Divide $R_{i-1} \oplus K_i$ to 2 groups of 8 bits, or just use 1 group of 16 bits, as we know that $2^{16}+1$ is also a prime.

Thank you!