Practical Constructions of Pseudorandom Permutations (Block Ciphers)

Yu Zhang

Harbin Institute of Technology

Cryptography, Autumn, 2022

Outline

1 Substitution-Permutation Networks

2 Feistel Networks

3 DES – The Data Encryption Standard

4 Increasing the Key Length of a Block Cipher

5 AES – The Advanced Encryption Standard

6 Differential and Linear Cryptanalysis – A Brief Look

Content

1 Substitution-Permutation Networks

2 Feistel Networks

3 DES – The Data Encryption Standard

4 Increasing the Key Length of a Block Cipher

5 AES – The Advanced Encryption Standard

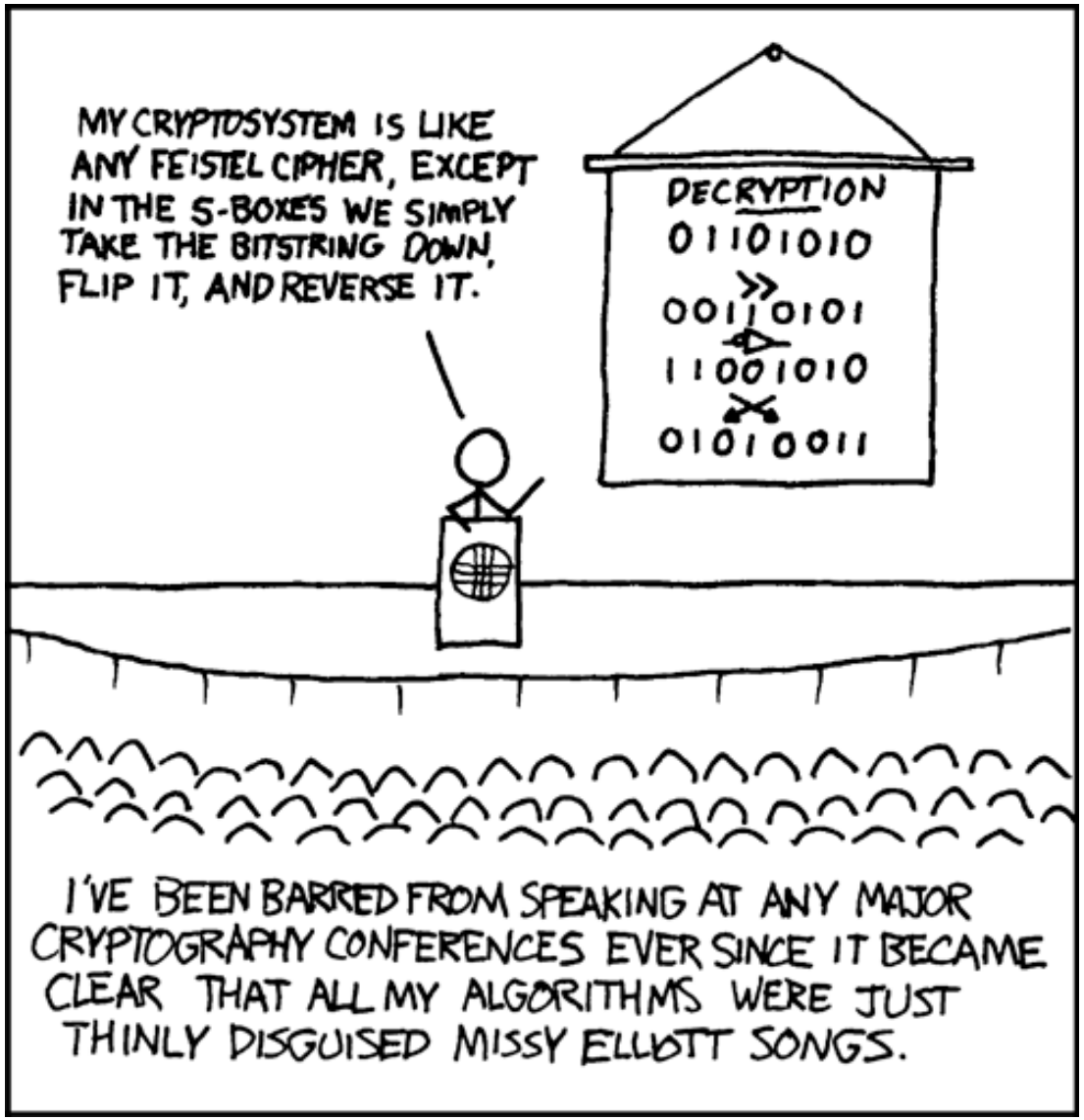
6 Differential and Linear Cryptanalysis – A Brief Look

Block Ciphers

- **Block Cipher** $F : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$.
  $F_k : \{0,1\}^\ell \to \{0,1\}^\ell$, $F_k(x) \stackrel{\text{def}}{=} F(k,x)$.
  n is key length, ℓ is block length.
- Constructions are **heuristic**, not proofed.
- Considered as **PRP** in practice, not encryption scheme.
  - In the call for proposals for AES: *The extent to which the algorithm output is indistinguishable from a random permutation on the input block.*
- Is "**good**" if the best known attack has time complexity roughly **equivalent to a brute-force search for the key**.
  - A cipher with $n = 112$ which can be broken in time 2^{56} is insecure.
  - In a non-asymptotic setting, $2^{n/2}$ may be insecure.

Comics On Blockcipher [xkcd:153]

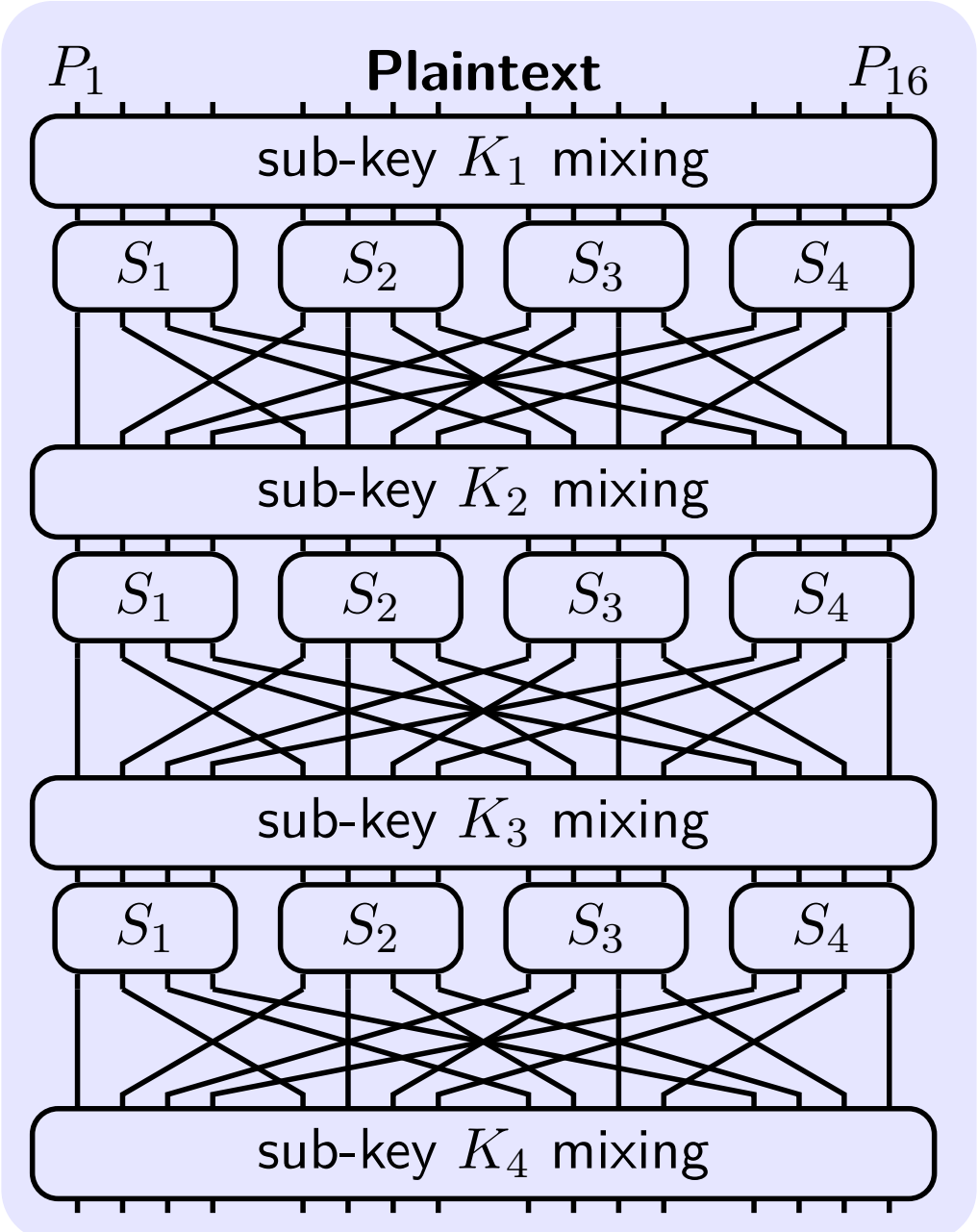
My cryptosystem is like any Feistel cipher, except in the S-Boxes we simply take the bitstring down, flip it, and reverse it.



The Confusion-Diffusion Paradigm

- **Goal**: Construct *concise* random-looking permutations.
  - Q: a block length of n bits require ____ bits for its representation.
- **Confusion**: making the relationship between the key and the ciphertext as complex and involved as possible.
  Construct a large random-looking permutation F from smaller random permutations f_i. $F_k(x) = f_1(x_1)f_2(x_2)\cdots f_i(x_i)$
- **Diffusion**: the redundancy in the statistics of the plaintext is dissipated in the statistics of the ciphertext.
- **Product cipher** combines multiple transformations.

A Substitution-Permutation Network



Design Principle 1 – Invertibility of The S-boxes

S-boxes must be invertible, otherwise the block cipher will not be a permutation.

Proposition 1

Let F be a keyed function defined by a SPN in which the S-boxes are all one-to-one and onto. The regardless of the key schedule and the number of rounds, F_k is a permutation for any choice of k.

Design Principle 2 – The Avalanche Effect

- **Avalanche effect**: changing a single bit of the input affects every bit of the output.
- **Strict avalanche criterion**: a single input bit is complemented, each of the output bits changes with a 50% probability.
- **Bit independence criterion**: output bits j and k should change independently when any single input bit i is inverted, for all i, j and k.
- S-box: changing a single bit of the input changes at least two bits in the output.
- P-box: the output bits of any given S-box are spread into different S-boxes in the next round.
- Q: For 4-bit S-boxes, changing 1 bit of the input affects ____ bits of the output after R rounds of SPN.

A Framework for KPA against Block Ciphers

KPA: know some plaintext/ciphertext pairs under the same key.

1. Observe relationship between PT/CT and k bits of the key.
2. Design a test on t bits based on the above relationship.
3. Search in k-bit space; a guess passes test with pr. 2^{-t}.
4. Use p PT/CT pairs to determine the key with exp. $2^{k-(p)t}$.

KPA against 1-round w/o final key-mixing w/ 16-bit key

Relationship PT $\oplus$ Key $\oplus$ Input-of-S-boxes $= 0$.

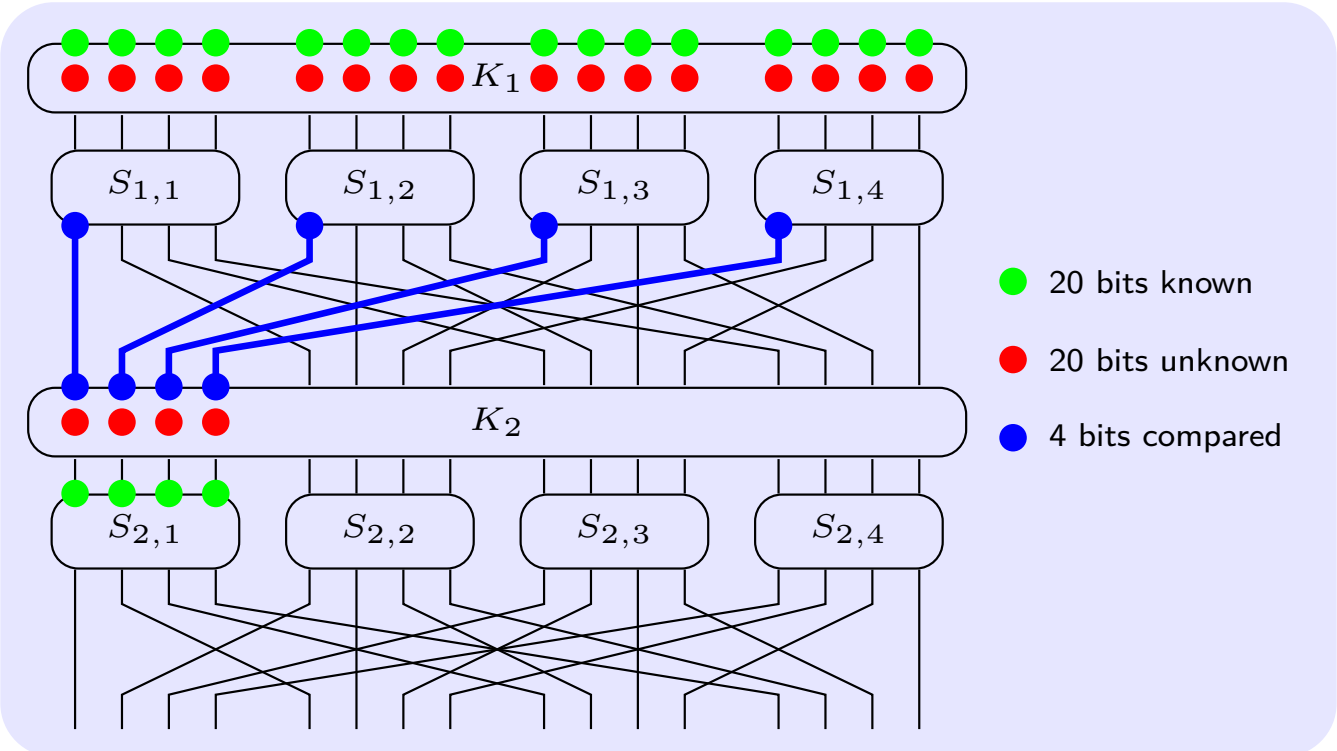
Test on $t = 16$ bits: Input-of-S-boxes $=$ PT $\oplus$ Key.

Search in $k = 16$ bit space; passing test with pr. $1/2^{16}$.

Determine the key with $p = 1$ PT/CT pair and exp. 1.

Attacks on Reduced-Round SPNs (Homework)

Attack on a 1-round SPN: 64-bit block, 128-bit key ($2 \times$ 64-bit sub-keys), $16 \times$ 4-bit S-boxes.



- Guessing 20 bits: 16 bits of the 1st sub-key, 4 bits of the 2nd.
- Guess passes the 4-bit test with pr. $1/2^4$ ($1/2^n$ for n-bit test).
- Use 8 I/O pairs to determine the key (with exp. $2^{20-4\times 8}$).
- Break with complexity $8 \cdot 2^{20} \cdot 16 = 2^{27} \ll 2^{128}$ (16 S-boxes).

Content

1 Substitution-Permutation Networks

2 Feistel Networks

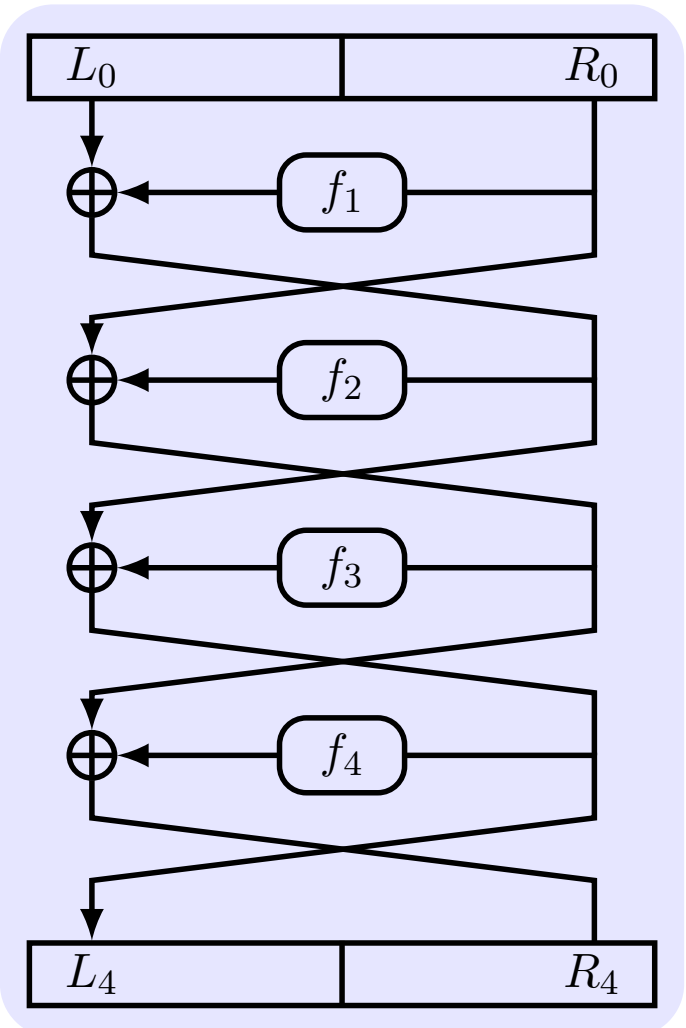
3 DES – The Data Encryption Standard

4 Increasing the Key Length of a Block Cipher

5 AES – The Advanced Encryption Standard

6 Differential and Linear Cryptanalysis – A Brief Look

Feistel Networks



- **Idea**: Construct an invertible function from non-invertible components.
- $L_i := R_{i-1}$ and $R_i := L_{i-1} \oplus f_i(R_{i-1})$
- **Inverting**: $L_{i-1} := ?$
- **Decryption**: Operate with sub-keys in reverse order.

Proposition 2

Luby-Rackoff Theorem: *Regardless of the mangler functions* $\{\hat{f}_i\}$ *and the number of rounds,* F_k *is a permutation for any choice of* k*.*

Examples

What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

(a) Each round function F outputs all 0s, regardless of the input.
(b) Each round function F is the identity function.

Content

1 Substitution-Permutation Networks

2 Feistel Networks

3 **DES – The Data Encryption Standard**

4 Increasing the Key Length of a Block Cipher

5 AES – The Advanced Encryption Standard

6 Differential and Linear Cryptanalysis – A Brief Look

The Design of DES

- 16-round Feistel network.
- 64-bit block
- 56-bit key, 48-bit sub-key. (64bit key with 8 check bits)
- Key schedule: 56 bits $\xrightarrow[\text{left rotation, PC}]{\text{divided into two halves}}$ 48 bits.
- Begin with Initial Permutation (IP) and end with IP^{-1}.
- Round function f is non-invertible with 32-bit I/O.
- f_i is determined by mangler function $\hat{f}_i$ and sub-key k_i.
- S-box is a 4-to-1 function, mapping 6-bit to 4-bit.

Overview of DES

Algorithm 1: DES

input : key k, message m

output: ciphertext c

$(k_1, \ldots, k_{16}) \leftarrow KeySchedule(k)$

$m \leftarrow IP(m)$

Parse m as $L_0 \| R_0$

for $r = 1$ **to** *16* **do**

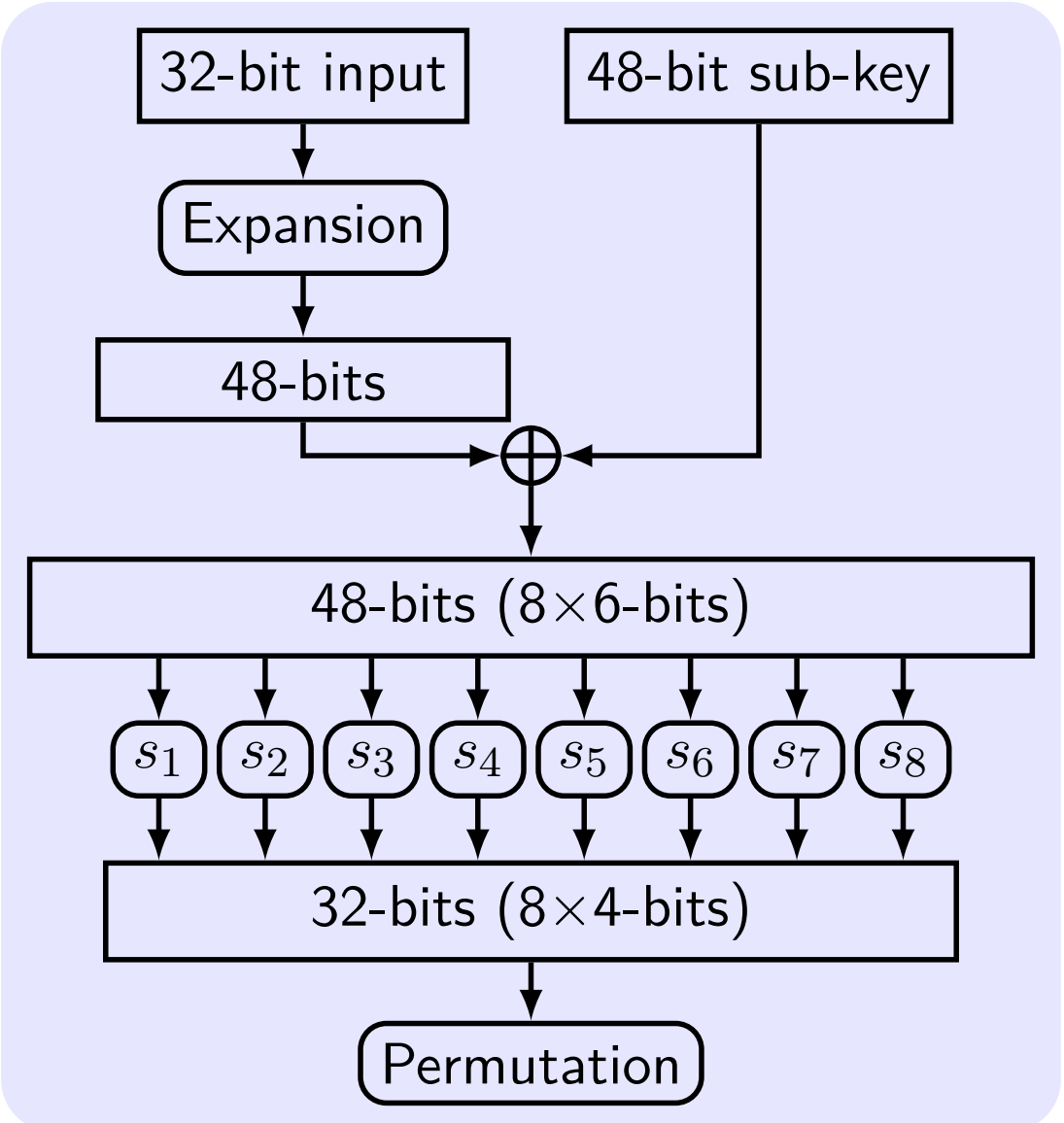
  $L_r \leftarrow R_{r-1}$

  $R_r \leftarrow f(k_r, R_{r-1}) \oplus L_{r-1}$

$c \leftarrow IP^{-1}(L_{16} \| R_{16})$

return c

The DES Mangler Function



An S-box in DES

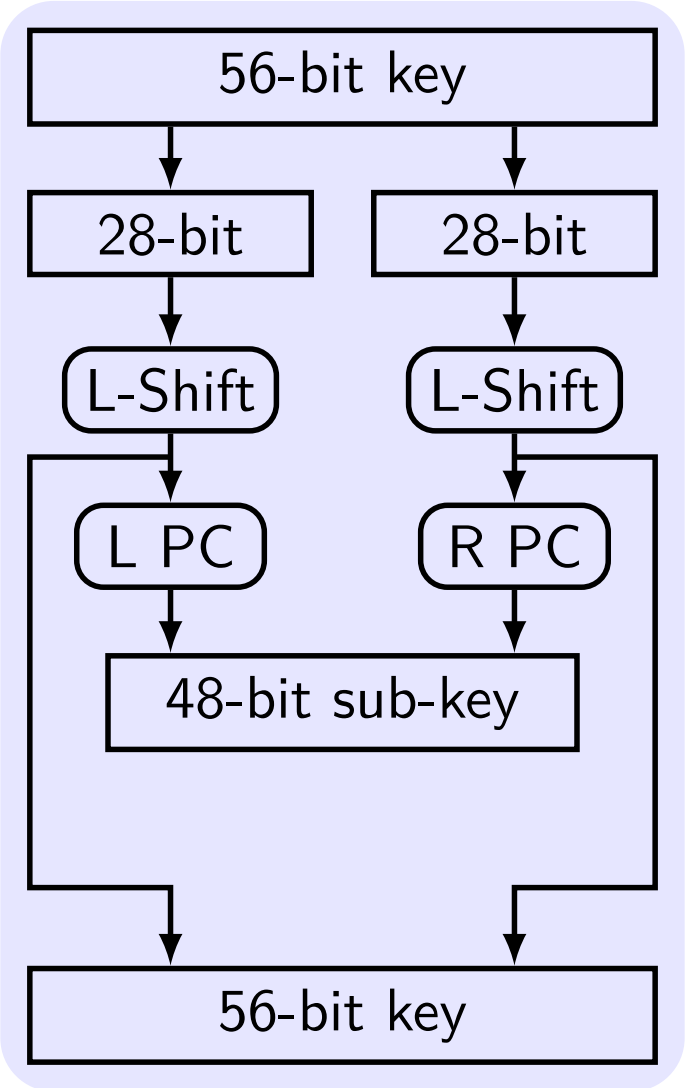
An S-box

Input: $b_{0,1,\ldots,5} = 011001$

Output: $S[b_{0,5}][b_{1,2,3,4}] = S[01][1100] = S[1][12] = 9 = 1001$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Key Schedule



Bits of shift is 1 or 2 in different rounds.

Weak Keys of DES

- **Weak keys**: makes the cipher behave in some undesirable way–producing *identical* sub-keys.

Weak keys (Key with check bits : key w/o check bits)

```
01010101 01010101   :   0000000 0000000
FEFEFEFE FEFEFEFE   :   FFFFFFF FFFFFFF
E0E0E0E0 F1F1F1F1   :   FFFFFFF 0000000
1F1F1F1F 0E0E0E0E   :   0000000 FFFFFFF
```

- **Semi-weak keys**: producing only two different sub-keys. A pair of semi-weak keys k_1, k_2: $F_{k_1}(F_{k_2}(M)) = M$.

Semi-weak key pairs (2 of total 6 pairs)

```
011F011F 010E010E   &   1F011F01 0E010E01
01E001E0 01F101F1   &   E001E001 F101F101
```

Chronology of DES

1973 NBS (NIST) publishes a call for a standard.

1974 DES is published in the Federal Register.

1977 DES is published as FIPS PUB 46.

1990 Differential cryptanalysis with CPA of 2^{47} plaintexts.

1997 DESCHALL Project breaks DES in public.

1998 EFF's Deep Crack breaks DES in 56hr at $250,000.

1999 Triple DES.

2001 AES is published in FIPS PUB 197.

2004 FIPS PUB 46-3 is withdrawn.

2006 COPACOBANA breaks DES in 9 days at $10,000.

2008 RIVYERA breaks DES within one day.

Content

1 Substitution-Permutation Networks

2 Feistel Networks

3 DES – The Data Encryption Standard

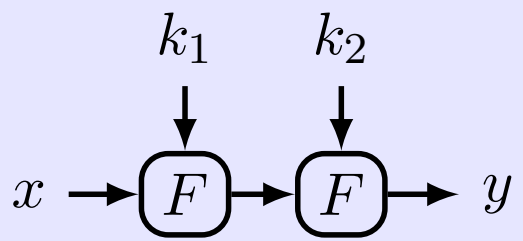
4 **Increasing the Key Length of a Block Cipher**

5 AES – The Advanced Encryption Standard

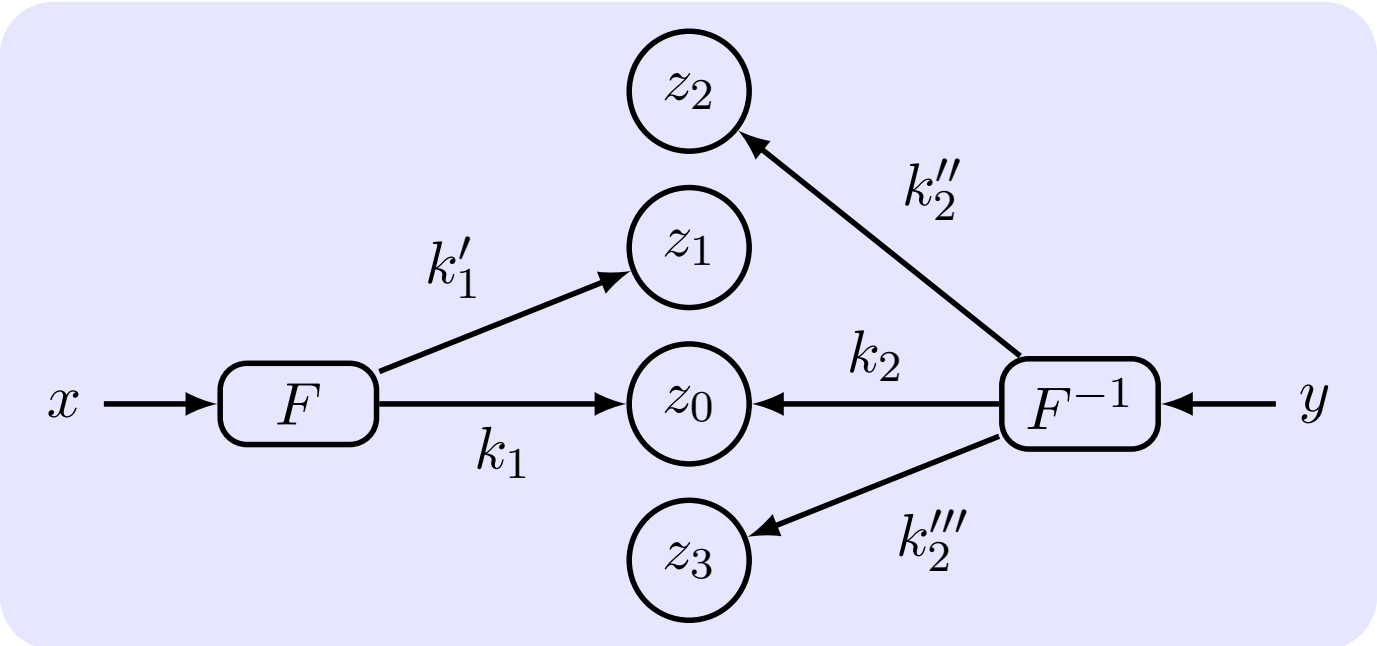
6 Differential and Linear Cryptanalysis – A Brief Look

Double Encryption

- **Internal tampering vs. Black-box constructions**: by modifying DES – in even the smallest way – we lose the confidence we have gained in DES.
- **Double encryption**: $y = F'_{k_1,k_2}(x) \stackrel{\text{def}}{=} F_{k_2}(F_{k_1}(x))$.

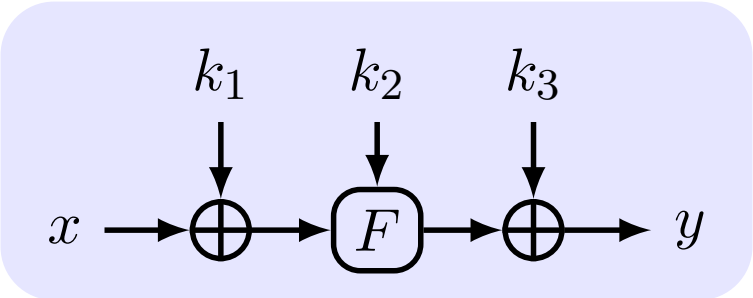


The Meet-In-the-Middle Attack



- $z_0 = F_{k_1}(x) = F_{k_2}^{-1}(y) \iff y = F'_{k_1,k_2}(x)$.
- Key pair (k_1, k_2) satisfies the equation with probability 2^{-n}.
- The number of such key pairs is $2^{2n}/2^n = 2^n$.
- With another two I/O pairs, the expected number of key pairs is $2^n/2^{2n} = 2^{-n}$. So that is it!
- $\mathcal{O}(2^n)$ time and $\mathcal{O}(2^n)$ space.

DESX



Whitening: XORing Input/Output with partial keys.
DESX:

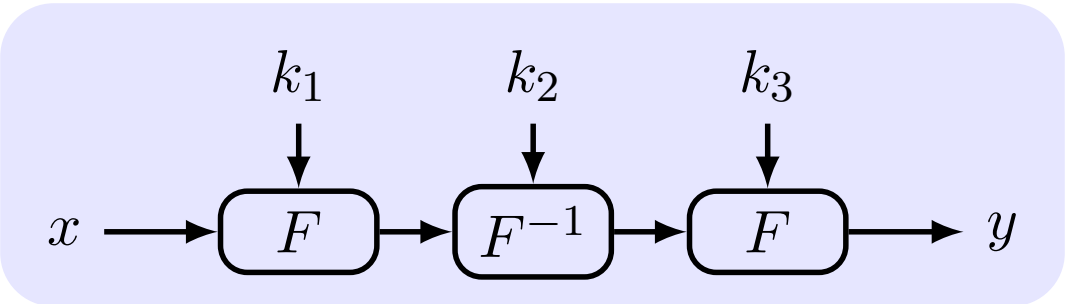
$$k = (k_1, k_2, k_3), |k_1| = |k_3| = 64, |k_2| = 56$$

$$y = k_3 \oplus F_{k_2}(x \oplus k_1)$$

$$x = k_1 \oplus F_{k_2}^{-1}(y \oplus k_3)$$

Security: $|k| = 184$, but break in time 2^{64+56}.

Triple Encryption



- $k_1 = k_2 = k_3$: a single F with backward compatibility.
- $k_1 \neq k_2 \neq k_3$: time 2^{2n} under the meet-in-the-middle attack.
- $k_1 = k_3 \neq k_2$: time 2^{2n} with 1 I/O pair; time 2^n with 2^n pair.
- **Triple-DES** (3DES): strong, but small block length and slow.

Content

1 Substitution-Permutation Networks

2 Feistel Networks

3 DES – The Data Encryption Standard

4 Increasing the Key Length of a Block Cipher

5 AES – The Advanced Encryption Standard

6 Differential and Linear Cryptanalysis – A Brief Look

AES – The Advanced Encryption Standard

- In 1997, NIST calls for AES.
- In 2001, Rijndael [J. Daemen & V. Rijmen] becomes AES.
- The first publicly accessible cipher for top secret information.
- Not only security, also efficiency and flexibility, etc.
- 128-bit block length and 128-, 192-, or 256-bit keys.
- Not a Feistel structure, but a SPN.
- Only non-trivial attacks are for reduced-round variants.
  - 2^{27} on 6-round of 10-round for 128-bit keys.
  - 2^{188} on 8-round of 12-round for 192-bit keys.
  - 2^{204} on 8-round of 14-round for 256-bit keys.

Overview of AES

Algorithm 2: AES

input : key k, message m

output: ciphertext c

$(k_1, \ldots, k_{10}) \leftarrow Expand(k)$

$s \leftarrow m \oplus k_0$

for $r = 1$ **to** *10* **do**

  $s \leftarrow SubBytes(s)$

  $s \leftarrow ShiftRows(s)$

  if $r \leq 9$ **then** $s \leftarrow MixColumns(s)$

  $s \leftarrow s \oplus k_R$

return $c \leftarrow s$

See ▸ an animation of Rijndael!

SM4

- ShangMi 4 (SM4): a block cipher "Information security technology—SM4 block cipher algorthm", used in the Chinese National Standard for Wireless LAN WAPI and also used with TLS
- Mainly developed by Lv Shuwang
- Declassified in 2006, published by State Cryptography Administration in 2012, and became a national standard (GB/T 32907-2016) in 2016
- SM1 (in-chip) and SM7 (lightweight) are also block ciphers, but are not published.

Content

1 Substitution-Permutation Networks

2 Feistel Networks

3 DES – The Data Encryption Standard

4 Increasing the Key Length of a Block Cipher

5 AES – The Advanced Encryption Standard

6 Differential and Linear Cryptanalysis – A Brief Look

Linear Cryptanalysis

Reference: "A Tutorial on Linear and Differential Cryptanalysis"
`www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf`

- Linear relationships between the input and output: the bit positions $i_1, ..., i_\ell$ and $i'_1, ..., i'_\ell$ have **bias** p if for randomly-chosen input x and key k, it holds that $y = F_k(x)$,

$$\Pr[x_{i_1} \oplus \cdots \oplus x_{i_\ell} \oplus y_{i'_1} \oplus \cdots \oplus y_{i'_\ell} = 0] = p + \frac{1}{2}.$$

- Not require CPA, KPA are sufficient.
- Attack steps:
  1. Construct the linear approximation table of S-boxes.
  2. Construct a linear approximation of the first $r - 1$ rounds with a big bias.
  3. Extracting sub-key bits of last round that satisfies the linear approximation well.

An Example of Linear Analysis of S-box

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

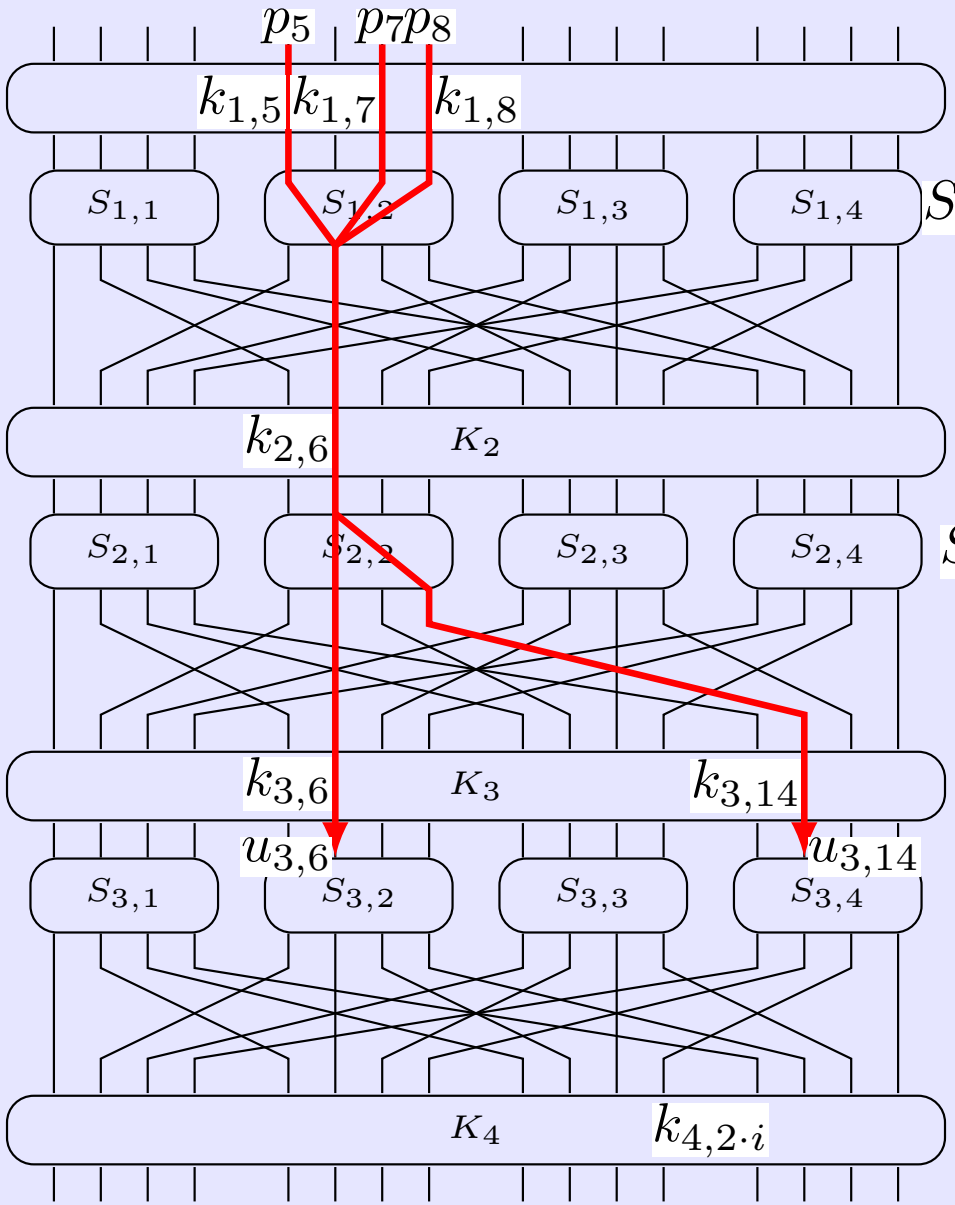
An Example of Linear Distribution Table

Input Sum	Output Sum 0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	–2	–2	0	0	–2	+6	+2	+2	0	0	+2	+2	0	0
2	0	0	–2	–2	0	0	–2	–2	0	0	+2	+2	0	0	–6	+2
3	0	0	0	0	0	0	0	0	+2	–6	–2	–2	+2	+2	–2	–2
4	0	+2	0	–2	–2	–4	–2	0	0	–2	0	+2	+2	–4	+2	0
5	0	–2	–2	0	–2	0	+4	+2	–2	0	–4	+2	0	–2	–2	0
6	0	+2	–2	+4	+2	0	0	+2	0	–2	+2	+4	–2	0	0	–2
7	0	–2	0	+2	+2	–4	+2	0	–2	0	+2	0	+4	+2	0	+2
8	0	0	0	0	0	0	0	0	–2	+2	+2	–2	+2	–2	–2	–6
9	0	0	–2	–2	0	0	–2	–2	–4	0	–2	+2	0	+4	+2	–2
A	0	+4	–2	+2	–4	0	+2	–2	+2	+2	0	0	+2	+2	0	0
B	0	+4	0	–4	+4	0	+4	0	0	0	0	0	0	0	0	0
C	0	–2	+4	–2	–2	0	+2	0	+2	0	+2	+4	0	+2	0	–2
D	0	+2	+2	0	–2	+4	0	+2	–4	–2	+2	0	+2	0	0	+2
E	0	+2	+2	0	–2	–4	0	+2	–2	0	0	–2	–4	+2	–2	0
F	0	–2	–4	–2	–2	0	+2	0	0	–2	+4	–2	–2	0	+2	0

$x_2 \oplus x_3 = y_1 \oplus y_3 \oplus y_4$ for 12 times, the bias is $12 - 8 = 4$ times

$x_2 \oplus x_3 : 0110 = 6, \quad y_1 \oplus y_3 \oplus y_4 : 1011 = B$, so $(6, B) = 4$

An Example of Linear Cryptanalysis



$S_{1,2}$: $x_1 \oplus x_3 \oplus x_4 = y_2$

$S_{2,2}$: $x_2 = y_2 \oplus y_4$

$u_{3,6} \oplus u_{3,14} \oplus$

$p_5 \oplus p_7 \oplus p_8 = 0$

Guess $k_{4,2\cdot i}$

Differential Cryptanalysis

- Specific differences Δ_x in the input that lead to specific differences Δ_y in the output with probability $p \gg 2^{-n}$.
- $x_1 \oplus x_2 = \Delta_x$, $F_k(x_1) \oplus F_k(x_2) = \Delta_y$ with probability p.
- This can be exploited by CPA.
- Attack steps:
  1. Construct the difference distribution table of S-boxes.
  2. Construct a differential characteristics of the first $r-1$ rounds with a big bias.
  3. Extracting sub-key bits of last round that satisfies the differential characteristics well.

An Example of Differential Analysis of S-box

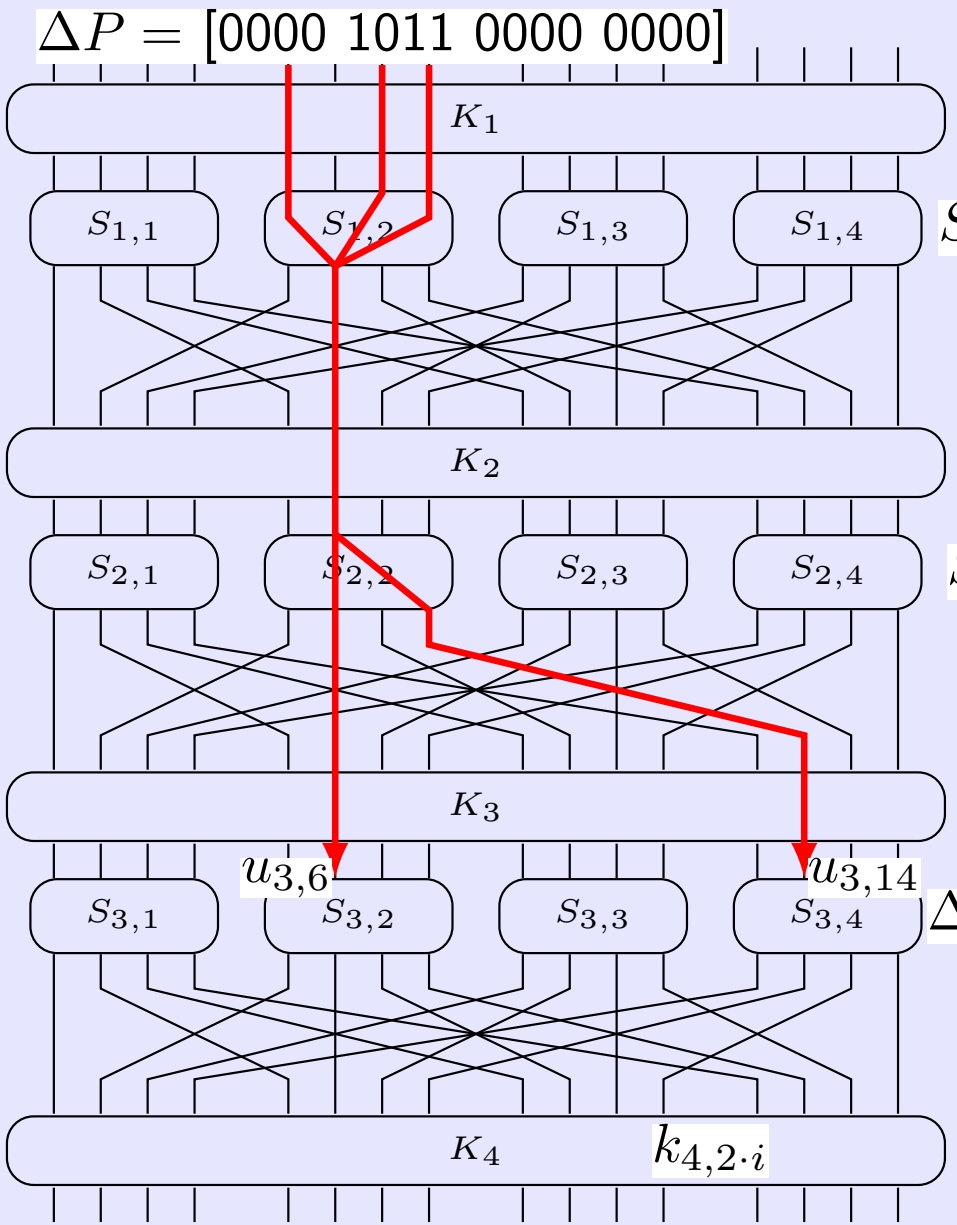
X	Y	ΔY		
		$\Delta X = 1011$	$\Delta X = 1000$	$\Delta X = 0100$
0000	1110	0010	1101	1100
0001	0100	0010	1110	1011
0010	1101	0111	0101	0110
0011	0001	0010	1011	1001
0100	0010	0101	0111	1100
0101	1111	1111	0110	1011
0110	1011	0010	1011	0110
0111	1000	1101	1111	1001
1000	0011	0010	1101	0110
1001	1010	0111	1110	0011
1010	0110	0010	0101	0110
1011	1100	0010	1011	1011
1100	0101	1101	0111	0110
1101	1001	0010	0110	0011
1110	0000	1111	1011	0110
1111	0111	0101	1111	1011

An Example of Differential Distribution Table

Input Difference	Output Difference 0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

$\Delta X = 1011 = B, \Delta Y = 0010 = 2$ for 8 times, so $(B, 2) = 8$

An Example of Differential Cryptanalysis



$S_{1,2}$: $\Delta X = B \rightarrow \Delta Y = 4$

$S_{2,2}$: $\Delta X = 4 \rightarrow \Delta Y = 5$

$\Delta U = [0000\ 0100\ 0000\ 0100]$

Guess $k_{4,2\cdot i}$

Remarks on Block Ciphers

- **Block length** should be sufficiently large
- **Message tampering** is not with message confidentiality
- **Padding**: TLS: For $n > 0$, n byte pad is $n, n, \ldots, n$ If no pad needed, add a dummy block
- **Stream ciphers vs. block ciphers**:
  - Steam ciphers are faster but have lower security
  - It is possible to use block ciphers in "stream-cipher mode"

Performance: Crypto++ 5.6, AMD Opetron 2.2GHz

	Block/key size	Speed MB/sec
RC4		126
Salsa20/12		643
Sosemanuk		727
3DES	64/168	13
AES-128	128/128	109

Summary

- Goal: Block cipher is PRP
- Constructions: confusion & diffusion, SPN, Feistel network, avalanche effect.
- Standards: DES, 3DES, AES
- Cryptanalysis: reduced round, meet-in-the-middle, differential and linear cryptanalysis.