

Practical Constructions of Pseudorandom Permutations (Block Ciphers)

Yu Zhang

HIT/CST/NIS

Cryptography, Spring, 2012

- 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**

- 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

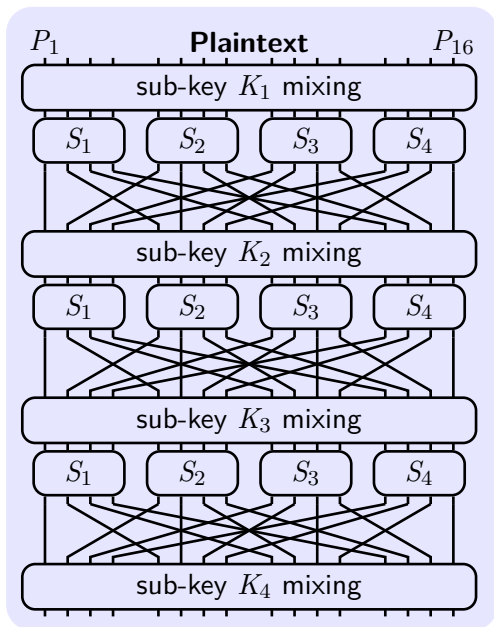
- **Block Cipher** $F : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$.
 $F_k : \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$, $F_k(x) \stackrel{\text{def}}{=} F(k, x)$.
 n is key length, ℓ is block length.
- Constructions are **heuristic**, not proofed.
- Considered as **PRP in practice**.
 - 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.

The Confusion-Diffusion Paradigm

- **Goal:** Construct *concise*¹ random-looking permutations.
- **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.

¹A block length of n bits would require $\log(2^n!) \approx n \cdot 2^n$ bits for its representation.

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. Then 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.

For 4-bit S -boxes, changing 1 bit of the input affects 2^R 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 SPN with 16-bit key

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

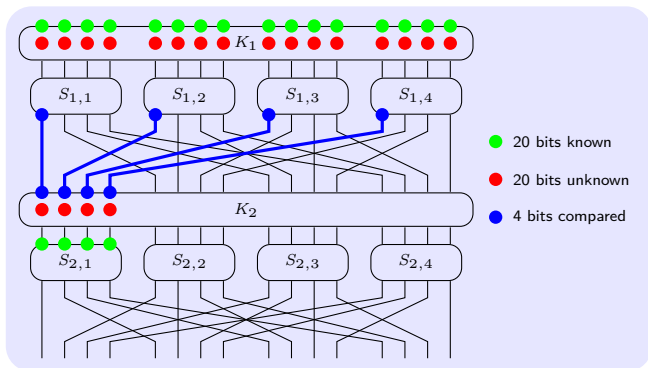
Test on $t = 16$ bits: $\text{Input-of-}S\text{-boxes} = \text{PT} \oplus \text{Key}$.

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

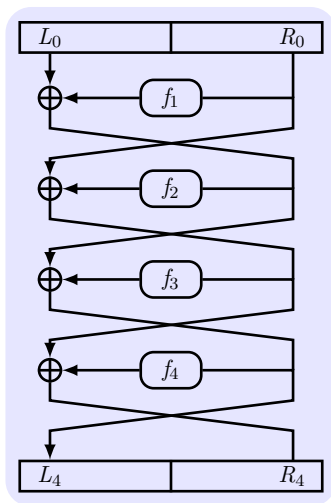
Attack on a 2-round SPN: 64-bit block, 128-bit key (2×64 -bit sub-keys), 16×4 -bit S -boxes, and mixing with XOR.



- 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).

- 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



Properties of Feistel Networks

- **Idea:** Construct an invertible function from non-invertible components.
- **Round function** $f_i(R) \stackrel{\text{def}}{=} \hat{f}_i(k_i, R)$ (\hat{f}_i mangler function).
- **Output:** $L_i := R_{i-1}$ and $R_i := L_{i-1} \oplus f_i(R_{i-1})$.
- **Inverting:** $L_{i-1} := R_i \oplus f_i(R_{i-1}) = R_i \oplus f_i(L_i)$.
- **Decryption:** Operate with sub-keys in reverse order.

Proposition 2

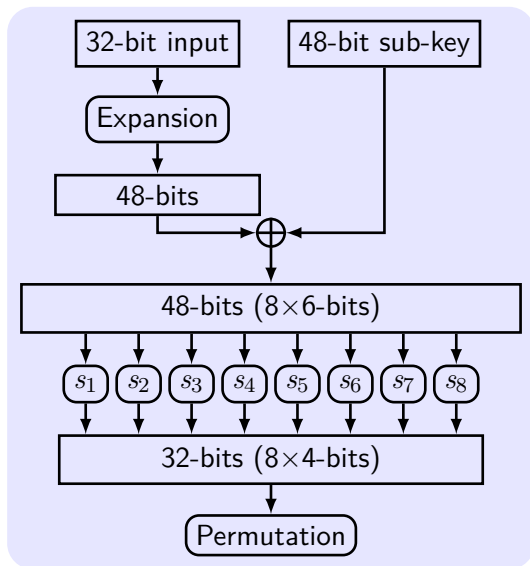
Luby-Rackoff Theorem: Let F be a keyed function defined by a Feistel network. Then regardless of the mangler functions $\{\hat{f}_i\}$ and the number of rounds, F_k is a permutation for any choice of k .

- 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.

The DES Mangler Function



An S -box in DES

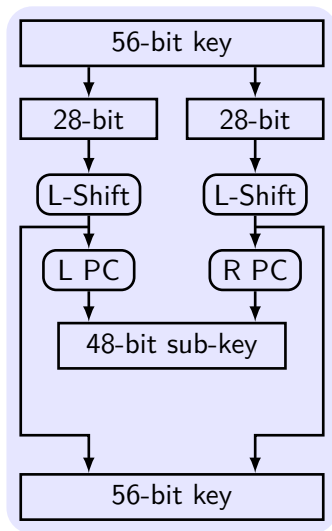
An S -box

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

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	:	00000000	00000000
FEFEFEFE	FEFEFEFE	:	FFFFFFF	FFFFFFF
E0E0E0E0	F1F1F1F1	:	FFFFFFF	00000000
1F1F1F1F	0E0E0E0E	:	00000000	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

Attacks on Reduced-Round Variants of DES

1-round (48-bit key):

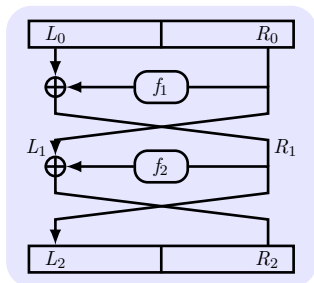
S -box is 4-to-1, so 4 possible values for each 6-bit key.

of possible keys: $4^{48/6} = 2^{16}$.

So a guess passes test with pr. $2^{-(48-16)}$.

Use another I/O pair to determine the key (with exp. 2^{-16}).

2-round: $L_0 || R_0, L_2 || R_2$ are known I/O pair.



$$L_1 = R_0$$

$$R_1 = L_0 \oplus f_1(R_0)$$

$$L_2 = R_1 = L_0 \oplus f_1(R_0)$$

$$R_2 = L_1 \oplus f_2(R_1).$$

$$f_1(R_0) = L_0 \oplus L_2$$

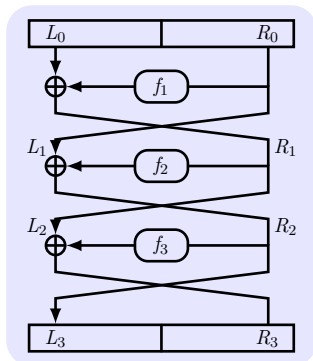
$$f_2(L_2) = R_2 \oplus R_0$$

So we know I/O pairs of both f_1 and f_2 .

Break in time $2 \cdot 2^{16}$ as two 1-round with two I/O pairs.

Attacks on Reduced-Round Variants of DES (Cont.)

3-round:



Without I/O pairs of any f , we know the inputs of f_1 and f_3 and the XOR of their outputs

$$(L_0 \oplus L_2) \oplus (L_2 \oplus R_3) = L_0 \oplus R_3.$$

Idea: The left/right half of the key affects the inputs only to the first/last four S -boxes. Brute-force needs $2 \cdot 2^{28}$.

- Check 16-bit XOR of outputs of four S -boxes on one half.
- $2^{28}/2^{16} = 2^{12}$ guesses on half-key pass check (with pr. 2^{-16}).
- Use another I/O pair to test 2^{12+12} keys (with exp. $2^{24-16 \times 2}$).
- Totally, $2 \cdot 2^{28} + 2^{24} < 2^{30}$ time and $2 \cdot 2^{12}$ space.

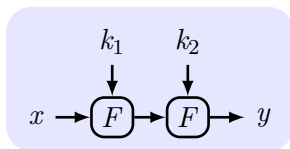
Chronology of DES

- 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.

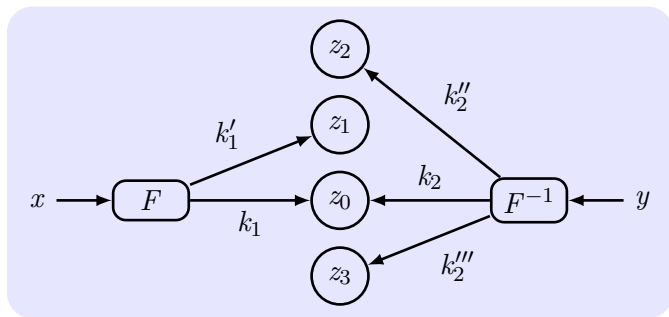
- 1 Substitution-Permutation Networks
- 2 Feistel Networks
- 3 DES – The Data Encryption Standard
- 4 Increasing the Key Length of a Block Cipher**
- 5 AES – The Advanced Encryption Standard
- 6 Differential and Linear Cryptanalysis – A Brief Look

Double Encryption

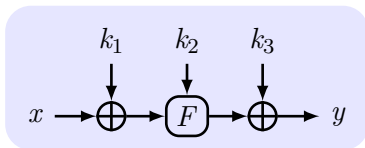
- **Internal tampering vs. Black-box constructions:** by modifying DES – in even the smallest way – we lose the confidence we have gained in DES.
- **Double encryption:** $y = F'_{k_1, k_2}(x) \stackrel{\text{def}}{=} F_{k_2}(F_{k_1}(x))$.



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.



Whitening: XORing Input/Output with partial keys.

DESX:

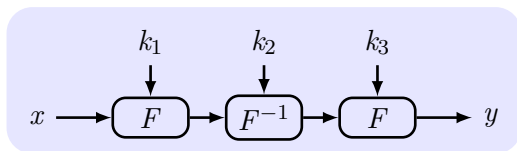
$$k = (k_1, k_2, k_3), |k_1| = |k_3| = 64, |k_2| = 56$$

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

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

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.

- 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.

The AES Construction

State: 4-by-4 array of bytes. The initial state is the plaintext.

- 1 AddRoundKey:** state XORed with the 128-bit sub-key.
- 2 SubBytes:** each byte replaced according to a single S -box.
- 3 ShiftRows:** each row cyclically shifted.
- 4 MixColumns:** each column multiplied by a matrix.

See an animation of Rijndael!.

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

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

- 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.

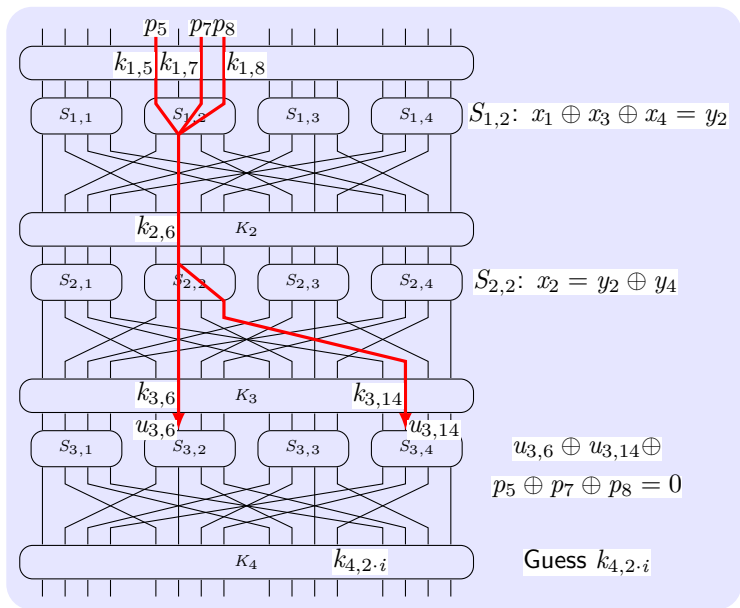
An Example of Linear Analysis of S -box

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

		Output Sum															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
I n p u t S u m	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

An Example of Linear 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.

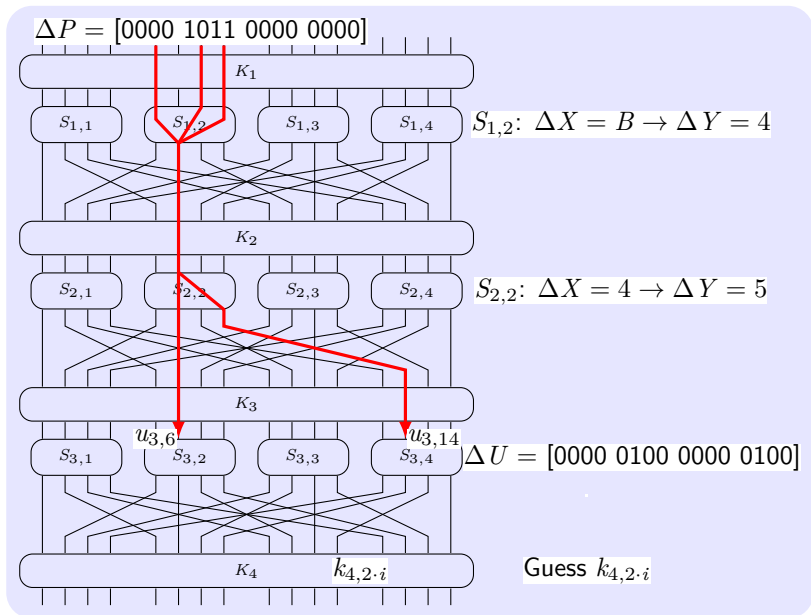
An Example of Differential Analysis of S -box

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

		Output Difference															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
I n P u t	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
D i f f e r e n c e	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

An Example of Differential Cryptanalysis



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