Practical Constructions of Pseudorandom Permutations (Block Ciphers)

Yu Zhang

HIT/CST/NIS

Cryptography, Spring, 2014

Outline

Content

Block Ciphers

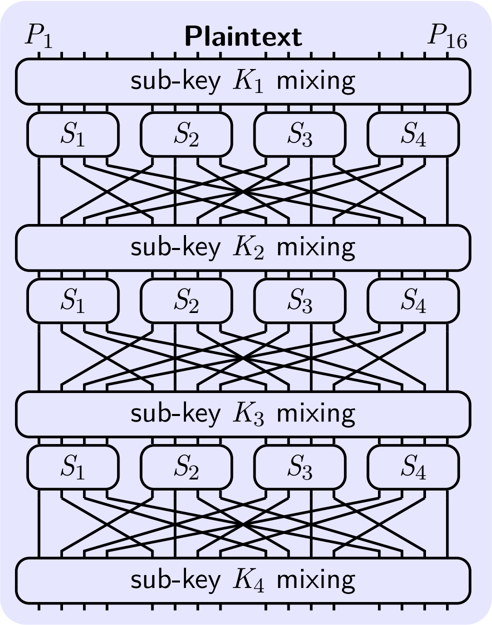
- **Block Cipher** $F : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$.
  $F_k : \{0,1\}^\ell \to \{0,1\}^\ell$, $F_k(x) \stackrel{\text{def}}{=} F(k,x)$.
  n is key length, ℓ is block length.
- Constructions are **heuristic**, not proofed.
- Considered as **PRP in practice**.
  - In the call for proposals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

[1] A 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. 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.

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

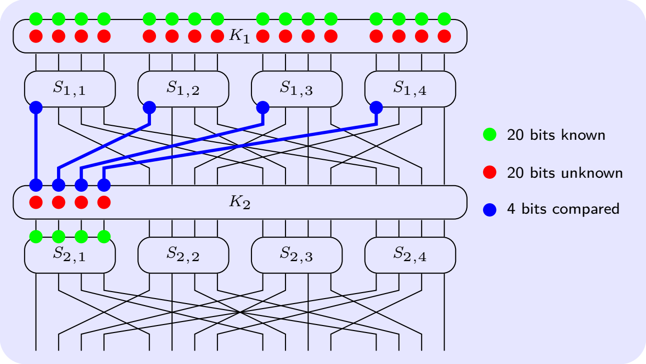
Test on $t = 16$ bits: Input-of-S-boxes $=$ PT $\oplus$ Key.

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

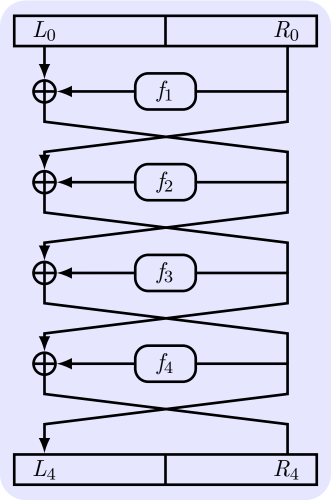
Attack on a 2-round SPN: 64-bit block, 128-bit key (2×64-bit sub-keys), 16×4-bit S-boxes, and mixing with XOR.



- 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. $2^{20-4\times8}$).
- Break with complexity $8 \cdot 2^{20} \cdot 16 = 2^{27} \ll 2^{128}$ (16 S-boxes).

Content

Feistel Networks



Properties of Feistel Networks

- **Idea**: Construct an invertible function from non-invertible components.
- **Round function** $f_i(R) \stackrel{def}{=} \hat{f}_i(k_i, R)$ ($\hat{f}_i$ 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

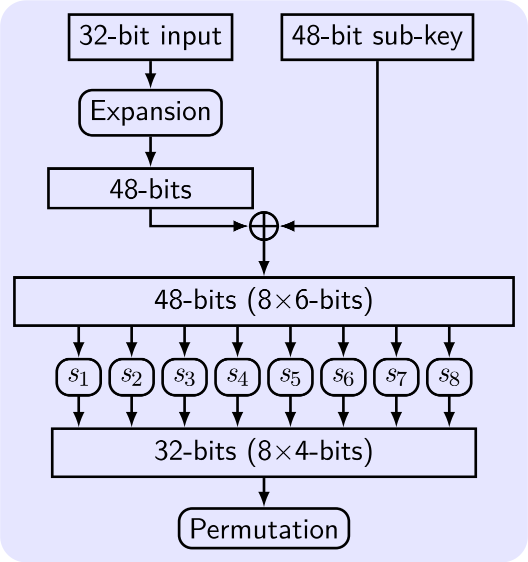
Luby-Rackoff Theorem*: Let F be a keyed function defined by a Feistel network. Then regardless of the mangler functions $\{\hat{f}_i\}$ and the number of rounds, F_k is a permutation for any choice of k.*

Content

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

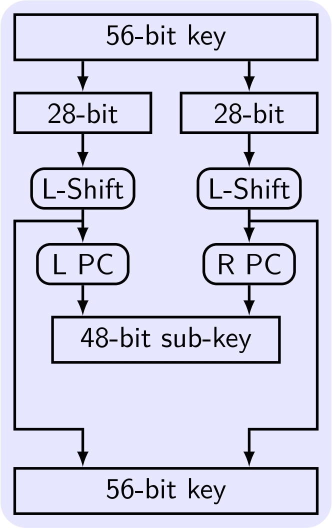
An S-box

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

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: $F_{k_1}(F_{k_2}(M)) = M$.

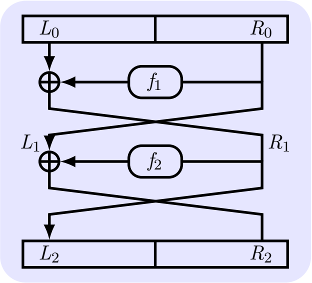
Semi-weak key pairs (2 of total 6 pairs)

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

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.



$$
\begin{aligned}
L_1 &= R_0 \\
R_1 &= L_0 \oplus f_1(R_0) \\
L_2 &= R_1 = L_0 \oplus f_1(R_0) \\
R_2 &= L_1 \oplus f_2(R_1). \\
f_1(R_0) &= L_0 \oplus L_2 \\
f_2(L_2) &= R_2 \oplus R_0
\end{aligned}
$$

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.

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.

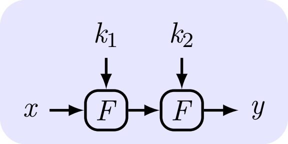
2006 COPACOBANA breaks DES in 9 days at $10,000.

2008 RIVYERA breaks DES within one day.

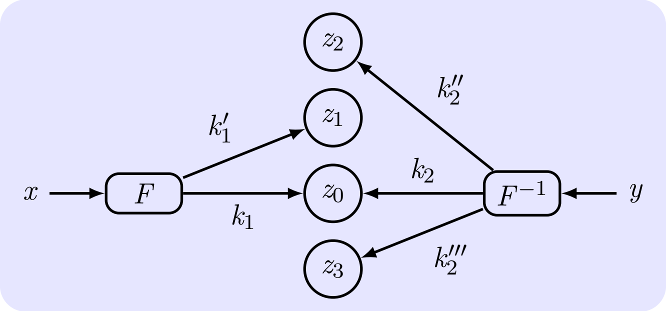
Content

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**: $y = F'_{k_1,k_2}(x) \overset{\text{def}}{=} F_{k_2}(F_{k_1}(x))$.

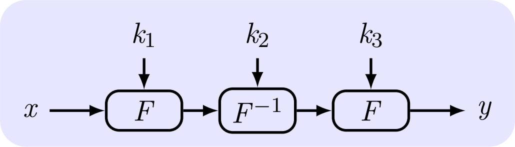


The Meet-In-the-Middle Attack



- $z_0 = F_{k_1}(x) = F_{k_2}^{-1}(y) \iff y = F'_{k_1,k_2}(x)$.
- 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.

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

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!.

Summary

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