Truncated Differentials

Lars R. Knudsen

June 2014

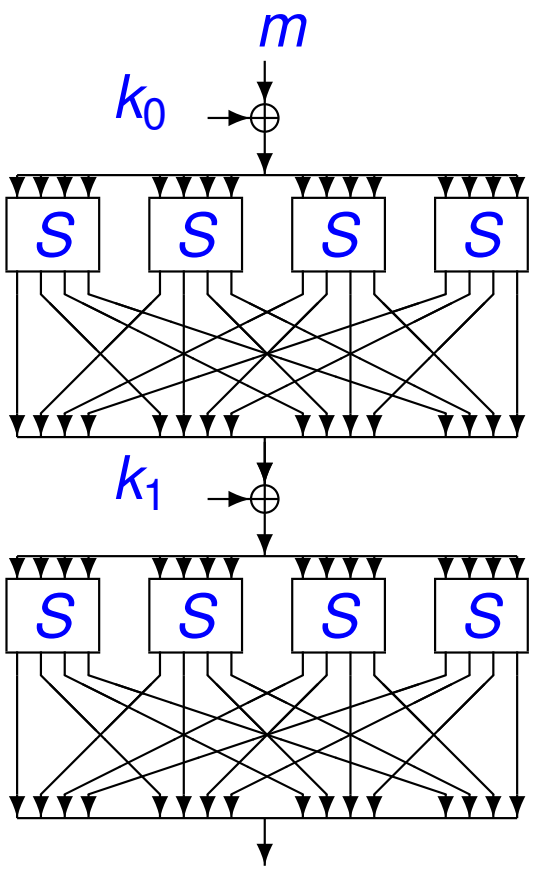
Outline

Differential cryptanalysis: the idea

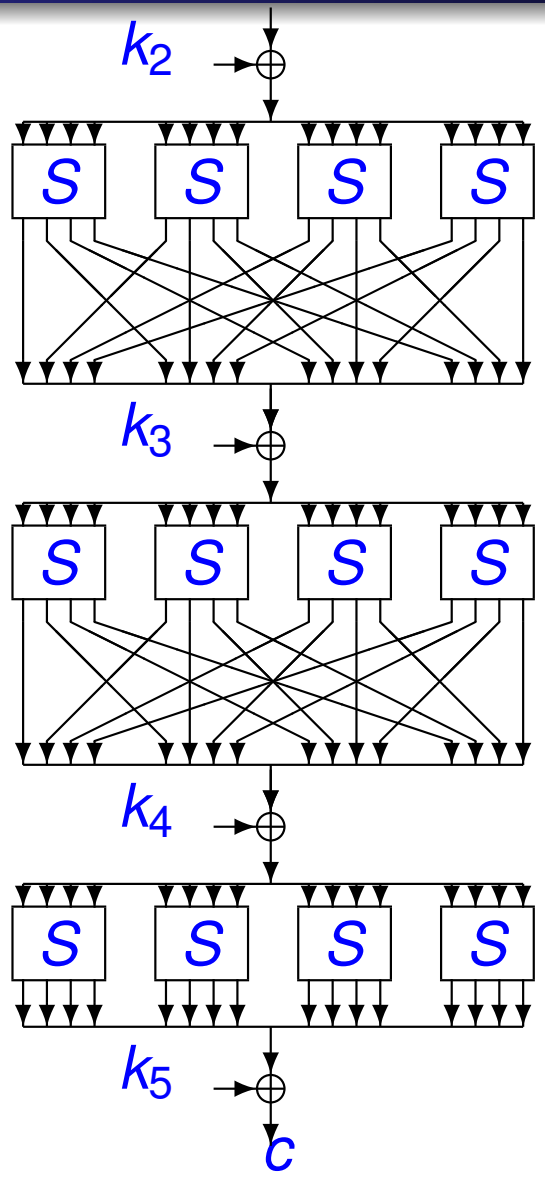
Differential cryptanalysis on iterated ciphers

- trace difference in chosen plaintexts through encryption process;
- predict difference in next to last round of encryption;
- guess key in last round, compute backwards.

CIPHERFOUR



5 rounds of CIPHERFOUR



Characteristic

Consider

$$(0,0,2,0) \overset{(S,S,S,S)}{\rightarrow} (0,0,2,0)$$

which has probability $6/16$ and note that

$$(0,0,2,0) \overset{P}{\rightarrow} (0,0,2,0)$$

Thus

$$(0,0,2,0) \overset{\mathcal{R}}{\rightarrow} (0,0,2,0)$$

Characteristic

$$(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0)$$

with probability

$$(6/16)^2$$

and

$$(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0)$$

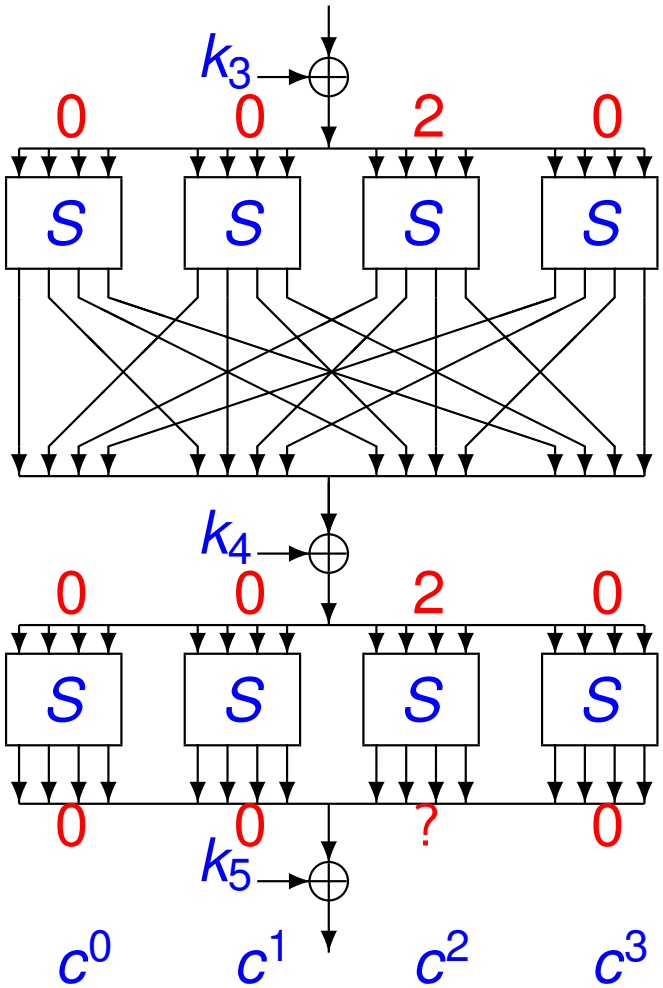
with probability

$$(6/16)^4 \approx 0.02.$$

Example

Attack 5 rounds by guessing (parts of) the last round key.

Differential Attack of CIPHERFOUR



Differentials

Observation

When using

$$(0,0,2,0) \stackrel{\mathcal{R}}{\to} (0,0,2,0) \stackrel{\mathcal{R}}{\to} (0,0,2,0) \stackrel{\mathcal{R}}{\to} (0,0,2,0) \stackrel{\mathcal{R}}{\to} (0,0,2,0)$$

we do not care about the intermediate differences!

What we are really interested in is

$$(0,0,2,0) \stackrel{\mathcal{R}}{\to} ? \stackrel{\mathcal{R}}{\to} ? \stackrel{\mathcal{R}}{\to} ? \stackrel{\mathcal{R}}{\to} (0,0,2,0)$$

or

$$(0,0,2,0) \stackrel{4\mathcal{R}}{\to} (0,0,2,0).$$

Differentials

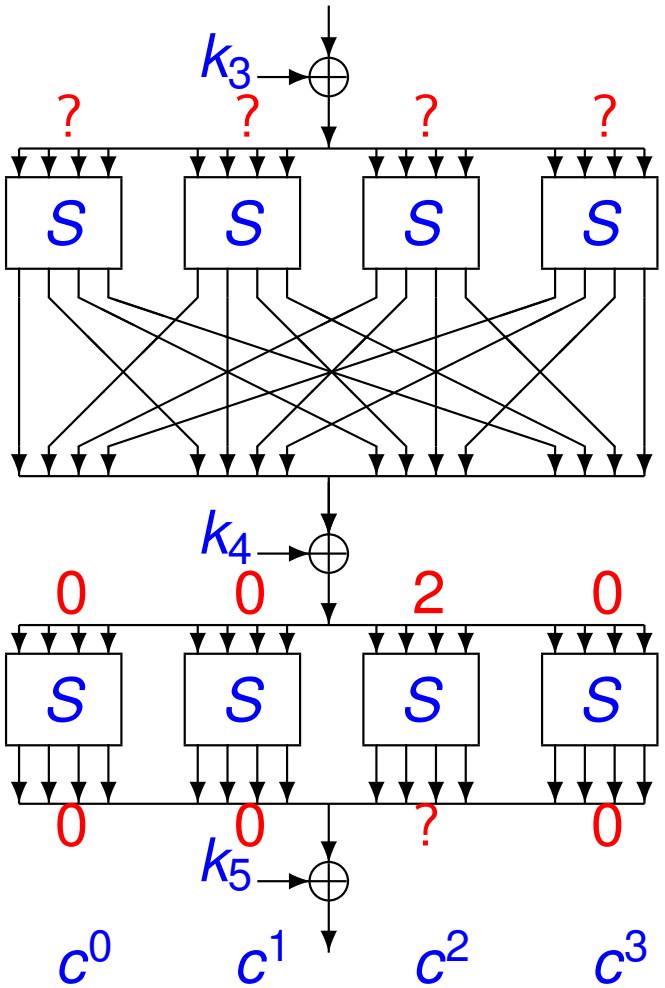
$$(0,0,2,0) \stackrel{4\mathcal{R}}{\rightarrow} (0,0,2,0).$$

There are at least four characteristics involved

$$\begin{aligned}
&(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0),\\
&(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,0,2) \xrightarrow{\mathcal{R}} (0,0,0,1) \xrightarrow{\mathcal{R}} (0,0,1,0) \xrightarrow{\mathcal{R}} (0,0,2,0),\\
&(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,0,2) \xrightarrow{\mathcal{R}} (0,0,1,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0),\\
&(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,0,2) \xrightarrow{\mathcal{R}} (0,0,1,0) \xrightarrow{\mathcal{R}} (0,0,2,0).
\end{aligned}$$

$$P((0,0,2,0) \stackrel{4\mathcal{R}}{\rightarrow} (0,0,2,0)) \approx 0.081 > 0.02.$$

Differential Attack of CIPHERFOUR



CIPHERFOUR: Experimental Results

Differential attack on 5 rounds

Attacker tries to determine four bits of the key

Experiment

Number of texts	Differential attack
32	64%
64	76%
128	85%
256	96%

Truncated differentials

Definition

A (differential) characteristic predicts the difference in a pair of texts after each round of encryption.

Definition

A differential is a collection of characteristics.

Truncated differentials

Definition

A truncated characteristic predicts only part of the difference in a pair of texts after each round of encryption.

Definition

A truncated differential is a collection of truncated characteristics.

Truncated differentials

S-box from before

Bit notation:

- $0010 \xrightarrow{S} 0001$ has probability $\frac{6}{16}$.
- $0010 \xrightarrow{S} 0010$ has probability $\frac{6}{16}$.
- $0010 \xrightarrow{S} 1001$ has probability $\frac{2}{16}$.
- $0010 \xrightarrow{S} 1010$ has probability $\frac{2}{16}$.
- $0010 \xrightarrow{S} \star 0 \star \star$ has probability 1.

Distribution table

in \out	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Truncated differentials

Input difference 2 to S-box lead only to output differences $1, 2, 9,$ and a. So for one round

$$(0000\ 0000\ 0010\ 0000) \xrightarrow{\mathcal{R}} \begin{cases} (0000\ 0000\ 0010\ 0000) \text{ or} \\ (0000\ 0000\ 0000\ 0010) \text{ or} \\ (0010\ 0000\ 0010\ 0000) \text{ or} \\ (0010\ 0000\ 0000\ 0010) \end{cases}$$

Truncated differentials

$$
\begin{aligned}
(0000\ \ 0000\ \ 0010\ \ 0000) &\xrightarrow{\mathcal{R}} (00\star0\ \ 0000\ \ 00\star0\ \ 00\star0)\\
(0000\ \ 0000\ \ 0000\ \ 0010) &\xrightarrow{\mathcal{R}} (000\star\ \ 0000\ \ 000\star\ \ 000\star)\\
(0010\ \ 0000\ \ 0010\ \ 0000) &\xrightarrow{\mathcal{R}} (\star0\star0\ \ 0000\ \ \star0\star0\ \ \star0\star0)\\
(0010\ \ 0000\ \ 0000\ \ 0010) &\xrightarrow{\mathcal{R}} (\star00\star\ \ 0000\ \ \star00\star\ \ \star00\star)
\end{aligned}
$$

$$
\left.\begin{array}{l}
(0000\ \ 0000\ \ 0010\ \ 0000)\\
(0000\ \ 0000\ \ 0000\ \ 0010)\\
(0010\ \ 0000\ \ 0010\ \ 0000)\\
(0010\ \ 0000\ \ 0000\ \ 0010)
\end{array}\right\} \xrightarrow{\mathcal{R}} (\star0\star\star\ \ 0000\ \ \star0\star\star\ \ \star0\star\star)
$$

Truncated differentials

- Leads to a 2-round truncated differential

$$(0000\ 0000\ 0010\ 0000) \xrightarrow{\mathcal{R}} (\star 0 \star\star\ 0000\ \star 0 \star\star\ \star 0 \star\star)$$

- Adding another round gives

$$(\star 0 \star\star\ 0000\ \star 0 \star\star\ \star 0 \star\star) \xrightarrow{\mathcal{R}} (\star 0 \star\star\ \star\ 0 \star\star\ \star\ 0 \star\star\ \star\ 0 \star\star).$$

Truncated differentials

This leads to a 3-round truncated differential

- $(0000\ 0000\ 0010\ 0000) \xrightarrow{3\mathcal{R}} (\star 0 \star\star\ \star\ 0 \star\star\ \star\ 0 \star\star\ \star\ 0 \star\star)$

of probability 1!

Can we extend this further?

Truncated differentials

- Consider the 1-round characteristic
  $(0000\ 0000\ 0010\ 0000) \xrightarrow{\mathcal{R}} (0000\ 0000\ 0010\ 0000).$
- A pair will follow this characteristic if $2 \xrightarrow{\mathcal{S}} 2$
- Choose 16 texts

$$(t_0,\ t_1,\ i,\ t_2),$$

  where $i = 0, \ldots, 15$ and t_0, t_1, t_2 are arbitrary and fixed.
- Any two (different) texts lead to a pair of difference

$$\begin{array}{cccc} (t_0 \oplus t_0 & t_1 \oplus t_1 & i \oplus j & t_2 \oplus t_2) = \\ (0000 & 0000 & \star\star\star\star & 0000). \end{array}$$

Truncated differentials

- How many pairs lead to difference (0000 0000 0010 0000) after the first S-box?
- Exactly eight (distinct pairs)!
- For these eight pairs one gets
  $(0000\ 0000\ \star\star\star\star\ 0000) \xrightarrow{\mathcal{R}} (0000\ 0000\ 0010\ 0000)$.
- With correct guess of four-bit key one can easily identify these eight.

Truncated differentials

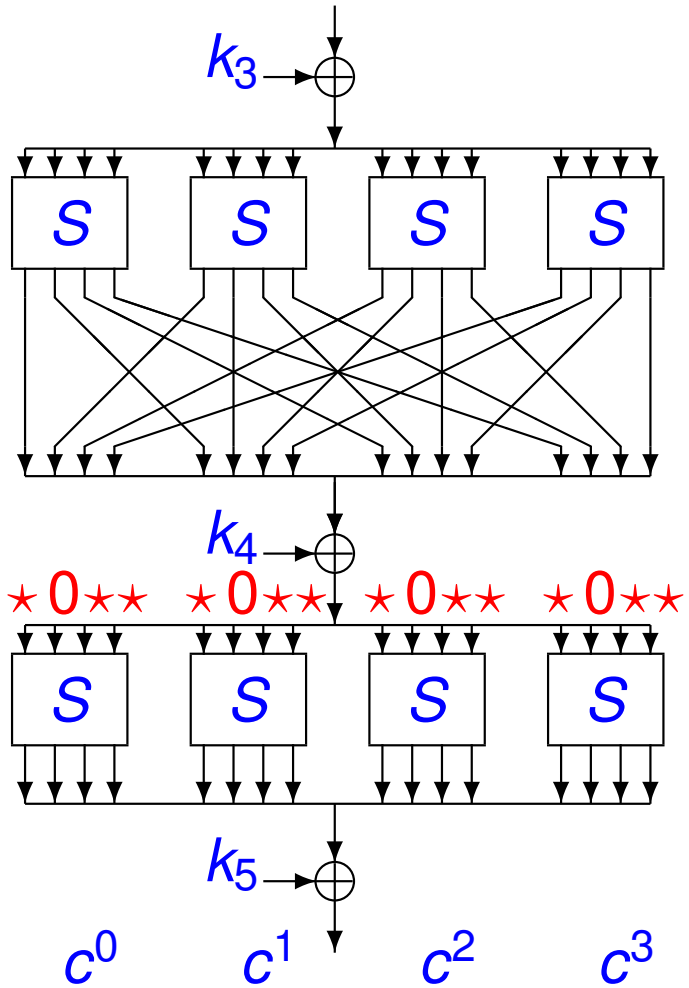
Summing up: yields a 4-round truncated differential

- $(0000\,0000\ \star\star\star\star\,0000) \xrightarrow{4\mathcal{R}} (\star 0\star\star\ \star\ 0\star\star\ \star\ 0\star\star\ \star\ 0\star\star)$

which for correct guess of 4-bit key in 1st round, gives 8 right pairs from pool of 16 texts.

5-round attack: run attack for all values of 4 bits of k_0 and 4 times 4 bits of k_5.

Differential Attack of CIPHERFOUR



Truncated differentials

5-round attack on CIPHERFOUR

Experiment

Number of texts	Differentials		Truncated differentials	
16	.		28%	(4+4)
32	.		78%	(4+9)
48	.		97%	(4+12)
64	76%	(4)		
128	85%	(4)		
256	96%	(4)		

Numbers in brackets denote the number of key bits identified

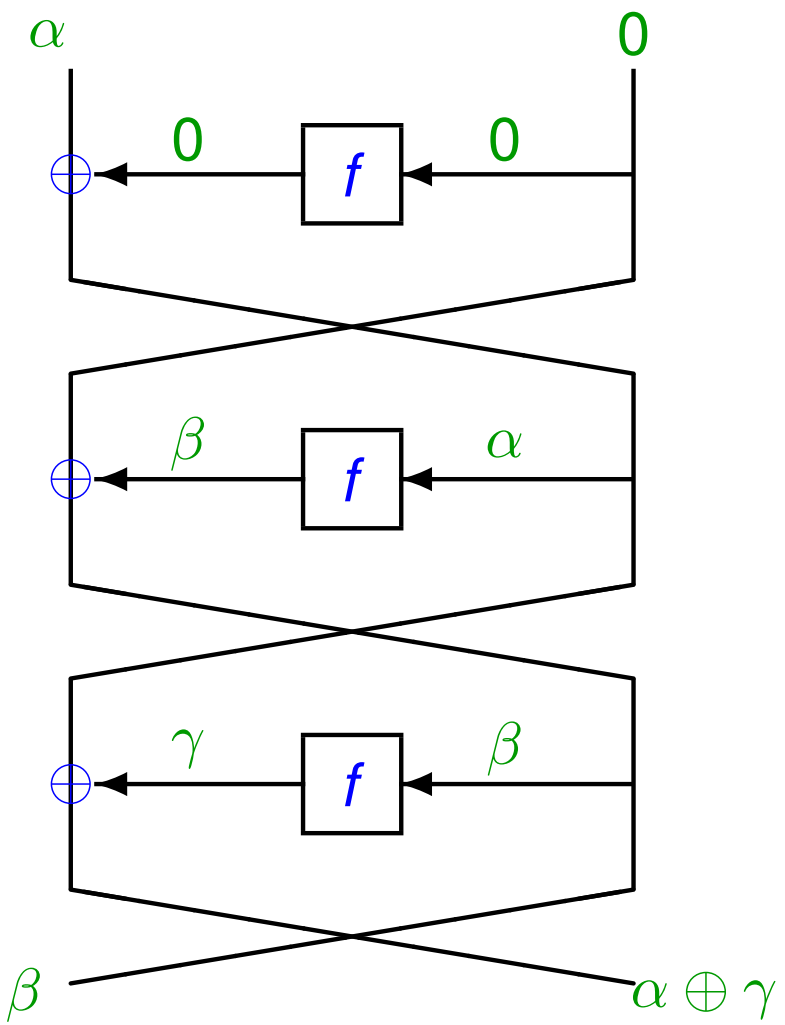
Impossible differentials

- Traditionally in differential attack, aim is to find differential of high probability
- A differential of low probability can be equally useful
- S/N should be different from one:
  - S/N > 1, right value of key suggested the **most**
  - S/N < 1, right value of key suggested the **least**

Truncated differentials - Feistel network

- Consider Feistel network where round function is a bijection for any fixed key
- Consider a differential $(\alpha, 0)$ such that the difference in the left halves of the plaintexts is α and where the right halves are equal
- It follows that after 5 rounds of encryption, the difference in the ciphertexts will never be $(0, \alpha)$
- Can be used in attacks on such ciphers with more than 5 rounds by guessing keys and computing backwards
- For the correct key guesses the computed difference will never be $(0, \alpha)$

Truncated differentials - Feistel network

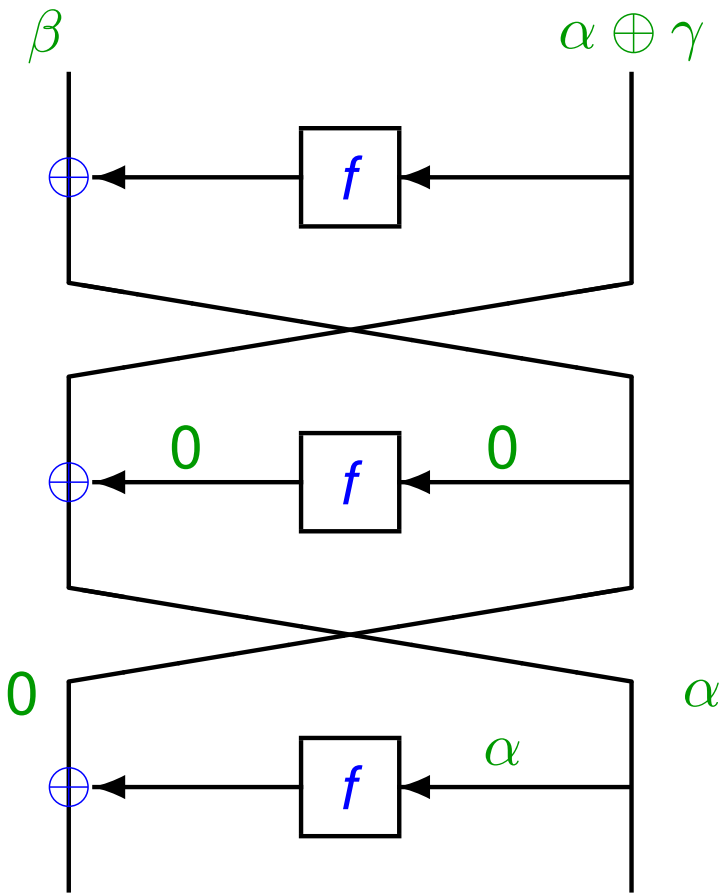


$\alpha \neq 0$

$\beta \neq 0$

$\gamma \neq 0$

Truncated differentials - Feistel network



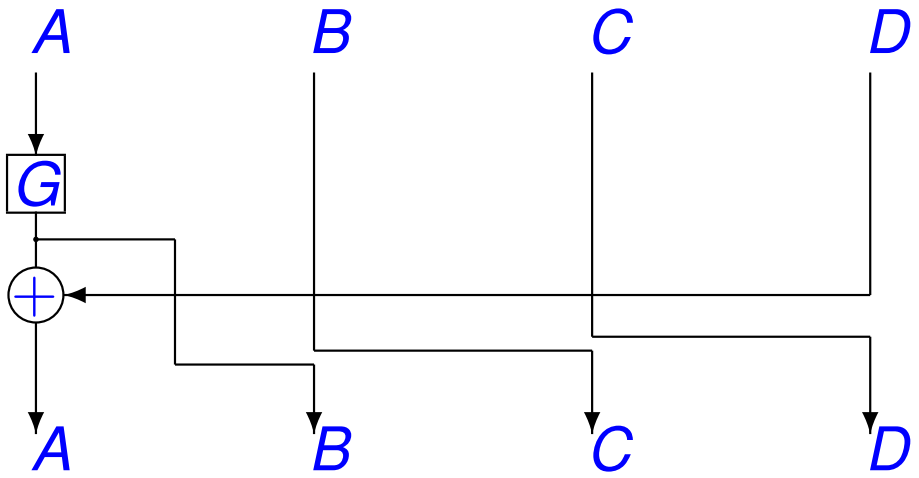
Skipjack (Biham, Biryukov, Shamir)

- Skipjack - a 32-round iterated block cipher by NSA
- there exists truncated differentials of Skipjack
  - for 12 encryption rounds of probability one
    $(0, a, 0, 0) \xrightarrow{12r} (b, c, d, 0)$
  - for 12 decryption rounds of probability one
    $(f, g, 0, h) \xleftarrow{12r} (e, 0, 0, 0)$
  - for 24 rounds of probability zero $(0, a, 0, 0) \xrightarrow{24r} (e, 0, 0, 0)$
- these can be used to break Skipjack with 31 rounds faster than by an exhaustive key search

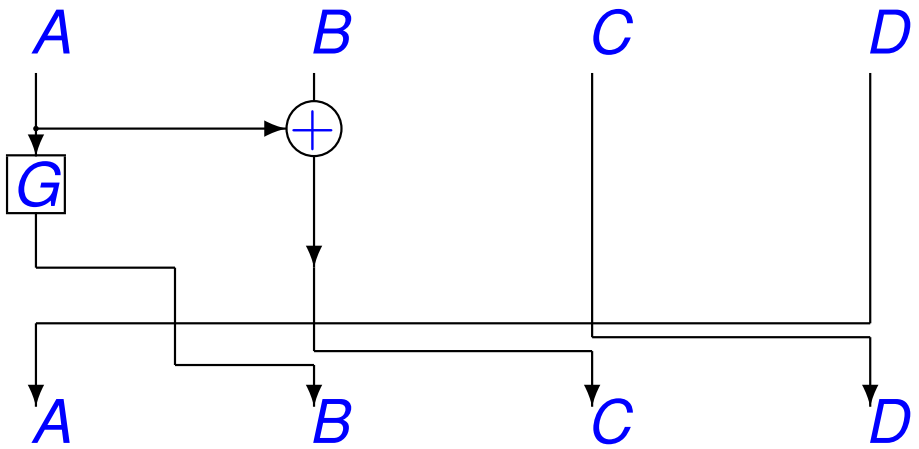
Skipjack (continued)

- Skipjack is an iterated 64-bit block cipher using an 80-bit key and running in 32 rounds, see Figure next page. Encryption of a 64-bit plaintext consists of first applying eight A-rounds, then eight B-rounds, once again eight A-rounds and finally eight B-rounds. A round counter is added to one of the 16-bit words in each round. The key schedule is simple but this and the round counter is not important for the illustration here.
- There is a twelve-round truncated differential of probability one through 4 A-rounds and 8 B-rounds.
- There is a twelve-round truncated differential of probability one through 4 inverse B-rounds and 8 inverse A-rounds.

Skipjack graph (G takes 16-bit round key)



Skipjack A-round



Skipjack B-round