Differential cryptanalysis of PUFFIN and PUFFIN2

Céline Blondeau[1,2] and Benoît Gérard[3]

[1] INRIA project-team SECRET
[2] Aalto University School of Science
[3] Université catholique de Louvain, UCL Crypto Group

ECRYPT Workshop on Lightweight cryptography

-

28/11/2011

Preliminary remarks

Main contributions

- Breaking both versions of PUFFIN.
- Tree-based technic for estimating time complexity.

Tree-based estimate relies on strong assumptions:

- provides a lower bound on complexity,
- may not be the most relevant tool for cryptanalysis,
- does not threaten the first contribution,
- is the relevant tool for security analysis.

This presentation is security analysis oriented.

Outline

Summary

Lightweight SPN ciphers

Round function composed of:

- a key mixing (key addition);
- a non-linear layer (S-boxes);
- a diffusion layer (permutation).

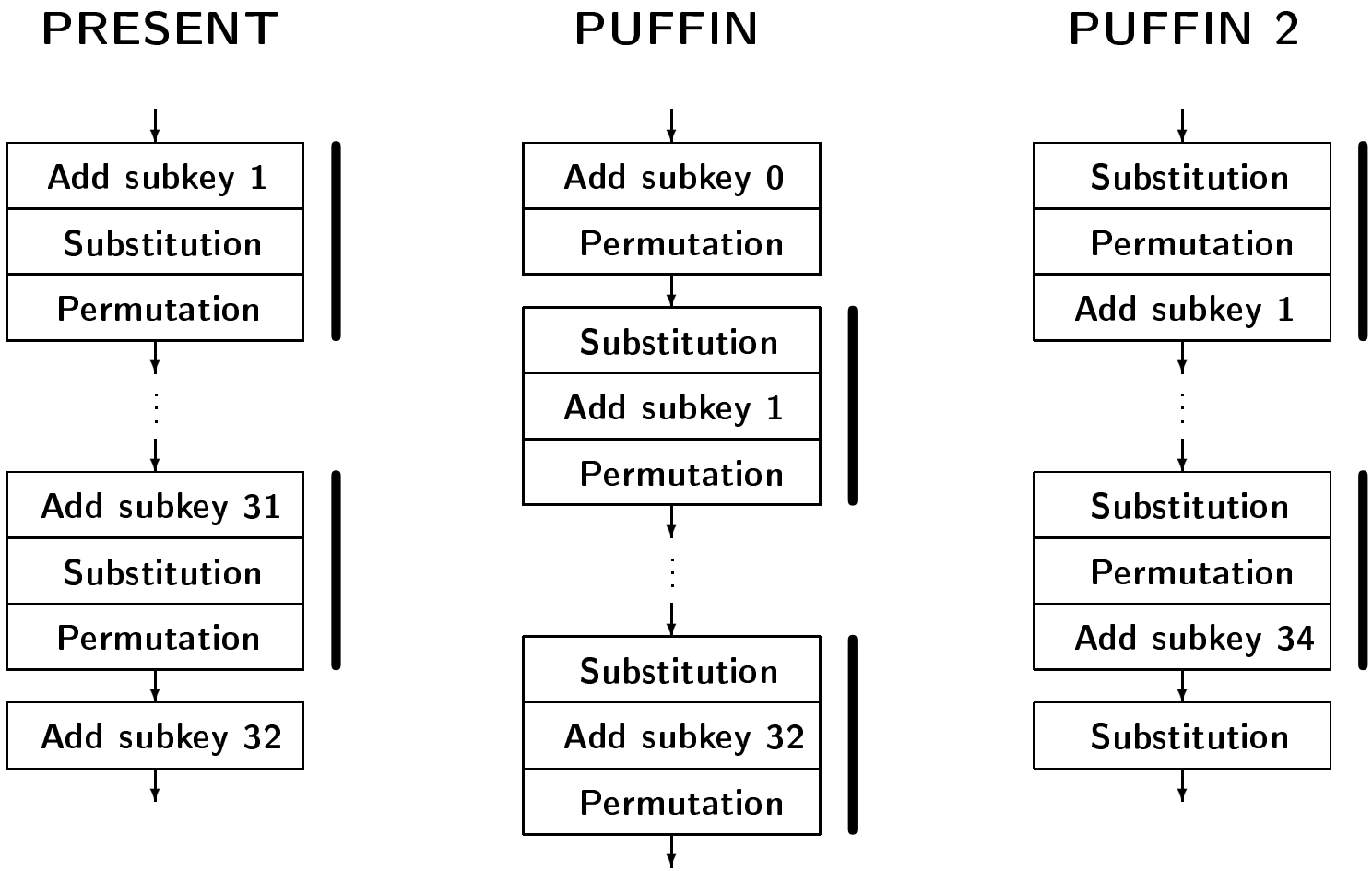
Most known and studied: PRESENT.

Design goal for PUFFIN: PRESENT-like involutional cipher.

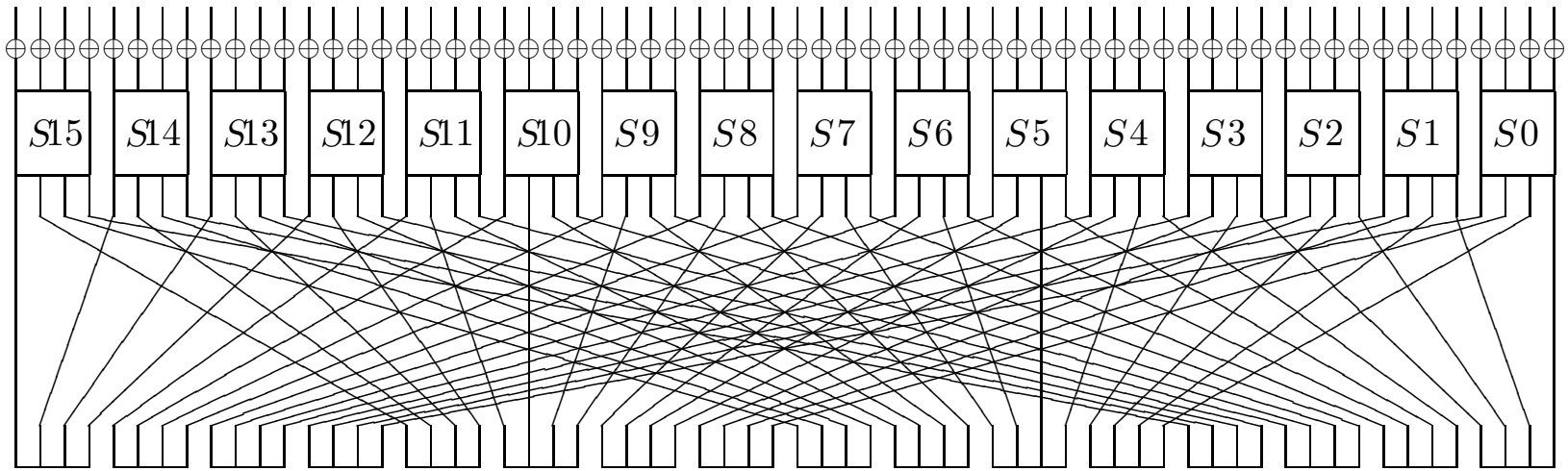
PUFFIN1/2 security issues

PUFFIN: broken in [Leander EUROCRYPT 2011].
PUFFIN2: patched version of PUFFIN.

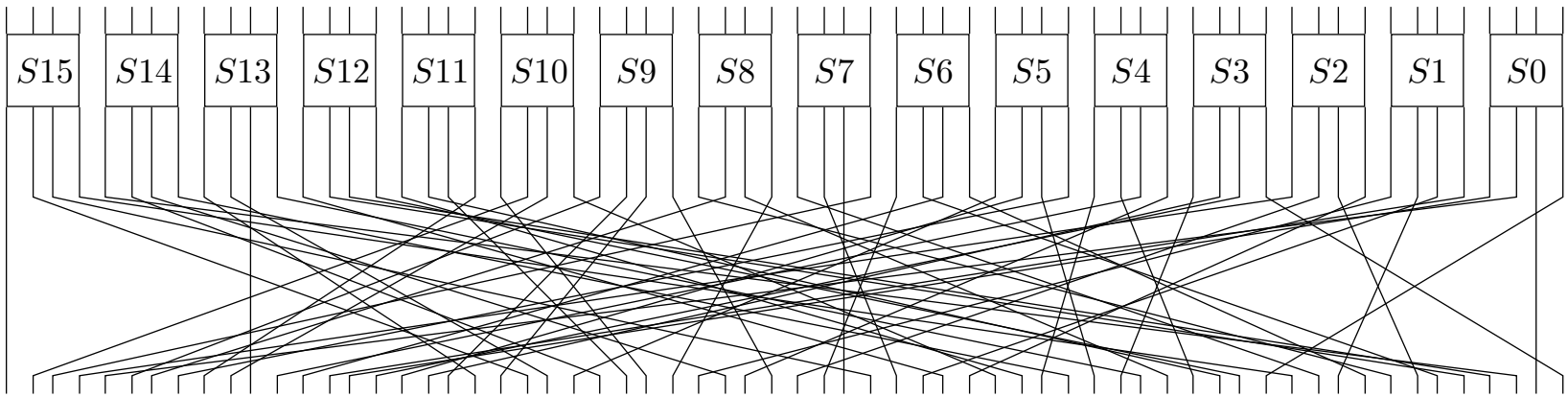
PRESENT, PUFFIN and PUFFIN 2



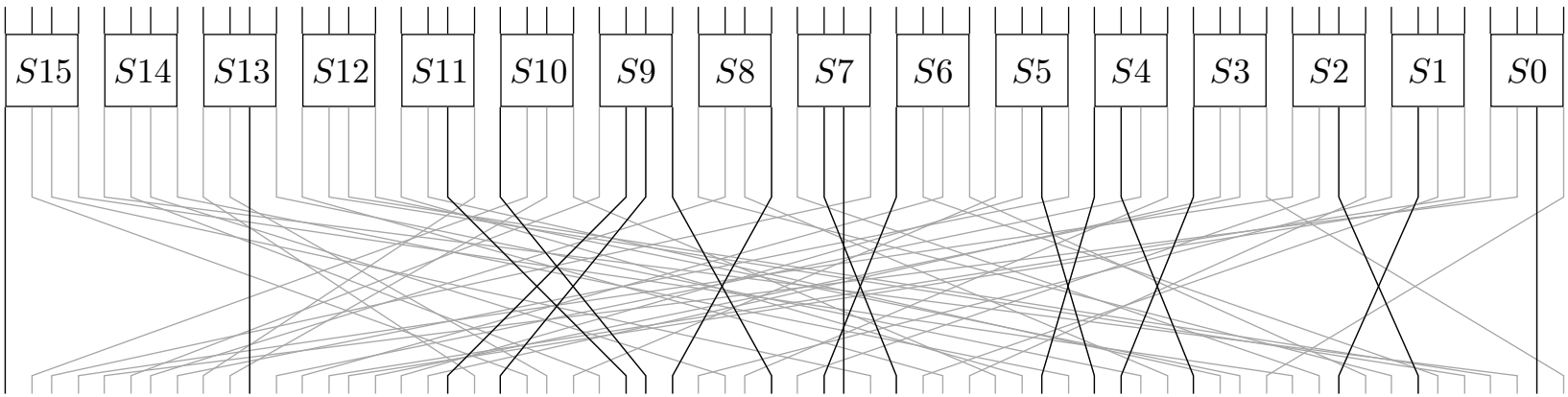
PRESENT permutation layer



PUFFIN1/2 permutation layer



PUFFIN1/2 permutation layer



PRESENT and PUFFIN1/2 S-box

PRESENT S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\mathrm{S}(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

PUFFIN1/2 S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\mathrm{S}(x)$	D	7	3	2	9	A	C	1	F	4	5	E	6	0	B	8

PRESENT and PUFFIN1/2 S-box

PRESENT S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\mathrm{S}(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

PUFFIN1/2 S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\mathrm{S}(x)$	D	7	3	2	9	A	C	1	F	4	5	E	6	0	B	8

PRESENT and PUFFIN1/2 S-box

PRESENT S-box

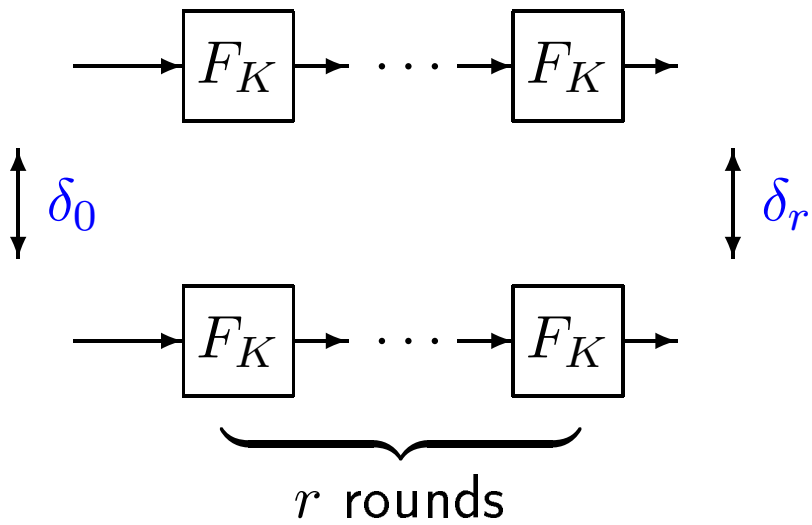
x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\mathrm{S}(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

PUFFIN1/2 S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\mathrm{S}(x)$	D	7	3	2	9	A	C	1	F	4	5	E	6	0	B	8

Summary

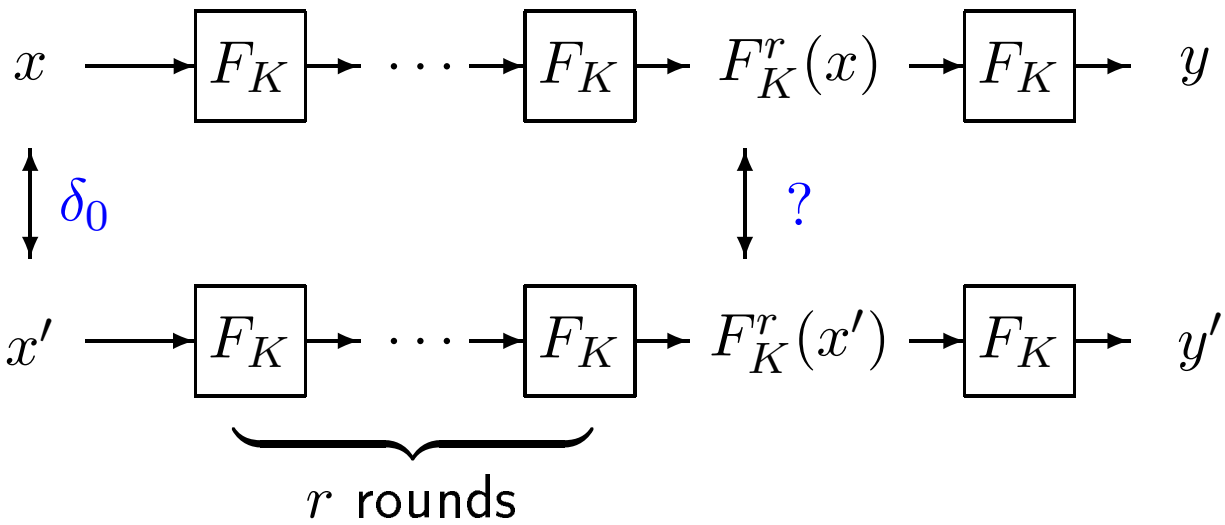
Differential attacks on iterated ciphers



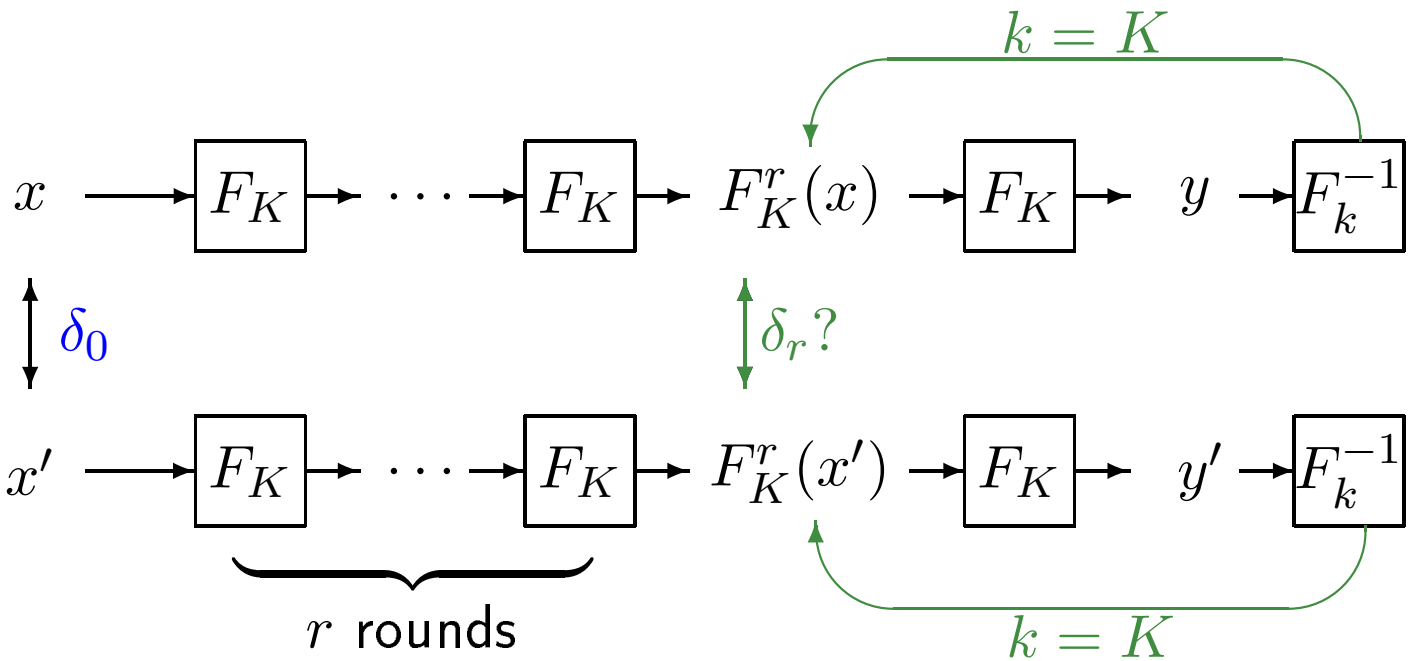
Differential probability

$$\Pr\left[\delta_0 \to \delta_r\right] \stackrel{\text{def}}{=} \Pr_{X,K}\left[F_K^r(X) \oplus F_K^r(X \oplus \delta_0) = \delta_r\right].$$

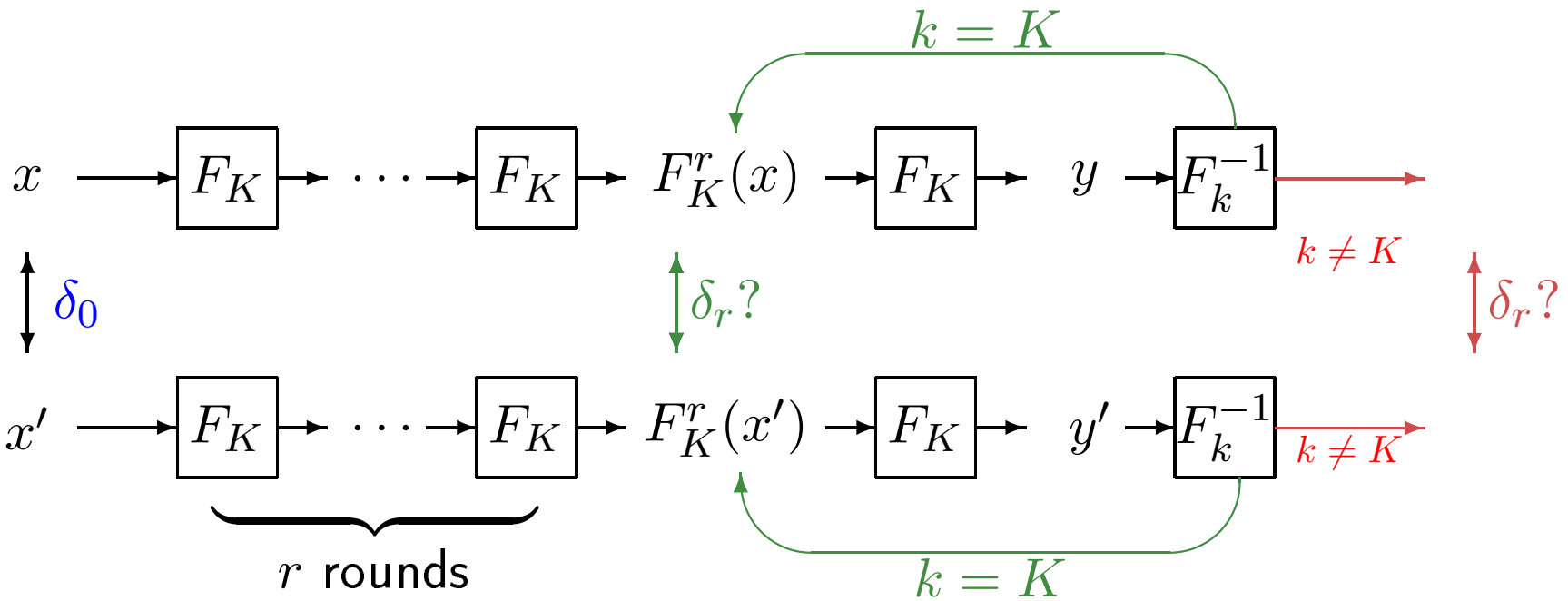
Differential attacks on iterated ciphers



Differential attacks on iterated ciphers



Differential attacks on iterated ciphers



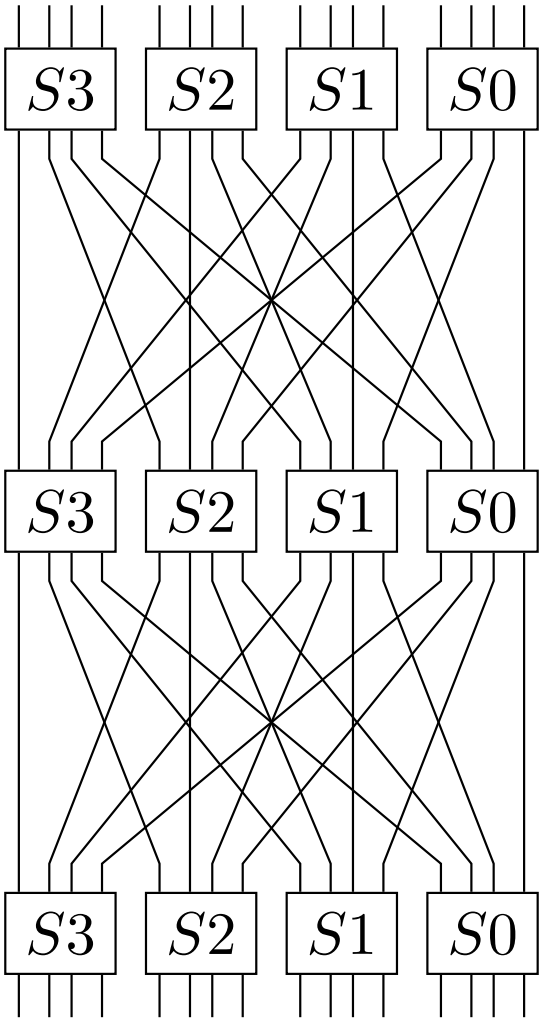
Basic Principle:

For each last-round subkey candidate k, compute

$$D(k) = \#\{(y, y') \text{ such that } F_k^{-1}(y) \oplus F_k^{-1}(y') = \delta_r\}.$$

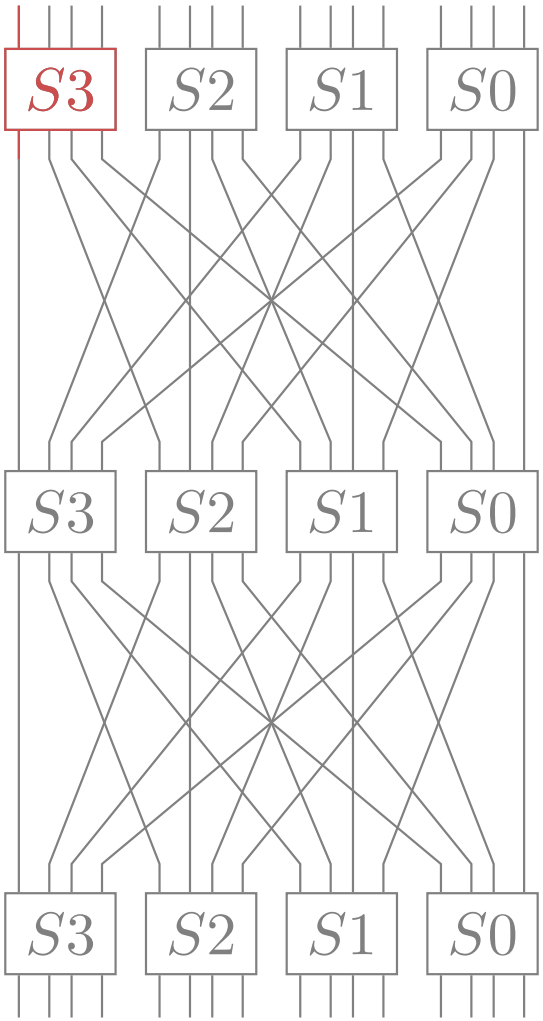
Finding good differentials

Differentials and differential trails



Finding good differentials

Differentials and differential trails



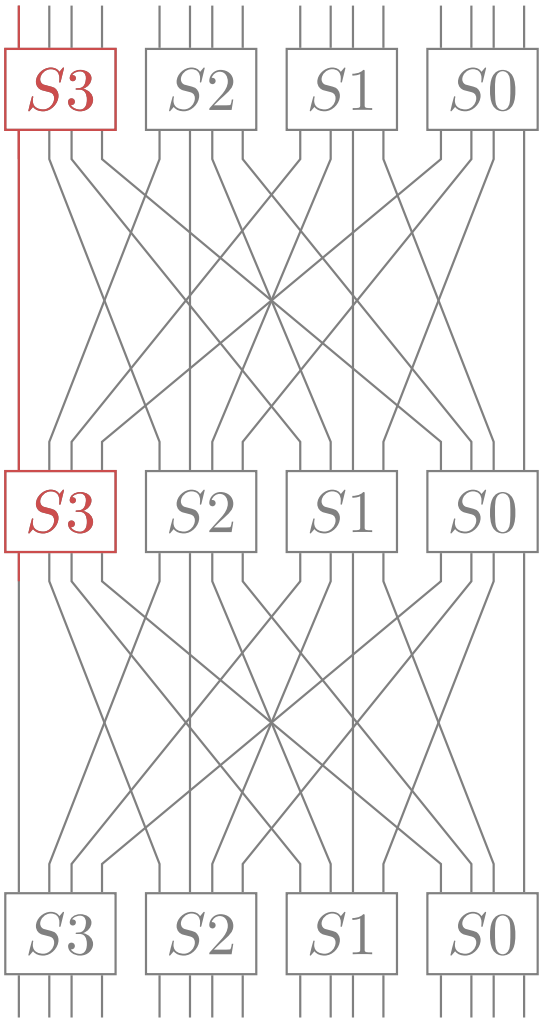
1-round differential

(δ_0, δ_1)

$$\begin{aligned} \delta_0 &= \texttt{0x8000}, \\ \delta_1 &= \texttt{0x8000} \end{aligned}$$

Finding good differentials

Differentials and differential trails



2-round differential trail

$(\delta_0, \delta_1, \delta_2)$

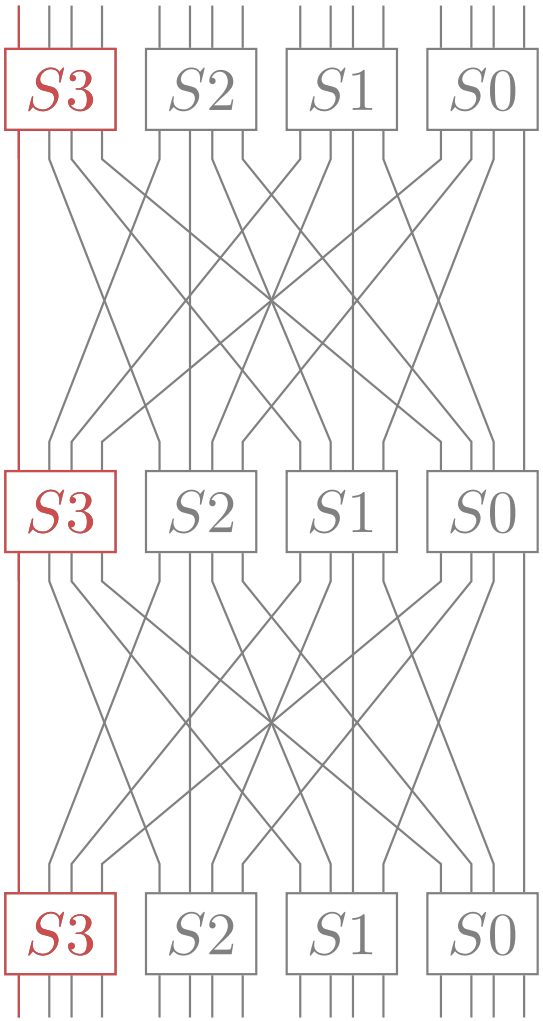
$$\begin{aligned} \delta_0 &= \texttt{0x8000}, \\ \delta_1 &= \texttt{0x8000}, \\ \delta_2 &= \texttt{0x8000} \end{aligned}$$

Trail probability for Markov ciphers:

$$\Pr\left[\delta_0 \to \delta_1 \to \delta_2\right] = \Pr\left[\delta_0 \to \delta_1\right] \cdot \Pr\left[\delta_1 \to \delta_2\right].$$

Finding good differentials

Differentials and differential trails



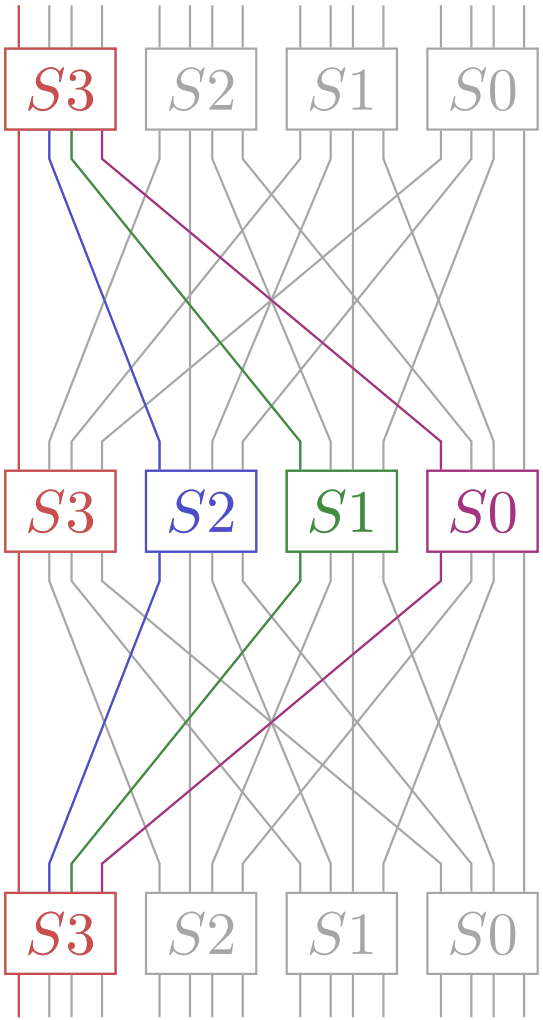
3-round differential trail

$(\delta_0, \delta_1, \delta_2, \delta_3)$

$$\begin{aligned} \delta_0 &= \texttt{0x8000}, \\ \delta_1 &= \texttt{0x8000}, \\ \delta_2 &= \texttt{0x8000}, \\ \delta_3 &= \texttt{0x8000}. \end{aligned}$$

Finding good differentials

Differentials and differential trails



(0x8000, 0x8000, 0x8000, 0x8000)

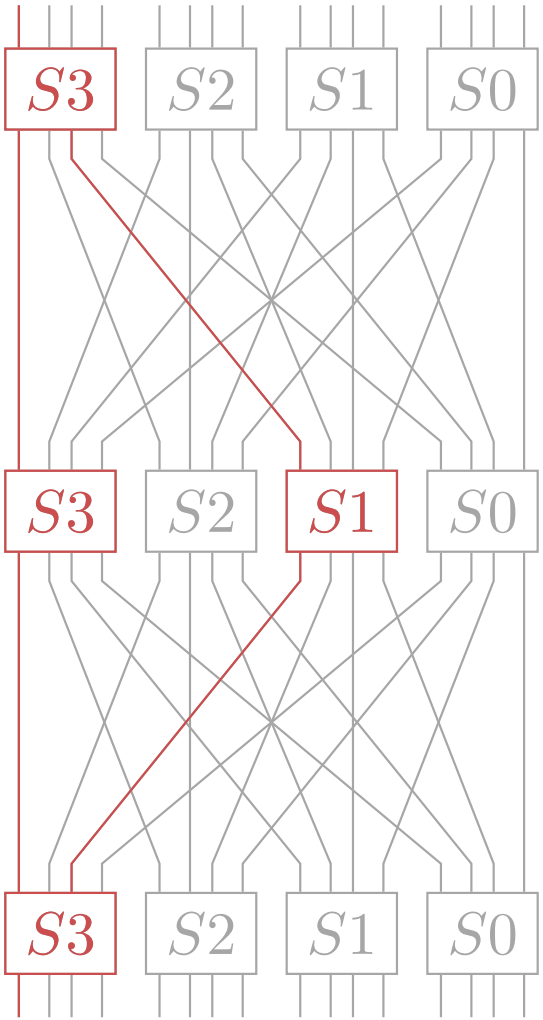
(0x8000, 0x0800, 0x4000, 0x8000)

(0x8000, 0x0080, 0x2000, 0x8000)

(0x8000, 0x0008, 0x1000, 0x8000)

Finding good differentials

Differentials and differential trails



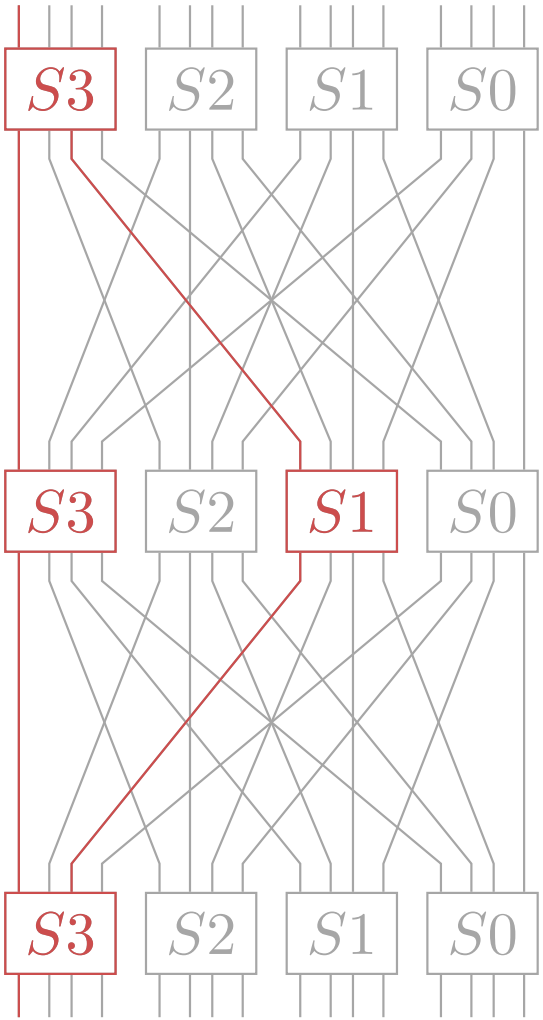
$$(\texttt{0x8000}, \texttt{0x8080}, \texttt{0xA000}, \texttt{0x8000})$$

$$\Pr\left[\texttt{0x8080} \rightarrow \texttt{0xA000}\right] = \left(\Pr\left[\texttt{0x8} \rightarrow \texttt{0x8}\right]\right)^2.$$

More active S-boxes $\Rightarrow$ smaller trail probability.

Finding good differentials

Differentials and differential trails



- The differential probability is the sum of trail probabilities:

$$\Pr\left[\delta_0 \to \delta_3\right] = \sum_{\delta_1,\delta_2} \Pr\left[\delta_0 \to \delta_1 \to \delta_2 \to \delta_3\right].$$

- Lower-bound by considering most significant trails.
- Significant trails obtained using Branch-and-Bound.

Extensions of differential cryptanalysis

Many extensions:

- inverting $r' > 1$ last rounds;
- using more differentials;
- using impossible differentials;
- using unlikely differentials;
- using higher order differentials;
- using truncated differentials;
- ...

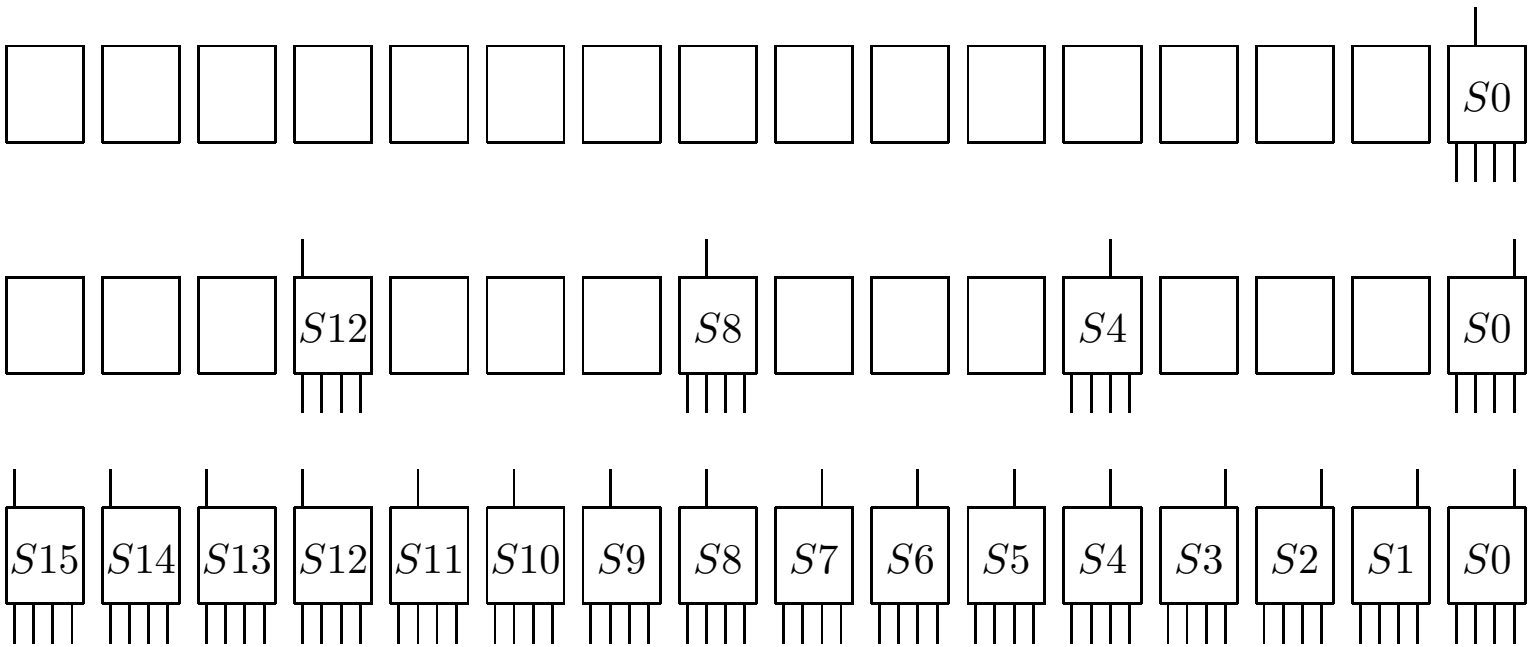
Extensions of differential cryptanalysis

Many extensions:

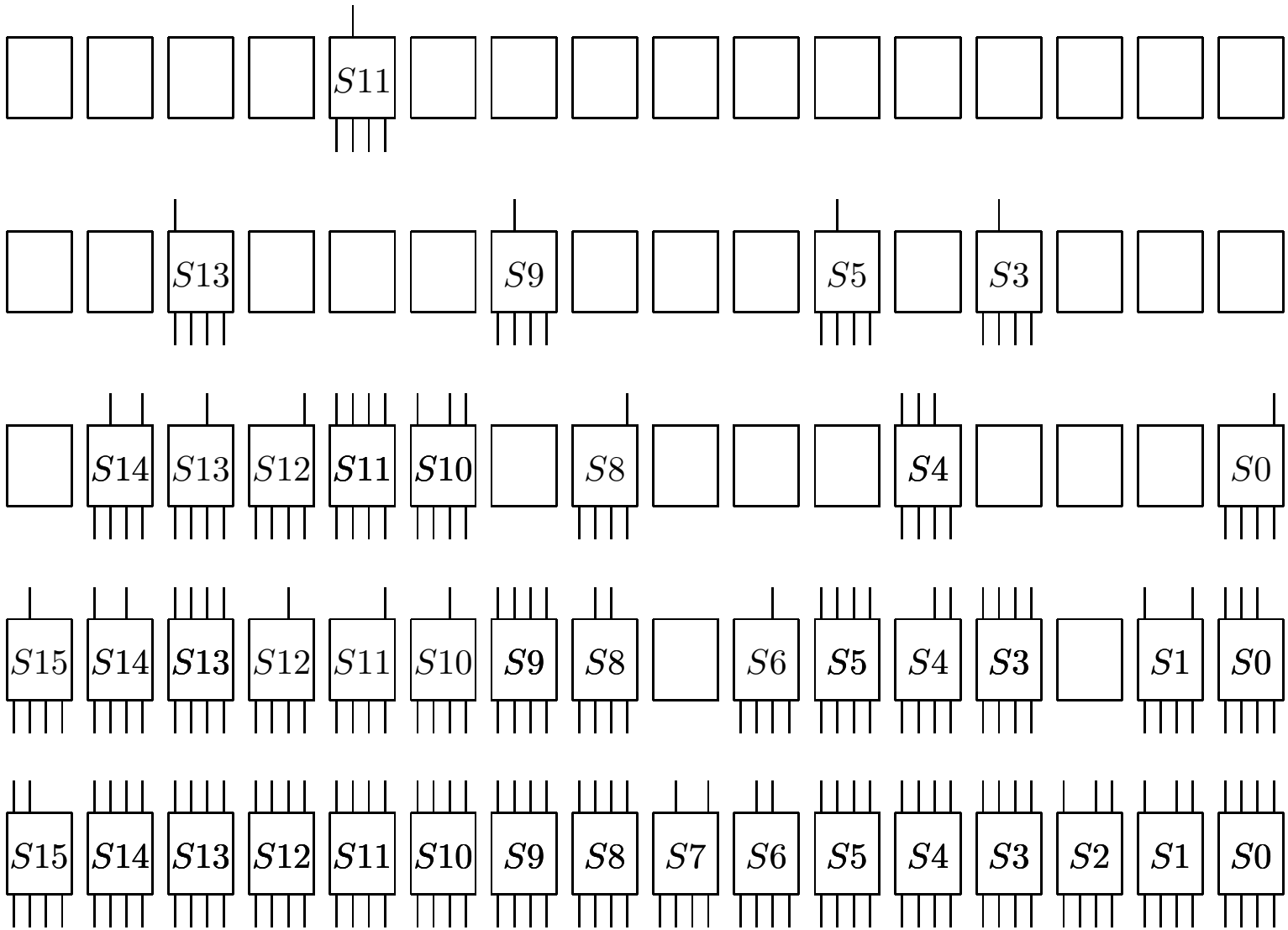
- **inverting $r' > 1$ last rounds;**
- **using more differentials;**
- using impossible differentials;
- using unlikely differentials;
- using higher order differentials;
- using truncated differentials;
- ...

Summary

PRESENT permutation layer diffusion



PUFFIN1/2 permutation layer diffusion



S-box differential uniformity

Differential uniformity

$$\delta(a,b) \stackrel{\text{def}}{=} \#\{x \in \mathbb{F}_2^d, \texttt{Sbox}(x) \oplus \texttt{Sbox}(x \oplus a) = b\}.$$

$$\delta(\texttt{Sbox}) \stackrel{\text{def}}{=} \max_{a,b \neq 0} \delta(a,b).$$

Criterion for evaluating S-box resistance against differential cryptanalysis. For s active S-boxes

$$\text{Trail probability} \leq \left(\frac{\delta(\texttt{Sbox})}{2^d}\right)^s.$$

For PRESENT and PUFFIN S-boxes, $\delta(\texttt{Sbox}) = 4$ (optimal).

PRESENT S-box differential table

	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	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
a	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
b	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
c	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
d	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
e	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
f	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

PRESENT S-box differential table

	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**	4	**0**	0	0	4	**0**	4	0	0	0	4	0	0
2	0	**0**	**0**	2	**0**	4	2	0	**0**	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	**0**	**0**	0	**0**	4	2	2	**0**	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	**0**	**0**	2	**0**	0	0	2	**0**	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
a	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
b	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
c	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
d	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
e	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
f	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

PUFFIN1/2 S-box differential table

	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	2	0	4	0	0	2	0	0	0	2	4	0	2	0	0
2	0	0	0	0	0	4	0	0	2	0	4	2	0	2	2	0
3	0	4	0	0	2	0	2	0	2	0	0	2	0	0	2	2
4	0	0	0	2	4	0	2	0	0	2	0	0	0	2	2	2
5	0	0	4	0	0	2	0	2	0	0	0	0	0	2	4	2
6	0	2	0	2	2	0	2	0	2	0	2	0	2	0	2	0
7	0	0	0	0	0	2	0	2	2	2	0	4	2	0	0	2
8	0	0	2	2	0	0	2	2	0	2	2	0	2	0	0	2
9	0	0	0	0	2	0	0	2	2	4	2	0	2	2	0	0
a	0	2	4	0	0	0	2	0	2	2	2	0	2	0	0	0
b	0	4	2	2	0	0	0	4	0	0	0	0	2	2	0	0
c	0	0	0	0	0	0	2	2	2	2	2	2	0	0	2	2
d	0	2	2	0	2	2	0	0	0	2	0	2	0	4	0	0
e	0	0	2	2	2	4	2	0	0	0	0	0	2	0	0	2
f	0	0	0	2	2	2	0	2	2	0	0	0	2	0	2	2

PUFFIN1/2 S-box differential table

	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	**2**	**0**	4	**0**	0	2	0	**0**	0	2	4	0	2	0	0
2	0	**0**	**0**	0	**0**	4	0	0	**2**	0	4	2	0	2	2	0
3	0	4	0	0	2	0	2	0	2	0	0	2	0	0	2	2
4	0	**0**	**0**	2	**4**	0	2	0	**0**	2	0	0	0	2	2	2
5	0	0	4	0	0	2	0	2	0	0	0	0	0	2	4	2
6	0	2	0	2	2	0	2	0	2	0	2	0	2	0	2	0
7	0	0	0	0	0	2	0	2	2	2	0	4	2	0	0	2
8	0	**0**	**2**	2	**0**	0	2	2	**0**	2	2	0	2	0	0	2
9	0	0	0	0	2	0	0	2	2	4	2	0	2	2	0	0
a	0	2	4	0	0	0	2	0	2	2	2	0	2	0	0	0
b	0	4	2	2	0	0	0	4	0	0	0	0	2	2	0	0
c	0	0	0	0	0	0	2	2	2	2	2	2	0	0	2	2
d	0	2	2	0	2	2	0	0	0	2	0	2	0	4	0	0
e	0	0	2	2	2	4	2	0	0	0	0	0	2	0	0	2
f	0	0	0	2	2	2	0	2	2	0	0	0	2	0	2	2

Best differential trails and security margins

Best differential trails:

- 14-round PRESENT: 2^{-62},
- 14-round PUFFIN1/2 : 2^{-28},
- 31-round PUFFIN1/2 : 2^{-62}.

Best known differential attack:

- 18-round PRESENT,
- ?31+4?-round PUFFIN1/2 .

Summary

Using a single differential

Attacks on PUFFIN (32 rounds / 128-bit key)

r'	$\Pr[\delta_0 \to \delta_r]$	N	Time C.	P_S
3	$2^{-53.59}$	$2^{57.49}$	$2^{85.10}$	0.75
4	$2^{-52.07}$	$2^{56.04}$	$2^{76.84}$	0.79
5	$2^{-49.71}$	$2^{52.45}$	$2^{101.95}$	0.85

Attacks on PUFFIN2 (34 rounds / 80-bit key)

r'	$\Pr[\delta_0 \to \delta_r]$	N	Time C.	P_S
3	$2^{-57.90}$	$2^{61.25}$	$2^{61.35}$	0.75
4	$2^{-56.35}$	$2^{59.47}$	$2^{60.07}$	0.63
5	$2^{-53.59}$	$2^{55.60}$	$2^{70.21}$	0.87

Attacks proposed on PUFFIN and PUFFIN2

Attacks on PUFFIN (32 rounds / 128-bit key)

r'	$\lvert\Delta\rvert$	N	Time C.	P_S
4	830	$2^{52.16}$	$2^{95.40}$	0.77
5	954	$2^{49.42}$	$2^{108.84}$	0.59

Attacks on PUFFIN2 (34 rounds / 80-bit key)

r'	$\lvert\Delta\rvert$	N	Time C.	P_S
4	115	$2^{55.58}$	$2^{64.66}$	0.58
5	210	$2^{52.30}$	$2^{74.78}$	0.78

- Both PUFFIN and PUFFIN2 are broken.
- Are 36 rounds safe ?

Attacks proposed on PUFFIN and PUFFIN2

Attacks on PUFFIN (32 rounds / 128-bit key)

r'	$\lvert\Delta\rvert$	N	Time C.	P_S
4	830	$2^{52.16}$	$2^{95.40}$	0.77
5	954	$2^{49.42}$	$2^{108.84}$	0.59

Attacks on PUFFIN2 (34 rounds / 80-bit key)

r'	$\lvert\Delta\rvert$	N	Time C.	P_S
4	115	$2^{55.58}$	$2^{64.66}$	0.58
5	210	$2^{52.30}$	$2^{74.78}$	0.78

- Both PUFFIN and PUFFIN2 are broken.
- Are 36 rounds safe ?
  - No: at least 39 rounds are required.

Summary

Conclusion

cipher (key bits)	rnds	Data C.	Time C.	Success P.	
PUFFIN (128)	32	2^{58}	2^{124}	> 0.25	[Leander11]
PUFFIN (128)	32	$2^{52.16}$	$2^{95.40}$	0.77	this work
PUFFIN (128)	32	$2^{49.42}$	$2^{108.84}$	0.59	this work
PUFFIN2 (80)	34	$2^{55.58}$	$2^{64.66}$	0.58	this work
PUFFIN2 (80)	34	$2^{52.30}$	$2^{74.78}$	0.78	this work

PUFFIN and PUFFIN2 were claimed to be secure against linear and differential attacks.

Why ?

- x Only considering one differential trail.
- x Implicitly assuming that attacker will only invert one round.

Differentials used, probability estimates . . .

. . . and matlab code can be found on my website.

`www.benoitgerard.com/LC2011.html`