Design of Lightweight S-Boxes

Anne Canteaut

Sébastien Duval

Gaëtan Leurent

Léo Perrin

Sebastien.Duval@inria.fr

December 15, 2017

Table of Contents

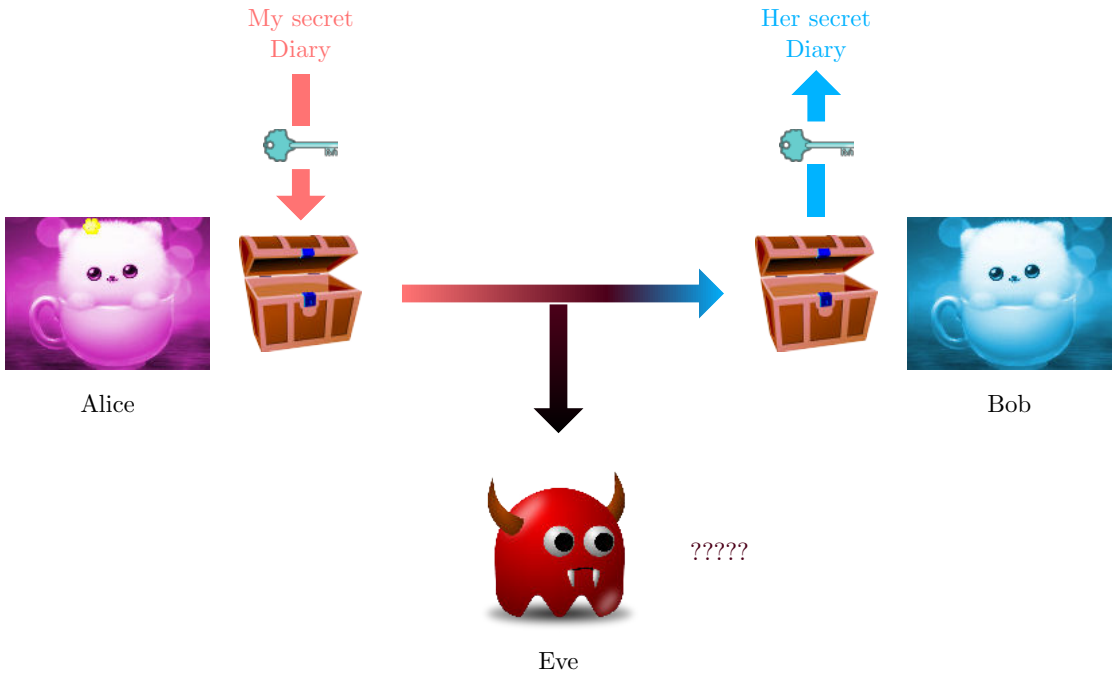
1 Introduction

2 4- to 8-bit S-Boxes

3 3- to 6-bit S-Boxes

4 Conclusion

Symmetric Encryption

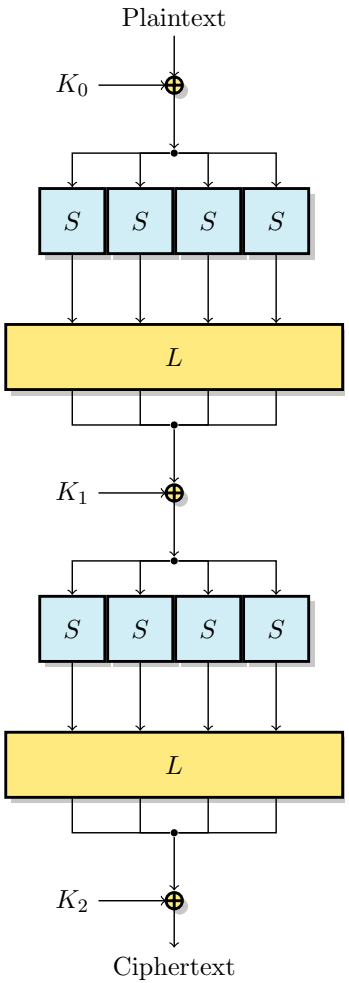


Security of Block Ciphers

Shannon's criteria

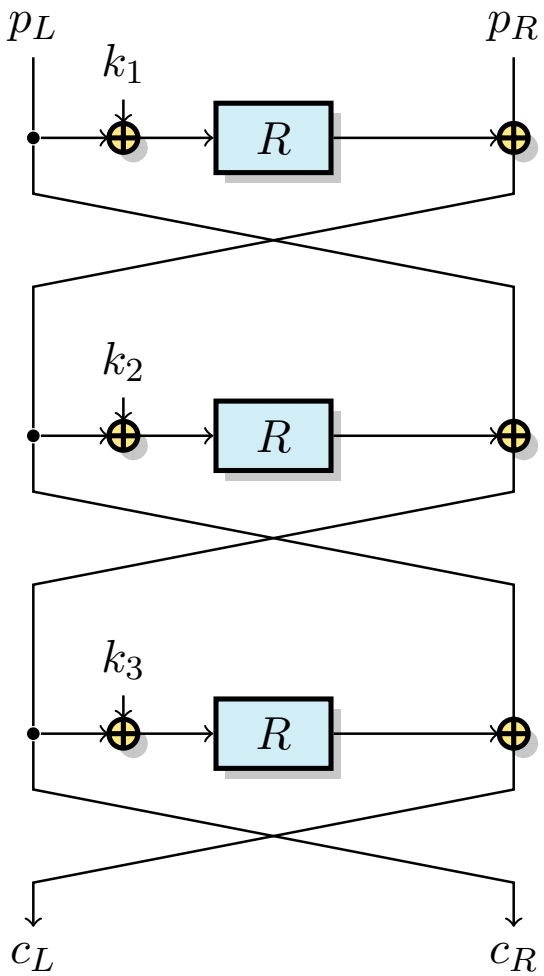
1. Diffusion
   - Every bit of plaintext and key must affect every bit of the output
   - We usually use linear functions
2. Confusion
   - Relation between plaintext and ciphertext must be intractable
   - Requires non-linear operations
   - Often implemented with tables: S-Boxes

SPN Ciphers



- Rijndael/AES (J. Daemen, V. Rijmen, 1988)
- Succession of confusion/diffusion layers
- Good for parallelism and easy to implement

Feistel Ciphers



- Lucifer (H. Feistel, D. Coppersmith, 1973), then DES
- Reduce the problem to half the size
- Fast (but sequential), cheap to implement
- Almost involutory

S-Box

Definition 1 (S-Box)

We will call *Substitution-Box* or *S-Box* any mapping from $\mathbb{F}_2^m$ into $\mathbb{F}_2^n$, $n, m \geq 0$.

Main Desirable Properties

- Permutation ($\Rightarrow n = m$)
- Non-linear ($\Rightarrow n$ small)
- Resistant to differential attacks
- Resistant to linear attacks
- High algebraic degree

Differential Properties

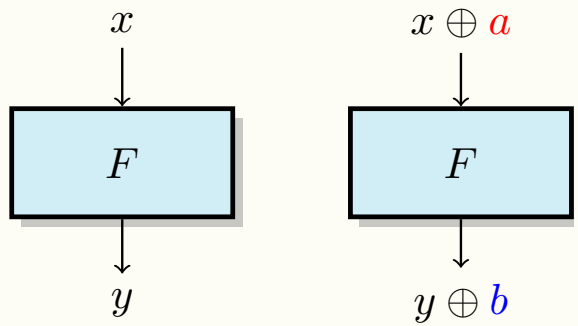
Definition 2 (Differential Uniformity)

Let F be a function over $\mathbb{F}_2^n$. The table of differences of F is:

$$\delta_F(a, b) = \#\{x \in \mathbb{F}_2^n \mid F(x \oplus a) \oplus F(x) = b\}.$$

Moreover, the differential uniformity of F is

$$\boldsymbol{\delta(F)} = \max_{a \neq 0, b} \delta_F(a, b).$$



- F is resistant against differential attacks if $\delta(F)$ is small
- F is called APN if $\delta(F) = 2$

Table of Differences

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	2	0	0	0	0	2	2	0	4	0	4	2	0	0
2	0	0	2	4	2	0	0	0	2	4	0	0	0	0	2	0
3	0	2	2	0	4	0	0	0	2	0	0	2	0	0	4	0
4	0	2	0	0	0	0	0	2	0	4	0	2	4	2	0	0
5	0	4	0	0	2	0	0	2	0	0	0	4	0	2	2	0
6	0	0	0	4	0	4	0	0	0	4	4	0	0	0	0	0
7	0	0	2	0	0	4	0	2	2	4	0	0	0	2	0	0
8	0	2	2	2	0	2	0	0	2	0	0	0	2	0	2	2
9	0	0	2	2	2	0	2	0	0	0	0	0	0	2	2	4
10	0	4	2	0	0	0	4	2	0	0	2	0	0	0	0	2
11	0	0	0	0	0	2	2	0	0	0	2	2	2	4	2	0
12	0	0	2	2	2	2	0	0	2	0	0	2	2	0	0	2
13	0	0	0	2	2	0	2	2	2	0	0	0	0	0	2	4
14	0	0	0	0	0	0	4	0	2	0	2	4	0	2	0	2
15	0	2	0	0	2	2	2	4	0	0	2	0	2	0	0	0

Remark

All the values are even:

$$S(x) \oplus S(x \oplus a) = b \iff S((x \oplus a) \oplus a) \oplus S(x \oplus a) = b$$

The Big APN Problem

The Big APN Problem

We know how to get:

- APN functions on $\mathbb{F}_2^n$,
- APN permutations on $\mathbb{F}_2^n$, n odd,
- permutations with $\delta = 4$ on $\mathbb{F}_2^n$.

Are there any APN permutations on $\mathbb{F}_2^n$, n even ?

2009: Dillon S-Box

Browning, Dillon, McQuistan, Wolfe: APN permutation on $\mathbb{F}_2^6$.

The Still Big APN Problem

Are there any other APN permutations on $\mathbb{F}_2^n$, n even ?

Linear Properties

Definition 3 (Linearity)

Let F be a function over $\mathbb{F}_2^n$. The linear approximation table (LAT) of F is the matrix λ_F:

$$\lambda_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot F(x)}.$$

Moreover, the linearity of F is

$$\mathcal{L}(F) = \max_{a,b \neq 0} |\lambda_F(a,b)|.$$

- F is resistant to linear attacks if $\mathcal{L}(F)$ is small

Lightweight S-Boxes (1)

The S-Box is the most costly component of a blockcipher.
Main reason: no structure.

Generic implementation

Table of images:

$$[5, 7, 10, 15, 2, 3, 1, 8, 0, 9, 11, 14, 12, 6, 13, 5]$$

Cost to implement an n-bit function: $n2^n$
Example:

- 64-bit function: $2^{70} =$ zettabit $= 2^{30}\,Tb$ (maybe Google has it).
- 8-bit function: $2^{11} = 2Kb$ (a bit large).
- 4-bit function: $2^6 = 64$ bits (small).

Lightweight S-Boxes (2)

In this work

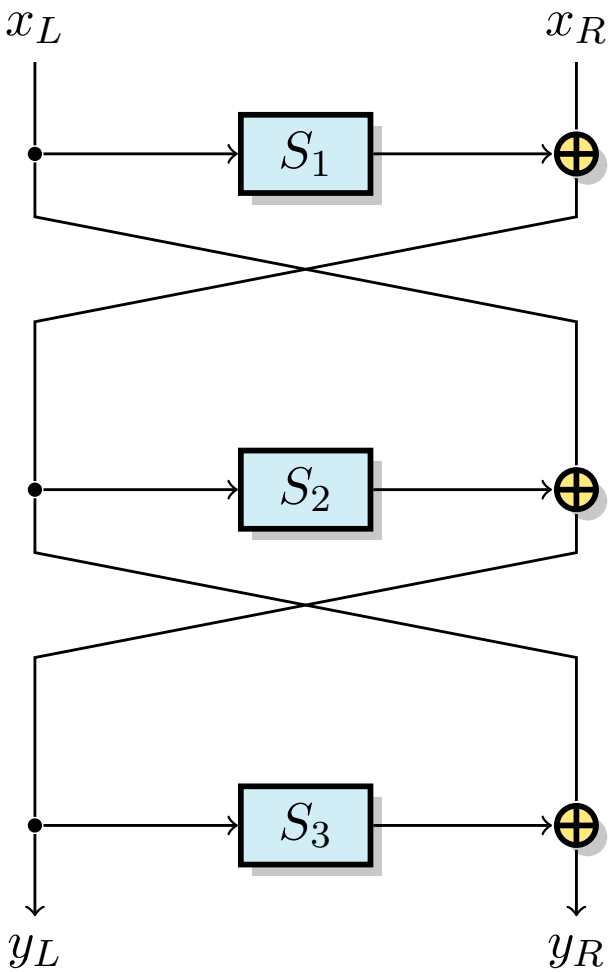
Cryptographically strong S-Boxes with a structure.
Technic: Build a big S-Box from smaller ones.
Example:

- 8-bit function: $2^{11} = 2Kb$ (a bit large).
- 3 4-bit functions: $3 \times 2^6 = 192$ bits (small).

We will study 3 structures: Feistel networks, MISTY-like networks, Butterflies.
$\Rightarrow$ Cryptographically strong S-Boxes
$\Rightarrow$ $2n$-bit functions from n-bit functions

4- to 8-bit S-Boxes

3-round Feistel: previous results

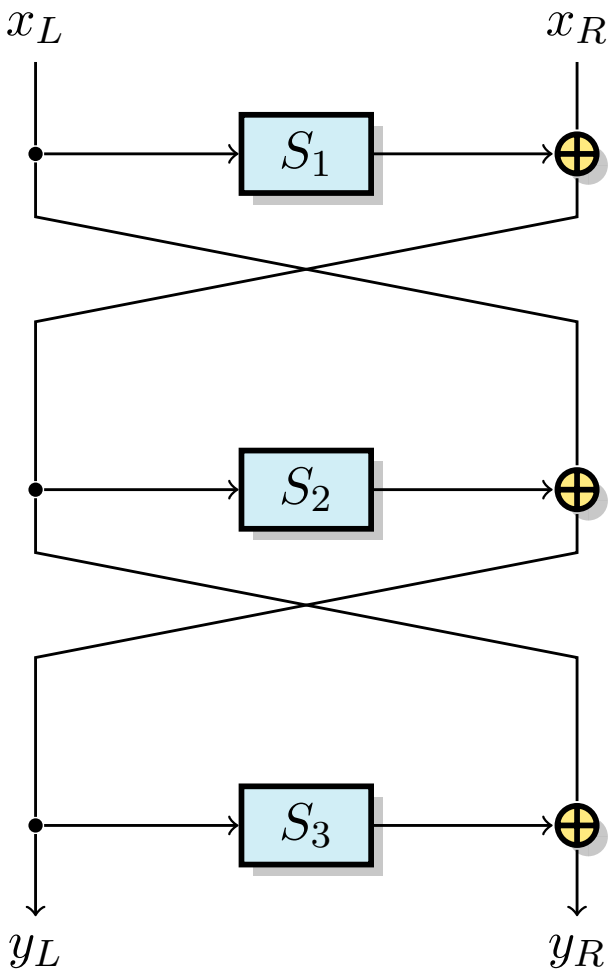


Li and Wang (CHES 2014):

- $\delta(F) \geq 2\delta(S_2)$
- $\delta(F) \geq 2^{n+1}$ if S_2 is not a permutation

- If $n = 4$:
- $\delta(F) \geq 8$, and if $\delta(F) = 8$, then $\mathcal{L}(F) \geq 64$
- $\delta(F) = 8$ and $\mathcal{L}(F) = 64$ is obtainable

3-round Feistel: Results

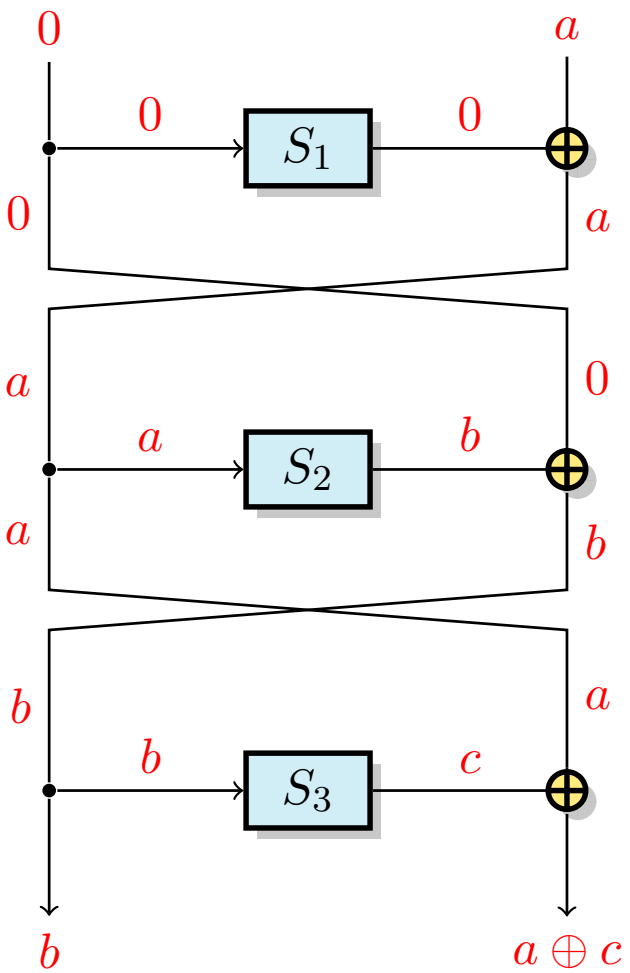


Canteaut, Duval, Leurent (SAC 2015):

- $\delta(F) \geq \delta(S_2) \max(\delta_{min}(S_1), \delta_{min}(S_3))$
- $\delta(F) \geq 2^{n+1}$ if S_2 is not a permutation
- $\delta(F) \geq \max_{i\neq 2, j\neq i,2}(\delta(S_i)\delta_{min}(S_j), \delta(S_i)\delta_{min}(S_2^{-1}))$ if S_2 is a permutation where $\delta_{min}(S) = \min_{a\neq 0} \max_b \delta_S(a \to b)$
- These bounds involve all 3 S-Boxes

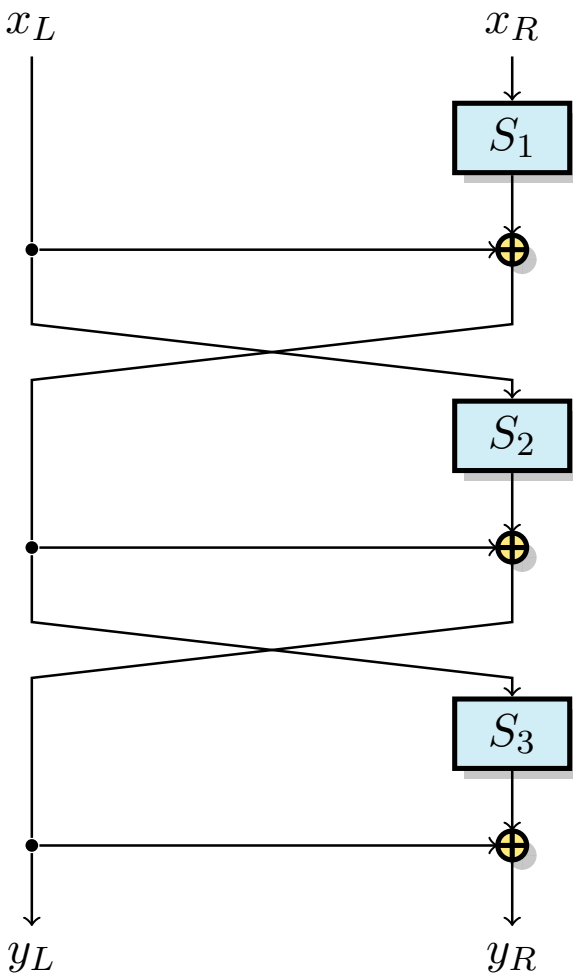
- If $n = 4$: Best permutation has $\delta(F) = 8$, $\mathcal{L}(F) = 64$.

Sketch of Proof



1. Prove that these differentials are the best for an attacker
2. One of S_i is canceled, simplifies the analysis
3. Prove that the equations have at least $\delta(S_2)\delta_{min}(S_3)$ solutions

3-round MISTY: Results



Canteaut, Duval, Leurent (SAC 2015):

- $\delta(F) \geq \delta(S_1) \max(\delta_{min}(S_2), \delta_{min}(S_3))$
- $\delta(F) \geq 2^{n+1}$ if S_1 is not a permutation
- $\delta(F) \geq \max_{i\neq 1, j\neq i,1}(\delta(S_i)\delta_{min}(S_j), \delta(S_i)\delta_{min}(S_1^{-1}))$ if S_1 is a permutation
  where $\delta_{min}(S) = \min_{a\neq 0} \max_b \delta_S(a \to b)$
- There was no previous result on MISTY with fixed key

- If $n = 4$: Best function has $\delta(F) = 8$, $\mathcal{L}(F) = 64$.
- If $n = 4$: Best permutation has $\delta(F) = 16$, $\mathcal{L}(F) = 64$.

Instanciating the 4-bit S-Boxes

Permutation with $\delta = 4$

- Easy search
  We use the results from Üllrich & al.
- 9 instructions
  - 4 non-linear
  - 4 XOR
  - 1 copy

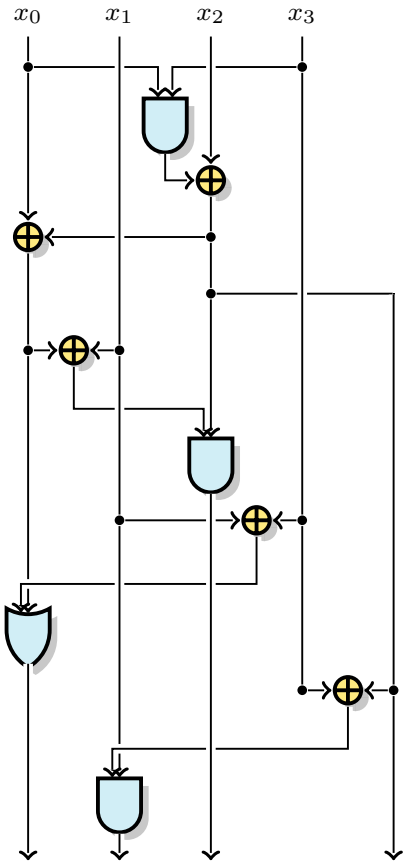
- 4 non-linear gates is optimal

APN function

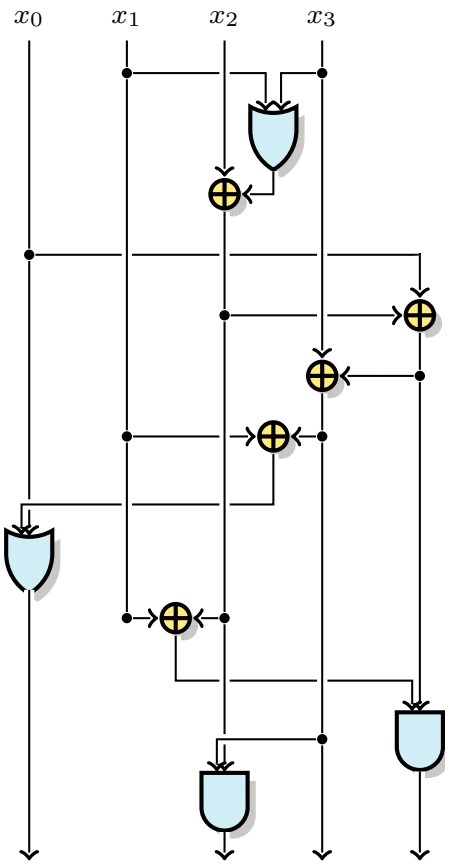
- Costly search
  - No filter for permutations
  - 6k core-hours
- 10 instructions
  - But 6 non-linear
- 11 instructions
  - 4 non-linear
  - 5 XOR
  - 2 copies

- 4 non-linear gates is optimal

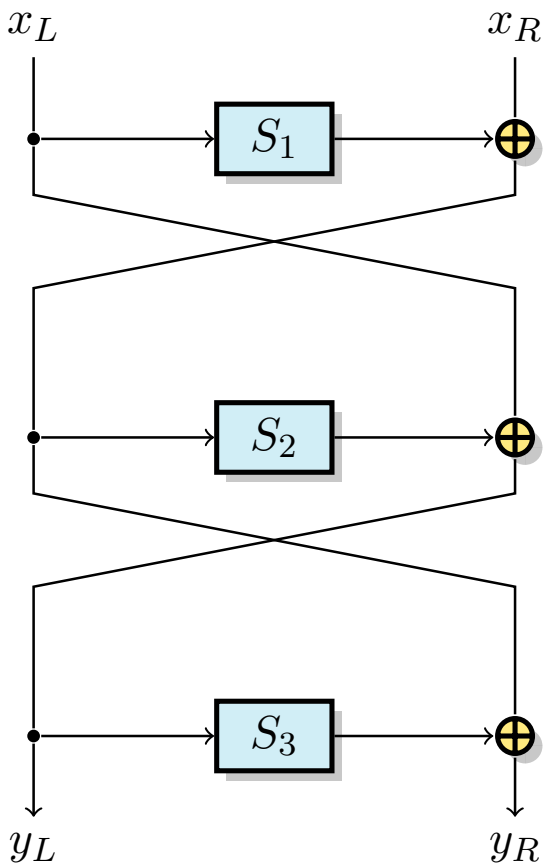
Instanciating the 8-bit S-Boxes



S_1 and S_3.

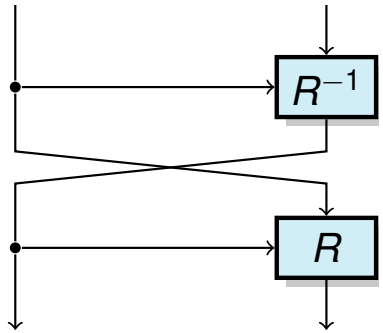


S_2.

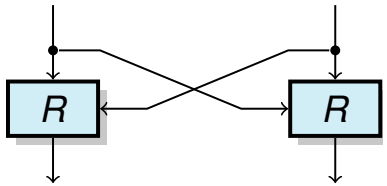


3- to 6-bit S-Boxes

Butterflies: Definitions (1) [Perrin et al.]



H_R: *Open Butterfly*



V_R: *Closed Butterfly*

$R_k : x \mapsto R(x, k)$ permutation $\forall k$.

Open Butterfly and Closed Butterfly are CCZ-equivalent $\Rightarrow$ share the same sets

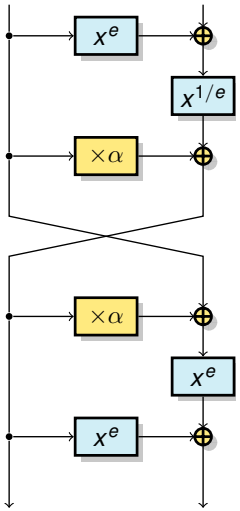
$$\{\delta_{H_R}(a,\, b)\}_{a,b} = \{\delta_{V_R}(a,\, b)\}_{a,b},$$

$$\{\mathcal{L}_{H_R}(a,\, b)\}_{a,b} = \{\mathcal{L}_{V_R}(a,\, b)\}_{a,b}.$$

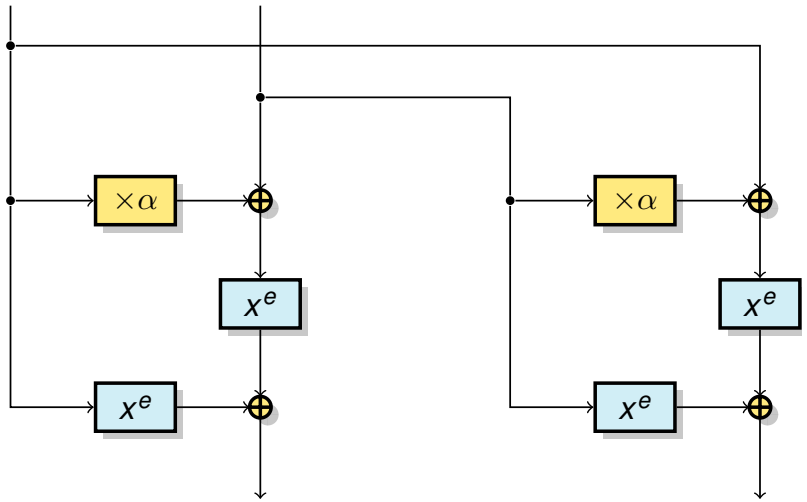
In particular, $\delta(H_R) = \delta(V_R)$ and $\mathcal{L}(H_R) = \mathcal{L}(V_R)$.

Butterflies: Definitions (2)

$$R_k[e, \alpha] = (x \oplus \alpha k)^e \oplus k^e, \text{ with } gcd(e, 2^n - 1) = 1.$$



H_R: *Open Butterfly*



V_R: *Closed Butterfly*

Most interesting case for study: $e = 3 \times 2^t$.
Then R is **quadratic**, and V_R is **quadratic**.

Butterflies: Properties

Theorem 1 (Properties of Butterflies)

Let $e = 3 \times 2^t$, $\alpha \notin \{0, 1\}$, *n odd.*

- $\delta(\mathrm{H}_R) \leq 4$, $\delta(\mathrm{V}_R) \leq 4$,
- V_R *is quadratic,*
- H_R *has algebraic degree* $n + 1$.

Theorem 2 (APN Butterflies)

If $n = 3$ *and* $x \mapsto x^e$ *is APN, then* H_R *is an APN permutation (affine equivalent to the Dillon permutation).*

Open Questions of [Perrin et al.]

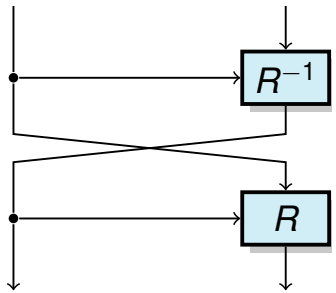
Open Questions of [Perrin et al.]

- Nonlinearity/Linearity of H_R (and V_R),
- Can we find α such that H_R is APN for some $n > 3$?

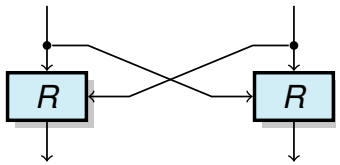
Butterflies: Results

- Generalisation of butterflies (quadratic case)
- Study of generalised butterflies
- Computed linearity of (generalised) butterflies
- Condition for APN $\Rightarrow$ No other APN butterflies

Generalised Butteflies: Definitions



$H_{\alpha,\beta}$: *Open Butterfly*



$V_{\alpha,\beta}$: *Closed Butterfly*

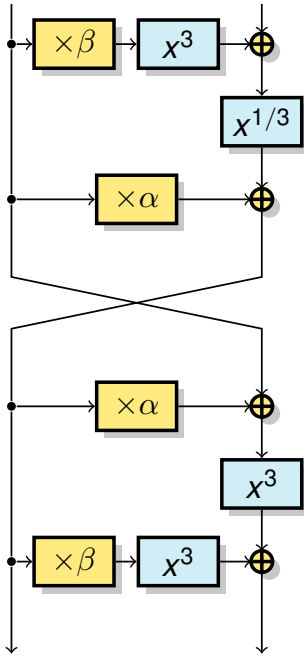
Degree restriction:

- $R_y : x \mapsto R(x, y)$ permutation $\forall y$.
- Degree of R is at most 3:
- Then R can be written:

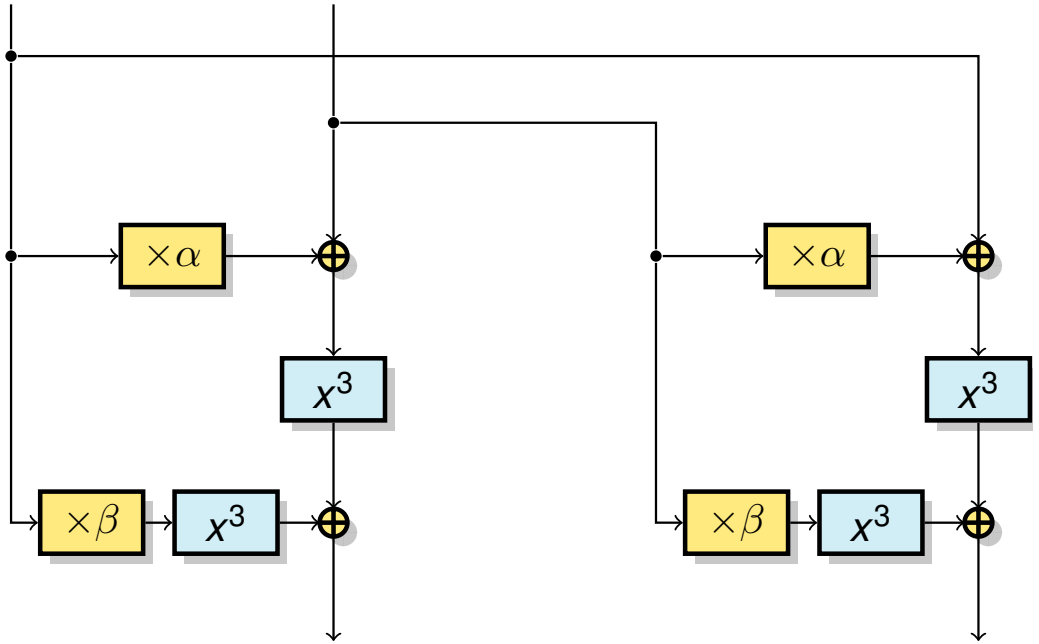
$$R(x, y) = (x \oplus \alpha y)^3 \oplus \beta y^3$$

with $\alpha, \beta \in \mathbb{F}_2^n$.

Generalised Butterflies: Definitions (2)



$H_{\alpha,\beta}$: *Open Butterfly*



$V_{\alpha,\beta}$: *Closed Butterfly*

Equivalences

- $H_{\alpha,\beta}$ and $V_{\alpha,\beta}$ are CCZ-equivalent.
- When $\alpha = 1$, $H_{\alpha,\beta}$ is equivalent to a 3-round Feistel network.

- Butterfly with $e = 3 \times 2^t$ is affine-equivalent to Butterfly with $e = 3$.
- $V_{\alpha,\beta}$ and V_{α^2,β^2} are affine-equivalent.
- If $\alpha \neq 1$, $V_{\alpha,\beta}$ and $V_{\alpha,\beta^{-1}(1+\alpha)^6}$ are affine-equivalent.

Property of Quadratic Functions

Property 1 (Linearity of Quadratic Functions)

Let f be a quadratic Boolean function of n variables.

$$\mathrm{LS}(f) = \{a \in \mathbb{F}_2^n : D_a f \text{ is constant}\}$$

Then $\mathcal{L}(f) = 2^{\frac{n+s}{2}}$, *with* $s = \dim \mathrm{LS}(f)$.

Moreover, the Walsh coefficients of f only the values $\pm 2^{\frac{n+s}{2}}$ *and* 0.

Linear Properties

Theorem 3

Let $n > 1$ be an odd integer and (α, β) be a pair of nonzero elements in $\mathbb{F}_{2^n}$.

- *If $\beta \neq (1+\alpha)^3$,*

$$\mathcal{L}(V_{\alpha,\beta}) = 2^{n+1}$$

and the Walsh coefficients of $V_{\alpha,\beta}$ belong to $\{0, \pm 2^n, \pm 2^{n+1}\}$.

- *If $\beta = (1+\alpha)^3$,*

$$\mathcal{L}(V_{\alpha,\beta}) = 2^{\frac{3n+1}{2}}.$$

Differential Properties

Theorem 4 (Differential uniformity)

Let $n > 1$ odd, $\alpha, \beta \in \mathbb{F}_{2^n} \setminus \{0\}$. Then:

- *If $\beta \neq (1+\alpha)^3$, $\delta(\mathrm{H}_{\alpha,\beta}) \leq 4$.*
- *If $\beta = (1+\alpha)^3$, $\delta(\mathrm{H}_{\alpha,\beta}) = 2^{n+1}$.*

Theorem 5 (APN Condition)

Let $\alpha \neq 0, 1$. $\mathrm{H}_{\alpha,\beta}$ is APN if and only if:

$$\beta \in \{(\alpha+\alpha^3), (\alpha^{-1}+\alpha^3)\} \text{ and } \mathrm{Tr}\left(\mathcal{A}_\alpha(e)\right) = 1, \forall\ e \notin \{0, \alpha, 1/\alpha\},$$

where $\mathcal{A}_\alpha(e) = \frac{e\alpha(1+\alpha)^2}{(1+\alpha e)(\alpha+e)^2}$.

This condition implies that $n = 3$.

Differential Properties

Theorem 4 (Differential uniformity)

Let $n > 1$ odd, $\alpha, \beta \in \mathbb{F}_{2^n} \setminus \{0\}$. Then:

- *If $\beta \neq (1+\alpha)^3$, $\delta(\mathrm{H}_{\alpha,\beta}) \leq 4$.*
- *If $\beta = (1+\alpha)^3$, $\delta(\mathrm{H}_{\alpha,\beta}) = 2^{n+1}$.*

Theorem 5 (APN Condition)

Let $\alpha \neq 0, 1$. $\mathrm{H}_{\alpha,\beta}$ is APN if and only if:

$$\beta \in \{(\alpha+\alpha^3), (\alpha^{-1}+\alpha^3)\} \text{ and } \mathrm{Tr}\left(\mathcal{A}_\alpha(e)\right) = 1, \forall\ e \notin \{0, \alpha, 1/\alpha\},$$

where $\mathcal{A}_\alpha(e) = \frac{e\alpha(1+\alpha)^2}{(1+\alpha e)(\alpha+e)^2}$.

This condition implies that $n = 3$.

Spectra: $\alpha = 1$ (3-round Feistel Network)

Proposition 1

For $\alpha = \beta = 1$, the difference distribution tables of the butterflies $V_{1,1}$ and $H_{1,1}$ contain the values 0 and 4 only.

Spectra: Generalised Butterflies

Corollary 6 (Walsh and differential spectra of generalised butterflies)

Let α and β be two nonzero elements in $\mathbb{F}_{2^n}$ such that $\beta \neq (1+\alpha)^3$.

- *Walsh spectrum:*

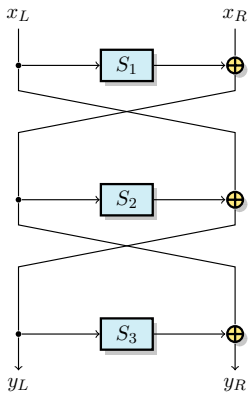
$$\left|\widehat{\mathrm{H}_{\alpha,\beta}}(u,v)\right| = \begin{cases} 0, & 3\times 2^{2n-2}(2^n-1)(2^n+1-C) \text{ times} \\ 2^n, & 2^{2n}(2^n-1)C \text{ times} \\ 2^{n+1}, & 2^{2n-2}(2^n-1)(2^n+1-C) \text{ times.} \end{cases}$$

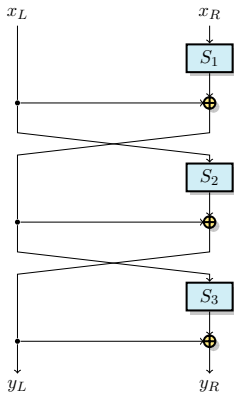
where $(2^n-1)C$ is the number of bent components of $\mathrm{V}_{\alpha,\beta}$.

- *Table of differences:*

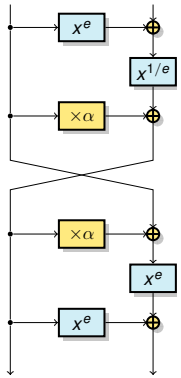
$$\delta_{\mathrm{H}_{\alpha,\beta}}(a,b) = \begin{cases} 2, & 2^{2n-2}(2^n-1)\times 3C \text{ times} \\ 4, & 2^{2n-3}(2^n-1)(2^{n+2}+4-3C) \text{ times} \end{cases}$$

Comparison





- For any n.
- Good cryptographic properties
- $\delta(F) \geq 2\delta(S)$, $\mathcal{L}(F) \geq \mathcal{L}(S)^2$
- If $n = 4$:
  $\delta(F) = 8$, $\mathcal{L}(F) = 64$.
- Cost: $3n2^n$ bits of memory



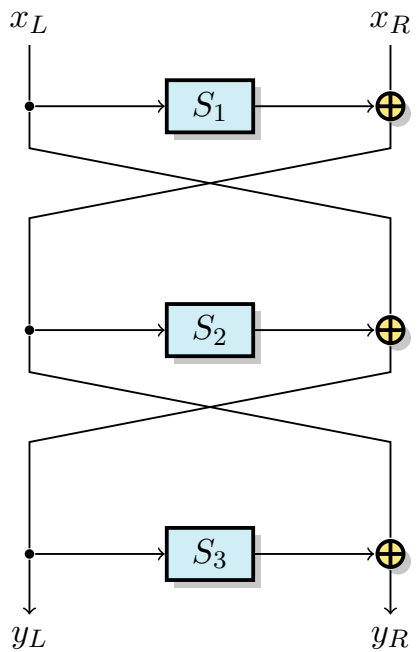
- For odd n
- Excellent cryptographic properties
- $\delta(F) \leq 4$, $\mathcal{L}(F) \leq 2^{n+1}$
- If $n = 3$:
  $\delta(F) = 2$, $\mathcal{L}(F) = 16$.
- Cost: $4n2^n$ bits of memory

Conclusion

- For any n.

- Good cryptographic properties
- Cost: $3n2^n$ bits of memory

Overall: 3-round Feistel



- For odd n

- Butterfly with $\alpha = 1 \Leftrightarrow$ 3-round Feistel
- Excellent cryptographic properties
- Cost: $3n2^n$ bits of memory

Open Problems

- Feistel-Butterflies (when $\alpha = 1$): What happens for n even?
- MISTY-like networks with a multiplication by α?
- Prove upper bounds for δ an $\mathcal{L}$ for Feistel and MISTY
- Feistel and MISTY with 4 rounds?

Questions ?