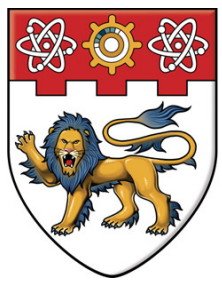
SoK: PEIGEN – a Platform for Evaluation, Implementation, and Generation of S-boxes

Zhenzhen Bao Jian Guo San Ling Yu Sasaki



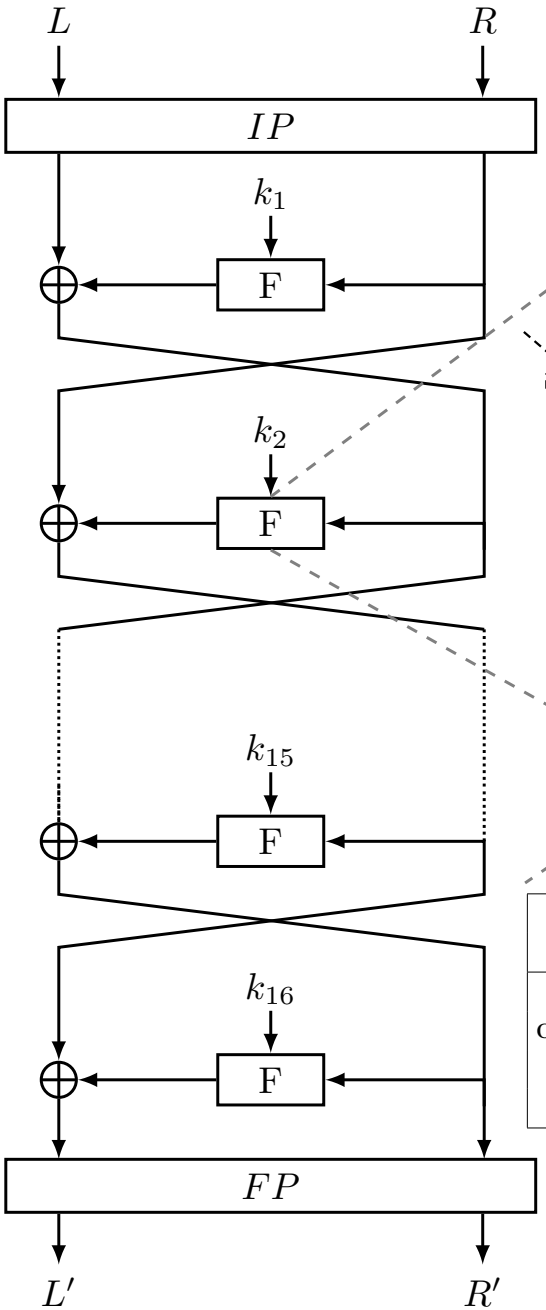
NANYANG TECHNOLOGICAL UNIVERSITY

NTT

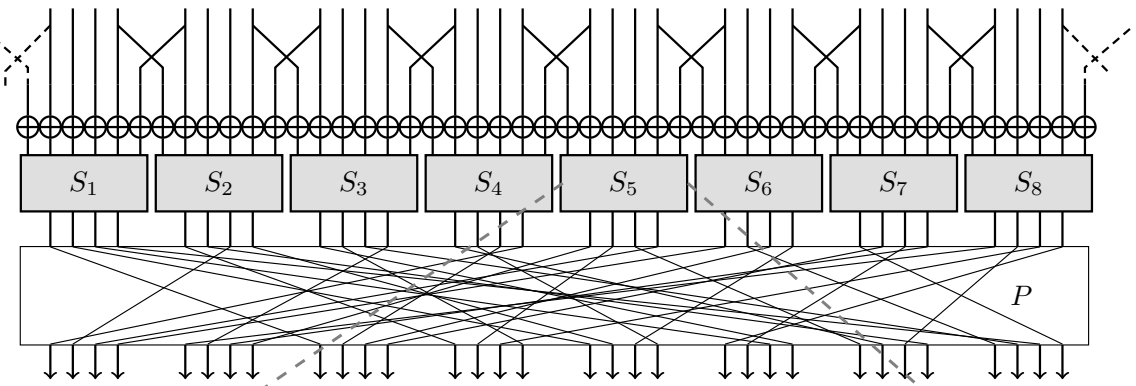
FSE 2019 – March 27, 2019 @ Paris, France

Outline

S(ubstitution)-boxes



The old Shannon idea: sequential application of **Confusion** and **Diffusion**



S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

This figure is modified from https://www.iacr.org/authors/tikz/

PEIGEN– a **P**latform for **E**valuation, **I**mplemention, and **GEN**eration of S-boxes

For n-bit S-boxes ($3 \leq n \leq 8$):

1. **Evaluation**: given a set of n-bit S-boxes, evaluate security-related properties:
   - DDT, LAT, BCT, ACT, ANF, LS, $\mathcal{V}_S(u)$, (v, w)-linearity
   - Equivalence relations: PXE, LE, AE
2. **Implementation**: given a set of n-bit S-boxes and the specific implementation configuration, generate implementations which are good in terms of
   - `BGC`, `GEC`, `MC`, and `Depth`
3. **Generation**: given a set of criteria,
   - if together with a set of S-boxes, filter out S-boxes fulfilling the given criteria
   - generate new S-boxes fulfilling the given criteria

Done efficiently:

Only efficient for $n = 3, 4$:

Not support yet:

S-boxes

An S-box mapping n bits to m bits – a vectorial Boolean function in n variables and with m output bits:

$$S : \mathbb{F}_2^n \to \mathbb{F}_2^m$$

Coordinates of an S-box S [Nyb94]

An S-box S in n variables and with m output bits has m coordinates:

$$S_{e_i} : \mathbb{F}_2^n \to \mathbb{F}_2,$$

where $\{e_i\}_{i<m}$ is the standard basis for $\mathbb{F}_2^m$ for $1 \leq i \leq m$.

S-boxes

Table representation of an S-box S

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

Bit-sliced representation of an S-box S

$S(x)$	3	8	F	1	A	6	5	B	E	D	4	2	7	0	9	C	Hex
S_{e_4}	0	1	1	0	1	0	0	1	1	1	0	0	0	0	1	1	C396
S_{e_3}	0	0	1	0	0	1	1	0	1	1	1	0	1	0	0	1	9764
S_{e_2}	1	0	1	0	1	1	0	1	1	0	0	1	1	0	0	0	19B5
S_{e_1}	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1	0	52CD

S-boxes

Algebraic Normal Form (ANF) of a Boolean function [Can16]

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented by an n-variate polynomial over $\mathbb{F}_2$, named the *algebraic normal form* of f:

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} \alpha_u \prod_{i=1}^{n} x_i^{u_i}, \text{ where } \alpha_u \in \mathbb{F}_2.$$

From bit-sliced representation to ANF and vice versa:

$$\alpha_u = \bigoplus_{x \preceq u} f(x) \text{ and } f(x) = \bigoplus_{u \preceq x} \alpha_u,$$

$$\text{where } x \preceq u \text{ iff } x_i \leq u_i \; \forall \; 1 \leq i \leq n.$$

$$\begin{aligned}
S_{e_4} &= 1 + x_0 + x_1 + x_2 + x_3 + x_0x_3 + x_1x_3 + x_0x_1x_2 + x_1x_2x_3 \\
S_{e_3} &= 1 + x_1 + x_3 + x_0x_1 + x_0x_2 + x_1x_3 + x_0x_1x_2 + x_1x_2x_3 \\
S_{e_2} &= x_0 + x_0x_2 + x_1x_2 + x_1x_3 + x_0x_1x_2 + x_0x_2x_3 + x_1x_2x_3 \\
S_{e_1} &= x_0 + x_2 + x_3 + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 + x_0x_2x_3 + x_1x_2x_3
\end{aligned}$$

In this example, we start from 0 to index input variables, different with the above definition

S-boxes

Components of an S-box S [Nyb94]

An S-box S with n input bits and m output bits has 2^m components, which are the linear combinations of its m coordinates:

$$\begin{array}{rccc} S_\lambda : & \mathbb{F}_2^n & \to & \mathbb{F}_2 \\ & x & \mapsto & \lambda \cdot S(x) \end{array} \qquad \lambda \in \mathbb{F}_2^m$$

where $a \cdot b$ is the inner product of a and b, *i.e.*, $\bigoplus_{i=1}^{n} a_i \cdot b_i$.

An S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is said to be *balanced* if it takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times

Balancedness characterized by components [Car10]

An S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is balanced if and only if all its non-trivial component functions are balanced.

A balanced vectorial Boolean function mapping $\mathbb{F}_2^n$ to itself is an n-bit *permutation*.

Outline

Resistance to Differential Cryptanalysis (DC)

Derivative of S [Nyb91]

For a vectorial Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the derivative of S to the direction $a \in \mathbb{F}_2^n$ is defined as

$$\begin{array}{rccc} D_a S : & \mathbb{F}_2^n & \to & \mathbb{F}_2^m \\ & x & \mapsto & S(x) \oplus S(x \oplus a) \end{array}$$

Difference Distribution Table (DDT)

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

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	·	·	4	·	·	·	4	·	4	·	·	·	4	·	·
2	·	·	·	2	·	4	2	·	·	·	2	·	2	2	2	·
3	·	2	·	2	2	·	4	2	·	·	2	2	·	·	·	·
4	·	·	·	·	·	4	2	2	·	2	2	·	2	·	2	·
5	·	2	·	·	2	·	·	·	·	2	2	2	4	2	·	·
6	·	·	2	·	·	·	2	·	2	·	·	4	2	·	·	4
7	·	4	2	·	·	·	2	·	2	·	·	·	2	·	·	4
8	·	·	·	2	·	·	·	2	·	2	·	4	·	2	·	4
9	·	·	2	·	4	·	2	·	2	·	·	·	2	·	4	·
A	·	·	2	2	·	4	·	·	2	·	2	·	·	2	2	·
B	·	2	·	·	2	·	·	·	4	2	2	2	·	2	·	·
C	·	·	2	·	·	4	·	2	2	2	2	·	·	·	2	·
D	·	2	4	2	2	·	·	2	·	·	2	2	·	·	·	·
E	·	·	2	2	·	·	2	2	2	2	·	·	2	2	·	·
F	·	4	·	·	4	·	·	·	·	·	·	·	·	·	4	4

Difference Distribution Table (DDT)

$$\mathcal{U}(S) \triangleq \max_{a \in \mathbb{F}_2^n \setminus \{0\}, b \in \mathbb{F}_2^m} \delta_S(a,b)$$

$a \backslash b$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	·	·	4	·	·	·	4	·	4	·	·	·	4	·	·
2	·	·	·	2	·	4	2	·	·	·	2	·	2	2	2	·
3	·	2	·	2	2	·	4	2	·	·	2	2	·	·	·	·
4	·	·	·	·	·	4	2	2	·	2	2	·	2	·	2	·
5	·	2	·	·	2	·	·	·	·	2	2	2	4	2	·	·
6	·	·	2	·	·	·	2	·	2	·	·	4	2	·	·	4
7	·	4	2	·	·	·	2	·	2	·	·	·	2	·	·	4
8	·	·	·	2	·	·	·	2	·	2	·	4	·	2	·	4
9	·	·	2	·	4	·	2	·	2	·	·	·	2	·	4	·
A	·	·	2	2	·	4	·	·	2	·	2	·	·	2	2	·
B	·	2	·	·	2	·	·	·	4	2	2	2	·	2	·	·
C	·	·	2	·	·	4	·	2	2	2	2	·	·	·	2	·
D	·	2	4	2	2	·	·	2	·	·	2	2	·	·	·	·
E	·	·	2	2	·	·	2	2	2	2	·	·	2	2	·	·
F	·	4	·	·	4	·	·	·	·	·	·	·	·	·	4	4

Difference Distribution Table (DDT)

Differential Uniformity of S [Nyb93]

$$\mathcal{U}(S) \triangleq \max_{a \in \mathbb{F}_2^n \setminus \{0\}, b \in \mathbb{F}_2^m} \delta_S(a,b)$$

- $\mathcal{U}(S) \geq 2$ for any S-box.
- $\mathcal{U}(S) = 2$ for Almost Perfect Nonlinear (APN) functions.
- If $\mathcal{U}(S) \leq \delta$, S is called differentially δ-uniform.
- There is no APN Permutation on $\mathbb{F}_2^4$.
- Unknown if APN Permutations exist on $\mathbb{F}_2^n$ if n is even and $n \geq 8$.
- Hence, differentially 4-uniform are of great interest when n is even.

Difference Distribution Table (DDT)

The frequency of the maximum occurs in the DDT of an S-box:

$$\mathcal{U}_{\text{Freq}}(S) \triangleq \#\{(a,b) \mid \delta_S(a,b) = \mathcal{U}(S),\ a \in \mathbb{F}_2^n \setminus \{0\},\ b \in \mathbb{F}_2^m\}$$

Differential Spectrum [BCC10; CR15]

The *differential spectrum* of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the multiset

$$\mathcal{D}_{\text{spec}}(S) \triangleq \{\delta_S(a,b) \mid a \in \mathbb{F}_2^n \setminus \{0\}, b \in \mathbb{F}_2^m\}.$$

Difference Distribution Table (DDT)

$$\mathcal{D}_{\text{spec}}(S) \triangleq \{\delta_S(a,b) \mid a \in \mathbb{F}_2^n \setminus \{0\}, b \in \mathbb{F}_2^m\}.$$

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	·	·	4	·	·	·	4	·	4	·	·	·	4	·	·
2	·	·	·	2	·	4	2	·	·	·	2	·	2	2	2	·
3	·	2	·	2	2	·	4	2	·	·	2	2	·	·	·	·
4	·	·	·	·	·	4	2	2	·	2	2	·	2	·	2	·
5	·	2	·	·	2	·	·	·	·	2	2	2	4	2	·	·
6	·	·	2	·	·	·	2	·	2	·	·	4	2	·	·	4
7	·	4	2	·	·	·	2	·	2	·	·	·	2	·	·	4
8	·	·	·	2	·	·	·	2	·	2	·	4	·	2	·	4
9	·	·	2	·	4	·	2	·	2	·	·	·	2	·	4	·
A	·	·	2	2	·	4	·	·	2	·	2	·	·	2	2	·
B	·	2	·	·	2	·	·	·	4	2	2	2	·	2	·	·
C	·	·	2	·	·	4	·	2	2	2	2	·	·	·	2	·
D	·	2	4	2	2	·	·	2	·	·	2	2	·	·	·	·
E	·	·	2	2	·	·	2	2	2	2	·	·	2	2	·	·
F	·	4	·	·	4	·	·	·	·	·	·	·	·	·	4	4

$$\mathcal{U} = 4, \mathcal{D}_{\text{spec}} = \{0 : 159, 2 : 72, 4 : 24, 16 : 1\}$$

Resistance to Linear Cryptanalysis (LC)

Walsh transform of an S-box [Car10]

The *Walsh transform* of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is defined as:

$$\mathcal{W}_S(\alpha, \beta) = \mathcal{W}_{S_\beta}(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\beta \cdot S(x) \oplus \alpha \cdot x}, \quad \alpha \in \mathbb{F}_2^n, \ \beta \in \mathbb{F}_2^m.$$

The value taken by the transform at point (α, β) is called the *Walsh coefficient* of S at point (α, β).

Walsh coefficient $\sim$ Bias of linear approximations:

$$\mathcal{W}_S(\alpha, \beta) = 2^{n+1} \cdot \varepsilon_S(\alpha, \beta)$$

Linear Approximation Table (LAT)

$$\mathcal{W}_S(a,b) \triangleq \sum_{x \in \mathbb{F}_2^n} (-1)^{S_b(x)+\langle a,x \rangle}$$

$a \backslash b$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	·	·	·	·	−8	·	−8	·	·	·	·	·	−8	·	8
2	·	·	4	4	−4	−4	·	·	4	−4	·	8	·	8	−4	4
3	·	·	4	4	4	−4	−8	·	−4	4	−8	·	·	·	−4	−4
4	·	·	−4	4	−4	−4	·	8	−4	−4	·	−8	·	·	−4	4
5	·	·	−4	4	−4	4	·	·	4	4	−8	·	8	·	4	4
6	·	·	·	−8	·	·	−8	·	·	−8	·	·	8	·	·	·
7	·	·	·	8	8	·	·	·	·	−8	·	·	·	·	8	·
8	·	·	4	−4	·	·	−4	4	−4	4	·	·	−4	4	8	8
9	·	8	−4	−4	·	·	4	−4	−4	−4	−8	·	−4	4	·	·
A	·	·	8	·	4	4	4	−4	·	·	·	−8	4	4	−4	4
B	·	−8	·	·	−4	−4	4	−4	−8	·	·	·	4	4	4	−4
C	·	·	·	·	−4	−4	−4	−4	8	·	·	−8	−4	4	4	−4
D	·	8	8	·	−4	−4	4	4	·	·	·	·	4	−4	4	−4
E	·	·	4	4	−8	8	−4	−4	−4	−4	·	·	−4	−4	·	·
F	·	8	−4	4	·	·	−4	−4	−4	4	8	·	4	4	·	·

Resistance to Linear Cryptanalysis (LC)

Linearity of an S-box [Nyb94]

The *linearity* of a vectorial Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the maximum linearity of its non-trivial components $\{S_\beta \mid \beta \in \mathbb{F}_2^m \setminus \{0\}\}$.

$$\mathcal{L}(S) = \max_{\lambda \in \mathbb{F}_2^m \setminus \{0\}} \mathcal{L}(S_\beta) = \max_{\alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^m \setminus \{0\}} |\mathcal{W}_S(\alpha, \beta)| .$$

- $\mathcal{L}(S) \geq 2^{n/2}$, and equility cannot hold for permutation.
- For 4×4-bit bijective S-box S, $\mathcal{L}(S) \geq 8$ [LP07]

Linear Approximation Table (LAT)

$$\mathcal{L}(S) = \max_{\lambda \in \mathbb{F}_2^m \setminus \{0\}} \mathcal{L}(S_\beta) = \max_{\alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^m \setminus \{0\}} |\mathcal{W}_S(\alpha, \beta)|$$

$a \backslash b$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	·	·	·	·	−8	·	−8	·	·	·	·	·	−8	·	8
2	·	·	4	4	−4	−4	·	·	4	−4	·	8	·	8	−4	4
3	·	·	4	4	4	−4	−8	·	−4	4	−8	·	·	·	−4	−4
4	·	·	−4	4	−4	−4	·	8	−4	−4	·	−8	·	·	−4	4
5	·	·	−4	4	−4	4	·	·	4	4	−8	·	8	·	4	4
6	·	·	·	−8	·	·	−8	·	·	−8	·	·	8	·	·	·
7	·	·	·	8	8	·	·	·	·	−8	·	·	·	·	8	·
8	·	·	4	−4	·	·	−4	4	−4	4	·	·	−4	4	8	8
9	·	8	−4	−4	·	·	4	−4	−4	−4	−8	·	−4	4	·	·
A	·	·	8	·	4	4	4	−4	·	·	·	−8	4	4	−4	4
B	·	−8	·	·	−4	−4	4	−4	−8	·	·	·	4	4	4	−4
C	·	·	·	·	−4	−4	−4	−4	8	·	·	−8	−4	4	4	−4
D	·	8	8	·	−4	−4	4	4	·	·	·	·	4	−4	4	−4
E	·	·	4	4	−8	8	−4	−4	−4	−4	·	·	−4	−4	·	·
F	·	8	−4	4	·	·	−4	−4	−4	4	8	·	4	4	·	·

Resistance to Linear Cryptanalysis (LC)

The frequency of the maximum occurs in the LAT of an S-box:

$$\mathcal{L}_{\text{Freq}} \triangleq \#\{(\alpha,\beta) \mid \mathcal{W}_S(\alpha,\beta) = \mathcal{L}(S),\ \alpha \in \mathbb{F}_2^n,\ \beta \in \mathbb{F}_2^m \setminus \{0\}\}$$

Walsh spectrum of an S-box [Car10]

The *Walsh spectrum* of S is the multiset

$$\mathcal{W}_{\text{spec}}(S) \triangleq \{\mathcal{W}_S(\alpha,\beta) \mid \alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^m \setminus \{0\}\}.$$

The *extended Walsh spectrum* of S is the multi-set of the absolute of values in $\mathcal{W}_{\text{spec}}(S)$. The Walsh support of S is those (α,β) such that $\mathcal{W}(\alpha,\beta) \neq 0$.

Linear Approximation Table (LAT)

$$\mathcal{W}_{\text{spec}}(S) \triangleq \{\mathcal{W}_S(\alpha,\beta) \mid \alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^m \setminus \{0\}\}.$$

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	·	·	·	·	−8	·	−8	·	·	·	·	·	−8	·	8
2	·	·	4	4	−4	−4	·	·	4	−4	·	8	·	8	−4	4
3	·	·	4	4	4	−4	−8	·	−4	4	−8	·	·	·	−4	−4
4	·	·	−4	4	−4	−4	·	8	−4	−4	·	−8	·	·	−4	4
5	·	·	−4	4	−4	4	·	·	4	4	−8	·	8	·	4	4
6	·	·	·	−8	·	·	−8	·	·	−8	·	·	8	·	·	·
7	·	·	·	8	8	·	·	·	·	−8	·	·	·	·	8	·
8	·	·	4	−4	·	·	−4	4	−4	4	·	·	−4	4	8	8
9	·	8	−4	−4	·	·	4	−4	−4	−4	−8	·	−4	4	·	·
A	·	·	8	·	4	4	4	−4	·	·	·	−8	4	4	−4	4
B	·	−8	·	·	−4	−4	4	−4	−8	·	·	·	4	4	4	−4
C	·	·	·	·	−4	−4	−4	−4	8	·	·	−8	−4	4	4	−4
D	·	8	8	·	−4	−4	4	4	·	·	·	·	4	−4	4	−4
E	·	·	4	4	−8	8	−4	−4	−4	−4	·	·	−4	−4	·	·
F	·	8	−4	4	·	·	−4	−4	−4	4	8	·	4	4	·	·

$\mathcal{L} = 8$, Extended $\mathcal{W}_{\text{spec}} = \{0 : 123, 4 : 96, 8 : 36, 16 : 1\}$

Resistance to DC and LC

For Ciphers with Bit-Permutation Linear Layer

The differential branch number of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathcal{BN}_{\mathrm{D}}(S) = \min\{\mathrm{wt}(a)+\mathrm{wt}(b) \mid \delta_S(a,b) \neq 0,\ a \in \mathbb{F}_2^n \setminus \{0\},\ b \in \mathbb{F}_2^m\}.$$

The linear branch number of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathcal{BN}_{\mathrm{L}}(S) = \min\{\mathrm{wt}(u) + \mathrm{wt}(v) \mid \mathcal{W}_S(u,v) \neq 0,\ u \in \mathbb{F}_2^n,\ v \in \mathbb{F}_2^m \setminus \{0\}\}.$$

$\mathrm{DDT}_1(S)$

The sub-table of DDT containing entries (a, b) where $\mathrm{wt}(a) = \mathrm{wt}(b) = 1$.

$\mathrm{LAT}_1(S)$

The sub-table of LAT containing entries (u, v) where $\mathrm{wt}(u) = \mathrm{wt}(v) = 1$.

Resistance to DC and LC

For Ciphers with Bit-Permutation Linear Layer

$\mathcal{U}_1(S)$ and $\mathcal{L}_1(S)$ [LP07]

$$\mathcal{U}_1(S) = \max_{a \in \mathbb{F}_2^n \setminus \{0\}, b \in \mathbb{F}_2^m} \{\delta_S(a,b) \mid \mathrm{wt}(a) = \mathrm{wt}(b) = 1\},$$

$$\mathcal{L}_1(S) = \max_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m \setminus \{0\}} \{\mathcal{W}_S(a,b) \mid \mathrm{wt}(a) = \mathrm{wt}(b) = 1\}.$$

CardD1(S) and CardL1(S) [Zha+15]

$$\mathrm{CardD1}(S) \triangleq \#\{(a,b) \mid \delta_S(a,b) \neq 0,\ \ \mathrm{wt}(a) = \mathrm{wt}(b) = 1\}$$

$$\mathrm{CardL1}(S) \triangleq \#\{(a,b) \mid \mathcal{W}_S(a,b) \neq 0,\ \ \mathrm{wt}(a) = \mathrm{wt}(b) = 1\}.$$

Difference Distribution Table (DDT and DDT_1)

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

$a\backslash b$	0	1	2	4	8	3	5	6	9	A	C	7	B	D	E	F
0	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	·	·	·	·	4	·	·	4	·	·	4	·	4	·	·
2	·	·	·	·	·	2	4	2	·	2	2	·	·	2	2	·
4	·	·	·	·	·	·	4	2	2	2	2	2	·	·	2	·
8	·	·	·	·	·	2	·	·	2	·	·	2	4	2	·	4
3	·	2	·	2	·	2	·	4	·	2	·	2	2	·	·	·
5	·	2	·	2	·	·	·	·	2	2	4	·	2	2	·	·
6	·	·	2	·	2	·	·	2	·	·	2	·	4	·	·	4
9	·	·	2	4	2	·	·	2	·	·	2	·	·	·	4	·
A	·	·	2	·	2	2	4	·	·	2	·	·	·	2	2	·
C	·	·	2	·	2	·	4	·	2	2	·	2	·	·	2	·
7	·	4	2	·	2	·	·	2	·	·	2	·	·	·	·	4
B	·	2	·	2	4	·	·	·	2	2	·	·	2	2	·	·
D	·	2	4	2	·	2	·	·	·	2	·	2	2	·	·	·
E	·	·	2	·	2	2	·	2	2	·	2	2	·	2	·	·
F	·	4	·	4	·	·	·	·	·	·	·	·	·	·	4	4

DDT_1

$\mathcal{U} = 4$, $\mathcal{D}_{\text{spec}} = \{0 : 159, 2 : 72, 4 : 24, 16 : 1\}$, $\mathcal{U}_1 = 0$, $\mathcal{D}_{\text{spec}_1} = \{0 : 16\}$

Linear Approximation Table (LAT and LAT_1)

$$\mathcal{W}_S(a,b) \triangleq \sum_{x\in\mathbb{F}_2^n}(-1)^{b\cdot S(x)\oplus a\cdot x}$$

$a\backslash b$	0	1	2	4	8	3	5	6	9	A	C	7	B	D	E	F
0	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	LAT_1	·	·	·	·	−8	·	·	·	·	−8	·	−8	·	8
2	·	·	4	−4	4	4	−4	·	−4	·	·	·	8	8	−4	4
4	·	·	−4	−4	−4	4	−4	·	−4	·	·	8	−8	·	−4	4
8	·	·	4	·	−4	−4	·	−4	4	·	−4	4	·	4	8	8
3	·	·	4	4	−4	4	−4	−8	4	−8	·	·	·	·	−4	−4
5	·	·	−4	−4	4	4	4	·	4	−8	8	·	·	·	4	4
6	·	·	·	·	·	−8	·	−8	−8	·	8	·	·	·	·	·
9	·	8	−4	·	−4	−4	·	4	−4	−8	−4	−4	·	4	·	·
A	·	·	8	4	·	·	4	4	·	·	4	−4	−8	4	−4	4
C	·	·	·	−4	8	·	−4	−4	·	·	−4	−4	−8	4	4	−4
7	·	·	·	8	·	8	·	·	−8	·	·	·	·	·	8	·
B	·	−8	·	−4	−8	·	−4	4	·	·	4	−4	·	4	4	−4
D	·	8	8	−4	·	·	−4	4	·	·	4	4	·	−4	4	−4
E	·	·	4	−8	−4	4	8	−4	−4	·	−4	−4	·	−4	·	·
F	·	8	−4	·	−4	4	·	−4	4	8	4	−4	·	4	·	·

$\mathcal{L} = 8$, $\mathcal{W}_{\text{spec}} = \{0:123, 4:96, 8:36, 16:1\}$, $\mathcal{L}_1 = 4$, $\mathcal{W}_{\text{spec}_1} = \{0:8, 4:8\}$

Resistance to DC and LC

Constructing S-boxes from DDT and LAT

An S-box is completely specified by its LAT:

Recover the S-box from its LAT [Per17]

Let S be a vectorial Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then each coordinate S_{e_i} (for $1 \leq i \leq m$) can be recovered by using:

$$S_{e_i}(x) = \frac{1}{2} - \frac{1}{2^{n+1}} \sum_{a \in \mathbb{F}_2^n} \mathcal{W}_S(a, 2^i)(-1)^{a \cdot x}.$$

Start from a desired DDT (resp. LAT) which guarantees a high resistance against cryptanalysis, and to construct S-boxes having this specific DDT (resp. LAT)
Reconstruct the class of DDT-equivalent S-boxes from a given DDT [Bou+18; DH18].

Resistance to Boomerang Attack

Boomerang Connectivity Table (BCT) of an invertible $n \times n$ S-box S [Cid+18]

A $2^n \times 2^n$ table that precomputes the following quantity for all (a, b):

$$\beta_S(a,b) \triangleq \#\left\{x \in \mathbb{F}_2^n \mid S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\right\}.$$

The *boomerang uniformity*, denoted by $\mathcal{BU}(S)$, is the highest value in the BCT excluding the entry $(0, 0)$:

$$\mathcal{BU}(S) = \max_{a,b \in \mathbb{F}_2^n \setminus \{0\}} \beta_S(a,b).$$

The *boomerang differential spectrum* is the multiset

$$\mathcal{BD}_{\text{spec}}(S) \triangleq \{\beta_S(a,b) \mid a \in \mathbb{F}_2^n \setminus \{0\}, b \in \mathbb{F}_2^n\}.$$

Boomerang Connectivity Table (BCT)

$$\beta_S(a,b) \triangleq \#\{x \in \mathbb{F}_2^n \mid S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}$$

$a\backslash b$	0	1	2	4	8	3	5	6	9	A	C	7	B	D	E	F
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	·	·	4	·	2	2	2	·	4	2	2	2	·	4	·
2	16	·	·	·	4	4	·	·	2	2	4	4	·	2	2	8
4	16	·	·	16	·	·	·	·	8	8	·	·	·	8	8	·
8	16	·	·	4	·	2	2	2	4	·	2	2	2	4	·	·
3	16	2	2	4	·	2	·	·	4	·	2	2	2	4	·	·
5	16	·	2	4	2	·	2	·	·	6	·	·	2	·	6	·
6	16	2	2	·	4	4	2	2	·	·	4	4	·	·	·	8
9	16	2	2	·	·	·	2	2	2	2	·	·	·	2	2	·
A	16	2	2	4	·	2	·	·	·	4	2	2	2	·	4	·
C	16	2	·	4	2	·	·	2	6	·	·	·	2	6	·	·
7	16	·	2	4	2	·	2	·	6	·	·	·	2	6	·	·
B	16	2	2	·	4	4	2	2	·	·	4	4	·	·	·	8
D	16	·	·	·	8	8	·	·	·	·	8	8	·	·	·	16
E	16	2	·	4	2	·	·	2	·	6	·	·	2	·	6	·
F	16	2	2	·	4	4	2	2	·	·	4	4	·	·	·	8

BCT_1

$\mathcal{BU} = 16$, $\mathcal{BD}_{\text{spec}} = \{0:107, 2:64, 4:32, 6:8, 8:12, 16:33\}$

Resistance to Algebraic Attacks

Algebraic degree of a Boolean function $\deg(f)$

For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$\deg(f) \triangleq \max\{\mathrm{wt}(u) \mid u \in \mathbb{F}_2^n \text{ and } \alpha_u \neq 0 \in \mathbb{F}_2 \text{ in } \mathrm{ANF}_f\}.$$

Algebraic degree of an S-box $\mathrm{Deg}(S)$

$$\mathrm{Deg}(S) = \max_{i \in \{0,\cdots,n-1\}} \deg(S_{e_i}) = \max_{\lambda \in \mathbb{F}_2^m \setminus \{0\}} \deg(S_\lambda).$$

The mimimal algebraic degree of an S-box S

$$\min \deg(S) \triangleq \min_{\lambda \in \mathbb{F}_2^m \setminus \{0\}} \deg(S_\lambda).$$

Resistance to Algebraic Attacks

The number of non-trivial components of S with the maximal degree

$$\mathrm{Deg}_{\mathrm{Freq}} \triangleq \#\{\lambda \mid \deg(S_\lambda) = \mathrm{Deg}(S),\ \lambda \in \mathbb{F}_2^m \setminus \{0\}\}$$

The degree spectrum of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathrm{Deg}_{\mathrm{spec}}(S) \triangleq \{\deg(S_\lambda) \mid \lambda \in \mathbb{F}_2^m \setminus \{0\}\}$$

where S_λ are component functions of S.

Resistance to Algebraic Attacks

$$
\begin{array}{l}
y_{0001b} = \quad + x_0 + \quad + x_2 + x_3 + x_0x_1 + x_0x_2 + x_1x_2 + \quad + \quad + + x_0x_1x_2 + + x_0x_2x_3 + x_1x_2x_3 \,, \deg = 3, te = 9, \; re = 4 \\
y_{0010b} = \quad + x_0 + \quad + \quad + \quad + \quad + x_0x_2 + x_1x_2 + \quad + x_1x_3 + + x_0x_1x_2 + + x_0x_2x_3 + x_1x_2x_3 \,, \deg = 3, te = 7, \; re = 4 \\
y_{0011b} = \quad + \quad + \quad + x_2 + x_3 + x_0x_1 + \quad + \quad + \quad + x_1x_3 + + \quad + + \quad + \quad , \deg = 2, te = 4, \; re = 4 \\
y_{0100b} = 1 + \quad + x_1 + \quad + x_3 + x_0x_1 + x_0x_2 + \quad + \quad + x_1x_3 + + x_0x_1x_2 + + \quad + x_1x_2x_3 \,, \deg = 3, te = 8, \; re = 4 \\
y_{0101b} = 1 + x_0 + x_1 + x_2 + \quad + \quad + \quad + x_1x_2 + \quad + x_1x_3 + + \quad + + x_0x_2x_3 + \quad , \deg = 3, te = 7, \; re = 4 \\
y_{0110b} = 1 + x_0 + x_1 + \quad + x_3 + x_0x_1 + \quad + x_1x_2 + \quad + \quad + + \quad + + x_0x_2x_3 + \quad , \deg = 3, te = 7, \; re = 4 \\
y_{0111b} = 1 + \quad + x_1 + x_2 + \quad + \quad + x_0x_2 + \quad + \quad + \quad + + x_0x_1x_2 + + \quad + x_1x_2x_3 \,, \deg = 3, te = 6, \; re = 4 \\
y_{1000b} = 1 + x_0 + x_1 + x_2 + x_3 + \quad + \quad + \quad + x_0x_3 + \quad + + \quad + + \quad + \quad , \deg = 2, te = 6, \; re = 4 \\
y_{1001b} = 1 + \quad + x_1 + \quad + \quad + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_3 + \quad + + x_0x_1x_2 + + x_0x_2x_3 + x_1x_2x_3 \,, \deg = 3, te = 9, \; re = 4 \\
y_{1010b} = 1 + \quad + x_1 + x_2 + x_3 + \quad + x_0x_2 + x_1x_2 + x_0x_3 + x_1x_3 + + x_0x_1x_2 + + x_0x_2x_3 + x_1x_2x_3 \,, \deg = 3, te = 11, re = 4 \\
y_{1011b} = 1 + x_0 + x_1 + \quad + \quad + x_0x_1 + \quad + \quad + x_0x_3 + x_1x_3 + + \quad + + \quad + \quad , \deg = 2, te = 6, \; re = 3 \\
y_{1100b} = \quad + x_0 + \quad + x_2 + \quad + x_0x_1 + x_0x_2 + \quad + x_0x_3 + x_1x_3 + + x_0x_1x_2 + + \quad + x_1x_2x_3 \,, \deg = 3, te = 8, \; re = 4 \\
y_{1101b} = \quad + \quad + \quad + \quad + x_3 + \quad + \quad + x_1x_2 + x_0x_3 + x_1x_3 + + \quad + + x_0x_2x_3 + \quad , \deg = 3, te = 5, \; re = 4 \\
y_{1110b} = \quad + \quad + \quad + x_2 + \quad + x_0x_1 + \quad + x_1x_2 + x_0x_3 + \quad + + \quad + + x_0x_2x_3 + \quad , \deg = 3, te = 5, \; re = 4 \\
y_{1111b} = \quad + x_0 + \quad + \quad + x_3 + \quad + x_0x_2 + \quad + x_0x_3 + \quad + + x_0x_1x_2 + + \quad + x_1x_2x_3 \,, \deg = 3, te = 6, \; re = 4
\end{array}
$$

$$\mathrm{Deg} = 3, \min \deg = 2, \mathrm{Deg}_{\mathrm{spec}} = \{2 : 3, 3 : 12\}$$

Resistance to Algebraic Attacks

Maximal degree of the product of k coordinates

Let S be a vectorial Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$. For any integer k, $1 \leq k \leq m$, $d_k(S)$ denotes the maximal algebraic degree of the product of any k (or fewer) coordinates of S

$$d_k(S) = \max_{K \subseteq \{1,\ldots,m\}, |K| \leq k} \deg \left(\prod_{i \in K} S_{e_i} \right).$$

In particular, $d_1(S) = \deg(S)$.

Example 1 (MISTY1 7-bit S-box)

k	1	2	3	4	5	6	7
d_k	3	5	5	6	6	6	7

Resistance to Algebraic Attacks

Higher-order differential, Zero-sum distinguishers

Degree of the composition $G \circ F$ [BCC11; BC13b]

Let $F : \mathbb{F}_2^{nt} \to \mathbb{F}_2^{nt}$ corresponding to the concatenation of t smaller balanced S-boxes, $S_1, \ldots, S_t$, defined over $\mathbb{F}_2^n$. Then, for any function G from $\mathbb{F}_2^{nt}$ into $\mathbb{F}_2^{\ell}$, we have

$$\deg(G \circ F) \leq nt - \frac{nt - \deg(G)}{\gamma}, \quad \texttt{where}$$

$$\gamma = \max_{1 \leq i \leq n-1} \frac{n-i}{n - \max_{1 \leq j \leq t} d_i(S_j)}.$$

Most notably, we have

$$\gamma \leq \max_{1 \leq j \leq t} \max\left(\frac{n-1}{n - \deg(S_j)}, \frac{n}{2} - 1, \deg({S_j}^{-1})\right).$$

Resistance to Division-Property-Based Integral Attacks

The appearance of monomials in the ANFs of $x \mapsto \pi_v(S(x))$ for $v \in \mathbb{F}_2^n$, which is defined as a set

$$\mathcal{V}_S(u) \triangleq \bigcup_{w \in \mathtt{Succ}(u)} V_S(w),$$

where

$$\text{and} \quad V_S(w) \triangleq \{v \in \mathbb{F}_2^n : \pi_v(S(x)) \text{ contains } \pi_w(x)\}$$

and where $\mathtt{Succ}(u) = \{x \in \mathbb{F}_2^n : u \preceq x\}$ which is an affine subspace of dimension $(n - \mathrm{wt}(u))$ [BC16].

A table representation of $\mathcal{V}_S(u)$ for all u is useful to understand the resistance against division-property-based attacks. Such a table is recommended to not contain columns or rows that are too sparse.

Resistance to Division-Property-Based Integral Attacks

$\mathcal{V}_S(u) \triangleq \bigcup_{w \in \mathtt{Succ}(u)} V_S(w)$ and $V_S(w) \triangleq \{v \in \mathbb{F}_2^n : \pi_v(S(x)) \text{ contains } \pi_w(x)\}$,
where $\mathtt{Succ}(u) = \{x \in \mathbb{F}_2^n : u \preceq x\}$ and $\pi_w(x) = \prod_{i=1}^{n} x_i^{w_i}$

$u\backslash v$	0	1	2	4	8	3	5	6	9	A	C	7	B	D	E	F
0	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
8		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3		x	x	x		x	x	x	x	x	x	x	x	x	x	x
5		x	x	x		x		x	x	x	x	x		x	x	x
6		x	x	x		x	x	x	x	x	x	x	x	x	x	x
9		x	x		x	x	x	x	x	x	x	x	x	x	x	x
A		x	x	x		x	x	x	x	x	x	x	x	x		x
C		x	x	x		x	x	x	x	x	x	x	x	x	x	x
7		x	x	x		x				x	x	x		x	x	x
B											x	x	x			x
D		x	x					x	x			x		x	x	x
E		x	x	x		x	x	x		x			x	x		x
F																x

Resistance to Interpolation Attacks

Univariate polynomial representation

Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be any n-bit S-box. The vectors of $\mathbb{F}_2^n$ can be interpreted as elements of a finite field $\mathbb{F}_{2^n}$, and S can be written as a unique univariate polynomial of $\mathbb{F}_{2^n}[X]$:

$$S(X) = \sum_{i=0}^{2^n-1} v_i X^i$$

Univariate degree

The univariate degree of an n-bit S-box $S : X \mapsto \sum_{i=0}^{2^n-1} v_i X^i$ is

$$\max(\{i, v_i \neq 0\}).$$

Relation with its algebraic degree: $\mathrm{Deg}(S) = \max(\{\mathrm{wt}(i), v_i \neq 0\})$.

If the **univariate degree** of a function is too low or the **number of terms** in the polynomial representation is too small, it may lead to interpolation attacks [JK01].

Resistance to Truncated Differential and Subspace Trail Attacks

Linear structures of a Boolean function [Eve87; MS89]

The *linear space* of a Boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ is the linear subspace of those a such that $D_a f$ is a constant function c, *i.e.,*

$$\mathrm{LS}(f) \triangleq \{a \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus a) = c, \text{ where } c \text{ is constant in } \mathbb{F}_2\}.$$

Such a, $a \neq 0$, is said to be a *c-linear structure* of f.

Linear structures of an S-box [Eve87; Lai94; Dub01]

A *linear structure* of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a triple (λ, a, c) such that a is a c-linear structure of the *component function* $S_\lambda(x)$, *i.e.,*

$$(\lambda, a, c) \ \texttt{s.t.} \ S_\lambda(x) \oplus S_\lambda(x \oplus a) = c \text{ for } \forall x \in \mathbb{F}_2^n.$$

This implies that for all output differences b of the S-Box compatible with the input difference a, we have $\lambda \cdot b = c$.
Let $\#$ LS denote the number of linear structures of an S-box.

Resistance to Truncated Differential and Subspace Trail Attacks

$$\#\,\mathrm{LS} = 9, \quad \mathrm{Deg}_{\mathrm{spec}}(S) = \{\deg(S_\lambda) \mid \lambda \in \mathbb{F}_2^n \setminus \{0\}\} = \{2:3, 3:12\}$$

Noekeon	Piccolo	PRESENT	Rectangle	LBlock_0
(0100, 0001, 1)	(0100, 0001, 0)	(0001, 0001, 1)	(0001, 0100, 1)	(0001, 0001, 1)
(0100, 1010, 1)	(0100, 1000, 1)	(0001, 1000, 1)	(0001, 1000, 1)	(0001, 0010, 1)
(0100, 1011, 0)	(0100, 1001, 1)	(0001, 1001, 0)	(0001, 1100, 0)	(0001, 0011, 0)
(1000, 0001, 1)	(1000, 0001, 1)	(1010, 0001, 1)	(0010, 0001, 1)	(0010, 0011, 1)
(1000, 1000, 0)	(1000, 0010, 0)	(1010, 1110, 1)	(0010, 0100, 1)	(0010, 1000, 1)
(1000, 1001, 1)	(1000, 0011, 1)	(1010, 1111, 0)	(0010, 0101, 0)	(0010, 1011, 0)
(1100, 0001, 0)	(1100, 0001, 1)	(1011, 0001, 0)	(0011, 0100, 0)	(0011, 0011, 1)
(1100, 0010, 1)	(1100, 1010, 1)	(1011, 0110, 1)	(0011, 1001, 1)	(0011, 1001, 0)
(1100, 0011, 1)	(1100, 1011, 0)	(1011, 0111, 1)	(0011, 1101, 1)	(0011, 1010, 1)

$$\#\,\mathrm{LS} = 3, \quad \mathrm{Deg}_{\mathrm{spec}}(S) = \{\deg(S_\lambda) \mid \lambda \in \mathbb{F}_2^n \setminus \{0\}\} = \{2:1, 3:14\}$$

Golden_S0	Golden_S1	Golden_S2	Golden_S3	Qarma_sigma0
(1111, 0100, 0)	(0111, 0010, 0)	(1111, 0100, 0)	(0110, 0010, 1)	(0100, 0100, 0)
(1111, 1010, 1)	(0111, 1100, 1)	(1111, 1001, 1)	(0110, 0101, 1)	(0100, 1011, 1)
(1111, 1110, 1)	(0111, 1110, 1)	(1111, 1101, 1)	(0110, 0111, 0)	(0100, 1111, 1)

$$\#\,\mathrm{LS} = 0, \quad \mathrm{Deg}_{\mathrm{spec}}(S) = \{\deg(S_\lambda) \mid \lambda \in \mathbb{F}_2^n \setminus \{0\}\} = \{3:15\}$$

PRINCE	TWINE	KLEIN	JH_0/1	Qarma_sigma1/2	Panda	Midori_Sb1
Have no linear structure						

Resistance to Truncated Differential and Subspace Trail Attacks

A way to efficiently find all linear structures of an S-box by using its ACT [MT14]

An S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ has a linear structure
$(\lambda, a, c) \iff |\mathrm{ACT}_S(a, \lambda)| = 2^n$ where $a \in \mathbb{F}_2^n \setminus \{0\}, \lambda \in \mathbb{F}_2^m \setminus \{0\}$.
If $\mathrm{ACT}_S(a, \lambda) = +2^n$ (resp. -2^n), $c = 0$ (resp. $c = 1$).

The Auto-Correlation Table (ACT) [ZZI00]

The ACT_S of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a $2^n \times 2^m$ matrix, in which the element $\mathrm{ACT}_S(a, \lambda)$ in row a and column λ is equal to the auto-correlation coefficient $r_{S_\lambda}(a)$ of the component function S_λ on a.

Where, the auto-correlation coefficient of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ on $a \in \mathbb{F}_2^n$ is defined by

$$r_f(a) \triangleq \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{f(x \oplus a)} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus a)}.$$

Auto-Correlation Table (ACT and ACT_1)

$a\backslash b$	0	1	2	4	8	3	5	6	9	A	C	7	B	D	E	F
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	·	−8	−8	·	·	−8	·	−8	·	·	8	·	8	·	·
2	16	·	·	−8	−16	·	·	·	·	·	8	−8	·	·	·	8
4	16	·	·	·	−16	−16	·	·	·	·	·	·	16	·	·	·
8	16	−8	·	−8	·	·	·	−8	·	−8	·	8	·	·	8	·
3	16	−8	·	8	·	·	−8	·	·	−8	·	−8	·	8	·	·
5	16	8	·	·	·	·	·	−8	·	8	−8	·	·	·	−8	−8
6	16	−8	−8	·	16	·	·	·	−8	−8	·	·	·	·	·	·
9	16	·	·	·	·	−16	·	·	·	·	·	·	·	·	·	·
A	16	·	−8	8	·	·	·	−8	−8	·	·	−8	·	·	8	·
C	16	·	8	·	·	·	−8	·	8	·	−8	·	·	−8	·	−8
7	16	·	8	·	·	·	·	−8	8	·	−8	·	·	·	−8	−8
B	16	·	·	−8	·	·	·	·	·	·	8	−8	−16	·	·	8
D	16	−8	−8	·	·	16	8	8	−8	−8	·	·	·	−8	−8	·
E	16	8	·	·	·	·	−8	·	·	8	−8	·	·	−8	·	−8
F	16	·	·	·	·	·	8	8	·	·	·	·	−16	−8	−8	·

ACT_1

Resistance to Cube-like Attacks

(v, w)-linearity [BC13a]

Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Then

$$S \text{ is } (v, w)\textbf{-linear}$$

if there exist two linear subspaces $V \subset \mathbb{F}_2^n$ and $W \subset \mathbb{F}_2^m$ with $\dim V = v$ and $\dim W = w$, such that, for all $\lambda \in W$,

$$S_\lambda : x \mapsto \lambda \cdot S(x)$$

has **degree at most 1** on all cosets of V.

The parameters (v, w) quantify the ability of the S-box to propagate affine relations, which influences the resistance to cube-like attacks.

Resistance to Cube-like Attacks

$v \setminus w$	1	2	3	4
1	31	31	31	31
2	155	155	155	155
3	155	155	60	5
4	20	5	0	0

The number $N_{(v,w)}$ of subspaces V of dimension v for which there exists a w-dimensional W such that the S-box is (v, w)-linear with respect to (V, W).

Basis of V	W
{0x02,0x04,0x08,0x10}	{0x00,0x02,0x04,0x06}
{0x01,0x04,0x08,0x10}	{0x00,0x04,0x08,0x0c}
{0x01,0x02,0x08,0x10}	{0x00,0x08,0x10,0x18}
{0x01,0x02,0x04,0x10}	{0x00,0x01,0x10,0x11}
{0x01,0x02,0x04,0x08}	{0x00,0x01,0x02,0x03}

The 5 pairs of subspaces (V, W) where $|V| = v = 4$ and $|W| = w = 2$ with respect to which the S-box is linear.

Resistance to Invariant Subspace Attack: Non-linear

Nonlinear invariants [TLS16]

$g(x) \oplus g(S(x)) = c$, where g is a non-linear Boolean function, and c is a constant.

Example 2 (A Nonlinear invariant for the S-box S in Scream)

$$g(x) = x_1x_2 \oplus x_0 \oplus x_5$$

Then,

$$g(x) \oplus g(S(x)) = 1, \forall x \in \mathbb{F}_2^8$$

Example 3 (A Nonlinear invariant for the S-box S in Midori64)

$$g(x) = x_2x_3 \oplus x_0 \oplus x_1 \oplus x_2$$

Then,

$$g(x) \oplus g(S(x)) = 0, \forall x \in \mathbb{F}_2^4$$

Resistance to Invariant Subspace Attack: Non-linear

Nonlinear invariants for the linear layer [TLS16]

If the linear transformation consists of cell-wise permutation and multiplications by binary orthogonal matrices and if there is a quadratic invariant for the S-box, $\oplus_{i=1}^{t} g(\mathbf{x_i})$ is non-linear invariant for the linear layer, thus also invariant for the entire cipher.

Thus, for ciphers with binary orthogonal linear function, **the number of quadratic invariant** for the S-box might be a concerned criterion.

Invariant Properties under Simple Transformations

Many cryptographic properties (differential uniformity, linearity, differential spectrum, extended Walsh spectrum, algebraic degree, (v, w)-linearity, etc.) are invariant under simple transformations.

Criteria	**Equivalence**	**Criteria**	**Equivalence**	**Criteria**	**Equivalence**
$\mathcal{U}$, $\mathcal{D}_{\mathrm{spec}}$	CCZ [CP18]	$\mathcal{L}$, $\mathcal{W}_{\mathrm{spec}}$	CCZ [CP18]	Deg, $\mathrm{Deg}_{\mathrm{spec}}$	EA [CP18]
$\mathcal{U}_1$, $\mathcal{D}_{\mathrm{spec}_1}$	PXE (obvious)	$\mathcal{L}_1$, $\mathcal{W}_{\mathrm{spec}_1}$	PXE (obvious)	$\mathrm{Deg}_{\mathrm{spec}_{cor}}$	PXE (obvious)
d_k	AE [GRW16]	$\#\,\mathrm{LS}$	AE [MS89]	$(v, w)-$linearities	AE [BC13]

Known function equivalence that preserves particular criteria

Invariant Properties under Simple Transformations

Two functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are

Permutation-XOR-equivalent (PXE)

If $\exists$ two bit permutations $P_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $P_2 : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and two constants $c_1 \in \mathbb{F}_2^n$ and $c_2 \in \mathbb{F}_2^m$, s.t.

$$G(x) = (P_2 \circ F \circ P_1)(x \oplus c_1) \oplus c_2.$$

Linear-equivalent (LE)

If $\exists$ two linear permutations $L_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $L_2 : \mathbb{F}_2^m \to \mathbb{F}_2^m$, s.t.

$$G(x) = (L_2 \circ F \circ L_1)(x).$$

Affine-equivalent (AE)

If $\exists$ two affine permutations $A_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $A_2 : \mathbb{F}_2^m \to \mathbb{F}_2^m$, s.t.

$$G(x) = (A_2 \circ F \circ A_1)(x).$$

Invariant Properties under Simple Transformations

Extended-Affine equivalent (EA)

If $\exists$ two affine permutations $A_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $A_2 : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and an affine function $C : \mathbb{F}_2^n \to \mathbb{F}_2^m$, s.t.

$$G(x) = (A_2 \circ F \circ A_1)(x) \oplus C(x).$$

Carlet-Charpin-Zinoviev equivalent (CCZ) [CCZ98]

If $\exists$ an affine permutation A of $\mathbb{F}_2^n \times \mathbb{F}_2^m$, s.t., the graph of F is mapped to the graph of G, i.e.,

$$\{(x, F(x)) \mid x \in \mathbb{F}_2^n\} \xrightarrow{A} \{(x, G(x)) \mid x \in \mathbb{F}_2^n\}.$$

Outline

Existing Tools

Source	Secu-rity	MC	BGC/ GC	GEC	Depth	CPU cycles	Method	Speed	Opti-mal	Open code
[Gla]	✘	✘	✔	✘	✘	✘	Heur. DFS	✔	✘	✔
[Osv00]	✘	✘	✘	✘	✘	✔	Heur.	-	✘	✘
[WS10]	✘	✘	✘	✘	✘	✔	Instr. first Gen.	✔	✔	✘
[Ull+11]	✘	✘	✔	✘	✘	✘	ID-DFS + AE	-	✔	✘
[BMP13]	✘	✔	✔	✘	✘	✘	Two-step Heur.	-	✘	✘
[CHM11]	✘	✔	✔	✘	✘	✘	Two-step SAT	-	✘	✘
[Sto16]	✘	✔	✔	✘	✔	✘	SAT	✘	✔	✔
[Guo+16]	✘	✘	✘	✘	✔	✘	LUT	✔	✔	✘
[Jea+17]	✘	✔	✔	✔	✘	✘	MITM + BFS	✔	✘	✔
[MLCA]	✔	✘	✘	✘	✘	✘	-	✘	✘	✔
[Mag]	✔	✘	✘	✘	✘	✘	-	✘	✘	✘
[FJ]	✔	✘	✘	✘	✘	✘	-	✘	✘	✔

Implementation – Performance Criteria

- Bit-sliced gate complexity (`BGC`) [CHM11; Sto16]:
  - the smallest number of operations in {`AND`, `OR`, `XOR`, `NOT`} (sometimes includes `ANDN`);
  - bit-sliced gate implementations can be translated to bit-sliced software implementations
- Gate Equivalent complexity (`GEC`) [Jea+17]:
  - the smallest number of Gate Equivalents (GEs) required to implement an S-box, given the cost of atomic operations
  - available gates and gate sizes dependent on different technologies, e.g. UMC/180nm, TMSC/65nm;
- Multiplicative complexity (`MC`) [BPP00; Sto16]:
  - the minimum number of `AND` gates necessary in an `XOR`-`AND` circuit implementing the S-box
- Circuit depth complexity (`Depth`) [Ban+15; Guo+16]:
  - the sum of sequential path delays of basic operations in the critical path
  - It is reasonable to assume that depths of basic operations equal their GEs, because delays depend on the number of the transistors to be sequentially proceeded in the operation [Ban+15]

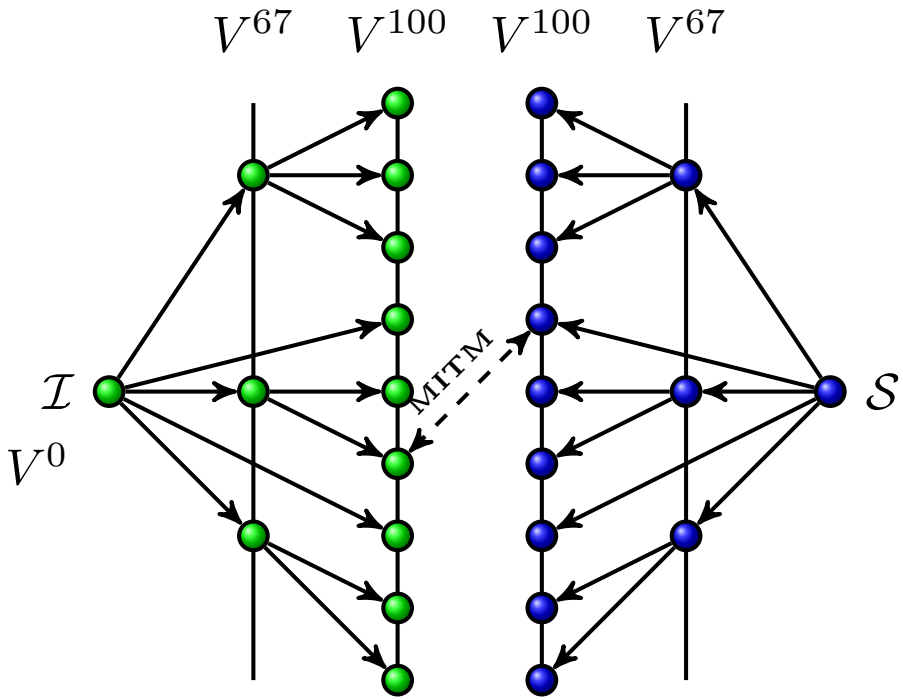
Implementation – Weight of Operations

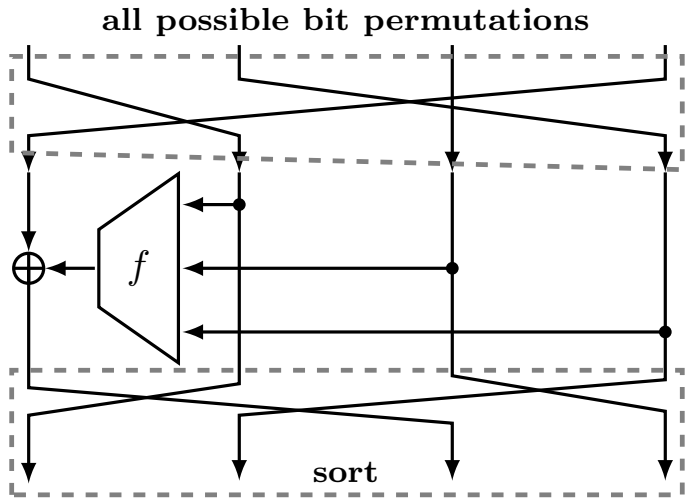
Tech.	NAND NOR	AND OR	NOT	XOR	XNOR	ANDN	ORN	NAND3 NOR3	MAOI1	MOAI1
UMC 180nm	1.00	1.33	0.67	3.00	3.00	1.67	1.67	1.33	2.67	2.00
TSMC 65nm	1.00	1.50	0.50	3.00	3.00	1.50	1.50	1.50	2.50	2.50
Software	-	1.00	1.00	1.00	-	1.00	-	-	-	-
Depth (GEs)	1.00	1.50	0.50	2.00	2.00	-	-	-	-	-
Depth (Soft.)	1.00	1.00	1.00	1.00	1.00	-	-	-	-	-
Multiplica-tive	-	1.00	0.00	0.00	-	-	-	-	-	-

Cost of atomic operations under various techniques [Jea+17]

Approach and Improvement

Bi-directional Dijsktra's shortest path finding algorithm in LIGHTER:





choices for f are small combinations of atomic operations, e.g., $f(x_1, x_2, x_3) = ((x_1 \texttt{ AND } x_2) \texttt{ ORN } x_3)$

Approach and Improvement

On the basis of the non-linear part of `LIGHTER`, we propose the following optimizations:

1. **Composition and concatenation:** use the isomorphism between the two graphs expanded from the two roots respectively encoding the identity function $\mathcal{I}$ and an target function $\mathcal{S}$, and use $F_1 \circ \mathcal{I} = F_2 \circ \mathcal{S} \Rightarrow F_1 \circ \mathcal{I} \circ F_2^{-1} = S$
2. **Pre-computation:** the graph is expanded from $\mathcal{I}$ without any given target and thus this graph can be built once and for all.
3. **Use equivalence** between different decompositions of an implementation: if an implementation can be found by using the concatenation of two short instruction sequences $\texttt{Imp}_1 \| \texttt{Imp}_2$, then it can also be found by using the composition $\texttt{Imp}'_1 \| \texttt{Imp}'_2$, where $\texttt{Imp}'_1 = \texttt{Imp}_1 \| \texttt{Ins}_1$ and $\texttt{Imp}_2 = \texttt{Ins}_1 \| \texttt{Imp}'_2$

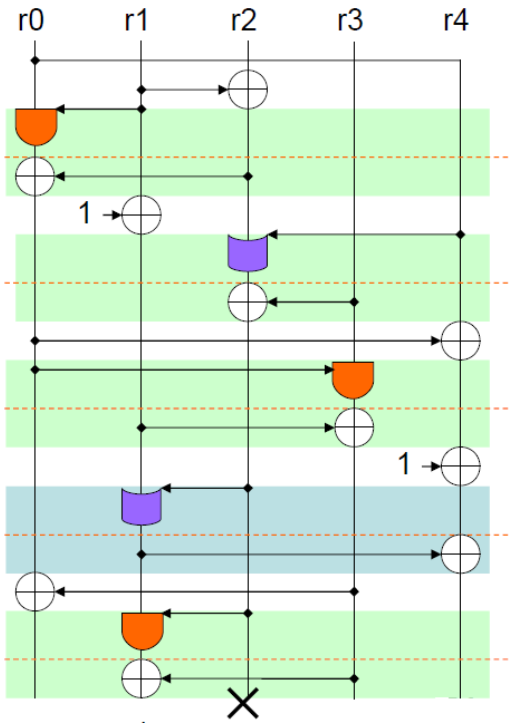
Enriched functionalities:

1. **Extend the cover range** of implementation target from 4-bit S-boxes to 3 $\sim$ 8-bit S-boxes.
2. **Support finding** `Depth`**-optimal** implementations

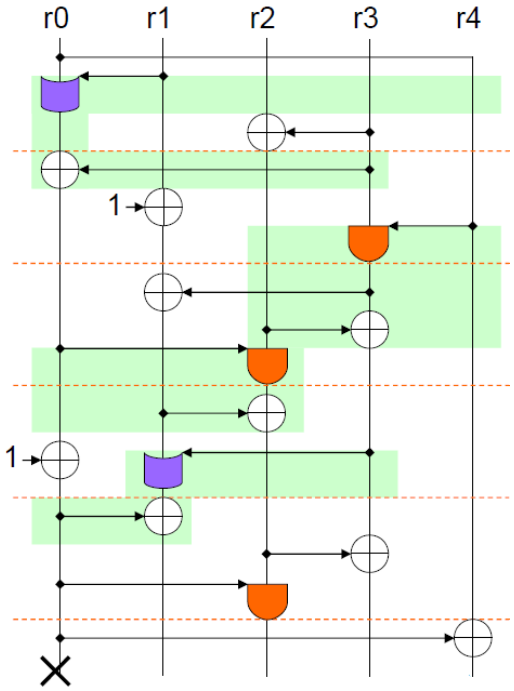
Outline

Using Simple Circuit

- Security-derived: Serpent, Rectangle
  - Step 1: Choose an S-box with good cryptographic properties
  - Step 2: Decompose to a set of instructions for the bit-sliced implementation
- Performance-derived: Noekeon, Luffa
  - Step 1: Construct a set of instructions with some properties
  - Step 2: Check if the S-box has desirable properties



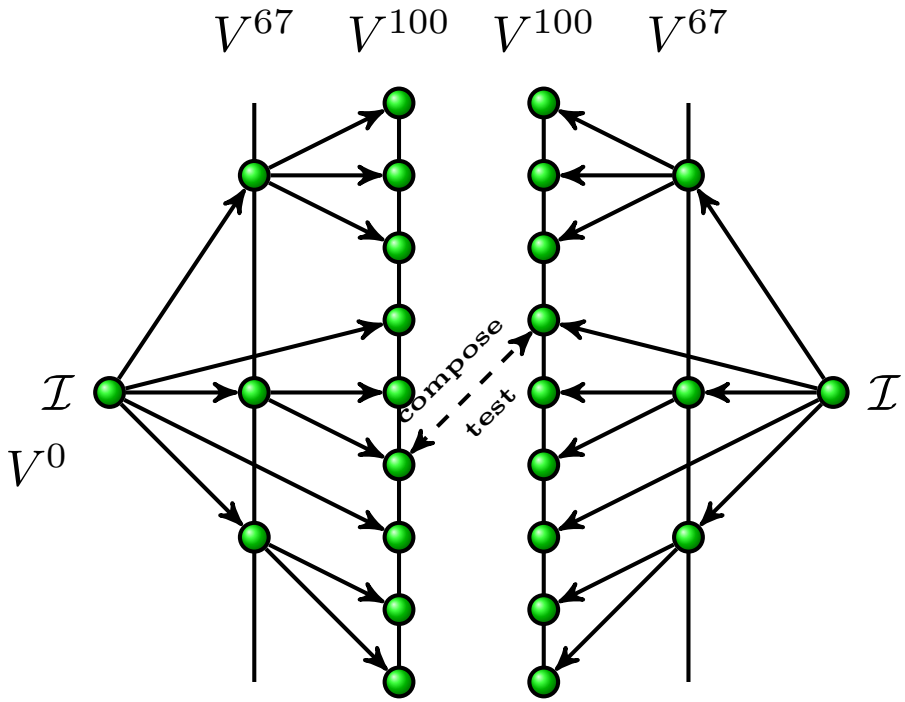
(a) Luffa v1 [Wat10]

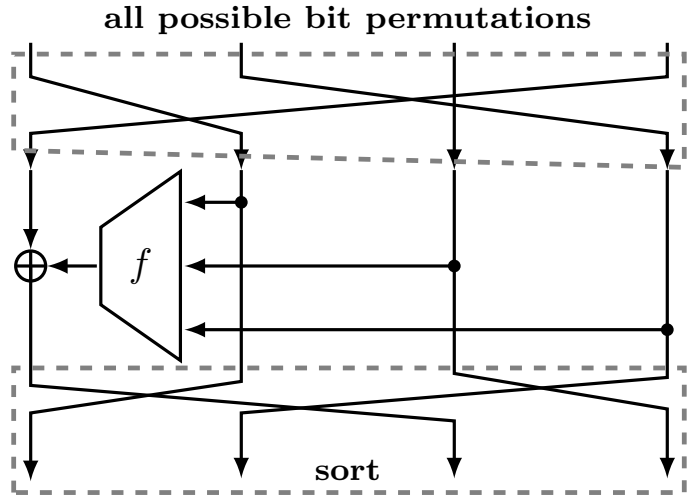


(b) Luffa v2 [Wat10]

Approach

Compose and test:





choices for f are small combinations of atomic operations, e.g.,
$f(x_1, x_2, x_3) = ((x_1 \texttt{ AND } x_2) \texttt{ ORN } x_3)$

e.g., CriteriaSet = $\{\mathcal{U} \leq 4,\ \mathcal{L} \leq 8,\ \mathcal{U}_1 = 0,\ \mathcal{L}_1 \leq 4,\ \texttt{BGC} \leq 11\}$

Generation from Instruction Combinations

There are two usages in PEIGEN with respect to generation of S-boxes fulfilling given criteria:

1. **Filtering out good S-boxes**: Given a set of n-bit S-boxes and a set of criteria, PEIGEN filters out the S-boxes fulfilling the criteria, outputs the detailed evaluations of their security properties and their implementations under a given configuration on gates;
2. **Generating new S-boxes from scratch**: Given a set of criteria, PEIGEN
    1. generates a set of S-boxes fulfilling the given criteria, outputs the detailed evaluations of their security properties and their implementations under a given configuration on gates;
    2. classifies the generated S-boxes in accordance with their detailed properties by distributing the results on the generated S-boxes into different folders.

Outline

Summary and Future Work

1. We tried to provide a survey on known results on the design of S-boxes reflected in studies on various attacks, and a comprehensive check-list for designers.
2. A platform PEIGEN is built, aiming to provide the community an open platform to facilitate the research and use of S-boxes.
3. PEIGEN is still at an early stage, there are some missing functionalities, and for larger S-boxes ($\geq$ 5-bit), it is not yet powerful enough for the implementation and generation of strong S-boxes. We believe both heuristic and theoretical approaches exist for larger S-boxes and can be integrated into this platform.
4. The source codes of PEIGEN and generated results are available via `https://github.com/peigen-sboxes/PEIGEN`.

Thanks for your attention!

References I

[Nyb94] Kaisa Nyberg. "S-boxes and Round Functions with Controllable Linearity and Differential Uniformity". In: *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*. Ed. by Bart Preneel. Vol. 1008. LNCS. Springer, 1994, pp. 111–130. DOI: 10.1007/3-540-60590-8_9. URL: https://doi.org/10.1007/3-540-60590-8_9.

[Can16] Anne Canteaut. "Lecture Notes on Cryptographic Boolean Functions". In: *Inria, Paris, France* (2016). https://www.paris.inria.fr/secret/Anne.Canteaut/poly.pdf.

[Car10] Claude Carlet. "Vectorial Boolean Functions for Cryptography". In: *Boolean models and methods in mathematics, computer science, and engineering* 134 (2010), pp. 398–469.

[Nyb91] Kaisa Nyberg. "Perfect Nonlinear S-Boxes". In: *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*. Ed. by Donald W. Davies. Vol. 547. Lecture Notes in Computer Science. Springer, 1991, pp. 378–386. ISBN: 3-540-54620-0. DOI: 10.1007/3-540-46416-6_32. URL: https://doi.org/10.1007/3-540-46416-6_32.

[Nyb93] Kaisa Nyberg. "Differentially Uniform Mappings for Cryptography". In: *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*. Ed. by Tor Helleseth. Vol. 765. Lecture Notes in Computer Science. Springer, 1993, pp. 55–64. ISBN: 3-540-57600-2. DOI: 10.1007/3-540-48285-7_6. URL: https://doi.org/10.1007/3-540-48285-7_6.

[BCC10] Céline Blondeau, Anne Canteaut, and Pascale Charpin. "Differential Properties of Power Functions". In: *IJICoT* 1.2 (2010), pp. 149–170. DOI: 10.1504/IJICOT.2010.032132. URL: https://doi.org/10.1504/IJICOT.2010.032132.

[CR15] Anne Canteaut and Joëlle Roué. "On the Behaviors of Affine Equivalent Sboxes Regarding Differential and Linear Attacks". In: *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9056. Lecture Notes in Computer Science. Springer, 2015, pp. 45–74. ISBN: 978-3-662-46799-2. DOI: 10.1007/978-3-662-46800-5_3. URL: https://doi.org/10.1007/978-3-662-46800-5_3.

References II

[Hon+00] Seokhie Hong et al. “Provable Security against Differential and Linear Cryptanalysis for the SPN Structure”. In: *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*. Ed. by Bruce Schneier. Vol. 1978. Lecture Notes in Computer Science. Springer, 2000, pp. 273–283. ISBN: 3-540-41728-1. DOI: 10.1007/3-540-44706-7_19. URL: https://doi.org/10.1007/3-540-44706-7_19.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002. ISBN: 3-540-42580-2. DOI: 10.1007/978-3-662-04722-4. URL: https://doi.org/10.1007/978-3-662-04722-4.

[Par+03] Sangwoo Park et al. “Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structures and AES”. In: *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*. Ed. by Thomas Johansson. Vol. 2887. Lecture Notes in Computer Science. Springer, 2003, pp. 247–260. ISBN: 3-540-20449-0. DOI: 10.1007/978-3-540-39887-5_19. URL: https://doi.org/10.1007/978-3-540-39887-5_19.

[LP07] Gregor Leander and Axel Poschmann. “On the Classification of 4 Bit S-Boxes”. In: *Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings*. Ed. by Claude Carlet and Berk Sunar. Vol. 4547. Lecture Notes in Computer Science. Springer, 2007, pp. 159–176. ISBN: 978-3-540-73073-6. DOI: 10.1007/978-3-540-73074-3_13. URL: https://doi.org/10.1007/978-3-540-73074-3_13.

[Zha+15] Wentao Zhang et al. “A New Classification of 4-bit Optimal S-boxes and Its Application to PRESENT, RECTANGLE and SPONGENT”. In: *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*. Ed. by Gregor Leander. Vol. 9054. Lecture Notes in Computer Science. Springer, 2015, pp. 494–515. ISBN: 978-3-662-48115-8. DOI: 10.1007/978-3-662-48116-5_24. URL: https://doi.org/10.1007/978-3-662-48116-5_24.

[Per17] Léo Perrin. “Cryptanalysis, Reverse-Engineering and Design of Symmetric Cryptographic Algorithms”. PhD thesis. University of Luxembourg, 2017. URL: http://orbilu.uni.lu/handle/10993/31195.

References III

[Bou+18] Christina Boura et al. “Two Notions of Differential Equivalence on Sboxes”. In: *IACR Cryptology ePrint Archive* 2018 (2018), p. 617. URL: https://eprint.iacr.org/2018/617.

[DH18] Orr Dunkelman and Senyang Huang. “Reconstructing an S-box from its Difference Distribution Table”. In: *IACR Cryptology ePrint Archive* 2018 (2018), p. 811. URL: https://eprint.iacr.org/2018/811.

[Cid+18] Carlos Cid et al. “Boomerang Connectivity Table: A New Cryptanalysis Tool”. In: *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10821. Lecture Notes in Computer Science. Springer, 2018, pp. 683–714. ISBN: 978-3-319-78374-1. DOI: 10.1007/978-3-319-78375-8_22. URL: https://doi.org/10.1007/978-3-319-78375-8_22.

[BCC11] Christina Boura, Anne Canteaut, and Christophe De Cannière. “Higher-Order Differential Properties of Keccak and *Luffa*”. In: *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*. Ed. by Antoine Joux. Vol. 6733. Lecture Notes in Computer Science. Springer, 2011, pp. 252–269. ISBN: 978-3-642-21701-2. DOI: 10.1007/978-3-642-21702-9_15. URL: https://doi.org/10.1007/978-3-642-21702-9_15.

[BC13b] Christina Boura and Anne Canteaut. “On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$”. In: *IEEE Trans. Information Theory* 59.1 (2013), pp. 691–702. DOI: 10.1109/TIT.2012.2214203. URL: https://doi.org/10.1109/TIT.2012.2214203.

[BC16] Christina Boura and Anne Canteaut. “Another View of the Division Property”. In: *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. Lecture Notes in Computer Science. Springer, 2016, pp. 654–682. ISBN: 978-3-662-53017-7. DOI: 10.1007/978-3-662-53018-4_24. URL: https://doi.org/10.1007/978-3-662-53018-4_24.

[JK01] Thomas Jakobsen and Lars R. Knudsen. “Attacks on Block Ciphers of Low Algebraic Degree”. In: *J. Cryptology* 14.3 (2001), pp. 197–210. DOI: 10.1007/s00145-001-0003-x. URL: https://doi.org/10.1007/s00145-001-0003-x.

References IV

[Eve87] Jan-Hendrik Evertse. "Linear Structures in Blockciphers". In: *Advances in Cryptology - EUROCRYPT '87, Workshop on the Theory and Application of of Cryptographic Techniques, Amsterdam, The Netherlands, April 13-15, 1987, Proceedings*. Ed. by David Chaum and Wyn L. Price. Vol. 304. LNCS. Springer, 1987, pp. 249–266. ISBN: 3-540-19102-X. DOI: 10.1007/3-540-39118-5_23. URL: https://doi.org/10.1007/3-540-39118-5_23.

[MS89] Willi Meier and Othmar Staffelbach. "Nonlinearity Criteria for Cryptographic Functions". In: *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Vol. 434. Lecture Notes in Computer Science. Springer, 1989, pp. 549–562. ISBN: 3-540-53433-4. DOI: 10.1007/3-540-46885-4_53. URL: https://doi.org/10.1007/3-540-46885-4_53.

[Lai94] Xuejia Lai. "Additive and Linear Structures of Cryptographic Functions". In: *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*. Ed. by Bart Preneel. Vol. 1008. LNCS. Springer, 1994, pp. 75–85. DOI: 10.1007/3-540-60590-8_6. URL: https://doi.org/10.1007/3-540-60590-8_6.

[Dub01] Sylvie Dubuc. "Characterization of Linear Structures". In: *Des. Codes Cryptography* 22.1 (2001), pp. 33–45.

[MT14] Rusydi H. Makarim and Cihangir Tezcan. "Relating Undisturbed Bits to Other Properties of Substitution Boxes". In: *Lightweight Cryptography for Security and Privacy - Third International Workshop, LightSec 2014, Istanbul, Turkey, September 1-2, 2014, Revised Selected Papers*. Ed. by Thomas Eisenbarth and Erdinç Öztürk. Vol. 8898. LNCS. Springer, 2014, pp. 109–125. ISBN: 978-3-319-16362-8. DOI: 10.1007/978-3-319-16363-5_7. URL: https://doi.org/10.1007/978-3-319-16363-5_7.

[ZZI00] Xian-Mo Zhang, Yuliang Zheng, and Hideki Imai. "Relating Differential Distribution Tables to Other Properties of Substitution Boxes". In: *Des. Codes Cryptography* 19.1 (2000), pp. 45–63. DOI: 10.1023/A:1008359713877. URL: https://doi.org/10.1023/A:1008359713877.

[BC13a] Christina Boura and Anne Canteaut. "A New Criterion for Avoiding the Propagation of Linear Relations Through an Sbox". In: *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*. Ed. by Shiho Moriai. Vol. 8424. Lecture Notes in Computer Science. Springer, 2013, pp. 585–604. ISBN: 978-3-662-43932-6. DOI: 10.1007/978-3-662-43933-3_30. URL: https://doi.org/10.1007/978-3-662-43933-3_30.

References V

[TLS16] Yosuke Todo, Gregor Leander, and Yu Sasaki. "Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64". In: *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10032. LNCS. 2016, pp. 3–33. ISBN: 978-3-662-53889-0. DOI: 10.1007/978-3-662-53890-6_1. URL: https://doi.org/10.1007/978-3-662-53890-6_1.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. "Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems". In: *Des. Codes Cryptography* 15.2 (1998), pp. 125–156. DOI: 10.1023/A:1008344232130. URL: https://doi.org/10.1023/A:1008344232130.

[Gla] Brian Gladman. *Finding Efficient Boolean Function Decompositions for the Serpent S-boxes and Their Inverses*. http://brg.a2hosted.com//oldsite/cryptography_technology/serpent/anal1.cpp. Accessed: 2018-11.

[Osv00] Dag Arne Osvik. "Speeding up Serpent". In: *AES Candidate Conference*. 2000, pp. 317–329.

[WS10] Dai Watanabe and Hitachi SDL. "How to Generate the S-box of Luffa". In: *Early Symmetric Crypto Seminar, ESC2010*. 2010.

[Ull+11] Markus Ullrich et al. "Finding Optimal Bitsliced Implementations of $4\times$ 4-bit S-boxes". In: *SKEW 2011 Symmetric Key Encryption Workshop, Copenhagen, Denmark*. 2011, pp. 16–17.

[BMP13] Joan Boyar, Philip Matthews, and René Peralta. "Logic Minimization Techniques with Applications to Cryptology". In: *J. Cryptology* 26.2 (2013), pp. 280–312. DOI: 10.1007/s00145-012-9124-7. URL: https://doi.org/10.1007/s00145-012-9124-7.

[CHM11] Nicolas Courtois, Daniel Hulme, and Theodosis Mourouzis. "Solving Circuit Optimisation Problems in Cryptography and Cryptanalysis". In: *IACR Cryptology ePrint Archive* 2011 (2011), p. 475. URL: http://eprint.iacr.org/2011/475.

References VI

[Sto16] Ko Stoffelen. "Optimizing S-Box Implementations for Several Criteria Using SAT Solvers". In: *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*. Ed. by Thomas Peyrin. Vol. 9783. Lecture Notes in Computer Science. Springer, 2016, pp. 140–160. ISBN: 978-3-662-52992-8. DOI: 10.1007/978-3-662-52993-5_8. URL: https://doi.org/10.1007/978-3-662-52993-5_8.

[Guo+16] Jian Guo et al. "Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs". In: *IACR Trans. Symmetric Cryptol.* 2016.1 (2016), pp. 33–56. DOI: 10.13154/tosc.v2016.i1.33-56. URL: https://doi.org/10.13154/tosc.v2016.i1.33-56.

[Jea+17] Jérémy Jean et al. "Optimizing Implementations of Lightweight Building Blocks". In: *IACR Trans. Symmetric Cryptol.* 2017.4 (2017), pp. 130–168. DOI: 10.13154/tosc.v2017.i4.130-168. URL: https://doi.org/10.13154/tosc.v2017.i4.130-168.

[MLCA] Rusydi H. Makarim, Yann Laigle-Chapuy, and Martin R. Albrecht. *SageMath 8.2: sage.crypto.sbox*. http://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/sbox.html. Accessed: 2018-11.

[Mag] *Magma Computational Algebra System*. http://magma.maths.usyd.edu.au. Accessed: 2018-11.

[FJ] Jean-Pierre Flori and Jérémy Jean. *libapn*. https://github.com/ANSSI-FR/libapn. Latest commit on Apr 2018.

[BPP00] Joan Boyar, René Peralta, and Denis Pochuev. "On the Multiplicative Complexity of Boolean Functions over the Basis $(\wedge, \oplus, 1)$". In: *Theor. Comput. Sci.* 235.1 (2000), pp. 43–57. DOI: 10.1016/S0304-3975(99)00182-6. URL: https://doi.org/10.1016/S0304-3975(99)00182-6.

[Ban+15] Subhadeep Banik et al. "Midori: A Block Cipher for Low Energy". In: *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*. Ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9453. Lecture Notes in Computer Science. Springer, 2015, pp. 411–436. ISBN: 978-3-662-48799-0. DOI: 10.1007/978-3-662-48800-3_17. URL: https://doi.org/10.1007/978-3-662-48800-3_17.

References VII

[Dae95] Joan Daemen. *Cipher and hash function design, strategies based on linear and differential cryptanalysis, PhD Thesis*. http://jda.noekeon.org/. K.U.Leuven, 1995.

[Pic+17] Stjepan Picek et al. "Evolving S-boxes based on cellular automata with genetic programming". In: *Genetic and Evolutionary Computation Conference, Berlin, Germany, July 15-19, 2017, Companion Material Proceedings*. Ed. by Peter A. N. Bosman. ACM, 2017, pp. 251–252. ISBN: 978-1-4503-4939-0. DOI: 10.1145/3067695.3076084. URL: http://doi.acm.org/10.1145/3067695.3076084.

[Mar+17] Luca Mariot et al. "Cellular Automata Based S-boxes". In: *IACR Cryptology ePrint Archive* 2017 (2017), p. 1055. URL: http://eprint.iacr.org/2017/1055.

[Wat10] Dai Watanabe. *How to generate the S-box of Luffa*. 2010. URL: http://www.cryptolux.org/mediawiki-esc2010/images/b/b7/Esc2010_watanabe_100111.pdf.

[Pre95] Bart Preneel, ed. *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*. Vol. 1008. LNCS. Springer, 1995. DOI: 10.1007/3-540-60590-8. URL: https://doi.org/10.1007/3-540-60590-8.