On Boolean Functions in Symmetric Cryptography

Valentin Suder

(Advisor: Pascale Charpin)

Project-Team SECRET

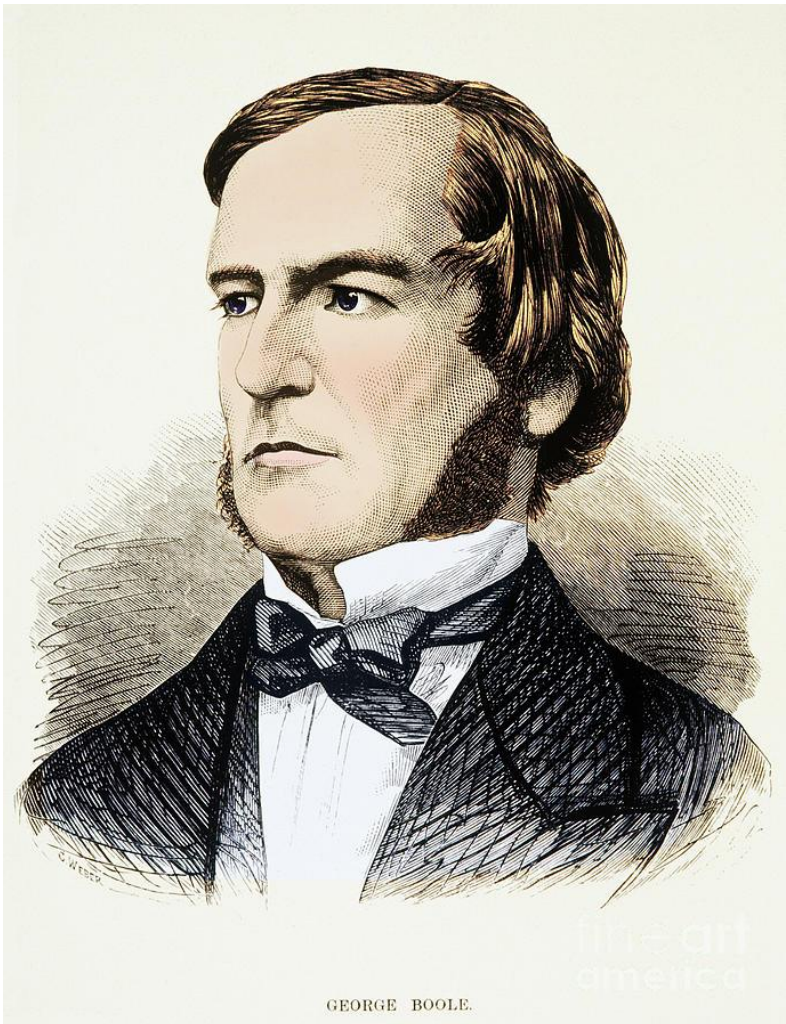
valentin.suder@inria.fr

Project-Team SECRET

SEcurité CRyptographie Et Transmission.

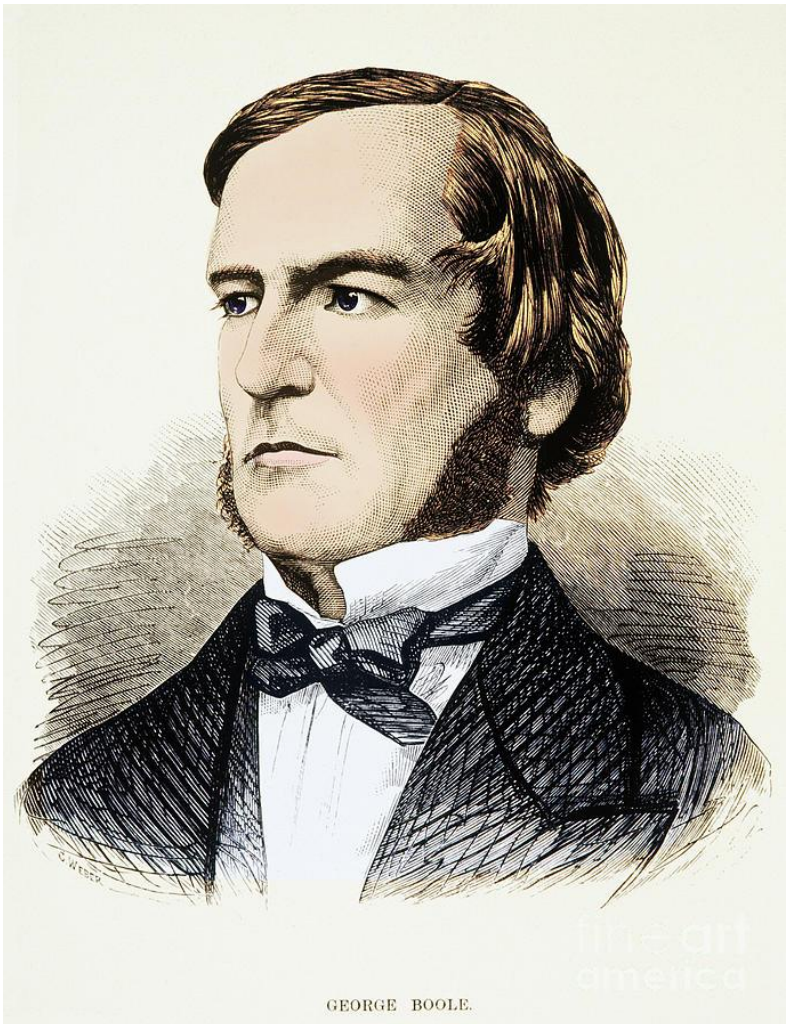
Outline

George Boole



- 2 November 1815 – 8 December 1864.
- English mathematician, philosopher and *logician*.
- known as a founder of the field of Computer Science.

George Boole



- 2 November 1815 – 8 December 1864.
- English mathematician, philosopher and *logician*.
- known as a founder of the field of Computer Science.
- Notable contribution:
  Boolean Algebra.

Boolean Algebra

— Possible values of the variables: TRUE or FALSE.

— Basic operations: AND, OR and NOT.

AND	FALSE	TRUE
FALSE	FALSE	FALSE
TRUE	FALSE	TRUE

OR	FALSE	TRUE
FALSE	FALSE	TRUE
TRUE	TRUE	TRUE

	NOT
FALSE	TRUE
TRUE	FALSE

Many other operations can be built from these basic operations.

Boolean Algebra

First introduced by G. Boole in "*An Investigation of the Laws of Thought*", 1854.

The term "Boolean Algebra" is suggested by *Sheffer* in 1913.

Boolean Algebra (a.k.a. *digital logic*) is fundamental in Computer Science, Set Theory, Statistics...

Backgrounds

Preliminaries

Example

Is taking my umbrella a good option?

Example

Is taking my umbrella a good option?

1. Is it raining?

Example

Is taking my umbrella a good option?

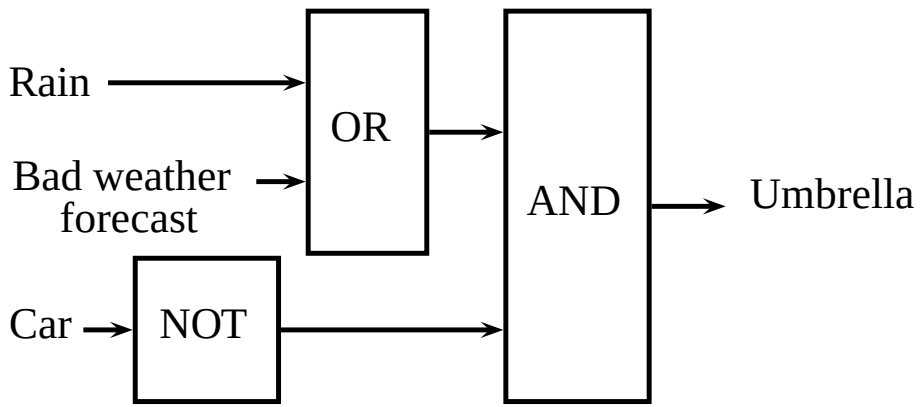
1. Is it raining?

2. Bad weather forecast?

Example

Is taking my umbrella a good option?

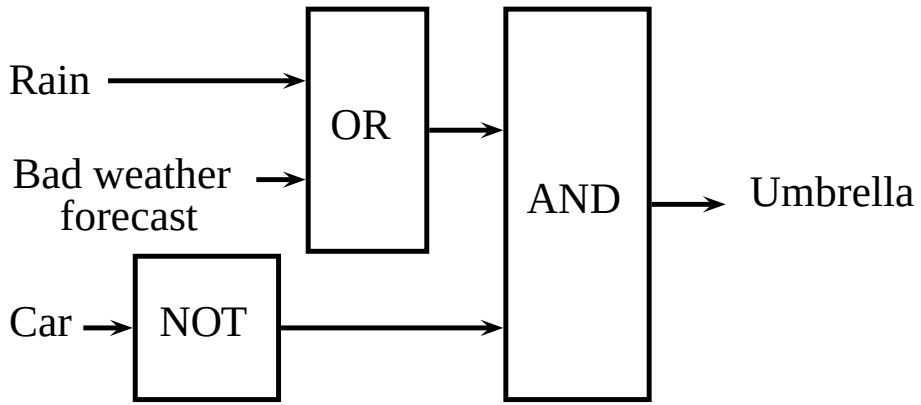
1. Is it raining?
2. Bad weather forecast?
3. But . . . do I go by car?



Example

Is taking my umbrella a good option?

1. Is it raining?
2. Bad weather forecast?
3. But . . . do I go by car?



Rain	x	✓	x	✓	x	✓	x	✓
Bad weather forecast	x	x	✓	✓	x	x	✓	✓
Car	x	x	x	x	✓	✓	✓	✓
Umbrella	x	✓	✓	✓	x	x	x	x

Definitions

Boolean Functions

Binary Representation

$\mathbb{F}_2 = (\{0,1\}, \oplus, \cdot)$: Finite Field of 2 elements.

$$1, 0 \longleftrightarrow \text{TRUE, FALSE,}$$
$$\oplus \text{ (addition modulo 2)} \longleftrightarrow \text{XOR (Exclusive OR),}$$
$$\cdot \longleftrightarrow \text{AND.}$$

Remark:

$$XOR(A, B) = OR(AND(A, NOT(B)), AND(NOT(A), B)).$$

XOR	FALSE	TRUE
FALSE	FALSE	TRUE
TRUE	TRUE	FALSE

Boolean Functions

Truth table of a Boolean function.

x_0	0	1	0	1	0	1	0	1
x_1	0	0	1	1	0	0	1	1
x_2	0	0	0	0	1	1	1	1
$f(x_0, x_1, x_2)$	0	1	1	1	0	0	0	0

Definition

A *Boolean function* of n variables is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$.

$$\begin{array}{rccc} f: & \mathbb{F}_2^n & \to & \mathbb{F}_2 \\ & (x_0, \ldots, x_{n-1}) & \mapsto & f(x_0, \ldots, x_{n-1}). \end{array}$$

Boolean Functions

Value vector of f: word of 2^n bits consisting of every $f(x)$, for $x \in \mathbb{F}_2^n$.

Example: $f(x_0, x_1, x_2) = (0, 1, 1, 1, 0, 0, 0, 0)$.

Definition [Hamming weight]

The Hamming weight of a Boolean function f, $wt(f)$, is the *binary weight* of its value vector.

Example: $wt(f) = wt(0, 1, 1, 1, 0, 0, 0, 0) = 3$.

A Boolean function of n variables is *balanced* if and only if $wt(f) = 2^{n-1}$.

Algebraic Normal Form (ANF)

Proposition

Any Boolean function f of n variables has a unique multivariate polynomial representation:

$$f(x_0, \ldots, x_{n-1}) = \bigoplus_{u=(u_0,\ldots,u_{n-1}) \in \mathbb{F}_2^n} a_u x^u, \qquad x^u = \prod_{i=0}^{n-1} x_i^{u_i},$$

and $a_u \in \mathbb{F}_2$.

Example:

$$\begin{aligned} x^{110} &= x_0 x_1 \\ f(x_0, x_1, x_2) &= x_0 \oplus x_0 x_1 \oplus x_0 x_1 x_2. \end{aligned}$$

Moreover, the coefficients of the ANF and the value of f satisfy:

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

where $x \preceq u$ if and only if $x_i \leq u_i$ for all i.

Example

x_0	0	1	0	1	0	1	0	1
x_1	0	0	1	1	0	0	1	1
x_2	0	0	0	0	1	1	1	1
$f(x_0, x_1, x_2)$	0	1	1	1	0	0	0	0

$$a_{000} = f(000) = 0$$
$$a_{100} = f(000) \oplus f(100) = 1$$
$$a_{010} = f(000) \oplus f(010) = 1$$
$$a_{110} = f(000) \oplus f(100) \oplus f(010) \oplus f(110) = 1$$
$$a_{001} = f(000) \oplus f(001) = 0$$
$$a_{101} = f(000) \oplus f(100) \oplus f(001) \oplus f(101) = 1$$
$$a_{011} = f(000) \oplus f(010) \oplus f(001) \oplus f(011) = 1$$
$$a_{111} = \bigoplus_{x \in \mathbb{F}_2^3} f(x) = wt(f) \pmod 2 = 1.$$

Then $f(x) = x_0 \oplus x_1 \oplus x_0x_1 \oplus x_0x_2 \oplus x_1x_2 \oplus x_0x_1x_2$.

Definitions

Vectorial Boolean Functions

Vectorial Boolean Functions

Definition [Vectorial Boolean Function]

A vectorial Boolean function of n *inputs* and m *outputs* ((n, m)-function) is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$:

$$\begin{array}{rccc} F: & \mathbb{F}_2^n & \to & \mathbb{F}_2^m \\ & (x_0, \ldots, x_{n-1}) & \mapsto & (y_0, \ldots, y_{m-1}). \end{array}$$

The Boolean functions $f_i: (x_0, \ldots, x_{n-1}) \mapsto y_i$, $0 \leq i \leq m-1$, are called the coordinate functions.

Linear combinations of the *coordinate functions*:

$$x \mapsto \lambda \cdot (f_0(x), \ldots, f_{m-1}(x)), \ \lambda \in \mathbb{F}_2^m, \ \lambda \neq 0,$$

are called the component functions.

Proposition

An (n, n)-function is a permutation of $\mathbb{F}_2^n$ if and only if all its *component functions* are balanced.

Example of a Vectorial Boolean Function

$n = 4$

$$
\begin{array}{lcl}
0 & \leftrightarrow & (0,0,0,0) \\
1 & \leftrightarrow & (1,0,0,0) \\
2 & \leftrightarrow & (0,1,0,0) \\
3 & \leftrightarrow & (1,1,0,0) \\
4 & \leftrightarrow & (0,0,1,0) \\
5 & \leftrightarrow & (1,0,1,0) \\
6 & \leftrightarrow & (0,1,1,0) \\
7 & \leftrightarrow & (1,1,1,0)
\end{array}
\qquad
\begin{array}{lcl}
8 & \leftrightarrow & (0,0,0,1) \\
9 & \leftrightarrow & (1,0,0,1) \\
a & \leftrightarrow & (0,1,0,1) \\
b & \leftrightarrow & (1,1,0,1) \\
c & \leftrightarrow & (0,0,1,1) \\
d & \leftrightarrow & (1,0,1,1) \\
e & \leftrightarrow & (0,1,1,1) \\
f & \leftrightarrow & (1,1,1,1)
\end{array}
$$

Example of a Vectorial Boolean Function

$n = 4$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S_0(x)$	1	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1
$S_1(x)$	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0
$S_2(x)$	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1
$S_3(x)$	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	0

$x = (x_0, x_1, x_2, x_3)$:

$$S_0(x) = 1 + x_0 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_2x_3 + x_1x_2x_3$$
$$S_1(x) = 1 + x_3 + x_0x_1 + x_0x_2 + x_0x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3$$
$$S_2(x) = 1 + x_1 + x_3 + x_0x_1 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_1x_3 + x_0x_2x_3$$
$$S_3(x) = 1 + x_2 + x_3 + x_0x_2 + x_1x_3 + x_2x_3 + x_0x_2x_3 + x_1x_2x_3$$

Identifying $\mathbb{F}_2^n$ with the Finite Field $\mathbb{F}_{2^n}$

Let α be a root of an *irreducible polynomial* of degree n over $\mathbb{F}_2$. The Finite Field $\mathbb{F}_{2^n}$ consists of every linear combinations of elements $1, \alpha, \ldots, \alpha^{n-1}$ over $\mathbb{F}_2$.

$$\begin{array}{rccc} \varphi: & \mathbb{F}_2^n & \simeq & \mathbb{F}_{2^n} \\ (x_0, \ldots, x_{n-1}) & \mapsto & \sum_{i=0}^{n-1} x_i \alpha^i, & \end{array}$$

Example: $n = 4$, α a root of the *irreducible polynomial* $1 + x + x^4$.

	0	1	2	3	4	5	6	7
$\mathbb{F}_2^4$	$(0,0,0,0)$	$(1,0,0,0)$	$(0,1,0,0)$	$(1,1,0,0)$	$(0,0,1,0)$	$(1,0,1,0)$	$(0,1,1,0)$	$(1,1,1,0)$
$\mathbb{F}_{2^4}$	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
$\mathbb{F}_{2^4}$	0	1	α	α^4	α^2	α^8	α^5	α^{10}

	8	9	a	b	c	d	e	f
$\mathbb{F}_2^4$	$(0,0,0,1)$	$(1,0,0,1)$	$(0,1,0,1)$	$(1,1,0,1)$	$(0,0,1,1)$	$(1,0,1,1)$	$(0,1,1,1)$	$(1,1,1,1)$
$\mathbb{F}_{2^4}$	α^3	$1+\alpha^3$	$\alpha+\alpha^3$	$1+\alpha+\alpha^3$	$\alpha^2+\alpha^3$	$1+\alpha^2+\alpha^3$	$\alpha+\alpha^2+\alpha^3$	$1+\alpha+\alpha^2+\alpha^3$
$\mathbb{F}_{2^4}$	α^3	α^{14}	α^9	α^7	α^6	α^{13}	α^{11}	α^{12}

Univariate Polynomial Representation

Proposition

Any (n, n)-function F admits a unique univariate polynomial representation over $\mathbb{F}_{2^n}$, of degree at most $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \qquad c_i \in \mathbb{F}_{2^n}.$$

Univariate Polynomial Representation

Example: $n = 4$

α a root of the *primitive polynomial* $1 + x + x^4$.

x	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
$S(x)$	α^{12}	α^{11}	α^7	α^5	0	α^6	α^{10}	α^2	α^9	α^{13}	α^{14}	α^3	1	α^8	α	α^4

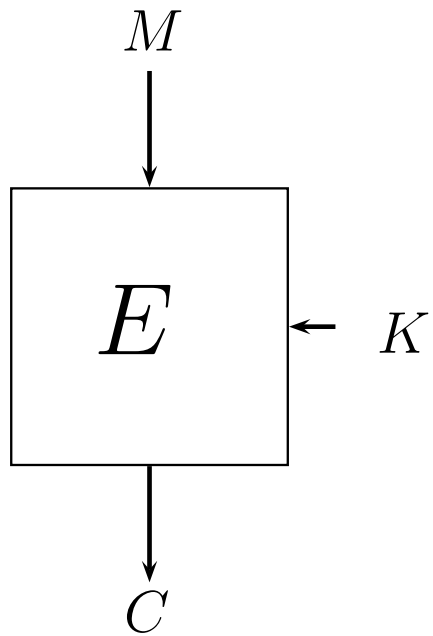
$$S(x) = \alpha^{12} + \alpha^2 x + \alpha^{13} x^2 + \alpha^6 x^3 + \alpha^{10} x^4 + \alpha x^5 + \alpha^{10} x^6 + \alpha^2 x^7 + \alpha^9 x^8 + \alpha^4 x^9 + \alpha^7 x^{10} + \alpha^7 x^{11} + \alpha^5 x^{12} + x^{13} + \alpha^6 x^{14}.$$

Symmetric Cryptography

Block Ciphers

Block Ciphers

$M \in \mathbb{F}_2^m$: plaintext,
$C \in \mathbb{F}_2^m$: ciphertext,
$K \in \mathbb{F}_2^k$: key.



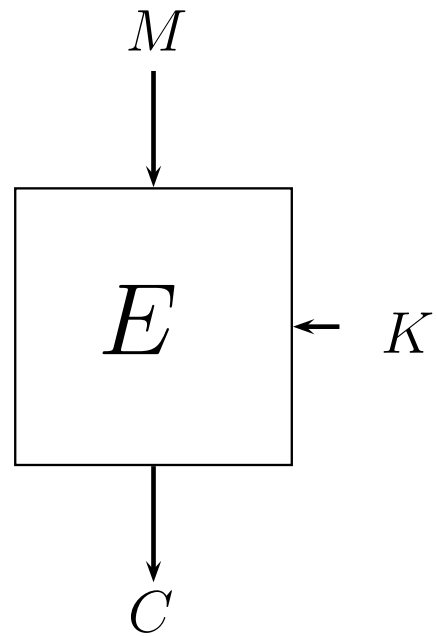
Block Cipher

$$E: \quad \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$$
$$(M, K) \mapsto E(M, K) = C.$$

For a fixed key $K \in \mathbb{F}_2^k$,
$E_K(M) \mapsto C$, is a permutation of $\mathbb{F}_2^m$.

Block Ciphers

$M \in \mathbb{F}_2^m$: plaintext,
$C \in \mathbb{F}_2^m$: ciphertext,
$K \in \mathbb{F}_2^k$: key.



Block Cipher

$$E: \quad \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$$
$$(M, K) \mapsto E(M, K) = C.$$

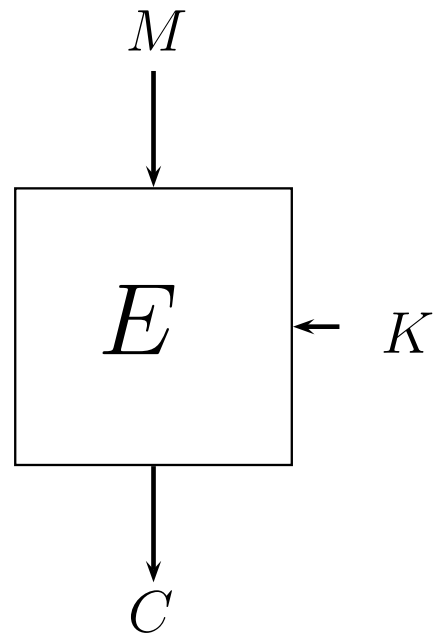
For a fixed key $K \in \mathbb{F}_2^k$,
$E_K(M) \mapsto C$, is a permutation of $\mathbb{F}_2^m$.

Problems? In practice: $m \geq 64$ and $k \geq 80$ (!!!)

- For one key K, E_K permutes 2^{64} elements!

Block Ciphers

$M \in \mathbb{F}_2^m$: plaintext,
$C \in \mathbb{F}_2^m$: ciphertext,
$K \in \mathbb{F}_2^k$: key.



Block Cipher

$$E: \quad \mathbb{F}_2^m \times \mathbb{F}_2^k \to \mathbb{F}_2^m$$
$$(M, K) \mapsto E(M, K) = C.$$

For a fixed key $K \in \mathbb{F}_2^k$,
$E_K(M) \mapsto C$, is a permutation of $\mathbb{F}_2^m$.

Problems? In practice: $m \geq 64$ and $k \geq 80$ (!!!)

- For one key K, E_K permutes 2^{64} elements!
- 2^{80} different permutations!

Substitution Permutation Networks

Add Round Key

$$\begin{array}{rcl} \mathbb{F}_2^m x \mathbb{F}_2^m & \rightarrow & \mathbb{F}_2^m \\ (M, SubK) & \mapsto & M \oplus SubK. \end{array}$$

$M = (M_0, \ldots, M_{m/n-1})$, $M_i \in \mathbb{F}_2^n$ (word).

SBox (substitution)

Nonlinear Permutation:

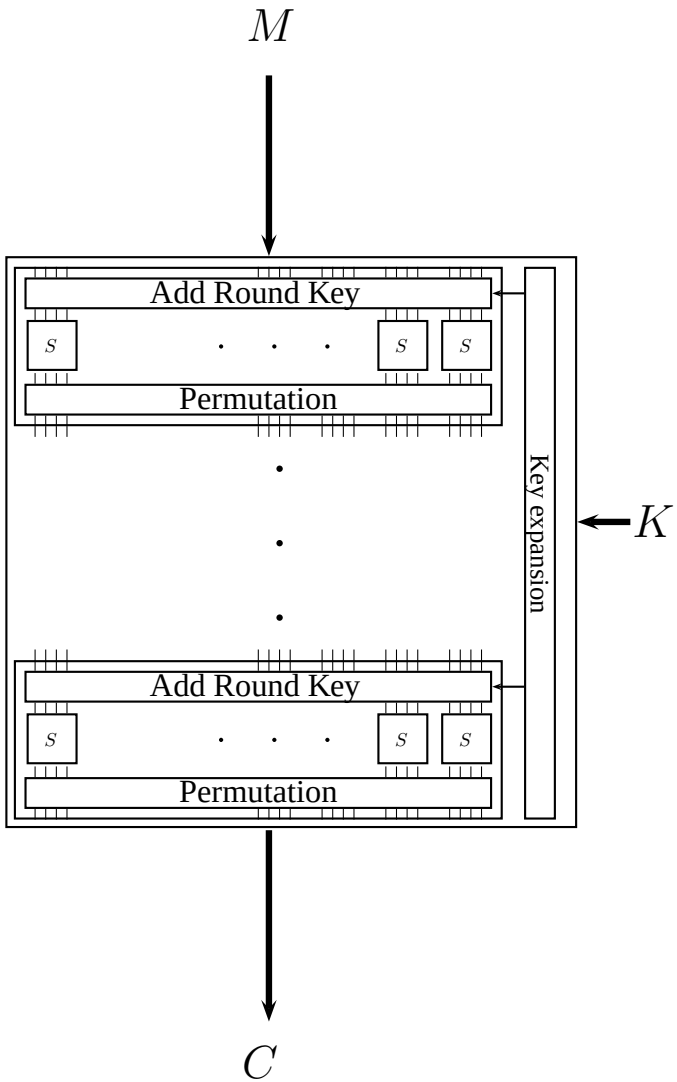
$$\begin{array}{rcl} S: \quad \mathbb{F}_2^n & \rightarrow & \mathbb{F}_2^n \\ M_i & \mapsto & (S_0(M_i), \ldots, S_{n-1}(M_i)). \end{array}$$

In practice: $n = 4,\ 8$.

Permutation (diffusion)

Linear Permutation:

$$\mathbb{F}_2^m \rightarrow \mathbb{F}_2^m.$$



Example of an SBox

$n = 4$

Multivariate:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S_0(x)$	1	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1
$S_1(x)$	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0
$S_2(x)$	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1
$S_3(x)$	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	0

Univariate:

x	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
$S(x)$	α^{12}	α^{11}	α^7	α^5	0	α^6	α^{10}	α^2	α^9	α^{13}	α^{14}	α^3	1	α^8	α	α^4

Example of an SBox

$n = 4$

Multivariate:

$$S_0(x) = 1 + x_0 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_2x_3 + x_1x_2x_3$$
$$S_1(x) = 1 + x_3 + x_0x_1 + x_0x_2 + x_0x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3$$
$$S_2(x) = 1 + x_1 + x_3 + x_0x_1 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_1x_3 + x_0x_2x_3$$
$$S_3(x) = 1 + x_2 + x_3 + x_0x_2 + x_1x_3 + x_2x_3 + x_0x_2x_3 + x_1x_2x_3$$

Univariate:

$$S(x) = \alpha^{12} + \alpha^2 x + \alpha^{13}x^2 + \alpha^6 x^3 + \alpha^{10}x^4 + \alpha x^5 + \alpha^{10}x^6 + \alpha^2 x^7 + \alpha^9 x^8 + \alpha^4 x^9 + \alpha^7 x^{10} + \alpha^7 x^{11} + \alpha^5 x^{12} + x^{13} + \alpha^6 x^{14}.$$

Symmetric Cryptography

Cryptographic Properties

Algebraic Degree of a Vectorial Boolean Function

Algebraic Degree

- The algebraic degree of a *Boolean function* $f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u$ is

$$deg_{alg}(f) = \max_{u \in \mathbb{F}_2^n} \{wt(u) \mid a_u = 1\}.$$

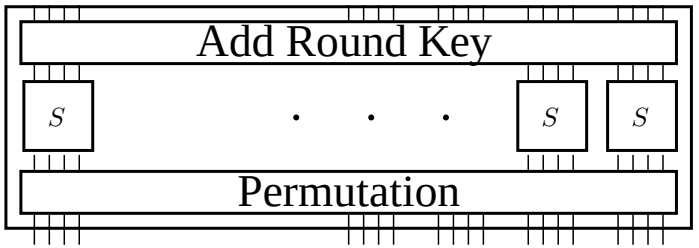
Example: $f(x_0, x_1, x_2) = x_0 \oplus x_0x_1 \oplus x_0x_1x_2$.
The Hamming weight of a Boolean function of n variables f, $wt(f)$, is odd *if and only if* $deg_{alg}(f) = n$.

Algebraic Degree

- The algebraic degree of a (n, m)-*function* F with coordinates $f_0, \ldots, f_{m-1}$ is

$$deg_{alg}(F) = \max_{0 \leq i \leq m-1} deg_{alg}(f_i).$$

Algebraic Degree



SBox: $S = (S_0, \ldots, S_{n-1})$.
Plaintext: $x = (x_0, \ldots, x_{n-1})$ (known).
Key: $\kappa = (k_0, \ldots, k_{n-1})$ (unknown).

Nonlinear system of m equations and m unknowns.

For all coordinate functions S_i,

$$S_i(x + \kappa) = \bigoplus_u s_u (x + \kappa)^u.$$

Example: $n = 4$,

$$\begin{aligned}(x + \kappa)^{0110} &= (x_1 \oplus k_1) \cdot (x_2 \oplus k_2) \\ &= x_1 x_2 \oplus x_1 k_2 \oplus x_2 k_1 \oplus k_1 k_2.\end{aligned}$$

Algebraic Degree

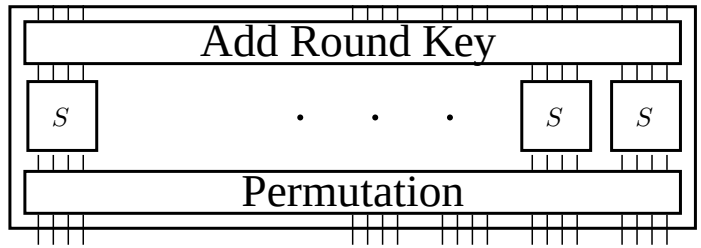
SBox: $S = (S_0, \ldots, S_{n-1})$.
Plaintext: $x = (x_0, \ldots, x_{n-1})$ (known).
Key: $\kappa = (k_0, \ldots, k_{n-1})$ (unknown).

For all coordinate functions S_i,

$$S_i(x + \kappa) = \bigoplus_u s_u (x + \kappa)^u.$$

Example: $n = 4$,

$$\begin{aligned}(x + \kappa)^{0110} &= (x_1 \oplus k_1) \cdot (x_2 \oplus k_2) \\ &= x_1 x_2 \oplus y_0 \oplus y_1 \oplus y_2.\end{aligned}$$



Nonlinear system of m equations and m unknowns.

$\Downarrow$

Linear system of m equations and $> m$ unknowns.

The lower the *algebraic degree* is, the less unknowns we have, the easier to resolve the system is.

Univariate degree

Univariate Degree

- The univariate degree of a (n, n)-*function* $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$ is

$$deg(F) = \max_{0 \leq i \leq 2^n-1} \{i \mid c_i \neq 0\}.$$

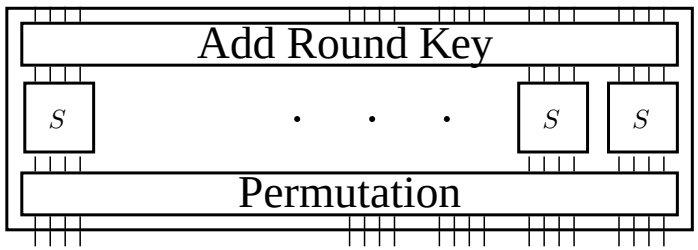
Remark:

The algebraic degree of a function $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$ is

$$deg_{alg}(F) = \max_{0 \leq i \leq 2^n-1} \{wt(i) \mid c_i \neq 0\}.$$

Univariate Degree

The univariate degree of the SBox, $deg(S)$, influences the univariate degree of the cipher E_K (and does not depend on K).



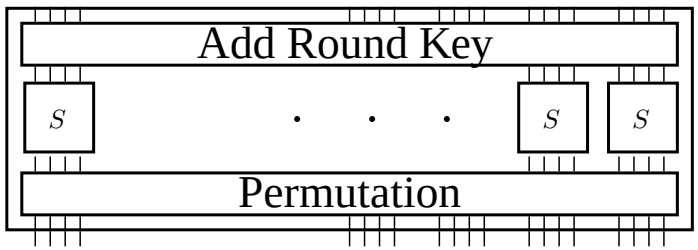
If $deg(E_K^{-1}) = d$ is "sufficiently" low

$$\Downarrow$$

with $d + 1$ pairs (C_i, M_i) of ciphertext/plaintext we can interpolate a unique polynomial E' of degree d such that $E'(C_i) = M_i$, $0 \leq i \leq d$.

Univariate Degree

The univariate degree of the SBox, $deg(S)$, influences the univariate degree of the cipher E_K (and does not depend on K).



If $deg(E_K^{-1}) = d$ is "sufficiently" low

$\Downarrow$

with $d + 1$ pairs (C_i, M_i) of ciphertext/plaintext we can interpolate a unique polynomial E' of degree d such that $E'(C_i) = M_i$, $0 \leq i \leq d$.

In conclusion, for every $C \in \mathbb{F}_{2^m}$,

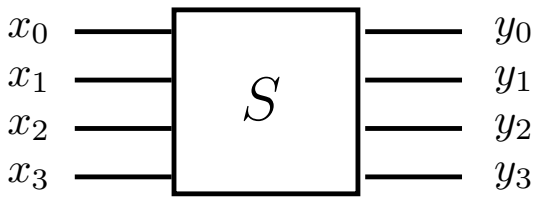
$$E'(C) = E_K^{-1}(C) = M.$$

Differential Property

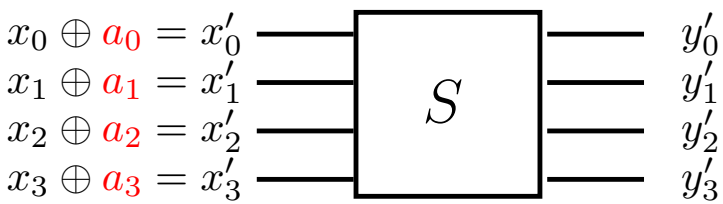
Definition

The differential uniformity of an SBox S is defined as

$$\delta(S) = \max_{a \neq 0,\ b \in \mathbb{F}_{2^n}} \#\{x \mid S(x) + S(x+a) = b\}.$$



$$y + y' = ?$$



S is Almost Perfect Nonlinear (APN) if and only if $\delta(S) = 2$.

Design Problem

Practical Requirements

What do we want for a *"good"* SBox?

What do we want for a *"good"* SBox?

- a high algebraic degree,

What do we want for a *"good"* SBox?

- a high algebraic degree,
- a high univariate degree,

What do we want for a *"good"* SBox?

- a high algebraic degree,
- a high univariate degree,
- a "low" differential uniformity,

What do we want for a *"good"* SBox?

- a high algebraic degree,
- a high univariate degree,
- a "low" differential uniformity,
- a "good" hardware/sofware implementation,

What do we want for a *"good"* SBox?

- a high algebraic degree,
- a high univariate degree,
- a "low" differential uniformity,
- a "good" hardware/sofware implementation,

⋮

What do we want for a *"good"* SBox?

- a high algebraic degree,
- a high univariate degree,
- a "low" differential uniformity,
- a "good" hardware/sofware implementation,

  ⋮

\+ a permutation,

What do we want for a *"good"* SBox?

- a high algebraic degree,
- a high univariate degree,
- a "low" differential uniformity,
- a "good" hardware/sofware implementation,

  ⋮

\+ a permutation,

\+ an inverse verifying all of these requirements (!!)

We already know that $\delta(S) = \delta(S^{-1})$.

Design Problem

APN Permutations

APN Permutations on $\mathbb{F}_{2^n}$

- n is odd: x^r for some (few) integers r.
  When $3|n$ but $9 \nmid n$, one of the shape $x^s + \gamma x^t$.

APN Permutations on $\mathbb{F}_{2^n}$

- n is odd: x^r for some (few) integers r.
  When $3|n$ but $9 \nmid n$, one of the shape $x^s + \gamma x^t$.
- $n = 4$: No APN Permutations.

APN Permutations on $\mathbb{F}_{2^n}$

- n is odd: x^r for some (few) integers r.
  When $3|n$ but $9 \nmid n$, one of the shape $x^s + \gamma x^t$.
- $n = 4$: No APN Permutations.
- $n = 6$: Dillon's function ['09]:

$$\begin{aligned}D(x) = {} & \alpha^{36}x^{60} + \alpha^{44}x^{58} + \alpha^{40}x^{57} + \alpha^{55}x^{56} + \alpha^{26}x^{54} + \alpha^{23}x^{53} \\ & + \alpha^{36}x^{52} + \alpha^{23}x^{51} + \alpha^{17}x^{50} + \alpha^{54}x^{49} + \alpha^{14}x^{48} \\ & + \alpha^{21}x^{46} + \alpha^{53}x^{45} + \alpha^{21}x^{44} + \alpha^{7}x^{43} + \alpha^{57}x^{42} \\ & + \alpha^{8}x^{41} + \alpha^{10}x^{40} + \alpha^{12}x^{39} + \alpha^{20}x^{38} + \alpha^{52}x^{37} \\ & + \alpha^{46}x^{36} + \alpha^{27}x^{35} + \alpha^{44}x^{34} + \alpha^{18}x^{33} + \alpha^{57}x^{32} \\ & + \alpha^{28}x^{30} + \alpha^{44}x^{29} + \alpha^{42}x^{28} + \alpha^{26}x^{27} + \alpha^{20}x^{26} \\ & + \alpha^{10}x^{25} + \alpha^{45}x^{24} + x^{23} + \alpha^{7}x^{22} + \alpha^{57}x^{21} + \alpha^{21}x^{20} \\ & + \alpha^{22}x^{19} + \alpha^{6}x^{17} + \alpha^{8}x^{16} + \alpha^{43}x^{15} + \alpha^{42}x^{13} \\ & + \alpha^{47}x^{12} + \alpha^{56}x^{11} + \alpha^{38}x^{10} + \alpha^{36}x^{8} + \alpha^{47}x^{7} \\ & + \alpha^{4}x^{6} + \alpha^{8}x^{5} + \alpha^{23}x^{4} + \alpha^{39}x^{3} + \alpha^{52}x^{2} + \alpha^{59}x.\end{aligned}$$

APN Permutations on $\mathbb{F}_{2^n}$

- n is odd: x^r for some (few) integers r.
  When $3|n$ but $9 \nmid n$, one of the shape $x^s + \gamma x^t$.
- $n = 4$: No APN Permutations.
- $n = 6$: Dillon's function ['09]:

$$\begin{aligned} D(x) = {} & \alpha^{36}x^{60} + \alpha^{44}x^{58} + \alpha^{40}x^{57} + \alpha^{55}x^{56} + \alpha^{26}x^{54} + \alpha^{23}x^{53} \\ & + \alpha^{36}x^{52} + \alpha^{23}x^{51} + \alpha^{17}x^{50} + \alpha^{54}x^{49} + \alpha^{14}x^{48} \\ & + \alpha^{21}x^{46} + \alpha^{53}x^{45} + \alpha^{21}x^{44} + \alpha^{7}x^{43} + \alpha^{57}x^{42} \\ & + \alpha^{8}x^{41} + \alpha^{10}x^{40} + \alpha^{12}x^{39} + \alpha^{20}x^{38} + \alpha^{52}x^{37} \\ & + \alpha^{46}x^{36} + \alpha^{27}x^{35} + \alpha^{44}x^{34} + \alpha^{18}x^{33} + \alpha^{57}x^{32} \\ & + \alpha^{28}x^{30} + \alpha^{44}x^{29} + \alpha^{42}x^{28} + \alpha^{26}x^{27} + \alpha^{20}x^{26} \\ & + \alpha^{10}x^{25} + \alpha^{45}x^{24} + x^{23} + \alpha^{7}x^{22} + \alpha^{57}x^{21} + \alpha^{21}x^{20} \\ & + \alpha^{22}x^{19} + \alpha^{6}x^{17} + \alpha^{8}x^{16} + \alpha^{43}x^{15} + \alpha^{42}x^{13} \\ & + \alpha^{47}x^{12} + \alpha^{56}x^{11} + \alpha^{38}x^{10} + \alpha^{36}x^{8} + \alpha^{47}x^{7} \\ & + \alpha^{4}x^{6} + \alpha^{8}x^{5} + \alpha^{23}x^{4} + \alpha^{39}x^{3} + \alpha^{52}x^{2} + \alpha^{59}x. \end{aligned}$$

- $n \geq 8$: ???

Thank you!