Introduction to cryptography

2A. Intermezzo: design of symmetric primitives

Gilles Van Assche
Olivier Markowitch

INFO-F-405
Université Libre de Bruxelles
2020-2021

Bit transposition vs permutation

Bit transposition $\Pi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$, with

$$(x_1, x_2, \ldots, x_n) = \Pi(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$$

for some permutation of the bit positions $1 \ldots n$.

not to be confused with

Permutation $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$, any bijective mapping within $\mathbb{Z}_2^n$.

Example of bit transposition

Let $n = 3$. There are $3! = 6$ possible bit transpositions over 3 bits. As an example, let us swap the first and last bits:

$x_1x_2x_3$	$\Pi(x_1, x_2, x_3)$
000	000
001	100
010	010
011	110
100	001
101	101
110	011
111	111

Other examples:

- DES: IP and the "permutation" P in F
- AES: `ShiftRows`
- KECCAK-f: π and ρ

Example of permutation

Let $n = 3$. There are $(2^3)! = 40320$ possible permutations over 3 bits. Let us build an arbitrary example by assigning each value once on the right hand side of the truth table:

$x_1x_2x_3$	$f(x_1, x_2, x_3)$
000	011
001	101
010	010
011	001
100	110
101	000
110	100
111	111

A bit transposition is a permutation, but not vice-versa in general.

Linearity and affinity

Let f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$, and let $\oplus$ denote the bitwise addition modulo 2.

Linearity

The function f is **linear** iff

$$\forall x, y \in \mathbb{Z}_2^n \ : \ f(x \oplus y) = f(x) \oplus f(y).$$

Affinity

The function f is **affine** iff

$$\forall x, y \in \mathbb{Z}_2^n \ : \ f(x \oplus y) = f(x) \oplus f(y) \oplus f(0^n).$$

Note: a linear function is also affine.

Linearity and affinity

Let f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$, and let $\oplus$ denote the bitwise addition modulo 2.

Linearity

The function f is **linear** iff

$$\forall x, y \in \mathbb{Z}_2^n \; : \; f(x \oplus y) = f(x) \oplus f(y).$$

Affinity

The function f is **affine** iff

$$\forall x, y \in \mathbb{Z}_2^n \; : \; f(x \oplus y) = f(x) \oplus f(y) \oplus f(0^n).$$

Note: a linear function is also affine.

Linearity and affinity

Let f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$, and let $\oplus$ denote the bitwise addition modulo 2.

Linearity

The function f is **linear** iff

$$\forall x, y \in \mathbb{Z}_2^n \ : \ f(x \oplus y) = f(x) \oplus f(y).$$

Affinity

The function f is **affine** iff

$$\forall x, y \in \mathbb{Z}_2^n \ : \ f(x \oplus y) = f(x) \oplus f(y) \oplus f(0^n).$$

Note: a linear function is also affine.

Linearity and affinity

Examples of linear functions:

- $f(x) = 0$
- $f(x, y) = x \oplus y$
- bit transpositions
- composition of the above

Examples of affine functions:

- $f(x) = x \oplus \text{constant}$
- linear functions
- composition of the above

Non-linearity

Let f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$, and let $\oplus$ denote the bitwise addition modulo 2.

Non-linearity

In the context of this class, the function f is **non-linear** if it is not affine (and therefore not linear).

Example: $f : \mathbb{Z}_2^2 \to \mathbb{Z}_2 : f(a, b) = ab$

$$f(1,0) = 0$$
$$f(0,1) = 0$$
$$f(1,1) = 1 \neq f(1,0) + f(0,1)$$

Non-linearity

Let f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$, and let $\oplus$ denote the bitwise addition modulo 2.

Non-linearity

In the context of this class, the function f is **non-linear** if it is not affine (and therefore not linear).

Example: $f : \mathbb{Z}_2^2 \to \mathbb{Z}_2 : f(a, b) = ab$

$$
\begin{aligned}
f(1,0) &= 0 \\
f(0,1) &= 0 \\
f(1,1) &= 1 \neq f(1,0) + f(0,1)
\end{aligned}
$$

Diffusion

Let f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$.

Diffusion

The function f provides **diffusion** if at least one input bit influences more than one output bit.

Example:

$$f : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2 : f(a, b) = (a, a + b)$$

Here the input a influences both output bits.

Diffusion

Let f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$.

Diffusion

The function f provides **diffusion** if at least one input bit influences more than one output bit.

Example:

$$f : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2 : f(a, b) = (a, a + b)$$

Here the input a influences both output bits.

Bend-mix-notch-shuffle

In primitives, we often would like that each output bit depends in a complicated (non-linear, non-symmetric) way on all in the input bits.

Idea: repeat a sequence of operations (=a round) that

- **bends** $\Rightarrow$ apply a non-linear mapping
- **mixes** $\Rightarrow$ apply a (usually, linear) mapping that diffuses to a number of bits
- **notches** $\Rightarrow$ do something to break the symmetry
- **shuffles** $\Rightarrow$ move the bits around to ensure global diffusion

[Terminology: idea of Joan Daemen]