Differential Cryptanalysis

May 12, 2024

Ji, Yong-hyeon
x

1 Definitions

1.1 S-Box

$$n\text{-bit } 01010\cdots \longrightarrow \boxed{\text{S-Box}} \longrightarrow m\text{-bit } 11001\cdots$$

S-Box

Definition 1. Let $n, m \in \mathbb{Z}^+$. A function

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

is a **S-Box**.

1.2 The XOR operation

$$\begin{array}{rccl} \oplus & : & \mathbb{F}_2 \times \mathbb{F}_2 & \longrightarrow & \mathbb{F}_2 \\ & & (x, y) & \longmapsto & z = x + y \bmod 2 \end{array}$$

x	y	$z = x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

Note (Thinking)**.**

$$\begin{array}{rccl} \oplus & : & \mathbb{F}_2 & \longrightarrow & [\mathbb{F}_2 \to \mathbb{F}_2] \\ & & x & \longmapsto & \oplus_x = \begin{cases} \mathrm{Id}(y) & : x = 0, \\ \neg(y) & : x = 1. \end{cases} \end{array}$$

$$\begin{array}{rccl} \oplus_n & : & \mathbb{F}_2^n \times \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^n \\ & & \left(\{x_i\}_{i=1}^n, \{y_i\}_{i=1}^n\right) & \longmapsto & \{x_i \oplus y_i\}_{i=1}^n \end{array}$$

Note. We use the notation 0_n to denote $0_n = (0, \ldots, 0)$.

Note (Thinking)**.**

$$\begin{array}{rcccl} \oplus_n & : & \mathbb{F}_2^n & \longrightarrow & [\mathbb{F}_2^n \to \mathbb{F}_2^n] \\ & & \{x_i\}_{i=1}^n & \longmapsto & (\oplus_n)_{\{x_i\}_{i=1}^n} = \{z_i\}_{i=1}^n, \text{ where } z_i = \begin{cases} \mathrm{Id}(y_i) & : x_i = 0, \\ \neg(y_i) & : x_i = 1. \end{cases} \end{array}$$

Proposition 1. *Let $X, Y, Z \in \mathbb{F}_2^n$. Then*

(1) $X \oplus_n Y = Y \oplus_n X$

(2) $(X \oplus_n Y) \oplus Z = X \oplus_n (Y \oplus Z)$

(3) $X \oplus_n 0_n = X = 0_n \oplus_n X$

(4) $X \oplus_n X = 0_n$

(5) $X \oplus_n Y = 0_n \implies X = Y$

(6) $A \oplus_n X = B \implies X = A \oplus_n B$

Note. By (4) and (5), we have $X \oplus_n Y = 0 \iff X = Y$.

Proof. PASS □

Remark 1.

- The binary operation $\oplus$ provides the structure of an **abelian group** on the set $\mathbb{F}_2^n$ with identity element 0_n.
- Because of the property (4)$X \oplus_n X = 0_n$, we see that *the inverse of any element is itself* with respect to the operation $\oplus$.

Definition 2. The **difference** of $X \in \mathbb{F}_2^n$ and $Y \in \mathbb{F}_2^n$ is defined as $X \oplus_n Y \in \mathbb{F}_2^n$.

2 Difference Set

2.1 Definition and Property

Difference Set of Bit-Sequence

Definition 3. Given $\alpha \in \mathbb{F}_2^n$, we define the **difference set** of α as follow:

$$\Delta_\alpha = \left\{(x_1, x_2) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : x_1 \oplus x_2 = \alpha \in \mathbb{F}_2^n\right\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n.$$

Proposition 2. *For any $\alpha \in \mathbb{F}_2^n$ the set Δ_α contains 2^n elements and can be expressed as*

$$\Delta_\alpha = \left\{(x, x \oplus \alpha) : x \in \mathbb{F}_2^n\right\}.$$

Proof. Let

$$\begin{aligned} S &:= \left\{(x_1, x_2) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : x_1 \oplus x_2 = \alpha \in \mathbb{F}_2^n\right\}, \\ T &:= \left\{(x, x \oplus \alpha) : x \in \mathbb{F}_2^n\right\}. \end{aligned}$$

We must show that $S = T$:

$(S \subseteq T)$ Let $(x, y) \in S$ then by definition $x \oplus y = \alpha$. Since $(x \oplus y = \alpha) \Rightarrow (y = x \oplus \alpha)$,

$$(x, y) = (x, x \oplus \alpha) \in T.$$

$(T \subseteq S)$ Let $(x, x \oplus \alpha) \in T$. Since

$$x \oplus (x \oplus \alpha) = \alpha,$$

$(x, x \oplus \alpha) \in S$.

□

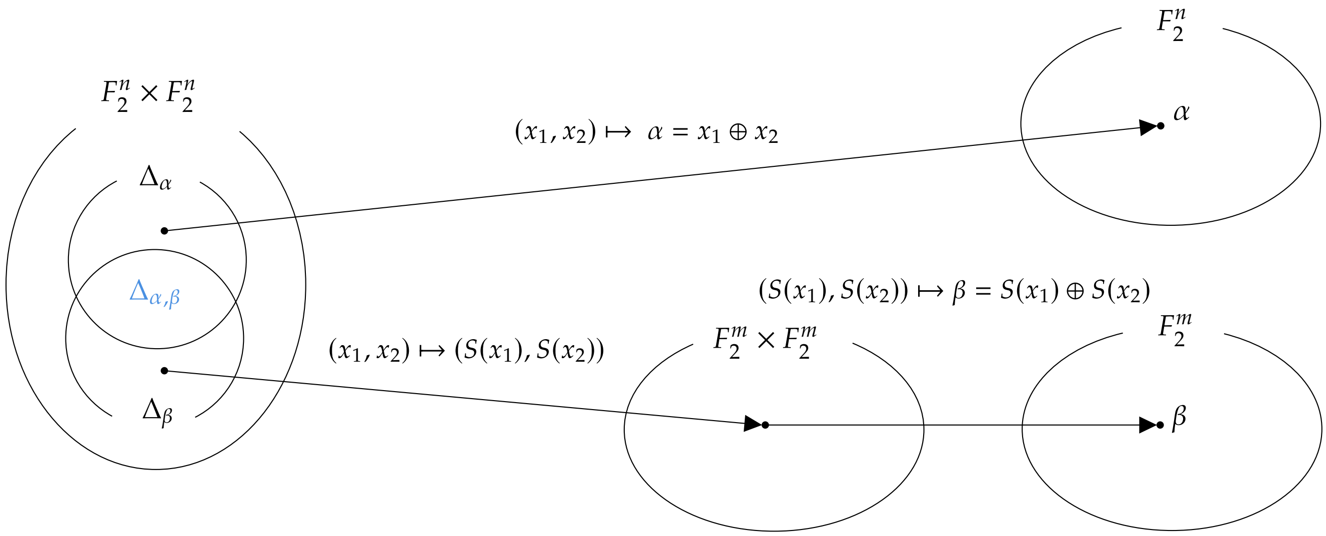
Corollary 2.1. *For any $\alpha \in \mathbb{F}_2^n$, we have $\Delta_\alpha \simeq \mathbb{F}_2^n$.*

Remark 2. Let us consider the case $\alpha = 0$ for the set Δ_α. When $\alpha = 0$ the difference set is

$$\Delta_0 = \left\{(x, x) : x \in \mathbb{F}_2^n\right\}$$

This set is often called the **diagonal** of $\mathbb{F}_2^n \times \mathbb{F}_2^n$.

2.2 Difference Sets of a S-BOX



Difference Set of a S-BOX

Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a S-box. Let $\alpha \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^m$. Consider

$$\begin{aligned}\Delta_\alpha &= \left\{(x_1, x_2) : x_1 \oplus x_2 = \alpha \in \mathbb{F}_2^n\right\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n \quad \text{and} \\ \Delta_\beta &= \left\{(x_1, x_2) : S(x_1) \oplus S(x_2) = \beta \in \mathbb{F}_2^m\right\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n.\end{aligned}$$

We define the **difference set** of S with respect to α and β by

$$\Delta_{\alpha,\beta} = \Delta_\alpha \cap \Delta_\beta = \left\{(x_1, x_2) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : x_1 \oplus x_2 = \alpha \in \mathbb{F}_2^n \text{ and } S(x_1) \oplus S(x_2) = \beta \in \mathbb{F}_2^m\right\}.$$

That is, $\Delta_{\alpha,\beta}$ is the set of ordered pairs of elements from $\mathbb{F}_2^n$ which have a difference of α and such that their images under S have a difference of β.

Remark 3.

- This can also written as

$$\Delta_{\alpha,\beta} = \left\{(x_1, x_2) \in \Delta_\alpha : (S(x_1), S(x_2)) \in \Delta_\beta\right\}.$$

- $\Delta_{\alpha,\beta}$ is always defined w.r.t. a given S-Box S. If we want to make this dependence explicit we can write $\Delta^S_{\alpha,\beta}$.

Cardinality of a Difference Set

We define $d_{\alpha,\beta}$ to be the cardinality of the finite set $\Delta_{\alpha,\beta}$, namely

$$d_{\alpha,\beta} := \left|\Delta_{\alpha,\beta}\right| \in \mathbb{Z}_{\geq 0}.$$

Remark 4.

- When $\alpha = 0$ and $\beta = 0$ we have $\Delta_{0,0} = \Delta_0 = \left\{(x, x) : x \in \mathbb{F}_2^n\right\}$.
- In general when $\alpha = 0$ we find that $\Delta_{0,\beta} = \begin{cases} \Delta_0 & : \beta = 0 \\ \emptyset & : \beta \neq 0 \end{cases}$
- Since $|\Delta_0| = 2^n$ and $|\emptyset| = 0$, $\quad d_{0,\beta} = \begin{cases} 2^n & : \beta = 0 \\ 0 & : \beta \neq 0 \end{cases}$.

Proposition 3. *The integer $d_{\alpha.\beta} \in \mathbb{Z}_{\geq 0}$ is always even.*

Proof. Recall that 0 is even.

(Case I) When $\alpha = 0$, we saw either $d_{0,\beta} \in \{0, 2^n\}$ and these are even in either case.

(Case II) Suppose that $\alpha \neq 0$ and $\Delta_{\alpha,\beta} \neq \emptyset$.

$\square$

Department of Information Security, Cryptology and Mathematics
College of Science and Technology
Kookmin University

References

[1] "Intro to Category Theory" YouTube, uploaded by Warwick Mathematics Exchange, 1 Feb 2023, https://www.youtube.com/watch?v=AUD2Rpoy604

[2] ProofWiki. "Definition:Metacategory" Accessed on [May 05, 2024]. https://proofwiki.org/wiki/Definition:Metacategory.

[3] nLab. "category" Accessed on [May 05, 2024]. https://ncatlab.org/nlab/show/category#Grothendieck61.