Differential Cryptanalysis

May 13, 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

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

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

Note (Thinking).

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

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

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

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

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

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

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

$\square$

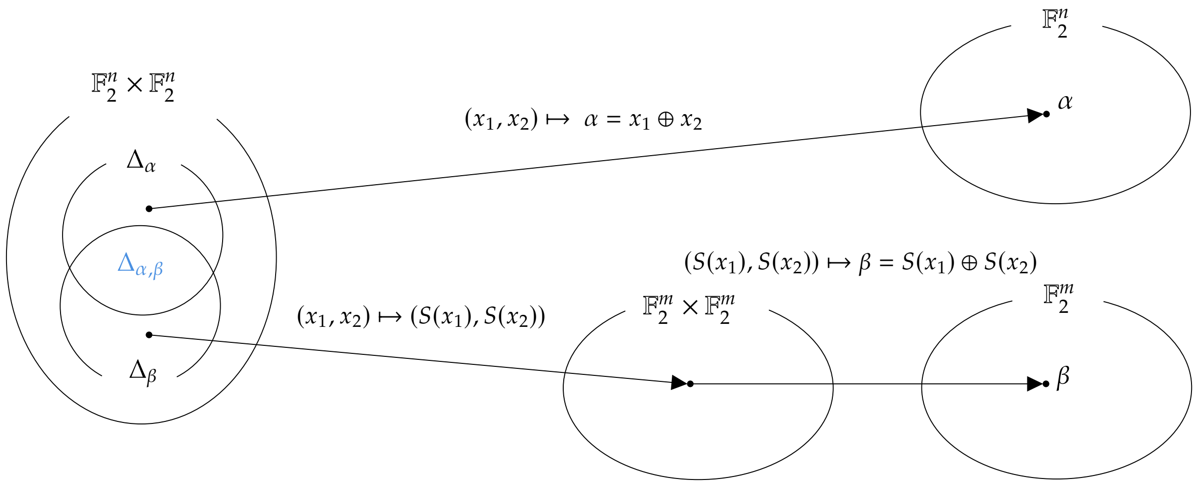
Corollary 2.1. *For any $\alpha \in \mathbb{F}_2^n$, we have $\Delta_\alpha \simeq \mathbb{F}_2^n$.*

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 $S : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ 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 $\delta_{\alpha,\beta}$ to be the cardinality of the finite set $\Delta_{\alpha,\beta}$, namely

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

Proposition 3.

$$\delta_{\alpha,\beta} = \#\left\{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta \in \mathbb{F}_2^m\right\}.$$

Proof.

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

□

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 $|\emptyset| = 0$, $\quad \delta_{0,\beta} = \begin{cases} 2^n & : \beta = 0 \\ 0 & : \beta \neq 0 \end{cases}$.

Proposition 4. *The integer $\delta_{\alpha,\beta} \in \mathbb{Z}_{\geq 0}$ is always even.*

Proof. Recall that 0 is even.

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

(Case II) Suppose that $\alpha \neq 0$ and $\Delta_{\alpha,\beta} \neq \emptyset$. Let $(x_1, x_2) \in \Delta_{\alpha,\beta}$ then

$$(x_2, x_1) \in \Delta_{\alpha,\beta} \quad \text{and} \quad x_1 \neq x_2.$$

Therefore $(x_1, x_2) \neq (x_2, x_1)$. So if we pair (x_1, x_2) and (x_2, x_1), we can partition $\Delta_{\alpha,\beta}$ into subsets, each subset having cardinality of 2.

□

3 The DDT of a S-Box

3.1 Definition and Property

Differential Distribution Table

Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a S-Box. The **differential distribution table** (abbreviated DDT) of S is a table (or matrix) with 2^n-rows and 2^m-columns. We denote it by $\mathcal{D}_S$ or just by $\mathcal{D}$.

- The rows are indexed by the elements $\alpha \in \mathbb{F}_2^n = \{0, \ldots, 2^n - 1\}$.
- The columns are indexed by the elements $\beta \in \mathbb{F}_2^m = \{0, \ldots, 2^m - 1\}$.
- The entry at row index α and column index β is given by $\delta_{\alpha,\beta} = |\Delta_{\alpha,\beta}|$. That is,

$$\mathcal{D} = (\delta_{\alpha,\beta})_{2^n \times 2^m}.$$

Remark 5. The DDT of a S-Box is just table of all the possible integer values $\delta_{\alpha,\beta}$.

$\mathcal{D}$	0	1	$\cdots$	β	$\cdots$	$2^m - 1$
0	2^n	0		$\cdots$		0
1						
$\vdots$						
α				$\delta_{\alpha,\beta}$		
$\vdots$						
$2^n - 1$						

Proposition 5. *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a S-Box with differential distribution table $\mathcal{D}$. The following properties hold for $\mathcal{D}$.*

(1) Every entry in $\mathcal{D}$ is a non-negative even integer between 0 and 2^n.

(2) The top-left entry of $\mathcal{D}$ is 2^n.

(3) The first row of $\mathcal{D}$ consists of all zeros except the first entry which is 2^n.

(4) If S is one-to-one then the first column of $\mathcal{D}$ consists all zeros except the first entry which is 2^n.

(5) The sum of the entries of each row is 2^n.

(6) If S is bijective then every row and column of the DDT add up to 2^n.

3.2 The DDT and Probabilities

When designing and analyzing attacks by differential cryptanalysis, we often want to translate the integer values from the DDT into probabilities.

Note. The **probability** p that E occurs is defined to be the quotient of the cardinalities of the sets E and Ω:

$$p = \frac{|E|}{|\Omega|}.$$

Probability of DDT

Definition 4. Let the universe is $\Omega = \Delta_\alpha$ and the event $E = \Delta_{\alpha,\beta}$. We define probability $p_{\alpha,\beta}$ as follows:

$$p_{\alpha,\beta} = \frac{|\Delta_{\alpha,\beta}|}{|\Delta_\alpha|} = \frac{\delta_{\alpha,\beta}}{2^n}.$$

Remark 6. Equivalently we can regard the universe $\Omega = \mathbb{F}_2^n$ and the event as the set

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

4 The DDT of a Linear S-Box

Linear S-Box

Definition 5. A S-Box $L : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is said to be **linear** if

$$x_1, x_2 \in \mathbb{F}_2^n \implies L(x_1 \oplus x_2) = L(x_1) \oplus L(x_2).$$

Proposition 6. *Let $L : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a linear S-Box. Let $\alpha \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^n$. Then the difference sets of L and their cardinalities are given by*

$$\Delta_{\alpha,\beta} = \begin{cases} \Delta_\alpha & : \beta = L(\alpha) \\ \emptyset & : \beta \neq L(\alpha) \end{cases}, \quad \delta_{\alpha,\beta} = \begin{cases} 2^n & : \beta = L(\alpha) \\ 0 & : \beta \neq L(\alpha) \end{cases}.$$

That is, every row of the DDT of L consists of all zeros except one entry with a value of 2^n.

Proof. Let $\alpha \in \mathbb{F}_2^n$. Assume that $(x_1, x_2) \in \Delta_\alpha$, namely $x_1 \oplus x_2 = \alpha$ then

$$L(x_1) \oplus L(x_2) = L(x_1 \oplus x_2) = L(\alpha).$$

So $(x_1, x_2) \in \Delta_{\alpha,\beta} \iff \beta = L(\alpha)$. □

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=AUD2Rpoy6O4

[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.