

Differential Cryptanalysis

May 10, 2024

Ji, Yong-hyeon

1 DDT

- Motivation
- Sequences of Bits
- The XOR operation
- Properties of XOR
- Difference of Sets
- Difference of Sets of a S-Box
- The DDT of a S-Box
- Properties of the DDT
- The DDT and Probabilities
- The DDT of a Linear S-Box
- The DDT of a XOR S-Box
- Code for the DDT
- The DDT's of the S-Boxes of DES
- The DDT's of the Rijndael S-Box

Motivation

- Let $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be a S-Box.
- We define the **differential distribution table** $\mathcal{D}_S \in M_{2^n \times 2^m}(\mathbb{Z}_{\geq 0})$, abbreviated as DDT.

Sequences of Bits

- $\mathbb{F}_2 \{0, 1\}$
- $\mathbb{F}_2^n = \{(x_1, \dots, x_n) : x_i \in \mathbb{F}_2\}$ and $|\mathbb{F}_2^n| = 2^n$
- $\mathbb{F}_2^n \simeq \mathbb{Z}_{2^n} = \{0, 1, \dots, 2^n - 1\}$

The XOR operation

- $\oplus : \mathbb{F}_2 \times \mathbb{F}_2 \rightarrow \mathbb{F}_2$.
- The operation XOR is like addition modulo 2.
- It is denoted by \oplus .

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

•

$$\begin{aligned}
 & \neg(p \iff q) \\
 & \neg((p \implies q) \wedge (q \implies p)) \\
 & \neg((\neg p \vee q) \wedge (\neg q \vee p)) \\
 & (p \wedge \neg q) \vee (q \wedge \neg p) \\
 & [(p \wedge \neg q) \vee q] \wedge [(p \wedge \neg q) \vee \neg p] \\
 & [(p \vee q) \wedge (\neg q \vee q)] \wedge [(p \vee \neg p) \wedge (\neg q \vee \neg p)] \\
 & (p \vee q) \wedge ()
 \end{aligned}$$

•

$$\begin{aligned}
& (p \vee q) \wedge (\neg(p \wedge q)) \\
& (p \vee q) \wedge (\neg p \vee \neg q) \\
& ((p \vee q) \wedge \neg p) \vee ((p \vee q) \wedge \neg q) \\
& [(p \wedge \neg p) \vee (q \wedge \neg p)] \vee [(p \wedge \neg q) \vee (q \wedge \neg q)] \\
& [F \vee (q \wedge \neg p)] \vee [(p \wedge \neg q) \vee F] \\
& (q \wedge \neg p) \vee (p \wedge \neg q)
\end{aligned}$$

Difference of Sets

Definition 1 (Difference Set). Given $\alpha \in \mathbb{F}_2^n$, we define the subset Δ_α of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ by

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

We call Δ_α the **difference set** of α .

Proposition 1. For any $\alpha \in \mathbb{F}_2^n$ the set Δ_α contains 2^n elements and can be expressed as

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

Proof. Let

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

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

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

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

□

- So $\Delta_\alpha \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n$ is bijective with \mathbb{F}_2^n

- A bijective map is given by

$$\begin{aligned}\varphi &: \mathbb{F}_2^n \longrightarrow \Delta_\alpha \\ x &\longmapsto (x, x \oplus \alpha)\end{aligned}$$

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

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

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

Difference Sets of A S-BOX

Definition 2. Let $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be a S-Box, and let $\alpha \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^m$. We define the **difference set** of S w.r.t. α and β by

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

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 1. This can also written as

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

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

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

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

- When $\alpha = 0$ and $\beta = 0$ we have

$$\Delta_{0,0} = \Delta_0 = \{(x, x) : x \in \mathbb{F}_2^n\}.$$

- 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 $|\emptyset| = 0$,

$$d_{0,\beta} = \begin{cases} 2^n & : \beta = 0 \\ 0 & : \beta \neq 0 \end{cases}$$

Proposition 2. *The integer $d_{\alpha,\beta} \in \mathbb{Z}_{\geq 0}$ is always even.*

Proof. Recall that 0 is even.

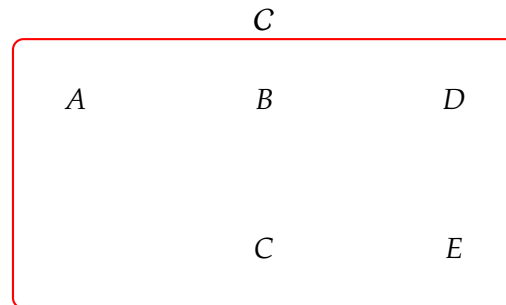
(Case I) When $\alpha = 0$, we saw either $d_{0,\beta} \in \{0, 2^n\}$ and these are even in either case.

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

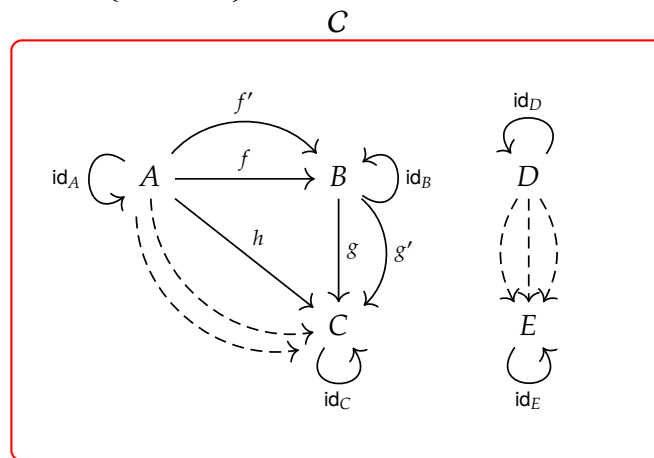
□

Remark 2. To describe a category it is necessary to specify:

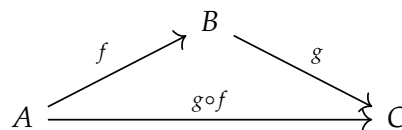
- (Objects) $\text{obj}(C) = \{A, B, C, D, E, \dots\}$



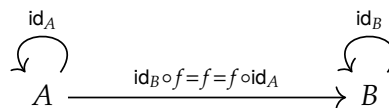
- (Morphisms) $\text{hom}(A, B) = \{f, f', \dots\}$; $\text{hom}(A, B) \neq \text{hom}(B, A)$



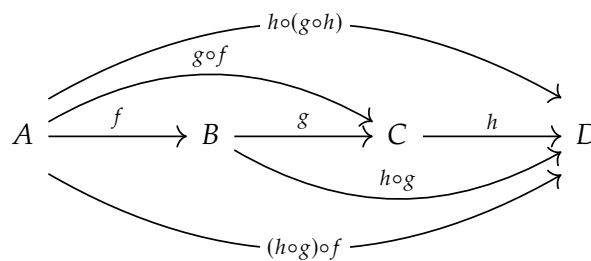
- (Composition)



- (Identity)



- (Associativity)



2 Examples

Example 1 (Trivial Category).

- $\text{obj}(C) = \{A\}$
- $\text{hom}(A, A) = \{\text{id}_A\}$

$$A \xrightarrow{\text{id}_A} A$$

Example 2.

- $\text{obj}(C) = \{A, B\}$
- $\text{hom}(A, B) = \{f\}$
- $\text{hom}(B, A) = \emptyset$

$$A \xrightarrow{f} B$$

Example 3. Let $(G, *)$ be a group.

- $\text{obj}(C) = \{X\}$
- $\text{hom}(X, X) = \{G\}$
- Define $g \circ f := g * f$

Example 4.

- **Set;**

$$\text{Set} \xrightarrow{\text{Function}} \text{Set}$$

- **Grp;**

$$\text{Group} \xrightarrow{\text{Homomorphism}} \text{Group}$$

- **Top;**

$$\text{Topological Space} \xrightarrow{\text{Continuous Map}} \text{Topological Space}$$

- **Vect_K;**

$$\text{Vector Space} \xrightarrow{\text{Linear Transformation}} \text{Vector Space}$$

Example 5.

- $f : x \rightarrow y$ if and only if $x \leq y$

$$x \xrightarrow{f} y \xrightarrow{g} z$$

$$x \xrightarrow{h} z$$

- $\text{id}_x : x \rightarrow x$ if and only if $x \leq x$

$$\begin{array}{ccc} & (\mathbb{R}, \leq) & \\ \text{Real Number} & \xrightarrow{\text{Ordering}} & \text{Real Number} \end{array}$$

3 Product and Dual Categories**3.1 Product Categories**

$$C \times \mathcal{D}$$

$$\text{obj}((C \times \mathcal{D})) = \text{obj}(C) \times \text{obj}(\mathcal{D})$$

$$\text{hom}_{C \times \mathcal{D}}((A, B), (A', B')) = \text{hom}_C(A, A') \times \text{hom}_{\mathcal{D}}(B, B')$$

$$\begin{array}{ccc} C & & \mathcal{D} \\ A \xrightarrow{f} A' & B \xrightarrow{g} & B' \end{array}$$

$$\begin{array}{ccc} C \times \mathcal{D} & & \\ (A, B) \xrightarrow{(f, g)} & (A', B') \end{array}$$

3.2 Dual Categories

$$\begin{array}{ccc} C & & C^{\text{op}} \\ A \rightarrow B & A \leftarrow & B \end{array}$$

4 Functors

$$F : \mathcal{C} \rightarrow \mathcal{D}$$

$$F : \text{obj}(\mathcal{C}) \rightarrow \text{obj}(\mathcal{D})$$

$$F : \text{hom}(\mathcal{C}) \rightarrow \text{hom}(\mathcal{D})$$

$$F : \mathcal{C} \longrightarrow \mathcal{D}$$

$$A \longmapsto F(A)$$

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ & \downarrow & \\ F(A) & \xrightarrow{\quad F(f) \quad} & F(B) \end{array}$$

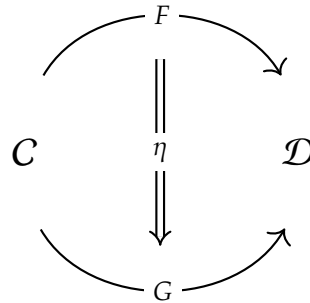
5 Natural Transformation

- Let

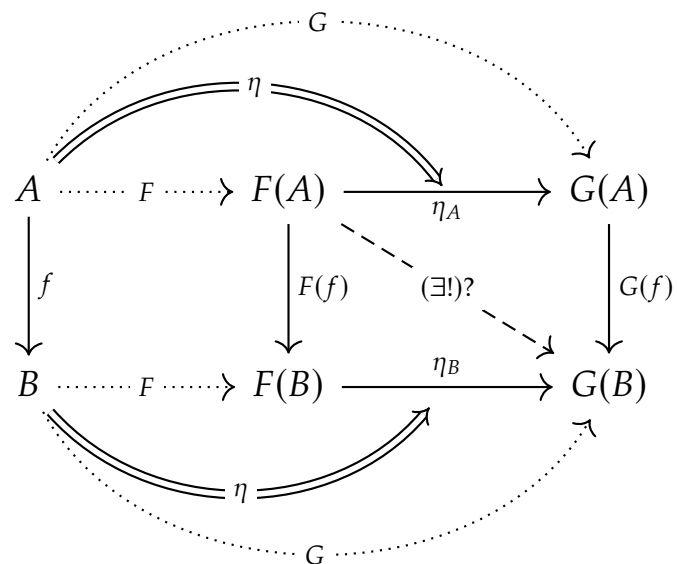
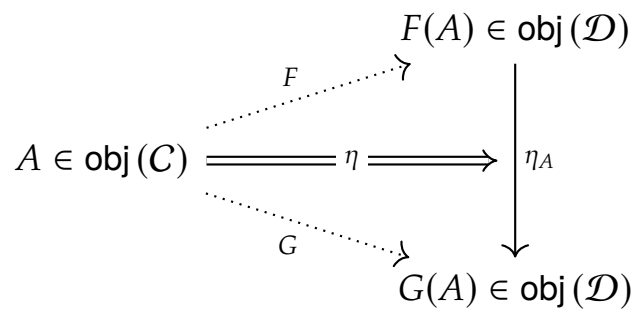
$$C \begin{matrix} \xrightarrow{F} \\ \xleftarrow{G} \end{matrix} \mathcal{D}$$

be categories and functors.

- A map



is a natural transformation





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>.