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

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

The XOR operation

- $\oplus : \mathbb{F}_2 \times \mathbb{F}_2 \longrightarrow \mathbb{F}_2$.
- 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

- $$\begin{aligned}
&\neg(p \iff q) \\
&\neg((p \implies q) \land (q \implies p)) \\
&\neg((\neg p \lor q) \land (\neg q \lor p)) \\
&(p \land \neg q) \lor (q \land \neg p) \\
&[(p \land \neg q) \lor q] \land [(p \land \neg q) \lor \neg p] \\
&[(p \lor q) \land (\neg q \lor q)] \land [(p \lor \neg p) \land (\neg q \lor \neg p)] \\
&(p \lor q) \land ()
\end{aligned}$$

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

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

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

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*

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

Proof. Let

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

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

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

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

□

- 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

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

- 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 $\mathbb{F}_2^n \times \mathbb{F}_2^n$.

Difference Sets of A S-BOX

Definition 2. Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 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

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

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

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

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 $\Delta^S_{\alpha,\beta}$.

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

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

- 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 $|\emptyset| = 0$,

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

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 $\Delta_{\alpha,\beta} \neq \emptyset$.

$\square$

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

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

$$\mathcal{C}$$

$$\begin{tikzcd}
A & B & D \\
& C & E
\end{tikzcd}$$

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

$$\mathcal{C}$$

$$\begin{tikzcd}
A \arrow[loop left, "\mathrm{id}_A"] \arrow[r, "f"] \arrow[r, bend left, "f'"] \arrow[dr, "h"] \arrow[dr, dashed, bend right] \arrow[dr, dashed, bend right=60] & B \arrow[loop right, "\mathrm{id}_B"] \arrow[d, "g"] \arrow[d, bend left, "g'"] & D \arrow[loop above, "\mathrm{id}_D"] \arrow[d, dashed] \arrow[d, dashed, bend left] \arrow[d, dashed, bend right] \\
& C \arrow[loop below, "\mathrm{id}_C"] & E \arrow[loop below, "\mathrm{id}_E"]
\end{tikzcd}$$

- (Composition)

$$\begin{tikzcd}
& B \arrow[dr, "g"] & \\
A \arrow[ur, "f"] \arrow[rr, "g\circ f"] & & C
\end{tikzcd}$$

- (Identity)

$$\begin{tikzcd}
A \arrow[loop above, "\mathrm{id}_A"] \arrow[r, "\mathrm{id}_B\circ f = f = f\circ \mathrm{id}_A"] & B \arrow[loop above, "\mathrm{id}_B"]
\end{tikzcd}$$

- (Associativity)

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[rr, bend left, "g\circ f"] \arrow[rrr, bend left=50, "h\circ(g\circ h)"] \arrow[rrr, bend right=50, "(h\circ g)\circ f"'] & B \arrow[r, "g"] \arrow[rr, bend right, "h\circ g"'] & C \arrow[r, "h"] & D
\end{tikzcd}$$

2 Examples

Example 1 (Trivial Category).

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

$$\begin{tikzcd} A \arrow[loop right, "\mathsf{id}_A"] \end{tikzcd}$$

Example 2.

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

$$A \xrightarrow{f} B$$

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

- $\mathsf{obj}(C) = \{X\}$
- $\mathsf{hom}(X, X) = \{G\}$
- 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**;

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

- $\mathbf{Vect}_K$;

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

Example 5.

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

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

$$x \xrightarrow{\qquad\quad h \qquad\quad} z$$

- $\mathsf{id}_x : x \longrightarrow x$ if and only if $x \leq x$

$$(\mathbb{R}, \leq)$$

$$\text{Real Number} \xrightarrow[\text{Ordering}]{} \text{Real Number}$$

3 Product and Dual Categories

3.1 Product Categories

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

$$\mathsf{obj}\left((\mathcal{C} \times \mathcal{D})\right) = \mathsf{obj}\,(\mathcal{C}) \times \mathsf{obj}\,(\mathcal{D})$$
$$\mathsf{hom}_{\mathcal{C}\times\mathcal{D}}((A, B), (A', B')) = \mathsf{hom}_{\mathcal{C}}(A, A') \times \mathsf{hom}_{\mathcal{D}}(B, B')$$

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

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

3.2 Dual Categories

$$\begin{array}{cc} \mathcal{C} & \mathcal{C}^{\mathrm{op}} \\ A \longrightarrow B & A \longleftarrow B \end{array}$$

4 Functors

$$
\begin{aligned}
F &: \mathcal{C} \to \mathcal{D} \\
F &: \mathsf{obj}(\mathcal{C}) \to \mathsf{obj}(\mathcal{D}) \\
F &: \mathsf{hom}(\mathcal{C}) \to \mathsf{hom}(\mathcal{D})
\end{aligned}
$$

$$
\begin{array}{rcrcl}
F & : & \mathcal{C} & \longrightarrow & \mathcal{D} \\
 & & A & \longmapsto & F(A)
\end{array}
$$

$$
\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, phantom, "\longmapsto" rotate] & B \\
F(A) \arrow[r, "F(f)"'] & F(B)
\end{tikzcd}
$$

5 Natural Transformation

- Let

$$\mathcal{C} \underset{G}{\overset{F}{\rightrightarrows}} \mathcal{D}$$

  be categories and functors.

- A map

$$\begin{tikzcd}
\mathcal{C} \arrow[rr, bend left=60, "F"] \arrow[rr, bend right=60, "G"'] & {} \arrow[phantom, from=1-2, to=1-2, "\Downarrow\eta"] & \mathcal{D}
\end{tikzcd}$$

  is a natural transformation

$$\begin{tikzcd}
 & F(A) \in \mathsf{obj}\,(\mathcal{D}) \arrow[dd, "\eta_A"] \\
A \in \mathsf{obj}\,(\mathcal{C}) \arrow[ur, dotted, "F"] \arrow[dr, dotted, "G"'] \arrow[r, Rightarrow, "\eta"] & {} \\
 & G(A) \in \mathsf{obj}\,(\mathcal{D})
\end{tikzcd}$$

$$\begin{tikzcd}
A \arrow[r, dotted, "F"] \arrow[d, "f"] \arrow[rr, dotted, bend left=60, "G"] \arrow[rr, Rightarrow, bend left=40, "\eta"] & F(A) \arrow[r, "\eta_A"'] \arrow[d, "F(f)"] \arrow[dr, dashed, "(\exists!)?"] & G(A) \arrow[d, "G(f)"] \\
B \arrow[r, dotted, "F"] \arrow[rr, dotted, bend right=60, "G"'] \arrow[rr, Rightarrow, bend right=40, "\eta"'] & F(B) \arrow[r, "\eta_B"] & G(B)
\end{tikzcd}$$

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.