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

Remark 1. To describe acategory it is necessary to specify:

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

$$\mathcal{C}$$

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

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

$$\mathcal{C}$$

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

- (Composition)

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

- (Identity)

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

- (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**;

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

- **Vect**$_K$;

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

Example 5.

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

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

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

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

$$\begin{array}{c} (\mathbb{R}, \leq) \\ \text{Real Number} \xrightarrow[\text{Ordering}]{} \text{Real Number} \end{array}$$

3 Product and Dual Categories

3.1 Product Categories

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

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

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

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

3.2 Dual Categories

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

4 Functors

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

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

$$
\begin{tikzcd}
A \arrow[rr, "f"] & {} \arrow[d, mapsto] & B \\
F(A) \arrow[rr, "F(f)"'] & {} & F(B)
\end{tikzcd}
$$

5 Natural Transformation

- Let
$$\mathcal{C} \underset{G}{\overset{F}{\rightrightarrows}} \mathcal{D}$$
be categories and functors.

- A map
$$\begin{tikzcd}
\mathcal{C} \arrow[r, bend left=60, "F"{name=U}] \arrow[r, bend right=60, "G"'{name=L}] & \mathcal{D} \arrow[Rightarrow, from=U, to=L, "\eta"]
\end{tikzcd}$$
is a natural transformation

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

$$\begin{tikzcd}
A \arrow[r, dotted, "F"] \arrow[d, "f"] \arrow[rr, Rightarrow, bend left, "\eta"] \arrow[rrr, dotted, bend left=50, "G"] & F(A) \arrow[rr, "\eta_A"'] \arrow[d, "F(f)"] \arrow[drr, dashed, "(\exists!)?"] & & G(A) \arrow[d, "G(f)"] \\
B \arrow[r, dotted, "F"] \arrow[rr, Rightarrow, bend right, "\eta"'] \arrow[rrr, dotted, bend right=50, "G"'] & F(B) \arrow[rr, "\eta_B"] & & G(B)
\end{tikzcd}$$

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.