

Differential Cryptanalysis

May 10, 2024

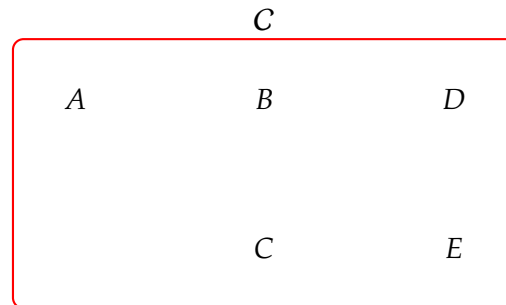
Ji, Yong-hyeon

1 DDT

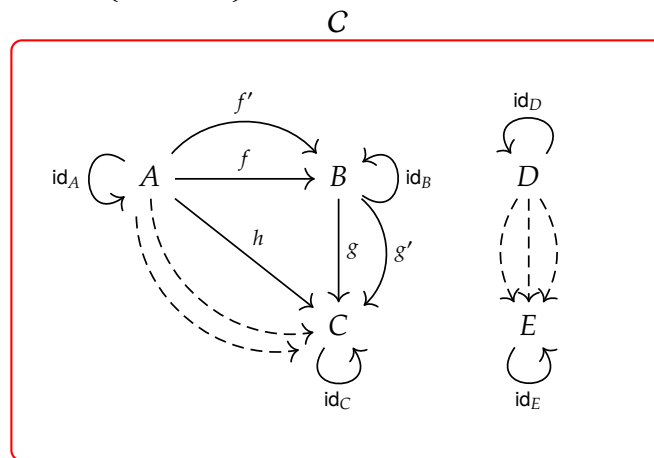
- Motivation
- Sequences of Bits
- The XOR operation
- Properties of XOR
- Difference of Sets
- Difference of Sets of a S-Box
- The DDT of a S-Box
- Properties of the DDT
- The DDT and Probabilities
- The DDT of a Linear S-Box
- The DDT of a XOR S-Box
- Code for the DDT
- The DDT's of the S-Boxes of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

Remark 1. To describe a category it is necessary to specify:

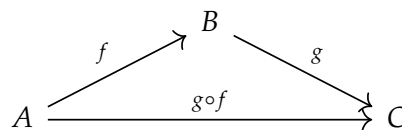
- (Objects) $\text{obj}(C) = \{A, B, C, D, E, \dots\}$



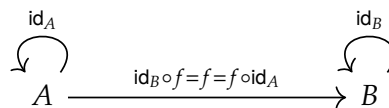
- (Morphisms) $\text{hom}(A, B) = \{f, f', \dots\}$; $\text{hom}(A, B) \neq \text{hom}(B, A)$



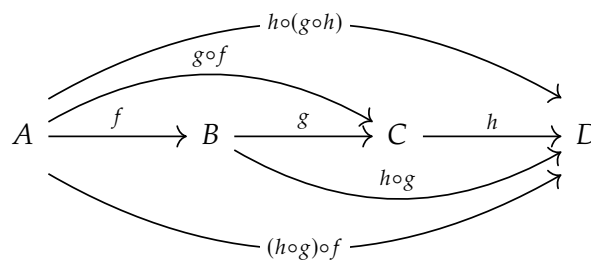
- (Composition)



- (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

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

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

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

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

$$A \longmapsto F(A)$$

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

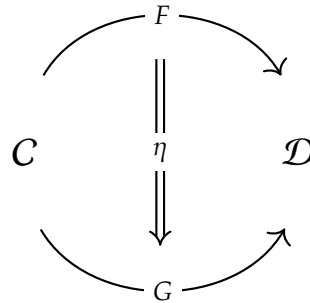
5 Natural Transformation

- Let

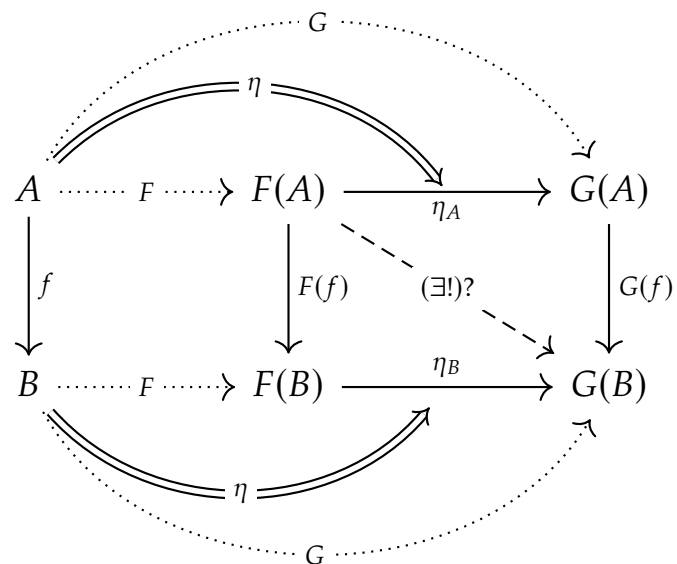
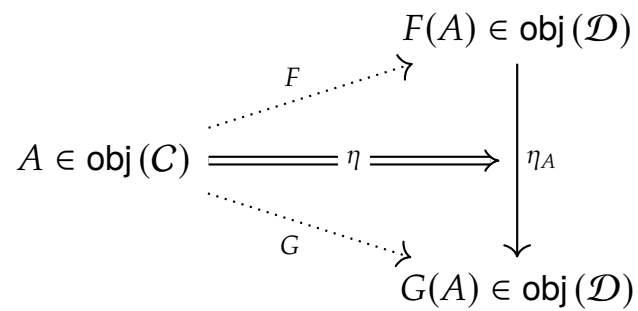
$$C \begin{matrix} \xrightarrow{F} \\ \xleftarrow{G} \end{matrix} \mathcal{D}$$

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>.