Cryptographic Mathematics

- A Journey from Concretization to Abstraction -

Ji, Yong-Hyeon

A document presented for
the Cryptographic Mathematics

Department of Information Security, Cryptology, and Mathematics
College of Science and Technology
Kookmin University

July 3, 2024

Contents

Chapter 1

Boolean Functions

- $S : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$
- $SL_2(\mathbb{Z}_2) = \{A_1, A_2, A_3, A_4, A_5, A_6\}$.
- order of special linear group $\left|SL_2(\mathbb{Z}_2)\right| = 6$.
- mathematical formula for the order of general linear group $\left|GL_n(\mathbb{Z}_q)\right| = (q^n - q)(q^{n-1} - q)\cdots(q^n - q^{n+1})$
- $\left|GL_n(\mathbb{F}_q)\right| = (q^n - q^0)(q^n - q)\cdots(q^n - q^{n-1})$
- $\left|SL_n(\mathbb{Z}_q)\right| = \frac{\left|GL_n(\mathbb{Z}_q)\right|}{q-1}$
- $\left|GL_2(\mathbb{Z}_2)\right| = (2^2 - 2^0)(2^2 - 2) = 3 \cdot 2 = 6$.
- $\left|SL_2(\mathbb{Z}_2)\right| = \frac{\left|GL_2(\mathbb{Z}_2)\right|}{2-1} = 6$.