GIFT - 64 / 128

- Lightweight Block Cipher -

Ji Yong-Hyeon

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

February 4, 2024

List of Symbols

$x_{n-1} \parallel x_{n-2} \parallel \cdots \parallel x_0$	n-bit plaintext (x_0 is LSB)
$k_7 \parallel k_6 \parallel \cdots \parallel k_0$	128-bit key state

Contents

Chapter 1

Specifications

Overview

Specification	GIFT-64-128	GIFT-128-128
Block Size (bits)	64	128
Key Size (bits)	128	128
Round Key Size (bits)	32	64
Number of Rounds	28	40
Design Strategy	Substitution-Permutation Network	Substitution-Permutation Network

Table 1.1: Specifications of GIFT-64-128 and GIFT-128-128

1.1 Key Schedule and Round Constants

1.2 Round Function

1.2.1 SubCells

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$GS(x)$	1	a	4	c	6	f	3	9	2	d	b	7	5	0	8	e

Table 1.2: Specifications of GIFT Sbox GS

1.2.2 PermBits

The permutation can be expressed as:

$$P_{64}(i) = 4 \cdot \left\lfloor \frac{i}{16} \right\rfloor + 16 \cdot \left[\left(3 \cdot \left\lfloor \frac{i \bmod 16}{4} \right\rfloor + (i \bmod 4) \right) \bmod 4 \right] + (i \bmod 4).$$

$$x_{P(i)} \leftarrow x_i$$

for $i \in \{0, \ldots, n-1\}$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{64}(i)$	0	17	34	51	48	1	18	35	32	49	2	19	16	33	50	3
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_{64}(i)$	4	21	38	55	52	5	22	39	36	53	6	23	20	37	54	7
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P_{64}(i)$	8	25	42	59	56	9	26	43	40	57	10	27	24	41	58	11
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P_{64}(i)$	12	29	46	63	60	13	30	47	44	61	14	31	28	45	62	15

Table 1.3: Specifications of GIFT-64 Bit Permutation

1.2.3 AddRoundKey

Appendix A

Additional Data A

A.1 Substitution-BOX

Bibliography

[1] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. *GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption (Full version)*. Temasek Laboratories, Nanyang Technological University, Singapore; School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore; School of Computer Science and Engineering, Nanyang Technological University, Singapore; NTT Secure Platform Laboratories, Japan; LASEC, École Polytechnique Fédérale de Lausanne, Switzerland. Emails: `bsubhadeep@ntu.edu.sg`, `emailpandey@gmail.com`, `thomas.peyrin@ntu.edu.sg`, `SSIM011@e.ntu.edu.sg`, `Todo.Yosuke@lab.ntt.co.jp`, `Sasaki.Yu@lab.ntt.co.jp`