128-bit Blockcipher CLEFIA

3/2-3/3 2010

Briefing on the submitted algorithm
in the CRYPTREC symposium

Masanobu Katagi

Sony Corporation

CLEFIA

Introduction

- CLEFIA
  - Presented in FSE2007
  - 128-bit blockcipher
    - Key Length 128/192/256bit
    - Compatible to top level specification of AES
  - Designer
    - T. Shirai, K. Shibutani, T. Akishita, S. Moriai (Sony)
    - T. Iwata(Nagoya Univ.)

Contents

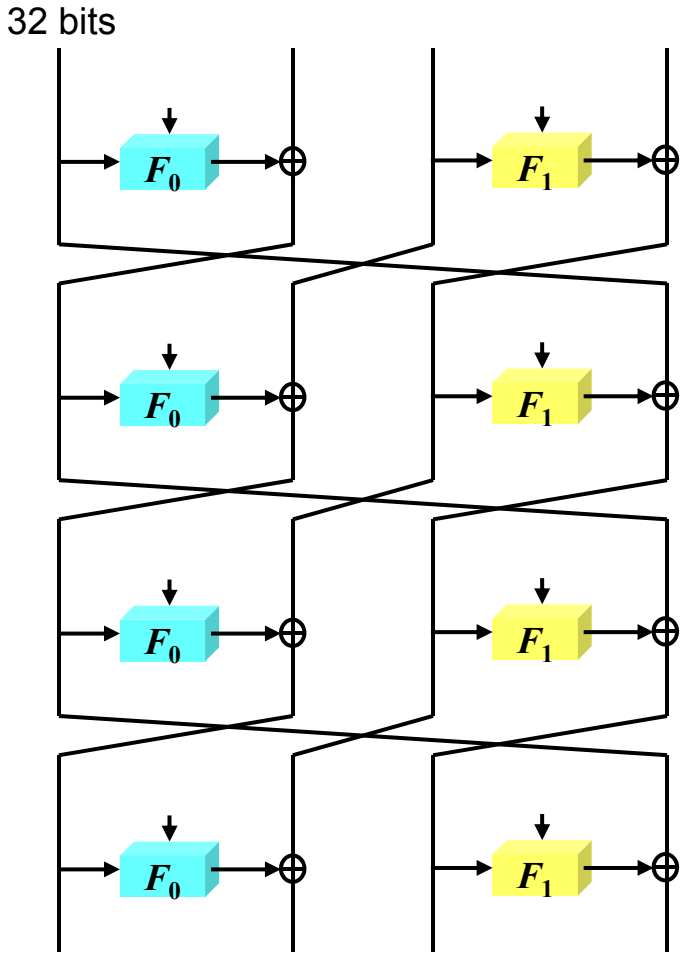
- Specifications
  - Algorithm Overview
  - Design Rationale
- Security Evaluations
- Performance Evaluations
- Information on Publication Status
- Summary

Specifications

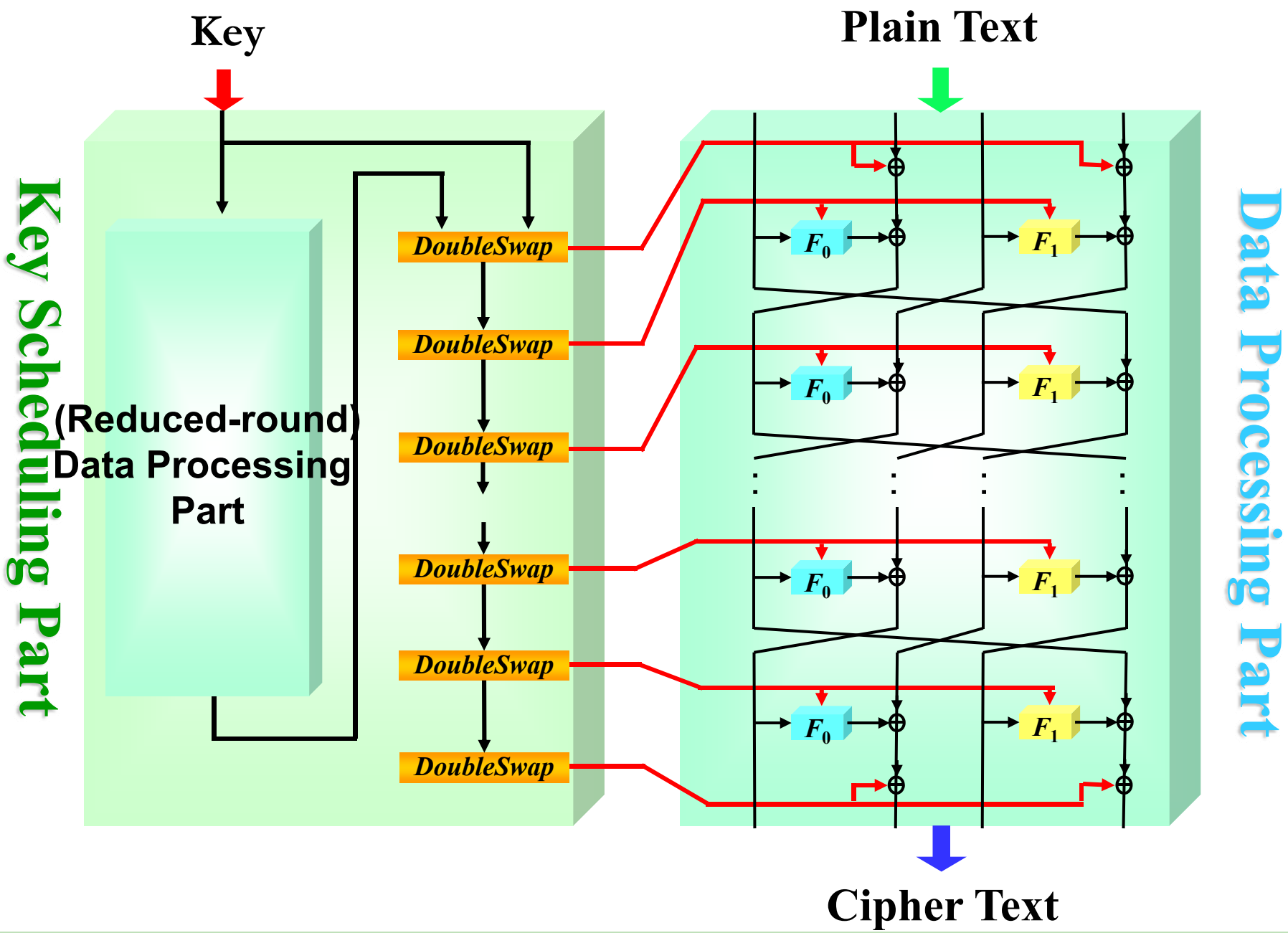
ALGORITHM OVERVIEW

CLEFIA: Algorithm Overview

- Blockcipher
  - Block size : 128 bits
  - Key length : 128/192/256 bits
- Fundamental Structure
  - Type-2 Generalized Feistel Structure (GFN)
    - data processing part and key scheduling part
  - Number of rounds:
    - 18 (128-bit key)
    - 22 (192-bit key)
    - 26 (256-bit key)

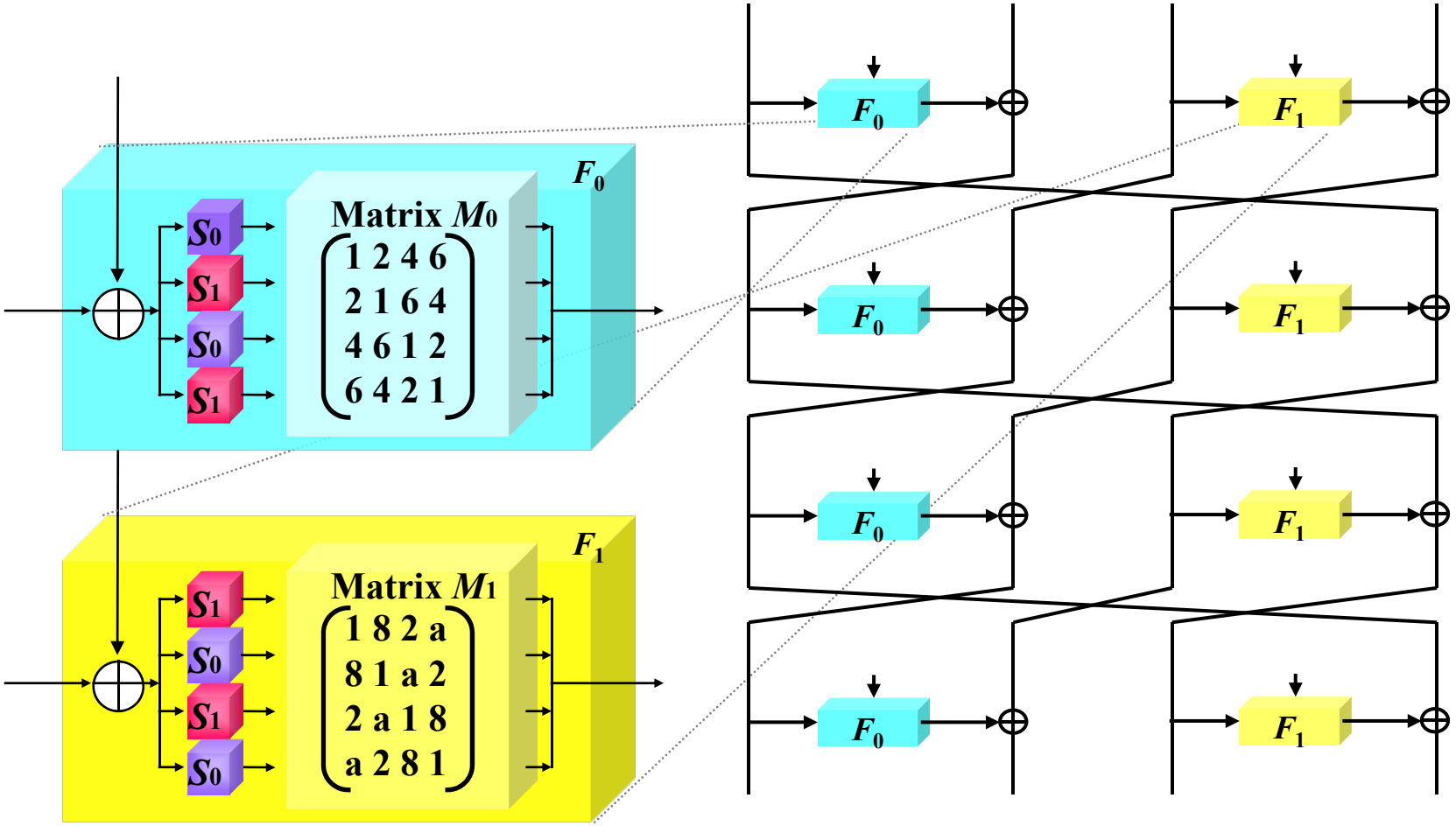


4-branch type-2 generalized Feistel structure



F-functions

- Substitution-Permutation (SP) Type



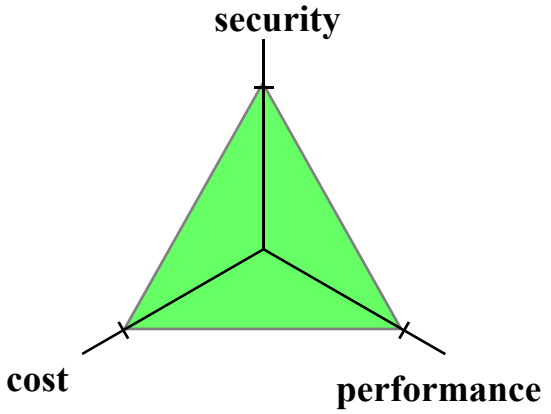
Specifications

DESIGN RATIONALE

Design Rationale (1/2)

- Background
  - Techniques of cryptanalysis have been advanced since the current list was selected
  - Needs for implementation on limited environment

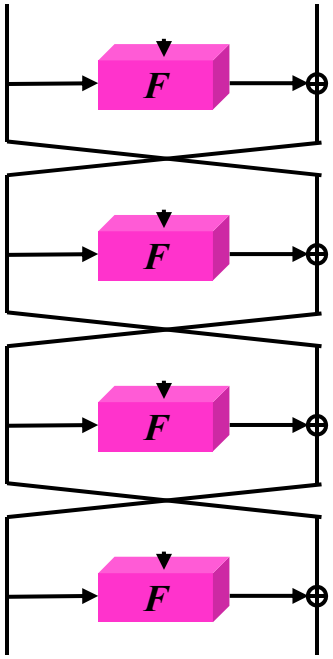
- Motivation
  - A new design for 128-bit blockcipher based on state-of-the-art techniques
  - Pursuit of “practical blockcipher”: balancing among three fundamental elements

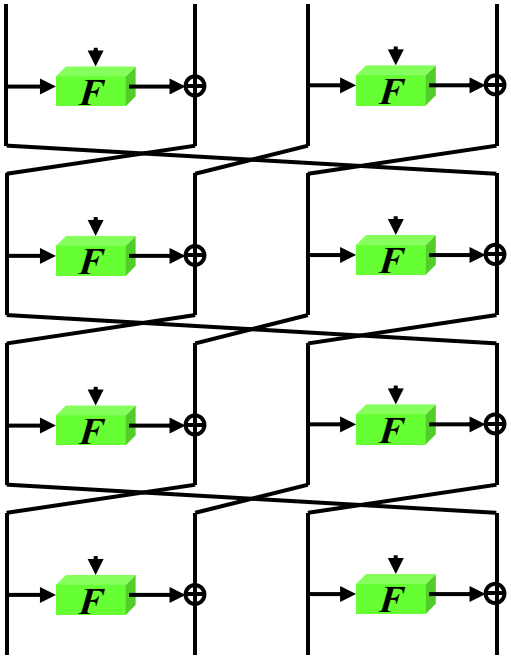


Design Rationale (2/2)

- Main features
  - Structure : Generalized Feistel Structure
    - Contribution to compact F-functions
  - F-functions: Diffusion Switching Mechanism
    - More immunity against differential / linear cryptanalysis
  - Key scheduling part: Generalized Feistel Structure
    - To enhance the immunity against related-key attacks
  - Lightweight Components:
    - Enable to efficient software and hardware implementations

1. Structure: Generalized Feistel Structure





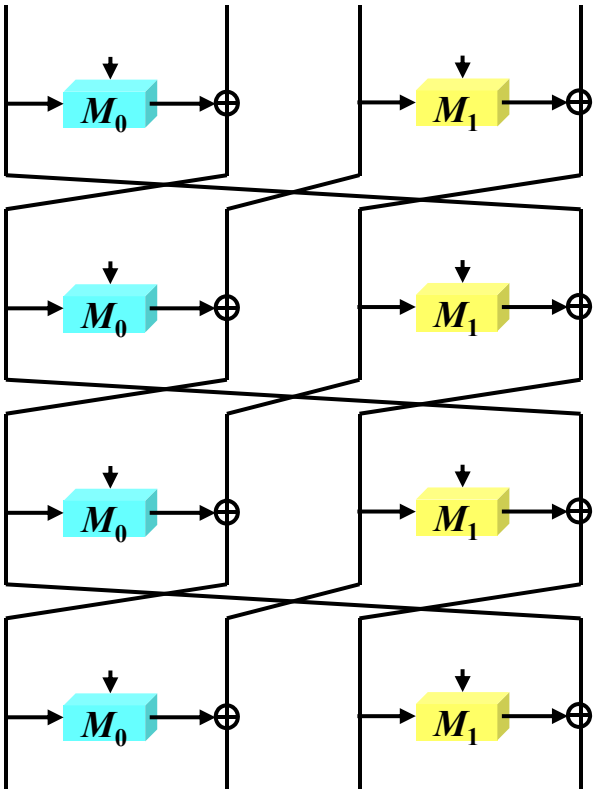
Features of
Generalized Feistel Structure

- The size of F-functions is smaller
- F-functions can be processed simultaneously
- Require more rounds

Diffusion Switching Matrix(DSM)

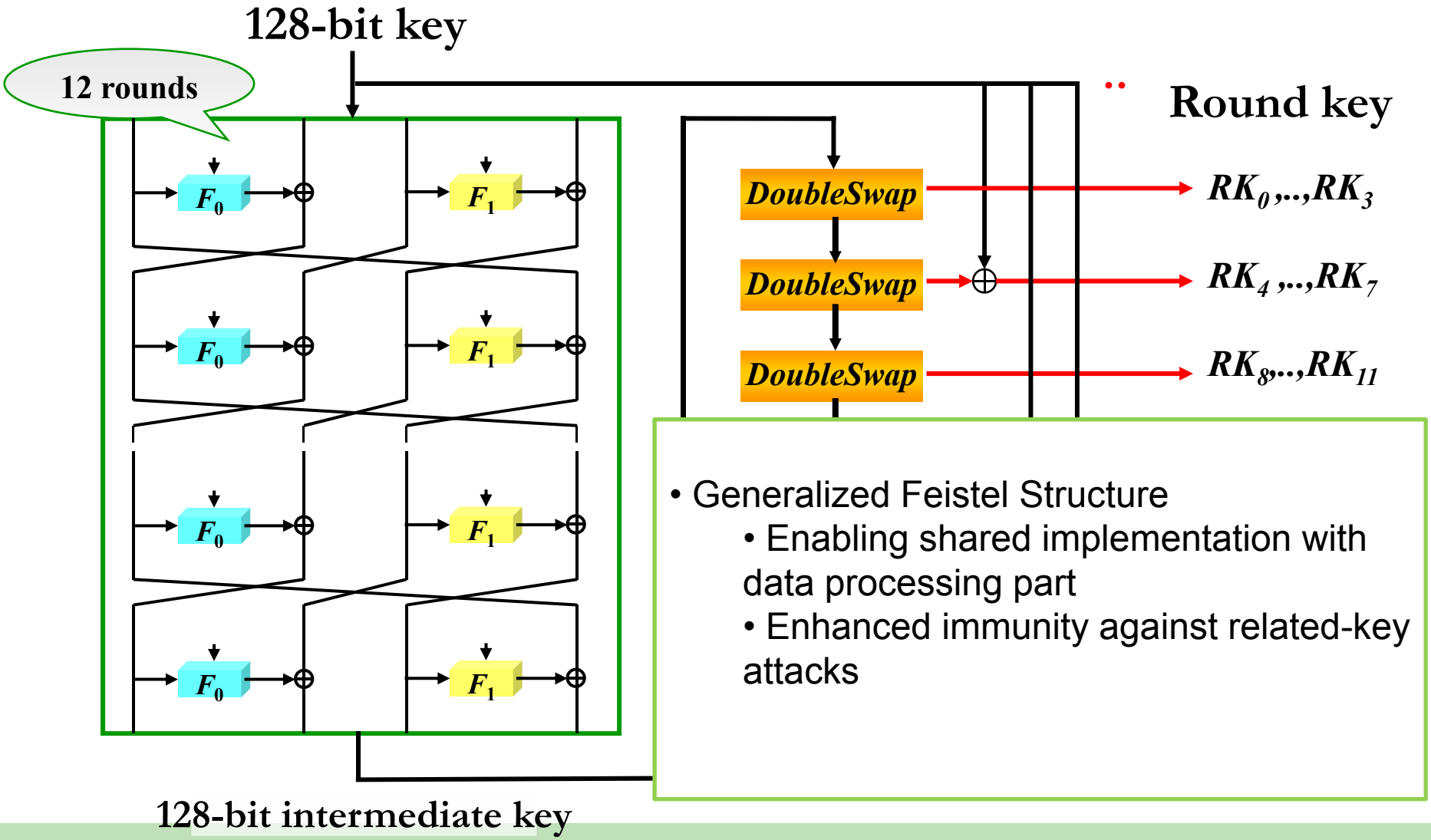
2. F-functions: Diffusion Switching Mechanism

- Apply Diffusion Switching Mechanism (DSM)
  - On Feistel-type structure, a method to enhance the immunity against differential/linear cryptanalysis by using multiple diffusion matrices
- Effects of DSM
  - Reduce the number of rounds
  - CLEFIA
    - w/o DSM: 16 rounds
    - w DSM: 12 rounds



M_0,M_1: diffusion matrices

3.Key Scheduling Part : Generalized Feistel Structure



- Generalized Feistel Structure
  - Enabling shared implementation with data processing part
  - Enhanced immunity against related-key attacks

4. Lightweight components

Design Aspects for Efficient Implementation of CLEFIA

GFN	· Small size F-functions (32-bit in/out) · No need for the inverse F-functions
SP-type F-function	· Enabling the fast table implementation in software
DSM	· Reducing the numbers of rounds
S-boxes	· Very small footprint of S_0 and S_1 in hardware
Matrices	· Using elements with low hamming weights only
Key Schedule	· Sharing the structure with the data processing part · Requiring only a 128-bit register for a 128-bit key · Small footprint of *DoubleSwap*

SECURITY EVALUATIONS

Self evaluations

All known attacks on block ciphers are considered to evaluate the security of CLEFIA

- Differential Cryptanalysis
- Linear Cryptanalysis
- Differential-Linear Cryptanalysis
- Boomerang Attack
- Amplified Boomerang Attack
- Rectangle Attack
- Truncated Differential Cryptanalysis
- Truncated Linear Cryptanalysis
- Impossible Differential Cryptanalysis
- Saturation Cryptanalysis
- Gilbert-Minier Collision Attack
- Higher Order Differential Cryptanalysis
- Interpolation Cryptanalysis
- XSL/Algebraic Attack
- χ^2/Statistical Cryptanalysis
- Slide Attack
- Related-Cipher Cryptanalysis
- Related-Key Cryptanalysis
- Related-Key Boomerang Cryptanalysis
- Related-Key Rectangle Cryptanalysis

External Evaluations

- CLEFIA had been evaluated by the following external researchers in 2007
  - Prof. Alex Biryukov
  - Prof. Vincent Rijmen
  - Prof. Serge Vaudenay
  - ABT(Prof. Lars R. Knudsen and Prof. Bart Preneel)
  - According to their reports, there is no security issue in CLEFIA

- Papers
  - Known attacks
    - Impossible differential attacks (on reduced-round CLEFIA)
  - Currently, full-round CLEFIA has enough security

PERFORMANCE EVALUATIONS

S/W performance

- 12.9cycles/byte, 1.48Gbps

Type of Implementation	Key Length [bit]	Encryption [cycles/byte]	Decryption [cycles/byte]	Key Setup (Encryption) [cycles]	Key Setup (Decryption) [cycles]
single-block	128	12.9	13.3	217	229
	192	15.8	16.2	272	293
	256	18.3	18.4	328	357
two-block parallel encryption	128	11.1	11.1	217	229
	192	13.3	13.3	272	293
	256	15.6	15.6	328	357

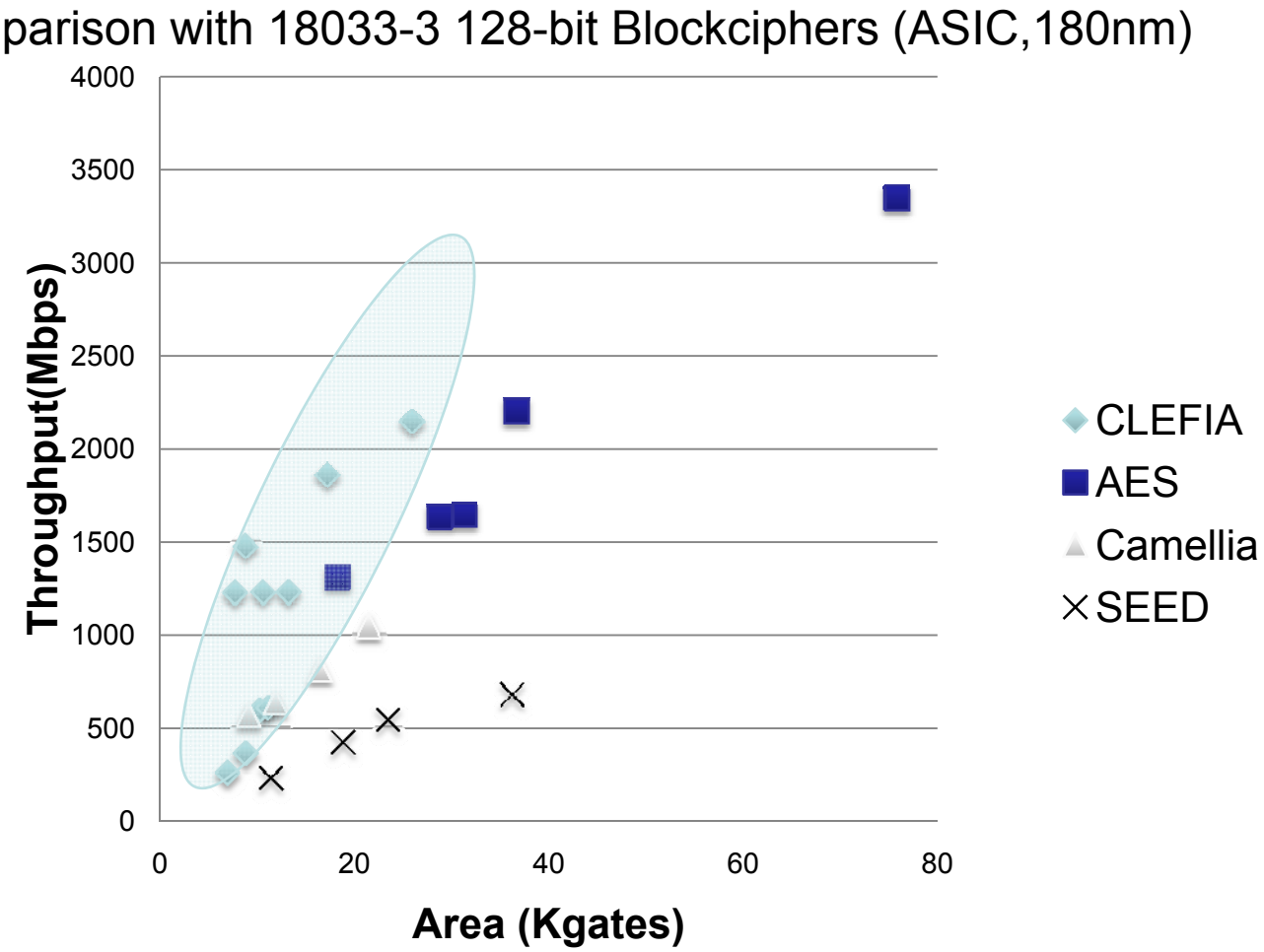
* CPU:AMD Athlon 64 processor 4000+ (2.4GHz)
OS:Windows XP 64-bit Edition, assembly language

H/W performance

- Gate size is less than 5K gates
- Higher efficiency (Speed/Area)

	Key Length	Enc/Dec (cycles)	Key Setup (cycles)	Area (gates)	Freq. (MHz)	Speed (Mbps)	Speed/Area (Kbps/gate)
CLEFIA (0.09μm)	128	18	12	5,979	225.83	1,605.94	268.63
				12,009	422.29	3,003.00	250.06
		36	24	4,950	201.28	715.69	144.59
				9,377	389.55	1,385.10	147.71
	192	22	20	8,536	206.56	1,201.85	140.81
				15,718	391.08	2,275.39	144.76
	256	26	20	8,482	206.56	1,016.95	119.89
				15,542	391.08	1,925.33	123.88

Hardware Performace（by External Experts）

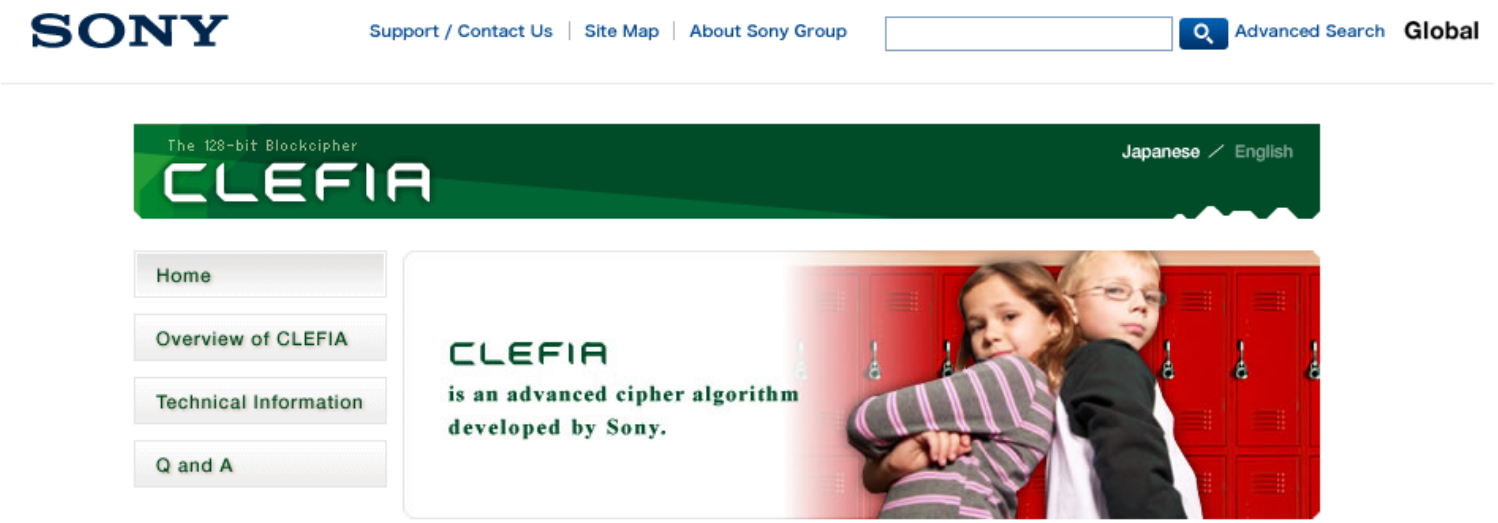


T. Sugawara, N. Homma, T. Aoki, and A. Satoh, “ASIC Implementations of the 128-bit Block Cipher CLEFIA." in Proceedings of Computer Security Symposium 2007 (CSS2007), pp. 175-180, 2007. (in Japanese)

INFORMATION ON PUBLICATION STATUS

Information on Publication Status (1/3)

- CLEFIA website
  - www.sony.net/clefia
  - Publish about technical information of CLEFIA



Information on Publication Status (2/3)

- Conference
  - Fast Software Encryption 2007
    - T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, “The 128-bit Blockcipher CLEFIA.” FSE 2007, LNCS 4593, pp. 181-195, Springer-Verlag, 2007.

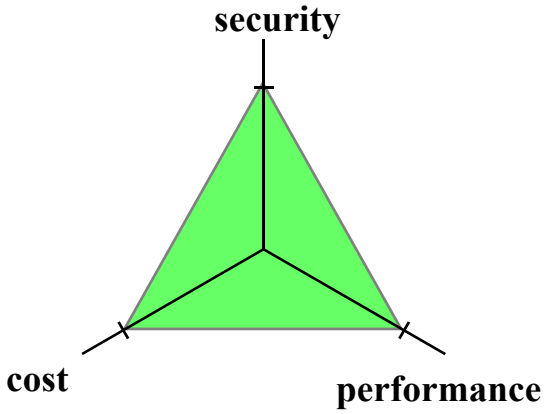
- Standardization
  - ISO/IEC JTC 1/SC27: proposed in the following standard
    - ISO/IEC 29192 – Information technology –Security Techniques – Lightweight cryptography – Part 2: Block ciphers
  - IETF: submitted as Internet draft
    - M. Katagi, S. Moriai, “The 128-bit Blockcipher CLEFIA”, October19, 2009. http://tools.ietf.org/html/draft-katagi-clefia-00

Information on Publication Status (3/3)

- Version
  - CLEFIA algorithm is uniquely specified by the submitted specification
  - CLEFIA has been presented and proposed under the same name and the same specification
- License Policy
  - Sony is prepared to make licenses available to use CLEFIA technology under CLEFIA essential patents on fair, reasonable and non-discriminatory terms.

Summary

- We propose 128bit blockcipher CLEFIA
- Security
  - CLEFIA has enough security against all known attacks of blockciphers
- Implementations
  - High performance and compact
  - Hardware performance of CLEFIA is particularly advantageous among other block ciphers



CLEFIA