A Compact and High-Speed Cipher Suitable for Limited Resource Environment

Taizo Shirai and Asami Mizuno

Taizo.Shirai@jp.sony.com
AsamiMizuno@jp.sony.com
Sony Corporation

3rd ETSI Security Workshop

Cryptographic Algorithms in GSM and UMTS

- Required Security Features are
  - Confidentiality (algorithm)
  - Integrity (algorithm)
- Algorithms in GSM, EDGE and GPRS
  - A3, A5 and A8
  - GEA3
- Algorithms in UMTS
  - 1st suite : UEA1(f8) and UIA1(f9)
    - Cryptographic engine : KASUMI - blockcipher
  - 2nd suite : UEA2 and UIA2
    - Cryptographic engine : SNOW 3G – streamcipher

Overview : KASUMI, SNOW 3G and AES

Comparison of three cryptographic algorithms

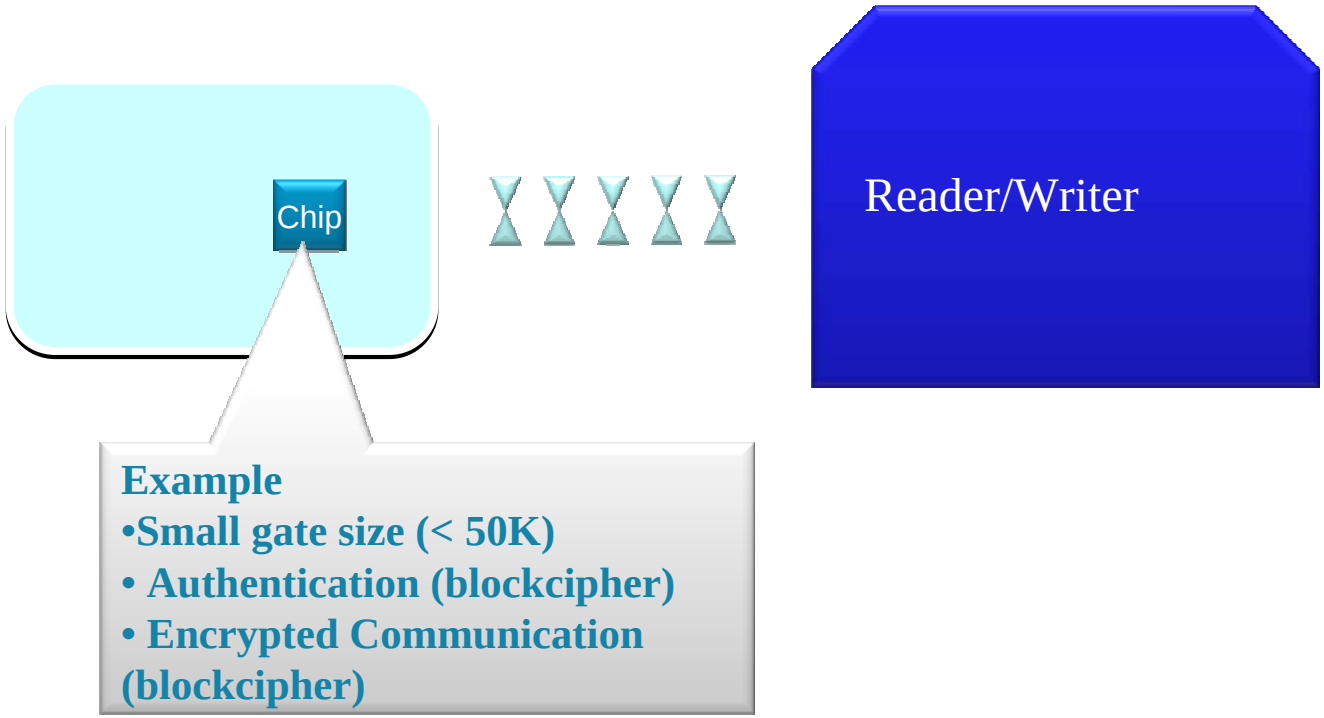
- KASUMI
  - Blockcipher
  - 64-bit block, 128-bit key
  - Enc/Dec: 3.7Kgates, 101Mbps ~ 9.9Kgates, 412Mbps @ 0.18µm CMOS [SAGE06]
- SNOW 3G
  - Streamcipher
  - 128-bit key, 128-bit IV
  - Generate Keystream: 10Kgates, 1.72 Gbps [SAGE06]
- AES
  - Blockcipher
  - 128-bit block, 128,192 and 256-bit keys
  - Enc/Dec: 5.4Kgates, 311Mbps ~ 21Kgates, 2.6Gbps @ 0.13µm CMOS [SM03]

Security for Limited Resource Environments

- KASUMI and SNOW 3G achieved preferable HW profile for UMTS
- However, more restricted environments also need security nowadays
- Examples for more restricted environments
  - Smart cards
  - RFID systems
  - Health care systems
- Recent challenges of designing new ciphers are aiming at lightweight implementation

Restricted Environment requiring Security 1

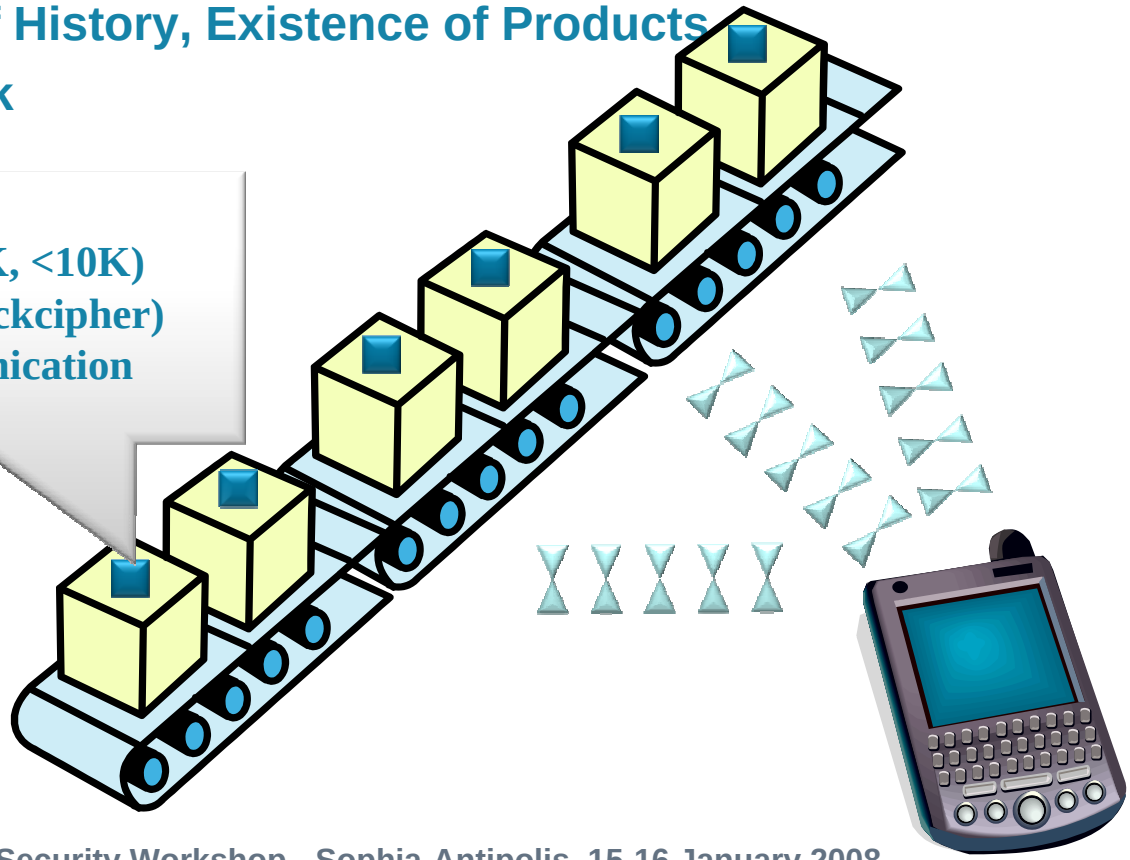
- Smart card system
  - Access Control, Electronic Ticket, Electronic Money



Restricted Environment requiring Security 2

- RFID system
  - Supply Chain Management
  - Management of History, Existence of Products
  - Sensor Network

Example
- Small gate size (< 5K, <10K)
- Authentication (blockcipher)
- Encrypted Communication (blockcipher)



Expected Requirements (generic)

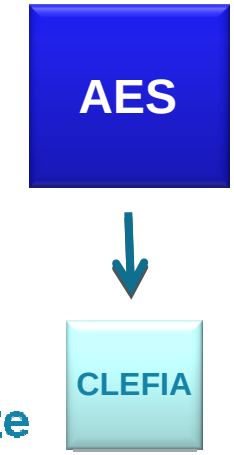
- Compact gate size
  - Afford for only limited resource for security in RFID (e.g. 5K)
  - Should include costly countermeasures against Side Channel Attacks
- Low power
  - Small device can use tiny battery
  - Power is passively supplied for some tokens
- High-speed
  - Lightweight implementations should avoid significant speed decreasing
  - Speed affects power consumption directly
- Security
  - Even lightweight ciphers should not decrease security level

Compact and High-Speed Blockcipher CLEFIA

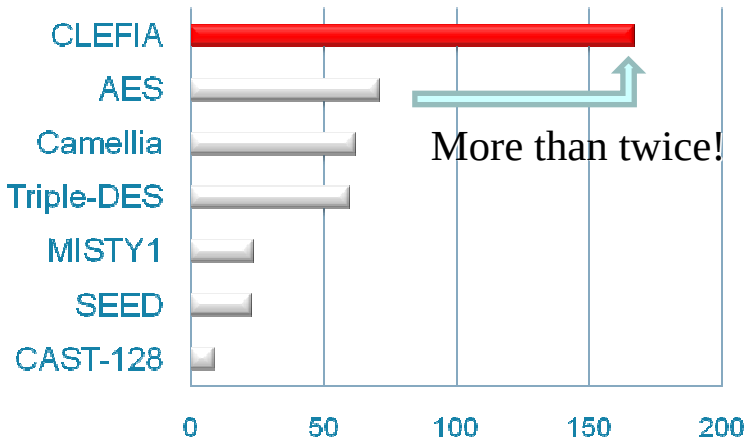
- First Presented at Fast Software Encryption 2007
- 128-bit blockcipher for I28, 192, and 256-bit keys
- Small footprint :

  5.0Kgates, 715 Mbps - 12Kgates, 3.0Gpbs @ 0.09µm

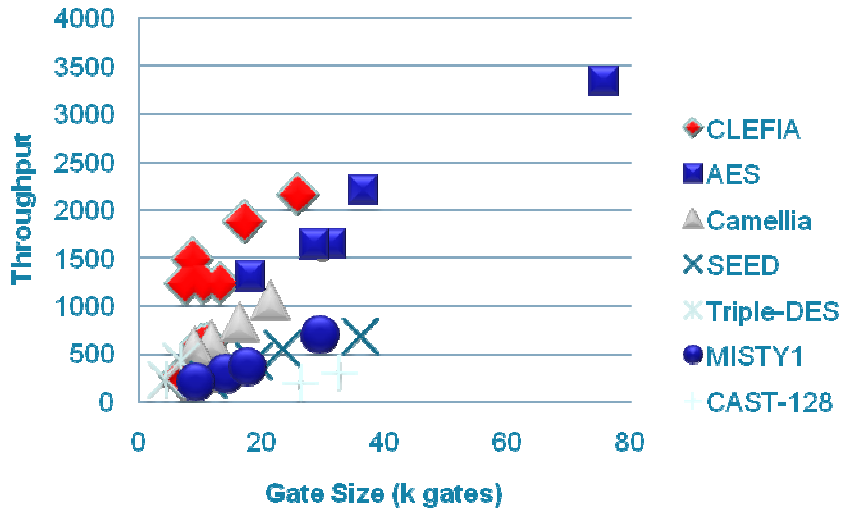
  (e.g AES 5.4Kgates, 311 Mbps - 21Kgates, 2.6Gbps @ 0.13µm)
- Software performance : as good as AES



Max. Efficiency (Kbps/gates)

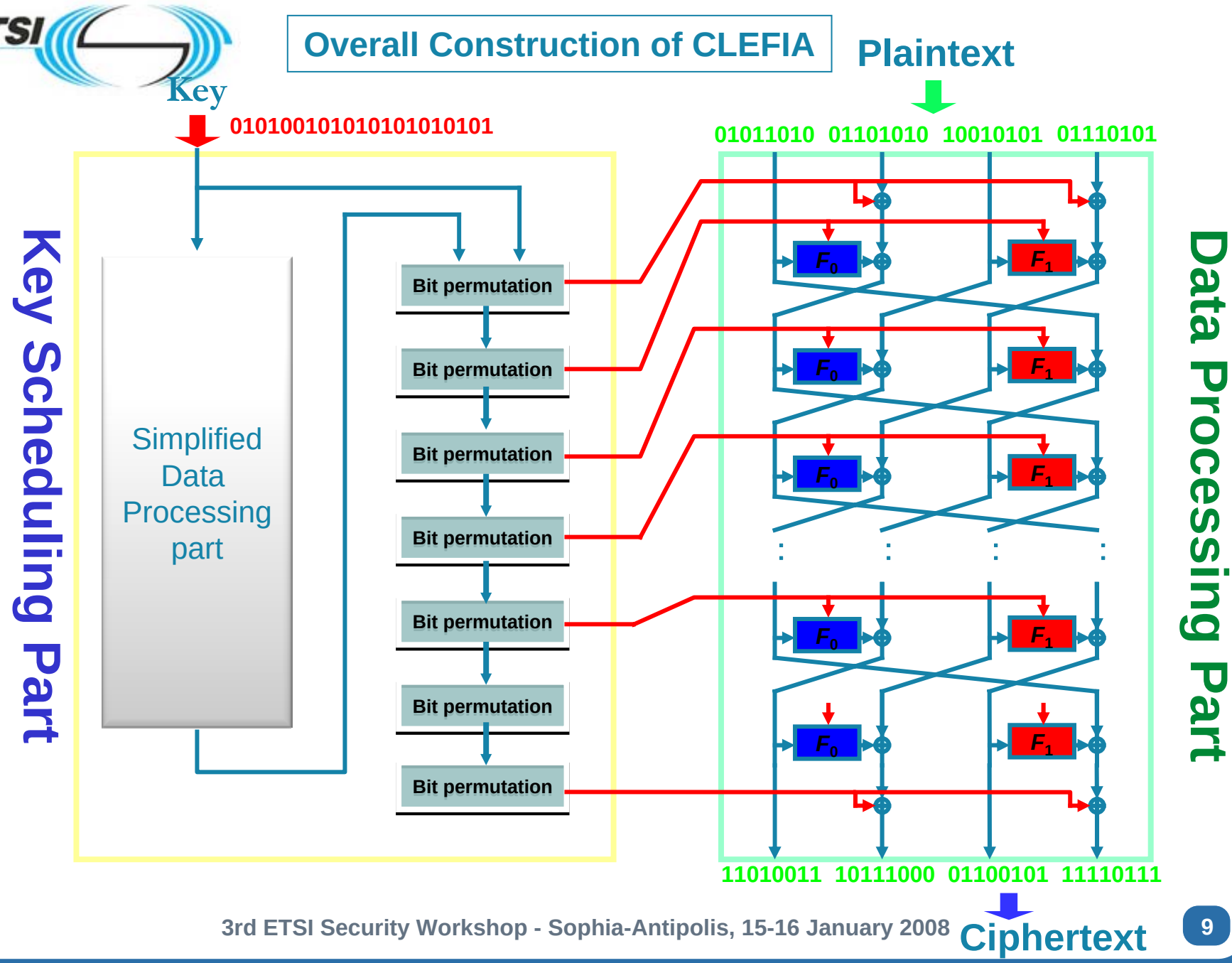


Throughput / Gate Size



- Comparison of Hardware Implementation with ISO standardized ciphers
  (CSS 2007, October2007 by Sugawara et al @ Tohoku Univ.)

Overall Construction of CLEFIA



Current Status of CLEFIA

- CLEFIA Web site is now open (www.sony.net/clefia)
  - Full papers are available (Specification, Rationale, Evaluation)
  - Recent topics are updated
- External evaluations have done by
  - ABT Crypto
    - Prof. L. R. Knudsen (DTU, Denmark)
    - Prof. B. Preneel (K.U.Leuven, Belgium)
  - Prof. A. Biryukov (Univ. of Luxembourg, Luxembourg)
  - Prof. V. Rijmen (K.U.Leuven, Beiguim)
  - Prof. S. Vaudenay (EPFL, Switzerland)
  - Four papers on CLEFIA have been published
- Related fields in ISO/IEC SC27
  - ISO/IEC 18033-3 Encryption algorithms – Block Ciphers
  - Study period on Light-weight cryptographic mechanisms

Comparison of CLEFIA with other new lightweight ciphers

	Docs.	Type	Key	Block Length	H/W	Process	Enc/ Dec	Efficiency*
KASUMI	ETSI/SAGE	Block	128	64	3.7K, 101Mbps ~ 9.9K, 412Mbps	0.18μm	Enc	27~47 (54~94)
SNOW 3G	ETSI/SAGE	Stream	128 + 128(IV)	N/A	10K gates, 1.72 Gbps	-	-	158 (N/A)
AES	NIST FIPS	Block	128,192,256	128	5.4K 311Mbps ~ 21K, 2.6Gbps	0.13μm	Enc/Dec	57~136 (82~196)
CLEFIA	FSE'07	Block	128,192,256	128	5.0K, 715Mbps ~ 12K, 3Gbps	0.09μm	Enc/Dec	144~268
HIGHT	CHES'06	Block	128	64	3.0K, 9.9 Mbps	0.25μm	Enc/Dec	3.3 (9.1)
PRESENT	CHES'07	Block	80	64	1.5K, 200Kbs @100Mhz	0.13μm	Enc	0.13 (0.19)

Suitable Situations of CLEFIA

- **Used for Strongly Restricted Situation of Hardware**
  - Only 4,950 gates achieving 715Mbps
  - Saved space can be used for additional functions
    - Modes of Operation, Countermeasure against DPA, DFA
- **Low Power**
  - CLEFIA's small footprint implies low power consumption
- **Balance in Software and Hardware**
  - Software performance is also good
  - A High power machine (software) + Small device (hardware)
- **Diversity**
  - Design philosophy of CLEFIA is sufficiently apart from KASUMI, SNOW 3G, AES
  - Coexistence with these algorithms

Conclusion

- CLEFIA is a compact and high-speed cipher suitable for limited resource environment
- Although CLEFIA is a young cipher published in 2007, thorough evaluation efforts have been done by experts
- KASUMI, SNOW3G, AES and CLEFIA may generate good diversity

Thank you for your attention

References

- [SAGE06] Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 5: Design and Evaluation Report
- [SM03] A. Satoh and S. Morioka, “Hardware-focused performance comparison for the standard block ciphers AES, Camellia, and Triple-DES." in Proceedings of ISC 2003, no. 2851 in LNCS, pp. 252-266, Springer-Verlag, 2003.
- [CLEFIA] T.Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata “The 128-bit Blockcipher CLEFIA.” in proceedings of FSE 2007, no. 4593 in LNCS, pp. 181-195, Springer-Verlag, 2007
- [HIGHT] *D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, S. Chee* “HIGHT: A New Block Cipher Suitable for Low-Resource Device.” in proceedings of CHES 2006, no. 4249 in LNCS, pp. 46-59, Springer-Verlag, 2006
- [PRESENT] *A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe* “PRESENT: An Ultra-Lightweight Block Cipher” in proceedings of CHES 2007, no. 4727 in LNCS, pp. 450-466, Springer-Verlag, 2007