Japan CRYPTREC Activity on Lightweight Cryptography

Shiho Moriai

NICT

CRYPTREC

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

CRYPTREC
Cryptography Research and Evaluation Commitees

Outline

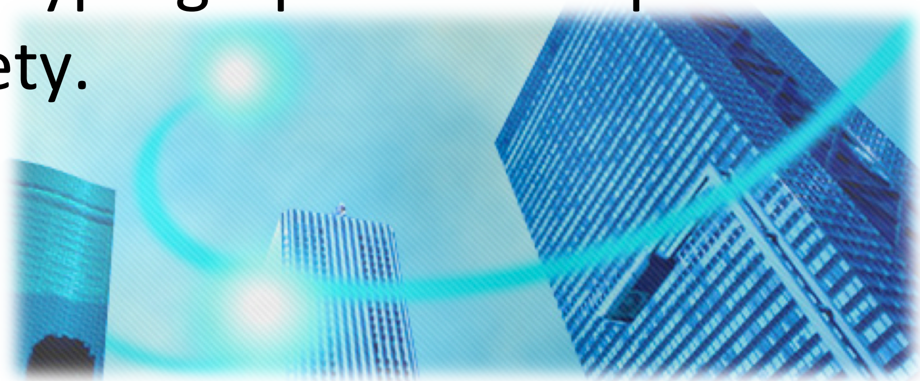
- CRYPTREC
- Lightweight Cryptography (LWC) WG
- Scope of LWC in CRYPTREC
- Advantages and Restrictions of LWC
- LWC for Internet of Things
- Future Plan

CRYPTREC

Cryptography Research and Evaluation Committees

- Project to evaluate and monitor the security of cryptographic techniques used in Japanese e-Government systems

- Goal of the project
  - To ensure the security of Japanese e-Government systems by using secure cryptographic techniques and to realize a secure IT society.

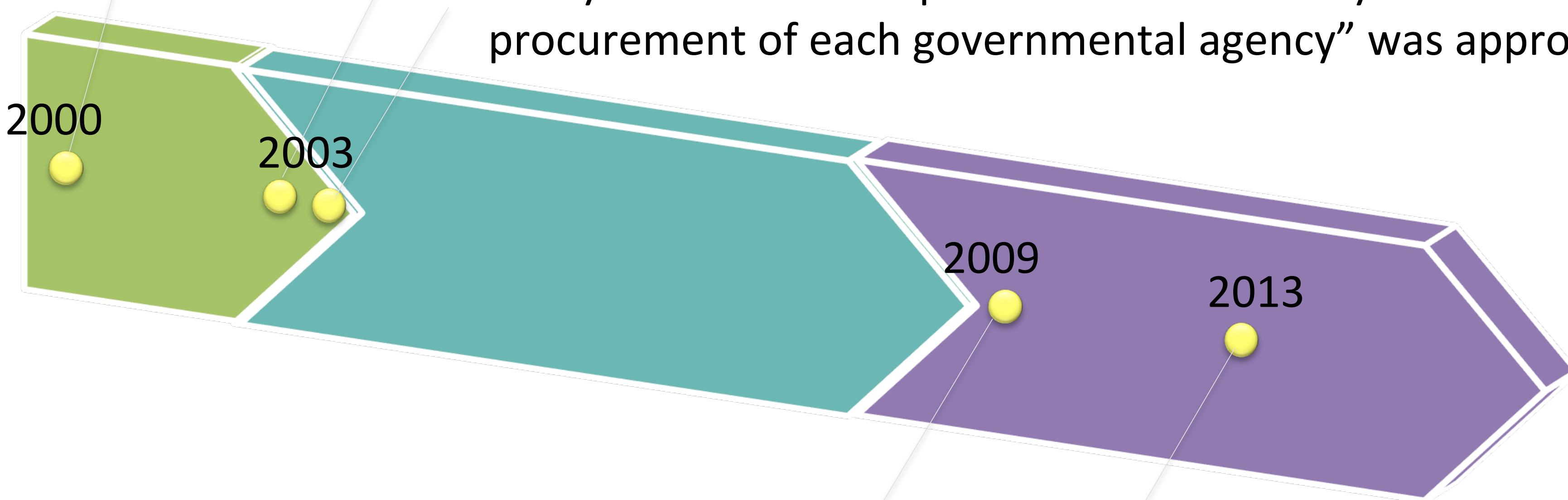


History of CRYPTREC

CRYPTREC launch, Call for cryptographic techniques

Publication of the e-Government Recommended Ciphers List

“Policy for the use of ciphers in information system procurement of each governmental agency” was approved



Call for cryptographic techniques for the revision of the e-Government Recommended Ciphers List

Publication of the CRYPTREC Ciphers List

CRYPTREC
Cryptography Research and Evaluation Commitees

Three Lists in the CRYPTREC Ciphers List

- **e-Government Recommended Ciphers List**
  - Recommended ciphers approved by CRYPTREC in terms of security and implementation aspects as well as current and future market deployment.

- **Candidate Recommended Ciphers List**
  - Candidate recommended ciphers approved by CRYPTREC in terms of security and implementation aspects.

- **Monitored Ciphers List**
  - The ciphers are not-recommended for use because of high risk of compromise while they are allowed to use only for interoperability with legacy systems.

CRYPTREC Ciphers List

CRYPTREC
Cryptography Research and Evaluation Commitees

e-Government Recommended Ciphers List

Classification		Cipher
Public key ciphers	Signature	DSA
		ECDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	Confidentiality	RSA-OAEP
	Key exchange	DH
		ECDH
Symmetric key ciphers	64-bit block ciphers	3-key Triple DES
	128-bit block ciphers	AES
		Camellia
	Stream ciphers	KCipher-2
Hash functions		SHA-256
		SHA-384
		SHA-512
Modes of operation	Encryption modes	CBC
		CFB
		CTR
		OFB
	Authenticated encryption modes	CCM
		GCM
Message authentication codes		CMAC
		HMAC
Entity authentication		ISO/IEC 9798-2
		ISO/IEC 9798-3

Candidate Recommended Ciphers List

- Key exchange
  - PSEC-KEM
- 64-bit block ciphers
  - CIPHERUNICORN-E, Hierocrypt-L1, MISTY1
- 128-bit block ciphers
  - CIPHERUNICORN-A, CLEFIA, Hierocrypt-3, SC2000
- Stream ciphers
  - Enocoro-128v2, MUGI, MULTI-S01
- MAC
  - PC-MAC-AES
- Entity Authentication
  - ISO/IEC 9798-4

Monitored Ciphers List

- Public-key Encryption
  - RSAES-PKCS1-v1_5
- Stream cipher
  - 128-bit key RC4
- Hash functions
  - RIPEMD-160, SHA-1
- MAC
  - CBC-MAC

CRYPTREC Organization

CRYPTREC
Cryptography Research and Evaluation Commitees

NISC National center of Incident readiness and Strategy for Cybersecurity

Management Standards for Information Security Measures for the Central Government Computer Systems

総務省 MIC Ministry of Internal Affairs and Communications

Advisory Board for Cryptographic Technology
(Secretariat:MIC,METI)

経済産業省 Ministry of Economy, Trade and Industry

国立研究開発法人 情報通信研究機構 NICT National Institute of Information and Communications Technology

IPA 独立行政法人情報処理推進機構 Information-technology Promotion Agency, Japan

Cryptographic Technology Evaluation Committee (Secretariat:NICT,IPA)

(1) Monitoring and evaluation of the security and implementation properties of the cryptographic technology
(2) Research on new-generation cryptographic technology
(3) Research on secure utilization of cryptographic technology

- Cryptanalysis Evaluation WG
- Lightweight Cryptography WG

Cryptographic Technology Promotion Committee (Secretariat:NICT,IPA)

(1) Research on the promotion of cryptographic technologies and the strengthening of IT security industries
(2) Research on the utilization status of cryptographic technologies and research of their promotion strategy
(3) Research on the strategy of cryptographic policy from mid-and-long term viewpoints

- Operational Guideline WG
- Standardization Promotion WG

http://www.cryptrec.go.jp/system.htm

CRYPTREC
Cryptography Research and Evaluation Commitees

Lightweight Cryptography (LWC) WG

- Goal
  - LWC WG started in 2013 so that appropriate lightweight cryptography can be selected and procured for e-government systems and any applications where they are required.

- Activities
  - Survey and research on state of the art in LWC
  - Research on applications of LWC
  - Implementation evaluation
  - Discussion of future plan
  - Publish reports as deliverables

LWC WG Committee Members

Chair	Naofumi Homma	Tohoku Univ.
	Kazumaro Aoki	NTT
	Tetsu Iwata	Nagoya Univ.
	Kazuto Ogawa	NHK Science & Technology Research Lab.
	Kazuo Sakiyama	The Univ. of Electro-Communications
	Kyoji Shibutani	Sony Corporation
	Daisuke Suzuki	Mitsubishi Electric Corporation
	Yuichiro Nariyoshi	Renesas Electric Corporation
	Kazuhiko Minematsu	NEC Corporation
	Hideyuki Miyake	Toshiba Corporation
	Dai Watanabe	Hitachi, Ltd.

CRYPTREC
Cryptography Research and Evaluation Commitees

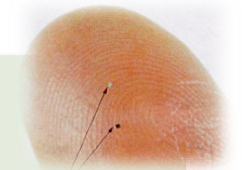
Scope of LWC in CRYPTREC

- "Cryptographic primitives with advantages (lightweight properties) over existing cryptographic primitives in specific efficiency measures admitting tradeoffs between efficiency and security"

Typical efficiency measures for LWC

Efficiency measures		Application examples
Hardware Implementation	**Gate Count（Power, Cost）**	RFID, Low-cost sensors
	Energy	Medical/healthcare devices, battery-powered devices
	Latency	Memory encryption, In-vehicle devices, Industrial control systems
Software Implementation	**Memory（ROM/RAM）**	Consumer electronics, Sensors, In-vehicle devices

Advantages of LWC



Gate Count

- Difference between LWC and AES (a few kgates) is critical in small chips e.g. 50µm square chips and in mature process technologies e.g. 180nm-350nm CMOS.

Energy

- As gate count is small, power/energy consumption is small. LWC is expected to relax requirements on power/energy consumption.

Latency

- There exists a lightweight primitive which achieves twice lower latency of AES with 1/10 gate counts (encrypts in < 10ns with 20kgate). Useful in applications where real-time response in the order of microseconds is required, e.g. industrial control systems.

Memory

- There exists a lightweight primitive which can be implemented within ¼ ROM of AES. There exist cases where only LWC can be implemented or a cheaper microprocessor can be adopted.

Implementation evaluation of LW block ciphers

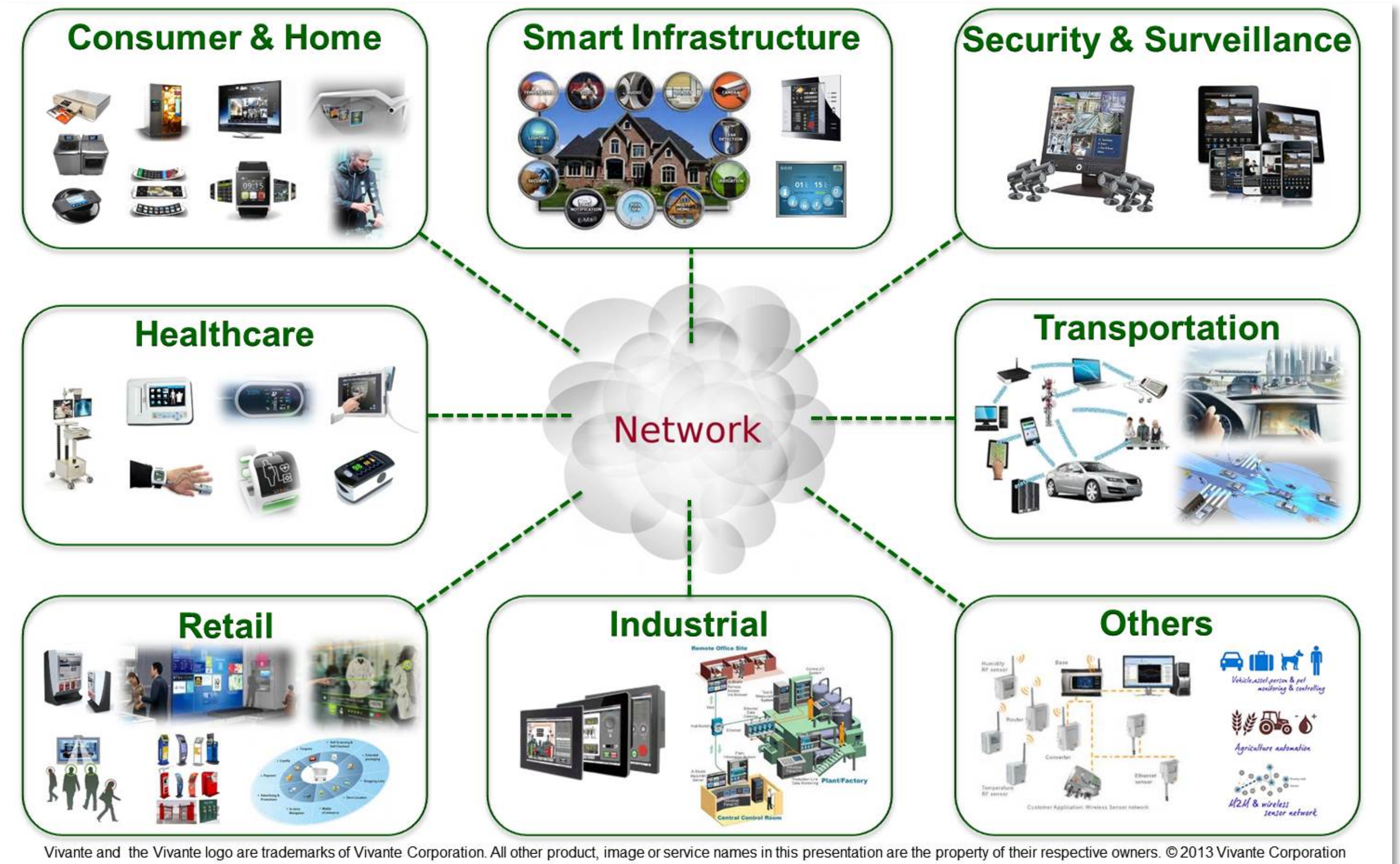
- Aim
  - Evaluate using the same interface and platform for a fair comparison.
- Target algorithms
  - AES, Camellia, CLEFIA, PRESENT, LED, Piccolo, TWINE, PRINCE
- Platform and Efficiency measures
  - H/W implementation
    - Standard CMOS cell library : NANGATE Open Cell Library (45nm CMOS)
    - 3 Architectures: Unrolled, Round, Serial implementations
    - Measures : Max Frequency, Throughput, Gate counts, Latency, Power, Peak power, Leak power
  - Embedded S/W implementation
    - Processor : Renesas Electronics RL78 (16bit microcontroller)
    - Measures : Speed, RAM size, ROM size

Restrictions of LWC (and Countermeasures)

- Security provided by LWC
  - Some lightweight cryptographic primitives are designed to have advantages (lightweight properties) in specific efficiency measures, so their security turn out to be sacrificed.
  - For example, for 64-bit block ciphers, a secret key should be changed after 2^{32} block encryptions (32GB).
  - However, there exist some countermeasures and special modes for beyond the "birthday bound" security.

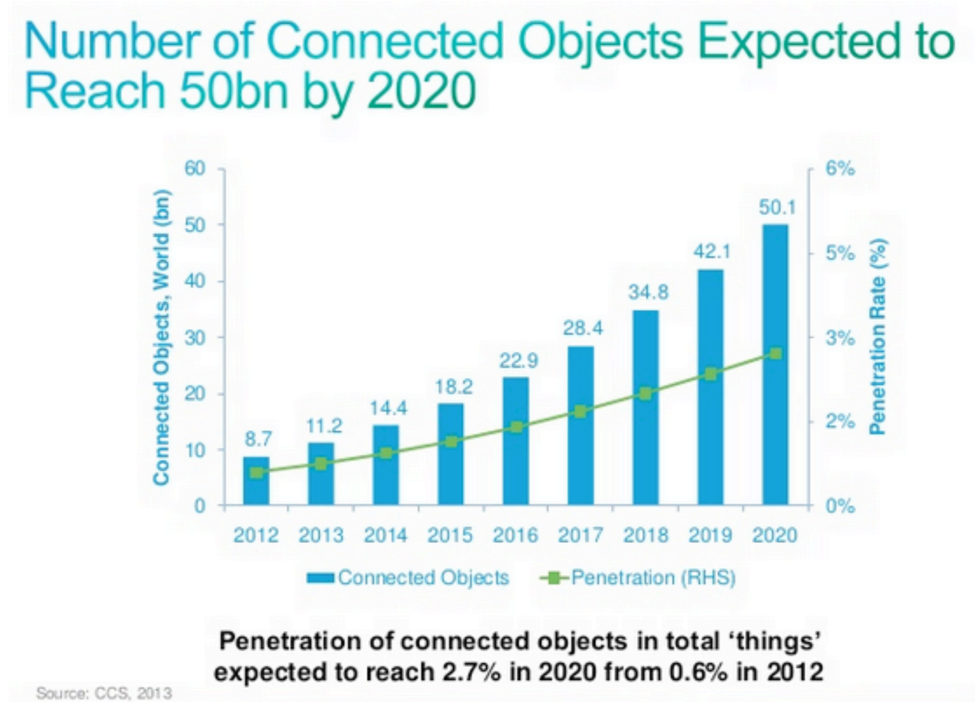
Internet of Things (IoT)

Everything is connected.



IoT: Number of connected objects

- Gartner — 26 bn by 2020
- IDC — 30 bn by 2020
- Cisco — 50 bn by 2020
- intel — 2000 bn by 2020



Current standard security solution can not be implemented on all the connected objects!

LWC for IoT

- In the IoT era, where 1000 bn sensors and 50 bn objects are connected, crypto techniques will be required for devices with low-end micro controllers.
- Crypto techniques will be implemented on more devices – not implemented at present. LWC can relax implementation requirements.
  - Automotive: Autonomous cars
  - Industrial control system: factories and plants are connected to clouds.

Hearing of Opinions on LWC Applications

- "Information security technologies for automotive"
  - Hisashi Oguma, Toyota InfoTechnology Center
    - Many ECUs are embedded in a car.
    - LWC can be useful for improving CAN security (data payload is 8 byte).
- "Study of requirements for cryptographic technology for control systems"
  - Toru Ohwada, Hitachi Ltd.
    - Extract requirements for cryptographic technology for control systems from real problems.
    - LWC with low-latency, low-cost, support for flexible data size will be useful. Key management with low resource and support for easy change of algorithms/key sizes will be helpful.

CRYPTREC
Cryptography Research and Evaluation Commitees

Contents of the CRYPTREC Report on LWC

1. Executive Summary
   - Scope
   - Advantages over existing cryptographic techniques
   - Restrictions (Security provided by lightweight primitives)
   - Future plan proposal
2. Survey of lightweight cryptographic primitives (security & implementation aspects)
   - Overview
   - Lightweight block ciphers
   - Lightweight stream ciphers
   - Lightweight hash functions
   - Lightweight MACs
   - Authenticated encryption

Available at CRYPTREC Web

Contents of the CRYPTREC Report on LWC (Cont.)

3. Survey of new trends related to lightweight cryptography
   - Low latency cryptography
   - Side channel attacks and countermeasures
   - CAESAR competition
   - Application examples and standardization
4. Hearing of opinions on lightweight cryptography applications from users
5. Benchmarking of lightweight block ciphers in embedded software and hardware

Available at CRYPTREC Web

Future Plan

- Deliver a guideline on lightweight cryptography
  - describes advantages and restrictions of LWC
  - shows security and performance evaluation/ comparison results
  - so that it facilitates easy selection of appropriate lightweight cryptographic primitives for users and promotion of LWC

Conclusion

CRYPTREC
Cryptography Research and Evaluation Commitees

- Introduced Japan CRYPTREC activity on LWC.
- Since LWC is expected to play an important role in IoT security, CRYPTREC will provide a guideline on LWC for users' easy selection of appropriate lightweight cryptographic primitives and promotion of LWC.
- CRYPTREC Report 2014 is available from below:

  http://cryptrec.go.jp/english/topics/cryptrec_20150716_c14report.html