Lightweight Cryptography for ITS Security

Shiho Moriai
Security Fundamentals Lab.
Cybersecurity Research Institite
NICT, Japan

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

Outline of my talk

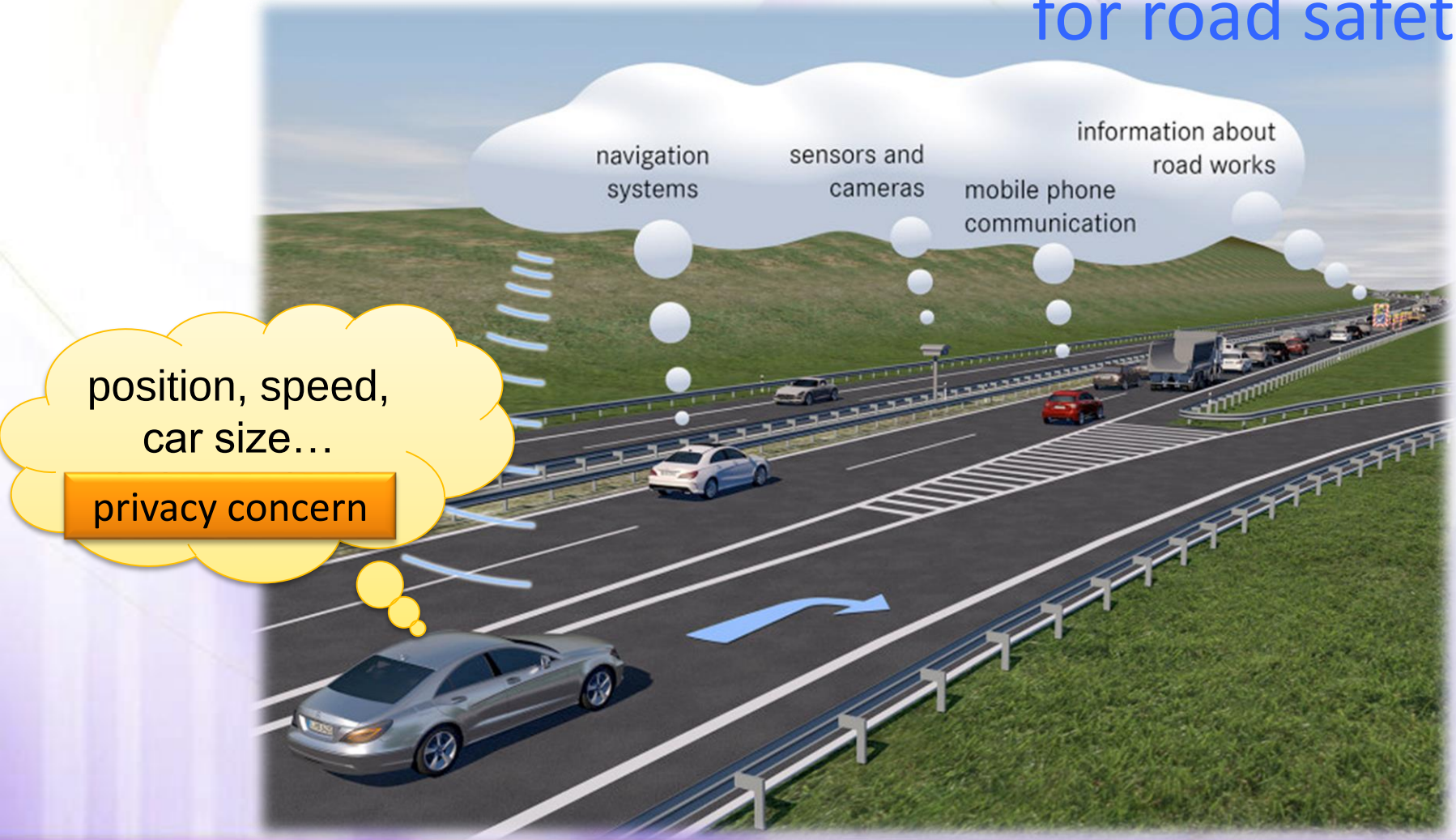
- Emerging Automotive/ITS Services
  - Automotive sensors are key factors
- Lightweight Cryptography
  - to protect automotive sensor data and address privacy concerns with “lightweight” cost
  - Standards and Guidelines
  - Implementation aspects

Emerging Automotive/ITS Services

Emerging Automotive/ITS Services

- V2X communication services

for road safety



http://www.carnectiv.com/2014/02/association-of-global-automakers-research-v2v/

Emerging Automotive/ITS Services

- Use of in-vehicle sensor data

to drive safe and save

Insurance company

upload

- Miles driven
- Acceleration
- Braking
- Right and left turns
- Speeds of 80 mph or over
- Time of day the car is driven

privacy concern

"Automobile Driver Fingerprinting" by Enev et al., in Proceedings on Privacy Enhancing Technologies, 2016(1):34-51

http://www.compare.com/compare-car-insurance/state-farm-drive-safe-and-save-review

Emerging Automotive/ITS Services

- Autonomous Driving

for safety and more

Correctness, integrity, authentication, and authenticity of sensory information is crucial to system reliability.

http://www.automotiveit.com/bosch-sees-gradual-progression-to-autonomous-driving/news/id-007672

Automotive Sensors

- Critical to system reliability
- Facing privacy issues

- Concerns
  - Insufficient Security Countermeasures
  - Resource-constrained
    - difficult to implement a full-fledged security solution
  - Misuse of the Data
  - Active Attacks (by data modification)

http://www.automotiveit.com/bosch-sees-gradual-progression-to-autonomous-driving/news/id-007672

Lightweight Cryptography

Lightweight Cryptography

- Cryptographic primitives with advantages (lightweight properties) in specific implementation efficiency measures
  - admitting tradeoffs between efficiency and security

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

History of Downsizing Cryptosystems

Hardware gate count

1925

Portable!!

ENIGMA

Efficient Hardware

2000

< 10Kgate

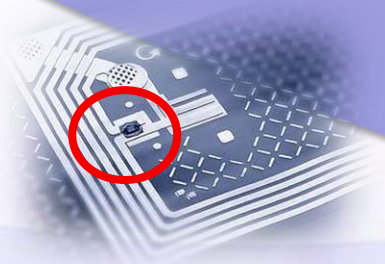
KASUMI, adopted by 3GPP standard

Lightweight Cryptography

2005

< 3Kgate

HIGHT, CLEFIA, PRESENT



Ultra Lightweight Cryptography

2010

< 1Kgate

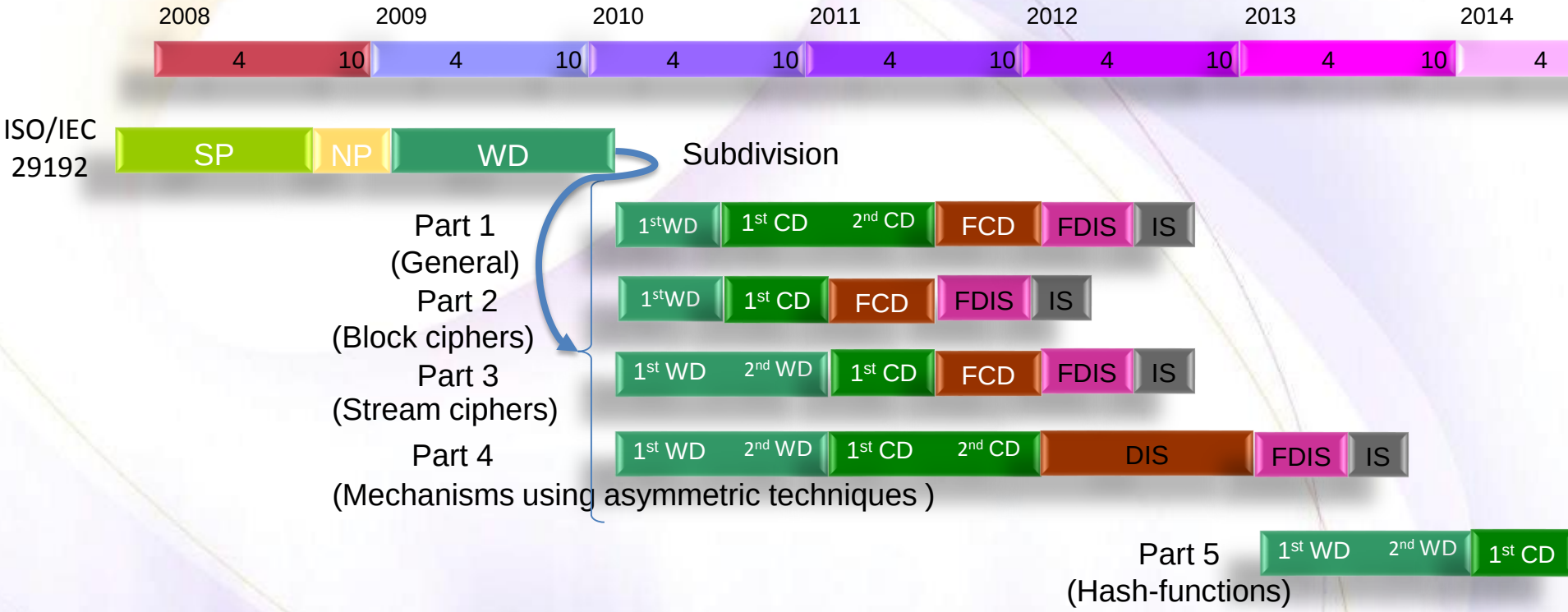
KATAN, Piccolo

2020?

Standards on Lightweight Cryptography

- ISO/IEC 29192 (Lightweight Cryptography)
  - Part 1: General
    - editors: Riaal Domingues, Shiho Moriai
  - Part 2: Block ciphers
    - editors: Shiho Moriai, Axel Poschmann
  - Part 3: Stream ciphers
    - editor: Hirotaka Yoshida
  - Part 4: Mechanisms using asymmetric techniques
    - editors: Matt Robshaw, Jean-Francois Misarsky
  - Part 5: Hash-functions
    - editors: Axel Poschmann, Shiho Moriai
  - Part 6: Message authentication codes (MACs)
    - editors: Hirotaka Yoshida, Suresh Ramasamy

ISO/IEC 29192 Standardization Status



Standardization stages in ISO/IEC

SP (Study Period)
NP (New Project)
WD (Working Draft)
CD (Committee Draft)
FCD (Final Committee Draft)
FDIS (Final Draft International Standard)
IS (International Standard)

Part 6 (MAC) started in 2016

ISO/IEC 29192 Standardization Status

- US
  - NSA designed lightweight block ciphers for IoT (SIMON & SPECK) and proposed them for ISO/IEC 29192-2.
  - NIST hold workshops on LWC and published the report NISTIR 8114 (2017.3).
    - Lightweight Cryptography Workshop 2015, 2016

Emerging Automotive/ITS Services

CRYPTREC

Cryptography Research and Evaluation Committees

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

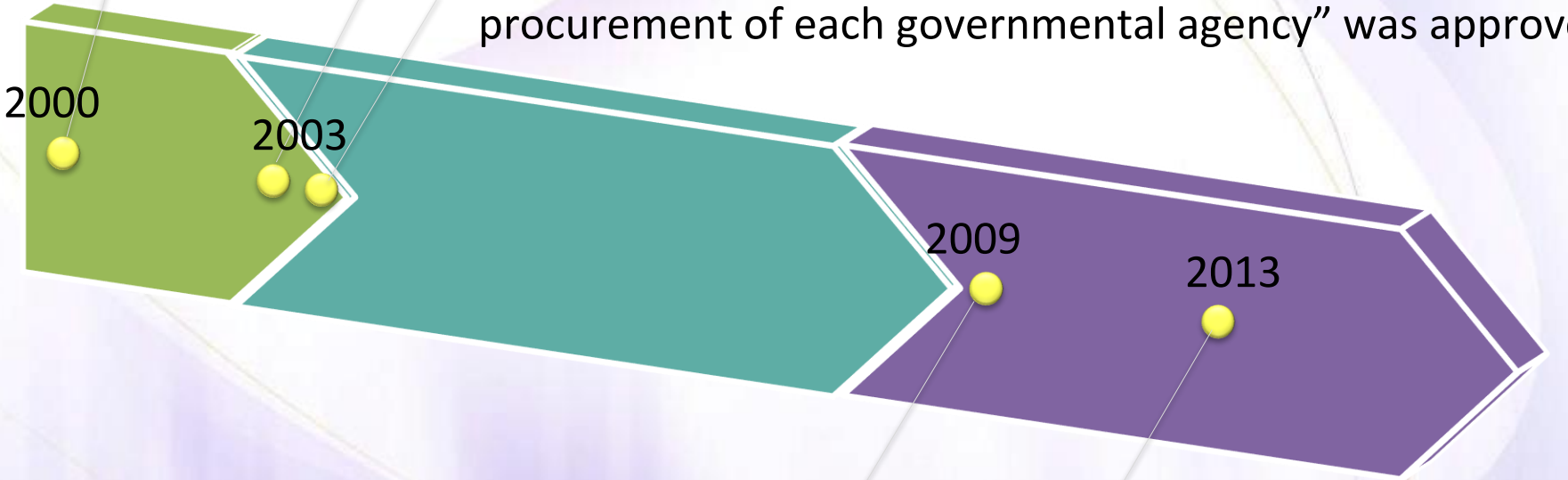
- Goal of the project
  - To ensure the security of Japanese e-Government systems by using secure cryptographic techniques and to realize a secure IT society.

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 Organization

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

Lightweight Cryptography WG

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

- Activities
  - Survey and research on state of the art in LWC
  - Research on applications of LWC
  - Implementation evaluation
  - Publish reports/guidelines 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.
	Hisashi Oguma	Toyota InfoTechnology Center
	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 Guideline on lightweight cryptography

- The guideline was written so that it facilitates easy selection of appropriate lightweight cryptographic primitives for (non-expert) users and promotion of LWC.
- It was published in both Japanese and English on the CRYPTREC web site.
  - http://www.cryptrec.go.jp/
- More than 100 pages

Contents of the Guideline (1/2)

1. Introduction
2. Lightweight Cryptography and Its Applications
    1. What is Lightweight Cryptography?
    2. Target Applications of Lightweight Cryptography
    3. Selection of Lightweight Cryptographic Algorithms and Parameters
    4. Effects of Lightweight Cryptography

Contents of the Guideline (2/2)

3. Comparing the Pe
   Lightweight Crypt
   1. Block Ciphers
   2. Authenticated Enc
4. Lightweight Cryp
   Schemes
   1. Block Ciphers
   2. Stream Ciphers
   3. Hash Functions
   4. Message Authenti
   5. Authenticated Enc

	Hash function
Name	Keccak
Designers	Guido Bertoni (STMicroelectronics), Joan Daemen (STMicroelectronics), Michaël Peeters (NXP Semiconductors), Gilles Van Assche (STMicroelectronics)
Publication	2008 (NIST SHA-3 Competition)
Specifications	http://keccak.noekeon.org/
Features	Keccak is a family of sponge functions. Seven permutations are defined and indicated by Keccak-f[b] (b ∈ 25, 50, 100, 200, 400, 800, 1,600). From the viewpoint of lightweight cryptography, the schemes using Keccak-f[100], Keccak-f[200], and Keccak-f[400] will be described.
Security Analysis	Many papers have analyzed Keccak, and no critical vulnerability has been reported.
Performance Analysis	Hardware implementation[6](130nm process)
Standardization	The scheme using Keccak-f[1600] is standardized by NIST in FIPS202 [3]. For SHA-3 derived functions, a series of special publication is available by NIST SP800-185 [4].
Market Deployment	SHA-3 is being adopted in many different applications. http://csrc.nist.gov/groups/STM/cavp/documents/sha3/sha3val.html, http://www.3gpp.org/DynaReport/35-series.htm.
Open Source Information	http://keccak.noekeon.org/files.html, https://github.com/gvanas/KeccakCodePackage

Keccak-f[b]	n	r	r'
Keccak-f[100]	80	20	20
Keccak-f[200]	64	72	72
Keccak-f[400]	128	144	144

∗ n: output length, r: input block length, r' : output block length

	Area [GE]	Latency [clk]	Throughput [kbps]
Keccak-f[100]	1250	800	2.5
Keccak-f[200]	2520	900	8.00
Keccak-f[400]	5090	1000	14.40

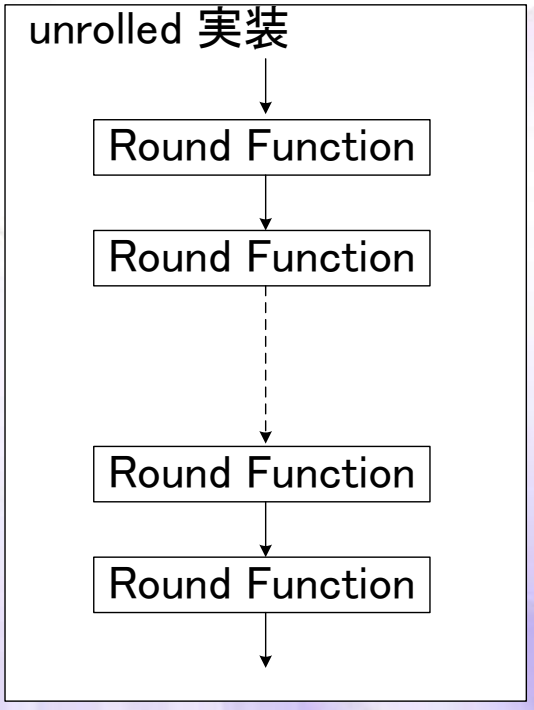
Figure 3.31: Speed with 512-byte ROM and 128-byte RAM

Implementation Evaluation

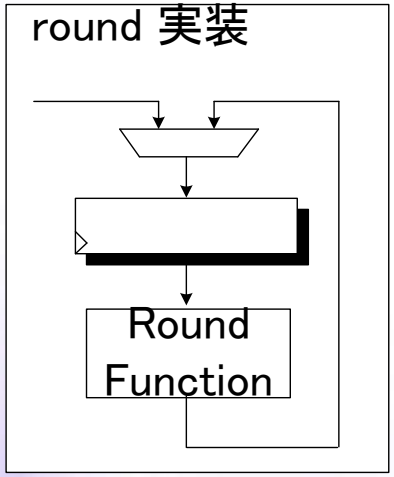
- Aim
  - Evaluate some lightweight block ciphers using the same interface and platform for a fair comparison.
- Target algorithms
  - 12 Lightweight Block ciphers
  - 10 Lightweight Authenticated Encryption schemes
- Implementation Platforms
  - Hardware implementation
    - ASIC (library : NANGATE Open Cell Library (45nm CMOS))
  - Embedded Software implementation
    - Processor : Renesas Electronics RL78 (16bit microcontroller)

Hardware Implementation

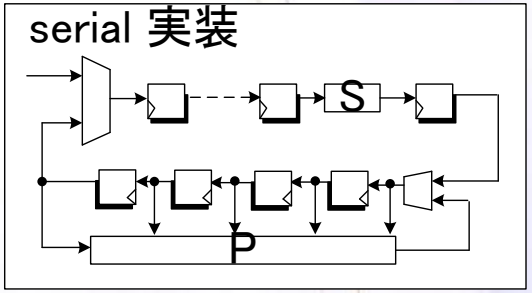
- Standard CMOS cell library : NANGATE Open Cell Library (45nm)
- 3 Architectures: Unrolled, Round, Serial implementations
- Measures : Max Frequency, Throughput, Gate counts, Latency, Power, Peak power, Leak power



High-Speed implementation



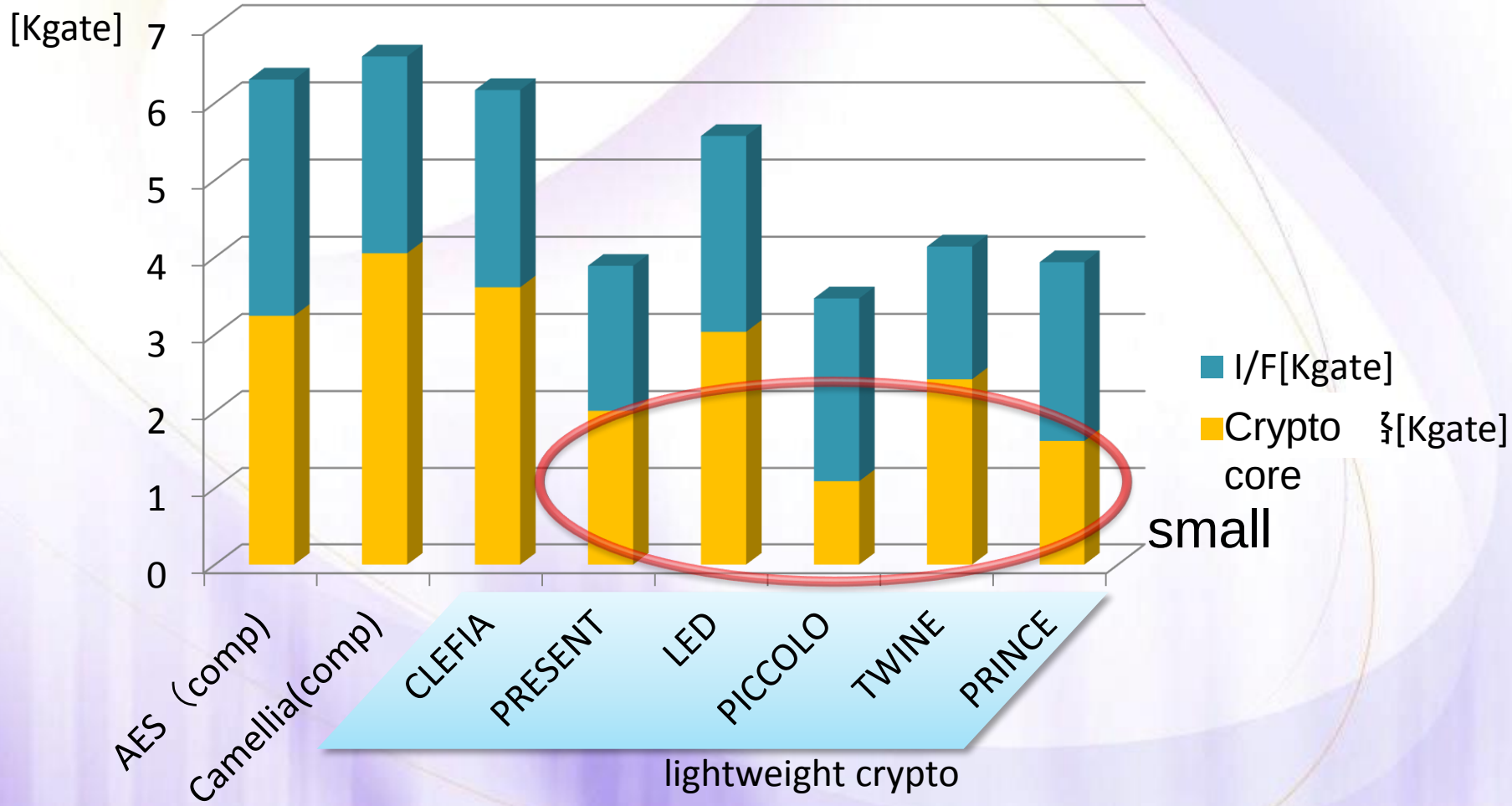
Standard implementation



Low-Cost implementation

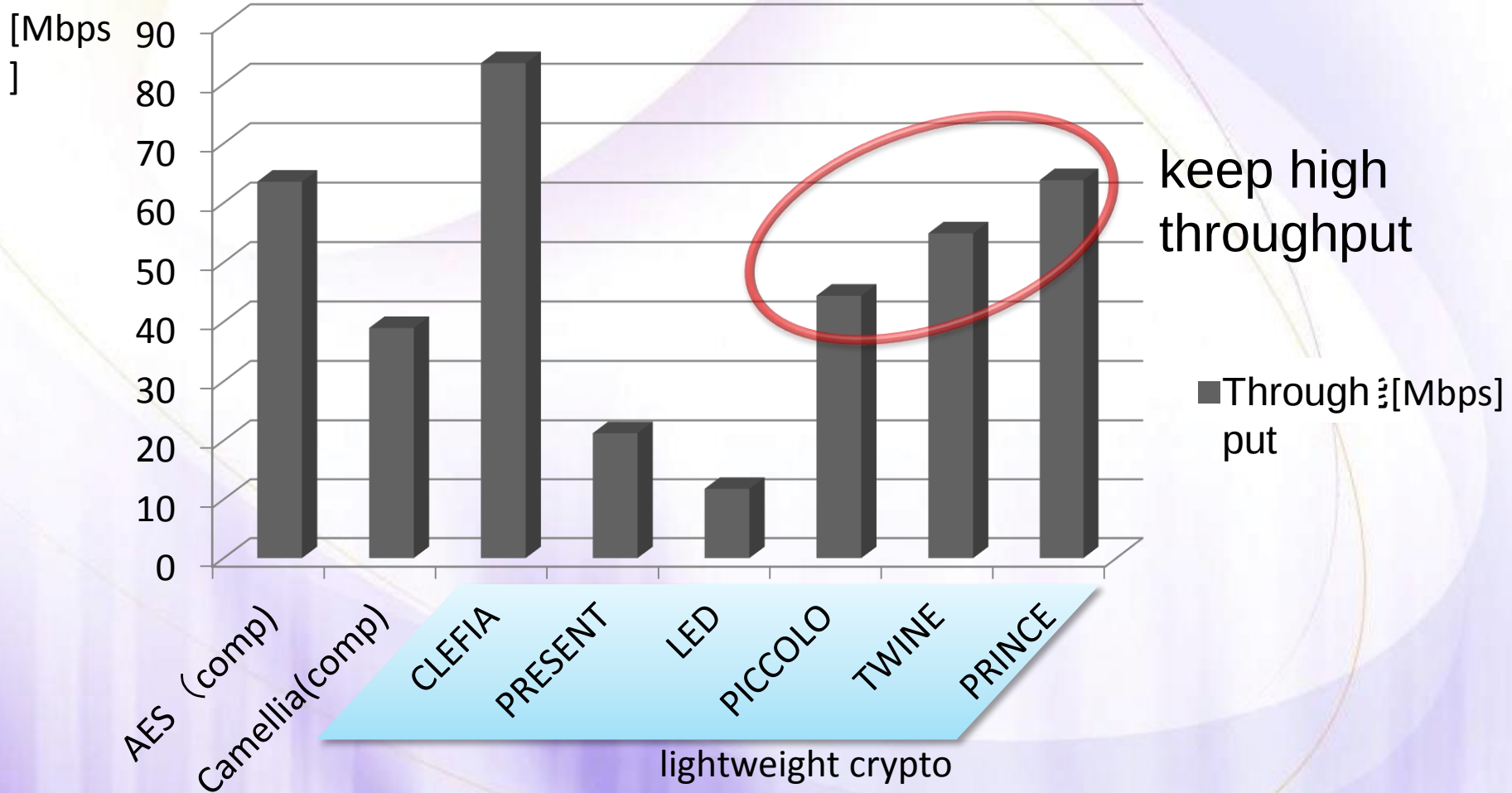
Serial Implementation (Low-cost)

Gate Count Crypto-core is small (1-3Kgates), but I/F (incl. registers for plaintext/ciphertext and key) can not be ignored.



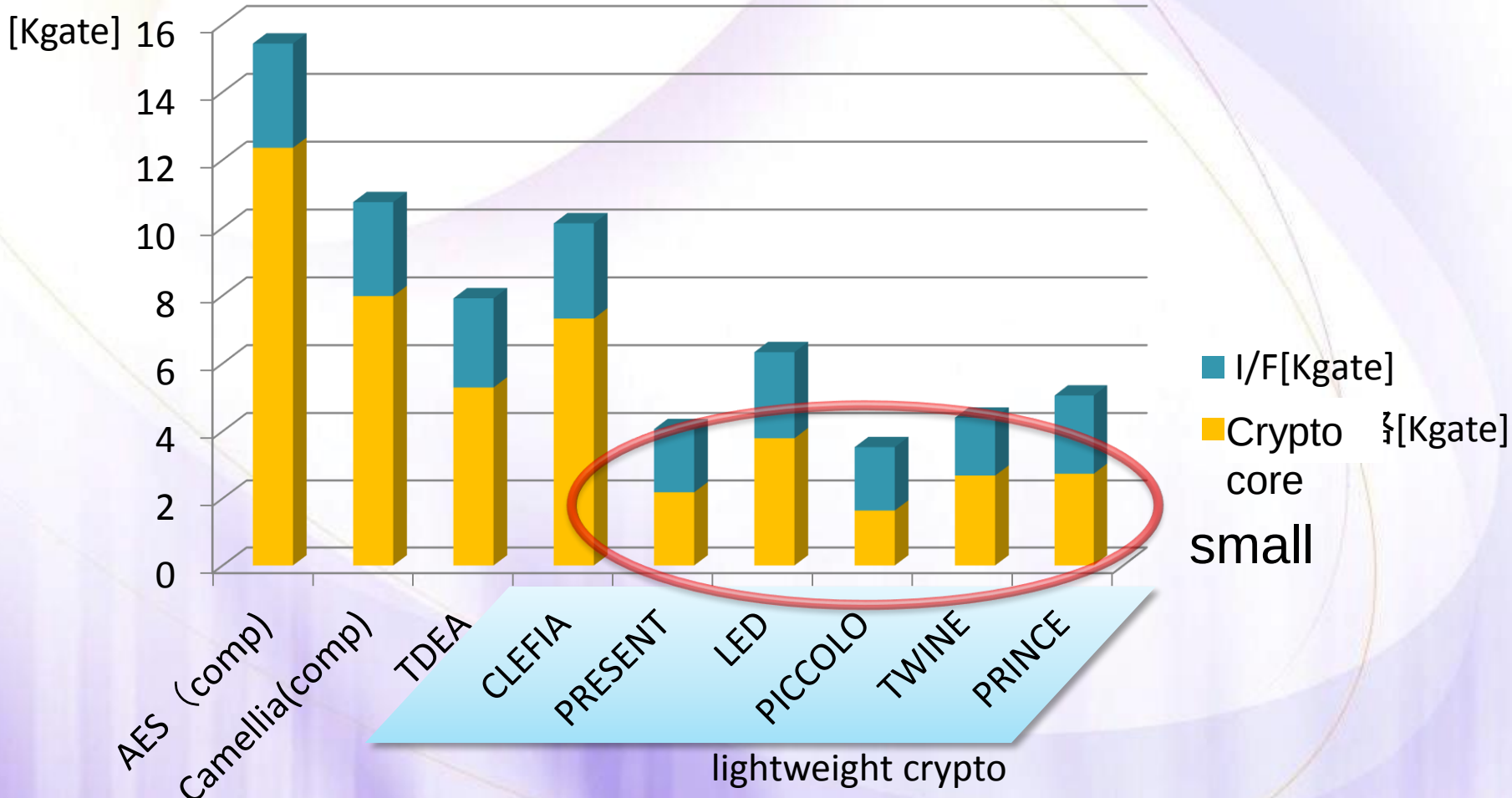
Serial Implementation (Low-cost)

Throughput Small gate size does not sacrifice speed in some lightweight crypto



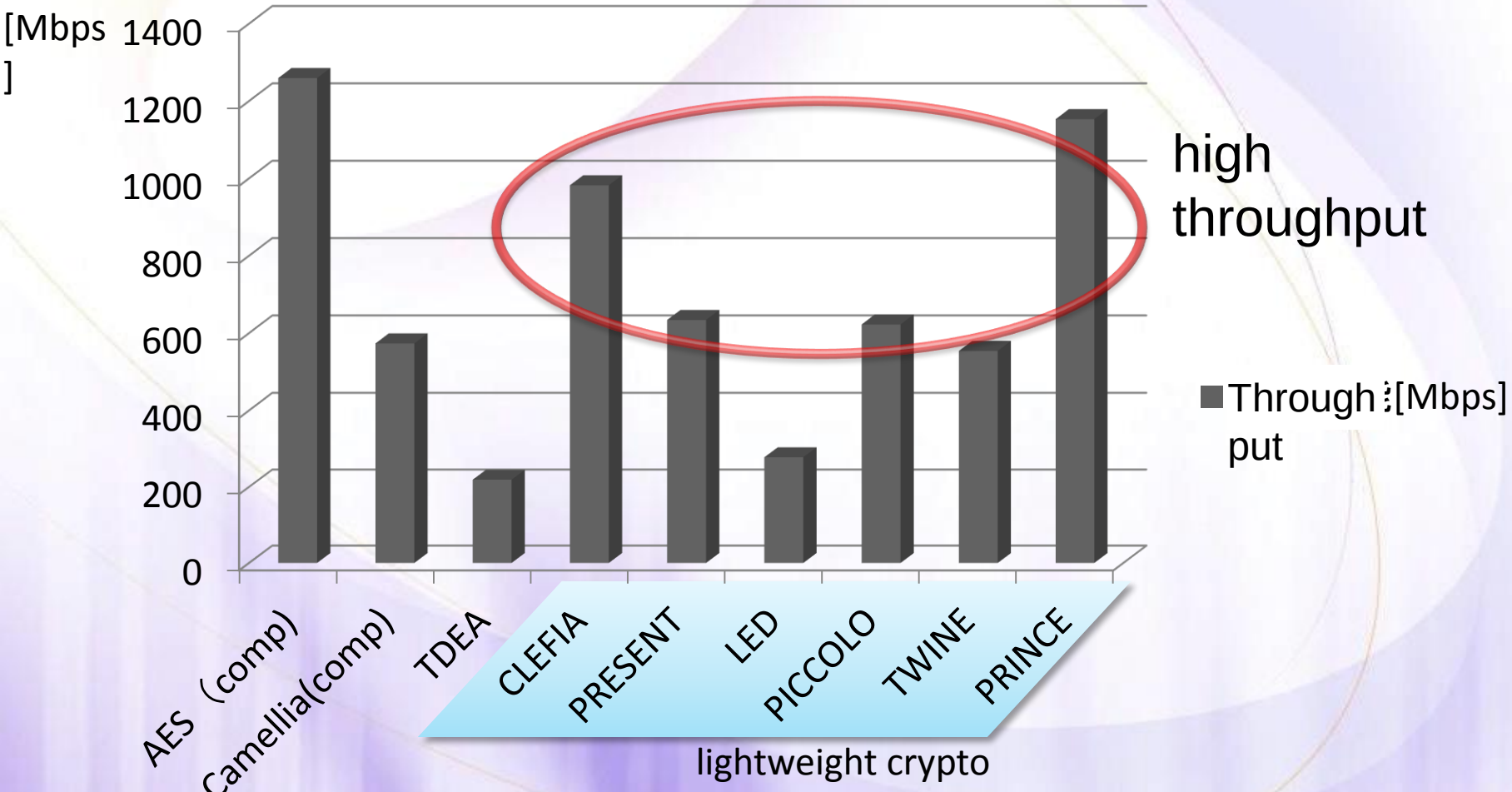
Round Implementation

Gate Count Many lightweight crypto can be implemented within ~4Kgates.



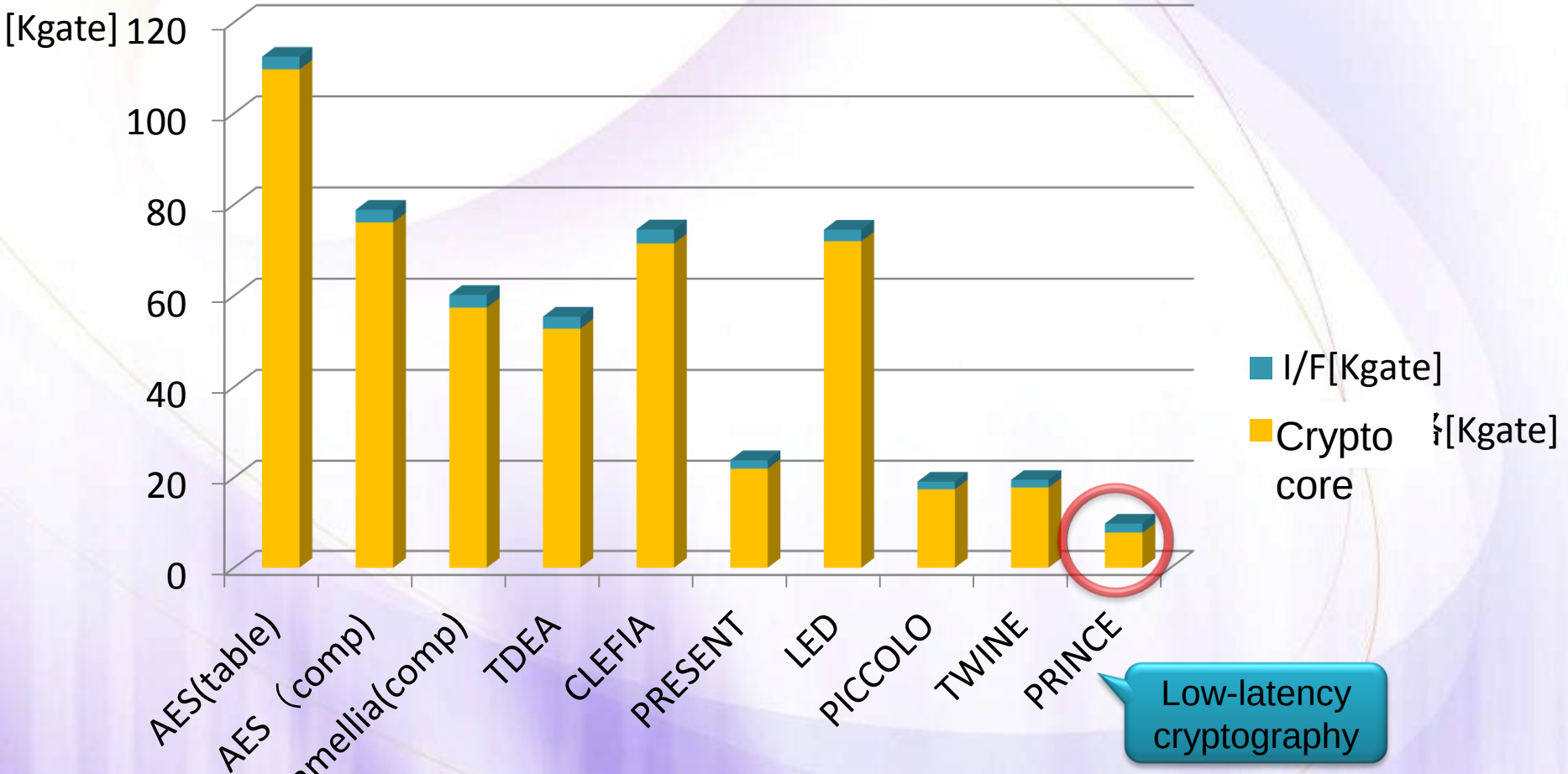
Round Implementation

Throughput Many lightweight crypto achieve 10 times higher throughput than AES with a similar gate size (~60Mbps with ~6Kgates).



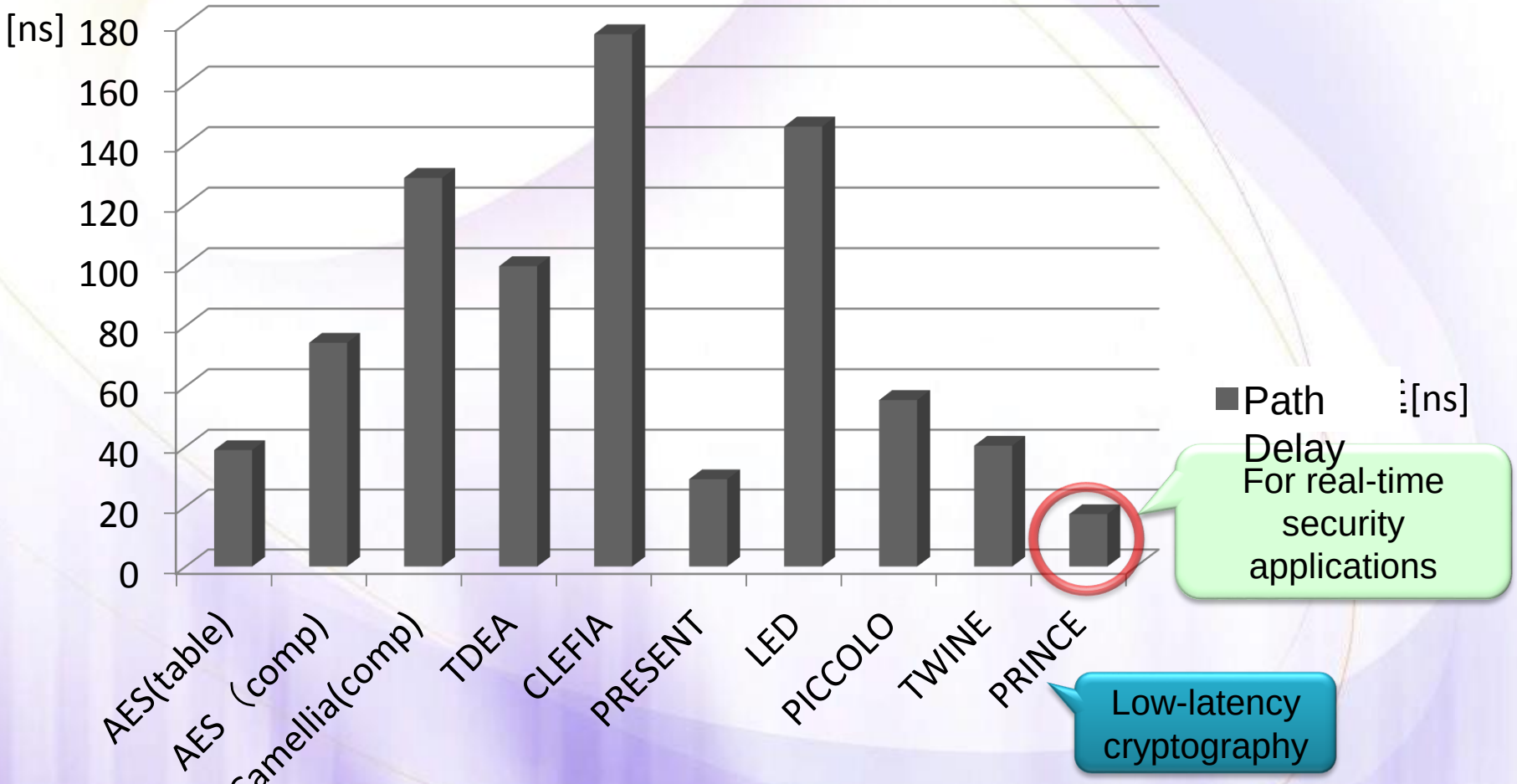
Unrolled Implementation (High-Speed)

Gate Count Low-latency cryptography can encrypt within one clock cycle with ~1/10 gate counts of AES.



Unrolled Implementation (High-Speed)

Path Delay Low-latency cryptography achieves real-time security (several ns) with less than 20 Kgate counts.



Embedded Software Implementation

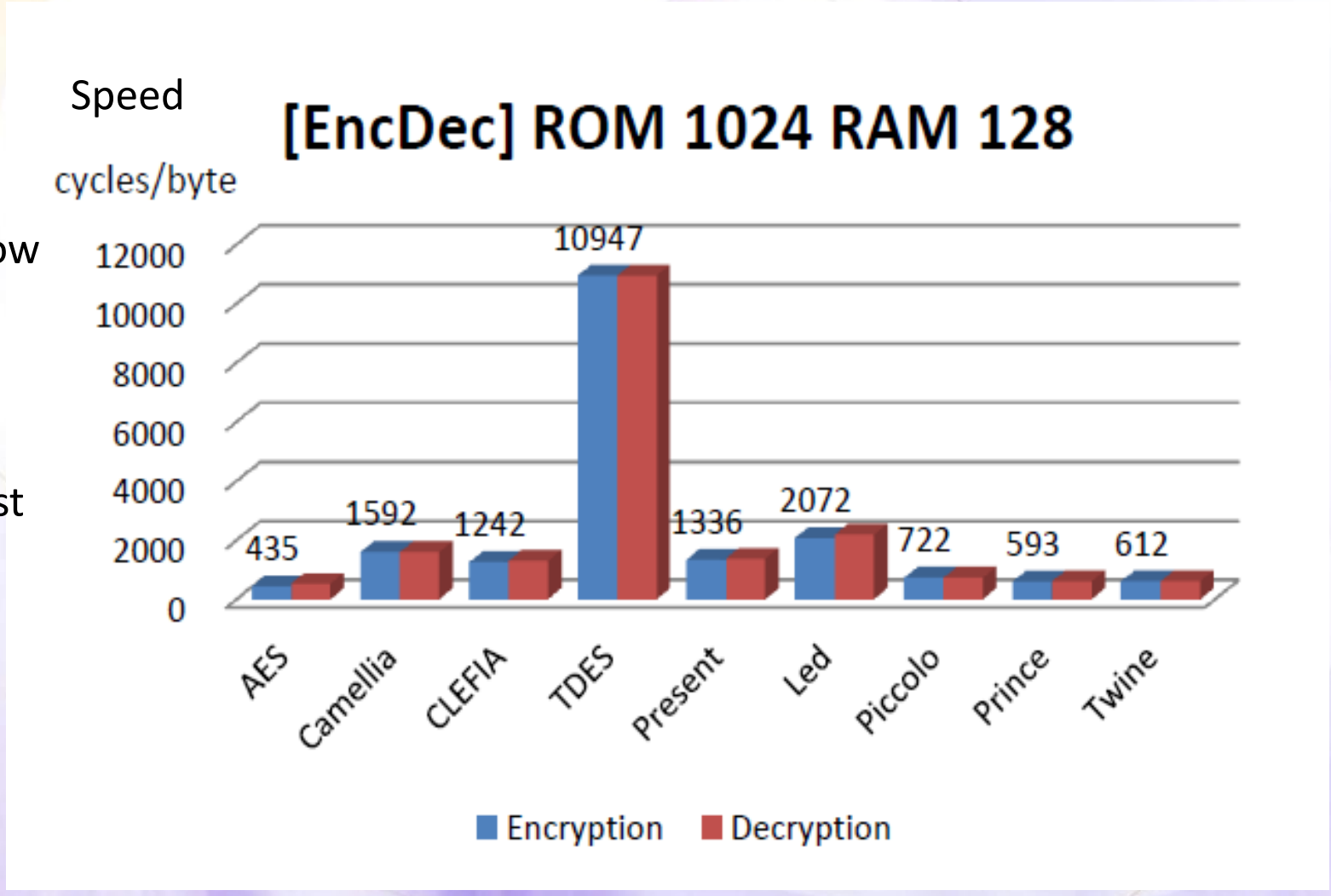
- Processor
  - Renesas Electronics RL78 (16bit microcontroller)
    - General-purpose (G1x series): ROM 1KB～, RAM 128B～
      Automotive (F1x series): ROM 8KB～, RAM 512B～

Only limited memory is available for crypto. Small memory requirement increases selection options of microcontrollers.

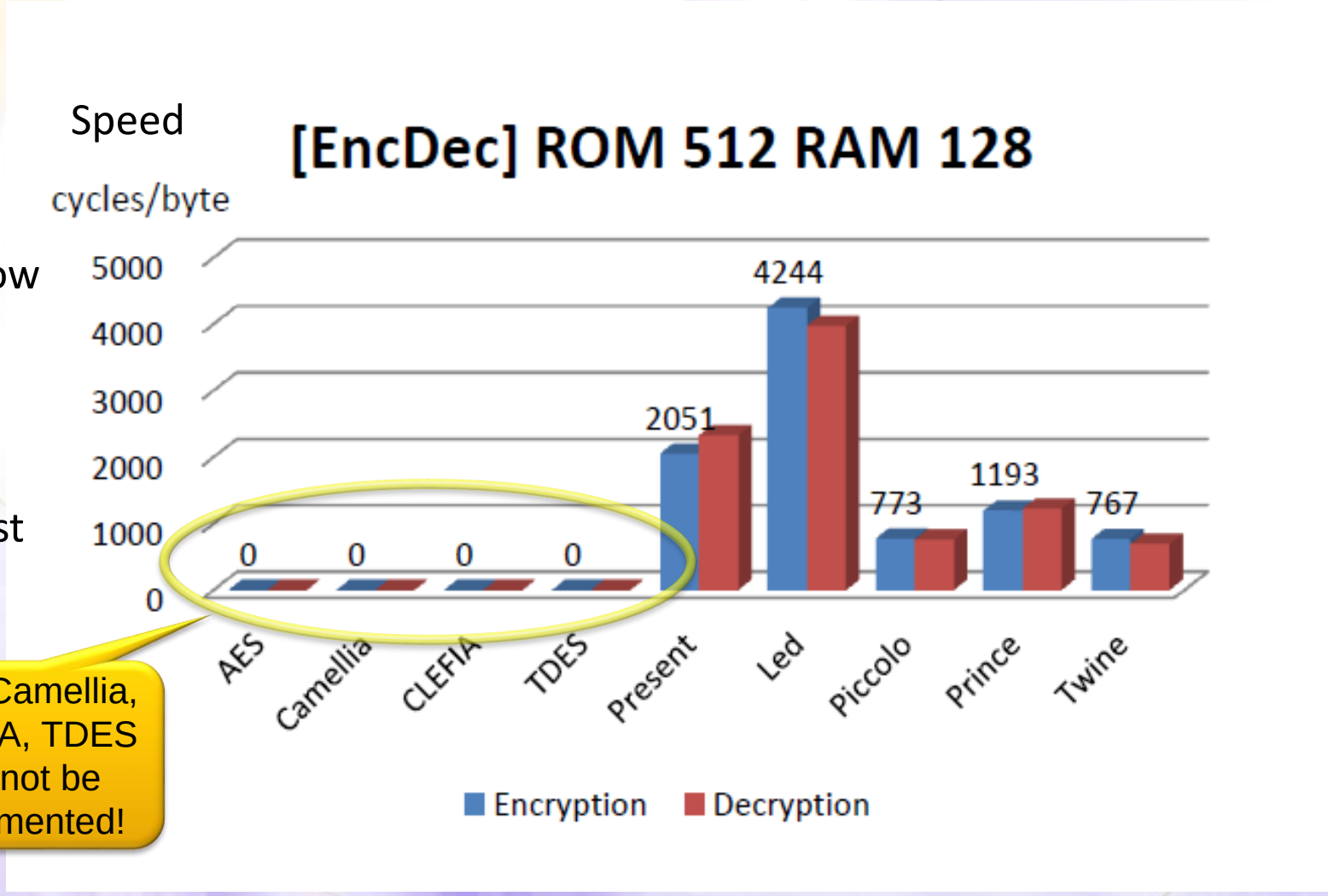
- Measures
  - Speed, RAM size, ROM size
  - Optimized for speed within 4 combinations of limited memory size (ROM, RAM).

ROM	512 Byte	1024 Byte
RAM	64 Byte	128 Byte

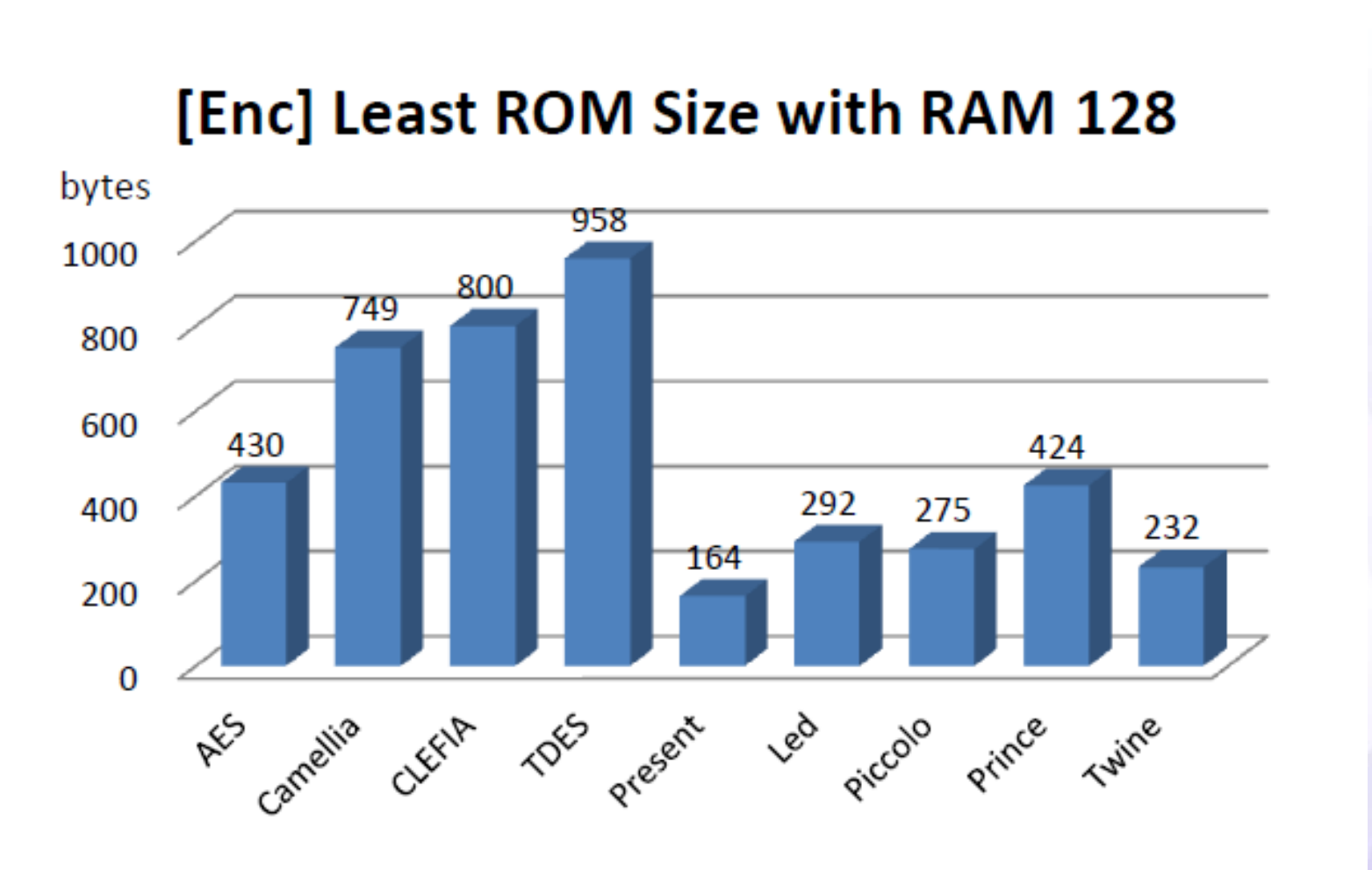
Implementation within (ROM 1024Byte, RAM 128Byte)



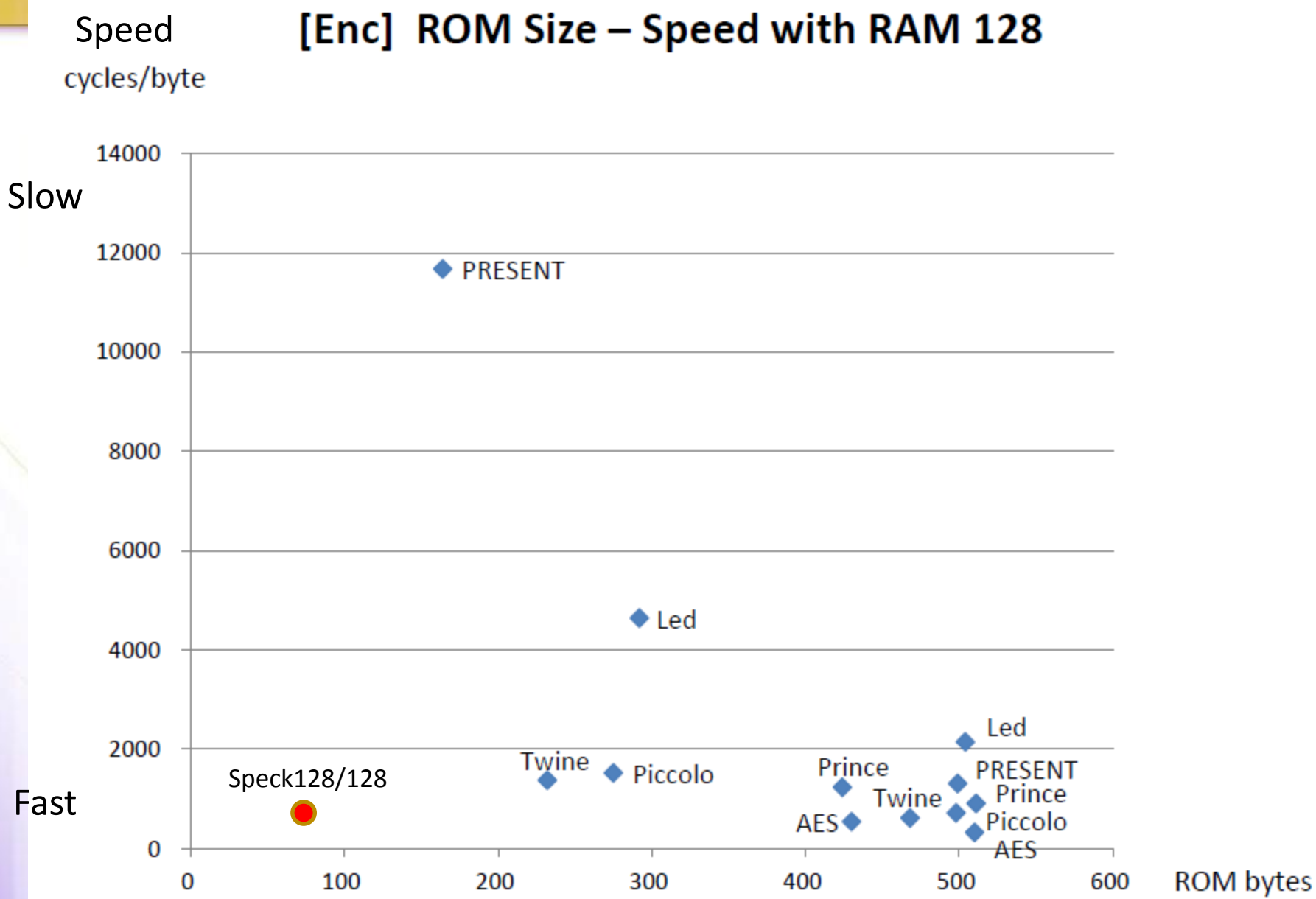
Implementation within (ROM 512Byte, RAM 128Byte)



Least ROM Size with RAM 128 byte



[Enc] ROM Size – Speed with RAM 128



Key Takeaways

- In emerging automotive/ITS services, protection of automotive sensor data is critical to system reliability and privacy concerns.
- Lightweight cryptography has great potentials for this purpose on resource-constrained devices.