17th International Forum on MPSoC for Software-defined Hardware

MPSoC 2017

Cipher IP for IoT Devices

July 6th, 2017

Fumio Arakawa, Makoto Ikeda
The University of Tokyo
Tsutomu Matsumoto
Yokohama National University

Outlines

- Motivations
- Project of cryptographic technology for IoT
  - Vision, R&D Plan & Targets
  - Background
  - Node and channel structure of secured IoT
  - Application example (Surveillance camera system)
  - Public key cryptography for IoT
  - Microcontroller system with Secure Cryptographic Unit (SCU)
  - R&D schedule and prospect of application
  - Project organization and members
- Initial results toward the less power and cost

Motivation

- Security is inevitable feature for all systems.
- However, small devices of IoT are not secured.
- Why?
- They are controlled by low-end processors/controllers
- They cannot support security features with SW.
- HW cipher IPs does not fit to the small devices.

- Cipher IPs with much less power and cost is necessary

- Research PJ for IoT systems with view of security
  - Theme: Cyber-Security for Critical Infrastructures
  - Sub-theme: Ultra low power cryptographic Implementation technology realizing IoT Security

Project of cryptographic technology for IoT

■ Vision

- Public key cryptography everywhere!

  by our Secure Cryptographic Unit (SCU)
- Enabling universal use of public key cryptography at end nodes and contributing to realize IoT security

■ R&D Plan & Targets

- R&D of SCU, "light, fast, strong" cryptographic module
  - Technology that flexibly realizes mutual authentication, data protection, etc., at the terminal node
- Demonstration of SCU usefulness by model system
  - Analysis of introduction to actual social systems
  - Building a model system (surveillance camera system)
- Advanced technology for stronger cryptographic module
  - Technology proposal against hardware Trojan

■ http://www.nedo.go.jp/content/100863674.pdf (in Japanese)

Background

Realizing potential threat to IoT

- IoT devices using Linux infect a large number of malware
  - Compliance with denial-of-service attacks over 600Gbps
  - This is observed by Honeypot for IoT (IoTPOT etc.)
- Increasing direct/indirect attack to terminal nodes of IoT

How we can realize security of IoT?

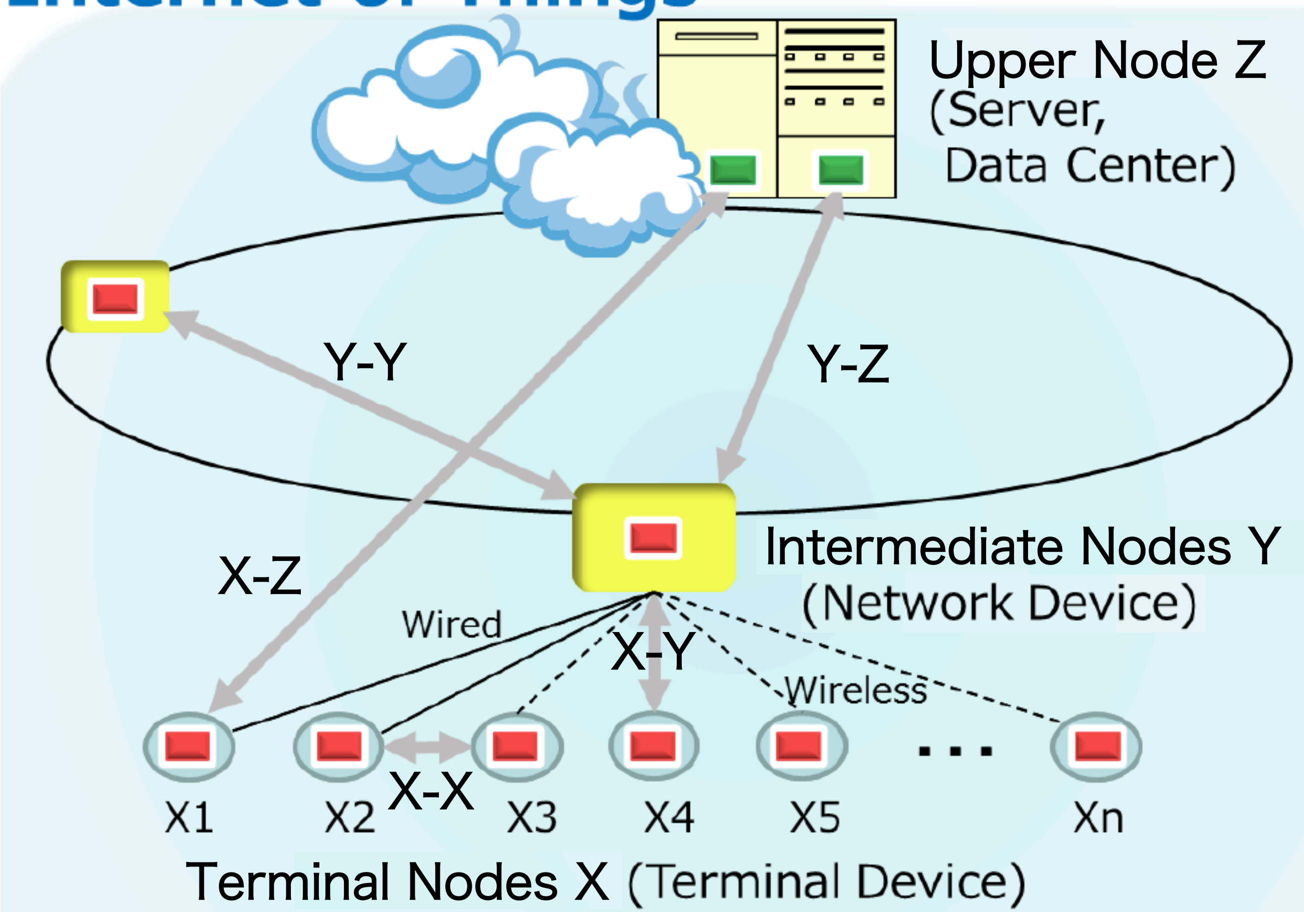
- TOP (Trusted Operational Platform for Cyber Security)
- Multilateral Approach

1. Multiple-level defense of total systems with unsecured nodes
2. **Make terminal nodes secured** (Our approach)
   - Utilizing public key cryptography
   - Limited resource, Severe environments, Long term supports
   - Exceeding limit of software implementation

Node and channel structure of secured IoT

- Nodes X and Y are protected and monitored.
- Channels X-X, Y-Y, X-Y, X-Z, Y-Z are protected.

Internet of Things

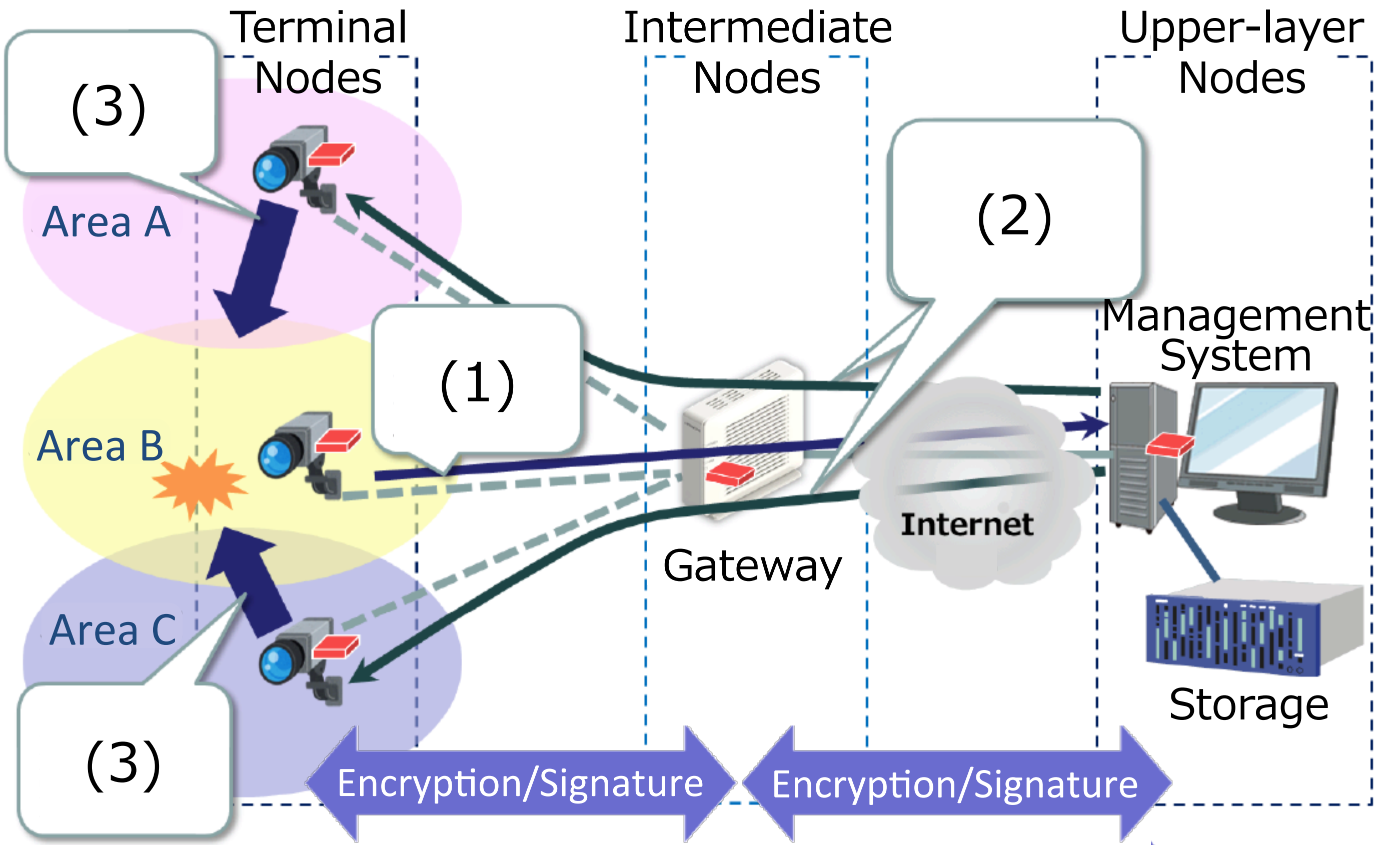


Various Terminal Devices
- Sensors/Actuators
- with/without
  - Controllers
  - OS
  - stable power source
- Wired/Wireless communications

Application example

◻ Surveillance camera system

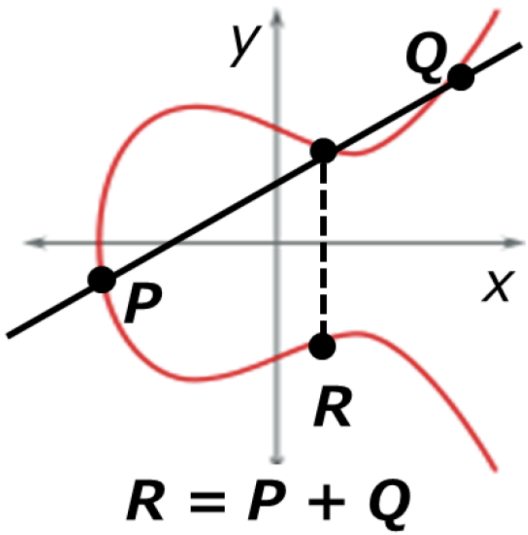
1) Camera in area B detects an abnormality or change, and reports it.
2) Management system controls the camera in areas A and C.
3) Camera faces to the area B to acquire detailed information.



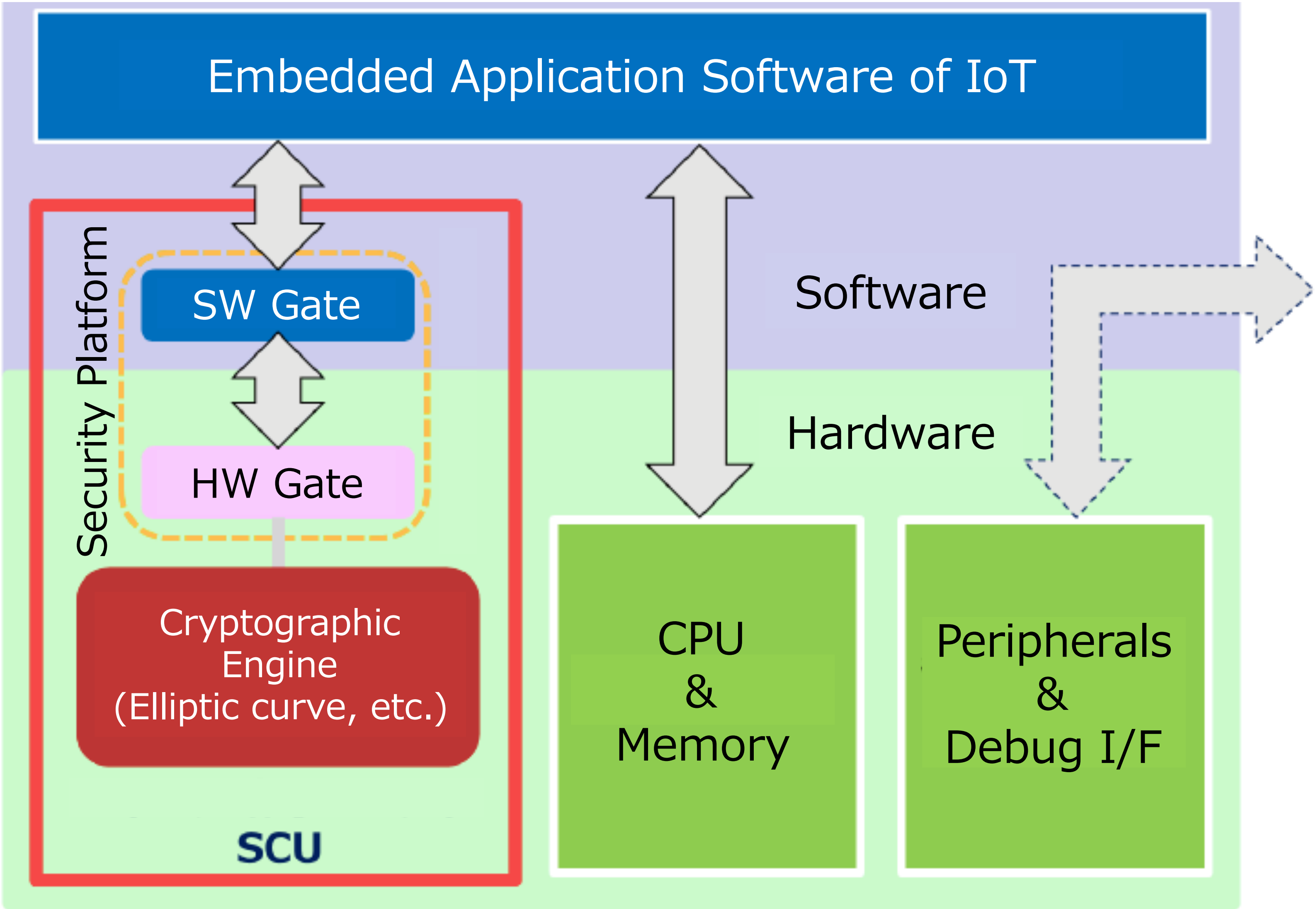
Public key cryptography for IoT

- Easier management than common key cryptography
  - Public (open) key for signature verification
  - Key management of a large number of terminal nodes
  - Significant contribution to support both of convenience and security on large-scale IoT systems
- Base of future advanced encryption technology
  - Enabling secret search, aggregate signature, etc.

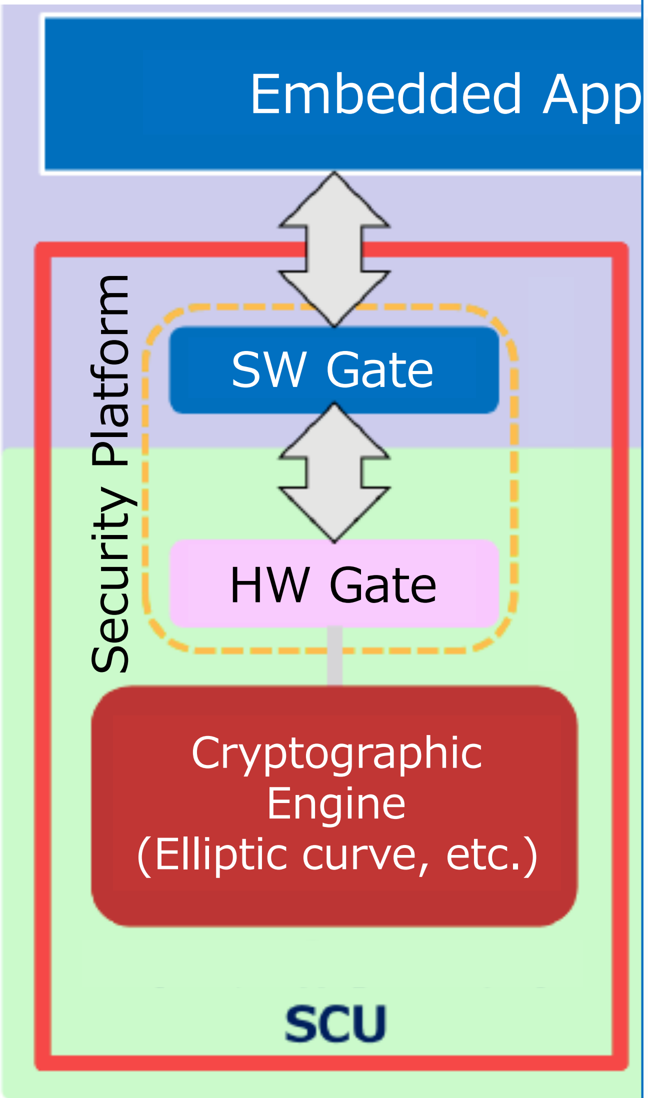
- Elliptic curve cryptography
  - For the same cryptographic class:
    - Shorter key length than RSA
    - Good for low power and low cost
  - Global standard is defined
    - Key sharing, signature, authentication, encryption, etc.



Microcontroller system with SCU



Secure Cryptographic Unit (SCU)



- **Hardware cryptographic engine**
  - Public key encryption
  - For terminal nodes
    - Ultra low power
    - Small & Low cost
  - For intermediate nodes
    - Ultra high speed
  - Common key encryption
- **Security platform**

  Even if an application is illegally altered or an illegal access to the cryptographic engine occurs, the security platform consisting of SW and HW gate functions reliably detects such attempts and blocks them.

Secure Cryptographic Unit (SCU)

Conforming limited conditions of IoT devices

- Low power for poor power resource of terminal nodes
- High speed to support various applications
- Generality for various elliptic curves
- Tamper resistance as a starting point of trust

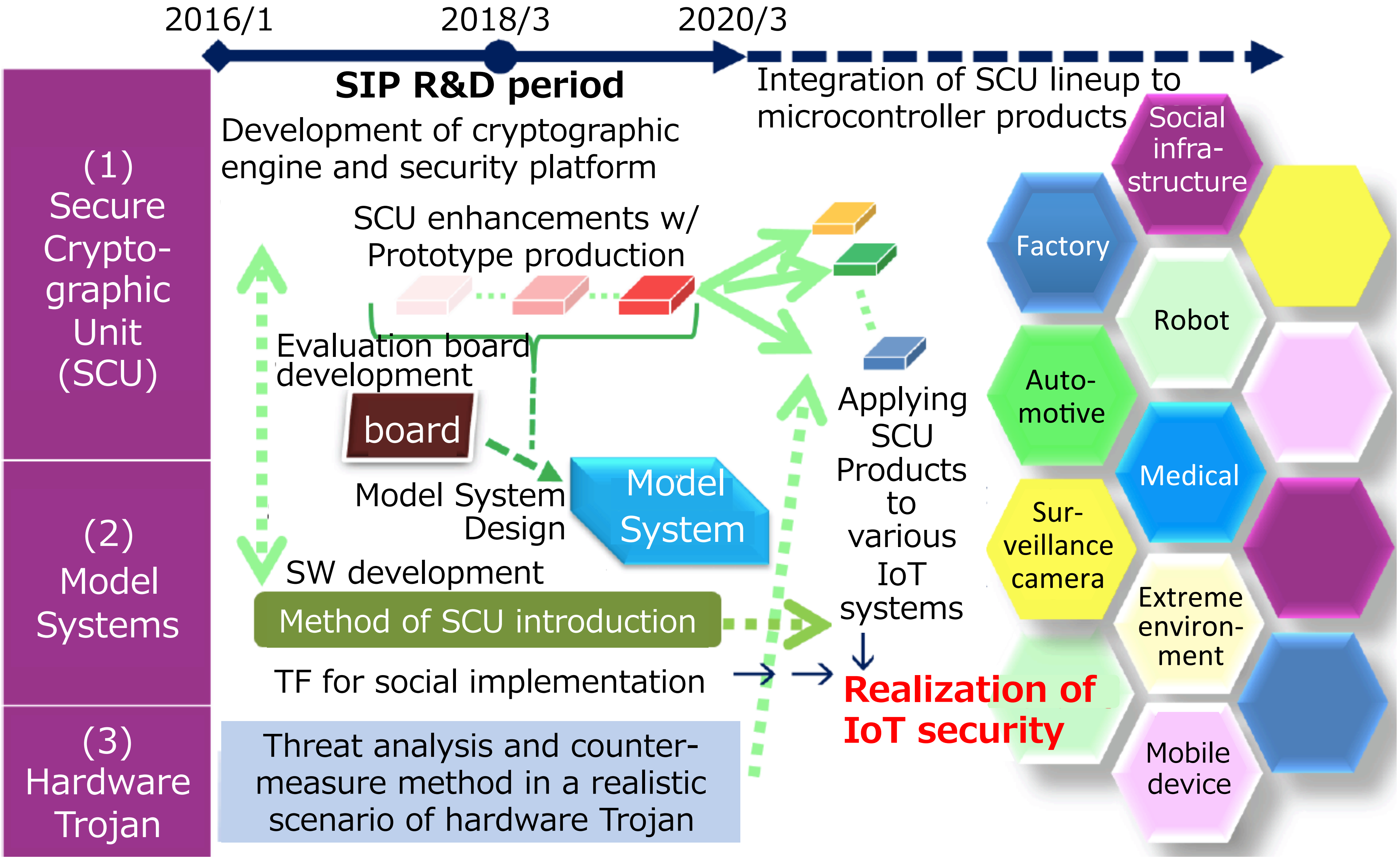
SW implementation on low-end microcontrollers

- Low power, but limited processing speed
- Limited memory shared with applications and cryptographic program
- Large overhead for tamper resistance

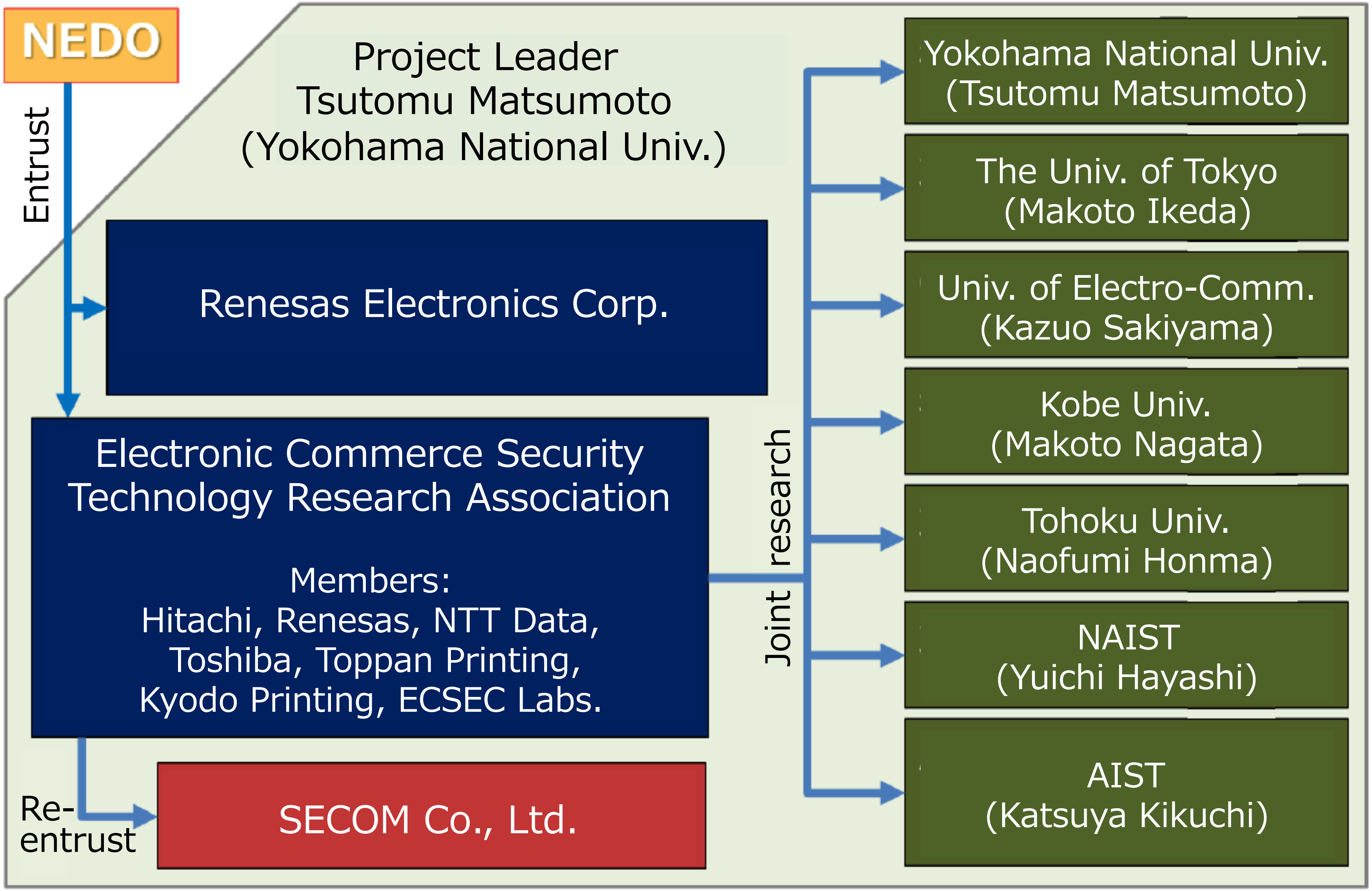
HW for overcoming limits of SW implementation

- Innovation by collaborating arithmetic architecture and semiconductor technology

R&D schedule and prospect of application



Project organization and members



Initial results toward the less power and cost

- Most of research of cryptography is for higher speed, higher functionality, and higher trustiness.
- So, there is not enough know-how to reduce cost and power.
- When we decrease arithmetic units for lower cost, control logic becomes dominant parts.
- Then, cost reduction becomes inefficient.
- We evaluated trade-off of cost and speed for various conditions.

Reference:

Ryosuke Saito, Makoto Ikea, "A Study of Area Efficient Implementation of Elliptic Curve Cryptography for IoT," SCIS 2017, Naha, Japan, Jan. 24 - 27, 2017 (In Japanese)

Initial results toward the less power and cost

- Trade-off of cost and speed for various conditions.
  - Parameters:
    - Jacobian/Affine coordinates
    - Montgomery/Fermat's little theorem (FLT) for Inverse calculations/Sharing Montgomery Multiplier for FLT
    - Radix: 1, 2, 4, 8, 16, 32, 128, and 256
  - Just for checking trade-off: Implementation is not optimized.
    - Laches are extensively used instead of memories.
  - The area reduction saturates around radix = 32 or 16.
  - Jacobian coordinate is good for speed,
    but not always good for cost.
- As a result, We can reduce parameter variations before intensive optimization.
    - Some idea is necessary for ultra low power, small & low cost.

Acknowledgement

- This work was supported by Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber-Security for Critical Infrastructure" (funding agency: NEDO).

Thank you