2-2 Implementation Technologies of Ultra-Low Power Public-Key Cryptography That Achieves IoT Security

Technologies for IoT

Public-key cryptography anywhere! Secure Cryptographic Unit

User Advantages of SCU and Policies for Widespread Use

Development technology	User advantages	Policies for widespread use
SCU	● Public key cryptography with tamper resistance can be incorporated into all terminal IoT devices. ● Scalable deployment is easily achieved: from terminal nodes through intermediate nodes to upper-level servers. ● Advantageous of small size, low power consumption, and high speed than the existing TPM products or other similar products.	● Conduct research on standard models and use cases to gain publicity and accelerate widespread use in the IoT market. ● Collaborate with advanced user companies to accumulate pioneering best practices. ● Roll out the application to various fields and uses. Improvement of guides. → Roll out of SCU model for use cases in a wide variety of fields.

Future View by Research Outcomes (Image)

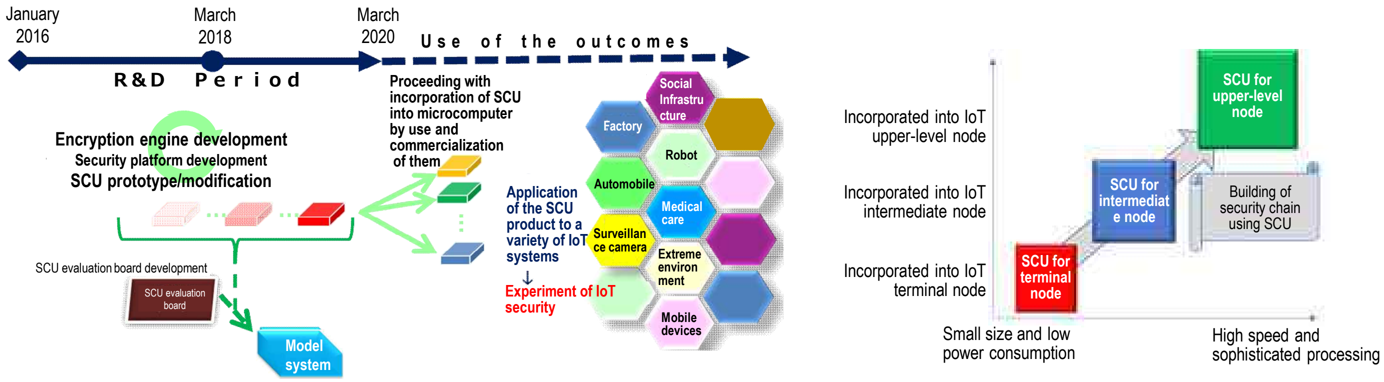


Image of Widespread Use of SCU (Spread of IoT by Use and Evolution by IoT Node)

Cross-ministerial Strategic Innovation Promotion Program (SIP) *ECSEC, Renesas Electronics*

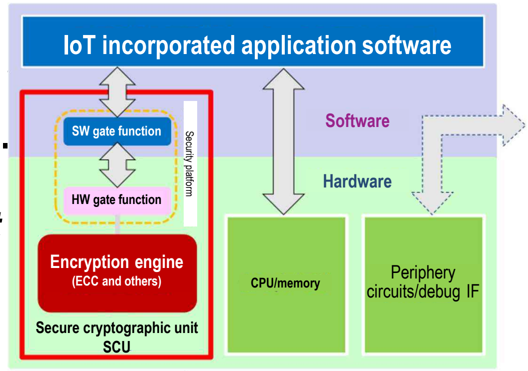
2-2 Implementation Technologies of Ultra-Low Power Public-Key Cryptography That Achieves IoT Security

Technologies for IoT

Public-key cryptography anywhere! Secure Cryptographic Unit

Secure Cryptographic Unit (SCU)

- **SCU is the light, fast, and robust module to be embedded into an IC chip that protects IoT devices from cyberattacks.**
- **SCU consists of an encryption engine and security platform. All the linked devices are made to have *the latest public-key cryptography function* incorporated, achieving the security of IoT.**



Features of Secure Cryptographic Unit (SCU)

SCU uses the state-of-the-art cryptographic and security technologies to provide scalable protection for terminal, intermediate, and upper-level nodes making up an IoT system.

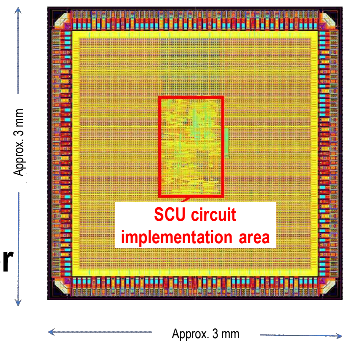
1. **A small, ultra-low power state-of-the-art public-key cryptography engine is incorporated for IoT terminal nodes.**
2. **Possible to secure tamper resistance and build life cycle management, which is considered as Root of Trust.**
3. **Scalable deployment is possible from low-end MCU (Micro Controller Unit) to high performance SOC (System On Chip).**

Key 1: SCU prototype chip KM10 series

This research produces a prototype chip and develop a model system that simulates application of SCU in an actual IoT system.

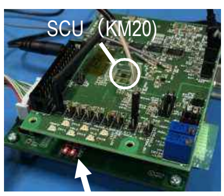
Main Specifications of SCU KM10 Series

- **Encryption engine: ECC (elliptic curve cryptography; 256-bit prime field), AES, SHA-256, ChaCha20-Poly1305, physical random number generator**
- **Security control: HW gate, SW gate**

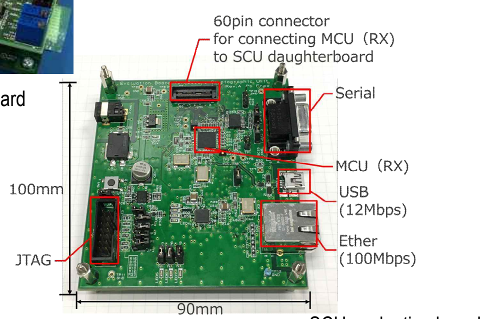


Key 2: SCU evaluation board

The SCU evaluation board, which is a development tool provided for development of IoT devices with SCU to be incorporated and application systems, can use the security platform of SCU to develop and evaluate applications.



SCU evaluation board (bottom)



SCU evaluation board

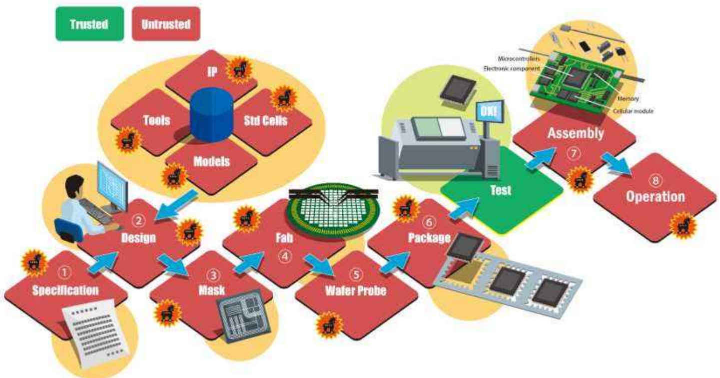
Cross-ministerial Strategic Innovation Promotion Program (SIP) *ECSEC, Renesas Electronics*

2-2 Implementation Technologies of Ultra-Low Power Public-Key Cryptography That Achieves IoT Security

Technologies for IoT

Development of Countermeasures Technologies against Hardware Trojans

Threats of hardware Trojans (HT)



In an unreliable supply chain, intentional electrical modifications are made to IC chips, substrates, connection lines, and other parts.

Emergence of HT whose implementation is inexpensive causes threats to expand to consumer products.

Attack Timing/Assumed Attacks/Assumptions/Cost

	Attack timing	Assumed attack	Assumptions of attacks	Cost of attacks	Attackers
Design and manufacturing processes of system LSI	(i) Requirement specifications	Malicious products provided by vendors			
	(ii) System LSI design	Design by malicious designers	Interventions to supply chains/Attacks through physical access to IC	High cost	Bespoke Professional
	(iii) Mask manufacturing	Falsification/replacement of masks during manufacturing			
	(iv) Chip manufacturing	Falsification of design by interventions of subcontracting vendors			
	(v) Chip verification	Falsification of wiring/circuits by subcontracting vendors			
	(vi) Package				
Manufacturing process of incorporated equipment	(vii) Incorporation into the control part	Incorporation of electronic components	Attack through physical access to equipment	Significantly lower cost than "High cost"	Bespoke Professional, Hobbyist
	(vii) Assembly of equipment				
After shipping	(viii) Operation of equipment	Incorporation of electronic components/writing of malware/incorporation of devices		Lower cost than the above	

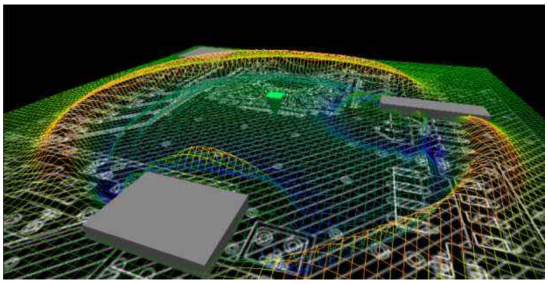
Issue 1: Building of a mechanism to prevent the control components of microcomputers and others from being infected with hardware Trojans (detection of Trojans during design and manufacturing processes, prevention of running)

Issue 2: Building of a mechanism to use safe control components to prevent hardware Trojan from being imported on the assumption that no hardware Trojan exists in the control components of microcomputer and others (detection of Trojans during design and manufacturing processes, prevention of running)

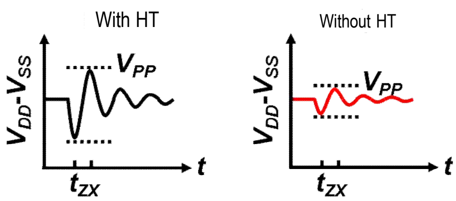
Solution technology for Issue 2 is presented

Issue 3: Consideration on how to take actions if a Trojan runs in the life cycle

Development of Technologies to Detect HT Inserted in an IC and Its Peripherals

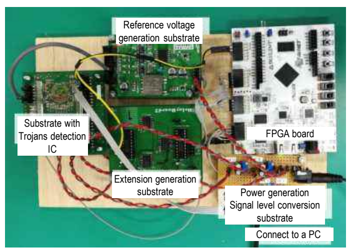


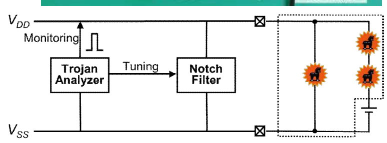
Sensing of surrounding IC and electrical element from an IC whose authenticity is guaranteed



Detection of the existence of HT from the circuit response using impulses emitted from the sensor.

HT detection test environment





Technologies for IoT

Cross-ministerial Strategic Innovation Promotion Program (SIP)

ECSEC, Renesas Electronics

2-2 Implementation Technologies of Ultra-Low Power Public-Key Cryptography That Achieves IoT Security – R&D Perspective –

Security Platform Technologies

Renesas Electronics

Achieved the development of design specifications and production of a design prototype of the SW gate/HW gate of the Secure cryptographic unit (SCU) and external secure access control to the SCU encryption engine.

Digital Circuit Design/Cryptography Implementation

Yokohama National Univ., Univ. of Tokyo, ECSEC

Achieved the light weight and fast public-key encryption engine through the development of design specifications, digital circuit design, and prototype production of the encryption engine of the Secure cryptographic unit (SCU) and ultra-efficient hardware implementation of elliptic curve cryptography (ECDSA).

Analog Circuit Design/Structure

Kobe Univ., AIST, ECSEC

Achieved the enhancement of both the performance and security of the system LSI through new development of analog implementation, 2.5 dimensional implementation, and other technologies for the entire system LSI with the Secure cryptographic unit.

Tamper Resistance Technology

Tohoku Univ., Yokohama National Univ., Kobe Univ., NAIST, ECSEC

Development, implementation, and evaluation of the technology that secures the tamper resistant of the Secure cryptographic unit (SCU). Achieved the robust public-key encryption engine.

Countermeasure Technology Against HW Trojans

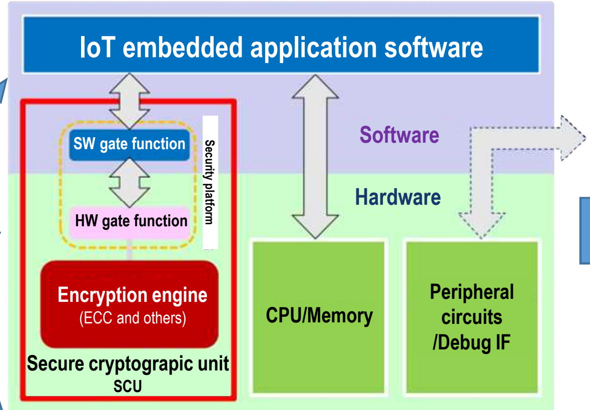
Univ. of Electro - Communications, NAIST, Kobe Univ., Yokohama National Univ., ECSEC

Sorting out of the cases of HW Trojan attack to embedded equipment, analysis of attack technologies in each product layer, and development of countermeasure technologies by focusing on HW Trojans.

Realization of the R&D Results as the Secure cryptographic unit (SCU)

The results of collaborative research by the research institutions are aggregated to the Secure cryptographic unit (SCU) mounted on the system LSI chip.
The SCU part is aimed to be supplied as the design IP of the system LSI to chip vendors. (Analog structure, anti-tampering technology, and countermeasure technologies against HW Trojans can be applied to other fields besides SCU.)

Example of a micro controller with built-in Secure cryptographic unit (SCU)

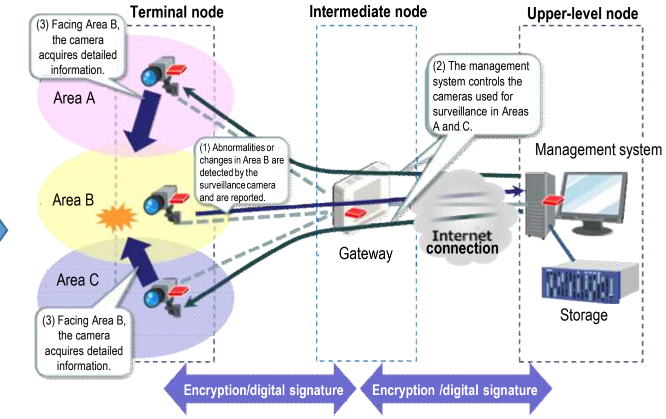


Building of Surveillance Camera System as a Model System

ECSEC

Built a surveillance camera system and verified it as one of verification examples of application of a system LSI chip with Secure cryptographic unit (SCU) to an IoT system. Note that the application range of SCU is wide: IoT in general that includes industrial equipment control, transportation/medical equipment, and robot.

Secure cryptograpic unit Application example: Surveillance camera system



For Social Implementation

Introduction Analysis ***SECOM***

For automobiles, medical equipment, and other systems each of which consists of parts and modules provided by multi-vendors and is likely to be interconnected with other systems and in the field where important assets that include including human lives are critically influenced, multiple models of feasible application and systems are proposed while considering the possibility of use with social application in a variety of cases.

Intellectual Property Strategy and Others ***ECSEC***

For handling of the research and development results as integrated intellectual property even after SIP is finished, one of the project participants, the Electronic Commerce Security Technology Research Association, is converted into a company that, as the business successor, will promote the intellectual operation and spread of SCU. Even during the research and development period, there has been inquiries about the use of intermediate outcomes from IoT users. The use of SCU is expected to be used as the core technology for security enhancement of IoT systems in a variety of IoT fields, such as industrial equipment control, transportation/medical equipment, and robot.

Practical use

R&D Schedule and Perspective of Practical Use