IDEC Chip Design Contest

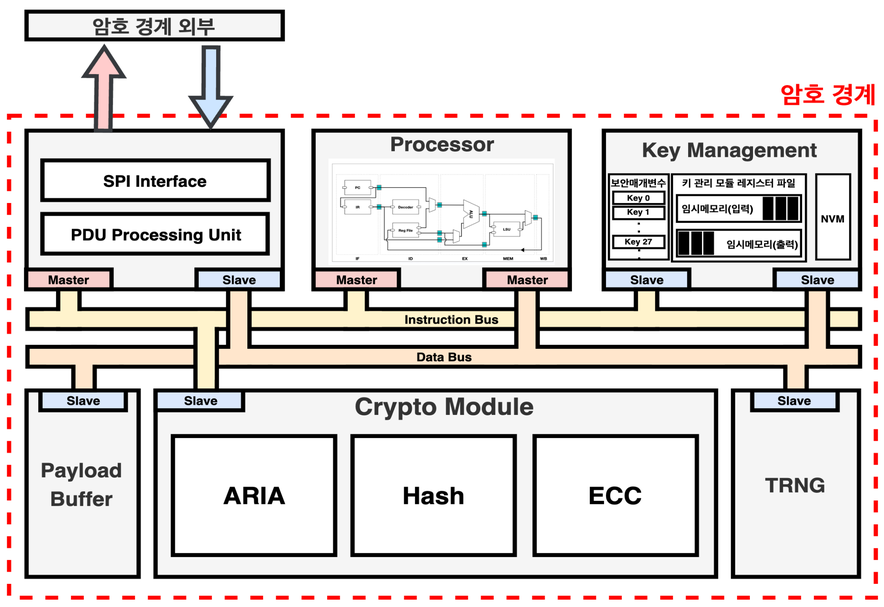
KCMVP-compliant security chip, for key management and TLS support in IOT environments

Dongwook Yun, Byeonguk Jeong, Eunse Kang, Howon Kim
Department of Computer Engineering, Pusan National University
Email : dongwook@islab.re.kr, byeonguk@islab.re.kr, eunse@islab.re.kr, howonkim@pusan.ac.kr

Abstract

The Fourth Industrial Revolution has driven IoT development and its integration into various embedded systems, raising significant security issues. Thus, providing data security (confidentiality, integrity, availability, etc.) is essential. This study proposes a low-power/high-performance security chip for IoT environments to address key management and communication security issues. The design complies with KCMVP(Korea Cryptographic Module Validation Program), requirements, ensuring stability and implementation suitability.

Security Chip



< System Overview>

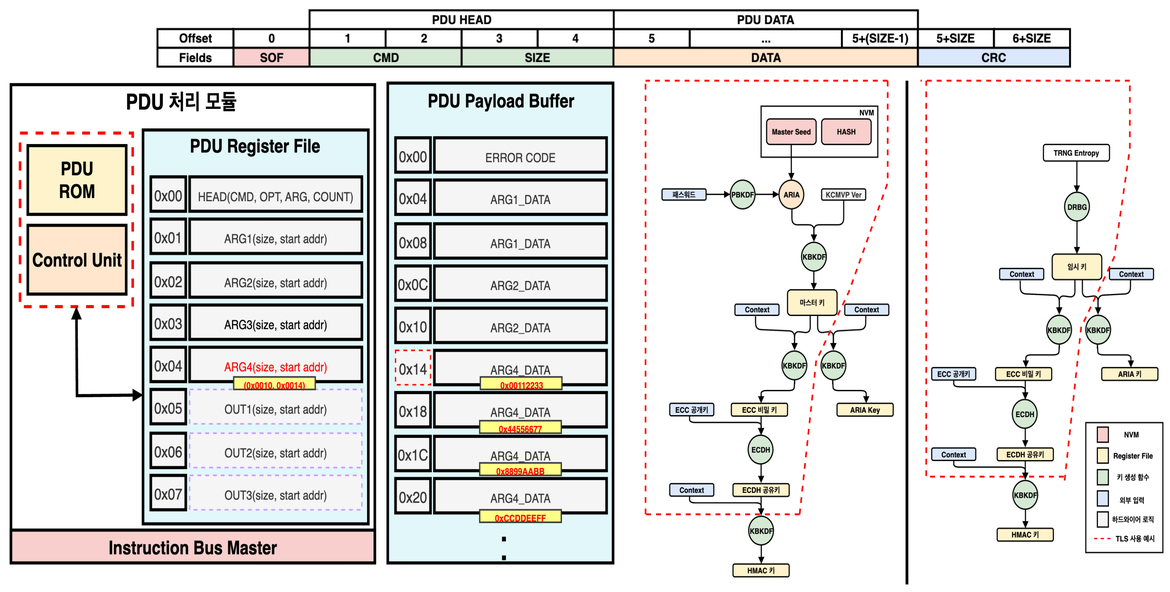
To solve the core security issues of the IoT environment, it consists of eight cryptographic algorithms (ARIA, ECDH, ECDSA, SHA-256, HMAC, DRBG, KBKDF, PBKDF) for TLS support, a key enclave for secure key management, and a hardware random number generator, with a processor for controlling each function and a ROM with firmware. The internal processor also supports special instruction extensions and a 16-bit compressed instruction set suitable for control of cryptographic modules, which is suitable for embedded systems with limited hardware resources.

Chip verification

< Open Chip Platform Test Board & Test Result >

In order to verify the chip with proposed design, we used Open Chip Platform Test Board. Through the SPI interface, it was confirmed in PDU format that the chip's memory read/write functions and the normal operation of ARIA-GCM mode were intact, and that ECDH and ECDSA keys necessary for TLS communication were correctly generated. Therefore, this chip supports secure key management and transport layer security (TLS) that comply with the security requirements of KCMVP, and it is expected to address security vulnerabilities when applied to IoT systems.

PDU Processing Unit & Key Management

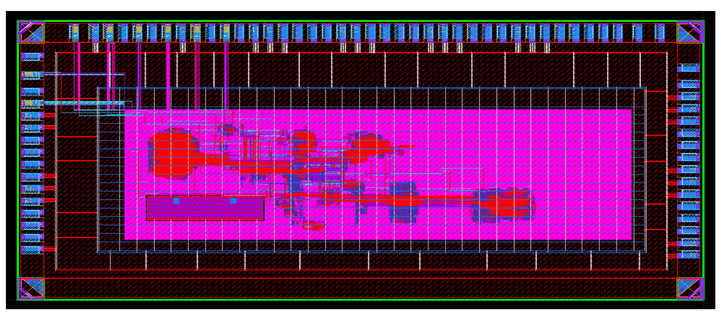


< PDU Format & PDU Pre-processing > **< Key management layer & TLS usage example >**

All commands for functions within the cryptographic boundary follow the PDU format. External commands and data are input into the PDU processing module and PDU payload buffer by distinguishing reference addresses from actual data to minimize memory copying. The PDU processing module delivers commands to each cryptographic core, and the upper module processes them by copying only the necessary data to the local register.

Keys are divided into master keys from NVM-stored seeds and temporary keys from DRBG. These keys are stored in a register file during cryptographic operations. NVM and the register file are isolated from external access via the external bus, and keys are zeroized in temporary memory after use for security. The diagram shows a TLS example: ECDSA keys from the master key are used for signing and verification, while ECDH keys from the temporary key are used for session establishment.

Chip Implemetation



< Chip layout & photograph>

Chip Specification	
Technology	Samsung 28nm
Core volatge	1.0V
I/O voltage	1.8V
Chip Size	4mm x 2mm
Clock Frequency	100MHz
Circuit Type	Digital
Designed Field	System Security

The chip fabrication and EDA tool were supported by the IC Design Education Center(IDEC), Korea.

반도체설계교육센터 IC DESIGN EDUCATION CENTER