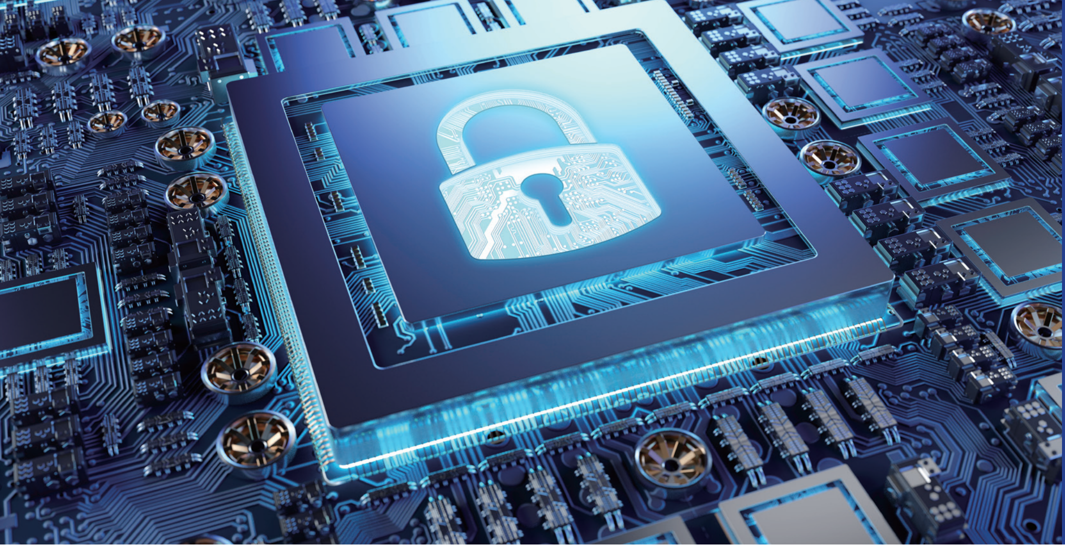

IoT Security chipset for connected world

RS1211
RS2332

RANiX's security chipset family provides hardware-based crypto-accelerators and secure key storage, plus anti-tampering and side channel attack protections . It easily embed trust and safety in IoT environment and devices. It fortifies the security function to various edge devices at much lower cost. This chip eliminates security vulnerability in the open connected world, enabling a safer and more trustworthy life at another higher level.

IoT Sensor Devices

To prevent data hijacking of illegal devices, legitimate devices are authenticated, and sensor control information and sensing data can be encrypted to transmit and receive data flawlessly. It also enables operation with low power of various sensors.

Secure Storage for Key and certificate

You can securely store the keys by encrypting and digesting the keys needed to encrypt and decrypt data. The secure storage guarantees the integrity of key data at all times by automatically checking changes in important key data from attackers. When the key is changed, an error is generated and the security of the encryption module is maintained.

Supported Link Protection

Our security chipset supports DTLS and TLS, which are standard protocol supporting secure end-to-end data protection. In addition, Our security chipset supports rich API for easy application and also it provides sample example codes as references.

High-Speed HW Crypto Engine

The Symmetric key algorithms AES and ARIA consist of HW engine supporting high-speed performance. In addition, HW Engine supports hash SHA256 for fast operation. It also has built-in accelerators for fast computation of asymmetric encryption RSA and ECC algorithms. There is H/W entropy for random number generation essential for key generation, so you can generate more secure and standard random numbers.

Power Analysis/ Abnormal Attack Detection

Our chipset detects attacks using Voltage, Glitch, Light, Temperature, and Clock, and zeroes important information after attack detection. In addition, it is possible to prepare for physical attacks by applying the technology to prevent SPA/DPA attacks, which are power analysis methods, and Active Shield technology.

Certification

RS1211 product was certified KS X ISO/IEC 19790 level 1 as a hardware type and RS2332 product was also certified KS X ISO/IEC 19790 level 2 as a hardware type.

IoT Security Chipset for connected world

RS1211/ RS2332

SPECIFICATIONS & FEATURES

RS1211

Crypto

- Symmetric Crypto Engines ARIA (128bit), LEA (128bit), AES (128bit)
  - CBC, GCM, CCM mode
- HYBRID Random Number Generator
  - CTR-DRBG With TRNG
- Monotonic Counter (up to 1,048,575) 4byte X 2ea

Security Function

- Countermeasure against Power Analysis Attack
  - SPA/DPA
- Device Authentication & data encryption protocol supports

Package

- Package Type: 8Pin DFN

Certified

- KCMVP Level 1
- OSCCA (preparation)

RS2332

Crypto

- Symmetric Alg. ARIA (128,192,256bit) - ECB, CBC, CTR, GCM
- Asymmetric Alg. ECDSA(256bits), ECDH,RSA(2048 bits)
- Hash Engines SHA256,HMAC-SHA256
- HYBRID Random Number Generator CTR-DRBG With TRNG

Security Function

- Countermeasures against Power Analysis Attack
  - SPA/DPA/CPA
- Abnormal Attack Detection Sensors
  - Voltage, Glitch(Power,Clock), Light, Temperature

Package

- Package Type: 24Pin QFN
- 4mm * 4mm * 0.75mm

Certified

- KCMVP Level 2
- OSCCA (preparation)

KCMVP: Korea Cryptographic Module. Validation Program
OSCCA: Office of the State Commercial Cryptography Administration

Group	Function	RS1211	RS2332
CPU Core	secure	-	ANDES S801-S 32-Bit Secure Core (64MHz)
Memory	RAM	2K Bits	32KByte
	ROM	8K bits	256KByte
Peripheral	Timer	-	32bit(8Ch), WDT,RTC
	Interface	Async I2C Slave	I2C, SPI : Master/Slave(2Ch) (Multi-function), UART: 2Ch (Multi-function), GPIO:Up to 32 (Multi-function), ISO7816
Crypto Alg	Symmetric	AES(~128),LEA(~128),ARIA(~128)	AES(~256),ARIA(~256)
	Asymmetric	-	RSA(~2048),ECC(~256)
	Hash	-	SHA(~512),HMAC-SHA256
	RNG	CTR-DRBG	CTR-DRBG
Power Consumption	Sleep Mode	VDD=3.6,Max < 0.01uA	Typ < 0.3mA
	Standby Current	Max < 70uA	Typ < 5mA
	Operation Mode	VDD=3.6,Max < 5mA	Typ < 12mA
certificate	KCMVP	Level 1	Level 2

@ All rights reserved by RANIX

KOREA : RANIX.Inc
RANIX Bldg, 25 Eonju-ro 135 -gil, Gangnam-gu, Seoul, Korea

CHINA : RANIX Smart Technology(Shanghai) Co.,Ltd.
11th Floor, Building No 10. Lane 2777, Jinxiu East Road,
Pudong New Area, Shanghai, China

Contact