



A Robust Core of Security Functions

Neo PUF

NeoPUF is eMemory's proprietary security IP based on Physical Unclonable Functions -- unique physical properties inherent from IC manufacturing variations. Based on an innovative PUF device utilizing competing trap assisted quantum tunneling scheme, NeoPUF provides a truly random number, just like tossing a coin with 50%-50% heads and tails probability. With its inborn, unpredictable and truly random features, NeoPUF can provide a hardware based fingerprint for individual ICs.



Inborn Secret

Inborn, unpredictable and ideal - true entropy



Reliable & Robust

Stable CRPs (Challenge/Response Pairs) up to 175°C and no aging decay



Secure Storage

Combined NeoFuse OTP and NeoPUF RNS provides high security storage



Fast Time to Market

Many qualified platforms are ready for IoT security applications

Highlights

- Stable Challenge-Response-Pairs without helper data
- Large entropy pool for flexible bitstream length and multi keys
- Passes NIST 800-22 / AIS-31



True Root of Trust

Key management combined with secure storage opens many security application scenarios

Key Functions for Security Applications



Hardware Root of Trust



Unique IDs or Keys Generation from NeoPUF



Secure Boot and Firmware Protection

PUF-based Solutions

PUF-based Solutions

Solutions embedded with NeoPUF IP can generate inherent and unique random numbers which can be used as UID, root key or nonce for security functions such as root of trust, key management, authentication and encryption.



PUFiot

PUFiot is a novel high-security crypto co-processor providing the functions of root of trust (PUFrt), key generation, block cipher, integrity check, identity verification and more.



PUFrt

PUFrt is a 5-in-1 HRoT solution composed of PUFsecurity's PUF-based products including PRTC (APB I/F), PUFuid, PUFtrng, PUFkeyst, and comprehensive anti-tamper designs.



Other PUF-based Solutions

PUF-based security function IP blocks include PUFuid, PUFtrng, PUFkeyst and crypto IPs such as AES, ECC and SHA.