ememory
Embedded Wisely, Embedded Widely

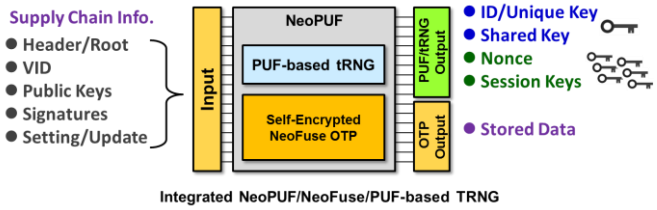
NeoPUF® – Silicon-based Hardware Root of Trust

Unique Fingerprint of Individual ICs

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 oxide rupture as an enrollment scheme, NeoPUF provides a truly random 1s and 0s bitstream, just like flipping an ideal coin with 50%-50% heads and tails probability. With its inborn, unpredictable and truly random features, NeoPUF can provide a silicon based fingerprint for individual ICs.

Applications

With its unique, inherent IC fingerprint, NeoPUF can be combined with other functions such as TRNG, Encrypt/Decrypt Engine, HASH or secure CPU to execute comprehensive silicon-based hardware root of trust. It can achieve anti-counterfeiting, chip authentication, secure boot, communication encryption. Supply chain security could benefit from a NeoPUF-based hardware root of trust.

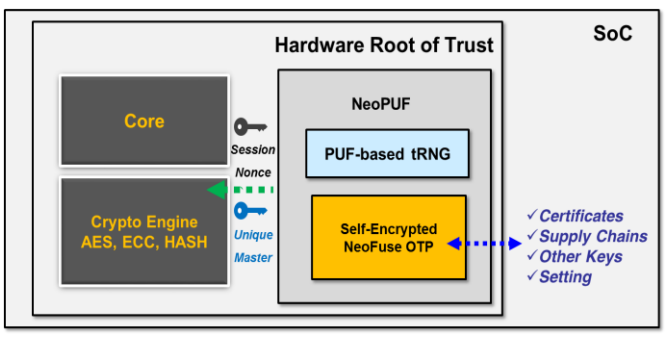


Integrated NeoPUF/NeoFuse/PUF-based TRNG

- ❖ Identification: Hardware ID tracking by OEMs
- ❖ Authentication: End-to-end authentication
- ❖ Encryption: Secure data integrity
- ❖ Secure key generation: Secure communication

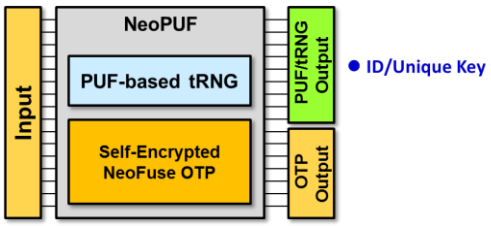
Hardware Root of Trust

NeoPUF can be executed as a hardware root of trust when combined with secure CPU and crypto engine functions.



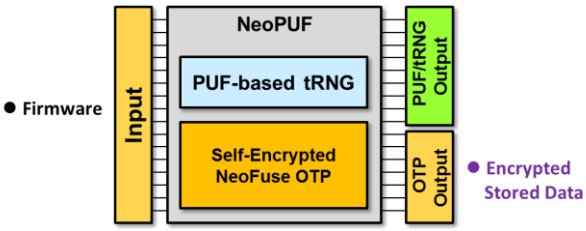
Unique IDs or Keys Generation from NeoPUF

NeoPUF can provide a unique ID for chip register, authentication or supply chain control.



Secure Boot and Firmware Protection

NeoPUF can provide a way for each chip to self-encrypt the NeoFuse OTP to protect valuable firmware or to execute secure boot function.



Performance

NeoPUF technology offers consistent performance, independent across different foundries and platforms, as well as being able to be easily adopted into 12" generic and derivative processes. Compared with conventional PUF solutions, NeoPUF's outstanding stability, true randomness, unpredictability, and ease to bring to production are unmatched. NeoPUF is ready for IoT, AI, FPGA, and automotive markets.

Features and Benefits

- ❖ Stable Challenge-Response-Pairs without helper data
- ❖ Inborn, unpredictable and truly random entropy
- ❖ Robust performance from -40°C to +175°C
- ❖ Large entropy pool for flexible bitstream length and multi keys
- ❖ High reliability without aging decay
- ❖ Passes NIST 800-22 / AIS-31

Metrics	Check by	NeoPUF	Ideal
Randomness	Hamming Weight (HW)	50%	50%
Uniqueness	Hamming Distance (HD)	50%	50%
Stability	Bit-Error-Rate (BER)	0	0
Repeatability	Intra-ID HD	0	0
Identifiability	Inter-ID/Intra-ID HD	∞	∞
Productivity	Yield and Reliability	Qualified	Qualified