Secure the connected world

www.pufsecurity.com

ABOUT US

WHO ARE WE ?

PUFsecurity is a subsidary of eMemory, focusing on PUF-based hardware security IP solutions.

PUFsecurity uses eMemory's industry-leading technology to develop customized PUF-based hardware security IPs that provide better performance and cost-efficiency to the market. We use core **NeoPUF®** and **NeoFuse®** IP to develop extended hardware security functions and solutions in an easy and cost-effective way.

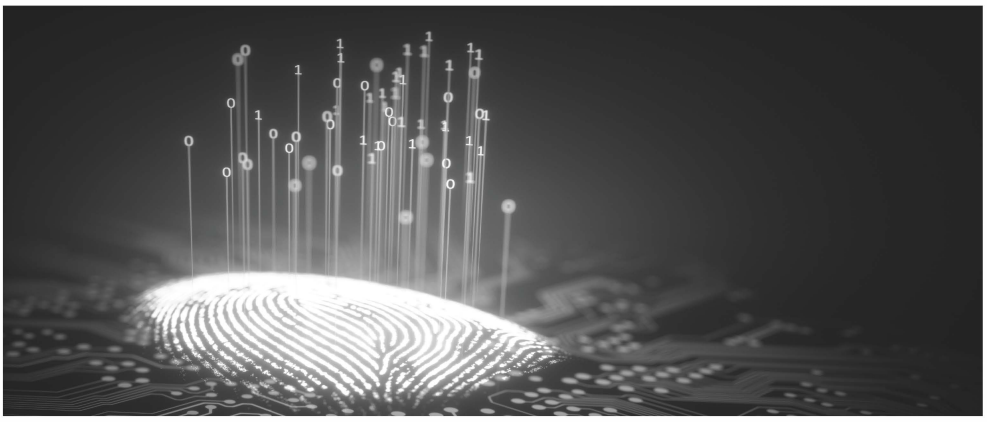
PUFrt

PUFrt Secure Macro with Secure OTP, UIDs and tRNG

PUFrt® (Root-of-Trust) is a PUF-based (Physical-Unclonable-Function) secure macro providing primitive functions of robust secret, trusted secure storage on chip by means of an endless supply of true random bits. Inside the macro, NeoPUF® provides unique identity (UID) up to 1Kb. NeoFuse® offers secure one-time-programmable (OTP) storage of 4Kb. PUFtrng serves as a true random number generator. Below we are going to introduce NeoFuse®, PUFuid, PUFtrng, PUFkeyst separately.

NeoPUF® is a weak PUF with limited CRPs (challenge-response-pairs) for generating true random bits, which can act as a silicon fingerprint. NeoPUF has the near ideal PUF characteristics of 50% HW (Hamming-Weight), 50% Inter-HD (Hamming-Distance), 0% Intra-ID HD and 0ppm BER (Bit-Error-Rate). NeoPUF and PUFtrng have passed the U.S. National Institute of Standards and Technology (NIST) SP800-22 and NIST SP800-90B IID statistical analyses.

NeoFuse® is an antifuse-based OTP technology with an internal charge pump design. By using PUF-based techniques of data masking and physical address scrambling (PUFkeyst), NeoFuse is well suited for secure code storage.



PUFuid

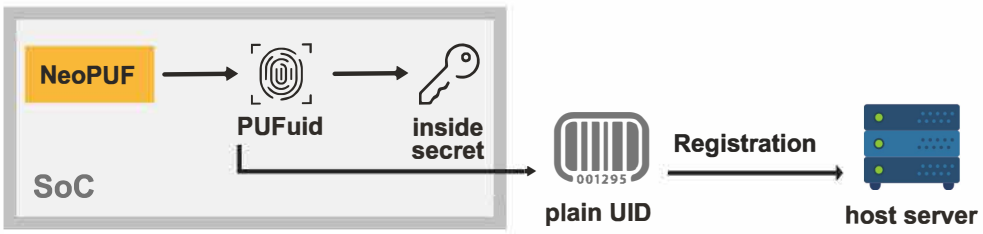
Generating chip secrets with inborn root-of-trust

Unique identity (UID) is an identifier that is generally stored on each chip. With this UID, chips can generate an internal secret for key generation or an external plaintext number for chip identification. The normal process of generating a UID is called key injection. To keep the secret UID safe, an expensive security facility and astrict set of operating procedures for key injection are required.

Unlike key injection, PUFuid extracts an embedded NeoPUF value as the chip's unique identity. NeoPUF's value varies from chip to chip due to native variations that arise during the manufacturing process. NeoPUF is impossible to clone or predict. Therefore, it can be viewed as the chip's fingerprint. PUFuid provides each chip with its own unique secret to protect selected data. It also provides a plaintext number UID for authentication. As a result, communications between a server and a given chip will be distinct from other chip/server interactions.

KEY FEATURES

1. Ideal randomness with 50% Hamming weight and Hamming distance.
2. On-demand keys for on-chip secret and off-chip ID generation.
3. Reliability of lifetime zero bit-error-rate (BER) and robustness of working under different circumstances (Temp: -40~175℃)
4. Compatibility with a wide range of CMOS processes.



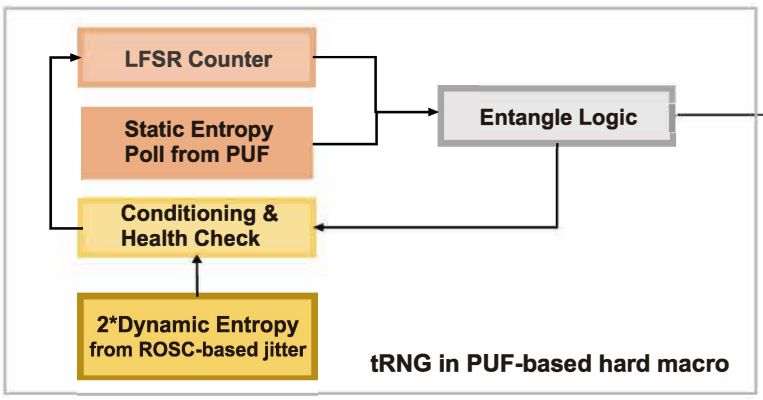
PUFtrng

True randomness with low power consumption and high-speed throughput

A conventional TRNG requires four high quality entropy sources and post processing algorithms to generate true random bits. When designing a high-quality entropy sources, many factors should be considered. Moreover, in order to enhance the resistance to varying environmental conditions, output should be modified by an approved post-processing method.In contrast, PUFtrng uses an entropy-assisted design to achieve a qualified TRNG. NeoPUF is a fixed random number pool with an ideal Hamming weight of 0.5, which is used as the multiplier for output randomness. NeoPUF is the key contributor to enhancing entropy engine output, making it a true random number generator. Furthermore, NeoPUF has a feature that resists changes in operating temperature so that randomness stay constant under different conditions. The entropy multiplier eliminates the need for post processing, resulting in higher throughput.

KEY FEATURE

1. No post-processing enabling low latency.
2. Ideal randomness (HW0.5) without the need of high-quality entropy source.
3. Unique random number pool for each PUFtrng.
4. High throughput and low power consumption.



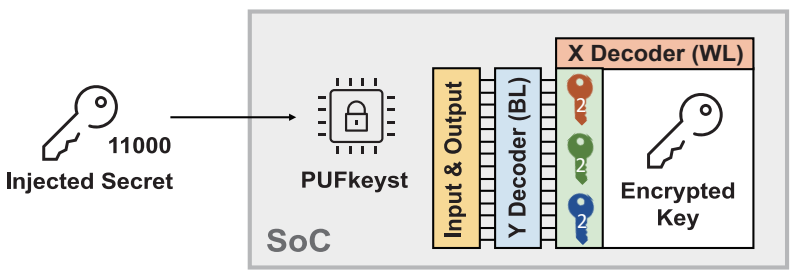
PUFkeyst

Simple and uncompromising key/data storage with PUF-based technology

Most widely used embedded key storage methods are based on One-Time Programmable (OTP) memory such as fuses or anti-fuses, or on Non-Volatile Memory (NVM) such as EEPROM or Flash. However, current key storage methods are facing threats including key leakage, manipulation, and deactivation. Key leakage is when the key has been revealed during operation. Manipulation often involves decapsulation and side channel attacks on the memory to change the value inside the memory. Deactivation uses fault injection to shut down the whole system. The security level of a system highly depends on the strength of its keys and keeping them secret. PUFkeyst provides a key storage method, allowing secret keys to remain invisible when stored. PUFkeyst entangles the keys with an embedded NeoPUF so that while the input data (such as a shared key) may be the same between chips, the actual stored data is unique from chip to chip. This enhances the difficulty for attackers since now a complete key cannot be pieced together from partial keys of different chips. Moreover, PUFkeyst can effectively prevent from key manipulation by entangling with NeoPUF. Hence, the security level for key storage can be enhanced without using a full-function crypto engine.

KEY FEATURE

1. Reliable scrambler ensures the key can't be read out directly.
2. Unique scramble value, making the stored information independent from chip-to-chip.
3. The value stored inside PUFkeyst cannot be changed or deleted.
4. Resistant to many physical attacks, including microscope imaging, probing, reverse engineering, etc.



PUFkeygen

Hardware acceleration security solution with benefit of PUF

Key generation is the process of generating keys for cryptography. All security functions involve key usage and crypto algorithms such as encryption, decryption, authentication, signature, secure storage, etc. Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and asymmetric-key algorithms (such as ECC). Keys can be categorized into many types, such as private key, public key, symmetric key, shared key, master key, root key, etc.

PUFkeygen uses the characteristics of NeoPUF and a circuit design to achieve a function for key generation. As the part of the hardware root-of-trust, the keys derived from NeoPUF through PUFkeygen have the features of uniqueness and non-repudiation. This approach can prevent the problem of key collision or the risk of key tampering that occurs with other key-generation functions. PUFkeygen combines with unique identity generation as a root key or master key, a true random number generator as nonce or session keys, and keys for secure storage for key encryption key or key wrapping function, etc.

KEY FEATURE

1. No CPU usage is needed and the key is compatible with various inter faces (e.g., APB, AHB, AXI, etc).
2. Improved security level for key generation functions, making them more impervious to attack.
3. Key generation with unique keys, high-speed throughput and efficient power consumption in a small footprint.
4. Secure storage for injected secret, extra OTP not necessary.

PUFenc

Secure inborn crypto engine keys with key length flexibility

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. The information or data, referred to as plaintext, will be encrypted by acrypto algorithm to generate the encrypted information so called ciphertext. Protecting keys is critical to the whole system. Normally, the key encryption key (KEK) is used for protecting cryptographic key.

PUFenc uses the NeoPUF as the key for encryption. It extracts the NeoPUF value to generate a crypto engine key. Only when the key is needed by the system can the value be extracted. This provides a more secure key for a crypto engine without using KEK. Moreover, PUFenc has the flexibility for different key lengths for a crypto engine.

KEY FEATURE

1. Embedded NeoPUF inside, preventing man-in-the-middle attacks.
2. A high-quality key for crypto engines.
3. Use of a NeoPUF value as a unique key, preventing collision.
4. Cryptographic keys constructed only when needed, which are unreadable through other means of access.

PUFauth

Symmetric authentication with robust protection of shared secret and high-quality nonces

Authentication technology provides access control for systems by checking whether a user's credentials match the credentials in a database of authorized users or in a data authentication server. The security level of authentication highly depends on key protection and protocol design.PUFauth provides an integrated PUF-based hardware solution including protocol design, key protection and session key generation

KEY FEATURE

1. Integrated PUF-based hardware solution including protocol design, shared key protection and session key generation.
2. Customized symmetric and asymmetric authentication protocol design.
3. Short initialization time for nonce generation.
4. PUFuid as the shared secret and key injection means of compliance.

PUFsecurity
an eMemory Company

CONTACT US

PUFsecurity Corporation
8F-1, No. 5, Tai-Yuan 1st St., Jhubei
City, Hsinchu County 30288, Taiwan
T +886-3-560-1010
F +886-3-560-1177
E info@pufsecurity.com

Jack (Sales)
jack@pufsecurity.com, wechat: Jackwang_123321
Aken (FAE)
aken@pufsecurity.com, wechat: wang_aken