ememory

Embedded Wisely, Embedded Widely

Run by Chips, Secured with Chips
Hardware Security with NeoPUF Solutions

WHITEPAPER

eMemory NeoPUF Entropy IP provides a quality PUF entropy up to 64K bits, and NeoPUF Key Manager IP offers a ready-to-use key generator to accelerate time-to-market. The solutions address key issues of existing technologies and can secure the hardware from the very beginning of chip manufacture.

Introduction

In today's ever connected world, security should be an integral part of chip design. The connected objects are enabled by chips, and they should also be protected with chips.

Many existing solutions do not satisfy high-security needs of the increasingly interconnected applications. Silicon Physically Unclonable Functions (PUFs), a security technology originally used in military applications and data centers, have gained tractions these days for its chip-unique and unpredictable nature.

PUF is analogous to human fingerprint, where each IC is born with its own unique identification due to the inherent differences of their physical properties. With eMemory's NeoPUF technology, each chip is capable of generating its own unique ID and keys, providing sources of trust in an unsecure environment.

The "personalization of keys" ensures that any attack is confined to the affected entity and has a minimum impact on the overall infrastructure. eMemory offers the following NeoPUF IP solutions to satisfy different needs of customers:

- NeoPUF Entropy: a PUF entropy source offering up to 64K random bits.
- NeoPUF Key Manager: a key generator providing a unique ID, a fixed number of master keys and unlimited session keys.

NeoPUF Entropy– Chip-Embedded Source of Trust

eMemory's NeoPUF Entropy is a PUF-based source of trust, which is unique to each chip, as the physical differences of IC are inherent from the silicon structure which is virtually impossible to be controlled or replicated. The IP provides a chip-unique ID and a reliable entropy.

The chip-embedded ID is essential to the supply chain risk management as it is proof against human interferences and reverse engineering. It is acknowledged that an ID assigned from outside of the chip risks data breaches and poses threats to the entire system.

With NeoPUF Entropy, every chip is capable of generating its own unique ID and keys, which serves as a damage control. Should an entity be attacked, the keys of other entities remain intact.

NeoPUF Entropy offers uniformly random outputs. Each bit is independent of each other and has a probability of 1⁄2 of producing "0" or "1". The IP passes NIST 800-22 and AIS-31 tests.

#	Statistical Test	Recommended n	Input Size		Sub-Test #	Decision Rule					Randonness Judgement
						Min. P-Value	Proportion		Uniformity		
		Length of bit string	n	bit stream(s)		P-Value > 0.01	mini	P/F	P-value of P-value > 0.0001	P/F	PASS/FAIL
1	Frequency	n>100	40000	75	1	-	73/75	PASS	0.238562	PASS	PASS
2	Block Frequence (m=128)	n>100	40000	75	1	-	75/75	PASS	0.72554	PASS	PASS
3	Cumulative sums - Forward	n>100	40000	75	1	-	74/75	PASS	0.519816	PASS	PASS
4	Cumulative sums - Reversed	n>100	40000	75	1	-	74/75	PASS	0.72554	PASS	PASS
5	Runs	n>100	40000	75	1	-	75/75	PASS	0.362174	PASS	PASS
6	Longest runs of ones	n>128	40000	75	1	-	75/75	PASS	0.295803	PASS	PASS
7	Binary Matrix Rank	n>38912	40000	75	1	-	73/75	PASS	0.808725	PASS	PASS
8	Spectral DFT	n>1000	40000	75	1	-	73/75	PASS	0.937294	PASS	PASS
9	Non-overlapping Templates (m=9)	n>8m-8	40000	75	148	-	71/75	PASS	0.00058	PASS	PASS
10	Overlapping Templates (m=9)	n>1E6	40000	75	1	-	75/75	PASS	0.036868	PASS	PASS
11	Serial (m=16, ∇Ψm2))	m< ($\log_2$ n)-2	40000	75	2	-	75/75	PASS	0.127498	PASS	PASS
12	Approximate Entropy (m=10)	m< ($\log_2$ n)-5	40000	75	1	-	75/75	PASS	0.339044	PASS	PASS
13	Universal	n>387840	1000000	3	1	0.341243	3/3	PASS	-	-	PASS
14	Linear complexity (M=500)	n>1E6	1000000	3	1	0.652199	3/3	PASS	-	-	PASS
15	Random Excursions	n>1E6	1000000	3	8	0.145246	3/3	PASS	-	-	PASS
16	Random Excursions Variant	n>1E6	1000000	3	18	0.036142	3/3	PASS	-	-	PASS

Figure 1. NeoPUF Entropy NIST 800-22 Test Results

More importantly, the PUF outputs are consistent without bit errors at an extended temperature range from -40°C to +150°C (Fig.2). The zero bit error rate eliminates the need for complicated error correction measures.

The NeoPUF Entropy IP includes all the necessary support, control circuitry, and a comprehensive test flow. The IP is available from 55nm to 7nm.

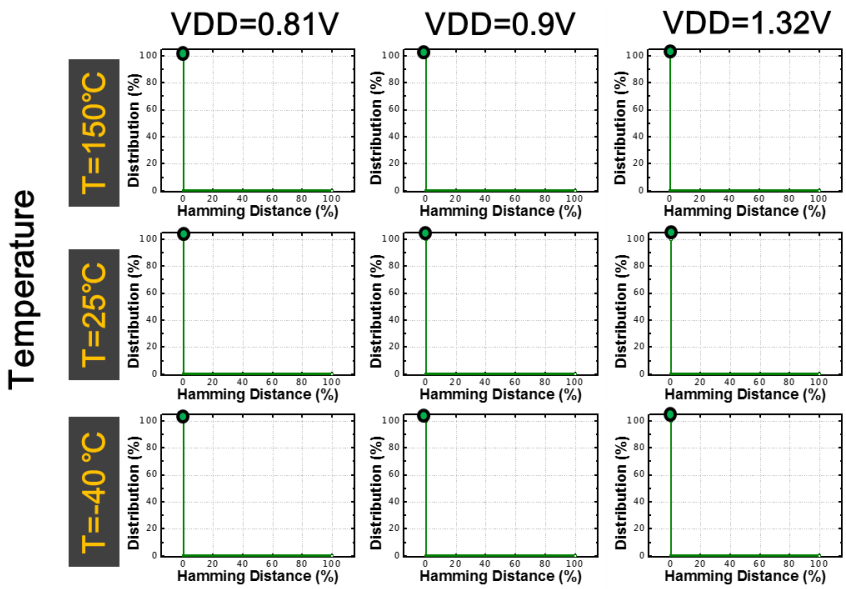


Figure 2. NeoPUF Intra-Chip Hamming Distance Test Results

NeoPUF Key Manager – All Key Materials Safeguarded

The NeoPUF Key Manager IP block is a self-contained enclosure, within which all key materials are safeguarded. The IP provides a chip-unique ID, master keys and session keys. A standard IP can generate the following items, and the length and the number of IDs and keys can be tailored to customers' needs.

- Hardware ID
- Multiple Master Keys
- Unlimited Session Keys (retrievable through Key Index)
- Unlimited Nonces and Initialization Vectors

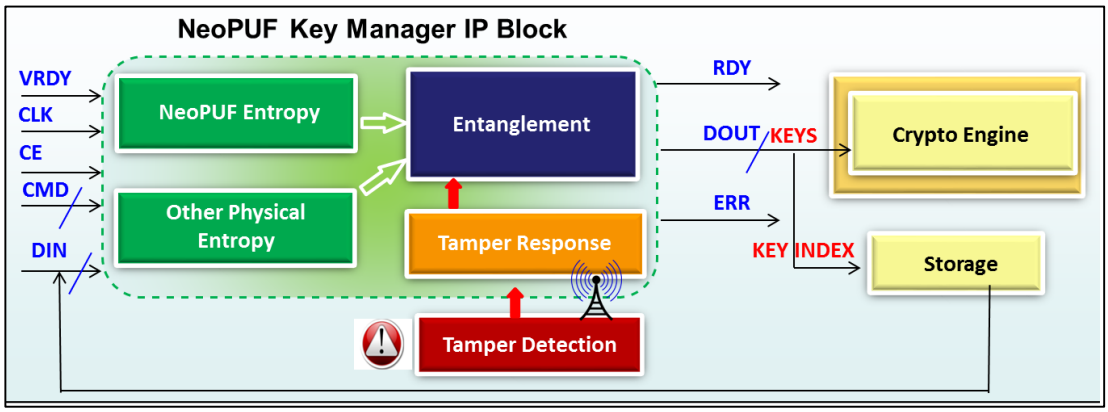


Figure 3. NeoPUF Key Manager IP

The ID and master keys are fixed for multiple uses. Upon a command, a master key is exported directly to the crypto engine.

The Key Manager also supports unlimited session keys and one-time pass operations. The external application does not need a TRNG if with the NeoPUF Key Manager. A key index (library) can be established and used to retrieve keys whenever needed. The index doesn't contain key materials and can be stored with proper protection.

It is not advisable to store the IDs and keys in an unsecure storage, and the interface between the key manager and the crypto engine should be secured with metal protection or sensing schemes.

In response to tamper alerts, NeoPUF Key Manager will go back to a default state. When the system resolves the threats, the key manager will be able to regenerate the keys/ID after a reboot.

NeoPUF Key Manager is designed to address disadvantages of existing solutions, such as unprotected key materials as well as unstable PUF outputs. Solving these disadvantages would not only increase security of the system, but would also reduce unnecessary overheads.

	NeoPUF Key Manager	SRAM PUF	TRNG
Reproducible Key	Yes	Yes	No
Reliable Output	Yes	Error correction and helper data needed	Yes
Immune to storage attacks	Yes	Vulnerable	Vulnerable
Unlimited Session Keys	Yes	No	No
Unlimited Nonces/Ivs	Yes	No	No
Key Retrieval Index	Yes	No	No

Figure 4. NeoPUF Key Manager Advantages

NeoPUF Key Manager safeguards all key materials within the IP block, without the need for an external storage. This eliminates the risks of key materials being stolen and cloned, while saving the costs and resources required for key protection.

In addition, the Key Manager can generate reliable PUF outputs, and hence no helper data or extra storage is required.

Application

In the wake of a series of attacks exploiting IoT vulnerabilities in recent years,

there have been calls for more attention to hardware security. NeoPUF solutions can safeguard the hardware from the very beginning of chip manufacture.

eMemory's NeoPUF Entropy provides a quality random source up to 64K bits. The customers have a full control on the size of the entropy and how it best fits into their in-house technologies.

On the other hand, the NeoPUF Key Manager IP is an easy-to-implement key generator. The generated keys can be used in cryptographic applications. The following are use cases of the Key Manager IP:

1. Unique ID (Fig.5)
   A device unique ID is generated on a ID Generation Command. The ID can be regenerated, and it is not advisable to store it in an unsecure storage.

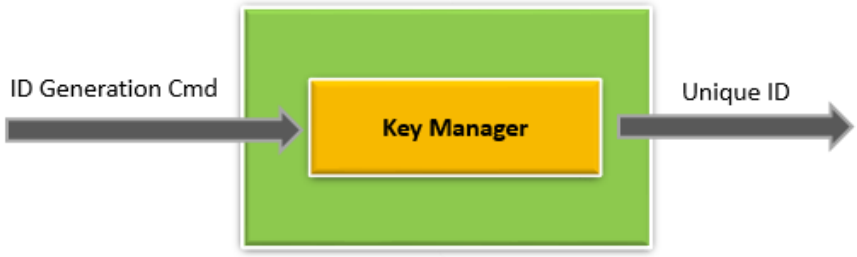


Figure 5. Unique ID Generation

2. Key Generation (Fig.6)
   The Key Manager provides a fixed number of master keys and unlimited session keys. A key can be generated with a Key Generation Command, and exported directly for crypto operations.

Figure 6. Key Generation

3. Nonce/IV Generation (Fig.7)
    1) The Key Manager supports unlimited nonces and initialization vectors.
    2) Nonces and Ivs can be generated with a Nonce Generation Command, and exported directly for crypto operations.

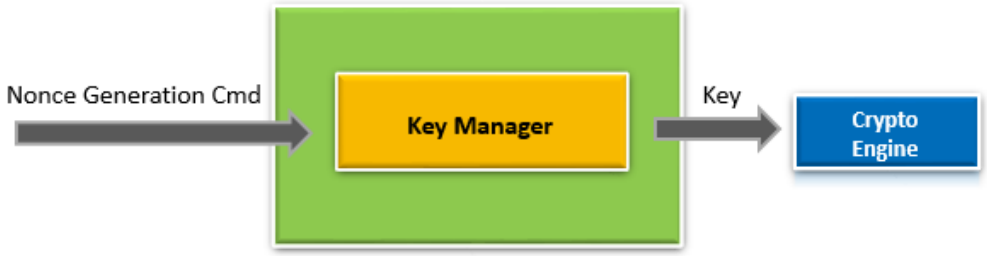


Figure 7. Nonce/IV Generation

4. Key Index (Fig.8)
    1) In this case, the user needs to reuse a key, and there is no secure storage for this key external to the Key Manager.
    2) He can give an Index Generation Command to create a key index and store this index outside of the key manager. Whenever the key is needed, he can give a Key Retrieval Command to retrieve the key.

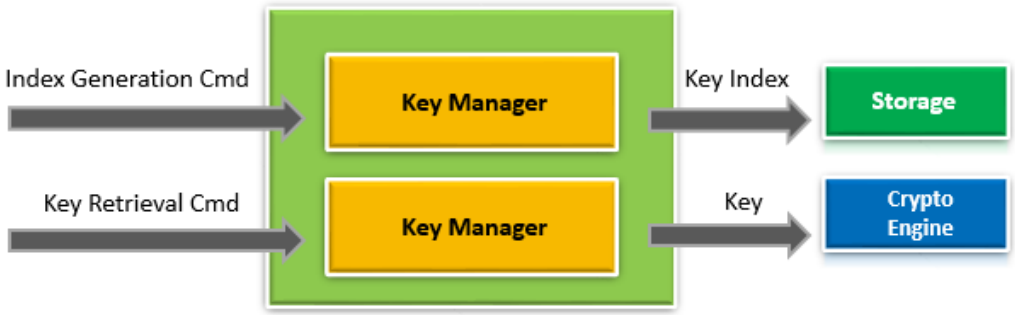


Figure 8. Key Index

5. Key/Data Entanglement (Fig.9)
    1) In this case, the user receives a common key or sensitive data from other entities and needs to protect it or use it later.
    2) He can give a Key Entanglement Command to create a key index for the received key/data. When he needs to use the key/data, he can obtain it using the Key Retrieval Command. He does not have to store the key/ data, and can just retrieve it whenever needed.

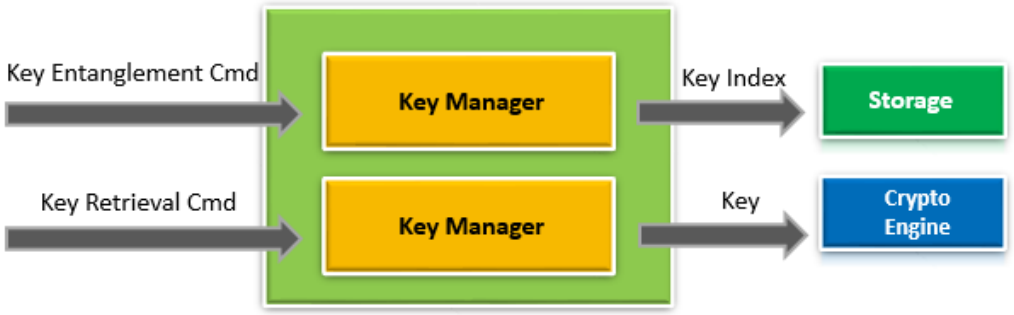


Figure 9. Key/Data Entanglement

Conclusion

eMemory's NeoPUF technology is ideal for crypto applications for its uniqueness and unpredictability. It is virtually impossible to be reverse engineered as silicon manufacturing variations cannot be controlled and replicated.

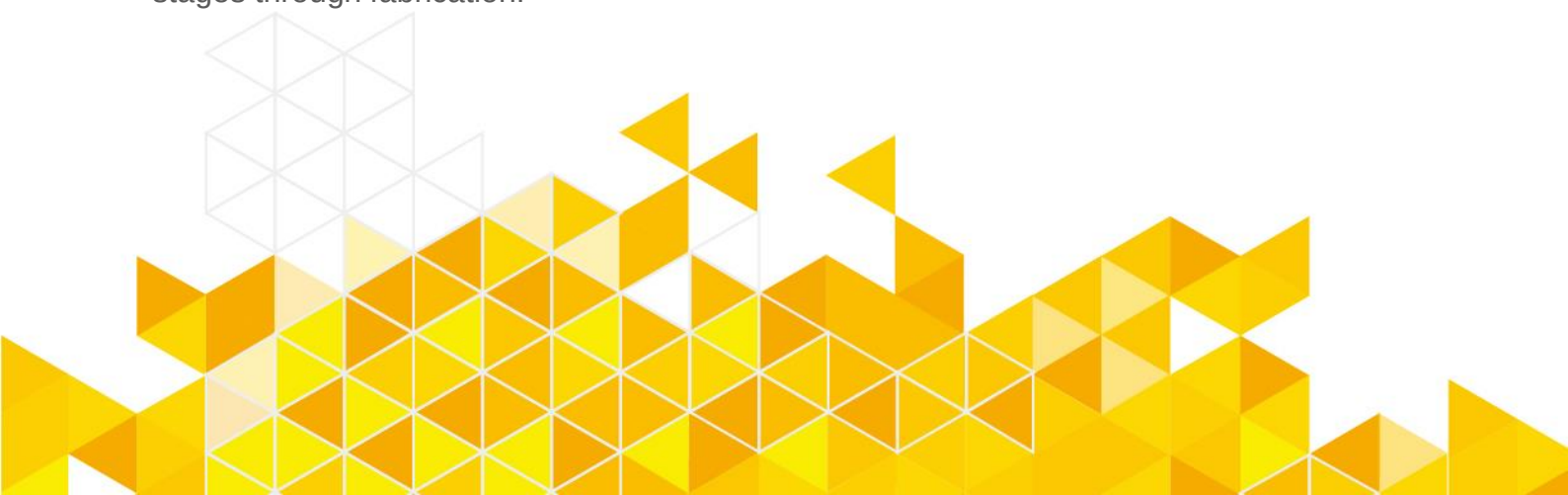
The NeoPUF Entropy IP provides a quality random source, which can be customized to meet customers' design requirements. Meanwhile, the NeoPUF Key Manager IP is a ready-to-use key generator which can help customers accelerate time-to-market.

NeoPUF generated IDs and keys are most secure in that they are born within the chip itself, eliminating any human induced interferences and safeguarding hardware from the very beginning of chip manufacture.

Wherever you need device unique ID and keys, you should seriously consider adopting the NeoPUF IP solutions. For more information, please contact us at sales@ememory.com.tw.

About eMemory

eMemory is a global leader in logic process embedded non-volatile memory (eNVM) silicon IP established in 2000. eMemory has devoted itself to research and development of innovative technologies, offering the industry's most comprehensive platforms of patented eNVM IP solutions which are supplied to semiconductor foundries, integrated devices manufacturers (IDMs), and fabless design houses worldwide. eMemory's eNVM silicon IPs support a wide range of applications, including trimming, function selection, code storage, parameter setting, encryption, and identification setting. The company has the world's largest NVM engineering team and prides itself on providing partners with a full-service solution that sees the integration of eMemory eNVM IP from initial design stages through fabrication.



ememory

Embedded Wisely, Embedded Widely

eMemory Technology Inc.
8F, No.5, Tai-Yuan 1st St., Jhubei City, Hsinchu County 30265 Taiwan
T +886-3-5601168 F +886-3-5601169
www.ememory.com.tw