

eMemory

智能物联网-嵌入式根密钥解决方案 与芯片防盗拷技术

Emory Liu
eMemory



2019年中国嵌入式技术大会
EMBEDDED TECHNOLOGY
Conference China 2019

IPR Notice

All rights, titles and interests contained in this information, texts, images, figures, tables or other files herein, including, but not limited to, its ownership and the intellectual property rights, are reserved to eMemory. This information may contain privileged and confidential information. Some contents in this information can be found in Logic Non-Volatile Memory (The NVM solutions from eMemory), published in 2014. Any and all information provided herein shall not be disclosed, copied, distributed, reproduced or used in whole or in part without prior written permission of eMemory Technology Inc.

eMemory, NeoBit, NeoFuse, NeoEE, NeoMTP, NeoROM, EcoBit and NeoPUF are all trademarks and/or service marks of eMemory in Taiwan and/or in other countries.

Outline

01

力旺电子(eMemory)简介

02

NeoPUF芯片指纹技术介绍

03

NeoPUF 于IoT硬件安全应用

04

NeoPUF+OTP芯片防伪介绍

05

NeoPUF+OTP (IP)授权金计算之应用介绍

06

NeoPUF完美随机数数据演示

07

总结

Outline

01

力旺电子(eMemory)简介

02

NeoPUF芯片指纹技术介绍

03

NeoPUF 于IoT硬件安全应用

04

NeoPUF+OTP芯片防伪介绍

05

NeoPUF+OTP (IP)授权金计算之应用介绍

06

NeoPUF完美随机数数据演示

07

总结

Corporate Overview



Founded

eMemory, funded in 2000, is the world's largest pure-play developer and provider of logic NVM technology. The revenue in 2018 is USD 49M



Employees

There are 250+ employees in eMemory and more than 70% of them are IP developers.



Innovation

We have 680+ patents issued and the cumulative customer tape-out is more than 4650.



Achievement

eMemory receive tsmc NVM IP Partner Award for 10 consecutive year. Our IP has shipped in more than 27 million wafers

eMemory

eMemory's IP Technology



Floating-gate(FG) OTP

Floating-gate(FG) OTP memory
Good for more-than-Moore platforms



Cost-Effective FG MTP

Logic-based embedded MTP memory
for medium density eFlash
replacement



High Reliability FG MTP

Applicable for Low-power and High-
Temperature applications



Anti-Fuse OTP

Applicable for generic & advanced lo
gic platforms



PUF Technology

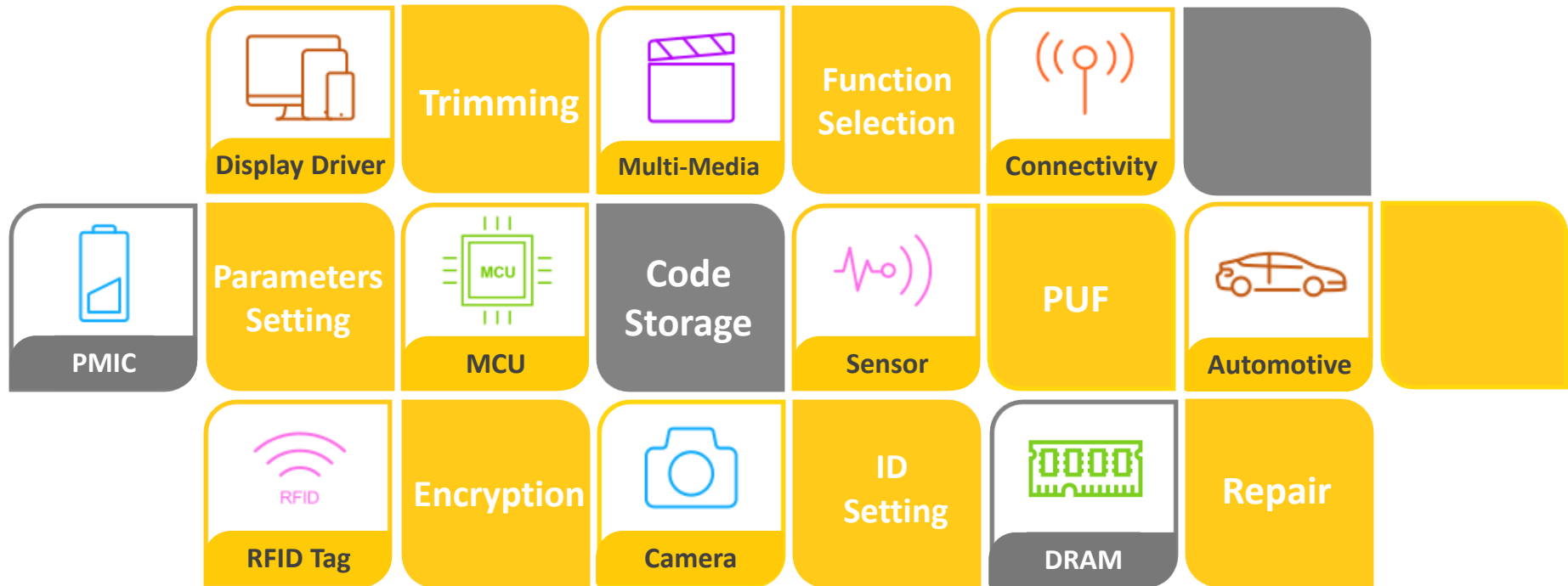
Robust, Random and Unique
Physical Unclonable Function (PUF)
Technology



Ultra-Low-Power MTP

Ultra-low-power embedded logic
MTP solution consuming only micro-
Watts (uW) of power

eMemory Solution for Various Applications



Outline

01

力旺电子(eMemory)简介

02

NeoPUF芯片指纹技术介绍

03

NeoPUF 于IoT硬件安全应用

04

NeoPUF+OTP芯片防伪介绍

05

NeoPUF+OTP (IP)授权金计算之应用介绍

06

NeoPUF完美随机数数据演示

07

总结

What is Physical Unclonable Functions ?

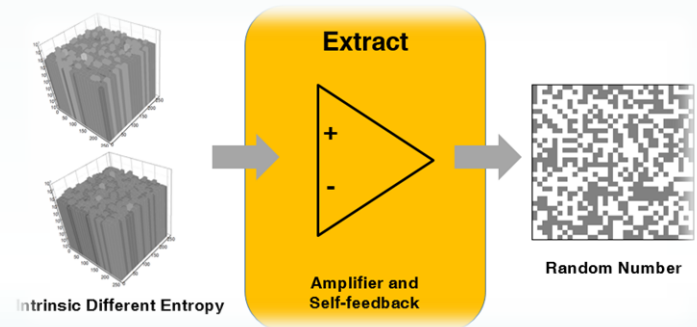
* 一万亿= 10^{12}

Human Fingerprint



指纹重复机率
 $1/10^{20}$ (12点)

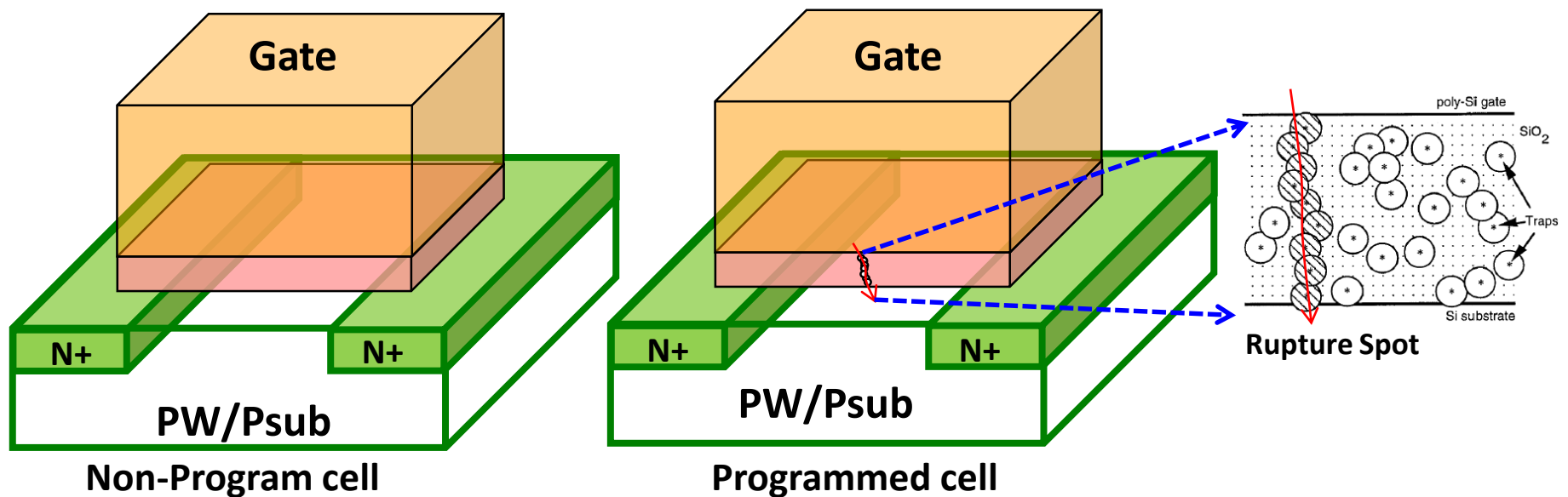
IC Fingerprint



$$2^{64} = 1.8 \times 10^{19} ; 2^{256} = 1.5 \times 10^{77}$$
$$2^{128} = 3.4 \times 10^{38} ; 2^{512} = 1.3 \times 10^{154}$$

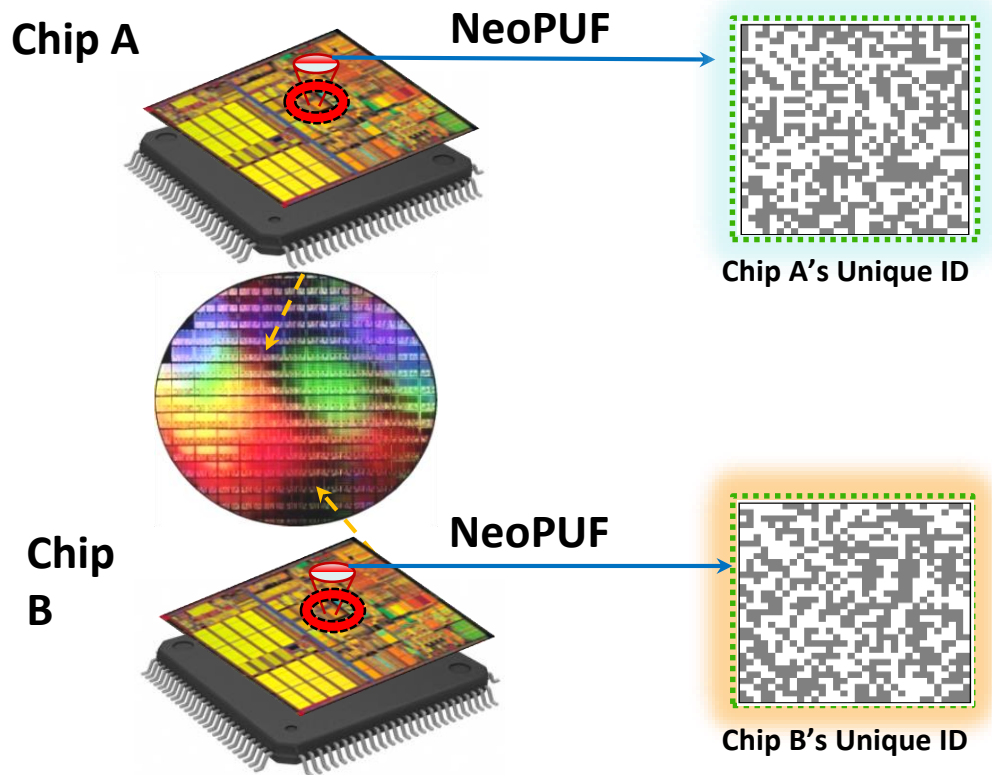
Secure Key Storage by Anti-Fuse

- Reliability, Stability: Anti-Fuse Fundamental
- Security: Hard to reverse by SEM/TEM/PVC
 - Good solution for secret storage



NeoPUF -Inborn Silicon ID

- **NeoPUF w/o ECC can offer 64K-bits ideal entropy pool**
 - 128-bits SRAM PUF needs 16K-bit SRAM source.



Inborn Silicon ID

- **Deep-rooted Root of Trust**
Based on uncontrollable silicon manufacturing variations
- **Unclonable & Unpredictable**
Manufacturing variations cannot be controlled or replicated
- **Chip-Unique**
Every Chip bears its unique
 - ✓ Chip ID
 - ✓ Entropy source

Outline

01

力旺电子(eMemory)简介

02

NeoPUF芯片指纹技术介绍

03

NeoPUF 于IoT硬件安全应用

04

NeoPUF+OTP芯片防伪介绍

05

NeoPUF+OTP (IP)授权金计算之应用介绍

06

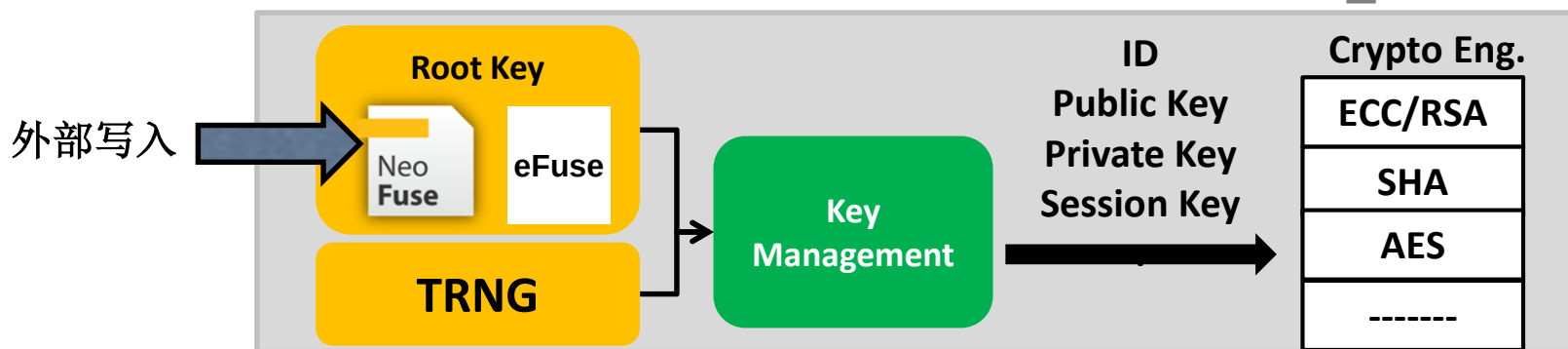
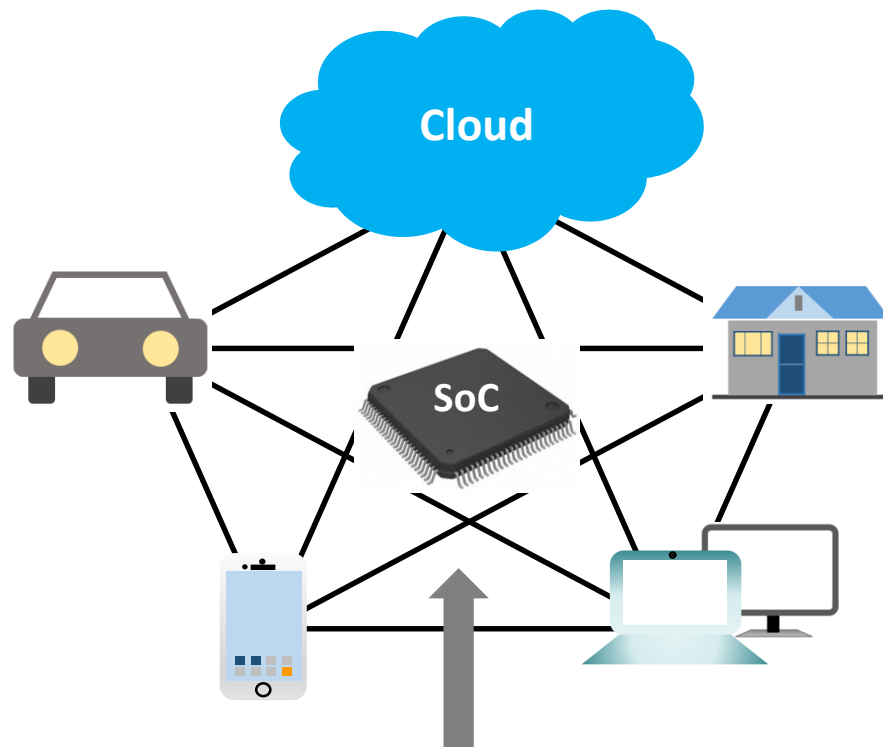
NeoPUF完美随机数数据演示

07

总结

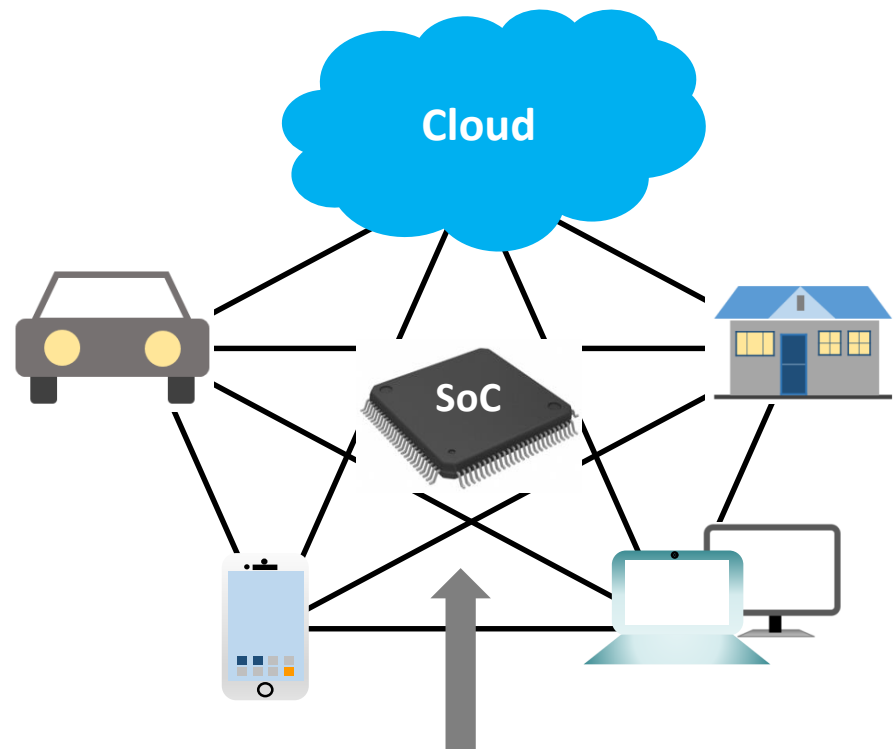
H/W Security in IoT World

- **Edge to Cloud**
 - Authentication
 - Communicate Data Encryption
- **Edge to Edge**
 - Authentication
 - Communicate Data Encryption
- **Edge to Local Memory**
 - Local Data Encryption



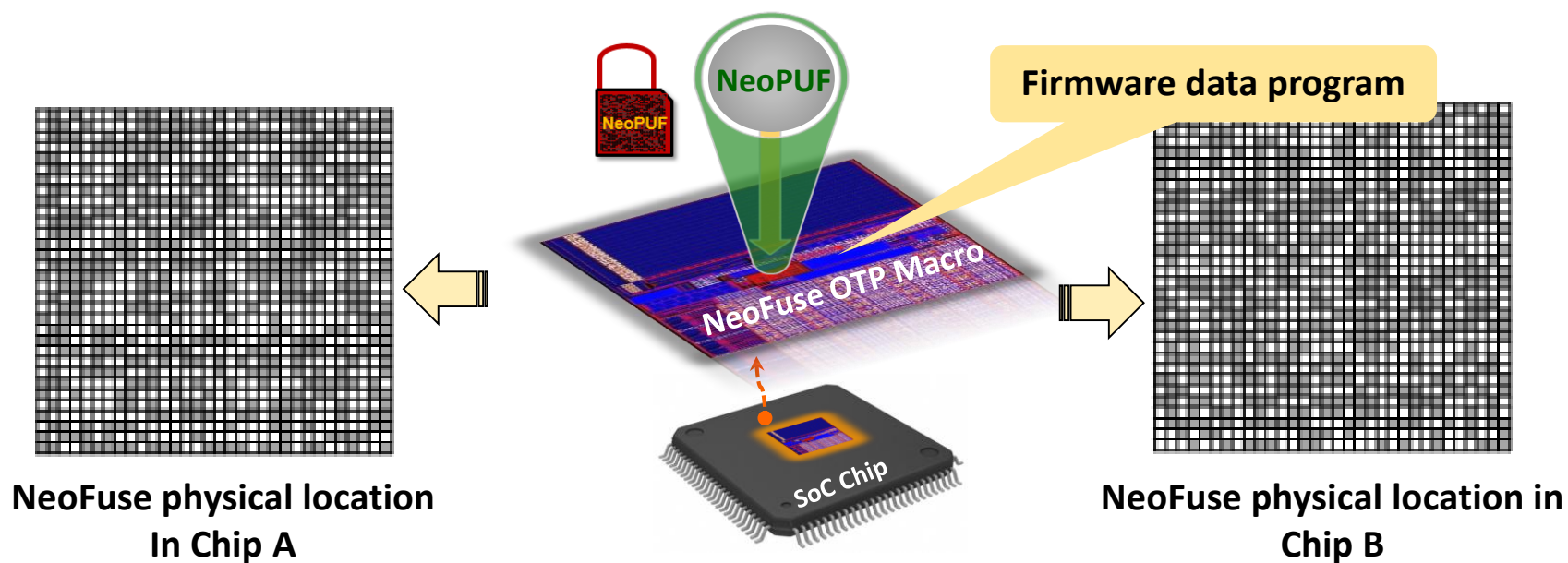
H/W Security in IoT World

- **Edge to Cloud**
 - Authentication
 - Communicate Data Encryption
- **Edge to Edge**
 - Authentication
 - Communicate Data Encryption
- **Edge to Local Memory**
 - Local Data Encryption



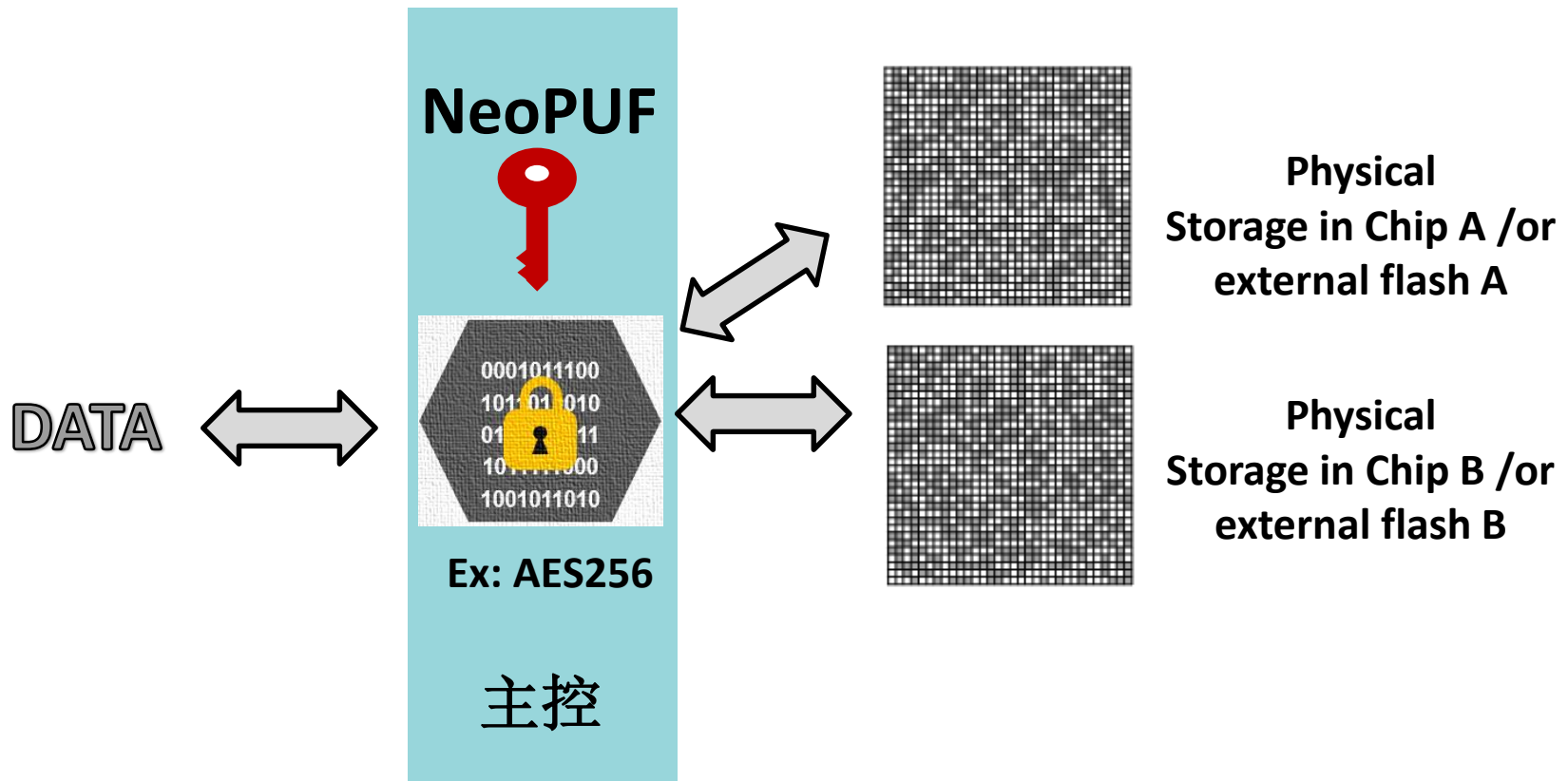
Enhanced Secure NeoFuse

- NeoFuse storage can be further protected and encrypted by NeoPUF with inborn secret



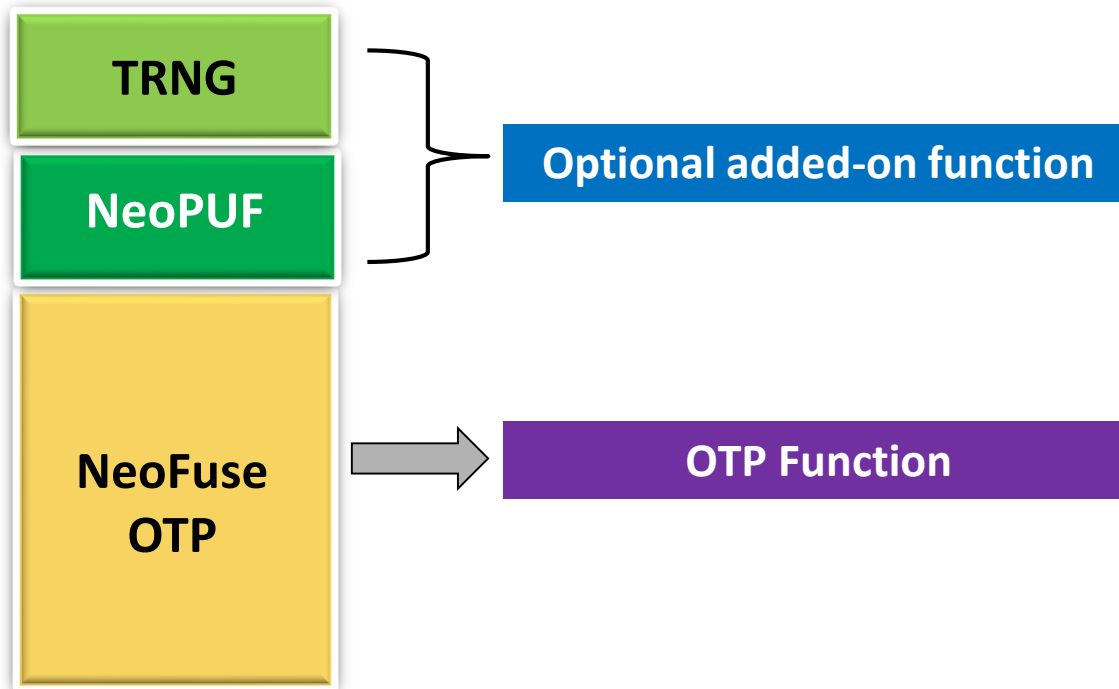
Secure Flash Storage

- eNVM storage can be also further protected using robust Neo PUF inborn secrets; Key length can be adjusted by encryption demand



OTP Added-on Functions

- Based on NeoFuse OTP technology, eMemory provides an optional PUF & TRNG functions



Outline

01

力旺电子(eMemory)简介

02

NeoPUF芯片指纹技术介绍

03

NeoPUF 于IoT硬件安全应用

04

NeoPUF+OTP芯片防伪介绍

05

NeoPUF+OTP (IP)授权金计算之应用介绍

06

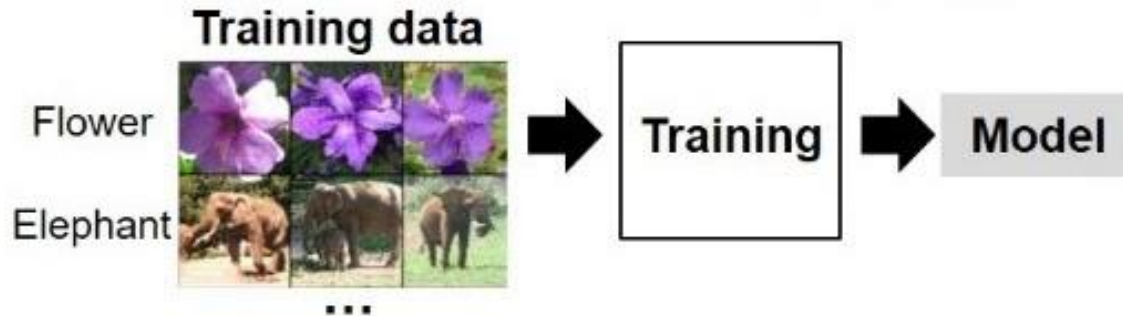
NeoPUF完美随机数数据演示

07

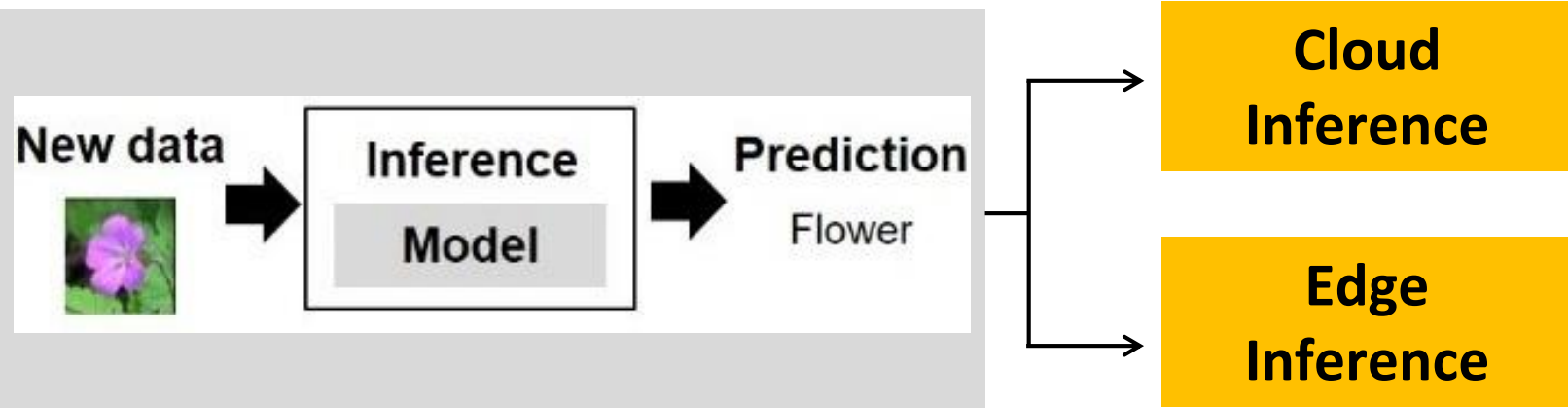
总结

Deep Learning Flow

Training

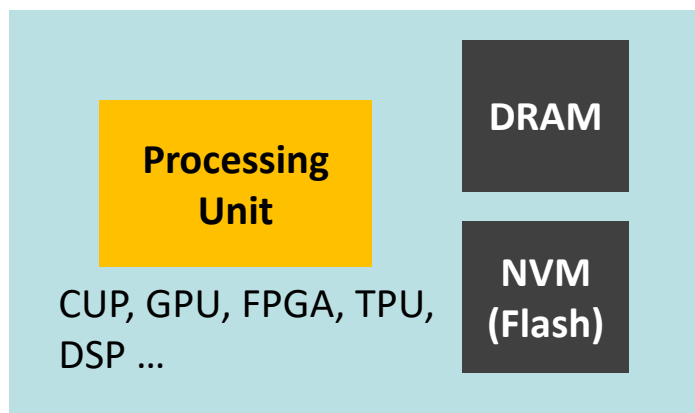


Inference



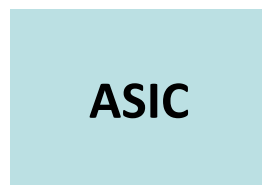
Security Risks for Edge Inferences

Scenario (module)



- Trained model & weighting with plaintext may be stolen
- Wrong behavior/hazards introduced due to unencrypted memory

Scenario (ASIC)

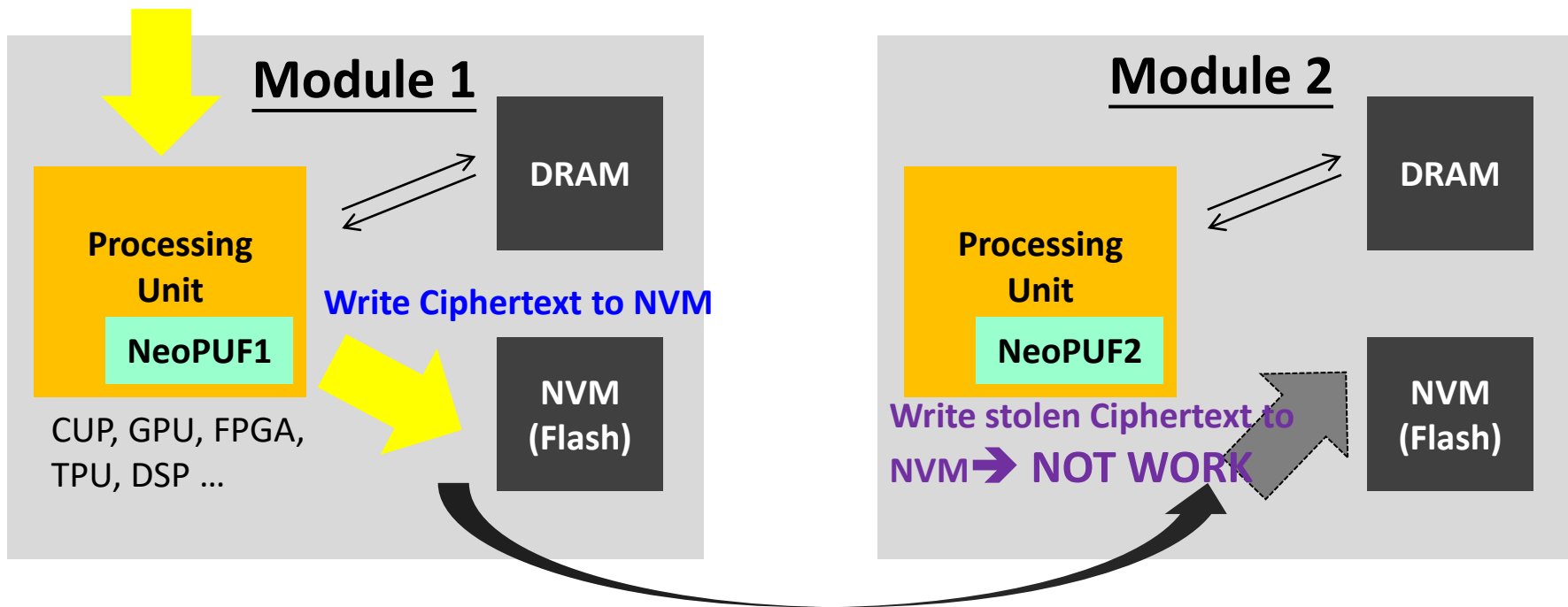


- ASIC may be reverse engineered
- Trained model may be stolen

NeoPUF for Edge Inference – Module

- Chip-intrinsic UID, secret keys, scramble table, I/O selection...are available to enhance security by using NeoPUF
→ Only intrinsic code can enable model

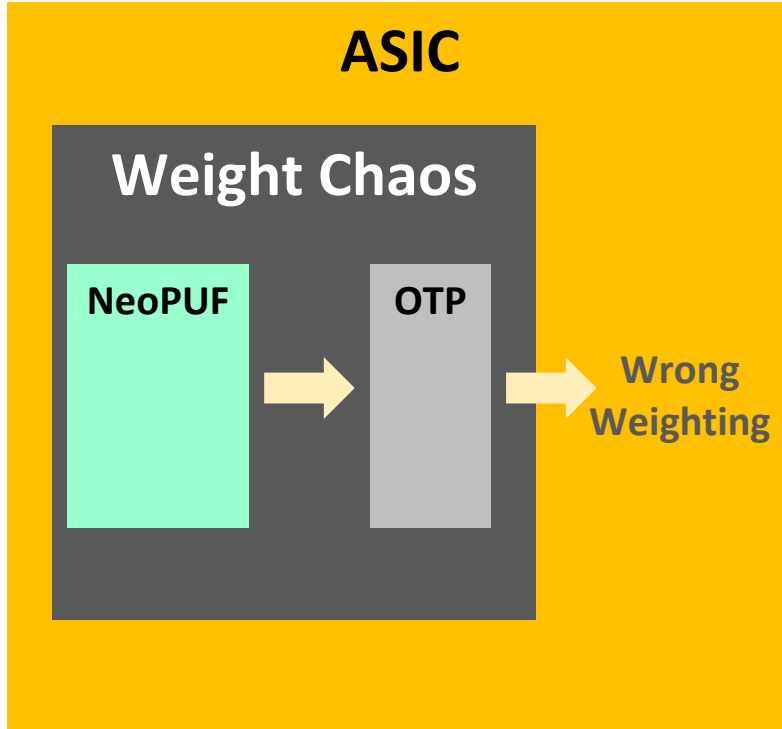
Input (Plaintext) trained model to Processing Unit



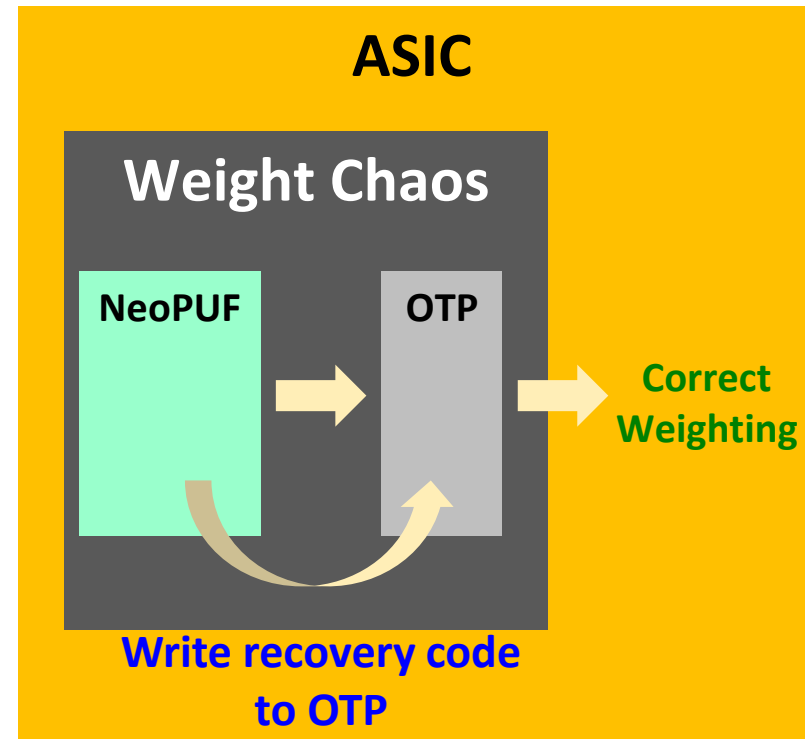
NeoPUF for Edge Inference – ASIC (1/2)

- Weight Chaos with intrinsic recovery code from NeoPUF protects ASIC inference from unauthorized cloning

Before Enable



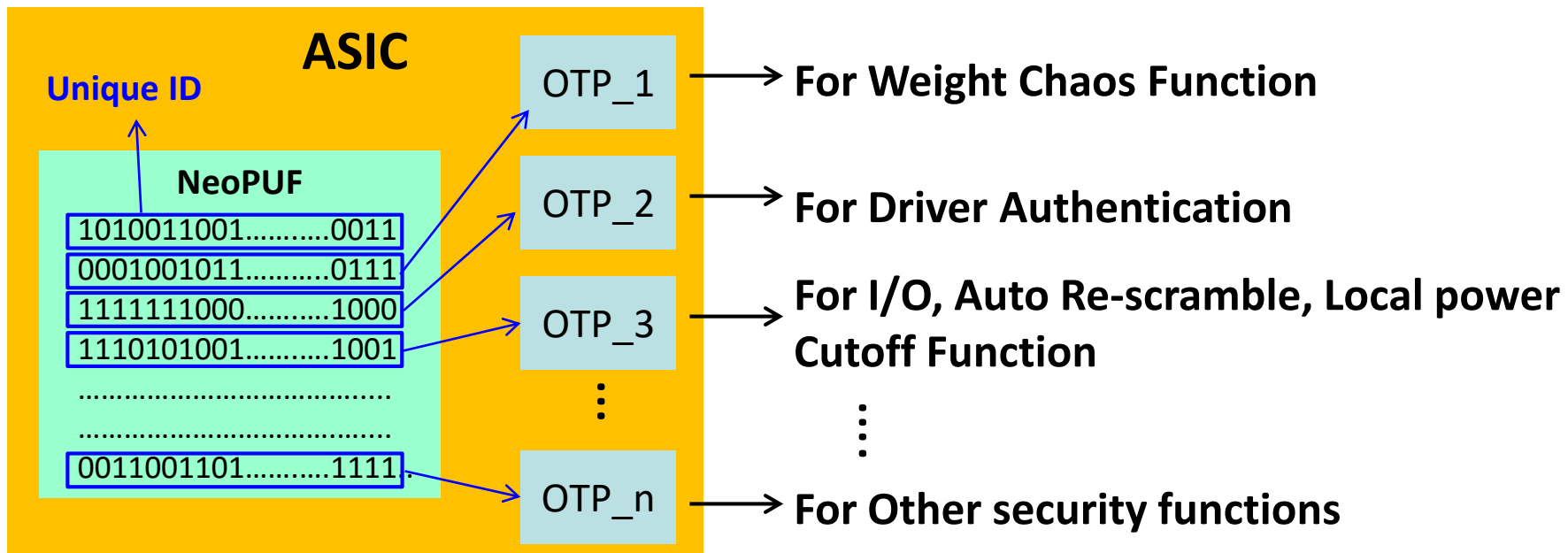
Enable



NeoPUF for Edge Inference – ASIC (2/2)

- With a large entropy pool, users can build in several kinds of security functions at once

Enable Command



Outline

01

力旺电子(eMemory)简介

02

NeoPUF芯片指纹技术介绍

03

NeoPUF 于IoT硬件安全应用

04

NeoPUF+OTP芯片防伪介绍

05

NeoPUF+OTP (IP)授权金计算之应用介绍

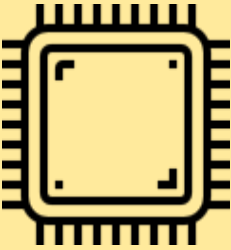
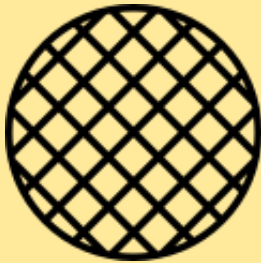
06

NeoPUF完美随机数数据演示

07

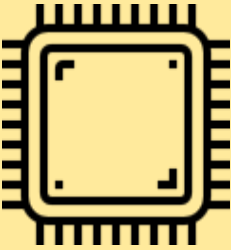
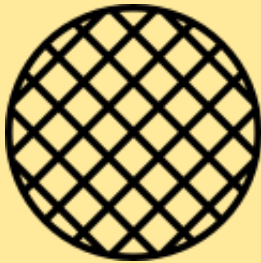
总结

IP/Compiler Ecosystem – Before

Stage	<u>IC Design</u> 	<u>Mass Production</u> 
Fee	• License Fee • Usage/NRE Fee	• Royalty
Problems	• Upfront fee will increase the barrier of adopting IP	• Hard to get real production record to count royalty.

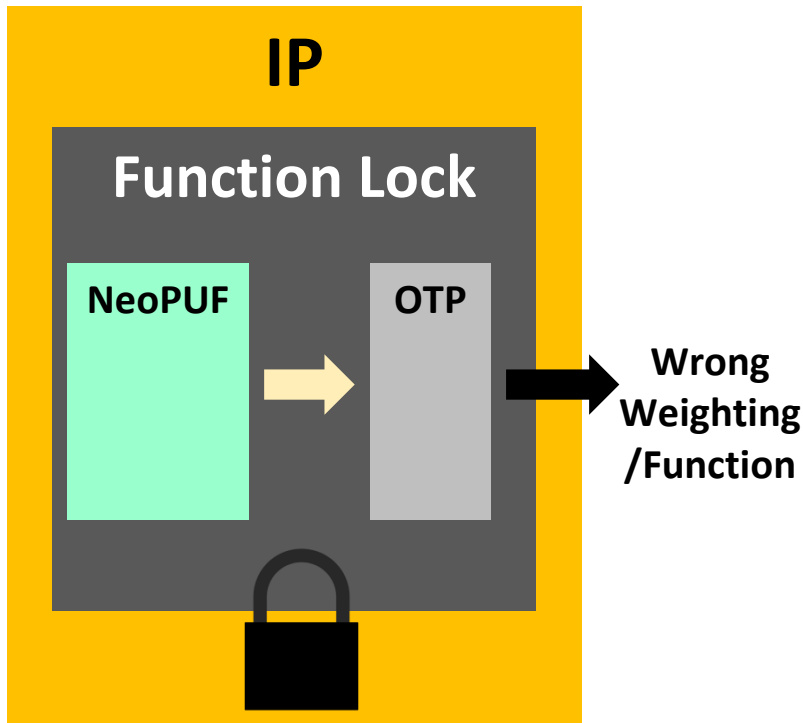
IP/Compiler Ecosystem – After

IP embeds eMemory's NeoPUF to count royalty die by die

Stage	<u>IC Design</u> 	<u>Mass Production</u> 
Fee	• Zero upfront fee	• Royalty
Benefit	• Lower the entry barrier	• Count royalty die by die • Prevent IP stolen by reverse-engineering

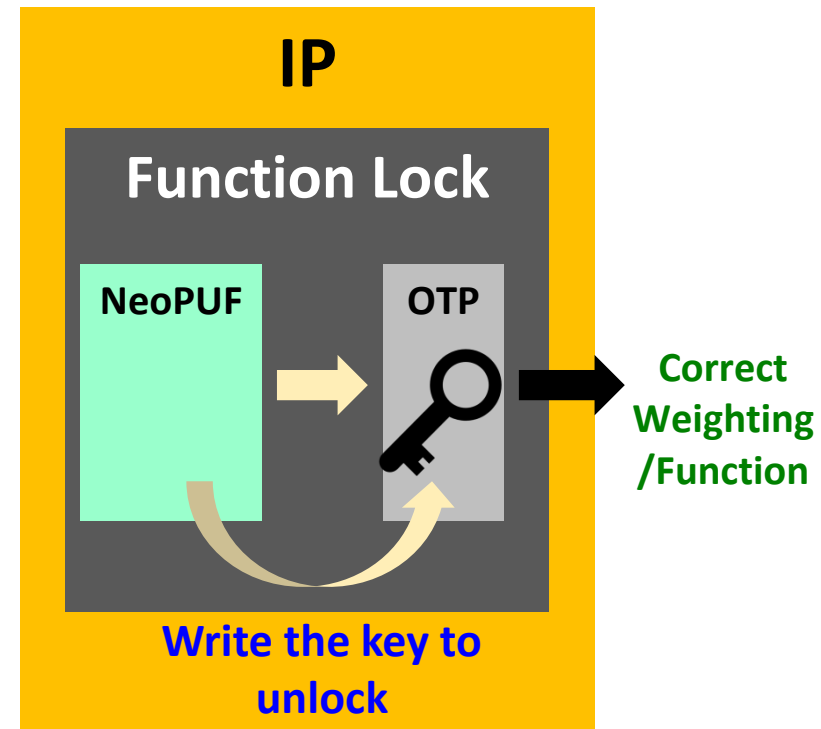
NeoPUF for Royalty Counting

Before Enable



- Use NeoPUF inborn entropy to lock function, power delivery, re-scaling weight...etc.
- IP can't work normally before enabling.

Enabled

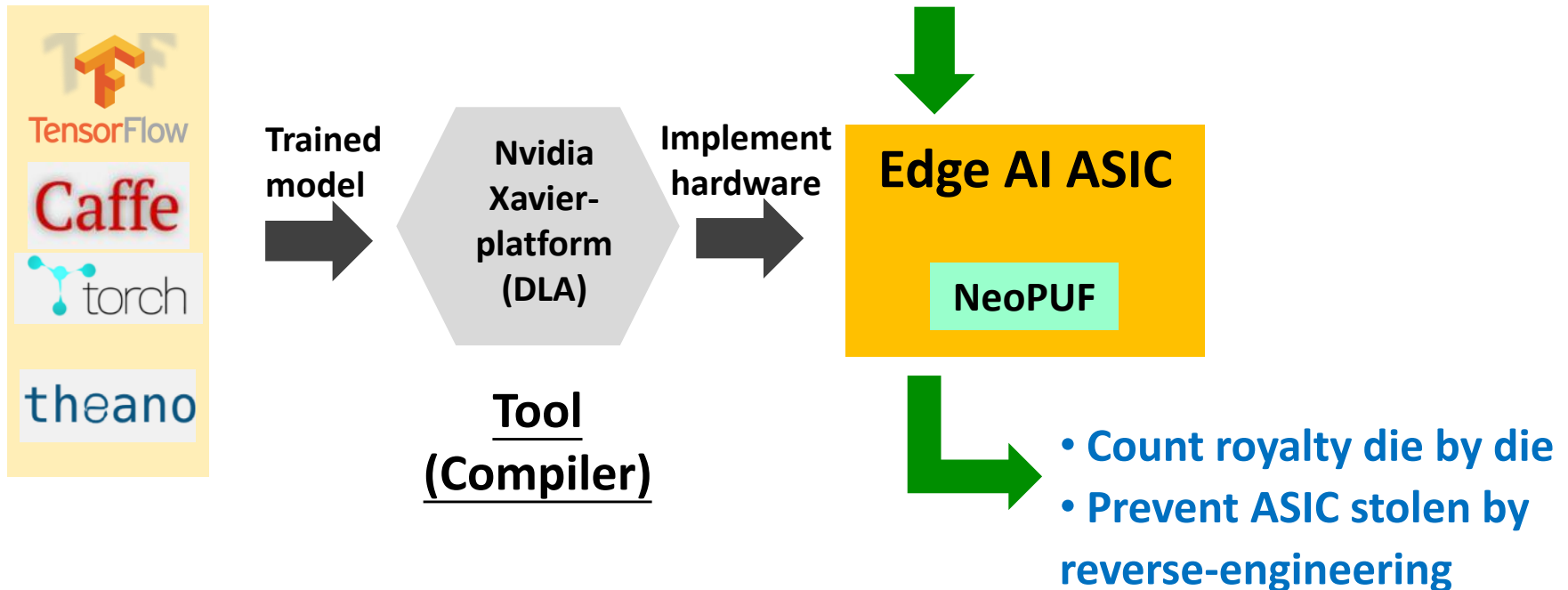


- IP provider enables IP during IC testing or via internet.
- After enable, the unlock key (from NeoPUF) will be auto-written into OTP.

Benefit Compiler Provider

- Same as IP provider, NeoPUF solution can help compiler provider to count royalty die by die

Chip can be enabled only if the designated command/**secret** key is executed.



Outline

01

力旺电子(eMemory)简介

02

NeoPUF芯片指纹技术介绍

03

NeoPUF 于IoT硬件安全应用

04

NeoPUF+OTP芯片防伪介绍

05

NeoPUF+OTP (IP)授权金计算之应用介绍

06

NeoPUF完美随机数数据演示

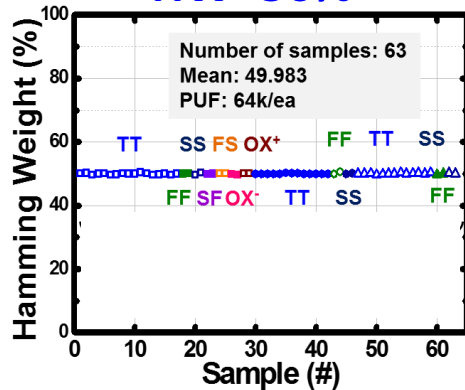
07

总结

Demonstration (55nm)

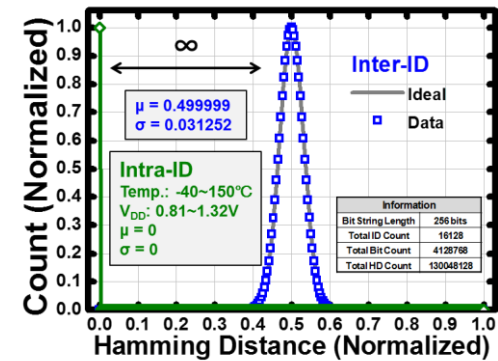
Randomness

HW=50%



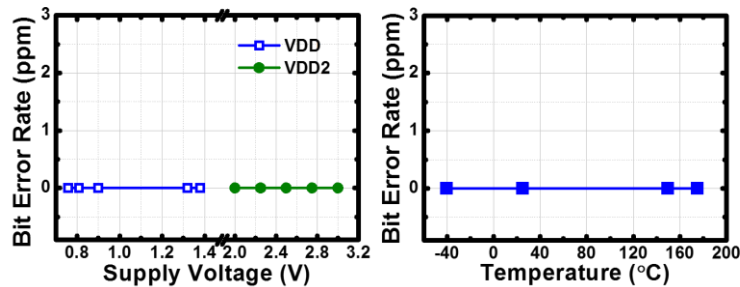
Uniqueness

$\mu_{\text{inter}}=0.5$

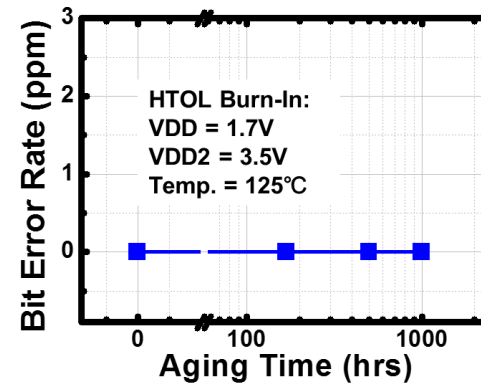


Stability

$\mu_{\text{intra}}=0$



Reliability



Randomness by NIST800-22

55LP/55emb-Flash

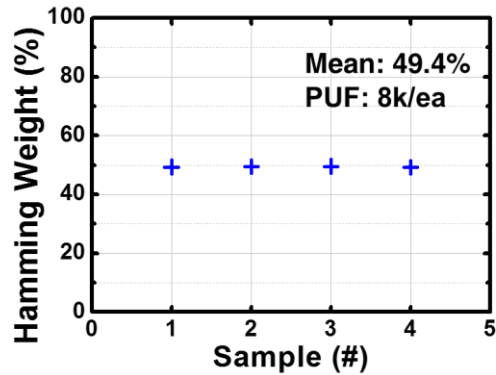
- NeoPUF passes NIST800-22 statistics randomness test from accumulated samples (TT/FF/SS/SF/FS/OX+/OX-)

#	S tatistical Test	Input Size		Sub-Test #	Decision Rule					Randomness Check
					Min. P-Value	Proportion		Uniformity		
		n	Bit stream(s)			P-Value		P/F	P-value of P-value	P/F
1	Frequency	40000	75	1	-	73/75	PASS	0.238562	PASS	PASS
2	Block Frequence (m=128)	40000	75	1	-	75/75	PASS	0.72554	PASS	PASS
3	Cumulative sums - Forward	40000	75	1	-	74/75	PASS	0.519816	PASS	PASS
4	Cumulative sums - Reversed	40000	75	1	-	74/75	PASS	0.72554	PASS	PASS
5	Runs	40000	75	1	-	75/75	PASS	0.362174	PASS	PASS
6	Longest runs of ones	40000	75	1	-	75/75	PASS	0.295803	PASS	PASS
7	Binary Matrix Rank	40000	75	1	-	73/75	PASS	0.808725	PASS	PASS
8	Spectral DFT	40000	75	1	-	73/75	PASS	0.937294	PASS	PASS
9	Non-overlapping Templates (m=9)	40000	75	148	-	71/75	PASS	0.00058	PASS	PASS
10	Overlapping Templates (m=9)	40000	75	1	-	75/75	PASS	0.036868	PASS	PASS
11	Serial (m=16, $\nabla\Psi m_2$))	40000	75	2	-	75/75	PASS	0.127498	PASS	PASS
12	Approximate Entropy (m=10)	40000	75	1	-	75/75	PASS	0.339044	PASS	PASS
13	Universal	1000000	3	1	0.341243	3/3	PASS	-	-	PASS
14	Linear complexity (M=500)	1000000	3	1	0.652199	3/3	PASS	-	-	PASS
15	Random Excursions	1000000	3	8	0.145246	3/3	PASS	-	-	PASS
16	Random Excursions Variant	1000000	3	18	0.036142	3/3	PASS	-	-	PASS

Demonstration (7nm)

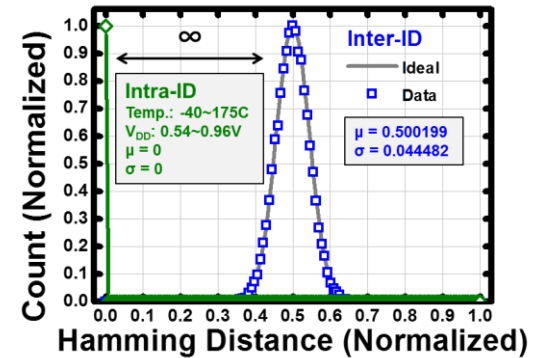
Randomness

HW=50%



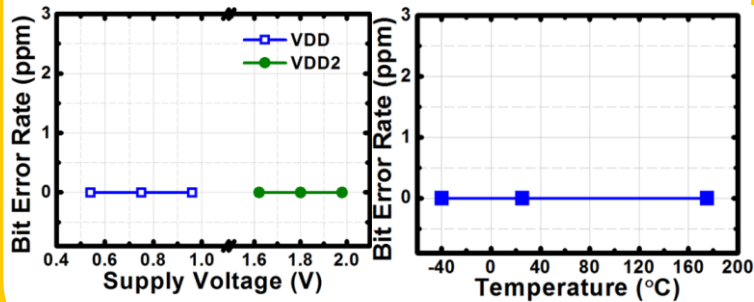
Uniqueness

$\mu_{\text{inter}} = 0.5$



Stability

$\mu_{\text{intra}} = 0$



Reliability

On-going

Randomness by NIST800-22

tsmc 7nm FinFET

- **NeoPUF in tsmc 7FF passed NIST800-22 statistics randomness test**

					Decision Rule				
Statistical Test	Recommended n	Input Size		Sub-Test #	Proportion		Uniformity		Randomness Judgement
	Length of bit string	n	bit stream(s)		mini	P/F	P-value of P-value > 0.0001	P/F	PASS/FAIL
Frequency	n>100	1050	30	1	29/30	PASS	0.534146	PASS	PASS
Block Frequence (m=128)	n>100	1050	30	1	28/30	PASS	0.468595	PASS	PASS
Cumulative sums - Forward	n>100	1050	30	1	30/30	PASS	0.804337	PASS	PASS
Cumulative sums - Reversed	n>100	1050	30	1	30/30	PASS	0.054199	PASS	PASS
Runs	n>100	1050	30	1	29/30	PASS	0.862344	PASS	PASS
Longest runs of ones	n>128	1050	30	1	30/30	PASS	0.299251	PASS	PASS
Spectral DFT	n>1000	1050	30	1	30/30	PASS	0.602458	PASS	PASS

Outline

01

力旺电子(eMemory)简介

02

NeoPUF芯片指纹技术介绍

03

NeoPUF 于IoT硬件安全应用

04

NeoPUF+OTP芯片防伪介绍

05

NeoPUF+OTP (IP)授权金计算之应用介绍

06

NeoPUF完美随机数数据演示

07

总结

Summary

- **NeoPUF is derived from NeoFuse, eMemory's OTP solution, with no additional masking layers needed beyond regular logic-based processes**
- **NeoPUF is demonstrated with ideal randomness, uniqueness, and robustness, immune from aging effects that plague other PUF solutions**
- **NeoFuse combined NeoPUF can provide an integrated macro with high secure OTP, inborn secure keys and TRNG for future IoT and security applications**
- **NeoPUF + OTP provide a new anti-clone function for IC & IP providers**

THANK YOU

Collaborate to
Reach the Summit

Embedded Wisely, Embedded Widely



emory@ememory.com.tw

ememory