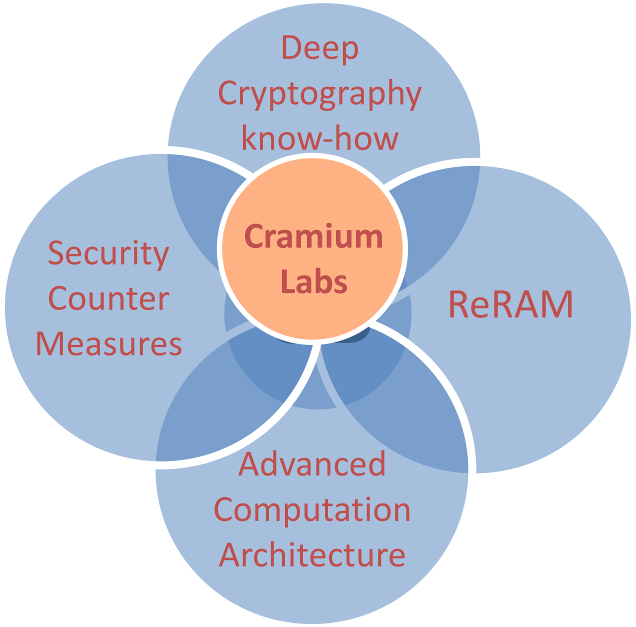
Secure Processing Unit

Cramium Labs

Cramium Labs Background

Company Overview

- A minority subsidiary of CrossBar Inc.
- CrossBar developed ReRAM and selector (1TnR high-density memory) technologies, enabling non-volatile memory storage to be embedded into any processor, microcontroller, FPGA, or as a standalone memory chip


Deep Cryptography know-how
Cramium Labs
Security Counter Measures
ReRAM
Advanced Computation Architecture

Technology Progress

- Authenticator IC production with ReRAM and PUF in 28nm
- Licensed ReRAM to Microchip
  - First silicon on 2Mbit ReRAM macro on 12nm FinFET in 1Q22
- More than 330 patents
- Top 20 semiconductor companies based on strength of patent portfolio - IEEE Spectrum (2016)

IEEE SPECTRUM

Backed by Reputable Financial and Strategic Investors

KLEINER PERKINS

MICROCHIP

CORRELATION VENTURES

ARTIMAN
WHITE SPACE INVESTMENTS

Lam RESEARCH

tao
capital partners

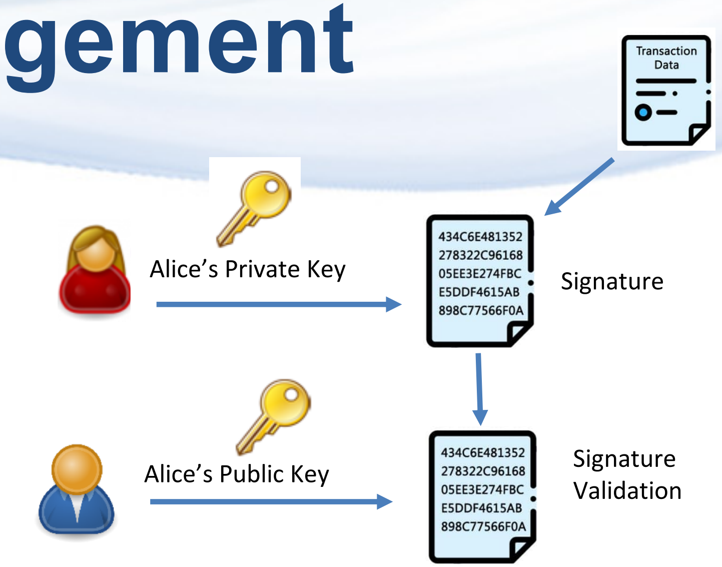
Korea Investment
Partners Co., Ltd.

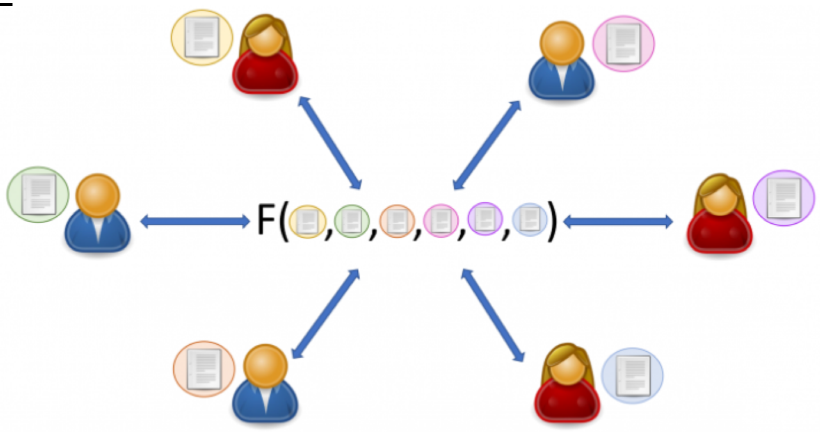
TYCHE PARTNERS
LP

TPK
touching tomorrow, today

Trend toward Distributed Key Management

- Commonly used **single key-pair** is not optimal
  - Created for a time when generating a key pair, generating a signature, and verifying a signature were all substantial compute tasks
  - Compute power no longer a limitation
  - Using a single private key is risky
- **Distributed Key Management** with **Threshold signatures** is the way of the future
  - Use of multiple devices/parties to manage loss, security, succession
  - System architectures for improved key management exist, however device and semiconductor support has been lacking so far
  - A highly performant and secure chip like Cramium SPU is well-suited for this purpose
- **Significant advantages**
  - Protection against theft/hacking
  - Protection against loss of "pin" or user error
  - Protection against interruption/succession problems



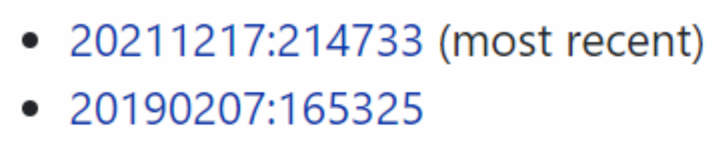


Multi-Party Computation (MPC) - Multiple party jointly come up with the same results w/o revealing secrets

Continuous Improvement of MPC Protocols

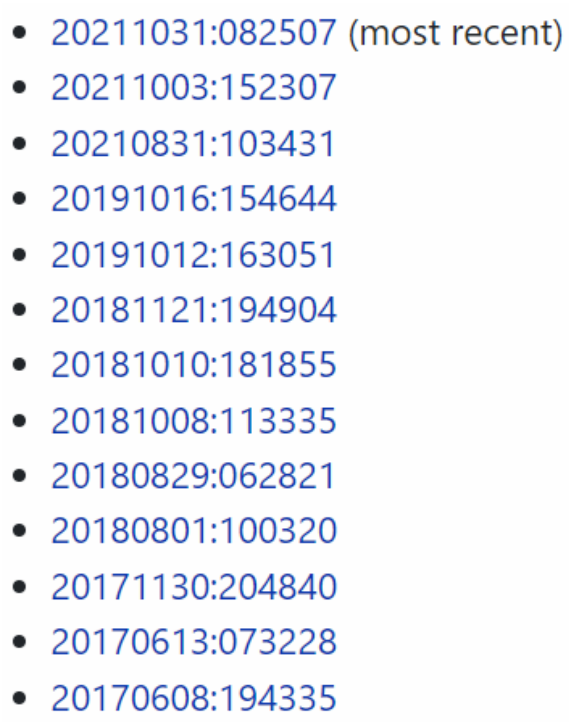
Revision history of major ECDSA MPC protocols

GG18 (https://eprint.iacr.org/2019/114)



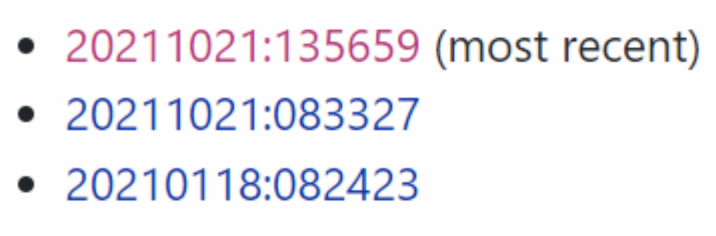
- 20211217:214733 (most recent)
- 20190207:165325

Lindell17 (https://eprint.iacr.org/2017/552)



- 20211031:082507 (most recent)
- 20211003:152307
- 20210831:103431
- 20191016:154644
- 20191012:163051
- 20181121:194904
- 20181010:181855
- 20181008:113335
- 20180829:062821
- 20180801:100320
- 20171130:204840
- 20170613:073228
- 20170608:194335

CGGMP21 (https://eprint.iacr.org/2021/060)



- 20211021:135659 (most recent)
- 20211021:083327
- 20210118:082423

- MPC protocols evolves continuously for improved security and performance

MPC - Key Generation

- SW-only based solution limits performance significantly

SW-only based solutions

CGGMP21 lib (https://github.com/taurusgroup/multi-party-sig)
5 round key generation with participant number = 4

	P0	P1	P2	P3
R1	2.42s	4.95s	4.07s	2.68s
R2	<1ms	<1ms	<1ms	<1ms
R3	2.18s	1.99s	720ms	2.08s
R4	<1ms	1.51ms	1.05ms	<1ms
R5	<1ms	<1ms	<1ms	<1ms

GG18 lib (https://github.com/bnb-chain/tss-lib)
4 round key generation with participant number = 4

	P0	P1	P2	P3
R1	14.41s	10.98s	10.56s	6.23s
R2	1.33s	1.34s	1.32s	1.35s
R3	22.33ms	25.18ms	25.43ms	23.56ms
R4	38.10ms	35.35ms	59.4ms	53.68ms

MPC - Key Generation Time Breakdown

CGGMP21

Paillier key generation & ZKP computation/verification take most time

Round 1	P0	P1	P2	P3
Paillier keygen	4.29s	3.61s	4.23s	5.19s
Pedersen parameters	12.8ms	22.4ms	11.9ms	12.9ms
ElGamal keygen	<1ms	23.5ms	<1ms	<1ms
VSS	<1ms	<1ms	<1ms	<1ms
Others (Schnorr random number etc)	<1ms	1.0ms	<1ms	<1ms
Round 1 total	4.31s	3.66s	4.24s	5.20s

Round 3	P0	P1	P2	P3
RID, other random number	<1ms	<1ms	<1ms	<1ms
Compute proof for well-formed Paillier key	1.43s	1.58s	1.97s	1.63s
Compute proof for correct Pedersen parameters	515ms	549ms	238ms	415ms
Paillier encryption of VSS shares	371ms	220ms	266ms	335ms
Round 3 total	2.31s	2.35s	2.47s	2.38s

MPC - Online Signing Time

CGGMP21

Verify – validate others ZKPs, commitments etc

Compute – compute ZKP, generates random numbers etc.

SW-only based solutions limit the scalability of MPC

unit: second

0 means <1ms

1-of-2

Round	P0	P1
R1 verify	NA	NA
R1 compute	0.141	0.131
R1 total	**0.141**	**0.131**
R2 verify	0.092	0.09
R2 compute	0.82	0.801
R2 total	**0.912**	**0.891**
R3 verify	0.463	0.458
R3 compute	0.071	0.072
R3 total	**0.534**	**0.53**
R4 verify	0.084	0.085
R4 compute	0	0
R4 total	**0.084**	**0.085**
R5 verify	0	0
R5 compute	0	0
R5 total	**0**	**0**
R1-5 total	**1.671**	**1.637**
Total*	**2.9 sec**	**2.9 sec**

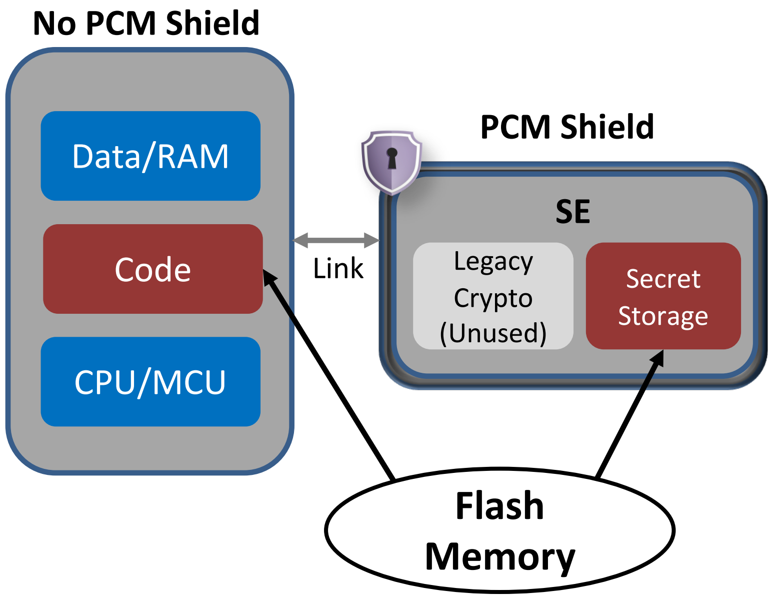
4-of-5

Round	P0	P1	P2	P3	P4
R1 verify	NA	NA	NA	NA	NA
R1 compute	0.684	0.826	0.706	0.677	0.665
R1 total	**0.684**	**0.826**	**0.706**	**0.677**	**0.665**
R2 verify	0.824	0.794	0.729	0.855	0.858
R2 compute	5.84	8.16	5.71	5.92	5.96
R2 total	**6.664**	**8.954**	**6.439**	**6.775**	**6.818**
R3 verify	4.097	3.533	4.166	4.134	4.138
R3 compute	0.206	0.32	0.269	0.273	0.183
R3 total	**4.303**	**3.853**	**4.435**	**4.407**	**4.321**
R4 verify	0.781	0.643	0.674	0.794	0.681
R4 compute	1	0	0	0	1
R4 total	**1.781**	**0.643**	**0.674**	**0.794**	**1.681**
R5 verify	0	0	0	0	0
R5 compute	0	0	0.005	0	0
R5 total	**0**	**0**	**0.005**	**0**	**0**
R1-5 total	**13.432**	**14.276**	**12.259**	**12.653**	**13.485**
Total*	**14.6 sec**	**14.6 sec**	**14.6 sec**	**14.6 sec**	**14.6 sec**

*Includes overhead such as goroutine synchronization, wait for other members to complete current round etc

Cold Storage for Crypto is “Broken”

- **Non-secure MCU works with discrete SE (Secure Element) over exposed bus**
- **Expensive due to lack of semiconductor industry support and integration**
  - A cold wallet can easily cost several hundred dollars
- **Rely on “off-the-shelf” semiconductor chips in addition to a SE**
  - Wrong cryptographic primitives, and fixed functionalities
  - Lack of “physical countermeasures” (PCM) shield
- **Based on traditional/controversial cryptography primitives**
  - Potential backdoors in NIST curves
- **Use non-secure, unreliable flash memory**
  - Susceptible to hardware hacking, vulnerable to harsh environment
  - Short shelf life (5-10 years max) due to discharge
- **Limited computational power and memory**
  - Use archaic single-key system
  - Cannot use sophisticated architectures such as multi-party computation (MPC)
- **Hard to setup/use and centralized security**
  - Steep learning curve, unforgiving product experience can trip up consumers by losing keys
  - SE requires strict NDA with proprietary/closed sources



Cramium SPU– A New Standard in Security

SPU is a crypto-native semiconductor chip that is developed from the ground-up for state-of-the-art security

✓ Next-Gen Memory (ReRAM)

- Replaces flash memory with ReRAM
- Much more secure
- Long lasting (>100 years)
- Integrates with advanced logic
- Large memory space

✓ Architecture

- Replacing multiple chips with a single SOC -> simple/cheap/small
- Single chip, no exposed buses
- Fully shielded with physical countermeasure (PCM)

✓ Open Development Kit (DevKit)

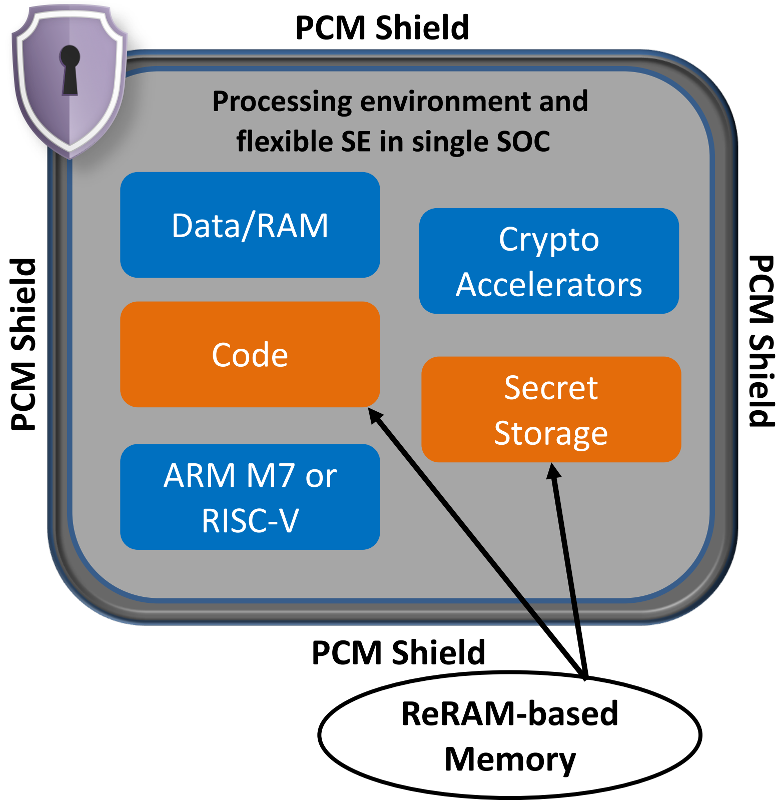
- Open-source software and DevKit
- Flexible “Super SE”

✓ Manufacturing

- Manufacturing by TSMC
- 22nm advanced process node
  - The most advanced node on security chip
- Attack-resistant, high performance
- Smaller die size and package - 7x7mm BGA
- Lower cost
- Lower power consumption

✓ Performance

- ARM Core M7 or RISC-V
- Accelerators orchestrated by powerful MCU
- Updated crypto accelerators implemented in silicon
  - secp256k1
  - Ed25519/Ristretto
  - BLS381
- Flexibility of SW with security of HW
- Multiple TRNG sources



Secure HW Acceleration and General Computing

HW acceleration (in 22nm) for general blockchain and emerging applications (e.g., MPC)

<u>Feature examples (non-exhaustive list)</u>

Public Key Crypto/Signature

ECC (ECDSA, Schnorr, EdDSA, curves - Secp256k1, Ed25519/Ristretto, P-256/384), RSA

Homomorphic Encryption

Paillier cryptosystem

Hash

RIPEMD160, SHA2, SHA3/Keccak, Blake2/3

Encryption

AES

Authentication, Key Derivation

HMAC, PBKDF2

Key Agreement

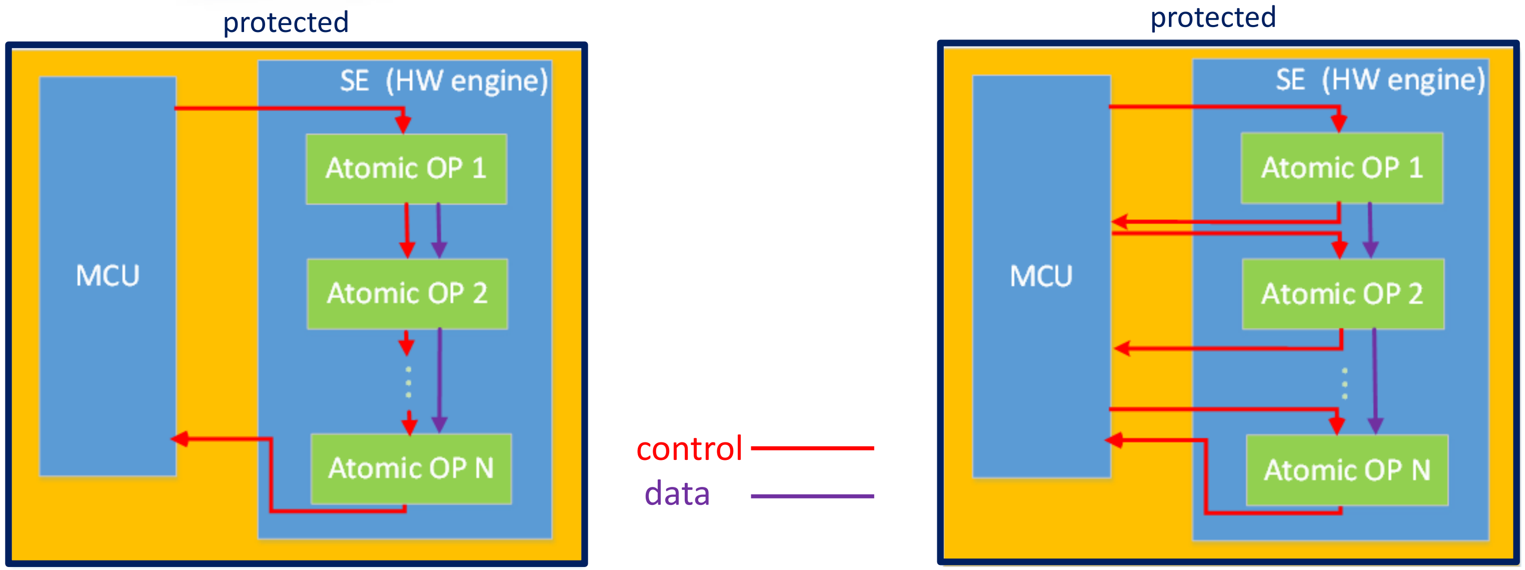
ECDH, X25519

ZKP Acceleration

Modulo operations

Security of Hardware Secure Element with Flexibility of Software

- SPU key slots can be designated to work in either of two modes



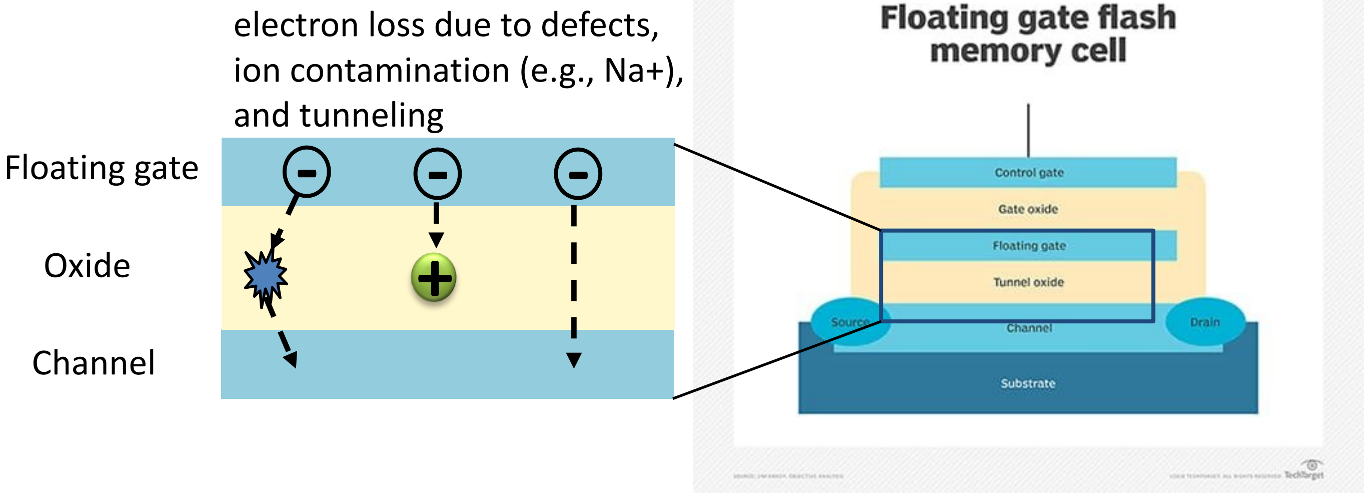
- Mode I
  - All work inside HW state machine
  - No visibility to M7 or AXI bus
  - This is similar to state-machine-based SE
- Mode II:
  - M7 can access accelerators, but handles intermediate product
  - Still under physical countermeasure shield
  - This is similar to core-based SE

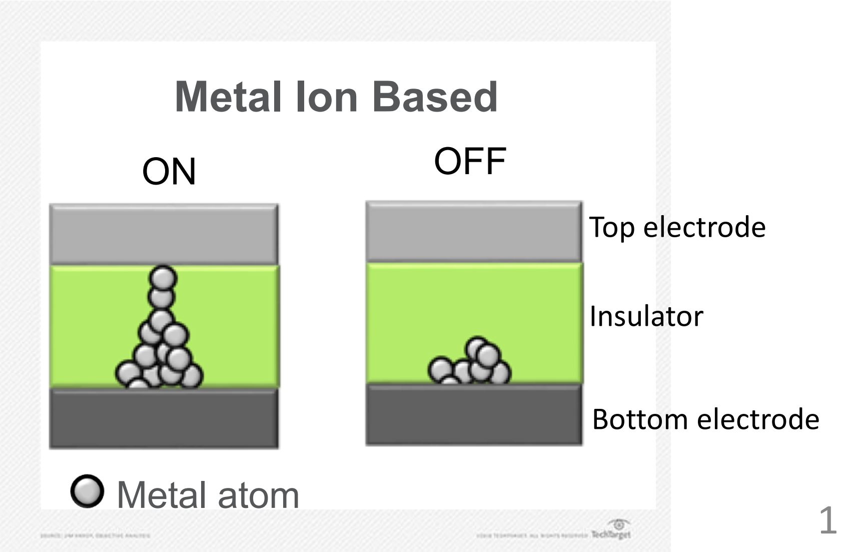
By providing both modes, SPU combines the security of HW-based SE with the flexibility of SW-based SE

ReRAM vs. Flash Memory

ReRAM is much better suited for NV storage in security hardware than the incumbent flash memory

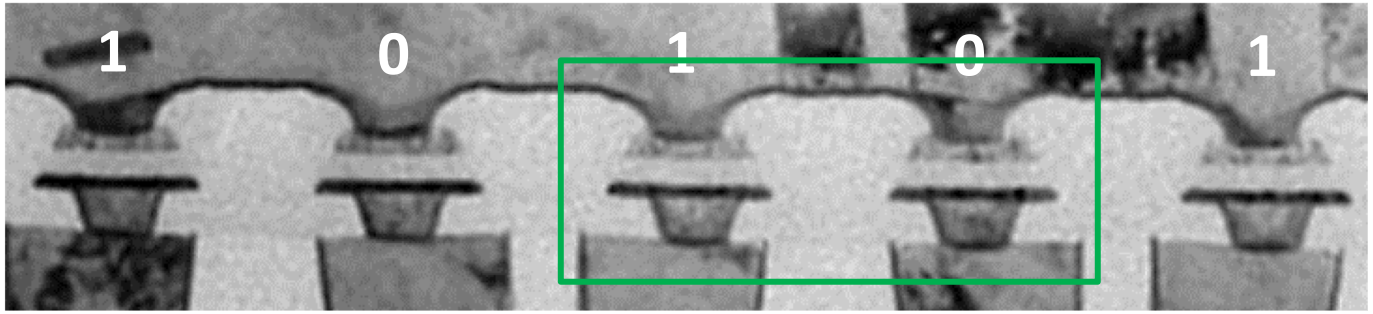
	Flash (Charge-Based)	ReRAM (Ion-based)
Security	✗ Vulnerable to optical attacks	✓ Cannot be read by physical means
Permanence	✗ Charge leaks continuously; unreliable and short-lived	✓ Metal-ion based, 100+ yrs shelf-life at room temperature
Integration	✗ Cannot be integrated with advanced logic below 28nm	✓ Can be integrated with advanced logic below 28nm


electron loss due to defects, ion contamination (e.g., Na+), and tunneling
Floating gate
Oxide
Channel
Floating gate flash memory cell
Control gate
Gate oxide
Floating gate
Tunnel oxide
Source
Channel
Drain
Substrate

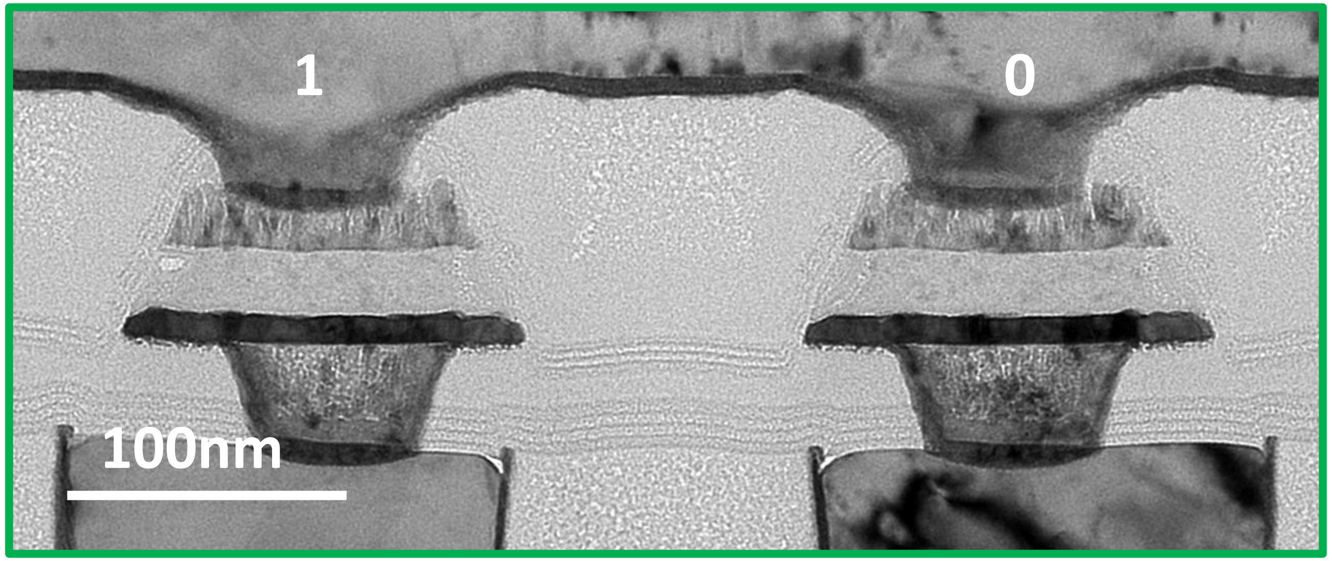


ReRAM – Against Invasive Attacks

- ReRAM utilizes inherently stochastic electro-chemical ionic movement
  - Invasive techniques (e.g. TEM) cannot effectively detect localized atomic level defects



PUF was programmed to 10101 and TEM was performed

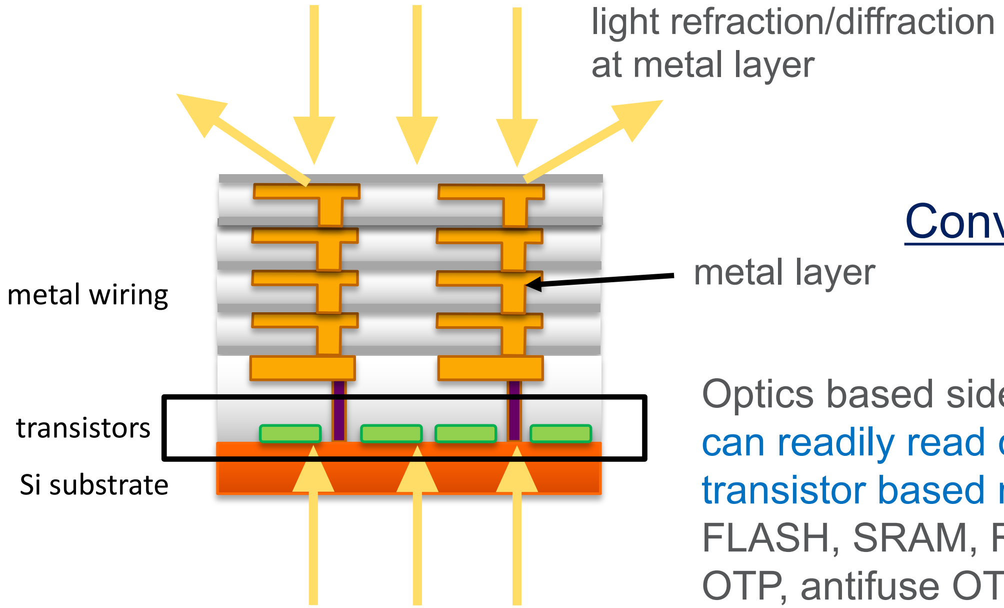


No difference found under TEM between 1 and 0 bits (tested over 100s of TEM trials)

ReRAM – Against Optical Attacks

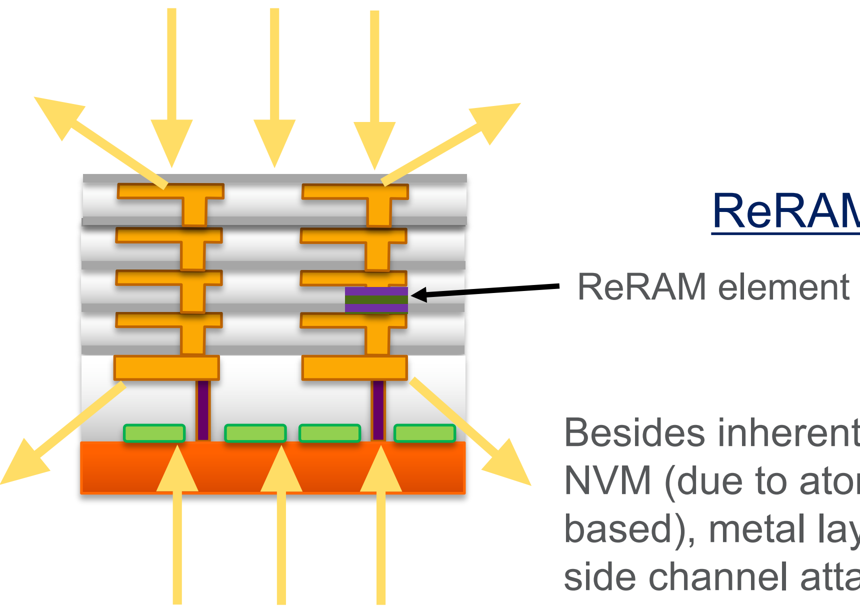
- Optics based side channel attacks (e.g. Photon Emission Analysis) are typically performed from the backside of a wafer
  - Light can easily go through Silicon substrate
- ReRAM is built in the middle metal layers ➔ fundamentally disabling attacks from wafer backside

Imaging attacks do not work



Conventional

Optics based side channel attacks can readily read contents of transistor based memory (e.g. FLASH, SRAM, ROM, floating-gate OTP, antifuse OTP)



ReRAM

Besides inherently being secure NVM (due to atomic-filament based), metal layers protect from side channel attacks further

Physical Countermeasure (PCM)

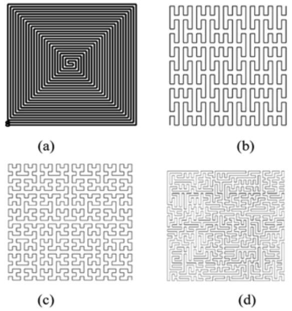
- PCM: deployed throughout the entire layout that protect a chip from invasive /physical attack.
- This protects the logic upon which all logical security relies.

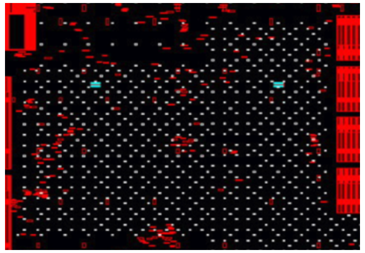
1. Physical Attacks (fib, probe, etc).

- Active Shield
- Security layout (redundant lines, dummy lines)
- Security Design (self-check, dynamic logic)

2. Fault Injection (laser, clock glitch, voltage glitch, EM/radiation, thermal)

- Glue Logic design (error coding, register mirror, write verify)
- Glue Cells (trigger cells) throughout chip
- Isolated clock
- Detectors (voltage, light...)



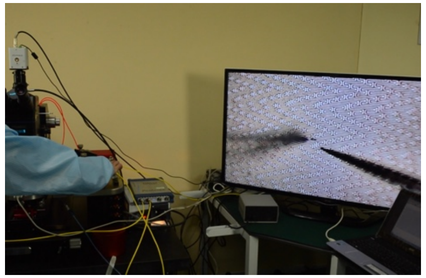


3. Side Channel (SPA, DPA, EM, ...)

- Algorithmic and implementation countermeasures
- Walkaround countermeasures (false operation, clock jitter, power balancing)

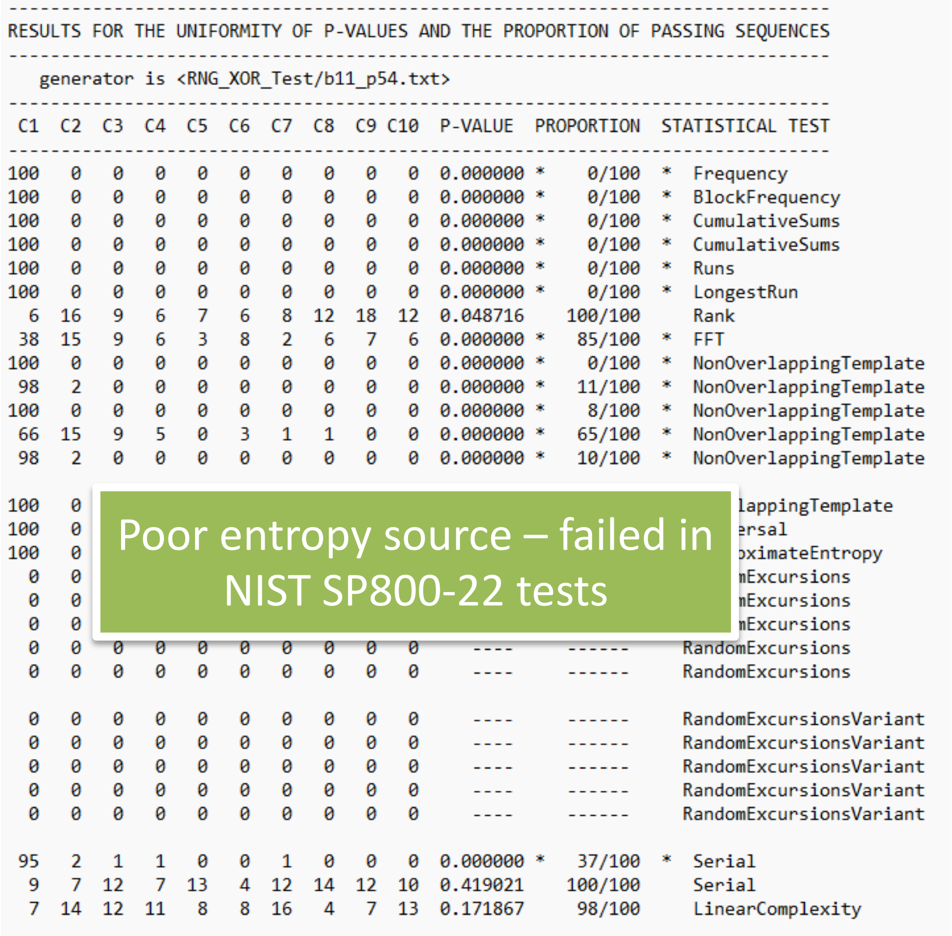
4. Other

- Strong/redundant lifecycle protection
- Multi-stage secure boot, multi-signature
- Memory protection (access control, encryption)
- Strong TRNG (multiple, self-checking)



TRNG – Multiple Entropy Sources

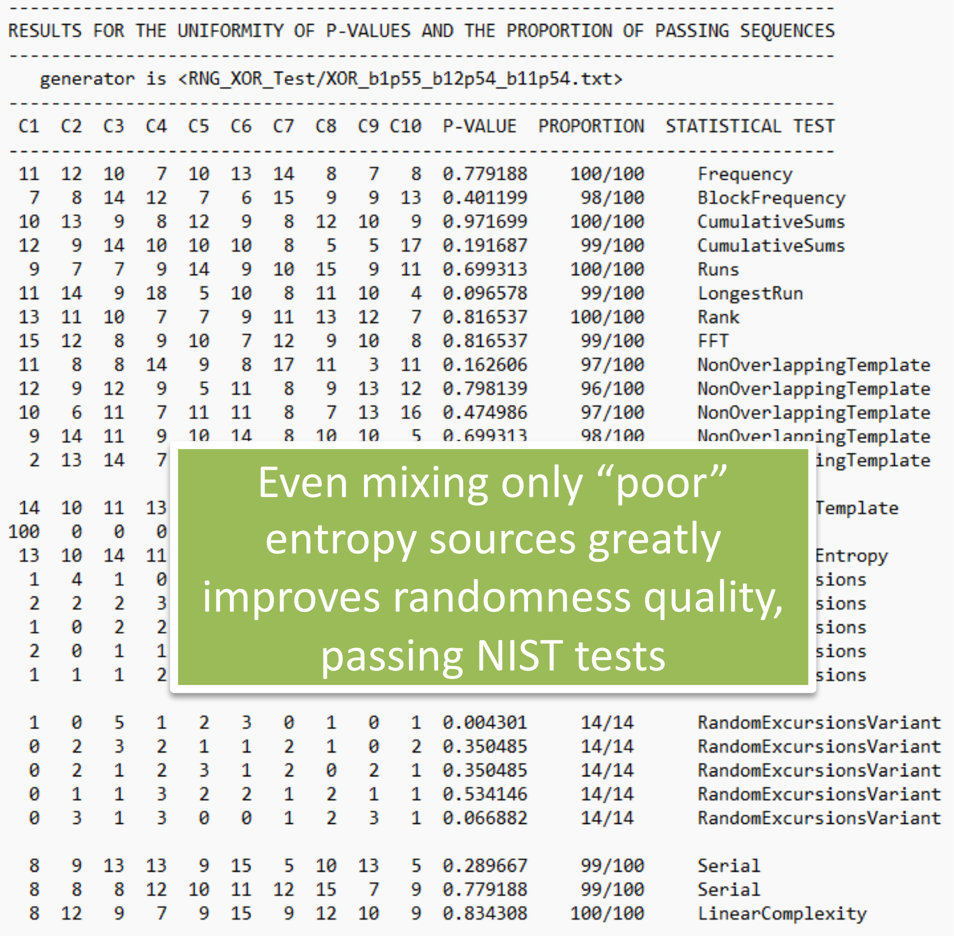
- TRNG is critical for the security of various cryptography primitives
- Cramium SPU provides multiple independent high quality entropy sources and an option to use external entropy source



```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <RNG_XOR_Test/b11_p54.txt>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
100   0   0   0   0   0   0   0   0   0  0.000000 *    0/100  *  Frequency
100   0   0   0   0   0   0   0   0   0  0.000000 *    0/100  *  BlockFrequency
100   0   0   0   0   0   0   0   0   0  0.000000 *    0/100  *  CumulativeSums
100   0   0   0   0   0   0   0   0   0  0.000000 *    0/100  *  CumulativeSums
100   0   0   0   0   0   0   0   0   0  0.000000 *    0/100  *  Runs
100   0   0   0   0   0   0   0   0   0  0.000000 *    0/100  *  LongestRun
  6  16   9   6   7   6   8  12  18  12  0.048716    100/100     Rank
 38  15   9   6   3   8   2   6   7   6  0.000000 *   85/100  *  FFT
100   0   0   0   0   0   0   0   0   0  0.000000 *    0/100  *  NonOverlappingTemplate
 98   2   0   0   0   0   0   0   0   0  0.000000 *   11/100  *  NonOverlappingTemplate
100   0   0   0   0   0   0   0   0   0  0.000000 *    8/100  *  NonOverlappingTemplate
 66  15   9   5   0   3   1   1   0   0  0.000000 *   65/100  *  NonOverlappingTemplate
 98   2   0   0   0   0   0   0   0   0  0.000000 *   10/100  *  NonOverlappingTemplate

100   0                                                          lappingTemplate
100   0                                                          ersal
100   0                                                          oximateEntropy
  0   0                                                          mExcursions
  0   0                                                          mExcursions
  0   0                                                          mExcursions
  0   0   0   0   0   0   0   0   0   0      ----      ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0      ----      ------    RandomExcursions

  0   0   0   0   0   0   0   0   0   0      ----      ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0      ----      ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0      ----      ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0      ----      ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0      ----      ------    RandomExcursionsVariant

 95   2   1   1   0   0   1   0   0   0  0.000000 *   37/100  *  Serial
  9   7  12   7  13   4  12  14  12  10  0.419021    100/100     Serial
  7  14  12  11   8   8  16   4   7  13  0.171867     98/100     LinearComplexity
```

Poor entropy source – failed in NIST SP800-22 tests

Mixing multiple entropy sources

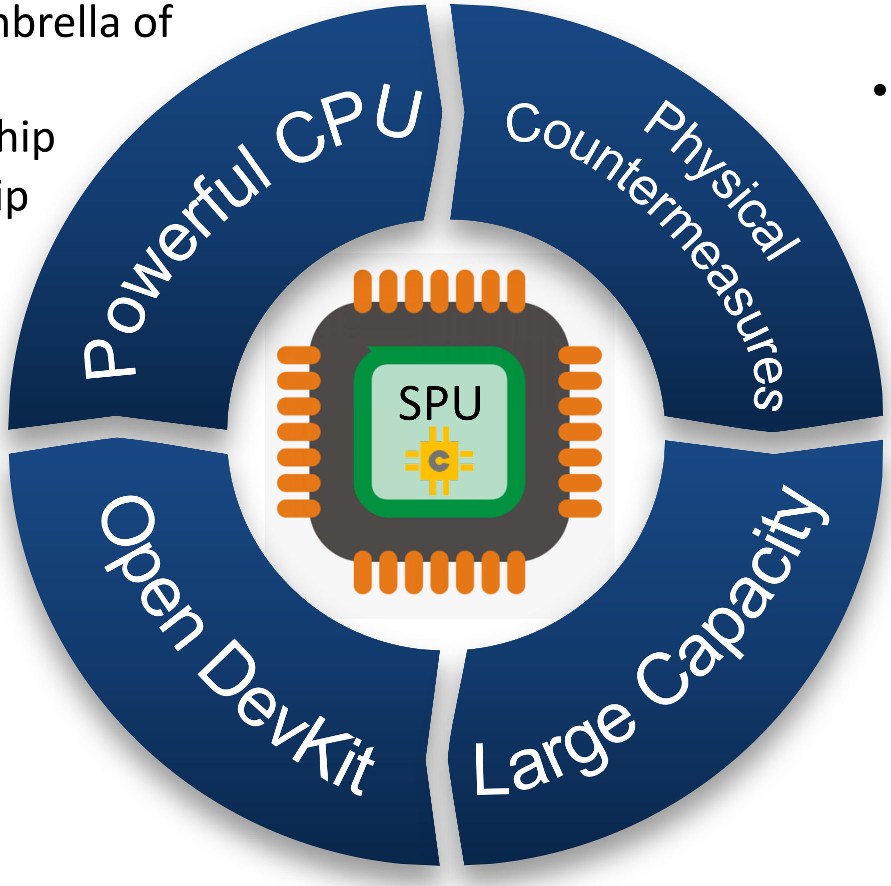


```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <RNG_XOR_Test/XOR_b1p55_b12p54_b11p54.txt>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
 11  12  10   7  10  13  14   8   7   8  0.779188    100/100     Frequency
  7   8  14  12   7   6  15   9   9  13  0.401199     98/100     BlockFrequency
 10  13   9   8  12   9   8  12  10   9  0.971699    100/100     CumulativeSums
 12   9  14  10  10  10   8   5   5  17  0.191687     99/100     CumulativeSums
  9   7   7   9  14   9  10  15   9  11  0.699313    100/100     Runs
 11  14   9  18   5  10   8  11  10   4  0.096578     99/100     LongestRun
 13  11  10   7   7   9  11  13  12   7  0.816537    100/100     Rank
 15  12   8   9  10   7  12   9  10   8  0.816537     99/100     FFT
 11   8   8  14   9   8  17  11   3  11  0.162606     97/100     NonOverlappingTemplate
 12   9  12   9   5  11   8   9  13  12  0.798139     96/100     NonOverlappingTemplate
 10   6  11   7  11  11   8   7  13  16  0.474986     97/100     NonOverlappingTemplate
  9  14  11   9  10  14   8  10  10   5  0.699313     98/100     NonOverlappingTemplate
  2  13  14   7                                                    ingTemplate

 14  10  11  13                                                    Template
100   0   0   0
 13  10  14  11                                                    Entropy
  1   4   1   0                                                    sions
  2   2   2   3                                                    sions
  1   0   2   2                                                    sions
  2   0   1   1                                                    sions
  1   1   1   2                                                    sions

  1   0   5   1   2   3   0   1   0   1  0.004301     14/14      RandomExcursionsVariant
  0   2   3   2   1   1   2   1   0   2  0.350485     14/14      RandomExcursionsVariant
  0   2   1   2   3   1   2   0   2   1  0.350485     14/14      RandomExcursionsVariant
  0   1   1   3   2   2   1   2   1   1  0.534146     14/14      RandomExcursionsVariant
  0   3   1   3   0   0   1   2   3   1  0.066882     14/14      RandomExcursionsVariant

  8   9  13  13   9  15   5  10  13   5  0.289667     99/100     Serial
  8   8   8  12  10  11  12  15   7   9  0.779188     99/100     Serial
  8  12   9   7   9  15   9  12  10   9  0.834308    100/100     LinearComplexity
```

Even mixing only “poor” entropy sources greatly improves randomness quality, passing NIST tests

Summary

SPU provides a flexible, programmable platform with substantial computing power and large storage for any Distributed Key Management architecture and general secure embedded computing



- All operation under umbrella of PCM
- Fast MPC support on chip
- Complex signing on chip

- Security levels commensurate with enterprise-level requirements

- Customizable security solutions

- Larger storage for keys and code than any SE

Questions & Suggestions?

- Any functionalities/crypto primitives you want us to implement?

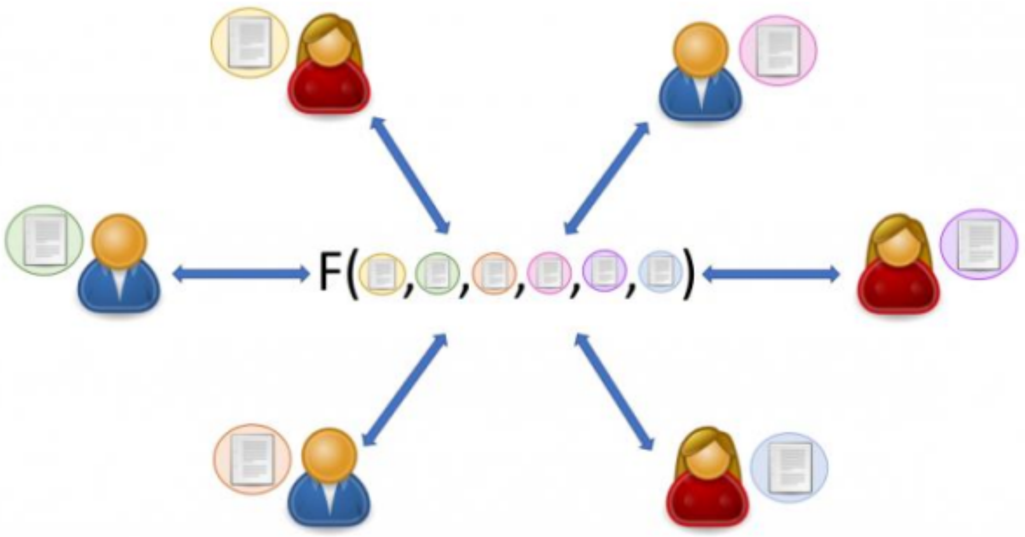
Thank You

info@cramiumlabs.com

Backup

Secure Multi-Party Computation (MPC)

- MPC protocols enable mutually-distrusting parties to jointly perform a computation without revealing any party's secret
  - Benefits for digital asset applications: distributed key generation/management, protection against theft/hacking, no single point of failure
- However, MPC is typically deployed in enterprise level (e.g., work stations and servers) due to heavy computation requirement



Multiple party jointly come up with the same verifiable results (image from esat.kuleuven.be)

ECDSA MPC Building Blocks – HW Acceleration

- Secret sharing & commitment schemes → SPU HW accelerated
  - VSS, (often) Pedersen’s commitment scheme
- Additively homomorphic encryption
  - Paillier cryptosystem → SPU HW accelerated
- Zero Knowledge Proof (ZKP) or Proof of Knowledge
  - Sigma Protocol (interactive) or Fiat-Shamir heuristic (non-interactive): single secret and/or batched version. Examples:
    - Proof of knowledge on secrets/shares claimed
    - Range proof for Paillier key, message, nonce → SPU HW accelerated
    - Proof for well-formed Paillier

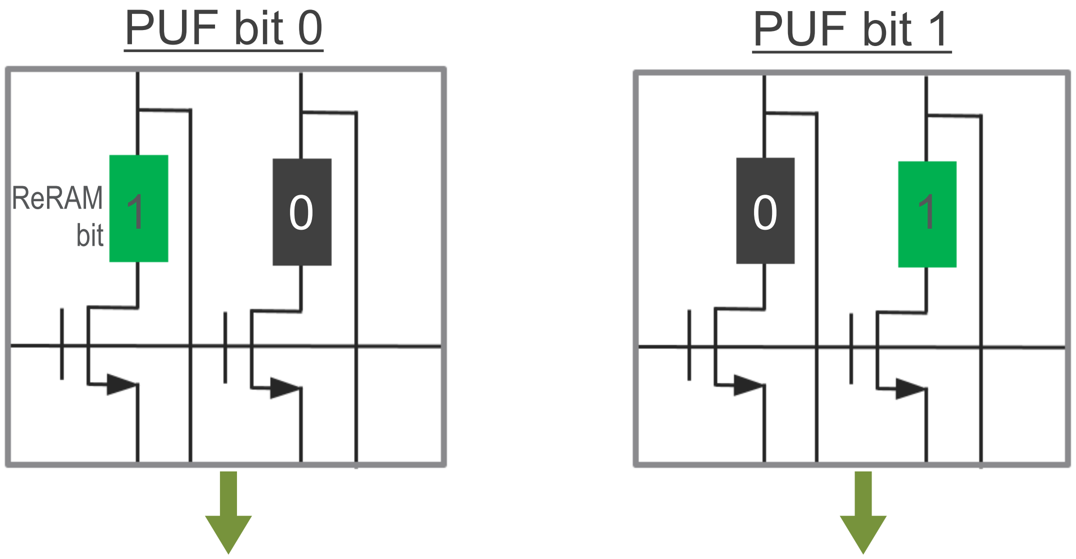
ReRAM PUF - Randomness

- Tested over 50 dies (> 100Mb) produced in 28nm production line
- Passed all 15 randomness tests (NIST SP 800-22)

NIST SP 800-22 STATISTICAL TEST		P-VALUE & CONCLUSION			
		@ -40°C	@ 25°C	@ 125°C	Randomness Test
1	Frequency	0.55454	0.34887	0.95901	All Passed
2	BlockFrequency	0.69315	0.35536	0.68087	All Passed
3	CumulativeSums	0.59252	0.85471	0.65172	All Passed
4	Runs	0.97820	0.30119	0.77590	All Passed
5	LongestRun	0.55609	0.85800	0.59172	All Passed
6	Rank	0.59498	0.71568	0.48466	All Passed
7	FFT	0.61093	0.72583	0.37018	All Passed
8	NonOverlappingTemplate	0.45598	0.57902	0.73444	All Passed
9	Serial	0.06801	0.69314	0.37313	All Passed
10	OverlappingTemplate	0.30283	0.94631	0.08016	All Passed
11	Universal	0.61906	0.45594	0.62797	All Passed
12	ApproximateEntropy	0.35805	0.49439	0.58487	All Passed
13	LinearComplexity	0.52631	0.21331	0.74771	All Passed
14	RandomExcursions	0.72034	0.14126	0.54795	All Passed
15	RandomExcursionsVariant	0.16661	0.01791	0.08311	All Passed

ReRAM PUF – Against Power Analysis Attacks

- Fundamental safeguard against power analysis is to have CONSTANT power consumption regardless of PUF bit states
  - Furthermore, low current read (~uA) is beyond power analysis resolution
- Voltage differential ReRAM PUF allows complementary read (= constant power), mitigating power analysis attack



Constant current/power consumption regardless of PUF bit state w/o compromising fast sensing speed