FERNS

Fingerprint Extraction and Random Numbers in SRAM

Wayne Burleson, Kevin Fu, Dan Holcomb (UMass Amherst) `rfid-cusp.org`

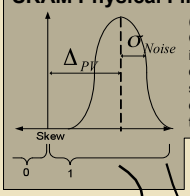
Problem: Identification (ID) and True Random Number Generation (TRNG) under constraints

- •Area Constraint (minimize cost)
- •Power Constraint (passive supply)

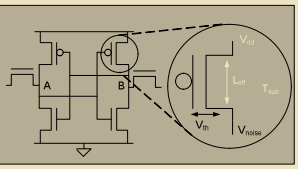
Solution: Use SRAM physical fingerprints for **both** ID and TRNG

- •No area overhead - reuse existing CMOS circuitry
- •Fingerprints generated by passive devices - power up before use

SRAM Physical Fingerprints:



(Right) Random threshold assignment in CMOS circuits gives each SRAM cell an inherent skew toward powering up to the 0 or the 1 state. Noise causes skew to deviate slightly from the inherent skew. (Left) If the distribution crosses the solid vertical bar, then the cell can power up to either state

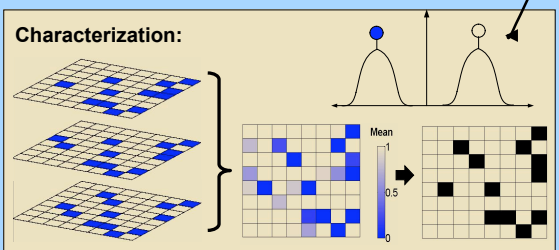


SRAM cells with large inherent skew power up to an identifying state

SRAM cells with small inherent skew power up to a random state and can be used for TRNG

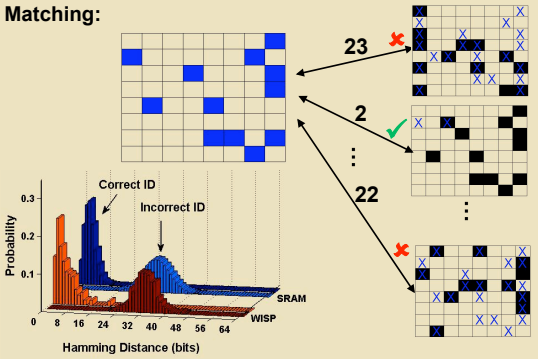
ID

Characterization:



The identity of each chip is learned by collecting multiple fingerprints from the chip and finding the tendency of each bit.

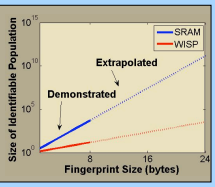
Matching:



Fingerprints are identified using Hamming Distance match against known fingerprint identities. The closest match is the identity.

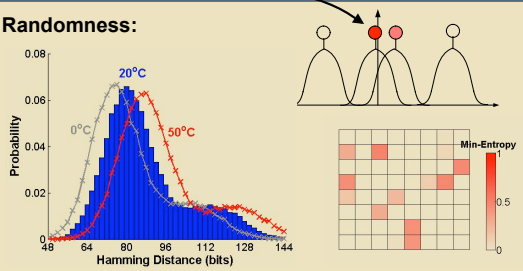
Results:

- •100% reliable ID using 64 bit fingerprints
- •Population of 5,120 SRAM virtual chips
- •Population of 15 virtual WISPs (Intel Research)
  - •Passively powered UHF RFID device



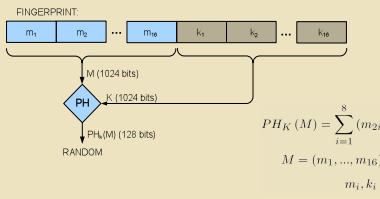
TRNG

Randomness:



(Left) 256 byte fingerprints from the same chip are practically unique. (Right) Min-entropy describes the amount of information contained in the most likely initial state of each bit. We measure an average of 0.05 bits of min-entropy per bit of SRAM.

Extraction:



$$PH_K(M) = \sum_{i=1}^{8} (m_{2i-1} + k_{2i-1})(m_{2i} + k_{2i})$$

$$M = (m_1, ..., m_{16}) \quad K = (k_1, ..., k_{16})$$

$$m_i, k_i \in GF(2)$$

The PH universal hash function is used as a randomness extractor. Both key and message come from the fingerprint. PH is designed for low hardware cost.

Results:

- •Closest match between 256 byte fingerprints was 45 bits (>10^6 comparisons)
- •128 bit random numbers extracted from 256 byte SRAMs (25k numbers)
  - •No specialized hardware
  - •Passes NIST approximate entropy test

dataset	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	PVAL	PROP
Raw	24523	244	76	75	34	19	10	14	4	1	0.0000	.0706
Extracted	2661	2614	2557	2590	2499	2526	2589	2570	2407	2487	0.0282	.9889

References

"Initial SRAM state as a fingerprint and source of true random numbers for RFID tags." RFID Security 2007. *D. Holcomb, W. P. Burleson, and K. Fu*
"Universal hash functions for emerging ultra-low-power networks." CNDS 2004. *K. Yuksel, J. P. Kaps and B. Sunar*
"Design of a passively-powered, programmable platform for UHF RFID systems." IEEE RFID 2007. *A. P. Sample, D. J. Yeager, P. S. Powledge, and J. R. Smith*
"A wirelessly-powered platform for sensing and computation." Ubicomp 2006. *J. R. Smith, A. Sample, P. Powledge, S. Roy, and A. Mamishev*

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
January 28-30, 2006
Atlanta, Georgia