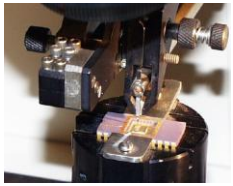
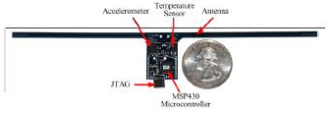
UMassAmherst

Hardware Security in Nanometer CMOS

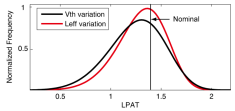
Prof. Wayne Burleson
Department of Electrical and Computer Engineering
University of Massachusetts Amherst
burleson@ecs.umass.edu
(visiting EPFL 2010-2011)

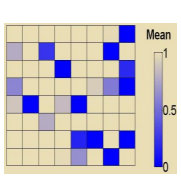
Implementation

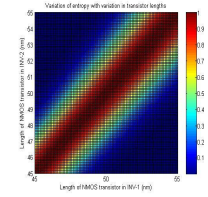




Analysis







Applications

Who am I?

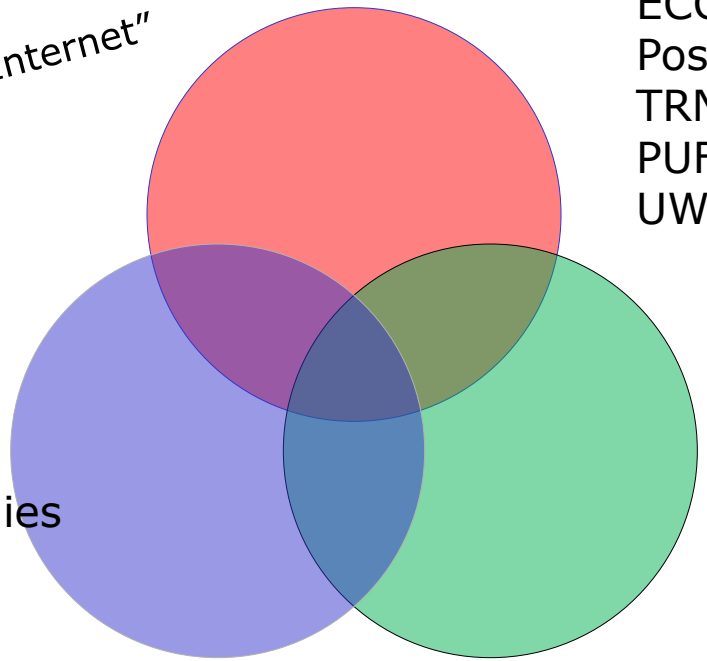
burleson@ecs.umass.edu

- VLSI Designer/Consultant
- I teach VLSI Design, Embedded Systems and most recently, Security Engineering
- I lead research on VLSI Circuits
  - Low-power and Side-channels (NSF)
  - Interconnects (SRC, Intel)
  - Clocking and Interfaces (NSF and Intel)
  - On-Chip Sensors (NSF, SRC)
  - SRAM (Intel, NSF)
  - Soft-errors (Sharp, Intel)
  - Thermal Sensing and Management (SRC, AMD)
- and VLSI Architecture, DSP, Arithmetic, Systems
  - Adaptive SOC (NSF)
  - On-chip Monitor NOC (SRC)
  - Video, 3D Graphics, DSP(NSF)
  - Crypto, Embedded Security (NSF, CISCO, Crypto Research)

Recent Projects in Nanometer CMOS Design
(funded by SRC, Intel, AMD, CRI, NSF)

- Ultra low-power CMOS design
  - Sub-threshold CMOS circuits
  - Intermittently powered devices (e.g. RFID)
  - Ultra lightweight Chip ID and True Random Number Generation
- Side-channel tolerant cryptographic hardware
  - Differential logic styles
  - Randomness insertion and data hiding
- On-Chip monitors for introspective run-time computing
  - Multi-core Monitor Network on Chip
  - Control and adaptation mechanisms in the presence of workload, power, thermal, reliability, and wear-out variations.
  - Intrusion and anomaly detection
- Thermal issues in mobile devices
  - Thermal management
  - Thermal sensing and calibration
- On-chip signaling for Multi-cores
  - Current-mode, Differential, NOC
  - Alternative signaling: PWM, CDMA
- High-performance clocking systems
  - Clocking in 3D processors
  - Jitter modeling and optimization

Hardware security = lightweight, embedded, EE



Crypto Implementations:

Block and Stream Ciphers
ECC
Post-Quantum Crypto
TRNG
PUF
UWB

Applications:

Transportation
Commerce
Assistive Technologies
Supply Chain
Pharmaceutical
Medical Devices

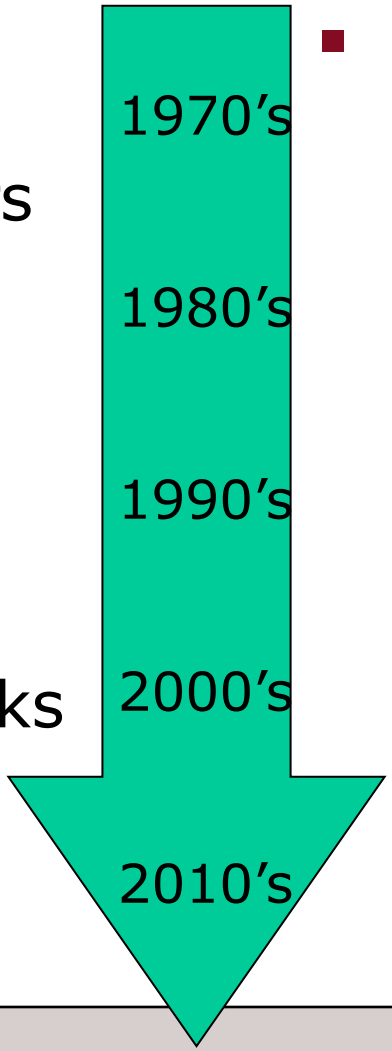
Threat Models:

Side-channels:
- Power
- Electromagnetics
- Fault Injection

Eavesdropping
Jamming/DoS
Power Depletion
Thermal Virus
Trojans

Trends in VLSI Research

- Driving Applications
  - Microprocessors
  - DSP
  - Video
  - Wireless
  - Hand-sets
  - Smart Cards
  - Sensor Networks
  - **RFID**
  - **Smart Dust**
  - …

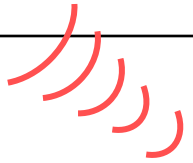


- Design Challenges
  - Area
  - Performance
  - Complexity
  - Test/Yield
  - Power
  - Flexibility
  - Reliability
    - Process
    - Voltage
    - Temperature
  - **Security/Privacy**

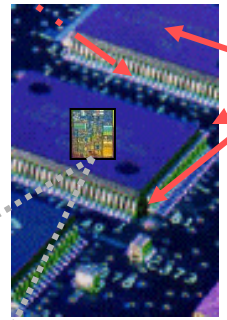
Attacks on Embedded Systems (Gogniat, Bossuet)

Remote attacks

Worm, virus, Trojan, tracking, etc.



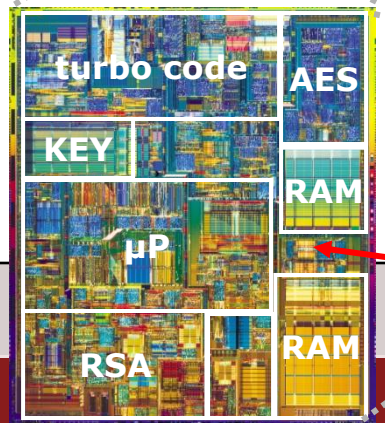
Proximity-based
Passive Hardware attacks
Power or EM analysis



Reversible active
proximity-based attacks

Fault injection

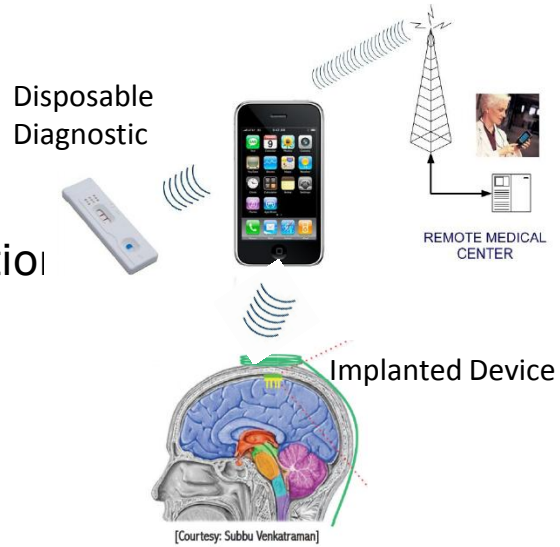
Eavesdropping



Irreversible
hardware attacks
Tampering

Some Motivating Applications

- **Secure Bio-sensor**
  - Motivations: Functions, Threats, Constraints
  - Solutions: NFC, EPC-C1-G2, PRESENT, PUF
  - Challenges, Development, Deployment/Evaluatio
  - Extensions and Future Enhancements



- **Privacy-Preserving Transportation Payments**
  - Motivations: Functions, Threats, Constraints
  - Solutions: E-Cash, Dynamic Pseudonyms, K-UWB, TRNG
  - Challenges, Development, Deployment/Evaluation
  - Extensions and Future Enhancements

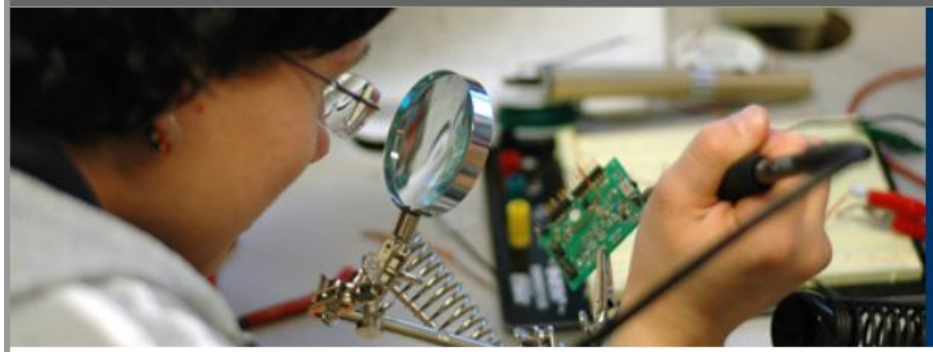
Doesn't the mobile phone solve all of our problems?

- Advantages
  - Computational power (multi-core, Ghz, RISC, DSP, accelerators,…)
  - Familiar interface
  - Widely deployed
  - Large battery
  - Numerous communication interfaces (GSM, WiFi, Bluetooth, NFC, GPS,…)
  - Already contains Trusted Platform Module (TPM), SIM and other robust security primitives.
  - Reliable, compact, robust
  - Trusted brands and service providers (and deep-pocketed…)
- Disadvantages
  - Complex, multi-function system (Swiss Army knife for security?)
    - Very hard to analyze & make security guarantees
  - Lots to go wrong: battery, wearout, software bugs, insider threats, etc.
  - Single point of failure, vulnerability: theft, loss,

rfid-cusp.org

RFID
Consortium for Security and Privacy

HOME | PEOPLE | BLOG | NEWS | PUBLICATIONS | PARTNERS | SPONSORS | CONTACT



OUR MISSION

RFID CUSP is a partnership between academic and industrial scientists specializing in RFID security and privacy. Our mission is to make RFID safe for consumers by conducting open research and educating the next generation work force that will develop, deploy and maintain secure RFID infrastructures.

Three principles of data security guide our research.

Planning ahead: Good security is built in, not bolted on. The Internet has taught a key lesson: It is less costly to anticipate threats and to secure systems from the start than to patch after the fact.

Open design: Public scrutiny usually breeds stronger systems than private finger-crossing. Openness has long been a cardinal rule of cryptography and a pillar of secure system design. Similarly, responsible disclosure of vulnerabilities holds the technology industry to high standards and brings vital education to the community.

Thinking holistically: Well conceived goals beget well conceived solutions. Thorough understanding of the uses and abuses of a system is the first step toward economical and effective security.

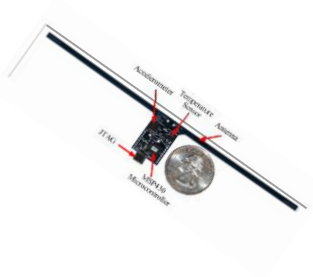
NEWS/EVENTS

RFIDSec Workshop
June 2011:
UMass Amherst will host the 2011 RFIDSec Workshop June 26-28, 2011. This event represents the first time that RFIDSec will be held in the United States.

WISP Summit
November 2009:
RFID CUSP researchers co-chair the WISP Summit at Intel Research on wirelessly powered sensor networks and computational RFIDs.

Archive >

BLOG



Some of our recent work (2007-2011)

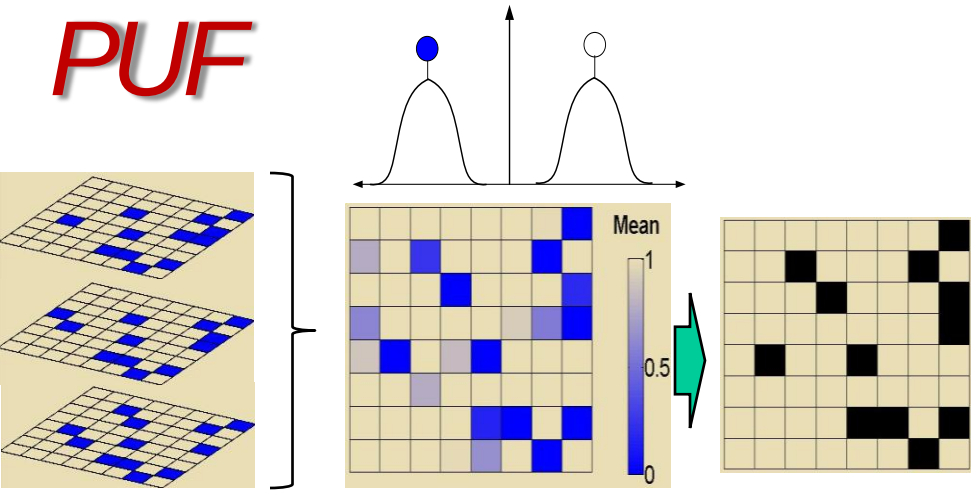
- Crypto Primitives
  - SRAM-based TRNG and Chip ID
  - Metastability-based TRNG (w/ Intel and TU Darmstadt)
  - Physical Unclonable Functions (PUF) in Sub-th CMOS (w/ Berkeley and TU Munich)

Image from www.verayo.com

- Attacks
  - Leakage-based side-channel analysis
  - Process variation impacts on side-channel attacks (w/ UCL)
  - Hardware Trojans using side-channels (w/ Bochum, CRI)
- Alternative Countermeasures
  - On-chip sensors and surveillance (w/ SRC)
  - Ultra wide-band for low-power security (w/ RSA and Stanford)
- Validation:
  - Test chip in 45nm SOI (w/ IBM)
  - Secure RFID Sensing on FPGA (w/ Intel and Bochum)

Chip ID and Random Numbers from SRAM Power-Up State

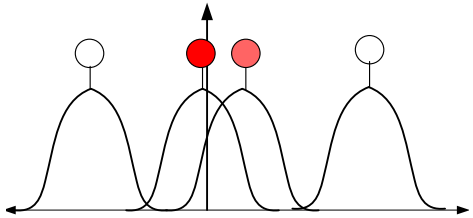
PUF

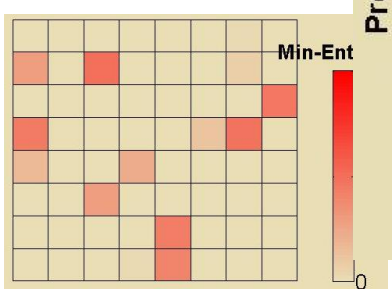


Harvest process variation in SRAMs for chip identification

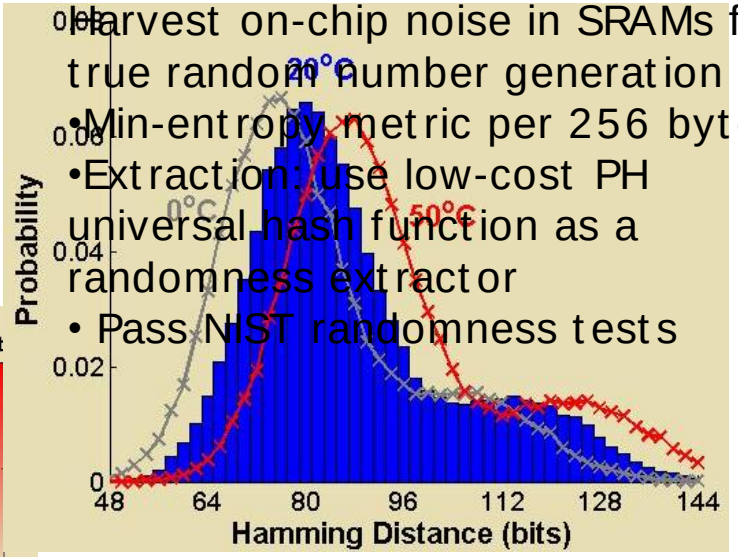
- Match: Hamming Distance match against known fingerprint identities
- Reliable ID using 64 bit fingerprints (> 19 bits in Hamming distance)

RNG

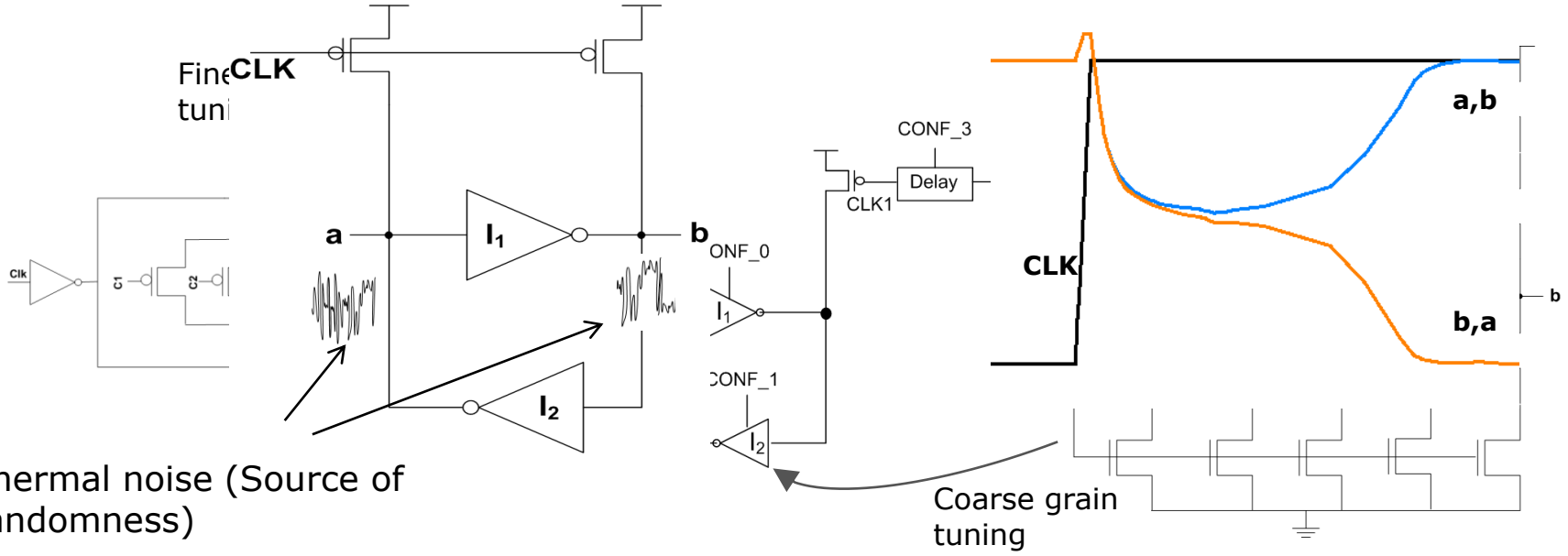




- Harvest on-chip noise in SRAMs for true random number generation
- Min-entropy metric per 256 bytes
- Extraction: use low-cost PH universal hash function as a randomness extractor
- Pass NIST randomness tests



Meta-stable True Random Number Generator (TRNG)



- Meta-stable circuits allow very lightweight TRNG circuits for RFID, smart cards, sensor nodes…
- But process variations introduce TRNG bias.
- Circuit-level calibration techniques can partially remove bias.

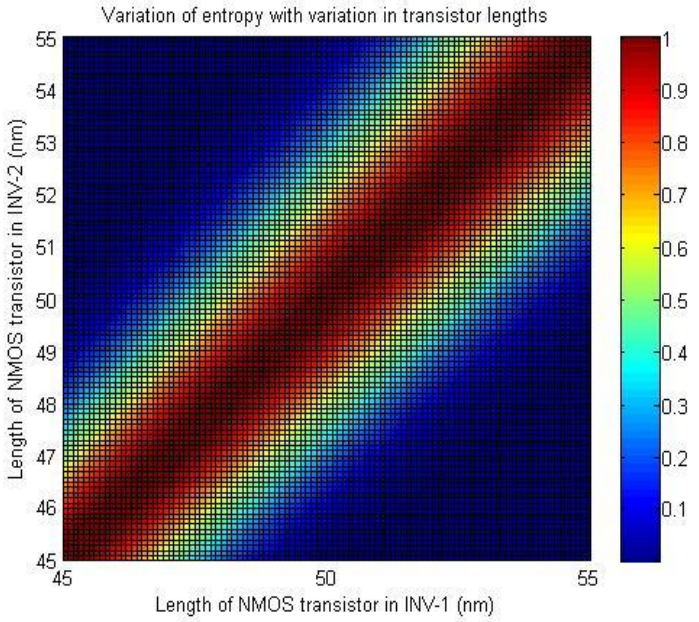
- **But when should calibration occur? And by whom?**

•S.Srinivasan*(Intel)*, **2.4GHz,7mW All-Digital,PVT-VariationTolerant TRNG in 45nm CMOS**,VLSI Circuits 2010
• V.Suresh and W.Burleson, **Entropy Extraction in Metastability-based TRNG**, HOST 2010

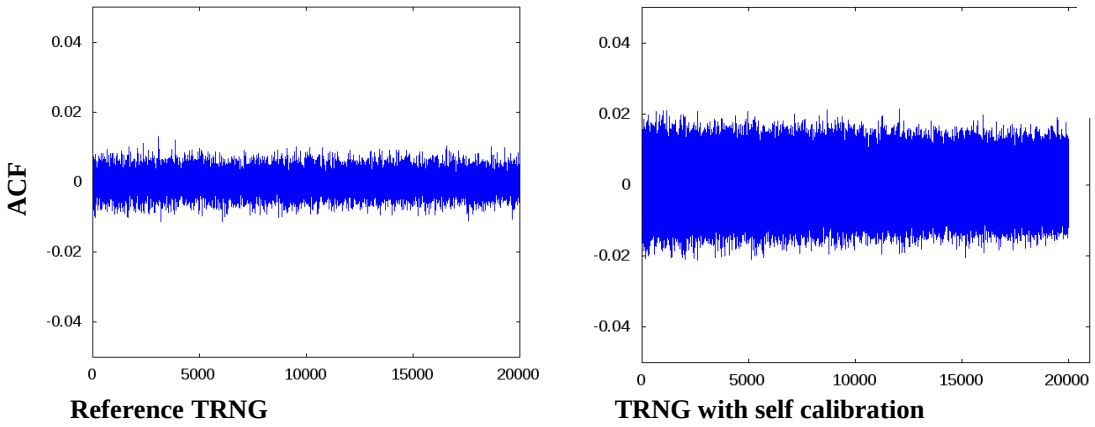
Entropy variation with transistor mis-match

Mean = $\left(\sqrt{\frac{\beta_1}{2}} - \sqrt{\frac{\beta_2}{2}}\right)(\mu_{noise} + V_{gs} - V_t)$

Variance = $\sigma^2_{noise}\left[\left(\sqrt{\frac{\beta_1}{2}} + \sqrt{\frac{\beta_2}{2}}\right)\right]$



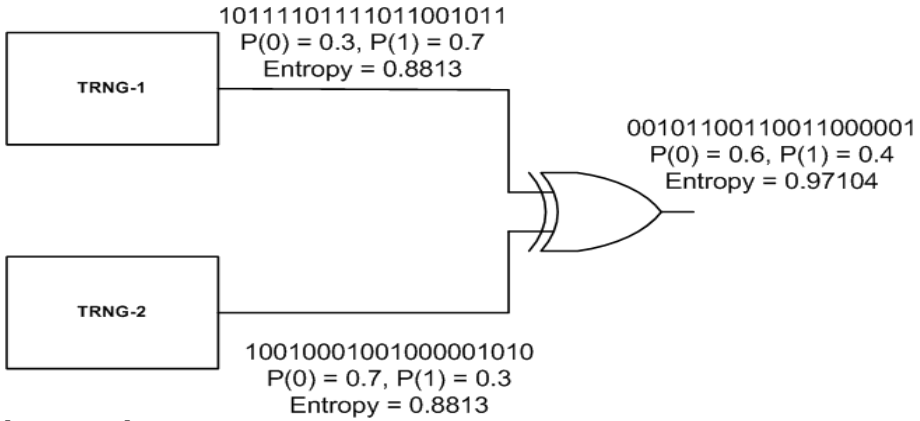
- Self-calibration techniques improve bit entropy, but may introduce correlation between bits



Autocorrelation factor for sample space of 100,000 bits with lag 20,000

Algorithmic entropy extractors

1. XOR



2. von Neumann (1951)

Input bit pairs (from TRNG)	Output from von Neumann Corrector
00	No output
01	1
10	0
11	No output

Raw bits from TRNG

10**11**00**10**10**01**00**01**10**10**01**01**11**00**10**00**10**10**01**01**

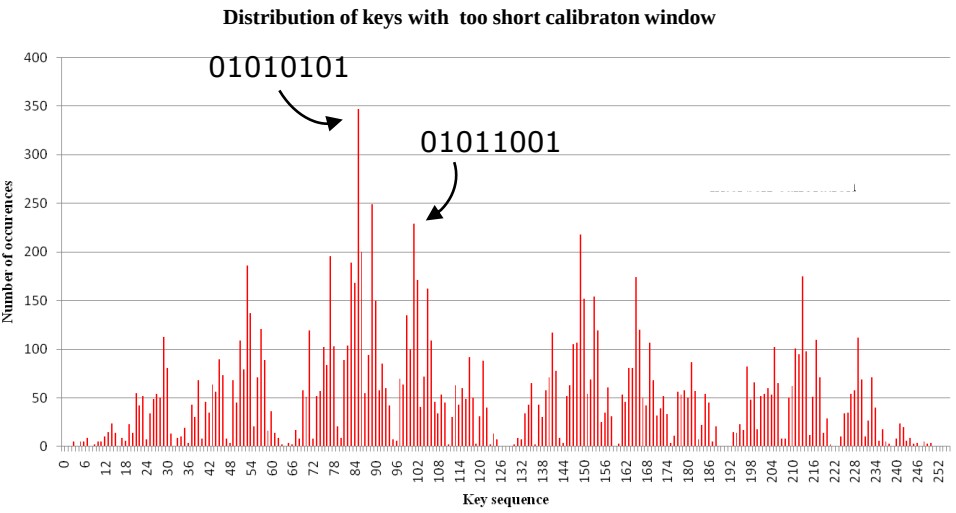
0 - - 0 0 1 - 1 0 0 1 1 - - 0 - 0 0 1 1

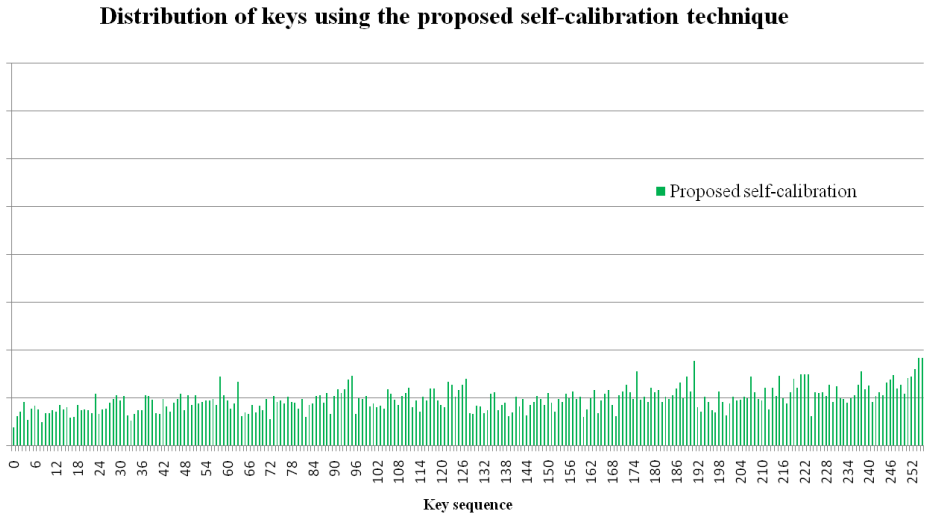
Output of von Neumann Corrector

3. Hash or block cipher (SHA, AES, etc..

von Neumann J., Various Techniques Used in Connection with Random Digits. In *National Bureau of Standards, Applied Math Series,* vol. 12. 1951, pp. 36-38.

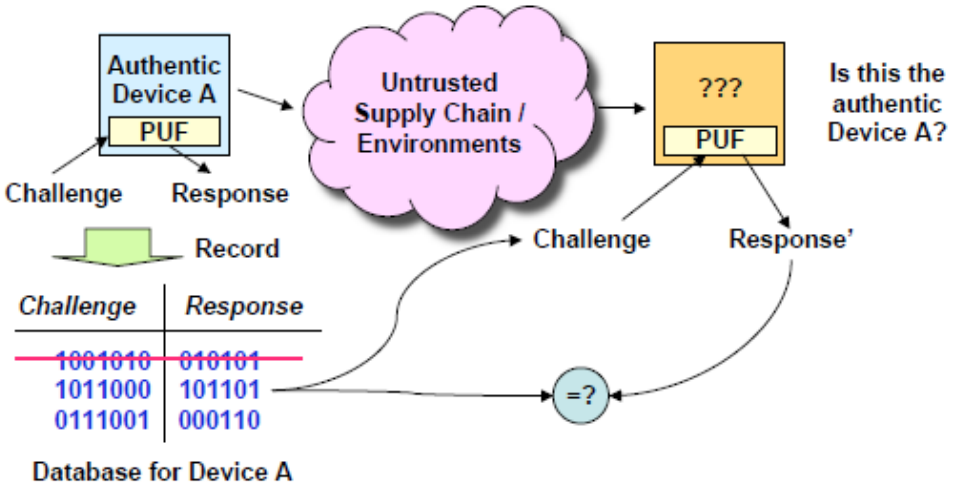
Self-calibration: the dangers of autonomous systems





- Complexity in the self-calibration mechanism
- Finite resources for statistical computations
- External influences on automaton (temp, EM)
- **Open Problem: Secure self-calibration**

Physical Unclonable Functions (PUFs)



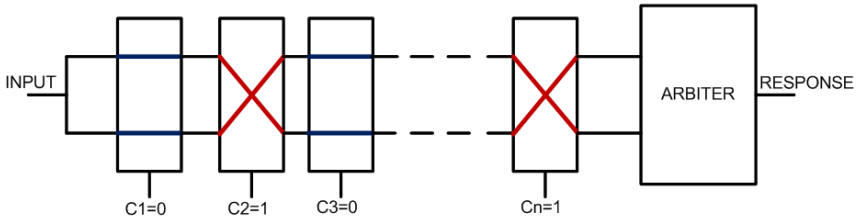
Chip Authentication scenario

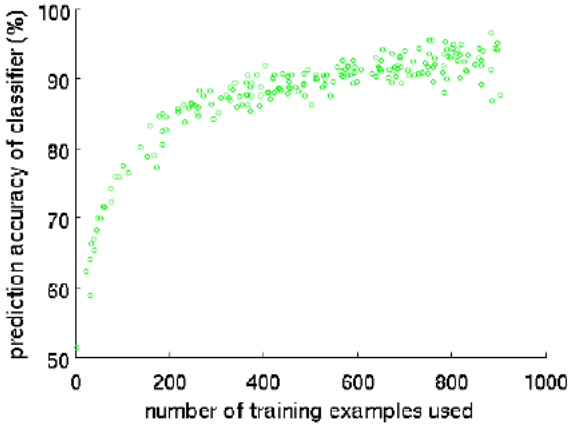
- Authentication – Challenge Response protocol
- Secret key generation, Random functions, Key-less crypto
- Apps: Certified execution, Counterfeit protection, IP discovery
- Metrics: Security, Uniqueness, Reliability, Efficiency (SURE)

G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation", In ACM/IEEE Design Automation Conference, 2007.

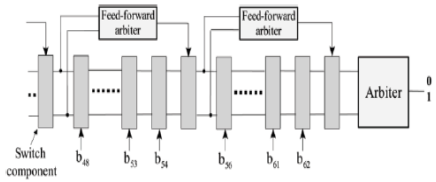
PUFs are vulnerable to machine learning attacks

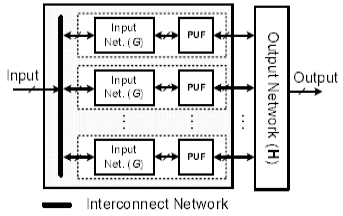
- Arbiter PUF vulnerable with a few hundred CRPs.





- More complex PUFs still vulnerable with more CRPs…





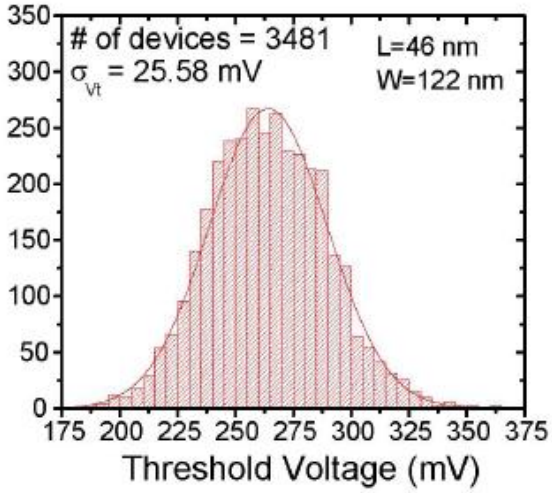
No. of Stages	FF-loops	Pred. Rate Best Run	CRPs	Training Time
64	6	97.72%	50,000	07:51 min
	7	99.38%	50,000	47:07 min
	8	99.50%	50,000	47:07 min
	9	98.86%	50,000	47:07 min
	10	97.86%	50,000	47:07 min
128	6	99.11%	50,000	3:15 hrs
	7	97.43%	50,000	3:15 hrs
	8	98.97%	50,000	3:15 hrs
	9	98.78%	50,000	3:15 hrs
	10	97.31%	50,000	3:15 hrs

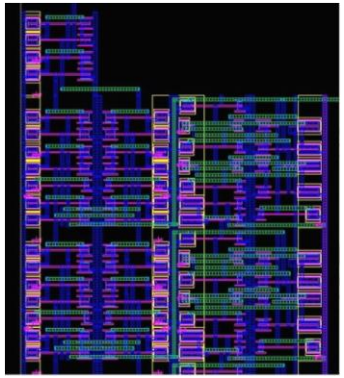
- **Open Problem: Secure PUFs that are hard to learn?**

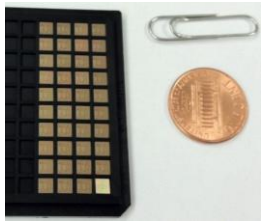
D. Lim, "Extracting secret keys from integrated circuits," M.S. thesis Massachusetts Inst. Technol., May 2004.
U. Ruhrmair, S. Devadas et al, "Modeling attacks on PUFs", ACM CCS, 2010

Sub-th PUF Design for Low Power and Security

- Sub-threshold circuits (Vdd < Vth):
  - Higher sensitivity to process variations = higher uniqueness
  - Low-power and secure applications: RFID
- Design metrics
  - Low power (sub-threshold)
  - Uniqueness (higher for reduced Vdd)
  - Reliability (Vdd and temperature common-mode)
  - Security (resist side-channel attacks and machine learning modeling attacks…)
- Implementation
  - 45nm SOI, chips currently under test
  - On-chip PRNG for self-test
  - 64 stage PUF, 418 gates, 47fJ/cycle







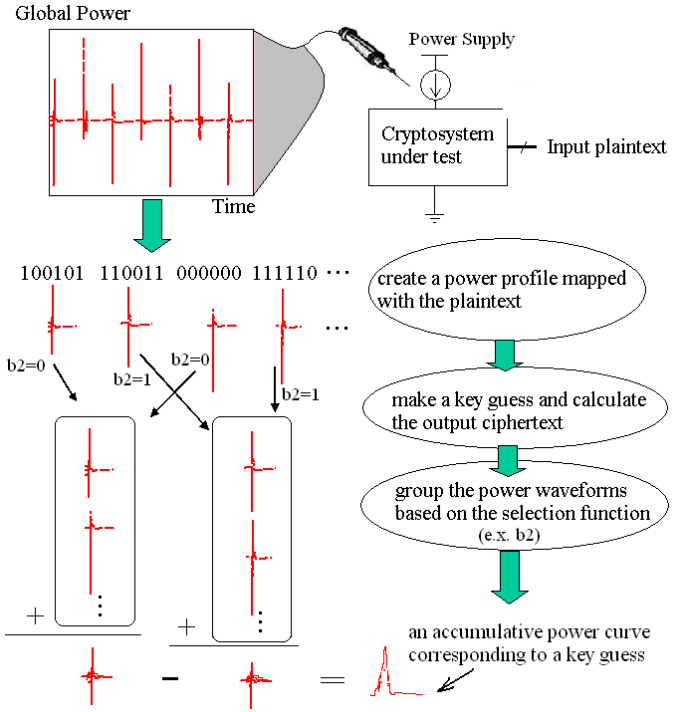
L. Lin, D. Holcomb, D. Krishnappa, P. Shabadi, W. Burleson, **Lower-power sub-threshold design of secure physical unclonable functions,** ISLPED) 2010.
L. Lin, et al.**, Design optimization and security validation of sub-threshold PUFs,** SECSI workshop, April 2010.

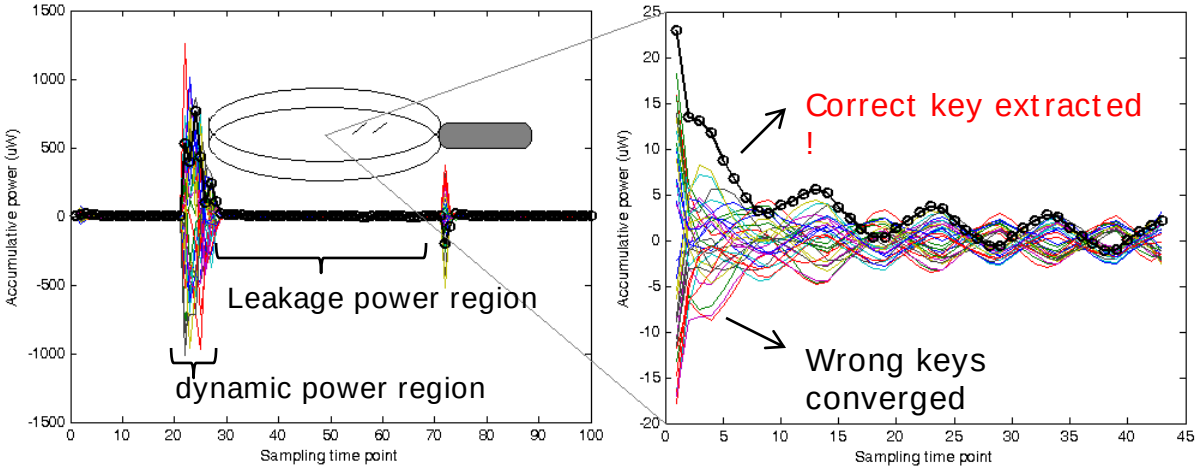
LDPA: Leakage-Based Differential Power Analysis

Differential power attacks can break cryptosystems by exploiting data-dependent dynamic power consumption

LDPA becomes a feasible side-channel attack

CMOS trends: data-dependent leakage power consumption becomes dominant in sub-90nm devices





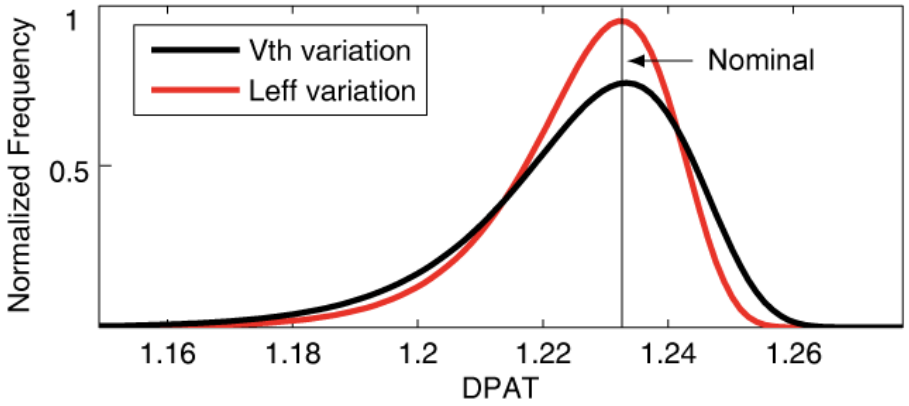
Accumulative power curves generated by differential power analysis algorithm:
(left) a global view of all key guessed curves;
(right) enlarged view of leakage power region where the key can be extracted.

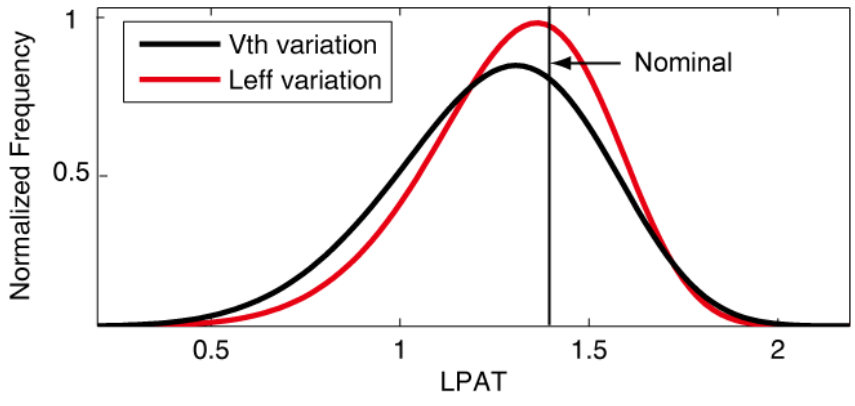
CMOS Process Variation Impacts on Power Side-channels

- Process variations impact both P_{dyn} and P_{leak}
- Define a metric: power-attack tolerance

$$PAT = \frac{1}{SNR} = \frac{\mu(P)}{\sigma(P)}$$

  - Monte-Carlo simulation to determine PAT distribution
  - Both standard CMOS and DPA-resistant logic gates degrading PAT
  - Process variations reduce the average efforts of a DPA attack by 57%
- Mitigation: Transistor sizing optimization
  - Compensate for PAT uncertainty and increase the mean PAT
  - Make DPA attacks more difficult by 39%
  - 0.9% power / 1.5% area overhead

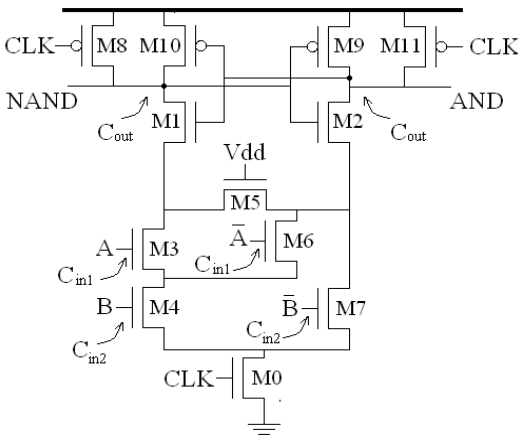


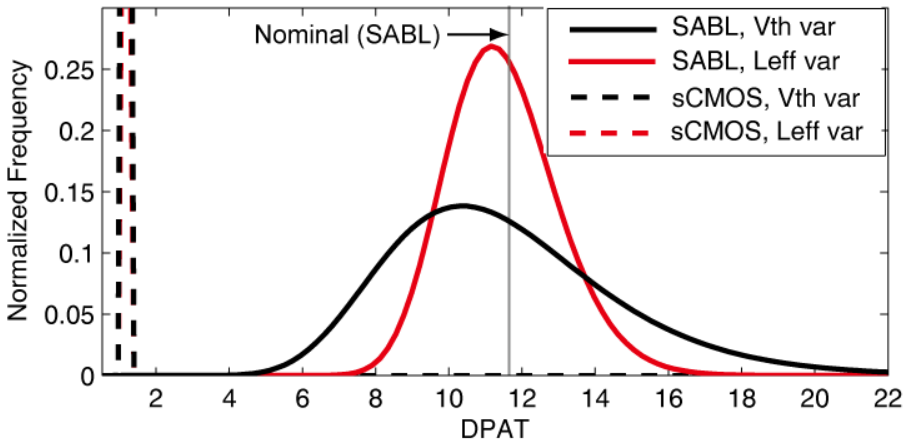


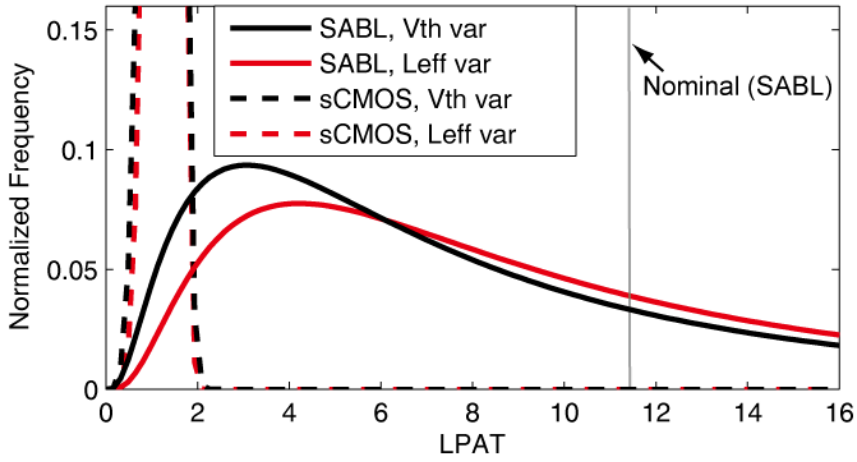
L. Lin and W. Burleson, **Analysis and Mitigation of Process Variation Impacts on Power-Attack Tolerance.** ACM/IEEE Design Automation Conference, July 2009.

Process variations increase the vulnerability of DPA-resistant logic! (although certain attacks may be more difficult)

- Sense Amplifier-Based Logic (SABL)[1]
  - Tolerates power attacks by power balancing circuit with 3-4x design overhead.
  - Ideally infinite PAT; but in reality, 10x larger than the PAT of equivalent CMOS gates.
- Process variation impacts on SABL
  - Results: 59-71% degradation probability
  - LPAT degrades even worse, as low as CMOS gates



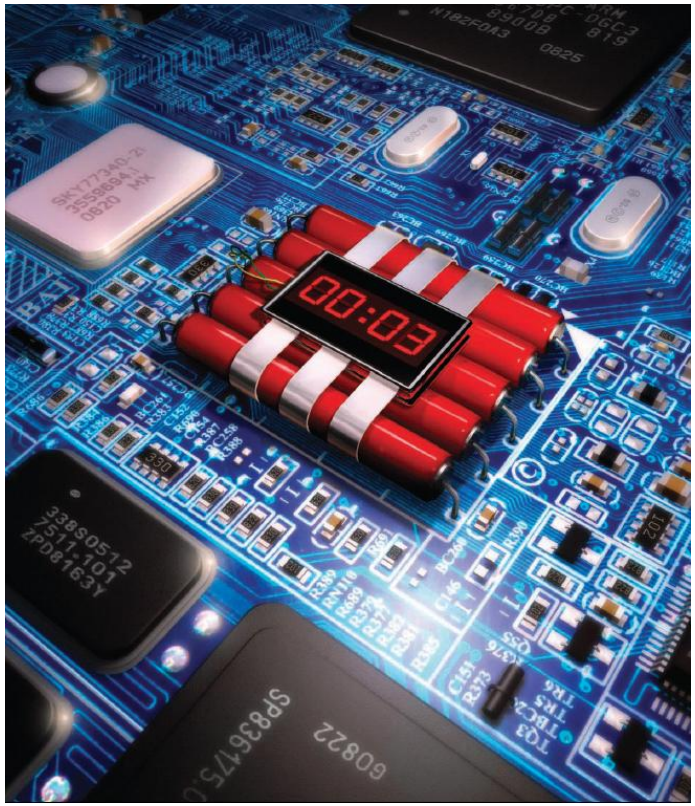




[1] K. Tiri, I. Verbauwhede, "Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology," CHES, 2003.

Hardware Trojans

- *Hacker in your Hardware*, Scientific American, August 2010 [1]

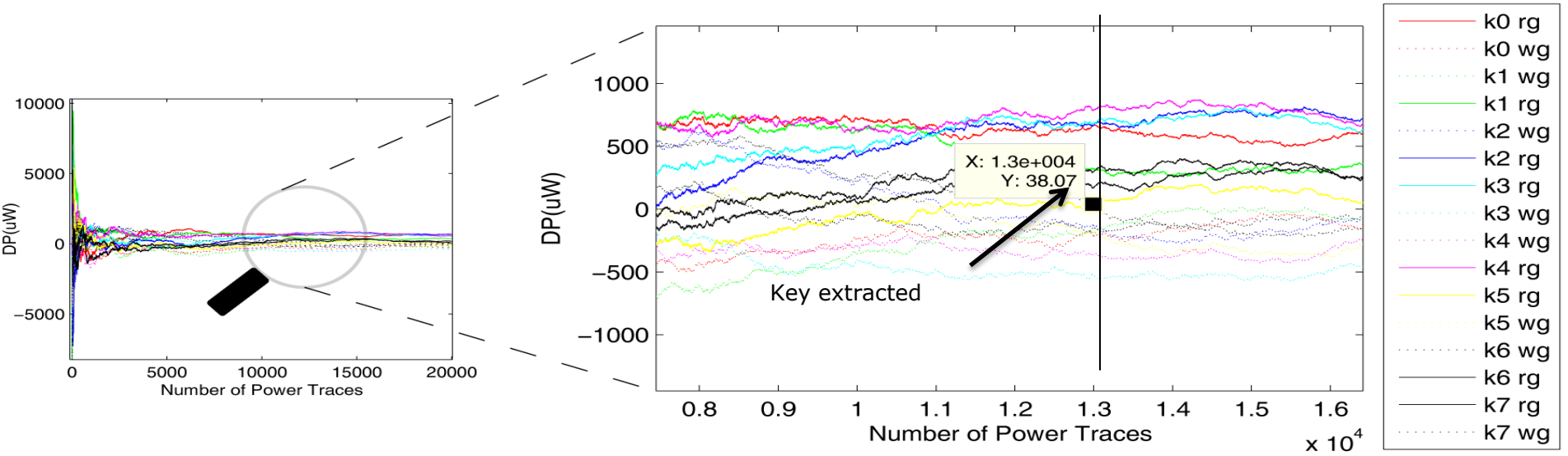


- Taxonomy of HW Trojans [2]
  - Time of insertion
  - Physical location
  - HW abstraction layer
  - Trigger Mechanism
  - Effects
- Countermeasures
  - Power fingerprints
  - Optical techniques
  - Memory gatekeeper
  - Secure system bus
  - Trusted Fabs (DARPA)
- Embedded Systems Challenge (ESC) http://poly.edu/csaw-embedded. Insertion and Detection games

[1] J. Villasenor, Hacker in your Hardware, *Scientific American*, August 2010.
[2] J. Rajendran, et al., Towards a comprehensive and systematic classification of hardware Trojans, ISCAS 2010.

Malicious Off-chip Leakage Enabled by Side-channels (MOLES)

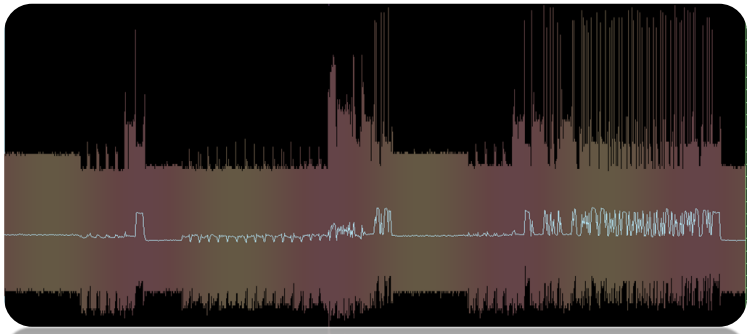
- A Novel HW Trojan**: Engineer** power side channels to convey secret info
- Method: use spread-spectrum (SS) techniques to hide MOLES leakage
  - ✓ Can leak multi-bit key with lightweight implementation
  - ✓ Only the attackers (MOLES designer) know SS sequence to exploit
  - ✓ Evade IC function tests, BIST and error detections
  - ✓ Evade side-channel analyses tests: SS side-channels appear as noise
- Validation: on both 45nm custom ASIC and FPGA
  - ✓ Leakage circuit: capacitive loads, power-dependent logic elements



1. L.Lin, M. Kasper, T.Guneysu, C. Paar, W. Burleson. **Trojan side-channels: lightweight hardware Trojans through side-channel engineering**. In Workshop on Cryptographic Hardware and Embedded Systems (CHES), September 2009.
2. L. Lin, W. Burleson, C. Paar, **Malicious Off-chip Leakage Enabled by Side-channels.** ACM/IEEE Intl. Conf. on Computer-Aided Design, 2009.

Side-Channel Watermarks: Smartcard and FPGA

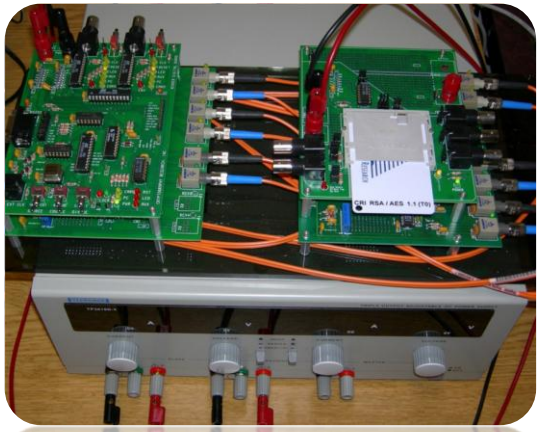
- Modify Smartcard Software with Side-channel watermarks
- Modify FPGA designs with Side-channel watermarks
- Detect Watermarks using side-channel analysis
- DPA Workstation (DPAWS) from Cryptography Research Inc. has state-of-art setup for Power and modification for EM



Smartcard power waveform

DPA Workstation with Smartcard fixture

DPA Workstation with Smartcard fixture



EM [probe on FPGA board

1. G. Becker, C. Paar, W. Burleson, "Software Watermarking with Side-Channels", to appear at NEWCAS 2011
2. A. Lakshminarasinhan, G. Becker,, W. Burleson "Watermarking with Electromagnetic Side-Channels, (in preparation)

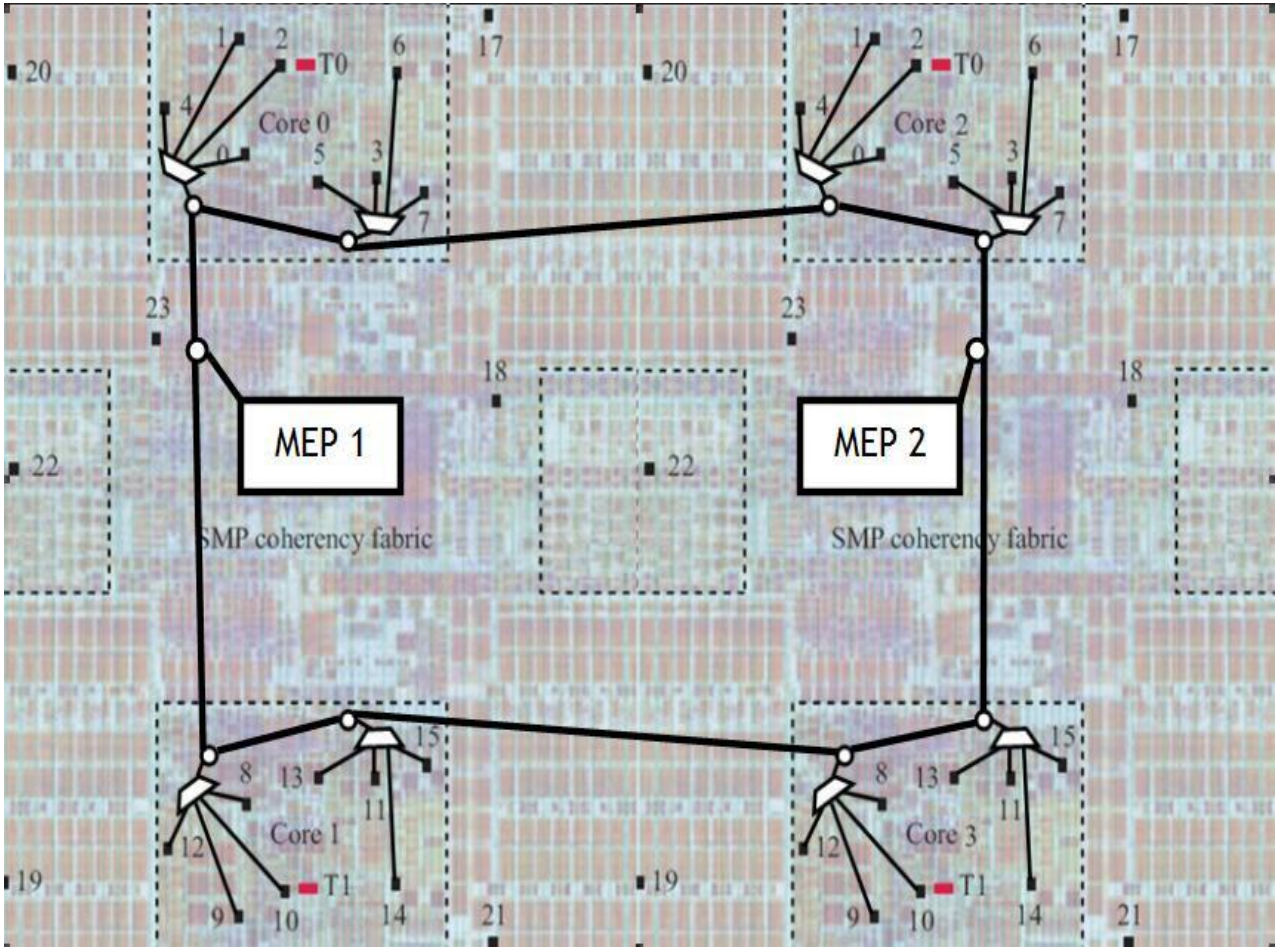
Some of our recent work (2007-2011)

- Crypto Primitives
  - SRAM-based TRNG and Chip ID
  - Metastability-based TRNG (w/ Intel)
  - Physical Unclonable Functions (PUF) in Sub-th CMOS (w/ Berkeley)
- Attacks
  - Leakage-based side-channel analysis
  - Process variation impacts on side-channel attacks
  - Hardware Trojans using side-channels (w/ Bochum)
- Alternative Countermeasures
  - On-chip sensors and surveillance (w/ SRC)
  - Ultra wide-band for low-power security (w/ RSA, Stanford)
- Validation:
  - Test chip in 45nm SOI (w/ IBM)
  - Secure RFID Sensing on FPGA (w/ Intel and Bochum)

Multi-core Surveillance with Networks of On-Chip Sensors

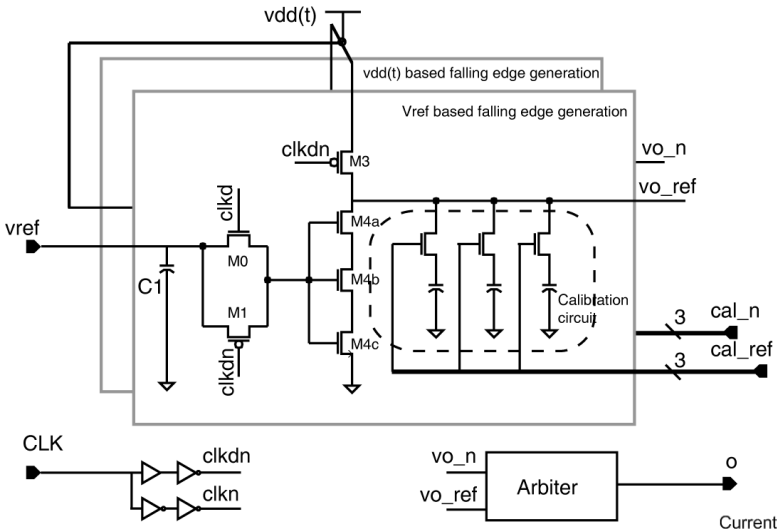
Networked Sensors for:
- -power
- -temperature
- -errors
- -delay margins
- -control flow
- -activity counters

Detection of:
- - thermal runaway
- - soft-errors
- - wearout
- - *Trojan*
- - *intrusion*

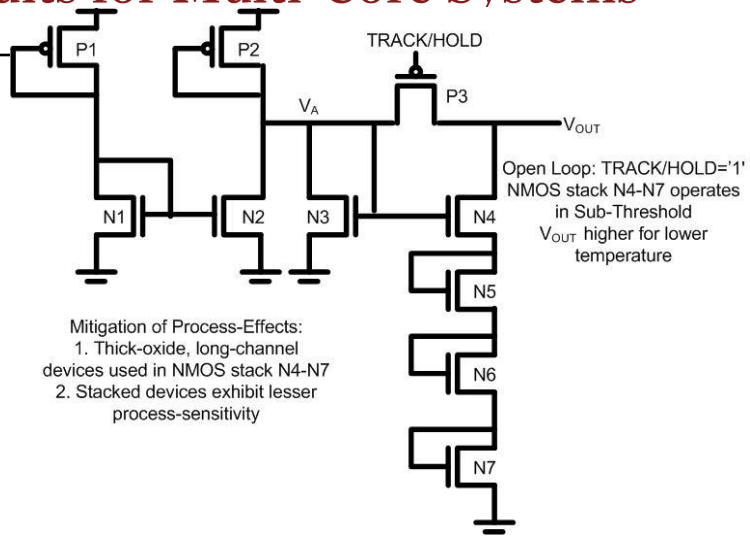


MEP = Monitor Executive Processor

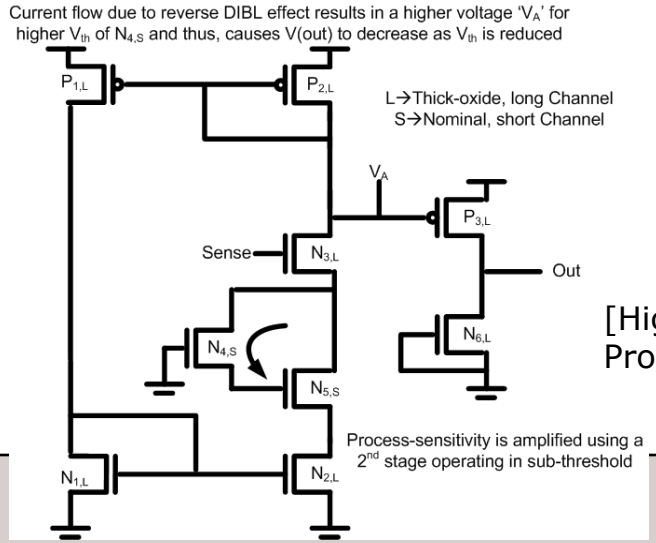
Lightweight and Robust PVT Sensing Circuits for Multi-Core Systems



[Low Latency Droop Detector]

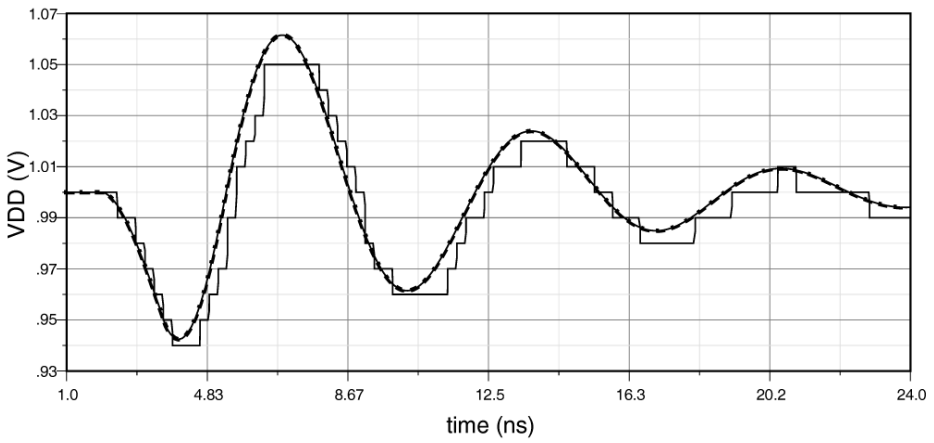


[High Sensitivity & Robust Thermal Sensor]

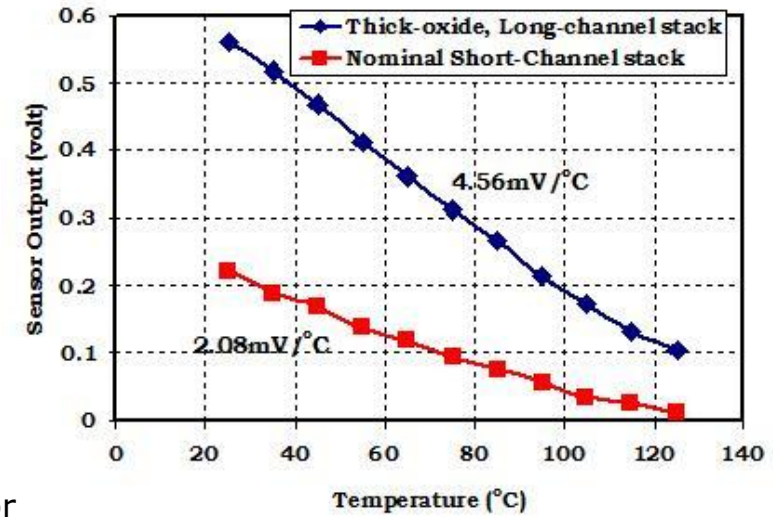


[High Sensitivity & VT-Invariant Process Monitor]

Post Layout Simulations in 45nm IBM-SOI

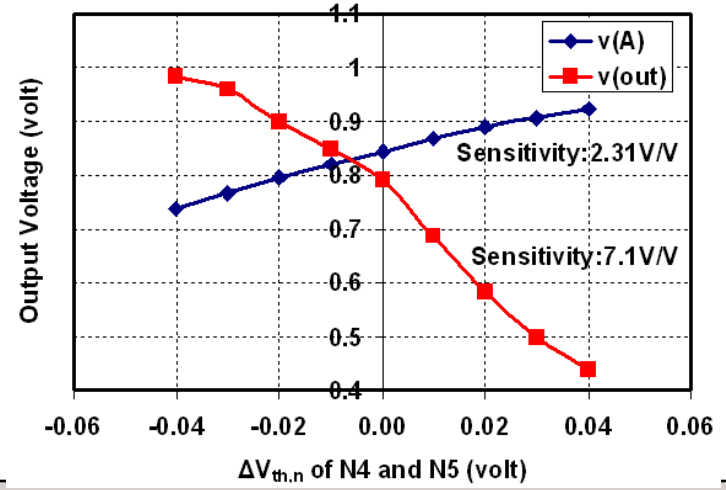


Comparison between simulated supply noise and droop detector output



Sub-Threshold thermal sensor output

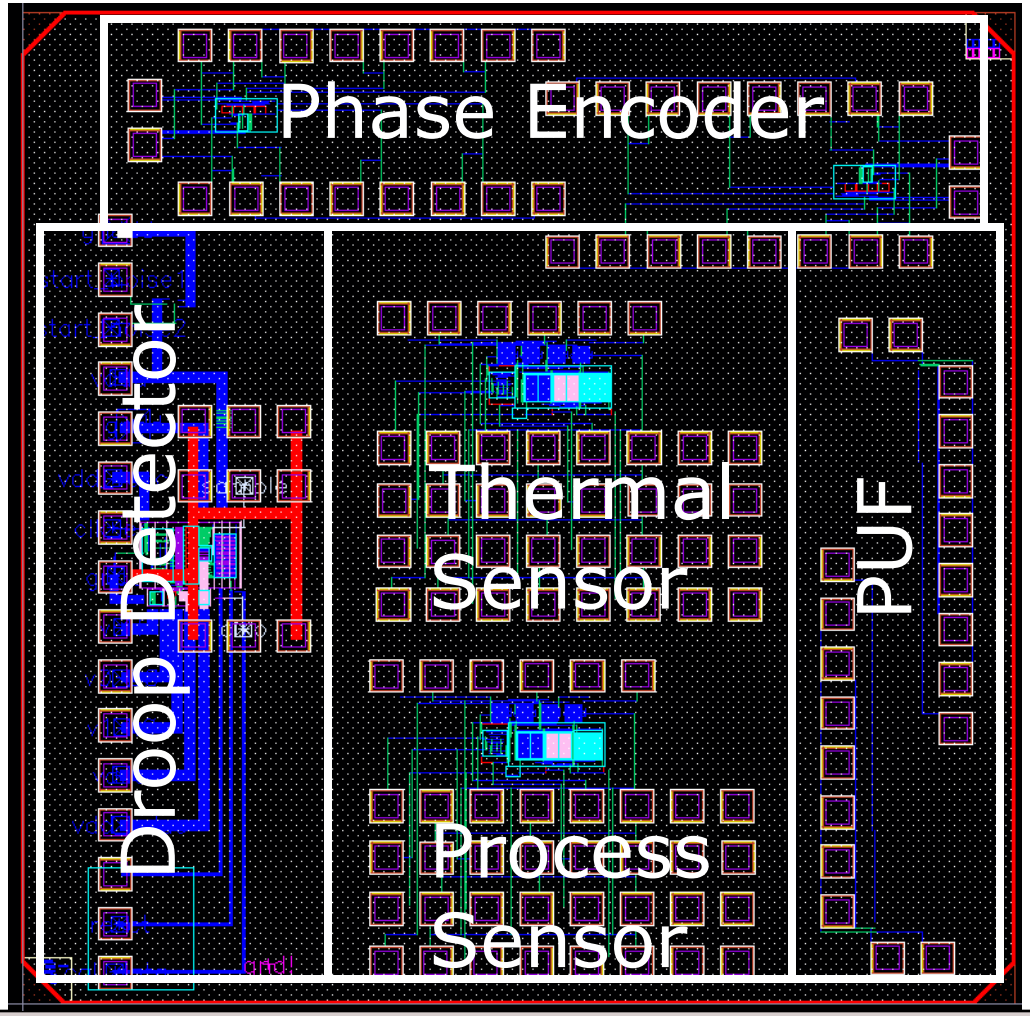
Specs: 12.4μ² 133.4μW 4.56 mV/ºC Resolution



Specs: 45.6μ² 13.4μW 7.1V/V Resolution

Sensitivity of NMOS Vth tracking circuit

Test-Chip in 45nm SOI, currently under test



- Ghz Droop Detector - Jinwook Jang (PhD)
- Process-Aware Sub-th Thermal Sensing Circuits - Basab Datta (PhD)
- DLL-based Phase Encoder - Ibis Benito (PhD)
- Sub-th PUF - Sudheendra Srivaths (MS)

10-Metal Layer Process
Silicon-on-Insulator, High-k, metal gate
Die-dimensions: 9mm^2
Land-count: 152
MOSIS foundry brokerage
Funded by NSF and SRC grants

Ultra-wideband Radio for Low Power Security

Motivation: Standard crypto algorithms (AES, etc.) can be too power/energy consuming for RFID tags, especially passive tags.

Idea: Can we save power by pushing some part of the cryptography to the Physical Layer? Employ impulse-radio ultra-wideband to "hide" the signal in the time-domain.

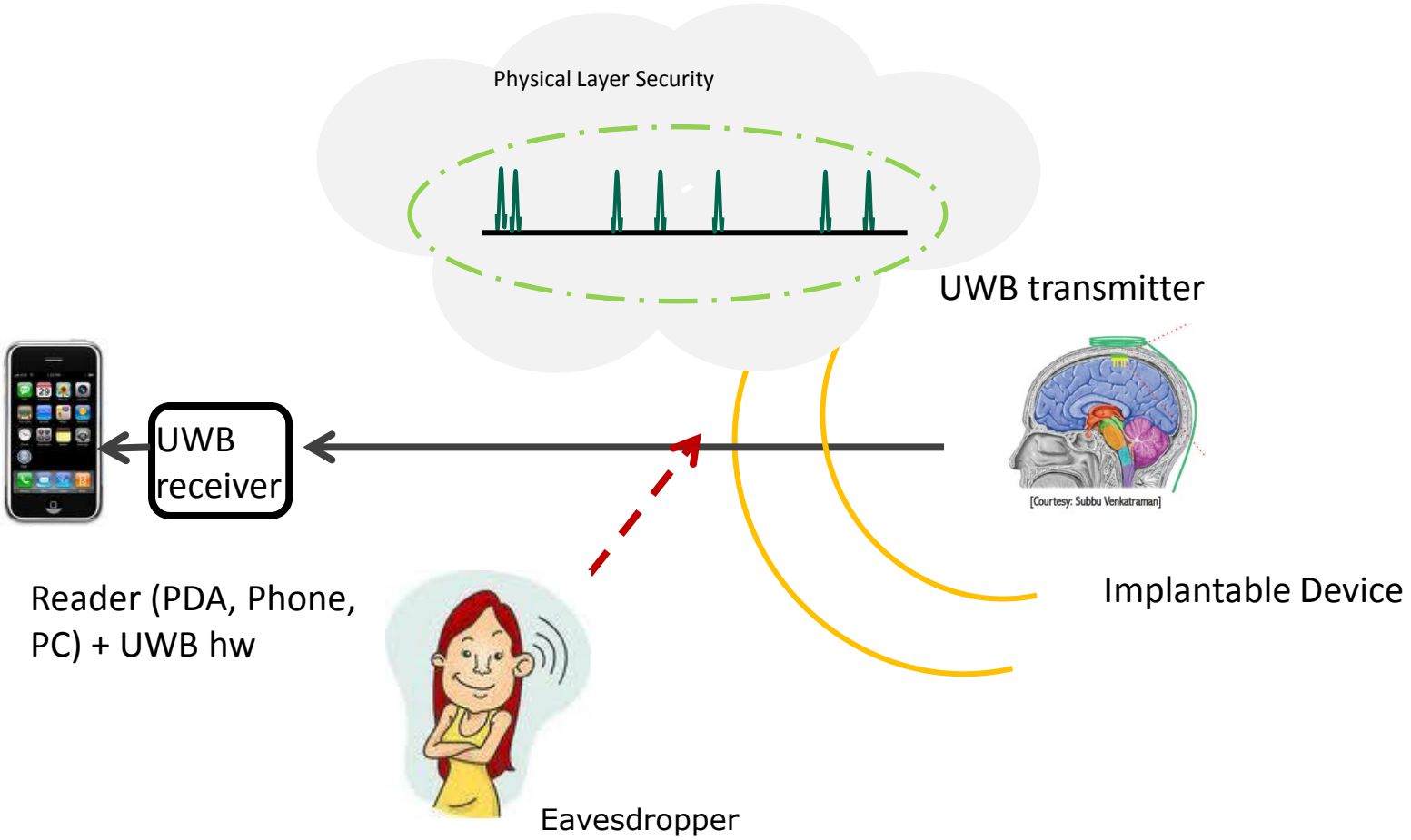
- Desired receiver (knows the key) can aggregate energy to perform channel estimation (and eventually decode). (D. Goeckel)
- Eavesdropper suffers from (asymptotically infinite,) noncoherent combining loss.

Questions:

1. Can we formulate a "hard" problem for the eavesdropper to solve? (Ari Juels – RSA Labs, Dan Boneh – Stanford)
2. How does the power consumption compare to all-digital schemes? (W. Burleson– digital, R. Jackson – analog/RF).
3. Is the scheme more side-channel tolerant? (W. Burleson and C. Paar).

Supported by NSF Cybertrust Exploratory Research grant

Idea: Use UWB to achieve physical layer security



36

Experiment with K-UWB schemes to optimize BER metrics

Goal (big picture):

Position UWB pulses with a key (K-UWB) so that receiver has advantage over eavesdropping adversary

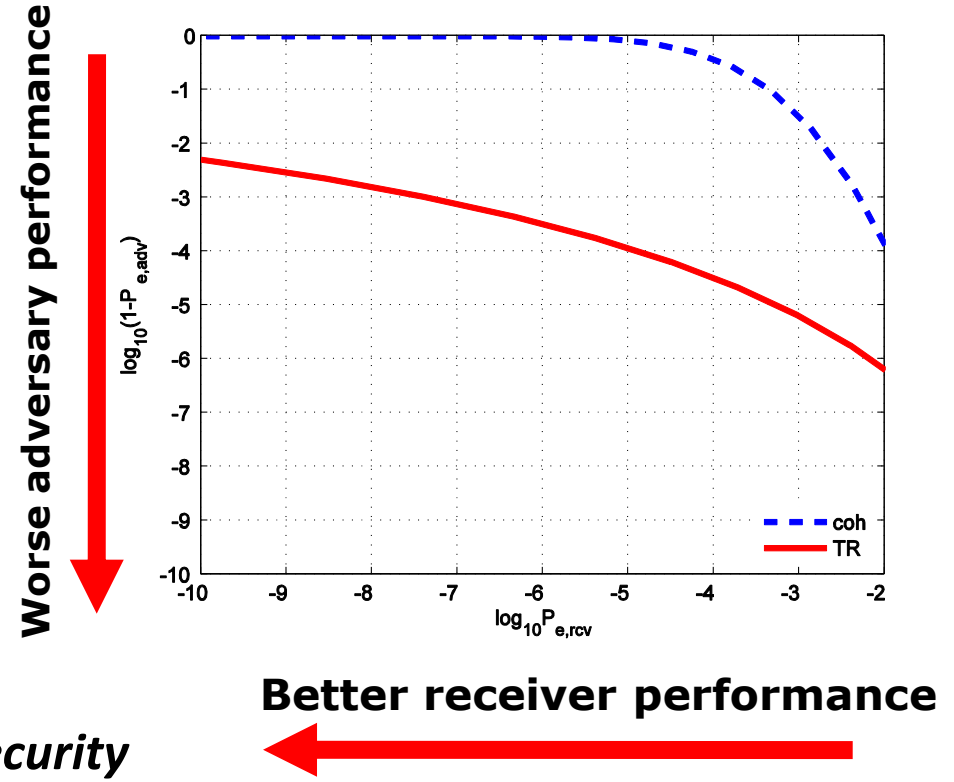
Choices:

Coherent vs. Transmitted Reference

Framed vs. Frameless

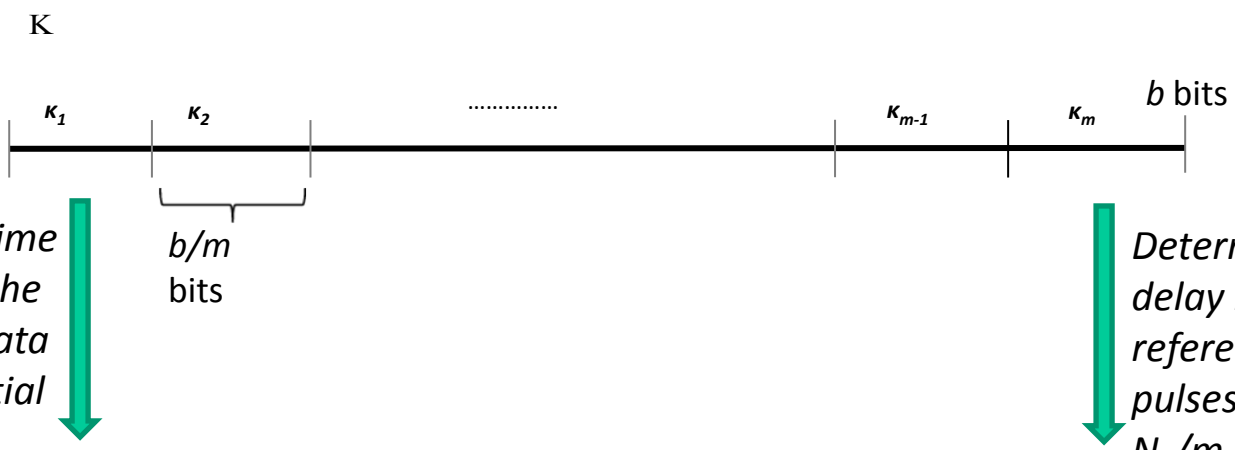
Information-theoretic security

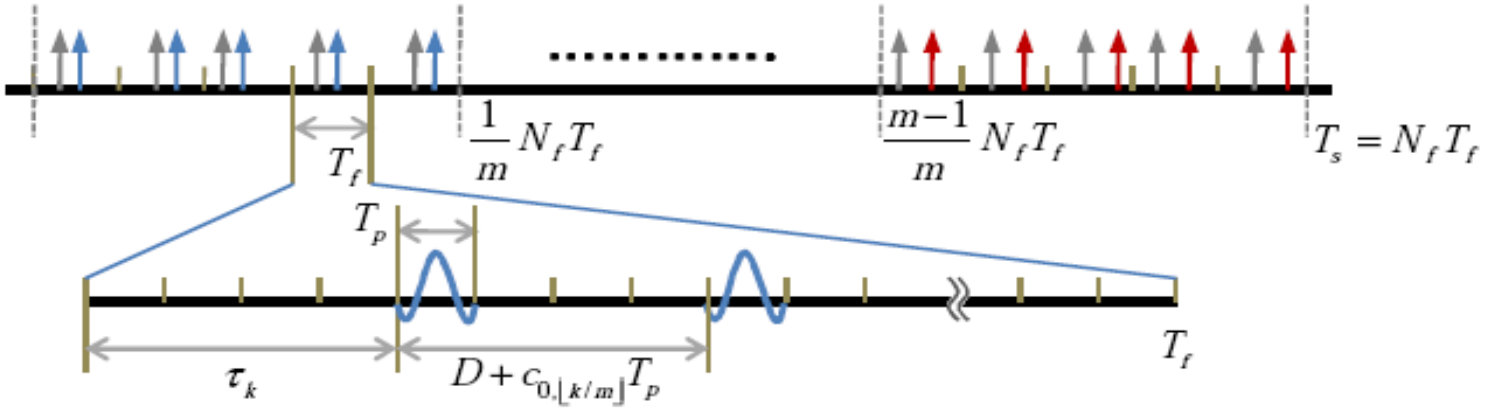
in contrast to Computation-theoretic security



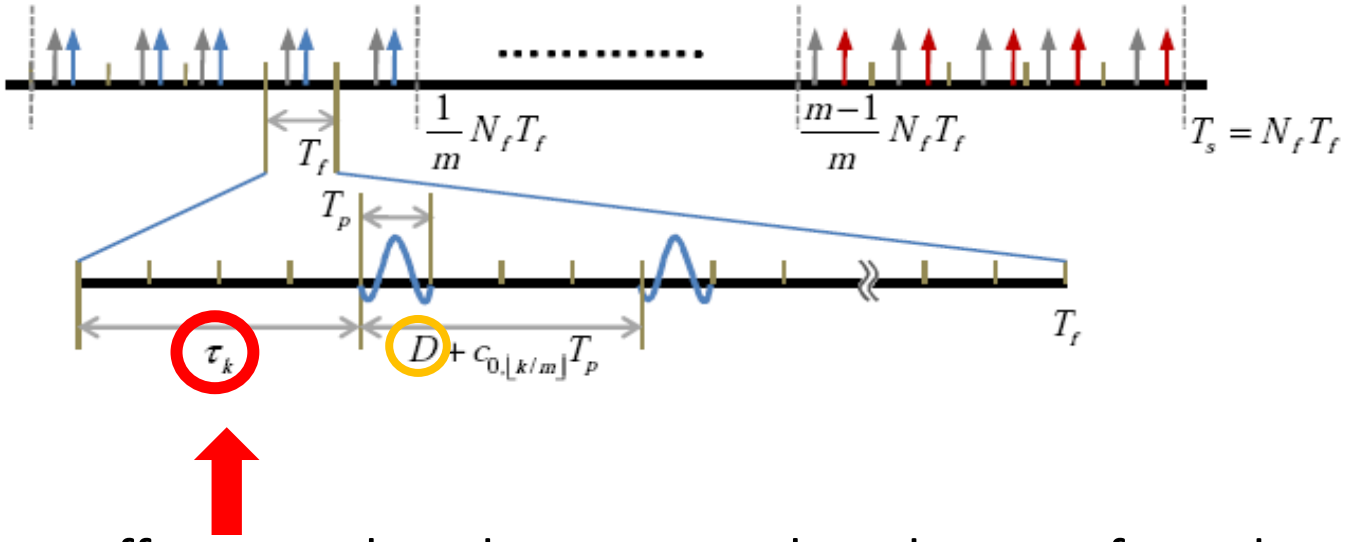
Time-referenced Keyed Impulse Radio K-UWB

b-bit secret key





Lightweight TRNG needed to confuse adversary.

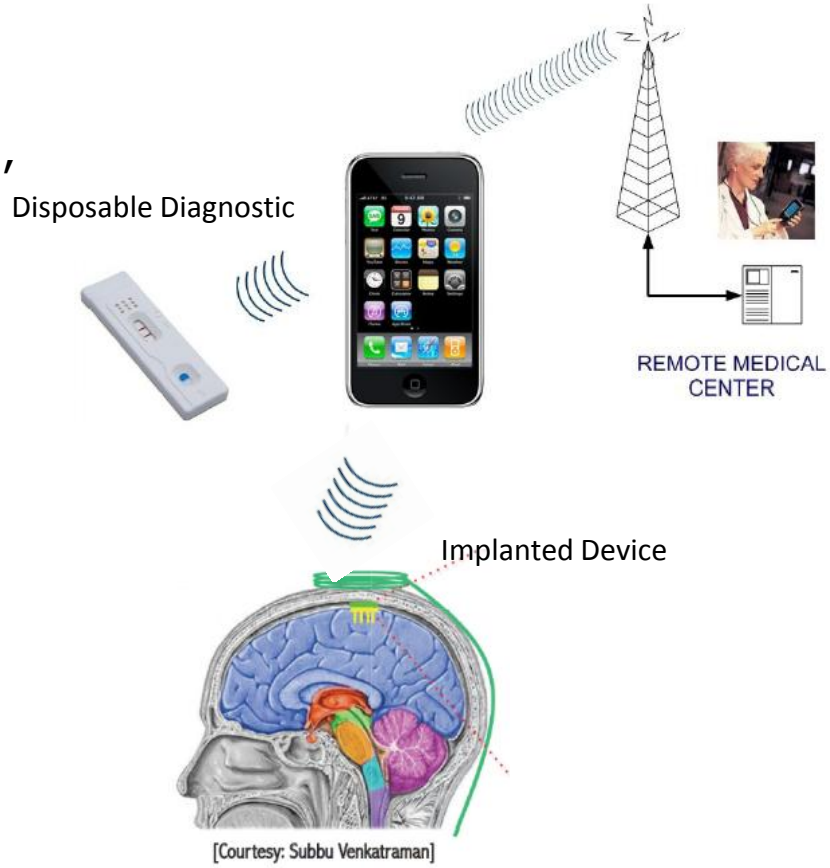


- Random offsets employed to prevent the adversary from detecting the transmitted signal coherently
- Generated by a very fast and light True Random Number Generator (TRNG)
- Intended receiver knows key but does not need to know TRNGs

Secure Platform for Bio-sensing

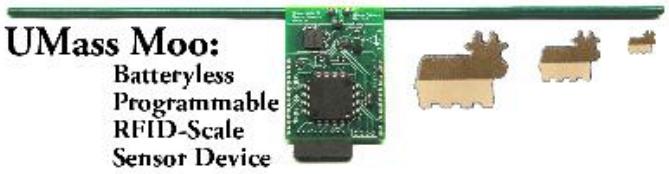
- Applications
  - Disposable Diagnostic
    - Low-cost, infectious disease detection (malaria, HIV, dengue, cholera)
  - Implantable Device
    - Sub-cutaneous multi-function sensor (drugs, antibodies, DNA, brain waves)
    - Pacemaker, Drug-delivery

- Security Technology
  - NFC Cell Phone
  - EPC Class 1, Gen 2 protocol
  - PRESENT Block Cipher (Encryption, Signing, Authentication)
  - PUF for low-cost ID and CRP



Images: Disposable Diagnostic: Gentag.com,
Brain Implant: Berkeley Wireless Research Center.

Prototyping RFID with the UMass Moo



SPQR Computer Science UMass

Overview Moo is a passive Computational RFID that harvests RFID reader energy from the UHF band, communicates with an RFID reader, and processes data from its onboard temperature sensor and accelerometer. Its function can be extended with its general-purpose I/Os, serial buses, and 12-bit ADC/DAC ports. The Moo provides a RFID-scale, fully programmable, batteryless sensing platform. The programs executes on an MSP430 microcontroller. The Moo 1.0 derives from the open source Intel DL WISP 4.1.

Documents An Introduction to the Architecture of Moo 1.0 (PDF, PPT).

Photos

(a) Moo with antenna removed.

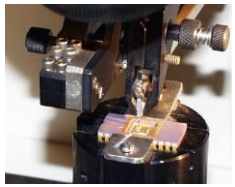
(b) Moo 1.0 + USB Programmer (zoom).

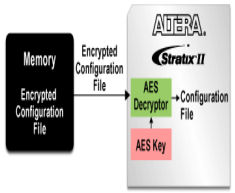
Applications

- *Transportation*
- Commerce
- Supply Chain
- Pharmaceutical
- *Medical Devices*
- Assistive Technologies
- Education (Learner modeling)
- Entertainment (DRM)
- …

Trusted & Reliable Embedded Networked Devices and Systems (TRENDS)

- **Projects:**
  - Architectures for Future RFID chips
  - Side-channel attack resistant design methods
  - Configurable hardware architectures
  - On-chip Monitoring for Attack Detection
  - Secure soft-processors
  - Power Depletion Attacks in Sensor Networks
  - Ultra-wideband Security
  - Integrated Payment Systems
- **Recent Funding**
  - NSF "Pay-as-you-Go"
  - NSF "UWB for Low-Power Security"
  - CISCO "Post-Quantum Crypto"
  - NSF "Smart Tags"
  - DARPA "Secure Sensor Networks"
  - Microsoft "Secure RFID"
  - NSF "Animated Spaces"
  - ARO "Network Vulnerability and Wireless Security"
  - ARO MURI "Ultra Wide Band"
  - NSF CAREER "Network Processors"
  - NSF CAREER "Supply Chain Management"





RFID CUSP

- **Participants**
  - W. Burleson (VLSI Systems)
    W. Gong (Systems and Control)
    R. Tessier (Embedded Systems)
    T. Wolf (Network Processors)
    A. Ganz (Networks)
    K. Fu (CS, RFID, Applied Crypto)
    D. Ganesan (CS, Sensor Networks)
    A. Muriel (IE, Asset Management)
    R. Jackson (RF, Analog Circuits)
    D. Goeckel (Wireless)
    J. Collura, (Transportation)
  - Industrial: Microsoft, IBM, RSA Labs, EMC, MITRE, CISCO, Altera, Intel, ThingMagic. Hitachi
  - Government: NIST, FTC, FDA
  - Academic
    - A. Lysyanskaya, Brown Univ.
    - M. Zarrillo, UMass Dartmouth
  - International:
    - C. Paar, A. Rupp, Germany
    - G. Gogniat, France
- **Educational Impact**
  - New courses in Cryptography, Security Engineering, Trustworthy Computing
  - Industrial workshops

Integrated Payment Systems for Transportation

Q: How to Finance Crumbling Transportation Infrastructure?
A: User Pay-as-you-Go Fees with Electronic Payment Systems.., but:

- Payment smart cards being deployed without adequate security or privacy considerations (January 2008 breaks of Translink and Mifare)

- Open road tolling being deployed in Texas, New Jersey and Florida with security and privacy vulnerabilities

- How to gather user behavior for system optimization without compromising privacy? (w/ Brown, TUDarmstadt)

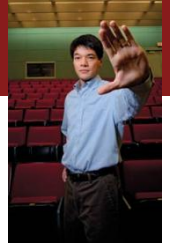
- Partial anonymization using e-cash schemes needs lightweight elliptic curve engine (w/ Bochum, Leuven)

- First UMass Workshop on Integrated Payment Systems for Transportation, Boston, Feb. 2009, 40 participants from industry, government and academics

- Working with MBTA, Mass Highways, E-Zpass, RSA, MIT, Volpe Center, to assess vulnerabilities and develop both short-term and long-term solutions

Privacy-preserving payments with tracking option

- **E-cash plus dynamic pseudonyms** allow users to opt-in to possible tracking and perhaps receive a discount on their fare. Other transportation payment solutions require users to trust infrastructure, black-box, obfuscation methods, etc. to varying degrees to ensure their privacy.
- **Users can choose to play a game or not.** If they play the game, they can trade off privacy for lower fares. Similarly, the transportation operators can play by offering reasonable discounts in order to incentivize users to give up some privacy in order to give up some information to allow operators to optimize their services. They can gain additional revenue by targeting advertising.
- **E-cash needs to become a culturally trusted anonymous payment** (as regular cash is today) . Pseudonyms will be a bit like Cookies where most users will opt-in and accept them for the convenience and reduced fares that they allow, but some users (e.g. Stallman, etc.) can stay anonymous. Various levels of privacy vs. convenience/economy can be provided. These levels may vary depending on culture, law and education of users.
- **Location-Privacy is hard for the general population to understand** since the vulnerability is defined by ever-improving tracking algorithms. Some users may wish to learn about these vulnerabilities, calculate risks and play the game, but others should be able to opt out and rest assured that their privacy is not being compromised. (Somewhat analogous to playing the stock market vs. staying in a less risky investment with one's savings).



Implantable Medical Devices (w/ Kevin Fu, UMass)

- Many medical devices rely on wireless connectivity for remote monitoring, remote therapies and software updates.
- Recent research identified several attacks and defenses for implantable cardiac defibrillators
  - Wireless communications were *unencrypted and unauthenticated*
  - Power depletion attacks
- Extensions to numerous other emerging implantable devices

WSJ.com THE WALL STREET JOURNAL. ONLINE

March 12, 2008

Heart-Device Hacking Risks Seen

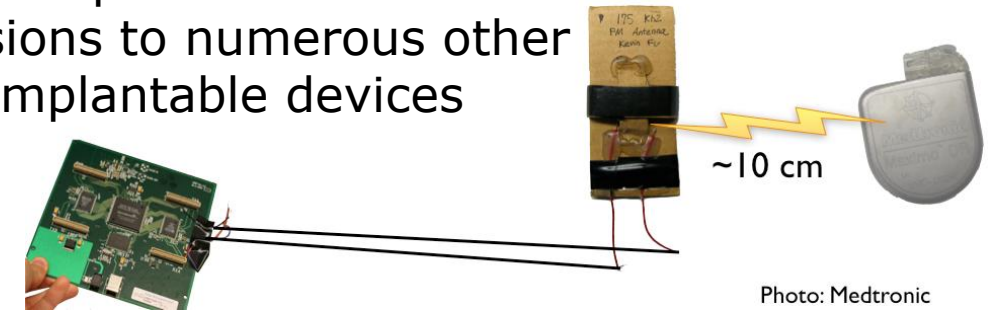


Photo: Medtronic

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses.
D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel.
In Proceedings of the 29th Annual IEEE Symposium on Security and Privacy, May 2008. **Outstanding Paper Award**

OMDRL (Open Medical Device Research Library)

- A collection of *used* medical devices for use in security research
- Overcomes reluctance of device manufacturers to offer devices for research.
- Includes pacemakers, glucose sensors, insulin pumps, etc.
- More information available from kevinfu@cs.umass.edu

Recent Event!

Speakers:

- Kevin Fu, UMass Amherst, USA
- Srdjan Capkun, ETHZ, CH
- Jos Huiskens, IMEC, NL
- Ahmad Sadeghi, Darmstadt, DE
- Ian Brown, Oxford, GB
- F. Valgimigli, Metarini, IT
- A. Guiseppi-Elie, Clemson, USA
- Q. Tan, Shanghai, China

Panel : How real and urgent are the security/privacy threats for IMDs? Which IMDs?

(just following IEEE ISMICT in nearby Montreux, Switzerland, www.ismict2011.org)

Recent Event!

Special Session : Hardware Security in VLSI

Session Organizers:

Wayne Burleson, U. Massachusetts, USA
Yusuf Leblebici, EPFL, Switzerland

GLSVLSI
May 2-4, 2011
EPFL, Lausanne, Switzerland

Speakers:

1. Farinaz Koushanfar, Rice University, USA
"Protecting ICs against piracy"
2. Ingrid Verbauwehde, KU Leuven, Belgium
"Physically Unclonable Functions: Benefit from Process Variations"
3. Christof Paar, Ruhr U, Bochum, Germany
"The Future of High-Speed Cryptography: New Computing Platforms and New Ciphers"

Conclusions

- Hardware security is the foundation of higher level secure systems
- Underlying CMOS fabric is changing, introducing new vulnerabilities (variations, noise, leakage). More changes with emerging nano-technologies.
- Variations and noise can help or hurt security. Be aware of them and think statistically.
- There's "plenty of room at the bottom" (e.g. PUFs, TRNG, UWB)
- RFID, Smart sensors, "Smart dust" have many hardware security challenges due to resource constraints.
- Higher- and lower-level defenses can augment cryptography.
- Validation of cryptosystems is challenging. Security is hard to measure.
- Security is hard! Cross-disciplinary security research spans Circuits, Architecture, Communications, Crypto, Manufacturing, Economics, Psychology and Application Domains (e.g. Transportation, Medical Device, RFID, etc.)

Hardware Security Challenges in Next Generation RFID

- Improved radio frequency communication range and power delivery efficiency
- Power efficiency (currently 20-30uW for digital)
- Energy storage (batteries and super-capacitors) to allow reader-less operation
- Data storage (currently 1-4K bits, moving to 10-100Kb, both volatile and non-volatile)
- Security services
  - Authentication (Hash functions, Device-tied functions)
  - Encryption (Private, Public)
  - Consensual reading
  - Intrusion detection
  - Side-Channel attacks (EM, power, fault-injection, gltich, timing)

- New HW-related features in Next Generation tags
  - Data Storage
    - Shared among multiple untrusted parties
    - Logging (e.g. for intrusion detection)
  - Sensors
    - Location
    - Temperature, Bacteria, Chemical
    - Off-line Computation
  - Time-aware (real-timers)
  - Reliability

Intel WISP