

# RFID Privacy: from Transportation Payment Systems to Implantable Medical Devices

Wayne Burleson

University of Massachusetts Amherst  
[burleson@ecs.umass.edu](mailto:burleson@ecs.umass.edu)

AMD Research Boston  
[wayne.burleson@amd.com](mailto:wayne.burleson@amd.com)

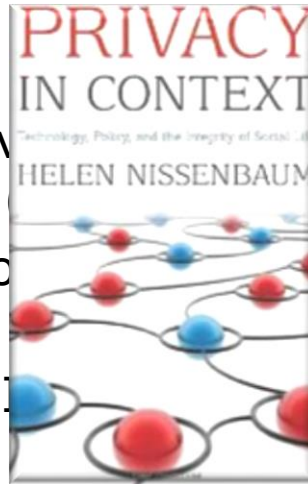


# Some notable dates in privacy

- 1953 European Convention on Human Rights, Article 8,
- 1981-82 Chaum: Anonymous email, E-cash
- 1990 Privacy International, 1991 PGP
- 1997 Diffie and Landau: Privacy on the Line (wiretapping)
- 1998 k-anonymity
- 1999 McNealy: "You have zero privacy anyway. Get over it."
- 2000 First PETS workshop (Berkeley)
- 2002 Tor
- 2003 Benetton: RFID privacy
- 2004 E-passports, mix-zones
- 2005 First RFIDSec (Graz)
- 2006 Differential privacy
- 2007 EZ-pass subpoenas, TJ Maxx data breach
- 2008 Bitcoins, Implantable Medical Device vulnerabilities
- 2009 Facebook – privacy changes
- 2010 Privacy by Design
- 2011 Wikileaks, Apple: iphone locations
- 2012 Google : shares history
- 2013 US Supreme Court allows DNA collection
- 2013 NSA : Snowden

# Privacy in many academic fields

- G. Tseitin et al, "Tracing individual public transportation from an anonymous transaction database", *Journal of Transportation*, 2006
- M. Hay, C. Li, G. Miklau, and ... the degree distribution of privacy. *International Conference on Data Mining*
- H. Nissenbaum "Privacy in Context". *Ethics*.
- L. Sankar, S.R. Rajagopalan, ... and privacy of data sources. *International Symposium on Information Theory*, 2010.
- R. Shokri, G. Theodorakopoulos, G. Danezis, J.P. J.Y. Le Boudec. Quantifying **location privacy**: sporadic location exposure. In *Privacy Enhancing Technologies*, 2011.
- C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel. Pripayd: Privacy friendly **pay-as-you-drive insurance**. *IEEE Transactions on Dependable and Secure Computing*, 2011.



Sexual and injecting drug partners



Potterat, et al.  
Risk network structure in the early epidemic phase of HIV transmission in Colorado Springs.  
*Sexually Transmitted Infections*, 2002.



# Why I find Privacy more interesting than Security

- Subtle threat model
  - Privacy metric is often a result of a very complex attack
  - Not yet conceived use of data
  - No boogie man
- Economics
  - what will people pay for privacy
- Human and social issues
  - Different cultures, ethics, opinions

"Instead of 'getting over it', citizens need to demand clear rules on privacy, security, and confidentiality." (Manes)

For each weakness, why was privacy compromised?

- Security
- Convenience
- Social
- Marketing
- Research

For each solution, why was privacy preserved?

- Anti-government
- Tax avoidance
- Contraband
- Principles

# RFID Privacy... haven't I heard this before?

## RFID Security and Privacy: A Research Survey

Ari Juels

*Invited Paper*

**Abstract**—This paper surveys recent technical research on the problems of privacy and security for radio frequency identification (RFID).

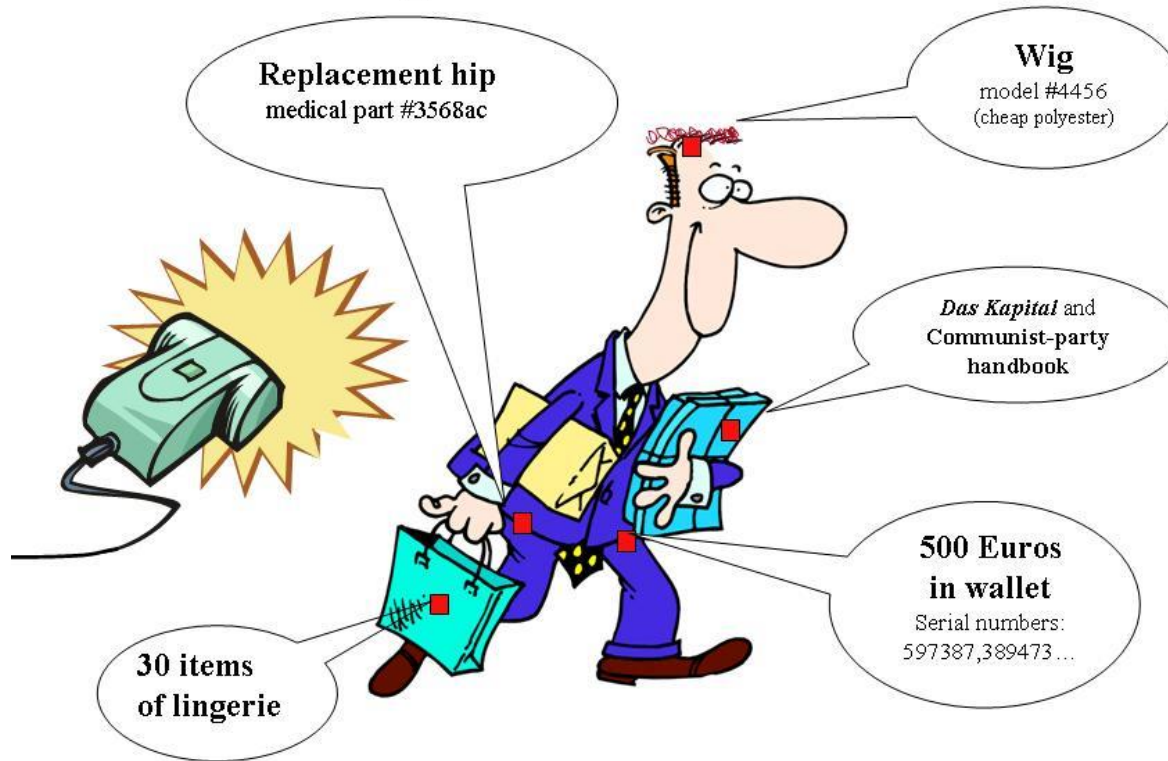
RFID tags are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next several years—and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work. While

- 1) *Unique identification*: A barcode indicates the type of object on which it is printed, e.g., “this is a 100 g bar of ABC brand 70% chocolate.” An RFID tag goes a step further. It emits a unique serial number that distinguishes among many millions of identically manufactured objects; it might indicate, e.g., that “this is 100 g bar of ABC brand 70% chocolate, serial no. 897 348 738.”<sup>1</sup> The unique identifiers in RFID tags can act as pointers to a database entries containing rich transaction histories for individual items

**Recommended reading!**

# RFID Privacy concerns... (what has changed since 2007?)

RFID tags will soon be *everywhere*...



Ari Juels, RSA Labs, 2007

Can they support privacy-preserving protocols?



# An updated view...



Implantable Medical Device



Public transportation systems



➤ Wireless IMD access reduces hospital visits by 40% and cost per visit by \$1800

*[Journal of the American College of Cardiology, 2011]*

# Comparing RFID Security/Privacy issues

	<b>Transportation payment systems</b>	<b>Implantable medical devices</b>
Cost	<ul style="list-style-type: none"><li>• very low cost,</li><li>• disposable</li></ul>	<ul style="list-style-type: none"><li>• expensive,</li><li>• (but some disposable applications)</li></ul>
User model	<ul style="list-style-type: none"><li>• time-aware,</li><li>• broad spectrum of population</li></ul>	<ul style="list-style-type: none"><li>• latency-tolerant</li><li>• life-critical</li><li>• may have multiple devices and health issues</li></ul>
Assets	<ul style="list-style-type: none"><li>• user identity</li><li>• location,</li><li>• habits</li></ul>	<ul style="list-style-type: none"><li>• user identity,</li><li>• health</li><li>• genomics, proteomics,...</li></ul>
Threat model	<ul style="list-style-type: none"><li>• tracking,</li><li>• marketing</li></ul>	<ul style="list-style-type: none"><li>• tracking,</li><li>• insurance fraud,</li><li>• discrimination</li></ul>



# Multi-disciplinary teams

- Transportation Payment Systems – “Pay as you Go”
  - Umass ECE – Security Engineering and VLSI
  - Umass Transportation – Transportation financing, user acceptance,
  - Umass CS - Wisp/Moo, Security Engineering
  - Brown - Crypto, E-cash
  - Umass Dartmouth – Transportation design and optimization
  - MBTA, - Data-sets, Real-world issues
  - EPFL CS – Location Privacy
  - KUL – ECC Engine
  
- Implantable Medical Devices
  - Umass ECE and CS – Security Engineering, IMDs
  - EPFL EE – Bio-sensors and prototyping
  - Bochum – Security Implementation (KECCAK)
  - MIT – Secure Communications
  - SHARPS – IMD Security, Privacy Ethics, Health Records
  - SPIMD book: Clemson, Metarini, Princeton, U. Michigan, Shanghai

# Multi-disciplinary teams

- Transportation Payment Systems – “Pay as you Go”
  - Umass ECE – G. Hinterwalder, C. Zenger, B. Gopal, A. Rupp, W. Burleson
  - Umass Transportation – M. Skelly, M. Plotnikov, J. Collura
  - Umass CS - A. Molina-Markham, K. Fu
  - Brown - F. Baltsami, A. Lysyanskaya
  - Umass Dartmouth – M. Zarrillo
  - MBTA, - S. Pepin
  - EPFL CS – R. Shokri, J-P. Hubaux
  - KUL – I. Verbauwehde
- Implantable Medical Devices
  - Umass ECE and CS – W. Burleson, K. Fu
  - EPFL EE – S. Carrara, S. Ghoreishizadeh, A. Pullini, J. Olivo, G. DeMicheli
  - Bochum – T. Yalcin, C. Paar
  - MIT – D. Katabe, S. Gollakata,...
  - SHARPS – H. Nissenbaum, D. Kotz, C. Gunter ...
  - SPIMD book: A. Guiseppi-Elie, Q. Tan, N. Jha, ...

# Public Transportation Payments



## Why Electronic Payments?

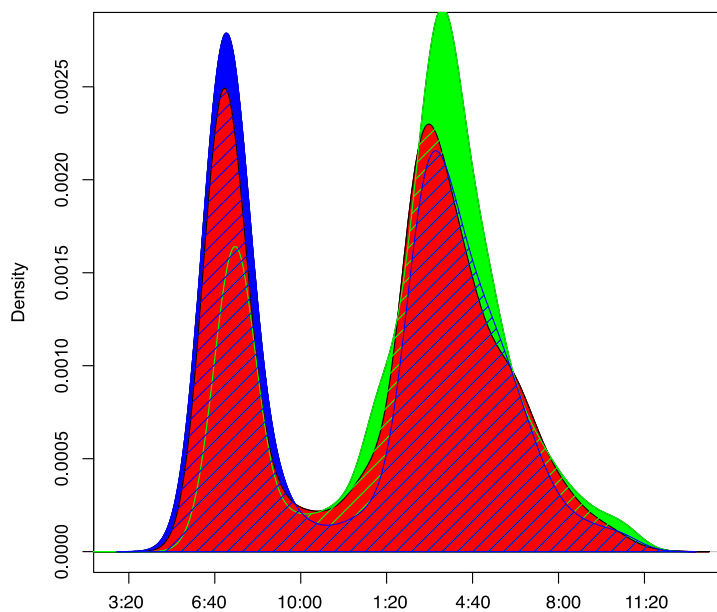
- Throughput and convenience
- Reduced revenue collection cost
- Variable and Dynamic pricing
- Collection of *meaningful* data



# Data extracted from Boston MBTA data-set

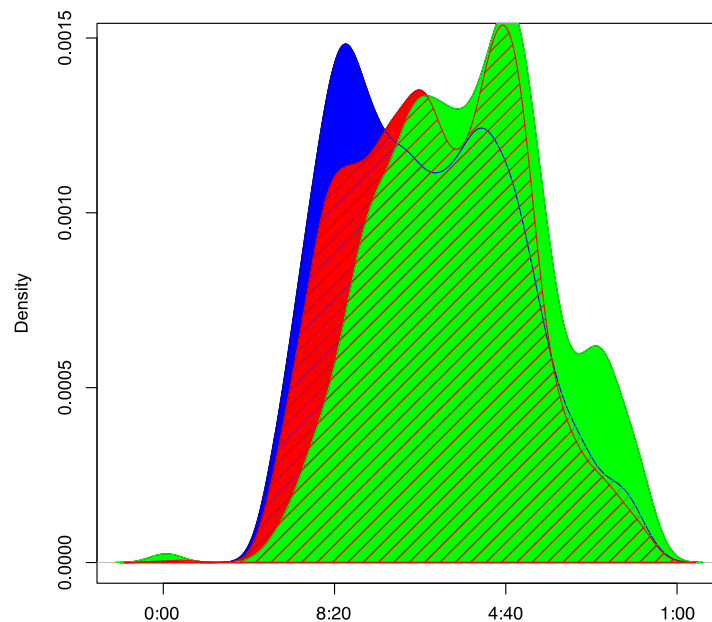
Riders are willing to offer some information for a reduced fare!

### Students



N = 6868 Bandwidth = 43.31

### Seniors



N = 4946 Bandwidth = 42.01

- Green = Bus line 1000
- Red = Bus line 1100
- Blue = Bus line 1300

### Uses of Data?:

- Advertising
- Services
- Security/Safety

# Public Transportation Payments

## Hacking the T: MBTA sues to keep MIT students from telling how they cracked the CharlieCard

By adamg - 8/

UPDATE: The discussing th

Wired repor convention t

The trans "publicly system h further s that wou

A hearing is

## Hackers Crack London Tube's Ticketing System

BY ALEXANDER

## Some call T's new Charlie Card an invasion of privacy But agency

## Card Passenger Tracking

October 16, 2012 5:34 PM

By Mac Dani

When T rider fear, commut

The new auto Aquarium an computer chi gates.

The new card by the Massa started on Sil

The technolo riders, cut do said



A passenger uses a Clipper card at a fare gate. (CBS)

Share 1

The Boston Globe

Like 2

Tweet 4



Share 3

View Co

SAN FRANCISCO (CBS 5) – Clipper Card holders may be unaware that the Metropolitan Transportation Commission stores information on their public transit movements for years, potentially allowing authorities track your previous locations.

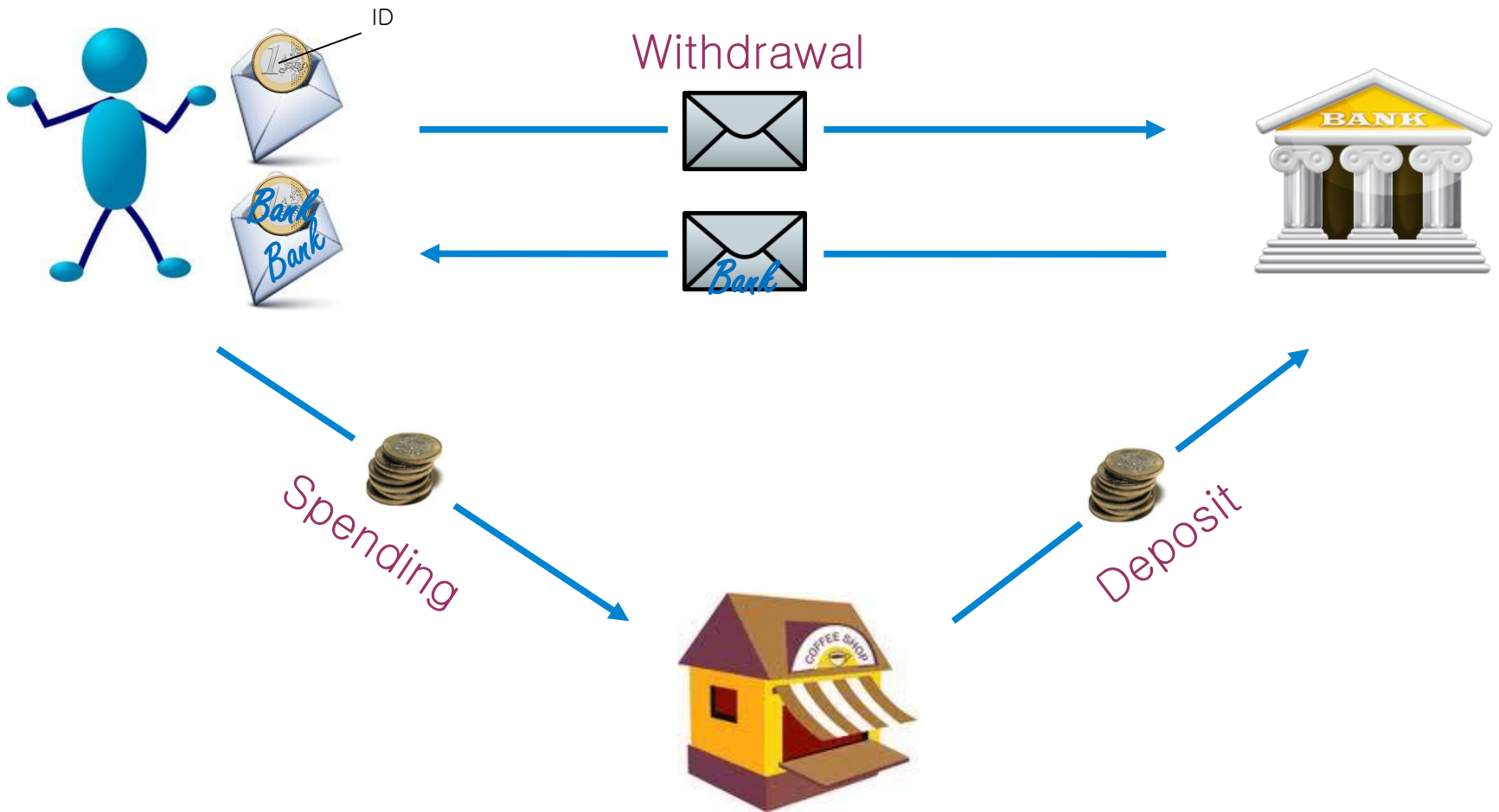
There are a million such fare cards used in the Bay Area at several transit agencies. When you register with the Metropolitan Transportation Commission when you buy it, police can

Filed Under

subscribe your records to show where you have and have n

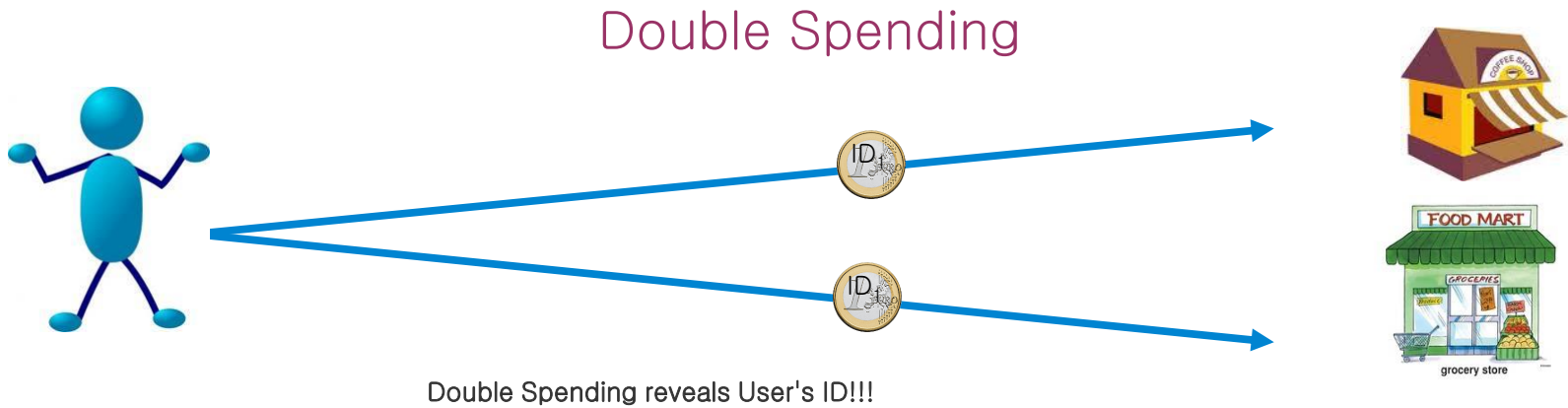
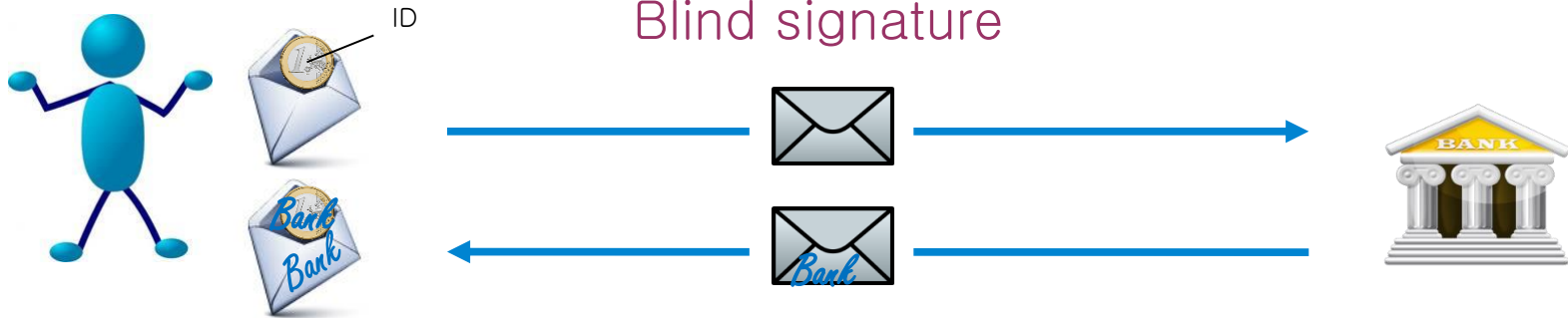
# E-cash

Chaum, 1982  
Brands, 1992





# E-cash



# E-cash in Public Transport

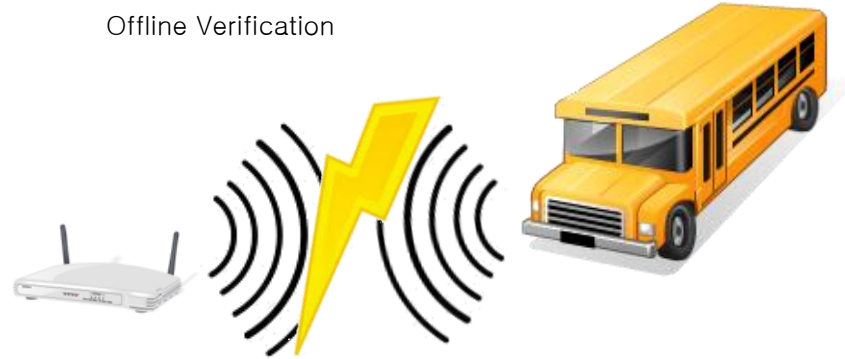
Different Denominations



Modular Payment Systems



Offline Verification



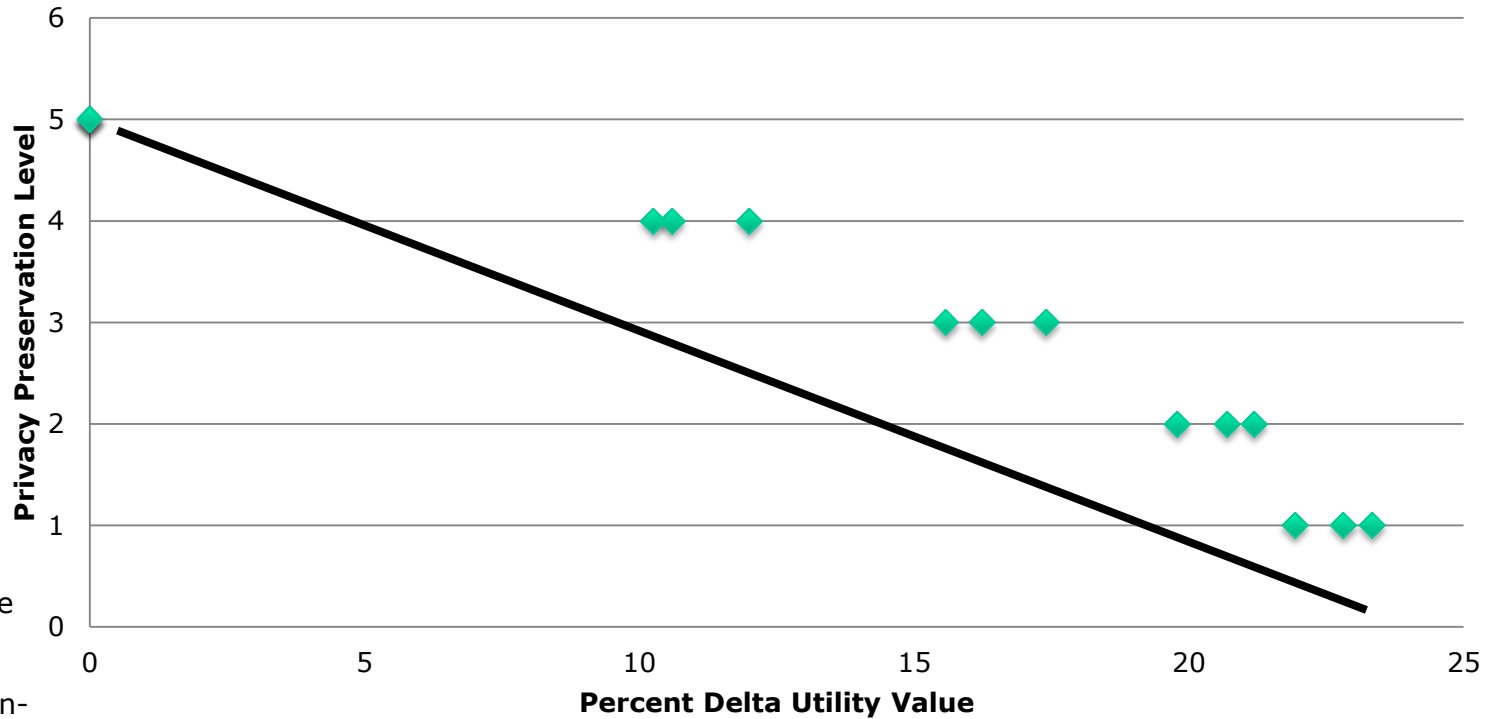
Encoding of attributes

- >67 Age
- 01003 Postal Code
- no Wheelchair access
- 6/10/14 Coin expiration



# Privacy Utility Tradeoffs

**Privacy Preservation vs Data Utility**



- User residence
- User income
- User politics
- User education-level
- User vehicle ownership
- ...

Ability to predict user choice of public vs. private transportation  
(Skelley and Collura, 2013)

# Which E-cash scheme?

- What we want:
  - Offline
  - Provable security
  - Efficient
  - Encoding of attributes
- Brands' untraceable offline cash scheme [Bra93]
  - Most efficient during spending phase
  - Blind signature not proven secure [BL12]
- Abe's scheme [Abe01]
  - Security proof, while only little less efficient
  - No encoding of attributes
- Anonymous Credentials Light [ACL12]
  - Based on Abe
  - Allows the encoding of attributes and has security proof







[Bra93] S. Brands. Untraceable Off-line Cash in Wallets with Observers. CRYPTO 1993

[Abe01] M. Abe. A secure three-move blind signature scheme for polynomially many signatures. EUROCRYPT 2001

[BL12] F. Baldimtsi, A. Lysyanskaya. On the security of one-witness blind signature schemes. IACR Crypto ePrint, 2012

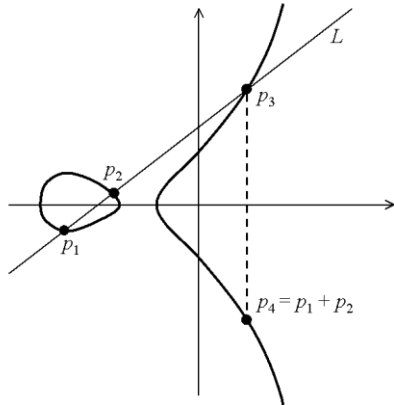
[ACL12] F. Baldimtsi, A. Lysyanskaya. Anonymous Credentials Light. IACR Crypto ePrint, 2012

# Brands' Scheme on RFID Tag

Withdrawal	 12 Exponentiations	 2 Exponentiations
Spending	 0 Exponentiations	 2 Exponentiations



Certicom ECC for implementation



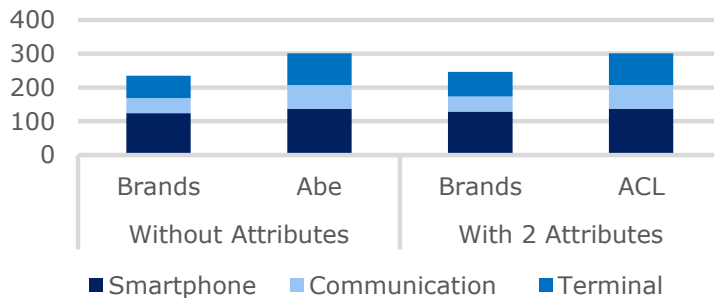
	Cycle Count	Execution time @16 MHz
Brands' withdrawing one coin	69 120 181	4.32 s
Brands' spending one coin	35 052	0.0022 s

G. Hinterwalder, C. Paar, and W.P. Burleson. Privacy Preserving Payments on Computational RFID Devices with Application in Intelligent Transportation Systems. RFIDsec 2012, Nijmegen, Netherlands.

# NFC-smartphone e-cash implementation

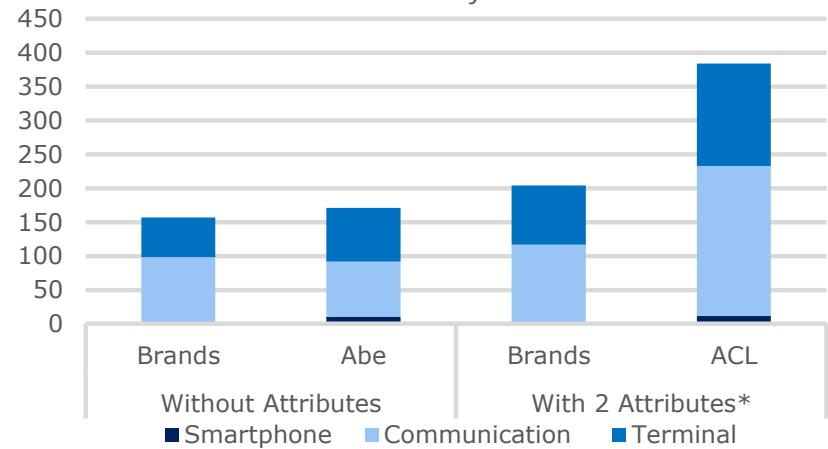


Execution time for **withdrawing** one coin on BlackBerry Bold 9900



All times in milli-seconds

Execution time for **spending** one coin on BlackBerry Bold 9900



\* when showing both

G. Hinterwalder, C. T. Zenger, F. Baldimtsi, A. Lysyanskaya, C. Paar, W. P. Burleson. Efficient E-cash in Practice: NFC-based Payments for Public Transportation Systems. To appear at 13th Privacy Enhancing Technologies Symposium (PETS 2013), Bloomington, USA.



# P4R: Prepayments with Refunds



A. Rupp, G. Hinterwalder, F. Baldimtsi, C. Paar. P4R: Privacy-Preserving Pre-Payments with Refunds for Transportation Systems. In Financial Cryptography and Data Security 2013 (FC 2013), Okinawa, Japan.

# P4R: Security/Privacy issues

- Transportation authority security
  - User cannot forge tickets
  - User cannot receive refunds that exceed the overall deposit for tickets minus the overall fare of trips
- User security
  - A passive adversary cannot steal tickets or refunds from a user
- User privacy
  - Adversary cannot differentiate between all possible trip sequences leading to the same total refund amount
- Features
  - Allows distance-based pricing (eg. even where exit is not known at time of boarding)
  - Allows dynamic variable pricing (eg. reduced fares on overcrowded buses, delayed trains, etc.)
- **Open Problem:** How can user prove they paid (to police on train) without revealing identity?

# Implantable and Wearable Medical Devices

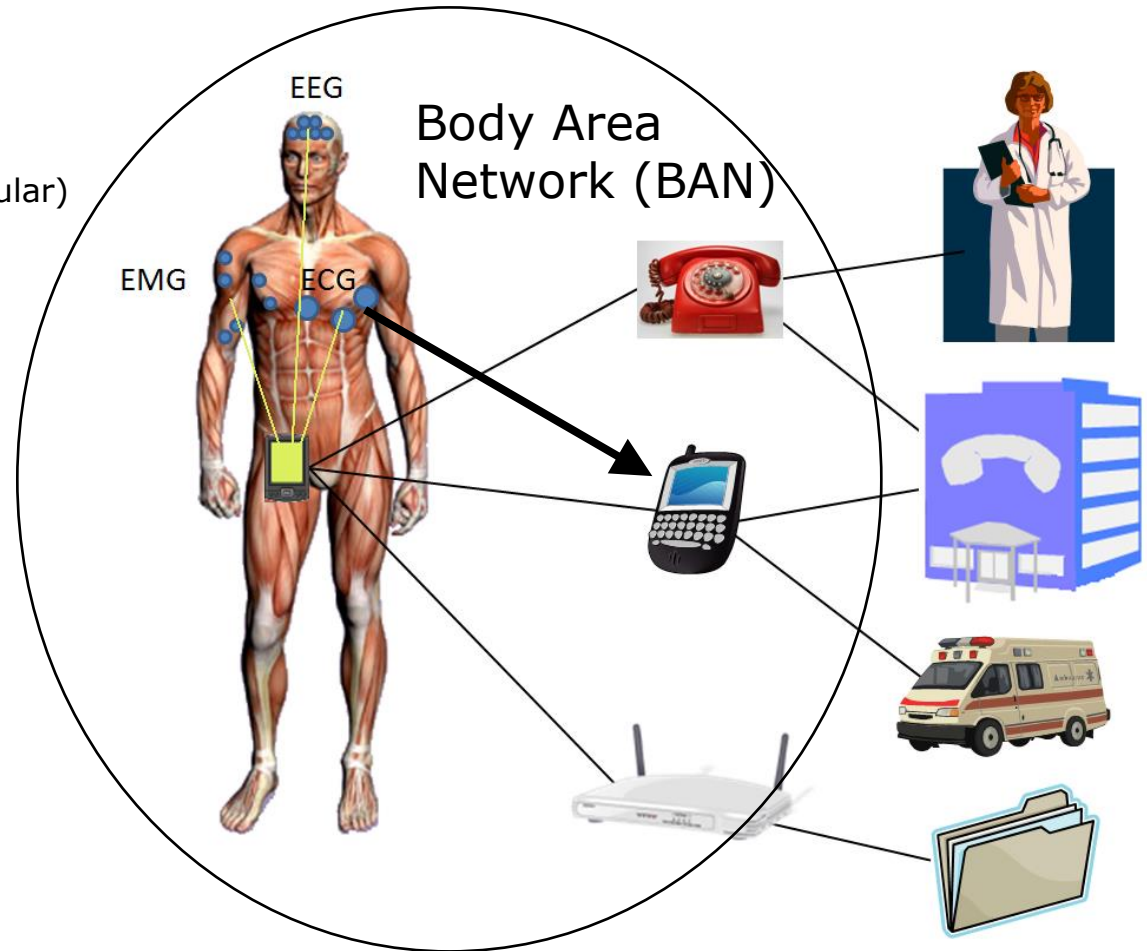
- **Bio-Medical**

- EEG Electroencephalography
- ECG Electrocardiogram
- EMG Electromyography (muscular)
- Blood pressure
- Blood SpO2
- Blood pH
- Glucose sensor
- Respiration
- Temperature
- Fall detection
- Ocular/cochlear prosthesis
- Digestive tract tracking
- Digestive tract imaging

- **Sports performance**

- Distance
- Speed
- Posture (Body Position)
- Sports training aid

- **Cyber-human interfaces**



# Security and Privacy in Implantable Medical Devices

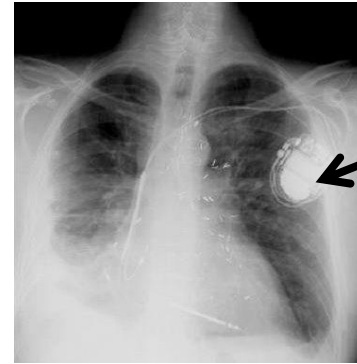
1. IMD's are an increasingly important technology
  - Leveraging many recent technologies in Nano/Bio/Info
  - Possible solutions to major societal problems
    - Clinical
    - Research
  - Many types of IMDs (see taxonomy coming up)
2. Security and Privacy increasingly relevant in modern society
  - Fundamental human rights
  - Quality of life, Related to safety/health
  - Acceptance of new technologies

*Combining 1. and 2., IMD Security and Privacy involves:*

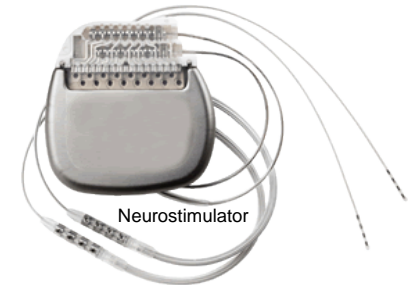
- *Protecting human life, health and well-being*
- *Protecting health information and record privacy*
- *Engineering Challenges!*

# IMD Examples

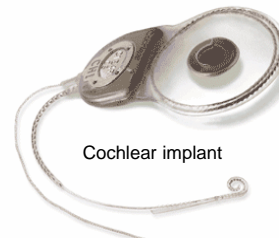
- Existing
  - Glucose sensor and insulin pump
  - Pacemaker/defibrillator
  - Neuro-stimulator
  - Cochlear implant
- Emerging
  - Ingestible “smart-pills”
  - Drug delivery
  - Sub-cutaneous biosensor
  - Brain implant
  - Deep cardiac implant
  - Smart Orthodontia
  - Glaucoma sensors and ocular implants
- Futuristic
  - Body 2.0 - Continuous Monitoring of the Human Body
  - Bio-reactors
  - Cyber-human Interfaces



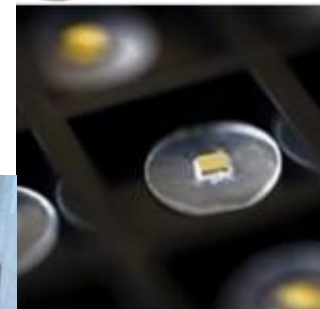
Pacemaker - Medtronic



Neurostimulator



Cochlear implant



Smart pill - Proteus biomedical

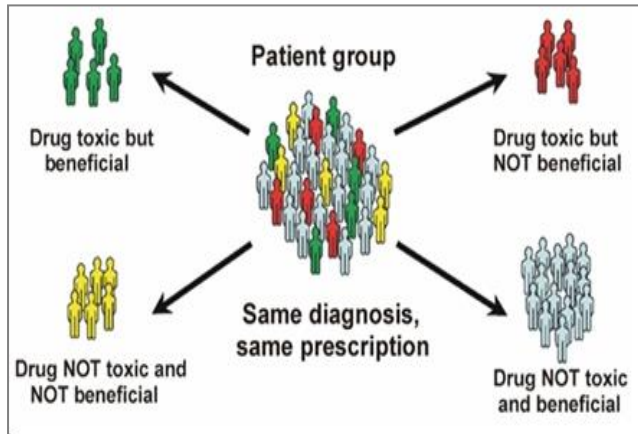


Subcutaneous biosensor - EPFL-Nanotera



concept illustration from [yankodesign](http://yankodesign.com)

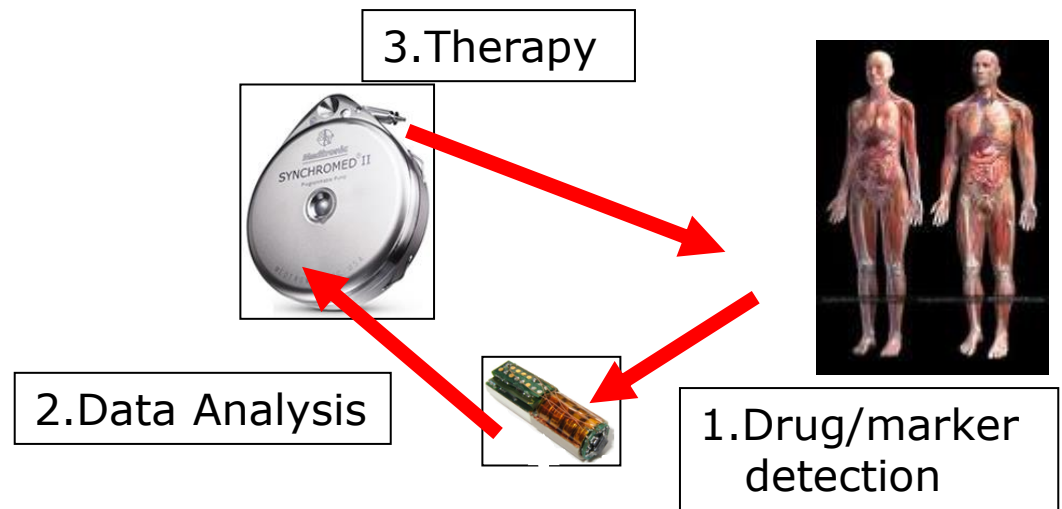
# Personalized Therapies with multiple IMDs



Therapeutic area	Rate of efficacy with standard drug treatment
Cancer (all types)	25%
Alzheimer's disease	30%
Incontinence	40%
Hepatitis C	47%
Osteoporosis	48%
Rheumatoid arthritis	50%
Migraine (prophylaxis)	50%
Migraine (acute)	52%
Diabetes	57%
Asthma	60%
Cardiac arrhythmias	60%
Schizophrenia	60%
Depression	62%

For depression, the data apply specifically to the drug class known as selective serotonin reuptake inhibitors.

Source: Brian B. Spear, Margo Heath-Chiozzi, and Jeffrey Huff, "Clinical Application of Pharmacogenetics," *Trends in Molecular Medicine* (May 2001).



The Development of new Implantable Medical Devices is a key-factor for succeeding in Personalized therapy



# Smart pills

***Raisin***, a digestible, ingestible microchip, can be put into medicines and food. Chip is activated and powered by stomach acids and can transmit to an external receiver from within the body! Useful for tracking existence and location of drugs, nutrients, etc.

*"...there's more silicon in a banana..." - Proteus CTO*



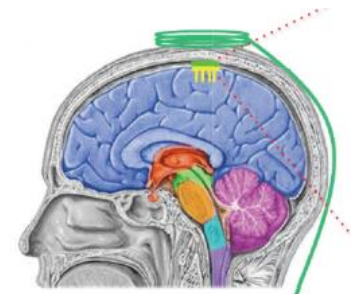
Ingestible Raisin microchip

# Axes for a taxonomy of IMDs

- Physical location/depth, procedure, lifetime,
- Sensing/Actuating functions, (sense, deliver drugs or stimulus, grow tissue!)
- Computational capabilities
- Data storage
- Communication: bandwidth, up-link, down-link, inter-device? Positioning system (IPS), distance to reader, noise
- Energy requirements, (memory, communication, computation,) powering, harvesting, storage, (battery or capacitive)?
- Vulnerabilities. Security functions (access control, authentication, encryption)
- Reliability and Failure modes

# Power/Energy Challenges

- Remote powered systems (RFID) limited to 10's of microwatts
- Near field powering improves this to milliwatts
- Current energy harvesting systems similarly limited...
  
- Small batteries typically store several 1000 Joules.
- Over several years of operation, this translates to 10's of microwatts
  
- Batteries are still large and heavy
- Rechargeable batteries dissipate heat and have safety concerns
- Non-rechargeable batteries require surgery for replacement
  
- Brain implants can not incur more than 1 degree temperature gradient without safety concerns



[Courtesy: Subbu Venkatraman]

# Security Goals for IMD Design

- Incorporate security **early**.
- **Encrypt** sensitive traffic.
- **Authenticate** third-party devices.
- Use well-studied cryptographic building blocks.
- Do not rely on **security through obscurity**.
- Use industry-standard source-code analysis.
- Develop a realistic **threat model**.

W. Burleson, B. Ransford, S. Clark, K. Fu, "Design Challenges for Secure Implantable Medical Devices", DAC, 2012

# Threat model – Understand your adversary!

- Motives:
  - Violence
  - Identity Theft
  - Insurance fraud
  - Counterfeit devices
  - Discrimination
  - Privacy
- Resources:
  - Individual
  - Organization
  - Nation-state...
- Attack vectors:
  - Wireless interfaces (eavesdropping, jamming, man-in-middle)
  - Data/control from unauthenticated sources
  - Data retention in discarded devices

# Privacy threat taxonomy

- D. Kotz, (Dartmouth)  
**A threat taxonomy for mHealth privacy,**  
NetHealth 2011

TABLE I  
PRIVACY-RELATED THREATS IN MHEALTH SYSTEMS

## Identity threats: mis-use of patient identities

---

patients	leave PHR credentials on public computer (identity loss)
patients	share passwords with outsiders (identity sharing)
patients	reveal passwords to outsiders (social-engineering attack)
insiders	mis-use identities to obtain reimbursement (insurance fraud) [12]
insiders	mis-use identities to obtain medical services (identity theft) [13]
outsiders	mis-use identities to obtain medical services (identity theft) [13]
outsiders	re-identifying PHI in de-identified data sets [14]
outsiders	observe patient identity or location from communications

## Access threats: unauthorized access to PHI or PHR

---

patients	consent preferences, as expressed, do not match those desired
patients	intentional (or unintentional) access beyond authorized limit
patients	mistaken modifications, because of over-privilege or inadequate controls
insiders	mistaken modifications, because of over-privilege or inadequate controls [15]
insiders	intentional unauthorized access, for curiosity or malice [15], [16]
insiders	intentional modifications, to obtain reimbursement (insurance fraud) [12]
outsiders	intentional unauthorized access, for curiosity or malice [17]
outsiders	intentional modifications, for fraud or malice [17]

## Disclosure threats: unauthorized disclosure of PII and PHI

---

### data at rest, in the PHR:

patients	inadvertent disclosure due to malware or file-sharing tools [13]
insiders	inadvertent disclosure due to malware or file-sharing tools [13]
insiders	inadvertent disclosure due to sharing passwords [15]
insiders	intentional disclosure, for profit or malice [16]
outsiders	intentional disclosure, for profit or malice [16]

### data at rest, in the mobile devices:

patients	loss of MN or SN exposes PHI, keys, SN types, sensing tasks
outsiders	theft of MN or SN exposes PHI, keys, SN types, sensing tasks

### data in transit:

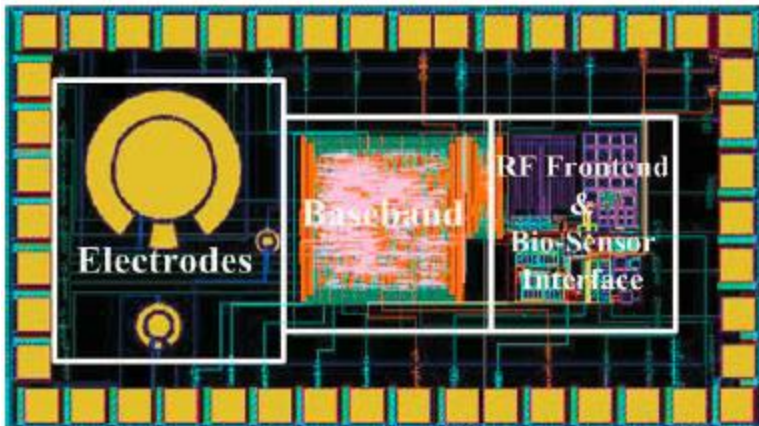
outsiders	eavesdrop on SN-MN, MN-PHR, PHR-PHR, PHR-client; traffic analysis and/or content decryption [18, for example]
outsiders	observe presence and type of sensors on patient [19]

---

# Lightweight Cryptography for Bio-sensors

## Hummingbird Stream Cipher

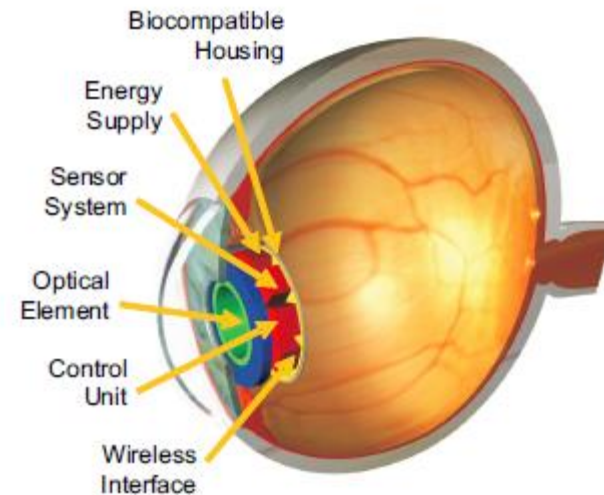
Glucose sensor



S. Guan, J. Gu, Z. Shen, J. Wang, Y. Huang, and A. Mason. **A wireless powered implantable bio-sensor tag system-on-chip for continuous glucose monitoring.** BioCAS 2011.

## AES Block Cipher


Ocular implant

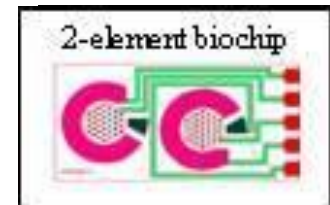


C. Beck, D. Masny, W. Geiselmann, and G. Bretthauer. **Block cipher based security for severely resource-constrained implantable medical devices.** International Symposium on Applied Sciences in Biomedical and Communication Technologies, ISABEL 2011.



# Secure Platform for Bio-sensing (Umass, EPFL, Bochum)

- Applications
  - Disposable Diagnostic
    - Low-cost, infectious disease detection (malaria, HIV, dengue, cholera)
    - DNA
  - Implantable Device
    - Sub-cutaneous multi-function sensor (drugs, antibodies)
    - Glucose/Lactate in Trauma victims
- Security Technology 
  - KECCAK (Authenticated Encryption)
  - PUF for low-cost ID and Challenge-Response
  - TRNG for crypto-primitive



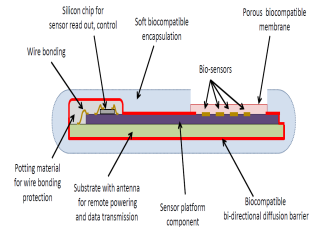
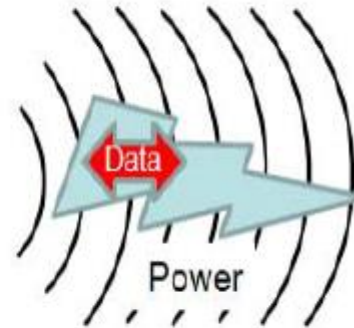
Images: Disposable Diagnostic: Gentag.com,  
Sub-cutaneous Implant: LSI, EPFL, NanoTera  
2-element biochip: CBBB, Clemson University

# Mobile – patch – implant

Bluetooth

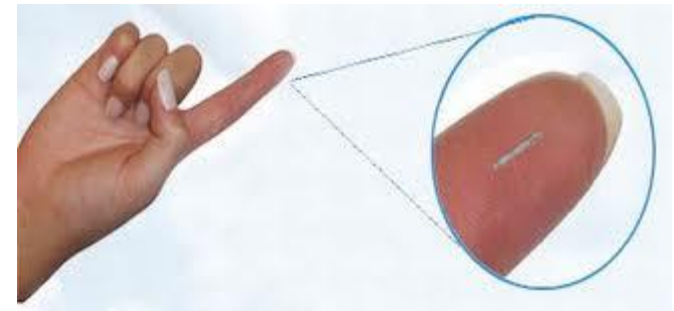


RFID/NFC



## Patch to Sensor communication:

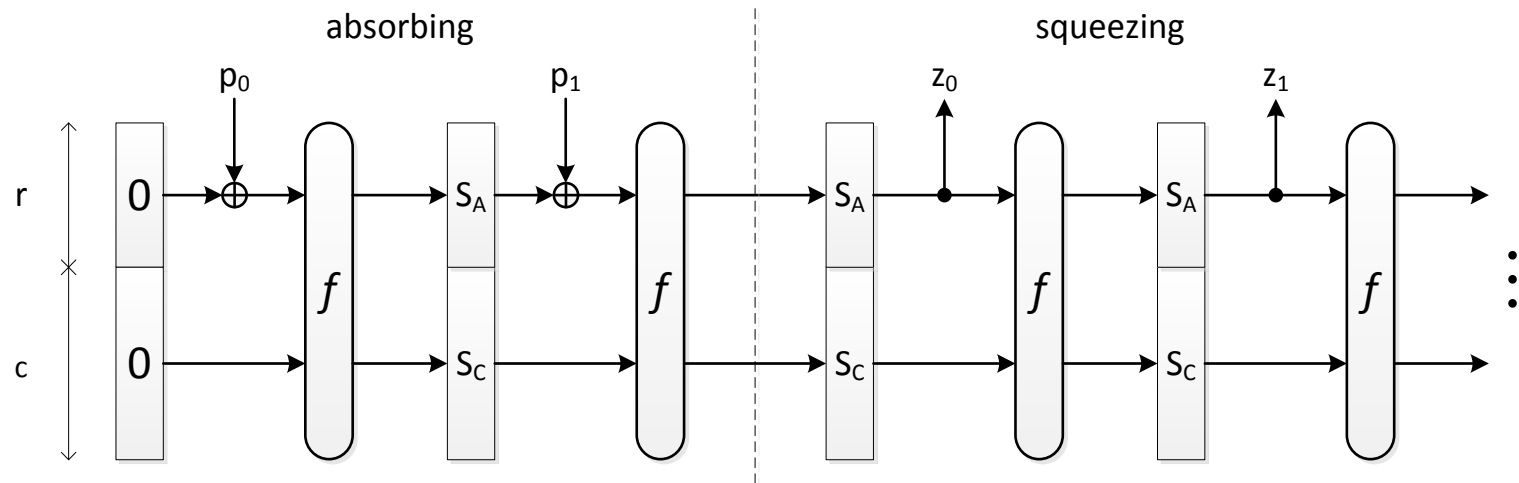
- (Very ) Low data-rates
- Implanted
  - hard to lose/steal/tamper!
- Short range
- Known orientation



# Authenticated Encryption: Resource-Efficient Schemes

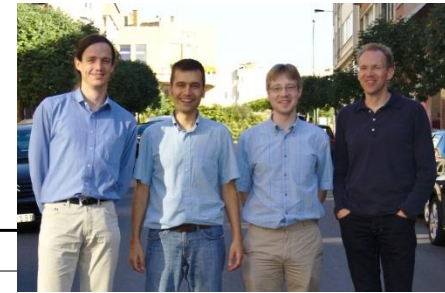
- Hummingbird-2 authenticated encryption algorithm
  - Very compact – as low as 2.2K GE!
  - The fastest version requires 4 cycles/word
- ALE – Authenticated Lightweight Encryption
  - AES-based scheme – Only 4 rounds used
  - Authentication part of encryption process
  - Not TOO light and not too fast (high-latency in AES rounds)
- Sponge-based authenticated encryption (SHA-3 - KECCAK)
  - Introduced after the “birth” of sponge functions
  - Uses the same sponge permutation for both encryption and authentication

# Sponge Functions



- Introduced during the SHA-3 competition with KECCAK
  - Permutation-based
  - Variable input length – pushed into the state during “absorbing,, phase
  - Arbitrary output – extracted from the state during “squeezing,, phase

# KECCAK



[Gilles Van Assche](#)<sup>1</sup>  
[Guido Bertoni](#)<sup>1</sup>, [Michaël Peeters](#)<sup>2</sup> [Joan Daemen](#)<sup>1</sup>  
<sup>1</sup>[STMicroelectronics](#)  
<sup>2</sup>[NXP Semiconductors](#)

---

## Pseudo-code of KECCAK- $f$

---

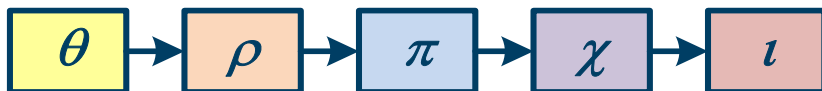
KECCAK- $f[b](A)$

- for  $i$  in  $0 \dots n_r - 1$   
   $A = \text{Round}[b](A, RC[i])$
- return  $A$

$\text{Round}[b](A, RC)$

- $\theta$  step:  
   $C[x] = A[x, 0] \oplus A[x, 1] \oplus A[x, 2] \oplus A[x, 3] \oplus A[x, 4], \forall x$  in  $0 \dots 4$   
   $D[x] = C[x - 1] \oplus \text{ROT}(C[x + 1], 1), \forall x$  in  $0 \dots 4$   
   $A[x, y] = A[x, y] \oplus D[x], \forall (x, y)$  in  $(0 \dots 4, 0 \dots 4)$
  - $\rho$  and  $\pi$  steps:  
   $B[y, 2x + 3y] = \text{ROT}(A[x, y], r[x, y]), \forall (x, y)$  in  $(0 \dots 4, 0 \dots 4)$
  - $\chi$  step:  
   $A[x, y] = B[x, y] \oplus ((\text{NOT}B[x + 1, y] \text{ AND } B[x + 2, y]), \forall (x, y)$  in  $(0 \dots 4, 0 \dots 4)$
  - $\chi$  step:  
   $A[0, 0] = A[0, 0] \oplus RC$
  - return  $A$
- 

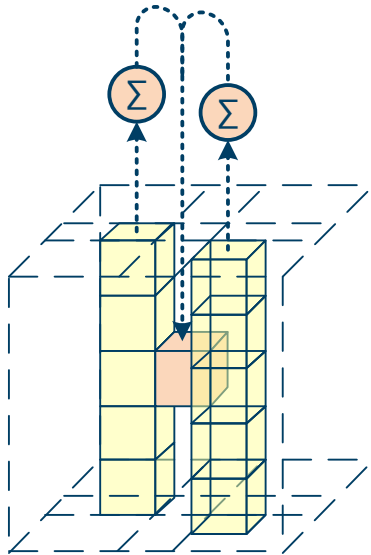
- Permutation function  $f$  :



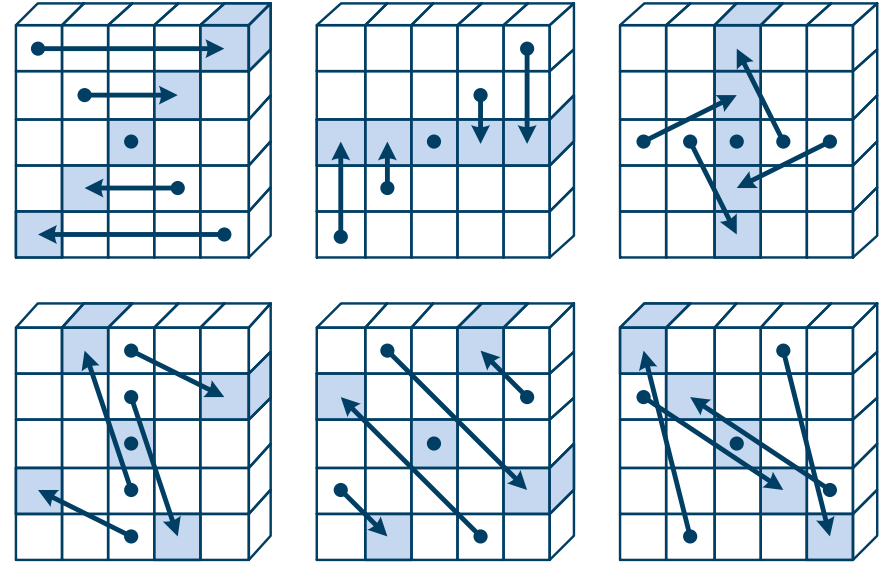
- State organized as a  $5 \times 5$  matrix of  $2l$ -bits ( $l=64$ )
- $r=1088, c=512$

# KECCAK Permutation Steps

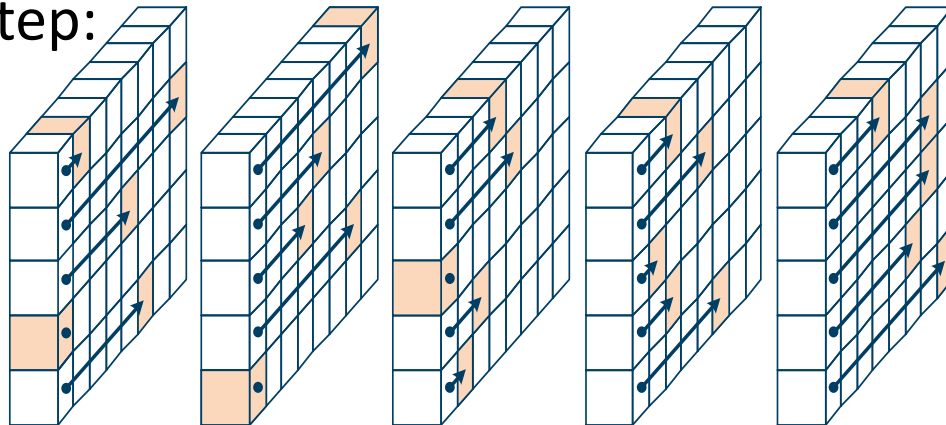
•  $\theta$  Step:



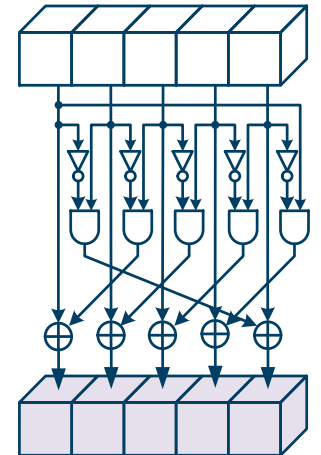
•  $\pi$  Step:



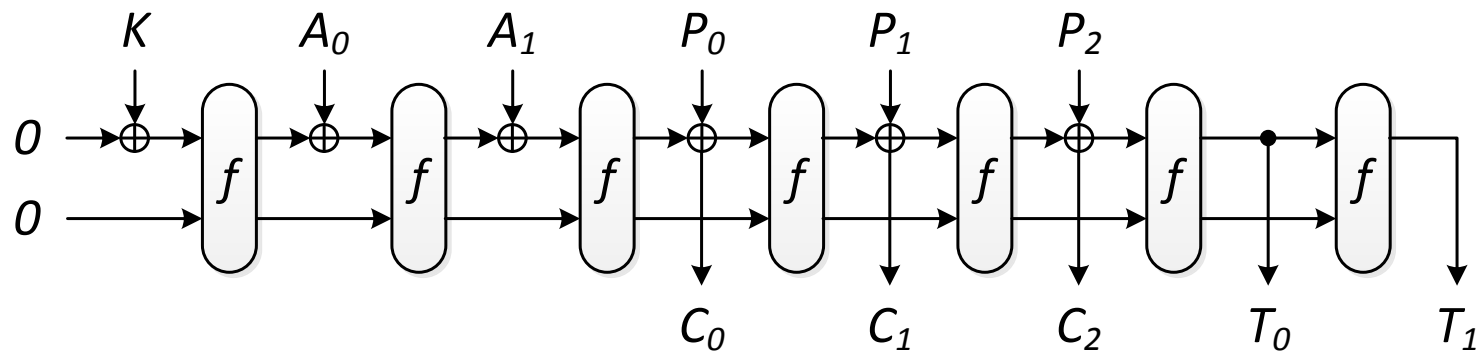
•  $\rho$  Step:



•  $\chi$  Step:



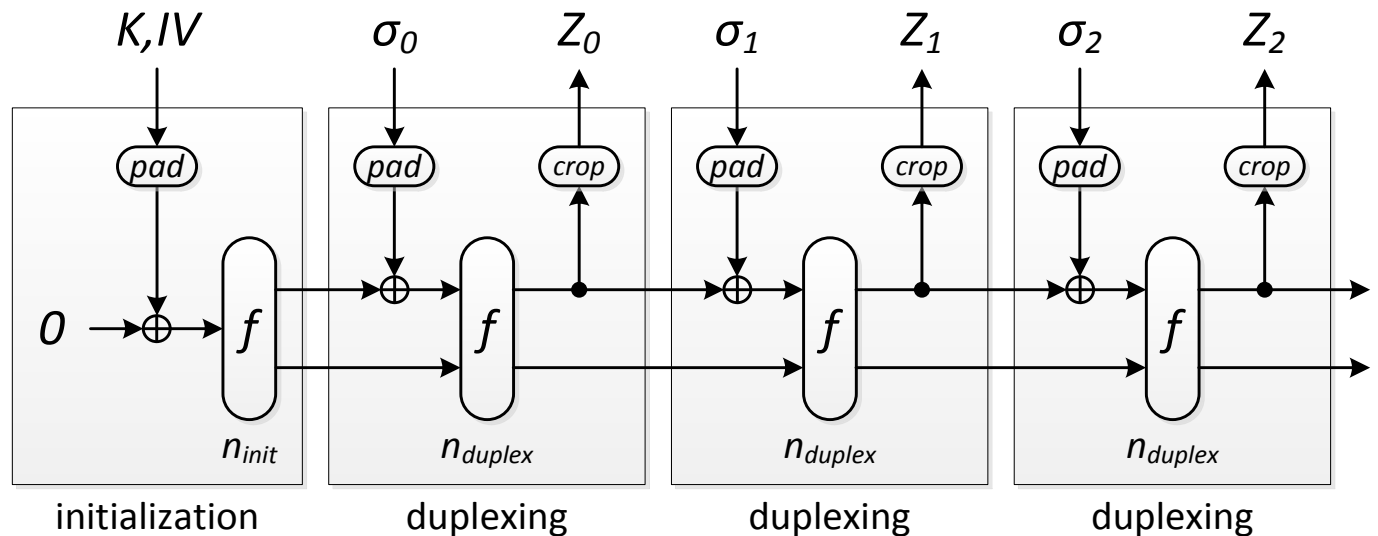
# Permutation-based Authenticated Encryption: SpongeWrap



- Key added onto the zero initial state
  - Followed by absorption of additional authentication data (AAD) into the state
- Each new plaintext is XORed with the internal state to generate a new ciphertext (similar to counter mode of operation)
  - Also absorbed into the internal state
- Message digest (with desired length) squeezed from internal state

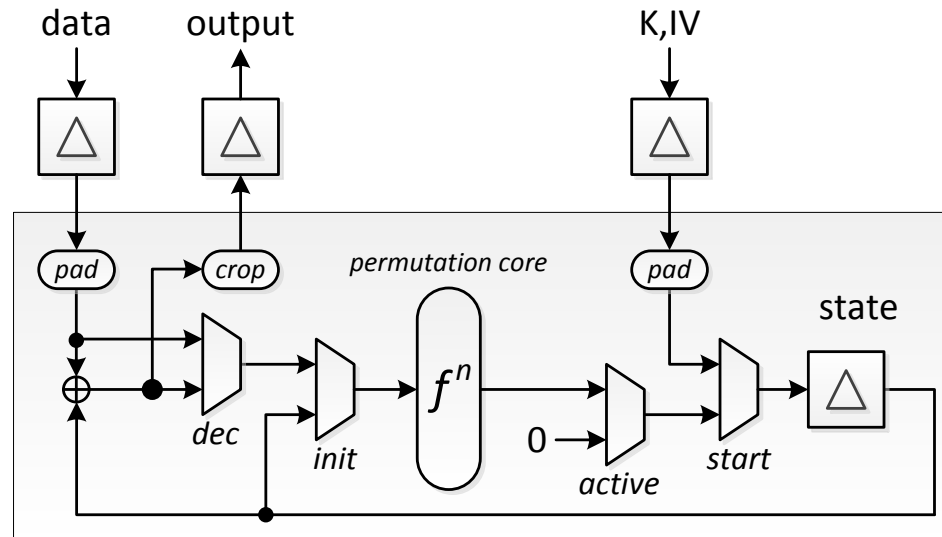


# Permutation-based Authenticated Encryption: DuplexSponge



- Based on SpongeWrap – run in duplex mode
  - Requires a unique IV – fragile, but considerably more secure
  - Number of duplex rounds as low as “1,, – extremely low latency → high data rates

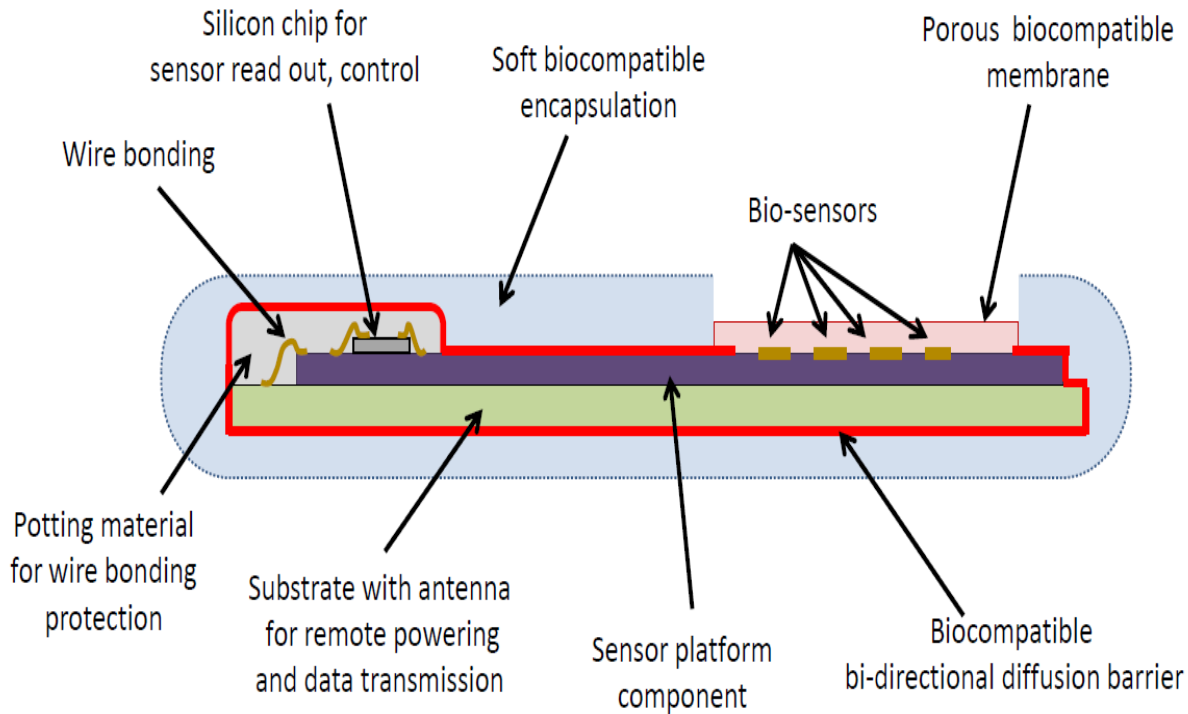
# Implementation Aspects



- Keccak-100 selected
- 93-bits of security:  $100 - 4(\text{data rate}) - 3(\text{padding and parity})$
- 320 cycles for initial key processing, 80 cycles per 16 bits of data
- Only 1550 GE for the authenticated encryption core
- 2280 GE including interface wrapper
- $< 7 \mu\text{W}$  @500 KHz

# Implantable bio-sensor

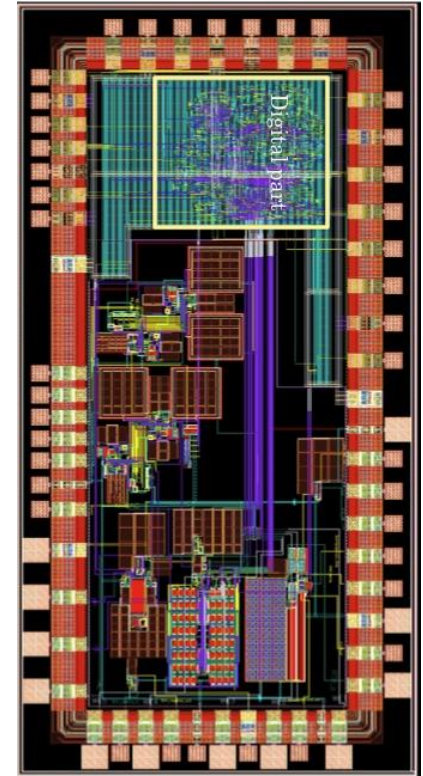
3mm x 5mm



S. Carrara, G. DeMicheli, EPFL, Nanotera

**Open Problem: Key distribution in IMDs? PUFs? DNA?**

Prototype mixed-signal IC 180nm, sensor circuitry, I/O, crypto



S. Ghoreishizadeh, EPFL,  
A. Pullini, EPFL  
T. Yalcin, Bochum  
W. Burleson, UMass

# Protecting existing IMDs

- Gollakota et al (MIT, UMASS), They Can Hear Your Heartbeats: Non-Invasive Security for Implanted Medical Devices, **SIGCOMM 2011 (Best Paper)**

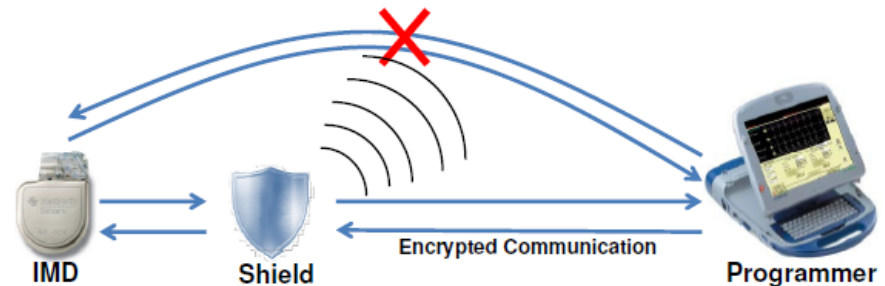


Figure 1—Protecting an IMD without modifying it: The shield jams any direct communication with the IMD. An authorized programmer communicates with the IMD only through the shield, with which it establishes a secure channel.

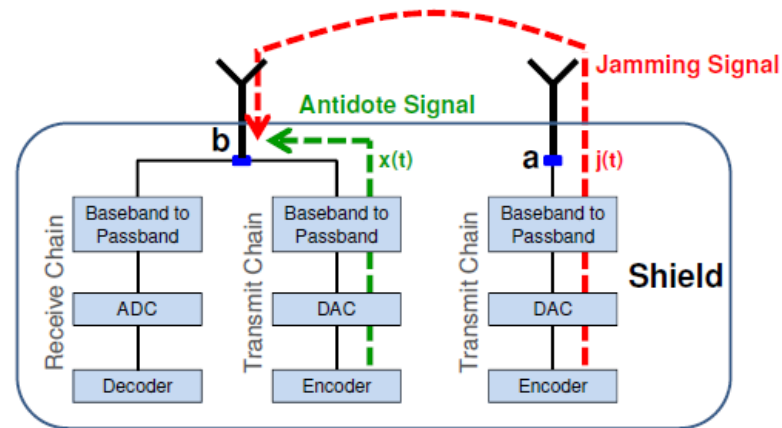


Figure 2—The jammer-cum-receiver design uses two antennas: a jamming antenna that transmits the jamming signal, and a receive antenna. The receive antenna is connected to both a transmit and receive chain. The antidote signal is transmitted from the transmit chain to cancel out the jamming signal in the receive chain.

# Design Tension Challenges

## **Security/Privacy goals**

- Authorization (personal, role-based, IMD selection)
- Availability
- Device software and settings
- Device-existence privacy
- Device-type privacy
- Specific-device ID privacy
- Measurement and Log Privacy
- Bearer privacy
- Data integrity

## **Safety/Utility goals**

- Data access
- Data accuracy
- Device identification
- Configurability
- Updatable software
- Multi-device coordination
- Auditable
- Resource efficient

# Design for Medical is different!

“Medical marches to a different cadence than most of the electronics industry. Design cycles can stretch from **three to five years** and cost \$10-15 million, thanks to the lengthy regulatory process. The product lifecycles can also extend over a **20 year** time span.”

*Boston Scientific*

- **What is the role of FDA and other regulators?**
  - FDA currently regulates safety, but not security

## **Security and Privacy for Implantable Medical Devices**

Burleson, Wayne; Carrara, Sandro (Eds.)

2014, XII, 202 p.

96 illus., 74 illus. in color.

ISBN 978-1-4614-1673-9

Due: October 31, 2013

Available Formats:

eBook

Hardcover



- Describes problems of security and privacy in implantable medical devices and proposes solutions
- Includes basic abstractions of cryptographic services and primitives such as public key cryptography, block ciphers and digital signatures
- Provides state-of-the-art research of interest to a multidisciplinary audience in electrical, computer and bio-engineering, computer networks and cryptography and medical and health sciences

**Content Level** » Professional/practitioner

**Keywords** » Biochip Safety and Reliability - Embedded Systems - Hardware Security - IMD Security - Implantable Biochip - Lightweight Security - Secure Body Area Network - Secure Implantable Medical Devices - Secure Integrated Circuits - Security in Embedded Systems

**Related subjects** » Biomedical Engineering - Circuits & Systems - Security and Cryptology

### **Table of contents**

Introduction.- Blood Glucose Monitoring Systems.- Wireless system with Multi-Analyte Implantable Biotransducer.- New Concepts in Human Telemetry.- In Vivo Bioreactor – New Type of Implantable Medical Devices.- Segue.- Design Challenges for Secure Implantable Medical Devices.- Attacking and Defending a Diabetes Therapy System.- Conclusions and A Vision to the Future.



in the USA...



SHARPS

## Strategic Healthcare IT Advanced Research Projects on Security

sharps.org

- SHARPS is a multi-institutional and multidisciplinary research project, supported by the Office of the National Coordinator for Health Information Technology, aimed at reducing security and privacy barriers to the effective use of health information technology. The project is organized around three major healthcare environments:
  - **Electronic Health Records (EHR)**
  - **Health Information Exchange (HIE)**
  - **Telemedicine (TEL)**
- A multidisciplinary team of computer security, medical, and social science experts is developing security and privacy policies and technology tools to support electronic use and exchange of health information.
- UIUC, Stanford, Berkeley, Dartmouth, CMU, JHU, Vanderbilt, NYU, Harvard/BethIsrael, Northwestern, UWash, UMass

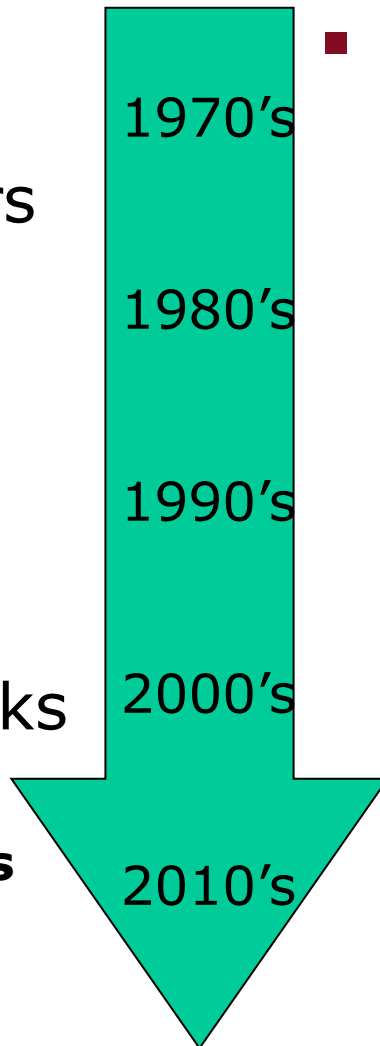
# The Future

- Pay as you \*
  - Consume
  - Dispose,...
- Future Platforms
  - Other remotely powered devices
  - Harvested power
- Future Privacy Threats
  - Side-channels
  - Big-data

# Trends in VLSI Research

## ■ Driving Applications

- Microprocessors
- DSP
- Video
- Wireless
- Hand-sets
- Smart Cards
- Sensor Networks
- **RFID**
- **Internet of Things**
- ...



## ■ Design Challenges

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

# Conclusions

- RFID takes many forms
  - If humans carry RFID in or on their person, privacy issues arise
  - Solutions vary depending on requirements
    - Algorithm
    - Implementation
- Much work to be done
  - Cyber-physical and cyber-human systems
  - Many exciting new applications
  - Many possible new threats
- Internet of Things – Privacy of Things

Thank you for your attention!  
And your questions!

Backup/Q&A slides

# Bio-sensors for hemorrhaging trauma victims

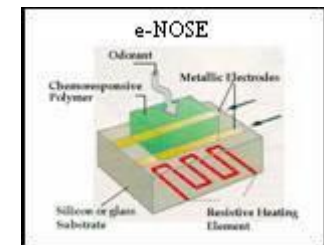
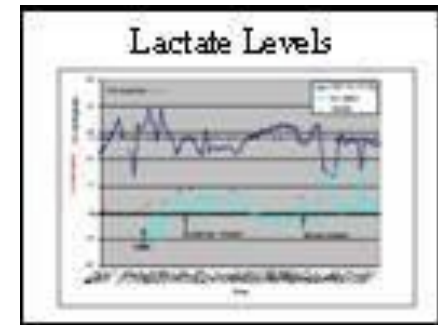
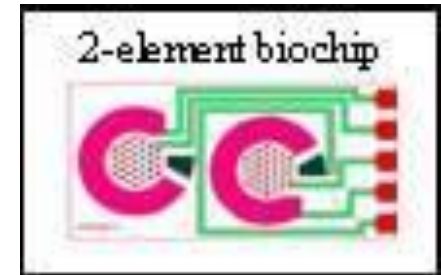
Implantable biosensor for monitoring lactate and glucose levels. Funded by the US Department of Defense

Developing a temporary implantable dual sensing element biochip with wireless transmission capabilities.

Applications in mass triage scenarios such as battlefields and natural disaster sites provide a means for medical personnel to make life saving decisions.

**Low-cost, short life-time, rapid deployment, life-saving**

Future applications in diabetes care, transplant organ health, and intensive care.



# Thoughts on: Privacy-preserving transportation payments

- **E-cash plus attributes** allow users to opt-in to possible tracking and 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) . Attributes 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, et al.) 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. See: *Contextual privacy* by H. Nissenbaum, 2012.
- **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).

# Security and Privacy Design Issues

- System Requirements
  - Sensor/Actuator Functionality, Software updates
  - Communications: Data-rate (>100kbps), Range/Channel (BAN)
  - Protocol Design: Asymmetric channel, ( Active RFID)
- Design Constraints
  - Power (battery-powered, harvested, or remote-powered device)
  - Size, Bio-compatibility, calibration
  - Long life-time, little maintenance, reliability
- Security Analysis
  - Assets: Human health and well-being, personal and health data
  - Threats: Device cloning and counterfeiting, Eavesdropping, Physical Layer Detection and Identification,
- Security Primitives
  - Public and private key crypto, block and stream ciphers, TRNG, PUF
  - Secure radios, Distance-bounding protocols, etc.



# Global cross-disciplinary efforts needed!

## Speakers:

- K. Fu Umass Amherst, USA
- S. Capkun, ETHZ, CH
- S. Carrara, EPFL, CH
- J. Huiskens, IMEC, NL
- A. Sadeghi, Darmstadt, DE
- I. Brown, Oxford, GB
- F. Valgimigli, Metarini, IT
- A. Guiseppi-Elie, Clemson, USA
- S. Khayat, UFM, Iran
- Q. Tan, Shanghai, China

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

Springer Book underway, to appear early 2013

<http://si.epfl.ch/SPIMD>

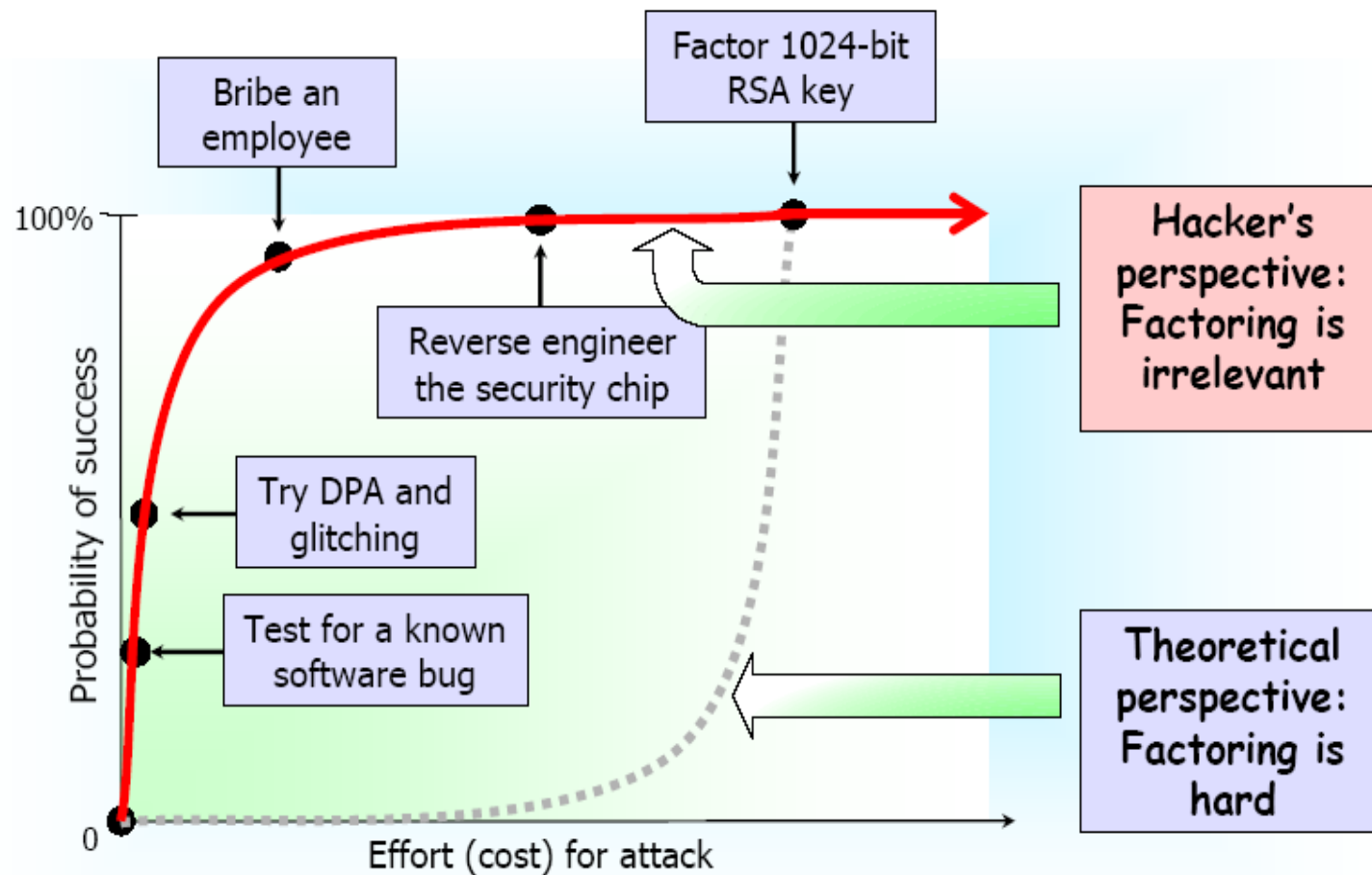


(co-located with IEEE ISMICT in nearby Montreux, Switzerland, [www.ismict2011.org](http://www.ismict2011.org))

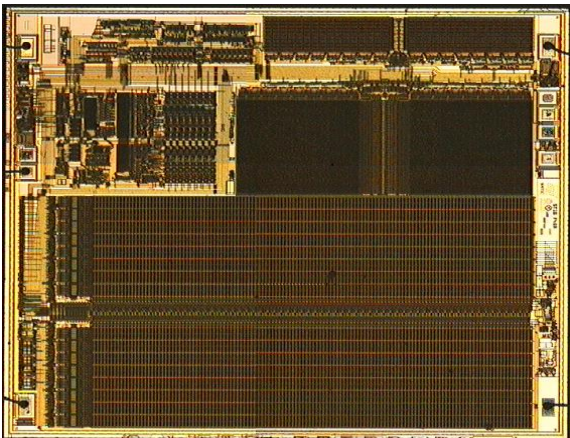
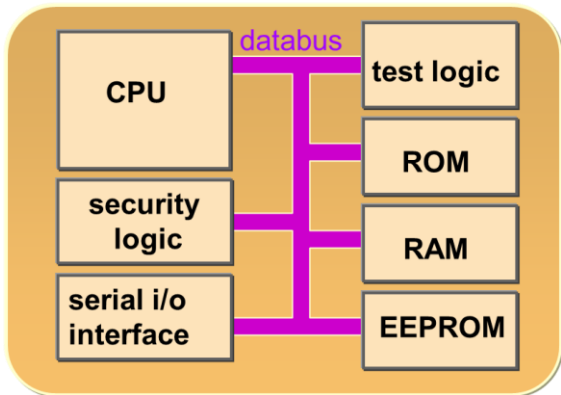
# Prototyping Security and Privacy Solutions

- Why?
- HW vs. SW
  
- How?
  - Moo
  - Biosensor
  - Umass 32nm

# Security Attacks: Theory vs. Practice



# Smart Card



# Security Goals for IMD Design

- Incorporate security **early**.
- **Encrypt** sensitive traffic.
- **Authenticate** third-party devices.
- Use well-studied cryptographic building blocks.
- Do not rely on **security through obscurity**.
- Use industry-standard source-code analysis.
- Develop a realistic **threat model**.

# Why is Hardware Security interesting for RFID and Ubiquitous Computing nodes?

- **Very cost-sensitive**, high-volume, justifies large design effort
- **Very low-power/energy** budget
- Low-level of complexity and efficiency requirements warrant **full-custom design**
  - Mostly hardware rather than software implementation
  - Very little memory ( $10^2$  -  $10^5$  bits), some is non-volatile
- **Soft real-time** performance requirements
- Side-channel leakage and tamper attacks require **careful circuit designs**
- **Mixed-signal design** due to unusual wireless communications and energy harvesting approach
- Application/Algorithm/Architecture/Circuit co-design, crossing traditional layers of abstraction





# 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



# Security Choice: Authenticated Encryption

- Best of both worlds
  - Combines encryption and authentication in a single scheme
  - Very well analyzed = several schemes
  - Even standardized – CCM, GCM, OCB, EAX, etc...
- Existing schemes
  - An encryption and a hash function running in parallel → Expensive – requires both primitives
  - As a block cipher mode of operation → The same encryption primitive used for both purposes – cheap but slow