A Lightweight Cryptographic System for Implantable Biosensors

Sara Ghoreishizadeh♫, Tolga Yalcin ♪, Antonio Pullini♮, Giovanni De Micheli♫, **Wayne Burleson**♯, and Sandro Carrara♫

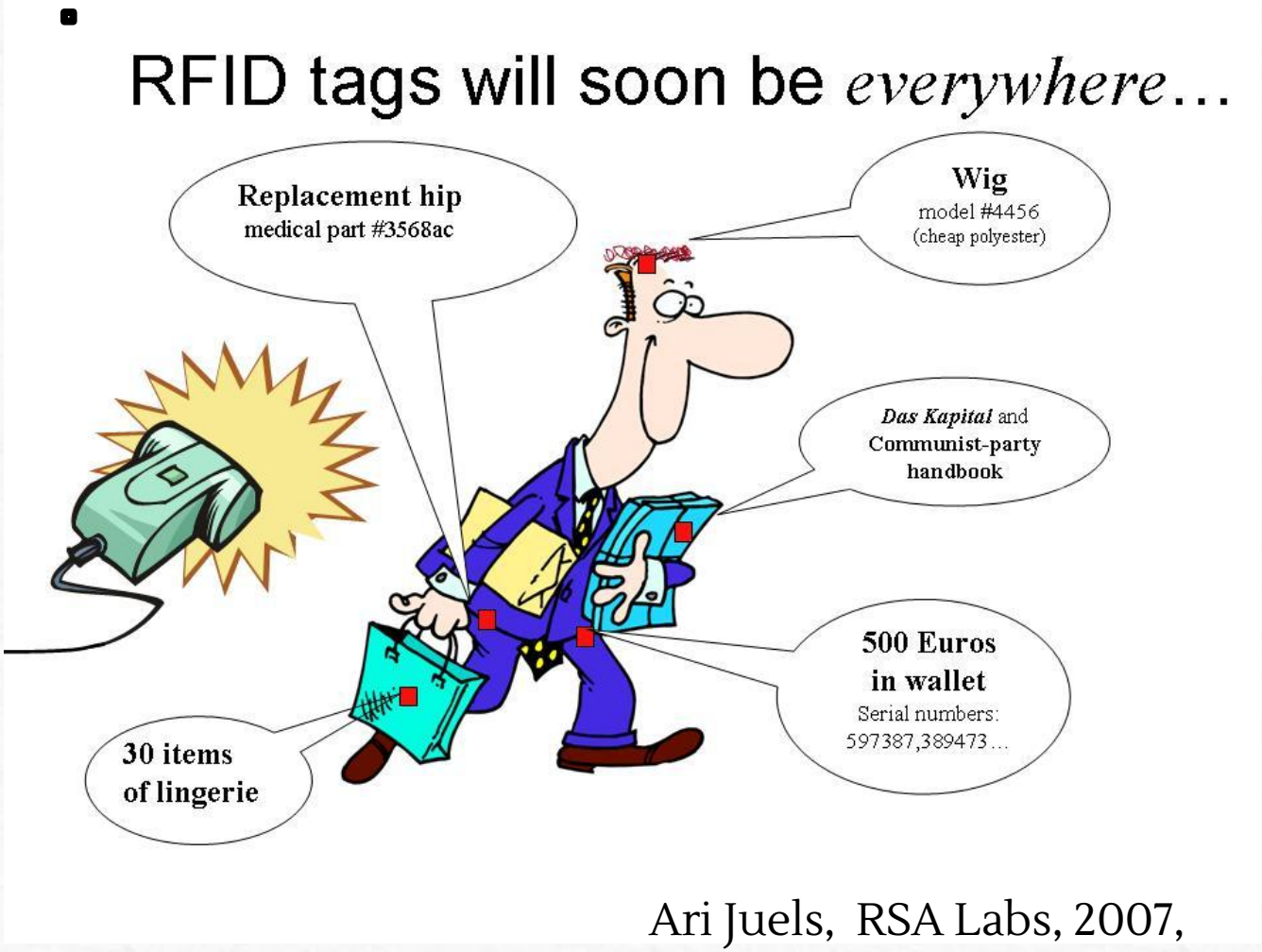
♫ EPFL, LSI – Lausanne, Switzerland,
♪ University for Information Science and Technology, Ohrid, Macedonia
♮ ETHZ, IIS- Zurich – Switzerland
♯ Department of Electrical and Computer Engineering UMass, Amherst, USA

Implantable and Wearable Medical Devices

- Bio-Medica
  - EEG E
  - ECG E
  - EMG E
  - Blood
  - Glucos
  - Respir
  - Tempe
  - Fall de
  - Ocular
  - Digest
- Sports perf
  - Distance, Speed, Rate of Climb
  - Heart and breathing rate
  - Posture (Body Position)
- Cyber-human interfaces

Images courtesy CSEM , Switzerland

Recall RFID Privacy concerns… mid-2000's?

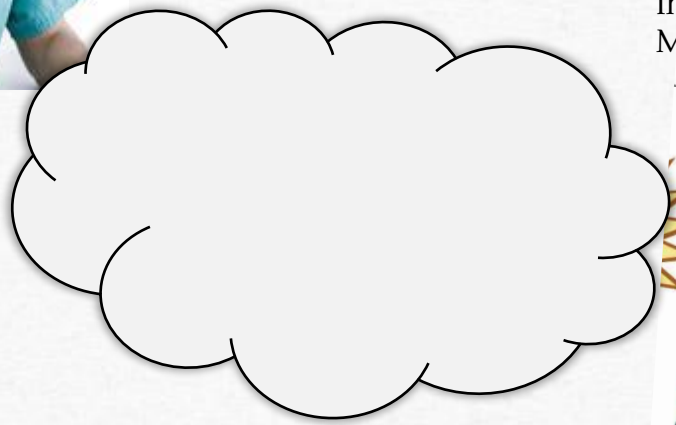


Ari Juels, RSA Labs, 2007,
now Cornell Tech

Can they support privacy-preserving protocols?

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

[Journal of the American College of Cardiology, 2011]



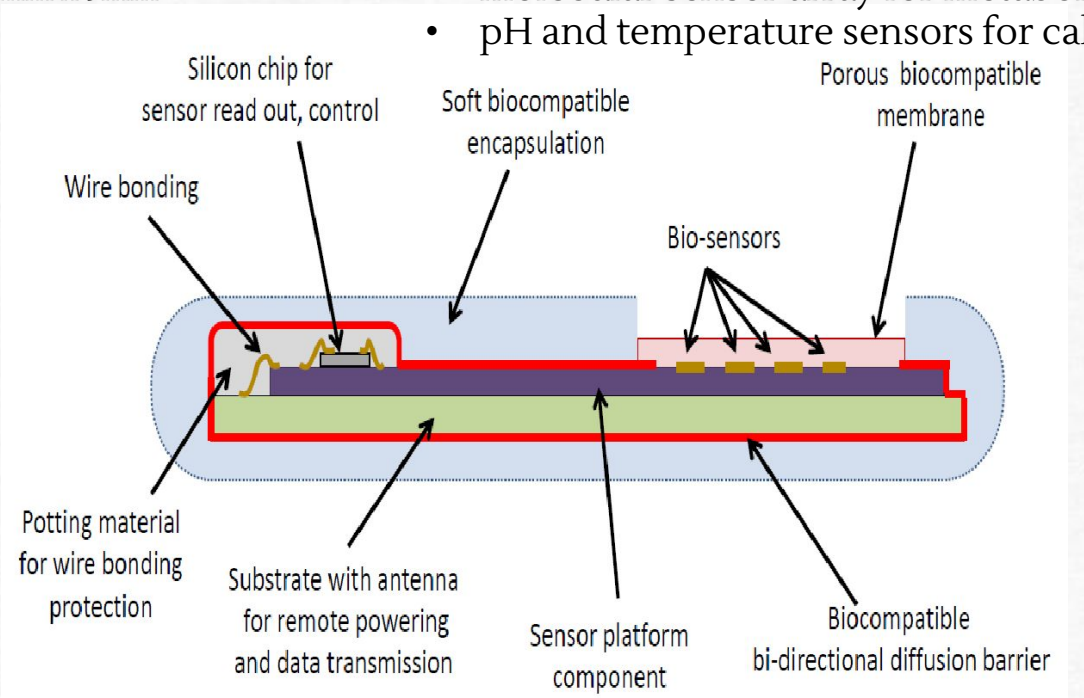
Implantable
Medical Device

Implantable bio-sensor

3mm x 5mm

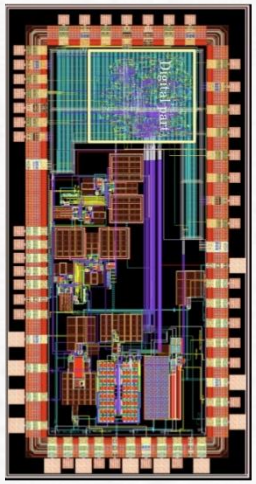
Personalized cancer drug monitoring:

- molecular sensor array for metabolite detection,
- pH and temperature sensors for calibration



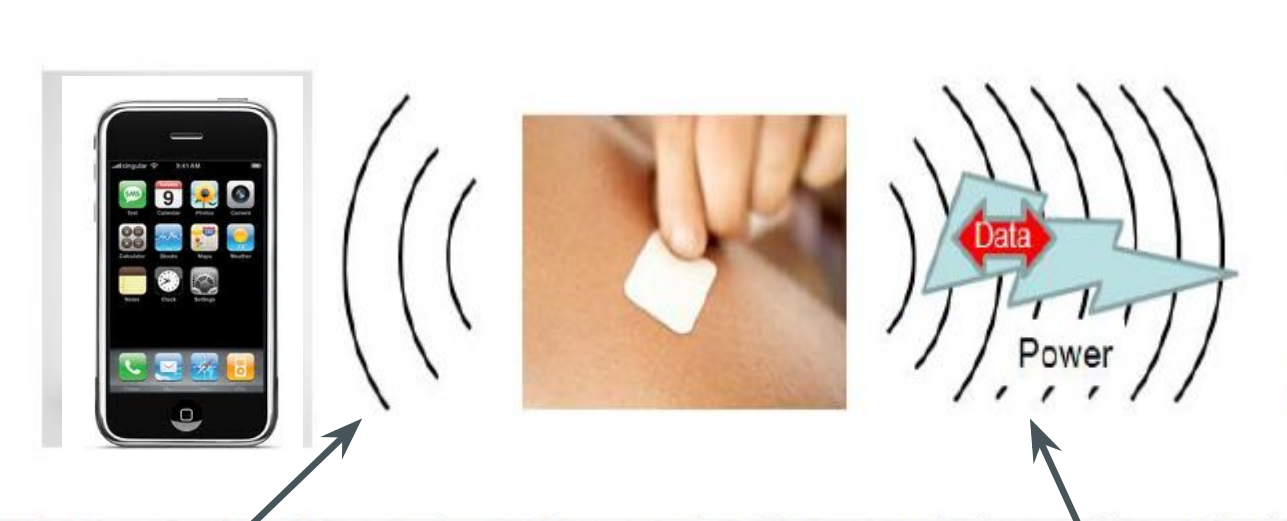
S. Carrara, G. DeMicheli,
EPFL, Nanotera IRONIC

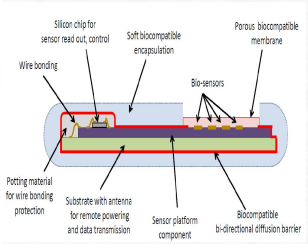
Prototype mixed-signal IC 180nm, sensor circuitry, I/O, crypto



S. Ghoreishizadeh, EPFL,
A. Pullini, EPFL/ETHZ
T. Yalcin, Bochum/UIST, Macedonia
W. Burleson, UMass

Mobile – patch – implant





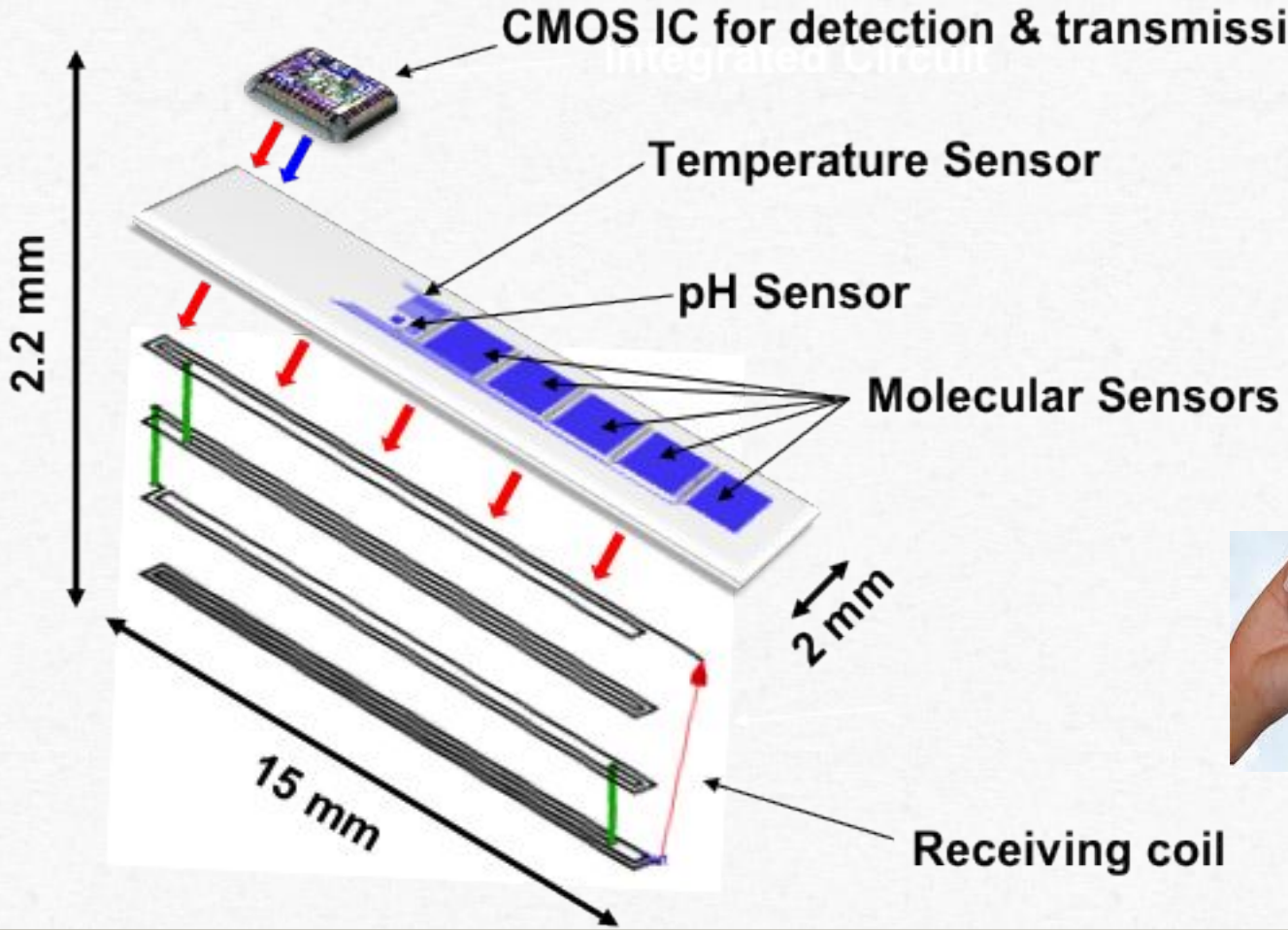
Bluetooth

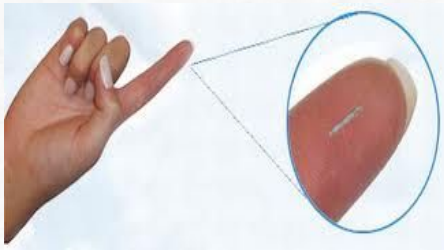
- Well-understood security

Patch to Sensor communication:

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

Implantable biosensing platform





Eventual size for injection

Security and Privacy of Biosensors

- What are your Assets?
  - Data confidentiality, authenticity and integrity
  - Human health and safety
- Challenges
  - Small infrequent data production and wireless transmission
  - Remotely powered by a removable patch
  - Low-power, small size and low-cost implementation
  - Compatibility with biosensor
  - Key management

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.**
- Model and protect against side-channels.

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

Threat model – Who is 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

Threats managed in our model

- Trusted patch is removed and placed on a rogue implant (e.g. falsified data for insurance fraud)

- Rogue patch is used to extract data from a trusted implant (e.g. stealing of personal health data)

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

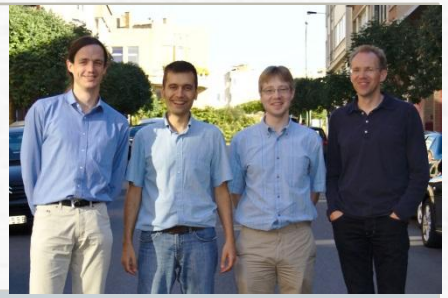
Proprietary
Non-standard!

- ALE – Authenticated Lightweight Encryption
  - AES-based scheme – Only 4 rounds used
  - Authentication part of encryption process
  - High-latency AES rounds

Too heavy!
Designed for bulk encryption

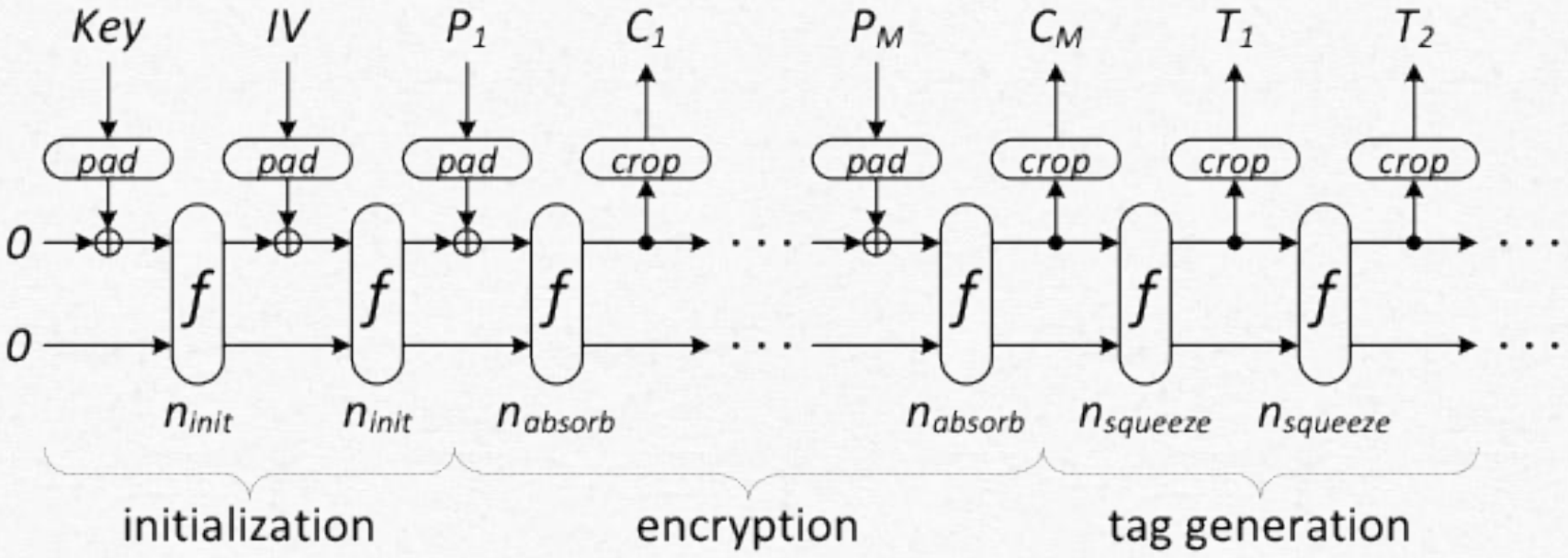
- **Sponge-based authenticated encryption (SHA-3 - KECCAK)**
  - Introduced after the "birth" of sponge functions
  - Uses the same sponge permutation for both encryption and authentication.

Authenticated Encryption



Gilles Van Assche[1]
Guido Bertoni[1], Michaël Peeters[2] Joan Daemen[1]
[1]STMicroelectronics
[2]NXP Semiconductors

The KECCAK algorithm
(recently standardized SHA-3)
in the Authenticated encryption mode:

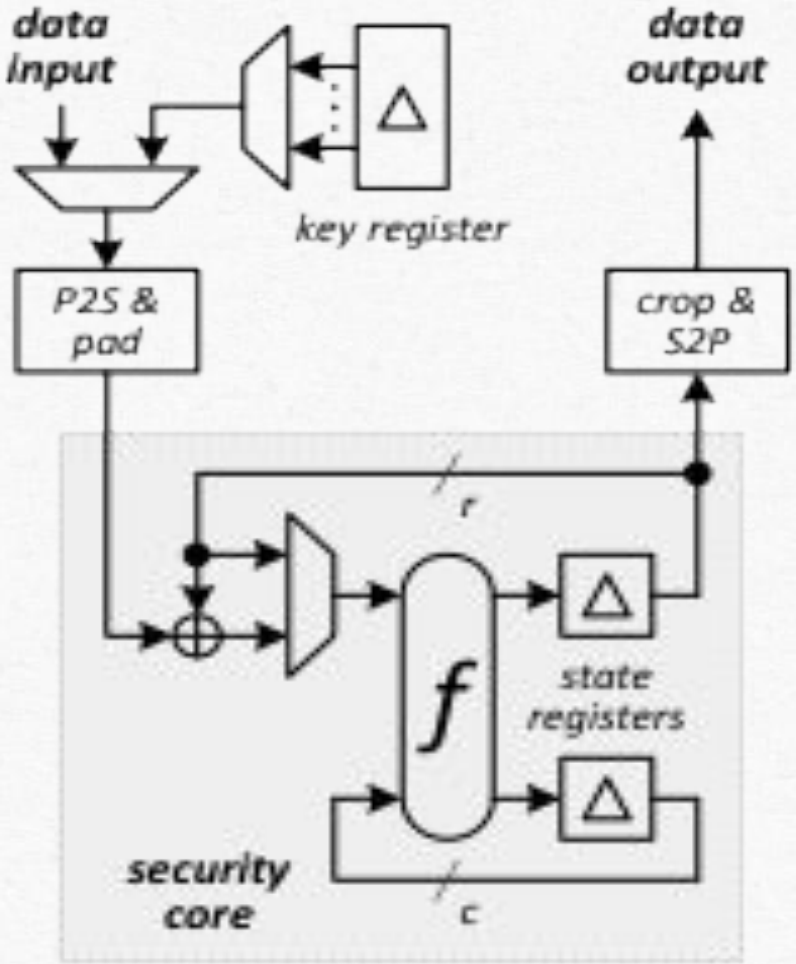


The Security Module

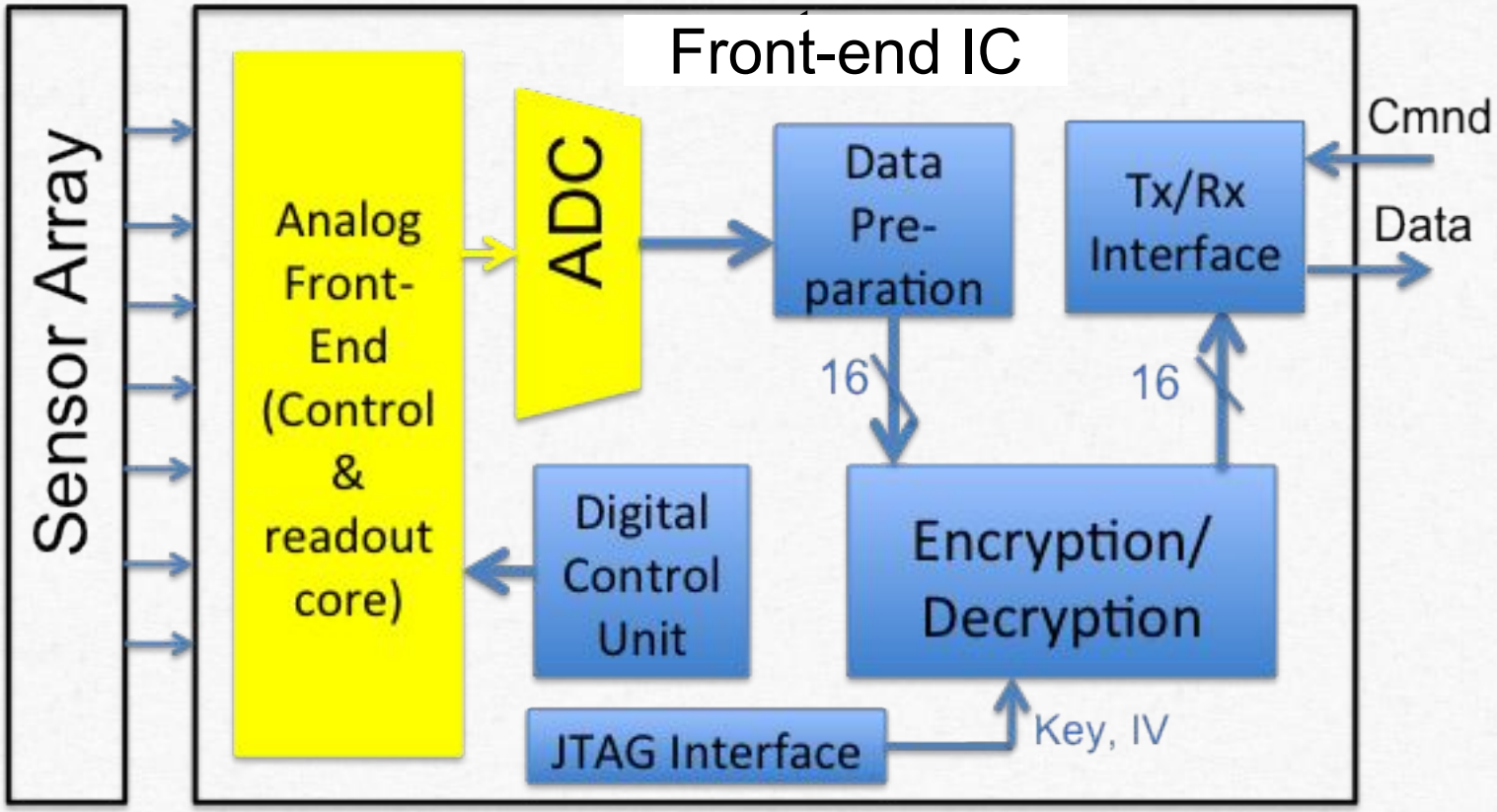
Inputs:
1- Key (80-bit)
3- IV (48-bit)
2- Data (64-bit)

Outputs:
1- IV (48-bit)
2- Ciphertext (64-bit)
3- Authentication Tag (32-bit)

Key will be burned into non-volatile memory at manufacturing (currently loaded via JTAG)

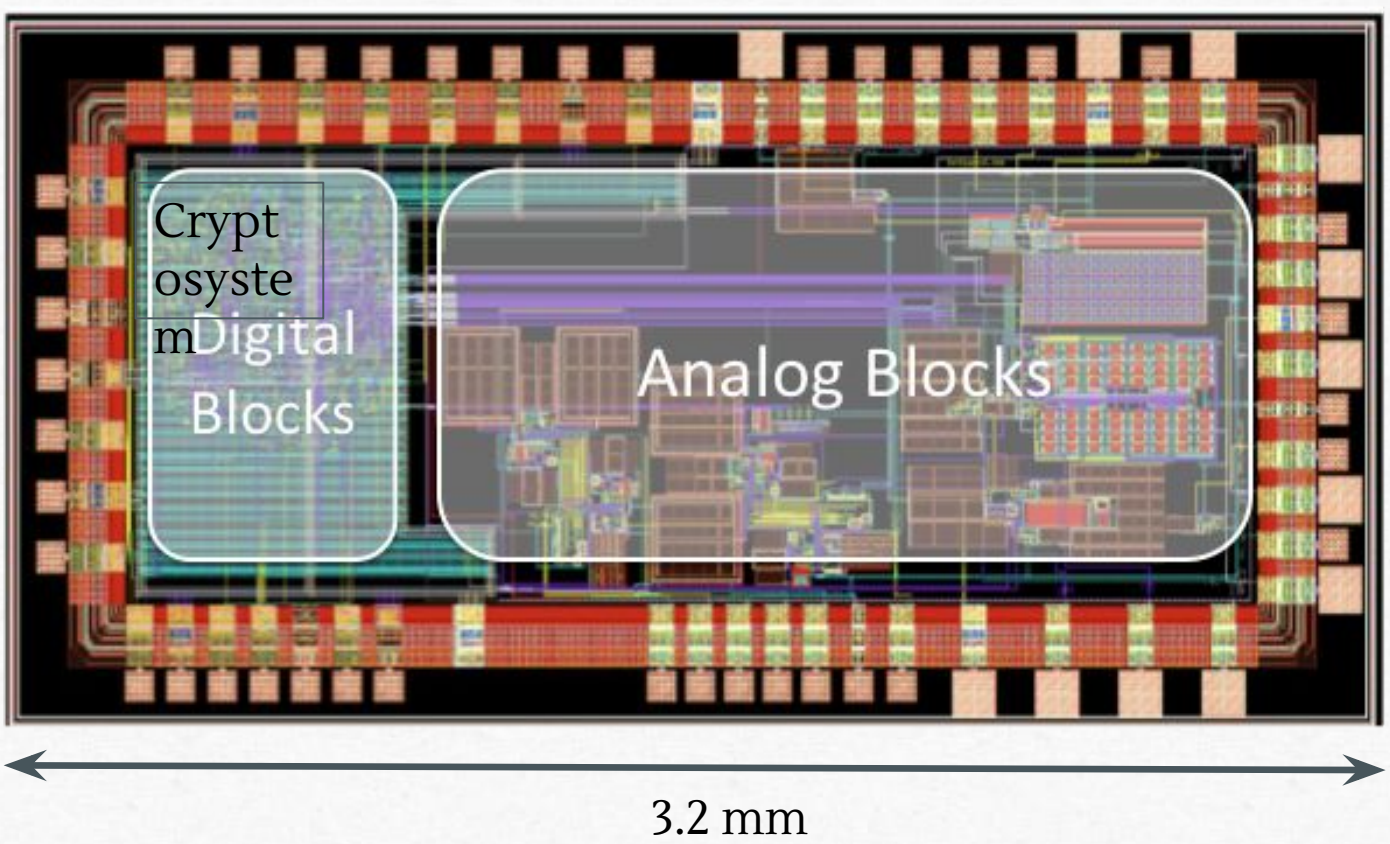


The Front-end IC



Overall Bio-sensor Layout

UMC 0.18 um

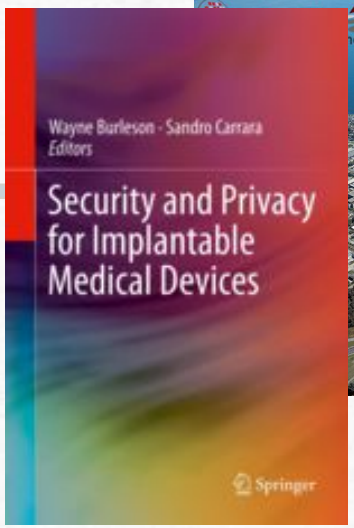


Cryptosystem Performance

Parameter	Value
Technology	UMC 0.18 um
Power consumption	7 uW
Clock	500 kHz
Area	1550 gate equivalents (2200 with wrapper)
Latency	1120 cycles
Throughput	100 kbps

Energy = .22 msec x 7 uW = 1.4 nJoules,
less than 1% of total biosensor power

Springer



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
Available: October 31, 2013

Available Formats:
eBook
Hardcover

- Describes problems of security and privacy in implantable medical devices and proposes some 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.

What is the role of regulators?

Up until very recently (ie this month), FDA regulated safety, but not security.

Star Tribune
October 01, 2014

The U.S. Food and Drug Administration on Oct 1, 2014 finalized guidelines strongly urging device makers to show that they've considered whether devices are vulnerable to intentional or unintentional cyber attacks, and the steps they took to reduce risk.

The FDA's seven-page announcement comes three weeks before a national workshop on cybersecurity and medical devices, scheduled for Oct. 21-22 in Arlington, Va. The meeting, which is being run in collaboration with the Department of Homeland Security, is intended to generate a national discussion among health care providers, devicemakers and IT experts on how to collaboratively improve the cybersecurity of medical devices implanted in the body or parked on hospital computer networks.

Summary

- Lightweight security system using SHA-3 (KECCAK)
- Dedicated hardware implementation with only 1550 gate equivalents, (smallest authenticated encryption reported!)
- Integrated into an IMD considering the unique threat models and constraints.
- Suitable for future IMDs to avoid vulnerabilities in both control and privacy.
- Key distribution and management remains a challenge
- Testing of crypto is a challenge (back-doors!)
- Thank you for your attention and questions!