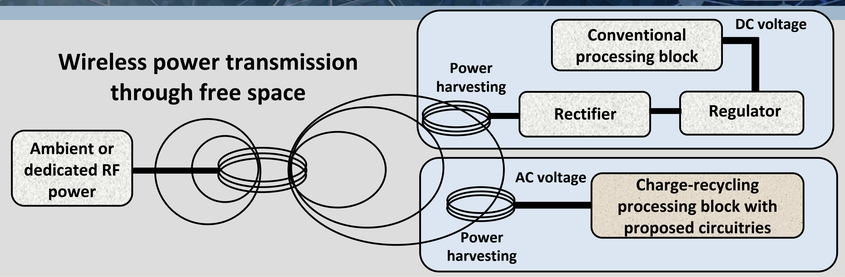
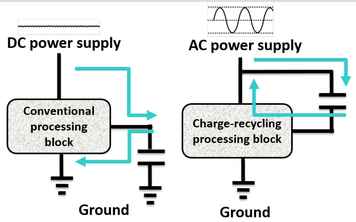
# Energy-Efficient and Secure Computing Methodology for RF-Powered IoT Devices

Emre Salman and Milutin Stanacevic
emre.salman@stonybrook.edu
Stony Brook University – SUNY
Stony Brook, New York




- More than an order of magnitude increase in energy efficiency
- Powerful local processing capability
- Elimination of the power losses due to rectification and regulation
- Elimination of the strong dependence on battery

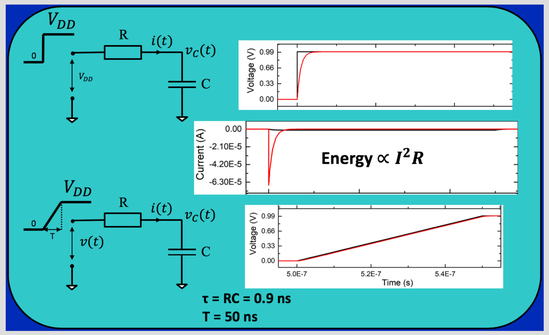
## Charge-Recycling Principle



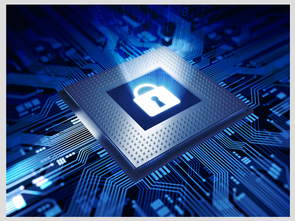

$E_{CMOS} = \alpha \frac{1}{2} CV_{DD}^2$ (a)

$E_{AL} = 2\frac{RC}{T} CV_{DD}^2$ (b)

## Adiabatic Switching



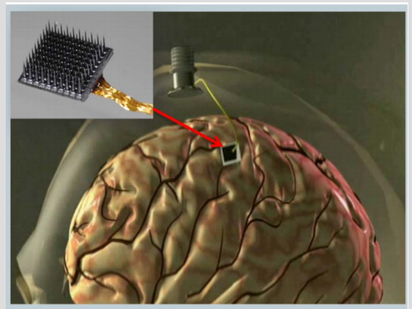

## Potential Applications



IoT Security

Structural health monitoring

Source: RFID, by AB&R

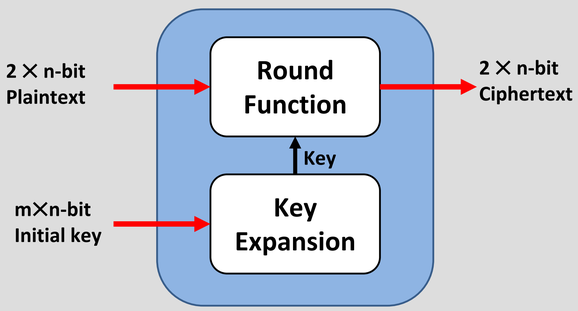


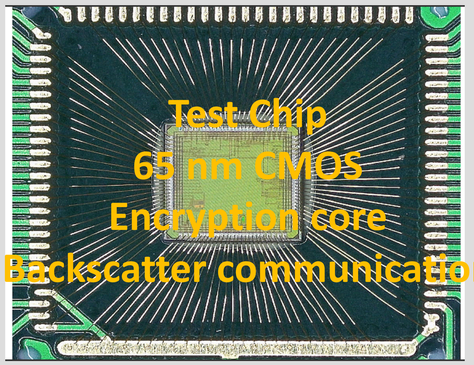
Source: A. V. Nurmikko *et al.*, Proceedings of the IEEE, 2010

## SIMON Cipher

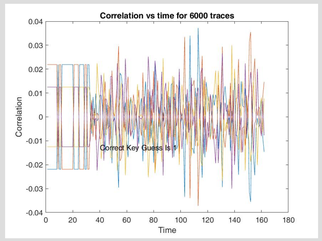
- Bit-serialized SIMON32/64
  - Lightweight cryptographic algorithm
  - 32-bit plaintext input
  - 64-bit initial keys
  - Consists of round function and key expansion

## Proposed Architecture

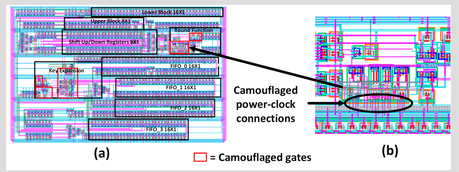



## Hardware Security




Enhanced side-channel resistance

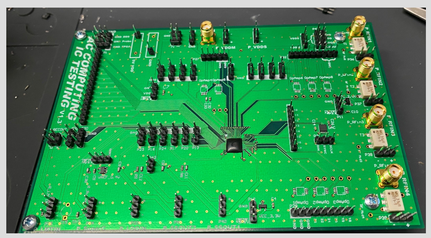



Lightweight obfuscation by camouflaging inherent phase differences

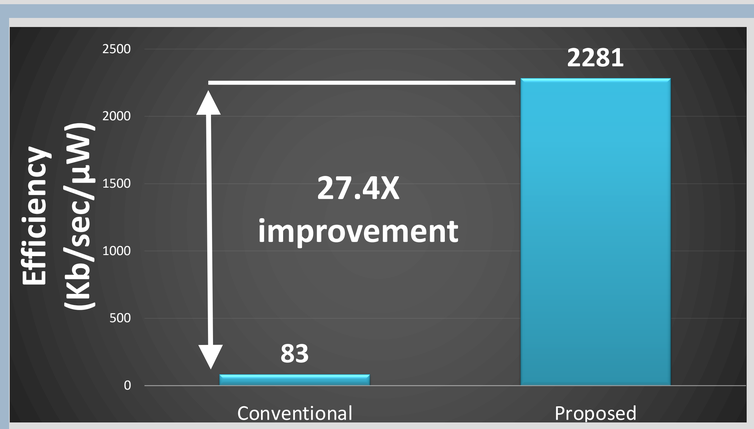
## Results

- RF signal amplitude is 1.2 V
- Operation frequency is 13.56 MHz
- 65 nm commercial CMOS technology

| Architecture | Conventional | Proposed |
|---|---|---|
| Logic | Static Logic | PAL |
| Average Power (µW) | 9.12 | 0.27 |
| Latency (clock cycles) | 576 | 704 |
| Energy (pJ) | 387 | 14 |
| Throughput (Kbps) | 753 | 616 |
| Efficiency (Kb/sec/µW) | 83 | 2281 |
| Number of Transistors | 2966 | 1242 |



Test PCB




## Broader Impact

- Two PhD students graduated
- One issued patent and one pending patent application
- Enables secure local processing capability for RF-powered applications with limited resources
- Contributions to IoT certificate program