Energy Recovery Computing for Low-Energy and Secure IoT Devices

Dr. Himanshu Thapliyal
VLSI Emerging Design And Nano Things Security (VEDANTS) Lab
Department of Electrical and Computer Engineering,
University of Kentucky, Lexington, KY
hthapliyal@uky.edu
Web: http://hthapliyal.engr.uky.edu/
Internet of Things (IoT)


Source: R. K. Krishnamurthy (Intel), Panel, ICCE 2019
Challenges in IoT Devices

Design Challenges in IoT devices

- **Energy-Efficiency**
  - Typically battery operated
  - Energy-efficient design

- **Security**
  - Vulnerable to hardware/malware attacks
  - Power analysis attacks
  - IC piracy, IC counterfeiting, Hardware trojan

Cyberattacks are threat to reliability, safety, consumer’s personal information and piracy or cloning of intellectual property.

Side Channel Attacks – Differential and Correlation Power Analysis (DPA/CPA)


Table 2. Comparison of ASIC-based DPA countermeasures with energy Recovery (ER) based design. Comparison is based on results in [1].

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>65nm</td>
<td>130nm</td>
<td>130nm</td>
<td>130nm</td>
</tr>
<tr>
<td>Standalone AES power/Freq</td>
<td>138.1mW/1.2GHz</td>
<td>10.5mW/40 MHz</td>
<td>33.32mW/100MHz</td>
<td>-50MHz</td>
</tr>
<tr>
<td>Operating Voltage (V)</td>
<td>1 (External)</td>
<td>0.4-1 (from IVR)</td>
<td>1.2 (External)</td>
<td>1.2 (External)</td>
</tr>
<tr>
<td>Power Overhead</td>
<td>-30%</td>
<td>5%</td>
<td>33%</td>
<td>-</td>
</tr>
<tr>
<td>Area overhead</td>
<td>6000um² (25%)</td>
<td>2135um² (103 gates)</td>
<td>7900um² (20%)</td>
<td>11K gates (67%)</td>
</tr>
<tr>
<td>Performance Overhead</td>
<td>0%</td>
<td>3.33%</td>
<td>50%</td>
<td>0%</td>
</tr>
<tr>
<td>Analysis Method</td>
<td>DPA</td>
<td>CPA, TVLA</td>
<td>DPA</td>
<td>CPA/ Fault-Attack</td>
</tr>
</tbody>
</table>

DPA Countermeasures
Talk Overview

- Energy Recovery Logic for low-power and DPA resistant circuits
- FinFET and Tunnel FET based energy recovery family
- Lightweight PRESENT-80 algorithm as benchmark circuit
- Adiabatic Logic-Based Energy-Efficient and Reliable PUF
- Hardware Trojan Detection Method Based on Energy Recovery Logic
- Adoption in Industry
Energy Recovery Logic

Energy dissipated in the adiabatic circuit is given by:

$$E_{\text{diss}} = \frac{RC}{T} CV_{dd}^2$$

- $T$ -> Transition period of power clock
- $R$ -> parasitic resistance
- $C$ -> load capacitance
- $V_{dd}$ -> voltage swing of the clock

### Current Traces of an Inverter

<table>
<thead>
<tr>
<th>Logic style</th>
<th>Charging</th>
<th>Discharging</th>
<th>Input transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Logic diagram" /></td>
<td><img src="image" alt="Charging diagram" /></td>
<td><img src="image" alt="Discharging diagram" /></td>
<td><img src="image" alt="Input transitions diagram" /></td>
</tr>
</tbody>
</table>

- **a)**
- **b)**
- **c)** proposed EE-SPFAL: minimum and uniform peak current for all possible input transitions

---

Adiabatic Logic base Low-Energy and Secure Solutions
Symmetric Pass Gate Adiabatic Logic (SPGAL)

<table>
<thead>
<tr>
<th>Transistors</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1, M2</td>
<td>Recover the energy from load capacitors</td>
</tr>
<tr>
<td>M3, M4</td>
<td>Perform logic operations</td>
</tr>
<tr>
<td>M5, M6</td>
<td>Reset the outputs (discharge the redundant charge)</td>
</tr>
</tbody>
</table>
SPGAL XOR gate

(a) Shows the schematic of SPGAL based XOR gate
(b) Shows the uniform current consumption of the SPGAL based XOR gate for various input transition.
AES Cryptographic Algorithm

<table>
<thead>
<tr>
<th>AES component</th>
<th>Max. Power (uW @10MHz)</th>
<th>Power ratio (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubBytes (S-Box)</td>
<td>1940</td>
<td>75</td>
</tr>
<tr>
<td>MixColumns</td>
<td>262</td>
<td>10</td>
</tr>
<tr>
<td>AddRoundKey</td>
<td>&gt;10</td>
<td>&gt;1</td>
</tr>
<tr>
<td>Data Selectors</td>
<td>&gt;10</td>
<td>&gt;1</td>
</tr>
<tr>
<td>FFs and Clock Drivers</td>
<td>400</td>
<td>15</td>
</tr>
</tbody>
</table>

Power consumption of each AES component [1], 1.5V CMOS standard cell

- AES is symmetric encryption algorithm
- Applications: Network appliances, voice communications etc.
- S-Box consumes much of the total power of AES designs

## S-Box circuit comparison results

<table>
<thead>
<tr>
<th>Logic</th>
<th>No. of transistors (S-Box)</th>
<th>Overhead (transistor)</th>
<th>Area (um²)</th>
<th>Energy dissipation</th>
<th>ESF</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMOS</td>
<td>2202</td>
<td>-</td>
<td>0.04</td>
<td>11.45 pJ</td>
<td>-</td>
</tr>
<tr>
<td>SQAL</td>
<td>3401</td>
<td>54%</td>
<td>0.0723</td>
<td>2.52 pJ</td>
<td>4.54</td>
</tr>
<tr>
<td>SPGAL (Proposed)</td>
<td>3624</td>
<td>64%</td>
<td>0.08</td>
<td>0.825 pJ</td>
<td>13.878</td>
</tr>
</tbody>
</table>

- **Energy Saving Factor (ESF)** is a measure of how much energy is used in a conventional CMOS gate or system with respect to its adiabatic logic counterpart.

FinFET and Tunnel FET

- FinFET: Strong gate control channels
- Higher on-state current, lower leakage, and faster switching speed
- Tunnel FET (TFET) subthreshold swing (SS) below 60 mV/dec (high on-current to off current ratio)
- Lower SS enables low-leakage with higher performance than CMOS at lower voltages

**Energy-Efficient**
- Dynamic power reduction \(\rightarrow\) Adiabatic logic technique
- Leakage power reduction \(\rightarrow\) FinFET/TFET devices

Ref: Chenming Hu, 3D FinFET and other sub-22nm Transistors, IPFA 2012
Current consumption of TunSAL XOR gate

- Uniform current consumption of TunSAL XOR for various input transitions
- Uniform current TunSAL gates makes it to countermeasure DPA attack at circuit level
Implementation of PRESENT-80

(a) One round implementation of PRESENT-80 using SPGAL, FinSAL and TunSAL gates
(b) 4-phase clocking scheme of SPGAL, FinSAL and TunSAL to implement PRESENT-80
Simulation Results on PRESENT-80 at 12.5 MHz:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>MOSFET</td>
<td>MOSFET</td>
<td>FinFET</td>
<td>Tunnel FET</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Tech (nm)</td>
<td>22</td>
<td>22</td>
<td>20</td>
<td>20</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>$V_{DD}$ (V)</td>
<td>1</td>
<td>1</td>
<td>0.9</td>
<td>0.3</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Avg. power (uW)</td>
<td>7.890</td>
<td>1.32</td>
<td>0.70</td>
<td>0.511</td>
<td>92</td>
<td>62</td>
<td>28</td>
</tr>
<tr>
<td>Avg energy (pJ)</td>
<td>20.83</td>
<td>3.564</td>
<td>1.795</td>
<td>1.257</td>
<td>93</td>
<td>65</td>
<td>30</td>
</tr>
</tbody>
</table>
DPA attack on PRESENT-80

DPA attack on PRESENT-80 implemented using
(a) Conventional CMOS gates (b) TunSAL gates
Adiabatic Physical Unclonable Function (PUF)

- Silicon fingerprint
- Process variations is boon
  - Variation is inherent in fabrication process
  - Unique for each physical instance
  - Hard to remove or predict
  - Relative variation increases as the fab process advances

Proposed

<table>
<thead>
<tr>
<th>Technology</th>
<th>Voltage</th>
<th>Success Rate</th>
<th>False Positive Rate</th>
<th>False Negative Rate</th>
<th>Power Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>45nm</td>
<td>1V</td>
<td>49.48%</td>
<td>49.41%</td>
<td>99.6%</td>
<td>0.08 fJ</td>
</tr>
</tbody>
</table>

## Proposed PUF Comparison

<table>
<thead>
<tr>
<th>PUF</th>
<th>Tech.</th>
<th>Vdd</th>
<th>Uniqueness</th>
<th>Uniformity</th>
<th>Reliability</th>
<th>Energy/bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>180nm</td>
<td>1.8 V</td>
<td>NA</td>
<td>NA</td>
<td>95.18%</td>
<td>1.37 pJ</td>
</tr>
<tr>
<td>[2]</td>
<td>180nm</td>
<td>3.3 V</td>
<td>49.37 %</td>
<td>NA</td>
<td>99.1%</td>
<td>23.9 pJ</td>
</tr>
<tr>
<td>[3]</td>
<td>40nm</td>
<td>0.9 V</td>
<td>47.22 %</td>
<td>NA</td>
<td>&gt;99.99%</td>
<td>17.8 pJ</td>
</tr>
<tr>
<td>[4]</td>
<td>28nm</td>
<td>0.6 V</td>
<td>49.11%</td>
<td>49.96%</td>
<td>88.39</td>
<td>0.05 fJ</td>
</tr>
<tr>
<td>Proposed</td>
<td>45nm</td>
<td>1V</td>
<td>49.48%</td>
<td>49.41%</td>
<td>99.6%</td>
<td>0.08 fJ</td>
</tr>
</tbody>
</table>

Adiabatic Logic Based Hardware Trojan Detection

- Malicious circuit in IC to perform faulty operations
- Designed to destroy systems or leak secret information
- Implemented as hardware modification to ASICs, microprocessor, DSP etc.


Adoption in Industry

Main Challenges in ER Computing:

- Not been widely adopted in industry as a mainstream methodology.
- Amount of time and effort required to design customized ER circuits.
- Must acquire specialized skills and learn ER methodologies to design ER circuits.

Solutions:

- To mainstream ER computing, it needs to be made designer-friendly.
- Necessary to develop a standard cell library and semi-automatic tools to reduce the time and effort in the design and verification of ER circuits.
- Power clock generation and distribution play an important role in determining the overall energy efficiency of the ER system.
2-Phase CPA resistant, adiabatic logic only requires 4 signals to operate while 4-Phase requires 8.

2-Phase clock designs also consume less area and are less complex.

The reduced interconnection area and complexity can lead to simpler yet energy efficient adiabatic designs.

2-Phase Adiabatic Logic

- 2-EE-SPFAL uses two sine waves 180° out of phase.
- 2-EE-SPFAL requires two discharge signals with equal period of their respective clocks.

Summary

ER computing is a promising candidate to implement hardware security primitives for IoT devices with stringent constraints on power consumption.