Energy-Efficient Circuits and Systems

ANANTHA P. CHANDRAKASAN

DEAN OF ENGINEERING
VANNEVAR BUSH PROFESSOR OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
Research Directions

• Hardware Security: Materials, circuit, protocols and system
  • Secure machine learning
  • Power and EM side-channel resilient circuits

• Embedded machine learning processors
  • Robust machine learning
  • NLP
  • Generative AI
  • In-memory/near-memory machine learning

• Low-Power IoT
  • Bio-medical ICs (wearable and ingestible)
  • Energy Harvesting
  • Energy-efficient ADC
  • Authenticated Wake-up receivers
A Secure Digital In-Memory Compute Macro with Protections Against Side-Channel and Bus Probing Attacks

Challenge ①: SCA Security
Solution: Threshold Implementation (TI)-inspired digital in-memory compute

Challenge ②: BPA Security
Solution: Lightweight model decryption on-chip

Challenge ③: Generate Secure Key
Solution: Reuse IMC SRAM for Physically Uncloneable Function (PUF)

Eliminate Constant Random Bits By:
a) Using TI-shared gates and sub-blocks with natively secure statistical properties  
b) Re-using previous unrelated computes as independent bits to refresh security

Challenge ④: MAC Security
Solution: MAC Security with additional encryption layers

<table>
<thead>
<tr>
<th></th>
<th>Unprotected</th>
<th>Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput* (GOPS)</td>
<td>41.0 / 9.10</td>
<td>81.9 / 10.2</td>
</tr>
<tr>
<td>Energy Efficiency* (TOPS/W)</td>
<td>90.2 / 14.4</td>
<td>6.94 / 0.89</td>
</tr>
<tr>
<td>Area Efficiency* (TOPS/mm2)</td>
<td>3.01 / 0.67</td>
<td>0.49 / 0.061</td>
</tr>
</tbody>
</table>

*at peak utilization, weight update is 5% of time
Trusted Execution Environment for DNNs

Cryptographic engine performs encryption and authentication for every off-chip traffic

Cryptographic metadata (e.g., hash tags) adds additional memory traffic

Kyoungmi Lee, Joel Emer, Mengjia Yan, A. Chandrakasan, [MICRO 2024]
Low Power NLP

Low-Power and Secure Communication System for Ingestible Devices

1. Low-power RF system based on duty-cycling & wake-up
2. Energy-efficient authentication protocol
3. Antenna design for ingestible device
4. Self-adaptable driver for drug release

Driving Voltage Modulation
for energy-efficient gold dissolution

Anode: Gold membrane, Cathode: Platinum
Temperature: 35-38°C
SGF: pH 1, [Cl] = 100 mM
Battery-free 5G energy harvester backscattering chips for asset identification in IoT - enabled warehouses

Key Features
• Harvests 5G energy for battery-free backscattering communication tags
• Ultra-low power, on-chip, PVT – resilient clock generation
• Built-in Manchester and convolutional code for enhanced backscattering resiliency

Deniz Umut Yildirim (CICC 2024)

<table>
<thead>
<tr>
<th>Process</th>
<th>65nm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freq.</td>
<td>3.5GHz</td>
</tr>
<tr>
<td>Antenna Area (cm²)</td>
<td>0.7</td>
</tr>
<tr>
<td>Sensitivity (dBm) or Wake-up power</td>
<td>-31</td>
</tr>
<tr>
<td>$V_{\text{rect}}$ (V), $R_{\text{load}}/P_{\text{load}}$ at sensitivity</td>
<td>0.9 @1nW</td>
</tr>
<tr>
<td>Cold-start charging time</td>
<td>18sec @ -31dBm</td>
</tr>
<tr>
<td>Communcation Scheme</td>
<td>OOK</td>
</tr>
<tr>
<td>Communication Bitrate</td>
<td>2.5kbps</td>
</tr>
<tr>
<td>Communication Power @ $V_{\text{dd}}$</td>
<td>0.12µW @ 0.9V</td>
</tr>
</tbody>
</table>