Sniff-SAR: A 9.8fJ/c.-s 12b secure ADC with detection-driven protection against power and EM side-channel attack

Ruicong Chen, Anantha Chandrakasan, Hae-Seung Lee
Massachusetts Institute of Technology
Outline

• Motivation
• Prior art
• Proposed Sniff-SAR architecture
• Measurement results
• Conclusions
Outline

• Motivation
• Prior art
• Proposed Sniff-SAR architecture
• Measurement results
• Conclusions
Power Side-Channel Attack (PSA)

- **Attacker**
  - Leaks information through power leakage.
  - Uses a CNN for analysis.

- **Secure ADC**
  - Secure mode: Each code has an un-trainable random waveform.
  - Active for all rounds.

- **Sniff-SAR**
  - Provides protection against Side-Channel Attacks.
  - Wasted power vs. less wasted power.

- **Results**
  - **Successful Attack**
  - **Fail to Attack**
Electro-magnetic Side-Channel Attack (EMSA)
New Era for Hardware Security

ADC Design Goals

- Security
- Sampling Speed
- Energy-efficiency
Outline

• Motivation
• Prior art
• Proposed Sniff-SAR architecture
• Measurement results
• Conclusions
Prior art

Switched capacitor Equalizer
T. Jeong, JSSC 2021
Equalization based protection

- Obscure the power traces by current equalizer

[JSSC’21]
Current equalizer
Prior art

Switched capacitor Equalizer
T. Jeong, JSSC 2021

Random timing conversion
M. Ashok, CICC 2022
Time-randomized protection

Random switching of unit caps

- Switch unit capacitors randomly
Prior art

Switched capacitor Equalizer
T. Jeong, JSSC 2021

Random timing conversion
M. Ashok, CICC 2022

Random mapping Conversion
R. Chen, VLSI 2022
Random mapping based protection

• Worst case conversion cycles can be improved

[VLSI’22] Randomizing the initial guess of LSB-first SAR
Outline

• Motivation
• Prior art
• Proposed Sniff-SAR architecture
• Measurement results
• Conclusions
This work

- Detection-driven protection

[VLSI’22]
Active for all rounds

[This work]
Detection-driven

Samples
1 2 3

Attack

Protection

Wasted power

Less wasted power
Proposed Sniff-SAR architecture

- Detection-driven protection
- More energy efficient and faster conversion scheme
**DAC schematic**

- Bottom-plate sampling
- Split DAC to save area
Flowchart of the secure SAR

P1. Random:
Start from random guess

\[ D_U = D_{RND} \]
\[ D_L = D_{RND} - 0.5FS \]
Sample \( V_{IN} \)

Set \( U = FS, L = 0 \)
Enable DAC

• P1: start from random guess
Flowchart of the secure SAR

P1. Random: Start from random guess

\[
D_U = D_{RND} \\
D_L = D_{RND} - 0.5FS
\]
Sample \( V_{IN} \)

Set \( U = FS, \ L = 0 \)
Enable DAC

P2. Search: Ternary search

Generate \( D_{RND} \)

\( U - 0.5R < D_{RND} < U \)

\( R > 2? \)

YES

\[
D_U = D_{RND} \\
D_L = D_{RND} - 0.5R
\]

\( R = U - L \)

Set \( U = D_U, \ L = D_L \)

Set \( L = D_U \)
\( R = U - L \)

Set \( U = D_L \)
\( R = U - L \)

- P2: un-balanced binary search according to previous comparators’ outputs
Flowchart of the secure SAR

**P1. Random:**
Start from random guess

- \( D_U = D_{RND} \)
- \( D_L = D_{RND} - 0.5FS \)

Sample \( V_{IN} \)

Set \( U = FS, L = 0 \)
Enable DAC

**P2. Search:**
Ternary search

Generate \( D_{RND} \)

\( U = 0.5R < D_{RND} < U \)

\( R > 2? \)

YES

- \( D_U = D_{RND} \)
- \( D_L = D_{RND} - 0.5R \)

NO

\( D_U = D_{RND} \)

\( D_L = D_{RND} - 0.5R \)

**P3. LSB:**
- UDAC and LDAC are combined
- LSB decision

\( D_U[N] = CMP_U \)

Finished
Purge DAC

1. \( CMP_U, CMP_L = (0,1) \)
2. \( CMP_U, CMP_L = (1,1) \)
3. \( CMP_U, CMP_L = (0,0) \)

- **P3:** combine DACs for LSB decision
Flowchart of the secure SAR

- P3: combine DACs for LSB decision

UDAC 10100 + 10

DAC 10100 + 01

LDAC 10100 + 00

Random start

Combine UDAC and LDAC
An example conversion
An example conversion
An example conversion

Two Regs: $U$, $L$
- $U$: upper bound (-1,1)
- $L$: lower bound (-1,1)
- $R_N$: $N^{th}$ test voltage (-1,1)
Compare with RaM-SAR

Sniff-SAR: One-pass search

RaM-SAR: Overshoot and search
PSA detector

- Detect the IR drop by the attack resistor
  - S. J. Kim, VLSI’21
EMSA detector

- Detect the LC frequency different using mutual inductance
  - N. Miura, VLSI’14
Outline

• Motivation
• Prior art
• Proposed Sniff-SAR architecture
• Measurement results
• Conclusions
### Chip specifications

<table>
<thead>
<tr>
<th>Process technology</th>
<th>65nm LP</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDD [V]</td>
<td>1.2</td>
</tr>
<tr>
<td>Resolution [b]</td>
<td>12</td>
</tr>
<tr>
<td>Sampling Rate [MS/s]</td>
<td>40</td>
</tr>
<tr>
<td>Area [mm²]</td>
<td>0.075</td>
</tr>
<tr>
<td>ENOB [b]</td>
<td>10.8</td>
</tr>
<tr>
<td>FoM (fJ/c.-s)</td>
<td>9.8</td>
</tr>
</tbody>
</table>
EM SCA testing setup
CNN-based side-channel attacks

1. **Dataset**
   - Collect side-channel traces (data) and corresponding digital outputs (labels) from 3 training ADCs

2. **Training**
   - Train the CNN for PSA or EMSA using the collected data and labels

3. **Inference**
   - Collect side-channel traces from unseen ADCs and attack the ADCs with the trained CNN
   - Examine attack accuracy
## Side-channel attack results (1)

### Bit-wise accuracy with ramp input (averaged across 3 ADCs)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VDD-side PSA(^1) (unprotected(^2))</td>
<td>99.18</td>
<td>98.46</td>
<td>97.25</td>
<td>98.76</td>
<td>99.75</td>
<td>99.38</td>
<td>99.16</td>
<td>96.75</td>
<td>93.48</td>
<td>92.12</td>
<td>88.17</td>
<td>83.26</td>
</tr>
<tr>
<td>VDD-side PSA (protected)</td>
<td>52.76</td>
<td>51.72</td>
<td>48.19</td>
<td>48.76</td>
<td>49.76</td>
<td>50.76</td>
<td>50.28</td>
<td>53.17</td>
<td>54.71</td>
<td>57.15</td>
<td>55.86</td>
<td>45.76</td>
</tr>
<tr>
<td>GND-side PSA (unprotected)</td>
<td>99.56</td>
<td>99.42</td>
<td>96.16</td>
<td>97.48</td>
<td>96.23</td>
<td>99.81</td>
<td>99.43</td>
<td>98.23</td>
<td>97.84</td>
<td>85.16</td>
<td>76.48</td>
<td>78.63</td>
</tr>
<tr>
<td>GND-side PSA (protected)</td>
<td>48.76</td>
<td>49.75</td>
<td>51.76</td>
<td>52.84</td>
<td>53.91</td>
<td>53.27</td>
<td>45.86</td>
<td>52.74</td>
<td>50.17</td>
<td>46.26</td>
<td>50.75</td>
<td>50.19</td>
</tr>
<tr>
<td>EMSA(^1) (unprotected)</td>
<td>99.43</td>
<td>98.16</td>
<td>99.47</td>
<td>99.28</td>
<td>98.71</td>
<td>99.72</td>
<td>98.63</td>
<td>99.75</td>
<td>96.17</td>
<td>93.28</td>
<td>90.45</td>
<td>88.94</td>
</tr>
<tr>
<td>EMSA (protected)</td>
<td>51.24</td>
<td>53.82</td>
<td>54.12</td>
<td>49.15</td>
<td>48.72</td>
<td>48.61</td>
<td>47.74</td>
<td>45.54</td>
<td>46.72</td>
<td>52.47</td>
<td>50.14</td>
<td>50.64</td>
</tr>
</tbody>
</table>

- 100% means the attacker can steal the bit easily
- 50% means the bit is well protected
### Side-channel attack results (2)

RMS error in LSB for various ADC input signals (averaged across 3 ADCs)

<table>
<thead>
<tr>
<th>RMS error (LSBs)</th>
<th>Ramp</th>
<th>ECG</th>
<th>Image</th>
<th>Sine0.1Fs</th>
<th>Sine0.2Fs</th>
<th>Sine0.3Fs</th>
<th>Sine0.4Fs</th>
<th>Sine0.5Fs</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDD-side PSA (unprotected)</td>
<td>52.76</td>
<td>20.16</td>
<td>32.14</td>
<td>16.78</td>
<td>20.16</td>
<td>25.76</td>
<td>23.75</td>
<td>45.13</td>
</tr>
<tr>
<td>VDD-side PSA (protected)</td>
<td>1985.25</td>
<td>2675.17</td>
<td>1863.76</td>
<td>2516.78</td>
<td>2394.64</td>
<td>1963.76</td>
<td>2246.76</td>
<td>1876.18</td>
</tr>
<tr>
<td>GND-side PSA (unprotected)</td>
<td>48.91</td>
<td>45.18</td>
<td>36.76</td>
<td>32.17</td>
<td>25.18</td>
<td>28.76</td>
<td>32.17</td>
<td>42.73</td>
</tr>
<tr>
<td>GND-side PSA (protected)</td>
<td>2054.12</td>
<td>1986.47</td>
<td>2163.76</td>
<td>2246.46</td>
<td>1768.46</td>
<td>1732.94</td>
<td>2234.76</td>
<td>2346.71</td>
</tr>
<tr>
<td>EMSA (unprotected)</td>
<td>36.04</td>
<td>53.17</td>
<td>78.46</td>
<td>62.17</td>
<td>58.76</td>
<td>63.76</td>
<td>56.84</td>
<td>31.93</td>
</tr>
<tr>
<td>EMSA (protected)</td>
<td>1806.74</td>
<td>1746.52</td>
<td>2246.37</td>
<td>2634.76</td>
<td>2519.46</td>
<td>2476.83</td>
<td>2546.98</td>
<td>2246.83</td>
</tr>
</tbody>
</table>

1. Convolutional Neural Network (CNN) based side-channel attack is done by collecting 500K samples from a ramp signal as in [3] on a training ADC and performing the attack on 3 other ADCs with 50K samples for various inputs.
2. The protected ADC is in the secure mode.

- **Small RMS error without protection**
- **Large RMS error with protection**
Example image of EMSA result

- Most information is leaked without protection
- Information is leakage is prevented with protection
Spectrum of the secure mode ADC

- SNDR = 67.05 dB
- Fs = 40 MS/s
-芬=19.8 MHz
- NFFT = 16384
## Comparison against prior art

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect Mode</td>
<td>Protected</td>
<td>Unprotected</td>
<td>Random Mapping</td>
<td>Random Switching</td>
<td>Current Equalizer</td>
<td>Noise Injection</td>
</tr>
<tr>
<td>Protected Blocks</td>
<td>All Blocks</td>
<td>-</td>
<td>All Blocks</td>
<td>All Blocks</td>
<td>All Blocks</td>
<td>CDAC only</td>
</tr>
<tr>
<td>Neutralized Attacks</td>
<td>EM + Power</td>
<td>-</td>
<td>EM + Power</td>
<td>EM + Power</td>
<td>Power only</td>
<td>Power only</td>
</tr>
<tr>
<td>Attack Method</td>
<td>CNN(^1)</td>
<td>-</td>
<td>CNN(^1)</td>
<td>CNN</td>
<td>CNN</td>
<td>Template-Matching</td>
</tr>
<tr>
<td>VDD-PSA RMSE(^2)</td>
<td>0.48</td>
<td>-</td>
<td>0.40</td>
<td>0.23</td>
<td>0.094</td>
<td>0.92(^3)</td>
</tr>
<tr>
<td>GND-PSA RMSE</td>
<td>0.50</td>
<td>-</td>
<td>0.38</td>
<td>N/A</td>
<td>0.21</td>
<td>N/A</td>
</tr>
<tr>
<td>EMSA RMSE</td>
<td>0.44</td>
<td>-</td>
<td>0.45</td>
<td>0.18</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Sampling Rate [MS/s]</td>
<td>40</td>
<td>45</td>
<td>25</td>
<td>2</td>
<td>1.25</td>
<td>1</td>
</tr>
<tr>
<td>Power [uW]</td>
<td>698</td>
<td>722</td>
<td>539.8</td>
<td>50.2(^3)</td>
<td>158.5</td>
<td>65.0</td>
</tr>
<tr>
<td>SNDR [dB]</td>
<td>66.6</td>
<td>67.2</td>
<td>67.2</td>
<td>48.1</td>
<td>69.2</td>
<td>54.1</td>
</tr>
<tr>
<td>SFDR [dB]</td>
<td>80.2</td>
<td>80.5</td>
<td>86.6</td>
<td>N/A</td>
<td>89.6</td>
<td>64.3</td>
</tr>
<tr>
<td>Area [mm(^2)]</td>
<td>0.075</td>
<td>0.075</td>
<td>0.072</td>
<td>0.073</td>
<td>0.5</td>
<td>0.075</td>
</tr>
<tr>
<td>FoM(_{\text{ meta}}) (fJ/conv.-step.)</td>
<td>9.8(^3)</td>
<td>8.5(^3)</td>
<td>11.3</td>
<td>120.7</td>
<td>54.3</td>
<td>151.5</td>
</tr>
<tr>
<td>DNL [LSB]</td>
<td>-0.68/0.31</td>
<td>-0.62/0.37</td>
<td>-0.49/+0.35</td>
<td>N/A</td>
<td>-0.72/+0.77</td>
<td>-0.6/+0.6</td>
</tr>
<tr>
<td>INL [LSB]</td>
<td>-0.73/0.39</td>
<td>-0.67/0.72</td>
<td>-0.76/+0.67</td>
<td>N/A</td>
<td>-1.01/+0.86</td>
<td>-1.2/+1.2</td>
</tr>
</tbody>
</table>

Notes:
- CNN\(^1\): Convolutional Neural Network
- VDD-PSA RMSE\(^2\): Voltage Domain Power Spectral Analysis Root Mean Square Error
- GND-PSA RMSE: Ground Domain Power Spectral Analysis RMSE
- EMSA RMSE: Electrically Masked Security Analysis RMSE
- FoM\(_{\text{ meta}}\): FoM Meta
- DNL: Differential Non-Linearity
- INL: Integral Non-Linearity

---

*Comparisons and data are for illustrative purposes only. Actual performance may vary.*
Outline

- Motivation
- Prior art
- Proposed Sniff-SAR architecture
- Measurement results
- Conclusions
Conclusions

• Side-channel attack (SCA) on-chip countermeasure techniques incur non-negligible power and performance overheads

• A secure ADC with detection-driven protection and more effective protection scheme is proposed

• The prototype in 65nm process achieves a FoM of 9.8fJ/c.-s

• The prototype can detect a 30ohm series resistor for PSA and an EM probe at a 0.16mm distance
Acknowledgments

• This research was supported by DARPA, MIT Center for Integrated Circuits and Systems (CICS), and the TSMC university shuttle program

• The author thank Saurav Maji and Maitreyi Ashok at MIT for their support and feedback