Side-Channel Countermeasures for Hardware: is There a Light at the End of the Tunnel?

11. Sep 2013

Amir Moradi
Ruhr University Bochum
Outline

- Power Analysis Attack
- Masking
- Problems in hardware
- Possible approaches
Measurement Setup
Measurement Setup
Measurement Setup
Measurement Setup
Measurement Setup
Power Analysis Attack

- Recovering the key of crypto devices
- Hypothetical model for power consumption
- Compare the model with side-channel leakage (power)
- How?

\[ k \]
\[ Sbox \]
\[ t \]
\[ p \]
\[ \text{Correlation} \]

<table>
<thead>
<tr>
<th>$k=00$</th>
<th>$S$</th>
<th>$[c9, 27, bc]$</th>
<th>$[99, 62, 27]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{power}$</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$k=01$</th>
<th>$S$</th>
<th>$[7d, eb, b6]$</th>
<th>$[41, ac, eb]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{power}$</td>
<td>6</td>
<td>6</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$k=ff$</th>
<th>$S$</th>
<th>$[55, 25, 17]$</th>
<th>$[6f, 20, 25]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{power}$</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Correlation:
- 0.011
- 0.060
- 0.231
- 0.095
Masking

- Well-known SCA countermeasure
- to make the SC leakages independent of expected intermediate values
- Randomness is required
- Let’s consider the most common one, Boolean Masking

\[ S(p \oplus k) \]

\[ S(p \oplus k) \oplus n \]
Univariate vs. Multivariate Attacks

\[ p \xrightarrow{k} S(p \oplus k) \]

DPA/CPA/MIA

\[ p \xrightarrow{k} \text{masked Sbox} \xrightarrow{m \oplus n} S(p \oplus k) \oplus n \]

bivariate MIA

- squaring: 2\textsuperscript{nd} order univariate
- multiply: 2\textsuperscript{nd} order bivariate
- addition: 1\textsuperscript{st} order bivariate

combining: DPA/CPA
Masking (software case)

- Sequential operations
- First, generation of the “masked Sbox” having the mask(s)
- Second, feeding the masked input
- Time consuming
- Low efficiency
  - but feasible to counteract against univariate attacks

\[
\forall a, S'(a \oplus m) = S(a) \oplus n
\]
Masking (hardware case)

- High efficiency is desired
- ad-hoc/heuristic schemes

- Processing the mask ($m$) and masked data ($i \oplus m$) simultaneously
  - joint distribution of SC leakages mainly because of GLITCHES
  - possible attacks
Successfully Attacking Masked AES Hardware...
Our Solution at CHES 2010 (Correlation-Enhanced)

\[ p_1 \]

\[
\begin{array}{ccc}
12 & 3d & 78 \\
0.01 & 0.15 & 0.12 \\
\end{array}
\]

\[
\begin{array}{ccc}
f9 & ab & 3d \\
0.24 & 0.05 & 0.11 \\
\end{array}
\]

\[ p_2 \]

\[
\begin{array}{ccc}
45 & 9a & cf \\
0.32 & 0.20 & 0.05 \\
\end{array}
\]

\[
\begin{array}{ccc}
04 & 17 & e2 \\
0.19 & 0.27 & 0.26 \\
\end{array}
\]
Our Solution at CHES 2010 (Correlation-Enhanced)

\[ p_1 \]

- \( k_1 \) \( \rightarrow \) \( Sbox \) \( \rightarrow \) \( p_1 \)
- \( p_2 \)
- \( \rightarrow \) \( k_2 \)

\[
\begin{array}{cccccc}
12 & 3d & 78 & \ldots & f9 & ab & 3d \\
0.01 & 0.15 & 0.12 & \ldots & 0.24 & 0.05 & 0.11 \\
\end{array}
\]

\[
\begin{array}{cccc}
00 & 01 & 02 & \ldots & fd & fe & ff \\
0.23 & 0.12 & 0.21 & \ldots & 0.06 & 0.09 & 0.14 \\
\end{array}
\]

\[
\begin{array}{cccc}
p_1 & p_2 \\
\text{power} & \text{power} \\
\end{array}
\]

\[
\begin{array}{cccc}
45 & 9a & cf & \ldots & 04 & 17 & e2 \\
0.32 & 0.20 & 0.05 & \ldots & 0.19 & 0.27 & 0.26 \\
\end{array}
\]

average
Our Solution at CHES 2010 (Correlation-Enhanced)

### Inputs and Outputs

- **Input 1 ($p_1$):**
  - **Sbox Transformation:**
  - **Power Distribution:** 0.23, 0.12, 0.21, ..., 0.06, 0.09, 0.14

- **Input 2 ($p_2$):**
  - **Power Distribution:** 0.32, 0.20, 0.05, ..., 0.19, 0.27, 0.26

- **Output:**
  - **Power Distribution:**
    - $p_1$: 0.01, 0.15, 0.12, ..., 0.24, 0.05, 0.11
    - $p_2$: 0.32, 0.20, 0.05, ..., 0.19, 0.27, 0.26

### Correlation Enhancement

- **Delta Key ($\Delta k$) Effect:**
  - **Input 2 ($p_2 \oplus \Delta k$):**
    - **Power Distribution:** 0.32, 0.20, 0.05, ..., 0.19, 0.27, 0.26
  - **Output ($\Delta k = 00$):**
    - **Power Distribution:** 0.32, 0.20, 0.05, ..., 0.19, 0.27, 0.26

---

**Note:**
- The values are illustrative and not actual power consumption data.
Our Solution at CHES 2010 (Correlation-Enhanced)

\[ p_1 \]
\[
\begin{array}{cccc}
\text{power} & 12 & 3d & 78 & \ldots & f9 & ab & 3d \\
0.01 & 0.15 & 0.12 & \ldots & 0.24 & 0.05 & 0.11
\end{array}
\]

\[ p_1 \]
\[
\begin{array}{cccc}
\text{power} & 00 & 01 & 02 & \ldots & fd & fe & ff \\
0.23 & 0.12 & 0.21 & \ldots & 0.06 & 0.09 & 0.14
\end{array}
\]

\[ p_2 \]
\[
\begin{array}{cccc}
\text{power} & 45 & 9a & cf & \ldots & 04 & 17 & e2 \\
0.32 & 0.20 & 0.05 & \ldots & 0.19 & 0.27 & 0.26
\end{array}
\]

\[ p_2 + \Delta k \]
\[
\begin{array}{cccc}
\text{power} & 00 & 01 & 02 & \ldots & fd & fe & ff \\
0.32 & 0.20 & 0.05 & \ldots & 0.19 & 0.27 & 0.26
\end{array}
\]

\[ p_2 + \Delta k \]
\[
\begin{array}{cccc}
\text{power} & 00 & 01 & 02 & \ldots & fd & fe & ff \\
0.20 & 0.32 & 0.17 & \ldots & 0.09 & 0.26 & 0.27
\end{array}
\]

\[ p_2 + \Delta k \]
\[
\begin{array}{cccc}
\text{power} & 00 & 01 & 02 & \ldots & fd & fe & ff \\
0.26 & 0.27 & 0.19 & \ldots & 0.05 & 0.20 & 0.32
\end{array}
\]

\[ \Delta k = 00 \]
\[ \Delta k = 01 \]
\[ \Delta k = ff \]
Our Solution at CHES 2010 (Correlation-Enhanced)

\[ k_1 \] \rightarrow p_1 \rightarrow \text{Sbox} \rightarrow p_1 \text{ power} \begin{array}{ccc} 00 & 01 & 02 \end{array} \ldots \begin{array}{ccc} \text{fd} & \text{fe} & \text{ff} \end{array} \begin{array}{ccc} 0.23 & 0.12 & 0.21 \end{array} \ldots \begin{array}{ccc} 0.06 & 0.09 & 0.14 \end{array}

\[ k_2 \] \rightarrow p_2 \rightarrow \text{Sbox} \rightarrow p_2 \text{ power} \begin{array}{ccc} 00 & 01 & 02 \end{array} \ldots \begin{array}{ccc} \text{fd} & \text{fe} & \text{ff} \end{array} \begin{array}{ccc} 0.32 & 0.20 & 0.05 \end{array} \ldots \begin{array}{ccc} 0.19 & 0.27 & 0.26 \end{array}

\[ \Delta k = 00 \]

\[ \Delta k = 01 \]

\[ \Delta k = \text{ff} \]

Correlation

\[ \begin{array}{c} 0.230 \\ 0.408 \\ \vdots \\ 0.839 \\ \vdots \\ 0.312 \end{array} \]
Masking (hardware case)

- Systematic schemes
  - Threshold Implementation

\[ i \oplus m_1 \oplus m_2 \rightarrow f_1 \rightarrow o_1 \]
\[ m_1 \rightarrow f_2 \rightarrow o_2 \]
\[ m_2 \rightarrow f_3 \rightarrow o_3 \]

\[ o_1 \oplus o_2 \oplus o_3 = S(i) \]

- Independent leakage of \( f_1, f_2, f_3 \), no first-order leakage
- Their joint distribution \((f_1, f_2, f_3)\) still depends on \( i \)
  - a univariate attack still possible
Masking (hardware case)

- Systematic schemes
  - Global Look-Up-Table (GLUT)

- High area overhead
- High performance
- Still the same story
  - Processing the mask ($m$) and masked data ($i \oplus m$) simultaneously
  - A univariate leakage
CT-RSA 2012 approach
*A First-Order Leak-Free Masking Countermeasure*

- GLUT
  - Register update model
    - HD model
  - Known leakage
    - Specific value for $\alpha$ and $f_\alpha$
    - Constant flipping bits of $M$ register
    - Uniform distribution of $\Delta R$
    - Two options for $f_\alpha$
    - Satisfying desired protection
      - Having “Register Update Model”
CT-RSA 2012 approach

- GLUT
  - The same story
  - Processing the mask ($m$) and masked data ($i \oplus F(m)$) simultaneously
  - a univariate leakage expected
    - no register update model!
Implementation (case of AES)

- Xilinx Virtex-5 (LX50) FPGA
- Using (6 to 1) **LUT6** (or 16k-bit **BRAM**)
- Giant table
  - 1M bits for GLUT
    - 21840 LUT6 of all 28800
    - or 16 LUT6 + 64 BRAM of all 96
  - no way to have more than one GLUT in a design
- Common design architecture
  - Serialized (shift-register type)
Practical Evaluation

- SASEBO-GII
- 3 designs (Conventional, 1\textsuperscript{st} CT-RSA, 2\textsuperscript{nd} CT-RSA)
  - each by LUT6
- 3MHz clock, 1 GS/s, 20MHz bandwidth
- Fixed # of measurements 1 million
- Univariate correlation collision attack, 1\textsuperscript{st} and 2\textsuperscript{nd} order moments
Register Update Model

1\textsuperscript{st} order

2\textsuperscript{nd} order

Conventional

1\textsuperscript{st} CT-RSA

2\textsuperscript{nd} CT-RSA
Identity Model (Register Input/Output)

Conventional

1\textsuperscript{st} CT-RSA

2\textsuperscript{nd} CT-RSA
Dual Cipher Concept

- AES dual ciphers by

- Two ciphers $E$ and $E'$ are called dual ciphers, if they are isomorphic, i.e., if there exist invertible transformations $f()$, $g()$ and $h()$ such that

  \[
  \forall P, K \quad E_K(P) = f(E'_g(K)(h(P)))
  \]

- If $f()$, $g()$ and $h()$ are restricted to linear functions (bitwsie matrix multiplication), square of AES can written easily
- The same for AES$^4$, AES$^8$, ... AES$^{128}$ 8 cases
- Irreducible polynomial also can be changed, 30 in GF(2$^8$)
- In sum 240 dual ciphers exist more by tower field approach (61200)
Dual Ciphers as SCA Countermeasure

- claimed by the original authors, implemented by many
Evaluation

- found problems:
  - Mask Reuse
    - All plaintext bytes (Sboxes) share the same mask
  - Concurrent Processing
    - of Mask and the Masked Data
  - Unbalance (zero value)
Practical Investigation

- As before (SASEBO-GII, 1GS/s, ...)

- Very high power consumption
- Very slow, maximum freq. of 21 MHz
- Very high area overhead, 26 times
Correlation Collision Attack (1st-Order)

using 500k traces
Zero Value CPA

using 100k traces
Masking (hardware case)

- One more systematic scheme
  - Multi-party computation + Shamir secret sharing
- Basic GF($2^8$) operations, e.g., addition is easy
  - Multiplication needs more effort
- An Sbox computation
Target Scheme - Design
Target Scheme - Design
Target Scheme - Design
Target Scheme - Design
Target Scheme - Design
Target Scheme - Design
Our Evaluations

- FPGA-based platform (Virtex-5 LX50)

<table>
<thead>
<tr>
<th>Design</th>
<th>FF #</th>
<th>FF %</th>
<th>LUT #</th>
<th>LUT %</th>
<th>Slice #</th>
<th>Slice %</th>
<th>SB CLK</th>
<th>MC + ARK CLK</th>
<th>Encryption CLK</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 SB MC</td>
<td>315</td>
<td>1%</td>
<td>1387</td>
<td>5%</td>
<td>859</td>
<td>12%</td>
<td>2112</td>
<td>192</td>
<td>22 896</td>
</tr>
<tr>
<td>16 SB MC</td>
<td>4275</td>
<td>15%</td>
<td>21328</td>
<td>74%</td>
<td>no fit</td>
<td></td>
<td>132</td>
<td>12</td>
<td>1431</td>
</tr>
</tbody>
</table>

- Moderate power consumption due to separation of different circuit stages (3MHz)
Attack Results, 10 million, 1\textsuperscript{st} and 2\textsuperscript{nd} orders

- The first known \textit{univariate} resistant design in hardware
Danger?

- Hardware platforms for performance
  - High throughput
    - which we did reach
  - High clock frequency
    - Power peaks may overlap
    - Problem? (@ 24Mhz)
Attack Results, 24MHz, 1 million

1\textsuperscript{st}-order

![Graph of 1\textsuperscript{st}-order correlation over time]

2\textsuperscript{nd}-order

![Graph of 2\textsuperscript{nd}-order correlation over time]

All because of processing the shares in consecutive clock cycles
Lesson Learned / Future Issues

- Design of a countermeasure based on a model
  - perfect protection
    - in theory and in practice?
  - more leakage sources and models in practice
- Exploiting leakage sources of the platform before design
- Cost of univariate resistance
  - security-performance tradeoff
- Processing the mask and masked data consecutively
  - slowly reaching the software performance?
    - making a processor by giant hardware?
Thanks!

Any questions?

amir.moradi@rub.de

Embedded Security Group, Ruhr University Bochum, Germany