Optimal Key Ranking for Side-Channel Attacks

N. Veyrat-Charvillon, B. Gérard, M. Renauld and F-X. Standaert

UCL Crypto Group, Université catholique de Louvain

CHES 2011, September 30
Standard \textbf{DPA} Attacks

Side-channel traces
Standard DPA Attacks

\[
\rho_{X,Y} = \frac{\text{cov}(X,Y)}{\sigma_X \sigma_Y}
\]
Standard DPA Attacks

Side-channel traces
→
some kind of statistics
→
rank subkeys

\[ \rho_{X,Y} = \frac{\text{cov}(X,Y)}{\sigma_X \sigma_Y} \]
Standard DPA Attacks

Side-channel traces → some kind of statistics → rank subkeys → output key(s)

\[ \rho_{X,Y} = \frac{\text{cov}(X,Y)}{\sigma_X \sigma_Y} \]
Key is incorrect!
Abort, Retry, Fail?
Let’s try again

Output another key, or two, or $2^{32}$!

Wait... how do we choose them?
Let’s try again

Output another key, or two, or \(2^{32}\)!

Wait... how do we choose them?
Let’s try again

Output another key, or two, or $2^{32}$!

Wait... how do we choose them?
Let’s try again

Output another key, or two, or $2^{32}$!

Wait... how do we choose them?
Random sampling: EUROCRYPT '91
Random sampling: EUROCRYPT '91

\[
\begin{array}{ccc}
0 & k_2^{(j)} & 1 \\
\hline
k_1^{(j)} & \cdot & \hline
1 & & \\
\end{array}
\]
Random sampling: EUROCRYPT '91

$0 \leq k_1^{(j)} \leq 1$

$0 \leq k_2^{(j)} \leq 1$
Random sampling: EUROCRYPT ’91
Random sampling: EUROCRYPT ’91
Random sampling: EUROCRYPT '91
Random sampling: EUROCRYPT '91

\begin{align*}
k_1^{(j)} & \quad k_2^{(j)} \\
0 & \quad 1
\end{align*}
Random sampling: EUROCRYPT ’91
Random sampling: EUROCRYPT '91
Random sampling: EUROCRYPT ’91
Random sampling: EUROCRYPT ’91
Optimal enumeration

\[ k_1^{(j)} \]

\[ k_2^{(j)} \]
Optimal enumeration

\[ k_1^{(j)} \]

\[ k_2^{(j)} \]

\[ 0 \]

\[ 1 \]
Optimal enumeration
Optimal enumeration
Optimal enumeration
## Sampling overhead

<table>
<thead>
<tr>
<th>#Trials</th>
<th>$2^{16}$</th>
<th>$2^{20}$</th>
<th>$2^{24}$</th>
<th>$2^{28}$</th>
<th>$2^{32}$</th>
<th>$2^{36}$</th>
<th>$2^{40}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling</td>
<td>0.04s</td>
<td>0.31s</td>
<td>10.1s</td>
<td>160s</td>
<td>2560s</td>
<td>11h</td>
<td>182h</td>
</tr>
<tr>
<td>Enumeration</td>
<td>0.03s</td>
<td>0.55s</td>
<td>9.2s</td>
<td>163s</td>
<td>3130s</td>
<td>12h</td>
<td>221h</td>
</tr>
<tr>
<td>Memory</td>
<td>405KB</td>
<td>2.7MB</td>
<td>20MB</td>
<td>225MB</td>
<td>1.8GB</td>
<td>10GB</td>
<td>70GB</td>
</tr>
</tbody>
</table>

![Graph showing overhead and memory as a function of key rank](image-url)
Success rate: optimal enumeration

![Graph showing the success rate as a function of traces, with 1 candidate.]
Success rate: optimal enumeration

![Graph showing success rate against number of traces for 2^4 candidates]
Success rate: optimal enumeration

- Traces vs. success rate for different numbers of candidates.
- The y-axis represents the success rate, ranging from 0.0 to 1.0.
- The x-axis represents the number of traces, ranging from 50 to 250.
- The graph shows a curve indicating how the success rate improves with an increase in the number of traces.
- The number of candidates is indicated on the right side of the graph: $2^8$ candidates.
Success rate: optimal enumeration

![Graph showing success rate with 2^{12} candidates and trace number on the x-axis and success rate on the y-axis.](image-url)
Success rate: optimal enumeration

2^{16} candidates
Success rate: optimal enumeration

- Success rate on the y-axis
- Traces on the x-axis
- 2^{20} candidates

Graph showing the relationship between number of traces and success rate for 2^{20} candidates.
Success rate: optimal enumeration

Success rate vs number of traces for 2^{24} candidates.
Success rate: optimal enumeration

2^{28} candidates

traces

success
Success rate: optimal enumeration

2^{32} candidates

success

traces

0.0 0.2 0.4 0.6 0.8 1.0

50 100 150 200 250
If at first you don’t succeed . . .

http://eprint.iacr.org/2012/???