Investigating Profiled Side-Channel Attacks
Against the DES Key Schedule

Johann Heyszl¹, Katja Miller¹, Florian Unterstein¹, Marc Schink¹, Alexander Wagner¹,
Horst Gieser²,
Sven Freud³, Tobias Damm³, Dominik Klein³, Dennis Kügler³

¹ Fraunhofer Institute for Applied and Integrated Security (AISEC)
² Fraunhofer Research Institution for Microsystems and Solid State Technologies (EMFT)
³ Federal Office for Information Security (BSI)

CHES, Sept. 2020
Motivation and Main Research Questions

- Several ePrint publications [WH17, WHG17, WH18] describe:
  - Successful profiled attack against DES key schedule of a commercial security controller
  - ‘Single trace attack’, ‘weak keys’, ‘remaining rest entropies as low as 19 bits’

- Important questions open/unanswered:
  - Wide distributions and SCA-weak keys reproducible using state of the art tooling?
  - Device-specific or more general - other devices?
  - Precise impact on 3-key triple-DES?
  - Predictable through simulation?
Empirical Study: Commercial Security Controller

- Security controller, Java-Card, programmable for investigation
- Target: DES key schedule

- Alignement
- t-Test on preliminary leakage assumption: Leakage detected and measurement position selected
- Correlation-based leakage test CPOI [DS16]: POI selection
### DES Key Schedule - Round Keys and Bit Transitions

<table>
<thead>
<tr>
<th>Round key #</th>
<th>Indices refer to the input key excluding parity bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8 44 29 52 42 14 28 49 1 7 16 36 2 30 22 21 38 50 51 0 31 23 15 35</td>
</tr>
<tr>
<td>1</td>
<td>1 37 22 45 35 7 21 42 51 0 9 29 52 23 15 14 31 43 44 50 49 16 8 28</td>
</tr>
<tr>
<td>2</td>
<td>44 23 8 31 21 50 7 28 37 43 52 15 38 9 1 0 42 29 30 36 35 2 51 14</td>
</tr>
<tr>
<td>3</td>
<td>30 9 51 42 7 36 50 14 23 29 38 1 49 52 44 43 28 15 16 22 21 45 37 0</td>
</tr>
<tr>
<td>4</td>
<td>16 52 37 28 50 22 36 0 9 15 49 44 35 38 30 29 14 1 2 8 7 31 23 43</td>
</tr>
<tr>
<td>5</td>
<td>2 38 23 14 36 8 22 43 52 1 35 30 21 49 16 15 0 44 45 51 50 42 9 29</td>
</tr>
<tr>
<td>6</td>
<td>45 49 9 0 22 51 8 29 38 44 21 16 7 35 2 1 43 30 31 37 36 28 52 15</td>
</tr>
<tr>
<td>7</td>
<td>31 35 52 43 8 37 51 15 49 30 7 2 50 21 45 44 29 16 42 23 22 14 38 1</td>
</tr>
<tr>
<td>8</td>
<td>49 28 45 36 1 30 44 8 42 23 0 52 43 14 38 37 22 9 35 16 15 7 31 51</td>
</tr>
<tr>
<td>9</td>
<td>35 14 31 22 44 16 30 51 28 9 43 38 29 0 49 23 8 52 21 2 1 50 42 37</td>
</tr>
<tr>
<td>10</td>
<td>21 0 42 8 30 2 16 37 14 52 29 49 15 43 35 9 51 38 7 45 44 36 28 23</td>
</tr>
<tr>
<td>11</td>
<td>7 43 28 51 16 45 2 23 0 38 15 35 1 29 21 52 37 49 50 31 30 22 14 9</td>
</tr>
<tr>
<td>12</td>
<td>50 29 14 37 2 31 45 9 43 49 1 21 44 15 7 38 23 35 36 42 16 8 0 52</td>
</tr>
<tr>
<td>13</td>
<td>36 15 0 23 45 42 31 52 29 35 44 7 30 1 50 49 9 21 22 28 2 51 43 38</td>
</tr>
<tr>
<td>14</td>
<td>22 1 43 9 31 28 42 38 15 21 30 50 16 44 36 35 52 14 7 8 14 45 37 29 49</td>
</tr>
<tr>
<td>15</td>
<td>15 51 36 2 49 21 35 31 8 14 23 43 9 37 29 28 45 0 1 7 38 30 22 42</td>
</tr>
</tbody>
</table>

- Key schedule, 56 bit keys, 16 rounds, half of round keys depicted (‘register C’)
- Round keys only permutations of initial key bits
- Bits re-occur, even subsequent bit-pairs re-occur

© Fraunhofer
Leakage Model and Template Attack

- Key bits from register C. Transitions as dashes between bits. Coloring depicts occurrence rate (e.g. red 3 times, blue 10 times)

- Leakage model investigated precisely through SNR calculations: Exclusive XOR-leakage
  - XORs grouped and profiled in templates (instead of bits)
  - Dashed boxes mark grouped XORs for templates (4 in register C, 8 in total)

- Template attack: 7 bit templates, 2.5 mio profiling, 300 POIs, 1k attacked keys, 1/3/900 traces per key for attacker

- State of the art key rank estimation because independent XORs → security level in bits
Single DES Results Show Wide Distribution

- Security level [bits] of 1k keys as histogram

- Reduction on average and widely distributed results with apparent weak keys (unlike usual DPA results)
- The limit is low (i.e. 2 bit for the all-zeros/all-ones keys). The more keys are tested, the more weak ones!
Single DES Results Show Wide Distribution

- Increasing the attack traces per key (to 3 and 900)
- Improvement for attacker
- Widely distributed even with high number of traces (while some noise factors are removed)
Security levels over increasing traces per attacked key (left: 10 randomly selected, right: 10 low security level keys)

Convergence to different levels - Key weaknesses inherent!

Conclude that leakage model and switching noise determine key weakness
Overview and Comparison

<table>
<thead>
<tr>
<th>This work</th>
<th>Wagner et al.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1k keys, 300 POIs</td>
<td>297k keys, 352 POIs</td>
</tr>
<tr>
<td>1 trace</td>
<td>3 traces</td>
</tr>
<tr>
<td>1.5×DES per trace (^1)</td>
<td>4×DES per trace</td>
</tr>
<tr>
<td>Mean [bit]</td>
<td>49.4</td>
</tr>
</tbody>
</table>

- Results similar, hence, reproducible
- What does this mean for actual applications - implications on triple-DES?

\(^1\) 1 DES includes 9 backwards rounds, hence, \(\approx 1.5\) DES
Impact on 3-key triple-DES

- Estimate 3-key triple-DES security (allowing meet-in-the-middle advantage while using SCA results)
- Empirical density of security levels
- Based on previously shown independent single DES results (3 different keys):
  1 trace (blue), 3 traces (orange), 900 traces (green), noise-free simulation (black, dashed)
Impact on 3-key triple-DES

<table>
<thead>
<tr>
<th></th>
<th>1 trace</th>
<th>3 traces</th>
<th>900 traces</th>
<th>sim.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean sec. level 1-key 1-DES [bit]</td>
<td>49.4</td>
<td>48.2</td>
<td>45.7</td>
<td>42.3</td>
</tr>
<tr>
<td>Mean sec. level 3-key 3-DES [bit]</td>
<td>96.1</td>
<td>93.8</td>
<td>88.7</td>
<td>82.1</td>
</tr>
<tr>
<td>Fraction of 3-key 3-DES cases &lt; 80 bit</td>
<td>0.24 %</td>
<td>0.43 %</td>
<td>6.3 %</td>
<td>37.4 %</td>
</tr>
<tr>
<td>Fraction of 3-key 3-DES cases &lt; 70 bit</td>
<td>0.0015 %</td>
<td>n.a.</td>
<td>0.32 %</td>
<td>4.0 %</td>
</tr>
</tbody>
</table>

- Security level for 3-key triple-DES high on average
- But small percentage of weak key-triples: E.g. 0.24 % < 80 bit after single trace attack - every 400th device
Generalisation through Simplified Simulation

- Simplified simulation: XOR leakage with equally weighted XOR-transitions
- No additional noise - only algorithm-dependent switching noise from key bits

- Wide distribution of security levels and weak keys even then! Issue must be more general
Simulation vs. Reality

- Security level attack results
- From simulated attack (x) and from actual measurements (y)
- Two classes: (blue) randomly selected, (red) random but \( \approx 90\% \) zeros/ones
- Simulation prediction very precise for uneven zeros/ones, less for general keys
- Lack of precision likely due to simplified model w/o weighted XOR-transitions
- Key weakness not device-specific for big part
Similar results with mean security level of **48.7** bit (≈ 3 bit more)

(460 POIs, 900 traces per key, 1000 keys)
Empirical Study: DES Engine in General Purpose µC

- STM32 HW DES engine
- Different leakage model: Exclusive value-based leakage
- Similar results! (100 traces per key, 10k attacked keys)
- Underlines generality of issue: Two different leakage models / implementations lead to widely distributed results!
Conclusion

- Wide distribution of security levels and weak keys exist
- Proven on different implementations/leakage models and in simulation
- More devices are affected if leakage from key schedule is existent (e.g. no effective masking)
- DES key schedule prone due to re-occurrence of transitions
- Impact on commercial security controller (3-DES) less dramatic than alleged (e.g. 0.24 % < 80)

Open

- How to assess security when results are widely distributed and weak keys exist?
- Maybe similar with profiled attacks against other algorithms’ key schedules if leakage is exploitable
References

From improved leakage detection to the detection of points of interests in leakage traces.

Investigating profiled side-channel attacks against the des key schedule.

Single-trace template attack on the DES round keys of a recent smart card.

Improved brute-force search strategies for single-trace and few-traces template attacks on the DES round keys.

Brute-force search strategies for single-trace and few - traces template attacks on the DES round keys of a recent smart card.
Impact of Noise Significant on Individual Traces

- When attacking the 900 traces as single trace attacks (same keys, left: 10 randomly selected, right: 10 low security level keys)
- Noise influence high on single traces - Even weak keys are often ‘strong’
- (Previously shown distribution for single trace already include this noise of course.)