Combined Fault and Side-Channel Attacks on the AES Key Schedule

François DASSANCE
Inside Secure

Alexandre VENELLI
Inside Secure

FDTC 2012
09/09/2012
Outline

1. Combined attack
2. Related work on combined attacks
   1. Asymmetric cryptosystems
   2. Symmetric cryptosystems
   3. Roche et al.’s attack on AES
3. Combined attacks on AES key schedule
   1. Recursive structure of the key schedule
   2. RCON
   3. Affine transformation
4. Complexity of our attacks
5. Countermeasures
6. Conclusion
Combined attack

• Combines a fault attack with a leakage analysis

• Main goal: attack implementations resistant against fault and leakage analysis

• New implementations + new countermeasures often necessary
**Algorithm 1** Binary SPA-FA resistant exponentiation

**Input:** $x \in \mathbb{G}$ and $d = (d_{k-1}, \ldots, d_0)_2 \in \mathbb{N}$

**Output:** $x^d$

1: $A \leftarrow x$
2: $R[0] \leftarrow x$
3: $R[1] \leftarrow 1$
4: for $i = 0$ to $k - 1$ do
5: \hspace{1em} $R[d_i] \leftarrow R[d_i].A$
6: \hspace{1em} $A \leftarrow A^2$
7: end for
8: $R[0] \leftarrow R[0].R[1]$
9: if $(R[0] \neq A)$ then
10: \hspace{1em} error
11: end if
12: return $R[1]$
Example of combined attack

Algorithm 1 Binary SPA-FA resistant exponentiation

Input: $x \in \mathbb{G}$ and $d = (d_{k-1}, \ldots, d_0)_2 \in \mathbb{N}$

Output: $x^d$

1: $A \leftarrow x$
2: $R[0] \leftarrow x$
3: $R[1] \leftarrow 1$
4: for $i = 0$ to $k - 1$ do
5: $R[d_i] \leftarrow R[d_i].A$
6: $A \leftarrow A^2$
7: end for
8: $R[0] \leftarrow R[0].R[1]$
9: if $(R[0] \neq A)$ then
10: error
11: end if
12: return $R[1]$
Outline

1. Combined attack
2. Related work on combined attacks
   1. Asymmetric cryptosystems
   2. Symmetric cryptosystems
   3. Roche et al.’s attack on AES
3. Combined attacks on AES key schedule
   1. Recursive structure of the key schedule
   2. RCON
   3. Affine transformation
4. Complexity of our attacks
5. Countermeasures
6. Conclusion
Asymmetric cryptosystems

- Fault Analysis + Simple Side-Channel Analysis

- Attack on atomic left-to-right exponentiation
  - Amiel, Villegas, Feix, Marcel - 2007

- Resistant algorithms for RSA and ECC
  - Schmidt, Tunstall, Avanzi, Kizhvatov, Kasper, Oswald - 2010

- Attack on scalar multiplication
  - Fan, Gierlichs, Vercauteren - 2011
Symmetric cryptosystems

- Fault Analysis + Differential Side-Channel Analysis

- Differential Behavioral Analysis: attack on non-masked AES
  - Robisson, Manet - 2007

- Attack on masked AES but not FA-protected. Reduce the DPA countermeasure of one order.
  - Clavier, Feix, Gagnerot, Rousselet - 2010

- Attack on AES FA-protected and with masking of any order
  - Roche, Lomné, Khalfallah - 2011
Roche et al. combined attack

• Principle:
  1. Repeatable fault on the 16 bytes of key state of round 9
  2. Record the power consumption curve
  3. Find a first-order correlation on the computation of the faulted ciphertext

• Main relation:

\[
\tilde{C}_i^j = SB(SB^{-1}(C_i^j \oplus k_{10}^j) \oplus e_9^j) \oplus k_{10}^j \oplus e_{10}^j
\]

• Complexity to retrieve the whole key:
  - \( N \) faults and \( 2^{28} A \)
  - \( A = \) any DSCA statistical function on \( N \) curves
## Efficiency

<table>
<thead>
<tr>
<th></th>
<th>Combined attack</th>
<th>High-order DSCA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of curves</strong></td>
<td>Few and fixed</td>
<td>A lot and increasing with the order of masking</td>
</tr>
<tr>
<td><strong>Complexity of key retrieval algorithm</strong></td>
<td>$2^{28} A$</td>
<td>$2^{12} A$</td>
</tr>
</tbody>
</table>
Remarks on Roche et al.

• Requires fault on the 16 bytes of the key
  – Not practical in all AES implementations
  – Not trivial with all fault injection techniques

• If a stuck-at fault model is considered, a masked bit induces a repeatability divided by 2

• High complexity of the key retrieval algorithm
Outline

1. Combined attack
2. Related work on combined attacks
   1. Asymmetric cryptosystems
   2. Symmetric cryptosystems
   3. Roche et al.’s attack on AES
3. Combined attacks on AES key schedule
   1. Recursive structure of the key schedule
   2. RCON
   3. Affine transformation
4. Complexity of our attacks
5. Countermeasures
6. Conclusion
Combined attacks on AES key schedule

• Attacks based on two properties of the key schedule:
  – Recursive structure
  – Use of constant values

• Our propositions improve:
  – The number of faults
  – The complexity of the key retrieval algorithm
Recursive structure (1)

• Round key $K_9$:

\[
K_9^0 = K_8^0 \oplus RCON_9 \oplus SB(K_8^{13}) \\
K_9^1 = K_8^1 \oplus SB(K_8^{14}) \\
K_9^2 = K_8^2 \oplus SB(K_8^{15}) \\
K_9^3 = K_8^3 \oplus SB(K_8^{12}) \\
K_9^j = K_8^j \oplus K_9^{j-4} \text{ for } 4 \leq j \leq 15
\]

• Relations between faults on $K_9$

• Ex: fault $e_9^0$ in $K_9^0$ \(\Rightarrow\) same fault on bytes 4, 8 and 12

• Relations between faults on $K_{10}$

• Ex: fault $e_9^0$ in $K_9^0$ \(\Rightarrow\) $e_9^0 = e_{10}^0 = e_{10}^8 = e_{10}^4 = e_{10}^{12} = 0$
Recursive structure (2)

- Needs $4N$ faults
- Improvements on the key retrieval algorithm
- To retrieve $K_{10}^0$
  - Loop only on $k_{10}^0$ and $e_9^0$ as $e_{10}^0 = e_9^0$
  - Complexity for this byte: $2^{16}A$
- Once $e_9^0$ is found $\Rightarrow e_9^4$, $e_9^8$ and $e_9^{12}$ are deduced
  - Simple loop on $k_{10}^j$ for $j = 4, 8, 12$
  - Complexity for each of these 3 bytes: $2^8A$
- Same method for $K_{9}^1$, $K_{9}^2$ and $K_{9}^3$
- Complexity for the whole key:
  $$4 \times (2^{16} + 3 \times 2^8)A$$
  $$= (2^{20} + 3 \times 2^{10})A$$
First column of $K_9$

\[
\begin{align*}
K_9^0 &= K_8^0 \oplus RCON_9 \oplus SB(K_8^{13}) \\
K_9^4 &= K_8^4 \oplus K_9^0 \\
K_9^8 &= K_8^8 \oplus K_9^4 \\
K_9^{12} &= K_8^{12} \oplus K_9^8
\end{align*}
\]

- One fault on $RCON_9$ affects 4 bytes of $K_9$ in the same way
- The fault can have a permanent effect
- Complexity similar to previous attack for 4 bytes:
  \[(2^{16} + 3 \times 2^8)A\]
RCON (2)

Combined Fault and Side-Channel Attacks on the AES Key Schedule – 09/09/2012
Attacking known constant values

- If the fault setup is characterized...

- $RCON_9 = 0x1B$

- Ex: if single bit stuck-at 0 or 1 model, only 4 possible values for $RCON_9$ (0x1A, 0x19, 0x13, 0x0B if stuck-at 0)

- Lower complexity for key retrieval algorithm (4 bytes): $2^{10}A$

- Whether stuck-at or bit-flip model, a fault on a constant will be XOR-ed $\rightarrow$ No impact on the repeatability
Affine transformation (1)

• Most DSCA countermeasures compute the SubBytes as

\[ SB(X) = \Omega \cdot \text{Inv}_{F_{2^8}}(X) \oplus \Delta \]

where \( \Omega \) is the matrix of the affine transformation and \( \Delta \) is the vector.

• Different attack scenarios are possible depending on the implementation
1. Transient fault on $\Delta$:
   - Same case as before
   - Complexity: $4N$ faults and $(2^{18} + 3 \times 2^{10})A$

2. Permanent fault. Different $\Delta_{SW}$ and $\Delta_{SB}$ for the SubWord and SubBytes
   - A fault $e_{SW}$ on $\Delta_{SW}$ affects round 9 and 10
   - Faulted round 9 key is $\tilde{K}^j_9 = K^j_9 \oplus e_{SW}$ for $0 \leq j \leq 15$
   - Relations between errors on $K_{10}$
     \[
     e_{10}^{j+4} = e_{10}^{j+12} = e_{10}^j \oplus e_{SW},
     \]
     \[
     e_{10}^{j+8} = e_{10}^j \text{ for } j = 0, 1, 2, 3
     \]
   - Complexity: $N$ faults and $(2^{24} + 3 \times 2^{16} + 3 \times 2^{10})A$
Affine transformation (3)

3. Permanent fault. Same $\Delta$ for SubWord and SubBytes
   - Same complexity as previous scenario
   - Data path modified $\rightarrow$ relation of key retrieval becomes
     $$SB(SB^{-1}(C_i^j \oplus k_{10}^j) \oplus e_{9}^j) \oplus e_{9}^j \oplus k_{10}^j \oplus e_{10}^j$$

   - If the fault setup is characterized, we can lower the complexity
     1. Transient fault:
        $4N$ faults and $2^{12}A$ (same complexity as classical DSCA)
     2. Permanent fault:
        $N$ faults and $(2^{20} + 3 \times 2^{10})A$
1. Combined attack
2. Related work on combined attacks
   1. Asymmetric cryptosystems
   2. Symmetric cryptosystems
   3. Roche et al.’s attack on AES
3. Combined attacks on AES key schedule
   1. Recursive structure of the key schedule
   2. RCON
   3. Affine transformation
4. Complexity of our attacks
5. Countermeasures
6. Conclusion
# Complexity of our attacks

<table>
<thead>
<tr>
<th>Attack</th>
<th># faults</th>
<th># A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key state $K_9$ (Roche et al.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Transient on 16 bytes</td>
<td>$N$</td>
<td>$2^{28}$</td>
</tr>
<tr>
<td>Key state $K_9$ (Roche et al.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Transient on 1 byte</td>
<td>$16N$</td>
<td>$2^{20}$</td>
</tr>
<tr>
<td>Key schedule</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Transient 1 byte</td>
<td>$4N$</td>
<td>$2^{18} + 3 \times 2^{10}$</td>
</tr>
<tr>
<td>RCON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Transient known on 1 byte</td>
<td>$N$</td>
<td>$2^{10}$</td>
</tr>
<tr>
<td>- Transient random on 1 byte</td>
<td>$N$</td>
<td>$2^{16} + 3 \times 2^{8}$</td>
</tr>
<tr>
<td>- Permanent known on 1 byte</td>
<td>$1$</td>
<td>$2^{10}$</td>
</tr>
<tr>
<td>- Permanent random on 1 byte</td>
<td>$1$</td>
<td>$2^{16} + 3 \times 2^{8}$</td>
</tr>
<tr>
<td>Affine transformation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Transient known on 1 byte</td>
<td>$4N$</td>
<td>$2^{12}$</td>
</tr>
<tr>
<td>- Transient random on 1 byte</td>
<td>$4N$</td>
<td>$2^{18} + 3 \times 2^{10}$</td>
</tr>
<tr>
<td>- Permanent known on 1 byte</td>
<td>$N$</td>
<td>$2^{20} + 3 \times 2^{10}$</td>
</tr>
<tr>
<td>- Permanent random on 1 byte</td>
<td>$N$</td>
<td>$2^{24} + 3 \times 2^{16} + 3 \times 2^{10}$</td>
</tr>
</tbody>
</table>
Outline

1. Combined attack
2. Related work on combined attacks
   1. Asymmetric cryptosystems
   2. Symmetric cryptosystems
   3. Roche et al.’s attack on AES
3. Combined attacks on AES key schedule
   1. Recursive structure of the key schedule
   2. RCON
   3. Affine transformation
4. Complexity of our attacks
5. Countermeasures
6. Conclusion
Countermeasures

• Masked coherence check:
  1. Store $C \oplus M_1$ and $C \oplus M_2$ two ciphertexts of the same message masked with $M_1$ and $M_2$
  2. Check $(C \oplus M_1) \oplus M_2 =? (C \oplus M_2) \oplus M_1$
  3. If no fault, demask and output the ciphertext $C$

• Does not detect a permanent fault on $RCON_9$. Needs a known answer test or integrity check on $RCON_9$
Outline

1. Combined attack
2. Related work on combined attacks
   1. Asymmetric cryptosystems
   2. Symmetric cryptosystems
   3. Roche et al.’s attack on AES
3. Combined attacks on AES key schedule
   1. Recursive structure of the key schedule
   2. RCON
   3. Affine transformation
4. Complexity of our attacks
5. Countermeasures
6. Conclusion
Conclusion

• Combined attacks are a real threat to most current crypto implementations

• We propose different attack paths on AES that lower the complexity of previous combined attacks

• Repeatability of our attacks on AES constants do not depend on a stuck-at or bit-flip fault

• Needs additional countermeasure to protect against an attack on $RCO N_9$
Thank you for your attention!

Contact: avenelli@insidefr.com