MitM Differential Fault Attack on AES-192

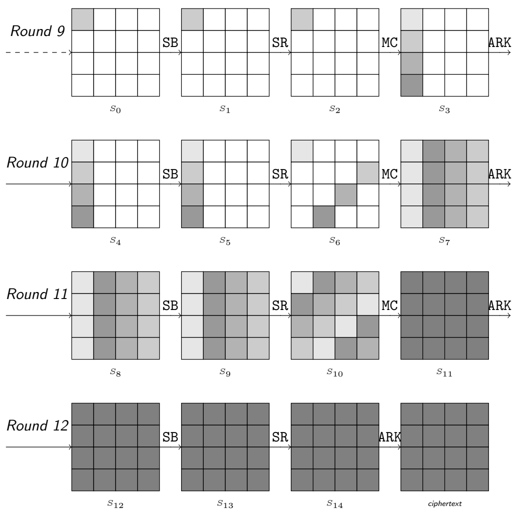

Figure 1: MitM differential fault analysis on `AES-192`.

Derbez *et al.*'s MitM DFA on AES-192[DFL11]

Derbez *et al.* simply extended the DFA attack on AES-128 for AES-192 in [DFL11]. Denote k_0 as the whitening key, and k_i $(i = 1, 2, ..., 12)$ as the subkey of Round i. Let $U_i = \mathtt{MC}^{-1}(k_i)$.

Step I. They first recover the key cells of AES-192 using the same MitM algorithm as AES-128: $\{k_{12}[1, 4, 11, 14], U_{11}[7]\}$, $\{k_{12}[2, 5, 8, 15], U_{11}[10]\}$, $\{k_{12}[0, 7, 10, 13], U_{11}[0]\}$ and $\{k_{12}[3, 6, 9, 12], U_{11}[13]\}$ according to the the filter of the equations between $\Delta S_8[0]$, $\Delta S_8[1]$, $\Delta S_8[2]$ and $\Delta S_8[3]$. The time of this step is the same with the DFA on AES-128, which is 3×2^{40}.

Step II. After recovering the 128-bit subkey k_{12}, in order to recover the full 192-bit key, they peel off the last round of AES-192 to perform a 3-round (Round 9-11) differential fault attacks following the idea of Piret and Quisquater [PQ03] with the same correct and faulty pairs. Therefore, an additional time complexity is required to implement Piret and Quisquater's attack, which is estimated as 2^{40} "Piret and Quisquater resolution" by Derbez *et al.* [DFL11].

Our Improved Attack

We introduce a new MitM DFA on AES-192, which uses the same Step I as Derbez *et al.* [DFL11] to recover k_{12}. But we do not use Piret and Quisquater's attack (Step II) to recover the remaining key bits.

A new Step II: After recovering k_{12}, we also peal off the last round. In order to recover the full 192-bit key, we need to recover the last two columns of k_{11}, which is equivalent to recovering $U_{11}[8, 9, 10, 11, 12, 13, 14, 15]$. Among those bytes, $U_{11}[10, 13]$ are already recovered in Step I.

After peel off Round 12, we can derive $\Delta S_8[8] = \Delta S_8[11]$, which is equivalent to

$$(SB^{-1}(A \oplus U_{11}[8]) \oplus SB^{-1}(\tilde{A} \oplus U_{11}[8])) = SB^{-1}(B \oplus U_{11}[15]) \oplus SB^{-1}(\tilde{B} \oplus U_{11}[15]), \quad (1)$$

where A and B are known values at this stage and only depend on the correct ciphertext and k_{12}, similar to $\tilde{A}$ and $\tilde{B}$. Then, we use Equ. (1) as a filter to build a local MitM attack, where two correct-faulty ciphertext pairs will provide a filter of 2^{-16}. Therefore, only one candidate of $U_{11}[8, 15]$ will remain. The time complexity of local MitM is 2×2^8 with about 2^8 memory.

Similarly, we can recovery $U_{11}[11, 14]$ and $U_{11}[9, 12]$ with similar matching equations like Equ. (1). The last two columns of k_{11} are recovered. The total time complexity of our new Step II is 6×2^8 with about 2^8 memory, which is smaller than Derbez *et al.*'s Step II.

Two correct-faulty ciphertext pairs needed in our new Step II can reuse the pairs from Step I, and no additional fault injections are needed here.

References

[DFL11] Patrick Derbez, Pierre-Alain Fouque, and Delphine Leresteux. Meet-in-the-middle and impossible differential fault analysis on AES. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer Science*, pages 274–291. Springer, 2011.

[PQ03] Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In Colin D. Walter, Çetin Kaya Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, volume 2779 of *Lecture Notes in Computer Science*, pages 77–88. Springer, 2003.