A Multi-Round Side Channel Attack on AES using Belief Propagation

Hélène Le Bouder[1] **Ronan Lashermes**[1] Yanis Linge[2]
Gaël Thomas[3] Jean Yves Zie

[1] INRIA Rennes, LHS/PEC

[2] STMicroelectronics

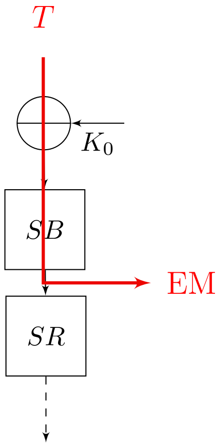
[3] Orange Labs Issy Les Moulineaux

January 26-27th, 2017

Context

Evaluate the power of Side-Channels Analyses.

- Side Channel Attacks on block ciphers : physical values of a device leak information about intermediate state of the cipher.
- Typical SCA links texts and measurements.
- Restricted on the first or last round.



Motivation

- Case of an attacker who can just observe leakages.
- No access to the device input and output.
- No template.

Overview of SCAs

Divide-and-Conquer (DC) methods

- Attack one key byte at a time
- E.g. DPA, CPA, MIA,. . .
- Enumeration to combine different key bytes

Global methods

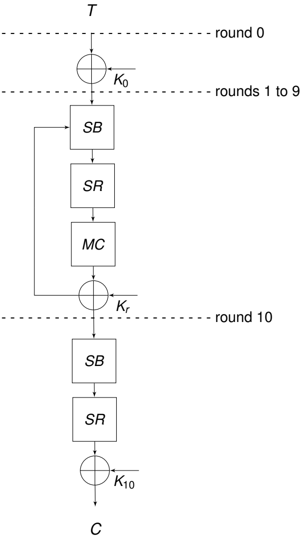
- Model whole algorithm and leakages
- Solve using SAT-solver, Gröbner bases or Belief Propagation (BP)

Our Contribution

- New side channel attack.
- The attacker only knows AES is running and is able to synchronize.
- No plain/ciphertexts, no template.
- No SPA on the Key Expansion, Round keys have already been precomputed.
- DC approach with two leakages to find a round key byte.
- Possible on any middle round of AES.
- Combine information over multiple rounds using BP.

Target cipher: AES

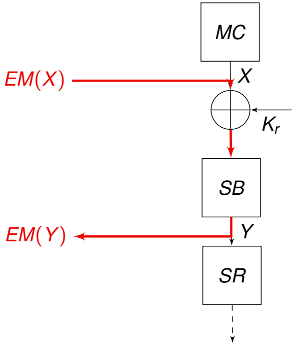
- 128-bit block cipher with 128-bit key.
- SB non-linear S-box, SR and MC linear layer.
- 11 rounds keys K_r, $r \in [\![0, 10]\!]$.
- K_0 master key, K_{r+1} derived from K_r using KeyExpansion.



Attack Path

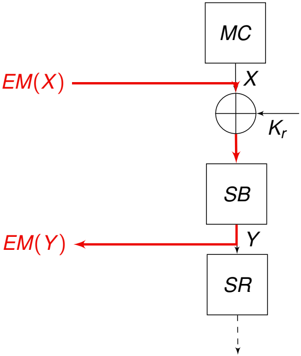
- Find two leakages for each round key.
- Chose the most leaking functions.
- Output of MC at round r.
- Output of SB at round $r + 1$.

Use the **Hamming Weight** (HW) model.



Does it works? (noise-free case)

- Denote $\hat{k}$ the correct key byte.
- For a pair of HW (h_x, h_y), let $\mathbb{K}_{(h_x,h_y)}$ be the set of possible keys for that pair.
- Repeat for every input value x, and build $\mathbb{K}(\hat{k}) = \bigcap_{x=0}^{255} \mathbb{K}_{(h_x,h_y)}$.
- The 256 sets $\mathbb{K}(\hat{k})$ are pair-wise different.



$$\mathbb{K}_{(h_x,h_y)} = \{k \text{ s.t. } \exists x \in HW^{-1}(h_x) \text{ and } HW\left(SB\left(k \oplus x\right)\right) = h_y\}$$

- Leakage considered as Hamming Weight (HW) with Gaussian noise

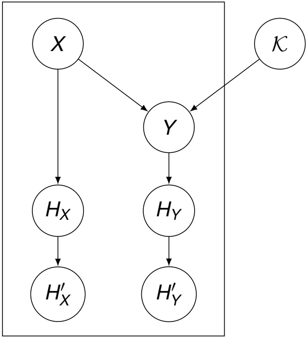
$$h'_z = h_z + \delta$$

with δ sampled from $\mathcal{N}\left(0, \sigma_Z^2\right)$.

- Goal: given n measurements $\{(h'_x, h'_y)\}_n$, estimate

$$A_k = \Pr\left[\mathcal{K} = k | \{(h'_x, h'_y)\}_n\right].$$

- Use Bayesian inference to derive it from $\Pr\left[(h_x, h_y)|\mathcal{K} = k\right]$ and pdf of $\mathcal{N}(0, \sigma_Z^2)$.



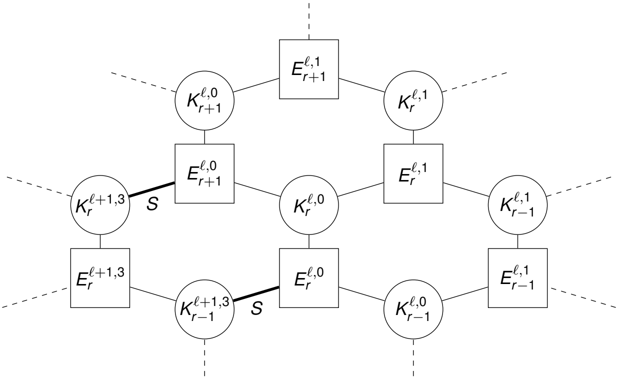
$$A_k \propto \prod_{i=1}^{n} \sum_{(h_x,h_y)} \mathcal{F}_{\sigma_X}\left(h'_{x,i} - h_x\right) \cdot \mathcal{F}_{\sigma_Y}\left(h'_{y,i} - h_y\right) \cdot \Pr\left[(h_x, h_y)|\mathcal{K} = k\right] \quad .$$

Crossing information using Belief Propagation

- Previous analysis can be conducted on every byte of every middle round key.
- Round keys linked by the relations of KeyExpansion (KE).
- Use BP to tie information together.
- Expected to work well because of KE sparse structure.
- Good at handling errors (inspired from coding theory).

BP in a nutshell

- BP relies on a bipartite graph: key bytes and equations of KE.
- To each node in the graph is associated some information.
- Nodes exchange information with their neighbours.
- Use Bayesian inference to improve their own knowledge.
- Iterate process to propagate information through the graph.



Simulation Results 1: on a single byte

- Randomly generated HW pairs with Gaussian noise $\mathcal{N}(0, \sigma^2)$.
- Different noise values σ, different numbers of traces n.
- Average rank of the good key byte $\hat{k}$, for 100 simulated attacks and for each possible value of $\hat{k}$, **without BP**.

$n \setminus \sigma$	0.1	0.2	0.3	0.5	1.0	1.5	2.0	3.0
100	1.2	1.3	2.3	14	66	96	107	119
1000	1	1	1	1	7.1	35	66	97
10000	1	1	1	1	1	2.2	12	48
100000	1	1	1	1	1	1	1.1	7.3

- Minimum (over the 9 round keys) Hamming distance between the guessed round key and the correct round key, **with BP**.

$n \setminus \sigma$	0.1	0.2	0.3	0.5	1.0	1.5	2.0	3.0
100	0	0	0	0	59	51	53	54
1000	0	0	0	0	0	39	46	51
10000	0	0	0	0	0	0	0	40
100000	0	0	0	0	0	0	0	0

- Improvement due to BP

$n \setminus \sigma$	0.1	0.2	0.3	0.5	1.0	1.5	2.0	3.0
100	✓	✓	✓	✓	×	×	×	×
1000	✓	✓	✓	✓	✓	×	×	×
10000	✓	✓	✓	✓	✓	✓	✓	×
100000	✓	✓	✓	✓	✓	✓	✓	✓

Conclusion

- New SCA with only leakage measurements, no text, no template.
- Combine the divide-and-conquer (DC) and global strategies.
- DC to score each round-key byte separately.
- Global using Belief Propagation to aggregate the knowledge on the round-key bytes.
- Simulation results shows the attack is effective.
- The hybrid approach, DC on key bytes, BP on KE, yield a good trade-off in efficiency vs computation cost.
- **Beware of the amount of information that can be extracted from side-channels.**

Future works

- The elephant in the room: is a noisy-leakage gaussian? Is it a good approximation?
- Requires practical experiments for confirmation.
- May the attack be adapted to accept other noise distribution?
- **Future of SCA:** take into account all leakages, not only one moment (the time dimension should not have a special treatment).

Thank you!

Any questions?

Our logo collection: