

A Note on Key Ranking for Optimal Collision Side-Channel Attacks

Cezary Glowacz

Deutsche Telekom Security GmbH
cezary.glowacz@t-systems.com

Abstract. In [1] we studied collision side-channel attacks, derived an optimal distinguisher for the key, and provided an optimal algorithm for maximizing the success rate of the attacks. In this note we show that the problem of key ranking using an optimal distinguisher for collision side-channel attacks is NP-hard and we provide lower bounds for key ranks in collision side-channel attacks.

Keywords: Collision Side-Channel Attacks · Key Ranking · Computational Complexity · Lower Bounds

1 Introduction

Side-channel attacks exploit measurable leakage signals emitted by the underlying hardware platform during execution of cryptographic functions. Given an adequate stochastic model of the emitted signals optimal strategies for key recovery can be derived. The optimality means that a key candidate with highest a posteriori probability conditioned on the measured leakage signals is identified and that the identification process can be performed within a useful time frame. Such optimal attack will maximize the success probability for finding the secret key in a sequence of side-channel attacks. In [1] we studied collision side-channel attacks, derived an optimal distinguisher for the key, and provided an optimal algorithm for key identification. The distinguisher for the key is a statistic based on the measured leakage signals which allows to decide for any two key candidates the order of their corresponding a posteriori probabilities. The optimal distinguisher can also be used to enumerate key candidates, i.e. to list the key candidates in descending order according to their a posteriori probability. The attacker can use the list and try each key candidate starting with the highest ranked one. In this context one may consider the n -th order success probability, i.e. the probability that the secret key can be found within the first n key candidates in the sorted list. In this meaning the attack presented in [1] is a 1-st order attack. In security evaluations it is important to know the position of the secret key, i.e. its rank, in the sorted key list even without actually creating the list. This allows to rate the effort needed to find the secret key using a statistically optimal search strategy. In this note we show that the problem of key ranking using an optimal distinguisher for collision side-channel attacks is NP-hard and we provide lower bounds for key ranks in collision side-channel attacks.

2 The NP-Hardness of Key Ranking for Collision Side-Channel Attacks

The optimal distinguisher $D_{opt.fun.gauss}$ and its objective function $D(k, x)$ which were derived in [1] for collision side-channel attacks assuming Gaussian distributed noise and Gaussian distributed leakage function values are restated in equations (1) and (2).

$$D_{opt.fun.gauss} = \operatorname{argmax}_{k \in (\mathbb{F}_2^n)^L} D(k, x) \quad (1)$$

$$D(k, x) = \sum_{q \in \mathbb{F}_2^n} \left(\sum_{l=1}^L x_{q \oplus k^{(l)}}^{(l)} \right)^2 \quad (2)$$

The distinguisher is defined for L n -bit S-Boxes. The components $x_q^{(l)} \in \mathbb{Z}$ of $x = (x_{(0)n}^{(1)}, \dots, x_{(1)n}^{(L)})$ represent the measured leakage signals during the calculation of the l -th S-Box with input data $q \in \mathbb{F}_2^n$. It is assumed that the actual input to the l -th S-Box is $q \oplus k^{*(l)}$, where $k^{*(l)} \in \mathbb{F}_2^n$ is a sub-key of the secret key $k^* \in (\mathbb{F}_2^n)^L$ used by the implementation under attack. The objective function $D(k, x)$ provides for each key candidate $k \in (\mathbb{F}_2^n)^L$ a value which is proportional to the a posteriori probability of k given the measured leakage signal vector x .

The key ranking problem for collision side-channel attacks is stated as follows. Given the measured leakage signal vector x calculate the number $R(x, d)$ of key candidates k s.t. $D(k, x) \geq d$. Actually, in the attack the number $R(x, D(k^*, x))$ is of interest.

To show the NP-hardness of the key ranking problem we reduce the NP-complete partition problem¹ to the key ranking problem.

Given a multiset instance $S = \{s^{(1)}, \dots, s^{(L)} \mid s^{(l)} \in \mathbb{N}\}$ of the partition problem we create in polynomial time an instance $x(S) = (x_{(0)}^{(1)} = -s^{(1)}, x_{(1)}^{(1)} = +s^{(1)}, \dots, x_{(0)}^{(L)} = -s^{(L)}, x_{(1)}^{(L)} = +s^{(L)})$ with the key set $(\mathbb{F}_2)^L$ of the key ranking problem.

Now, if $R(x(S), 1) < 2^L$ then there must be a key $k' \in (\mathbb{F}_2)^L$ for which $D(k', x(S)) = 0$.

With $\rho : \mathbb{F}_2 \rightarrow \{-1, 1\}$, $\rho(0) = -1$ and $\rho(1) = 1$ we then have

$$D(k', x(S)) = \left(\sum_{l=1}^L \rho(0 \oplus k'^{(l)}) s^{(l)} \right)^2 + \left(\sum_{l=1}^L \rho(1 \oplus k'^{(l)}) s^{(l)} \right)^2 = 0, \quad (3)$$

and because $\rho(0) = -\rho(1)$

$$D(k', x(S)) = 2 \left(\sum_{l=1}^L \rho(k'^{(l)}) s^{(l)} \right)^2 = 0. \quad (4)$$

Therefore, such k' exists if and only if the reduced partition problem S has a solution. This statement completes the reduction.

Remark: Similar reduction of the partition problem to the problem of finding the last ranked key shows that the later one is NP-hard. Contrary to this, the computational complexity of finding the first ranked key is unclear.

3 Lower Bounds for Key Ranks in Collision Side-Channel Attacks

In security evaluations lower bounds for the rank of the secret key are useful. Such lower bounds can be estimated by randomly sampling some subsets of candidate keys, i.e. by estimating the number of keys in a subsets with ranks higher than the rank of the right key. Working with subsets helps avoiding excessive number of samples needed for the estimation of lower bounds for the key rank, especially in case of small ranks of the secret key.

For the purpose of this section the distinguisher objective function $D(k, x)$ (2) is restated in equations (5) and (6).

$$D(k, x) = \sum_{i=1}^L \sum_{j=1}^L D_{i,j}(k^{(i)} \oplus k^{(j)}, x) \quad (5)$$

¹ See e.g. https://en.wikipedia.org/wiki/Partition_problem

$$D_{i,j}(d, x) = \sum_{q \in \mathbb{F}_2^n} x_q^{(i)} x_{q \oplus d}^{(j)} \quad (6)$$

Let $K(k^*, x, i, b)$ denote the set of the first b subkeys in a list of all subkeys $k^{(i)}$ without the subkey $k^{*(i)}$ sorted in descending order according to the values $D_{1,i}(k^{*(1)} \oplus k^{(i)}, x)$.

Let $K^*(k^*, x, i, b) = K(k^*, x, i, b-1) \cup \{k^{*(i)}\}$.

Let $C(L, c)$ denote the set of all combinations of c elements from the set of integers $\{2, \dots, L\}$.

Let $S(k^*, x, b, c) = \{k \in (\mathbb{F}_2^n)^L \mid k^{(i)} = k^{*(i)} \text{ if } i \notin C \text{ and } k^{(i)} \in K^*(k^*, x, i, b) \text{ if } i \in C \text{ for any } C \in C(L, c)\}$.

The size of the set $S(k^*, x, b, c)$ is $|S(k^*, x, b, c)| = \binom{L-1}{c} b^c$.

Assume that m keys k are randomly selected from a set $S(k^*, x, b, c)$ and that the number of selected k 's for which $D(k, x) > D(k^*, x)$ is r .

Then $\frac{r}{m} \binom{L-1}{c} b^c$ is an estimate of the number of k 's in the subset $S(k^*, x, b, c)$ of the key set $(\mathbb{F}_2^n)^L$ for which $D(k, x) > D(k^*, x)$ and therefore $2^n \frac{r}{m} \binom{L-1}{c} b^c$ is an estimate of a lower bound for the rank $R(x, D(k^*, x))$ (see section 2) of the right key. The factor 2^n accounts for the fixed subkey $k^{(1)} = k^{*(1)}$ for all $k \in S(k^*, x, b, c)$. In an attack the value of $k^{*(1)}$ must be obtained by brute force search and then the values of the other subkeys can be searched using the distinguisher because $D(k, x)$ depends on subkey differences $k^{(i)} \oplus k^{(j)}$ (see (5)).

Let p be a probability that $D(k, x) > D(k^*, x)$ for a randomly selected k from $S(k^*, x, b, c)$. The ratio $\tilde{p} = \frac{r}{m}$ is then an estimate for p . The number r is binomial distributed. If $p < \tilde{p}/4$ then the probability that $r \geq 3$ is less than 0.04². In simulations reported in section 4 we set the estimated lower bound to 0 in all cases of $r < 3$. It is now expected that in a fraction of $0.96 = 1 - 0.04$ of experiments $p > \tilde{p}/4$. This means for the lower bound v and its estimate $\tilde{v} \sim \tilde{p}$ that $v > \tilde{v}/4$ or $\log_2(v) > \log_2(\tilde{v}) - 2$.

4 Simulation Results

We present estimates of lower bounds for key ranks $R(x, D(k^*, x))$ (see section 2) using optimal distinguisher for collision side-channel attacks. We consider attacks on 16 key bytes, i.e. $L = 16$ and $n = 8$, similar to the AES case. We assume that the attacker has an access to a balanced set of traces. She observes each plaintext byte the same number of times, thanks to averaging she can just use 2^8 plaintexts per S-box. We utilize the balanced setup, and instead of varying the number of traces, we increase or decrease the variance σ^2 of the Gaussian noise in our simulations. The leakage function values have Gaussian distribution with variance $\sigma_\varphi^2 = 2$ corresponding to the variance of Hamming weights of random bytes. We refer to [1] for more details on this set-up. The estimates of lower bounds for key ranks $R(x, D(k^*, x))$ were calculated using results of $m = 2^{16}$ samples of sets $S(k^*, x, b, c)$ as described in section 3 for all $b \in \{2^1, 2^2, \dots, 2^n = 2^8\}$ and for all $c \in \{1, \dots, L-1 = 15\}$. The maximal value of these estimates was then taken as the final estimate of the lower bound for the right key rank. The simulations were performed 1,000 times for each given value of the noise variance σ^2 to obtain a distribution of the final estimates. Table 1 (left) lists the first 10- and 5- quantiles and the median of the distribution of the final estimates of the lower bounds for the key rank obtained for some values of noise variances. To make apparent the non-triviality of the obtained lower bounds

² In our case of small p and large m values an approximation of binomial by Poisson distribution with parameter $\lambda = 3/4$ can be used to calculate that probability.

for key ranks in collision attacks we listed in Table 1 (right) also quantiles of the distribution of upper limits for key ranks in perfectly profiled correlation power analysis (CPA) attacks³.

$\sigma^2/10$	1 st 10-quantile	1 st 5-quantile	median	$\sigma^2/21$	1 st 10-quantile	1 st 5-quantile	median
2	8	14	20	2	9	12	21
3	22	25	31	3	28	33	44
4	33	41	59	4	43	50	59
5	56	69	85	5	56	61	71
6	71	84	99	6	64	70	79
7	86	91	103	7	70	75	85

Table 1. \log_2 of quantiles of final lower bounds for key ranks in collision attacks (left), and of upper limits for key ranks in perfectly profiled CPA attacks (right).

5 Summary

In this note we showed that the key ranking problem for optimal collision side-channel attacks is NP-hard. In security evaluations lower bounds for the rank of the secret key are useful. In this note we estimated such lower bounds for collision side-channel attacks by randomly sampling some subsets of candidate keys, i.e. we estimated the number of keys in a subsets with ranks higher than the rank of the secret key. Working with subsets helps avoiding excessive number of samples needed for the estimation of lower bounds for the key rank, especially in case of small ranks of the secret key. Given the obtained lower bounds we conclude that key enumeration algorithms for collision side-channel attacks would at best allow to reduce the number of traces⁴ for successful attacks at high noise levels by a factor of ~ 2 at a cost of enumerating $\sim 2^{40}$ keys⁵.

References

1. Cezary Glowacz and Vincent Grosso. Optimal collision side-channel attacks. Cryptology ePrint Archive, Paper 2019/828, 2019. <https://eprint.iacr.org/2019/828>.
2. Romain Poussier, François-Xavier Standaert, and Vincent Grosso. Simple key enumeration (and rank estimation) using histograms: an integrated approach. Cryptology ePrint Archive, Paper 2016/571, 2016. <https://eprint.iacr.org/2016/571>.
3. Andreas Wiemers and Dominik Klein. Entropy reduction for the correlation-enhanced power analysis collision attack. Cryptology ePrint Archive, Paper 2017/1079, 2017. <https://eprint.iacr.org/2017/1079>.

³ The upper limits for key ranks in perfectly profiled CPA attacks were calculated using the public toolbox [2] in a simulation set-up similar to that used in case of collision side channel attacks.

⁴ The effective variance of Gaussian noise scales inversly proportional with the number of traces due to averaging the measured leakage signals over traces.

⁵ In that context one can also look at upper bounds of 0.92 and 0.71 for the success rate of the entropy reduction Algorithm 1, [3], Variant I with $W = 2^{40}$ (corresponding to a workload $\sim 2^{51}$) at noise with variances $\sigma^2 = 30$ resp. 40 in our simulation setup (see section 4). For $W = 2^{40}$ the algorithm is not successful if the number of key prefixes $(k^{(1)}, \dots, k^{(7)}) \in \{k^{*(1)}\} \times (\mathbb{F}_2^8)^6$ s.t. $\sum_{i=1}^7 \sum_{j=1}^7 D_{i,j}(k^{(i)} \oplus k^{(j)}, x) > \sum_{i=1}^7 \sum_{j=1}^7 D_{i,j}(k^{*(i)} \oplus k^{*(j)}, x)$ is greater than 2^{40} . The detection of such an event, and then the probability of these events, i.e. the upper bound for the success rate, were obtained by random sampling (256,000 samples for each event detection and 1,000 times for probability estimation).