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 estimates of 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 estimates of 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).

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

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

The distinguisher is defined for L n-bit S-Boxes. The components $x_q^{(l)} \in \mathbb{Z}$ of $x = (x^{(1)}_{(0)^n}, \dots, x^{L}_{(1)^n})$ 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 $q \oplus k^{\star(l)}$, where $k^{\star(l)} \in \mathbb{F}_2^n$ is a subkey of the secret key $k^\star \in (\mathbb{F}_2^n)^L$ 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 $R(x, D(k^\star, x))$ is of interest.

To show the NP-hardness of the key ranking problem we reduce the NP-complete partition problem[1] 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 $x(S) = (x^{(1)}_{(0)} = -s^{(1)}, x^{(1)}_{(1)} = +s^{(1)}, \dots, x^{(L)}_{(0)} = -s^{(L)}, x^{(L)}_{(1)} = +s^{(L)})$ 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 $\rho : \mathbb{F}_2 \to \{-1, 1\}$, $\rho(0) = -1$ and $\rho(1) = 1$ we then have

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

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

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

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. In contrast to this, the computational complexity of finding the first ranked key is unclear.

3 Estimates of 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 subset 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).

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

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

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

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

Let $C(L, c, j)$ denote the set of all combinations of c elements from the set of integers $\{1, ..., L\} \setminus \{j\}$.

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

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

Assume that m keys k are selected uniformly at random[2] from a set $S(k^\star, x, j, b, c)$ and that the number of selected k's for which $D(k, x) > D(k^\star, x)$ is r.

Then $\frac{r}{m}\binom{L-1}{c} b^c$ is a an estimate of the number of k's in the subset $S(k^\star, x, j, b, c)$ of the key set $(\mathbb{F}_2^n)^L$ for which $D(k, x) > D(k^\star, x)$ and therefore $2^n \frac{r}{m}\binom{L-1}{c} b^c$ is an estimate of a lower bound for the rank $R(x, D(k^\star, x))$ (see section 2) of the right key. The factor 2^n accounts for the fixed subkey $k^{(j)} = k^{\star(j)}$ for all $k \in S(k^\star, x, j, b, c)$. In an attack the value of $k^{\star(j)}$ 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 $D(k, x) > D(k^\star, x)$ for a randomly selected k from $S(k^\star, x, j, b, c)$. The ratio $\tilde{p} = \frac{r}{m}$ is then an estimate for p. The number r is binomial distributed. If $p < \tilde{p}/16$ then the probability that $r \geq 6$ is less than $3 * 10^{-6}$ [3]. In simulations reported in section 4 we set the estimated lower bound to 0 in all cases of $r < 6$. It is now expected that $p > \tilde{p}/16$ in a fraction of $1 - 3 * 10^{-6}$ of estimations. This means for the lower bound v and its estimate $\tilde{v} \sim \tilde{p}$ that $v > \tilde{v}/16$ or $log_2(v) > log_2(\tilde{v}) - 4$. In e.g. $120,000$ estimations it is expected that $log_2(v) > log_2(\tilde{v}) - 4$ holds in each case.

4 Simulation Results

We present estimates of lower bounds for key ranks $R(x, D(k^\star, x))$ (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. See [1] for more details about this set-up. The estimates of lower bounds for key ranks $R(x, D(k^\star, x))$ were calculated using results of $m = 2^{18}$ samples of sets $S(k^\star, x, j, b, c)$ as described in section 3 for $j = 1$, for all $b \in \{2^1 - 1, 2^2 - 1, \ldots, 2^n - 1 = 2^8 - 1\}$ and for all $c \in \{1, \ldots, L - 1 = 15\}$. 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 (overall $120,000 = 8 * 15 * 1,000$ estimations) for each given value of the noise variance σ^2 to obtain an empirical distribution of the final estimates. The actual lower bounds are expected to be not less than 4-bits below the final estimates (see section 3). Table 1 (left) lists the first 10- and 5- empirical quantiles and the empirical median of final estimates of lower bounds for the key rank obtained for some values of noise variances. As a benchmark for final estimates of the lower bounds Table 1 (right) lists the empirical quantiles of upper limits for key ranks in perfectly profiled correlation

[2] First an element $C \in C(L, c, j)$ and then for each $i \in C$ the subkeys $k^{(i)} \in K(k^\star, x, i, j, b)$ are selected uniformly at random.

[3] In our case of small p and large m values an approximation of binomial by Poisson distribution with parameter $\lambda = 6/16$ was used to calculate this probability.

power analysis (CPA) attacks[4]. The obtained empirical quantiles of estimates of lower bounds for key ranks in collision side-channel attacks grow faster with increasing noise variance than it is the case for the empirical quantiles of upper limits of key ranks in perfectly profiled CPA attacks. This fits the expected higher grow rate of quantiles of key ranks in collision side-channel attacks; in contrast to the set-up in perfectly profiled CPA attacks, in collision side-channel attacks no parameters of probability distribution of leakage function values are available.

$\sigma^2/25$ [5]	1st10-quantile	1st5-quantile	median
1.0	13	16	**20**
1.5	29	36	53
2.0	55	68	84
2.5	72	84	100
3.0	86	98	104

$\sigma^2/42$	1st10-quantile	1st5-quantile	median
1.0	9	12	**21**
1.5	28	33	44
2.0	43	50	59
2.5	56	61	71
3.0	64	70	79

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

5 Conclusions

We showed that the key ranking problem for optimal collision side-channel attacks is NP-hard and we provided estimates of lower bounds for key ranks in collision side-channel attacks. The method for the estimation of lower bounds can be used in security evaluations. The benefit of any practical key enumeration algorithm would be limited to reduce the number of traces by at best a factor of ~ 2 [6].

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.

[4] The upper limits for key ranks in perfectly profiled CPA attacks were calculated in the same simulation set-up using the toolbox [2].

[5] The optimal algorithm for collision side-channel attacks has success rates of 0.90 and 0.10 for noise variances $\sigma^2 \sim 11$ and ~ 19 in a similar simulation set-up (see [1]).

[6] I.e. a key enumeration algorithm would be useful in a range of noise variances σ^2 from ~ 25 to ~ 50. For $\sigma^2 \lessapprox 25$ the entropy reduction Algorithm 1, Variant I, [3] can be used; e.g. with $W = 2^{16}$ it has in the same simulation set-up a success rate of ~ 0.19 for the noise variance $\sigma^2 = 20$ and ~ 0.01 for $\sigma^2 = 30$. Note that the noise variance is inverse proportional to the number of traces in our set-up for collision side-channel attacks.