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.

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

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.

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).

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

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

The distinguisher is defined for L n-bit S-Boxes. The components $x_q^{(l)} \in \mathbb{Z}$ of $x = (x_{(0)^n}^{(1)}, \ldots, x_{(1)^n}^{L})$ 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 $q \oplus k^{\star(l)}$, 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 (see e.g. [3]) to the key ranking problem. Given a multiset instance $S = \{s^{(1)}, \ldots, s^{(L)} \mid s^{(l)} \in \mathbb{N}\}$ of the partition problem we create in polynomial time an instance $x(S) = (x_{(0)}^{(1)} = -s^{(1)}, x_{(1)}^{(1)} = +s^{(1)}, \ldots, x_{(0)}^{(L)} = -s^{(L)}, x_{(1)}^{(L)} = +s^{(L)})$ 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 $\sigma : \mathbb{F}_2 \to \{-1, 1\}$, $\sigma(0) = -1$ and $\sigma(1) = 1$ we then have

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

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

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

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

3 Conclusion and Outlook

In this note we showed that the key ranking problem for optimal collision side-channel attacks is NP-hard. In security evaluations also lower bounds for the rank of the secret key might be useful. One could try to estimate such lower bounds by randomly sampling some subset of candidate keys, i.e. to estimate the number of keys in a subset with ranks higher than the rank of the secret key. Working with a subset might help avoiding excessive number of samples needed for the estimation of a lower bound for the key rank, especially in case of small ranks of the secret key. Lower bounds could also be used to jointly study their tightness and the optimality of the entropy reduction approach given in [2] for collision side-channel attacks.

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. 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. Partition problem, https://en.wikipedia.org/wiki/partition_problem.