More Efficient Key Ranking for Optimal Collision Side-Channel Attacks

Cezary Glowacz

DT Security
cezary.glowacz@t-systems.com

Abstract. In [2] we studied collision side-channel attacks, and derived an optimal distinguisher for key ranking. In this note we propose a heuristic estimation procedure for key ranking based on this distinguisher, and provide estimates of lower bounds for secret key ranks in collision side-channel attacks. The procedure employs nonuniform sampling introduced in [1], and it is more efficient than the subset uniform sampling procedure [3].

Keywords: Collision Side-Channel Attacks, Key Ranking, Nonuniform Sampling

1 Introduction

Side-channel attacks exploit measurable leakage signals produced by the underlying hardware platform during execution of cryptographic functions. Given an adequate stochastic model of the signals optimal strategies for an attack on the secret key can be derived. In [2] we studied collision side-channel attacks based on an optimal distinguisher. The distinguisher is a function of a key and of the measured values of leakage signals which allows to decide for any two keys the order of their a-posteriori probabilities conditioned on the measured values, and it can be used to enumerate the keys in a descending order. The attacker can minimize his expected effort by trying each key starting with the first one in the enumeration until the secret key has been found. In security evaluations a lower bound for the position of the secret key, i.e. its rank, in the enumeration allows to rate the attacker's best case effort needed to find the secret key. In this note we propose a heuristic estimation procedure for key ranking based on the optimal distinguisher, and we provide estimates of lower bounds for secret key ranks in collision side channel attacks. The procedure employs nonuniform sampling introduced in [1], and it is more efficient than the subset uniform sampling procedure [3].

2 Background

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

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

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

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

The component $x^{(q)(l)}$ of $x \in (\mathbb{R}^{2^n})^L$ represents the measured value of the leakage signal during the calculation of the l-th of L n-bit S-Boxes with the 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 the l-th sub-key of the secret key $k^* \in (\mathbb{F}_2^n)^L$. The objective function $D(k,x)$ provides for each candidate key $k \in (\mathbb{F}_2^n)^L$ a value

which is strictly increasing with the a-posteriori probability of k conditioned on the measured values x. The rank of the secret key k^* is $r^* = |\{k \in (\mathbb{F}_2^n)^L | D(k,x) \geq D(k^*,x)\}|$.

3 Estimation of Lower Bounds for Secret Key Ranks

The nonuniform sampling for key ranking was presented in [1], and it was then used for the estimation of the expectation value of a secret key rank based on scores linked to the a-posteriori probabilities of the sub-keys. Such scores are not available in optimal collision side-channel attacks. However, given the secret key k^* and the measured values x an estimate $\tilde{r}$ of a lower bound r for the secret key rank r^* can be obtained by nonuniformly sampling the keys $k \in (\mathbb{F}_2^n)^L$ according to some heuristic probability distribution and counting the sampled keys k for which $D(k,x) \geq D(k^*,x)$ and which have the probability $p(k)$ of having been sampled less than some value $\hat{p}$.

Let $N_i = \{1,\ldots,i\} \subset \mathbb{N}$, and let $f \in \mathbb{R}^+$, $m \in \mathbb{Z}^+$, $s \in N_m$ and $\hat{u} \in \mathbb{Z}^+$ denote the estimation parameters.

For $i \in N_{L-1}$ and $d \in \mathbb{F}_2^n$ let $v_i(d) = \exp(\sum_{j=1}^{L} D_{i,j}(d \oplus k^{*(j)}, x)/L/f)$ (Variant I) and $v_i(d) = \exp(D_{i,L}(d \oplus k^{*(L)}, x)/f)$ (Variant II). Let $p_i(d) = v_i(d)/\sum_{q \in \mathbb{F}_2^n} v_i(q)$. The keys $k = (k^{(1)},\ldots,k^{(L-1)},(0)^n)$ are nonuniformly sampled m times by selecting each time $L-1$ values d_i for the sub-keys $k^{(i)}$ randomly according to the probability distribution $p_i(d)$. A key $k = (k^{(1)},\ldots,k^{(L-1)},(0)^n)$ is sampled with the probability $p(k) = \prod_{i=1}^{L-1} p_i(k^{(i)})$. Let $\hat{k} = (\hat{k}^{(1)},\ldots,\hat{k}^{(L-1)},(0)^n)$ be a sample s.t. $\hat{p} = p(\hat{k})$ has the s-th smallest value among the values $p(k)$ for the samples k for which $D(k,x) \geq D((k^{*(1)},\ldots,k^{*(L-1)},(0)^n),x)$. Let $r' = s/m/\hat{p}$. For any $k = (k^{(1)},\ldots,k^{(L-1)},(0)^n)$ and any $d \in \mathbb{F}_2^n$ we have $D(k,x) = D(k \oplus d^L, x)$. Hence, let $\tilde{r} = 2^n r'$ be an estimate of the lower bound of the secret key rank r^*.

Let $B(m,\bar{p};i)$ denote the binomial distribution. If s events are observed within m samples then the confidence coefficient of the lower bound $\frac{s}{\hat{u}m}$ for $\bar{p} = \frac{s}{m}$ is $\gamma(m,\frac{s}{\hat{u}m};s) = \sum_{i=0}^{s-1} B(m,\frac{s}{\hat{u}m};i)$ (see 2.3, [4]). In our case an event is defined as having sampled a key $k = (k^{(1)},\ldots,k^{(L-1)},(0)^n)$ for which $p(k) \leq \hat{p}$ and $D(k,x) \geq D((k^{*(1)},\ldots,k^{*(L-1)},(0)^n),x)$. As $p(k) \leq \hat{p}$ there must be at least $\bar{p}/\hat{p} = r'$ such keys. Then the confidence coefficient of the lower bound $\tilde{r}/\hat{u}$ for r is $\gamma(m,\frac{s}{\hat{u}m};s)$.

4 Simulation Results

We simulated attacks for Gaussian leakage function values φ_q and Gaussian noise $\eta_{q,l}$. The simulation parameters were $n = 8, L = 16, k^* = ((0)^n)^L$ and the noise variance σ^2. In a simulated attack we first created for each $q \in \mathbb{F}_2^n$ and for each $l \in N_L$ realisations φ_q and $\eta_{q,l}$ of independent standard normal random variables. Then the vector x was created by setting its components $x(q)(l) = \sqrt{2}\varphi_q + \sigma\eta_{q,l}$.

In each simulated attack the estimate $\tilde{r}$ of the lower bound r for the secret key rank r^* was estimated using Variant I for $\sigma^2/18.75 \leq 2.0$ and Variant II for $\sigma^2/18.75 > 2.0$ with $m = 2^{14}$ and $s = 3$. In Variant I for each $f \in \{20,50,70,100,150,200,250,300,400,500,600\}$ and in Variant II for each $f \in \{100,200,300,400,500,600,700,800,900,1000,1100\}$ estimates of the lower bound were calculated. Then a largest estimate was selected as $\tilde{r}$. The confidence coefficient of the lower bound $\tilde{r}/\hat{u}$ for r is $\gamma(m,\frac{s}{\hat{u}m};s) = 0.999$ for $\hat{u} = 16$. Attacks were simulated $1,000$ times for each noise variance σ^2, and empirical quantiles of lower bound estimates $\tilde{r}$ were calculated. The results are shown in Table 1.

$\sigma^2/18.75$	1^{st} decile	2^{nd} decile	median
1.0	8	9	15
1.5	23	27	37
2.0	38	44	55
2.5	58	66	84
3.0	76	85	99
3.5	87	95	105

Table 1: log_2 of empirical quantiles of lower bound estimates $\tilde{r}$.

The results fit the following reference data. For $\sigma^2 = 1.0 * 18.75$ the optimal algorithm for collision side-channel attacks has a 2^8-th order success rate of 0.1 in the same simulation set-up (see Fig. 1, [2]). For $\sigma^2 = 3.5 * 18.75$ the empirical median of secret key rank estimates is 2^{109} (each of $1,000$ estimates was obtained in our simulation set-up using 2^{24} uniform random samples from the set of all 2^{128} keys). Also, the results match those reported in [3], and in our set-up the proposed nonuniform sampling procedure is ~ 1000 times faster than the subset uniform sampling procedure [3].

References

[1] Camurati, G., Dell'Amico, M., Standaert, F.-X. (2022): MCRank: Monte Carlo Key Rank Estimation for Side-Channel Security Evaluations. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(1), 277–300. https://doi.org/10.46586/tches.v2023.i1.277-300

[2] Glowacz, C., Grosso, V. (2020): Optimal Collision Side-Channel Attacks. In: Belaïd, S., Güneysu, T. (eds) Smart Card Research and Advanced Applications. CARDIS 2019. Lecture Notes in Computer Science, vol 11833. Springer, Cham. https://doi.org/10.1007/978-3-030-42068-0_8

[3] Glowacz, C. (2022): A Note on Key Ranking for Optimal Collision Side-Channel Attacks. Cryptology ePrint Archive, Paper 2022/674. https://eprint.iacr.org/2022/674

[4] Scholz, F. (2019): Confidence bounds & intervals for parameters relating to the binomial, negative binomial, poisson and hypergeometric distributions with applications to rare events. https://faculty.washington.edu/fscholz/DATAFILES498B20 08/Confidence-Bounds.pdf