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 $r^* = |\{k \in (\mathbb{F}_2^n)^L \mid D(k,x) \geq D(k^*,x)\}|$.

3 Estimation of Lower Bounds for Secret Key Ranks

The nonuniform sampling for key ranking was presented in [1], and then it was 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 $p(k)$ and counting the sampled keys k for which $D(k,x) \geq D(k^*,x)$ and $p(k) \leq \hat{p}$ for some $\hat{p}$.

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

For $i \in N_{L-1}$ and $d \in \mathbb{F}_2^n$ let $v_i(d) = \exp(\sum_{j=1}^{L} D_{i,j}(d \oplus k^{*(j)}, x)/L/\hat{f})$ (Variant I) or $v_i(d) = \exp(D_{i,L}(d \oplus k^{*(L)}, x)/\hat{f})$ (Variant II), and $p_i(d) = v_i(d)/\sum_{q \in \mathbb{F}_2^n} v_i(q)$. For $k \in (\mathbb{F}_2^n)^{L-1} \times \{(0)^n\}$ let $p(k) = \prod_{i=1}^{L-1} p_i(k^{(i)})$. Let $S = \{k \in (\mathbb{F}_2^n)^{L-1} \times \{(0)^n\} \mid (D(k,x) \geq D(k^*,x)) \wedge (p(k) \leq \hat{p})\}$ and $p = \sum_{k \in S} p(k)$. Then $r = 2^n \frac{p}{\hat{p}} \leq 2^n |S|$ is a lower bound for the secret key rank r^*. The reason for the factor 2^n is: for each $k \in S$ there are $2^n - 1$ values $d \in \mathbb{F}_2^n \setminus \{(0)^n\}$ for which $k \oplus d \notin S$ and $D(k,x) = D(k \oplus d^L, x)$.

The keys $k \in (\mathbb{F}_2^n)^{L-1} \times \{(0)^n\}$ are sampled m times by randomly selecting values for the sub-keys $k^{(i)}$ of k according to the probability distributions $p_i(d)$. Let $\tilde{t}$ denote the number of sampled keys k for which $k \in S$, $B(m,p;i)$ denote the binomial distribution and $\gamma(m,p;l) = \sum_{i=0}^{l-1} B(m,p;i)$. The confidence coefficient $\gamma(m, \frac{\tilde{t}}{\hat{u}m}; \tilde{t})$ (see 2.3, [4]) of the lower bound $\frac{\tilde{t}}{\hat{u}m}$ for p is at least $\gamma(m, \frac{\hat{t}}{\hat{u}m}; \hat{t})$ for $\tilde{t} \geq \hat{t} \geq 3$ and $\hat{u} \geq 2$ (see 3, [3]). Our estimate $\tilde{r}$ of the lower bound r is $\tilde{r} = 2^n \frac{\tilde{t}}{m\hat{p}}$ when $\frac{\tilde{t}}{m\hat{p}} \geq 1$ and $\tilde{t} \geq \hat{t}$, and $\tilde{r} = 2^n$ otherwise (for each $d \in \mathbb{F}_2^n$ $D(k^* \oplus d^L, x) = D(k^*, x)$, hence $r^* \geq 2^n$). Then the confidence coefficient of the lower bound $\tilde{r}/\hat{u}$ for r is at least $\gamma(m, \frac{\hat{t}}{\hat{u}m}; \hat{t})$ for $\tilde{t} \geq \hat{t} \geq 3$ and $\hat{u} \geq 2$.

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 $\sigma^2/18.75 \geq 2.5$ with $\hat{t} = 3$, $m = 2^{20}$ and selected values for $\hat{f}$ and $\hat{p}$ (for each $\hat{f} \in \{(2+\sigma^2)1.2^i \mid i \in N_{16}\}$ we sampled 2^{16} keys $k \in (\mathbb{F}_2^n)^{L-1} \times \{(0)^n\}$ according to the distribution $p(k)$ and determined a value $\tilde{p}$ of the third smallest $p(k)$ (or 1 if none was found) of the sampled keys k for which $D(k,x) \geq D(k^*,x)$, then $\hat{f}$ and $\tilde{p}$ with the smallest $\tilde{p}$ were selected). The confidence coefficient of the lower bound $\tilde{r}/\hat{u}$ for r is at least $\gamma(m, \frac{\hat{t}}{\hat{u}m}; \hat{t}) = 0.999$ 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.

The results match those reported in [3] and they were obtained from around 500 times less key samples.

$\sigma^2/18.75$	1^{st} decile	2^{nd} decile	median
1.0	8	8	12
1.5	21	27	36
2.0	38	45	58
2.5	58	70	86
3.0	75	85	98
3.5	86	92	104

$\sigma^2/18.75$	1^{st} decile	2^{nd} decile	median
1.0	8	8	14
1.5	22	28	38
2.0	41	47	59
2.5	56	67	84
3.0	74	83	99
3.5	85	94	108

Table 1: log_2 of empirical quantiles of lower bound estimates $\tilde{r}$. Left: nonuniform sampling procedure. Right: 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