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

Cezary Glowacz

DT Security
cezary.glowacz@t-systems.com

Abstract. In [1] 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.

Keywords: Collision Side-Channel Attacks · Key Ranking

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 [1] 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 try each key starting with the first one for minimizing the expected number of trials 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.

2 Background

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 leakage function values and Gaussian noise are restated in the following equations

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

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

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

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 $q \oplus k^{\star(l)}$, where $k^{\star(l)} \in \mathbb{F}_2^n$ is the l-th sub-key of the secret key $k^\star \in (\mathbb{F}_2^n)^L$. 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 $k^\star$ is $r^\star = |\{k \in (\mathbb{F}_2^n)^L \mid D(k,x) \geq D(k^\star,x)\}|$.

3 Estimation of Lower Bounds for Secret Key Ranks

Given the secret key $k^\star$ and the measured values x an estimate $\tilde{r}$ of a lower bound r for the secret key rank $r^\star$ can be obtained by sampling some key subset $S \subseteq (\mathbb{F}_2^n)^L$ and counting sampled keys k for which $D(k,x) \geq D(k^\star,x)$.

Let $N_i = \{1,\ldots,i\} \subset \mathbb{N}$, and let $b \in N_{2^n-1}$, $c \in N_{L-1}$, $m, \hat{u} \in \mathbb{N}^+$ and $\hat{t} \in N_m$ denote the estimation parameters.

Let K_l denote a set of b largest regarding $\sum_{i=1}^{L} D_{l,i}(d \oplus k^{*(i)}, x)$ (Variant I) or $D_{l,L}(d \oplus k^{*(L)}, x)$ (Variant II) elements d from $\mathbb{F}_2^n \setminus \{k^{\star(l)}\}$, $C = \{N \subseteq N_{L-1} \mid |N| = c\}$, $S = \{k \in (\mathbb{F}_2^n)^L \mid \exists_{N\in C} \forall_{l\in N_L} (l \notin N \wedge k^{(l)} = k^{\star(l)} \vee l \in N \wedge k^{(l)} \in K_l)\}$ and $t = |\{k \in S \mid D(k,x) \geq D(k^\star,x)\}|$. Then $r = max\{2^n t, 2^n\}$ is a lower bound for the secret key rank $r^\star$. 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 $k \oplus d^L \notin S$ and $D(k \oplus d^L, x) = D(k,x)$. We have $r^\star \geq 2^n$ because for each $d \in \mathbb{F}_2^n$ $D(d^L \oplus k^\star, x) = D(k^\star, x)$. Hence, the lower bound can be set to $r = 2^n$ when $t = 0$.

The keys k are sampled from the set S uniformly at random; first N is sampled from C, then for each $l \in N$ the sub-key $k^{(l)}$ is sampled from K_l, and for each $l \in N_L \setminus N$ the sub-key $k^{(l)}$ is set to $k^{\star(l)}$. Let $\tilde{t}$ denote the number of keys k found in m samples for which $D(k,x) \geq D(k^\star,x)$, $B(m,p;i)$ denote the binomial distribution and $\gamma(m,p;l) = \sum_{i=0}^{l-1} B(m,p;i)$. The confidence coefficient $\gamma(m, \frac{\tilde{t}}{\hat{u}m}; \tilde{t})$ of the lower bound $\frac{\tilde{t}}{\hat{u}m}$ for $p = \frac{t}{|S|}$ (see 2.3, [2]) is at least $\gamma(m, \frac{\hat{t}}{\hat{u}m}; \hat{t})$ when $\tilde{t} \geq \hat{t} \geq 3$ and $\hat{u} \geq 2$.[1] Our estimate $\tilde{r}$ of the lower bound r is $\tilde{r} = 2^n \frac{\tilde{t}}{m}|S|$ when $\tilde{t} \geq \hat{t}$ and $\tilde{r} = 2^n$ otherwise. 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 $\hat{t} \geq 3$ and $\hat{u} \geq 2$.

[1] $\frac{d}{dp}\gamma(m,p;l) = -l\binom{m}{l}p^{l-1}(1-p)^{n-l} < 0$ (see 2, [2]) and $\frac{d^2}{dp^2}\gamma(m,p;l) = l\binom{m}{l}p^{l-2}(1-p)^{m-l-1}((m-1)p-(l-1)) < 0$ for $p < \frac{l-1}{m-1}$ hence $\gamma(m,p+\Delta_p;l+1) > \gamma(m,p;l) + \Delta_p \frac{\partial}{\partial p}\gamma(m,p+\Delta_p;l) + \binom{m}{l}(p+\Delta_p)^l(1-(p+\Delta_p))^{m-l}$ $= \gamma(m,p;l) - \Delta_p l\binom{m}{l}(p+\Delta_p)^{l-1}(1-(p+\Delta_p))^{m-l} + \binom{m}{l}(p+\Delta_p)^l(1-(p+\Delta_p))^{m-l}$ $= \gamma(m,p;l) + \binom{m}{l}(p+\Delta_p)^{l-1}(1-(p+\Delta_p))^{m-l}(p+\Delta_p(1-l))$ for $p+\Delta_p < \frac{l-1}{m-1}$. For $\tilde{t} > \hat{t} \geq 3$ and $\hat{u} \geq 2$ we then have $\gamma(m, \frac{\tilde{t}+1}{\hat{u}m}; \tilde{t}+1) > \gamma(m, \frac{\tilde{t}}{\hat{u}m}; \tilde{t}) > \cdots > \gamma(m, \frac{\hat{t}}{\hat{u}m}; \hat{t})$.

4 Simulation Results

We simulated attacks for Gaussian leakage function values φ_q and Gaussian noise $\eta_{q,l}$. The simulation parameters were $n = 8$, $L = 16$, $k^\star = ((0)^n)^L$ 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 $r^\star$ was estimated using Variant I for $\sigma^2/18.75 \leq 2.0$ and Variant II for $\sigma^2/18.75 > 2.0$ with $m = 2^{24}, \hat{t} = 32$ and selected values for b and c (for each $b \in N_{2^n-1}$ and each $c \in N_{L-1}$ estimates of the lower bound were calculated with $m = 2^{18}$ and $\hat{t} = 3$, then b and c with largest value of the estimate were selected). The confidence coefficient of the lower bound $\tilde{r}/\hat{u}$ for r is at least $\gamma(2^{24}, \frac{32}{\hat{u}*2^{24}}; 32) = 0.9997$ for $\hat{u} = 2$ and 0.9999999998 for $\hat{u} = 4$. 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	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 $\tilde{r}$.

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, [1]). 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).

References

1. Glowacz, C., Grosso, V.: Optimal collision side-channel attacks. Cryptology ePrint Archive, Paper 2019/828 (2019), https://eprint.iacr.org/2019/828
2. Scholz, F.: Confidence bounds & intervals for parameters relating to the binomial, negative binomial, poisson and hypergeometric distributions with applications to rare events (2019), https://faculty.washington.edu/fscholz/DATAFILES498B2008/ConfidenceBounds.pdf