SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Theoretical Analysis of Persistent Fault Attack

Fan ZHANG[1,2,3,4], Guorui XU[1,3,4*], Bolin YANG[1], Ziyuan LIANG[1,3,4] & Kui REN[3,4]

[1]*College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou* 310027*, P.R.China;*
[2]*State Key Laboratory of Cryptology, P.O.Box 5159, Beijing* 100878*, P.R.China;*
[3]*Institute of Cyberspace Research, Zhejiang University, Hangzhou* 310027*, P.R.China;*
[4]*Alibaba-Zhejiang University Joint Institute of Frontier Technologies, Hangzhou* 310027*, P.R.China*

Appendix A In the early work

Let n, η denote the number of all values and possible values, respectively. $n = 256$ and $\eta = n - 1 = 255$ for 8-bit bytes. Suppose the adversary can collect i ciphertexts after the encryption. Parts of them are faulty. Let θ_i be the "average" number of different values that he has observed for one specific ciphertext byte. Then, we can derive the following according to [1]:

$$\begin{aligned}
\theta_1 &= 1\,, \\
\theta_2 &= \frac{\eta - \theta_1}{\eta} + \theta_1\,, \\
\theta_3 &= \frac{\eta - \theta_2}{\eta} + \theta_2\,, \\
&\cdots \\
\theta_i &= \frac{1 - q^i}{1 - q}, \text{where } q = \frac{\eta - 1}{\eta}\,.
\end{aligned} \tag{A1}$$

Since $\eta = \frac{1}{1-q}$, when $\theta_i \to \eta = \frac{1}{1-q}$, from Eq. (A1) we have:

$$\theta_i = \frac{1 - q^i}{1 - q} \to \eta = \frac{1}{1 - q}\,.$$

It only states that θ_i will converge to $\eta = 255$ eventually($i \to +\infty$), but did not give a theoretical expectation value of i when θ_i equals η for the first time.

Appendix B In Case 1

Suppose t_j denotes the number of additional ciphertexts that is required to output a new value after $j-1$ different values observed. T denotes the total number of the ciphertexts that is required when all possible values observed. $T = \sum_{j=1}^{n-1} t_j$ and $t_1 = 1$.

Since the distribution of possible values is uniform, when the $(j-1)$-th value has been observed, the next new value comes with a fixed probability determined by j: $p_j = \frac{n-j}{n-1}$. Also, random variables t_j are independent.

Then we can easily derive this:

$$\begin{aligned}
E(T) &= \sum_{j=1}^{n-1} E(t_j) \\
&= \sum_{j=1}^{n-1} \frac{1}{p_j}
\end{aligned}$$

* Corresponding author (email: xugr@zju.edu.cn)

$$
\begin{aligned}
&= \sum_{j=1}^{n-1} \frac{n-1}{n-j} \\
&= (n-1) \times H_{n-1}\,,
\end{aligned} \tag{B1}
$$

where

$$H_n = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}\,.$$

Appendix C In Case 2

Let T, X_i be the total number of ciphertexts in one attack process and the number of ciphertexts when the adversary first find the s_i value, respectively. $T = \max_{i=0,1,2,\cdots,n-1} X_i$. So the expected number of ciphertexts $E(T)$ satisfies:

$$E(T) = E(\max_{i=0,1,2,\cdots,n-1} X_i)\,. \tag{C1}$$

For value s_j, the probability is p_j, $0 < j < n-1$, and $p_0 = 0$, $p_1 = \frac{2}{n}$, for other i, $p_i = \frac{1}{n}$. We can convert the maximum expression (Eq. (C1)) into a sum of a series of minimum expressions:

$$
\begin{aligned}
&E(T) = E(\max_{i=0,1,2,\cdots,n-1} X_i) \\
&= \sum_i E(X_i) - \sum_{i<j} E\left(\min(X_i, X_j)\right) + (-1)^{n+1} E\left(\min(X_1, X_2, \cdots, X_n)\right) \\
&= \sum_i \frac{1}{p_i} - \sum_{i<j} \frac{1}{p_i + p_j} + \cdots + (-1)^{n+1} \frac{1}{p_1 + \cdots + p_n} \\
&= \sum_{k=1}^{n-2} (-1)^{k+1} \left(\binom{n-2}{k} \frac{n}{k} + \binom{n-2}{k-1} \frac{n}{k+1} \right) + (-1)^n\,.
\end{aligned}
$$

This formula is not feasible to compute for computers because of the large permutation number $\binom{n-2}{k}$ and $\binom{n-2}{k-1}$. To make it easier to compute, we can make some transformation.

To construct an expression like Eq. (C2), using the idea of generating function:

$$
\begin{aligned}
(1-x)^{n-2} &= \sum_{k=0}^{n-2} \binom{n-2}{k} (-x)^k \\
(1-x)^{n-2} &= \sum_{k=0}^{n-2} \binom{n-2}{k} (-1)^k (x)^k \\
(1-x)^{n-2} &= \sum_{k=1}^{n-2} \binom{n-2}{k} (-1)^k (x)^k + 1 \\
\tfrac{(1-x)^{n-2}-1}{x} &= \sum_{k=1}^{n-2} \binom{n-2}{k} (-1)^k x^{k-1} \\
\int_0^1 \tfrac{(1-x)^{n-2}-1}{x} \mathrm{d}x &= \sum_{k=1}^{n-2} \binom{n-2}{k} (-1)^k \frac{x^k}{k} \Big|_{x=0}^{1} \\
&= \sum_{k=1}^{n-2} \binom{n-2}{k} (-1)^k \frac{1}{k}\,.
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
(1-x)^{n-2} &= \sum_{k=0}^{n-2} \binom{n-2}{k} (-1)^k x^k \\
(1-x)^{n-2} &= \sum_{k=1}^{n-1} \binom{n-2}{k-1} (-1)^{k-1} x^{k-1} \\
(1-x)^{n-2} &= \sum_{k=1}^{n-1} \binom{n-2}{k-1} (-1)^{k+1} x^{k-1} \\
x\left((1-x)^{n-2} - (-1)^n x^{n-2}\right) &= \sum_{k=1}^{n-2} \binom{n-2}{k-1} (-1)^{k+1} x^k \\
\int_0^1 \left(x((1-x)^{n-2} - (-1)^n x^{n-2})\right) \mathrm{d}x &= \sum_{k=1}^{n-2} \binom{n-2}{k-1} (-1)^{k+1} \frac{1}{k+1}\,.
\end{aligned} \tag{C2}
$$

Thus, the orgin form can be converted to:

$$E(T) = -n\int_0^1 \frac{(1-x)^{n-2}-1}{x}\mathrm{d}x + n\int_0^1 (x(1-x)^{n-1} - (-1)^n x^{n-1})\mathrm{d}x + (-1)^n\,. \tag{C3}$$

Eq. (C3) avoids the computation of large permutation numbers.

References

1 Zhang F, Lou X, Zhao X, Bhasin S, He W, Ding R, Qureshi S & Ren K. Persistent Fault Analysis on Block Ciphers. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 150-172.

2 Ferrante M & Saltalamacchia M. The coupon collector's problem. Materials matemàtics, 2014, 0001-35.

3 Flajolet P, Gardy D & Thimonier L. Birthday paradox, coupon collectors, caching algorithms and self-organizing search. Discrete Applied Mathematics, 1992, 39(3), 207-229.