Journal of Network and Computer Applications 38 (2014) 99–105

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

An improved side channel attack using event information of subtraction

Jong-Yeon Park[a], Dong-Guk Han[b,*], Okyeon Yi[b], JeongNyeo Kim[a]

[a] Electronics and Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea
[b] Department of Mathematics Kookmin University, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 26 October 2012
Received in revised form
4 March 2013
Accepted 8 May 2013
Available online 24 May 2013

Keywords:
RSA-CRT
Side channel attack
Equidistant message power analysis
CPA (correlation power analysis)

ABSTRACT

RSA-CRT is a widely used algorithm that provides high performance implementation of the RSA-signature algorithm. Many previous studies on each operation step have been published to verify the physical leakages of RSA-CRT when used in smart devices. This paper proposes SAED (subtraction algorithm analysis on equidistant data), which extracts sensitive information using the event information of the subtraction operation in a reduction algorithm. SAED is an attack method that uses algorithm-dependent power signal changes. An adversary can extract a key using differential power analysis (DPA) of the subtraction operation. This paper indicates the theoretical rationality of SAED, and shows that its results are better than those of other methods. According to our experiments, only 256 power traces are sufficient to acquire one block of data. We verify that this method is more efficient than those proposed in previously published studies.

1. Introduction

The function of authentication between devices and users is essential in secure environment. Therefore, the system leakages in authentication process mean that the security of the target system is fully broken. Especially on homeland security, access control module must block out unconfirmed men.

Digital signature is widely used for authentication module. Generally, almost all developers with implementation level, it is regarded that cryptographic algorithm used in digital signature is just secure. Although a cryptographic algorithm might be secure, we cannot guarantee that the security of the device utilizing the cryptographic algorithm because of the physical leakages. One of physical leakages is side channel attack (SCA) (Kocher, 1996). Side channel attack is a new topic of modern cryptography with physical provable security (Pietrzak). Since Kocher et al. proposed SCA, many studies have made progress in this research area. These studies can be divided into two categories.

The first category comprises studies of countermeasures against attack techniques (Allar and Giraud, 2001; Itoh et al., 2002; Mangard et al., 2007; Moradi and Mischke, 2012). When attack techniques have been published, suitable countermeasures against them have been proposed. The results of this kind of study are used as criteria for examining the safety of the cryptographic devices used by public institutions. These studies include arguments about the guarantee of theoretical safety. Not only countermeasures against attacks that are implemented in software exist, but also those that block any attempt to attack in the hardware layers (Mangard et al., 2007). For example, simple hardware solutions that use noise insertion exist.

The second category comprises studies on improved attack techniques. In general, these studies address the creation of new distinguishers. The main difference of this kind of study from those that involve only theoretical cryptographic analysis is that it considers the mathematical complexity. The adversary must have the criteria for distinguishing between a correct and an incorrect key. These distinguishers originate in a power consumption model.

Many attack techniques depend on distinguishers and many practical and theoretical techniques have been proposed, namely: DPA (differential power analysis) (Kocher et al., 1999); CPA (correlation power analysis) (Brier et al., 2004); template attack (Chari et al., 2003); improved DPA (Agrawal et al., 2003); and recently, MIA (mutual information analysis) (Oswald and Rohatgi, 2008), algebraic power analysis (Oren et al., 2012).

Another category of studies of enhanced-attack techniques addresses the development of new analysis methods, for example, a multi-round power analysis to break countermeasures applied by the block cipher algorithm (Zhou and Yung, 2010), or creates specialized techniques to attack the many implementation methods of public key cryptographic algorithms, for example, RSA (Rivest et al., 1978) and ECC (Koblitz). This category includes Boer et al.'s (2002) RSA-CRT algorithm attack on the reduction

* Corresponding author. Tel.: +82 10 9085 9743/+82 10 9790 2964/+82 42 860 6484.
E-mail addresses: flysohigh@etri.re.kr (J.-Y. Park), christa@kookmin.ac.kr (D.-G. Han), oyyi@kookmin.ac.kr (O. Yi), jnkim@etri.re.kr (J. Kim).

1084-8045/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2013.05.001

step, MRED, Novak's (2002) attack on the recombination step, and Amiel et al.'s (2007) study. In particular, there are many advanced studies on MRED, such as (Park et al., 2011), that address analysis methods and the interpretation of ghost key patterns.

This paper proposes an extension of the enhanced-side channel attack method against a public key algorithm. We use the fact that an unusual power signal occurs as a result of a characteristic event in the subtraction operation of a reduction algorithm. This method is called SAED (subtraction algorithm analysis on equidistant data), its idea is similar to MRED but the basis of principle is fully different. It does not use a Hamming weight-based power signal, but utilizes the fact that an arithmetic process event generates power information by using probabilistic analysis. To prove the efficacy of this attack, we adopt a new power signal model assumption, called the event-based power model. According to our results, SAED dramatically reduces the number of traces that is required to acquire the sensitive information about RSA-CRT.

2. Overview: MRED

Boer et al. (2002) introduced a brilliant power analysis of RSA-CRT. The target of this method is the initial reduction step $xp=x\text{mod}p$ of RSA-CRT. It uses

$$x–i \bmod p=r–i \tag{1}$$

With this property, an adversary can guess the value of r directly, although p is secret in the algorithm. The adversary inputs equidistant messages $\{x, x−1, x−2, \ldots\}$ in a row to acquire the power signal of Eq. (1)'s pattern. Finally, he can collect traces of outputs such as $\{r, r−1, r−2, \ldots\}$. In the analysis of the least significant byte (LSB), the LSB of r guessed by the adversary is expressed as $\{v_{ij}\}=\{(j–i) \bmod 256 | i=0,\ldots,N−1, j=0,\ldots,K−1\}$.

Table 1 shows the details of the method for computing v_{ij} to guess the LSB of r. If r is guessed correctly, the Hamming weight of v_{ij} should match the power signal at the time when r is computed. Thus, the adversary is able to acquire r using CPA. Table 2 shows the details of the method for computing h_{ij}, which is the Hamming weight of v_{ij}.

From the second byte, the same intermediate data h_{ij} as for CPA are used. The method differs from a general CPA mainly in its attack on the block ciphers. However, if one varies the distance of the input messages, it is possible to obtain a suitable power signal on each target byte. Eq. (2) is the general form derived from Eq. (1); the same CPA technique can be applied to upper bytes. Because the collected power traces have to be varied by $(2^8)^k$, the only difference in each byte attack is the common difference of this arithmetical progression when traces are collected. The other factors of the attack steps are the same as in CPA.

Table 1
Computation of $v_{i,j}$.

$v_{i,j}$	x_0	x_1	x_2	x_3	…	x_i
$v_{i,0}$	0	255	254	253	…	$−i$ mod 256
$v_{i,1}$	1	0	255	254	…	$(1−i)$ mod 256
$v_{i,2}$	2	1	0	255	…	$(2–i)$mod 256
…	…	…	…	…	…	…
$v_{i,255}$	255	254	253	252	…	$(255–i)$mod 256

Table 2
$v_{i,j}$-based 8 bit Hamming weight: $h_{i,j}$.

$h_{i,j}$	x_0	x_1	x_2	x_3	…	x_i
$h_{i,0}$	0	8	7	7	…	$HW(v_i,0)$
$h_{i,1}$	1	0	8	7	…	$HW(v_i,1)$
$h_{i,2}$	1	1	0	8	…	$HW(v_i,2)$
…	…	…	…	…	…	…
$h_{i,255}$	8	7	7	6	…	$HW(v_i,255)$

$$x–i(256)^k \text{mod } p=r–i(256)^k \tag{2}$$

where $i(256)^d≤p$, d is the byte-index from the least significant byte. For example, if k is 0, the attack target is the LSB. Finally, the fact that r is stored on the algorithm byte by byte makes CPA possible.

On the other hand, Eq. (2) always works where only $r>i(256)^k$ is valid. Otherwise, there exists t, such that $r≤t(256)^k$, by Eq. (3), and secret p can be computed directly.

$$p=GCD(x_0–F_k–i(256)^k, pq)$$
$$(F_k \text{ is searchedrup tok} - \text{th byte}) \tag{3}$$

$$p=GCD(x–r, N) \tag{4}$$

If the attacker fully acquires r by running the CPA many times, he can compute secret p directly by Eq. (4). Thus, the RSA algorithm is finally broken.

3. Subtraction algorithm analysis on equidistant data (SAED)

3.1. Difference between SAED and MRED

Algorithm 2 describes the attack algorithm of RSA-CRT CPA using SAED. It is different from Algorithm 1 in that the Hamming weight-power model is ignored; see Step1.1. This is because SAED does not depend on the data of r. Our method assumes that the power signal is influenced considerably by the algorithm changing as a result of equidistant inputs. We explain how it is possible to acquire the secret value using a non-Hamming weight assumption.

Algorithm 1. MRED(v -th byte)

```
INPUT: $s_1,\ldots,s_t$ $t$—equidistant power signal $T_v$
  OUTPUT: $v$th byte of $r$
    Step 1 For $j$ from 0 to 255
      Step 1.1 set $h_j=\{HW(i–j)\text{mod}256|j=1,2,\ldots,t\}$
      Step 1.2 $\rho_j=\rho(T_v, h_j)$
      Step 1.3 If $j=0$ then key$=0$, $\rho_{key}=\rho_j$
      Otherwise; if $\rho_{key}<\rho_j$ then, $r_v=j$, $\rho_{key}=\rho_j$
    Step 2 Return $r_v$
```

Algorithm 2. SAED (vth byte)

```
INPUT: $s_1,\ldots,s_t$ $t$—equidistant power signal $T_v$
  OUTPUT: $v$th byte of $r$
    Step 1 For $j$ from 0 to 255
      Step 1.1 set $n_j=\{(i–j)\text{mod}256|j=1,2,\ldots,t\}$
      Step 1.2 $\rho_j=\rho(T_v, n_j)$
      Step 1.3 If $j=0$ then key$=0$, $\rho_{key}=\rho_j$
      Otherwise; if $\rho_{key}<\rho_j$ then, $r_v=j$, $\rho_{key}=\rho_j$
    Step 2 Return $r_v$
```

3.2. Event-based power model

In power analysis, a power signal related to the sensitive values that the attacker wants to know occurs in a time zone. It follows this power signal model Mangard et al., 2007; Messerges et al., 2002.

$$P_{total}=P_{op}+P_{data}+P_{el.noise}+P_{const} \tag{5}$$

(P_{op}: operation dependent power signal, P_{data}: data dependent power signal, $P_{el.noise}$: electronic noise, P_{const}: constant value).