Chosen-message Power Analysis Attack Based on the Hamming Weight Model

CHEN Ai-dong, Wang Juan, XU Sen

1 School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China.
2 Information Security Institute, Chengdu University of Information Technology, Chengdu 610225, China

a itteam@126.com, b wangjuan@cuit.edu.cn, c xs.position@gmail.com

Abstract

The chosen-message in the power analysis attack is easy to be forbidden. For circumvent this problem, a new method is proposed, which is based on the analysis of the Montgomery Modular Multiplication algorithm. In this method, a large number which has very small Hamming weight is chosen as the plaintext and the information of the secret key is directed shown in the power curve. In the experiment on the 8051 chip, the recovery rate of the secret key is up to 99% from a single power sample and the efficiency of the attack is much higher than DPA and CPA. The results of the experiments show that there are many plaintexts which can be chosen in our method and the single method based on the chosen-message forbidden can't defense this new attack.

Keywords: Chosen-message attack, Simply Power Analysis, Montgomery multiplication algorithm

1. Introduction

The side-channel attack is a cryptographic attack method, which obtains secret information from the cryptographic equipment. There are many common side-channel attacks, such as Time Attack[1], Power Analysis Attack[2,5], Electric Magnetic attack[3], Fault attack[4] and so on. These attacks are classically discoursed in the literatures [1-5].

The chosen-message attack is a traditional cryptanalysis method. When it is combined with a power attack and the special plaintext or message is entered into the controlled device, the corresponding cipher text is obtained by the encryption from the attacked cryptographic system. In this process, the secret key can be restored by finding the relationship between the secret information and the power consumption characteristics of the captured power curves.

In the literature [6], a method was proposed by Yen et al, in which N-1 is selected as a plaintext. There may be only two intermediate results of each round of the Montgomery Modular Multiplication. The attacker can deduce the secret key based on this principle. Unfortunately, the specific experimental process didn’t be provided in this literature.

This chosen-message attack proposed by Yen et al. was realized by Atsushi Miyamoto et al. in the FPGA platform of Xilinx[7]. The correlation between the three secret key combinations and three waveforms were inferred by the authors. Moreover, the attack process and results were also provided by them. However, the defense to the attacks in the literature [6, 7] can use the simple forbidden chosen-message N-1 method. This method in the literature [7] is not universal.

2. Modular Exponentiation Operation

The modular exponentiation is the most important core operation in the RSA and various public-key algorithms. The form of modular exponentiation in RSA cryptosystem is as follows:

Encrypt: \( c = m^e \mod n \)
Decrpyt: \( m = c^d \mod n \)
Sign: \( s = m^d \mod n \)
Verify: \( m = s^e \mod n \)

International Journal of Digital Content Technology and its Applications (JDCTA) Volume 6, Number 10, June 2012
doi:10.4156/jdcta.vol6.issue10.4
is the ciphertext. \( m \) is the plaintext. \( e \) and \( n \) are public key. \( d \) is the secret key. \( s \) is the signature.

According to the scan direction of the exponent, the RSA algorithm can be divided into three forms. They are from left to right (LR), from right to left (RL) and mixed (RAD). Algorithm 1 was the example of LR binary notation. Montgomery algorithm is a reduction algorithm, which is often applied in the implementation. Algorithm 2\(^8\) is the reduction algorithm of the modular multiplication. Montgomery algorithm is applied to the LR exponentiation in Algorithm 3\(^8,11\).

**Algorithm 1: LR algorithm**

**Input:** \( g \in \mathbb{G} \) and \( e = (e_0 e_{t-1} \ldots e_1 e_0)_2 \)

**Output:** \( g^e \)

1. \( A \leftarrow 1 \)
2. For \( i = t \) downto 0 do:
   2.1 \( A \leftarrow A \cdot A \)
   2.2 If \( e_i = 1 \) then \( A \leftarrow A \cdot g \)
3. Return \((A)\)

**Algorithm 2: Montgomery modular multiplication**

**Input:** \( m = (m_{n-1} \ldots m_1 m_0)_b \), 
\[ x = (x_{n-1} \ldots x_1 x_0)_b \]
\[ y = (y_{n-1} \ldots y_1 y_0)_b \]
\[ R = b^n, \quad \gcd(m, b) = 1 \]
\[ = m^{-1} \cdot m \cdot b \]

**Output:** \( xy \cdot R^{-1} \cdot \) mod \( m \)

1. \( A \leftarrow 0 \) \((A = (a_n a_{n-1} \ldots a_1 a_0)_b)\)
2. For \( i = 0 \) to \((n - 1)\) do:
   2.1 \( u_i \leftarrow (a_0 + x_i y_b) m^{-1} \cdot \) mod \( b \)
   2.2 \( A \leftarrow (A + x_i y + u_i m) / b \)
3. If \( A \geq m \) then \( A \leftarrow A - m \)
4. Return \((A)\)

**Algorithm 3: Montgomery exponent operation**

**Input:** \( m = (m_{n-1} \ldots m_1 m_0)_b \), \( R = b^t \), 
\[ m = -m^{-1} \cdot m \cdot b \]
\[ e = (e_t \ldots e_0)_2, \quad e_t = 1, \quad x_1 < m \]

**Output:** \( x^e \) mod \( m \)

1. \( x \leftarrow M_{\text{ont}}(x, R^2 m \cdot \text{od} m) \)
2. For \( i = t \) downto 0 do:
   2.1 \( A \leftarrow M_{\text{ont}}(A, A) \)
   2.2 If \( e_i = 1 \) then \( A \leftarrow M_{\text{ont}}(A, \bar{x}) \)
3. \( A \leftarrow M_{\text{ont}}(A, 1) \)
4. Return \((A)\)

3. **New chosen-message SPA**

3.1 *power Analysis consumption model*

The Hamming weight power consumption model is that the power consumption of the operating operand is proportional or inversely proportional to the value of the bit\(^{10}\).

In real environment, the acquisition of the power curves is affected by the equipments, the environments and many other effects. The composition of each specific power consumption is as follows:

\[
P_{\text{total}} = P_o + P_{\text{data}} + P_{\text{clk}} + P_{\text{cm}} \quad (1)
\]

\(P_o:\) operation-dependent component
$P_{\text{data}}$: data-dependent component

$P_{\text{el.noise}}$: electronic noise

$P_{\text{const}}$: const component

$P_{\text{op}} = P_{\text{data}} + P_{\text{el.noise}}$  \( \tag{2} \)

$P_{\text{exp}}$: exploitable power consumption

$P_{\text{sw.noise}}$: switching noise

In Algorithm 1, each modular multiplication has the operands \( x, A, R \) and \( m \) which are used in the operation, where \( x \) is the value used in each round of Montgomery operations. \( R \) and \( m \) are constants, so in each round of Montgomery modular multiplication, the changes of the operands \( x \) and \( A \) are related to the power consumption. Based on the Hamming weight power consumption model, we can get:

$$P_{\text{total}} = P_{\text{op}} + f(HW(x), HW(A)) + P_{\text{el.noise}} + P_{\text{const}} \tag{3}$$

<table>
<thead>
<tr>
<th>The current secret key $e$</th>
<th>Operation</th>
<th>The main effect factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Square</td>
<td>$HW(A)$</td>
</tr>
<tr>
<td>1</td>
<td>Square</td>
<td>$HW(A)$</td>
</tr>
<tr>
<td>1</td>
<td>Multiply</td>
<td>$HW(x), HW(A)$</td>
</tr>
</tbody>
</table>

From Table 1, it is clear to see that $HW(x)$ is related to the power consumption of the modular multiplication when $e=1$. When the characteristics of $HW(x)$ are highlighted, the modular multiplication of $e=1$ will be found. Then, the secret key can be recovered.

### 3.2 Proposed new chosen-message SPA

Choosing the $x = \bar{x} \times R^{-1} \mod m$, let $HW(\bar{x})$ become a very small number and the value of $\bar{x}$ is big. During Montgomery operation, the modular multiplication $A \leftarrow M \text{ant}(A, \bar{x})$ is performed when $e=1$. The big difference between $HW(\bar{x})$ and $HW(A)$ is significant effect on $f(HW(\bar{x}), HW(A))$. From Formula \( \tag{3} \), we can see that this effect will be reflected upon the total power consumption, as shown in Figure 1.

![Fig 1 Proposed new chosen-message SPA](image)

In Figure 1, S is the modular square and M is the modular multiplication. Due to that $\bar{x}$, whose Hamming weight is small, is used in the operations of Montgomery modular multiplication, M shows a smaller power consumption.

### 4. Experiments

#### 4.1 Testing environment of the power consumption

This test object is the 8051 crypto chip and the composition of the test platform is as shown in Figure 2:
Fig 2 Testing environment of the power consumption

In this power consumption analysis platform, the workstation which is connected to the oscilloscope through the USB interface sets the parameters of the oscilloscope and the interface board. The workstation sends instructions or data to the interface board and receives the return data. The oscilloscope, whose type Model is Tektronix PPO4032, receives the instructions and the trigger signal. Then it collects the power consumption curves.

4.2 Analysis of experimental results

In the experimental platform as shown in Figure 2, firstly, the random number \( x_a \) is selected. Let \( x_a \) as the plaintext perform the RSA signature algorithm. And the power consumption curve is gotten as shown in Figure 3 (a). Then with the same exponent and modulus, choosing \( x_b = x_b \cdot R^{-1} \mod m \) (\( x_b = 2^{2023} \)), the power consumption curve is obtained as shown in Figure 3 (b).

(a) Input the random \( x_a \)

(b) Input the chosen-message \( x_b \)

(c) (b) amplified

Fig 3. Power consumption curves of 8051 chip

(a) Input the random \( x_a \)
In Figure 3 (a), the interval of each modular multiplication is obvious, but the correlation with the exponent can’t be seen with the naked eye. In figure 3 (b) and figure 3 (c), we can clearly distinguish the square and modular multiplication. The secret key can be recovered based on Figure 3 (c).

4.3 The selection and statistics of the revealing secret message

In the chosen-message SPA, attacker can distinguish the square and multiplication based on a single power consumption curve. And then recover the secret key. The chosen-message attack has the very high efficiency. But the defense to the chosen-message SPA proposed in the literature [6,7] is very easy to do, which is forbidding the making effective attack plaintext. But in the attack in this paper, the countermeasure to forbid is not invalid. In the table 2, there is an incomplete statistics of the message which we can choose.

4.4 The efficiency contrast

Table 1 The test results of the partial plaintext examples on the 8051

<table>
<thead>
<tr>
<th>HW(C.)</th>
<th>The span of the effective plaintext in theory</th>
<th>The amount of the effective plaintext</th>
<th>Whether the attack effect appear</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$2^{1023}, 2^{1022}, 2^{1021}, 2^{1020}, 2^{1019}, 2^{1018}$</td>
<td>6</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>$2^{1023} + \text{e.g.} 2^{1021}$</td>
<td>1022</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>$2^{1023} + 2^{1022}$</td>
<td>1022</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>$2^{1021} + \text{e.g.} 2^{1022}$</td>
<td>1020</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>$2^{1020} + \text{e.g.} 2^{1021}$</td>
<td>351</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>$2^{1019} + \text{e.g.} 2^{1020}$</td>
<td>251</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>$2^{1023} + \text{e.g.} 2^{1021} + 2^{1020}$</td>
<td>$2^{1022}$</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>$2^{1022} + \text{e.g.} 2^{1021} + 2^{1020}$</td>
<td>$2^{1022}$</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>$2^{1021} + \text{e.g.} 2^{1020} + 2^{1021}$</td>
<td>$2^{1022}$</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>$2^{1020} + \text{e.g.} 2^{1020} + 2^{1021}$</td>
<td>713</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>$2^{1019} + \text{e.g.} 2^{1020} + 2^{1021}$</td>
<td>209</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>$2^{1018} + \text{e.g.} 2^{1020} + 2^{1021}$</td>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>

The efficiency of the attack is a very important factor, because every smartcard have the lifecycle of itself. The higher efficiency the attack method has, the method is more effective.

The common side channel attack includes CPA, DPA, FA and SPA [3]. CPA and DPA are based on the statistic characteristics, these method needs collecting thousands upon thousands power consumption waves [3]. And the workstation which is used to statistics and analysis must have high-collocation.

The attack method proposed in this paper, attacker only needs a single power consumption wave to recover the secret key.

4.5 The countermeasure of the new SPA

Based on the analysis and statistics of the chapter 4.3, the amount of the plaintext is a large number. So the company of the clipper chip can’t use the forbidding specific message method to defense the proposed attack.

The dummy multiplication countermeasure is shown in the algorithm 4.
Algorithm 4: dummy multiplication Montgomery exponent Algorithm

<table>
<thead>
<tr>
<th>Input:</th>
<th>$m = (m_{t-1}...m_1m_0)_b$ , $R = b^t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m = -m^{-1}m \bmod b$</td>
<td></td>
</tr>
<tr>
<td>$e = (e_t...e_0)_2$ , $e_t = 1$ , $1 \leq x &lt; m$</td>
<td></td>
</tr>
<tr>
<td>Output:</td>
<td>$x^e \bmod m$</td>
</tr>
</tbody>
</table>

1. $\tilde{x} \leftarrow M_{on}(x, R^2 \bmod m) A \leftarrow R \bmod m$
2. For $i=t$ downto 0 do:
   2.1 $A \leftarrow M_{on}(A, A)$
   2.2 $U \leftarrow M_{on}(A, \tilde{x})$
   2.3 If $e_i = 1$ then $A \leftarrow U$
3. $A \leftarrow M_{on}(A, 1)$
4. Return $(A)$.

In the dummy multiplication, whether $e_i = 1$ or not the square and multiplication are performed together. Only when $e_i = 1$, the value of the multiplication will be assigned to the variable $A$. As a result of the high power consumption and the low power consumption appears alternatively, attacker can’t distinguish the square and multiplication.

In the masking base number algorithm, the base number is a random number. Attacker can’t control the Hamming weight of $\tilde{x}$ through choosing the specific. The testing result of the masking chip is as the fig.6 shown. So the masking base number algorithm can defense the SPA proposed in this paper[9].

![Fig.4. The power consumption of chosen-message $x = 2^{1023}$ on a masking base number 8051 chip](image)

5. Conclusion

Based on the Hamming weight power consumption model, a new method is proposed. In this method, a large value number but has a small Hamming weight is used in the signature operation. Using only a single power consumption curve, the attacker can clearly distinguish the square and multiplication and then recover more than 99% of the secret key. This attack is very efficient and has a certain degree of universality. The single shield specific number method can’t defense this attack.

Reference:


