Biometric Cryptosystem based Energy Attack Analysis

Jianbo Yao¹, Tao Zhang²
¹Department of Computer Science/Zunyi Normal College
No.830, Shanghai Road, 563002, Zunyi, Guizhou, P.R.China, Ph: +86852-8922406
²Westone information industry Co., LTD
No.8, Chuangye Road, Hi-Tech Zone, 610041, Chengdu, Sichuan, P.R.China, Ph: +86 85168215
e-mail: yaojianbo007@gmail.com ; zhangtao@uestc.edu.cn²

Abstract

Biometric cryptosystem provides a seamless connection between the biometrics and traditional password, and it represents a new development in the next generation cryptography. Even if the biometric cryptosystem is secure in algorithmic design, it may still be vulnerable to side-channel attack due to the physical leakage. To assess the possible side-channel attack on biometric cryptosystem, a secure biometric cryptosystem is designed and by measuring the energy consumption leaked. The simulation shows that the biometric cryptosystem can be extracted with bits of energy leakages.

Keywords: biometric cryptosystem, side-channel attack, energy attack, differential energy attack, energy consumption leakages

Copyright © 2012 Universitas Ahmad Dahlan. All rights reserved.

1. Introduction

As development of network technology, traditional cryptography technology as the identity authentication the main method cannot have satisfied development demand. Due to the biological characteristics of itself has stronger ability to identify and authentication, the biological characteristics and traditional cryptography combining the technology, the development of safety higher authentication technology has become the development trend [1-3]. A notable example is the biological public-key systems [4], [5], provide personal biological characteristics and traditional password techniques seamless connection, has been widely applied to electronic business, e-government contour safety field. However, biological public-key systems in use process still face some security issues: such as user biological template information management loopholes. Once the user's information from eavesdroppers biological template or missing, these important information will likely be attacker used for other has the same creature certification application system, so that the application system face security threat [6],[7]. Traditionally, on biological template information protection is primarily through using complexity and higher cryptographic algorithms to biological information safety analysis of main from mathematical sense on [8].

Biological template information even in algorithm is safe, also may be due to the side channels leak and become insecure. Biological template of information security and new threats of which comes from side channel attacks technology, side channel attacks using biological public-key systems runtime various leakage information, combined with statistical analysis method to crack biological template information.

The remainder of this paper is organized as follows. Section 2 introduces some preliminary knowledge on biometric cryptosystem. Section 3 is differential energy attack analysis based on biometric cryptosystem. Finally, a conclusion is presented in section 4.

2. Biometric Cryptosystem

2.1. Structure of Biometric Cryptosystem

The core idea of biometric cryptosystem combined the traditional key (such as passwords, user identity) with biometric information to generate safety higher biological keys. Biometric cryptosystem includes two different algorithms: biometric key binding algorithm and key retrieval algorithm. Algorithm realization ways is as shown in Figure 1.
The process of the key binding and key retrieval can be described in formula (1):

\[
\begin{aligned}
\text{key binding:} & \quad Bio + Key = BioKey \\
\text{key retrieval:} & \quad BioKey + Bio' = Key' \\
\end{aligned}
\]  

(1)

Here, \(Key\) is traditional key, \(Bio\) and \(Bio'\) are biometric templates, \(BioKey\) is biometric key.

The two algorithms are similar with the encryption and decryption in the traditional cryptosystem. Namely through a two-dimensional variables of input, producing a one-dimensional variable output. Differentia depends on: traditional cryptographic algorithm, and key input expressly produced ciphertext, and biometric cryptosystem is input biological characteristics and key, producing a higher level of security of biological keys. Compared with the traditional cryptography, because biometric characteristics by itself, biometric cryptosystem also have the following characteristics [9]:

(i) Fault-Tolerance: For the same two biological organisms sampling features \(Bio\) and \(Bio'\), when \(Bio\) and \(Bio'\) differences in the system constitution tolerance \(\delta\), the system can generate within the same key. Namely, if \(Bio - Bio' < \delta\), then \(Key = Key'\).

(ii) Distinctions: For different individual organisms sampling \(Bio\) and \(Bio'\), when \(Bio\) and \(Bio'\) differences in the system constitution tolerance \(\delta\) outside, the system can carry on the effective difference, assure cannot make the same key. Namely, if \(Bio - Bio' > \delta\), then \(Key \neq Key'\).

(iii) Mono-direction: For \(Bio\) biological characteristics, not through \(BioKey\) to reverse derived. Namely, we must ensure the safety of biological characteristics.

2.2. Design of Biometric Cryptosystem

In order to assess side channel attacks on biometric cryptosystem threat, establishing a typical biometric cryptosystem implementation scheme, the user's keystroke biological characteristics (twice keystroke between delay) [10] and secret sharing scheme combination [11], proposed safe biometric cryptosystem design method, its design process includes the following two stages: biological feature extraction phase and biometric cryptosystem formation stage.

1. Keystroke feature extraction: Keystroke is a different from other biological characteristics (such as fingerprints, iris) of new biological characteristics, in the past, the biological characteristics may require costly in sampling equipment can acquire, while keystroke extraction is very cheap, only need is the keyboard. Through user keystrokes and release button of delay between the statistical analysis, can generate and user identity corresponding biological characteristics [12]. User keystroke time characteristics shows as Figure 2.

According to the characteristics of keystroke delay division, can be divided into the following four categories [12]:

(i) PP(Press-Press) time delay: Keystroke process twice adjacent key event time intervals.

(ii) PR(Press-Release) time delay: A keystroke events and release event time intervals.
(iii) RP (Release-Press) time delay: A key release event with subsequently key event time intervals.
(iv) RR (Release-Release) time delay: Adjacent two buttons release event time intervals.

Figure 2. User keystroke time characteristics

For different users, can be based on the characteristics of keystroke statistical analysis to establish the corresponding user biological characteristics of keystroke can be used to distinguish different user. For example, user A and user B respectively input string "shenwumi", its corresponding keystroke delay characteristics (PP time and PR duration) is significant difference, Figure 3 and Figure 4 show user A and user B two different users of keystroke delay characteristics.

Figure 3. User A keystroke delay characteristics (PR duration and PP interval)

Figure 4. User A keystroke delay characteristics (PR duration and PP interval)

Through a lot of data sampling, in extracting keystroke Bio biological characteristics, to facilitate the latter stages of the operation, there is a need to convert Bio biological
characteristics and the corresponding binary string (hereinafter referred to as biological descriptor) \( b(i) \) [12]:

\[
b(i) = \begin{cases} 
0 & \text{if } \mu_{ai} + k \delta_{ai} < t_i \\
1 & \text{if } \mu_{ai} + k \delta_{ai} > t_i \\
\bot & \text{otherwise}
\end{cases}
\] (2)

Here, the parameter \( t_i \in R \) for the system in fixed parameters, \( u_{ai} \) and \( \delta_{ai} \) separately \( N \) times independent sampling experiment sample mean and variance. Biometric descriptor \( b(i) \) represents the corresponding with the lawful users; different user biometric descriptors are not the same.

2. Safe biometric cryptosystem design: Extract the keystroke biological characteristics and literature [11] scheme unifies, design key binding algorithm of biometric cryptosystem based on the keystroke characteristics:

(i) A set of positive prime numbers \( m_1 < m_2 < \ldots < m_n \) are chosen as the bases, where \((m_i,m_j) = 1\), for \( i \neq j \).

(ii) The secret key (traditional password) \( Key \) is divided into \( n \) shares by using Chinese remainder theory (CRT), that is, \( Key = Key \mod m_i, \ i = 1,...,n \).

(iii) Similarly, the \( L \)-bit biometric descriptor \( b_i \) is divided into \( n \) parts equally, and each part \( b_i \) is called sub-biocode.

(iv) After using error correction function \( \text{encoder}(Key) = cKey \), the biometric key is denoted as: \( BioKey = \bigcup_{i=1}^{n} (z_i,m_i) \). here \( z_i = cKey \otimes b_i, \ i = 1,...,n \). From the point of algorithmic complexity, the security of biometric template is \( O(2^{L/n}) \) [11].

3. Side-channel Attack on Biometric Cryptosystem

3.1. Experimental Environment and Attack Methods

In the implementation of the specific attack before first presents the following two hypotheses:

**Assumption 1:** attacker can obtain the whole information on \( Key \) or \( BioKey \) in biometric cryptosystem.

**Assumption 2:** attacker can get the detail of the algorithm of biometric cryptosystem.

In the above two assumptions, attack the ultimate goal is to obtain biological template information. Figure 5 is the experimental schemes for side-channel attack on biometric cryptosystem.

![Figure 5. The experimental schemes for side-channel attack](image-url)
The experiment environment consists of three parts: a main board for generating a biometric key, a measurement of the energy consumption and security analysis component.

The experiment process includes the following steps: Firstly, with thousands of keystroke training, the biometric template \( b(i) \) can be generated by using the statistic method proposed in [10]. Then, a user makes \( N \) (hundreds) independent keyboard inputs with the biometric template \( b \) and changeable passwords \( \text{Key} \) to generate the biometric key \( \text{BioKey} \). Specifically, during each execution of the key binding algorithm, the energy consumption has been recorded by a digital oscilloscope and the leakage set is denoted as \( \text{Leak} = \{O_1, O_2, ..., O_N\} \). For simplicity's sake, it is the change of Hamming Weight of energy leakage is analyzed. Similar analysis method sees literature [11].

3.2. Side-Channel Analysis

Once the leakage profiles are built, attacker can make a statistical analysis to extract the biometric template. The analytical process holds in three steps:

(i) Hypothesis: two different hypothesizes on the \( i \)-bit of biometric descriptor \( b(i) \) are made:

\[
H_0 : b(i) = 0 \quad \text{and} \quad H_1 : b(i) = 1
\]

(ii) Classification: As for the secure BKS implementation proposed in Section 3, a selection function \( \varphi(\text{Key}_i, b_i) = \text{Key}_i \oplus b_i \) is chosen, here parameters \( \text{Key}_i \) and \( b_i \) represent the \( i \)-bit of password and biometric template. According to the output of function \( \varphi(\text{Key}_i, b_i) \), the leakage \( \text{Leak} = \{O_1, O_2, ..., O_N\} \) is divided into two subsets:

\[
\begin{align*}
D_0 &= \{O_i | \varphi(\text{Key}_i, b_i) = 0, O_i \in \text{Leak}\} \\
D_1 &= \{O_i | \varphi(\text{Key}_i, b_i) = 1, O_i \in \text{Leak}\}
\end{align*}
\]

The average signal for the two subset has been computed as \( \overline{D_0} \) and \( \overline{D_1} \).

\[
\overline{D_0} = \frac{1}{|D_0|} \sum_{O \in D_0} O \quad \text{and} \quad \overline{D_1} = \frac{1}{|D_1|} \sum_{O \in D_1} O
\]

(iii) Comparison: the differential value \( \Delta D \) is computed as \( \Delta D = \overline{D_0} - \overline{D_1} \). If \( \Delta D > 0 \), the hypothesis \( H_i \) is supported and the \( b(i) \) is 1, otherwise the \( b(i) \) is 0.

3.3. Performance Analysis

Assume the energy consumption dependents on Hamming weight model. The noise contributions are ignored, since when averaging is used, these contributions will be removed. Differential energy attack (DPA) is performed with 1000 independent energy leakage measurements.

As depicted in Figure 6 and Figure 7, there are a negative peak when \( b(i) = 0 \) and a positive peak when \( b(i) = 1 \) among the differential results. That means the hypothesis and the measurement with high correlation. Therefore, the attacker can easily deduce the correct biometric template through statistical analysis.

Furthermore, the performance of DPA is quantified with the number of measurements to disclose (MTD). This number expresses how many measurements are on average necessary to correctly distinguish the correct secret key from all the wrong key guesses.

As shown in Figure 8 and Figure 9, the convergence of DPA attack has been analyzed with the sample number increasing from 2 to 1000. The simulation result has shown when the sample number is beyond 100, DPA attack can extract the correct biometric template successfully.
Figure 6. Successful DPA attack when template \( b(i) = 0 \)

Figure 7. Successful DPA attack when template \( b(i) = 1 \)

Figure 8. DPA convergence analysis when template \( b(i) = 0 \)
4. Conclusion

The biometric cryptosystem as the password system of a new application forms, its safety not to allow ignore. In this paper, side channel attacks technology is applied to biometric cryptosystem, energy attacks by the difference of biometric cryptosystem of biological template information are analyzed, and the results showed no any defensive measures of biometric cryptosystem, there are certain side channel leakages. The simulation analysis showed that a small amount of energy consumption leak could be cracked biometric cryptosystem of biological template information.

Acknowledgments

This research was supported by The Governor Specialized Fund Item of Guizhou Province for Excellence Science, Technology and Education Talent under grant Qian-sheng-zhuan-he-zhi No.(2009)27; The Science and Technology Foundation Item under grant Qian-ke-he-J-zhi No.[2009]2275; Doctoral Found item of Zunyi Normal College No.[201213SJ15].

References