第 37 卷 第 24 期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011 年 12 月
December 2011

• 安全技术 •

文章编号：1000—3428(2011)24—0103—03 文献标识码：A 中图分类号：TP393.08

基于生物密钥系统的能量攻击分析

姚剑波[1]，张 涛[2]

(1. 遵义师范学院计算机科学系，贵州 遵义 563002；2. 中国电子科技集团公司第三十研究所卫士通公司，成都 610041)

摘 要：为评估生物密钥系统在侧信道攻击下的安全性能，在分析生物密钥系统结构和特点的基础上，将用户的击键生物特征和秘密共享方案相结合，设计一个基于击键的安全生物密钥系统，并通过差分能量攻击技术测量安全生物密钥系统的功耗泄漏。仿真分析表明，攻击者借助少量的功耗泄露就可以破解生物密钥系统的信息。

关键词：生物密钥系统；侧信道攻击；差分能量攻击；功耗泄漏

Power Attack Analysis Based on Biometric Cryptosystem

YAO Jian-bo[1], ZHANG Tao[2]

(1. Department of Computer Science, Zunyi Normal College, Zunyi 563002, China;
2. Westone Corporation of No.30 Research Institute, China Electronics Technology Group Corporation, Chengdu 610041, China)

【Abstract】To assess the biometric cryptosystem performance in possible side-channel attacks, on the basis of analysis of the biometric cryptosystem structure and characteristics, a secure biometric cryptosystem based on the keystroke is designed by the combination of the user's keystroke biological characteristics and secret sharing scheme. Power consumption leakage of the safe biometric cryptosystem is measured with the Differential Power Attack(DPA). Simulation analysis shows the biometric cryptosystem can be extracted with bits of power leakages.

【Key words】biometric cryptosystem; side-channel attack; Differential Power Attack(DPA); power consumption leakage

DOI: 10.3969/j.issn.1000-3428.2011.24.034

1 概述

随着网络技术的发展，传统密码技术作为身份认证的主要手段已经不能满足发展需求。由于生物特征本身具有较强的鉴别和认证能力，因此将生物特征和传统密码技术相结合，开发安全性更高的认证技术已经成为发展趋势[1]。

在传统意义上，对生物模板信息的保护主要是采用复杂度较高的密码算法，并且对生物信息安全性的分析也主要从数学意义上展开[2]。

生物模板信息即使在算法上是安全的，也可能由于侧信道泄露而变得不安全[3]。生物模板信息安全的新威胁来源于侧信道攻击技术，而侧信道攻击利用生物密钥系统运行时的各种泄漏信息，因此，本文结合统计分析方法来破解生物模板信息。

2 生物密钥系统

2.1 生物密钥系统的结构

生物密钥系统的核心思想是将传统的密钥(如密码、用户标识)和生物特征信息相结合，以生成安全性较高的生物密钥。

生物密钥系统包含 2 个不同的算法[4]：生物密钥绑定算法和生物密钥松绑算法，其中，密钥绑定算法和密钥松绑算法的实现如下式所示：

$$Bio + Key = BioKey$$
$$BioKey + Bio' = Key' \quad (1)$$

其中，Key 为传统密钥；Bio 和 Bio' 分别为生物模板；$BioKey$ 为生物密钥。

式(1)非常类似于传统密码系统中的加密操作和解密操作，即通过一个二维变量的输入，产生一个一维变量的输出。不同点在于：传统的密码算法输入明文和密钥，产生密文，而生物密钥系统则是输入生物特征和密钥，产生一个更高安全级别的生物密钥。

由于生物特征本身的特性，与传统的密码系统相比，本文生物密钥系统还具有以下特点[4]：

(1)容错性：对于同一生物体的 2 次生物采样特征 Bio 和 Bio'，当 Bio 和 Bio' 的差异在系统设置的容忍度 δ 内，系统能生成相同的密钥。即如果 $Bio - Bio' < \delta$，则 $Key = Key'$。

(2)区别性：对于不同的生物个体的采样 Bio 和 Bio'，当 Bio 和 Bio' 的差异在系统设置的容忍度 δ 以外，系统能对其进行有效的区别，以此保证无法生成相同的密钥。即如果 $Bio - Bio' > \delta$，则 $Key \neq Key'$。

(3)单向性：对于生物特征 Bio，不能通过 $BioKey$ 进行逆向推导。即必须保证生物特征的安全性。

2.2 基于击键的生物密钥系统设计

本文建立一种具有代表性的生物密钥系统实现方案，通过将用户的击键生物特征(2 次击键之间的时延)[5]和秘密共享方案相结合[6]，提出安全的生物密钥系统设计方法，其设计过程包括以下 2 个阶段：生物特征提取阶段和生物密钥系统生成阶段。

2.2.1 击键特征的提取阶段

击键特征是一种不同于其他生物特征(如指纹、虹膜)的新型生物特征，以往的生物特征可能需要昂贵的采样设备才能获取，而击键特征的提取是非常廉价的，唯一需要的就是键盘。通过对用户击键和释放键之间的时延进行统计分析，

基金项目：贵州省科学技术基金资助项目(黔科合 J 字 2009(2275))

作者简介：姚剑波(1965－)，男，博士、CCF 高级会员，主研方向：信息安全；张 涛，博士

收稿日期：2011-06-21 **E-mail：**yaojianbo007@gmail.com

就可以生成与用户身份对应的生物特征[7]。用户击键的时间特征如图 1 所示。

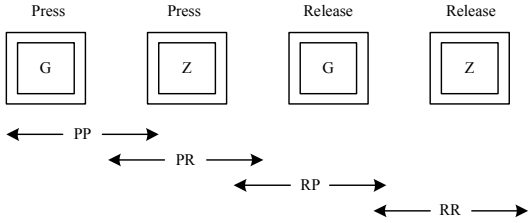

图 1 用户击键的时间特征

按击键时延的特征划分，可以分为以下 4 类[7]：

(1)PP(Press-Press)时延：击键过程中 2 次相邻的按键事件的时间间隔。

(2)PR(Press-Release)时延：某次击键事件和释放事件的时间间隔。

(3)RP(Release-Press)时延：某次按键释放事件与随后的按键事件的时间间隔。

(4)RR(Release-Release)时延：相邻 2 次按键释放事件的时间间隔。

对于不同的用户，可以通过对击键的特征进行统计分析来建立相应的用户生物特征，击键特征能用于区别不同的用户。例如，甲和乙 2 个用户分别输入字符串“shenwumi”，其对应的击键时延特征(PP 时间和 PR 持续时间)是有明显差别的，图 2 和图 3 显示了甲和乙 2 个不同用户的击键时延特征。

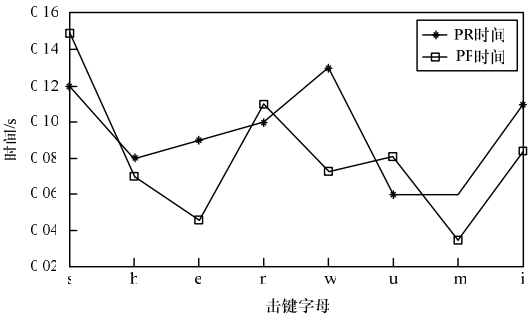

图 2 用户甲击键的时延特征

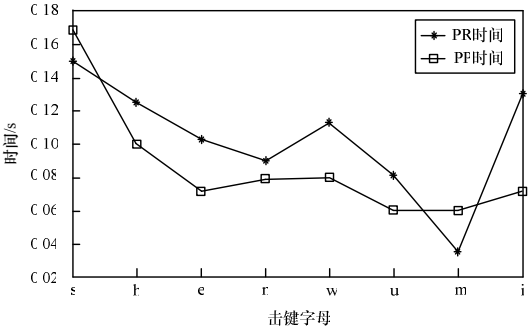

图 3 用户乙击键的时延特征

通过大量的数据采样，在提取击键的生物特征 *Bio* 后，为了便于后阶段的运算，需要将生物特征 *Bio* 转换为与之相对应的二进制字符串(以下简称生物描述符)$b(i)$[7]：

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

其中，参数 $t_i\in R$ 为系统中固定的参数；μ_{ai} 和 δ_{ai} 分别表示 N 次独立采样实验的样本均值与方差。生物特征描述符 $b(i)$ 代表了与之对应的合法用户，不同的用户的生物特征描述符是不相同的。

2.2.2 安全的生物密钥系统设计

将提取的击键生物特征与文献[6]的方案相结合，设计基于击键特征的生物密钥系统的密钥绑定算法：

(1)选择 n 个非负素数 $m_1<m_2<\cdots<m_n$ 作为模运算的基，其中，对 $i\neq j$，满足条件 $(m_i,m_j)=1$。

(2)利用中国剩余定理将传统的密钥 *Key* 分成 n 份，分割方法如下式所示：

$$Key_i\equiv Key \bmod m_i \quad i=1,2,\cdots,n \tag{3}$$

(3)类似地，将 L bit 的生物特征描述符 b_a 也同样的分割成 n 份，其中，每一份 b_i 被称为子生物特征标识码。

(4)在利用一个纠错函数 $encoder(Key_i)=cKey_i$ 对传统密钥进行处理后，生物密钥 *BioKey* 的生成如下：

$$BioKey=\bigcup_{i=1}^{n}(z_i,m_i)$$
$$z_i=cKey_i\otimes b_i \quad i=1,2,\cdots,n \tag{4}$$

从算法复杂度看，文献[6]指出生物模板的复杂度为 $O(2^{tL/n})$，因此，只要设计者选择合理的参数，攻击者很难获取模板 $b(i)$的信息。

3 生物密钥系统的差分能量攻击

3.1 实验环境与攻击方法

在实施具体的攻击之前，先给出以下 2 条假设：

假设 1 攻击者能够获取生物密钥系统中关于 *Key* 和 *BioKey* 的信息。

假设 2 攻击者能够获取生物密钥系统算法的实现细节，即算法是公开的。

在以上 2 条假设条件下，攻击的最终目标是获取生物模板信息。

实验环境包括 3 个部分：

(1)具有生物密钥系统的主板。

(2)功耗采样环境。

(3)侧信道攻击的分析环境。

实验过程包含以下步骤：

(1)用户通过上千次的击键训练，利用文献[7]中的方法提取击键模板信息 $b(i)$。

(2)在用户生物特征不变的条件下，该用户通过 N 次独立的键盘输入不同的密码，由此产生对应的生物密钥 *BioKey*。

特别地，在每一次生物密钥生成过程中，用仪器(如示波器)对功耗变化进行监测，并将该信息存储在泄漏信息库中，则 N 次运算的泄漏结合为：$Leak=\{O_1,O_2,\cdots,O_N\}$。

为简单起见，这里采用 Hamming Weight 的变化来对功耗泄漏进行分析，类似的分析方法见文献[6]。

3.2 差分能量攻击流程

在完成了功耗泄漏特征的采集后，攻击者可以利用统计分析方法来破解生物模板，分析步骤分为以下 3 步：

(1)建立假设：分别建立 2 个关于模板 $b(i)$ 的第 i bit 的不同假设：

$$H_0:\ b(i)=0$$
$$H_1:\ b(i)=1 \tag{5}$$

(2)泄露分类：构造选择函数：

$$\varphi(Key_i,b_i)=Key_i\oplus b_i \tag{6}$$

其中，参数 Key_i、b_i 分别表示第 i bit 所对应的密钥和生物模

板信息。根据选择函数输出值的不同，将功耗泄漏集合 $Leak=\{O_1,O_2,\cdots,O_N\}$ 分为 2 个不同的子集合，如下所示：

$$D_0=\{O_i\mid\varphi(Key_i,b_i)=0,O_i\in Leak\}$$
$$D_1=\{O_i\mid\varphi(Key_i,b_i)=1,O_i\in Leak\} \quad (7)$$

分别对以上子集合求取其平均泄漏信号 $\overline{D_0}$ 和 $\overline{D_1}$，可得：

$$\overline{D_0}=\frac{1}{|D_0|}\sum_{O_i\in D_0}O_i$$
$$\overline{D_1}=\frac{1}{|D_1|}\sum_{O_i\in D_1}O_i \quad (8)$$

(3)差分分析：通过计算差分值 $\Delta D=\overline{D_0}-\overline{D_1}$ 对步骤 1 的假设进行检验。当 $\Delta D>0$，则假设 H_1 成立，对应的生物模板第 i bit $b(i)$ 为 1；否则 $b(i)$ 为 0。

3.3　攻击性能分析

假设功耗模型为 Hamming Weight 模型，并且忽略噪音信号对功耗泄漏的影响，因为在差分分析的平均过程中，噪音信号能被有效地抵消。

在生物模板 $b(i)=0$ 和 $b(i)=1$ 条件下，分析差分能量攻击。当差分结果小于 0 时，对应在差分曲线上会产生一个负值的尖峰值，该值表明击键特征 $b(i)=0$，如图 4 所示；反之，当差分结果大于 0 时，对应在差分曲线上会产生一个正的尖峰值，该值表明击键特征 $b(i)=1$，如图 5 所示。

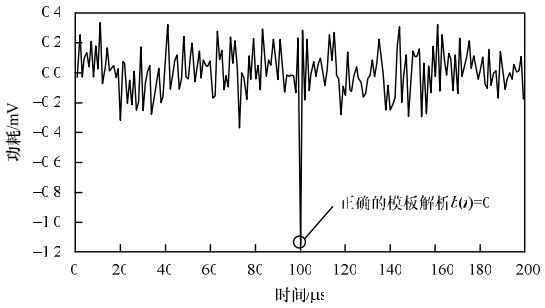

图 4　击键特征 $b(i)$=0 的 DPA 攻击

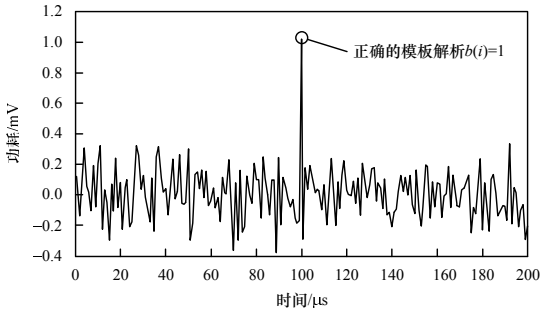

图 5　击键特征 $b(i)$=1 的 DPA 攻击

以上分析表明，通过侧信道攻击技术，攻击者可以获取生物模板信息。

为了对差分功耗攻击(Differential Power Attack, DPA)生物模板的攻击性能进行分析，引入参数 MTD(Measurements to Disclose)作为攻击性能的评价指标，该参数表明需要多少条采样信息才能成功地分析出生物模板信息。

图 6 和图 7 反映出在功耗采样数目发生变化时 DPA 攻击的收敛性，在仿真分析过程中，功耗样本数目从 2 逐步增加到 1 000，图 6 表明了生物模板为 $b(i)$=0 时的 DPA 攻击性能，当样本数目超过 200 条时，差分结果趋向于−1。同理，图 7 表明了生物模板为 $b(i)$=1 时的 DPA 攻击性能，当样本数目超过 100 条时，差分结果趋向于 1。综上，在仿真环境下，攻击者仅需要约 100 条功耗曲线就可以分析出生物模板信息。

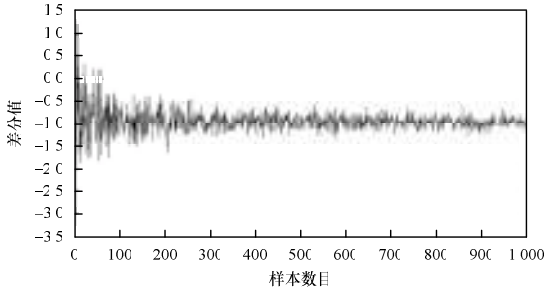

图 6　击键特征 $b(i)$=0 时攻击性能收敛性分析

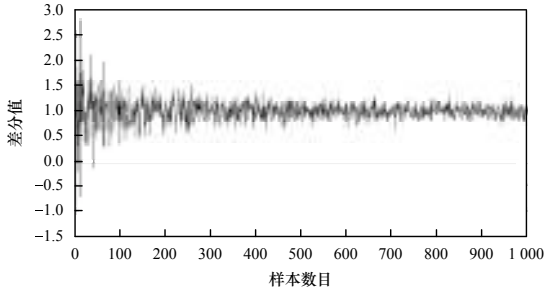

图 7　击键特征 $b(i)$= 1 时攻击性能收敛性分析

4　结束语

生物密码系统作为密码系统的一种新型应用形式，其安全性不容忽视，本文将侧信道攻击技术应用到生物密钥系统，通过差分能量攻击对生物密钥系统的生物模板信息进行了分析，结果表明，没有任何防御措施的生物密钥系统，存在一定的侧信道泄露。

参考文献

[1] Jain A K, Ross A, Pankanti S. Biometrics: A Tool for Information Security[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 125-143.

[2] Adler A. Can Images be Regenerated from Biometric Templates?[C]//Proc. of Biometrics Consortium Conference. Washington D. C., USA: [s. n.], 2003: 121-130.

[3] 杜之波，陈　运，吴　震，等. 防范边信道攻击的逆伪操作实现算法[J]. 计算机工程, 2010, 36(3): 131-133.

[4] Nichols R K. ICSA Guide to Cryptography[M]. [S. l.]: McGraw-Hill, 1999.

[5] Rodrigues R N, Yared G. Biometric Access Control Through Numerical Keyboards Based on Keystroke Dynamics[C]//Proc. of ICB'06. Hong Kong, China: [s. n.], 2006: 640-646.

[6] Li Qiong, Niu Xiamu, Sun Shenghe. A Novel Biometric Key Scheme[J]. Chinese Journal of Electronics, 2006, 15(1): 99-102.

[7] Monrose F, Reiter M K, Wetzel S. Password Hardening Based on Keystroke Dynamics[C]//Proc. of the 6th ACM Conf. on Computer and Communication Security. Singapore: [s. n.], 1999: 73-82.

编辑　任吉慧