第35卷 第14期 计 算 机 工 程 2009年7月
Vol.35 No.14 Computer Engineering July 2009
·安全技术· 文章编号：1000—3428(2009)14—0148—03 文献标识码：A 中图分类号：TP393.08

n-挠群上基于多重生物特征身份的签名方案

赵学锋，辛小龙
(西北大学数学系，西安 710127)

摘 要：针对基于单一生物特征身份的签名方案在实际应用中存在的问题，提出一种基于多重生物特征身份的签名方案，研究基于椭圆曲线的 *n*-挠群，对不同生物特征进行融合，介绍基于生物特征身份的公钥密码体制，仿真实验结果表明，该方案在安全性、稳定性以及可靠性等方面，均具有一定优越性。

关键词：*n*-挠群；公钥密码系统；数字签名

Signature Scheme in *n*-Torsion Groups Based on Multi-biometric Characteristic Identity

ZHAO Xue-feng, XIN Xiao-long
(Dept. of Mathematic, Northwest University, Xi'an 710127)

【Abstract】 Aiming at problems in practical application of single biometric identity-based signature scheme, a novel multi-biometric identity-based signature scheme is proposed. The elliptic curve-based *n*-torsion groups are researched. Different biometric characteristics are syncretized. The biometric identity-based public key cryptosystem is introduced. Simulation experimental results show this scheme has better performances in security, stability and reliability, and is effective and feasible.

【Key words】 *n*-toison group; public key cryptosystem; digital signature

1 概述

在开放式网络中，公钥密码系统的信息安全越来越受到广泛重视。数字签名，作为一种信息安全服务技术，在保证数据的安全性、真实性、不可抵赖性等方面起着重要作用，因此，被广泛应用于金融、商业、军事等领域。总体而言，数字签名方案分为2大类：基于证书的签名方案和基于身份的签名方案。基于身份的签名方案避免了基于证书的签名方案所需要的大量存储空间和计算时间，而成为数字签名的主流。然而，在传统的基于身份的签名方案中，一个特定身份的用户，需要到权威机构“证明”该身份是他本人的，需要增补文档或相关证书，仍涉及到证书管理。相对而言，将生物特征作为身份认证[1]可以节省大量时间，空间-生物特征分为生理特征和行为特征，人体固有的生理特征包括面部特征、指纹、手纹、虹膜、视网膜、耳廓、DNA等；行为特征包括击键动力学、手写字体识别、语音识别、步态识别等。生物特征具有安全、保密、方便、不易遗忘、防伪性能好、不易伪造或被盗、随身携带和随时随地可用等优点。生物特征特有的稳定性、唯一性在安全认证等身份识别领域有广泛应用。

由于单一生物特征在实际应用中呈现出各自的局限性，无法满足实际要求，因此建立基于多重生物特征的数字签名系统是必要的。本文提出建立在椭圆曲线 n-挠群上，基于多重生物特征的数字签名方案，提高了系统的安全性和可靠性。

2 由生物特征生成的签名密钥数据

在生物特征系统中，特征数据几乎不会在2次对生物特征的读取中完全一致，即产生了生物特征的模糊性与密码学的准确性间的矛盾。文献[2]提出一种基于生物特的密钥产生技术——“模糊提取器”(fuzzy exractor)，模糊提取器可以从生物特征输入中提取出几乎是均匀分布的随机串，由于提取过程是容错的，在下次输入的生物特征 R' 相对于最初的输入 R 只发生微小的变化时，提取出的数据是完全一致的。为度量生物特征输入的变化，引入3种度量：汉明距离，集合差异，编译距离。汉明距离表示在 R' 和 R 之间不同比特位的个数，它是最简单的一种度量。在汉明距离下，模糊提取器结构如下：模糊提取器可表示为(M, l, t)，其中，M 是个有限维的度量空间，它有具有生物特征的数据点和距离函数 $dis: M\times M\to Z^+$ 组成，该函数用来计算所选度量空间上2个点之间的距离；l 表示提取串的比特数；t 表示错误的极限值(若 $dis(b,b')\le t$，则 $b,b'\in M$ 被视为同一类)。

由2个函数 GEN, REP 来构造模糊提取器。GEN 是个概率性生成函数，输入 $b\in M$，它会输出一个“提取的串” $\alpha\in\{0,1\}^l$ 和一个“公开的串” β，REP 是个确定性恢复函数，它可以从对应的“公开的串” β 和任一非常接近于 b 的 b' 恢复出 α。具体如下：

$\forall b,b'\in M$，且 $dis(b,b')\le t$，如果 $GEN(b)\to\langle\alpha,\beta\rangle$，那么 $REP(b',\beta)\to\alpha$

汉明距离度量下空间 $M=\{0,1\}^n$ 中一个模糊提取器的结构：定义 C 是个 (n,k,t) 二进制纠错码，其中，k 表示信息的长度；n 表示码字的长度；t 表示纠错能力。编码函数 $C_e:\{0,1\}^k\to\{0,1\}^n$ 和解码函数 $C_d:\{0,1\}^n\to\{0,1\}^k$，码率为 k/n。$GEN(b)$ 产生一个随机串 $\alpha\in\{0,1\}^k$，且 $\beta=b\oplus C_e(U)$，同样，令 $REP(b',\beta)=C_d(b'\oplus\beta)=\alpha$，(当且仅当 $dis(b,b')\le t$)。

基金项目：陕西省自然科学基金资助项目(2007A19)
作者简介：赵学锋(1982－)，男，硕士研究生，主研方向：密码学；辛小龙，教授、博士生导师
收稿日期：2008-12-10 **E-mail：**zxf0527@yahoo.cn

3 从生物特征数据到椭圆曲线的映射

获取生物特征数据 α 后，将其映射到椭圆曲线 $E(F_q)$ 中生成密钥，具体分为 2 步：

$H_0:\{0,1\}^* \to \{0,1\}^{160}$

$g:\{0,1\}^{160} \to G^*$

其中，哈希函数 $H:\{0,1\}^* \to G^*$，H_0 是个标准哈希函数 $SHA-1$，它把 $\{0,1\}^*$ 先映射到集 $\{0,1\}^{160}$ 上，然后用一个确定性嵌入函数 g，把 $\{0,1\}^{160}$ 映射到 G^* 上。(G 是椭圆曲线 $E(F_q)$ 上的点组成的一个子群)，使得 $H(\alpha)=g(H_0(\alpha))$，$Q=g(H(\alpha))$，Q 是对应于串 α 的点。

4 *n*-挠群的相关知识[3]

设 E 是有限域上的椭圆曲线，$E(F_q)$ 表示坐标在 F_q 中的所有点的集合。又设 n 是一大素数并且满足条件 $n\,|\,\#E(F_q), n\nmid(q-1)$，$k$ 是满足条件 $n\,|\,(q^k-1)$ 的最小正整数。$E(F_q)$ 表示坐标在 F_{q^k} 中的所有点的集合。

定义1 设 P 是 E 上一个点，n 是满足条件 $nP=O$ 的最小正整数，称点 P 为n-挠点。

定义2 所有n-挠点形成的点集，构成一个加法群，称为n-挠群，记作 $E[n]$。

定义3 n-挠点上的 *Weil* 对 $e_n:E[n]\times E[n]\to\mu_n$，$\mu_n$ 是 F_{q^k} 中n-*th*单位根组成的 F_{q^k} 的子群。

Weil 对的性质有：

(1)双线性性：$e(aP,bQ)=e(P,Q)^{ab}, \forall a,b\in Z_n^*; P,Q\in E[n]$。

(2)恒等性：$e(P,P)=1$，$\forall P\in E[n]$。

(3)非退化性：$\exists P,Q\in E[n]$，使得 $e(P,Q)\neq 1$。

(4)可计算性：$\forall P,Q\in E[n]$，存在有效的算法计算 $e(P,Q)$。

定义 4 设 P 是 $E(F_q)[n]$ 的一个生成元，*Weil* 对的变形定义：$\hat{e}(P,P)=e(P,\varphi(P))$，其中，$\varphi$是椭圆曲线上的一个自同态，且 $\varphi(P)$ 和 P 线性无关，显然有 $\hat{e}(P,P)\neq 1$。

假设在 $E(F_q)[n]$ 和 F_{q^k} 计算离散对数问题(Disperse Logarithm Problem, DLP)是困难的，在 $E(F_q)[n]$ 上考虑如下 2 个问题：

(1)计算 Diffie-Hellman 问题(Computing Diffie-Hellman Problem, CDHP) 给定 $P, aP, bP\in E(F_q)[n]$，计算 abP。

(2)决策 Diffie-Hellman 问题(Desicive Diffie-Hellman Problem, DDHP) 给定 $P, aP, bP, cP\in E(F_q)[n]$，判断是否有 $c=ab \bmod n$ 成立。

定义 5 如果在 G 中，DDHP 容易而 CDHP 困难，则称 G 为间隙 Diffie-Hellman 群。

在 n-挠群 $E(F_q)[n]$ 中，DLP 的困难性决定了 CDHP 的困难性，但由于双线性对 $\hat{e}$ 的作用，DDHP 是容易解决的。

5 基于身份的签名方案

L.Cha-L.Cheon 的基于身份的签名方案如下[4]：

(1)系统建立。设 $G=E(F_q)[n]$ 是一挠群，P 是 G 的一个生成元，2 个 Hash 函数 $H:\{0,1\}\to G$ 和 $H_1:\{0,1\}^*\times G\to Z_n^*$，私钥产生中心 *PKG* 随机选取 $s\in Z_n^*$ 作为系统的主密钥，计算 $P_{pub}=sP$。系统的公开参数是 (G,P,P_{pub},H,H_1)。

(2)密钥提取。用户根据自己的身份向 *PKG* 索取签名密钥，用户将自己的身份 *ID* 发送给 *PKG*，接到用户的申请后，*PKG* 计算 $Q_{ID}=H_1(ID), D_{ID}=sQ_{ID}$，并把 D_{ID} 发送给对应的用户，D_{ID} 为该用户的签名密钥。

(3)签名。对给定的消息 M，签名者随机选取 $r\in Z_n^*$，计算 $U=rQ_{ID}, h=H(M,U)$ 和 $V=(r+h)D_{ID}$，消息 M 的签名是 $\sigma=(U,V)$，并发送给验证者。

(4)验证。接收到 σ 后，验证者计算 $h=H(M,U)$, $Q=U+hQ_{ID}$，判断 $\hat{e}(P,V)$ 和 $\hat{e}(P_{pub},Q)$ 是否相等。若相等，则 σ 是消息 M 的正确签名。

6 基于多重生物特征身份的签名方案

本文方案以 L.Cha-L.Cheon 的基于身份的签名方案为基础，基于多重生物特征身份的签名方案的实现是通过聚合签名，将在不同生物特征身份下得到的签名聚合为一个短签名。下面是具体的签名方案。

设 $G=E(F_q)[n]$ 是个挠群，n 满足上述条件，P 是 G 的一个生成元。$M=\{0,1\}^n$ 是个 n 维度量空间，H, H_0 是哈希函数，其中，$H_0:\{0,1\}^*\to\{0,1\}^{160}$ 是标准哈希函数 $SHA-1$；$H_0:\{0,1\}^*\to G, g:\{0,1\}^{160}\to G$ 是个确定性嵌入函数。

(1)系统建立。私钥产生中心 *PKG* 随机选取一个元 $s\in Z, P_{pub}=sP$，其中，s 是系统的主密钥；P 是的 G 生成元；P_{pub} 是系统的公钥。*PKG* 保管系统的主密钥 s，系统的公开参数为：$params=\{G,q,P,P_{pub},H,H_1,g\}$。

(2)密钥提取。从生物特征数据中提取出具有身份特征的比特串。首先用户输入其生物特征数据 $b_i(i=1,2,\cdots,n_0)$，*PKG* 会利用 (M,l,t) 模糊提取器中的 *GEN* 概率性生成函数，输出一个“提取的串” $\alpha_i\in\{0,1\}^l$ 和一个“公开的串” $\beta_i=b_i\oplus C_e(\alpha_i)\in\{0,1\}^n$，即 $GEN(b_i)\to\langle\alpha_i,\beta_i\rangle$，然后通过嵌入函数将生物特征数据 α_i 映射到椭圆曲线的一个点 $Q_i=g(H(\alpha_i))$。用系统的主密钥 s 和 Q_i，计算出私钥，具体为 $d_i=sQ_i$，其中，d_i 为签名方案的私钥；Q_i 为公钥。

(3)单一签名。对消息 $m\in\{0,1\}^*$ 的签名：$\forall r\in Z_n^*$，计算 $U_i=rQ_i, h_i=H_1(m,U_i)$ 以及 $V_i=(r+h_i)d_i$，对 m 的签名是 $\sigma_i=(U_i,V_i),(i=1,2,\cdots,n_0)$。

(4)签名的聚合。接收到所有签名之后，用户先对所有签名进行聚合。用户计算 $h_i=H_1(m,U_i)$ 和 $Q_i^*=U_i+h_iQ_i$，令 $U=\prod_{i=0}^{n_0}Q_i^*, V=\prod_{i=0}^{n_0}V_i$，则 $\sigma=(U,V)$ 可视为对多重生物特征的聚合签名，将其与签名者的生物特征加密数据集合 B 一起传送给验证者。

(5)签名的验证。验证者要有 2 个数据：1)从签名者生物特征数据提取出的“公开的串” β 可直接向密钥生成机构申请得到；2)签名者的生物特征加密数据集合 B，由签名者与签名一起传送给验证者。通过上述 2 个数据之后，验证者首先通过解密 B 获得签名者的生物特征数据 b_i'，当它与签名者在密钥生成机构存储的生物特征数据 b_i 满足 $dis(b_i,b_i')\le t$ 时，则 b_i,b_i' 被视为同一类，否则签名无效；当 b_i,b_i' 被视为同一类时，再利用模糊提取器 (M,l,t) 的“恢复函数” *REP* 得到“提取的串”。$\alpha:REP(b_i',\beta)=C_d(\beta\oplus b_i')=C_d(b_i\oplus C_e(\alpha)\oplus b_i')=C_d(C_e(\alpha))=\alpha$，通过 α 计算出签名者的公钥 Q_i。最后，只需验证等式：$\hat{e}(P,V)=\hat{e}(P_{pub},U)$，等式成立，接受签名，否则拒绝。

证明 消息 m 在不同的生物特征下的签名是 $\sigma_i(U_i,V_i)$，其中，$U_i = rQ_i$；$h_i = H_1(m,U_i)$；$V_i = (r+h_i)d_i$；$\hat{e}(P,V_i) = \hat{e}(P,(r+h_i)\ d_i) = \hat{e}(P,(r+h_i)sQ_i) = \hat{e}(P,Q_i)^{(r+h_i)s}$；$\hat{e}(P_{pub},Q_i^*) = \hat{e}(P_{pub},\alpha_i + h_iQ_i) = \hat{e}(sP,\mathrm{r}Q_i+\mathrm{h}_i Q_i) = \hat{e}(P,Q_i)^{(r+h_i)s}$。因此，若 $\hat{e}(P,V_i) = \hat{e}(P_{pub},\ Q_i^*)$，则 $\sigma_i(U_i,V_i),(i=1,2,\cdots,n_0)$ 是在不同生物特征下签名者对 m 的签名。

由上述结果可得聚合签名验证公式为

$$\hat{e}(P,V) = \hat{e}(P,\prod_{i=0}^{n_0} V_i) = \prod_{i=0}^{n_0}\hat{e}(P,V_i) = \hat{e}(P_{pub},\prod_{i=0}^{n_0} Q_i^*) = \hat{e}(P_{pub},U)$$

7 有效性分析

由于各种生物特征的识别都有其一定的适用范围和要求，单一的生物特征识别系统在实用中显现出各自的局限性，比如各种生物特征识别在普遍性、稳定性、准确性、防伪性以及接受程度等方面都有差别。现在对各种密码系统准确性和安全性的要求不断的提高，显然大多数情况下单一生物特征无法满足实际需要，故将不同特征结合建立基于多重生物特征的公钥系统是必要的。

在单一生物特征下，对消息 m 的签名 (U_i,V_i) 是群 $G = E(F_q)[n]$ 中的元素，经聚合后多重生物特征下的签名 (U,V) 也是该群中的元素。

在签名过程中，由于 *Weil* 对的计算较数乘和点加运算要复杂得多，因此系统的复杂度主要由 *Weil* 对的计算所决定，可以忽略数乘和点加运算，集中考虑在聚合过程中 *Weil* 对计算的变化。显然在给出的多重生物特征数字签名下，若对 n 个签名分别进行验证需要计算 $2n$ 次 *Weil* 对计算，且这些计算只能由验证者完成，若对签名先聚合再验证需要 2 次 *Weil* 对计算，而 *Weil* 对的计算较复杂，聚合签名大大减少 *Weil* 对的运算次数，降低其复杂度，因此，采取聚合的方式压缩多重生物特征身份数据是必要的，通过它形成一个短签名。

8 安全性分析

本文采用生物特征数据构造公钥，并应用于签名方案，与传统的基于证书的公钥密码和基于身份的公钥密码系统相比，生物特征具有更大的安全性。生物特征数据比较大，尤其在多重生物特征下，特征数据有很高的信息熵，可以抵御猜测攻击和字典攻击。

选择消息攻击，即若攻击者 A 获得了签名者 S 的部分生物特征数据 $b_1,b_2,\cdots,b_{n_0-k}$ 而剩余的生物特征数据 b_{n_0-k+1}，$b_{n_0-k+2},\cdots,b_{n_0}$ 是安全的。在上述假设下所得到的有效的攻击算法被称为利用选择消息攻击的存在性伪造方法。如果一个签名方案不存在这样的算法，则可以说该方案是安全的。本方案基于 L.Cha-L.Cheon 方案，该方案在随机预言模型下能抵御利用选择消息进行攻击的存在性伪造。

若攻击者 A 获得了签名者 S 的所有生物特征数据，在不知系统主密钥 s 的情况下，A 只能计算出 S 的公钥 Q^*，无法获得 S 的私钥 d。因此，当签名者的生物特征数据受到破解时，系统的安全性取决于系统主密钥 s 的安全性，它等同于一个标准的基于身份的公钥密码签名系统，而这种系统的安全性已有各种各样的分析论证。

9 结束语

本文利用生物特征构造公钥，将生物特征应用于签名方案中，在各种生物特征下形成的签名，经聚合后形成一个基于多重生物特征身份的聚合签名方案。该方案具有以下特点：(1)聚合签名减少了签名验证的工作量；(2)以签名者的生物特征作为公钥，解决了公钥管理问题；(3)该方案解决了基于单一生物特征签名的局限性，提高了系统的健壮性。下一步工作将研究多重生物特征身份数据的组合应用及其签名方案的可控性。

参考文献

[1] Burnett A. A Biometric Identity-based Signature Scheme[Z]. (2007-12-06). http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4426104.

[2] Dodis Y. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data[J]. SIAM Journal on Computing, 2008, 38(1): 97-139.

[3] Lawrence C. Elliptic Curves: Number Theory and Cryptography[M]. [S. l.]: CRC Press, 2003.

[4] Jand C. An Identity-based Signature from Gap Diffle-Hellman Groups[C]//Proc. of the IEEE Int'l Conf. on Public Key Cryptography. [S. l.]: IEEE Press, 2003.

编辑 陈 文

(上接第 144 页)

[3] Daniel D. On Distributed Fault-tolerant Detection in Wireless Sensor Networks[J]. IEEE Trans. on Computers, 2006, 55(1): 58-70.

[4] Kher S. Distributed Fault Detection of Wireless Sensor Networks[C]//Proc. of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks. Los Angeles, USA: ACM Press, 2006.

[5] Thaeler A. Fault-tolerant Target Detection in Sensor Networks[C]// Proc. of the IEEE Wireless Communications and Networking Conf.. New Orleans, USA: [s. n.], 2005.

编辑 陈 文

(上接第 147 页)

参考文献

[1] 张 燕, 冷文浩, 周 斌. 基于 Struts, Spring 和 Hibernate 的船舶性能系统的设计与实现[J]. 计算机工程与设计, 2008, 29(8): 2121-2124.

[2] 沈海波, 洪 帆. 基于企业环境的访问控制模型[J]. 计算机工程, 2005, 31(14): 144-146.

[3] 李建东, 张 铁, 王中文, 等. 角色访问控制技术在放射治疗中的应用[J]. 计算机工程, 2008, 34(10): 269-270.

编辑 索书志