Identity-Based Digital Signature Scheme with Forward Security

TANG Lei, LIU Yali

College of Computer Science & Technology, Xuzhou Normal University, Xuzhou, China

e-mai: *tangleii@yahoo.com.cn*

Abstract: Combining with forward security, this paper proposes an identity-based digital signature scheme with forward security which makes use of identity-based signature scheme from bilinear pairings defined on elliptic curves. The detailed security analysis shows that the proposed scheme has the feature of correctness, forward-secure and resisting forging attack, which makes the whole signature scheme have certain theoretical and practical values. The security of the scheme is based on the elliptic curve discrete logarithm hard problem of non-super-singular elliptic curve over finite field which has no efficient attack method by now.

Keywords: identity-based; forward security; elliptic curve; bilinear pairings; elliptic curve discrete logarithm

基于身份的前向安全数字签名方案

唐　蕾，刘亚丽

徐州师范大学计算机科学与技术学院，徐州，中国，221116

e-mail: tangleii@yahoo.com.cn

【摘　要】本文利用基于身份和椭圆曲线上双线性对的签名方案，结合前向安全特性，构造了一种基于身份的前向安全数字签名方案。详细的安全性分析表明：新方案具备有效性、前向安全性和抗伪造性等性质，方案的安全性建立在目前还没有有效攻击方法的有限域上非超奇异椭圆曲线离散对数困难问题之上，具有一定的理论和实用价值。

【关键词】基于身份；前向安全；椭圆曲线；双线性对；椭圆曲线离散对数

1 引言

使用证书和证书服务器是目前解决公钥存储的主要手段，它是 PKI 的一个基本组成部分，但使用证书带来了存储和管理开销的问题。为了简化基于证书的公钥体制负担最重的密钥管理过程，减少证书管理开销，1984 年 Shamir 提出了基于身份的公钥密码体制[1]。其基本思想：用户采用姓名、地址、E-mail、身份证号码等身份信息作为其公钥，由一个作为可信第三方的密钥生成中心(Key Generate Center, KGC)为其产生相应的私钥并经过秘密信道传送至该用户。使用基于身份的密码系统，不需要保存每个用户的公钥证书。系统中每个用户都有一个身份，用户的公钥可以由任何人根据其身份计算出来，而私钥则是由可信中心统一生成。自从 Shamir 的开创性工作以来，众多学者对于基于身份的密码系统进行了广泛研究，包括基于身份的加密体制、基于身份的数字签名机制以及基于身份的签密机制等。其中，基于身份的数字签名机制成为数字签名研究领域的一大热点课题，利用椭圆曲线上的 Weil 配对（Weil Pairing）的双线性性质[2]，构造了基于身份的加密方案[3]、基于身份的数字签名方案[4,5]等，其安全性建立在椭圆曲线离散对数困难问题之上。

前向安全数字签名是信息安全风险控制的主要措施之一，目前已成为数字签名的一个重要研究方面。术语“前向安全”最先出于文献［6］，此后，Ross Anderson 提出了前向安全数字签名思想[7]，解决了通常数字签名的一些缺陷：一旦密钥丢失(或被窃取)，由这个密钥生成的以前所有签名都变得无效。前向安全数字签名要求即使对手在盗得当前时段签名密钥的情况下，也不能伪造与密钥被盗前时段相关的数字签名。其思想本质是尽可能减少由于密钥泄露所带来的对系统安全的影响和损失。自 Ross Anderson 将前向安全的性质引入数字签名之后，具有前向安全特性的签名方案也相继出现[8,9]。

本文在基于 Weil 对的短签名方案[10]的基础上，根据椭圆曲线离散对数问题求解的困难性，结合前向安

全特性，利用双线性映射在椭圆曲线上构造了一种基于身份的前向安全数字签名方案。方案通过引入身份信息辅助私钥进化，签名者用带有 ID 信息的时段私钥进行签名；且通过引入参数建立 i 时段签名和 i 时段私钥之间的联系，从而确保签名的前向安全性和抗伪造性，有一定的理论和实用价值。

2 相关知识

2.1 双线性对

假设 G_1，G_2 分别为有限域 F_p 上的椭圆曲线有理点群的加法子群和乘法子群且阶均为大素数 q，在 G_1，G_2 中离散对数问题均是难解的。$P(x, y)$为 G_1 的生成元，称为基点，满足 $qP=O$（O 代表椭圆曲线上的无穷远点）。

双线性映射是指在 G_1 和 G_2 这两个群由椭圆曲线上的 Weil 对派生得到满足下列性质的一个映射 e: $G_1\times G_1\rightarrow G_2$：

1) 双线性性：对任意$P, Q, R\in G_1$，任意$a, b\in Z_q^*$，有$e(P+Q, R)=e(P, R)e(Q, R)$, $e(P, Q+R)=e(P, Q)e(P, R)$, $e(aP, bQ)=e(P, Q)^{ab}$；

2) 非退化性：存在$P, Q\in G_1$，使得$e(P, Q)\neq 1$；

3) 可计算性：对所有的$P, Q\in G_1$，存在一个有效的多项式时间算法计算$e(P, Q)$。

在群G_1上，定义以下几个困难性问题：

1) 椭圆曲线离散对数问题(ECDLP)：给定$P, Q\in G_1$，很难找到一个存在的整数n使得$P=nQ$；

2) 计算Diffie-Hellman问题(CDHP)：给定三元组$(P, aP, bP)\in G_1^3$，对$a, b\in Z_q^*$，计算abP是困难的，不存在多项式时间算法；

3) 决策Diffie-Hellman问题(DDHP)：给定四元组$(P, aP, bP, abP)\in G_1^4$，对于$a, b, c\in Z_q^*$，判断$c=ab \bmod q$是否成立；

4) Gap Diffie-Hellman问题(GDHP)：在素数阶循环群G_1上，DDHP在多项式时间内能被解决，但没有任何可能的多项式时间算法可以解决CDHP，则称群G_1是一个间隙Diffie-Hellman(GDH)群。

2.2 基于身份的数字签名方案

一个基于身份的签名方案由四个算法组成：系统初始化，密钥提取，签名生成和签名验证。系统中包含三方：可信中心、签名者和验证者。

设G_1, G_2, q, e同2.1设置。设ID是一个表示用户身份的一个字符串，H_1, H_2是公开的加密用哈希函数[3]，$H_1:\{0,1\}^*\rightarrow G_1$, $H_2:\{0,1\}^*\times G_2\rightarrow F_q$。

1) 系统初始化(Setup)：可信中心随机选取一个元素$P\in G_1$和一个整数$t\in F_q$。计算$Q_{TA}=tP$，公开(P, Q_{TA})，保密t，t称为系统主密钥，系统中所有用户的私钥均由它生成。

2) 密钥提取(Extract)：当用户需要与他的身份对应的私钥时，向可信中心提出申请。可信中心在验证了用户的身份后给出用户身份所对应的私钥。设用户的身份由一个字符串ID给出，则他的公钥可以使用$Q_{ID}=H_1(\text{ID})$算出，私钥$S_{ID}=tQ_{ID}$。然后通过安全信道将S_{ID}送给用户。用户的密钥对为（Q_{ID}, S_{ID}）。

3) 签名生成(Sign)：为了签名一个消息m，签名者选取$P_1\in G_1$, $k\in F_q$，计算：$r=e(P_1, P)^k$；$v=H_2(m, r)$；$U=vS_{ID}+kP_1$。所得签名是$(U, r)\in(G_1, G_2)$。

4) 签名验证(Verify)：计算$e(U, P)$, $e(Q_{ID}, Q_{TA})^v$，检查验证等式$e(U, P)= e(Q_{ID}, Q_{TA})^v r$是否成立。

此签名方案由文献[4]构造，其安全性依赖于求解群G上Diffie-Hellman问题的困难性，可以证明在(random oracle)模型下是安全的。

2.3 前向安全数字签名方案

前向安全数字签名方案具有一个重要的环节——密钥进化，在签名的整个生命周期内公钥不改变，验证算法和标准签名方案的验证算法相似。因此一个前向安全数字签名方案是一个密钥进化数字签名方案，主要包括以下四个算法：

1) 密钥生成算法：由安全参数k和时间段总数T，生成初始密钥和公钥对(SK_0, PK)。

2) 密钥进化算法：在签名有效期内公钥PK保持不变，而密钥随时段j的变化进行进化更新。记第$j(1\leq j\leq T)$时段的密钥为SK_j，进入j时段时，首先根据$SK_j=f(SK_{j-1})$计算SK_j，这里f是一个单向函数，确保不能由SK_j计算出SK_{j-1}，求得SK_j后立即删除SK_{j-1}。

3) 签名算法：用第$j(1\leq j\leq T)$时段的密钥SK_j对消息m签名，生成第j时段对消息m的签名$(j, Sig(m))$。

4) 验证算法：用公钥PK、消息m来验证一个宣称j时段的签名$(j, Sig(m))$是否确实为j时段的签名密钥SK_j在消息m上的签名。

3 基于身份的前向安全数字签名方案

3.1 系统建立

$G_1, G_2, P(x, y), q, e$: 同 2.1 设置；

H_1: $\{0, 1\}^*\rightarrow G_1$, H_2: $\{0, 1\}^*\rightarrow G_1$ 为两个密码学哈

978-1-935068-06-8 © 2009 SciRes.

希函数；

{G_1, G_2, e, q, P, H_1, H_2:}:系统初始参数。

3.2 密钥生成

1) KGC 选择两个大素数 p_1, $q_1 \in Z_q^*$，令 $N=p_1q_1 \in Z_q^*$；

2) KGC 选择随机数 $s_0 \in Z_q^*$作为系统初始密钥并保密；

3) KGC 计算公钥 $P_{pub} = s_0{}^{q^T} P$，其中 T 为公钥有效期；

4) KGC 公布系统公钥 $PK=\{T, P_{pub}\}$。

3.3 密钥进化

若 $i=T+1$，则 s_i 为空串；

若 $1 \le i \le T$，则 $s_i = s_{i-1}{}^q \pmod N$ 。

KGC 删除系统密钥 s_{i-1}，保密 i 时段的系统密钥 s_i。

3.4 密钥提取

1) 签名者 S 提取其身份信息 ID 给 KGC，KGC 计算 $Q_{ID}=H_1(ID) \in G_1$ 作为 S 的公钥；

2) 在 i 时段，KGC 计算 $S_{IDi}=s_iQ_{ID}$ 作为 S 的私钥，然后通过安全信道将 S_{ID} 送给用户；

3) 用户的密钥对为（Q_{ID}, S_{ID}）。

3.5 签名算法

S 引入一个新的参数 R_i 将 i 时段的签名和该时段的私钥 s_i 建立关联。

1) S 计算 $P_m=H_2(m) \in G_1$；

2) S 计算参数 $R_i = s_iQ_{ID}{}^{q^{T-i}} P_m$；

3) S 计算 $S_m = S_{IDi}{}^{q^{T-i}+1} P$；

4) S 发送 (i, R_i, S_m) 给验证者。

3.6 验证算法

验证者验证：$e(S_mP_m, P) = e(R_iQ_{ID}P, P_{pub})$；

若等式成立，则接受签名；否则，拒绝签名。

4 安全性分析

4.1 有效性

根据方案中的相关等式进行如下有效性验证，考察签名验证中的等式：

$$\begin{aligned} e(S_mP_m, P) &= e(S_{IDi}{}^{q^{T-i}+1} PP_m, P) = e(s_i{}^{q^{T-i}+1} Q_{ID}{}^{q^{T-i}+1} PP_m, P) \\ &= e(s_i s_0{}^{q^T} Q_{ID}{}^{q^{T-i}} Q_{ID} PP_m, P) \\ &= e(s_i Q_{ID}{}^{q^{T-i}} P_m Q_{ID} s_0{}^{q^T} P, P) \\ &= e(R_i Q_{ID} s_0{}^{q^T} P, P) = e(R_i Q_{ID} P, P)^{s_0{}^{q^T}} \\ &= e(R_i Q_{ID} P, s_0{}^{q^T} P) = e(R_i Q_{ID} P, P_{pub}) \end{aligned}$$

由此可得验证等式 $e(S_mP_m, P)=e(R_iQ_{ID}P, P_{pub})$成立，因此签名方案正确，$(i, R_i, S_m)$ 为有效签名。

4.2 前向安全性

本方案采用的密钥进化算法 $s_i = s_{i-1}{}^q \pmod N$ 是单向函数，若想通过此算法求出 i 时段之前的系统密钥是基于求模 n 的 m 方根的难度，其困难性等价于因子分解问题，因此系统密钥 s_i 的进化具有前向安全性。

在签名过程中，即使攻击者盗取了某一时段 i 的私钥 s_i，也最多只能通过密钥进化算法 $s_i = s_{i-1}{}^q \pmod N$ 求出 $i+1$ 时段的私钥 s_{i+1}，进而伪造 $i+1$ 时段的签名而无法伪造 i 时段之前的签名。假设 i 时段的系统密钥 s_i 泄露，攻击者伪造 $j(j<i)$时段的最终签名记为 (j, R_j', S_m')，其中 R_j' 由攻击者通过 $R_j' = s_j' Q_{ID}{}^{q^{T-j}} P_m$ 计算得出(s_j'为攻击者伪造的 j 时段系统密钥)。由于 $s' \ne s_j = s_0{}^{q^j}$，故验证过程无法通过，详细过程见 4.3 抗伪造性分析。

因此，本方案系统密钥 s_i 的进化和 i 时段的签名 (i, R_i, S_m) 均具有真正的前向安全性。

4.3 抗伪造性

参数 R_i 作为签名的重要组成部分在 i 时段公开，由 $R_i = s_iQ_{ID}{}^{q^{T-i}} P_m$ 可知，若想通过 R_i 得到 i 时段的系统密钥 s_i 是基于椭圆曲线离散对数的难题，根本不可行；又由于 $S_{IDi}=s_iQ_{ID}$，如果攻击者通过截取 i 时段的用户密钥 S_{IDi} 想获取系统密钥 s_i 也是基于椭圆曲线离散对数的难题。从而保证了 i 时段的系统密钥 s_i 的双重安全性；同理也不可能通过签名 $S_m = S_{IDi}{}^{q^{T-i}+1} P$ 得到 i 时段的用户密钥 S_{IDi}。

i 时段的最终签名为 (i, R_i, S_m)，由 R_i、S_m 和 S_{IDi} 的公式可知，如果无法知道系统密钥 s_i，则显然不可能得到 i 时段的用户密钥 S_{IDi}，进而也无法构造 i 时段的有效签名 (i, R_i, S_m)；且由验证公式可知，在不知道系统密钥 s_i 的情况下，通过伪造 i 时段的系统密钥 s_i'伪造 i 时段的用户密钥 S_{IDi}'，进而伪造签名 (i, R_i', S_m')，则验证无法通过。

假设攻击者伪造 j 时段的系统密钥 s_j'，通过 $R_j' = s_j' Q_{ID}^{q^{T-j}} P_m$ 构造参数 R_j'，且通过 S_{IDj}'=s_j'Q_{ID} 构造 S_{IDj}'，进而伪造的最终签名记为 (j, R_j', S_m')，但是在验证过程中，由于 $s' \neq s_j = s_0^{q^j}$，所以有

$$\begin{aligned} e(S_m' P_m, P) &= e(S_{IDj}'^{q^{T-j}+1} P P_m, P) = e(s_j'^{q^{T-j}+1} Q_{ID}^{q^{T-j}+1} P P_m, P) \\ &= e(s_j' s_j'^{q^{T-j}} Q_{ID}^{q^{T-j}+1} P P_m, P) \neq e(s_j' s_j^{q^{T-j}} Q_{ID}^{q^{T-j}} Q_{ID} P P_m, P) \\ &= e(s_j' s_0^{q^T} Q_{ID}^{q^{T-j}} Q_{ID} P P_m, P) = e(s_j' Q_{ID}^{q^{T-j}} P_m Q_{ID} s_0^{q^T} P, P) \\ &= e(R_j' Q_{ID} s_0^{q^T} P, P) = e(R_j' Q_{ID} P, P)^{s_0^{q^T}} \\ &= e(R_j' Q_{ID} P, s_0^{q^T} P) = e(R_j' Q_{ID} P, P_{pub}) \end{aligned}$$

因此验证无法通过，故本方案具有抗伪造性。

5 结束语

本方案是在椭圆曲线密码体制的背景下利用前向安全特性构造基于身份的数字签名方案的一个有效尝试。方案同时具备有效性、前向安全性和抗伪造性等性质，其安全性基于有限域上非超奇异椭圆曲线离散对数困难问题，从而确保了整个签名算法的安全性，在电子商务领域得以更加广泛的应用。

Reference (参考文献)

[1] A Shamir. Identity-based cryptosystems and signature schemes [C]. In: Proc Crypto 1984, LNCS, Springer-Verlag, 1985, 196, 47-53.

[2] J H Silverman. The Arithmetic of Elliptic Curves [J]. Graduate Texts in Mathematic, Springer-Verlag, 1986, 106: 96-99.

[3] D Boneh, M Franklin. Identity-Based Encryption from the Weil pairing [C]. In: Proc Crypto 2001, LNCS, Springer-Verlag, 2001, 2139, 213-229.

[4] F Hess. Exponent group signature schemes and efficient identity based signature schemes based on pairing. Available from http://eprint.iacr.org, 2002.

[5] K Paterson. ID-based signatures from pairing on elliptic curves. Available from hhttp://eprint.iacr.org, 2002.

[6] Christoph G G. An identity-based key-exchange protocol [C]. Lecture Notes in Computer Science. Advances in Cryptology EUROCRYPT89, Houthalen, Belgium. New York: Springer-Verlag, 1990, 29-37.

[7] Anderson R. Two remarks on public key cryptology [C]. The Fourth Annual Conference on Computer and Communications Security. New York: ACM Press, 1997, 148-160.

[8] Krawczyk H. Simple forward-secure signatures from any signature scheme [C]. In: Proceedings of the 7th ACM Conference on Computer and Communications Security. Athens, Greece, Nov. 1-4, ACM Press, 2000, 108-115.

[9] Abdalla M, Reyzin L. A new forward-secure digital signature scheme [C]. Advances in Cryptology-ASIACRYPT 2000, T. Okamoto (Ed.), LNCS 1976, Springer-Verlag, 2000, 116-129.

[10] Boneh D, Lynn B and Shacham H. Short signatures from the Weil pairing [C]. In Advance in Cryptology-Asiacrypt'2001, LNCS 2248. Gold Coast, Australia, Springer-Verlag, 2001, 514-532.

978-1-935068-06-8 © 2009 SciRes.