一种不含双线性对的无证书有序多重签名方案*

罗文俊，李长英
（重庆邮电大学 计算机科学与技术学院，重庆 400065）

摘　要：提出了一种不含双线性对的无证书有序多重签名方案，即结合不含双线对运算的无证书签名和有序多重签名的思想。与一般无证书数字签名体制不同的是，不含双线性对运算的无证书密码体制没有复杂的双线性对运算，且在计算效率方面具有明显的优势。最后对方案进行安全分析，能抵抗替换公钥攻击，安全性较高。

关键词：无证书签名；双线性对；离散对数问题；有序多重签名
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2012)04-1427-03
doi:10.3969/j.issn.1001-3695.2012.04.063

Certificateless sequential multi-signature scheme without pairings

LUO Wen-jun, LI Chang-ying
(*College of Computer Science & Technology, Chongqing University of Posts & Telecommunications, Chongqing* 400065, *China*)

Abstract: This paper proposed a certificateless sequential multi-signature scheme without pairings, it combined the theory with certificateless signature without pairings and sequential multi-signature. Compared with the general certificateless digital signature system, certificateless signature scheme without pairings had no heavy cost pairing operation and obvious advantages in the calculation efficiency. Finally, through the security analysis, the signature scheme can resist the attack of the replace public key and the safety is higher.

Key words: certificateless digital signature; bilinear pairing; discrete logarithm problem; sequential multi-signature

0　引言

多重签名是一种由多个签名者合作签署同一个文件的特殊数字签名。它分为两种：若签名时必须严格按照次序进行签名，则有序多重签名；若所有的签名者可以同时对消息签名，则广播多重签名。目前提出的多重签名大多是基于离散对数和身份的[1,2]，其存在证书管理和密钥托管问题，在实际应用中效率较低。

Al-Riyami 等人[3]在 2003 年提出无证书公钥密码学（CL-PKC）。无证书公钥密码体制既能避免基于证书（PKI）公钥密码体制的证书管理问题，又能克服基于身份的公钥密码体制（ID-PKC）的密钥托管问题。无证书密码体制中，用户的私钥由两部分组成：a）用户自己随机选的秘密值；b）PKG 利用用户的身份信息给出的且只能产生用户的部分私钥，这样就不存在传统公钥密码体制的证书管理耗费问题。

无证书签名一经提出就受到广泛关注，即一些无证书方案相继提出[4~12]，但这些方案都是基于椭圆曲线构造，导致付出昂贵的双线性对运算代价。因此，本文在现有的研究基础上[10,11]，利用 Schnorr 签名的思想，将不含双线性对的无证书签名方案与有序多重签名方案相结合，构造了一种新的不含双线性对的无证书有序多重签名方案。因为没有昂贵的双线性对运算代价，相比其他现有的无证书签名方案，效率大大提高。该方案安全性基于离散对数问题的难解性。

1　无证书数字签名体制

1.1　无证书数字签名的一般模型

一个无证书数字签名体制一般由以下四个多项式时间算法组成：

a）系统建立算法。该算法是由 PKG 完成的概率多项式时间算法。

b）密钥生成算法。该算法是由 PKG 和用户合作完成的概率多项式时间算法。

c）签名算法。该算法是由签名用户完成的概率多项式时间算法。

d）验证算法。该算法是由验证者完成的确定性多项式时间算法。

1.2　无证书数字签名的数学基础

设 G_1 与 G_2 为两个阶为 q 的循环群，q 为大素数，其中 G_1 是以加法的形式表示的，G_2 是以乘法的形式表示的，p 为 G_1 的生成元。假设 G_1 和 G_2 这两个群中的离散对数问题都是困难问题。若映射 $e:G_1\times G_1\to G_2$ 满足下列性质，则此映射称为可允许的双线性映射。

1）双线性　对于所有的 $P,Q,R\in G_1$ 和 $a,b\in \mathbf{Z}_q$，有：$e(P+Q,R)=e(P,R)e(Q,R)$，$e(aP,bQ)=e(P,Q)^{ab}=e(abP,Q)$。

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

3）可计算性　对于所有的 $P,Q\in G_1$，存在一个有效的算

收稿日期：2011-08-23；**修回日期**：2011-09-25　　**基金项目**：国家自然科学基金资助项目（60963023）；重庆市自然科学基金资助项目（2010BB2402）

作者简介：罗文俊（1966-），男，重庆人，教授，博士，主要研究方向为信息安全、密码学（luowj@cqupt.edu.cn）；李长英（1985-），女，重庆人，硕士研究生，主要研究方向为信息安全、密码学.

法计算 $e(P,Q)$。

2 没有双线性对运算的无证书签名方案

文献[9]中提出了一个不含双线对运算的无证书签名方案,该方案是基于 Diffie-Hellman 困难问题的。回顾一下文献中的不需要双线性对运算的无证书签名方案,方案描述如下:

a)系统初始化。输入安全参数 k,PKG 产生 p、q 两个素数,且$\frac{q}{(p-1)}$,g 是随机选 Z_p^* 的一个阶为 q 的生成元,PKG 任意选取主密钥 $x\in Z_p^*$,并计算 $y=g^x \bmod p$,选择 hash 函数:

$$H_1:\{0,1\}^*\times Z_p^*\to Z_q^*$$

$$H_2:\{0,1\}^*\times\{0,1\}^*\times Z_p^*\to Z_p^*$$

b)用户密钥提取。输入用户的身份 ID 后,首先 PKG 随机选取 $s\in Z_p^*$,计算 $w=g^s \bmod p$,$d=s+xH_1(\mathrm{ID},w)$,PKG 返回 $D_{\mathrm{ID}}=d$作为用户 ID 的部分私钥,$p_{\mathrm{ID}}=w$ 作为用户 ID 的部分公钥。然后随机选择 $z\in Z_q^*$ 作为用户 ID 的秘密值,则用户的私钥 $SK_{\mathrm{ID}}=(d,z)$,公钥 $PK_{\mathrm{ID}}=(w,u)$。

c)签名算法。输入消息 m,签名者 s 首先验证等式 $g^d=wy^{H_1(\mathrm{ID},w)} \bmod p$ 是否成立,如果不成立,则放弃签名;否则计算 $\sigma=dH_2(m,\mathrm{ID},w)+z \bmod q$ 作为签名。

d)验证算法。验证者接收到对消息 m 的无证书签名 σ 之后,计算 $h_1=H_1(\mathrm{ID},w)$,$h_2=H_2(m,\mathrm{ID},w)$,计算等式 $g^\sigma=u(wy^{h_1})^{h_2} \bmod p$是否成立,若成立则接受;否则拒绝。

3 不含双线性对的无证书有序多重签名方案

本章将不含双线性对的无证书签名与有序多重签名的理论(有序多重签名方案理论在这里就不作介绍)相结合,提出了一种不含双线性对运算的无证书有序多重签名方案。此方案是基于离散对数困难问题的,方案的具体描述如下:

a)系统初始化。输入安全参数 k,PKG 产生 p、q 两个素数,且$\frac{q}{(p-1)}$,g 是随机选 Z_p^* 的一个阶为 q 的生成元,由 g 产生的子群记为 G。PKG 任意选取主密钥 $x\in Z_q^*$,并计算 $y=g^x \bmod p$。选择 hash 函数:

$$H_1:\{0,1\}^*\times Z_p^*\to Z_q \quad H_2:\{0,1\}^*\times Z_p^*\times Z_p^*\to Z_q$$

$$H_3:\{0,1\}^*\times\{0,1\}^*\times(Z_p^*)^4\times Z_q^*\times Z_p^*\to Z_q$$

系统公开参数 $\mathrm{params}=\{p,q,g,G,y,H_1,H_2,H_3\}$,主密钥 $msk=x$。

b)用户密钥提取。有序多重签名中有 i 个用户,其中 $i\in(1,2,\cdots,n)$。第一个用户输入他的身份 ID_1 后,PKG 首先随机选择 $s_1,t_1\in Z_q^*$,然后计算

$$\begin{cases}p_1=g^{s1} \bmod p\\ d_1=s_1+xH_1(\mathrm{ID}_1,p_1) \bmod q\\ Q_1=g^{t1} \bmod p\\ T_1=t_1+xH_2(\mathrm{ID}_1,p_1,Q_1) \bmod q\end{cases}$$

对于 $i\in(2,3,\cdots,n)$的用户,首先输入他们的身份 ID_i,然后 PKG 随机选择 $s_i,t_i\in Z_q^*$,计算:

$$\begin{cases}p_i=p_{i-1}\cdot g^{si} \bmod p\\ d_i=s_i+xH_1(\mathrm{ID}_i,p_i) \bmod q\\ Q_i=Q_{i-1}\cdot g^{ti} \bmod p\\ T_i=t_i+xH_2(\mathrm{ID}_i,p_i,Q_i) \bmod q\end{cases}$$

PKG 返回用户的部分私钥 $D_{\mathrm{ID}_i}=d_i$,用户的部分公钥 $p_{\mathrm{ID}_i}=(p_i,Q_i,T_i)$。用户随机选取 $z_i\in Z_q^*$,并输出 $s_{\mathrm{ID}_i}=z_i$ 作为用户的秘密值。输出用户的私钥 $SK_{\mathrm{ID}_i}=(D_{\mathrm{ID}_i},s_{\mathrm{ID}_i})=(d_i,z_i)$,用户的公钥 $PK_{\mathrm{ID}_i}=(P_{\mathrm{ID}_i},\mu_i)=(p_i,Q_i,T_i,g^{zi})$,然后公开用户的公钥。

签名验证者 V 随机选择一个素数 $k_v\in Z_q^*$,计算$f_v=g^{k_v} \bmod p$,公开 f_v 给所有的签名者,当签名者产生 S_i 的公钥 $PK_{\mathrm{ID}_i}=(P_{\mathrm{ID}_i},\mu_i)=(p_i,Q_i,T_i,g^{zi})$,那么他计算 $F_i=f_v^{t_i} \bmod p$ 并发送 F_i 给签名验证者,验证者验证等式

$$\begin{cases}F_i=(Q_{i-1}^{-1}\cdot Q_i)^{k_v} \bmod p\\ Q_i^{k_v} \bmod p\neq 1 \bmod p\end{cases}$$

是否成立,如果上述等式成立,则证明用户的公钥没有被替换,用户可以申请签名;否则中止签名请求。

c)签名算法。输入消息 m,给定系统参数 params、签名者的身份 ID_i 以及对应的公钥 $PK_{\mathrm{ID}_i}=(p_i,Q_i,T_i,\mu_i)$,签名者 S_i 完成下面的签名:

(a)签名者 $S_i(i\in(1,2,\cdots,n)$首先验证下面两个等式:$g^{T_{i-1}}\cdot Q_{i-2}=Q_{i-1}\cdot y^{H_2(\mathrm{ID}_{i-1},p_{i-1},Q_{i-1})} \bmod p$(其 $Q_0=1$)是否成立,如果不成立,则放弃签名;否则签名者 S_i 随机选取两个整数 $r_i,r'_i\in Z_q^*$,计算 $c_i=g^{ri} \bmod p$,$c'_i=g^{r'i} \bmod p$。然后令 $u_i=H_3(m,\mathrm{ID}_i,c_i,c'_i,PK_{\mathrm{ID}_i})$。计算 $v_i=r_i-u_iz_i \bmod q$,$w_i=r'_i-u_id_i \bmod q$,并发送对消息 m 的签名 $\sigma_i=(u_i,v_i,w_i)$给下一个签名者。

(b)当签名者 $S_i(i\in(2,3,\cdots,n)$收到 S_{i-1} 对消息 m 的无证书签名 $\sigma_{i-1}=(u_{i-1},v_{i-1},w_{i-1})$后,则首先验证等式 $u_{i-1}=H_3(m,\mathrm{ID}_{i-1},g^{v_{i-1}}\mu_{i-1}^{u_{i-1}},g^{w_{i-1}}(p_{i-1}y^{H_1(\mathrm{ID}_{i-1},p_{i-1})})^{u_{i-1}},PK_{\mathrm{ID}_{i-1}})$是否成立,如果等式成立,则接受;否则拒绝。

d)验证算法。给定系统参数 params、签名者的身份 ID_i 以及对应的公钥 $PK_{\mathrm{ID}_i}=(p_i,Q_i,T_i,\mu_i)$,当所有的签名者完成了对消息 m 的签名,最后一个签名者 S_n 将对消息 m 的无证书签名 $\sigma_n=(u_n,v_n,w_n)$发送给签名验证者 V,系统验证者 V 收到签名后,验证下面两个等式:

$$g^{T_n}\cdot Q_{n-1}=Q_n\cdot y^{H_2(\mathrm{ID}_n,p_n,Q_n)} \bmod p$$

$$u_n=H_3(m,\mathrm{ID}_n,g^{v_n}\mu_n^{u_n},$$

$$g^{w_n}(p_ny^{H_1(\mathrm{ID}_n,p_n)})^{u_n},PK_{\mathrm{ID}_n})$$

如果上述两个等式成立,则输出接受,此方案的多重签名有效;否则无效拒绝。

4 方案的安全性分析

4.1 正确性证明

签名者 S_1 的公钥如下:

$$PK_{\mathrm{ID}_1}=(P_{\mathrm{ID}_1},\mu_1)=(p_1,Q_1,T_1,g^{z1})=$$

$$(g^{s1},g^{t1},t_1+xH_2(\mathrm{ID}_1,p_1,Q_1),g^{z1})$$

签名者 $S_i(i\in(2,3,\cdots,n))$的公钥如下:

$$PK_{\mathrm{ID}_i}=(P_{\mathrm{ID}_i},\mu_i)=(p_i,Q_i,T_i,g^{zi})=$$

$$(p_{i-1},g^{si},Q_{i-1}\cdot g^{t1},t_1+xH_2(\mathrm{ID}_i,p_i,Q_i),g^{zi})$$

所有签名者的签名如下:

$$\begin{cases}c_i=g^{ri} \bmod p,c'_i=g^{r'i} \bmod p\\ u_i=H_3(m,\mathrm{ID}_i,c_i,c'_i,PK_{\mathrm{ID}_i})\\ v_i=r_i-u_iz_i \bmod q\\ w_i=r'_i-u_id_i \bmod q\end{cases}$$

验证等式如下:

$$g^{T_{i-1}} \cdot Q_{i-2} = Q_{i-1} \cdot y^{H_2(\mathrm{ID}_{i-1}, p_{i-1}, Q_{i-1})} \bmod p \tag{1}$$

$$u_{i-1} = H_3(m, \mathrm{ID}_{i-1}, g^{v_{i-1}} \mu_{i-1}^{u_{i-1}}, g^{w_{i-1}}(p_{i-1} y^{H_1(\mathrm{ID}_{i-1}, p_{i-1})})^{u_{i-1}}, PK_{\mathrm{ID}_{i-1}}) \tag{2}$$

1)证明式(1)

$$g^{T_{i-1}} \cdot Q_{i-2} = g^{t_{i-1} + xH_2(\mathrm{ID}_{i-1}, p_{i-1}, Q_{i-1})} \cdot Q_{i-2} = g^{t_{i-1}} \cdot Q_{i-2} \cdot g^{xH_2(\mathrm{ID}_{i-1}, p_{i-1}, Q_{i-1})} = (g^{t_{i-1}} \cdot Q_{i-2})(g^x)^{H_2(\mathrm{ID}_{i-1}, p_{i-1}, Q_{i-1})} = Q_{i-1} \cdot y^{H_2(\mathrm{ID}_{i-1}, p_{i-1}, Q_{i-1})} \bmod p$$

2)证明式(2)

$$c_{i-1} = g^{r_{i-1}} = g^{v_{i-1} + u_{i-1} z_{i-1}} = g^{v_{i-1}} \cdot (g^{z_{i-1}})^{u_{i-1}} = g^{v_{i-1}} \mu_{i-1}^{u_{i-1}}$$

所以等式 $u_{i-1} = H_3(m, \mathrm{ID}_{i-1}, g^{v_{i-1}} \mu_{i-1}^{u_{i-1}}, g^{w_{i-1}}(p_{i-1} y^{H_1(\mathrm{ID}_{i-1}, p_{i-1})})^{u_{i-1}}, PK_{\mathrm{ID}_{i-1}})$ 成立。

如果所有签名者在所提供的条件下对消息 m 签名,那么下面两个等式

$$g^{T_n} \cdot Q_{n-1} = Q_n \cdot y^{H_2(\mathrm{ID}_n, p_n, Q_n)} \bmod p$$

$$u_n = H_3(m, \mathrm{ID}_n, g^{v_n} \mu_n^{u_n}, g^{w_n}(p_n y^{H_1(\mathrm{ID}_n, p_n)})^{u_n}, PK_{\mathrm{ID}_n})$$

将成立。

3)证明等式

$$\begin{cases} F_i = (Q_{i-1}^{-1} \cdot Q_i)^{k_v} \bmod p \\ Q_i^{k_v} \bmod p \neq 1 \bmod p \end{cases}$$

在签名前,系统验证者通过验证等式 $F_i = \mu_i^{k_v} \bmod p$ 是否成立来验证用户公钥正确性,证明如下:

$$F_i = f_v^{t_i} \bmod p = (g^{k_v})^{t_i} \bmod p = (g^{t_i})^{k_v} \bmod p$$

$$(Q_{i-1}^{-1} \cdot Q_i)^{k_v} = (Q_{i-1}^{-1} \cdot Q_{i-1} \cdot g^{t_i})^{k_v} = (g^{t_i})^{k_v} \bmod p$$

综上而知,方案的正确性显然成立。

4.2　抵抗替换公钥攻击

替换公钥攻击:攻击者不知道系统主密钥,但可以替换用户公钥,抽取可信中心生成的部分私钥或者直接获得签名密钥,然后发出签名请求。如果攻击者已经替换了用户的公钥,此时向签名预言发出签名请求,则签名预言机返回的签名将是不正确的,因为将不给定任何额外的假设,此时如同随机预言模型。但是如果攻击者发出签名请求的同时又将已替换的公钥和相应的秘密信息也发送给签名预言机,那么假设预言器的回答是正确的。

如果攻击者令 $Q_i = Q_{i-1} \cdot g^{at_i} \bmod p$, $T_i = at_i + xH_2(\mathrm{ID}_i, p_i, Q_i)$,则替换签名者的公钥如下:

$$PK_{\mathrm{ID}_i} = (P_{\mathrm{ID}_i}, \mu_i) = (p_i, Q_i, T_i, g^{z_i}) = (p_{i-1} \cdot g^{S_i}, s_i + xH_1(\mathrm{ID}_i, p_i), Q_{i-1} \cdot g^{at_i}, at_i + xH_2(\mathrm{ID}_i, p_i, Q_i), g^{z_i})$$

则签名者验证等式 $g^{T_i} \cdot Q_{i-1} = Q_i \cdot y^{H_2(\mathrm{ID}_i, p_i, Q_i)} \bmod p$ 是否成立。证明如下:

$$g^{T_i} \cdot Q_{i-1} = g^{at_i + xH_2(\mathrm{ID}_i, p_i, Q_i)} \cdot Q_{i-1} = g^{at_i} \cdot Q_{i-1} \cdot g^{xH_2(\mathrm{ID}_i, p_i, Q_i)} = (g^{at_i} \cdot Q_{i-1})(g^x)^{H_2(\mathrm{ID}_i, p_i, Q_i)} = Q_i \cdot y^{H_2(\mathrm{ID}_i, p_i, Q_i)} \bmod p$$

通过上面的证明,等式 $g^{T_i} \cdot Q_{i-1} = Q_i \cdot y^{H_2(\mathrm{ID}_i, p_i, Q_i)} \bmod p$ 成立,所以通过替换公钥实现攻击。

签名者公开他们的公钥 $PK_{\mathrm{ID}_i} = (p_i, Q_i, T_i, \mu_i)$ 后,系统验证者验证等式 $\begin{cases} F_i = (Q_{i-1}^{-1} \cdot Q_i)^{k_v} \bmod p \\ Q_i^{k_v} \bmod p \neq 1 \bmod p \end{cases}$ 是否成立。

证明等式 $F_i = (Q_{i-1}^{-1} \cdot Q_i)^{k_v}$。

$$F_i = f_v^{t_i} \bmod p = (g^{k_v})^{t_i} \bmod p = (g^{t_i})^{k_v} \bmod p (Q_{i-1}^{-1} \cdot Q_i)^{k_v} = (Q_{i-1}^{-1} \cdot Q_{i-1} \cdot g^{at_i})^{k_v} = (g^{at_i})^{k_v}$$

通过证明而知,$F_i \neq (Q_{i-1}^{-1} \cdot Q_i)^{k_v}$,故等式 $\begin{cases} F_i = (Q_{i-1}^{-1} \cdot Q_i)^{k_v} \bmod p \\ Q_i^{k_v} \bmod p \neq 1 \bmod p \end{cases}$ 不成立,则驳回签名请求。

通过验证签名者公钥的正确性来抵抗替换公钥攻击。签名者公开他们的公钥 $PK_{\mathrm{ID}_i} = (p_i, Q_i, T_i, \mu_i)$ 后,系统验证者用等式 $\begin{cases} F_i = (Q_{i-1}^{-1} \cdot Q_i)^{k_v} \bmod p \\ Q_i^{k_v} \bmod p \neq 1 \bmod p \end{cases}$ 来验证公钥的正确性。如果上面的等式成立,则用户的公钥有效,没有被替换,就发出签名请求;否则终止请求。

5　结束语

尽管人们在双线性映射的技术复杂性和如何提高其计算速度方面已做了大量工作,但双线性对运算仍然是已知最复杂的密码操作。在同等安全级下(椭圆曲线上 160 bit 的群元素等同于 1 024 bit RSA 安全级别),运行一次双线性对所需的时间约为有限域上指数运算的 10 倍。本文将不含双线性对运算的无证书签名与有序多重签名的思想结合,提出一种不含双线性对的无证书有序多重签名方案。本文方案虽然在公钥长度和签名长度等方面有所增加,但与一般的无证书签名相比,大大降低了计算效率,因为一般的无证书签名运用的是双线性对密码体制。另外,本文方案能有效地抵抗替换公钥攻击,具有较强的安全性。

参考文献

[1] 张骏. Li-Yang 多重签名方案的安全性分析及改进[J]. 计算机工程与应用,2009,45(20):125-128,139.

[2] 于佳,郝蓉,孔凡玉,等. 标准模型下的前向安全多重签名:安全模型和构造[J]. 软件学报,2010,21(11):2920-2932.

[3] A1-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]//Advances in ASIACRYPT 2003, vol 2894. Berlin: Springer-Verlag, 2003: 452-473.

[4] 洪东招,谢琪. 有效的无证书签名[J]. 计算机应用,2010,30(7):1809-1811.

[5] BARBOSA M, FARSHIM P. Certificateless signcryption [C]//Proc of ACM Symposium on Information, Computer and Communications Security. New York: ACM Press,2008: 369-372.

[6] TSO R, YI Xun, HUANG Xin-yi. Efficient and short certificateless signature [C]//Proc of the 7th International Conference on Cryptology and Network Security. Berlin: Springer-Verlag, 2008: 64-79.

[7] ZHANG Lei, ZHANG Fu-tai. Certificateless signature and blind signature[J]. Journal of Electronics,2008,25(5): 629-636.

[8] HUANG Xin-yi, MU Yi, SUSILO W, *et al*. Certificateless signature revisited[C]//Proc of the 12th Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2007: 308-322.

[9] 王会歌,王彩芬,李泳斌,等. 没有 pairing 的无证书公钥签名方案[J]. 计算机应用,2008,28(6):1395-1397.

[10] BACK J, SAFAVI-NAINI R, SUSILO W. Certificateless public key encryption without pairing[C]//Proc of the 8th Information Security Conference. Berlin: Springer-Verlag, 2005: 134-148.

[11] SUN Yin-xia, ZHANG Fu-tai, BACK J. Strongly secure certificateless public key encryption without pairing[C]//Proc of the 6th International Conference on Cryptology and Network Security. Berlin: Springer-Verlag, 2007: 194-208.

[12] 刘景伟,孙蓉,马文平. 高效的基于 ID 的无证书签名方案[J]. 通信学报,2008,29(2):87-94.