第34卷 第20期 计 算 机 工 程 2008年10月
Vol.34 No.20 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)20—0164—03 文献标识码：A 中图分类号：TP393

基于身份的无可信中心门限环签名方案

李 琥，何明星，罗大文
(西华大学数学与计算机学院，成都 610039)

摘 要：已有的多数基于身份的门限环签名方案不能克服密钥托管问题，而能克服密钥托管问题的基于身份的无可信中心签名方案存在效率不高的缺陷。该文利用分布式秘密共享思想和双线性对，提出一个有效的基于身份的无可信中心门限环签名方案。该方案能保证不诚实的PKG无法伪造环签名，有效避免了密钥托管问题。同时该方案只需要2次对运算，比已有的门限环签名方案和无可信中心的基于身份的签名方案效率更高。

关键词：环签名；秘密共享；门限环签名；双线性对；密钥托管

ID-based Threshold Ring Signature Scheme Without Trusted Party

LI Xiao, HE Ming-xing, LUO Da-wen
(School of Mathematics and Computer Engineering, Xihua University, Chengdu 610039)

【Abstract】 Most previous ID-based threshold ring signatures cannot give over the problem of key escrow. Whereas, the ID-based ring signatures which can get over the problem of key escrow have some drawback of low efficiency. In this paper, the thought of distributed secret sharing and bilinear parings are adopted, and an efficient ID-based threshold ring signature scheme without a trusted party is proposed. The proposed scheme can ensure that the dishonest Private Key Generator(PKG) cannot impersonate the ring members to sign a message. The problem of key escrow can be avoided availably. The proposed scheme only needs two bilinear parings. It is more efficient than the previous schemes of ID-based threshold ring signature and ID-based signature without trusted party.

【Key words】 ring signature; secret sharing; threshold ring signature; bilinear parings; key escrow

1 概述

随着电子商务、电子选举、电子彩票等广泛应用，对签名者的隐私要求越来越高。为了更好地保护签名者的隐私，2001年，Rivest等[1]第一次提出环签名方案。它是一种新的匿名签名技术，对于签名者而言是无条件匿名的，它因签名参数由一定的规则首尾相连形成一个环而得名。环签名的签名验证者能验证环签名的有效性，并能确定签名者是环中成员，但无法确定签名者的具体身份。即使是Private Key Generator(PKG)也不能通过签名来确定签名者的具体身份。因此，环签名能保证签名者的身份无条件隐藏。

近年来，基于身份的密码体制是密码学研究的一个热点问题。这种密码体制思想是由Shamir[2]于1984年首次提出来的，其目的是为了简化PKI的密钥管理以及取消公钥证书的使用。它将用户的个人信息(如姓名、身份证号、E-mail地址、电话号码等)作为个人的公钥，这样用户就不再需要公钥证书，从而提高了管理的效率和系统的安全性。基于身份的密码体制有一个天生的缺陷，那就是密钥托管问题。成员的私钥由可信的PKG生成，PKG知道所有成员的私钥，并能假冒某个成员进行签名，因此大多数基于身份的密码体制总是假设PKG绝对可信。为了避免密钥托管问题，许多无可信中心的基于身份的密码协议[3-5]相继被提出。

2004年Sherman S. M. Chow利用双线性对提出了基于身份的门限环签名方案[6]，该方案需要$n+1$次对运算。2006年，张士兵等提出了一种新的基于身份的双线性对门限环签名方案[7]，该方案是对Chow的方案[6]进行改进，只需要2次对运算。然而文献[6-7]都不能避免密钥托管问题。

大多数基于身份的签名方案[3-7]都利用了双线性对(bilinear pairings)运算，而算法的时间复杂度也主要取决于对运算的多少，因此要提高基于身份的密码方案的有效性关键在于如何尽可能地减少对运算的次数。

2 双线性映射的性质及几个数学问题

2.1 双线性映射的性质

设q是一个大素数，G_1和G_2分别为q阶加法循环群和乘法循环群。映射$\hat{e}:G_1\times G_2\to G_2$具有如下性质：

(1)双线性：对所有$P,Q\in G_1$，$\alpha,\beta\in Z_q$，有

$\hat{e}(\alpha P,\beta Q)=\hat{e}(P,Q)^{\alpha\beta}$

(2)非退化性：存在$P,Q\in G_1$，使得

$\hat{e}(P,Q)\neq 1$

(3)可计算性：对任意的$P,Q\in G_1$，存在有效算法计算$\hat{e}(P,Q)$。

2.2 几个数学问题

(1)离散对数问题(DLP)：已知P,Q，寻找$n\in z_q^*$，使

基金项目：国家自然科学基金资助项目(60473030)；四川省教育厅自然科学预研基金资助项目(2004c015)

作者简介：李 琥(1972－)，男，副教授、硕士，主研方向：密码学，信息安全；何明星，教授、博士；罗大文，讲师、硕士

收稿日期：2007-11-06 **E-mail：**lxgbxh@126.com

$Q=nP$。

(2)决定性 Diffie-Hellman 问题(DDHP)：已知 P,aP,bP,cP，$a,b,c\in Z_q^*$，确定 $c=ab \bmod q$ 是否成立。

(3)计算性 Diffie-Hellman 问题(CDHP)：已知 P,aP,bP，$a,b\in Z_q^*$，计算 abP。

3 有效的无可信中心基于身份的门限环签名方案

3.1 参数设置

设 $(G_1,+)$, $(G_2,.)$ 是 2 个阶为素数 q 的循环群，P 是 G_1 的生成元。$H(.)$ 和 $H_0(.)$ 是 2 个安全的哈希函数，$H:\{0,1\}^*\to G_1$，$H_0:\{0,1\}^*\to Z_q^*$。$\hat{e}$ 是一个映射：

$\hat{e}:G_1\times G_1\to G_2$。

PKG 随机选取 $s\in_R Z_p^*$ 作为主密钥，并计算公钥 $P_{pub}=sP$。系统公钥为

$\{G_1,\ G_2,\ \hat{e}(.,.),\ q,\ P,\ P_{pub},\ H(.),\ H_0(.)\}$

3.2 密钥生成过程

n 个环成员首先利用分布式秘密共享的方式共享一个 $r\in Z_q^*$，具体做法如下：

每个环成员 ID_i 任选一个函数

$f_i(x)=R_i+a_{i,1}x+\cdots+a_{i,\ t-1}x^{t-1} \bmod q$

其中，$R_i,a_{i,1},\cdots,a_{i,t-1}\in_R Z_q^*$。

ID_i 计算 $R_{ij}=\ f_i(j) \bmod q$，$j=1,2,\cdots,n$。

ID_i 把 R_{ij} 安全地发送给 ID_j，并公开 $R_iP,a_{i,1}P,\cdots,a_{i,t-1}P$。

ID_i 收到 R_{ji} 后验证 $R_{ji}P=R_jP+\sum_{k=1}^{t-1}i^k a_{j,\ k}P$ 是否成立，如果成立则接受 R_{ji}。

ID_i 计算 $r_i=\sum_{i=1}^{n}R_{ji} \bmod q$，并公开 r_iP。则 n 个环成员间就共享了 $r=\sum_{i=1}^{n}l_ir_i$ 和 $rP=\sum_{i=1}^{n}l_ir_iP$，其中 $l_i=\sum_{j=1,j\neq i}^{n}\frac{-i}{j-i}$。$r_i$ 作为环成员 ID_i 的签名部分私钥。

环成员 ID_i 向 PKG 提交其身份 ID_i，$rP=\sum_{i=1}^{n}l_ir_iP$ 和 r 的使用期限 T，PKG 计算 $Q_{ID_i}=H(ID_i\|T,rP)$，环成员的公钥为 (Q_{ID_i},rP)。PKG 计算 $S_{ID_i}=sQ_{ID_i}$ 作为环成员的私钥，并把 S_{ID_i} 安全地发送给环成员，则环成员 ID_i 的签名私钥为 $(S_{ID_i},\ r_i)$。

3.3 签名过程

假设 n 个环成员构成的集合为 $A=\{ID_1,ID_2,\cdots,ID_n\}$。不失一般性，假设实际签名人集合为 $B=\{ID_1,ID_2,\cdots,ID_t\}$。签名算法描述如下：

(1)对集合 A/B 中成员 ID_k $(k=t+1,t+2,\cdots,n)$，任选 $U_k\in G_1,\ h_k\in Z_q^*$。

(2)集合 B 中成员其中一个 ID_i 任选 $x_i\in Z_q^*$，计算 $U_i=x_iP-\sum_{j=t+1}^{n}(U_j+h_jQ_{ID_i})$；集合 B 中其余成员 ID_j 任选 $x_j\in Z_q^*$ $(j=1,2,\cdots,t,\ j\neq i)$，并计算 $U_j=x_jP$。

(3)集合 B 中成员计算 $h_0=H_0(A,t,m,\bigcup_{k=1}^{n}\{U_k\},T,rP)$，并利用 h_0 及 $h_k(k=t+1,t+2,\cdots,n)$ 构造一个 $n-t$ 次多项式 $f(x)\in Z_q[x]$，使得

$f(0)=h_0$，$f(k)=h_k$，$\ k=t+1,t+2,\cdots,n$

(4)集合 B 中成员 ID_i，计算

$h_i=f(i)\ \ i=1,2,\cdots,t$

(5)集合 B 中成员 ID_i 计算

$V_i=h_iS_{ID_i}+(x_i+l_ir_i)P_{pub}$，$\ i=1,2,\cdots,t$

其中，$l_i=\sum_{j=1,j\neq i}^{t}\frac{-i}{j-i}$。

(6)计算 $V=\sum_{i=1}^{t}V_i$，则门限环签名为

$\sigma=\{A,t,m,\bigcup_{k=1}^{n}U_k,f,V,T,rP\}$

3.4 验证过程

(1)签名验证者首先计算 $h_0=H_0(A,t,m,\bigcup_{k=1}^{n}\{U_k\},T,rP)$，验证 $f(x)$ 是否为 $n-t$ 次多项式，并且 h_0 是否为 $f(x)$ 的常数项。如果不成立，则拒绝该签名。

(2)签名验证者计算 $h_k=f(k),\ k=1,2,\cdots,n$。

(3)验证 $\hat{e}(P,V)=\hat{e}(P_{pub},rP+\sum_{i=1}^{n}(U_i+h_iQ_{ID_i})$ 是否成立，如果成立，则门限环签名 σ 为有效签名，否则为无效签名。

4 正确性、安全性及有效性分析

4.1 正确性

$$\hat{e}(P,V)=\hat{e}(P,\sum_{j=1}^{t}V_j)=$$

$$\hat{e}(P,\sum_{j=1}^{t}(h_js_{ID_j}+(x_i+l_ir_i)P_{pub})=$$

$$\hat{e}(P,\sum_{j=1}^{t}h_js_{ID_j})\hat{e}(P,\sum\nolimits_{j=1}^{t}(x_i+l_ir_i)P_{pub}))=$$

$$\hat{e}\ (P_{pub},\sum_{j=1}^{t}h_jQ_{ID_j})\ \hat{e}(P_{pub},\sum_{j=1}^{t}(x_i+l_ir_i)P)$$

而

$$\hat{e}(P_{pub},\sum_{j=1}^{t}(x_i+l_ir_j)P)=\hat{e}(P_{pub},\sum_{j=1}^{t}x_iP)\hat{e}(P_{pub},(\sum_{j=1}^{t}l_jr_j)P)=$$

$$\hat{e}(P_{pub},\sum_{j=1}^{t}x_iP)\hat{e}(P_{pub},rP)=$$

$$\hat{e}(P_{pub},(\sum_{j=1,j\neq i}^{t}x_jP)+x_iP)\hat{e}(P_{pub},\ rP)=$$

$$\hat{e}(P_{pub},\sum_{j=1}^{n}U_j+\sum_{j=t+1}^{n}h_jQ_{ID_j}))\hat{e}(P_{pub},rP)=$$

$$\hat{e}(P_{pub},\ rP+\sum_{j=1}^{n}U_j+\sum_{j=t+1}^{n}h_jQ_{ID_j})$$

故 $\hat{e}(P,V)=\ \hat{e}\ (P_{pub},\sum_{j=1}^{t}h_jQ_{ID_j})\ \hat{e}(P_{pub},\sum_{j=1}^{t}(x_i+l_ir_i)P)=$

$$\hat{e}(P_{pub},\ rP+\sum_{j=1}^{n}(U_j+h_jQ_{ID_j}))$$

4.2 安全性分析

(1)签名者的签名私钥 S_{ID_i} 和 r_i 对其他签名者不会泄漏。首先，在密钥生成过程中，其他环成员 ID_j $(j\neq i)$ 不能从 r_iP 中解得 r_i，这是 DLP 离散对数问题。即使是 $t-1$ 个环成员合谋也无法得到其他签名者的部分签名私钥 r_i。其次，在签名过程中，由于 $x_i\in Z_q^*$ 是任选的，B 中环成员无法从 V_i 中确定出 $h_iS_{ID_i}$ 和 $(x_i+l_ir_i)P_{pub}$，从而无法解出 S_{ID_i} 和 r_i。因此在环签名过程中，签名者的签名私钥 S_{ID_i} 和 r_i 对其他签名者不会泄漏。

(2)签名者的签名部分私钥 r_i 对 PKG 是保密的。在密钥生成过程中 PKG 无法独立地从 rP 中得到 r_iP，即使是他能腐蚀 $t-1$ 个环成员得到 $r_iP=l_i^{-1}(rP-\sum_{j=1,j\neq i}^{t}l_jr_jP)$，由 DLP 离散对数困难性问题知，他无法解出 r_i 来。在签名过程中，虽然 PKG 知道所有环成员的签名私钥 S_{ID_i}，但由于 x_i 是任取的，即使

PKG 能腐蚀 $t-1$ 个环成员，PKG 也不能从 $(x_i+l_ir_i)P=V_i-h_iS_{ID_i}$ 中得到 r_iP。事实上，PKG 能猜到 r_i 的概率仅为 $\frac{1}{q}$。

(3)门限环签名签名不可伪造性。

1)不诚实的 PKG 不能伪造合法的门限环签名。

本方案采用的是门限方案，总是假定攻击者最多能腐蚀 $t-1$ 个合法环成员，从而最多能得到 $t-1$ 个签名私钥 (S_{ID_i},r_i)。

定理 1 不诚实的 PKG 如果能腐蚀 $t-1$ 个环成员并能伪造一个合法的门限环签名，则 PKG 具有求解 DLP 离散对数的能力。因此不诚实的 PKG 无法伪造合法的门限环签名。

证明：假设不诚实的 PKG 能利用 $t-1$ 个签名私钥 (S_{ID_i},r_i) 伪造出一个有效的门限环签名：

$$\sigma'=\{A,t,m',\bigcup_{k=1}^{n}U_k',f',V',T,rP\}$$

不失一般性，假设不诚实的 PKG 腐蚀了环成员 $ID_1,ID_2,\cdots,ID_{t-1}$，并假冒 ID_t 进行签名，这里签名人集合仍记为 $B=\{ID_1,ID_2,\cdots,ID_t\}$。不诚实的 PKG 对选择的消息 m' 进行伪造签名，步骤如下：

① 对集合 A/B 中成员 ID_k $(k=t+1,t+2,\cdots,n)$，任选 U_k',h_k'。

② 集合 B 中成员 ID_t 任选 $x_t'\in Z_q^*$，计算 $U_t'=x_t'P-\sum_{j=t+1}^{n}(U'+h_j'Q_{ID_i})$；集合 B 中其余成员 ID_j 任选 $x_j'\in Z_q^*$ $(j=1,2,\cdots,t-1)$，计算 $U_j'=x_j'P$。

③集合 B 中成员计算 $h_0'=H_0(A,t,m',\bigcup_{k=1}^{n}\{U_k'\},T,rP)$，并利用 h_0' 及 h_k' $(k=t+1,t+2,\cdots,n)$ 构造一个 $n-t$ 次多项式 $f'(x)\in Z_q^*[x]$，使得

$$f'(0)=h_0',\ f'(k)=h_k',\ k=t+1,t+2,\cdots,n$$

④集合 B 中成员 ID_i，计算 $h_i'=f'(i),\ i=1,2,\cdots,t$。

⑤集合 B 中成员 ID_i 计算 $V_i'=h_i'S_{ID_i}+(x_i'+l_ir_i)P_{pub}$，$i=1,2,\cdots,t-1$，其中，$l_i=\sum_{j=1,j\neq i}^{t}\frac{-i}{j-i}$。成员 ID_t 计算 $V_t'=h_t'S_{ID_t}+(x_t'+l_tr_t')P_{pub}$。

⑥计算 $V'=\sum_{i=1}^{t}V'$，则伪造的门限环签名为

$$\sigma'=\{A,t,m',\bigcup_{k=1}^{n}U_k',f',V',T,rP\}$$

假设 $\sigma'=\{A,t,m',\bigcup_{k=1}^{n}U_k',f',V',T,rP\}$ 是一个合法的签名，即 $\hat{e}(P,V')=\hat{e}(P_{pub},rP+\sum_{i=1}^{n}(U'+h_i'Q_{ID_i})$ 成立。则

$$\hat{e}(P,(\sum_{i=1}^{t-1}l_ir_iP_{pub}+l_tr_t'P_{pub}))=\hat{e}(P_{pub},(\sum_{i=1}^{t}l_ir_i+l_tr_t')P)=\hat{e}(P_{pub},rP)$$

否则 σ' 不能通过验证。故不诚实的 PKG 能伪造一个 $r_t'=r_t$ 使得 $l_tr_t'P=l_tr_tP=rP-\sum_{i}^{t-1}l_ir_iP$。

从而 PKG 就能找到一个合适的 r'，使得 $r'P=rP$。换句话说 PKG 能从 rP 中解出 r 来，从而 PKG 具有求解 DLP 离散对数的能力。

由 DLP 离散对数困难性问题知，不诚实的 PKG 不能从 rP 中解出 r 来，因此不诚实的 PKG 是不能伪造有效的门限环签名。事实上找到一个 r' 使得 $r'P=rP$ 的概率等于猜到 r 的概率，仅等于 $\frac{1}{q}$。

因此，提出的方案能有效地防止不诚实的 PKG 伪造环签名，从而有效地避免了密钥托管问题。

2)非法用户或攻击者 C 不能伪造门限环签名。

定理 2 攻击者 C 如果腐蚀 $t-1$ 个合法环成员，并能伪造一个有效的门限环签名，则攻击者 C 具有求解 DLP 离散对数的能力。因此攻击者 C 不能伪造门限环签名方案。

(4)不可否认性

由于提出的方案能保证环签名不可伪造性，故一旦出现合法的环签名，环成员不能否认该签名是 t 个环成员代表整个环所签的名。

4.3 有效性分析

提出的无可信中心基于身份的门限环签名方案是高效的。在签名和验证过程中共使用了 $4n$-1 次G_1加法运算，$2n+2t$ 次G_1乘法运算，在签名过程中没有对运算，在验证过程中只有 2 个对运算，(其中，n为环成员的个数，t为门限值)比门限方案SLS方案[6]和Z-W方案[7]更有效。

提出的方案既是门限方案，同时又能有效地克服密钥托管问题。目前能克服密钥托管问题的基于身份的签名方案中效率最高的LXQ方案[4]只使用了 3 次对运算，而提出的无可信中心的门限环签名方案只使用了 2 次对运算，因此本文的方案效率更高。提出的方案与其他方案在效率方面的具体比较见表 1 和表 2。

表 1 本文方案与其他门限环签名方案的比较

	SLS方案[6]	Z-W方案[7]	本文方案
G_1加法运算	$3n$	$4n$-1	$4n$-1
G_1乘法运算	$4n$	$4n$	$2n+2t$
G_2乘法运算	n-1	0	0
对运算	n+1	2	2
能否避免密钥托管问题	不能	不能	能

表 2 本文方案与其他无可信中心的签名方案的比较

	CZK方案[3]	LXQ方案[4]	CL-RSS方案[5]	本文方案
签名过程中使用的对运算	0	0	$2n$-1	0
验证过程中使用的对运算	4	3	$3n$+1	2
是否能避免密钥托管问题	能	能	能	能

5 结束语

本文提出了有效的无可信中心门限环签名方案，该方案既是 (t,n) 门限方案，又能有效地克服密钥托管问题。提出的方案是安全的，签名者的签名私钥不会泄漏，同时该方案不能伪造，除了门限值t个合法用户外，其他非法用户，包括PKG也不能生成有效的门限环签名。提出方案在签名和验证过程中共使用了 $4n$-1 次G_1加法运算，$2n+2t$次G_1乘法运算，在签名过程中没有对运算，在验证过程中只有 2 个对运算，比已有基于身份的门限环签名方案和无可信中心的基于身份的环签名方案效率更高。

参考文献

[1] Rivest R L, Shamir A, Tauma Y. How to Leak a Secret[C]//Proc. of ASIACRYPT'01. [S. l.]: Springer, 2001: 552-565.

[2] Shamir A. Identity-based Cryptosystems and Signature Schemes [C]//Proc. of CRYPTO'84, LNCS 196. Berlin, Germany: Springer, 1984: 47- 53.

(下转第 169 页)