第 39 卷 第 12 期
Vol.39 No.12

计 算 机 工 程
Computer Engineering

2013 年 12 月
December 2013

• 安全技术 •

文章编号：1000—3428(2013)12—0141—03 文献标识码：A 中图分类号：TP309.2

无双线性对的无证书分布环签名方案

张春生[1]，苏本跃[1]，姚绍文[2]

(1. 安庆师范学院计算机与信息学院，安徽 安庆 246133；2. 云南大学软件学院，昆明 650091)

摘 要：现有分布环签名方案大多基于双线性对运算或模指运算，计算效率不高。针对该问题，提出一种无双线性对运算和模指运算的无证书分布环签名方案，只进行椭圆曲线上的模乘运算。通过复杂度分析结果证明该方案是高效的，仅需 $2s+3t-2$ 次模乘运算(t 表示存取结构中子集的个数，s 表示实际签名子集中成员的个数)，并且若方案存取结构中所有子集的成员数均设为某一门限值，该方案即成为无证书门限环签名方案。

关键词：分布环签名；无证书；计算性 Diffie-Hellman 问题；无双线性对运算；存取结构；门限环签名

Certificateless Distributed Ring Signature Scheme Without Bilinear Pairing

ZHANG Chun-sheng[1], SU Ben-yue[1], YAO Shao-wen[2]

(1. School of Computer and Information, Anqing Normal University, Anqing 246133, China;
2. School of Software, Yunnan University, Kunming 650091, China)

【Abstract】The previous distributed ring signature schemes need bilinear pairing operation or exponent operation, and their computation efficiency is not high. For improving the efficient of operations, a new certificateless distributed ring signature scheme without bilinear pairings operation or exponent operation is proposed. The scheme only needs a modular multiplication on elliptic curves. The results of complexity analysis show that the proposed scheme is efficient, and it only needs $2s+3t-2$ modular multiplication(t is the number of subsets of access structure, s is the number of members of actual signing subset). In addition, the scheme becomes a certificateless threshold ring signature scheme when the number of all subsets members of access structure is set to a certain threshold value.

【Key words】distributed ring signature; certificateless; Computational Diffie-Hellman Problem(CDHP); operation without bilinear pairing; access structure; threshold ring signature

DOI: 10.3969/j.issn.1000-3428.2013.12.030

1 概述

无证书公钥密码体制[1]是由第三方密钥生成中心(Key Generation Center, KGC)生成用户的部分私钥和部分公钥，用户的私钥是由用户选择一个秘密值和这个部分私钥共同生成。因此，它既解决了传统公钥密码体制中对证书的使用和验证过程，又解决了基于身份的密码系统[2]的私钥托管问题，极大地提高了系统的运行效率。

分布环签名推广了个人环签名[3]和门限环签名[4]。在环签名中，签名是由用户群组中某一个签名者生成；在门限环签名中，签名是由群组中不少于某个门限值的用户合作生成的，验证者可以验证签名是由这个群组中不少于门限值的用户共同产生，但无法知道具体的签名参与者；在分布环签名中，由用户群组构成若干个能够产生签名的子集，每一个子集都可以匿名地代表所有子集(群组)产生签名，验证者可以验证签名是由所有子集中的某一个子集签署，但无法确认具体是哪一个子集。文献[5]构造了 2 种基于身份的分布环签名方案，但方案无法克服私钥托管问题。文献[6]构造了 2 种无证书的分布环签名方案，但方案采用了双线性对运算，效率不高。文献[7]构造了面向授权子集环签名方案，但方案没有给出所采用的密码体制，并采用了模指数运算，效率不高。根据文献[8]执行一个 512 位 Tate pairing 需要花费 20 ms，而一个 1 024 位素数模指数操作却只需要 8.80 ms。运行一次双线性对操作的时间至少是椭圆曲线上点乘运算的 20 倍以上[9]。因此，无双线性对运算和指数运算的方案具有更高的效率。本文提出一个无双线性对运算和模指运算的无证书分布环签名方案，它无需双线性对运算和指数运算，既极大地提高了效率，又能满足环签名的

基金项目：安徽省高校省级自然科学基金资助项目(KJ2011B077)

作者简介：张春生(1968－)，男，讲师、硕士，主研方向：密码学，网络与信息安全；苏本跃、姚绍文，教授、博士

收稿日期：2012-10-26 **修回日期：**2012-12-18 **E-mail：**zhangchsh2000@126.com

安全需求。

2 相关知识

2.1 困难问题

计算性 Diffie-Hellman 问题(Computational Diffie-Hellman Problem, CDHP)：G 为 q 阶的循环加法群，P 为 G 中 q 阶的生成元，对任意的 $a,b\in Z_q^*$，给定 $aP,bP\in G$，计算 abP。离散对数问题(Discrete Logarithm Problem, DLP)：G 为 q 阶的循环加法群，P 为 G 中 q 阶的生成元，对任意的 $a\in Z_q^*$，给定 $P,aP\in G$，计算 a。

2.2 无证书密码体制的攻击类型

参照文献[10]给出了 2 种类型的无证书公钥密码系统敌手：

(1)攻击者可以查询用户公钥或替换合法用户的公钥，但不知道系统主密钥和用户的私钥。

(2)攻击者可以获得系统主密钥，但不知道用户的私钥，也不能同时替换合法用户公钥。

定义 在 2 种类型敌手的攻击下，若攻击者能在多项式时间内，以不可忽略的概率输出一个关于消息 m 和 Γ 存取结构的有效签名，则称攻击成功。

3 新的无证书分布环签名方案

3.1 方案描述

假设所有用户集合 $U=\{U_1,U_2,\cdots,U_n\}$ 构成一个群组，由群组中若干个用户构成的可产生正确环签名的子集为 $\Gamma_i=\{U_1,U_2,\cdots,U_{n_i}\}(n_i\prec n)$，由 Γ_i 构成一个新的集合 $\Gamma=\{\Gamma_1,\Gamma_2,\cdots,\Gamma_t\}$ 称为存取结构，$\Gamma_i\subseteq U(i=1,2,\cdots,t)$ 可以匿名地代表 Γ 联合计算签名，验证者可以验证签名是由 Γ 中的某一个 Γ_i 签署，但无法确认真正的签名子集。

(1)系统参数建立。k 为输入安全参数，生成 2 个大素数 p、q，且 $q|p-1$。G 为循环加法群，P 为 G 中 q 阶的生成元，选择 2 个安全 Hash 函数 $H_1:\{0,1\}^*\times G\to Z_q^*$、$H_2:\{0,1\}^*\to Z_q^*$，$m$ 为明文消息，KGC 随机选择主密钥 $z\in Z_q^*$，计算 $P_0=zP$，公开系统参数 (p,q,P,P_0,H_1,H_2)，系统主密钥 z 保密。

(2)用户部分密钥的生成。输入用户身份 ID_i，KGC 随机选择 $d_i\in Z_q^*$，计算 $Y_i=d_iP$、$Q_i=H_1(ID_i,Y_i)$、$y_i=d_i+zQ_i$，Y_i 为用户的部分公钥，y_i 为用户的部分私钥，y_i 通过安全渠道传给用户 ID_i，ID_i 通过等式 $Y_i+H_1(ID_i,Y_i)P_0=y_iP$ 是否成立判断部分私钥是否有效。

(3)用户私钥生成。用户 ID_i 随机选择一个 $x_i\in Z_q^*$ 作为自己的秘密值，计算 $X_i=x_iP$，生成用户私钥 $SK_i=(x_i,y_i)$，公钥 $PK_i=(X_i,Y_i)$。

(4)联合公钥集的生成。Γ_i 中的用户共同计算 Γ_i 的联合公钥 $L_i=\sum_{U_j\in\Gamma_i}(X_j+Y_j+Q_jP_0)$，则存取结构 Γ 的联合公钥集为 $L=(L_1,L_2,\cdots,L_t)$。

(5)签名过程。具体如下：1)假设 $\Gamma_s=\{U_1,U_2,\cdots,U_{n_s}\}$ 匿名地代表 Γ 计算签名，$\Gamma_s\in\Gamma$，Γ_s 中的一个成员如 U_1 随机选取不同的 $r_i\in Z_q^*(i=1,2,\cdots,t,i\neq s)$，计算并广播 $R_i=r_iP$，则 Γ_s 中每一个成员都可计算 $h_i=H_2(\Gamma,m,R_i)$。2) Γ_s 中的每一个成员 $U_j\in\Gamma_s\ (j=1,2,\cdots,n_s)$ 随机选取不同的 $a_j\in Z_q^*$，计算并广播 $A_j=a_jP$，则 Γ_s 中的每一个成员均可计算 $R_s=\sum_{j=1}^{n_s}A_j-\sum_{i=1,i\neq s}^{t}h_iL_i$、$h_s=H_2(\Gamma,m,R_s)$。3) Γ_s 中每一个成员计算并广播 $\omega_j=h_s(x_j+y_j)P(j=1,2,\cdots,n_s)$，则 Γ_s 中任一成员均可计算：

$$\sigma=\sum_{j=1}^{n_s}A_j+\sum_{j=1}^{n_s}\omega_j+\sum_{i=1,i\neq s}^{t}R_i \tag{1}$$

Γ_s 对消息 m 的签名为：

$$(\Gamma,m,L,R_1,R_2,\cdots,R_t,h_1,h_2,\cdots,h_t,\sigma)$$

(6)验证过程。验证者对 $(i=1,2,\cdots,t)$ 依次验证 $h_i=H_2(\Gamma,m,R_i)$：

$$\sigma=\sum_{i=1}^{t}h_iL_i+\sum_{i=1}^{t}R_i \tag{2}$$

若方案的存取结构 $\Gamma=\{\Gamma_1,\Gamma_2,\cdots,\Gamma_t\}$ 中所有子集 $\Gamma_i(i=1,2,\cdots,t)$ 的成员数 $|\Gamma_i|$ 相等且为某一门限值 τ 时，即 $|\Gamma_i|=\tau$，上述方案即成为无证书门限环签名方案。

3.2 方案分析

3.2.1 正确性分析

如果签名子集中每一个成员都按照上述协议执行，$h_i=H_2(\Gamma,m,R_i)$ 显然成立。

下面为式(2)的具体证明过程：

$$\begin{aligned}\sigma&=\sum_{j=1}^{n_s}A_j+\sum_{j=1}^{n_s}\omega_j+\sum_{i=1,i\neq s}^{t}R_i=\\&\sum_{j=1}^{n_s}A_j+\sum_{j=1}^{n_s}h_s(x_j+y_j)P+\sum_{i=1,i\neq s}^{t}R_i=\\&\sum_{j=1}^{n_s}A_j-\sum_{i=1,i\neq s}^{t}h_iL_i+\sum_{i=1,i\neq s}^{t}h_iL_i+\\&\sum_{j=1}^{n_s}h_s(x_j+y_j)P+\sum_{i=1,i\neq s}^{t}R_i=\\&R_s+\sum_{i=1,i\neq s}^{t}h_iL_i+\sum_{j=1}^{n_s}h_s(x_j+y_j)P+\sum_{i=1,i\neq s}^{t}R_i=\\&R_s+\sum_{i=1,i\neq s}^{t}h_iL_i+h_sL_s+\sum_{i=1,i\neq s}^{t}R_i=\\&\sum_{i=1}^{t}h_iL_i+\sum_{i=1}^{t}R_i\end{aligned}$$

由式(2)可以得出，验证者可以验证签名是由存取结构

Γ 中的某一个 Γ_i 签署，但无法确认真正的签名子集。

3.2.2 安全性分析

安全性分析具体如下：

(1)无条件匿名性(参照文献[11]中的证明方法)

定理 1 将散列函数视作随机问答器，方案满足无条件匿名性，即对由所有用户集合 U 所产生的可能签名子集合 $\Gamma=\{\Gamma_1,\Gamma_2,\cdots,\Gamma_t\}$，验证者能正确猜出实际签名子集的概率不大于 $1/t$。

证明：一方面，对 $\Gamma_i\subseteq U\left(i=1,2,\cdots,t\right)$，猜测联合公钥 L_i 是等概率的，猜测出 L_i 的概率为 $1/t$。另一方面，对任一签名子集 $\Gamma_s\in\Gamma$ 中的成员所选取的 $r_i\in Z_q^*(i=1,2,\cdots,t,i\neq s)$ 是随机选取的，则计算 R_i 的概率为 $\frac{1}{q-1}\times\frac{1}{q-2}\times\cdots\times\frac{1}{q-t+1}$。另外，$\Gamma_s$ 中的成员选取 a_j 也是随机选取的，计算 R_s 的概率为 $\frac{1}{q-t}$。因此，计算 $R_i\left(i=1,2,\cdots,t\right)$ 的概率为 $\frac{1}{q-1}\times\frac{1}{q-2}\times\cdots\times\frac{1}{q-t+1}\times\frac{1}{q-t}$。因此，对任意的 $\Gamma_i\subseteq U\left(i=1,2,\cdots,t\right)$ 能正确计算实际签名子集的概率不超过 $1/t$，方案满足无条件匿名性。

(2)不可伪造性

文献[11]利用 Forking 引理证明了无证书的环签名方案的安全性，文献[12]通过 Forking 引理证明了一般环签名的安全性。本文方案采用的是分布环签名方案，考虑一种强攻击，假定攻击者是不诚实的 KGC，具有系统主密钥，也可以计算用户的部分私钥 y_i，并且 KGC 腐蚀了实际签名子集 Γ_s 中的 $\left|\Gamma_s\right|-1$ 个成员($\left|\Gamma_s\right|$ 表示 Γ_s 中成员的个数)。

定理 2 假如不诚实的 KGC 腐蚀了实际签名子集 Γ_s 中的 $\left|\Gamma_s\right|-1$ 个成员，并能伪造一个合法的分布环签名，则 KGC 具有求解离散对数问题的能力。因此，不诚实的 KGC 无法伪造合法的分布环签名。

证明：为了描述方便，假设不诚实的 KGC 假冒实际签名子集 Γ_s 中的 U_1 进行签名，他可以计算该用户的部分私钥 y_1，因此，可设 KGC 用来假冒签名的私钥为 $SK_c=(x_c,y_1)$，并能利用其余 $\left|\Gamma_s\right|-1$ 个用户的私钥 $SK_i=(x_i,y_i)$，伪造出一个有效的分布环签名，则利用 Forking 引理能得到 2 个有效无证书的分布环签名：

$$(\Gamma,m,L,R_1,R_2,\cdots,R_t,h_1,h_2,\cdots,h_t,\sigma)$$

$$(\Gamma,m,L,R_1,R_2,\cdots,R_t,h_1',h_2',\cdots,h_t',\sigma')$$

由 $\sigma=\sum_{j=1}^{n_s}A_j+\sum_{j=1}^{n_s}\omega_j+\sum_{i=1,i\neq s}^{t}R_i$、$\sigma'=\sum_{j=1}^{n_s}A_j+\sum_{j=1}^{n_s}\omega_j'+\sum_{i=1,i\neq s}^{t}R_i$ 两式相减得到：

$$\sigma-\sigma'=\sum_{j=1}^{n_s}\omega_j-\sum_{j=1}^{n_s}\omega_j'=$$

$$h_s(x_1+y_1)P+\sum_{j=2}^{n_s}h_s(x_j+y_j)P-$$

$$(h_s(x_c+y_1)P+\sum_{j=2}^{n_s}h_s(x_j+y_j)P)=$$

$$h_s(x_1+y_1)P-h_s(x_c+y_1)P=$$

$$h_s(x_1-x_c)P$$

$$h_s^{-1}(\sigma-\sigma')=(x_1-x_c)P \tag{3}$$

从式(3)中求解 x_1，则 KGC 具有求解离散对数问题的能力，因此，不诚实的 KGC 无法伪造合法的分布环签名。

3.2.3 效率分析

由于系统建立、用户密钥生成的时间开销不大，而且可以通过预处理来完成，因此本文方案的效率分析主要考虑签名和验证 2 个阶段。为了对比方便，假设用来对比的方案选取同样的存取结构 $\Gamma=\{\Gamma_1,\Gamma_2,\cdots,\Gamma_t\}$，实际进行签名的子集均为 $\Gamma_s=\{U_1,U_2,\cdots,U_{n_s}\}$，用 $\left|\Gamma_s\right|$ 表示 Γ_s 中成员的个数。与文献[6-7]方案的复杂度比较见表 1。

表 1 本文方案与文献[6-7]方案的复杂度比较

方案	模乘运算	模指运算	双线性对运算
文献[6]方案	$2\left\|\Gamma_s\right\|+3t-2$	0	$3n+1$
文献[7]方案	$2\left\|\Gamma_s\right\|^2+2\left\|\Gamma_s\right\|+t-2$	$\left\|\Gamma_s\right\|+2t-2$	0
本文方案	$2\left\|\Gamma_s\right\|+3t-2$	0	0

由表 1 可得，文献[6]需要进行 $2\left|\Gamma_s\right|+3t-2$ 次模乘(t 表示存取结构中子集的个数，s 表示实际签名子集中成员的个数)和 $3n+1$ 双线性对运算，文献[7]需进行 $2\left|\Gamma_s\right|^2+2\left|\Gamma_s\right|+t-2$ 次模乘和 $\left|\Gamma_s\right|+2t-2$ 次模指运算，而本文方案无需对运算和模指运算，仅需要 $2\left|\Gamma_s\right|+3t-2$ 次模乘运算，是目前已知方案中效率最高的。

4 结束语

本文提出了一种高效的无证书分布环签名方案，方案规避了双线性对运算和模指运算，只需要模乘运算，通过对系统的效率分析表明方案是高效的。如何设计标准模型下无双线性对运算的无证书分布环签名方案是下一步研究的方向。

参考文献

[1] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography[C]//Proc. of ASIACRYPT'03. [S. l.]: Springer-Verlag, 2003.

[2] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]//Proc. of CRYPTO'84. New York, USA: Springer, 1984.

(下转第 147 页)