文章编号: 1000-8608(2007)03-0429-04

# 基于椭圆曲线密码体制的 $(t, n)$门限群签名方案

刘 文 琦*, 魏 蕾, 杨 建 华

(大连理工大学 电子与信息工程学院, 辽宁 大连 116024)

**摘要:** 针对网络通信中很多门限群签名协议存在不具备不可冒充性、追查签名成员方法复杂及稳定性差等问题, 提出了一个基于椭圆曲线密码体制的门限群签名方案, 并对其进行了安全性分析. 该方案具有如下特点: 通过引入成员的真实身份、化名及参与签名者的化名集合, 使得方案具有不可冒充性和可追查性, 且实现方式较为简洁; 通过间接分配群私钥, 能够方便添加和注销群成员, 只需更新一些公开参数; 方案基于椭圆曲线密码体制, 具有密钥长度短、运算开销小的优点.

**关键词:** 密码学; 门限群签名; 椭圆曲线
**中图分类号:** TP309 **文献标识码:** A

## 0 引 言

门限群签名是门限密码学的重要组成部分, 其概念是由 Boyd[1]、Desmedt等[2]引入的. 门限群签名的主要目标是将团体的签名密钥以 $(t, n)$ 门限方案的方式分散给多人管理, 由他们合作行使签名权力. 门限群签名具有如下优点[3,4]: (1) 攻击者若想得到签名密钥, 必须至少得到 $t$ 个子密钥, 这是困难的; (2) 即使某些成员不合作, 不愿意出示子密钥, 或者泄漏、篡改子密钥, 或者丢失子密钥都不会影响签名消息的认证与恢复; (3) 实现权力分配, 避免滥用职权.

目前, 人们已经提出了许多门限群签名方案[5-7], 但这些方案大多存在以下的问题: (1) 不具有不可冒充性, 群组内各小组产生的门限群签名没有区别, 可以相互冒充; (2) 实现事后追查参与签名成员的方法复杂, 计算量和信息的交互量都比较大; (3) 系统稳定性差, 当注销成员时, 需要重新分配其他成员的子密钥, 并更改相应的公开信息.

针对以上问题, 本文提出一个基于椭圆曲线密码体制的门限群签名方案.

## 1 方案的描述

该方案分为 3个阶段: 系统初始化阶段、门限群签名的产生阶段、门限群签名的验证阶段. 由一个可信中心 $TC$、$n$ 个签名者和一个签名合成者 $C$ 来共同实施.

### 1.1 系统初始化阶段

该方案的安全参数如下:

a 可信中心 $TC$ 选取有限域 $F_q$ 上一条安全的椭圆曲线 $E(F_q)$, 保证该椭圆曲线的离散对数问题是难解的. 在 $E(F_q)$ 上选一基点 $G$, $G$ 的阶数为 $l$($l$ 为一个大素数). 然后选择一个安全的单向 Hash函数 $h(x)$.

b. 令 $Q = \{P_1, P_2, \cdots, P_n\}$ 是 $n$ 个签名者的集合, $TC$ 选择随机数 $b_i \in \{1, 2, \cdots, l-1\}$, 计算 $ID_i = b_i \cdot G$, 确保当 $i \neq j (i, j = 1, 2, \cdots, n)$ 时, $ID_i \neq ID_j$, 并且 $(ID_i)_x \neq (ID_j)_x$, 带有下标 $x$ 表示该点的横坐标. 将 $b_i$ 作为 $P_i$ 的真实身份, $ID_i$ 作为 $P_i$ 的化名.

c. $TC$ 随机选取 $X_Q \in \{1, 2, \cdots, l-1\}$ 作为群组 $Q$ 的私钥, 公钥 $Y_Q = X_Q \cdot G$. $TC$ 随机选择 $n$

收稿日期: 2005-09-25; 修回日期: 2007-03-22
作者简介: 刘文琦* (1973-), 女, 副教授; 杨建华 (1958-), 男, 教授.

个不同的元素 $c_i \in \{1, 2, \cdots, l-1\}$, 作为 $P_i$ 的子密钥, 然后 $TC$ 随机产生 $t-1$ 次多项式

$$f(x) = X_Q + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \bmod l \tag{1}$$

计算

$$Y_i = f((ID_i)_x) \cdot G; \quad i = 1, 2, \cdots, n \tag{2}$$

$$d_i = f((ID_i)_x) - (c_i \cdot G)_x \bmod l, \quad i = 1, 2, \cdots, n \tag{3}$$

d $TC$ 将 $b_i$、$c_i$ 秘密发送给 $P_i$. 将 $E(F_q)$、$G$、$l$、$Y_Q$、$Y_i$、$ID_i$、$d_i$ 存放于公告栏, 这些数据任何人都可以访问, 但不能更改.

**1.2** 门限群签名的产生阶段

假设组 $Q$ 中 $t$ 个签名者, 不妨设为 $Q_t = \{P_1, P_2, \cdots, P_t\}$, 同意对消息 $m$ 签名, 签名步骤如下:

a 每个 $P_i \in Q_t$ 选取随机数 $k_i \in \{1, 2, \cdots, l-1\}$, 计算并公开 $K_i = k_i \cdot G$, 计算部分签名

$$s_i = k_i h(m \| ASID \| K_x) + b_i + L_i(d_i + (c_i \cdot G)_x) \pmod l \tag{4}$$

其中

$$L_i = \prod_{j \in Q_t, j \neq i} [-(ID_j)_x ((ID_i)_x - (ID_j)_x)^{-1}], K = \sum_{j \in Q_t} K_j = (K_x, K_y)$$

$ASID$ 表示参与此次签名的所有签名者的化名集合. 然后将 $s_i$ 传送给签名合成者 $C$.

b $C$ 收到所有的 $s_i (i = 1, 2, \cdots, t)$ 后, 查询公告栏中对应的公开信息, 计算

$$L_i = \prod_{j \in Q_t, j \neq i} [-(ID_j)_x ((ID_i)_x - (ID_j)_x)^{-1}]$$

$$K = \sum_{j \in Q_t} K_j = (K_x, K_y)$$

验证

$$s_i \cdot G = h(m \| ASID \| K_x) \cdot K_i + ID_i + L_i \cdot Y_i \tag{5}$$

若上式不成立, 则要求 $P_i$ 重新发送 $s_i$ 或终止协议过程. 若成立, 则计算

$$ID = \sum_{i \in Q_t} ID_i \tag{6}$$

$$S = \sum_{i \in Q_t} s_i \bmod l \tag{7}$$

则消息 $m$ 的门限群签名是 $(S, ID, K, ASID)$.

**1.3** 门限群签名的验证阶段

验证者验证等式

$$S \cdot G = h(m \| ASID \| K_x) \cdot K + ID + Y_Q \tag{8}$$

若等式成立, 则说明信息 $m$ 的门限群签名 $(S, ID, K, ASID)$ 是有效的.

式(8)证明如下:

$$S = \left(\sum_{i \in Q_t} k_i\right) \cdot h(m \| ASID \| K_x) + \sum_{i \in Q_t} b_i + \sum_{i \in Q_t} L_i (d_i + (c_i \cdot G)_x) \pmod l = \left(\sum_{i \in Q_t} k_i\right) \times h(m \| ASID \| K_x) + \sum_{i \in Q_t} b_i + X_Q \pmod l$$

根据 Lagrange插值公式

$$S \cdot G = h(m \| ASID \| K_x) \cdot \left(\sum_{i \in Q_t} k_i \cdot G\right) + \sum_{i \in Q_t} b_i \cdot G + X_Q \cdot G = h(m \| ASID \| K_x) \times \left(\sum_{i \in Q_t} K_i\right) + \left(\sum_{i \in Q_t} ID_i\right) + Y_Q = h(m \| ASID \| K_x) \cdot K + ID + Y_Q$$

证毕

## 2 方案性能分析

本方案除了具有门限特性和群特性以外, 同时具有以下特点:

a 本方案既保证了匿名性, 又实现了不可冒充性和可追查性. 当签名合成者利用式(5)对部分签名进行验证, 或者验证者利用式(8)对门限群签名进行验证时, 由于式(5)和(8)仅仅涉及了签名者的化名, 签名合成者及验证者均不能确定对应的成员是谁, 此方案具有匿名性. 完成式(4)所示部分签名时, 需要 $b_i$, 这一项是由 $TC$ 分配的, 在该群组中标识每个签名者的真实身份, 之所以在每个群组中选择一个随机数对应该签名者的真实身份, 是为了防止常用的标识身份的身份证号、姓名等被其他签名者盗用而冒充该签名者进行签名, $b_i$ 是每个签名者秘密特有的, 其他人没有这个参数, 不能伪造这个签名者的部分签名, 由此保证了签名的不可冒充性.

签名完成后, 事后追查参与签名的成员时, 首先由 $ASID$ 得出参与签名的签名者的化名, 再根据可信中心处保留的化名与真实身份的对应关系, 即可得出哪些成员参与了这次签名, 实现可追查性. 现有方案中实现可追查性的方法多与文献[8]的方法类似: 生成一个 $t$ 次多项式作为身份识

别函数, 这样的方法使得方案变得复杂, 计算量和信息交互量都较大. 相比较而言, 本文利用化名和化名集合 $ASID$ 实现可追查性的方法更为简洁.

b. 该方案的稳定性有所改进. 增加成员时, $TC$ 为该成员分发子密钥和真实身份标志, 计算该成员的公开信息并添加到公告栏. 当删除某个成员时, $TC$ 只需重新选择群私钥及 $t-1$次多项式, 然后计算并更新其他成员的公开信息即可.

增加成员 $P_{n+1}$时, $TC$ 只需为 $P_{n+1}$随机生成一个子密钥 $c_{n+1}$和一个秘密身份标志 $b_{n+1}$, 计算

$$ID_{n+1} = b_{n+1} \cdot G \tag{9}$$

$$Y_{n+1} = f((ID_{n+1})_x) \cdot G \tag{10}$$

$$d_{n+1} = f((ID_{n+1})_x) - (c_{n+1} \cdot G)_x \bmod l \tag{11}$$

然后增加公告栏信息: $ID_{n+1}$, $Y_{n+1}$, $d_{n+1}$, 不需更改其他用户的信息.

当系统需要删除某个成员 $P_k$时, $TC$ 重新选择一个群私钥 $x_Q'$和 $t-1$次多项式 $f'(x)$, 满足 $f'(0) = x_Q'$, 计算$Y_Q' = x_Q' \cdot G$. 然后利用新的 $f'(x)$计算

$$Y_i' = f'((ID_i)_x) \cdot G;\quad i = 1, 2, \cdots, n,\ i \neq k \tag{12}$$

$$d_i' = f'((ID_i)_x) - (c_i \cdot G)_x \bmod l,\quad i = 1, 2, \cdots, n,\ i \neq k \tag{13}$$

更新公告栏信息 $(Y_i', d_i',\ i = 1, 2, \cdots, n,\ i \neq k)$, 并更新群公钥 $Y_Q'$. 此时不更改或删除 $d_k$, 则 $P_k$的子密钥失效.

目前的方案中在删除成员时必须重新分配其他所有成员的子密钥, 并更新相应公开信息, 才能使被删除成员的子密钥无效. 在本方案中, 无需更改其他成员的秘密信息, 只更新公开信息即可. 这样提高了方案的稳定性, 而且减少了秘密信息的交互量.

c. 该方案在保证系统数据信息安全性的基础上, 充分发挥了椭圆曲线密码系统密钥长度短、效率高的优势. 基于椭圆曲线的密码体制[9, 10]是目前已知的公钥体制中, 对每一比特所提供加密强度最高的一种体制, 具有安全性高、密钥量小、灵活性好的特点. 因此, 本方案的算法更加简洁、高效.

## 3　安全性分析

该方案的安全性基于求解有限域上椭圆曲线离散对数问题的困难性和 Shamir门限方案的安全性.

a. 该方案中攻击者无法通过式 (4) 中的 $s_i$求得子密钥 $c_i$, 因为 $k_i$、$b_i$都是未知的, 由此不可能求出 $(c_i \cdot G)_x$, 而且即使得到了 $c_i \cdot G$的横坐标, 也不可能求出 $c_i$, 这等价于求解椭圆曲线密码的离散对数问题. 同样, 基于离散对数的难解性, 也无法由公开信息 $K_i$、$ID_i$、$Y_i$ $(i = 1, 2, \cdots, n)$、$Y_Q$求得随机数 $k_i$、秘密身份标志 $b_i$、签名者私钥 $x_i$和群私钥 $X_Q$.

b. 该方案具有防欺骗性, 能够识别出欺骗者. 成员提交部分签名 $s_i$后, 签名合成者根据式 (5) 对 $s_i$进行验证, 若等式不成立, 说明该成员未提供正确的签名, 即为欺骗者.

c. 本方案能够抵抗伪造攻击. 分析式 (8) 所示的验证方程, $Y_Q$是由 CA 公正过的群公钥, 是固定的. 若攻击者想伪造一个门限群签名, 给定$m'$、$ASID'$、$ID'$, 代入式 (8) 得

$$S \cdot G = h(m' \| ASID') \cdot K + ID' + Y_Q \tag{14}$$

求满足式 (14) 的 $S$和$K$ 是困难的, 这面临着求解椭圆曲线离散对数问题. 反之, 若给定 $S'$和 $K'$, 代入式 (8) 得

$$S' \cdot G = h(m \| ASID) \cdot K' + ID + Y_Q \tag{15}$$

计算满足上式的 $m$、$ASID$、$ID$, 需要进行 Hash函数的逆运算, 这在计算上是不可行的. 同样, 对式 (4) 进行分析, 部分签名也是不可伪造的. 因此, 该方案能够抵抗伪造攻击.

d. 本方案能够抵抗合谋攻击. 任意少于 $t$个签名者无法重构多项式 $f(x)$, 也就不能得到群组的私钥 $X_Q$和 $f((ID_i)_x)$ $(i = 1, 2, \cdots, n)$, 不能伪造门限群签名. 当合谋者达到 $t$个时, 他们能够重构多项式 $f(x)$, 进而得到群组的私钥 $X_Q$和 $f((ID_i)_x)$ $(i = 1, 2, \cdots, n)$, 但是由于这 $t$个成员没有其他成员的真实身份 $b_i$这个参数, 仍然不能伪造其他成员的门限群签名. 因此, 该方案能够抵抗合谋攻击, 是强壮的.

## 4　结　　语

本文提出了一个基于椭圆曲线密码体制的门

限群签名方案. 此方案不仅能满足门限群签名的基本性质, 而且克服了大多数方案中实现不可冒充性与可追查性方法复杂、稳定性差以及密钥长度长、效率低等缺点. 同时本文也分析了多种攻击方式, 得到了在求解有限域上椭圆曲线离散对数问题困难性的假设下, 本方案是安全的结论.

## 参考文献:


[1] BOYD C. Digital multisignatures [C] // **Cryptography and Coding**. Oxford: Claredon Press, 1989: 241–246

[2] DESMEDT Y, FRANKEL Y. Threshold cryptosystems [C] // **Gilles Brassard Proceedings CRYPTO′89**. Berlin: Springer-Verlag, 1990: 307–315

[3] SHAMIR A. How to share a secret [J]. **Commun ACM**, 1979, **22**(11): 612–613

[4] PEDERSEN T P. A threshold cryptosystem without a trusted party [C]// DAVIES D W. **Proceedings of Eurocrypt′91, Lecture Notes in Computer Science 547**. Berlin: Springer-Verlag, 1991: 221–238

[5] 徐秋亮. 改进门限 RSA 数字签名体制 [J]. 计算机学报, 2000, **23**(5): 449–453

[6] WANG C T, CHANG C C, LIN C H. Generalization of threshold signature and authenticated encryption for group communications [J]. **IEICE Trans on Fundamentals**, 2000, **E83-A**(6): 1228–1237

[7] WANG G. On the security of the Li-Hwang-Lee-Tsai threshold group signature scheme [C] // **Proceedings of Information Security and Cryptology**. Berlin: Springer-Verlag, 2003: 75–89

[8] LU Lang-ru, ZHAO Ren-jie. A $(t, n)$ threshold group signature scheme[C] // 密码学进展——Chinacrypt′96. 北京: 科学出版社, 1996: 177–184

[9] VANSTONE S A, ZUCCHERATO R J. Elliptic curve cryptosystems using curves of smooth order over the ring $Z_n$ [J]. **IEEE Trans on Inf Theory**, 1997, **43**(4): 1231–1237

[10] 张方国, 陈晓峰, 王育民. 椭圆曲线离散对数的攻击现状 [J]. 西安电子科技大学学报, 2002, **29**(3): 398–401


# $(t, n)$ Threshold group signature scheme based on elliptic curve cryptosystem


LIU Wen-qi*, WEI Lei, YANG Jian-hua

(School of Electr and Inf Eng, Dalian Univ of Technol, Dalian 116024, China)



**Abstract** Aiming at the problems of the threshold group signature in network communication, such as pseudo character, complex traceable method, poor stability and so on, a threshold group signature scheme based on elliptic curve cryptosystem is presented, and its security analysis is proposed. The scheme has following advantages: introducing members′ actual identities, aliases and alias aggregate of achieving the signature, the scheme can briefly realize the un-pseudo and traceable character. By indirectly distributing group secrete key, it is convenient to add and delete members, and only need to update some public parameters. Based on elliptic curve cryptosystem, the scheme′s key length is short and operation cost is low.



**Keywords** cryptography; threshold group signature; elliptic curve