# 基于椭圆曲线的 Schnorr 型高效多重群签名方案*

王国才,刘美兰
(中南大学 信息科学与工程学院,湖南 长沙 410083)

**摘 要**:多重群签名是既具有群签名的性质,又具有多重数字签名性质的特殊的群签名。在基于中国剩余定理的群签名的基础上进行改进,引入椭圆曲线的 Schnorr 型广播多重数字签名,将动态群签名方案与多重数字签名理论巧妙地结合起来,提出了一个基于椭圆曲线的 Schnorr 型高效的广播多重群签名方案。方案中群成员可以高效动态增删,签名时加入时间戳,防止消息重放,并且综合椭圆曲线和 Schnorr 数字签名的密钥短、速度快的优势,实现了方案的安全高效,适用于智能终端系统中,实用性更强。

**关键词**:群签名;多重签名;多重群签名;Schnorr;椭圆曲线;中国剩余定理

**中图分类号**:TP393 **文献标识码**:A **文章编号**:1674-7720(2013)13-0058-02

# Schnorr type efficient multiple group signature scheme with the elliptic curve

Wang Guocai, Liu Meilan
(College of Information Science and Engineering, Central South University, Changsha 410083, China)

**Abstract**: Multiple group signature is a special group signature which has both the nature of the group signature and multiple digital signature nature. This paper improves a kind of group signature which is based on the Chinese remainder theorem, and combines with the elliptic curve Schnorr type multi-digital signature. The paper combines dynamic group signature scheme with multiple digital signature theory skillfully c, and proposes Schnorr type efficient broadcasting multiple group signature scheme with the elliptic curve. Group members can be added and deleted effectively. Adding timestamp to the signature scheme, in order to prevent message replay. Because of elliptic curve and Schnorr digital signatures' key short and speed advantage, the safety and efficiency of the scheme realize better. It is suitable for intelligent terminal system and more practical.

**Key words**: group signature; multisignature; multiple group signature; Schnorr; elliptic curve; the Chinese remainder theorem

群签名首先由 Chaum 和 Van Heyst 提出[1],随后人们对其进行了大量的研究。随着电子商务和电子政务大范围的应用与普及,许多应用环境对群签名提出了多种特殊的要求,而传统的群签名方案难以提供较好的解决办法,因此各种基于群签名的特殊群签名方案被相继提出,成为了群签名研究中一个值得关注的方向。多重群签名是用于解决几个群体同时对一个消息进行签名的特定应用环境,目前对此方面的研究还处于起步阶段。2007 年,谭逊等人首次提出了一种新群签名技术——多重群签名[2],该方案简单,但签名长度与签名群体呈线性关系,导致效率偏低,实用性不强。2009 年,黄华提出了一种基于离散对数的无序多重群签名方案[3]及一种基于离散对数的有序多重群签名方案[4],该方案加入身份识别和时间限制,通信量大,效率不高。2011 年,鲁飞等人[5]在基于中国剩余定理的群签名方案的基础上进行改进,综合应用 RSA 和 Schnorr 签名算法,并满足了非关联性,方案具有动态增删群签名、密钥短、运算速度快及安全性高的特点。本文在此基础上进行改进,并结合多重数字签名[6]理论构建高效的多重群签名方案。

## 1 基于中国剩余定理的群签名方案

### 1.1 系统初始化阶段

群管理员 GA($ID_{GA}$ 为群管理员 GA 的身份信息)秘密地选择两个大素数 $t$、$w$,计算 $n=tw$,选择 $e \in Zn$,并求

*基金项目:铁道部科技研究开发计划(2012X014-C)

$d$，使得 $ed\equiv 1(\bmod \phi(n))$，其中 $\phi(n)$ 是欧拉函数。群管理员的公钥和私钥分别为 $e$ 和 $d$。群管理员再另选两个大素数 $p$、$q$，$q$ 是 $p-1$ 的一个素因子，$g$ 是 $Z_p^*$ 的元素，$g^q=1 \bmod p$，选择一个公开的 hash 函数 $h$，用户 Ui 向群管理员提出申请并提供身份证明，群管理员选择大素数 $p_i\in Z_p^*$，当 $i\neq j$ 时，$\gcd(p_i,g)=1$ 且 $\gcd(p_i,p_j)=1$。把 $p_i$ 传送给 $U_i$，$U_i$ 随机选择 $x_i$，计算 $y_i=g^{xi} \bmod p_i$，并把 $y_i$ 发送给群管理员。群管理员计算同余式组：$c=y_1P_1'P_1+y_2P_2'P_2+\cdots+y_kP_k'P_k \pmod P$。其中 $P=p_1p_2\cdots p_k$；$P_i=P/p_i$；$P_iP_{i'}\equiv 1(\bmod_{pi})$。群公钥为 $(g,c,e)$。

### 1.2 群成员加入阶段

若 $U_{k+1}$ 申请加入群，群管理员选择大素数 $p_{k+1}$，$\gcd(p_{k+1},p_i)=1(i\neq k+1)$。把 $p_{k+1}$ 秘密传送给 $U_{k+1}$，$U_{k+1}$ 随机选择 $x_{k+1}$，$y_{k+1}=g^{xk+1}(\bmod p_{k+1})$。把 $y_{k+1}$ 传送给群管理员，群管理员重新计算出新的 $c$，$c=y_1P_1'P_1+y_2P_2'P_2+\cdots+y_kP_k'P_k(\bmod P)+y_{k+1}P'_{k+1}P_{k+1}(\bmod P)$，在上式中 $P=P\cdot p_{k+1}$，$Pi=P_ip_{k+1}$，$P'_i=P'_ip_{k+1}(\bmod P_i)$，$i=1,2,\cdots,k$，$P_{k+1}P'_{k+1}=1(\bmod P_i)$，然后 GA 计算 $x_{k+1}'=(IDGAy_{k+1})-d$，并将 $x_{k+1}'$ 秘密地传给 $U_{k+1}$，则 $U_{k+1}$ 的私钥为 $(x_{k+1},x_{k+1}')$，同时 GA 保存 $(ID_{k+1},x_{k+1},x_{k+1}')$。

### 1.3 群成员撤销阶段

设系统现有 $k$ 个群成员，现若要撤销群成员 $U_j$，群管理员将 $y_j$ 改为 $y_j'$，且 $y_j'\neq y_j \bmod p_j$。重新计算新的 $c'$ 为 $c'=y_1 P'_1P_1+y_2 P'_2P_2+\cdots+y_{j'}P'_jP_j+\cdots+y_kP'_kP_k(\bmod P)$，保存新的 $c'$。

## 2 基于椭圆曲线的 Schnorr 型高效的广播多重群签名方案

广播多重签名是指签名管理中心将签名消息广播给所有签名者，签名者单独对消息签名，然后发送给签名采集者，再由签名验证者来完成最后的多重签名验证工作。

### 2.1 方案描述

此方案包括系统参数的选取、签名过程和验证过程。方案的参与者有：签名管理中心 SMC（负责系统建立、消息的发送、协调签名者完成签名）、若干群签名者 $U_i$、签名收集者 $U_c$ 和签名验证者 $U_v$。

### 2.2 系统参数选取

签名管理中心 SMC 选取 $N$ 为元素个数为 $q$ 的有限域，全局参数表示为 $(q,FR,a,b,G,n,l)$，FR 为 $GF(q)$ 中的一个元素，定义椭圆曲线 $E:y_2=x_3+ax+b$，基点 $y_2=x_3+ax+b$，$xG,yG\in GF(q)$，$G\in E$，$G$ 的阶为素数 $n$，$n>2\ 160$，$n>4\sqrt{q}$，$\#E(GF(q))$ 为椭圆曲线构成群的阶，$l=\#E(GF(q))/n$。以上全局参数供各群体参与者在签名过程中使用。

各个参与签名的群体内部初始化参考 1.1，群成员动态增删参考 1.2 及 1.3。参与签名的群成员者把其公钥和其群管理员身份信息即 $(yk,IDGAk)$ 发到 SMC 进行注册。

假设消息 $m$ 将有 $n$ 个群体参与签名，分别标志为 $U_1、U_2、\cdots、U_n$，参与者 $U_i(i=1,2,\cdots,n)$ 随机选择一个数 $d_i$ 作为其私钥，$U_i$ 对应的公钥为 $Q_i=diG$，相应的系统公钥为 $Q=\sum_{i=1}^{n}d_iG\in E(GF(q))$。

### 2.3 签名生成

SMC 将消息 $m$ 发送到每一个群体参与签名者 $U_i(i=1,2\cdots,n)$，$U_i$ 和 $U_c$ 收到消息后进行如下操作：

（1）SMC 随机生成 $n$ 个数 $w_i$，选一个单向散列函数 $H$，然后把 $E_i=H(w_i)$ 发送给 $U_i$，$U_i$ 收到 $E_i$ 后选择一个随机数 $k_i,k_i\in[1,n-1]$，计算 $EikiG=(x_i,y_i)$，$r_i=x_i \bmod n$；将 $r_i$ 发送给签名收集者 $U_c$；

（2）$U_c$ 收到 $r_i$ 后，计算 $R=\sum_{i=1}^{n}r_i \bmod P$ 和 $e=h(m\|R)$，将 $R$ 发送给每一位签名者 $Ui$（即将 $R$ 广播出去）；

（3）对于消息 $m$，$U_i$ 计算 $s_i=Eiki-di(e+R)\bmod n$，$s_i$ 作为用户 $U_i$ 对消息 $m$ 的签名，将 $(s_i,r_i,t_i)$ 发送到 $U_c$，其中 $t_i$ 为 $U_i$ 的签名时间，加入时间戳，防止消息重放。

（4）$U_c$ 收到 $(s_i,r_i,t_i)$ 后，检查时间戳 $t_i$，如果 $t_i$ 在有效范围内，计算 $R=\sum_{i=1}^{n}r_i \bmod P$，$s=s_1+s_2+\cdots+s_n$，并将 $(s_i,r_i,t_i,R)$ 发送给签名验证者 $Uv$。

### 2.4 验证过程

签名验证者 $Uv$ 收到消息 $(s_i,r_i,t_i,R)$ 后，计算 $X_i=s_iG-(e+R)Q_i=(x_i,y_i)$，验证 $v_i=r_i \bmod n$ 是否成立，其中 $(i=1,2,\cdots,n)$，如果等式成立则认为 $U_i$ 对消息的签名有效，否则签名无效。证明如下：

$$R=\sum_{i=1}^{n}r_i \bmod P,\ s=s_1+s_2+\cdots+s_n,\ s_i=E_ik_i-d_i(e+R)\bmod n$$

得到

$$\begin{aligned}&-s_iG=-[E_ik_i-d_i(e+R)]G\\&=-E_ik_i+d_i(e+R)G\\&=-E_ik_iG+(e+R)Q_i\\&\Rightarrow s_iG-(e+R)Q_i=E_ik_iG=(x_i,y_i)\\&\Rightarrow X_i=s_iG-(e+R)Q_i=E_ik_iG=(x_i,y_i).\end{aligned}$$

可得 $v_i=r_i \bmod n$。

$$-sG=\sum_{i=1}^{n}-[E_ik_i-d_i(e+R)]G \bmod n$$

$$=-\sum_{i=1}^{n}E_ik_iG+\sum_{i=1}^{n}d_i(e+R)G \bmod n$$

$$\Rightarrow sG-\sum_{i=1}^{n}(e+R)Q_i \bmod n=\sum_{i=1}^{n}E_ik_iG$$

$$\Rightarrow sG-(e+R)Q \bmod n=\sum_{i=1}^{n}E_ik_iG$$

由上述推论过程可得，$U_v$ 收到签名 $(s_i, r_i, R, t_i)$ 后验证 $v_i = r_i \bmod n$ 是否成立，才能确定所有签名是否有效。

## 3 安全性和性能分析

### 3.1 满足群签名的安全性

(1)匿名性：一个群成员签名之后，只有群管理员能确定签名人的身份。

(2)防伪造性：各签名者把其公钥和群管理员身份信息即(yk，IDGAk)已在 SMC 注册，所以只有群成员才能产生有效的签名。

(3)可追踪性：群管理员可以通过在 SMC 的注册信息，通过验证 $x_{k+1'} = (\mathrm{IDGA}y_{k+1}) - d$ 是否成立，可以确定签名人的身份。

(4)抗联合攻击：签名者签名时，需要 SMC 的配合才能生成真正的签名，其他子集合无法产生有效的签名。

### 3.2 多重签名的安全性

本文是基于椭圆曲线体制，方案的安全性是基于椭圆曲线的离散对数问题，保证了方案体制上的安全性。若攻击者以 $U_c$ 的身份伪造所有的签名是困难的，所以防伪造性强。

### 3.3 方案性能分析

方案基于椭圆曲线，其密钥长度小、安全性能高，整个数字签名耗时小；其次，Schnorr 数字签名比 ElGamal、RSA 密钥短，较现有的其他基于椭圆曲线的多重数字签名运算速度快。因此，本方案综合应用椭圆曲线和 Schnorr 密码体制密钥小、速度快等优点，降低了通信成本，更具有安全性和实用性。

本文提出了一个新的基于椭圆曲线的 Schnorr 型高效广播多重群签名方案，方案基于椭圆曲线，安全性更高，且对存储空间和带宽要求小，具有广泛的应用前景，同时结合 Schnorr 数字签名的密钥短、速度快的优势，与现有的其他多重群签名方案比较，此方案更加灵活、安全、高效。

## 参考文献

[1] CHAUM D, VAN HEYST E. Group signatures[A]. In EUROCRYPT′91 [C]. Berlin:Springer-Verlag,1991(547):257-265.

[2] 谭逊，孙艳蕊.一种新群签名技术——多重群签名[J].计算机安全，2007(6):30-31.

[3] 黄华.一种基于离散对数的无序多重群签名方案[J].信息与电脑(理论版)，2009(7):102-103.

[4] 黄华.一种基于离散对数的有序多重群签名方案[J].计算机与现代化，2010(7):58-59.

[5] 鲁飞，张亚平，马建军.一种基于中国剩余定理的群签名方案的密码学分析和改进[J].计算机应用研究，2011，28(6):2192-2195.

[6] LTAKURA K,NAKAMURA K. A public key cryptosystem suitable for digital multi-signature[J]. Nec Research and Development, 1983,71(10):1-8.

(收稿日期：2013-03-06)

作者简介：

王国才，男，1963 年生，副教授，硕士生导师，主要研究方向：计算机通信保密，计算机网络技术应用与网络信息安全，信息系统工程。

刘美兰，女，1988 年生，硕士研究生，主要研究方向：网络信息安全。