基于 ECC 的存在特权集的门限群签名方案

董玉蓉

（贵州大学 计算机科学与信息学院，贵州 贵阳 520025）

摘 要：通过对一种 ElGamal 类型存在特权集的门限群签名方案的分析研究，提出了一种基于 ECC 的存在特权集的门限群签名方案。该方案能有效防止 KDC 的欺诈，且只有在同时满足(t,n)和(t_1,n_1)门限签名时才能生成消息的有效签名，从而实现了门限特性，并具有门限群签名应有的性质。

关键词：特权集；秘密共享；门限群签名；ECC

中图分类号：TP309 **文献标识码**：A **文章编号**：1674-7720(2011)02-0089-04

Threshold group signature scheme with privilege subsets based on ECC

Dong Yurong

(Computer Science and Information College, Guizhou University, Guiyang 520025, China)

Abstract: Through the analysis and study of a threshold group signature scheme which is based on ElGamal type, in order to solve the deficiency of the scheme, a new threshold group signature scheme with privileged subsets based on ECC is proposed. The proposed scheme can prevent the fraud of KDC efficiently. Only when the scheme satisfiesand (t,n) and (t_1,n_1)threshold signature, the valid signature can be generated, thus the scheme reached the property of threshold. The program also has the properties of threshold group signature.

Key words: privileged subjects; secret sharing; threshold group signature; ECC

群签名方案首次由 Chanm 和 VanHeyst 于 1991 年提出。在群签名方案中，允许每个成员都可以代表整个群体进行签名。在群签名方案中引入秘密共享，解决密钥安全与有效保管问题的同时也形成了一类新的群签名方案——门限群签名方案，即群体中的某些给定子集可以代表整个群体签名。在门限群签名方案中，门限群签名是由参加签名的各个成员所签署的部分数字签名按照某种方式结合后产生。2003 年，BELLARE M 等人提出了群签名的简化形式定义[1]。在这之后，不少学者提出的门限群签名方案均采用形式化的方法证明方案的安全性。参考文献[2]提出良好的门限群签名应该具备以下一些性质：群签名特性、门限特性、不可伪造性、验证简单性、匿名性、可追查性、强壮性。参考文献[3]中，Chen Feng 等人基于 Shamir 秘密共享体制并结合“存在特权集的门限群签名方案”的思想[4]，构造了一类基于离散对数问题的 ElGamal 类型的存在特权集的门限群签名方案。

本文利用椭圆曲线密码体制的特点对 Chen Feng 的方案进行改进。新的方案与原方案的共同点在于都使用双重秘密共享技术和单签名构造群签名的技术[3]，不同之处在于新方案实现了群成员的加入和撤销，提高了方案的通用性。同时，为了防止密钥分配中心的欺诈[5]，各用户对自己私钥的有效性进行了验证，并且利用椭圆曲线密码体制的特点优化本方案，进而提高了方案的效率和安全性。

1 一种 ElGamal 类型的存在特权集的门限群签名方案

Chen Feng 依据离散对数问题提出了一种存在特权集的 ElGamal 类型门限群签名方案。

其基本设计流程如下：

(1)初始化：由可信的密钥认证中心 KAC 选取 2 个安全参数 p、q，在有限域 F_q 上随机选取两个多项式 $f(x)$、$g(x)$，次数分别为 $(t-1)$、(t_1-1)，并取有限域 F_q 的本原元 α。

(2)群密钥及秘密碎片的产生：群密钥 d 及群公钥 z 由 KAC 随机选取的两个多项式构成。利用“双重”SSS 秘密共享方案为各签名者建立公私钥碎片。

(3)签名：群签名由参与签名的成员和签名服务机构

SC 共同生成：每个成员先生成自己的单签名，然后发送给 SC 验证该单签名是否为合法签名，再由 SC 决定是否接受；如果接受的单签名满足门限要求，则计算组合出群对消息的签名。

Chen Feng 方案可简单描述为：在计算机网络开放式环境下，一个能够被完全信任的中心是不存在的。该方案的群密钥和群成员的秘密份额都由可信的密钥认证中心决定，不能保证密钥认证中心分发给各用户的密钥碎片有效，存在密钥分配中心欺诈的问题。此外方案没有考虑到群成员的安全有效的加入和撤销，因此不满足群签名的特性。

2 本文方案

本文提出的基于 ECC 的存在特权集的门限群签名方案共分为六个阶段：系统初始化、群密钥产生、群成员的加入和撤销、密钥分发、单个签名生成与验证、群签名生成。

2.1 系统初始化阶段

该方案的系统参数意义如下：

KDC：密钥分配中心；

Clerk：签名服务者，负责颁布签名；

G：由 n 个签名方组成的群体，至少有其中 t 方参与才可产生合法签名；

G_1：G 的子集，有 $n_1(n_1<n)$ 个成员。至少有其中 $t_1(t_1<t)$ 方参与才可产生合法签名，称为特权子集；

G_2：G 的子集，其中的签名方为普通用户；

u_i：群成员 p_i 的公开身份；

ID_i：群成员 p_i 的真实身份。

该方案的安全参数描述为：

(1)密钥分配中心 KDC 给定任一有限域 $F_p(p$ 为大素数)，并定义 F_p 上的一条安全椭圆曲线 $E(F_p)$，保证该椭圆曲线的离散对数问题是难解的。在 $E(F_p)$ 上选一基点 P，其阶数为 $q(q$ 为一个大于 160 bit 的大素数)。另外，KDC 还选择一个单向安全的 Hash 函数 $H()$。

(2)KDC 构造 2 个秘密多项式 $f(x)\in_R F_q[x]$，$g(x)\in_R F_q[x]$，次数分别为 $(t-1)$ 和 (t_1-1)。

$$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}\bmod q$$

$$g(x)=b_0+b_1x+\cdots+b_{t_1-1}x^{t_1-1}\bmod q$$

其中，$a_0=f(0)$，$b_0=g(0)$，$a_i,b_j\in Z_q^*(i=1,2,\cdots,t-1;j=1,2,\cdots,t_1-1)$。

2.2 群密钥的产生

群密钥：由 KDC 产生，即 $d=[f(0)+g(0)]=a_0+b_0$。

群公钥：$Y=(a_0+b_0)\cdot P$。

Clerk 随机地为用户 p_i 选择群内公开身份 $u_i\in Z_q^*$。

2.3 群成员的加入

(1)群成员 p_i 随机选取 $k_i\in Z_q^*$，并计算 $R_i=k_i\cdot P=(x_i,y_i)$，并将 (k_i,K_i) 在群内公开。

(2)签名服务者 Clerk 通过验证 $R_i\neq R_j(i\neq j)$ 是否成立，来检验群成员 p_i、p_j 是否选择了同样的随机数。若 $R_i=R_j$，说明这两个群成员选择了相同的随机数，则 Clerk 通知他们重新选取并进行计算。若 $R_i\neq R_j$，则进行下一步。

(3)每个群成员计算 $K=\sum_{i=1}^{t}k_i$，$R=\sum_{i=1}^{t}R_i$(每个群成员 p_i 计算出的 R 值都相同)，$\sigma_i=H(u_i\|ID_i)$，将 σ_i 发送给 Clerk，并在群内通过信道匿名广播 K、R。

(4)Clerk 验证 $\sigma_i=H(u_i\|ID_i)$ 是否成立：

若 $\sigma_i\neq H(u_i\|ID_i)$，则说明群成员 p_i 伪造了一个群内公开身份，Clerk 拒绝 p_i 加入签名生成过程，并通知 KDC 拒绝为其分发秘密钥碎片。

若 $\sigma_i=H(u_i\|ID_i)$，则接受 p_i 加入，通知 KDC 为其分发秘密钥碎片。

(5)群成员的撤销。设该系统现有 $k(k\geqslant t)$ 个群成员，撤销群成员 p_j 的过程如下：Clerk 将 p_j 在群内的公开身份 u_j 置为 1。在验证用户身份合法性时，若检测到 $\sigma_j=H(1)$，则拒绝 p_j 加入签名群，同时通知 KDC 拒绝 p_j 为分发秘密钥碎片。

2.4 密钥分配及验证

(1)密钥分配

秘密钥碎片分发采用“双重”SSS[3]，分别是 (t,n) 和 (t_1,n_1) 门限。将密钥 d 分割成多种组合，d 的每种组合都与包含 t 个不同用户的子集相对应。

如果群成员 p_i 是普通用户，则得到相对应的秘密碎片 $d_i=f(x_i)$，并由 KDC 在群内广播其公钥 $Y_i=d_i\cdot P=f(x_i)\cdot P$；如果群成员 p_i 是特权集用户，则得到的秘密碎片为 $d_i=[f(x_i)+g(y_{ij})]$，由 KDC 公开其公钥为 $Y_i=d_i\cdot P=[f(x_i)+g(y_{ij})]\cdot P$。以上的过程利用“双重”SSS 秘密共享方案为各群成员建立了公、私钥碎片。

最后，KDC 公开参数为：$E(F_p)$，P，p，q，$H()$。

(2)群成员对各自密钥的验证

根据 Pedersen VSS 验证方法[5]，群成员 p_i 可通过式(1)和式(2)验证 KDC 为其分配的密钥 d_i 的有效性：

若群成员 p_i 为特权集用户，则验证：

$$d_i\cdot P=\sum_{j=0}^{t-1}\ddot{v}(a_j\cdot P)+\sum_{j=0}^{t_1-1}\ddot{v}(b_j\cdot P) \tag{1}$$

若群成员 p_i 为普通用户，则验证：

$$d_i\cdot P=\sum_{j=0}^{t-1}\ddot{v}(a_j\cdot P) \tag{2}$$

若等式成立，证明 KDC 分配给群成员 p_i 的密钥 d_i 是正确、有效的。否则就说明 KDC 欺诈。

2.5 单个签名生成与验证

假设现有 t 个群成员参与群签名的生成，设被签署的消息为 m。则签名步骤如下：

(1)每个参与签名的群成员(以下简称签名者)p_i 计算 $R=\sum_{i=1}^{t}R_i=(x,y)$(每个 u_i 计算出的 (x,y) 的值都相同)。计算 $r=H[H(m),x]$。

(2)若签名者 p_i 为普通用户,则计算:

$$s_i=(r\cdot d_i\cdot C_i+k_i)\bmod q=[r\cdot f(x_i)\cdot C_i+k_i]\bmod q$$

若签名者 p_i 为特权集用户,则计算:

$$s_i=(r\cdot d_i\cdot C_i+k_i)\bmod q=[r\cdot f(x_i)+g(y_{ij})\cdot C_i+k_i]\bmod q$$

其中差值系数 $C_i=\prod_{j=1,j\neq i}^{t}\frac{-x_j}{x_i-x_j}\bmod q$ 由 Lagrange 插值多项式得出。签名者 p_i 发送(m,s_i)给 Clerk。

(3)Clerk 验证单签名:Clerk 接收到各个签名消息 s_i 后,利用签名者 p_i 的公钥验证其单个签名的有效性,验证等式为:

$$R_i=s_i\cdot P-r_i\cdot C_i\cdot Y_i \tag{3}$$

若等式成立,则接受该单签名,否则拒绝接受单签名。

2.6 群签名的生成

如果 Clerk 接受的单签名分别满足(t,n)、(t_1,n_1)门限的要求,则计算 $s=\sum_{i=1}^{t}s_i\bmod q$,并输出$(r,s)$作为签名者群体对消息 m 的数字签名。

3 方案分析

3.1 正确性分析

(1)单签名的验证

假设至少有 t 个人参与签名,且恰为 $1,2,\cdots,t$,其中至少有 t_1 个人属于特权用户集,并且签名者没有欺诈行为。不论是普通用户还是特权用户,都可以通过式(3)验证单签名的正确性。

因为 $Y_i=d_i\cdot P$

$$s_i=(r\cdot d_i\cdot C_i+k_i)\bmod q$$

所以

$$s_i\cdot P=(r\cdot d_i\cdot C_i)\cdot P$$

$$s_i\cdot P-r\cdot Y_i\cdot C_i=k_i\cdot P=R_i$$

上述过程验证了单签名的正确性。

(2)群签名的验证

假设签名组成员都严格按照签名的步骤对消息进行签名,就有

$$\begin{aligned}s_i\cdot P-r\cdot Y&=\sum_{i=1}^{t}s_i\cdot P-r\cdot(d_i\cdot P)\\&=\left\{\sum_{i=1}^{t}[(r\cdot d_i\cdot C_i+k_i)\bmod q)]\right\}\cdot P-r\cdot(d_i\cdot P)\\&=\sum_{i=1}^{t}k_i\cdot P+(\sum_{i=1}^{t}d_i\cdot C_i\bmod q)\cdot r\cdot P-r\times(d_i\cdot P)\end{aligned}$$

由 Lagrange 插值多项式性质有:

$$\begin{aligned}&\sum_{i=1}^{t}d_i\cdot C_i\bmod q\\&=\left[\sum_{i=1}^{t}f(x_i)+\sum_{i=1;j=1}^{t_1}g(y_{ij})\right]\cdot\prod_{j=1,j\neq i}^{t}\frac{-x_j}{x_i-x_j}\bmod q\\&=f(0)+g(0)=d\end{aligned}$$

所以有:

$$s\cdot P-r\cdot Y=\sum_{i=1}^{t}k_i\cdot P=R$$

上述过程通过式(3)对群签名的正确性进行了验证。

3.2 安全性分析

根据门限群签名的特性对该方案进行安全性分析。

(1)匿名性

由于签名者使用的是公开身份,公开身份和真实身份的对应关系只有 Clerk 和签名者本身知道。其他用户只知道通过广播信道传播出的 R_i 的值,并不能依据 R_i 来确定用户的真实身份,也就无法根据群签名(在未经特许的情况下)追踪各签名方的真实身份。因此该方案具有匿名性。

(2)不可伪造性

参与签名的群成员只有获得合法身份,才能获得秘密钥碎片进而生成有效的部分签名,非法用户无法伪造有效部分签名。Clerk 通过验证 $\sigma_i=H(u_i\|ID_i)$ 来确定群成员的身份是否合法。

(3)可追查性

如果事后签名出现矛盾,在得到许可的情况下,需要调查哪些成员参与签名,Clerk 很容易确定签名方的真实身份。

(4)抗合谋攻击

在秘密钥碎片的分发上采用“双重”SSS。当进行合谋攻击时,如果不符合特权条件的要求,即使有 t 个或 t 个以上签名者参与,$g(0)$的恢复也是不可能的,进而无法得到群密钥;如果有不足 t 个人参与签名,即使符合特权条件的要求($g(0)$可以恢复)也不可能恢复 $f(0)$,从而无法得到群密钥。可见,该方案能抵抗合谋攻击。

(5)可撤销性

签名者 p_i 被撤销后,在开始新的签名过程时,KDC 公布了新的 Y',p_j 就不能继续参与群签名的生成,因为此时群公钥由原来的 Y 变成了 Y'。

若签名者 p_j 继续使用原来的私钥 d_j 参与新的群签名的生成,Clerk 在收到 p_j 的单签名 s_j 后,要根据 p_j 的公钥 Y_j 验证式(3)是否成立。然而 Clerk 在信道内无法获得与 p_j 相对应的 Y_j,也就无法验证式(3),因此 Clerk 拒绝接受该单签名。所以,被撤销后的签名者 p_j 并不能继续参与群签名的生成。

(6)门限特性

由于方案是基于双重 Shamir 秘密共享建立的,因此在签名阶段具有门限方案的安全性:任意少于 t 个群的成员无法得到有效签名,且任意少于 t_1 个特权集成员也无法得到有效签名。

3.3 效率分析

本方案的建立基于椭圆曲线密码体制,与 ElGamal 类型的基于离散对数问题的原方案相比密钥长度和签名长度都大大降低。

ECC 算法只需采用较短的密钥就可达到与离散对数算法相同的加密强度。ECC 算法具有每比特最高的安全强度。由于智能卡在 CPU 处理能力和 RAM 大小上受限，采用一种运算量小但同时能提供高加密强度的公钥密码机制对于实现数字签名的应用非常关键。ECC 在这方面具有明显的优势，160 bit ECC 算法的安全性与 1 024 bit 采用基于离散对数问题的算法安全性相同。因此，采用椭圆曲线密码体制设计的门限群签名方案的计算量和通信量都要小于基于离散对数问题的 ElGamal 密码体制的门限群签名方案。

本文基于椭圆曲线密码体制和双重 Shamir 秘密共享体制，结合 Chen Feng 的特权集思想，设计了一个同时具有门限群签名功能和门限共享验证功能的存在特权集的门限群签名方案，该方案不但克服了目前一些方案的缺陷和弱点，而且具有更高的实现效率。方案除了具有门限群签名的性质外，还可以利用公开验证功能防止 KDC 欺诈。相对于原方案，本方案是基于椭圆曲线密码体制建立的，在安全性和效率方面考虑得更全面。但是，如何将该方案推广到实际应用中，仍有待于进一步研究。

参考文献

[1] BELLARE M, MICCIANCIO D, WARINSCHI B. Foundation of group signatures: formal definitions, simplified requirements, and a construction based on generalassumptions[C]. Proc of EUROCRPT 2003, LNCS2656. Berlin: Springer-Verlag, 2003: 614-629.

[2] 王贵林，卿斯汉. 几个门限群签名方案的弱点[J]. 软件学报，2000，11(10)：1326-1332.

[3] 陈伟东，冯登国. 一类存在特权集的门限群签名方案[J]. 软件学报，2005，16(7)：1289-1295.

[4] 石怡，冯登国. 一类新型(t_j, t, n)-门限群签名方案的设计与分析[M]. 北京：科学出版社，2000.

[5] 彭长根，李祥，罗文俊. 一种面向群组通信的通用门限签密方案[J]. 电子学报，2007，35(1)：64-67.

(收稿日期：2010-07-31)

作者简介：

董玉蓉，女，1985年生，硕士研究生，主要研究方向：密码学与信息安全。