无可信中心秘密共享加密模式*

郑芳芳,侯整风,丁 凉,朱晓玲
(合肥工业大学 计算机与信息学院,安徽 合肥 230009)

摘 要:在基于椭圆曲线离散对数的安全机制的前提下,讨论了(t,n)门限加密模式。在该模式中,系统公钥由成员协同产生,t个或t个以上成员可以间接地解开密文。由于(t,n)门限加密模式秘密信息较少,所以具有良好的安全性,且计算复杂度较低。

关键词:秘密共享;可信中心;加密

中图分类号:TP309.7 **文献标识码**:A **文章编号**:1674-7720(2010)23-0058-03

Secret sharing encryption mode without trusted center

ZHENG Fang Fang, HOU Zheng Feng, DING Liang, ZHU Xiao Ling
(School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: Based on the difficulty of solving the discrete logarithm problem of elliptic curve, this paper discusses the (t,n) threshold encryption scheme and presents a shared secret encrypted mode without a trusted center. In the model, the system public key generated by the members of the cooperative. t or more members can indirectly solve ciphertext. Since the model has little secret information, it has good security and low computational complexity.

Key words: secret sharing; trusted center; encryption

门限秘密共享由SHAMIR[1]和BLAKLEY[2]于1979年独立提出,他们分别利用有限域中的Lagrange插值多项式和几何映射构造出了(t,n)门限秘密共享方案,这些方案存在着可信中心。随后许多学者对可信中心的存在情况进行了深入研究。1991年,INGEMARSSON和SIMMONS[3]提出了一种无可信中心秘密共享思想。HARN[4]于1994年提出了一种基于ELGamal签名的、不需要可信中心的门限群签名方案,该方案没有可信中心,但是超过门限值的成员能够协同恢复其他成员的私钥。参考文献[5-7]等分别提出了一个无需可信中心的门限签名方案,但签名者之间需要进行秘密通信来交换信息。参考文献[8]提出的门限签名方案无需秘密通信。随后,很多学者对这方面进行了大量的研究和改进[9-10]。

目前,无可信中心秘密共享的研究主要集中在门限数字签名上,对于门限加密的研究尚且不多。为此,本文在基于椭圆曲线公钥体制的前提下,提出了无可信中心秘密共享加密模式。该模式中,成员协同作用生成各自的秘密份额,参与者之间无需传递任何秘密信息。由秘密份额计算出相关的可公开信息,从而生成系统公钥。解密过程中,也是由合作的参与者通过秘密份额计算一个可验证的伪份额,最终间接地完成解密,从而保证了系统私钥可重复使用。利用公开信息来验证参与者提供的有用信息,在很大程度上提高了系统的执行效率。

1 预备知识

1.1 SHAMIR的门限秘密共享方案

(1)初始化阶段:秘密分发者D随机地从$GF(q)$(q为素数且$q>n$)中选取n个不同的非零元素$x_1,x_2,\cdots,x_n$,D将x_i分配给$P_i(i=1,2,\cdots\cdots,n)$,且$x_i$的值是公开的。

(2)秘密分发阶段:设共享秘密为$s\in GF(q)$,D随机地选择$GF(q)$中的$t-1$个元素$a_1,a_2,\cdots,a_{t-1}$,构造一个$t-1$次多项式$f(x)=s+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1} \bmod q$,$D$计算$y_i=f(x_i)(i=1,2,\cdots,n)$,$y_i$作为$s$的子秘密。

(3)秘密恢复阶段:t个成员$P_i(i=1,2,\cdots,t)$交换各自的秘密份额,得到:$(x_1,y_1),(x_2,y_2),(x_3,y_3),\cdots,(x_t,y_t)$,就可通过式(1)恢复共享秘密$s$。

*基金项目:安徽省自然科学基金资助项目(090412051);广东省教育部产学研结合项目(2008B090500240)

$$s=\sum_{i=1}^{t} y_i \prod_{j=1,j\neq i}^{t} \frac{-x_j}{x_i-x_j} \bmod q \tag{1}$$

1.2 椭圆曲线实现 Elgamal 密码体制

首先选取一条椭圆曲线 $E_p(a,b)$，p 为一个奇素数，G 为椭圆曲线的基点，q 为 G 的阶，$E_p(a,b)$和 G 公开。设明文为 m，将明文通过编码嵌入到曲线上得点 P_m，再对点 P_m 进行加密。另设用户 U_A 及 U_B。

(1)U_B 加密：用户 U_A 选 S_A 作为私钥，并以 $P_A=S_AG$ 作为公钥。任一用户 U_B 如果想向 U_A 发送消息 P_m，可选取一随机正整数 k，产生以下点对作为密文：$C_m=\{kG,P_m+kP_A\}$。

(2)U_A 解密：U_A 解密时，以密文点对中的第 2 个点减去用自己的秘密钥与第 1 个点的倍乘，即 $P_m+kP_A-S_AkG=P_m+k(S_AG)-S_AkG=P_m$。

2 本方案的描述

2.1 系统初始化

初始化过程完成各参与者的私钥、秘密份额及系统公钥的产生。假设 $P=\{P_1,P_2,\cdots,P_n\}$为 n 个成员的集合，每个成员 $P_i(P_i\in P)$拥有私钥 d_i，ID_i 是每个 P_i 唯一的身份标识，t 为门限值。首先选取一条椭圆曲线 $E_p(a,b)$，G 为椭圆曲线的基点，q 为 G 的阶，$E_p(a,b)$和 G 公开。

(1)$P_i\in P$ 在$[1,q-1]$中随机选择一个整数 d_i 作为私钥，公钥为 d_iG，并产生随机数集$\{a_{i,k}|k=1,2,\cdots,t-1\}$。构造一个 $t-1$ 次多项式：

$$f_i(x)=d_i+a_{i,1}x+\cdots+a_{i,t-1}x^{t-1} \bmod q \tag{2}$$

其中 $d_i=f_i(0)$。P_i 把 $f_i(ID_j)$发送给其他 $n-1$ 个成员 $P_j(j\neq i)\in P$。$f_i(ID_i)$自己保留。再计算验证参数：$\alpha_{ik}=a_{ik}G$，$k\in\{1,2,\cdots,t-1\}$。

每个 P_j $(j\neq i)\in P$ 接收到其他 $n-1$ 个成员的广播信息后，P_j 通过式(3)验证 $f_i(ID_i)$：

$$f_i(ID_j)G=d_iG+\sum_{k=1}^{t-1}(ID_j)^k\alpha_{ik} \tag{3}$$

若式(3)成立，则 $f_i(ID_j)$有效；否则，P_j 拒绝 $f_i(ID_j)$，并要求 P_i 重新发送。

(2) 秘密份额的生成：每个 P_i 从其他 $n-1$ 个成员接收到了所有正确的秘密份额以后，通过式(4)计算各自的秘密份额，并广播 $Y_i=F(ID_i)G \bmod q$。

$$F(ID_i)=\sum_{j=1}^{n} f_j(ID_i) \bmod q \tag{4}$$

(3) 系统公钥生成：系统私钥 $F(0)=\sum_{i=1}^{t}F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j} \bmod q$，基于拉格朗日插值多项式，利用公开信息计算系统公钥：

$$\begin{aligned}y&=F(0)G \bmod q\\&=(\sum_{i=1}^{t}F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j} \bmod q)G \bmod q\\&=[(\sum_{i=1}^{t}F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j} \bmod q)\cdot(G \bmod q)] \bmod q\\&=(\sum_{i=1}^{t}F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}G) \bmod q\\&=\sum_{i=1}^{t}(\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}F(ID_i)G \bmod q) \bmod q\\&=\sum_{i=1}^{t}(\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}Y_i) \bmod q\end{aligned} \tag{5}$$

然后公开 y。

2.2 加密过程

为不失一般性，假设明文为 m，将 m 通过编码映射到曲线上得点 P_m，再对点 P_m 进行加密。

(1)U_A 选取一个随机数 k，并使其满足 $1\leqslant k\leqslant q-1$。

(2)计算 $C_1=kG \bmod q$ 和 $C_2=P_m+ky \bmod q$，产生点对密文：$C_m=\{C_1,C_2\}$。

(3)将密文 C_m 发送给 P。

2.3 验证过程

P 中任意 t 个或 t 个以上的参与者合作可以解开密文，为不失一般性，设 P 中 t 个参与者集合为 $W=\{P_1,P_2,\cdots,P_n\}$。收到密文后，W 中每个成员 P_i 利用自己的秘密份额，通过式(6)各自计算出 $s_i(i=1,2,\cdots,t)$，参与者彼此交换份额 s_i。

$$s_i=F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}C_1 \tag{6}$$

每个 P_i $(j\neq i)\in P$ 能够通过判断等式 $s_iG=C_1Y_i\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}$ 是否成立来验证 $P_i(i=1,2,\cdots,t)$所提供的份额的真伪。如果等式成立，那么 P_i 所提交的份额是正确的，接着执行下面的步骤；否则就要求 P_i 重新发送份额。

2.4 解密过程

当收到了 t 份 s_i 后，就通过式 (7) 计算得出 $F(0)C_1 \bmod q$。

$$\begin{aligned}F(0)C_1 \bmod q&=[(\sum_{i=1}^{t}F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j} \bmod q)\cdot(KG \bmod q)] \bmod q\\&=(\sum_{i=1}^{t}F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}KG) \bmod q\\&=\sum_{i=1}^{t}(F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}KG \bmod q)\\&=\sum_{i=1}^{t}(F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}C_1)\\&=\sum_{i=1}^{t}s_i\end{aligned} \tag{7}$$

解密时，以密文对中的第 2 个点减去用组私钥与第 1 个点的倍乘，即：

$$P_m=P_m+[k(F(0)G \bmod q)-F(0)kG \bmod q] \bmod q=$$

$$P_m+k(F(0)G \bmod q)\bmod q-F(0)kG \bmod q=$$
$$P_m+ky \bmod q-F(0)kG \bmod q= \quad (8)$$
$$C_2-F(0)C_1=$$
$$C_2-\sum s_i$$

3 方案分析

3.1 方案特点

(1)本方案不需要可信中心管理参与者的密钥,成员协同产生各自的秘密份额,每个参与者只需保留一个自己的私钥和一份秘密份额。

(2)在初始化阶段,系统公钥由达到门限值的成员组协同产生并公开,但这些成员组是无法共同生成系统私钥 $F(0)$ 的,即 P 中任一成员都不知道系统私钥。

(3)秘密份额产生后,公开 $Y_i=F(ID_i)G \bmod q$,系统公钥不是由系统私钥直接产生,而是由公开信息间接生成。在解密过程中,每个合作的参与者只需向解密者提交一个由秘密份额计算的、可验证的伪份额 s_i,即可间接达到解密效果。

3.2 安全性分析

(1)系统私钥 $F(0)$ 是安全的。基于求解椭圆曲线上离散对数问题的困难性,由系统公钥 $y=F(0)G \bmod q$ 无法计算出系统私钥 $F(0)$,由 $\sum_{i=1}^{t} s_i=F(0)C_1 \bmod q$ 也不能计算出系统私钥 $F(0)$,从公钥 $d_iG(i\in\{1,2,\cdots,n\})$ 无法得到 $d_i(i\in\{1,2,\cdots,n\})$,所以无法生成系统公钥 $F(0)=\sum_{i=1}^{n} f_i(0)\bmod q=\sum_{i=1}^{n} d_i \bmod q$。对于由每个成员的秘密份额得出的公开信息 $Y_i=F(ID_i)G \bmod q(i\in\{1,2,\cdots,t\})$,由于无法获取秘密份额 $F(ID_i)$,故无法生成系统私钥 $F(0)=\sum_{i=1}^{t} F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}\bmod q$。

(2)能够有效地阻止主动攻击。如果有伪造者想要假冒成合法成员 P 中的一员(如 P_i),那么它要构造一个多项式 $f_i'(x)$。但是,由于伪造者不知道 P_i 的私钥 d_i,所以 $f_i'(0)\neq d_i$。如果 $f_i'(0)\neq d_i$,则份额 $f_i'(ID_i)$ 就不满足式(3)的验证,从而达不到伪造的初衷,所以伪造者不能阻止诚实成员生成系统公钥。

(3) 解密前能够验证 P_i 是否提供虚假信息来欺骗其他参与者。解密过程中,解密者通过判断式 $s_iG=C_1Y_i\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}$ 成立与否来验证各成员提供的信息的真伪。除了 s_i 以外,其他信息均公开或可计算,所以要伪造一个新的满足条件等式的 s_i 是不可行的。

(4) 有别于传统的研究方法,本方案中对防欺骗研究侧重于安全交换协议。具体做法体现在方案中秘密份额的生成和认证,能在事前有效地阻止恶意成员的欺骗行为。是否满足式(3)是判断份额正确性的标准。

本文构造了一个无可信中心的秘密共享加密模式,每个参与者只需要产生一个私钥,秘密份额由成员协同产生,成员协同产生用于加密的系统公钥,t 个或 t 个以上成员利用秘密份额计算并提供正确的信息,可以间接地解开密文。本文是基于椭圆曲线公钥密码体制的,系统私钥的安全性基于椭圆曲线上的离散对数问题的难解性。该方案中,每个成员需保留的秘密信息只有一个自己的私钥和一份秘密份额,即使存在着超过门限值的成员协同作用,也无法将其他成员的私钥恢复,使无可信中心的特点及优点得到了较好的实现。

参考文献

[1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979,22(11):612-613.

[2] BLAKLEY G R. Safe guarding cryptographic keys [C], Proceedings of National Computer Conference. Montvale, NJ: AFIPS Press, 1979: 313-317.

[3] INGEMARSSON I, SIMMONS G L. A protocol to set up shared secret schemes without the assistance of a mutually trusted party [C]. Proceedings of Eurocrypt'90, Mar 21-24, 1991: 266-282.

[4] HARN L. Group-oriented (t,n) threshold digital signature scheme and digital multisignature [J]. IEEE Proceeding of Computer and Digital and Techniques, 1994, 141(5): 307-313.

[5] 王斌,李建华.无可信中心的(t,n)门限签名方案[J].计算机学报,2003,26(11):1581-1584.

[6] MIYAZAKI K, TAKARAGI K. A threshold digital signature scheme for a smart card based system. IEICE Trans. Fundamentals, 2001, E84-A(1): 205-213.

[7] CHANG Ting Yi, YANG Chou Chen, HWANG Min Shiang. A threshold signature scheme for group communications without a shared distribution center. Future Generation Computer Systems, 2004, 20(6): 1013-1021.

[8] TAKARAGI K, MIYAZAKI K, TAKAHASHI M, et al. A threshold digital signature issuing scheme without secret communication[EB/OL]. http://grouper.ieee.org/groups/1363/Study Group/ contributions/th-sche.pdf, 2002-12-01.

[9] 庞辽军,谭示崇,王育民.一个预防欺诈的(t,n)门限数字签名方案[J].电子与信息学报,2007,29(4):895-897.

[10] 庞辽军,李慧贤,王育民.一个(t,n)门限签名-(k,m)门限验证的群签名方案[J].计算机科学,2006,33(11):76-78.

(收稿日期:2010-07-11)

作者简介:

郑芳芳,女,1986 年生,硕士研究生,主要研究方向:密码学,网络安全。

侯整风,男,1958 年生,教授,主要研究方向:计算机网络,信息安全。