基于 ECC 的门限秘密共享方案及其安全性

庞辽军，詹 阳，王育民
(西安电子科技大学 综合业务网理论与关键技术国家重点实验室，陕西 西安 710071)

摘要：基于椭圆曲线密码体制，提出一个新的 (t,n) 门限秘密共享方案. 该方案使用各参与者的私钥作为他们的秘密份额，秘密分发者不需要进行秘密份额的分配. 在秘密分发过程中，秘密分发者只需计算一些公开信息，而无需向各参与者传递任何信息. 在秘密重构过程中，每个合作的参与者只需向秘密计算者提交一个由秘密份额计算的、可验证的伪份额. 由于无需可信中心管理参与者密钥，且在秘密分发阶段无需任何秘密通信，因此，该方案具有良好的安全性和执行效率.

关键词：椭圆曲线密码体制；秘密共享；门限方案
中图分类号：TP918 **文献标识码**：A **文章编号**：1001-2400(2006)04-0572-04

Threshold secret sharing scheme based on ECC and its security

PANG Liao-jun, *ZHAN Yang*, *WANG Yu-min*
(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

Abstract: Based on elliptic curve cryptography, a novel (t,n) threshold secret sharing scheme is proposed. Each participant's private-key is used as his secret shadow and the secret dealer does not have to distribute each participant's secret shadow. In the secret distribution phase, the dealer only needs to compute some public values without sending any information to each participant. And in the secret recovery phase, each cooperative participant only needs to submit a verifiable pseudo-shadow instead of his secret shadow. The trusted center to manage participants' keys is eliminated and no secret communication is required in the secret distribution phase, so the scheme is characterized by excellent security as well as high efficiency.

Key Words: elliptic curve cryptography; secret sharing; threshold scheme

秘密共享概念是由 Shamir[1] 和 Blakley[2] 于 1979 年分别独立提出的. 自从秘密共享被提出后，许多研究人员对其做了大量的研究，并取得了不少成果[3~5]. 在大多数秘密共享方案中，参与者的秘密份额都是由秘密分发者选取并安全的传送给相应的参与者. 在实际应用中，这不仅增加了秘密分发者的计算、传输和存储复杂度，而且会使得秘密分发者常常成为攻击者的攻击目标，影响系统的安全性.

基于 ECC[6](椭圆曲线密码学)提出了一个新的 (t,n) 门限秘密共享方案. 它使用各参与者的私钥作为他们的秘密份额，秘密分发者不需要进行秘密份额的分配，而且在秘密分发过程中，秘密分发者只需计算一些公开信息，而不需要向各参与者传递任何信息，从而很大程度上提高了秘密分发的效率.

1 方案构成

1.1 系统参数

假设 E 为一条椭圆曲线，p 为一个奇素数，F_p 为包含 p 个元素的有限域，a 为椭圆曲线的基点，q 为 a 的

收稿日期：2005-08-07
基金项目：973 国家重大项目资助(G1999035805)；“十五”国家部委预研资助项目(Y1010122)
作者简介：庞辽军(1978-)，男，西安电子科技大学博士研究生.

阶,这里 q 也是一个奇素数. 系统由 n 个参与者和一位为各参与者所信赖的秘密分发者组成. 不失一般性,令 $P=\{P_1,P_2,\cdots,P_n\}$ 是 n 个参与者的集合,用 ID_i 表示参与者 P_i 的公开身份信息,它可以惟一代表参与者 P_i.

该方案还需要一个公告牌[4]. 任何人都有权阅读或下载公告牌上的内容,而只有系统中的合法用户才能在自己的权限允许的目录中发布信息,或修改、更新已发布的内容. 公告牌主要完成参与者之间的信息交流与发布. 例如,参与者的公开身份 ID_i 可通过其进行公开.

1.2　初始化过程

初始化过程主要完成各参与者的公钥、私钥以及群公钥的生成. 在该过程中,每个参与者 P_i 需要执行如下步骤:

(1) 随机选择一个整数 d_i.

(2) 随机构造一个 $(t-1)$ 次多项式 $f_i(x)=f_{i,0}+f_{i,1}x+\cdots+f_{i,t-1}x^{t-1} \bmod q$,其中多项式的系数 $f_{i,0}$, $f_{i,1},\cdots,f_{i,t-1}$ 为 Z_q 中的元素,并满足 $f_i(0)=f_{i,0}=d_i$ 且 $f_{i,t-1}\neq 0$.

(3) 对 P 中每一个参与者 $P_j(j\neq i)$,计算 $f_i(\mathrm{ID}_j)$,并将计算结果通过安全信道发送给相应的参与者 P_j. 同时,计算并公布校验信息 $f_{i,l}\cdot a$ $(l=0,1,\cdots,t-1)$. 参与者之间的安全信道只要求是保密信道即可,而不要求其为认证信道,可以通过预共享密钥或公钥密码技术来建立.

参与者 P_j 收到 $f_i(\mathrm{ID}_j)$ 后,可通过下面的等式来验证 $f_i(\mathrm{ID}_j)$ 的有效性.

$$f_i(\mathrm{ID}_j)\cdot a=\sum_{l=0}^{t-1}(\mathrm{ID}_j)^l(f_{i,l}\cdot a) \quad . \tag{1}$$

若等式(1)成立,那么 $f_i(\mathrm{ID}_j)$ 是有效的;否则是无效的,这时可要求 P_i 重新发送 $f_i(\mathrm{ID}_j)$.

(4) 如果参与者 P_i 已经收到其他每个参与者 $P_j(j\neq i)$ 按如上方法计算的秘密数据并验证有效,那么,P_i 可计算其私钥为 $\mathrm{SK}_i=\sum_{j=1}^{n}f_j(\mathrm{ID}_i)$.

(5) P_i 利用公开信息计算公钥 $\mathrm{GPK}=\sum_{j=1}^{n}f_{j,0}\cdot a$ 和他自己的公钥 $\mathrm{PK}_i=\mathrm{SK}_i\cdot a$,并将其通过公告牌进行公布.

1.3　秘密分发过程

不失一般性,假设所共享的秘密为 S,秘密分发者可执行以下步骤来完成秘密的分发:

(1) 采用文献[7]的方法,在椭圆曲线 E 上选取一个点 P_S,使得 P_S 的 x 坐标等于秘密 S.

(2) 在 $[1,q-1]$ 内随机选取一个整数 w.

(3) 计算 $B=w\cdot a \bmod q$ 和 $C=P_S+w\cdot \mathrm{GPK} \bmod q$.

(4) 将 B 和 C 在公告牌上进行公开.

1.4　秘密重构过程

任意 t 个或 t 个以上的参与者合作可重构所共享的秘密 S. 不失一般性,选取 P 中 t 个参与者 $P_1,P_2,\cdots,P_t$ 为例来说明秘密重构过程. 秘密重构过程如下:

(1) 每个合作的参与者 $P_i(i=1,2,\cdots,t)$ 利用自己的私钥计算 $e_i=B\cdot \mathrm{SK}_i\cdot a_i$,其中 $a_i=\prod_{j\in P,j\neq i}(\mathrm{ID}_j/(\mathrm{ID}_j-\mathrm{ID}_i))$. 然后,将计算结果 e_i 提交给指定的秘密计算者.

(2) 秘密计算者在收到每个合作的参与者 P_i 发送的 e_i 时,可利用公开信息重新计算 a_i,并通过验证等式 $B\cdot \mathrm{PK}_i\cdot a_i=e_i\cdot a$ 是否成立来验证 P_i 提交的信息的正确性. 如果等式成立,那么 P_i 所提交的信息是正确的,接着执行下面的步骤;否则,说明 P_i 没有诚实地给出自己的计算结果,或者消息在传送过程中可能出错,这时,秘密计算者可要求其重新发送 e_i,或者进行其他相应的出错处理.

(3) 通过如下计算,秘密计算者可得到椭圆曲线上的点 $P_S=C-\sum_{i=1}^{t}e_i$.

(4) 秘密计算者从所得的点 P_S 的 x 坐标得到所共享的秘密 S.

2 分析和讨论

2.1 正确性分析

定理 1 在初始化阶段,参与者 P_j 能够验证 P_i 所发送的信息 $f_i(\mathrm{ID}_j)$ 的真伪.

证明 根据参与者 P_i 所公开的校验信息 $f_{i,l}\cdot a(l=0,1,\cdots,t-1)$,等式(1)可写成

$$f_i(\mathrm{ID}_j)\cdot a = f_{i,0}\cdot a + \mathrm{ID}_j\cdot f_{i,1}\cdot a + (\mathrm{ID}_j)^2\cdot f_{i,2}\cdot a + \cdots + (\mathrm{ID}_j)^{t-1}\cdot f_{i,t-1}\cdot a \quad .$$

根据公开信息,P_j 可通过验证上式是否成立来验证 P_i 所发送的信息 $f_i(\mathrm{ID}_j)$ 的正确性,以便防止 P_i 进行欺骗.

定理 2 在秘密重构阶段,秘密计算者能够验证合作的参与者 P_i 所发送的信息 e_i 的真伪.

证明 由等式 $e_i = B\cdot \mathrm{SK}_i\cdot a_i$ 可得到等式 $B\cdot \mathrm{PK}_i\cdot a_i = e_i\cdot a$,其中 PK_i 是 P_i 的公钥($\mathrm{PK}_i = \mathrm{SK}_i\cdot a$).接着,秘密计算者可通过公开信息计算出 a_i.这时,秘密计算者就可通过验证 $B\cdot \mathrm{PK}_i\cdot a_i = e_i\cdot a$ 是否成立来发现 e_i 的真伪.

定理 3 在秘密重构阶段,秘密计算者计算的点 P_S 的 x 坐标等于所共享的秘密 S.

证明 由等式 $C = P_S + w\cdot \mathrm{GPK} \bmod q$, $B = w\cdot a \bmod q$, $e_i = B\cdot \mathrm{SK}_i\cdot a_i$ 和 $\mathrm{SK}_i = \sum_{j=1}^{n} f_j(\mathrm{ID}_i)$,以及 Lagrange 插值定理[1],可得到:

$$C - \sum_{i=1}^{t} e_i = C - \sum_{i=1}^{t} B\cdot \mathrm{SK}_i\cdot a_i =$$

$$C - B\Big(\sum_{i=1}^{t}\Big(\sum_{k\in P} f_k(\mathrm{ID}_i)\cdot \prod_{j\in P, j\neq i}(\mathrm{ID}_j/(\mathrm{ID}_j - \mathrm{ID}_i))\Big)\Big) =$$

$$C - B\sum_{k\in P}\Big(\sum_{i=1}^{t} f_k(\mathrm{ID}_i)\cdot \prod_{j\in P, j\neq i}(\mathrm{ID}_j/(\mathrm{ID}_j - \mathrm{ID}_i))\Big) =$$

$$C - w\cdot a\cdot \sum_{k\in P} f_{k,0} = C - w\cdot \sum_{k\in P} f_{k,0}\cdot a = P_S + w\cdot \mathrm{GPK} - w\cdot \mathrm{GPK} = P_S \quad .$$

因此,结论得证.

2.2 安全性分析

本方案可能会存在以下攻击.下面,通过对这些攻击进行分析来说明方案的安全性.

(1) 在初始化阶段,某参与者 P_i 发送给其他参与者 $P_j(i\neq j)$ 一个假的信息 $f_i'(\mathrm{ID}_j)$ 来试图欺骗 P_j.

分析 由定理 1 可知,通过等式(1)可验证 $f_i'(\mathrm{ID}_j)$.因为多项式 $f_i(x)$ 的系数校验信息 $f_{i,l}\cdot a\ (l=0,1,\cdots,t-1)$ 是公开的.因此,任何假的信息 $f_i(\mathrm{ID}_j)$ 都不会使等式(1)的验证成立.

(2) 在秘密重构阶段,某参与者 P_i 可能会提供假的信息 e_i 来欺骗其他参与者.

分析 由定理 2 可知,通过等式 $B\cdot \mathrm{PK}_i\cdot a_i = e_i\cdot a$ 可验证 P_i 提交信息的真伪.由于除 e_i 外其他的信息都是公开的或可计算的,因此,要找到一个假的 e_i 并满足等式是不可行的.

(3) 攻击者试图由参与者 P_i 的公钥 PK_i 来推导他的私钥 SK_i.

分析 攻击者通过 P_i 的公钥 PK_i 来推导其私钥 SK_i 面临着求解椭圆曲线离散对数问题的困难性.而且,各参与者间使用的都是安全信道,因此,要得到参与者 P_i 的私钥是计算上不可行的.

(4) 攻击者试图由群公钥 GPK 来推导群私钥 GSK.

分析 定理 3 证明过程中的 $\sum_{i=1}^{t}\Big(\sum_{k\in P} f_k(\mathrm{ID}_i)\cdot \prod_{j\in P, j\neq i}(\mathrm{ID}_j/(\mathrm{ID}_j - \mathrm{ID}_i))\Big)$ 实质上就是集合 P 的群私钥 GSK,且满足 $\mathrm{GPK} = \mathrm{GSK}\cdot a$[7].如果能得到 GSK,就可直接由 B 和 C 求出 S.而由群公钥 GPK 来推导群私钥 GSK 同样面临求解椭圆曲线离散对数问题的困难性.

(5) 攻击者试图从公开信息 B 和 C 中直接计算出秘密 S 来.

分析 要从公开信息 B 和 C 中直接计算出秘密 S,攻击者将会面临求解椭圆曲线离散对数问题的困难性,因此,这种攻击无法奏效.

3 结　论

在 ECC 的基础上,提出了一个新的 (t,n) 门限秘密共享方案. 参与者的秘密份额为各自的私钥;在秘密分发阶段,秘密分发者不需要向各参与者传送任何信息;在秘密重构阶段,每个合作的参与者只需提交一个伪份额,且任何人可验证该信息的真实性. 本方案不需要可信中心管理参与者密钥,同时又具有 ECC 在安全性和计算效率方面的优点,因此,具有良好的安全性和执行效率.

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. Safeguarding Cryptographic Keys[A]. Proc AFIPS 1979 Natl Conf[C]. New York: AFIPS Press, 1979. 313-317.

[3] Xu Chunxiang, Fu Xiaotong, Xiao Guozhen. A Vector Space Secret Sharing Scheme Against Cheating[J]. Journal of Xidian University, 2002, 29(4): 527-529.

[4] Pang Liaojun, Wang Yumin. A New (t,n) Multi-secret Sharing Scheme Based on Shamir's Secret Sharing[J]. Applied Mathematics and Computation, 2005, 167(2): 840-848.

[5] 庞辽军,王育民. 一个基于几何性质的(t,n)多重秘密共享方案[J]. 西安交通大学学报,2005, 39(4): 425-428.

[6] Miyazaki K, Takaragi K. A Threshold Digital Signature Scheme for a Smart Card Based System[J]. IEICE Trans on Fundamentals, 2001, E84-A(1): 205-213.

[7] Chang T Y, Yang C C, Hwang M S. A Threshold Signautre Scheme for Group Communications without a Shared Distribution Center[J]. Future Generation Computer Systems, 2004, 20(6): 1 013-1 021.

(编辑: 高西全)

(上接第 567 页)

[3] Intarapanich A, Kafle P L, Davies R J, et al. Effect of Tap Gain Correlation on Capacity of OFDM MIMO Systems[J]. IEE Electron Lett, 2004, 40(1): 86-88.

[4] Adachi F, Tjhung T T. Tapped Delay Line Model for Band-limited Multipath Channel in DS-CDMA Mobile Radio[J]. IEE Electron Lett, 2001, 37(5): 318-319.

[5] Kermoal J P, Schumacher L, Pedersen K I, et al. A Stochastic MIMO Radio Channel Model with Experimental Validation [J]. IEEE J Select Areas Comm, 2002, 20(6): 1 211-1 226.

[6] Brewer J W. Kronecker Products and Matrix Calculus in System Theory[J]. IEEE Trans on Circuits Syst, 1978, 25(9): 772-781.

[7] Chizhik D, Farrokhi F R, Ling J, et al. Effect of Antenna Separation on the Capacity of BLAST in Correlated Channels [J]. IEEE Commun Lett, 2000, 4(11): 337-339.

[8] Oyman O, Nabar R U, Bolcskei H, et al. Characterizing the Statistical Properties of Mutual Information in MIMO Channels[J]. IEEE Trans on Signal Processing, 2003, 51(11): 2 784-2 795.

(编辑: 高西全)