基于椭圆曲线离散对数的组签名方案

石润华,仲 红
(安徽大学 计算机科学与技术学院,安徽 合肥 230039)

摘 要:介绍了组签名及其安全性要求,并提出了两种基于椭圆曲线离散对数的组签名方案。理论分析表明这两个方案是安全、有效的,而且均符合组签名的安全性要求。其中,对于第一种方案,授权签名非常简单,特别适宜于成员较少的组签名;而对于第二种方案,签名与组大小无关,尤其适宜于大型动态组的签名。

关键词:公钥密码;椭圆曲线;离散对数;组签名
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2007)11-0153-04

Group Signature Schemes Based on Elliptic Curve Discrete Logarithm

SHI Run-hua, ZHONG Hong
(School of Computer Science and Technology, Anhui University, Hefei 230039, China)

Abstract: Introduces group signature and its security character, and proposes two group signature schemes based on elliptic curve discrete logarithm. The theory analysis shows that the schemes are correct, secure and efficient, and satisfy the group security character. Where, for the first scheme, it is very simple to authorize the signature, which fits the small group, and for the second scheme, it is irrespective between the signature size and the group size, which fits the large dynamic group.

Key words: public-key cryptography; elliptic curve; discrete Logarithm; group signature

0 引 言

椭圆曲线密码体制,即基于椭圆曲线离散对数问题的各种公钥密码体制,最早于1985年由Miller[1]和Koblitz[2]分别独立地提出。它是利用有限域上椭圆曲线的有限点群代替基于离散对数问题密码体制中的有限循环群所得到的一类密码体制。椭圆曲线密码系统(ECC)是迄今为止每比特具有最高安全强度的密码系统。与其他公钥密码系统相比,椭圆曲线密码系统除了安全性高外,还具有计算负载小、密钥尺寸短、占用带宽少等优点[3~5]。因此,椭圆曲线密码系统被认为是下一代通用的公钥密码系统。

数字签名最早由Diffie和Hellman[6]提出。数字签名是一个与信息 m 和签名者公钥有关系的二进制字符串,是手写签名的数字模拟。一方面,已知签名者的公钥和信息 m,每个人能验证一个签名;另一方面,仅仅签名者,也即知道私钥的一方,能够计算一个签名。例如:RSA数字签名[7],厄格玛尔(ElGamal)数字签名[8,9],Schnorr数字签名[10],椭圆曲线数字签名[11]。

组签名由Chaum和Van Heyst[12]于1991年第一次提出。接着Chen和Pedersen[13]对其进行了改进,提出了两种新的不可否认的组签名方案。随后Jan Camenisch等[14,15]又对其进行了修改。在组签名方案中,一个经授权的组成员能代表组进行有效签名。任何人能验证它的有效性,却不知签名者的身份,即具有匿名签名的特征。另外,除了组管理者以外的任何人都不能确定两个签名是否是同一成员所签。但在引起纠纷时,一个可信赖的组管理者通过打开程序,能识别出签名者的身份。基于这些特点,组签名在匿名投票、电子商务、军事、法律等领域有着广泛应用。

但已有的组签名方案多是建立在DLP计算难题之上,而文中提出了两种基于ECDLP的组签名方案。第一种方案,特别适宜于成员较少的组签名,而第二种方案尤其适合于大型动态组的组签名。

1 基于椭圆曲线离散对数的组签名方案

一般地一个完整的组签名方案应该包括以下五个

收稿日期:2007-01-29
基金项目:安徽省自然科学基金资助项目(070412051);安徽高校省级重点自然科学研究项目(KJ2007A043);安徽大学人才队伍建议经费资助
作者简介:石润华(1974-),男,安徽安庆人,硕士,讲师,研究方向为信息安全;仲 红,博士,副教授,研究方向为信息安全、分布式计算。

部分[16]：

(1)建立(SETUP)：系统初始化，生成组管理者私钥、公钥(组公钥)。

(2)加入(JOIN)：根据组管理者和新成员之间的交互协议，生成新成员的私钥、公钥，及签名资格证书(授权)。

(3)签名(SIGN)：输入待签名信息、组成员私钥、组公钥、签名资格证书，生成有效的签名。

(4)验证(VERIFY)：输入签名的信息、签名和组公钥，确定签名是否有效。

(5)打开(OPEN)：输入用户签名和组管理者的私钥，生成签名者的身份标识。

而一个有效的组签名方案还应该满足下列安全性要求：

①正确性：任何一个经授权的组成员按照签名程序生成的签名都是有效的。

②不可伪造性：仅有授权的组成员能够生成一个有效的签名。

③匿名性：除非组管理者，识别签名者的身份是计算难题。

④不可连接性：除了组管理者，确定两个签名是否是同一成员所签，也是计算难题。

⑤可跟踪性：组管理者总能在需要时打开签名者的身份标识。

⑥不可陷害性：组管理者或者任何一个组成员都不能陷害别的组成员，生成一个与别的组成员有关的签名。

⑦抵抗联合攻击性：即使一些授权的组成员串通在一起，也不能产生一个有效的不可被跟踪的组签名。

根据这些特点和要求，设计了以下两种基于ECDLP的组签名方案。

1.1 方案一

①建立：在有限域 $F_q(q = p \text{ or } 2^m)$ 上选择一条安全的椭圆曲线，确定椭圆曲线域参数 $D = (q, FR, a, b, G, n, h)$[10]。随机选择一整数 $d, 0 < d < n$，作为组管理者的私钥。计算 $Q = dG$，作为组公钥。选择一单向无冲突函数 $H: \{0,1\}^* \rightarrow \{0,1\}^l$。初始化表 $S = \emptyset$(初始为空)，S 用来存放经组管理者授权可代表组签名的合法用户的公钥。组管理者公布椭圆曲线域参数 $D = (q, FR, a, b, G, n, h)$、组公钥 Q、表 S 和函数 H。组管理者保密私钥 d。

②加入：若用户 u_i 想加入签名组，则要向组管理者登记，申请签名资格证书(即授权)。首先用户 u_i 秘密地随机选取一个整数 $x_i, 0 < x_i < n$，作为私钥。计算出公钥 $Y_i = x_iG$。用户通过安全渠道送 Y_i 给组管理者，组管理者经过审核该用户身份后，若同意该用户加入组并可代表组进行签名，则把用户公钥 Y_i 加入表 $S = \{Y_1, \cdots, Y_{i-1}\}$，并再次公开发布 $S = \{Y_1, \cdots, Y_i\}$。

③签名：经组管理者授权的用户，对信息 m 进行签名包括以下三个步骤：

第一步，加密代表其身份的标识 Y_i(简单起见，这里把用户公钥 Y_i 作为其身份标识)，以便在引起纠纷时，组管理者可运行打开程序，识别签名者的身份。用户随机选择一个整数 $k, 0 < k < n$。计算：$A = k \cdot G$ 和 $B = k \cdot Q + Y_i$。

第二步，基于椭圆曲线离散对数的知识证明的签名，证明用户确实知道 Y_i 的椭圆曲线离散对数，即知道 $x_i(Y_i = x_iG)$ 但不泄露任何与身份有关的信息。签名者随机选取整数 $k_1, k_2 \in (0, n)$，计算 $\bar{r} = F_x(k_1Q + k_2G)$，$\bar{s}_1 = (k_1 - \bar{r}k) \bmod n$，$\bar{s}_2 = (k_2 - \bar{r}x_i) \bmod n$，其中 F_x 是一个取点 x 坐标的函数。

第三步，基于椭圆曲线离散对数相等的知识证明的签名。即在 $i \in [1, t]$ 中，至少有一个 i 对应的点 $B - Y_i$ 以 Q 为基点的椭圆曲线离散对数；与点 A 以 G 为基点的椭圆曲线离散对数相等的知识证明的签名(因为其中存在一个 $B - Y_i = kQ + Y_i - Y_i = kQ$，而 $A = kG$)，其中 $t = |S|$。从而保证 B 中加密的 Y_i 确实是经组授权的用户标识。随机选取整数 $k_i \in (0, n), i \in [1, t], c_i \in (0, n), i \in [1, t]$。令 $B_i = B - Y_i, i \in [1, t], e = \text{Int}(H(m))$ (Int() 表示字符转换成整数)。假设用户 u_j 正在签名，则计算：

$$r_j = k_jQ, r_i = k_iQ - c_iB_i, i \in [1, j-1] \cup [j+1, t]$$

$$t_j = k_jG, t_i = k_iG - c_iA, i \in [1, j-1] \cup [j+1, t]$$

$$s_j = e(k_j + c_jk) (\text{mod } n), s_i = ek_i, i \in [1, j-1] \cup [j+1, t]$$

则用户 u_j 对信息 m 的数字签名为 $(A, B, \bar{r}, \bar{s}_1, \bar{s}_2, c_1, \cdots, c_m, s_1, \cdots, s_m, r_1, \cdots, r_m, t_1, \cdots, t_m)$。

④验证：若 $F_x(\bar{s}_1Q + \bar{s}_2G + \bar{r}B) = \bar{r}$，且 $s_ie^{-1}Q = c_iB_i + r_i, s_ie^{-1}G = c_iA + t_i, i \in [1, t], B_i = B - Y_i, Y_i \in S$ 均成立，则签名有效，否则无效，其中 $e = \text{Int}(H(m))$。

⑤打开：在引起纠纷时，组管理者计算 $ID = B - dA$，就可打开签名者身份标识。因为 $ID = B - dA = k \cdot Q + Y_i - dkG = kQ + Y_i - kQ = Y_i$。

签名验证的证明：

第一步，

$$\bar{s}_1Q + \bar{s}_2G + \bar{r}B = (k_1 - \bar{r}k)Q + (k_2 - \bar{r}x_i)G +$$

$\bar{r}B = k_1Q + k_2G + \bar{r}(B - kQ - x_iG) = k_1Q + k_2G + \bar{r}(B - kQ - Y_i) = k_1Q + k_2G$

所以

$$F_x(\bar{s}_1Q + \bar{s}_2G + \bar{r}B) = F_x(k_1Q + k_2G) = \bar{r}$$

第二步,

当 $i = j$ 时

$s_je^{-1}Q = e(k_j + c_jk)e^{-1}Q = (k_j + c_jk)Q = k_jQ + c_jkQ = r_j + c_j(B - Y_j) = c_jB_j + r_j$

$s_je^{-1}G = e(k_j + c_jk)e^{-1}G = (k_j + c_jk)G = k_jG + c_jkG = c_jA + t_j$

当 $i \neq j$ 时

$s_ie^{-1}Q = ek_ie^{-1}Q = k_iQ = c_iB_i + r_i$

$s_je^{-1}G = ek_ie^{-1}G = k_iG = c_iA + t_i$

1.2 方案二

①建立:在有限域 $F_q(q = p \text{ or } 2^m)$ 上选择一条安全的椭圆曲线,确定椭圆曲线域参数 $D = (q, FR, a, b, G, n, h)$。随机选择一整数 $d, 0 < d < n$,作为组管理者的私钥。计算 $Q = dG$,作为组公钥。选择单向无冲突函数 $H: \{0,1\}^* \to \{0,1\}^l$,定义函数 $F_x: P \to x$,其中 $P = (x, y)$ 是椭圆曲线上的点。组管理者公布椭圆曲线域参数 $D = (q, FR, a, b, G, n, h)$、组公钥 Q 和函数 H 及 F_x。组管理者保密私钥 d。

②加入:若用户 u_i 想加入签名组,则要向组管理者 M 登记,申请签名资格证书(即签名授权)。需执行以下交互协议:

u_i:随机选取整数 $z_i \in (1, n)$,计算 $ID_i = z_iG$。把 ID_i 送给 M。

M:随机选取整数 $k \in (1, n)$,计算 $P_m = kG$,把 P_m 送给 u_i。

u_i:随机选取整数 $t \in (1, n)$,计算 $P_i = P_m + tG$,把 P_i 送给 M。

M:计算 $s_m = dF_x(ID_i + P_i) + k$,把 s_m 送给 u_i。计算并保存 $(ID_i, F_x(ID_i + P_i)Q)$,用以组管理者在运行打开程序时,鉴别用户身份。

u_i:计算 $x_i = s_m + t$。

u_i:检验 $Y_i = x_iG = F_x(ID_i + P_i)Q + P_i$ 成立否。若成立,则 (P_i, x_i) 就是组管理者授权的签名资格证书,并作为用户的签名私钥。

③签名:

第一步,加密代表其身份的标识 ID_i,以便在引起纠纷时,组管理者可运行打开程序,识别签名者的身份。用户随机选择一个整数 $l_1, 0 < l_1 < n$。计算 $A = l_1 \cdot G, B = (l_1 + F_x(ID_i + P_i))Q$(间接加密 ID_i)。

第二步,基于椭圆曲线离散对数相等的知识证明的签名。保证上一步已加密的身份标识 ID_i,与组管理者授权的签名资格证书中含有(间接)的用户标识 ID_i 相同。这样就间接证明了第一步中加密的确实是签名者自己的真实身份标识。令 $C = (x_i - l_2)G, l_2 \in (0, n), D = P_i + l_3G, l_3 \in (0, n)$。用户随机选择整数 k_1、k_2 和 $k_3, k_1, k_2, k_3 \in (0, n)$。计算 $r = F_x(k_1G + k_1Q + k_2G + k_3G), s_1 = k_1 - rl_1 (\text{mod } n), s_2 = k_2 - rl_2 (\text{mod } n), s_3 = k - rl_3 (\text{mod } n)$。

第三步,用户用签名私钥 (P_i, x_i) 对信息 m 进行如下签名。用户 u_i 随机选取整数:t_1、t_2 和 $t_3, t_1, t_2, t_3 \in (1, n)$ 并计算:

$e = \text{Int}(H(m))$ (Int() 表示字符转换成整数)

$\bar{r} = F_x(t_1G - t_2Q - t_3eG)$

$\bar{s}_1 = e(t_1 - \bar{r}x_i) (\text{mod } n)$

$\bar{s}_2 = e(t_2 - \bar{r}F_x(ID_i + P_i)) (\text{mod } n)$

$P = t_3eG - \bar{r} \cdot P_i$

用户 u_i 对信息 m 的有效签名为 $(A, B, C, D, P, r, s_1, s_2, s_3, \bar{r}, \bar{s}_1, \bar{s}_2)$。

④验证:若 $r = F_x(s_1G + s_1Q + s_2G + s_3G + r(A + B - C + D))$,并且 $\bar{r} = F_x(\bar{s}_1e^{-1}G - \bar{s}_2e^{-1}Q - P)$ 均成立,则签名有效,否则无效,其中 $e = \text{Int}(H(m))$。

⑤打开:在引起纠纷时,组管理者计算 $B - dA$,就可打开签名者身份标识。因为 $B - dA = l_1 \cdot Q + F_x(ID_i + P_i)Q - dl_1G = l_1Q + F_x(ID_i + P_i)Q - l_1Q = F_x(ID_i + P_i)Q$。根据计算结果查找对应的 $(ID_i, F_x(ID_i + P_i)Q)$,即可得到签名者的 ID_i。

签名验证的证明:

因为

$$s_1G + s_1Q + s_2G + s_3G - r(A + B - C + D) = (k_1 - rl_1)G = (k_1 - rl_1)Q + (k_2 - rl_2)G + (k_3 - rl_3)G + r(l_1G + (l_1 + F_x(ID_i + P_i))Q - (x_i - l_2)G + (P_i + l_3G)) = k_1G + k_1Q + k_2G + k_3G + r(F_x(ID_i + P_i)Q - x_iG + P_i) = k_1G + k_1Q + k_2G + k_3G$$

所以

$$F_x(s_1G + s_1Q + s_2G + s_3G + r(A + B - C + D)) = F_x(k_1G + k_1Q + k_2G + k_3G) = r$$

又因为

$$\bar{s}_1e^{-1}G - \bar{s}_2e^{-1}Q - P = e(t_1 - \bar{r}x_i)e^{-1}G - e(t_2 - \bar{r}F_x(ID_i + P_i))e^{-1}Q - (t_3eG - \bar{r} \cdot P_i) = t_1G - t_2Q - t_3eG + \bar{r}(-x_iG + F_x(ID_i + P_i)Q + P_i) = t_1G - t_2Q - t_3eG$$

所以

$$F_x(\bar{s}_1e^{-1}G - \bar{s}_2e^{-1}Q - P) = F_x(t_1G - t_2Q - t_3eG)$$

$= \bar{r}$

2 安全性分析

以上方案的正确性,来源于上面签名验证的证明。而安全性都是建立在椭圆曲线离散对数计算难题之上。下面分析方案均符合组签名的安全性要求。

经组管理者授权的用户称为合法用户,在以上两个方案中,只有合法用户才能进行有效签名。因为非法用户不知道签名私钥,除非他能破解椭圆曲线离散对数问题,否则他不可能伪造签名。另外虽然是合法用户,但他不可能知道其它合法用户的签名私钥,所以也不可能伪造、陷害其它合法用户进行有效签名。因此,两方案均具有不可伪造性和不可陷害性。其次,在以上两方案中,对于两次不同的签名,参数完全不同,两者之间没有任何关系,所以均具有匿名签名和不可连接性。再有,在引起纠纷时,组管理者都可以执行打开程序,辨别签名者身份。也即均具有可跟踪性和抵抗联合攻击性。因此,方案均符合组签名的安全性要求。

在所提出的两种方案中,组管理者的公、私钥在签名组建立过程中就已生成,用户公、私钥也是在签名前就已定好,与组大小无关。这不仅能保证方案更安全,而且更有效。另外,在方案一中,虽然签名与组大小成线性关系,但授权签名极其简单,只需把用户公钥加入表 S 中,并再次公开发布 S,所以特别适宜于成员相对较少的组签名。而在方案二中,签名与组大小无关,这一特性使得这一方案非常适合于有着许多成员的大型动态组的组签名。

3 总 结

文中分析了组签名及其安全性要求。基于目前组签名方案多是建立在 DLP 计算难题之上,而 ECDLP 是比一般 DLP 困难得多的问题,提出了两种基于 ECDLP 的组签名方案。这两种方案均是建立在 ECDLP 计算难题之上,并满足组签名的所有安全性要求。在所设计的两种方案中,其中第一种方案授权签名非常简单,特别适合于成员较少的组签名;而后一种方案,签名与组大小无关,这一特性使得这一方案非常适宜于成员较多的大型动态组的组签名。

参考文献:

[1] Miller V. Uses of elliptic curves in cryptography[C]//Advances in Cryptology - CRYPTO'85, Lecture Notes in Computer Science, volume 218. [s. l]: Springer - Verlag, 1986: 417 - 426.

[2] Koblitz N. Elliptic curve cryptosystems[J]. Math Comp, 1987,48:203 - 209.

[3] 石润华,钟 诚. 基于椭圆曲线密码体制的大型动态多播组的分层二级密钥管理[J]. 计算机工程与科学,2003,25(6):22 - 24.

[4] 石润华,葛丽娜,钟 诚. 椭圆曲线密码体制上一种快速 kP 算法[J]. 计算机工程与科学,2004,26(4):55 - 58.

[5] Shi Runhua, Cheng Jiaxing. Two New Fast Methods for Simultaneous Scalar Multiplication in Elliptic Curve Cryptosystems[C]//Networking and Mobile Computing, Third International Conference, ICCNMC 2005. Lecture Notes in Computer Science 3619. Berlin, Heidelberg: Springer - Verlag, 2005:462 - 470.

[6] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 22:644 - 654.

[7] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public - key cryptosystems[J]. Communications of the ACM, 1978, 21(2):120 - 126.

[8] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[C]//In Blakley G R, Chaum D. Advances in Cryptology - CRYPTO'84, volume 196 of Lecture Notes in Computer Science. Berlin, Heidelberg: Springer - Verlag, 1985:10 - 18.

[9] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans on Information Theory, 1985, 31(4):469 - 472.

[10] Schnorr C P. Efficient signature generation for smart cards [J]. Journal of Cryptology, 1991, 4(3):239 - 252.

[11] Johnson D, Menezes A, Vanstone S. The Elliptic Curve Digital Signature Algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1):36 - 63.

[12] Chaum D, van Heyst E. Group signatures[C]//Advances in Cryptology - EUROCRYPT' 91, volume 547 of Lecture Notes in Computer Science. Berlin, Heidelberg: Springer - Verlag, 1991:257 - 265.

[13] Chen L, Pedersen T P. New group signature schemes[C]// Advances in Cryptology - EUROCRYPT'94, volume 950 of Lecture Notes in Computer Science. Berlin, Heidelberg: Springer - Verlag, 1995:171 - 181.

[14] Camenish J, Stadler M. Efficient Group Signature Schemes for Large Groups[C]//Advances in Cryptology - CRYPTO'97, volume 1294 of Lecture Notes in Computer Sciences. Berlin, Heidelberg: Springer Verlag, 1997:410 - 424.

[15] Camenisch J. Efficient and Generalized Group Signatures[C/OL]. 2001. Advances in Cryptology - EUROCRYPT' 97. Available at http://citeseer. nj. nec. com/camenisch97 efficient. html.

[16] Bresson E, Stern J. Efficient Revocation in Group Signatures [EB/OL]. 2001. http://citeseer. nj. nec. com/476498. html.