文章编号:1009-3087(2013)05-0076-04

# 一种高效的无证书广播签密方案

李战虎[1,2],樊 凯[1],李 晖[1]
(1. 西安电子科技大学 ISN 重点实验室,陕西 西安 710071;2. 咸阳师范学院 数学与信息科学学院,陕西 咸阳 712000)

**摘 要**:为了能使保密信息能够更安全、更有效地通过不安全的广播信道发送给已授权的用户集及公钥密码中的密钥托管问题,结合整数环上圆锥曲线上的密码技术,提出了一种新型的无证书广播签密方案。先分析方案的正确性,其次在基于大数分解和圆锥曲线上离散对数双重困难问题下分析了方案具有强不可伪造性和机密性,最后分析了方案的有效性。结果表明,所提方案在签密和解签密上减少了运算量,提高了网络运算效率。

**关键词**:签密;广播;无证书;圆锥曲线;整数环
**中图分类号**:TP309.7;TN918 **文献标志码**:A

## An Efficient Certificateless Broadcast Signcryption Scheme

*LI Zhan-hu*[1,2], *FAN Kai*[1], *LI Hui*[1]
(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China;
2. Xianyang Normal Univ., Xianyang 712000, China)

**Abstract**: In order to securely and efficiently transmit the privacy information to authorized users' set through the unsafe channel and avoid key escrow, a new type certificateless broadcast signcryption scheme was put forward by using the cryptographic techniques on conic curve. First, correction of the scheme was analyzed and then the scheme was proven to have the properties of stronger unforgeability and confidentiality by using the hard problems of large number factorization and discrete logarithm on conic curve. Finally, the efficiency of the scheme was analyzed. It was shown that it has the high efficiency in computation cost for signcryption and designcryption, which improves the efficiency of network operation.

**Key words**: signcryption; broadcast; certificateless; conic curve; integer ring

1997年,Zheng[1]首次提出了签密概念。签密技术本质上是将加密技术和签密技术融入在同一个逻辑过程中,从而同时可以实现消息的保密性和认证性,相比于传统的"先加密,再签名"技术无论在方法上还是计算量上都更为有效。因此关于签密技术的研究引起了众多学者的极大关注[2-4]。1984年,Shamir[5]提出了基于身份的密码体制(identity-based cryptography)的概念,简化了密钥的管理。在基于身份的密码体制中,用户的公钥可以由用户的身份信息直接生成,而用户的私钥则是由私钥生成中心(private key generator,PKG)生成。基于身份的密码体制取消了公钥证书,减少了公钥证书的存储和合法性验证,减少了建立和管理公钥认证架构的系统复杂性和代价。然而,直到2001年,Boneh和Franklin[6]才首次给出了1个利用椭圆曲线上的双线性映射(bilinear-map)可实现而且安全的基于身份的加密方案。由此,基于身份的加密或签名体系得到了迅速发展[7-11]。但是,该体制也存在这样一个缺陷:所有用户私钥都是由PKG生成,这就使得PKG可以很容易的冒充任何用户而不被发现。为了解决在基于身份的密码体制中所存在的密钥托管问题,Al-Riyami和Paterson[12]提出了无证书密码体制(certificateless cryptography)概念。该体制不需要公钥证书,且没有密钥托管问题,是介于PKI和基于身份的密码体制之间的1种密码模式。无证书密码

**收稿日期**:2013-04-11
**基金项目**:国家自然科学基金资助项目(61303216);中国博士后科学基金资助项目(2013M542328);中央高校基本科研业务费专项资金项目(K5051201003);国家科技重大专项项目(2012ZX03002003);陕西省自然科学基金项目(2009JQ1009);陕西省自然科学专项基金项目(09Jk803);咸阳师范学院专项科研基金项目(11XSYK305)
**作者简介**:李战虎(1978—),男,博士生. 研究方向:网络与信息安全.

体制仍然是使用 PKG 的可信第三方,但是这个第三方并不知道用户的私钥。PKG 利用自己的主密钥和用户的身份计算出 1 个部分私钥并将这个部分私钥发送给用户,用户联合部分私钥和自己的秘密信息生成实际的私钥。所以这个系统不是基于身份的,因为公钥并不能从用户的身份直接计算出来。

广播加密是针对于 1 个发送者和多个接收者所提出的密码技术,这种技术是将加密的消息通过不安全的信息通道发送给动态改变的用户集,例如数字电视系统、局域网络系统等等。广播加密确保只有已经授权的用户才能够解密密文,未经授权的用户是得不到任何消息的。广播签密是通过将广播加密技术和数字签名技术结合起来的密码技术,因此可以同时能够对信息的保密和认证提供有效的处理。Fiat 和 Naor[13] 首先形式化了介绍了广播加密这一问题,该问题引起了密码学者的极大兴趣[14-17]。Selvi 等[18] 提出 1 个可证明安全的基于身份的广播签密方案。祁正华等[19] 在 Selvi 方案的基础上提出了 1 个改进的基于身份的广播签密方案(IBSC),对广播签密运行环境的安全性和运算效率进行有效的改进。

基于上述的基本思想,作者利用整数环上圆锥曲线上的密码技术提出了 1 个基于双难问题下的无证书广播签密方案,所提签密方案除了解决常规基于身份的签密体制所存在的密钥托管问题外,在安全性上也具有更好的保障,同时和已有的广播签密方案相比,在签、解密算法阶段计算量上均有极大的改进。

## 1　整数环上的圆锥曲线

正整数环 $Z_n$ 上的圆锥曲线 $C_n(a,b)$ 定义为同余方程 $y^2 = ax^2 - bx(\mathrm{mod}\ n)$,其中,$(a,n) = (b,n) = 1$,且 $n = pq$,这里 $p,q$ 为 2 个不同的大素数。孙琦等[20] 定义了曲线 $C_n(a,b)$ 上点的加法"+"和点乘运算,指出了 $(C_n(a,b), +)$ 构成了一个有限交换群,这为在群 $C_n(a,b)$ 上建立密码体制奠定了理论基础。进一步地,当 $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$,$p+1 = 2r$,$q+1 = 2s$,其中 $r,s$ 也是素数时,在曲线 $C_n(a,b)$ 上存在着这样一类点 $G$,其阶为 $N_n = 2rs$,称这样的点为基点。而集合 $S = \{0,G,2G,\cdots,(N_n-1)G\}$ 构成了 $C_n(a,b)$ 的一个子群。相比椭圆曲线,圆锥曲线是具有明文嵌入容易,同时也易于从曲线中恢复出明文、曲线群的阶容易计算,点的易于求逆等性质的代数曲线。研究表明[21],圆锥曲线由于明文嵌入容易,点的运算简单,如果利用标准二进制来表示,则更能节约近 $\frac{1}{4}$ 的运算量,并被证明无法再改进。

群 $S$ 上的困难问题 —— 离散对数和椭圆曲线上的离散对数一样,在圆锥曲线上也存在离散对数困难问题,即就是给定曲线上的两个点 $P,Q \in S$,寻找一个正整数 $K \in Z_{N_n}$ 使得 $Q = kP$ 在计算上是不可行的。

基于以上特征,在 $C_n(a,b)$ 上建立公钥密码和数字签名逐渐得到充实和完善。关于 $C_n(a,b)$ 的公钥密码方案和数字签名方案已经得到了许多学者的关注。尤其是最近几年,利用曲线 $C_n(a,b)$ 已经得到了许多具有特殊意义的数字签名和数字签密。

## 2　圆锥曲线上的广播签密方案

方案主要包含了系统建立、密钥提取、用户注册、用户注销、签密和解签密几个部分。

1) 系统建立:选择 1 个密码学上的圆锥曲线 $C_n(a,b): y^2 = ax^2 - bx(\mathrm{mod}\ n)$,其中,$a,b \in Z_n$,且和 $n$ 均互素,$n = pq$,$p$、$q$ 为 2 个不同的大素数,且满足 $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) - 1$。$G$ 为 $C_n(a,b)$ 的基点,其阶为 $N_n = 2rs$,其中,$r,s$ 也是素数。选择 $H(\,)$,$H_1(\,)$ 为 2 个抗碰撞的哈希函数。

公开:$n,a,b,G,H$;保密:$p,q,N_n$。

2) 密钥提取:① 假设有 $l$ 个用户 $U_i$,用户包括广播者的身份为 $ID_i \in \{0,1\}^*$,系统计算 $K_{ID_i} = H_1(ID_i)$ 且 $(K_{ID_i},N_n) = 1$,计算 $K_{ID_i}L_{ID_i} \equiv 1(\mathrm{mod}\ N_n)$,$T_i = L_{ID_i}G$。② 每个用户选择 1 个随机数 $0 < d_i \leq n$,计算 $Q_i = d_iG \neq 0$,广播者也选择 1 个随机数 $0 < d_B \leq n$,计算 $Q_B = d_BG \neq 0$,则每个用户的公开钥为 $(K_{ID_i},Q_i)$,私钥为 $(T_i,d_i)$。广播者的公开钥为 $(K_{ID_B},Q_B)$,私钥为 $(T_B,d_B)$。

3) 注册:每个用户 $U_i$ 向广播者注册时,计算 $S_i = H(d_iQ_B(\mathrm{mod}\ n))$,然后将注册信息 $(ID_i,S_i)$ 发送给广播者,广播者收到此信息后,计算 $S_i' = H(d_BQ_i(\mathrm{mod}\ n))$,若 $S_i' = S_i$,令 $x_i$ 为 $S_i$ 的横坐标,若 $x_i$ 为零,则返回到 2) 的第 ② 步,重新选择随机数。则将 $(ID_i,x_i)$ 添加到注册表中 $L_B$,并修改用户表。将 $ID_i$ 添加到用户表 $L_U$ 中,并修改注册表多项式 $T(x) \leftarrow T(x)(x-x_i)$,$f_B(x) \leftarrow T(x)+1$。注册表多项式的初始值 $T(x) = f_B(x) = 1$。如若用户 $U_i$ 需要向广播者注销时,则向广播者提出申请,广播者查找注册表 $L_B$,更新注册多项式 $T(x) \leftarrow$

$T(x)(x-x_i)^{-1}, f_B(x) \leftarrow T(x)+1$ 同时从注册表 $L_B$ 中删除 $(ID_i, x_i)$,从用户表 $L_U$ 中删除 $ID_i$。

4) 签密:为了将消息 $m \in \{0,1\}^*$ 发送给各个注册用户,广播者进行以下操作:

①随机选择一个点 $R \in C_n(a,b)$ 和正整数 $t$,计算 $P_0 = c_0R, P_1 = c_1R, P_2 = c_2R, \cdots, P_l = c_lR$。其中,$c_i$ 为注册多项式展开式中 $x^i$ 系数。

②$y = H(R) \oplus m, V = tT_B + R, U = H(m \| tG)$。

广播者的广播密文为 $(P_0, P_1, \cdots, P_l, y, V, U)$。

5) 解签密:注册用户 $U_i$ 利用 $S_i = d_iQ_B$ 计算出 $x_i$,计算 $R = \sum_{i=0}^{l} x^iP_i$,恢复出密文 $m = H(R) \oplus y$。计算 $W = (V-R)K_{ID_B}$,验证等式 $U = H(m \| W)$ 是否成立,若成立,则接收该密文。

## 3 方案分析

1) 正确性:如果密文是按照上面的步骤由广播者产生,且在传播的过程中没有发生任何改变,则每个注册用户 $U_i$ 通过可以 $S_i = d_iQ_B$ 计算出相应的 $x_i$,进一步计算

$$R = \sum_{i=0}^{l} x^iP_i = \left(\sum_{i=0}^{l} c_ix^i\right)R = R,$$

则

$$y = H(R) \oplus m,$$

$$W = (V-R)K_{ID_B} = tS_BK_{ID_B} = tG。$$

所以 $U = H(m \| W)$,算法验证有效。

2) 保密性:从以上注册信息合签密算法过程可以看出,只有注册用户和签密者才能计算出解密密钥 $x_i$,任何第三方在不知双发私钥 $d$ 的情况下是无法得出双方的会话密钥 $S_i$。同时由双方的公开密钥 $Q_i$、$Q_B$ 去计算 $S_i$,则由圆锥曲线上的离散对数问题困难性可知在计算上是不可行的。因此任何非注册用户是无法获得明文消息的。除此之外,利用注册多项式的动态改变,及时更新注册列表和注册多项式,所以当用户的注册信息被更新后,那么撤销用户的一切信息也在注册表中被删除,从而注册多项式也同时发生相应的改变,这样撤销用户也是无法通过原有的解密密钥 $x$ 进行解密。所以该方案具有强的保密性。

3) 不可伪造性:该算法主要基于大数分解和曲线上的离散对数问题的困难性。由于签名算法是基于圆锥曲线上的 RSA 签名思想,克服了传统签名方法的同态性,从而该方案可以抵抗以重放攻击来伪造合法的签名。其次圆锥曲线上的 RSA 签名可以抵抗低加密指数攻击和低解密指数攻击[20],也能抵抗利用有限简单连分数展式求出解密私钥[22]。所以该方案具有更强的不可伪造性。

4) 效率分析:在本方案中以 $Pm$ 表示圆锥曲线上的点乘运算,$Ad$ 表示加法运算;$Pm'$ 表示椭圆曲线上的乘法运算,$Ad'$ 表示加法运算;$e$ 表示对运算,$e'$ 表示指数运算,$h$ 表示哈希运算,忽略掉数的乘法运算及 bit 或运算,则和祁正华等所提的广播签密方案相比,信息计算量比较如表 1 所示。

**表 1 运算效率比较表**

**Tab. 1 Comparison of operation efficiency**

| 签密方案 | 用户注册 | 签密 | 解签密 |
|---|---|---|---|
| 文献[16] | $2Pm' + 3e + h$ | $e + e' + 3h + (2l+4)Pm' + 2Ad'$ | $(t+1)e' + e + 3h + (l+3)Pm' + (t+1)Ad'$ |
| 本方案 | $2Pm + 2h$ | $2h + (l+3)Pm + Ad'$ | $2h + (l+2)Pm + Ad' + (t+1)e'$ |

由于椭圆曲线上的乘运算和加运算相比于圆锥曲线在计算量上要大[23],其次椭圆曲线上的对运算计算代价也是非常大的,因此作者所提的方案在通信代价上明显具有一定的优势。如果使用标准二进制来表示点运算的话,则计算量更能节约近 1/4。

## 4 结 论

利用整数环上的圆锥曲线上的密码技术提出了一个高效的无证书广播签密方案,该方案在基于大整数分解和圆锥曲线上的离散对数双难问题下具有更强的安全性和抗破解性,此外提出的广播签密方案和祁正华等所提方案相比,改进了签密算法和解签密算法,减少了通信代价,提高了计算效率,使得签密方案更加具有实用性。

**参考文献:**

[1] Zheng Y. Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption)[C]//Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. London, UK, 1997:165-179.

[2] Liu Z, Hu Y, Zhang X, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010,180(3):452-464.

[3] Li F, Khan M K. A survey of identity-based signcryption [J]. IETE Technical Review, 2011, 28(3): 265 – 272.

[4] Pang Liaojun, Cui Jingjing, Li Huixian, et al. A new multi-receiver ID-based anonymous signcryp-tion [J]. Chinese Journal of Computer, 2011, 34(11): 2014 – 2113. [庞辽军, 崔静静, 李慧贤, 等. 新的基于身份的多接收者匿名签密方案[J]. 计算机学报, 2011, 34(11): 2014 – 2113.]

[5] Shamir A. Identity-based cryptosystems and signature schemes [C]//Advances in Cryptology—CRYPTO 1984. Berlin: Springer, 1984: 47 – 53.

[6] Boneh D, Franklin M. Identity based encryption from the Weil pairing [J]. SIAM Journal on Computing, 2003, 32(3): 586 – 615.

[7] Bellare M, Waters B, Scott Y. Identity-based Encryption secure against selective opening attack [C]//Proceedings of TCC 2011. 2011: 235 – 252.

[8] Icart T. How to hash into elliptic curves [C]//Advances in Cryptology—CRYPTO 2009. Berlin, Germany: Springer, 2009, LNCS 5677: 303 – 316.

[9] Du Hongzhen, Wen Qiaoyan. An efficient Identity-based aggregate signature scheme [J]. Journal of Sichuan University: Engineering Science Edition, 2011, 43(1): 87 – 90. [杜红珍, 温巧燕. 一个高效的基于身份的聚合签名方案[J]. 四川大学学报: 工程科学版, 2011, 43(1): 87 – 90.]

[10] Ren Yanli, Gu Dawu, Wang Shuozhong, et al. Anonymous identity-based encryption scheme without random oracle [J]. Journal of University of Science and Technology of China, 2012, 42(4): 296 – 301. [任艳丽, 谷大武, 王朔中, 等. 标准模型中基于身份的匿名加密方案. 中国科学技术大学学报, 2012, 42(4): 296 – 301.]

[11] Xu Ning, Yang Geng. Key establish scheme for optical encryption system based on IBE [J]. Journal on Communications, 2012, 33(3): 121 – 128. [徐宁, 杨庚. 基于身份加密机制的光学加密密钥系统. 通信学报, 2012, 33(3): 121 – 128.]

[12] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C]//Advances in Cryptology—ASIACRYPT2003, Springer-Verlag, 2003, LNCS 2894: 452 – 473.

[13] Fiat A, Naor M. Broadcast encryption [C]//Advances in Cryptology—CRYPTO '93: Proceedings of the 13th Annual International Cryptology Conference. 1994, LNCS 773: 480 – 491.

[14] Gentry C, Waters B. Adaptive security in broadcast encryption systems [C]//Proceedings of Eurocrypt Cologne. Germany, 2009.

[15] Kim I T, Hwang S O. An efficent identity-based broadcast signcryption scheme for wireless sensor networks [C]//Proceedings of 6th International Symposium on Wireless and Pervasive. Computing (ISWPC), 2011: 1 – 6.

[16] Sun Jin, Hu Yupu, Zhang Leyou. Identity-based broadcast encryption based on Ad hoc networks [J]. Computer Science, 2011, 38(2): 46 – 49. [孙瑾, 胡予濮, 张乐友. 基于 Ad hoc 网的身份型广播加密方案[J]. 计算机科学, 2011, 38(2): 46 – 49.]

[17] Zhang Weiren, Hu Yupu, Yang Xiaoyuan. An new identity-based broadcast encryption scheme over lattice [J]. Journal of Beijing University of Posts and Telecommunications, 2012, 35(6): 112 – 115. [张伟仁, 胡予濮, 杨晓元. 格上新的身份类广播加密方案[J]. 北京邮电大学学报, 2012, 35(6): 112 – 115.]

[18] Selvi S, Vivek S, Gopalakrishnan R, et al. Provably secure ID-based broadcast signcryption (IBBSC) scheme [R]. Cryptology ePrint Archive, Report 2008/225.

[19] Qi Zhenghua, Ren Xunyi, Yang Geng, et al. An ID-based broadcast signcryption scheme [J]. Journal of Sichuan University: Engineering Science Edition, 2012, 44(1): 118 – 122. [祁正华, 任勋益, 杨庚, 等. 一种基于身份的广播签密方案[J]. 四川大学学报: 工程科学版, 2012, 44(1): 118 – 122.]

[20] Sun Qi, Zhu Wenyu, Wang Biao. The conic curve over $Z_n$ and public-key cryptosystem protocol [J]. Journal of Sichuan University: Natural Science Edition, 2005, 42(3): 471 – 478. [孙琦, 朱文余, 王标. 环 $Z_n$ 上圆锥曲线和公钥密码协议[J]. 四川大学学报: 自然科学版, 2005, 42(3): 471 – 478.]

[21] Dai Zongduo, Pei Dingyi, Yanh Junhui, et al. Cryptanalysis of a public key cryptosystem based on conic curves [C]. The International Workshop on Cryptographic Techniques & E-Commerce, Hong Kong, 2000.

[22] Wang Biao, Fang Yingjue, Lin Honggang. QV signature protocol on conic curve over $Z_n$ ring [J]. Science in China, 2009, 39(2): 212 – 217. [王标, 方颖珏, 林宏刚, 等. 基于环 $Z_n$ 上圆锥曲线的 QV 签名方案[J]. 中国科学, 2009, 39(2): 212 – 217.]

[23] Li Hangyu. The scalar multiplication of points on a conic over finite fields [J]. Information Security and Communications Privacy, 2007(8): 64 – 69.

(编辑　杨　蓓)