文章编号:1001 - 9081(2011)04 - 0978 - 03
doi:10.3724/SP.J.1087.2011.00978

基于秘密共享的广播加密方案

廖志委,王晓明
(暨南大学 信息科学技术学院,广州 510632)
(liaowells@126.com)

摘　要:现在,越来越多的应用要求广播加密方案的解密算法的计算量尽可能小。针对这一需求,给出了秘密共享在广播加密中的另一种应用,通过预先重构插值份额,从而减少解密时重构的计算量。分析表明,改进后的方案只需对明文进行一次加密,授权用户利用各自私钥就能进行解密,而且解密时只需较小的计算量,并能实现安全地剔除用户、添加用户,而不需要授权用户改变私钥,能抗合谋攻击。

关键词:广播加密;秘密共享;抗合谋性;离散对数;付费电视
中图分类号:TP309.7　　**文献标志码**:A

Broadcast encryption scheme based on secret sharing

LIAO Zhi-wei, WANG Xiao-ming
(*College of Information Science and Technology, Jinan University, Guangzhou Guangdong* 510632, *China*)

Abstract: The broadcast encryption scheme was required to minimize the amount of decryption computation by many applications. Concerning this requirement, a new broadcast encryption scheme was proposed by using secret sharing in another way. The improved scheme reduced the amount of decryption computation by pre-reconstructing the interpolation share. Analysis shows that the improved scheme just needs to encrypt once the plaintext, and then the subscribers can decrypt the cipher text using their secret keys with less computation. The improved scheme can also remove and add subscribers securely without the changing of subscribers' secret keys, and is of collusion-resistant property.

Key words: broadcast encryption; secret sharing; collusion-resistance; discrete logarithm; pay-TV

0　引言

广播加密[1-2]是指在每一次会话中,广播者都必须加密会话密钥,然后在不安全的信道上分发给动态群用户,只有授权用户才能解密秘密信息。广播加密方案最早由 Fiat 和 Naor 提出[1],然后不断有新方案提出[2-6]。

随着 Internet 的发展,广播加密得到越来越广泛的应用,如付费电视、视频会议等,而这些应用也对广播加密方案提出了新的需求。付费电视等系统由一个广播者和一组授权用户组成。广播者利用组密钥对信号进行加密,然后广播给全组授权用户。用户端通过解码器,利用嵌入的解密密钥对接收到的广播信号进行解密。广播者需要对组内成员的更新进行管理,进行剔除用户和添加用户等操作。因为受解码器计算能力的限制,付费电视等应用要求广播加密方案在解密时所需的计算量尽可能少,而且能在不需要授权用户改变私钥的情况下安全地添加授权用户和剔除过期用户。

Mu 和 Varadharajan[3]基于离散对数问题的难解性提出了一种非对称广播加密方案(简称 MV 方案),并声称适用于付费电视等系统。但是 MV 方案存在缺陷,不能安全地剔除用户,而且其加密方案参数有冗余。

文献[4-5]基于秘密共享提出了可证明安全的多接收者公钥加密方案,文献[6]利用双线性对提出了基于身份的广播加密方案,但是这些方案在解密时所需的计算量还是比较大。

本文首先论证了 MV 方案的缺陷,然后基于 Shamir 的秘密共享方案提出了新的广播加密方案,给出了秘密共享在广播加密中的另一种应用,适用于付费电视等应用。

1　MV 方案分析

1.1　MV 方案简介

1.1.1　系统初始化

假设系统最大能容纳 n 个用户,实际用户数为 $m(0 < m \leqslant n)$。

1) 构造 Z_q 上的 n 次多项式:$f(x) = \prod_{i=1}^{n}(x - x_i) \equiv \sum_{i=0}^{n} a_i x^i \pmod q$,计算 $g_i \equiv g^{a_i} \pmod p (i = 0,1,\cdots,n)$。其中 p,q 为大素数,$q \mid p-1$,Z_p^* 为有限域 Z_p 的乘法群,g 为其一生成元,x_i 为 Z_q 中的随机数。

2) 计算加密密钥 $A = \prod_{j=1}^{n}\left(\prod_{i=0}^{n-1} g_i^{x_j^i}\right) \pmod p$。

3) 选取整数 $b \in_R Z_q$,并计算其逆元 b^{-1}。

4) 令集合 $S = \{x; x \in Z_q \wedge x^2 \equiv x \pmod q\}$。选取 n 个数 $s_i \in S$,计算 $s = \prod_{i=1}^{n} s_i \pmod q$。

5) 为每个用户计算解密密钥:

$$\bar{x}_i = b^{-1} \sum_{j=1, j\neq i}^{n} x_j^n \bmod q;\ i = 1,2,\cdots,n$$

$$\hat{x}_i = s_i x_i^n \bmod q;\ i = 1,2,\cdots,n$$

1.1.2　加密

选取随机数 $k \in_R Z_q$,计算 $\bar{g} = g^{sk} \pmod p$ 和 $\hat{g} = g^{sbk} \pmod$

收稿日期:2010 - 10 - 08;**修回日期**:2010 - 11 - 02。　**基金项目**:国家自然科学基金资助项目(61070164;60773083);广东省自然科学基金资助项目(8151063201000022);广东省科技计划项目(2010B010600025)。

作者简介:廖志委(1986 -),男,广东梅州人,硕士研究生,主要研究方向:密码学、信息安全;　王晓明(1960 -),女,重庆人,教授,博士,主要研究方向:计算机网络安全、现代密码学。

$p)$,对明文 M,计算密文 $C = MA^{sk} (\mathrm{mod}\ p)$。广播密文对$(\bar{g},\hat{g},C)$。

1.1.3　解密

授权用户 i 利用解密密钥解密,$M = C\hat{g}^{\bar{x}_i}\bar{g}^{\hat{x}_i} (\mathrm{mod}\ p)$。

1.1.4　剔除用户

MV 方案给出两种剔除用户的方案。

1)剔除用户 γ,重新计算加密密钥 $A = \prod_{j=1,j\neq\gamma}^{n}\left(\prod_{i=0}^{n-1} g_i^{x_j^i}\right) (\mathrm{mod}\ p)$,计算新参数 $d = g^{-\hat{x}_\gamma} (\mathrm{mod}\ p)$,计算 $s = \prod_{i=1,i\neq\gamma}^{n} s_i (\mathrm{mod}\ q)$。加密时对 C 的计算改为:$C = MA^{sk}d^{sk} (\mathrm{mod}\ p)$。解密操作不用改变。

2)剔除用户 γ,只需重新计算 $s = \prod_{i=1,i\neq\gamma}^{n} s_i (\mathrm{mod}\ q)$,其余操作不用改变。

1.2　MV 方案分析

从 MV 方案简介可知,广播者只需对明文进行一次加密操作,授权用户收到广播密文后,利用自己的私钥就能正确恢复明文,而且授权用户解密只需较少计算量。

但是其剔除用户的方案并不能安全地剔除用户,而且加密方案中用到的 s 冗余了。

1.2.1　用户剔除分析

首先分析方案中用到的参数 s。参数 $s = \prod_{i=1}^{n} s_i (\mathrm{mod}\ q)$,其中 $s_i \in S$,对任意的 $s_i \in S$ 要求满足 $s_i s_i \equiv s_i (\mathrm{mod}\ q)$。求解 s_i 即求解方程 $s_i^2 - s_i - kq = 0$,由求根公式可得 $s_i = \frac{1 \pm \sqrt{1+4kq}}{2}$,由 s_i 是整数,得 $\sqrt{1+4kq}$ 必为奇数,也就是说 $s_i = \frac{1 \pm (1+2k_1 q)}{2}$,即 $s_i = 1 + k_1 q$。由此可得对任意的 $s_i, s_j \in S$,有 $s_j s_i \equiv s_j (\mathrm{mod}\ q)$。

MV 方案的第一种剔除用户方案,剔除用户 γ 时,重新计算 $s = \prod_{i=1,i\neq\gamma}^{n} s_i (\mathrm{mod}\ q)$,加密密钥 $A = \prod_{j=1,j\neq\gamma}^{n}\left(\prod_{i=0}^{n-1} g_i^{x_j^i}\right) (\mathrm{mod}\ p)$,添加新参数 $d = g^{-\hat{x}_\gamma} (\mathrm{mod}\ p)$。被剔除的用户 γ 收到新密文后的解密过程如下:

$$C\hat{g}^{\bar{x}_\gamma}\bar{g}^{\hat{x}_\gamma} = MA^{sk}d^{sk}(g^{shk})^{b^{-1}\sum_{j=1,j\neq\gamma}^{n} x_j^n}(g^{sk})^{s_\gamma x_\gamma^n}$$

由于对任意的 $s_i, s_j \in S$,有 $s_j s_i \equiv s_j (\mathrm{mod}\ q)$,所以 $ss_\gamma \equiv s (\mathrm{mod}\ q)$,所以上式等价于:

$$MA^{sk}(g^{sk})^{\sum_{j=1,j\neq\gamma}^{n} x_j^n} = M\prod_{j=1,j\neq\gamma}^{n}(g^{sk})^{\sum_{i=0}^{n} a_i x_j^i} = M$$

可见被剔除的用户 γ 还是可以恢复明文,所以该方案无法安全地剔除用户。

第二种剔除用户的方案只是重新计算了 $s = \prod_{i=1,i\neq\gamma}^{n} s_i$。但由于 $s = ss_\gamma \bmod q$,所以被剔除的用户 γ 还是可以正确恢复明文的。所以第二种剔除用户的方案也无法安全地剔除成员。

1.2.2　参数冗余分析

MV 方案加密的安全性是依靠 $\bar{x}_i, x_i$,而不是 s_i。因为如果能够获得 $\bar{x}_i, x_i$,那么就能够构造解密密钥$(\bar{x}_i, \hat{x}_i')$,正确地恢复明文。

因为 s_i 必为 $1 + kq$ 的形式,所以我们可以构造出 $s_i' \in S$,且 $s_i' \neq s_i$,然后构造解密密钥 $\hat{x}_i' = s_i' x_i^n \bmod q$,然后解密密文:

$$C\hat{g}^{\bar{x}_i}\bar{g}^{\hat{x}_i'} = MA^{sk}(g^{shk})^{b^{-1}\sum_{j=1,j\neq i}^{n} x_j^n}(g^{sk})^{s_i' x_i^n}$$

由前面可知 $ss_i' \equiv s (\mathrm{mod}\ q)$,所以上式等于:

$$MA^{sk}(g^{sk})^{\sum_{j=1}^{n} x_j^n} = M\prod_{i=1}^{n}(g^{sk})^{\sum_{j=0}^{n} a_i x_j^i} = M$$

可见解密密钥$(\bar{x}_i, \hat{x}_i')$ 可以正确地恢复明文,所以 MV 方案加密的安全性是依靠 x_i,而不是 s_i。因此在加密过程中加入 s 和解密密钥中加入 s_i 是多余的。

由以上分析可知,虽然 MV 方案给出的加密方案是安全的,而且在解密时所需的计算量也比较少,但是其用户剔除方案却无法安全地剔除用户,所以并不能像其声称的那样适用于付费电视等应用。

2　基于秘密共享的广播加密方案

本文基于秘密共享方案,提出了一种新的广播加密方案。本方案只需对明文进行一次加密操作,然后授权用户利用自己的私钥来解密得到正确明文,而且解密只需较少计算量,并能在不需要授权用户改变私钥的情况下安全地剔除用户和添加用户,而且能抵抗合谋攻击。本方案适用于付费电视等应用。

2.1　方案描述

2.1.1　系统初始化

假设系统最大能容纳 n 个成员,实际成员数为 $m(0 < m \leqslant n)$。

1)系统中心选取大素数 p, q,且 $q \mid p-1$。Z_p^* 为有限域 Z_p 的乘法群,g 为其一生成元。随机选取 $r \in Z_q$ 作为主密钥。随机选取 n 次多项式 $f(x) = r + \sum_{i=1}^{n} a_i x^i (\mathrm{mod}\ q)$,其常数项为 r,即 $f(0) = r$。从 Z_q 中随机选取 n 个不同的数 x_i 构成集合 $X_n = \{x_1, x_2, \cdots, x_n\}$,$n$ 个不同的数 w_i,本方案中的算术运算如无特别说明,都是模 p 运算。

2)计算加密密钥 $A = g^r$。

3)计算:

$$B_i' = \sum_{j=1}^{n} f(x_j)\frac{-w_i}{x_j - w_{ik=1,k\neq j}}\prod_{k=1,k\neq j}^{n}\frac{-x_k}{x_j - x_k} (\mathrm{mod}\ q)$$

$$B_i = g^{B_i'};\ i = 1,2,\cdots,m$$

4)计算每个用户的解密密钥:

$$D_i = f(w_i)\prod_{j=1}^{n}\frac{-x_j}{w_i - x_j} (\mathrm{mod}\ q);\ i = 1,2,\cdots,m$$

系统中心公开 $p, g, n, m, A, x_i, w_i, B_i$ 等参数,解密密钥 D_i 安全地分发给各个授权用户,例如对于付费电视应用,解密密钥 D_i 则嵌入在授权用户的解码器中。

2.1.2　加密阶段

广播者随机选取 $k \in Z_q$,计算 $E_0 = g^k$,对每个授权用户计算 $E_i = B_i^k (i = 1,2,\cdots,m)$,对明文 M,计算密文 $C = M \oplus A^k$,然后广播密文对$(C, E_0, E_1, \cdots, E_m)$。

2.1.3　解密阶段

授权用户 i 收到密文对后,取出对应的 E_i,然后进行如下计算,恢复明文:

$$d = E_i E_0^{D_i}, M = C \oplus d$$

2.1.4　剔除用户和添加用户

1)剔除用户 γ,广播者只需在加密时,计算 $E_i = B_i^k (i = 1,2,\cdots,m, i \neq \gamma)$,其余操作不用改变。

2)添加用户时,系统中心为新用户 w_l 计算:

$$B_l' = \sum_{j=1}^{n} f(x_j)\frac{-w_l}{x_j - w_l}\prod_{k=1,k\neq j}^{n}\frac{-x_k}{x_j - x_k} (\mathrm{mod}\ q)$$

$$B_l = g^{B_l'}$$

计算解密密钥:

$$D_l = f(w_l)\prod_{j=1}^{n}\frac{-x_j}{w_l - x_j}(\mathrm{mod}\ q)$$

然后安全地分发给该用户。

2.2 方案分析

本方案利用秘密共享方案把主密钥 r 拆分为 $n+m$ 份，任何 $n+1$ 份子密钥能重构出 r。广播者为每个授权用户重构 n 份子密钥，授权用户利用自己拥有的 1 份子密钥和接收到的 n 份子密钥来重构 r，从而恢复明文；非授权用户无法凑够 $n+1$ 份子密钥，所以无法恢复明文。本方案还能在不需要授权用户改变私钥的情况下安全地剔除用户、添加用户，并且能抗合谋攻击。

2.2.1 正确性分析

授权用户 i 收到密文对后，取出对应的 E_i，利用自己的解密密钥，计算：

$$d = E_i E_0^{D_i} = (g^k)^{\left[f(w_i)\prod_{j=1}^{n}\frac{-x_j}{w_i-x_j}\right]+\sum_{j=1}^{n}f(x_j)\frac{-w_i}{x_j-w_i}\prod_{k=1,k\neq j}^{n}\frac{-x_k}{x_j-x_k}}$$

由拉格朗日插值公式，可知：

$$\left[f(w_i)\prod_{j=1}^{n}\frac{-x_j}{w_i-x_j}\right]+\sum_{j=1}^{n}\frac{-w_i}{x_j-w_i}f(x_j)\prod_{k=1,k\neq j}^{n}\frac{-x_k}{x_j-x_k}=r$$

所以上式等价于：$g^{kr}=A^k$，因此 $C\oplus d = M\oplus A^k\oplus A^k = M$，所以授权用户能正确地恢复明文。

2.2.2 安全性分析

由于 $m\leqslant n$，所以即使 m 个授权用户合谋，也无法重构出主密钥 r，所以本方案能抗合谋攻击。

剔除用户时，广播者只需要不广播该用户对应的 E_i，由解密过程可知该用户接收到密文对也无法恢复明文，而其他授权用户依然能够得到对应的 E_i，所以能正确恢复明文。所以本方案能安全地剔除用户，而不需要授权用户改变私钥。

添加用户时，广播者只需为该新用户计算新的 E_l，然后把解密密钥 D_l 安全地分发给该用户。广播者加密时计算 C_0，并广播出去。所以新用户能够得到对应的 E_l，结合自己的 D_l 就能正确地恢复明文。所以本方案能安全地添加用户，而不需要授权用户改变私钥。

2.2.3 性能分析

由加密阶段可知，本方案只需对明文进行一次加密操作，而在授权用户进行解密时，只需少量的计算就能恢复明文，剔除用户时也无需额外的开销。

3 结语

MV 方案虽然在解密时所需的计算量较少，但它并不能安全地剔除成员，而且其加密方案的参数有冗余。本文基于秘密共享方案，对 MV 方案进行改进，提出了新的广播加密方案。本方案不但具有 MV 方案解密计算量少的良好特性，并能在不需要授权用户改变私钥的情况下安全地对用户组进行剔除、添加等管理操作，适用于付费电视等应用。

参考文献：

[1] FIAT A, NAOR M. Broadcast encryption [C]// CRYPTO '93: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, LNCS 773. Berlin: Springer-Verlag, 1994: 480 - 491.

[2] NAOR D, NAOR M, LOTSPIECH J B. Revocation and tracing schemes for stateless receivers [C]// CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, LNCS 2139. Berlin: Springer-Verlag, 2001: 41 - 62.

[3] MU Y, VARADHARAJAN V. Robust and secure broadcasting [C]// INDOCRYPT '01: Proceedings of the Second International Conference on Cryptology in India: Progress in Cryptology, LNCS 2247. Berlin: Springer-Verlag, 2001: 223 - 231.

[4] 鲁力，胡磊. 基于 Weil 对的多接收者公钥加密方案[J]. 软件学报, 2008, 19(8): 2159 - 2166.

[5] 庞辽军，李慧贤，焦李成，等. 可证明安全的多接收者公钥加密方案设计与分析[J]. 软件学报, 2009, 20(10): 2907 - 2914.

[6] BAEK J, SAFAVI-NAINI R, SUSILO W. Efficient multi-receiver identity-based encryption and its application to broadcast encryption [C]// PKC '05: Proceedings of Public Key Cryptography, LNCS 3386. Berlin: Springer-Verlag, 2005: 380 - 397.

（上接第 959 页）

参考文献：

[1] FRIDRICH J, GOLJAN M, SOUKAL D. Perturbed quantization steganography [J]. Multimedia Systems, 2005, 11(2): 98 - 107.

[2] SALLEE P. Model-based steganography [C]// IWDW2003: Proceedings of International Workshop on Digital Watermarking, LNCS 2939. Berlin: Springer-Verlag, 2004: 154 - 167.

[3] SALLEE P. Model-based methods for steganography and steganalysis [J]. International Journal of Image and Graphics, 2005, 5(1): 167 - 189.

[4] FRIDRICH J, GOLJAN M, HOGEA D. Steganalysis of JPEG image: Breaking the F5 algorithm [C]// 5th International Workshop on Information Hiding, LNCS 2578. Berlin: Springer-Verlag, 2002: 310 - 323.

[5] SHI Y Q, CHEN CHUNHUA, CHEN WEN. A Markov process based approach to effective attacking JPEG steganography [C]// IH2006: Information Hiding 2006, LNCS 4437. Berlin: Springer-Verlag, 2007: 249 - 264.

[6] FRIDRICH J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes [C]// IH2004: Information Hiding 2004, LNCS 3200. Berlin: Springer-Verlag, 2004: 67 - 81.

[7] RODRIGUEZ B, PETERSON G. Detecting steganography using multi-class classification [M]// IFIP: International Federation for Information Processing 2007, Advances in Digital Forensics III. Berlin: Springer-Verlag, 2007, 242: 193 - 204.

[8] SHI Y Q, XUAN G, ZOU D, *et al*. Steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network [C]// IEEE International Conference on Multimedia and Expo. Washington, DC: IEEE, 2005: 157 - 164.

[9] TRIVEDI S, CHANDRAMOULI R. Secret key estimation in sequential steganography [J]. IEEE Transactions on Signal Processing, 2005, 53(2): 746 - 757.

[10] 谭舜泉，黄继武，杨志华. 基于 Hilbert-Huang 变换的 JPEG2000 隐写分析[J]. 计算机学报, 2006, 29(9): 1702 - 1709.

[11] HUANG N E, SHEN Z, LONG S R, *et al*. The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis [C]// Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences. [S.l.]: Royal Society of London, 1998, 454: 903 - 995.

[12] CHANG C C, LIN C J. LIBSVM: A library for support vector machines [EB/OL]. (2005 - 09 - 20) [2010 - 06 - 11]. http://www.csie.ntu.edu.tw.

[13] PHILIP G. Adding images to your site [EB/OL]. (2005 - 09 - 12) [2010 - 07 - 17]. http://philip.greenspun.com.