接收者无状态下可扩展的公钥广播加密方案

石雅男,黄根勋,王 旭
SHI Ya-nan,HUANG Gen-xun,WANG Xu

信息工程大学 理学院 数学物理系,郑州 450001
Department of Mathematics and Physics,Institute of Science,Information Engineering University,Zhengzhou 450001,China
E-mail:xxgcatz@163.com

SHI Ya-nan,HUANG Gen-xun,WANG Xu.Scalable public key broadcast encryption scheme for stateless receiver.Computer Engineering and Applications,2008,44(20):135-137.

Abstract: Broadcast encryption scheme is a widely used cryptosystem for a group of receivers.In this paper,a new public key broadcast encryption scheme is proposed under the CS method by the use of identity expression in HIBE.By setting nodes in advance for potential users,the scheme can be used for stateless receiver,which will have enormous application in practice with the least number of private keys and high efficiency.

Key words: broadcast encryption;public key cryptosystem;stateless receiver;CS method;HIBE;IBE

摘 要:广播加密是一种应用广泛的群组保密通信系统。在CS方法的基础上利用HIBE中身份的表示方法提出一种新的公钥广播加密方案,同时采用预留节点的方法在接收者无状态的情况下真正实现了系统的可扩展性。与已有方案比较,该方案的系统参数大大减少,同时具有用户密钥持有量小且运算效率高的优点,在实际的无状态接收装置中有着广泛的应用。

关键词:广播加密;公钥密码体制;无状态接受;CS方法;HIBE;IBE
DOI:10.3778/j.issn.1002-8331.2008.20.041 **文章编号:**1002-8331(2008)20-0135-03 **文献标识码:**A **中图分类号:**TP309

广播加密方案是一种在不安全信道上传输数字信息给多个用户的密码系统,它能够使广播中心根据需要动态选取不同的用户组进行广播加密,从而以点对多点的方式安全高效地实现消息的保密传输。随着计算机网络及信息传输技术的飞速发展,广播加密在数字媒体传输及版权保护领域有着巨大的应用需求,这些需求使得对该领域的研究越加广泛和深入。

广播加密应用的一种常见情形是无状态接收者(Stateless Receiver)的情况:在系统的整个生命周期内接收者无法改变自身设置,解密操作只能按照系统初始设置进行。例如当用户处于离线状态无法更新或私钥被保存在防篡改(tamper-resistant)的硬件中时,解密运算只能在初始设置下完成。这种情况常见于受版权保护的媒体播放器(CD和DVD)、卫星接收装置等。特别是当有用户加入或退出系统时,如果用户私钥发生改变,解密操作将无法进行。

1993年,A.Fiat和M.Naor首次提出广播加密的概念并对该问题进行了研究[1]。在此基础上,D.Naor等人针对无状态接收者的情况引入基于二叉树结构的"子集-覆盖"(Subset-Cover)框架,给出当有任意用户撤销时广播加密的一般方法[2]。与此同时,他们提出该框架的两种有效实现方法:CS(Complete Subtree)方法和SD(Subset Difference)方法。此后,文献[3]提出SD方法的改进方法。其中CS方法的实现较为简单,可操作性强。上述广播加密系统均基于对称密码体制,广播中心与用户持有相同的私钥,这使得广播中心成为整个系统的瓶颈,一旦发生密钥泄漏将造成无法估量的损失。同时,对称密钥的使用只允许可信发送方广播加密消息,限制了其他广播者。然而,在广播加密系统中公钥密码体制的引入又会带来大量公钥的使用,从而增加了系统运行和维护的负担。此外,当有新用户加入时系统必须重建二叉树的结构,用户私有信息也将随之改变,在接收者无状态情况下限制了系统的扩展。文献[2]中建议用基于身份的思想解决大量公钥使用的问题;Y.Dodis和N.Fazio在文献[4]中利用IBE算法给出基于CS方法的公钥广播加密方案,但仍未解决系统可扩展的问题。

本文针对CS方法构造了一种新的公钥广播加密方案。该方案采用HIBE[5]中身份的表示方法唯一标识了各节点在二叉树中的位置,使得广播者只需知道系统参数及用户身份(即地址)就可广播加密消息,与方案[6]相比系统参数大大减少。与此同时该方案还采用文献[7]中预留节点的方法,从真正意义上达到了接收者无状态的要求。

1 预备知识

1.1 双线性映射

设 G 和 G_T 为两个阶数为素数 p 的乘法循环群。定义映射

作者简介:石雅男(1982-),女,在读硕士,主要研究领域为信息安全与密码学;黄根勋(1964-),男,博士,副教授,主要研究领域为应用代数与信息安全;王旭(1981-),男,在读硕士,主要研究领域为信息安全。

收稿日期:2007-10-18 **修回日期:**2008-01-22

$e:G\times G\to G_T$为双线性映射当且仅当满足性质：

(1)双线性：对于任意的$g_1,g_2\in G,\alpha,\beta\in Z_p$，满足等式$e(g_1^{\alpha},g_2^{\beta})=e(g_1,g_2)^{\alpha\beta}$；

(2)非退化性：存在$g\in G$满足$e(g,g)\neq 1$；

(3)可计算性：对于任意的$g_1,g_2\in G$存在一个有效算法计算$e(g_1,g_2)$。

双线性映射可以用超椭圆曲线上 Weil 对[8]和 Tate 对[9]实现。

1.2 HIBE 方案

1984 年，Shamir 在公钥密码的基础上提出基于身份加密(IBE)的思想[10]。它采用标识用户身份的信息：姓名、E-mail 地址等作为用户的公钥，用户私钥通过称为私钥生成器(PKG)的可信第三方由用户身份信息及系统主密钥生成，简化了公钥密码系统中密钥管理的问题。层次结构下基于身份的加密方案(HIBE)是 IBE 在层次结构下的推广，它采用树状结构组织 PKG，用户公钥由该用户身份及其隶属 PKG 身份组成的地址向量唯一标识。其中根 PKG 为它下面的域 PKG 产生私钥，用户私钥由上级域 PKG 生成，有效地减轻了单一 PKG 为用户生成私钥的负担，扩大了系统的适用范围。

目前 HIBE 方案的研究主要利用双线性映射，根据用户私钥及密文长度大致可分为两类，其中一类方案中用户私钥及密文长度随用户所在层次递增[11,12]，另一类方案中用户私钥随用户所在层次递减且密文长度固定[13,14]。与第一类方案相比，后者计算量小且节省带宽，效率更高。

2 广播加密方案

2.1 子集-覆盖框架和 CS 方法

子集-覆盖框架将用户作为二叉树的叶子节点由 Subset 算法和 Cover 算法组成。Subset 算法对用户集合 U 进行划分，使得每个用户属于不同的集合。当有用户子集 R 被系统撤销时，Cover 算法将授权用户集合 $U\backslash R$ 划分为若干个互不相交的集合，使得这些集合的并集覆盖了所有的合法用户。

CS 方法是对子集-覆盖框架中 Subset 算法和 Cover 算法的具体实现。其中 Subset 算法将二叉树中每个节点所包含的叶子节点看作一个集合，每个用户属于若干个祖先节点所对应的集合，如根节点对应的集合为所有用户集合 U。Cover 算法将 R 个撤销用户节点与各个祖先节点组成一棵 Steiner 树，其上节点的一级子节点(不在该树中)所对应的集合即为划分结果。

2.2 广播加密方案的一般形式

在广播加密系统中，广播者对消息进行加密得到密文头部以及密文主体，并将其发送给一群合法用户，每一个合法用户利用其私有信息从密文头部恢复出会话密钥，进而利用该会话密钥解密密文主体。对于不属于该群组的任意非法用户，均不能成功进行如上的解密操作。

文献[2]在子集-覆盖框架下定义了广播加密方案的一般形式，由三个算法组成：

(1)初始化算法

系统调用 Subset 算法将用户集合分成不同的子集$S_1,S_2,\cdots,S_w\subseteq U$，并随机分配每个集合$S_i$长期密钥$L_i\in\Gamma(1\leqslant i\leqslant w)$。对于每个用户 u 系统分配私有信息P_u，使得对于任意满足$u\in S_i$的用户可通过P_u计算出L_i。

(2)广播加密算法

给定消息 M 和被撤销的集合 R，系统调用 Cover 算法将授权用户集合 $U\backslash R$ 划分为互不相交的子集和$\{S_{R_1},S_{R_2},\cdots,S_{R_m}\}$。随机选取会话密钥 $K\in\mathrm{K}$ 广播加密消息即密文 $C=([R_1,E(L_{R_1},K)]\|[R_2,E(L_{R_2},K)]\|\cdots\|[R_m,E(L_{R_m},K)],F_{\mathrm{K}}(M))$，其中第一部分称为密文头部，$F_{\mathrm{K}}(M)$称为密文主体。

(3)用户端解密算法

当用户 u 收到密文后，在密文头部查找 R_i 满足 $u\in S_{R_i}$(如果 $u\in R$，查找结果为空)，利用私有信息 P_u 计算密钥 L_{R_i} 并解密会话密钥 K，恢复消息 M。

其中 E 和 F_K 为广播加密方案用到的两类加密算法，E 可以为对称加密算法或公钥加密算法。通常情况下为提高效率减少带宽，F_K 应采用快速且无密文扩展的加密算法，如消息 M 和密钥 K 的异或。

2.3 节点预留方法

节点预留方法指的是在系统构建二叉树结构时预留部分节点来代表潜在用户，当有新用户注册时，系统将预留节点分配给该用户，系统运行期间预留节点被视为撤销用户节点。在系统建立之前应选择恰当的预留节点数，使之能够满足一定时间内用户扩展的需求。

3 可扩展的公钥广播加密方案

设系统总用户数量 $N^*=N+N'$，其中 N 为系统建立时已注册用户的数量，N'为潜在用户的数量，则形成用户二叉树的深度 $l=\log N^*+1$。设根节点所在的层为第 0 层，那么用户所在的层为第 l 层。将注册用户在叶子节点上从左到右依次排列，预留节点排在已注册用户节点的后面。设用户 u 的身份为 I_l，定义二叉树中除用户以外其余节点的身份，使之能够唯一标识该节点，如定义根节点的身份为 I_0。若用户 u 祖先节点(不包括根节点)的身份为 $I_i(0<i<l)$，其中 i 表示 u 的第 i 层祖先节点，那么用户地址 $ID=(I_0,I_1,\cdots,I_l)$，它的第 i 层祖先节点的地址 $ID_i=(I_0,I_1,\cdots,I_i)$。这种基于 HIBE 中身份的表示方法(即地址)唯一标识了各节点在二叉树中的位置。

采用文献[12]中密文长度固定的 HIBE 算法(BBG-HIBE)，设 g 是 G 中的生成元，双线性映射 $e:G\times G\to G_T$。随机选取 $\alpha\in Z_p$，$g_2,g_3,h_1,\cdots,h_l\in G$，令 $g_1=g^{\alpha}$，$g_4=g_2^{\alpha}$。

系统公开参数 $param=(g,g_1,g_2,g_3,h_1,\cdots,h_l)$，主密钥 $msk=g_4$。

3.1 初始化算法

在 Subset 算法将用户集合分成不同子集的情况下，初始化算法主要解决用户私有信息的分配。在此过程中系统充当 HIBE 中 PKG，调用系统主密钥生成用户私有信息，并以安全的方式发送。

对于用户 u，该用户所对应的地址 $ID=(I_0,I_1,\cdots,I_l)$。系统随机选取 $r\in Z_p$，计算用户私有信息 $P_u=(d,\eta)=([g_2^{\alpha}g_3^{r},g^{r}],[h_1^{r},\cdots,h_l^{r}])$，其中 d 为用户私钥，应妥善保存，η 为密钥生成参数。对于其上第 i 层身份为 I_i 的祖先节点，长期密钥 $L_u^i=g_2^{\alpha}(h_1^{I_1}\cdots h_i^{I_i}g_3)^{r}$。

3.2 广播加密算法

广播加密算法主要涉及授权用户集合的划分和密文头部分的计算。设 Cover 算法将授权用户集合划分为互不相交的子集和$\{S_1,S_2,\cdots,S_m\}$,对于集合 $S_i(1\leqslant i\leqslant m)$,它所对应节点的地址 $ID_i=(I_0,I_1,\cdots,I_l)$。随机选取 $s\in Z_p$,计算其所对应的部分密文头 $H_i=[i,(e(g_1,g_2)^s\cdot K,g^s,(h_1^{I_1}\cdots h_i^{I_i}g_3)^s)]$,最后得到完整的密文头 $H=H_1\parallel H_2\parallel\cdots\parallel H_m$。

3.3 用户端解密算法

当用户 u 收到密文后在密文头部分查找 $H_i=[i,(B_1,B_2,B_3)]$ 满足 $u\in S_i$。设集合 S_i 所对应节点处于该二叉树的第 k 层,用户由私有信息 P_u 计算,$L_k=g_2^{\alpha}(h_1^{rI_1}\cdots h_i^{rI_i}g_3^{r})=g_2^{\alpha}(h_1^{I_1}\cdots h_l^{I_l}g_3)^r$,恢复会话密钥 $K=B_1\dfrac{e(g^r,B_3)}{e(B_2,L_k)}$,最后解密消息。会话密钥的正确性验证如下:

$$B_1\frac{e(g^r,B_3)}{e(B_2,L_k)}=\frac{e(g^{\alpha},g_2^s)e(g^r,(h_1^{I_1}\cdots h_i^{I_i}g_3)^s)}{e(g^s,g_2^{\alpha}(h_1^{I_1}\cdots h_l^{I_l}g_3)^r)}\cdot K=$$

$$\frac{e(g^s,g_2^{\alpha})e(g^s,(h_1^{I_1}\cdots h_i^{I_i}g_3)^r)}{e(g^s,g_2^{\alpha}(h_1^{I_1}\cdots h_l^{I_l}g_3)^r)}\cdot K=K$$

4 方案分析

上述方案采用 HIBE 中地址的表示方法使得广播者只需知道授权用户集合中各个合法用户的地址及系统参数就可广播加密消息,有效地解决了系统中大量公钥的存储、查询等管理问题,扩大了系统的适用范围。同时采用密文长度固定的 HIBE 算法使得用户只需保密两个私钥,配合 l 个密钥生成参数即可恢复长期密钥。与方案[6]的路径表示法相比,系统参数减少了近一半。

由于采用预留节点的方法,系统广播加密消息时将预留节点视为撤销用户节点,对已注册用户节点的划分不产生影响。当新用户注册时,系统按顺序将他们置于预留节点的位置,原有二叉树的子集-覆盖结构及系统参数不需发生变化,完全实现了接收者无状态的需求。

此外,该方案的安全性由 CS 方法及 BBG-HIBE 算法的安全性保障,在 CS 方法的正确划分下,BBG-HIBE 在标准模型下是 IND-sID-CCA 安全的,因此任意非法用户均不能得到解密消息的任何信息。

5 结束语

本文在 CS 方法的基础上采用 HIBE 中的身份表示法及预留节点的方法构造了一种接收者无状态下可扩展的公钥广播加密方案。该方案减少了公钥广播加密系统中大量公钥使用带来的系统运行和维护的负担,系统参数较已有方案大大减少,真正满足了接收者无状态的需要。同时该方案中用户密钥持有量小,运算效率高,在实际中有着广泛的应用前景。

参考文献:

[1] Fiat A,Naor M.Broadcast encryption[C]//Stinson D.LNCS773:Advances in Cryptology-CRYPTO 1993.Berlin,Germany:Springer-Verlag,1993:480-491.

[2] Naor D,Naor M,Lotspiech J.Revocation and tracing schemes for stateless receiver[C]//Kilian J.LNCS2139:Advances in Cryptology-CRYPTO 2001.Berlin,Germany:Springer-Verlag,2001:41-62.

[3] Halevy D,Shamir A.The LSD broadcast encryption scheme[C]//Yung M.LNCS2442:Advances in Cryptology-CRYPTO 2002,Berlin,Germany:Springer-Verlag,2002:47-60.

[4] Dodis Y,Fazio N.Public key broadcast encryption for stateless receivers[C]//Feigenbaum J.LNSC2696:Proceedings of Digital Right Management Workshop 2002.Berlin,Germany:Springer-Verlag,2002:61-80.

[5] Horwitz J,Lynn B.Toward hierarchical identity-based encryption[C]//Knudsen L R.LNCS2332:Advances in Cryptology -EUROCRYPT 2002,Amsterdam,The Netherlands,April 28 -May 2,2002.Berlin,Germany:Springer-Verlag,2002:466-481

[6] 陈昭智,郑建德.一种基于身份分层结构加密算法的广播加密方案[J].厦门大学学报:自然科学版,2006,45(3):342-346.

[7] 匡建民,谷大武.广播加密方案的一个注记[J].计算机工程,2006,32(2):147-148.

[8] Boneh D,Franklin M.Identity based encryption from the Weil pairing[C]//Kilian J.LNCS2139:Advances in Cryptology-CRYPTO 2001.Berlin:Springer-Verlag,2001:213-229.

[9] Galbraith S D,Harrison K,Soldera D.Implementing the Tate pairing[C]//Fieker C,Kohel D R.LNCS2369:ANTS.Berlin,Germany:Springer-Verlag,2002:324-337.

[10] Shamir A.Identity-based cryptosystems and signature schemes[C]//Blakley G R,Chaum D.LNCS196:Advances in Cryptology-CRYPTO 1984,Santa Barbara,CA,USA,August 19 -23,1985.Berlin,Germany:Springer-Verlag,1984:47-53.

[11] Gentry C,Silverberg A.Hierarchical ID -based cryptography[C]//Zheng Yuliang.LNCS2501:Advances in Cryptology -ASIACRYPT 2002,Queenstown,New Zealand,December 1-5,2002.Berlin,Germany:Springer-Verlag,2002:548-566.

[12] Boneh D,Boyen X.Efficient selective -ID secure identity based encryption without random oracles[C]//Cachin C,Camenisch J.LNCS3027:Advances in Cryptology-EUROCRYPT 2004,International Conference on the Theory and Applications of Cryptographic Techniques,Interlaken,Switzerland,May 2-6,2004.Berlin,Germany:Springer-Verlag,2004:223-238.

[13] Boneh D,Boyen X,Goh Eu-Jin.Hierarchical identity based encryption with constant size ciphertext[C]//Cramer R.LNCS3494:Advances in Cryptology -EUROCRYPT 2005,Aarhus,Denmark,May 22-26,2005.Berlin,Germany:Springer-Verlag,2005:440-456.

[14] Au Man Ho,Liu J K,Yuen T Hon,et al.Practical hierarchical identity based encryption and signature scheme without random oracles,2006/368[R/OL].Cryptology ePrint Archive,2006.http://eprint.iacr.org/.