可证安全的基于证书广播加密方案

李继国,张亦辰,卫晓霞
(河海大学计算机与信息学院,江苏南京 210098)

摘 要: 广播加密可使发送者选取任意用户集合进行广播加密,只有授权用户才能够解密密文.但是其安全性依赖广播中心产生和颁布群成员的解密密钥.针对这一问题,本文提出基于证书广播加密的概念,给出了基于证书广播加密的形式化定义和安全模型.结合基于证书公钥加密算法的思想,构造了一个高效的基于证书广播加密方案,并证明了方案的安全性.在方案中,用户私钥由用户自己选取,证书由认证中心产生,解密密钥由用户私钥和证书两部分组成,克服了密钥托管的问题.在方案中,广播加密算法中的双线性对运算可以进行预计算,仅在解密时做一次双线性对运算,提高了计算效率.

关键词: 广播加密;基于证书加密;双线性对
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2016)05-1101-10
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.05.013

A Provably Secure Certificate-Based Broadcast Encryption Scheme

LI Ji-guo, ZHANG Yi-chen, WEI Xiao-xia
(*College of Computer and Information Engineering, Hohai University, Nanjing, Jiangsu* 210098, *China*)

Abstract: Broadcast encryption allows a sender to securely broadcast to any subset of the group members. However, its security heavily depends on broadcast centre to generate and distribute decryption secret keys for group members. In order to solve the above problem, we propose the notion of certificate-based broadcast encryption, describe the formal definition and security model of the certificate-based broadcast encryption. Furthermore, we also provide an efficient certificate-based broadcast encryption scheme. In our scheme, the decryption key includes user's private key and a certificate, where the private key is chosen by user himself, and the certificate is generated by certification authority. Therefore, our scheme overcomes the key escrow problem. In addition, our scheme is efficient, because it needs only one paring in decryption algorithm and paring operation in encryption algorithm can be pre-computed.

Key words: broadcast encryption; certificate-based encryption; bilinear paring

1 引言

对于有 N 个用户的系统,假设需要通过公开的信道发送某个消息给其中 S 个用户,要求只有这 S 个用户能够解密密文,其余用户不能由密文恢复出消息.直观的方法是用这 S 个用户的公钥分别进行加密,将对应的密文通过公开信道传送,由于这 S 个用户拥有对应的私钥,可以保证只有指定用户才能进行解密.但这种方法的计算代价很大,消息发送者需要将同一段消息加密 S 次并传输,而广播加密就可以很好地解决这类问题.广播加密方案是实现一点对多点通信的一种方式,在一个广播加密系统中,广播者可以对某个集合内的用户发起广播,加密后的消息在公开信道上进行传送,任何监听广播的用户均能获得广播密文,只有被授权的合法接收者才可以进行解密,恢复出广播消息,而其它监听广播信道的不法用户均无法恢复广播的明文.在收费电视、数字版权保护、安全电子邮件等特殊领域,其效率远远高于传统的点对点通信方式,有广泛的实际应用背景.

广播加密是一种在不安全信道上给一组用户传输加密信息的密码体制,它可使发送者选取任意用户集合进行广播加密,只有授权用户才能够解密密文.2001年,Naor等人[1]用完备子树和子集差分的方法巧妙地构造了一个高效的广播加密方案,该方案分割集合的

收稿日期:2014-07-29;修回日期:2014-11-28 责任编辑:马兰英
基金项目:国家自然科学基金(No.61272542);中央高校基本科研项目(No.2013B07014)

效率很高,并使用数学知识证明了两种分割方法的正确性,适用于数量较大的合法用户和数量较少的非法用户集合. Boneh 等人[2,3]提出了可抗完全联合攻击的广播加密方案,方案的优点是缩短了密文和密钥的长度,其缺点是公钥长度与接收用户数目成正比. 为了克服文献[2,3]中的缺点,Liu 等人[4]提出了一个公钥定长的广播加密方案,并缩减了私钥的长度,并证明方案在随机预言模型下可抵抗完全联合攻击. 2007 年,Delerablée[5]结合基于身份的公钥密码体制提出了基于身份的广播加密方案,方案中密文和私钥长度都是固定的,但是公钥长度与接收用户集合数目成线性关系. Gentry 和 Waters[6]提出一个半静态安全的新概念,并给出从半静态安全系统到自适应安全系统的通用"双密钥"转换. 进一步,构造了具有固定密文长度的广播加密系统. 最近,Boneh 等[7]使用多线性映射技术较好地解决了公钥广播加密中密文和密钥过长的问题,并给出三个构造. 提出的方法能够完全抵抗任意数量合谋者的攻击. 上述方案中接收者的解密密钥都是由广播中心计算生成,通过安全通道发送给各个用户,存在密钥托管问题,并且需要建立安全信道. Tan 等人[8]提出了一个传统公钥密码体制下的安全公钥广播加密方案,用户的私钥由用户自己选择,避免了密钥托管问题,但是用户私钥由 6 个群元素组成,公钥由 4 个群元素组成,用户的密钥存储代价较大,并且存在证书管理问题. Phan 等[9]去除了群管理者,提出了分布式动态广播加密的概念,利用"黑盒"思想,给出一个具体的构造,该构造可以看作子集覆盖框架的拓展. 伍前红等[10]结合了广播加密和群密钥协商提出了捐助广播加密(Contributory Broadcast Encryption)密码原语. 在这种新密码原语下,提出了具有短密文的捐助广播加密方案. 为了解决叛徒跟踪和撤销问题,Hofheinz 和 Striecks[11]基于文献[12],提出了具有跟踪和撤销的广播加密方案. Boneh 和 Zhandry[13]使用不可区分混淆技术,构造了多方密钥交换,高效广播加密和叛徒跟踪方案.

Gentry[14]在 2003 年首次提出基于证书的公钥密码体制(Certificate-Based Cryptography,简称 CBC),该体制中用户私钥由用户自己选取,加密方案中的解密密钥由用户私钥和 CA 颁发的证书构成. 由于解密密钥由两部分组成,且证书在公开信道中发送,避免了密钥托管和建立安全信道的问题,也简化了证书的管理,所以基于证书的公钥密码体制为构建安全高效的公钥基础设施 PKI(Public Key Infrastructure,简称 PKI)提供了有效的方法. 2006 年,Morillo 等人[15]基于 Waters[16] IBE(Identity-Based Encryption,简称 IBE)方案提出了第一个标准模型下满足自适应选择密文安全的 CBE(Certificate-Based Encryption,简称 CBE)方案. Dodis 等人[17]利用选择密文安全的 IBE 方案和 PKE(Public Key Encryption,简称 PKE)方案以及一次签名构造出选择密文安全的 CBE 方案. 为了减少通信代价,Galindo 等人[18]对文献[17]中的 CBE 方案进一步改进,缩短了密文的长度,使其安全规约更加简洁,并在标准模型下证明了方案是自适应选择密文安全的. Lu 等人[19]提出高效的基于证书加密方案,该方案通过预计算减少了双线性对的运算次数,仅在解密时做一次双线性对运算,与其它方案相比提高了计算效率.

本文集成基于证书公钥密码体制[14,20,21]的思想,首次提出基于证书广播加密的概念,给出方案的形式化定义和安全模型,构造了一个具体的基于证书广播加密方案,并证明方案在自适应选择密文攻击下是安全的. 提出的广播加密方案中用户的私钥为两个群元素,用户的公钥也由两个群元素组成,用户的密钥存储代价较低. 在方案中,广播加密算法中的双线性对运算可以进行预计算,仅在解密时做一次双线性对运算,计算效率较高. 并且广播系统中的用户可以随时加入或退出广播系统,而不需要对其它用户的密钥进行更新. 此外,本文提出的方案可以抵抗完全联合攻击.

2 困难问题假设

定义 1 双线性映射 G_1 和 G_2 是两个 q 阶加法循环群,G_T 是 q 阶乘法循环群,q 为大素数. P_1 和 P_2 分别是群 G_1、G_2 的两个生成元,双线性映射 $e:G_1\times G_2\to G_T$ 具备以下三个性质[17,18]:

(1)双线性:对任意的 $P\in G_1$,$Q\in G_2$,$a,b\in Z_q$,有 $e(aP,bQ)=e(P,Q)^{ab}$.

(2)非退化性:$e(P_1,P_2)\neq 1$(G_T 中单位元).

(3)可计算性:e 是可有效计算的.

若 G_1 和 G_2 相同,该双线性映射被称为对称双线性映射,G_1 和 G_2 不同则称为非对称双线性映射. 本文使用的双线性映射为对称双线性映射.

定理 1 如果 $p=2q+1$,且 p 和 q 为两个大的奇素数,对于整数 a,若 $0<a<p-1$,那么 $-a^2$ 为模 p 的二次非剩余,同时也是模 p 的本原元[8].

定义 2 *k* − *mBDHI* 问题[22] (Modified BDHI for k-values):G_1 是 q 阶加法循环群,其中 q 为大素数,P 是群 G_1 的生成元,给定 $(P,sP,(h_1+s)^{-1}P,(h_2+s)^{-1}P,\cdots,(h_k+s)^{-1}P)$(其中 $s\in Z_q^*$ 未知,$h_1,h_2,\cdots,h_k\in Z_q^*$ 已知),计算出 $e(P,P)^{(s+h)^{-1}}$,满足 $h\notin\{h_1,h_2,\cdots,h_k\}$.

概率多项式时间算法 A 解决 G_1 上的 $k-mBDHI$ 问题的优势定义为:$Succ_{A,G_1}^{k\text{-}mBDHI}=\Pr[A(P,sP,(h_1+s)^{-1}P,(h_2+s)^{-1}P,\cdots,(h_k+s)^{-1}P)=e(P,P)^{(s+h)^{-1}}]$,其中:$h_1,h_2,\cdots,h_k$ 已知,$s,h\in Z_q^*$,s 未知,$h\notin\{h_1,h_2,\cdots,h_k\}$.

$k-mBDHI$ 困难问题假设　如果不存在概率多项式时间算法 A 能以不可忽略的优势解决 G_1 上的 $k-mBDHI$ 问题,则称群 G_1 上的 $k-mBDHI$ 问题是难解的.

定义 3　判断 Diffie-Hellman 问题(DDH 问题)　在有限域中,g 为 q 阶乘法循环群的一个生成元,q 为大素数,已知(g,g^a,g^b,T),其中 $a,b\in Z_q^*$ 且 a,b 未知,判断 T 是否等于 g^{ab}.

DDH 困难问题假设　若不存在概率多项式时间算法能以不可忽略的优势判断 T 是否等于 g^{ab},则称 DDH 问题在有限域中是难解的.

3　基于证书广播加密方案的形式化定义及安全模型

结合基于证书加密方案的形式化定义和广播加密的一般构造,下面分别给出基于证书广播加密方案的形式化定义及安全模型.

3.1　基于证书广播加密的形式化定义

设 S_N 为所有广播用户的集合,其中 $N=\{1,2,\cdots,n\}$. 一个基于证书的广播加密方案由一个广播密钥封装机制和一个对称加密方案组成,包括下面五个算法:

系统参数设置算法 Setup　该算法由 CA 运行. CA 选择系统的安全参数 ζ,运行此算法产生主公钥和主密钥(mpk,msk)以及其它系统参数,公开系统参数 $params$(包括系统主公钥 mpk),CA 保存系统主密钥 msk.

用户密钥生成算法 Extract　该算法由用户 $ID_i(i\in N)$运行. 用户 ID_i 利用系统参数 $params$ 生成自己的公/私钥对(PK_i,SK_i),私钥 SK_i 自己保存,公钥 PK_i 公开.

证书产生算法 Certify　该算法由 CA 中心运行. CA 以用户 ID_i 的身份信息、公钥 PK_i、系统参数 $params$ 和主私钥 msk 为输入,产生用户证书 $Cert_{ID_i,t}$,并通过公开信道发送给用户 ID_i.

加密算法 Enc　该算法由广播者运行. 广播者选择广播集合 $S=\{ID_1,ID_2,\cdots,ID_w\}$,满足 $w\leqslant n$. 对于需要广播的消息 m,算法以广播集合 S、广播公钥 PK_S 和系统公开参数 $params$ 为输入,先计算$(Hdr,k)=Enc(S,PK_S)$,其中报头 Hdr 是对对称密钥 k 的封装,$k\in K$,K 为对称加密方案(E,D)的密钥空间,再用对称加密算法 E 以 k 为密钥对 m 进行加密,生成对应的密文 $C_0=E_k(m)$,将 $C=(S,Hdr,C_0)$通过广播信道进行广播.

解密算法 Dec　该算法由用户 $ID_i(ID_i\in S)$运行. 在收到广播密文 C 后,用户 ID_i 首先利用私钥 SK_i、证书 $Cert_{ID_i,t}$ 以及报头信息 Hdr 恢复出对称加密算法的密钥 $k=Dec(Hdr,SK_i,Cert_{ID_i,t})$,最后以 k 和对称加密方案的解密算法 D 恢复出对应的消息 $m=D_k(C_0)$或者直接输出无效标志 $\perp$.

一个安全的基于证书广播加密方案必需满足以下性质:

(1)正确性　按照方案的步骤正常运行生成的广播密文可以被合法用户正确解密.

(2)保密性　在不知道合法用户的私钥和证书的情况下,任何监听广播的用户都无法正确解密.

(3)抗联合攻击　若广播集合外的所有用户联合起来也无法破解广播密文,则称该方案可抵抗完全联合攻击.

(4)用户的动态加入和退出　可以方便的实现用户加入和退出广播集合,并且对于新加入的用户而言,只能正常解密加入后的广播消息,而不能解密之前的广播消息,对于已撤销的用户而言,不能对撤销之后的广播消息进行解密.

3.2　基于证书广播加密的安全模型

2005 年,Boneh 等人[2]定义了广播加密的静态安全模型. 2007 年,Delerablée[5]结合基于身份公钥加密的性质,给出了基于身份广播加密方案的安全模型. 本文结合上述两个安全模型以及 Gentry[14]提出的基于证书加密方案的安全模型,引入公钥替换攻击思想[23~26],首次刻画了基于证书广播加密方案的安全模型. 在本文所定义的安全模型下,基于证书广播加密方案的安全性是指在自适应选择密文攻击下,对于静态敌手而言是密文不可区分的,且能抵抗完全联合攻击.

基于证书广播加密方案中包含两类攻击者 A_I 和 A_{II}. A_I 模拟了未认证的用户这一类敌手,它可以获得任意用户的私钥,不可以获得目标广播集合内任何用户的证书,但可以询问目标广播集合外任意用户的证书,可以进行除目标密文外的解密询问,A_I 还可以进行公钥替换攻击,可以获得替换后公钥所对应的证书,但若敌手 A_I 对目标广播集合内的用户进行了公钥替换攻击,则 A_I 不能询问替换后公钥所对应的证书. A_{II}模拟了一个恶意的 CA,它拥有系统主密钥,可以生成任意用户的证书,不可以询问目标广播集合内用户的私钥,但可以获得目标广播集合外任意用户的私钥,A_{II}也可以进行公钥替换,但不可以替换目标广播集合内用户的公钥,可以进行除目标广播密文外的解密询问.

广播加密方案一般是由一个密钥封装算法和一个对称加密算法组成,对称加密算法都是选取自适应选择密文攻击下安全的算法,在定义方案的安全模型时只对密钥封装算法部分进行定义. 由于我们的安全模型是针对静态敌手,所以敌手在系统参数生成前需要确定目标广播集合. 结合上述两类敌手及其各自不同的攻击能力,下面分别给出两类敌手与挑战者之间的游戏:

游戏 1

初始化阶段 A_I 选择目标广播集合 $S^*, S^* \subseteq S_N$.

系统参数设置 挑战者 C 运行算法 Setup,生成系统的主公/私钥对(mpk, msk)以及其它系统参数,C 保存主私钥 msk,把系统参数 $params$(包括主公钥 mpk)发送给 A_I.

第一阶段询问(Phase 1) 在该阶段,A_I 可向挑战者 C 自适应地进行下列询问:

公钥询问 A_I 提交任意用户 ID_i 的身份信息,C 返回 ID_i 所对应的公钥信息.

私钥提取询问 A_I 提交用户 ID_i 的身份信息,C 返回 ID_i 所对应的私钥.

公钥替换 A_I 提交(ID_i, PK_i', SK_i'),C 将 ID_i 的公钥替换为 PK_i'.

证书询问 A_I 提交(ID_i, PK_i),若 $ID_i \in S^*$,C 拒绝回复询问;否则 C 运行证书生成算法,返回(ID_i, PK_i)对应的证书.

解密询问 A_I 提交(ID_i, S_i, Hdr_i),其中 $ID_i \in S_i$. C 运行解密算法返回对应的 k_i 或无效标志 $\perp$.

挑战阶段 A_I 判断 Phase 1 询问结束后,C 运行广播加密算法,计算$(Hdr^*, k^*) = Enc(S^*, PK_{S^*}), k^* \in K$,然后 C 随机选择 $\lambda \in \{0,1\}, k \in K$,令 $k_\lambda = k^*, k_{1-\lambda} = k$,将$(Hdr^*, k_{1-\lambda}, k_\lambda)$返回给 A_I.

第二阶段询问(Phase 2):A_I 可继续类似 Phase1 中的步骤进行询问,但解密询问时不可对 Hdr^* 进行询问.

猜测 Phase 2 询问结束后 A_I 输出 λ',若 $\lambda' = \lambda$,则称 A_I 赢得该游戏.

我们定义 A_I 赢得游戏 1 的优势为:

$$Adv_{A_I}^{Static-IND-CCA2} = |2\Pr[\lambda' = \lambda] - 1| = |\Pr[\lambda' = 1 | \lambda = 1] - \Pr[\lambda' = 1 | \lambda = 0]|.$$

定义 4(静态自适应选择密文攻击下密文不可区分 *Static-IND-CCA2*) 如果经过最多 q_{PK} 次公钥询问、q_{SK} 次私钥询问、q_r 次公钥替换询问、q_C 次证书询问、q_d 次解密询问后,不存在概率多项式时间的静态(static)敌手 A_I 能在 t 时间内以不可忽略的优势赢得游戏 1,即 $Adv_{A_I}^{Static-IND-CCA2} < \varepsilon$,那么就称该基于证书的广播加密方案对于静态敌手 A_I 是$(t, q_t, \varepsilon)-IND-CCA2$ 安全的,其中 $q_t = (q_{PK} + q_{SK} + q_r + q_C + q_d)$.

游戏 2

初始化阶段 A_{II} 选择目标广播集合 $S^*, S^* \subseteq S_N$.

系统参数设置 挑战者 C 运行算法 Setup,生成系统的主公/私钥对(mpk, msk)以及其它系统参数,将主私钥 msk 和系统参数 $params$(包括系统主公钥 mpk)都发送给敌手 A_{II}.

第一阶段询问(Phase 1) 在该阶段,A_{II} 可以自适应地向挑战者 C 进行下列询问:

公钥询问 A_{II} 提交任意用户 ID_i 的身份信息,C 返回 ID_i 对应的公钥信息.

私钥提取询问 A_{II} 提交用户 ID_i 的身份信息,若 $ID_i \in S^*$,C 拒绝回复询问;否则返回用户 ID_i 所对应的私钥.

公钥替换 A_{II} 提交(ID_i, PK_i', SK_i'),若 $ID_i \in S^*$,C 拒绝替换;否则 C 将 ID_i 的公钥替换为 PK_i'.

解密询问 A_{II} 提交(ID_i, S_i, Hdr_i),其中 $ID_i \in S_i$,C 运行解密算法返回对应的 k_i 或无效标志 $\perp$.

挑战阶段 A_{II} 判断 Phase 1 询问结束后,C 运行广播加密算法,生成$(Hdr^*, k^*) = Enc(S^*, PK_{S^*}), k^* \in K$,随机选择 $\lambda \in \{0,1\}, k \in K$,令 $k_\lambda = k^*, k_{1-\lambda} = k$,将$(Hdr^*, k_{1-\lambda}, k_\lambda)$返回给 A_{II}.

第二阶段询问(Phase 2) A_{II} 可类似 Phase 1 中的步骤继续进行询问,但解密询问时不可对目标 Hdr^* 进行询问.

猜测 Phase 2 询问结束后 A_{II} 输出 λ',若 $\lambda' = \lambda$,则称 A_{II} 赢得该游戏.

我们定义 A_{II} 赢得游戏 2 的优势为:

$$Adv_{A_{II}}^{Static-IND-CCA2} = |2\Pr[\lambda' = \lambda] - 1| = |\Pr[\lambda' = 1 | \lambda = 1] - \Pr[\lambda' = 1 | \lambda = 0]|.$$

定义 5(静态自适应选择密文攻击下密文不可区分 *Static-IND-CCA2*) 如果经过最多 q_{PK} 次公钥询问、q_{SK} 次私钥询问、q_r 次公钥替换询问、q_d 次解密询问后,不存在概率多项式时间的静态(static)敌手 A_{II} 能在 t 时间内以不可忽略的优势赢得游戏 2,即 $Adv_{A_{II}}^{Static-IND-CCA2} < \varepsilon$,那么就称该基于证书广播加密方案对于静态敌手 A_{II} 是$(t, q_t, \varepsilon)-IND-CCA2$ 安全的,其中 $q_t = (q_{PK} + q_{SK} + q_r + q_d)$.

注:敌手在进行询问时,允许敌手询问目标广播集合以外的所有用户信息,因此本文给出的安全模型是可以抵抗完全联合攻击的.

4 基于证书广播加密方案

在这部分中,首次提出了一个基于证书广播加密方案,并对它进行正确性分析. 该方案由以下五个算法组成:

系统参数设置算法 Setup 该算法由 CA 中心运行,系统安全参数为 ζ. G_1 为一个 q 阶加法循环群,G_2 为一个 q 阶乘法循环群,$p = 2q + 1$,其中 p, q 均为大素数,$e: G_1 \times G_1 \to G_2$ 是(G_1, G_2)上可计算的双线性映射. P 是群 G_1 的一个生成元,随机选择 $s \in Z_q^*$ 作为系统主私钥 msk,计算主公钥 mpk 为 $Q = sP, g_1 = e(P, P)$,CA 任选一个整数 a,满足 $0 < a < p - 1$,令 $g_2 = -a^2$(a 可销毁或保

密). 再选 $p_i=2q_i+1, i\in\{1,2,\cdots,n\}$,满足 $p<p_i$,由定理 1 可知,g_2 为 $p_i(i\in\{1,2,\cdots,n\})$ 的公共本原元. *CA* 选择三个安全可抗碰撞的哈希函数:$H_1:\{0,1\}^*\rightarrow Z_q^*$, $H_2:G_2\times Z_q^*\rightarrow Z_q^*$, $H_3:Z_q^*\times Z_q^*\rightarrow Z_q^*$, K 为对称密钥集合,S_N 为所有用户的集合,$N=\{1,2,\cdots,n\}$. 主私钥 s 由 *CA* 保存,公开系统参数 $params:\{\zeta,G_1,G_2,e,q,P,Q,g_1,g_2,p,S_N,p_i,K,H_1,H_2,H_3\}$.

用户密钥生成算法 Extract　该算法由用户 ID_i 运行. 用户 ID_i 随机选择 $x_{i1},x_{i2}\in Z_{p_i}^*$ 作为其私钥 $SK_i=(SK_{i1},SK_{i2})$,计算 $PK_{i1}=g_2^{x_{i1}}\bmod p_i$, $PK_{i2}=x_{i2}P$,用户 ID_i 的公钥 $PK_i=(PK_{i1},PK_{i2})$. 私钥由用户自己保存,公钥公开.

证书产生算法 Certify　该算法由 *CA* 中心运行. 对于用户 ID_i 的身份信息及其对应的公钥 PK_i,*CA* 选择时间参数 τ,先计算 $h_i=H_1(\tau\parallel ID_i\parallel PK_i)$,然后计算用户 ID_i 的证书 $Cert_{ID_{i,\tau}}=\dfrac{1}{h_i+s}PK_{i2}$,通过公开信道发送给 ID_i.

加密算法 Enc　该算法由广播者运行. 广播加密算法由一个密钥封装算法和一个安全的对称加密算法共同来实现:

步骤 1　广播者选择需要广播的集合 $S\subseteq S_N$.

步骤 2　对于 $ID_i\in S$,广播者依次计算 $h_i=H_1(\tau\parallel ID_i\parallel PK_i)$, $Q_{ID_i\in S}=h_iP+Q$.

步骤 3　广播者随机选择 $r,\sigma\in Z_q^*$,计算 (Hdr,k): $k=H_2(g_1^r,\sigma)$, $k\in K$, $Q'_{ID_i}=rQ_{ID_i\in S}=r(h_iP+Q)$,根据中国剩余定理可计算 $PK^S=\sum_{ID_i\in S}PK_{i1}^rM_iY_i\bmod M_S$,其中 $M_S=\prod_{ID_i\in S}p_i$, $M_i=M_S/p_i$, $M_iY_i\equiv 1\bmod p_i$. $Hdr=(Q'_{ID_i},g_2^r,\sigma\cdot PK_S,H_3(\sigma,k))$. 对于消息 m,运用对称加密算法 E 生成密文 $C_0=E_k(m)$.

步骤 4　广播者通过公开的广播信道广播消息 $C=(Hdr,S,C_0)$.

解密算法 Dec　该算法由用户 $ID_i(ID_i\in S)$ 运行. 在收到广播密文 C 后,用户 ID_i 以其私钥 SK_i、证书 $Cert_{ID_i,\tau}$ 为输入,按照下面的步骤计算,最后输出 C 对应的消息 m 或者无效标志 $\perp$:

步骤 1　用户 $ID_i\in S$ 计算 $\sigma'=\dfrac{\sigma\cdot PK_S}{(g_2^r)^{x_{i1}}}\bmod p_i$.

步骤 2　计算 $g_1^{r'}=e(Q'_{ID_i},Cert_{IDi,\tau})^{1/x_{i2}}$.

步骤 3　计算 $k'=H_2(g_1^{r'},\sigma')$.

步骤 4　验证 $H_3(\sigma',k')$ 是否等于 $H_3(\sigma,k)$,若相等,则以对称加密方案中的解密算法 D 返回 $m=D_{k'}(C_0)$,否则返回 $\perp$.

对于广播的消息该方案只需要进行一次加密,系统可以对 $g_1=e(P,P)$ 进行预计算,加密算法中就不需要进行双线性对运算,仅在解密算法中做一次双线性对运算,提高了计算效率.

该方案可以实现用户的动态加入和退出,在该方案中,当有新用户加入系统时,该用户只要选择密钥 $x_{i1},x_{i2}\in Z_{p_i}^*$ 并公开公钥,要求 $p_i>p$ 且未出现过,而不需要改变系统内其它用户的公、私钥,由于在加密阶段新加入用户的公钥 $PK_{i1}=g_2^{x_{i1}}\bmod p_i$ 没有参与广播集合公钥 $PK_S=\sum_{ID_i\in S}PK_{i1}^rM_iY_i\bmod M_S$ 的生成,因此新加入用户不能使用中国剩余定理解密之前的广播消息;当要撤销某用户时,只要将其公钥信息删除,也不需要改变系统内其它用户的公、私钥. 对于已撤销用户而言,因为在加密阶段不再使用撤销用户的公钥 $PK_{i1}=g_2^{x_{i1}}\bmod p_i$ 产生广播集合公钥 $PK_S=\sum_{ID_i\in S}PK_{i1}^rM_iY_i\bmod M_S$,所以撤销用户无法使用中国剩余定理对撤销之后的广播消息进行解密.

正确性分析

本文的方案里,广播集合里的合法用户可将接收到的正确的广播密文恢复出对应的广播消息.

(1)用户 $ID_i\in S$ 收到广播密文后计算:

$$\sigma'=\frac{\sigma\cdot PK_S}{(g_2^r)^{x_{i1}}}\bmod p_i=\frac{\sigma\cdot PK_S}{(g_2^{x_{i1}})^r}\bmod p_i$$
$$=\frac{\sigma\cdot PK_S}{PK_{i1}^r}\bmod p_i=\sigma.$$

(2)用户根据 Q'_{ID_i} 计算:

$$g_1^{r'}=e(Q'_{ID_i},Cert_{IDi,\tau})^{1/x_{i2}}$$
$$=e\left(r(h_iP+Q),\frac{1}{h_i+s}PK_{i2}\right)^{1/x_{i2}}$$
$$=e\left(r(h_i+s)P,\frac{x_{i2}}{h_i+s}P\right)^{1/x_{i2}}$$
$$=e(P,P)^r=g_1^r$$

(3)根据 σ' 和 $g_1^{r'}$ 就可以恢复出对称加密的密钥 $k'=H_2(g_1^{r'},\sigma')$,若 $H_3(\sigma',k')=H_3(\sigma,k)$,由对称加密方案的解密算法 D 可正确恢复出明文 $m=D_{k'}(C_0)$,否则输出 $\perp$.

5　安全性证明

下面根据 3.2 节提出的安全模型给出本方案的安全性证明. 由于不同的敌手具备不同的能力,本文刻画了两个游戏来模拟不同敌手与挑战者之间的交互,从而证明方案的安全性. 本文提出的方案是由一个密钥封装算法和一个安全的对称加密算法构成,假定选取的对称加密算法为自适应选择密文安全的算法,在进行安全性证明时,只对密钥封装算法部分进行分析,分析敌手是否能由头文件 *Hdr* 以不可忽略的优势区分出

对称加密算法的对称密钥 k. 由于是静态敌手,所以在系统参数产生之前两类敌手都需要先选定目标广播集合.

定理 2 如果存在概率多项式时间静态敌手 A_I,经过最多 q_{PK}次公钥询问、q_{SK}次私钥询问、q_r 次公钥替换询问、q_{H_1}次 H_1 询问、q_{H_2}次 H_2 询问、q_C 次证书询问、q_d 次解密询问后,在最多 t 时间内以不小于 ε 的概率赢得游戏 1,那么就存在一个算法可以在 t'时间内以不小于 ε' 的概率解决 $k-mBDHI$ 问题,其中 $k\geq(q_{H_1}-w)$,$\varepsilon'=(1-w/q_t)^{q_d}\varepsilon/q_{H_2}$,$w$ 为广播集合内的用户个数,$q_t=(q_{PK}+q_{SK}+q_r+q_C+q_d)$.

证明 给定一个 $k-mBDHI$ 问题实例 $(P,sP,(h_1+s)^{-1}P,(h_2+s)^{-1}P,\cdots,(h_k+s)^{-1}P)$,其中 $s\in Z_q^*$ 未知,$h_1,h_2,\cdots,h_k\in Z_q^*$ 已知. 构造算法 B,B 模拟挑战者与敌手 A_I 交互,最后输出 $e(P,P)^{(s+h)^{-1}}$,满足 $h\in Z_q^*$ 且 $h\notin(h_1,h_2,\cdots,h_k)$.

初始化阶段 A_I 选择目标广播集合 $S^*\subseteq S_N$,$|S^*|=w$.

系统参数设置算法(Setup) B 运行算法 Setup. B 令系统主公钥 $Q=sP$,其中 sP 为 $k-mBDHI$ 困难问题的输入,主私钥为 s 未知. 将系统参数 $params=\{\zeta,G_1,G_2,e,q,P,Q,g_1,g_2,p,S_N,p_i,K,H_1,H_2,H_3\}$ 发送给 A_I.

第一阶段询问(Phase 1) B 保存列表 $L_{A_I}:\{ID_i,PK_i,SK_i,h_i,Cert_{ID_{i,\tau}},\delta\}$,列表初始化为 $\{\perp,\perp,\perp,\perp,\perp,0\}$,列表 $L_{H_2}:\{(g_i,\sigma_i),k_i\}$,初始化为 $\{(\perp,\perp),\perp\}$. 在该阶段,A_I 可以向 B 自适应地进行下列询问:

公钥询问 A_I 提交任意用户 ID_i 的身份信息,B 检查 L_{A_I}:

(1)若未对 ID_i 进行过任何询问,即 ID_i 为 $\perp$,B 选择 $x_{i1},x_{i2}\in Z_{p_i}^*$ 作为其私钥 SK_i,计算 $PK_{i1}=g_2^{x_{i1}}\bmod p_i$,$PK_{i2}=x_{i2}P$,用户 ID_i 的公钥 $PK_i=(PK_{i1},PK_{i2})$,B 将 $\{ID_i,(g_2^{x_{i1}},x_{i2}P),(x_{i1},x_{i2}),\perp,\perp,0\}$ 添加到列表 L_{A_I}中,返回 ID_i 的公钥 PK_i.

(2)若 ID_i 不为 $\perp$,B 直接返回 ID_i 的公钥 PK_i.

私钥提取询问 A_I 提交用户 ID_i 的身份信息,B 检查 L_{A_I}.

(1)若未对 ID_i 进行过任何询问,即 ID_i 为 $\perp$,则 B 选择 $x_{i1},x_{i2}\in Z_{p_i}^*$ 作为其私钥 SK_i,计算 $PK_{i1}=g_2^{x_{i1}}\bmod p_i$,$PK_{i2}=x_{i2}P$,用户 ID_i 的公钥 $PK_i=(PK_{i1},PK_{i2})$,B 将 $\{ID_i,(g_2^{x_{i1}},x_{i2}P),(x_{i1},x_{i2}),\perp,\perp,0\}$ 添加到列表 L_{A_I}中,返回 ID_i 的私钥 SK_i.

(2)若 ID_i 不为 $\perp$,B 直接返回 ID_i 的私钥 SK_i.

公钥替换 A_I 提交 (ID_i,PK_i',SK_i'),B 直接更新列表 L_{A_I}为:$\{ID_i,PK_i',SK_i',\perp,\perp,1\}$.

H_1 询问 A_I 提交用户的身份信息 ID_i 和公钥信息 PK_i,B 检查 L_{A_I}:

(1)若 $ID_i\notin S^*$,B 随机选择 h_i,满足 $h_i\in(h_1,h_2,\cdots,h_k)$ 且未曾出现过,更新列表 L_{A_I}为:$\{ID_i,PK_i,SK_i,h_i,\perp,\delta\}$,$\delta$ 表示保持原状. B 返回 h_i.

(2)若 $ID_i\in S^*$,B 随机选取 $h_i'\in Z_q^*$,$h_i'\notin(h_1,h_2,\cdots,h_k)$ 且未曾出现过,更新列表 L_{A_I}:$\{ID_i,PK_i,SK_i,h_i',\perp,\delta\}$,$\delta$ 表示保持原状. B 返回 h_i'.

H_2 询问 A_I 提交 (g_i,σ_i),B 检查 L_{H_2}:

(1)若存在 $\{(g_i,\sigma_i),k_i\}$ 元组,则 B 返回 k_i.

(2)若不存在 $\{(g_i,\sigma_i),k_i\}$ 元组,B 随机选择 $k_i\in K$ 且未曾出现过,将 $\{(g_i,\sigma_i),k_i\}$ 添加到 L_{H_2}中,返回 k_i.

证书询问 A_I 提交用户 ID_i 的身份信息,若 $ID_i\in S^*$,B 输出 $\perp$ 并退出(对目标集合中用户公钥询问证书,拒绝询问),否则若 $ID_i\notin S^*$ 则检查 L_{A_I},$Cert_{IDi,\tau}$不为 $\perp$ 时,直接返回 $Cert_{IDi,\tau}$,否则:

(1)若未对 ID_i 进行过任何询问,即 ID_i 为 $\perp$,B 先进行公钥询问,任意选择 $x_{i1},x_{i2}\in Z_{p_i}^*$ 作为其私钥 $SK_i=(SK_{i1},SK_{i2})$,计算 $PK_{i1}=g_2^{x_{i1}}\bmod p_i$,$PK_{i2}=x_{i2}P$,用户 ID_i 的公钥 $PK_i=(PK_{i1},PK_{i2})$,再随机选择 h_i,满足 $h_i\in(h_1,h_2,\cdots,h_k)$ 且未曾出现过,计算 $Cert_{IDi,\tau}=\frac{1}{h_i+s}P\cdot SK_{i2}=\frac{1}{h_i+s}x_{i2}P=\frac{1}{h_i+s}PK_{i2}$,其中 $\frac{1}{h_i+s}P$ 为困难问题的输入. 将 $\{ID_i,(g_2^{x_{i1}},x_{i2}P),(x_{i1},x_{i2}),h_i,\frac{1}{h_i+s}x_{i2}P,0\}$ 添加到列表 L_{A_I}中. 返回 $Cert_{IDi,\tau}$.

(2)ID_i 不为 $\perp$ 时,若 h_i 为 $\perp$,则 B 随机选择 h_i,满足 $h_i\in(h_1,h_2,\cdots,h_k)$ 且未曾出现过,计算 $Cert_{IDi,\tau}=\frac{1}{h_i+s}P\cdot SK_{i2}=\frac{1}{h_i+s}x_{i2}P=\frac{1}{h_i+s}PK_{i2}$,$\frac{1}{h_i+s}P$ 为困难问题的输入,B 更新列表 L_{A_I}:$\{ID_i,PK_i,SK_i,h_i,\frac{1}{h_i+s}x_{i2}P,\delta\}$,$\delta$ 表示保持原来的状态;若 h_i 不为 $\perp$,则 B 直接计算 $Cert_{IDi,\tau}=\frac{1}{h_i+s}P\cdot SK_{i2}=\frac{1}{h_i+s}x_{i2}P=\frac{1}{h_i+s}PK_{i2}$,$\frac{1}{h_i+s}P$ 为困难问题的输入,B 更新列表 L_{A_I}:$\{ID_i,PK_i,SK_i,h_i,\frac{1}{h_i+s}x_{i2}P,\delta\}$,$\delta$ 表示保持原来的状态. 返回 $Cert_{IDi,\tau}$.

解密询问 A_I 对 (ID_i,S_i,Hdr_i) 进行询问,其中 $ID_i\in S_i$. 若 $ID_i\in S^*$,则 B 失败并退出;否则 B 按步骤计算生成 $(SK_i,Cert_{ID_{i,\tau}})$,运行解密算法:

(1) $\frac{\sigma_i\cdot PK_{S_i}}{(g_2^{r_i})^{x_{i1}}}\bmod p_i=\frac{\sigma_i\cdot PK_{S_i}}{(g_2^{x_{i1}})^{r_i}}\bmod p_i=\frac{\sigma_i\cdot PK_{S_i}}{PK_{i1}^{r_i}}\bmod p_i=\sigma_i$.

(2)根据头文件 Hdr_i 恢复出的 Q_{ID_i}'再计算

$$e(Q_{ID_i}',Cert_{IDi,\tau})^{1/x_{i2}}=e(r_i(h_iP+Q),\frac{1}{h_i+s}x_{i2}P)^{1/x_{i2}}$$

$$=e(r_i(h_i+s)P,\frac{x_{i2}}{h_i+s}P)^{1/x_{i2}}$$
$$=e(P,P)^{r_i}$$
$$=g_1^{r_i}$$

(3)根据 σ_i 和 $g_1^{r_i}$ 计算出对称加密的密钥 $k_i=H_2(g_1^{r_i},\sigma_i)$,验证 $H_3(\sigma_i,k_i)$通过后返回对应的 k_i.

挑战阶段　A_I 判断 Phase 1 询问结束后,B 运行广播加密算法:

(1)对于 $ID_i\in S^*$,选择 $l_i\in Z_q^*$,计算 $Q_{ID_i}^*=l_iP$.

(2)B 随机选择 $\sigma,r\in Z_q^*$,生成(Hdr^*,k^*):随机选择 $k^*\in K$,根据中国剩余定理可计算 $PK_{S^*}=\sum_{ID_i\in S^*}PK_{i1}^r M_iY_i \bmod M_{S^*}$,其中 $M_{S^*}=\prod_{ID_i\in S^*}p_i$, $M_i=M_{S^*}/p_i$, $M_iY_i\equiv 1\bmod p_i$. $Hdr^*=(Q_{ID_i\in S^*}^*,g_2^r,\sigma\cdot PK_{S^*},H_3(\sigma,k^*))$. B 再随机选择 $\lambda\in\{0,1\}$, $k\in K$,令 $k_\lambda=k^*$, $k_{1-\lambda}=k$,将 $(Hdr^*,k_{1-\lambda},k_\lambda)$返回给 A_I.

第二阶段询问(Phase 2)　A_I 可继续进行 Phase 1 中的各种询问,但解密询问时不可对(ID_i,S^*,Hdr^*)进行询问,其中 $ID_i\in S^*$.

猜测　Phase 2 询问结束后 A_I 猜测 $\lambda'\in\{0,1\}$. B 在 L_{H_2}中随机选择$\{(g_i,\sigma_i),k_i\}$,B 输出$(g_i)^{1/l_i}$作为 $k-mBDHI$ 的解.

分析

由定义可知,$Q_{ID_i}^*=l_iP=r(h_i'P+Q)=r(h_i'+s)P$,即 $l_i=r(h_i'+s)$,若 $g_i=e(P,P)^r$,则 $(g_i)^{1/l_i}=e(P,P)^{r\cdot(1/l_i)}=e(P,P)^{r\cdot 1/r(h_i'+s)}=e(P,P)^{1/(h_i'+s)}$,因为 $h_i'\notin(h_1,h_2,\cdots,h_k)$,所以 B 解决了 $k-mBDHI$ 困难问题.

下面分析 B 解决 $k-mBDHI$ 困难问题的概率:

B 要解决 $k-mBDHI$ 困难问题就必须保证在与 A_I 进行交互时没有失败退出. 由游戏模拟过程可知,当 A_I 对目标集合内用户进行解密询问时,B 挑战失败. 记事件 E_1 表示 A_I 未对目标集合内用户进行解密询问,其概率 $\Pr[E_1]=(1-w/q_t)^{q_d}$.

事件 E_2 表示 L_{H_2}中存在$\{(g^*,\sigma^*),k^*\}$,即 A_I 对(g^*,σ^*)进行过 H_2 询问,则 $\Pr[\lambda'=\lambda]=\Pr[\lambda'=\lambda\mid E_2]\Pr[E_2]+\Pr[\lambda'=\lambda\mid\neg E_2]\Pr[\neg E_2]\geq\varepsilon$,若 A_I 未对(g^*,σ^*)进行 H_2 询问,而是随机猜测,则 $\Pr[\lambda'=\lambda\mid\neg E_2]=1/2$,即 $\Pr[\lambda'=\lambda]=\Pr[\lambda'=\lambda\mid E_2]\Pr[E_2]+\frac{1}{2}\Pr[\neg E_2]\geq\Pr[E_2]+\frac{1}{2}\Pr[\neg E_2]=\frac{1}{2}(1+\Pr[E_2])$,可知 $\Pr[E_2]\geq 2\Pr[\lambda'=\lambda]-1=\varepsilon$.

事件 E_3 表示 B 选择了满足需要的$\{(g^*,\sigma^*),k^*\}$元组,其概率 $\Pr[E_3]\geq 1/q_{H_2}$.

B 要成功破解 $k-mDBDHI$ 问题必须保证事件 E_1, E_2, E_3 同时发生,$\Pr[B\ Success]\geq(1-w/q_t)^{q_d}\cdot\varepsilon\cdot 1/q_{H_2}=(1-w/q_t)^{q_d}\varepsilon/q_{H_2}$,即若存在概率多项式时间的敌手 A_I 能在 t 时间内以不可忽略的优势 ε 赢得游戏 1,则必然存在一个概率多项式时间的算法能够以不小于 ε' 的概率解决 $k-mBDHI$ 问题,其中 $\varepsilon'=(1-w/q_t)^{q_d}\varepsilon/q_{H_2}$. 而由于 $k-mBDHI$ 困难问题是难解的,所以不存在概率多项式时间的敌手 A_I 能在 t 时间内以不可忽略的优势赢得游戏 1,即该方案能够抵抗第一类敌手攻击.

定理 3　如果存在概率多项式时间静态敌手 A_{II},经过最多 q_{PK}次公钥询问、q_{SK}次私钥询问、q_r 次公钥替换询问、q_d 次解密询问后,在最多 t 时间内以不小于 ε 的概率赢得游戏 2,那么就存在一个算法可以在 t'时间内以不小于 ε' 的概率解决 DDH 问题,其中 $\varepsilon'=(1-w/q_t)^{q_d}(1+\varepsilon)/2$,$w$ 为广播集合内的用户个数,$q_t=(q_{PK}+q_{SK}+q_r+q_d)$.

证明　(g,g^a,g^b,T)为一个 DDH 问题的输入,构造算法 B,在游戏中 B 模拟挑战者与敌手 A_{II}进行交互,最后判断 T 是否等于 g^{ab}.

初始化阶段　A_{II}选择目标广播集合 $S^*\subseteq S_N$, $|S^*|=w$.

系统参数设置算法　挑战者 B 运行算法 Setup. B 随机选择 $s\in Z_q^*$ 作为系统主私钥 msk,P 为群 G_1 生成元,计算主公钥 $Q=sP$,令 $g_2=g$(素阶乘法循环群中每个群元素都为群的生成元,单位元除外),g 为 DDH 困难问题的输入. 系统参数 $params=\{\zeta,G_1,G_2,e,q,P,Q,g_1,g,p,S_N,p_i,K,H_1,H_2,H_3\}$,其中 H_1,H_2,H_3 为三个可公开计算的抗碰撞哈希函数,将主私钥 s 和系统参数 $params$ 发送给敌手 A_{II}.

第一阶段询问(Phase 1)　B 保存列表 $L_{A_{II}}$:$\{ID_i,PK_i,SK_i,\delta\}$,初始化为$\{\perp,\perp,\perp,0\}$,$A_{II}$可以自适应地向挑战者 B 进行下列询问:

公钥询问　A_{II}提交任意用户 ID_i 的身份信息,B 检查 $L_{A_{II}}$:

(1)ID_i 为 $\perp$ 时,即未对 ID_i 进行过任何询问,若 $ID_i\in S^*$,B 任意选择 $t_i,x_{i2}\in Z_{p_i}^*$,计算 $PK_{i1}=(g^a)^{t_i}\bmod p_i$, $PK_{i2}=x_{i2}P$,用户 ID_i 的公钥 PK_i 为(PK_{i1},PK_{i2}),即用户的 $SK_{i1}=at_i$,而 g^a 为 DDH 困难问题的输入,a 未知,所以 B 并不知道真正的第一部分私钥,只知道 t_i 的值. B 更新列表 $L_{A_{II}}$:$\{ID_i,(g^{at_i},x_{i2}P),(t_i,x_{i2}),\perp,0\}$,此处 t_i 并非真正的第一部分私钥,而是 B 选取的随机值,返回 ID_i 的公钥 $PK_i=(g^{at_i},x_{i2}P)$;$ID_i\notin S^*$ 时,B 任意选择 $x_{i1},x_{i2}\in Z_{p_i}^*$,计算 $PK_{i1}=g^{x_{i1}}\bmod p_i$, $PK_{i2}=x_{i2}P$,用户 ID_i 的公钥 PK_i 为(PK_{i1},PK_{i2}),B 更新列表 $L_{A_{II}}$:$\{ID_i,(g^{x_{i1}},x_{i2}P),(x_{i1},x_{i2}),\perp,0\}$,返回 ID_i 的公钥 $PK_i=(g^{x_{i1}},x_{i2}$

P);

(2)若 ID_i 已存在,B 直接返回 ID_i 的公钥 PK_i.

私钥提取询问 A_{II}提交用户 ID_i 的身份信息,若 $ID_i \in S^*$,B 拒绝并输出 $\perp$ 退出,若 $ID_i \notin S^*$,B 检查 $L_{A_{II}}$:

(1)若 ID_i 不存在,B 任意选择 $x_{i1}, x_{i2} \in Z_{p_i}^*$ 作为其私钥 SK_i,计算 $PK_{i1} = g^{x_{i1}} \bmod p_i$,$PK_{i2} = x_{i2}P$,用户 ID_i 的公钥 PK_i 为 (PK_{i1}, PK_{i2}),B 将 $\{ID_i, (g^{x_{i1}}, x_{i2}P), (x_{i1}, x_{i2}), \perp, 0\}$ 添加到列表 $L_{A_{II}}$ 中,返回 ID_i 的私钥 SK_i.

(2)若 ID_i 已存在,B 直接返回 ID_i 的私钥 SK_i.

公钥替换 A_{II}提交 (ID_i, PK_i', SK_i'),若 $ID_i \in S^*$,B 拒绝替换并输出 $\perp$ 退出,否则 B 直接更新列表 L_{A_I} 为: $\{ID_i, PK_i', SK_i', 1\}$.

解密询问 A_{II}对 (ID_i, S_i, Hdr_i) 进行解密询问,其中 $ID_i \in S_i$. 若 $ID_i \in S^*$,则 B 失败并退出;否则,B 同时拥有系统主密钥和用户私钥,直接运行解密算法:

$$\begin{aligned}(1)\frac{\sigma_i \cdot PK_{S_i}}{(g^{r_i})^{x_{i1}}} \bmod p_i &= \frac{\sigma_i \cdot PK_{S_i}}{(g^{x_{i1}})^{r_i}} \bmod p_i \\ &= \frac{\sigma_i \cdot PK_{S_i}}{PK_{i1}^{r_i}} \bmod p_i \\ &= \sigma_i.\end{aligned}$$

(2)根据 $r_i Q_{ID_i}$ 再计算

$$\begin{aligned}&e(r_i Q_{ID_i}, Cert_{IDi,\tau})^{1/x_{i2}} \\ &= e\left(r_i(h_i P + Q), \frac{1}{h_i + s} PK_{i2}\right)^{1/x_{i2}} \\ &= e\left(r_i(h_i + s)P, \frac{x_{i2}}{h_i + s} P\right)^{1/x_{i2}} \\ &= e(P,P)^{r_i} \\ &= g_1^{r_i}\end{aligned}$$

(3)根据 σ_i 和 $g_1^{r_i}$ 计算出对称加密的密钥 $k_i = H_2(g_1^{r_i}, \sigma_i)$,验证 $H_3(\sigma_i, k_i)$ 后返回对应的 k_i 或 $\perp$.

挑战阶段 A_{II}决定 *Phase* 1 询问结束后,B 运行广播加密算法:

(1)对于 $ID_i \in S^*$,B 计算 $Q_{ID_i \in S^*} = h_i P + Q$.

(2)B 随机选择 $r, \sigma \in Z_q^*$,计算目标 (Hdr^*, k^*): $k^* = H_2(g_1^r, \sigma)$,$k^* \in K$,$PK_{S^*} = \sum_{ID_i \in S^*} T^{t_i} M_i Y_i \bmod M_{S^*}$,其中 $M_{S^*} = \prod_{ID_i \in S^*} p_i$,$M_i = M_{S^*}/p_i$,$M_i Y_i \equiv 1 \bmod p_i$,$Hdr^* = (rQ_{ID_i \in S^*}, g^b, \sigma \cdot PK_{S^*}, H_3(\sigma, k^*))$,其中 g^b、T 为 DDH 困难问题的输入,b 未知. B 再随机选择 $\lambda \in \{0,1\}$,$k \in K$,令 $k_\lambda = k^*$,$k_{1-\lambda} = k$,将 $(Hdr^*, k_{1-\lambda}, k_\lambda)$ 返回给 A_{II}.

第二阶段询问(Phase 2) A_{II}可类似 Phase 1 中的步骤继续进行询问,但解密询问时不可以对 (ID_i, S^*, Hdr^*) 进行询问,其中 $ID_i \in S^*$.

猜测 Phase 2 询问结束后猜测 $\lambda' \in \{0,1\}$,若 $\lambda' = \lambda$,则 B 输出 $T = g^{ab}$,否则输出 $T \neq g^{ab}$.

分析

由于 $k^* = H_2(g_1^r, \sigma)$,所以 A_{II}想赢得游戏就需要计算出 g_1^r、σ. 对于第二类敌手,它拥有系统主密钥,所以可以计算出 $g_1^r = e(rQ_{ID_i}, \frac{P}{h_i + s}) = e(P,P)^r$,因此尽管选择的随机数 r 与 b 可能不一样,但是对 A_{II}来讲,它能正确计算出 g_1^r,挑战报头 Hdr^* 对它来讲是合法的. 而计算 σ 的关键部分为 $(g^b, \sigma \cdot PK_{S^*})$,若 $T = g^{ab}$,则:

$$\begin{aligned}PK_{S^*} &= \sum_{ID_i \in S^*} T^{t_i} M_i Y_i \bmod M_{S^*} \\ &= \sum_{ID_i \in S^*} (g^{ab})^{t_i} M_i Y_i \bmod M_{S^*} \\ &= \sum_{ID_i \in S^*} (g^{at_i})^b M_i Y_i \bmod M_{S^*} \\ &= \sum_{ID_i \in S^*} (PK_{i1})^b M_i Y_i \bmod M_{S^*}\end{aligned}$$

即挑战者 B 再挑战阶段构造的挑战密文满足合法的密文格式,反之,若 $T \neq g^{ab}$,则 Hdr^* 并不是合法的报头,只是一个随机数,但是 A_{II}分辨不出,此时 A_{II}不能从之前的询问中获得任何帮助,只能以 $\frac{1}{2}$ 的概率猜对.

下面分析 B 成功破解 DDH 问题的概率:

B 要解决 DDH 困难问题就必须保证在与 A_{II}进行交互时没有失败退出. 由游戏模拟过程可知,当 A_{II}对目标集合内用户进行解密询问时,B 挑战失败. 记事件 E_1 表示 A_{II}未对目标集合内用户进行解密询问,其概率 $\Pr[E_1] = (1 - w/q_t)^{q_d}$.

E_2 表示在 A_{II}未退出游戏、输出猜测后 B 解决 DDH 困难问题的概率,则 $\Pr[E_2] = \Pr[\lambda' = \lambda \mid T = g^{ab}] \cdot \Pr[T = g^{ab}] + \Pr[\lambda' \neq \lambda \mid T \neq g^{ab}] \cdot \Pr[T \neq g^{ab}]$. $T = g^{ab}$ 时 A_{II}能够区分 λ' 的概率不小于 $(1/2 + \varepsilon)$,即 $\Pr[\lambda' = \lambda \mid T = g^{ab}] \geq (1/2 + \varepsilon)$,$T \neq g^{ab}$ 时 A_{II}不能从各种询问中获得有用信息,只能随机猜测 λ',即 $\Pr[\lambda' = \lambda \mid T \neq g^{ab}] = \Pr[\lambda' \neq \lambda \mid T \neq g^{ab}] = 1/2$,因此 B 在 A_{II}输出猜测后解决 DDH 困难问题的概率 $\Pr[E_2] \geq (1/2 + \varepsilon) \cdot 1/2 + 1/2 \cdot 1/2 = (\varepsilon + 1)/2$.

B 要成功破解 DDH 困难问题必须保证事件 E_1,E_2 同时发生,即 $\Pr[B\ Success] = \Pr[E_1] \cdot \Pr[E_2] \geq (1 - w/q_t)^{q_d}(1 + \varepsilon)/2$.

若存在概率多项式时间的敌手 A_{II}能在 t 时间内以不可忽略的优势 ε 赢得游戏 2,则必然存在一个概率多项式时间的算法能够以不小于 ε' 的概率解决 DDH 问题,其中 $\varepsilon' = (1 - w/q_t)^{q_d}(1 + \varepsilon)/2$. 而由于 DDH 问题是难解的,所以不存在概率多项式时间的敌手 A_{II}能在 t 时间内以不可忽略的优势赢得游戏 2,即该方案是能抵抗第二类敌手攻击的.

6 结论

本文构造了一个高效的基于证书广播加密方案,并证明了方案在自适应选择密文攻击下是安全的. 在基于证书广播加密方案中,用户的密钥由用户自己选择,而不是由广播中心分发,避免了密钥托管的问题,同时,由于证书通过公开信道发送,也就不需要建立安全信道. 对于需要广播的消息,广播发送者只需要进行一次加密. 系统可以对双线性对进行预计算,因此在加密过程中就不需要进行双线性对的运算,在解密时只要做一次双线性对运算,提高了计算效率. 并且该方案可以实现用户的动态加入和撤销,不需要更新其它用户的密钥信息,新添加的用户只需将公钥信息添加到公钥列表,而撤销的用户只需删除其公钥信息. 但本文给出的具体构造中密文长度与广播集合中用户数量呈线性增长,下一步将重点研究密文定长广播加密方案.

参考文献

[1] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receiver[A]. Advances in Cryptography-CRYPTO 2001[C]. LNCS 2139, Berlin: Springer-Verlag, 2001. 41 – 62.

[2] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys[A]. Advances in Cryptology-CRYPTO 2005[C]. LNCS 3621, Berlin: Springer-Verlag, 2005. 258 – 275.

[3] Boneh D, Waters B. A fully collusion resistant broadcast, traces, and revokes system[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. ACM New York, NY, USA: 2006. 211 – 220.

[4] Liu Y R, Tzeng W G. Public key broadcast encryption with low number of keys and constant decryption time[A]. PKC 2008[C]. LNCS 4939, Berlin: Springer-Verlag, 2008. 380 – 396.

[5] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys[A]. Advances in Cryptology-ASIACRYPT 2007[C]. LNCS 4833, Berlin: Springer-Verlag, 2007. 200 – 215.

[6] Gentry C, Waters B. Adaptive security in broadcast encryption systems (with short ciphertexts)[A]. Advances in Cryptology-EUROCRYPT 2009[C]. LNCS 5479, Berlin: Springer-Verlag, 2009. 171 – 188.

[7] Boneh D, Waters B. Zhandry M. Low overhead broadcast encryption from multilinear maps[A]. Advances in Cryptology-CRYPTO 2014[C]. LNCS 8616, Berlin: Springer-Verlag, 2014. 206 – 223.

[8] Tan Z W, Liu Z J, Xiao H G. A fully public key tracing and revocation scheme provably secure against adaptive adversary[J]. Journal of Software, 2005, 16(7): 1333 – 1343.

[9] Phan D H, Pointcheval D, Strefler M. Decentralized dynamic broadcast encryption[A]. Security and Cryptography for Networks[C]. LNCS 7485, Berlin: Springer-Verlag, 2012. 166 – 183.

[10] Wu Q H, Qin B, Zhang L, Ferrer J D, Farràs O. Bridging broadcast encryption and group key agreement[A]. Advances in Cryptology-ASIACRYPT 2011[C]. LNCS 7073, Berlin: Springer-Verlag, 2011. 143 – 160.

[11] Hofheinz D, Striecks C. A generic view on trace-and-revoke broadcast encryption schemes[A]. Topics in Cryptology-CT-RSA 2014[C]. LNCS 8366, Berlin: Springer-Verlag, 2014. 48 – 63.

[12] Wee H. Threshold and revocation cryptosystems via extractable hash proofs[A]. Advances in Cryptology-EUROCRYPT 2011[C]. LNCS 6632, Berlin: Springer-Verlag, 2011. 589 – 609.

[13] Boneh D, Zhandry M. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation[A]. Advances in Cryptology-CRYPTO 2014[C]. LNCS 8616, Berlin: Springer-Verlag, 2014. 480 – 499.

[14] Gentry C. Certificate-based encryption and the certificate revocation problem[A]. Advances in Cryptology-EUROCRYPT 2003[C]. LNCS 2656, Berlin: Springer – Verlag, 2003. 272 – 293.

[15] Morillo P, Ràfols C. Certificate-based encryption without random oracles[DB/OL]. Cryptology ePrint Archive, Report 2006/12, 2006.

[16] Waters B. Efficient identity-based encryption without random oracles[A]. Advances in Cryptology-EUROCRYPT 2005[C]. LNCS 3494, Berlin: Springer-Verlag, 2005. 114 – 127.

[17] Dodis Y, Katz J. Chosen-ciphertext security of multiple encryptions[A]. TCC 2005[C]. LNCS 3378, Berlin: Springer-Verlag, 2005. 188 – 209.

[18] Galindo D, Morillo P, Ràfols C. Improved certificate-based encryption in the standard model[J]. Journal of Systems and Software, 2008, 81(7): 1218 – 1226.

[19] 陆阳,李继国,肖军模. 一个高效的基于证书的加密方案[J]. 计算机科学,2009,36(9):28 – 31.
Lu Y, Li J G, Xiao J M. Efficient certificate-based encryption scheme[J]. Computer Science, 2009, 36(9): 28 – 31. (in Chinese)

[20] Li J G, Huang X Y, Hong M X, Zhang Y C. Certificate-based signcryption with enhanced security features[J]. Computers and Mathematics with Applications. 2012, 64(6): 1587 – 1601.

[21] Li J G, Wang Z W, Zhang Y C. Provably secure certificate-based signature scheme without pairings[J]. Informa-

tion Sciences,2013,233(6):313 – 320.

[22] Selvi S, Vivek S, Shukla D. Efficient and provable secure certificateless multi-receiver signcryption [A]. ProvSec 2008[C]. LNCS 5324, Berlin: Springer-Verlag, 2008. 52 – 67.

[23] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[A]. Advances in Cryptology-ASIACRYPT 2003[C]. LNCS 2894, Berlin: Springer-Verlag, 2003. 452 – 473.

[24] Li J G, Huang X Y, Mu Y, Susilo W, Wu Q H. Certificate-based signature: security model and efficient construction [A]. Advances in Cryptology-EuroPKI' 07 [C]. LNCS 4582, Berlin: Springer-Verlag, 2007. 110 – 125.

[25] Li J G, Huang X Y, Mu Y, Susilo W, Wu Q H. Constructions of certificate-based signature secure against key replacement attacks [J]. Journal of Computer Security, 2010, 18(3): 421 – 449.

[26] Li J G, Huang X Y, Zhang Y C, Xu L Z. An efficient short certificate-based signature scheme [J]. Journal of Systems and Software, 2012, 85(2): 314 – 322.

作者简介

李继国(通信作者) 男,1970 年生于黑龙江富裕,博士,教授,博士生导师,主要研究领域为信息安全、密码学理论与技术、云计算安全等. E-mail: ljg1688@163.com

张亦辰 女,1971 年生于黑龙江齐齐哈尔,学士,博士研究生,讲师,主要研究领域为密码学理论与技术.