基于身份的代理重签名广播签密方案

李超零[1] 陈 越[1] 王成良[2] 李文俊[3] 王双进[3]
(信息工程大学电子技术学院 郑州 450004)[1] (解放军 73672 部队 南京 210016)[2]
(解放军 73501 部队 东山 363400)[3]

摘 要 针对云计算组数据共享等应用中的数据机密性和完整性需求,提出了一种基于身份的代理重签名广播签密方案,该方案能通过执行一次代理重签名将原签密者的广播签密转换为重签密者的广播签密。利用计算性双线性Diffie-Hellman问题和计算性Diffie-Hellman问题的困难性假设,证明了方案在选择多身份、适应性选择密文攻击下具有不可区分性,在选择多身份选择消息攻击下具有不可伪造性。该方案具有公开可验证性,支持任何第三方对签密正确性的验证。最后,给出了方案在云计算组数据共享中的应用实例。

关键词 代理重签名,广播签密,随机预言机模型,双线性对,公开可验证
中图法分类号 TP309 **文献标识码** A

Identity-based Broadcast Signcryption with Proxy Re-signature

LI Chao-ling[1] CHEN Yue[1] WANG Cheng-liang[2] LI Wen-jun[3] WANG Shuang-jin[3]
(Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou 450004, China)[1]
(Unit 73672 of the PLA, Nanjing 210016, China)[2] (Unit 73501 of the PLA, Dongshan 363400, China)[3]

Abstract To protect data confidentiality and integrity in cloud data sharing and other applications, an identity-based broadcast signcryption scheme with proxy re-signature was proposed. This scheme could transform a broadcast signcryption from the initial signcrypter to the re-signcrypter by executing a proxy re-signature. It is proved that this scheme has indistinguishability against chosen multiple identities and adaptive chosen ciphertext attacks and existential unforgeability against chosen multiple identities and message attacks in terms of the hardness of CBDH(computational bilinear diffie-hellman) problem and CDH(computational diffie-hellman) problem. At last, its application in cloud data sharing was introduced.

Keywords Proxy re-signature, Broadcast signcryption, Random oracle model, Bilinear map, Public verifiability

签密能在一个合理的逻辑步骤内同时实现数字签名和公钥加密,从而能一次性实现对数据的机密性和完整性保护,并且在计算量、密文长度和通信成本等方面比传统的"先签名再加密"方法更具优势,因而得到了研究人员的广泛关注,也在电子现金支付和密钥分配等方面得到了广泛的应用。

目前,签密方案的研究主要集中于具有特殊性质的签密方案的设计与应用,如代理签密、多重代理签密、门限签密、基于身份的签密、多接收者签密、代理重签密等[1-9]。在代理重签密方面,文献[5]通过扩展RSA-TBOS签密方案,提出了一个RSA-TBOS代理重加密签密方案;文献[6]在普通的基于身份签密方案的基础上,提出了一个基于身份的代理重加密签密方案。这两个方案实现了对解密功能的转换,可以应用于保密认证的电子邮件转发和分布式存储等方面,但其对签密的认证需要明文信息的直接参与,不具有公开可验证性,同时也增大了密钥管理的复杂度。针对文献[6]中方案不支持公开可验证的问题,文献[7]对其进行了改进,并进一步提出了适用于带半可信第三方(Semi-Trusted Third Party, STTP)的认证邮件协议的代理重加密签密方案。文献[8,9]提出了一种基于身份的代理重签密方案,同时实现了对解密和验证功能的转换,该方案具有公开可验证性,对既需要保密又需要连续认证的电子邮件或路由认证协议具有良好的适用性。这些代理重签密方案都只针对单一接收者的情况,不能满足对多接收者代理重签密的需求,并且在某些应用中(如组数据共享)只要求对签密中的验证功能进行转换。因而,本文提出了一种基于身份的代理重签名广播签密方案,即由代理对原签密者的广播签密进行验证功能转换,以得到重签密者对明文消息的广播签密。该方案具有公开可验证性,任何第三方在得到公开参数和重签密者公钥后都可以验证签密的正确性,并且该过程不会泄漏任何有关数据明文或参与者隐私的信息。在计算性双线性Diffie-Hellman问题和计算性Diffie-Hellman问题假设下证明了方案的安全性,并给出了方案在云计算组数据共享中的应用实例。

到稿日期:2012-07-28 返修日期:2012-11-22 本文受国家973项目(2012CB315901)资助。
李超零(1985-),男,博士生,主要研究方向为可信计算、云计算,E-mail:lichunxiang-01@163.com;**陈 越**(1965-),男,教授,博士生导师,主要研究方向为网络与信息安全;**王成良**(1982-),男,硕士,助理工程师,主要研究方向为现代密码学;**李文俊**(1982-),男,硕士,工程师,主要研究方向为网络与信息安全。

1 形式化定义

一个基于身份的代理重签名广播签密(Identity-based Broadcast Signcryption with Proxy Re-signature,IBSPR)方案由以下5个算法组成。

系统建立(Setup):给定安全参数 k,密钥生成中心(Public Key Generator,PKG)生成系统公开参数 cp 和系统公私钥对 (s,P_{pub})。

密钥提取(Extract):给定一个用户身份 ID_U,PKG 运行算法 $Extract(ID_U)$,得到用户私钥 S_U 并以安全的方式发送给用户。

签密(Signcrypt):给定 n 个接收人的身份 $ID_1,\cdots,ID_n$ 和消息 m,身份为 ID_A 的原签密者计算 $Signcrypt(m,S_A,ID_1,\cdots,ID_n)$,得到签密密文 σ。

重签名(Resign):对于重签密者身份为 ID_B 的情况,Proxy 运行算法 $Resign(\sigma,ID_A,ID_B)$,该算法首先验证 σ 中签名的有效性,验证通过后将 σ 中的签名转化为 ID_B 的签名,得到新的签密密文 σ'。

解签密(Designcrypt):收到密文 σ' 后,接收人 $ID_i(1\leqslant i\leqslant n)$ 运行算法 $Designcrypt(\sigma',S_{ID_i},ID_B)$,该算法首先验证 σ' 中签名的有效性,通过后解密得到消息 m。

2 安全模型

我们在"选择多身份攻击"模型[10]下定义 IBSPR 方案的机密性和不可伪造性。

机密性又称为适应性选择密文攻击下的密文不可区分性,IBSPR 方案在选择多身份、适应性选择密文攻击下的不可区分性定义如下。

定义 1(机密性) 若没有任何多项式有界的敌手能以不可忽略的优势赢得以下游戏,则称一个 IBSPR 方案在选择多身份、适应性选择密文攻击下具有不可区分性。

系统建立:挑战者 $\mathscr{C}$ 运行 Setup 算法生成系统主密钥 s 和公开参数 cp,$\mathscr{C}$ 将参数 cp 发送给敌手 $\mathscr{A}$ 并秘密保存主密钥 s。收到参数 cp 后,敌手 $\mathscr{A}$ 输出多个目标身份 $ID_1^*,\cdots,ID_n^*$。

询问阶段:在该阶段,敌手 $\mathscr{A}$ 可以进行一系列询问,包括密钥提取询问、签密询问和解签密询问。

• $\mathscr{A}$ 选择一个身份 ID_U 并询问其私钥。$\mathscr{C}$ 运行算法 $Extract(ID_U)$ 得到相应的私钥 S_U,并将其返回给 $\mathscr{A}$。这里,$\mathscr{A}$ 不能询问相应于目标身份的私钥,即 $ID_U\neq ID_i^*$ $(1\leqslant i\leqslant n)$。

• 签密询问:$\mathscr{A}$ 选择一个消息 m、原签密者的身份 ID_A、重签密者的身份 ID_B 和 n 个接收人的身份 $ID_{R_1},\cdots,ID_{R_n}$,询问经代理重签名广播签密后的密文。$\mathscr{C}$ 运行算法 $\sigma=Signcrypt(m,S_A,ID_{R_1},\cdots,ID_{R_n})$ 和 $\sigma'=Resign(\sigma,ID_A,ID_B)$,并将 σ' 返回给 $\mathscr{A}$。

• 解签密询问:$\mathscr{A}$ 选择一个密文 σ' 和接收人身份 ID_{R_i} $(1\leqslant i\leqslant n)$,询问解签密结果。$\mathscr{C}$ 运行算法 $Designcrypt(\sigma',S_{R_i},ID_B)$ 得到相应的明文 m,并将其返回给 $\mathscr{A}$;若密文无效,则返回 $\perp$。

挑战密文生成:$\mathscr{A}$ 选择两个等长的明文 m_0 和 m_1、原签密者私钥 S_A 和重签密者私钥 S_B,并将它们发送给 $\mathscr{C}$。$\mathscr{C}$ 随机选择一个比特 $b\in\{0,1\}$,计算 $\sigma_*=Signcrypt(m_b,S_A,ID_1^*,\cdots,ID_n^*)$ 和 $\sigma_*'=Resign(\sigma,ID_A,ID_B)$,得到一个给目标身份的代理重签名的广播签密密文 σ_*',并将其返回给 $\mathscr{A}$。

猜测:获得挑战密文后,$\mathscr{A}$ 可以继续进行如上询问,但它不能询问挑战密文 σ_*' 在任何一个目标身份下的解签密结果。同时,由于密文 σ' 可以看作是消息密文和接收人信息两部分的组合,$\mathscr{A}$ 可以询问得到一个密文 σ'',使得 σ'' 与 σ' 的消息密文部分相同,而只有接收人信息部分不同。因而,$\mathscr{A}$ 也不能询问对一个密文 σ_*'' 的解签密结果,其中 σ_*'' 与 σ_*' 消息密文部分相同而接收人信息部分不同。最后,$\mathscr{A}$ 输出一个比特 b' 作为对 b 的猜测。

若 $b'=b$,则称 $\mathscr{A}$ 赢得该游戏,其赢得游戏的优势定义为:$Adv(\mathscr{A})=2\Pr[b'=b]-1$。

IBSPR 在选择多身份、选择消息攻击下的存在性不可伪造的安全定义中,允许敌手代表多个攻击目标身份中的一个伪造密文。我们通过如下的在挑战者 $\mathscr{C}$ 和伪造者 $\mathscr{F}$ 间的游戏来定义 IBSPR 在选择多身份、选择消息攻击下的存在性不可伪造。

定义 2(不可伪造性) 若没有任何多项式有界的敌手能以不可忽略的优势赢得以下游戏,则称一个 IBSPR 方案具有选择多身份选择消息攻击下的存在不可伪造性。

系统建立:挑战者 $\mathscr{C}$ 运行 Setup 算法生成系统主密钥 s 和公开参数 cp,$\mathscr{C}$ 将参数 cp 发送给敌手 $\mathscr{F}$ 并秘密保存主密钥 s。收到参数 cp 后,敌手 $\mathscr{F}$ 输出多个目标身份 $ID_1^*,\cdots,ID_n^*$。

询问阶段:$\mathscr{F}$ 可以进行一系列询问,包括密钥提取询问、签密询问和解签密询问。

• 密钥提取询问:$\mathscr{F}$ 选择一个身份 ID_U 并询问其私钥。$\mathscr{C}$ 运行算法 $Extract(ID_U)$ 得到相应的私钥 S_U,并将其返回给 $\mathscr{F}$。这里,$\mathscr{F}$ 不能询问相应于目标身份的私钥,即 $ID_U\neq ID_i^*$ $(1\leqslant i\leqslant n)$。

• 签密询问:$\mathscr{F}$ 选择一个消息 m、原签密者的身份 ID_A、重签密者的身份 ID_B 和 n 个接收人的身份 $ID_{R_1},\cdots,ID_{R_n}$,询问经代理重签名广播签密后的密文。$\mathscr{C}$ 运行算法 $\sigma=Signcrypt(m,S_A,ID_{R_1},\cdots,ID_{R_n})$ 和 $\sigma'=Resign(\sigma,ID_A,ID_B)$,并将 σ' 返回给 $\mathscr{F}$。

• 解签密询问:$\mathscr{F}$ 选择一个密文 σ' 和接收人身份 ID_{R_i} $(1\leqslant i\leqslant n)$,询问解签密结果。$\mathscr{C}$ 运行算法 $Designcrypt(\sigma',S_{R_i},ID_B)$ 并将得到的结果返回给 $\mathscr{F}$,这个结果由签过名的明文、原签密者的公钥和重签密者的公钥组成;若密文无效,则返回 $\perp$。

伪造:$\mathscr{F}$ 生成一个密文 σ' 和 n 个任意接收人的密钥对 $(ID_{R_1},S_{R_1}),\cdots,(ID_{R_n},S_{R_n})$,要求这个密文没有询问过 $\sigma=Signcrypt(m,S_A,ID_{R_1},\cdots,ID_{R_n})$ 和 $\sigma'=Resign(\sigma,ID_A,ID_B)$。其中,$ID_B=ID_i^*$ $(1\leqslant i\leqslant n)$,$ID_A$ 可以为任意身份。若利用某个接收人的私钥对 σ' 解密所得结果为一个签过名的消息 (m,Sig,ID_A,ID_B),并且 (m,Sig) 对于身份 ID_B 是有效的消息签名对,则称 $\mathscr{F}$ 赢得了该游戏。

定义 3(公开可验证性) 对于一个 IBSPR 方案,在获得系统公开参数和重签密者公钥的情况下,任何第三方都能验证该密文的重签密者是否为指定的签密者,并且验证者不能获得有关签密者和接收人更多的信息,则称该方案具有公开可验证性。

3 双线性对及相关数学困难问题

设 G_1 是一个阶为素数 q 的加法循环群，其生成元为 p，G_2 是一个阶为 q 的乘法循环群，随机数 $a,b\in Z_q^*$。假设群 G_1 和 G_2 上的离散对数问题都是困难的。

定义 4(双线性对) 称 G_1 和 G_2 之间的映射 $e:G_1\times G_1\to G_2$ 为一个双线性对，若其满足以下条件：

- 双线性：对任意的 $P,Q\in G_1$，有 $e(aP,bQ)=e(P,Q)^{ab}$；
- 非退化性：存在 $P,Q\in G_1$，使得 $e(P,Q)\neq 1$；
- 可计算性：对于 $P,Q\in G_1$，存在一个有效的算法计算 $e(P,Q)$。

定义 5(计算性双线性 Diffie-Hellman 问题，CBDH) 给定 G_1，G_2 和 e，以及 $P,aP,bP,cP\in G_1$，计算 $e(P,P)^{abc}$，其中 $a,b,c\in Z_q^*$ 且为未知的。一个概率多项式时间算法 $\mathcal{G}$ 解决 G_1 中的 CBDH 问题的优势定义为：$Adv_{\mathcal{G}}^{CDH}=\Pr[\mathcal{G}(P,aP,bP,cP)=e(P,P)^{abc}]$。

CBDH 假设：对于所有的概率多项式时间算法 $\mathcal{G}$，概率 $Adv_{\mathcal{G}}^{CDH}$ 是可忽略的。

定义 6(计算性 Diffie-Hellman 问题，CDH) 给定 P，$aP,bP\in G_1$，计算 abP，其中 $a,b\in Z_q^*$ 且为未知的。一个概率多项式时间算法 $\mathcal{G}$ 解决 G_1 中 CDH 问题的优势定义为：$Adv_{\mathcal{G}}^{DH}=\Pr[\mathcal{G}(P,aP,bP)=abP]$。

CDH 假设：对于所有的概率多项式时间算法 $\mathcal{G}$，概率 $Adv_{\mathcal{G}}^{DH}$ 是可忽略的。

4 方案构造

Setup：给定安全参数 $k\in\mathbf{N}$，PKG 选择一个阶为素数 $q(q\geqslant 2^k)$ 的循环加群 G_1 和同阶的循环乘群 G_2，并定义一个双线性映射 $e:G_1\times G_1\to G_2$。设 P 表示 G_1 的生成元，随机选择参数 $s\in Z_q^*$ 作为系统主密钥，并计算系统公钥 $P_{pub}=sP$。选择 3 个密码学 Hash 函数 $H_0:\{0,1\}^*\to G_1$，$H_1:\{0,1\}^*\times G_1\times G_1\to Z_q^*$，$H_2:G_2\to\{0,1\}^t$，其中，$t$ 表示用户身份标识和明文消息连接后的长度。系统公开参数为 $cp=(q,G_1,G_2,e,P,P_{pub},H_0,H_1,H_2)$。

Extract：给定用户 U 的身份 $ID_U\in\{0,1\}^*$，PKG 计算其公钥 $Q_U=H_0(ID_U)$ 和相应的私钥 $S_U=sQ_U$。

Signcrypt：假设广播签密的接收人为 $ID_1,\cdots,ID_n$，Alice(身份为 ID_A)对消息 m 进行初始化广播签密，并将签密密文提交给 Proxy，由 Proxy 将签名转化为 Bob(身份为 ID_B)的签名。Alice 执行如下操作：

(1)随机选择 $r\in Z_q^*$ 和 $Q_R\in G_1$，计算 $X=rP$，$Q_A=H_0(ID_A)$，$Q_B=H_0(ID_B)$，$Q_{R_S}=r(Q_B-Q_A)$，$Q_i=H_0(ID_i)(1\leqslant i\leqslant n)$；

(2)计算 $V=e(rP_{pub},Q_R)$，$C=H_2(V)\oplus(ID_A\parallel m)$，$h=H_1(C,X,Q_R)$，$W=hS_A+rQ_A$，$U_i=r(Q_R+Q_i)$，$T_i=(ID_i,U_i)(1\leqslant i\leqslant n)$，其中 $S_A=sQ_A$；

(3)得到签密密文 $\sigma=(X,W,C,Q_R,T_1,\cdots,T_n)$，并将 σ 和 Q_{R_S} 发送给 Proxy。

Resign：收到 σ 和 Q_{R_S} 后，Proxy 执行如下操作：

(1)计算 $h'=H_1(C,X,Q_R)$，验证等式 $e(P,W)=e(X+h'P_{pub},Q_A)$ 是否成立，若成立，则向 PKG 申请重签名私钥，否则返回⊥；PKG 计算 $S_{R_S}=S_B-S_A$，并将其返回给 Proxy；

(2)计算 $W'=W+h'S_{R_S}+Q_{R_S}$，则新的签密密文为 $\sigma'=(X,W',C,Q_R,T_1,\cdots,T_n)$。

Designcrypt：收到密文 σ' 后，身份为 ID_i 的接收人可以验证签名的有效性，并利用其私钥 S_i 解密得到消息 m。

(1)计算 $h''=H_1(C,X,Q_R)$，验证等式 $e(P,W')=e(X+h''P_{pub},Q_B)$ 是否成立，若成立，则执行(2)，否则返回⊥；

(2)计算 $V'=e(P_{pub},U_i)e(X,S_i)^{-1}$，$(ID_A\parallel m)=C\oplus H_2(V')$。

5 安全性分析

5.1 正确性

$$\begin{aligned}e(P,W)&=e(P,hS_A+rQ_A)=e(P,hsQ_A+rQ_A)\\&=e((hs+r)P,Q_A)=e(X+hP_{pub},Q_A)\end{aligned}$$

$$\begin{aligned}W'&=W+h'S_{R_S}+Q_{R_S}\\&=hS_A+rQ_A+h(S_B-S_A)+r(Q_B-Q_A)\\&=hS_B+rQ_B\end{aligned}$$

所以 $e(P,W')=e(X+hP_{pub},Q_B)$。

$$\begin{aligned}V'&=e(P_{pub},U_i)e(X,S_i)^{-1}\\&=e(P_{pub},r(Q_R+Q_i))e(X,sQ_i)^{-1}\\&=e(rP_{pub},Q_R+Q_i)e(rP_{pub},Q_i)^{-1}\\&=e(rP_{pub},Q_R)e(rP_{pub},Q_i)e(rP_{pub},Q_i)^{-1}\\&=e(rP_{pub},Q_R)\end{aligned}$$

5.2 机密性

定理 1 在随机预言机模型下，若存在一个敌手 $\mathcal{A}$，其经过至多 q_{H_0} 次 H_0 询问、q_{H_1} 次 H_1 询问、q_{H_2} 次 H_2 询问、q_{Ex} 次 Extract 询问、q_{SC} 次签密询问和 q_{De} 次解签密询问后，能以不可忽略的优势 ε 区分两个有效的签密密文，则存在一个算法 $\mathcal{C}$，其能以优势 $Adv_{\mathcal{C}}^{BDH}\geqslant(\varepsilon-q_{H_2}q_{De}/2^k)/q_{H_2}$ 解决 CBDH 问题的一个实例。

证明：给定 CBDH 问题的一个随机实例 $(P,aP,bP,cP)\in G_1$，$\mathcal{C}$ 的目标是计算 $e(P,P)^{abc}=e(P,Q)^{ab}$，其中 $Q=cP$。$\mathcal{C}$ 将 $\mathcal{A}$ 作为子程序，并在定义 1 的游戏中扮演 $\mathcal{A}$ 的挑战者。为便于描述，假设对于任意身份 ID，$\mathcal{A}$ 进行至多一次 H_0 询问和密钥提取询问，并且在将 ID 用于其它任何询问前已经询问了 $H_0(ID)$。在该游戏中，$\mathcal{A}$ 向 $\mathcal{C}$ 询问随机预言机 $H_i(i=0,1,2)$，$\mathcal{C}$ 为每个随机预言机维持一个列表 $L_i(i=0,1,2)$ 用于记录其回答，以避免预言机的随机回答间产生碰撞，当预言机对新询问的回答与已有的回答相同时，需要重新生成随机回答，直到无碰撞产生。按如下方式进行游戏：

系统建立：$\mathcal{C}$ 生成系统参数 cp 并将其发送给 $\mathcal{A}$，其中 $P_{pub}=bP$，b 模拟系统主密钥并且对于 $\mathcal{C}$ 是未知的。$\mathcal{A}$ 输出多个目标身份 $ID_1^*,\cdots,ID_n^*$。

询问阶段：$\mathcal{A}$ 向 $\mathcal{C}$ 进行如下的一系列询问。

H_0 询问：对于一个身份 ID_j 的询问 $H_0(ID_j)$，$\mathcal{C}$ 首先检查列表 L_0 中是否存在条目 (ID_j,λ_j,Q_j)，若存在，则返回 Q_j；否则，执行如下操作：

(1)若 $ID_j=ID_i^*(1\leqslant i\leqslant n)$，则随机选择 $\lambda_i^*\in Z_q^*$ 并计算 $Q_j=\lambda_i^*P-Q$；否则，随机选择 $\lambda_j\in Z_q^*$ 并计算 $Q_j=\lambda_jP$；

(2)将条目 (ID_j,λ_j,Q_j) 加入列表 L_0 并返回 Q_j。

H_1 询问：对于一个询问 $H_1(C_j,X_j,Q_{R_j})$，$\mathcal{C}$ 首先检查列表 L_1 中是否存在条目 $(C_j,X_j,Q_{R_j},h_{1_j})$，若存在，则向 $\mathcal{A}$ 返回 h_{1_j}；否则 $\mathcal{C}$ 随机选择 $h_{1_j}\in Z_q^*$ 并将其返回给 $\mathcal{A}$，最后将条目 $(C_j,X_j,Q_{R_j},h_{1_j})$ 添加到列表 L_1 中。

H_2 询问：对于一个询问 $H_2(V_j)$，$\mathcal{C}$ 首先检查列表 L_2 中

是否存在条目(V_j,h_{2_j})，若存在则向$\mathcal{A}$返回h_{2_j}；否则，$\mathcal{C}$随机选择$h_{2_j}\in\{0,1\}^l$并将其返回给$\mathcal{A}$，最后将条目(V_j,h_{2_j})添加到列表L_2中。

密钥提取询问：对于一个身份ID_j($ID_j\neq ID_i^*$，$1\leqslant i\leqslant n$)的密钥提取询问，$\mathcal{C}$在列表L_0中查找(ID_j,λ_j,Q_j)并向$\mathcal{A}$返回$S_j=\lambda_j P_{pub}$。

签密询问：收到一个对明文m、原签密者身份ID_A、重签密者身份ID_B和n个接收人身份$ID_{R_1},\cdots,ID_{R_n}$的签密询问后，$\mathcal{C}$首先检查$ID_A\neq ID_i^*\wedge ID_B\neq ID_i^*$($1\leqslant i\leqslant n$)是否成立。若成立，则$\mathcal{C}$按正常的签密算法生成一个代理重签名广播签密密文；否则，$\mathcal{C}$随机选取$r',h_1,\lambda_R\in Z_q^*$，计算$X=r'P-h_1P_{pub}$，$W=r'Q_A$，$Q_R=\lambda_R P$，$V=e(X,\lambda_R P_{pub})$，并检查列表$L_2$中是否存在字段值等于所计算$V$值的条目，若存在，则重新选取$(r',h_1,\lambda_R)$直到无碰撞产生。然后，$\mathcal{C}$将新条目添加到相应的列表中，并计算$C=H_2(V)\oplus(ID_A\parallel m)$和$U_i=(\lambda_R+\lambda_{R_i})X(1\leqslant i\leqslant n)$。重签名阶段，计算$W'=r'Q_B$。

解签密询问：当收到$\mathcal{A}$关于签密密文$\sigma'=(X,W',C,Q_R,T_1,\cdots,T_n)$、原签密者身份$ID_A$和重签密者身份$ID_B$的解签密询问$Designcrypt(\sigma',ID_{R_i})$时，$\mathcal{C}$首先检查$ID_{R_i}\neq ID_i^*$($1\leqslant i\leqslant n$)是否成立。若成立，则$\mathcal{C}$查询列表$L_0$得到条目$(ID_{R_i},\lambda_{R_i},Q_{R_i})$，计算$S_{R_i}=\lambda_{R_i}P_{pub}$，利用该私钥即可进行正常的解签密运算；否则，$\mathcal{C}$查询$(ID_B,\lambda_B,Q_B)\in L_0$、$(C,X,Q_R,h_1)\in L_1$和$(V,h_2)\in L_2$，使其满足$e(P,W')=e(X+h_1P_{pub},Q_B)$、$(ID_A\parallel m)=C\oplus h_2$，若存在满足该条件的元组，则向$\mathcal{A}$返回$m$，否则返回$\perp$。

挑战：$\mathcal{A}$输出两个等长明文m_0和m_1、任意的原签密者ID_A和重签密者ID_B的私钥S_A和S_B，向$\mathcal{C}$请求接收人为$ID_1^*,\cdots,ID_n^*$的挑战密文。$\mathcal{C}$随机选择一个比特$b\in\{0,1\}$，按如下方式计算消息m_b的签密密文：$X^*=aP$，$Q_R^*=Q$，$V^*=e(aP_{pub},Q)$，$C^*=H_2(V^*)\oplus(ID_A\parallel m_b)$，$h^*=H_1(C^*,X^*,Q)$，$W^*=h^*S_A+aQ_A$，$W^{*\prime}=h^*S_B+aQ_B$，$U_i^*=\lambda_i^*X^*$，$T_i^*=(ID_i^*,U_i^*)$($1\leqslant i\leqslant n$)。最后，$\mathcal{C}$向$\mathcal{A}$返回挑战密文$\sigma^{*\prime}=(X^*,W^{*\prime},C^*,Q_R^*,T_1^*,\cdots,T_n^*)$。

收到签密密文$\sigma^{*\prime}$后，$\mathcal{A}$可以继续进行上述各类询问，但其不能询问该密文在任何目标身份下的解签密结果，也不能询问与$\sigma^{*\prime}$仅有接收人信息部分不同的密文在某个身份下的解签密结果。最后，$\mathcal{A}$输出一个比特b'作为对b的猜测。此时，$\mathcal{C}$随机选择列表L_2中的一项(V_j,h_{2_j})，输出的V_j作为对CBDH实例的解。

在签密询问中，当$ID_A=ID_i^*\vee ID_B=ID_i^*$($1\leqslant i\leqslant n$)时，令$X=r'P-h_1P_{pub}=(r'-h_1b)P$，因此参数$r=r'-h_1b$；$W=r'Q_A=(r+h_1b)Q_A=h_1S_A+rQ_A$，同理，$W'=r'Q_B=h_1S_B+rQ_B$；$U_i=(\lambda_R+\lambda_{R_i})X=(\lambda_R+\lambda_{R_i})(r'-h_1b)P=r(Q_R+Q_i)$($1\leqslant i\leqslant n$)。因此，对签密的模拟是完美的。

在挑战过程中，令$X^*=aP$，因此参数$r=a$；$W^*=h^*S_A+aQ_A$，$W^{*\prime}=h^*S_B+aQ_B$；$U_i^*=\lambda_i^*X^*=\lambda_i^*aP=a((\lambda_i^*P-Q)+Q)=a(Q_i+Q_R^*)$。因此，对挑战的模拟也是完美的。若$\mathcal{A}$的猜测是正确的，即$b'=b$，则$\mathcal{A}$需要以$V^*=e(aP_{pub},Q)=e(P,P)^{abc}$询问预言机$H_2$，从而列表$L_2$中将添加条目$(V^*,h_2^*)$，$\mathcal{C}$从该条目中可以获得$e(P,P)^{abc}$的值。

在上述整个模拟过程中，若模拟是完美的，则得到一个CBDH实例的解$V^*=e(aP_{pub},Q)=e(P,P)^{abc}$的概率与实际情况是相同的，而使得该模拟不完美的唯一可能是一个有效的密文在解签密询问中被丢弃。对于列表L_2中的每一项(V_j,h_{2_j})，在预言机H_1的值域内存在唯一的h_{1_j}能提供一个有效的密文。因而，一个有效的密文在解签密询问中被丢弃的概率不大于$q_{H_2}/2^k$。而在整个模拟过程中，敌手$\mathcal{A}$进行了q_{De}次解签密询问，并且对于每次挑战，$\mathcal{C}$从列表L_2中随机选择一项作为对CBDH实例的解，因此$Adv_{\mathcal{C}}^{CBDH}\geqslant(\varepsilon-q_{H_2}q_{De}/2^k)/q_{H_2}$。

5.3 不可伪造性

定理2 在随机预言机模型下，若存在一个伪造者$\mathcal{F}$，其经过至多q_{H_0}次H_0询问、q_{H_1}次H_1询问、q_{H_2}次H_2询问、q_{SC}次签密询问和q_{De}次解签密询问后，能以不可忽略的优势$\varepsilon\geqslant 10n(q_{SC}+1)(q_{SC}+q_{H_1})/q+q_{H_2}q_{De}/2^k$攻破IBSPR方案的不可伪造性，则存在一个算法$\mathcal{C}$，其能以优势$Adv_{\mathcal{C}}^{DH}\geqslant 1/9$解决CDH问题的一个实例。

给定CDH问题的一个实例$(P,aP,bP)\in G_1$，$\mathcal{C}$的目标是计算abP。直接证明算法$\mathcal{C}$利用伪造者$\mathcal{F}$解决该CDH实例比较困难，为此先给出一个定义2的变体游戏。在该变体游戏的开始，伪造者必须首先对输出的某个目标身份进行承诺。在游戏的“伪造”步骤中，若伪造的密文对于承诺的身份(作为重签密者)不是有效的密文，则伪造者不能赢得该游戏。根据该变体游戏的定义，得到以下引理。

引理1 在随机预言机模型下，若存在一个伪造者$\mathcal{F}$，其经过至多q_{H_0}次H_0询问、q_{H_1}次H_1询问、q_{H_2}次H_2询问、q_{SC}次签密询问和q_{De}次解签密询问后，能以不可忽略的优势赢得定义2的游戏，则存在另一个伪造者$\mathcal{F}'$，其能以优势$\varepsilon'\geqslant(\varepsilon-q_{H_2}q_{De}/2^k)/n$赢得上述变体游戏。

从而，对定理2的证明只需要考虑伪造者$\mathcal{F}'$对变体游戏的攻击。在IBSPR方案中，当重签密者和接收人的身份固定时，$\mathcal{F}'$可以看作是对非基于身份的代理重签名签密方案的攻击者。利用机密性证明中对各类询问的模拟，并结合分叉引理[11]，可以得到如下的引理。

引理2 若存在一个伪造者$\mathcal{F}'$，其经过至多q_{H_0}次H_0询问、q_{H_1}次H_1询问、q_{H_2}次H_2询问、q_{SC}次签密询问后，能以优势$\varepsilon'\geqslant 10(q_{SC}+1)(q_{SC}+q_{H_1})/q$赢得上述变体游戏，则存在一个算法$\mathcal{C}$，其能以$Adv_{\mathcal{C}}^{DH}\geqslant 1/9$的优势解决CDH问题的一个实例。

在引理2中，由于$\mathcal{F}'$的目标是伪造一个有效的签密密文，因此不需要进行解签密询问。由引理1和引理2，可以证明定理2的正确性。

5.4 公开可验证性

任何第三方在获得系统公开参数cp、重签密者公钥Q_B和密文$\sigma'=(X,W',C,Q_R,T_1,\cdots,T_n)$后，都能通过验证等式$e(P,W')=e(X+h''P_{pub},Q_B)$是否成立来判断该密文的重签密者是否为指定的签密者，其中$h''=H_1(C,X,Q_R)$。在验证过程中，验证者不能获得有关密文以及签密和接收者的更多信息。

6 应用实例

云计算的存储和共享服务为用户组共享数据和协同计算提供了便利的方法。数据所有者可以将数据存储在云服务器上，并创建一个用户组，允许对自身数据具有访问权限的其他用户加入该组，并为不同的用户赋予不同的访问权限，从而使组内的所有用户能共享组数据并允许具有写权限的用户对相

应数据进行更新。在该共享服务中，需要对数据进行机密性和完整性保护，并对其实施访问控制。针对这些安全性需求，文献[12]提出了一种综合了远程数据完整性检查、用户延迟撤销、密钥轮换和广播加密等技术的安全性保障方案，但其不能支持除所有者外的其他组用户对数据的更新，并该方案由于是对多种技术的综合，因此较复杂。文献[13]提出了一种支持用户撤销的共享数据审计方案，其通过采用代理重签名技术，将被撤销用户对数据的签名转换为其他用户的签名，从而使组内的未撤销用户仍可以访问和验证数据。但该方案不能对数据实施机密性保护和访问控制，并且服务器需要保存大量的重签名密钥(当组用户数为 n 时，重签名密钥数为 $n(n+1)$)。采用基于身份的代理重签名广播签密技术，可以为数据共享服务提供更好的安全性方案，其总体架构如图 1 所示。

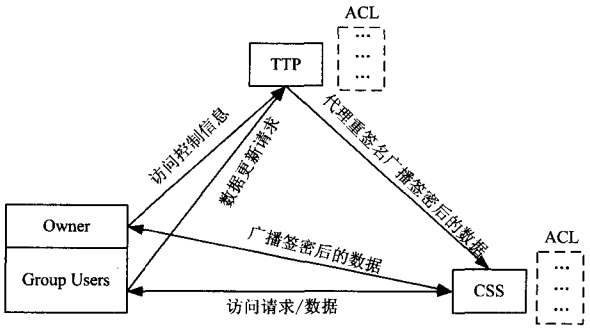

图 1　应用实例架构

该方案的主要工作原理为：Owner 以其自身和组用户为接收人对数据进行广播签密后，将结果存储到云存储服务器(Cloud Storage Server，CSS)上，并将组用户对数据的访问控制信息(主要包括用户 ID 和访问权限)分别发送给 CSS 和可信第三方(Trusted Third Party，TTP)，CSS 和 TTP 根据收到的访问控制信息维护一张访问控制列表(Access Control List，ACL)。当组用户向 CSS 提交数据访问请求时，CSS 首先检查该用户是否具有相应的访问权限，若通过检查，则向其返回相应的数据(包含该用户信息的签密密文 $\sigma'=(X,W',C,Q_R,T_i)$)；否则，拒绝该数据访问请求。当数据访问请求为“更新”时，CSS 还需要将对被请求数据具有访问权限的组用户的信息返回给数据请求者。当组用户需要对数据执行更新时，需要首先对更新后的数据进行广播签密，并将更新请求和签密密文提交给 TTP。TTP 检查该用户是否具有相应的“写”权限，若通过检查，则对密文进行代理重签名，将其转换为重签名者为 Owner 的代理重签名广播签密密文，并将结果提交给 CSS 存储；否则，拒绝该数据更新请求。

该方案主要具有以下特点：

(1)通过签密为数据提供了机密性和完整性保护。

(2)实现了对数据的访问控制，可以为各组用户授予不同的访问权限。

(3)支持对组用户的撤销：申请离开或被撤销的用户可以利用自己的私钥解签密以前具有访问权限的数据，这等价于从本地存储设备中访问以前具有访问权限的数据，但其不能解签密新的数据。

(4)支持组用户对数据的更新。

(5)TTP 作为重签名代理只需要保存少量的重签名密钥(当组用户数为 n 时，重签名密钥数也为 n)。

结束语　本文设计了一种基于身份的代理重签名广播签密方案，其特点为：只需要代理进行一次重签名运算，即可将原签密者的一个广播签密转换为重签密者的广播签密；具有公开可验证性，任何第三方在获得系统公开参数和重签密者公钥的情况下都可以验证签密的正确性；在随机预言机模型下是可证安全的。应用实例分析表明，该基于身份的代理重签名广播签密方案对于云计算组数据共享等应用具有良好的适用性。下一步将研究标准模型下可证安全的基于身份的代理重签名广播签密方案。

参 考 文 献

[1] 俞惠芳，王彩芬，王之仓. 基于 ECC 的自认证代理签密方案[J]. 计算机科学，2010，37(7)：91-92，101

[2] Zuo Wei-ping. An ID-Based Proxy Multi-signcryption Scheme from Pairings[C]// Proceedings of 2010 International Conference on Multimedia Information Networking and Security. Washington，DC，USA：IEEE Computer Society，2010：403-405

[3] Li Fa-gen，Yu Yong. An Efficient and Provably Secure ID-Based Threshold Signcryption Scheme[C]// Proceedings of 2008 International Conference on Communications，Circuits and Systems. Berlin：Springer-Verlag，2008：488-492

[4] 柏骏，张申绒，崔晓臣. 基于多接收者签密算法的门限密钥更新协议[J]. 计算机应用，2011，31(2)：507-510

[5] Kirtane V，Rangan C P. RSA-TBOS Signcryption with Proxy Re-encryption[C]// Proceedings of the 8th ACM Workshop on Digital Rights Management. NewYork，NY，USA：ACM，2008：59-66

[6] Chandrasekar S，Ambika K，Rangan P C. Signcryption with Proxy Re-encryption[EB/OL]. http://eprint. iacr. org/2008/276，2011-10-05

[7] Wang Cai-fen，Cao Xiao-jun. An Improved Signcryption with Proxy Re-encryption and Its Application[C]// Proceedings of 7th International Conference on Computational Intelligence and Security. Washington，DC，USA：IEEE Computer Society，2011：886-890

[8] 王会歌，王彩芬，曹浩，等. 新的基于身份的代理重签密[J]. 计算机应用，2011，31(11)：2986-2989

[9] Wang Hui-ge，Wang Cai-fen，Cao Hao. ID-Based Proxy Re-signcryption Scheme[C]// Proceedings of 2011 IEEE International Conference on Computer Science and Automation Engineering. Washington，DC，USA：IEEE Computer Society，2011：317-321

[10] Duan Shan-shan，Cao Zhen-fu. Efficient and provably secure multi-receiver identity-based signcryption[C]// Proceedings of the 11th Australasian Conference on Information Security and Privacy. Berlin：Springer-Verlag，2006：195-206

[11] Pointcheval D，Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology，2000，13(3)：361-396

[12] Barsoum A F，Hasan M A. Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems[EB/OL]. http://cacr. uwaterloo. ca/techreports/2012/cacr2012- 05. pdf，2012-03-10

[13] Wang Bo-yang，Li Bao-chun，Li Hui. Public Auditing for Shared Data with Efficient User Revocation in the Cloud[EB/OL]. http://ste. xidian. edu. cn/ lihui/cloud12. pdf，2012-05-03