doi:10.3969/j.issn.1000-436x.2014.05.005

支持用户撤销的属性认证密钥协商协议

李强，冯登国，张立武
(中国科学院 软件研究所 可信计算与信息保障实验室，北京 100190)

摘 要：用户撤销是基于属性的认证密钥协商(ABAKA, attribute-based authenticated key agreement)协议在实际应用中所必需解决的问题。通过将 Waters 的基于属性的加密方案和 Boneh-Gentry-Waters 的广播加密方案相结合，提出了一个支持用户撤销的 ABAKA 协议。该协议能够实现对用户的即时撤销且不需要密钥权威对所有未被撤销的用户私钥进行定期更新。相比于现有的协议，该协议具有较高的通信效率，并能够在标准模型和修改的 ABCK 模型下可证安全，具有弱的完美前向安全性，并能够抵抗密钥泄露伪装攻击。

关键词：认证；密钥协商；基于属性；密钥撤销；标准模型
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)05-0033-11

Attribute-based authenticated key agreement protocol supporting revocation

LI Qiang, FENG Deng-guo, ZHANG Li-wu
(TCA, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: Revocation is a crucial issue for the practical use of attribute-based authenticated key agreement (ABAKA) protocols. A new ABAKA protocol supporting revocation was proposed. The protocol based on Waters' ciphertext-policy attribute-based encryption and Boneh-Gentry-Waters' broadcast encryption was constructed. In the protocol, revocation can be done immediately without affecting any non-revoked users and does not require users to update keys periodically by interacting with the key authority. Compared with the existing ABAKA protocols, the protocol is more efficient in communication complexity. The protocol is provably secure in the standard model and modified ABCK model. The protocol can also provide weak perfect forward secrecy and key compromise impersonation resilience.

Key words: authentication; key agreement; attribute-based; key revocation; standard model

1 引言

认证密钥协商协议是构建安全网络环境的基础，通过认证密钥协商协议，在通信系统中为通信的参与者提供身份认证，为身份已经确认的参与方之间建立共享密钥，用来加密传递的消息。传统的基于公钥的认证协议都是对用户身份实现认证，而在分布式尤其是云计算环境中应用服务只需要验证用户是否拥有获取服务的资格即可，基于公钥的认证方式向应用服务泄露了过多的用户信息，从而损害了用户隐私。自 2005 年 Sahai 等人[1]首次提出基于属性的加密方案以来，由于天然的隐私保护优势以及灵活的访问控制策略，大量的基于属性的加密方案[2~4]、签名方案[5,6]以及安全协议[7~12]相继被提出。

2009 年，Wang 等人[7]提出了第一个随机预言机(RO, random oracle)模型下基于属性的两方认证密钥协商协议。由于该协议只能在 RO 模型下可证

收稿日期：2013-03-15；**修回日期**：2013-07-08
基金项目：国家重点基础研究发展计划(“973”计划)基金资助项目(2013CB338003)；国家高技术研究发展计划(“863”计划)基金资助项目(2012AA01A403)；国家自然科学基金资助项目(91118006)
Foundation Items: The National Basic Research Program of China (973 Program) (2013CB338003); The National High Technology Research and Development Program of China (863 Program) (2012AA01A403); The National Natural Science Foundation of China (91118006)

安全，Wang 等人[8]提出了另一个标准模型下的基于属性的两方认证密钥协商协议，接下来 Wang 等人[9]又在该协议的基础上加入了可撤销机制。然而上述方案只是把用户属性看作进行认证的一种身份串，即认证策略为用户拥有消息中所有的属性，因此并没有实现灵活的认证策略，此外上述方案都是在 BR(bellare-rogaway)模型下证明协议的安全性。2010 年，Yoneyama 等人[10]在 Waters[4]的加密方案基础上提出了一个 1 轮的 RO 模型下基于属性的两方认证密钥协商协议，该协议支持通用认证策略(与、或、门限)，并在 eCK(extended canetti-krawczyk)模型下可证安全。Birkett 等人[11]提出了第一个标准模型下支持通用认证策略的基于属性的两方认证密钥协商协议，该协议使用了基于谓词的签名方案，若所使用的签名方案支持通用认证策略，则该协议也支持同样的策略，但该协议需要运行 3 轮且安全性证明是在 BR 模型中进行的。2011 年，Yoneyama[12]在 Waters[4]的加密方案基础上又提出了一个 1 轮的标准模型下基于属性的两方认证密钥协商协议，该协议支持通用的认证策略，并在 CK 模型下可证安全。但是该协议采用了 Boneh 等人[13]方案中的一次性签名的转化方法将只能抵抗选择明文攻击(CPA)的加密方案转化为能够抵抗选择密文攻击(CCA)的密钥封装方案，该方法将一次性签名的验证密钥比特串的每一位(0 或 1)映射为 2 个冗余属性，从而导致协议通信量和系统的公共参数都增加了 $2k$ 个群元素，其中 k 为一次性签名方案中验证密钥的比特串长度，因此这种转化方法增加了协议的复杂度。

在实际的应用中，经常会出现用户离职、私钥丢失、甚至用户恶意泄露私钥等情况，因此对用户私钥进行撤销是实际应用中必须解决的问题，也是基于属性的密码研究的一个难点[14]。传统的基于 PKI 的系统中，可以通过证书撤销列表来对用户证书进行撤销，然而在基于属性的认证密钥协商协议中，由于使用属性来描述用户身份，每个属性被多个用户共享，因此对用户私钥的撤销会影响其他用户的私钥。Attrapadung 等人[15,16]将属性加密中的撤销分为间接撤销和直接撤销两类，在间接撤销模式下，由密钥权威周期性地对用户私钥进行更新，只有未被撤销的用户才能更新私钥；在直接撤销模式下，发送者将用户撤销列表嵌入到密文中，只有不在撤销列表中的用户才能正确解密。Wang 等人[9]的基于属性的认证密钥协商协议采用了间接撤销模式，即需要密钥权威对用户私钥进行定期更新，因此不能实现对用户的即时撤销。该方案对用户属性进行撤销，因此撤销一个用户的私钥也会影响到其他用户，相当于对整个系统属性进行撤销。在密钥更新阶段，密钥权威需要对所有未被撤销用户进行密钥更新，工作量较大，容易成为系统瓶颈。此外，该方案没有实现灵活的通用认证策略，且只能在 BR 模型下证明协议安全性。

本文针对已有的属性认证密钥协商协议的不足，提出了一个标准模型下支持用户撤销的属性认证密钥协商协议。该协议采用直接撤销模式，将用户标识嵌入在用户私钥中并在通信消息密文中嵌入用户撤销列表，若用户被撤销，则无法实现认证。该协议能够实现对用户的即时撤销，且不需要密钥权威对所有未被撤销用户私钥进行定期更新，撤销代价较小。本文借鉴了 Lai 等人[17]基于身份的加密方案中提出的一个简洁高效的从 CPA 到 CCA 的转化方法，并将其应用于基于属性的认证协议中，提高了协议通信效率。本文所提协议支持通用认证策略，并能够在标准模型和修改的 ABCK 模型下可证安全，具有弱的完美前向安全性，并能够抵抗密钥泄露伪装攻击。

2 预备知识

2.1 访问结构

定义 1[18] 令 $P=\{P_1,P_2,\cdots,P_n\}$ 是参与方的集合，一个访问结构 $\mathbb{A}$ 是 2^P 的一个非空子集，即 $\mathbb{A}\subseteq 2^P\setminus\{\varnothing\}$。若访问结构 $\mathbb{A}$ 是单调的，则有 $\forall B,C$，若 $B\in\mathbb{A}$ 且 $B\subseteq C$，则有 $C\in\mathbb{A}$。访问结构 $\mathbb{A}$ 中的集合称为授权集合，不在访问结构 $\mathbb{A}$ 中的集合称为非授权集合。

2.2 线性秘密分享方案

定义 2[18] 令 $P=\{P_1,P_2,\cdots,P_n\}$ 是参与方的集合，$(\boldsymbol{M},\rho)$ 代表着一个访问结构 $\mathbb{A}$，其中，$\boldsymbol{M}$ 是一个 $l\times n$ 的矩阵，ρ 是一个从 $\{1,2,\cdots,l\}$ 到 P 的映射，即将矩阵 $\boldsymbol{M}$ 中的每一行映射到一个参与方。一个线性秘密分享方案(LSSS, linear secret sharing schemes)包含 2 个有效的算法。

秘密分享算法。若要分享一个秘密值 s，首先随机选取 $n-1$ 个值 $v_1,v_2,\cdots,v_{n-1}\in\mathbb{Z}_p$ 和 s 组成一个 n 维的向量 $\vec{v}=(s,v_1,v_2,\cdots,v_{n-1})^{\mathrm{T}}$。令 $\overrightarrow{M_i}$ 为矩阵第 i

行所代表的向量，然后将 $\lambda_i = \overrightarrow{M_i}\vec{v}$ 作为参与方 $\rho(i)$ 所获得的秘密分享值。

秘密恢复算法。对一个授权集合即参与方的集合 $S \in \mathbb{A}$，令 $I = \{i : \rho(i) \in S\}$，则可以根据 $\boldsymbol{M}$ 有效的计算出一组恢复系数 $\{\mu_i\}_{i\in I}$，使得 $\sum_{i\in I}\mu_i \cdot \overrightarrow{M_i} = (1,0,\cdots,0)$，从而可以计算 $\sum_{i\in I}\mu_i\lambda_i = \sum_{i\in I}\mu_i\overrightarrow{M_i}\vec{v} = s$。而对非授权集合 I，则存在一个向量 $\vec{\omega} = (\omega_1,\omega_2,\cdots,\omega_n)^{\mathrm{T}} \in \mathbb{Z}_p{}^n$ 使得 $\omega_1 = -1$，且对 $i \in I$，有 $\overrightarrow{M_i}\vec{\omega} = 0$。

2.3　双线性映射

定义 3　设 G, G_T 是 2 个阶均为 p 的循环群(p 为素数)，g 为 G 的一个生成元，双线性映射 e 是 $G\times G \to G_T$ 的一个映射，若 e 满足以下 3 个性质，则称 e 是一个有效的从 G 到 G_T 的双线性映射。

1) 双线性: $\forall a,b \in \mathbb{Z}_p, e(g^a, g^b) = e(g,g)^{ab}$。

2) 非退化性: $e(g,g) \neq 1$。

3) 可计算性:对 $\forall x, y \in G$，存在一个有效的多项式时间算法来计算 $e(x,y)$。

2.4　DPBDHE 假设

定义 4[4]　设 G, G_T 是 2 个阶均为 p 的循环群(p 为素数)，g 为 G 的一个生成元，e 是 $G\times G \to G_T$ 的一个双线性映射，随机选择 $a, s, b_1, b_2, \cdots, b_n \in \mathbb{Z}_p$，并给定以下元组

$$g^s, g^a, \cdots, g^{a^n}, g^{a^{n+2}}, \cdots, g^{a^{2n}}$$

$$\forall 1 \leqslant j \leqslant n \quad g^{sb_j}, g^{a/b_j}, \cdots, g^{a^n/b_j}, g^{a^{n+2}/b_j}, \cdots, g^{a^{2n}/b_j}$$

$$\forall 1 \leqslant j,k \leqslant n, j \neq k \quad g^{asb_k/b_j}, \cdots, g^{a^n sb_k/b_j}$$

若不存在一个算法，能够在多项式时间内以不可忽略的概率区分 $e(g,g)^{sa^{n+1}}$ 和群 G_T 中的随机元素，则称 DPBDHE(decisional parallel bilinear diffie-hellman exponent)假设成立。

2.5　强随机提取器

定义 5[12]　称一个函数 $Ext : \{0,1\}^d \times \{0,1\}^n \to \{0,1\}^m$ 是强随机提取器，若对于任意的 $\{0,1\}^n$ 上且最小熵 $H_\infty(X) \geqslant k$ 的均匀分布 X，$Ext(s,X)$ 和 $\{0,1\}^m$ 上的随机串统计上不可区分，其中 s 是在种子空间 $\{0,1\}^d$ 上随机选择的种子。

2.6　伪随机函数集

定义 6[12]　称一个函数集 $F = \{F_s\}_{s\in K}$ 是伪随机的，若不存在一个区分者 $\mathcal{D}$，能够在多项式时间内以不可忽略的概率区分 $F_k(\cdot)$ 和 $RF(\cdot)$，其中，k 是在密钥空间 K 中随机选择的密钥，RF 是一个随机选择的真随机函数。

3　安全模型

在本文中，对文献[12]中定义的 ABCK 模型进行了修改，使之能够适应支持用户撤销的属性认证密钥协商协议的安全性分析。该模型能够证明协议满足弱的完美前向安全性(wPFS)并能抵抗密钥泄露伪装攻击(KCI)。

前向安全性(FS, forward secrecy)：如果协议参与者的长期私钥被敌手获得，而敌手不能由此计算出参与者在私钥泄露前协商获得的会话密钥，则称该协议具有前向安全性。前向安全性可分为完美前向安全性(PFS, perfect forward secrecy)和弱的完美前向安全性(WPFS, weak perfect forward secrecy)。如果长期私钥泄露前的会话受到了敌手的破坏而敌手仍无法获得这次会话的会话密钥，则称该协议具有完美前向安全性；若协议只能保证敌手在获得参与者的长期私钥后，之前的那些未被敌手破坏的会话的会话密钥不能被敌手获得，则称该协议具有弱的完美前向安全性。

抵抗密钥泄露伪装攻击(KCI, key compromise impersonation resilience)：如果敌手得到了一个协议参与者 A 的长期私钥，则毫无疑问敌手可以伪装成 A 与其他用户执行协议，但是不能使攻击者伪装成其他用户与 A 成功完成协议。

协议实体。每一个协议实体 U 都被视为概率多项式时间的图灵机，具有属性集 S_U，并且每个实体可以并行地执行多个会话实例。若一个由 A 发起的与 B 之间的会话产生了消息 $m_1, m_2, \cdots, m_n$，则该会话 ID 被 A 标识为 $sid = (I, S_A, S_B, m_1, \cdots, m_n)$，被 B 标识为 $sid = (R, S_B, S_A, m_1, \cdots, m_n)$。一个会话是完成的，是指通信双方在会话中计算出了一个会话密钥。而一个完成会话 $(I, S_A, S_B, m_1, \cdots, m_n)$ 的匹配会话是 $(R, S_B, S_A, m_1, \cdots, m_n)$；反之亦然。

攻击者模型。攻击者 $\mathcal{A}$ 被视为控制了协议实体间所有通信的概率多项式时间的图灵机。攻击者可以执行以下询问。

1) $Send(m)$：攻击者通过发送如下形式的消息激活会话：$(I, S_A, S_B, m_1, \cdots, m_k)$ 或者 $(R, S_B, S_A, m_1, \cdots, m_{k+1})$，并得到相应的输出消息。

2) $Key\,\mathrm{Re}veal(sid)$：若会话 sid 已完成，则返回攻击者会话密钥，否则返回终止符号 $\perp$。

3) $State\text{Re}veal(sid)$：若会话 sid 未完成，则返回攻击者该会话的内部状态，包括选取的随机数以及中间的计算结果，但是不包括该会话的私钥；若会话 sid 已完成，则返回终止符号 $\perp$。

4) $Corrupt(U,S_U)$：该询问允许攻击者获取实体 U 的属性集 S_U 所对应的私钥，并能完全控制该实体的行为。若攻击者对实体 U 执行了该询问，则实体 U 被称为不诚实实体，否则称其为诚实实体。

定义 7（新鲜性）：记 $sid^*=(I,S_A,S_B,m_1,\cdots,m_n)$ 或者 $(R,S_B,S_A,m_1,\cdots,m_n)$ 是一个具有属性集 S_A 的诚实实体 A 和具有属性集 S_B 的诚实实体 B 之间的已完成会话，若 sid^* 存在匹配会话，记作 $\overline{sid^*}$。会话 sid^* 是新鲜的，是指下面的条件都不成立。

1) 攻击者执行了询问 $Key\text{Re}veal(sid^*)$，或者在 $\overline{sid^*}$ 存在的情况下执行了询问 $Key\text{Re}veal(\overline{sid^*})$。

2) $\overline{sid^*}$ 存在，攻击者执行了询问 $State\text{Re}veal(sid^*)$ 或者 $State\text{Re}veal(\overline{sid^*})$。

3) $\overline{sid^*}$ 不存在，攻击者执行了询问 $State\ \text{Re}veal(sid^*)$。

安全性游戏。初始时刻，攻击者 $\mathcal{A}$ 得到一个诚实协议实体集合，并可以执行任何上述询问。在游戏过程中，攻击者执行下述询问。

$Test(sid^*)$：其中，sid^* 是一个新鲜会话。通过公平的掷币协议选择 $b\in\{0,1\}$，若 $b=0$，则返回攻击者会话 sid^* 的会话密钥，否则返回一个在密钥空间里随机选择的串。

游戏继续进行，直到攻击者 $\mathcal{A}$ 输出一个对 b 的猜测 b'，若 $b=b'$ 且会话 sid^* 仍然是新鲜的，则称攻击者赢得了该攻击游戏，定义攻击者 $\mathcal{A}$ 在上述游戏中的优势为

$$Adv_{\Pi}^{ABAKA}(\mathcal{A})=\left|\Pr[\mathcal{A}\ wins]-\frac{1}{2}\right|$$

定义 8（ABCK 安全性）：一个支持用户撤销的 ABAKA 协议 Π 在 ABCK 模型下是安全的，是指下面的条件同时成立。

1) 若 2 个诚实的协议实体 A 和 B 完成了匹配会话，A 和 B 均不在系统的撤销列表中且双方属性均满足对方指定的访问结构即 $S_A\in\mathbb{A}_B$ 且 $S_B\in\mathbb{A}_A$，则除了一个可忽略概率，协议双方计算出相同的会话密钥。

2) 对任何一个概率多项式时间的攻击者 $\mathcal{A}$，若 $\overline{sid^*}$ 存在且攻击者获得系统主密钥，则 $Adv_{\Pi}^{ABAKA}(\mathcal{A})$ 是可忽略的。

3) 对任何一个概率多项式时间的攻击者 $\mathcal{A}$，若 $\overline{sid^*}$ 不存在，令 A 为 sid^* 会话的拥有者则攻击者获得 A 的私钥，且 $Adv_{\Pi}^{ABAKA}(\mathcal{A})$ 在下列情况下是可忽略的。

a) 若协议实体 B 在系统撤销列表中，则攻击者可以获得 B 的私钥。

b) 若协议实体 B 不在系统撤销列表中且实体 B 的属性不满足测试会话中 A 指定的访问结构即 $S_B\notin\mathbb{A}_A^*$，则攻击者可以获得 B 的私钥。

其中，条件 2)能够证明协议满足 wPFS，条件 3)能够证明协议抵抗 KCI 攻击。而 ABAKA 协议 Π 在修改的 ABCK 模型下是选择安全的，是指攻击者 $\mathcal{A}$ 在安全游戏初始阶段预先选择要挑战的系统用户撤销列表以及 sid^* 对应的访问结构和 $\overline{sid^*}$ 对应的访问结构(若 $\overline{sid^*}$ 存在)。

4 协议构造

4.1 基本思想

本文的协议结合了 Waters[4]的属性加密方案和 Boneh 等人[19]的广播加密方案，将用户身份标识嵌入到私钥并与用户属性绑定，然后将系统用户撤销列表嵌入到通信消息密文，若用户身份在撤销列表中，即使其拥有的属性满足对方指定的认证策略也无法完成认证，从而能够实现对用户私钥权限的即时撤销，且不影响其他用户的私钥。本文借鉴了 Lai 等人[17]基于身份的加密方案中提出的一个简洁高效的从 CPA 到 CCA 的转化方法，并将其应用于基于属性的认证协议中。相比于现有的基于属性的认证密钥协商协议，本文所提协议在增加了撤销功能的同时也提高了协议通信效率。

4.2 具体实现

系统建立。选择阶为大素数 p 的群 G,G_T，记 g 为 G 的一个生成元，$e:G\times G\to G_T$ 是双线性映射。系统选择一个抗碰撞散列函数 $H:\{0,1\}^*\to\mathbb{Z}_p$，一个伪随机函数 F 和一个强随机提取器 $Ext(s,\cdot)$，其中 s 是在种子空间随机选择的种子。令系统中用户集合为 U，用户数为 n。系统维护一个公开的用户撤销列表 R，若用户私钥被撤销则将该用户身份标识 ID 加入该撤销列表中，令 W 表示未被撤销用户集合即 $W=U-R$。令系统中属性个数为 m，随机

选择 $\alpha,\gamma\in\mathbb{Z}_p$，对任意的 $i=1,2,\cdots,n,n+2,\cdots,2n$，计算 $g_i=g^{\alpha^i}$，并计算 $v=g^{\gamma}$，随机选择 $h_1,\cdots,h_m,w,\delta_1,\delta_2,\delta_3\in G$。系统的主密钥为 $MSK=(\alpha,\gamma)$，公开参数为

$$PK=(g_1\cdots g_n,g_{n+2}\cdots g_{2n},h_1\cdots h_m,v,w,\delta_1,\delta_2,\delta_3)$$

用户私钥抽取。该过程为身份标识为 ID 和属性集合为 S_{ID} 的用户产生私钥。系统随机选择 $r\in\mathbb{Z}_p$，对任意 $\forall x\in S_{ID}$，计算: $K_{ID_x,3}=h_x^r$，并计算 $K_{ID,1}=g^{\alpha^{ID}\gamma+\alpha r},K_{ID,2}=g^r$。最终计算用户私钥 $SK_{ID}=(K_{ID,1},K_{ID,2},\{K_{ID_x,3}\}_{x\in S_{ID}})$。

密钥交换。假设协议的参与方为 A 和 B，其中 A 的属性集合为 S_A，私钥为 SK_A，B 的属性集合为 S_B，私钥为 SK_B。A 和 B 分别指定访问结构 $\mathbb{A}_A$ 和 $\mathbb{A}_B$，并分别发送消息 mem_A 和 mem_B 给对方，若双方身份标识均不在系统撤销列表中即 $A,B\notin R$ 且双方属性均满足对方指定的访问结构即 $S_A\in\mathbb{A}_B$，$S_B\in\mathbb{A}_A$，则 A 和 B 都能计算出共同的会话密钥 K_{AB}，具体过程如下。

1) A 指定对方需要满足的访问结构 $\mathbb{A}_A$，其对应访问控制矩阵为 $((M_A)_{l_A\times n_A},\rho_A)$。$A$ 随机选取向量 $\overrightarrow{s_A}=(x_A,s_{A,2},\cdots,s_{A,n_A})^{\mathrm{T}}\in\mathbb{Z}_p^{n_A}$，并计算分享向量 $(\lambda_{A,1},\lambda_{A,2},\cdots,\lambda_{A,l_A})^{\mathrm{T}}=M_A\overrightarrow{s_A}$，然后 A 随机选取 $d_A,y_A,t_{A,1},t_{A,2},\cdots,t_{A,l_A}\in\mathbb{Z}_p$，计算 $C_{A,1}=g^{x_A},C_{A,2}=(v\prod_{j\in W}g_{n+1-j})^{x_A},C_{A,3}=g^{y_A}$，对 $\forall i\in\{1\cdots l_A\}$，计算 $C_{A_i,1}=g^{\alpha\lambda_{A,i}}h_{\rho_A(i)}^{-t_{A,i}},C_{A_i,2}=g^{t_{A,i}}$ 最后计算 $C_{A,4}=(\delta_1^{c_A}\delta_2^{d_A}\delta_3)^{x_A}$，其中，$c_A=H(M_A,C_{A,1},C_{A,2},C_{A,3},\{C_{A_i,1},C_{A_i,2}\}_{i\in\{1\ldots l_A\}})$，最后 A 发送给 B 消息为

$$mem_A=((M_A,\rho_A),C_{A,1},C_{A,2},C_{A,3},C_{A,4},\{C_{A_i,1},C_{A_i,2}\}_{i\in\{1\cdots l_A\}},d_A)$$

2) B 指定对方需要满足的访问结构 $\mathbb{A}_B$，其对应的访问控制矩阵为 $((M_B)_{l_B\times n_B},\rho_B)$。$B$ 随机选取 $\overrightarrow{s_B}=(x_B,s_{B,2},\cdots,s_{B,n_B})^{\mathrm{T}}\in\mathbb{Z}_p^{n_B}$，并计算分享向量 $(\lambda_{B,1},\lambda_{B,2},\cdots,\lambda_{B,l_B})^{\mathrm{T}}=M_B\overrightarrow{s_B}$，然后 B 随机选取 $d_B,y_B,t_{B,1},t_{B,2},\cdots,t_{B,l_B}\in\mathbb{Z}_p$，并计算 $C_{B,1}=g^{x_B},C_{B,2}=(v\prod_{j\in W}g_{n+1-j})^{x_B},C_{B,3}=g^{y_B}$，对 $\forall i\in\{1\cdots l_B\}$，计算 $C_{B_i,1}=g^{\alpha\lambda_{B,i}}h_{\rho_B(i)}^{-t_{B,i}},C_{B_i,2}=g^{t_{B,i}}$ 最后计算 $C_{B,4}=(\delta_1^{c_B}\delta_2^{d_B}\delta_3)^{x_B}$，其中 $c_B=H(M_B,C_{B,1},C_{B,2},C_{B,3},\{C_{B_i,1},C_{B_i,2}\}_{i\in\{1\cdots l_B\}})$，最后 B 发送给 A 消息为

$$mem_B=((M_B,\rho_B),C_{B,1},C_{B,2},C_{B,3},C_{B,4},\{C_{B_i,1},C_{B_i,2}\}_{i\in\{1\cdots l_B\}},d_B)$$

3) A 获取消息 mem_B 后，假定 A 不在系统撤销列表中且属性满足 B 指定的访问结构，即 $A\in W$ 且 $S_A\in\mathbb{A}_B$，令 $I_A=\{i:\rho_B(i)\in S_A\}$ 为授权的属性集合，因此 A 可以得到恢复系数 $\{\mu_{A,i}\in\mathbb{Z}_p\}_{i\in I_A}$ 使 $\sum_{i\in I_A}\mu_{A,i}\lambda_{B,i}=x_B$。首先判断 $e(g,C_{B,4})=e(C_{B,1},\delta_1^{c_B}\delta_2^{d_B}\delta_3)$ 是否成立，其中 $c_B=H(M_B,C_{B,1},C_{B,2},C_{B,3},\{C_{B_i,1},C_{B_i,2}\}_{i\in\{1\cdots l_B\}})$ 若上式不成立，则返回 $\perp$。否则 A 计算

$$\sigma_1=e(g_1,g_n)^{x_A},\sigma_3=e(C_{B,3},w)^{y_A}=e(g,w)^{y_Ay_B}$$

$$\sigma_2=\frac{\prod_{i\in I_A,x=\rho_B(i)}(e(K_{A_x,3},C_{B_i,2})e(K_{A,2},C_{B_i,1}))^{\mu_{A,i}}}{e(K_{A,1},C_{B,1})}\cdot\frac{e(g_A,C_{B,2})}{e(\prod_{j\in W,j\neq A}g_{n+1-j+A},C_{B,1})}=\frac{\prod_{i\in I_A}(e(h_{\rho_B(i)}^r,g^{t_{B,i}})e(g^r,g^{\alpha\lambda_{B,i}}h_{\rho_B(i)}^{-t_{B,i}}))^{\mu_{A,i}}}{e(g^{\alpha^A\gamma+\alpha r},g^{x_B})}\cdot\frac{e(g^{\alpha^A},g^{\gamma x_B})e(g^{\alpha^A},(\prod_{j\in W}g_{n+1-j})^{x_B})}{e(\prod_{j\in W,j\neq A}g_{n+1-j+A},g^{x_B})}=e(g_1,g_n)^{x_B}$$

同理，B 获取消息 mem_A 后，假定 B 不在系统撤销列表中且属性满足 A 指定的访问结构即 $B\in W$ 且 $S_B\in\mathbb{A}_A$，令 $I_B=\{i:\rho_A(i)\in S_B\}$ 为授权属性集合，因此 B 可以得到恢复系数 $\{\mu_{B,i}\in\mathbb{Z}_p\}_{i\in I_B}$ 使 $\sum_{i\in I_B}\mu_{B,i}\lambda_{A,i}=x_A$，首先判断 $e(g,C_{A,4})=e(C_{A,1},\delta_1^{c_A}\delta_2^{d_A}\delta_3)$ 是否成立，其中，$c_A=H(M_A,C_{A,1},C_{A,2},C_{A,3},\{C_{A_i,1},C_{A_i,2}\}_{i\in\{1\ldots l_A\}})$ 若上式不成立，则返回 $\perp$。否则 B 计算：

$$\sigma_2=e(g_1,g_n)^{x_B},\sigma_3=e(C_{A,3},w)^{y_B}=e(g,w)^{y_Ay_B}$$

$$\sigma_1=\frac{\prod_{i\in I_B,x=\rho_A(i)}(e(K_{B_x,3},C_{A_i,2})e(K_{B,2},C_{A_i,1}))^{\mu_{B,i}}}{e(K_{B,1},C_{A,1})}\cdot\frac{e(g_B,C_{A,2})}{e(\prod_{j\in W,j\neq B}g_{n+1-j+B},C_{A,1})}=\frac{\prod_{i\in I_B}(e(h_{\rho_A(i)}^r,g^{t_{A,i}})e(g^r,g^{\alpha\lambda_{A,i}}h_{\rho_A(i)}^{-t_{A,i}}))^{\mu_{B,i}}}{e(g^{\alpha^B\gamma+\alpha r},g^{x_A})}\cdot$$

$$\frac{e(g^{\alpha^B},g^{\gamma x_A})e(g^{\alpha^B},(\prod_{j\in W}g_{n+1-j})^{x_A})}{e(\prod_{j\in W,j\neq B}g_{n+1-j+B},g^{x_A})}$$
$$=e(g_1,g_n)^{x_A}$$

A 和 B 计算出相同的 $\sigma_1,\sigma_2,\sigma_3$ 后，通过随机提取器计算

$$\sigma'_1=Ext(s,\sigma_1),\sigma'_2=Ext(s,\sigma_2),\sigma'_3=Ext(s,\sigma_3)$$

令会话 ID 为 $sid=(mem_A,mem_B)$，最后双方计算共同的会话密钥为

$$K_{AB}=F_{\sigma'_1}(sid)\oplus F_{\sigma'_2}(sid)\oplus F_{\sigma'_3}(sid)$$

5 协议安全性与性能分析

5.1 安全性证明

定理 1 若定义 4 中的 DPBDHE 假设成立，且 F 是一个伪随机函数，$Ext(s,\cdot)$ 是一个强随机提取器，则上述协议在修改的 ABCK 模型中是安全的。

证明 在修改的 ABCK 模型定义的安全游戏中，假设攻击者 $\mathcal{A}$ 至多激活 N 个协议参与者，每个参与者至多激活 L 个会话，令 sid^* 表示 Test 阶段攻击者要挑战的测试会话，实体 A 为该会话的拥有者，实体 B 为其匹配会话 $\overline{sid^*}$ 的拥有者，Suc 表示攻击者 $\mathcal{A}$ 赢得该游戏，则以下 2 种情况覆盖了攻击者的所有行为。

1) 情况 E_1：若测试会话的匹配会话 $\overline{sid^*}$ 存在且攻击者 $\mathcal{A}$ 获得系统主密钥。

2) 情况 E_2：若测试会话的匹配会话 $\overline{sid^*}$ 不存在且攻击者 $\mathcal{A}$ 获得 sid^* 对应的私钥，同时若协议实体 B 在系统撤销列表中，则攻击者可以获得 B 的私钥，若协议实体 B 不在系统撤销列表中且实体 B 的属性不满足测试会话中 A 指定的访问结构，则攻击者可以获得 B 的私钥。

以下分 2 种情况证明协议安全性。

1) $\Pr[E_1\wedge Suc]$ 是可忽略的

使用一系列攻击游戏证明攻击者在这种情况下的优势是可忽略的。令 $Adv_{\mathcal{A}}^{ABAKA}(k)$ 表示攻击者 $\mathcal{A}$ 在游戏 k 中的攻击优势。

Game0 该游戏与实际的安全性游戏一致，因此攻击者 $\mathcal{A}$ 的优势 $Adv_{\mathcal{A}}^{ABAKA}(0)$ 等于攻击者攻击实际协议的优势。

Game1 该游戏与 Game0 的区别在于，若 2 个不同的会话拥有相同的会话 ID，即 2 个不同会话的协议双方以及协议双方产生的消息完全相同，则游戏终止。这种情况发生的概率相当于随机选择 2 个随机数发生碰撞的概率，因此 $\left|Adv_{\mathcal{A}}^{ABAKA}(1)-Adv_{\mathcal{A}}^{ABAKA}(0)\right|\leqslant negl$。

Game2 该游戏与 Game1 的区别在于，游戏开始选择协议通信方 A 及其意定的通信伙伴 B，并随机选择一个整数 $i\in[1,L]$，若攻击者 $\mathcal{A}$ 选择的测试会话是通信方 A 进行的第 i 次会话且其通信伙伴为 B，则游戏继续，否则游戏终止。由于攻击者选择的测试会话满足上述条件的概率为 $\frac{1}{N^2L}$，因此 $Adv_{\mathcal{A}}^{ABAKA}(2)\geqslant\frac{1}{N^2L}\cdot Adv_{\mathcal{A}}^{ABAKA}(1)$。

Game3 在该游戏中，随机选择 $\sigma_3^*\in G_T$ 代替测试会话中计算的 $\sigma_3^*=e(g,w)^{y_A^*y_B^*}$，除此以外，Game3 和 Game2 相同。若 $\left|Adv_{\mathcal{A}}^{ABAKA}(3)-Adv_{\mathcal{A}}^{ABAKA}(2)\right|$ 是不可忽略的，则可以构造一个多项式时间的挑战者 $\mathcal{S}$ 能够以不可忽略的优势解决定义 4 中的困难问题。$\mathcal{S}$ 按照下述步骤模拟安全性游戏。

Init $\mathcal{S}$ 运行攻击者 $\mathcal{A}$，$\mathcal{A}$ 输出要挑战的 2 个访问结构 $\mathbb{A}_A^*$ 和 $\mathbb{A}_B^*$ 以及系统用户撤销列表 R^* 返回给 $\mathcal{S}$，并令 $W^*=U-R^*$ 表示未被撤销用户集合。

Setup 令系统用户数为 n，属性个数为 m。$\mathcal{S}$ 随机选择 $\alpha,\gamma\in\mathbb{Z}_p$，对任意的 $i=1,2,\cdots,n,n+2,\cdots,2n$，计算 $g_i=g^{\alpha^i}$，并计算 $v=g^{\gamma}$，随机选择 $h_1,\cdots,h_m,\delta_1,\delta_2,\delta_3\in G$，并令 $w=g^s$。$\mathcal{S}$ 将系统主密钥 $MSK=(\alpha,\gamma)$ 发送给攻击者 $\mathcal{A}$，因此 $\mathcal{A}$ 可以使用主密钥生成所有用户的私钥。同时 $\mathcal{S}$ 输出系统的公开参数 $PK=(g_1\cdots g_n,g_{n+2}\cdots g_{2n},h_1\cdots h_m,v,w,\delta_1,\delta_2,\delta_3)$。

$\mathcal{S}$ 按照如下方式生成测试会话中通信双方 A 和 B 之间的消息 mem_A^* 和 mem_B^*，测试会话是 A 进行的第 i 次会话。$\mathcal{S}$ 首先令 $C_{A,3}^*=g^a,C_{B,3}^*=g^{a^n}$，其他消息都按照协议规则生成。即 $\mathcal{S}$ 随机选择向量 $\overrightarrow{s_A^*}=(x_A^*,s_{A,2}^*,\cdots,s_{A,n_A^*}^*)^{\mathrm{T}}\in\mathbb{Z}_p^{n_A^*}$，并计算分享向量 $\overrightarrow{\lambda_A^*}=(\lambda_{A,1}^*,\lambda_{A,2}^*,\cdots,\lambda_{A,l_A^*}^*)^{\mathrm{T}}=M_A^*\overrightarrow{s_A^*}$，$\mathcal{S}$ 随机选择 $d_A^*,t_{A,1}^*,t_{A,2}^*,\cdots,t_{A,l_A^*}^*\in\mathbb{Z}_p$，并计算 $C_{A,1}^*=g^{x_A^*},C_{A,2}^*=(v\prod_{j\in W^*}g_{n+1-j})^{x_A^*}$，对任意 $\forall i\in\{1\cdots l_A^*\}$，计算 $C_{A_i,1}^*=g^{\alpha\lambda_{A,i}^*}\cdot h_{\rho_A^*(i)}^{-t_{A,i}^*},C_{A_i,2}^*=g^{t_{A,i}^*}$ 最后计算 $C_{A,4}^*=(\delta_1^{c_A^*}\delta_2^{d_A^*}\delta_3)^{x_A^*}$，其中 $c_A^*=H(M_A^*,C_{A,1}^*,C_{A,2}^*,C_{A,3}^*,\{C_{A_i,1}^*,C_{A_i,2}^*\}_{i\in\{1\cdots l_A^*\}})$。$\mathcal{S}$ 输出

A 发送给 B 消息

$$mem_A^* = ((M_A^*, \rho_A^*), C_{A,1}^*, C_{A,2}^*, C_{A,3}^*, C_{A,4}^*, \{C_{A_i,1}^*, C_{A_i,2}^*\}_{i\in\{1\cdots l_A^*\}}, d_A^*)$$

同理 $\mathcal{S}$ 可计算 mem_B^*，随机选择向量 $\overrightarrow{s_B^*} = (x_B^*, s_{B,2}^*, \cdots, s_{B,n_B^*}^*)^{\mathrm{T}} \in \mathbb{Z}_p^{n_B^*}$，并计算分享向量 $\overrightarrow{\lambda_B^*} = (\lambda_{B,1}^*, \lambda_{B,2}^*, \cdots, \lambda_{B,l_B^*}^*)^{\mathrm{T}} = M_B^* \overrightarrow{s_B^*}$。$\mathcal{S}$ 随机选择 $d_B^*, t_{B,1}^*, t_{B,2}^*, \cdots, t_{B,l_B^*}^* \in \mathbb{Z}_p$，并计算 $C_{B,1}^* = g^{x_B^*}, C_{B,2}^* = (v\prod_{j\in W^*} g_{n+1-j})^{x_B^*}$，对任意的 $\forall i \in \{1\cdots l_B^*\}$，计算 $C_{B_i,1}^* = g^{\alpha\lambda_{B,i}^*} h_{\rho_B^*(i)}^{-t_{B,i}^*}$，$C_{B_i,2}^* = g^{t_{B,i}^*}$ 最后计算 $C_{B,4}^* = (\delta_1^{c_B^*}\delta_2^{d_B^*}\delta_3)^{x_B^*}$，其中 $c_B^* = H(M_B^*, C_{B,1}^*, C_{B,2}^*, C_{B,3}^*, \{C_{B_i,1}^*, C_{B_i,2}^*\}_{i\in\{1\ldots l_B^*\}})$。$\mathcal{S}$ 输出 B 发送给 A 消息

$$mem_B^* = ((M_B^*, \rho_B^*), C_{B,1}^*, C_{B,2}^*, C_{B,3}^*, C_{B,4}^*, \{C_{B_i,1}^*, C_{B_i,2}^*\}_{i\in\{1\cdots l_B^*\}}, d_B^*)$$

Simulation　$\mathcal{S}$ 用列表 $\mathcal{L}$ 记录 $\mathcal{A}$ 对会话密钥的询问 KeyReveal，然后按照协议规范和安全性游戏规则进行如下模拟。

① $Send(I, S_P, S_{\bar{P}})$：若 $I = A$，且该会话是 A 的第 i 次会话，则 $\mathcal{S}$ 返回在 Setup 阶段计算的 mem_A^*，否则 $\mathcal{S}$ 依据协议规范进行响应，并记录 $(S_P, S_{\bar{P}}, mem_P)$。

② $Send(R, S_{\bar{P}}, S_P, mem_P)$ 和 $Send(I, S_{\bar{P}}, S_P, mem_{\bar{P}})$：$\mathcal{S}$ 依据协议规范计算出会话密钥 K 并返回，将会话密钥 K 加入列表 $\mathcal{L}$，并记录所有的会话状态，标记 $(S_P, S_{\bar{P}}, mem_P, mem_{\bar{P}})$ 为已完成会话。

③ $Key\,\mathrm{Re}veal(sid)$：若会话 sid 已完成则返回其在列表 $\mathcal{L}$ 中对应的会话密钥 K，若会话未完成则返回终止符号 $\perp$。

④ $State\,\mathrm{Re}veal(sid)$：若会话 sid 未完成则返回记录的该会话的所有内部状态信息，若会话已完成则返回终止符号 $\perp$。

⑤ $Corrupt(U, S_U)$：$\mathcal{S}$ 返回 Setup 阶段生成的用户私钥 SK_U。

⑥ $Test(sid^*)$：$\mathcal{S}$ 计算 $\sigma_1^* = e(g_1, g_n)^{x_A}$ 和 $\sigma_2^* = e(g_1, g_n)^{x_B}$，并令 $\sigma_3^* = \mathcal{T}$。$\mathcal{S}$ 使用 $\sigma_1^*, \sigma_2^*, \sigma_3^*$ 计算出会话密钥 K^* 并返回给攻击者 $\mathcal{A}$。

⑦ 如果 $\mathcal{A}$ 输出猜测 b'，$\mathcal{S}$ 输出 b'。

若 $\mathcal{T} = e(g,g)^{sa^{n+1}}$，则 $\mathcal{S}$ 模拟的安全性游戏与 Game2 相同，若 $\mathcal{T}$ 是随机选择的，则 $\mathcal{S}$ 模拟的安全性游戏与 Game3 相同。若 $\left|Adv_{\mathcal{A}}^{ABAKA}(3) - Adv_{\mathcal{A}}^{ABAKA}(2)\right|$ 是不可忽略的，$\mathcal{S}$ 能够以不可忽略的优势解决定义 4 中的困难问题。因此 $\left|Adv_{\mathcal{A}}^{ABAKA}(3) - Adv_{\mathcal{A}}^{ABAKA}(2)\right| \leqslant negl$。

Game4　在该游戏中，从强随机提取器的值域空间随机选择 $\sigma_3'^*$ 代替测试会话中计算的 $\sigma_3'^* = Ext(s, \sigma_3^*)$，除此以外，Game4 和 Game3 相同。

由于在 Game3 中 σ_3^* 是随机选择的，σ_3^* 有足够的最小熵。因此，由强随机提取器的定义，$\left|Adv_{\mathcal{A}}^{ABAKA}(4) - Adv_{\mathcal{A}}^{ABAKA}(3)\right| \leqslant negl$。

Game5　在该游戏中，从伪随机函数的值域空间随机选择 β，并用 $K^* = F_{\sigma_1'^*}(sid^*) \oplus F_{\sigma_2'^*}(sid^*) \oplus \beta$ 代替测试会话的 $K^* = F_{\sigma_1'^*}(sid^*) \oplus F_{\sigma_2'^*}(sid^*) \oplus F_{\sigma_3'^*}(sid^*)$，除此以外，Game5 与 Game4 相同。

若 $\left|Adv_{\mathcal{A}}^{ABAKA}(5) - Adv_{\mathcal{A}}^{ABAKA}(4)\right|$ 是不可忽略的，则可以构造一个多项式时间的区分者 $\mathcal{D}$ 能够以不可忽略的概率区分伪随机函数 $F_k(\cdot)$ 和一个真随机函数 $RF(\cdot)$，其中 k 是在密钥空间中随机选择的密钥。$\mathcal{D}$ 按照下述步骤模拟安全性游戏。

Setup　$\mathcal{D}$ 设置系统主密钥以及所有用户的私钥。

Simulation　$\mathcal{D}$ 用列表 $\mathcal{L}$ 记录 $\mathcal{A}$ 对会话密钥的询问 KeyReveal，然后按照协议规范和安全性游戏规则进行如下模拟。

① $Send(I, S_P, S_{\bar{P}})$：$\mathcal{D}$ 依据协议规范计算 mem_P 并返回，同时记录 $(S_P, S_{\bar{P}}, mem_P)$。

② $Send(R, S_{\bar{P}}, S_P, mem_P)$ 和 $Send(I, S_{\bar{P}}, S_P, mem_{\bar{P}})$：$\mathcal{D}$ 依据协议规范计算出会话密钥 K 并返回，将会话密钥 K 加入列表 $\mathcal{L}$，并记录所有的会话状态，标记 $(S_P, S_{\bar{P}}, mem_P, mem_{\bar{P}})$ 为已完成会话。

③ $Key\,\mathrm{Re}veal(sid)$：若会话 sid 已完成则返回其在列表 $\mathcal{L}$ 中对应的会话密钥 K，若会话未完成则返回终止符号 $\perp$。

④ $State\,\mathrm{Re}veal(sid)$：若会话 sid 未完成则返回记录的该会话的所有内部状态信息，若会话已完成则返回终止符号 $\perp$。

⑤ $Corrupt(U, S_U)$：$\mathcal{D}$ 返回 Setup 阶段生成的用户私钥 SK_U。

⑥ $Test(sid^*)$：$\mathcal{D}$ 计算会话密钥 $K^* = F_{\sigma_1'^*}(sid^*) \oplus F_{\sigma_2'^*}(sid^*) \oplus F^*(sid^*)$ 并返回给攻击者 $\mathcal{A}$。

⑦ 如果 $\mathcal{A}$ 输出猜测 $b'=0$，则 $\mathcal{D}$ 输出 F^* 为伪随机函数 F，否则 $\mathcal{D}$ 输出 F^* 为真随机函数 RF。

若 $F^*=F$，则 $\mathcal{D}$ 模拟的安全性游戏与 Game4 相同；若 $F^*=RF$，则 $\mathcal{D}$ 模拟的安全性游戏与 Game5 相同。若 $\left|Adv_{\mathcal{A}}^{ABAKA}(5)-Adv_{\mathcal{A}}^{ABAKA}(4)\right|$ 是不可忽略的，则 $\mathcal{D}$ 能够以不可忽略的优势区分伪随机函数 F 和真随机函数 RF。因此 $\left|Adv_{\mathcal{A}}^{ABAKA}(5)-Adv_{\mathcal{A}}^{ABAKA}(4)\right|\leqslant negl$。

在 Game5 中，测试会话中的会话密钥是完全随机的，攻击者 $\mathcal{A}$ 的优势是可忽略的，即 $Adv_{\mathcal{A}}^{ABAKA}(5)=0$，因此 $\Pr[E_1\wedge Suc]$ 可忽略。

2) $\Pr[E_2\wedge Suc]$ 是可忽略的

使用一系列攻击游戏证明攻击者在这种情况下的优势是可忽略的。

Game0 该游戏与实际的安全性游戏一致，因此攻击者 $\mathcal{A}$ 的优势 $Adv_{\mathcal{A}}^{ABAKA}(0)$ 等于攻击者攻击实际协议的优势。

Game1 该游戏与 Game0 的区别在于，若 2 个不同的会话拥有相同的会话 ID，即 2 个不同会话的协议双方以及协议双方产生的消息完全相同，则游戏终止。这种情况发生的概率相当于随机选择 2 个随机数发生碰撞的概率，因此 $\left|Adv_{\mathcal{A}}^{ABAKA}(1)-Adv_{\mathcal{A}}^{ABAKA}(0)\right|\leqslant negl$。

Game2 该游戏与 Game1 的区别在于，游戏开始选择协议通信方 A，并随机选择一个整数 $i\in[1,L]$，若攻击者 $\mathcal{A}$ 选择的测试会话是通信方 A 进行的第 i 次会话则游戏继续，否则游戏终止。由于攻击者选择的测试会话满足上述条件的概率为 $\frac{1}{N^2L}$，因此 $Adv_{\mathcal{A}}^{ABAKA}(2)\geqslant\frac{1}{N^2L}\cdot Adv_{\mathcal{A}}^{ABAKA}(1)$。

Game3 在该游戏中，随机选择 $\sigma_1^*\in G_T$ 代替测试会话中计算的 $\sigma_1^*=e(g_1,g_n)^{x_A^*}$，除此以外，Game3 和 Game2 相同。若 $\left|Adv_{\mathcal{A}}^{ABAKA}(3)-Adv_{\mathcal{A}}^{ABAKA}(2)\right|$ 是不可忽略的，则可以构造一个多项式时间的挑战者 $\mathcal{S}$ 能够以不可忽略的优势解决定义 4 中的困难问题。假定测试会话中通信方 A 的意定通信伙伴为 B，$\mathcal{S}$ 按照下述步骤模拟安全性游戏。

Init $\mathcal{S}$ 运行攻击者 $\mathcal{A}$，$\mathcal{A}$ 输出测试会话中要挑战的访问结构 $\mathbb{A}_A^*$ 以及系统用户撤销列表 R^* 返回给 $\mathcal{S}$。令系统用户集合为 U，$W^*=U-R^*$ 表示未被撤销用户集合。令系统属性个数为 m，用户数为 n。$\mathbb{A}_A^*$ 对应的访问控制矩阵为 $((M_A^*)_{l_A^*\times n_A^*},\rho_A^*)$，其中 $l_A^*,n_A^*\leqslant n$。

Setup 首先，$\mathcal{S}$ 生成系统公开参数。$\mathcal{S}$ 隐含设置主密钥 $\alpha=a$，对任意 $i=1,2,\cdots,n,n+2\cdots2n$，设置 $g_i=g^{a^i}$。随机选择 $z_1,z_2,\cdots,z_m\in\mathbb{Z}_p$，对任意的 $1\leqslant j\leqslant m$，令集合 I 表示所有 $\rho_A^*(i)=j$ 的集合，若 $I\neq\phi$，则 $h_j=g^{z_j}\prod_{i\in I}g^{aM_{A(i,1)}^*/b_i}\cdot g^{a^2M_{A(i,2)}^*/b_i}\cdots g^{a^{n_A^*}M_{A(i,n_A^*)}^*/b_i}$，若 $I=\phi$，则 $h_j=g^{z_j}$。$\mathcal{S}$ 随机选择 $w\in G,v',d_2,d_3,e_1,e_2,e_3\in\mathbb{Z}_p$，同时计算 $v=g^{v'}\cdot(\prod_{j\in W^*}g_{n+1-j})^{-1}$，并计算其他公开参数

$$\delta_1=g^{a^n}g^{e_1},\ \delta_2=g^{a^nd_2}g^{e_2},\ \delta_3=g^{a^nd_3}g^{e_3}$$

$\mathcal{S}$ 输出系统的公开参数 $PK=(g_1\cdots g_n,\ g_{n+2}\cdots g_{2n},\ h_1\cdots h_m,v,w,\delta_1,\delta_2,\delta_3)$。

接下来，$\mathcal{S}$ 为身份标识为 ID 和属性集合为 S_{ID} 的用户产生私钥。由定义 8 中 ABCK 安全性定义，以下分 2 种情况生成用户私钥。

① $ID\in R^*$

$\mathcal{S}$ 随机选择 $r\in\mathbb{Z}_p$，对任意 $\forall x\in S_{ID}$，计算：$K_{ID_x,3}=h_x^r$，并计算 $K_{ID,2}=g^r$，然后计算 $K_{ID,1}=g^{\alpha^{ID}\gamma+\alpha r}=g^{a^{ID}v'}(\prod_{j\in W^*}g_{n+1-j+ID})^{-1}\cdot g^{ar}$，由于 $ID\in R^*$，则 $ID\notin W^*$，因此 $\mathcal{S}$ 能够模拟用户私钥 $SK_{ID}=(K_{ID,1},K_{ID,2},\{K_{ID_x,3}\}_{x\in S_{ID}})$。

② $ID\notin R^*$ 且 $S_{ID}\notin\mathbb{A}_A^*$

由于 $ID\notin R^*$，则 $ID\in W^*$。由于 $S_{ID}\notin\mathbb{A}_A^*$，则存在一个向量 $\vec{\omega}=(\omega_1,\omega_2,\cdots,\omega_{n_A^*})^{\mathrm{T}}\in\mathbb{Z}_p^{n_A^*}$，且 $\omega_1=-1$，对 $\rho_A^*(i)\in S_{ID}$，有 $M_{A(i)}^*\cdot\vec{\omega}=0$。$\mathcal{S}$ 随机选择 $r'\in\mathbb{Z}_p$，并令 $r=r'-\omega_1a^n-\cdots-\omega_{n_A^*}a^{n+1-n_A^*}=r'-\sum_{1\leqslant i\leqslant n_A^*}\omega_ia^{n+1-i}$ $\mathcal{S}$ 计算 $K_{ID,2}=g^r=g^{r'}\prod_{1\leqslant i\leqslant n_A^*}(g^{a^{n+1-i}})^{-\omega_i}$ 以及

$$\begin{aligned}K_{ID,1}&=g^{\alpha^{ID}\gamma+\alpha r}\\&=g^{a^{ID}v'}(\prod_{j\in W^*}g_{n+1-j+ID})^{-1}\cdot g^{a(r'-\sum_{1\leqslant i\leqslant n_A^*}\omega_ia^{n+1-i})}\\&=g^{a^{ID}v'+ar'}(\prod_{j\in W^*,j\neq ID}g_{n+1-j+ID})^{-1}\prod_{2\leqslant i\leqslant n_A^*}(g^{a^{n+2-i}})^{-\omega_i}\end{aligned}$$

对任意的 $\forall x\in S_{ID}$，令集合 I 表示所有 $\rho_A^*(i)=x$

集合。若 $I=\phi$，则可以计算 $K_{ID_x,3}=h_x^r=(K_{ID,2})^{z_x}$，若 $I\neq\phi$，由于 $M^*_{A(i)}\cdot\vec{\omega}=0$，可以计算

$$K_{ID_x,3}=h_x^r$$
$$=(g^r)^{z_x}\prod_{i\in I}\prod_{1\leqslant k\leqslant n_A^*}\Big(\big(\frac{a^k}{b_i}\big)^{r'}\prod_{1\leqslant l\leqslant n_A^*}\big(g^{\frac{a^{n+1+k-l}}{b_i}}\big)^{-\omega_l}\Big)^{M^*_{A(i,k)}}$$
$$=(K_{ID,2})^{z_x}\prod_{i\in I}\prod_{1\leqslant k\leqslant n_A^*}\Big(\big(\frac{a^k}{b_i}\big)^{r'}\prod_{\substack{1\leqslant l\leqslant n_A^*\\ l\neq k}}\big(g^{\frac{a^{n+1+k-l}}{b_i}}\big)^{-\omega_l}\Big)^{M^*_{A(i,k)}}$$

因此 $\mathcal{S}$ 能够模拟用户私钥 $SK_{ID}=(K_{ID,1},K_{ID,2},\{K_{ID_x,3}\}_{x\in S_{ID}})$。

最后，$\mathcal{S}$ 按如下方式生成通信方 A 的第 i 次会话的消息 mem_A^*。$\mathcal{S}$ 令 $C^*_{A,1}=g^s$，随机选取 $s'_{A,2},s'_{A,3},\cdots,s'_{A,n_A^*}\in\mathbb{Z}_p$ 并隐含设置向量 $\vec{s_A^*}=(s,sa+s'_{A,2},\cdots,sa^{n_A^*-1}+s'_{A,n_A^*})^{\mathrm{T}}\in\mathbb{Z}_p^{n_A^*}$，由 $\vec{\lambda_A^*}=(\lambda^*_{A,1},\lambda^*_{A,2},\cdots,\lambda^*_{A,l_A^*})^{\mathrm{T}}=M_A^*\vec{s_A^*}$ 计算分享向量得 $\lambda^*_{A,i}=\sum_{1\leqslant j\leqslant n_A^*}M^*_{A(i,j)}sa^{j-1}+\sum_{2\leqslant j\leqslant n_A^*}M^*_{A(i,j)}s'_{A,j}$，对 $\forall i\in\{1\cdots l_A^*\}$，隐含设置 $t^*_{A,i}=sb_i$，$\mathcal{S}$ 计算

$$C_{A_i,1}=g^{a\lambda^*_{A,i}}h_{\rho_A^*(i)}^{-t^*_{A,i}}$$
$$=\prod_{1\leqslant j\leqslant n_A^*}(g^{sa^j})^{M^*_{A(i,j)}}\cdot\prod_{2\leqslant j\leqslant n_A^*}(g^a)^{M^*_{A(i,j)}s'_{A,j}}\cdot(g^{sb_i})^{-z_i}\cdot$$
$$\Big(\prod_{k\in I}\prod_{1\leqslant j\leqslant n_A^*}(g^{a^j\cdot s\cdot(b_i/b_k)})^{-M^*_{A(k,j)}}\Big)$$
$$=\Big(\prod_{2\leqslant j\leqslant n_A^*}g^{aM^*_{A(i,j)}s'_{A,j}}\Big)g^{-z_isb_i}\Big(\prod_{\substack{k\in I\\ k\neq i}}\prod_{1\leqslant j\leqslant n_A^*}\big(g^{\frac{a^jsb_i}{b_k}}\big)^{-M^*_{A(k,j)}}\Big)$$
$$C_{A_i,2}=g^{t_{A,i}}=g^{sb_i}$$

$\mathcal{S}$ 随机选取 $y_A^*\in\mathbb{Z}_p$，计算 $C^*_{A,3}=g^{y_A^*}$，同时可计算 $C^*_{A,2}=(v\prod_{j\in W^*}g_{n+1-j})^s=g^{sv'}$。$\mathcal{S}$ 可以计算

$$c_A^*=H(M_A^*,C^*_{A,1},C^*_{A,2},C^*_{A,3},\{C^*_{A_i,1},C^*_{A_i,2}\}_{i\in\{1\cdots l_A^*\}})$$

并令 $d_A^*=-(c_A^*+d_3)/d_2$，从而 $\mathcal{S}$ 可以计算

$$C^*_{A,4}=(\delta_1^{c_A^*}\delta_2^{d_A^*}\delta_3)^s$$
$$=((g^{a^n}g^{e_1})^{c_A^*}(g^{a^nd_2}g^{e_2})^{-(c_A^*+d_3)/d_2}(g^{a^nd_3}g^{e_3}))^s$$
$$=(g^s)^{e_1c_A^*+e_2d_A^*+e_3}$$

$\mathcal{S}$ 生成的通信方 A 的消息为

$$mem_A^*=((M_A^*,\rho_A^*),C^*_{A,1},C^*_{A,2},C^*_{A,3},C^*_{A,4},\{C^*_{A_i,1},C^*_{A_i,2}\}_{i\in\{1,2\cdots,l_A^*\}},d_A^*)$$

Simulation　$\mathcal{S}$ 用列表 $\mathcal{L}$ 记录 $\mathcal{A}$ 对会话密钥的询问 KeyReveal，然后按照协议规范和安全性游戏规则进行如下模拟。

① $Send(I,S_P,S_{\bar{P}})$：若 $I=A$，且该会话是 A 的第 i 次会话，则 $\mathcal{S}$ 返回在 Setup 阶段计算的 mem_A^*，否则 $\mathcal{S}$ 依据协议规范进行响应，并记录 $(S_P,S_{\bar{P}},mem_P)$。

② $Send(R,S_{\bar{P}},S_P,mem_P)$ 和 $Send(I,S_{\bar{P}},S_P,mem_{\bar{P}})$：$\mathcal{S}$ 依据协议规范将获取的消息 mem_P 解析为

$$mem_P=((M_P,\rho_P),C_{P,1},C_{P,2},C_{P,3},C_{P,4},\{C_{P_i,1},C_{P_i,2}\}_{i\in\{1,2,\cdots,l_P\}},d_P)$$

假定 $S_{\bar{P}}$ 满足访问结构 (M_P,ρ_P)，计算

$$c_P=H(M_P,C_{P,1},C_{P,2},C_{P,3},\{C_{P_i,1},C_{P_i,2}\}_{i\in[1,l_P]})$$

判断 $e(g,C_{P,4})=e(C_{P,1},\delta_1^{c_P}\delta_2^{d_P}\delta_3)$ 是否成立，若该式不成立则返回终止符号 $\perp$，否则 $\mathcal{S}$ 判断 $c_P+d_Pd_2+d_3=0$ 是否成立，若成立则 $\mathcal{S}$ 模拟失败，否则 $\mathcal{S}$ 计算

$$\sigma_1=e(\frac{C_{P,4}}{(C_{P,1})^{c_Pe_1+d_Pe_2+e_3}},(g^a)^{\frac{1}{c_P+d_Pd_2+d_3}})$$
$$=e((\frac{g^{a^nc_P}g^{e_1c_P}g^{a^nd_2d_P}g^{e_2d_P}g^{a^nd_3}g^{e_3}}{g^{c_Pe_1+d_Pe_2+e_3}})^{x_P},(g^a)^{\frac{1}{c_P+d_Pd_2+d_3}})$$
$$=e(g_1,g_n)^{x_P}$$

$\mathcal{S}$ 依据协议规则能够计算出 σ_2,σ_3，因此 $\mathcal{S}$ 能够计算出会话密钥 K 并返回，并将会话密钥 K 加入列表 $\mathcal{L}$，记录所有的会话状态，标记 $(S_P,S_{\bar{P}},mem_P,mem_{\bar{P}})$ 为已完成会话。

③ $KeyReveal(sid)$：若会话 sid 已完成则返回其在列表 $\mathcal{L}$ 中对应的会话密钥 K，若会话未完成则返回终止符号 $\perp$。

④ $StateReveal(sid)$：若会话 sid 未完成则返回记录的该会话的所有内部状态信息，若会话已完成则返回终止符号 $\perp$。

⑤ $Corrupt(U,S_U)$：$\mathcal{S}$ 返回 Setup 阶段生成的用户私钥 SK_U。

⑥ $Test(sid^*)$：$\mathcal{S}$ 令 $\sigma_1^*=\mathcal{T}$ 并计算 $\sigma_2^*=e(g_1,g_n)^{x_B^*}$ 和 $\sigma_3^*=e(g,w)^{y_A^*y_B^*}$。$\mathcal{S}$ 使用 $\sigma_1^*,\sigma_2^*,\sigma_3^*$ 计算出会话密钥 K^* 并返回给攻击者 $\mathcal{A}$。

⑦ 如果 $\mathcal{A}$ 输出猜测 b'，$\mathcal{S}$ 输出 b'。

首先分析挑战者 $\mathcal{S}$ 模拟失败的概率，当 $c_P + d_P d_2 + d_3 = 0$ 时 $\mathcal{S}$ 模拟失败，该等式成立的概率至多为 $1/p$，从而挑战者 $\mathcal{S}$ 模拟失败的概率为 q_D / p，其中，q_D 为攻击者进行 $Send(R, S_{\bar{P}}, S_P, mem_P)$、$Send(I, S_{\bar{P}}, S_P, mem_{\bar{P}})$ 查询的次数，而 q_D / p 在信息论中是可忽略的，因此挑战者 $\mathcal{S}$ 模拟失败的概率是可忽略的。若 $\mathcal{T} = e(g,g)^{sa^{n+1}}$，则 $\mathcal{S}$ 模拟的安全性游戏与 Game2 相同，若 $\mathcal{T}$ 是随机选择的，则 $\mathcal{S}$ 模拟的安全性游戏与 Game3 相同。若 $\left| Adv_{\mathcal{A}}^{ABAKA}(3) - Adv_{\mathcal{A}}^{ABAKA}(2) \right|$ 是不可忽略的，则 $\mathcal{S}$ 能够以不可忽略的优势解决定义 4 中定义的 DPBDHE 困难问题。因此 $\left| Adv_{\mathcal{A}}^{ABAKA}(3) - Adv_{\mathcal{A}}^{ABAKA}(2) \right| \leqslant negl$。

Game4 在该游戏中，从强随机提取器的值域空间随机选择 σ'^{*}_1 代替测试会话中计算的 $\sigma'^{*}_1 = Ext(s, \sigma^{*}_1)$，除此以外，Game4 和 Game3 相同。

由于在 Game3 中 σ^{*}_1 是随机选择的，σ^{*}_1 有足够的最小熵。因此，由强随机提取器的定义，$\left| Adv_{\mathcal{A}}^{ABAKA}(4) - Adv_{\mathcal{A}}^{ABAKA}(3) \right| \leqslant negl$。

Game5 在该游戏中，从伪随机函数的值域空间随机选择 β，并用 $K^{*} = \beta \oplus F_{\sigma'^{*}_2}(sid^{*}) \oplus F_{\sigma'^{*}_3}(sid^{*})$ 代替测试会话的 $K^{*} = F_{\sigma'^{*}_1}(sid^{*}) \oplus F_{\sigma'^{*}_2}(sid^{*}) \oplus F_{\sigma'^{*}_3}(sid^{*})$，除此以外，Game5 与 Game4 相同。

若 $\left| Adv_{\mathcal{A}}^{ABAKA}(5) - Adv_{\mathcal{A}}^{ABAKA}(4) \right|$ 是不可忽略的，则可以构造一个多项式时间的区分者 $\mathcal{D}$ 能够以不可忽略的概率区分伪随机函数 $F_k(\cdot)$ 和一个真随机函数 $RF(\cdot)$，其中 k 是在密钥空间中随机选择的密钥。$\mathcal{D}$ 按照下述步骤模拟安全性游戏。

Setup $\mathcal{D}$ 设置系统主密钥以及所有用户的私钥。

Simulation $\mathcal{D}$ 用列表 $\mathcal{L}$ 记录 $\mathcal{A}$ 对会话密钥的询问 KeyReveal，然后按照协议规范和安全性游戏规则进行如下模拟。

① $Send(I, S_P, S_{\bar{P}})$：$\mathcal{D}$ 依据协议规范计算 mem_P 并返回，同时记录 $(S_P, S_{\bar{P}}, mem_P)$。

② $Send(R, S_{\bar{P}}, S_P, mem_P)$ 和 $Send(I, S_{\bar{P}}, S_P, mem_{\bar{P}})$：$\mathcal{D}$ 依据协议规范计算出会话密钥 K 并返回，将会话密钥 K 加入列表 $\mathcal{L}$，并记录所有的会话状态，标记 $(S_P, S_{\bar{P}}, mem_P, mem_{\bar{P}})$ 为已完成会话。

③ $KeyReveal(sid)$：若会话 sid 已完成则返回其在列表 $\mathcal{L}$ 中对应的会话密钥 K，若会话未完成则返回终止符号 $\perp$。

④ $StateReveal(sid)$：若会话 sid 未完成则返回记录的该会话的所有内部状态信息，若会话已完成则返回终止符号 $\perp$。

⑤ $Corrupt(U, S_U)$：$\mathcal{D}$ 返回 Setup 阶段生成的用户私钥 SK_U。

⑥ $Test(sid^{*})$：$\mathcal{D}$ 计算会话密钥 $K^{*} = F^{*}(sid^{*}) \oplus F_{\sigma'^{*}_2}(sid^{*}) \oplus F_{\sigma'^{*}_3}(sid^{*})$ 并返回给攻击者 $\mathcal{A}$。

⑦ 如果 $\mathcal{A}$ 输出猜测 $b' = 0$，则 $\mathcal{D}$ 输出 F^{*} 为伪随机函数，否则 $\mathcal{D}$ 输出 F^{*} 为真随机函数 RF。

若 $F^{*} = F$，则 $\mathcal{D}$ 模拟的安全性游戏与 Game4 相同；若 $F^{*} = RF$，则 $\mathcal{D}$ 模拟的安全性游戏与 Game5 相同。若 $\left| Adv_{\mathcal{A}}^{ABAKA}(5) - Adv_{\mathcal{A}}^{ABAKA}(4) \right|$ 是不可忽略的，则 $\mathcal{D}$ 能够以不可忽略的优势区分伪随机函数 F 和真随机函数 RF。因此 $\left| Adv_{\mathcal{A}}^{ABAKA}(5) - Adv_{\mathcal{A}}^{ABAKA}(4) \right| \leqslant negl$。

在 Game5 中，测试会话中的会话密钥是完全随机的，攻击者 $\mathcal{A}$ 的优势是可忽略的，即 $Adv_{\mathcal{A}}^{ABAKA}(5) = 0$，因此 $\Pr[E_2 \wedge Suc]$ 可忽略。

综合 2 种情况下 $\Pr[E_1 \wedge Suc]$ 和 $\Pr[E_2 \wedge Suc]$ 均是可忽略的，则有 $\Pr[Suc]$ 是可忽略的，因此定理 1 得证。

5.2 安全性与通信效率比较

本节将本文所提协议与已有的支持通用认证策略的基于属性的认证密钥协商协议进行比较，其中文献[11]中的协议采用文献[6]中的基于属性的签名方案。在比较协议通信效率时，l 和 n 分别 F 表示访问控制矩阵的行数和列数，sig 和 vk 分别表示一次性签名方案签名和验证密钥的大小，k 表示一次性签名方案中验证密钥的比特串长度。

从表 1 中可以看出，虽然文献[10]中的协议能够抵抗临时密钥泄露攻击(LEK, leakage of ephemeral key)，但是本文所提协议能够在标准模型下可证安全，且通信效率也具有很大优势；相比于文献[11]中的协议，本文所提协议在通信效率、协议运行轮数以及安全性质上都有明显的优势；由于文献[12]中的协议采用了一次性签名的转化方法，将验证密钥比特串的每一位(0 或 1)映射为 2 个冗余属性，若采用 RSA 签名且验证密钥比特串长度为 1 024 位，则系统的公开参数和协议通信量都将增加 2 048 个群元素，而在实际应用中，冗余属性的个数远多于系统实际需要的属性个数，从而增加了系统

表 1　　**安全性质与通信效率比较**

协议	协议轮数	安全模型	安全性质	用户撤销	通信效率
文献[10]中协议	1	选择安全&RO 模型	wPFS，KCI，LEK	×	$ln+1$
文献[11]中协议	3	全安全&标准模型	wPFS	×	$7l+12$
文献[12]中协议	1	选择安全&标准模型	wPFS，KCI	×	$2l+2k+\|sig\|+\|vk\|$
本文协议	1	选择安全&标准模型	wPFS，KCI	√	$2l+5$

的复杂性，因此相比于该协议，本文所提协议通信效率较高。此外，本文所提协议能够实现对用户的即时撤销，且不需要密钥权威对所有未被撤销用户私钥进行定期更新，撤销代价较小。

6　结束语

本文针对已有的属性认证密钥协商协议的不足，提出了一个支持用户撤销的基于属性的认证密钥协商协议。该协议结合了 Waters[4]的属性加密方案和 Boneh 等人[19]的广播加密方案，能够实现对用户私钥权限的即时撤销，且不需要密钥权威对所有未被撤销用户私钥进行定期更新，降低了用户撤销代价。本文借鉴了 Lai 等人[17]提出的一个简洁高效的从 CPA 到 CCA 的转化方法，并将其应用于基于属性的认证协议中，提高了协议通信效率。此外，本文对现有的 ABCK 模型进行了修改，使之能够适应支持用户撤销的属性认证密钥协商协议的安全性分析。本文所提协议支持通用认证策略，并能够在标准模型和修改的 ABCK 模型下可证安全，具有弱的完美前向安全性，并能够抵抗密钥泄露伪装攻击。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. Cryptology-EUROCRYPT 2005[C]. Berlin: Springer-Verlag, 2005. 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. New York: ACM, 2006. 89-98.

[3] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Proceedings of the 2007 IEEE Symposium on Security and Privacy[C]. Washington DC, 2007. 321-334.

[4] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[A]. PKC 2011[C]. Springer, Heidelberg ,2011.53-70.

[5] LI J, AU M H, SUSILO W, *et al*. Attribute-based signature and its applications[A]. ASIACCS 2010[C].2010.60-69.

[6] OKAMOTO T, TAKASHIMA K. Efficient attribute-based signatures for non-monotone predicates in the standard model[A]. PKC 2011[C]. Springer, Heidelberg ,2011.35-52.

[7] WANG H, XU Q, BAN T. A provably secure two-party attribute-based key agreement protocol[A]. IIH-MSP 2009[C]. 2009.1042-1045.

[8] WANG H, XU Q, FU X. Two-party attribute-based key agreement protocol in the standard model[A]. ISIP 2009[C]. 2009. 325-328.

[9] WANG H, XU Q, FU X. Revocable attribute-based key agreement protocol without random oracles[A]. JNW 4[C]. 2009.787-794.

[10] YONEYAMA K. Strongly secure two-pass attribute-based authenticated key exchange[A]. Pairing 2010[C]. Springer, Heidelberg, 2010.147-166.

[11] BIRKETT J, STEBILA D. Predicate-based key exchange[A]. ACISP 2010[C]. Springer, Heidelberg, 2010.282-299.

[12] YONEYAMA K. Two-party round-optimal session-policy attribute-based authenticated key exchange without random oracles[A]. ICISC 2011[C]. Springer, 2011.467-489.

[13] BONEH D, CANETTI R, HALEVI S, *et al*. Chosen-ciphertext security from identity-based encryption[J]. SIAM J Comput, 2007,36(5): 1301-1328.

[14] 苏金树, 曹丹, 王小峰等. 属性基加密机制[J]. 软件学报, 2011, 22(6): 1299-1315.
SU J S, CAO D, WANG X F, *et al*. Attribute based encryption schemes[J]. Journal of Software, 2011,22(6):1299-1315.

[15] ATTRAPADUNG N, IMAI H. Attribute-based encryption supporting direct/indirect revocation modes[A]. Proc of the Cryptography and Coding 2009[C]. Berlin: Springer-Verlag, 2009.278-300.

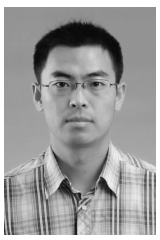
[16] ATTRAPADUNG N, IMAI H. Conjunctive broadcast and attribute-based encryption[A]. Pairing-Based Cryptography-Pairing 2009[C]. Berlin: Springer-Verlag, 2009.248-265.

[17] LAI J, DENG R H, LIU S, *et al*. Efficient CCA-secure PKE from identity-based techniques[A]. CT-RSA 2010[C]. Springer, Heidelberg, 2010.132-147.

[18] BEIMEL A. Secure Schemes for Secret Sharing and Key Distribution[D]. Israel Institute of Technology, Technion,1996.

[19] BONEH D, GENTRY C, WATERS B. Collusion resistant broadcast encryption with short ciphertexts and private keys[A]. CRYPTO 2005[C]. Springer, Heidelberg, 2005.258-275.

作者简介：



李强（1984-），男，吉林舒兰人，中国科学院博士生，主要研究方向为网络与系统安全。

冯登国（1965-），男，陕西靖边人，中国科学院研究员、博士生导师，主要研究方向为密码学与信息安全。

张立武（1976-），男，山东淄博人，博士，中国科学院高级工程师，主要研究方向为信息与系统安全。