软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(10):2397−2408 [doi: 10.13328/j.cnki.jos.004505]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

标准模型下可证安全的属性基认证密钥交换协议*

魏江宏, 刘文芬, 胡学先

(数学工程与先进计算国家重点实验室(解放军信息工程大学),河南 郑州 450001)

通讯作者: 魏江宏, E-mail: jianghong.wei.xxgc@gmai.com

摘 要: 在Waters的属性基加密方案的基础上,提出了一个在标准模型下可证安全的两方属性基认证密钥交换协议.在修改的BJM模型中,给出了所提协议在判定性双线性Diffie-Hellman假设下的安全性证明.此外,针对无会话密钥托管的应用需求,在基本协议的基础上,构造了能够有效防止会话密钥托管的属性基认证密钥交换协议.在计算效率方面,所提协议与现有的仅在随机预言模型下可证安全的属性基认证密钥交换协议相当.

关键词: 属性基加密;认证密钥交换;属性认证;标准模型

中图法分类号: TP309

中文引用格式: 魏江宏,刘文芬,胡学先.标准模型下可证安全的属性基认证密钥交换协议.软件学报,2014,25(10):2397−2408. http://www.jos.org.cn/1000-9825/4505.htm

英文引用格式: Wei JH, Liu WF, Hu XX. Provable secure attribute based authenticated key exchange protocols in the standard model. Ruan Jian Xue Bao/Journal of Software, 2014,25(10):2397−2408 (in Chinese). http://www.jos.org.cn/1000-9825/4505.htm

Provable Secure Attribute Based Authenticated Key Exchange Protocols in the Standard Model

WEI Jiang-Hong, LIU Wen-Fen, HU Xue-Xian

(State Key Laboratory of Mathematical Engineering and Advanced Computing (PLA Information Engineering University), Zhengzhou 450001, China)

Corresponding author: WEI Jiang-Hong, E-mail: jianghong.wei.xxgc@gmai.com

Abstract: Based on Waters' attribute based encryption scheme, this paper proposes a two-party attribute based authenticated key exchange protocol with provable security in the standard model. The detailed proof of the security is presented in the modified BJM model under the decisional bilinear Diffie-Hellman assumption. In addition, to satisfy the requirement that the session key should not be escrowed by the trusted third party, a new protocol, which can cancel the escrow of the session key, is constructed from the basic protocol. The computation efficiency of the proposed protocols is nearly equivalent to the computation efficiency of the available ABAKE protocols with provable secure attribute in the random oracle model.

Key words: attribute based encryption; authenticated key exchange; attribute authentication; standard model

认证密钥交换(authenticated key exchange,简称AKE)协议是密码学中的一个基本模块,在实现彼此认证的基础上,能够为开放网络上的通信节点建立会话密钥,为后续的通信会话提供机密性、完整性、可用性等安全服务.根据所基于的密钥基础设施的不同,AKE协议大致可分为基于公钥密码的AKE协议、基于对称密码的AKE协议、基于口令的AKE协议等不同类型.本文主要关注基于公钥密码的AKE协议中的一类,即,基于属性的AKE(attribute based AKE,简称ABAKE)协议.

为了解决复杂信息系统中的细粒度访问控制问题和传统公钥密码体制在分布式网络中应用时存在的缺陷,密码学者提出了基于属性的加密(attribute based encryption,简称ABE)机制[1].ABE机制能够支持属性的与、

* 基金项目: 国家重点基础研究发展计划(973)(2012CB315905)
收稿时间: 2012-07-02; 定稿时间: 2013-09-26

或、非和门限操作,实现灵活的访问控制策略,因而在分布式领域具有良好的应用前景,如细粒度访问控制、隐私保护、组密钥管理、定向广播等等[2].如同基于身份的 AKE 协议是建立在身份基加密的基础之上,学者在 ABE 体制研究的基础上开始设计 ABAKE 协议.首先,作为一种 AKE 协议,ABAKE 协议能够为上层的密码算法提供安全的会话密钥,用以保障在不安全网络上所传输信息的机密性、完整性、可用性、不可抵赖性和可控性;其次,作为一种特殊的 AKE 协议,ABAKE 协议继承了 ABE 体制的优势,即,利用属性描述用户,实现了对用户身份的保护,这也使得 ABAKE 协议能够满足一些特定应用场景的需求,如网上医疗系统、网上聊天室、军队指挥系统、电子投票系统等等.下面通过一个例子来说明 ABAKE 协议的应用场景.

在一个社交网站上,当用户向网站注册时,管理员依据用户的属性(如性别、年龄、职业等等)给每个用户分发相应的属性私钥.如图 1 所示,当 Alice 想和一个年龄在 23 岁~27 岁之间、职业是教师的女性交流时,推导一个认证策略$\mathcal{T}_{\text{Alice}}$;当 Bob 想和一个年龄在 25 岁~30 岁之间、职业是医生的男性交流时,推导一个认证策略$\mathcal{T}_{\text{Bob}}$.若 Alice 和 Bob 都拥有相应的属性私钥,则双方就能通过彼此的认证策略,最后可通过 ABAKE 协议协商出一个会话密钥,实现安全地通信.可以看出:在这样一种场景中,通信双方只需验证对方是否满足自己的要求,而无需关注通信方的具体身份信息,这在一定程度上保护了用户隐私.

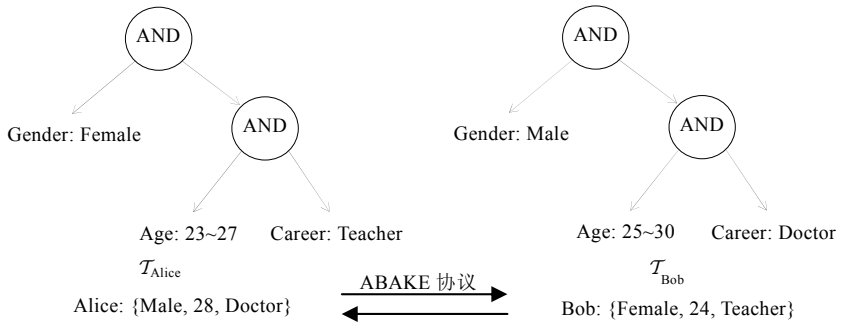


Fig.1 An application example of ABAKE protocol

图 1 ABAKE 协议应用场景实例

最早的 ABAKE 协议是 Ateniese[3]提出的一个基于属性的秘密握手机制,该机制中,只要通信双方所匹配的属性数目超过某个预先设定的门限,双方就能协商出一个会话密钥,其所处理的认证策略比较简单,即,只支持属性的门限操作.Wang 等人[4]基于 ABE 体制提出了一个 ABAKE 协议的变体,在他们的协议中,用户属性被进行 Hash 运算后当做一个用户标识,没有实现基于用户属性的认证.因此,该协议更类似于基于身份的 AKE 协议.2010 年,Yoneyama[5]利用 NAXOS 协议的设计技巧,提出了一个两轮 ABAKE 协议,并在修改后的 eCK 模型中给出了安全性证明.据我们所知,现有文献中的 ABAKE 协议都只是在随机预言(random oracle,简称 RO)模型下可证安全的.但标准模型是比随机预言模型更为自然、更为合理的一类分析模型,且能比随机预言模型提供更强的安全性保证,因此,设计标准模型下可证安全的 ABAKE 协议更具有实际意义.

本文在 Waters[6]的 ABE 方案的基础上,采用 MTI 协议族“加密-解密”的设计思想,并借鉴标准模型下可证安全的基于身份 AKE 协议[6−9]的设计方法,设计了一个标准模型下可证安全的 ABAKE 协议.基于判定性双线性 Diffie-Hellman(decisional bilinear Diffie-Hellman,简称 DBDH)问题的困难性,给出了所提协议在修改后的 BJM 模型中的安全性证明.与仅有的在随机预言模型下可证安全的 ABAKE 协议相比,新设计的协议不仅在安全性上具有优势,同时计算效率也相当,因此更适合在实际中应用.

本文第 1 节介绍一些预备知识.第 2 节给出协议的具体构造.第 3 节在标准模型下证明所提协议的安全性.第 4 节讨论所提协议的安全性和计算效率.最后一节总结全文.

1 预备知识

1.1 相关密码组件

定义 1(双线性映射). 假设 G 和 G_1 是两个阶均为大素数 p 的循环群,而 g 是 G 的一个生成元,双线性映射 $e:G\times G\to G_1$ 为具有如下性质的映射:

(1) 双线性:若 $u,v\in G$,且 $a,b\in\mathbb{Z}_p$,则 $e(u^a,v^b)=e(u,v)^{ab}$;

(2) 非退化性: $e(g,g)\neq 1_{G_1}$;

(3) 可计算性:对任意的 $u,v\in G$,存在一个有效的多项式时间算法来计算 $e(u,v)$.

定义 2(访问结构[10]). 假设在实体集$\mathbb{P}=\{P_1,P_2,\ldots,P_n\}$上共享了一个秘密,若$\mathbb{P}$的一个子集能够重构该秘密,则称这个子集为一个授权子集;否则,称其为非授权子集.所有授权子集构成的集族$\mathcal{T}$,称为对该秘密的一个访问结构.一个访问结构$\mathcal{T}$称为单调的,是指若 $A\in\mathcal{T},A\subseteq B\subseteq\mathbb{P}$,则 $B\in\mathcal{T}$.

定义 3(线性秘密共享机制[6]). 一个定义在实体集$\mathbb{P}$上的线性秘密共享机制(linear secret sharing scheme,简称 LSSS)具有下述性质:

(1) 所有实体的共享组成$\mathbb{Z}_p$上的一个向量;

(2) 存在一个$l\times n$的共享生成矩阵$\boldsymbol{M}$和一个从$\{1,2,\ldots,l\}$到$\mathbb{P}$的映射ρ,随机选取 $\boldsymbol{v}=(x,v_2,\ldots,v_n)\in\mathbb{Z}_p^n$,其中,$x$是要共享的秘密,则$\boldsymbol{Mv}^T$就是利用共享生成矩阵得到的关于$x$的$l$个共享组成的向量,其中,共享$(\boldsymbol{Mv}^T)_i$属于实体$\rho(i)$.

按照上述方法定义的 LSSS 具有线性可重构性:假设Π是一个针对访问结构$\mathcal{T}$的 LSSS,对授权用户集 $S\in\mathcal{T}$,定义 $I=\{i:\rho(i)\in S\}\subseteq\{1,\ldots,l\}$,则存在常数集$\{\omega_i:\omega_i\in\mathbb{Z}_p,i\in I\}$使得 $\sum_{i\in I}\omega_i\boldsymbol{M}_i=(1,0,\ldots,0)$,从而有:

$$\sum_{i\in I}\omega_i\boldsymbol{M}_i\boldsymbol{v}^T=\sum_{i\in I}(\omega_i\boldsymbol{M}_i)\boldsymbol{v}^T=x;$$

而对于非授权用户集,存在行向量 $\boldsymbol{\omega}\in\mathbb{Z}_p^n$ 使得$\boldsymbol{\omega}(1,0,\ldots,0)^T=-1$,并且 $\boldsymbol{\omega}\boldsymbol{M}_i^T=0,i\in I$.

定义 4(DBDH 假设). 给定阶为大素数 p 的群 G 和 G_1 以及双线性映射 $e:G\times G\to G_1$,群 G 上的 DBDH 问题是指:给定 $g,W=g^w,V=g^v,Z=g^z,R\in G$,判断 $R=e(g,g)^{wvz}$ 是否成立.定义一个算法$\mathcal{S}$解决 DBDH 问题的优势为

$$|\Pr[\mathcal{S}(g,W,V,Z,e(g,g)^{wvz})=0]-\Pr[\mathcal{S}(g,W,V,Z,R)=0]|;$$

而 DBDH 假设成立是指:对任意一个多项式时间算法$\mathcal{S}$,其解决 DBDH 问题的优势是可忽略的.

1.2 Waters ABE方案

本节介绍 Waters[6]提出的一个在标准模型下可证安全的 ABE 方案,该方案包含以下 4 种算法:

- *Setup*$(T,n_{\max})$.

对于属性域规模参数 T 和 LSSS 矩阵的最大列数 $n_{\max}$,选择一个阶为大素数 p 的群 G 和 G_1 以及双线性映射 $e:G\times G\to G_1$,记 g 为 G 的一个生成元.随机选取 $h_{j,att}\in G,1\leqslant j\leqslant n_{\max},1\leqslant att\leqslant T$.随机选取$\alpha,a\in\mathbb{Z}_p$,设置系统主公钥 MPK 为 $g,e(g,g)^{\alpha},g^a$,系统主密钥 MSK 为 g^{α}.

- *KeyGen*(MSK,S_U).

对于一个用户属性集 S_U,选择随机数 $t_1,\ldots,t_{n_{\max}}\in\mathbb{Z}_p$, 生成如下用户私钥 SK_U:

$$K_U=g^{\alpha}g^{at_1};L_{U_j}=g^{t_j},j=1,\ldots,n_{\max};K_{U_{att}}=\prod\nolimits_{j=1,\ldots,n_{\max}}h_{j,att}^{t_j},\forall att\in S_U.$$

- *Encrypt*$(MPK,(\boldsymbol{M},\rho),m)$.

$(\boldsymbol{M},\rho)$是表示访问结构的 LSSS,其中,$\boldsymbol{M}$ 是一个 $l\times n_{\max}$ 的矩阵.随机选择一个向量 $\boldsymbol{v}=(x,v_2,\ldots,v_{n_{\max}})\in\mathbb{Z}_p^{n_{\max}}$, 密文 CT 计算如下:

$$C=me(g,g)^{\alpha x};C'=g^x;C_{i,j}=g^{aM_{i,j}v_j}h_{j,\rho(i)}^{-x},1\leqslant i\leqslant l,1\leqslant j\leqslant n_{\max},$$

$(\boldsymbol{M},\rho)$与密文 CT 一起发送.

- *Decrypt*(CT,SK_U).

假设 S_U 满足($\boldsymbol{M}$,ρ)对应的访问结构,记 $I\subseteq\{1,\ldots,l\}=\{i:\rho(i)\in S_U\}$,则存在一组常数集$\{\omega_i:\omega_i\in\mathbb{Z}_p,i\in I\}$使得$\sum_{i\in I}\omega_i\boldsymbol{M}_i=(1,0,...,0)$,然后计算:

$$e(C',K_U)\Big/\prod_{j=1,\ldots,n_{\max}}e(L_{U_j},\prod_{i\in I}C_{i,j}^{\omega_i})\prod_{i\in I}e(K_{U_{\rho(i)}}^{\omega_i},C')=e(g,g)^{\alpha x},m=C/e(g,g)^{\alpha x}.$$

1.3 扩展的BJM模型

为分析基于身份 AKE 协议的安全性,Chen[8]等学者对 BJM 模型[11]进行了扩展,定义了 ID-BJM 模型.本节对 ID-BJM 模型进行修改,使其能够适应于 ABAKE 协议的安全性分析.称修改后的 BJM 模型为 AB-BJM 模型.

AB-BJM 模型包含一个协议参与者集合 P 和一个主动攻击者$\mathcal{M}$,协议的每个参与者被形式化为预言机.协议的一次运行称为一个会话,并定义 $\Pi_{A,B}^s$ 和 $\Pi_{B,A}^s$ 为第 s 个会话的参与方,其中,A 和 B 表示系统中的用户,并具有属性集 S_A 和 S_B 以及相应的属性私钥 SK_A 和 SK_B.另外,每个协议参与方 $\Pi_{A,B}^s$ 都推导了一个认证策略 $\mathcal{T}_{A,B}^s$ (即 ABE 机制中的访问结构).攻击者$\mathcal{M}$被模型化为概率多项式时间的图灵机,并具有执行 *Send*,*Corrupt* 和¬¬*Reveal* 询问请求的能力.

定义 5(匹配会话). 如果某个协议参与者 $\Pi_{A,B}^s$ 发出的每条消息都被相继传送到另外一个协议参与者 $\Pi_{B,A}^r$,并且 $\Pi_{B,A}^r$ 的应答消息被传回到 $\Pi_{A,B}^s$,作为其会话脚本记录相应的下一条消息,则称这两个协议参与者之间拥有了匹配会话.

在 AB-BJM 模型中,通过定义一个挑战者$\mathcal{C}$和攻击者$\mathcal{M}$之间的安全性游戏来定义 ABAKE 协议的安全性.该游戏分为两个阶段:

在第 1 阶段中,攻击者自适应地进行下述询问请求:

- *Send*($\Pi_{A,B}^s$,m) :攻击者通过该请求初始化一个会话或者向会话参与者发送消息.协议参与者 $\Pi_{A,B}^s$ 接受到消息 m 后按照协议规范执行该协议并输出消息 m',或者输出一个符号表示接受或者拒绝该会话,并将每个收到和发出的消息都记入其会话脚本中.若输入消息 m 是系统安全参数,则 $\Pi_{A,B}^s$ 为会话的发起者;否则, $\Pi_{A,B}^s$ 担任响应者角色;
- *Corrupt*(S_U):攻击者通过该询问获得系统中具有属性集 S_U 的用户 U 的长期私钥 SK_U.接受过 *Corrupt* 询问的用户的状态被称为"已腐化";
- *Reveal*($\Pi_{A,B}^s$) :攻击者通过该询问获取会话密钥.若协议参与者 $\Pi_{A,B}^s$ 的状态是"已接受",则输出该参与方的会话密钥;否则,返回一个符号⊥表示终止.接受了 *Reveal* 询问的协议参与者状态是打开的.

在游戏的某一时刻,$\mathcal{M}$向一个新鲜的协议参与者 $\Pi_{A,B}^s$ 进行一次 *Test* 询问,获得该询问的输出消息.其中,新鲜性和 *Test*($\Pi_{A,B}^s$) 定义如下:

定义 6(新鲜参与者). 一个协议参与者 $\Pi_{A,B}^s$ 被称为是新鲜的,是指以下条件同时成立:

(1) $\Pi_{A,B}^s$ 处于"已接受"状态;

(2) $\Pi_{A,B}^s$ 未被打开,即没有接受 *Reveal* 询问;

(3) 对满足 $S_U\in\mathcal{T}_{A,B}^s$ 的任何用户 U,攻击者没有进行 *Corrupt*(S_U)询问;

(4) 与 $\Pi_{B,A}^s$ 拥有匹配会话的协议参与者 $\Pi_{B,A}^r$(如果存在的话)未被打开.

定义 *Test*($\Pi_{A,B}^s$). 若 $\Pi_{A,B}^s$ 是新鲜的,则挑战者通过随机选取 $b\in\{0,1\}$来回答该询问:

- 若 b=0,则输出协议参与者 $\Pi_{A,B}^s$ 的会话密钥;
- 否则,输出一个在密钥空间中随机选取的与会话密钥等长的串.

在游戏的第 2 阶段,攻击者可以继续自适应地执行第 1 阶段中的 3 种询问请求,但不能对已经接受过 *Test*

询问的协议参与者 $\prod_{A,B}^{s}$ 或者与其拥有匹配会话的协议参与者 $\prod_{B,A}^{r}$(如果存在的话)进行 *Reveal* 询问,也不能对满足 $S_U \in \mathcal{T}_{A,B}^{s}$ 的任何用户 U 进行 *Corrupt* 询问.

最后,攻击者$\mathcal{M}$输出一个比特 b'作为对 b 的猜测.若 $b'=b$,则称$\mathcal{M}$赢得了该安全性游戏.定义攻击者$\mathcal{M}$的猜测优势为

$$Adv^{\mathcal{M}}(\lambda)=|\Pr[b'=b]-1/2|,$$

其中,λ是安全参数.

定义 7(AB-BJM 安全性). 一个 ABAKE 协议在 AB-BJM 模型下是安全的,是指下述条件同时成立:

(1) 在只有被动攻击者的情况下,拥有匹配会话的协议参与者 $\prod_{A,B}^{s}$ 和 $\prod_{B,A}^{r}$ 在接受状态时共享相同的会话密钥,且均匀分布在密钥空间$\{0,1\}^k$上;

(2) 对任意概率多项式时间的攻击者$\mathcal{M}$, $Adv^{\mathcal{M}}(\lambda)$ 是可忽略的.

1.4 安全属性

类似于基于身份的 AKE 协议,ABAKE 协议也需要满足以下几个基本安全属性:

(1) 已知会话密钥安全性:这是指攻击者不能从已经泄露的会话密钥中得到其他会话密钥的信息;

(2) 抗未知密钥共享攻击:这是指协议参与者没有与攻击者共享会话密钥;

(3) 前向安全:这是指协议参与方中的一方或者多方的长期私钥泄露不影响之前已经建立的会话密钥的安全性.基本的前向安全性,是指协议参与方中一方的长期私钥泄露不影响之前建立的会话密钥的安全性;完善的前向安全性,是指协议参与双方的长期私钥都泄露后,之前已经建立的会话密钥仍是安全的;主密钥前向安全性,是指在系统主密钥泄露之后,之前建立的会话密钥仍是安全的;

(4) 抗密钥泄露后的假冒攻击:这是指当协议参与者的长期私钥泄露后,攻击者可以假冒该参与者,但不能假冒其他协议参与者;

(5) 会话密钥托管:这是指可信第三方通过监控协议参与者的通信过程,就可以根据捕获的消息恢复出会话密钥.协议是否应该具有会话密钥托管性质,取决于具体的应用环境.例如:某些应用环境的安全性要求较高,要求可信第三方能够对所有会话过程进行监控;有些应用环境注重用户隐私,则需要防止会话密钥被可信第三方恢复.

在AB-BJM模型中,攻击者具有获取用户私钥、获取会话密钥和修改协议交互消息的能力,因此,在AB-BJM模型下安全的 AB-AKE 协议能够抵抗密钥泄露伪装攻击、未知密钥共享攻击,并满足已知会话密钥安全,同时还具有基本的前向安全性.

2 协议描述

本节将 MTI 协议族"加密-解密"的设计思想应用于 ABAKE 协议,给出本文的第 1 个在标准模型下可证安全的 ABAKE 协议(简称为 ABAKE1).该协议通过将 Waters ABE 方案嵌入到其中,使得协议双方的属性集在分别满足彼此的认证策略时,能够用自己的属性私钥以类似于解密的方式从对方发送的消息中得到秘密信息,进而利用该秘密信息计算出相同的会话密钥.ABAKE1 协议包括系统建立、私钥生成和密钥交换这 3 个阶段,具体构造描述如下.

- 系统建立.

选择一个阶为大素数 p 的乘法循环群 G 和一个从 G 到 G_1 的有效双线性映射 $e:G\times G\to G_1$.随机选择$\alpha,a\in\mathbb{Z}_p$,并记 g 为 G 的生成元.对于 LSSS 矩阵最大列数 $n_{\max}$ 和系统属性域规模参数 T,随机选取 $h_{j,att}\in G, 1\leqslant j\leqslant n_{\max}, 1\leqslant att\leqslant T$.选择安全的 Hash 函数 $H:\{0,1\}^*\to\{0,1\}^k$ 作为会话密钥生成函数.系统的主密钥为 g^{α},公开参数为

$$\{\{h_{j,att}, 1\leqslant j\leqslant n_{\max}, 1\leqslant att\leqslant T\}, g, e(g,g)^{\alpha}, g^{a}, H, G\}.$$

- 私钥生成.

在该系统中,每个用户 U 都具有一个属性集 S_U,系统根据用户属性集为每个用户按照如下方法构造私钥:

$$SK_U=\left\{K_U=g^{\alpha}g^{at_1},\{L_{U_j}=g^{t_j},1\leqslant j\leqslant n_{\max}\},\left\{K_{U_{att}}=\prod_{j=1,...,n_{\max}}h_{j,att}^{t_j},att\in S_U\right\}\right\},$$

其中, $\boldsymbol{t}=(t_1,t_2,...,t_{n_{\max}})\in\mathbb{Z}_p^{n_{\max}}$ 是系统随机选取的向量.

- 密钥交换.

假设协议的参与方为 A 和 B,他们分别具有属性集 S_A 和 S_B,相应的私钥分别为 SK_A 和 SK_B.密钥交换阶段中的消息交互过程如图 2 所示,具体描述如下:

1. A 推导一个 B 的属性集 S_B 所能满足的访问结构 $((\boldsymbol{M}_A)_{l_A\times n_{\max}},\rho_A)$. A 随机选取 $\boldsymbol{x}=(x_1,x_2,...,x_{n_{\max}})\in\mathbb{Z}_p^{n_{\max}}$, 计算 $X=g^{x_1},m_A=\{X_{i,j}=g^{a\cdot x_j\cdot M_{A_{i,j}}}h_{j,\rho_A(i)}^{-x_1},1\leqslant i\leqslant l_A,1\leqslant j\leqslant n_{\max}\}$. A 将 $T_A=\{X,m_A\}$和 $((\boldsymbol{M}_A)_{l_A\times n_{\max}},\rho_A)$ 发送给 B;
2. B 推导一个 A 的属性集 S_A 所能满足的访问结构 $((\boldsymbol{M}_B)_{l_B\times n_{\max}},\rho_B)$. B 随机选取 $\boldsymbol{y}=(y_1,y_2,...,y_{n_{\max}})\in\mathbb{Z}_p^{n_{\max}}$, 计算 $Y=g^{x_1},m_B=(Y_{i,j}=g^{ay_jM_{B_{i,j}}}h_{j,\rho_B(i)}^{-y_1},1\leqslant i\leqslant l_A,1\leqslant j\leqslant n_{\max})$. B 将 $T_B=\{Y,m_B\}$和 $((\boldsymbol{M}_B)_{l_B\times n_{\max}},\rho_B)$ 发送给 A;
3. A 利用 $((\boldsymbol{M}_B)_{l_B\times n_{\max}},\rho_B)$ 计算一组常数$\{\omega_i:\omega_i\in\mathbb{Z}_p,\rho_B(i)\in S_A\}$,使得 $\sum_{\rho_B(i)\in S_A}\omega_i\cdot\boldsymbol{M}_{B_i}=(1,0,...,0)$,然后计算共享秘密:

$$k_{AB}=(e(g,g)^{\alpha})^{x_1}\cdot e(Y_1,K_A)\Big/\left(\prod_{j=1,...,n_{\max}}e\left(\prod_{\rho_B(i)\in S_A}Y_{i,j}^{\omega_i},L_{A_j}\right)\right)\prod_{\rho_B(i)\in S_A}e(Y_1,K_{A_{\rho_B(i)}}^{\omega_i})=e(g,g)^{\alpha(x_1+y_1)}.$$

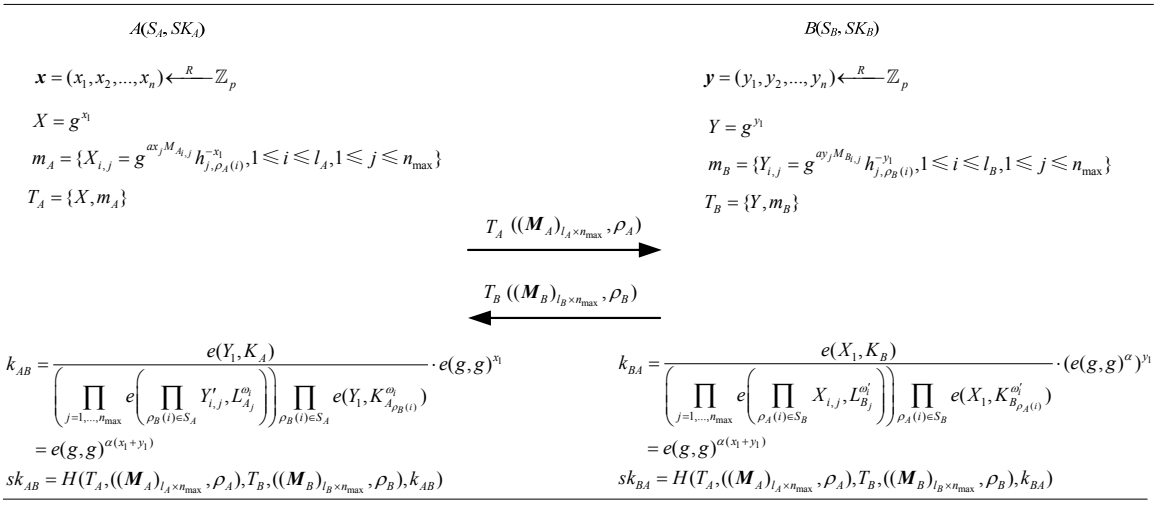


Fig.2 ABAKE1 protocol

图 2 ABAKE1 协议

A 计算会话密钥 $sk_{AB}=H(T_A,((\boldsymbol{M}_A)_{l_A\times n_{\max}},\rho_A),T_B,((\boldsymbol{M}_B)_{l_b\times n_{\max}},\rho_B),k_{AB})$.

B 同样利用 $((\boldsymbol{M}_A)_{l_A\times n_{\max}},\rho_A)$ 计算一组常数 $\{\omega_i':\omega_i'\in\mathbb{Z}_p,\rho_A(i)\in S_B\}$, 使得 $\sum_{\rho_A(i)\in S_B}\omega_i'\cdot\boldsymbol{M}_{A_i}=(1,0,...,0)$, 然后计算共享秘密:

$$k_{BA}=(e(g,g)^{\alpha})^{y_1}\cdot e(X_1,K_B)\Big/\left(\prod_{j=1,...,n_{\max}}e\left(\prod_{\rho_A(i)\in S_B}X_{i,j}^{\omega_i'},L_{B_j}\right)\right)\prod_{\rho_A(i)\in S_B}e(X_1,K_{A_{\rho_A(i)}}^{\omega_i'})$$
$$=e(g,g)^{\alpha(x_1+y_1)}.$$

B 计算会话密钥 $sk_{BA}=H(T_A,((\boldsymbol{M}_A)_{l_A\times n_{\max}},\rho_A),T_B,((\boldsymbol{M}_B)_{l_B\times n_{\max}},\rho_B),k_{BA})$.

协议正确性分析:代入 A 的私钥并利用双线性映射的性质,容易得到:

$$
\begin{aligned}
&e(Y_1,K_A)\Big/\left(\prod_{j=1,\ldots,n_{\max}} e\left(\prod_{\rho_B(i)\in S_A} Y_{i,j}^{\omega_i},L_{A_j}\right)\cdot\prod_{\rho_B(i)\in S_A} e(Y_1,K_{A_{\rho_B(i)}}^{\omega_i})\right)\\
&=e(g^{y_1},g^{\alpha}g^{a\cdot t_1})\Big/\prod_{j=1,\ldots,n_{\max}} e\left(\prod_{\rho_B(i)\in S_A} g^{a\omega_i y_j M_{B_{i,j}}}h_{j,\rho_B(i)}^{-\omega_i y_1},g^{t_j}\right)\cdot 1\Big/\prod_{\rho_B(i)\in S_A} e\left(g^{y_1},\prod_{j=1,\ldots,n_{\max}} h_{j,\rho_B(i)}^{\omega_i t_j}\right)\\
&=e(g^{y_1},g^{\alpha})e(g^{y_1},g^{at_1})\Big/\left(\prod_{j=1,\ldots,n_{\max}} e(g^{ay_j\sum_{\rho_B(i)\in S_A}\omega_i M_{B_{i,j}}},g^{t_j})e\left(\prod_{\rho_B(i)\in S_A} h_{j,\rho_B(i)}^{-\omega_i y_1},g^{t_j}\right)\right)\cdot 1\Big/\prod_{\rho_B(i)\in S_A} e\left(g^{y_1},\prod_{j=1,\ldots,n_{\max}} h_{j,\rho_B(i)}^{\omega_i t_j}\right)\\
&=e(g,g)^{\alpha y_1}e(g^{y_1},g^{at_1})\Big/\left(e(g^{ay_1},g^{t_1})\cdot\prod_{j=1,\ldots,n_{\max}} e\left(\prod_{\rho_B(i)\in S_A} h_{j,\rho_B(i)}^{-\omega_i y_1 t_j},g\right)\right)\cdot 1\Big/\prod_{\rho_B(i)\in S_A} e\left(g,\prod_{j=1,\ldots,n_{\max}} h_{j,\rho_B(i)}^{\omega_i y_1 t_j}\right)\\
&=e(g,g)^{\alpha y_1}.
\end{aligned}
$$

从而可得 $k_{AB}=e(g,g)^{\alpha x_1}\cdot e(g,g)^{\alpha y_1}=e(g,g)^{\alpha(x_1+y_1)}$;

同理可得 $k_{BA}=e(g,g)^{\alpha y_1}\cdot e(g,g)^{\alpha x_1}=e(g,g)^{\alpha(x_1+y_1)}$,从而有:

$$
\begin{aligned}
sk_{AB}&=H(T_A,((M_A)_{l_A\times n_{\max}},\rho_A),T_B,((M_B)_{l_B\times n_{\max}},\rho_B),k_{AB})\\
&=H(T_A,((M_A)_{l_A\times n_{\max}},\rho_A),T_B,((M_B)_{l_B\times n_{\max}},\rho_B),k_{BA})\\
&=sk_{BA}.
\end{aligned}
$$

因此,用户 A 与 B 独立计算的两个会话密钥 sk_{AB} 与 sk_{BA} 相同,这也就说明 A 与 B 通过执行一次协议,成功地协商出了相同的会话密钥.

3 安全性证明

本节在 AB-BJM 模型中证明协议 ABAKE1 是安全的.

定理. 在 DBDH 假设成立的条件下,ABAKE1 协议在 AB-BJM 模型中是安全的.

证明:

- 我们首先说明,协议 ABAKE1 满足定义 7 中的条件(1).

若两个协议参与者按照协议规范执行协议,并且攻击者是被动的,则两个协议参与者都能正确地接受到对方的消息,他们之间拥有匹配会话.又根据协议的正确性分析可得 $k_{AB}=k_{BA}$.所以,两个协议参与方最后能够计算出相同的会话密钥,并且均匀地分布于密钥空间上.

- 其次,我们证明协议 ABAKE1 满足定义 7 中的条件(2).

下面我们将证明:若存在多项式时间的攻击者$\mathcal{M}$,能以不可忽略的优势赢得安全性游戏,则我们可以构造一个概率多项式时间的模拟器$\mathcal{S}$,以不可忽略的优势解决 DBDH 问题.

在开始模拟之前,我们假设攻击者最多涉及到N个协议用户,最多建立 q_e 个会话.$\mathcal{S}$选取$J\in(0,q_e)$和两个协议用户 A,B,并猜测攻击者将会对协议参与者 $\Pi_{A,B}^{J}$ 进行 *Test* 询问.模拟器$\mathcal{S}$接收到DBDH挑战$(G,G_1,g,p,W=g^w,V=g^v,Z=g^z,R)$,以及由攻击者提供的挑战认证策略 $\mathcal{T}_{A,B}^{*}$ 和 $\mathcal{T}_{B,A}^{*}$,用 LSSS 分别表示为 $(\boldsymbol{M}_A^{*},\rho_A^{*})$ 和 $(\boldsymbol{M}_B^{*},\rho_B^{*})$,其中, $\boldsymbol{M}_A^{*}$ 是 $l_A^{*}\times n_{\max}$ 矩阵, $\boldsymbol{M}_B^{*}$ 是 $l_B^{*}\times n_{\max}$ 矩阵.在上述假设的基础上,模拟器$\mathcal{S}$的具体构造如下.

初始化. $\mathcal{S}$随机选取$\alpha'\in\mathbb{Z}_p$,令 $e(g,g)^{\alpha}=e(g^w,g^v)\cdot e(g,g)^{\alpha'}$,则$\alpha=wv+\alpha'$.对属性域内的任一属性 $att\in\{1,\ldots,T\}$和 $j\in\{1,2,\ldots,n_{\max}\}$,随机选择 $z_{j,att}\in\mathbb{Z}_p$,若存在 $i\in\{1,2,...,l_A^{*}\}$ 使得 $\rho_A^{*}(i)=att$, 则令 $h_{j,att}=g^{z_{j,att}}W^{M_{A_{i,j}}}=g^{z_{j,att}}g^{wM_{A_{i,j}}}$; 否则,令 $h_{j,att}=g^{z_{j,att}}$.$\mathcal{S}$设置系统私钥为 g^{α},并发送$\{\{h_{j,att},1\leqslant j\leqslant n_{\max},1\leqslant att\leqslant T\},g,e(g,g)^{\alpha},W\}$给攻击者$\mathcal{M}$.

由于 $z_{j,att}$ 是随机选取的,因此,按照上述方法生成的公开参数与真实系统中的公开参数具有相同的分布.

Corrupt(S_U):由于 $S_U\notin\mathcal{T}_{A,B}^{*}$,则根据 LSSS 的定义可得:$\mathcal{S}$可计算一个向量 $\boldsymbol{\omega}=(\omega_1,\omega_2,...,\omega_{n_{\max}})\in\mathbb{Z}_p^{n_{\max}}$,使得对任意$1\leqslant i\leqslant l_A^{*}$,若有 $\rho_A^{*}(i)\in S_U$, 则 $\boldsymbol{\omega}\cdot(\boldsymbol{M}_{A_i}^{*})^{T}=0$, 并且 $w_1=-1$.$\mathcal{S}$选取随机向量 $\boldsymbol{t}=(t_1,t_2,...,t_{n_{\max}})\in\mathbb{Z}_p^{n_{\max}}$,然后计算:

$$K_U = g^{\alpha'} W^{t_1} = g^{\alpha} g^{w(t_1+\omega_1 \cdot v)};$$
$$L_{U_j} = g^{t_j} \cdot V^{w_j} = g^{t_j + v \cdot \omega_j}.$$

- 对任意 $att \in S_U$,若不存在 $1 \leqslant i \leqslant l_A^*$ 使得 $\rho_A^*(i) = att$, 则有:

$$K_{U_{att}} = \prod_{j=1,\ldots,n_{\max}} L_j^{z_{j,att}} = \prod_{j=1,\ldots,n_{\max}} h_{j,att}^{t_j + \omega_j \cdot v},$$

其中, $h_{j,att} = g^{z_{j,att}}$;

- 否则,若存在 $1 \leqslant i \leqslant l_A^*$ 使得 $\rho_A^*(i) = att$, 则有:

$$K_{U_{att}} = \prod_{j=1,\ldots,n_{\max}} g^{z_{j,att} \cdot t_j} \cdot g^{v \cdot z_{j,att}} \cdot g^{w \cdot M^*_{A_{i,j}} \cdot t_j} = \prod_{j=1,\ldots,n_{\max}} h_{j,att}^{t_j + \omega_j v},$$

其中, $h_{j,att} = g^{z_{j,att}} \cdot g^{w M_{A_{i,j}}}$.

最后,模拟器$\mathcal{S}$返回攻击者$\mathcal{M}$相应于属性集 S_U 的私钥:

$$SK_U = \left\{ K_U = g^{\alpha} g^{w(v+\omega_1 \cdot t_1)}, \{L_{U_j} = g^{t_j + v \cdot \omega_j}, 1 \leqslant j \leqslant n_{\max}\}, \left\{ K_{U_{att}} = \prod_{j=1,\ldots,n_{\max}} h_{j,att}^{t_j + v \cdot \omega_j}, att \in S_U \right\} \right\}.$$

若令 $t'_j = t_j + v \cdot \omega_j$,则可以看出$\mathcal{S}$生成用户私钥满足正确的分布,即,$\mathcal{S}$生成的用户私钥对$\mathcal{M}$来说是有效的.

Send$(\Pi^s_{A,B}, m)$:$\mathcal{S}$维护一个最初记录为空的列表 $\mathcal{L}_S = (\Pi^s_{A,B}, \boldsymbol{x}, m, m', k_{AB}, sk_{AB})$ (列表项初始化为(⊥,⊥,⊥,⊥,⊥,⊥)),其中,m 是会话参与者收到的协议消息,$\boldsymbol{x}$ 是$\mathcal{S}$为 $\Pi^s_{A,B}$ 选取的随机向量,m'是 $\Pi^s_{A,B}$ 在接收到消息 m 后产生的消息,k_{AB} 是计算的共享秘密,sk_{AB} 是最后的会话密钥.当$\mathcal{S}$收到消息 m 后,按照如下方法处理.

(1) 若 m 是安全参数,则将 $\Pi^s_{A,B}$ 设置为会话的发起者,分两种情况处理:

- 若 $s=J$,则$\mathcal{S}$随机选取 $x_2, \ldots, x_{n_{\max}} \in \mathbb{Z}_p$,$x_1=0$,记向量 $\boldsymbol{x}^* = (z + x_1, z + x_2, \ldots, z + x_{n_{\max}}) \in \mathbb{Z}_p^{n_{\max}}$, 然后计算:

$$\begin{aligned} X &= g^{x_1^*} = Z; \\ m_A &= \left\{ X_{i,j} = g^{w \cdot x_j^* \cdot M^*_{A_{i,j}}} \cdot h^{-x_1^*}_{j,\rho_A^*(i)}, 1 \leqslant i \leqslant l_A^*, 1 \leqslant j \leqslant n_{\max} \right\} \\ &= \left\{ X_{i,j} = g^{w \cdot (z+x_j) \cdot M_{A_{i,j}}} g^{-z \cdot z_{j,\rho_A^*(i)}} g^{-z \cdot w \cdot M^*_{A_{i,j}}}, 1 \leqslant i \leqslant l_A^*, 1 \leqslant j \leqslant n_{\max} \right\} \\ &= \left\{ X_{i,j} = W^{x_j \cdot M^*_{A_{i,j}}} \cdot Z^{z_{j,\rho_A^*(i)}}, 1 \leqslant i \leqslant l_A^*, 1 \leqslant j \leqslant n_{\max} \right\}; \end{aligned}$$

最后,$\mathcal{S}$记 $m' = (X, m_A, \mathcal{T}^*_{A,B})$, 然后将列表项更新为 $(\Pi^s_{A,B}, \perp, \perp, m', \perp, \perp)$ (由于$\mathcal{S}$不知道 z,故列表中的 $\boldsymbol{x}$ 记为⊥);

- 若 $s \neq J$,则$\mathcal{S}$按正常的协议规范执行,并更新列表$\mathcal{L}_S$.

(2) 若 m 不是安全参数,$\mathcal{S}$查询列表$\mathcal{L}_S$,然后分情况处理:

- 若列表$\mathcal{L}_S$ 中不存在记录 $(\Pi^s_{A,B}, \boldsymbol{x}, m, m', k_{AB}, sk_{AB})$, 则将 $\Pi^s_{A,B}$ 设置为会话的响应者,然后按照协议规范选取随机向量 $\boldsymbol{x}$,计算 m',k_{AB} 和 sk_{AB},并更新列表$\mathcal{L}_S$;
- 若列表$\mathcal{L}_S$ 中存在记录 $(\Pi^s_{A,B}, \boldsymbol{x}, \perp, m', \perp, \perp)$, 则此时 $\Pi^s_{A,B}$ 是一个会话的发起者,$\mathcal{S}$按照协议规范计算 k_{AB} 和 sk_{AB},然后将列表项更新为 $(\Pi^s_{A,B}, \boldsymbol{x}, m, m', k_{AB}, sk_{AB})$;
- 若列表中$\mathcal{L}_S$ 存在记录 $(\Pi^s_{A,B}, \perp, \perp, m', \perp, \perp)$, 则此时 $\Pi^s_{A,B}$ 就是$\mathcal{S}$在初始阶段所猜测的协议参与者.假设 $m = (Y = g^{y_1}, m_B, \mathcal{T}_{B,A})$, $\mathcal{S}$可计算出 $e(g,g)^{\alpha y_1}$,然后令 k_{AB}=$R \cdot e(Z, g^{\alpha'})$,$sk_{AB}$=$H(m', m, k_{AB})$,并更新列表.可以看出:若 R=$e(g,g)^{wvz}$,则 sk_{AB} 就是一个有效的会话密钥;否则,sk_{AB} 就是一个取自密钥空间的随机值.

Reveal$(\Pi^s_{A,B})$: 若 $\Pi^s_{A,B}$ 是$\mathcal{S}$在初始化阶段所猜测的协议参与者,或者是与其拥有匹配会话的协议参与者(如果存在的话),则$\mathcal{S}$终止模拟;否则,$\mathcal{S}$通过查询列表$\mathcal{L}_S$ 返回相应值.

Test($\Pi^s_{A,B}$):在模拟过程中的某个时刻,攻击者选择一个新鲜的协议参与者 $\Pi^s_{A,B}$ 进行 *Test* 询问:

- 若 $\Pi^s_{A,B}$ 不是模拟器$\mathcal{S}$在初始化阶段所猜测的协议参与者,则$\mathcal{S}$终止模拟;
- 否则,$\mathcal{S}$返回会话密钥 $sk_{AB}=H(m',m,k_{AB})$,其中,$k_{AB}=R\cdot e(Z,g^{\alpha})$.

输出:当攻击者完成第 1 阶段的询问后,可以继续进行 Corrupt,Send 和 Reveal 这 3 种询问,但要求不能破坏接受了 *Test* 询问的协议参与者的新鲜性.一旦攻击者决定完成询问,输出一个比特 b'作为对测试协议参与者的会话密钥的猜测.$\mathcal{S}$收到 b'后,则将其作为对 R 的猜测.

分析:可以看出,在整个模拟过程中,模拟器$\mathcal{S}$至少以 $1/(N^2q_s)$的概率不会终止模拟.而在$\mathcal{S}$没有终止模拟的情况下,对攻击者$\mathcal{M}$而言,$\mathcal{S}$所模拟的安全性游戏与真实的安全性游戏是不可区分的.因此,若假设攻击者$\mathcal{M}$在真实的安全性游戏中的猜测优势为ε,则其在$\mathcal{S}$所模拟的安全性游戏中的猜测优势就为$\varepsilon/(N^2q_s)$.

若 $R=e(g,g)^{wvz}$,$\mathcal{S}$所模拟的安全性游戏就是完善的,$\mathcal{M}$猜测 b 的优势就是$\mathcal{S}$判断 R 的优势,即$\varepsilon/(N^2q_s)$;若 R 是随机数,则$\mathcal{M}$猜测 b 的优势为 0,判断 R 的优势同样为 0.因此,我们可得:

$$|\Pr[\mathcal{S}(g,W,V,Z,e(g,g)^{wvz})=0]-\Pr[\mathcal{S}(g,W,V,Z,R)=0]|=\varepsilon/(N^2q_s)-0=\varepsilon/(N^2q_s).$$

通过上述分析可得:若有攻击者能以不可忽略的优势ε赢得安全性游戏,则我们就可以构造一个模拟器$\mathcal{S}$以不可忽略的优势$\varepsilon/(N^2q_s)$解决 DBDH 问题.这与 DBDH 假设矛盾,因此,协议 ABAKE1 满足定义 7 中的条件(2).

综之,协议 ABAKE1 满足定义 7,因此在 AB-BJM 模型中是安全的. □

4 安全性和效率分析

由于协议 ABAKE1 在 AB-BJM 模型中是可证安全的,因此协议 ABAKE1 能够抵抗密钥泄露伪装攻击、未知密钥共享攻击,并满足已知密钥安全,同时还具有基本的前向安全性.

但是,当通信双方的长期私钥都泄露后,攻击者可根据消息记录和用户私钥恢复出 $e(g,g)^{\alpha x_1}$ 和 $e(g,g)^{\alpha y_1}$, 进而恢复出共享秘密值 $e(g,g)^{\alpha x_1}\cdot e(g,g)^{\alpha y_1}=e(g,g)^{\alpha(x_1+y_1)}$ 和会话私钥.另外,在系统主密钥 g^{α}泄露的情况下,攻击者能利用 $X=g^{x_1}$ 和 $Y=g^{y_1}$ 计算出 $k_{AB}=e(g^{\alpha},X)\cdot e(g^{\alpha},Y)=e(g,g)^{\alpha(x_1+y_1)}$, 进而也能恢复出会话密钥.

因此,协议 ABAKE1 不具有完善的前向安全性和主密钥前向安全性,也即具有密钥托管的性质,因此也就只能应用于某些要求可信第三方能够对所有会话过程进行监控的环境中.

下面我们对协议 ABAKE1 进行增强,给出一个具有主密钥前向安全性的 ABAKE 协议(简称 ABAKE2);然后,将本文所提两个 ABAKE 协议与已有的 ABAKE 协议从安全性和计算效率两个方面作一比较.

4.1 无会话密钥托管的ABAKE协议

在本节,我们在协议 ABAKE1 的基础上,通过计算一个额外的 Diffie-Hellman 秘密,给出能够防止会话密钥托管的 ABAKE 协议 ABAKE2.

协议 ABAKE2 同样包含系统建立、私钥生成和密钥交换这 3 个阶段,其中,系统建立和私钥生成阶段与协议 ABAKE1 完全相同.协议 ABAKE2 的具体流程如下:

1. 与协议 ABAKE1 完全相同;
2. 与协议 ABAKE1 完全相同;
3. A 利用 $((\boldsymbol{M}_B)_{l_B\times n_{\max}},\rho_B)$ 计算一组常数$\{\omega_i:\omega_i\in\mathbb{Z}_p,\rho_B(i)\in S_A\}$,使得 $\sum_{\rho_B(i)\in S_A}\omega_i\cdot\boldsymbol{M}_{B_i}=(1,0,...,0)$, 然后计算共享秘密:

$$\begin{aligned}k_{AB}&=(e(g,g)^{\alpha})^{x_1}\cdot e(Y_1,K_A)\Bigg/\left(\prod_{j=1,...,n_{\max}}e\left(\prod_{\rho_B(i)\in S_A}Y_{i,j}^{\omega_i},L_{A_j}\right)\right)\prod_{\rho_B(i)\in S_A}e(Y_1,K_{A_{\rho_B(i)}}^{\omega_i})\\&=e(g,g)^{\alpha(x_1+y_1)};\\k'_{A,B}&=Y^{x_1}=g^{x_1\cdot y_1}.\end{aligned}$$

A 计算会话密钥 $sk_{AB}=H(T_A,((\boldsymbol{M}_A)_{l_A\times n_{\max}},\rho_A),T_B,((\boldsymbol{M}_B)_{l_B\times n_{\max}},\rho_B),k_{AB},k'_{AB})$.

B 同样利用 $((\boldsymbol{M}_A)_{l_A\times n_{\max}},\rho_A)$ 计算一组常数 $\{\omega_i':\omega_i'\in\mathbb{Z}_p,\rho_B(i)\in S_A\}$, 使得 $\sum_{\rho_A(i)\in S_B}\omega_i'\cdot\boldsymbol{M}_{A_i}=(1,0,...,0)$, 然后计算共享秘密:

$$k_{BA}=(e(g,g)^{\alpha})^{y_1}\cdot e(X_1,K_B)\Bigg/\left(\prod_{j=1,...,n_{\max}}e\left(\prod_{\rho_A(i)\in S_B}X_{i,j}^{\omega_i'},L_{B_j}\right)\right)\prod_{\rho_A(i)\in S_B}e(X_1,K_{A_{\rho_A(i)}}^{\omega_i'})$$

$$=e(g,g)^{\alpha(x_1+y_1)};$$

$$k'_{B,A}=X^{y_1}=g^{x_1\cdot y_1}.$$

B 计算会话密钥 $sk_{BA}=H(T_A,((\boldsymbol{M}_A)_{l_A\times n_{\max}},\rho_A),T_B,((\boldsymbol{M}_B)_{l_b\times n_{\max}},\rho_B),k_{BA},k'_{BA})$.

协议 ABAKE2 与协议 ABAKE1 的不同之处在于:在最终的会话密钥生成过程中,协议 ABAKE2 增加了一个额外的 Diffie-Hellman 共享秘密 k'_{AB} 和 $k'_{B,A}$.在这种情况下,即使系统主密钥泄露,由于 x_1 和 y_1 是由协议参与者选取的,因此攻击者无法计算 k'_{AB} 和 $k'_{B,A}$,也就无法恢复会话密钥.所以,协议 ABAKE2 具有主密钥前向安全性,当然也就具有完善的前向安全性.而 ABAKE2 协议的主密钥前向安全性导致其不具有会话密钥托管的性质,因此能够应用于一些注重用户隐私的应用环境,防止会话密钥被可信第三方恢复.

类似于 ABAKE1 协议的安全性证明,我们对第 1.3 节的 AB-BJM 模型稍加修改后,即攻击者能够通过一个 *Corrupt* 询问请求得到系统主密钥,同样能在 DBDH 假设下给出协议 ABAKE2 的安全性证明.

4.2 安全性和效率比较

到目前为止,有关 ABAKE 协议的研究并不多.在本节,我们挑选两个典型的 ABAKE 协议,与本文所提的两个协议从安全性和计算效率上进行比较.

在比较协议安全性时,我们用 ksk 表示已知会话密钥攻击,fs-b 表示基本的前向安全性,fs-p 表示完善的前向安全性,fs-m 表示主密钥前向安全性,uks 表示未知密钥共享攻击,kci 表示密钥泄露伪装攻击.从表 1 中可以看出,只有本文所提协议是在标准模型下可证安全的.与 Wang[4]的协议相比,我们的协议实现了真正意义上的属性认证,并能够表达丰富的认证策略;与 Yoneyama[5]的协议相比,我们的协议具有较弱的安全性假设,易于在实际中应用.

Table 1 Comparisons of ABAKE protocols on security

表 1 ABAKE 协议安全性比较

协议	安全属性						安全模型	安全性假设	认证策略
	ksk	fs-b	fs-p	fs-m	uks	kci			
Wang[4]	√	√	×	×	√	√	RO	BDH	×
Yoneyama[5]	√	√	√	√	√	√	RO	GBDH	LSSS
ABAKE1	√	√	×	×	√	√	Standard	DBDH	LSSS
ABAKE2	√	√	√	√	√	√	Standard	DBDH	LSSS

在比较协议计算效率时,用 P 表示双线性对运算,E 和 C 分别表示群 G 中的指数运算和元素的比特长度,T 和 C_1 分别表示群 G_1 中的指数运算元素的比特长度,C_T 表示一个 LSSS 矩阵的比特长度,CT 表示用户发送的消息的比特长度,SK 表示用户的属性私钥的比特长度,PK 表示系统公钥的比特长度,k 表示用户的属性集规模,t 表示系统的属性域规模,$l\times n$ 表示 LSSS 矩阵规模(l 也是 LSSS 矩阵中出现的属性数目),$n_{\max}$ 表示系统所允许的 LSSS 矩阵的最大列数,统计内容为协议成功运行一次的单方运算消耗和存储消耗.从表 2 中可以看出,我们的协议在时间复杂度上与 Yoneyama[5]的协议基本相同.而 Wang 等人[4]的协议由于没有实现属性认证,因而计算效率较高.相比于 ABAKE1 协议,ABAKE2 协议由于不具有会话密钥托管的性质,因而也就多了一次额外的指数运算.在空间复杂度方面,Wang 等人[4]的协议由于功能上有所欠缺,其空间复杂度也就最低.而本文所提出的两个 ABAKE 协议空间复杂度完全相同,与 Yoneyama[5]的协议只是在系统公钥的规模上有所区别.可以看出,本文所提协议的空间复杂度与系统参数呈线性关系,完全可以由 PBC(pairing-based cryptography)数据包[12]实现.

Table 2 Comparisons of ABAKE protocols on complexity

表 2 ABAKE 协议复杂度比较

协议	时间复杂度			空间复杂度		
	P	*E*	*T*	*CT*	*SK*	*PK*
Wang[4]	k+2	k+2	1	(1+k)·C	2k·C	3·C
Yoneyama[5]	n+1+k	2(l×n+k)+2	1	(l×n+1)·C	($n_{\max}$+1+k)·C	2·C+C_1
ABAKE1	n+1+k	2(l×n+k)+1	1	(l×n+1)·C	($n_{\max}$+1+k)·C	($n_{\max}$×t+2)·C+C_1
ABAKE2	n+1+k	2(l×n+k)+2	1	(l×n+1)·C	($n_{\max}$+1+k)·C	($n_{\max}$×t+2)·C+C_1

5 总 结

本文在 Waters 的 ABE 方案的基础上,提出了一个在标准模型下可证安全的 ABAEKE 协议,并在 AB-BJM 模型中证明了所提协议在 DBDH 假设下是安全的,使得该协议具有未知密钥共享安全性、已知会话密钥安全性、基本前向安全性等基本安全属性.此外,针对无会话密钥托管的应用需求,我们对基本协议进行了扩展,给出了一个能够有效防止密钥托管的 ABAKE 协议.

References:

[1] Sahai A, Waters B. Fuzzy identity-based encryption. In: Cramer R, ed. Advances in Cryptology-Eurocrypt 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 457–473. [doi: 10.1007/11426639_27]

[2] Su JS, Cao D, Wang XF, Sun YP, Hu QL. Attribute-Based encryption schemes. Ruan Jian Xue Bao/Journal of Software, 2011, 22(6):1299−1315 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3993.htm [doi: 10.3724/SP.J.1001.2011.03993]

[3] Ateniese G, Kirsch J, Blanton M. Secret handshakes with dynamic and fuzzy matching. In: Arbaugh W, ed. Proc. of the NDSS 2007. 2007. 159−177.

[4] Wang H, Xu Q, Ban T. A provably secure two-party attribute-based key agreement protocol. In: Sakano H, ed. Proc. of the IIH-MSP 2009. New York: IEEE Computer Society, 2009. 1042−1045. [doi: 10.1109/IIH-MSP.2009.92]

[5] Yoneyama K. Strongly secure two-pass attribute-based authenticated key exchange. In: Joye M, ed. Proc. of the Paring 2010. LNCS 6487, Berlin: Springer-Verlag, 2010. 147−166. [doi: 10.1007/978-3-642-17455-1_10]

[6] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Catalano D, ed. Proc. of the PKC 2011. LNCS 6571, Berlin: Springer-Verlag, 2011. 53−70. [doi: 10.1007/978-3-642-19379-8_4]

[7] Wang SB, Cao ZF, Dong X. Provably secure identity based authenticated key agreement protocols in the standard model. Chinese Journal of Computers, 2007,30(10):1842−1852 (in Chinese with English abstract).

[8] Chen L, Cheng Z, Smart NP. Identity-Based key agreement protocols from pairings. Int'l Journal of Information Security, 2007, 6(4):213−241. [doi: 10.1007/s10207-006-0011-9]

[9] Gao ZG, Feng DG. Efficient identity-based authenticated key agreement protocol in the standard model. Ruan Jian Xue Bao/ Journal of Software, 2011,22(5):1031−1040 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3828.htm [doi: 10.3724/SP.J.1001.2011.03828]

[10] Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Haifa: Israel Institute of Technology, 1996.

[11] Blake S, Johnson C, Menezes A. Key agreement protocols and their security analysis. In: Darnell M, ed. Proc. of the 6th IMA Int'l Conf. on Cryptography and Coding. LNCS 1335, Berlin: Springer-Verlag, 1997. 30–45. [doi: 10.1007/BFb0024447]

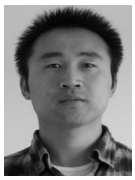
[12] The pairing-based cryptography library. http://crypto.stanford.edu/pbc/

附中文参考文献:

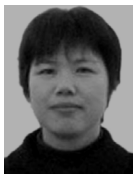
[2] 金树,曹丹,王小峰,孙一品,胡乔林.属性基加密体.软件学报,2011,22(6):1299−1315. http://www.jos.org.cn/1000-9825/3993.htm [doi: 10.3724/SP.J.1001.2011.03993]

[7] 王圣宝,曹珍富,董晓蕾.标准模型下可证安全的身份基认证密钥协商协议.计算机学报,2007,30(10):1842−1852.

[9] 高志刚,冯登国.高效的标准模型下基于身份认证密钥协商协议.软件学报,2011,22(5):1031−1040. http://www.jos.org.cn/1000-9825/3828.htm [doi: 10.3724/SP.J.1001.2011.03828]



魏江宏(1987－),男,甘肃通渭人,博士生,主要研究领域为信息安全.
E-mail: jianghong.wei.xxgc@gmai.com



刘文芬(1965－),女,博士,教授,博士生导师,CCF 会员,主要研究领域为概率统计在通信和密码学中的应用.
E-mail: wenfenliu@sina.com

胡学先(1982－),男,博士,讲师,主要研究领域为信息安全.
E-mail: xuexian@gmail.com