软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(12):3183−3195 [doi: 10.13328/j.cnki.jos.004825]

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

ABeCK 模型下安全的基于属性的认证密钥协商协议*

高海英

(中国人民解放军信息工程大学,河南 郑州 450001)

通讯作者: 高海英, E-mail: ghyyueyue@126.com

摘 要: 基于属性的认证密钥协商(attribute-based authenticated key agreement,简称 ABAKE)协议可在保护身份隐私的通信环境中为用户建立共享的会话密钥,ABeCK(attribute-based extended Canetti-Krawczyk)模型是适用于ABAKE 协议安全性分析的一种安全强度较高的模型.首先在 GCDH(gap computational Diffie-Hellman)假设的基础上提出了 GCPBDHE(gap computational parallel bilinear Diffie-Hellman exponent)假设,然后,基于 Waters 属性基加密方案提出了一个基于属性的认证密钥协商协议,并在 GCPBDHE 假设和 CDH 假设成立的条件下,证明了该方案在ABeCK 模型下是安全的.与现有的 ABeCK 模型下安全的 ABAKE 协议相比,降低了通信开销.

关键词: 基于属性;密钥协商;ABeCK 模型;GCDH 假设;GCPBDHE 假设

中图法分类号: TP309

中文引用格式: 高海英.ABeCK 模型下安全的基于属性的认证密钥协商协议.软件学报,2015,26(12):3183−3195. http://www.jos.org.cn/1000-9825/4825.htm

英文引用格式: Gao HY. Attribute-Based authenticated key agreement protocol secure in ABeCK model. Ruan Jian Xue Bao/ Journal of Software, 2015,26(12):3183−3195 (in Chinese). http://www.jos.org.cn/1000-9825/4825.htm

Attribute-Based Authenticated Key Agreement Protocol Secure in ABeCK Model

GAO Hai-Ying

(The PLA Information Engineering University, Zhengzhou 450001, China)

Abstract: Attribute-based authenticated key agreement (ABAKA) protocol is used to establish session key among parties in the communication environment in which the identity information of individual is protected. Attribute-based extended Canetti-Krawczyk (ABeCK) model is a model with more security applying to the security proof of ABAKE protocol. This paper presents gap computational parallel bilinear Diffie-Hellman exponent (GCPBDHE) assumption based on gap computational Diffie-Hellman (GCDH) assumption. Based on Waters scheme, it establishes an ABAKA protocol, and proves its security in ABeCK model under GCPBDHE and CDH assumptions. Compared with the existing ABAKE protocols, the new protocol is more efficient in communication cost.

Key words: attribute-based; key agreement; ABeCK model; GCDH assumption; GCPBDHE assumption

密钥协商协议是密码学的基本组件之一,利用密钥协商协议,可以在不安全的信道上建立安全信道.所谓认证密钥协商协议,就是通信双方确信对方的真实身份,同时,协议结束后双方确信两者共享了一个只有他们知道的会话密钥.

1984 年,Shamir[1]首次提出了基于身份的加密(identity based encryption,简称 IBE)方案的概念,该方案的特点是用户的公钥是用户的身份信息.2005 年,Sahai 和 Waters[2]提出了基于模糊身份的加密(fuzzy IBE)方案,同时,他们将模糊 IBE 的概念进行推广,提出了基于属性加密(attribute-based encryption,简称 ABE)的概念.ABE 方案将用户属性信息或一个访问控制策略作为用户的身份,同时,密文对应一个访问控制策略或一组属性信息,当且

* 基金项目: 国家自然科学基金(61272488, 61272041, 61202491)
Foundation item: National Natural Science Foundation of China (61272488, 61272041, 61202491)
收稿时间: 2014-03-12; 修改时间: 2014-07-16; 定稿时间: 2015-02-06

仅当属性信息满足相应的访问控制策略时才能正确解密.利用 ABE 方案,可以实现对密文数据的细粒度的访问控制,因此,ABE 方案可用于访问控制、云计算等互联网应用中.基于 ABE 的思想,Wang 等人[3]于 2009 年提出了基于属性的认证密钥协商协议的概念,其目标是使通信双方在公开信道上,无需明确对方身份的情况下,如果两个参与者的属性均满足对方选择的访问控制策略,那么通信双方便能够实现对实体的认证,同时达成一个共同的会话密钥.ABAKA 协议可被用于涉及身份隐私的保密通信环境中,用户希望向对方隐藏自己的身份,同时,对方又需要验证该用户是一个合法用户.通过使用 ABAKA 协议,通信双方能够产生一个安全信道,同时,在保证不泄露身份信息的情况下完成双方的认证.

随着 ABE 方案研究的不断深入,已提出了多个 ABAKA 协议,其中,文献[3–5]分别提出了 BR 模型下可证明安全的 ABAKE 方案.这些方案采用的设计方法是:首先,基于密文策略的 ABE 方案构造出密文策略的基于属性的密钥封装方案,利用密钥封装方案传送协议双方选取的秘密信息,若两个参与者的属性均满足对方选择的访问控制策略,则正确解密出秘密信息;最后,利用密钥抽取算法计算共享会话密钥.目前,ABAKE 协议的安全模型有 BR 模型、CK 模型、ABeCK 模型、CK+模型.在这些安全模型中,攻击者的攻击能力依次增强.Choudary 等人[6]将两方 ABAKA 协议扩展到群 ABAKA 协议,给出了构造群 ABAKA 协议的一般方法,但该方法需要用到一次性数字签名,效率较低.任勇军等人[7]将基于属性的密钥封装方案与密钥抽取算法结合设计了在 CK 模型下可证明安全的 ABAKA 协议.Kazuki Yoneyama[8]基于 Waters 方案[9]提出了在 ABeCK 模型下可证明安全的 ABAKE 方案.魏江宏等人[10]将该协议从单属性机构扩展到多属性机构.李强等人[11]提出了在 CK+模型下可证明安全的 ABAKA 协议.

本文首先在 GCDH 假设的基础上提出 GCPBDHE 假设,然后提出一种效率更高的 ABAKE 方案,在 GCPBDHE 和 CDH 假设同时成立的条件下,证明该方案在 ABeCK 模型下是安全的.与文献[8]中提出的 ABeCK 模型下安全的 ABAKE 协议相比,降低了通信开销,并且在一定参数设置下也降低了计算复杂度.

1 预备知识

1.1 双线性映射

定义 1. 设 G,G_T 都是阶为素数 p 的乘法循环群,g 为 G 的生成元.双线性对 $e:G\times G\to G_T$ 为具有如下性质的映射:

(1) 双线性:对于任意的 $u,v\in G, a,b\in Z_p^*$,满足:$e(u^a,v^b)=e(u,v)^{ab}$;

(2) 非退化性:$e(g,g)\neq 1$,1 是 G_T 的单位元;

(3) 可计算性:对任意的 $u,v\in G$,存在有效的多项式算法计算 $e(u,v)$.

1.2 CDH假设

定义 2. 设 G 是阶为素数 p 的乘法循环群,g 是 G 的生成元,随机选取 $b,c\in Z_p^*$,给定二元组(g^b,g^c),若不存在多项式时间算法以不可忽略的概率计算出 g^{bc},则称 CDH 假设成立.

1.3 DBDH随机预言机

定义 3. 设 G 和 G_T 都是阶为素数 p 的乘法循环群,g 是 G 的生成元,DBDH 随机预言机的输入是$(g^a,g^b$,职$g^c,T)\in G^3\times G_T$,若 $T=e(g,g)^{abc}$,则输出 1;否则输出 0.

1.4 访问结构

定义 4. 设 $P=\{P_1,P_2,\ldots,P_n\}$是参与方构成的集合,一个访问结构 AS 是 2^P 的一个非空集合.称 AS 是单调访问结构,则对于 2^P 的任意两个集合 B,C,若 $B\in AS$,且 $B\subseteq C$,则 $C\in AS$.若集合在访问结构 AS 中,则称为授权集合,否则称为非授权集合.

1.5 线性秘密共享方案

定义 5. 令参与方集合为 $P=\{P_1,P_2,\ldots,P_n\}$,(M,ρ)表示访问结构 AS,其中,M 是 $l\times n$ 的矩阵,ρ是集合$\{1,2,\ldots,l\}$到 P 的映射,即,矩阵 M 中的每一行表示一个参与方.线性秘密共享方案(linear secret sharing schemes,简称 LSSS)包含两个算法:

- 秘密分享算法:设 s 是秘密值.随机选取 $r_2,r_3,\ldots,r_n\in Z_p$,令向量 $v=(s,r_2,r_3,\ldots,r_n)^T$,将$\lambda_i=M_i\cdot v$ 作为参与方$\rho(i)$的秘密分享值,其中,M_i 表示矩阵的第 i 行;
- 秘密重构算法:设参与方的集合为 S.
  - 若 S 为授权集合,即 $S\in AS$,令 $I=\{i:\rho(i)\in S\}$,则存在一个多项式时间算法,计算出系数$\{w_i\}_{i\in I}$,使得 $\sum_{i\in I}w_iM_i=(1,0,\ldots,0)$,即,恢复出秘密值 $\sum_{i\in I}w_i\lambda_i=s$;
  - 对于非授权集合 S,则存在一个多项式时间算法,计算出 n 维向量 $w=(w_1,w_2,\ldots,w_n)^T\in Z_p^n$,使得 $w_1=-1$;且对于 $i\in I$,有 $M_i\cdot w=0$.

2 GPBDHE 假设

基于 DPBDHE 假设[9]和 GBDH 假设[12],本节给出了 GPBDHE 假设,详见定义 6.

定义 6. 设 G 和 G_T 都是阶为素数 p 的乘法循环群,g 是 G 的生成元,随机选取 $a,s,b_1,b_2,\ldots,b_q\in Z_p^*$,给定:

$$Y=\left(\begin{array}{l} g,g^s,g^a,\ldots,g^{(a^q)},g^{(a^{q+2})},\ldots,g^{(a^{2q})},\forall j\in\{1,2,\ldots,q\} \\ g^{s\cdot b_j},g^{a/b_j},\ldots,g^{(a^q/b_j)},g^{(a^{q+2}/b_j)},\ldots,g^{(a^{2q}/b_j)},\forall j,k\in\{1,2,\ldots,q,k\neq j\} \\ g^{(a\cdot s\cdot b_k/b_j)},g^{(a^2\cdot s\cdot b_k/b_j)},\ldots,g^{(a^q\cdot s\cdot b_k/b_j)}) \end{array}\right),$$

并且允许敌手调用定义 3 给出的 DBDH 随机预言机,在该条件下,若不存在多项式时间敌手 A 以不可忽略的概率计算出 $e(g,g)^{a^{q+1}s}$,则称 GPBDHE 假设成立.

定义 6 说明了 GPBDHE 问题是一个可判定问题,但属于不可解问题.而 DPBDHE 假设说明了 DPBDHE 问题是不可判定问题,一个不可判定问题一定是不可解问题,因此,DPBDHE 困难假设比 GPBDHE 困难假设要强.

3 ABeCK 模型介绍

本节介绍适用于 ABAKE 协议安全性分析的扩展 eCK 模型,即 ABeCK 模型[8].

在 ABeCK 模型中,每个协议参与者 P 都具有属性集合 S_P,并且能够并行执行多个会话.

若由 A 发起的一个与 B 之间的会话产生了消息 $m_1,\ldots,m_n$,则该会话被 A 标示为 $sid=(Init,S_A,S_B,m_1,\ldots,m_n)$,被 B 标示为 $sid=(Resp,S_B,S_A,m_1,\ldots,m_n)$.若协议双方生成了相同的会话密钥 K,则称该会话是完成的.一个完成会话$(Init,S_A,S_B,m_1,\ldots,m_n)$的匹配会话是$(Resp,S_B,S_A,m_1,\ldots,m_n)$,反之亦然.

在 ABeCK 模型中,攻击者 A 可以自适应地进行以下询问:

- *Send*(*message*): A 发送消息给某个协议参与方,并根据协议规范得到回答;
- *SessionReveal*(*sid*):若 *sid* 是一个已完成的会话,A 得到 *sid* 的会话密钥,否则,得到一个错误标识;
- *EphemeralReveal*(*sid*): A 得到 *sid* 的临时私钥;
- *StaticReveal*(S_P): A 得到属性集合 S_P 对应的长期私钥 SK_P;
- *MasterReveal*: A 得到系统主私钥 MSK;
- *Establish*(P,S_P): A 以 P 的身份申请到属性集合 S_P 的私钥.若 P 是由攻击者 A 调用 *Establish*(P,S_P)伪造的,则称用户 P 是不诚实用户.

为了定义 ABAKE 协议的安全性,首先给出会话新鲜性的定义.

定义 7. 设一个已完成的会话 $sid^*=(Init,S_A,S_B,m_1,\ldots,m_n)$或$(Resp,S_B,S_A,m_1,\ldots,m_n)$,若存在匹配会话,令匹配会话是 $\overline{sid^*}$.用户 A,B 制定的访问控制策略是 AS_A,AS_B.若以下所有条件均不成立,则称 sid^*是新鲜会话:

- 条件 1:A 查询 $SessionReveal(sid^*)$,或者在 $\overline{sid^*}$ 存在的条件下,查询了 $SessionReveal(\overline{sid^*})$;
- 条件 2: $\overline{sid^*}$ 存在,A 同时查询了 $StaticReveal(S_P)(S_P\in AS_B)$和 $EphemeralReveal(sid^*)$;或者 A 同时查询了 $StaticReveal(S_P)(S_P\in AS_A)$和查询了 $EphemeralReveal(\overline{sid^*})$;
- 条件 3: $\overline{sid^*}$ 不存在,A 同时查询了 $StaticReveal(S_P)(S_P\in AS_B)$和 $EphemeralReveal(sid^*)$;或者 A 查询了 $StaticReveal(S_P)$,其中,$S_P\in AS_A$.

注: A 查询 $MasterReveal$,等价于查询 $StaticReveal(S_P)$,其中,S_P 是任意用户 P 的属性集合.

A 经过一系列查询后,选择一个新鲜会话进行 $Test$ 查询,$Test$ 查询定义如下:

$Test(sid^*)$:sid^*是一个新鲜会话.模拟者接收到 A 申请的 $Test(sid^*)$后,随机选取 1 比特 $b\in\{0,1\}$,若 b=0,返回 sid^*对应的会话密钥;否则,返回一个随机密钥.

A 接收到 $Test$ 查询结果后,输出 b 的猜测结果 b'.A 攻击成功的概率 $\Pr[A\text{ 攻击成功}]=\Pr[b'=b]$.

下面给出 ABeCK 安全性的定义.

定义 8. 若一个 ABAKE 协议满足以下条件:

(1) 若两个诚实用户 A 和 B 完成了匹配会话,并且属性集合 $S_A\in AS_B$,属性集合 $S_B\in AS_A$,协议双方最终协商出相同的会话密钥;

(2) 不存在多项式时间敌手 A,使得$|\Pr[A\text{ 攻击成功}]-1/2|>\varepsilon$,

则称该协议在 ABeCK 模型下是安全的.另外,若在 sid^*中 A 声明了访问结构 AS_A(若 $\overline{sid^*}$ 存在, A 也声明了 AS_B),则称该协议在 ABeCK 模型下是选择安全的.

4 ABeCK 安全的 ABAKE 协议

4.1 协议描述

(1) 系统建立

选取阶为素数 p 的群 G 和 G_T 以及 G 的生成元 g,随机选取 U 个元素 $h_1,h_2,\ldots,h_U\in G$,其中,U 是系统用户属性集合的个数,第 $i(1\leqslant i\leqslant U)$个属性对应元素 h_i.随机选取$\alpha,a\in Z_p$,安全杂凑函数 $H_1:\{0,1\}^*\to Z_p$,$H:\{0,1\}^*\to\{0,1\}^k$.令 $g_T=e(g,g)$,设置系统公钥 $MPK=(g,g_T,g_T^{\alpha},g^a,h_1,\ldots,h_U)$,系统主私钥 $MSK=g^{\alpha}$.

(2) 私钥生成

令用户 P 的属性集合为 S_P,私钥产生中心随机选取 $t_P\in Z_p$,计算:

$$K_P=g^{\alpha}g^{a\cdot t_P},L_P=g^{t_P},\{\forall x\in S_P,K_{P,x}=h_x^{t_P}\}.$$

用户 P 对应的私钥 $SK_P=(K_P,L_P,\{K_{P,x},\forall x\in S_P\})$.

(3) 密钥协商

假设用户 A 是协议的发起方,B 是接收方.A 的属性集是 S_A,对应私钥 $SK_A=(K_A,L_A,\{K_{A,x},\forall x\in S_A\})$;$B$ 的属性集是 S_B,对应私钥 $SK_B=(K_B,L_B,\{K_{B,x},\forall x\in S_B\})$.$A$ 与 B 进行密钥协商的主要过程是:首先,A 选取访问结构 AS_A,生成消息 EPK_A,将 EPK_A 发送给 B;然后,B 选取访问结构 AS_B,生成消息 EPK_B,将 EPK_B 发送给 A;最后,若 S_A 满足访问结构 AS_B,S_B 满足访问结构 AS_A,则 A 和 B 可计算出共享密钥 K.具体过程如下:

Step 1. A 选取访问结构 AS_A,AS_A 对应的 LSSS 矩阵记为 M_A,M_A 的规模是 $l_A\times n_A$,M_A 的行向量与属性之间的一一对应关系记为ρ_A.

A 随机选取 $er_0,er_1,\ldots,er_{l_A},ex_2,ex_3,\ldots,ex_{n_A}\in Z_p$,计算:

$$s_A=H_1(K_A,L_A,\{K_{A,j},\forall j\in S_A\},er_0),$$
$$r_i=H_1(K_A,L_A,\{K_{A,j},\forall j\in S_A\},er_i),1\leqslant i\leqslant l_A,$$
$$x_k=H_1(K_A,L_A,\{K_{A,j},\forall j\in S_A\},ex_k),2\leqslant k\leqslant n_A.$$

令向量 $v=(s_A,x_2,x_3,\ldots,x_{n_A})\in(Z_p)^{n_A}$,计算$\lambda_i=v\cdot M_A(i)$,其中,$M_A(i)$是 M_A 的第 i 行,i=1,…,l_A.

令 $er_0,er_1,...,er_{l_A},ex_2,ex_3,...,ex_{n_A}$ 是 A 的临时私钥,A 计算:

$$X=g^{s_A},(U_i=g^{a\lambda_i}h_{\rho_A(i)}^{-r_i},D_i=g^{r_i}),1\leqslant i\leqslant l_A(\text{令集合}\{U,D\}=\{(U_i,D_i),1\leqslant i\leqslant l_A\}).$$

A 发送消息 $EPK_A=(X,\{U,D\},M_A,\rho_A)$给 B.

Step 2. B 接收到 A 发送的消息 EPK_A 后,判断自己的属性集合 S_B 是否满足访问结构(M_A,ρ_A):若不满足,协议终止;若 S_B 满足访问结构(M_A,ρ_A),B 选取访问结构 AS_B,AS_B 对应的 LSSS 矩阵记为 M_B,M_B 的规模是 $l_B\times n_B$,M_B 的行向量与属性之间的一一对应关系记为ρ_B.

B 随机选取 $er_0',er_1',...,er_{l_B}',ex_2',ex_3',...,ex_{n_B}'\in Z_p$,计算:

$$s_B=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},er_0'),$$
$$r_i'=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},er_i'),1\leqslant i\leqslant l_B,$$
$$x_k'=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},ex_k'),2\leqslant k\leqslant n_B.$$

令 $v'=(s_B,x_2',x_3',...,x_{n_B}')\in(Z_p)^{n_B}$,计算 $\lambda_i'=v'\cdot M_B(i)$,其中,$M_B(i)$是矩阵 M_B 的第 i 行,i=1,…,l_B.

令 $er_0',er_1',...,er_{l_B}',ex_2',ex_3',...,ex_{n_B}'$ 是 B 的临时私钥,B 计算:

$$Y=g^{s_B},(V_i=g^{a\lambda_i'}h_{\rho_B(i)}^{-r_i'},E_i=g^{r_i'}),1\leqslant i\leqslant l_B(\text{令集合}\{V,E\}=\{(V_i,E_i),1\leqslant i\leqslant l_B\}).$$

B 发送消息 $EPK_B=(Y,\{V,E\},M_B,\rho_B)$给 A.

Step 3. A 接收到EPK_B后,判定属性集合 S_A 是否满足访问结构(M_B,ρ_B),若不满足,协议终止;否则,按照以下方式计算共享密钥:

令 $I_A=\{i:\rho_B(i)\in S_A\}$,计算 $\{w_A(i)\in Z_p\}_{i\in I_A}$,使得 $\sum_{i=1}^{l_B}w_A(i)\cdot M_B(i)=(1,0,0,...,0)$, $M_B(i)$是矩阵 M_B 的第 i 行,i=1,…,l_B.

计算:

$$\sigma_1=(g_T^{\alpha})^{s_A},$$
$$\sigma_2=e(Y,K_A)\Big/\left(\left(\prod_{i\in I_A}e(V_i,L_A)e(E_i,K_{A,\rho_B(i)})\right)^{w_A(i)}\right),$$
$$\sigma_3=Y^{s_A}.$$

最后,计算出共享密钥 $K_{AB}=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$.

B 收到 EPK_A,并且在 Step 2 中已经判断出自己的属性集合 S_B 满足访问结构(M_A,ρ_A),则 B 按如下方式计算共享密钥.

令 $I_B=\{i:\rho_A(i)\in S_B\}$,计算 $\{w_B(i)\in Z_p\}_{i\in I_B}$,使得 $\sum_{i=1}^{l_A}w_B(i)\cdot M_A(i)=(1,0,0,...,0)$, $M_A(i)$是矩阵 M_A 的第 i 行,i=1,…,l_A.

计算:

$$\sigma_1=e(X,K_B)\Big/\left(\prod_{i\in I_B}(e(U_i,L_B)e(D_i,K_{B,\rho_A(i)}))^{w_B(i)}\right),$$
$$\sigma_2=(g_T^{\alpha})^{s_B},$$
$$\sigma_3=X^{s_B}.$$

最后,计算出共享密钥 $K_{BA}=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$.

4.2 协议的正确性

根据双线性对的性质,A 计算:

$$\sigma_1=(g_T^{\alpha})^{s_A},$$

$$\sigma_2=e(Y,K_A)\Big/\left(\prod_{i\in I_A}(e(V_i,L_A)e(E_i,K_{A,\rho_B(i)}))^{w_A(i)}\right)$$

$$=e(g^{s_B},g^{\alpha})e(g^{s_B},g^{at_A})\Big/\left(\prod_{i\in I_A}e(g^{a\lambda_i'},g^{t_A})^{w_A(i)}e(h_{\rho_B(i)}^{-r_i'},g^{t_A})^{w_A(i)}e(g^{r_i'},h_{\rho_B(i)}^{t_A})^{w_A(i)}\right)$$

$$=e(g^{s_B},g^{\alpha})e(g^{s_B},g^{at_A})\Big/e(g^{a},g^{t_A})^{\sum_{i\in I_A}\lambda_i'w_A(i)}$$

$$=e(g^{s_B},g^{\alpha})e(g^{s_B},g^{at_A})/e(g^{a},g^{t_A})^{s_B}$$

$$=e(g,g)^{\alpha s_B}$$

$$=(g_T^{\alpha})^{s_B},$$

$$\sigma_3=Y^{s_A}=g^{s_As_B}.$$

$$K_{AB}=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)=H((g_T^{\alpha})^{s_A},(g_T^{\alpha})^{s_B},g^{s_As_B},EPK_A,EPK_B) \quad (1)$$

同理,B 计算:

$$\sigma_1=e(X,K_B)\Big/\left(\prod_{i\in I_B}(e(U_i,L_B)e(D_i,K_{B,\rho_A(i)}))^{w_B(i)}\right)$$

$$=e(g^{s_A},g^{\alpha}g^{at_B})\Big/\left(\prod_{i\in I_B}(e(g^{a\lambda_i}h_{\rho_A(i)}^{-r_i},g^{t_B})e(g^{r_i},h_{\rho_A(i)}^{t_B}))^{w_B(i)}\right)$$

$$=e(g^{s_A},g^{\alpha})e(g^{s_A},g^{at_B})\Big/\left(\prod_{i\in I_B}e(g^{a\lambda_i},g^{t_B})^{w_B(i)}e(h_{\rho_A(i)}^{-r_i},g^{t_B})^{w_B(i)}e(g^{r_i},h_{\rho_A(i)}^{t_B})^{w_B(i)}\right)$$

$$=e(g^{s_A},g^{\alpha})e(g^{s_A},g^{at_B})\Big/e(g^{a},g^{t_B})^{\sum_{i\in I_B}\lambda_iw_B(i)}$$

$$=e(g^{s_A},g^{\alpha})e(g^{s_A},g^{at_B})/e(g^{a},g^{t_B})^{s_A}$$

$$=(g_T^{\alpha})^{s_A},$$

$$\sigma_2=(g_T^{\alpha})^{s_B},$$

$$\sigma_3=X^{s_B}=g^{s_As_B}.$$

$$K_{BA}=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)=H((g_T^{\alpha})^{s_A},(g_T^{\alpha})^{s_B},g^{s_As_B},EPK_A,EPK_B) \quad (2)$$

由公式(1)和公式(2)可知,$K_{AB}=K_{BA}$.

4.3 协议的安全性

定理 1. 若 GCPBDHE 假设和 CDH 假设同时成立,并且 H,H_1 是随机预言机,则本文提出的 ABAKE 协议在 ABeCK 模型下具有选择安全性.

协议的安全性证明过程见附录.

4.4 协议对比

本节将已有的 ABAKE 协议与本文的协议进行对比,对比结果见表 1.

Table 1 Comparison of protocols

表 1 协议的对比

方案	消息长度	计算复杂性	安全模型
文献[4]	$(\|S\|+2)$个 G 上的点	$(\|S\|+2)P+(\|S\|+2)E_1+1E_2$	BR&标准模型
文献[7]	$(\|S\|+1)$个 G 上的点和 1 个 G_T 上的点	$(\|S\|)P+(\|S\|+3)E_1+(\|S\|)E_2$	CK&标准模型
文献[8]	$(l\times n_{\max}+1)$个 G 上的点	$(n_{\max}+\|S\|+1)P+(l\times(n_{\max}+n)+2\|S\|)E_1+2E_2+(l\times n_{\max}+1)H$	eCK&RO 模型
本文协议	$(2l+1)$个 G 上的点	$(2\|S\|+1)P+(3l+1+2\|S\|)E_1+2E_2+(l\times n+1)H$	eCK&RO 模型
文献[11]	$(2l+4)$个 G 上的点	$(2\|S\|+2)P+(3l+5)E_1+2E_2+H+3Ext$	CK+&标准模型

其中,$n_{\max}$ 表示系统中 LSSS 矩阵的列的最大规模;$l\times n$ 表示 LSSS 矩阵的规模;$|S|$表示用户属性集的规模;P 表示双线性映射;E_1 表示 G 上的指数运算;E_2 表示 G_T 上的指数运算;H 表示 Hash 运算,需要指出的是,若协议中采取了不同的 Hash 运算,例如 t_1 次 H_1 运算和 t_2 次 H 运算,这里简记为(t_1+t_2)次 H 运算;Ext 表示随机提取器的计算复杂度.

一般情况下,$n_{\max}>2$.因此,由表 1 可以看出:与文献[8]相比,同样在 AbeCK&RO 模型下,本文提出的协议降低了消息长度;同时,在 $n_{\max}\geqslant|S|$的情况下,也降低了计算复杂度.

5 结束语

本文对 GCDH 假设进行了扩展,提出了 GCPBDHE 假设,提出了基于属性的认证密钥协商协议.在 GCPBDHE 假设和 CDH 假设成立的条件下,证明了该协议在 ABeCK 模型下是安全的.如何设计安全强度和效率更高的 ABAKE 协议,是下一步要解决的问题.

致谢 审稿专家和编辑老师为本文提出了宝贵的修改建议,在此表示衷心的感谢.

References:

[1] Shamir. Identity-Based cryptosystems and signature schemes. In: Proc. of the CRYPTO'84. Santa Barbara: Springer-Verlag, 1984. 47−53. [doi: 10.1007/3-540-39568-7_5]

[2] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proc. of the EUROCRYPT 2005. Aarhus: Springer Press, 2005. 457−473. [doi: 10.1007/11426639_27]

[3] Wang H, Xu QL, Ban T. A provably secure two-party attribute-based key agreement protocol. In: Proc. of the 5th Int'l Conf. on Intelligent Information Hiding and Multimedia Signal Processing. IEEE Press, 2009. 1042−1045. [doi: 10.1109/IIH-MSP.2009.92]

[4] Wang H, Xu QL. Revocable attribute-based key agreement protocol without random oracles. Journal of Networks, 2009,4(8): 787−794. [doi: 10.4304/jnw.4.8.787-794]

[5] Wang H, Xu QL. Two-Party attribute-based key agreement protocol in the standard model. In: Proc. of the 2009 Int'l Symp. on Information Processing (ISIP 2009). Huangshan: Springer-Verlag, 2009. 325−328.

[6] Gorantla MC, Boyd C, Nieto JMG. Attribute-Based authenticated key exchange. In: Proc. of the 15th Australasian Conf. on Information Security and Privacy (ACISP 2010). Sydney: Springer-Verlag, 2010. 300−317. [doi: 10.1007/978-3-642-14081-5_19]

[7] Ren YJ, Wang JD, Zhuang Y, Tan CH, Fang LM. Attribute-Based authenticated key agreement protocol. Journal of LanZhou University (Nature Sciences), 2010,46(2):103−110 (in Chinese with English abstract).

[8] Yoneyama K. Strongly secure two-pass attribute-based authenticated key exchange. In: Proc. of the Pairing-Based Cryptography. Yamanaka Hot Spring: Springer-Verlag, 2010. 147−166. [doi: 10.1007/978-3-642-17455-1_10]

[9] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Proc. of the 14th Int'l Conf. on Practice and Theory in Public Key Cryptography (PKC2011). Taormina: Springer-Verlag, 2011. 53−70. [doi: 10.1007/978-3-642-19379-8_4]

[10] Wei JH, Hu XX, Liu WF. Attribute-Based authenticated key exchange protocol in multiple attribute authorities environment. Journal of Electronics & Information Technology, 2012,34(2):451−456 (in Chinese with English abstract). [doi: 10.3724/SP.J.1146.2011.00701]

[11] Li Q, Feng DG, Zhang LW, Gao ZG. Enhanced attribute-based authenticated key agreement protocol in the standard model. Chinese Journal of Computers, 2013,36(10):2156−2167 (in Chinese with English abstract).

[12] Okamoto T, Pointcheval D. The gap-problems: A new class of problems for the security of cryptographic schemes. In: Proc. of the 4th Int'l Conf. on Practice and Theory in Public Key Cryptography (PKC 2001). Taormina: Springer-Verlag, 2011. 104−118. [doi: 10.1007/3-540-44586-2_8]

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

附中文参考文献:

[7] 任勇军,王建东,庄毅,谭沧海,方黎明.基于属性的认证密钥协商协议.兰州大学学报(自然科学版),2010,46(2):103−110.

[10] 魏江宏,胡学先,刘文芬.多属性机构环境下的属性基认证密钥协商协议.电子与信息学报,2012,34(2):451−456. [doi: 10.3724/SP.J.1146.2011.00701]

[11] 李强,冯登国,张立武,高志刚.标准模型下增强的基于属性的认证密钥协商协议.计算机学报,2013,36(10):2156−2167.

附录: 定理 1 的证明

证明:令 A 是 ABAKE 协议的攻击者,S 是该协议的模拟者,S 的目的是利用 A 解决 CDH 问题或 GCPBDHE 问题.证明该定理的思路是:针对本文设计的 ABAKE 协议,若 A 在多项式时间内能以一个不可忽略的优势区分出测试会话 sid^*的会话密钥和随机选取的会话密钥,则 S 就能在多项式时间内以不可忽略的优势解决 CDH 问题或 GCPBDHE 问题.

令 $\Pr[Suc]$表示 A 攻击成功的概率,即,对 sid^*的会话密钥给出正确判决的概率.

令:

- $AskH$ 表示事件: A 对 sid^*对应的$(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$进行 H 函数查询;
- $\overline{AskH}$ 表示事件: A 未对 sid^*的$(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$进行 H 函数查询.

由于 $\Pr[Suc\wedge\overline{AskH}]=1/2$,因此得到公式(3)成立:

$$\Pr[Suc]=\Pr[Suc\wedge AskH]+\Pr[Suc\wedge\overline{AskH}]=\Pr[Suc\wedge AskH]+1/2 \tag{3}$$

令:

- $AskS$ 表示事件: A 在进行 $StaticReveal$ 查询或 $MasterReveal$ 查询之前,对 $SK_P=(K_P,L_P,\{K_{P,j},\forall j\in S_P\})$进行 H_1 查询;
- $\overline{AskS}$ 表示 $AskS$ 的补事件.

由公式(3)可得:

$$\begin{aligned}\Pr[Suc]&=\Pr[Suc\wedge AskH]+1/2\\&=\Pr[Suc\wedge AskH\wedge AskS]+\Pr[Suc\wedge AskH\wedge\overline{AskS}]+1/2.\end{aligned}$$

由于测试会话一定是一个新鲜会话,并且根据攻击者 A 的攻击行为,我们定义以下事件:

(1) 事件 E_1:测试会话 sid^*没有匹配会话 $\overline{sid^*}$,攻击者对满足访问结构 AS_A 的属性集合 S 进行了 $StaticReveal(S)$查询;

(2) 事件 E_2:测试会话 sid^*没有匹配会话 $\overline{sid^*}$,攻击者对测试会话 sid^*进行了 $EphemeralReveal(sid^*)$查询;

(3) 事件 E_3:测试会话 sid^*存在匹配会话 $\overline{sid^*}$,攻击者对满足访问结构 AS_A 的属性集合 S 进行了 $StaticReveal(S)$查询,并且对满足访问结构 AS_B的属性集合 S 进行了 $StaticReveal(S)$查询;或者进行了 $MasterReveal$ 查询;

(4) 事件 E_4:测试会话 sid^*存在匹配会话 $\overline{sid^*}$,攻击者进行了 $EphemeralReveal(sid^*)$和 $EphemeralReveal(\overline{sid^*})$ 查询;

(5) 事件 E_5:测试会话 sid^*存在匹配会话 $\overline{sid^*}$,攻击者对满足访问结构 AS_B 的属性集合 S 进行了 $StaticReveal(S)$查询;并且进行了 $EphemeralReveal(\overline{sid^*})$ 查询;

(6) 事件 E_6:测试会话 sid^*存在匹配会话 $\overline{sid^*}$,攻击者对满足访问结构 AS_A 的属性集合 S 进行了 $StaticReveal(S)$查询;并且进行了 $EphemeralReveal(sid^*)$查询.

根据 E_1~E_6 定义可知:

$$Suc \wedge AskH \wedge \overline{AskS} = \bigcup_{i=1}^{6}(Suc \wedge AskH \wedge \overline{AskS} \wedge E_i) \tag{4}$$

由公式(3)和公式(4)得到:

$$\begin{aligned}\Pr[Suc] &= \Pr[Suc \wedge AskH \wedge AskS] + \Pr[Suc \wedge AskH \wedge \overline{AskS}] + 1/2\\ &= \Pr[Suc \wedge AskH \wedge AskS] + \Pr\left[\bigcup_{i=1}^{6}(Suc \wedge AskH \wedge \overline{AskS} \wedge E_i)\right] + 1/2\\ &\leqslant \Pr[Suc \wedge AskH \wedge AskS] + \sum_{i=1}^{6}\Pr[(Suc \wedge AskH \wedge \overline{AskS} \wedge E_i)] + 1/2.\end{aligned}$$

令:

$$\begin{aligned}p_0 &= \Pr[Suc \wedge AskH \wedge AskS],\\ p_i &= \Pr[Suc \wedge AskH \wedge \overline{AskS} \wedge E_i], 1 \leqslant i \leqslant 6,\end{aligned}$$

则有:

$$\Pr[Suc] \leqslant \sum_{i=0}^{6} p_i + 1/2 \tag{5}$$

首先假设执行该密钥协商协议的系统用户个数是 N,每个用户至多进行 L 次密钥协商.下面分析 p_i,i=0, 1,…,6 与 S 解决 GCPBDHE 困难问题和 CDH 困难问题的成功率之间的关系.

(1) 事件 $Suc \wedge AskH \wedge AskS$

模拟者 S 随机选择两个用户 A 和 B,并且以 $1/(N^2L)$的概率猜测 A 的第 $i_A \in [1,L]$次会话是攻击者 A 选取的测试会话,将该测试会话记为 sid^*.在事件 $AskS$ 中,允许攻击者 A 在进行 *StaticReveal* 查询或 *MasterReveal* 查询之前执行 SK_A 的 H_1 查询,这说明攻击者在进行 *StaticReveal* 查询或 *MasterReveal* 查询之前已经得到了 A 的长期私钥 SK_A.

模拟者 S 在系统设置中随机选取$\alpha' \in Z_p$,令 $g_T^{\alpha} = e(g^a, g^{a^q})e(g,g)^{\alpha'}$,即$\alpha=\alpha'+a^{q+1}$,则模拟者 S 在接收到攻击者申请的 SK_A 的 H_1 查询请求时,模拟者 S 得到了 $SK_A=(K_A,L_A,\{K_{A,j},\forall j \in S_A\})$.

由于 $K_A / L_A^{a'} = g^{\alpha} = g^{\alpha'+a^{q+1}}$, 因此,$S$ 利用 $e((K_A / L_A^{a'}), g^s) / e(g^{\alpha'}, g^s)$ 可以计算出 $e(g,g)^{a^{q+1}s}$.

因此:

$$\Pr[S \text{ 解决 GCPBDHE 困难问题}] \geqslant p_0/(N^2L).$$

(2) 事件 $Suc \wedge AskH \wedge \overline{AskS} \wedge E_1$

在事件 $Suc \wedge AskH \wedge \overline{AskS} \wedge E_1$,模拟者 S 已知:

$$\begin{aligned}&g, g^s, g^a, ..., g^{(a^q)}, g^{(a^{q+2})}, ..., g^{(a^{2q})}, \forall j \in \{1,2,...,q\},\\ &g^{s \cdot b_j}, g^{a/b_j}, ..., g^{(a^q/b_j)}, g^{(a^{q+2}/b_j)}, ..., g^{(a^{2q}/b_j)}, \forall j,k \in \{1,2,...,q, k \neq j\},\\ &g^{(a \cdot s \cdot b_k / b_j)}, g^{(a^2 \cdot s \cdot b_k / b_j)}, ..., g^{(a^q \cdot s \cdot b_k / b_j)}),\end{aligned}$$

并且接收到攻击者 A 给出的挑战访问结构 (M_A^*, ρ_A^*) 和 (M_B^*, ρ_B^*),其中, M_A^* 是 $l_A^* \times n_A^*$ 规模的矩阵, M_B^* 是 $l_B^* \times n_B^*$ 规模的矩阵.S 对方案进行如下模拟:

- 系统建立

S 随机选取$\alpha' \in Z_p$,令 $g_T^{\alpha} = e(g^a, g^{a^q})e(g,g)^{\alpha'}$, 则$\alpha=\alpha'+a^{q+1}$.该系统用户最多有 U 个属性,对属性集合中的每个属性 x,随机选取 $z_x \in Z_p$.令集合 $\Lambda_x = \{i : \rho_A^*(i) = x, 1 \leqslant i \leqslant l_A^*\}$, 模拟者 S 定义 h_x:

$$h_x = g^{z_x} \prod_{i \in \Lambda_x} g^{aM_{A_i,1}^*/b_i} \cdot g^{a^2 M_{A_i,2}^*/b_i} \cdot \ldots \cdot g^{a^{n_A^*} M_{A_i,n_A^*}^*/b_i},$$

其中, $M_{A_{i,j}}^*$ 是 M_A^* 矩阵的第 i 行 j 列的元素.需要说明的是:若集合 Λ_x 是空集,则 $h_x = g^{z_x}$.

假设系统中有 N 个用户,每个用户最多进行 L 次密钥协商.模拟者 S 随机选择用户 A,B,并且以 $1/N^2L$ 猜测 A 的第 $i_A \in [1,L]$次密钥协商是攻击者攻击的测试会话,将该测试会话记为 sid^*.S按以下方式模拟 A 的第 i_A 次

会话发送的消息 EPK_A:

令 $X=g^s$, S 随机选择 $r_1,r_2,...,r_{l_A^*},x_2,x_3,...,x_{n_A^*}\in Z_p$,则分享的秘密向量为

$$v=(s,sa+x_2,sa^2+x_3,\ldots,sa^{n-1}+x_{n_A^*})\in(Z_p)^{n_A^*}.$$

对于任意的 $i\in\{1,...,n_A^*\}$,定义 $R_i=\{k:\rho_A^*(k)=\rho_A^*(i),k=1,2,...,l_A^*,且k\neq i\}$,计算:

$$U_i=h_{\rho_A^*(i)}^{r_i}\left(\prod_{j=2,...,n_A^*}(g^a)^{M_{A_{i,j}^*}^* x_j}\right)(g^{b_i s})^{-z_{\rho_A^*(i)}^*}\left(\prod_{k\in R_i}\prod_{j=1,...,n_A^*}(g^{a^j\cdot s\cdot(b_i/b_k)})^{M_{A_{k,j}^*}^*}\right),$$

$$D_i=g^{-r_i}g^{-sb_i},$$

其中,$M_{A_{i,j}^*}^*$ 是 M_A^* 矩阵的第 i 行 j 列的元素.

$EPK_A=(X,\{U,D\},M_A^*,\rho_A^*)$ 是用户 A 在会话 sid^* 中发出的消息.

- 模拟过程

为了回答攻击者对 H_1,H 的查询,S 建立两个列表 L_{H_1} 和 L_H;为了回答攻击者对 *SessionReveal* 的查询,$\mathcal{S}$建立列表$\mathcal{L}_K$.

① $H_1(K_P,L_P,\{K_{P,j},\forall j\in S_P\},x)$:如果存在 $(K_P,L_P,\{K_{P,j},\forall j\in S_P\},*)\in\mathcal{L}_{H_1}$, $\mathcal{S}$返回相应查询值;否则,$\mathcal{S}$随机选取 $x'\in Z_p$,将 x'返回给攻击者,并在 L_{H_1} 中记录$(K_P,L_P,\{K_{P,j},\forall j\in S_P\},x')$.

② $H(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}})$:

(a) 如果存在 $(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}},*)\in L_H$, $\mathcal{S}$返回相应查询值;

(b) 如果不存在 $(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}},*)\in L_H$, $\mathcal{S}$判断 P 是否是 A、$\bar{P}$ 是否是 B、该会话是否为 A 的第 i_A 次会话,若都成立,接着调用 DBDH 随机预言机,若:

$$DBDH(X,g^a,g^{a^q},\sigma_1/e(X,g^{\alpha'}))=1,$$
$$DBDH(Y,g^a,g^{a^q},\sigma_2/e(Y,g^{\alpha'}))=1,$$
$$e(X,Y)=e(g,\sigma_3)$$

都成立,则$\mathcal{S}$终止,并且输出$\sigma_1/e(X,g^{\alpha'})$(此时, $\sigma_1/e(X,g^{\alpha'})=e(g,g)^{a^{q+1}s}$, $s_A=s$);

(c) 如果不存在 $(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}},*)\in L_H$, 调用 DBDH 随机预言机,若:

$$DBDH(X,g^a,g^{a^q},\sigma_1/e(X,g^{\alpha'}))=1(即\sigma_1/e(X,g^{\alpha'})=e(g,g)^{a^{q+1}s_P}),$$
$$DBDH(Y,g^a,g^{a^q},\sigma_2/e(Y,g^{\alpha'}))=1(即\sigma_1/e(X,g^{\alpha'})=e(g,g)^{a^{q+1}s_{\bar{P}}}),$$
$$e(X,Y)=e(g,\sigma_3)$$

都成立,则生成一个随机数 $K\in\{0,1\}^k$ 返回给攻击者,并在 L_H 中记录:

$$(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}},K).$$

③ $Send(I,S_P,S_{\bar{P}})$: 若 $P=A$,并且该会话是 A 的第 i_A 次会话,$\mathcal{S}$将 EPK_A 返回给攻击者;否则,$\mathcal{S}$按照协议执行过程生成 EPK_P 返回给用户,并记录 $(S_P,S_{\bar{P}},EPK_P)$.

④ *SessionReveal*(*sid*):模拟者查询 L_K,若攻击者申请 sid^*的会话密钥,则 S 失败终止;若 *sid* 在 L_K 列表中,则 S 将列表中的会话密钥 K 返回给攻击者;若 *sid* 不在 L_K 列表中,查询 L_H,将 H 中 *sid* 对应的 K 返回给用户,并将(*sid*,K)记录在列表 L_K 中.

⑤ *EphemeralReveal*(*sid*):若攻击者申请 sid^*的临时私钥,则 S 失败终止;否则, S 返回给攻击者 $er_0,er_1,\ldots,er_l$, $ex_2,ex_3,\ldots,ex_n\in Z_p$,其中,$l,n$ 分别是访问结构对应的矩阵 M 的行和列数.

⑥ *StaticReveal*(S_P):在事件 E_1 中,用户属性集合 S_P 不满足访问结构 M_A^*,因此,模拟者可以找到向量:

$$w=(w_1,...,w_{n_A^*})\in(Z_p)^{n_A^*},$$

其中,$w_1=-1$;并且对于任意满足条件 $\rho_A^*(i)\in S_P$ 的行标识 i,满足条件 $w\cdot M_A^*(i)=0$. 模拟者选取一个随机数 $r\in Z_p$,

模拟者令 $t=r+w_1a^q+w_2a^{q-1}+...+w_{n_A^*}a^{q-n_A^*+1}$.

利用已知的 $g^a,...,g^{(a^q)}$, 计算出 $L_P=g^r\prod_{i=1,...,n_A^*}(g^{a^{q+1-i}})^{w_i}=g^t, K_P=g^{\alpha'}g^{ar}\prod_{i=2,...,n_A^*}(g^{a^{q+1-i}})^{w_i}=g^{\alpha'}g^{at}$.

$\forall x\in\mathcal{S}_P$,令集合 $\Lambda_x=\{i:\rho_A^*(i)=x,i=1,2,...,l_A^*\}$, 模拟者计算 $K_{P,x}$:

$$K_{P,x}=L_P^{z_x}\prod_{i\in\Lambda_x}\prod_{j=1,...,n_A^*}\left(g^{(a^j/b_i)r}\prod_{\substack{k=1,...,n_A^*\\k\neq j}}(g^{a^{q+1+j-k}/b_i})^{w_k}\right)^{M_{i,j}^*}.$$

若 Λ_x 是空集,则模拟者令 $K_{P,x}=L_P^{z_x}$.

⑦ *MasterReveal*:$\mathcal{S}$失败终止.

⑧ *Test*(*sid*):若测试会话不是 sid^*,S 失败终止;否则,S 随机生成$\xi\in\{0,1\}^k$,将ξ返回给攻击者.

在事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_1$ 中,若攻击者$\mathcal{A}$攻击成功,则攻击者必然查询了 $H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$.因此,根据步骤②中情况(b)的分析,攻击者利用$\sigma_1/e(X,g^{\alpha'})$可以计算出 $e(g,g)^{a^{q+1}s}$. 因此,

$$\Pr[S\text{ 解决 GCPBDHE 问题}]\geqslant p_1/(N^2L).$$

(3) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_2$

在事件 E_2 中,测试会话 sid^*不存在匹配会话 $\overline{sid^*}$,A 可以查询 $EphemeralReveal(sid^*)$,但不能查询满足访问结构(M_B,ρ_B)的长期私钥和满足访问结构(M_A,ρ_A)的长期私钥,或者不能查询系统主私钥.由于 H_1 是随机预言机,并且 H_1 的输入包括属性集对应的长期私钥,故$\mathcal{A}$以一个可以忽略的概率得到正确的 $s_A,r_1,r_2,...,r_{l_A^*},x_2,x_3,...,x_{n_A^*}$.因此与 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_1$ 事件中 S 的模拟过程相似,同样得到模拟者$\mathcal{S}$的成功率:

$$\Pr[S\text{ 解决 GCPBDHE 问题}]\geqslant p_2/(N^2L).$$

(4) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$

在事件 E_3 中,测试会话 sid^*存在匹配会话 $\overline{sid^*}$,A 可以查询 *MasterReveal*,或者可以同时查询满足访问结构(M_B,ρ_B)的长期私钥和满足访问结构(M_A,ρ_A)的长期私钥,但是不允许查询 $EphemeralReveal(sid^*)$和 *Ephemeral Reveal* $(\overline{sid^*})$.模拟者 S 以 $1/(N^2L)$的概率猜测测试会话是 sid^*,即:会话双方是 A,B,并且是 A 的第 i_A 次会话.模拟者 S 的目的是解决 CDH 问题,即:模拟者已知(g^b,g^c),求解 g^{bc}. S 模拟的方案在系统建立和私钥生成阶段与真实方案相同, S 在生成 EPK_A 和 EPK_B 的过程中嵌入 g^b,g^c,具体方法如下:

A 随机选择 $er_1,...,er_{l_A},ex_2,ex_3,...,ex_{n_A}\in Z_p$, 计算:

$$r_i=H_1(K_A,L_A,\{K_{A,j},\forall j\in S_A\},er_i),1\leqslant i\leqslant l_A,$$
$$x_k=H_1(K_A,L_A,\{K_{A,j},\forall j\in S_A\},ex_k),2\leqslant k\leqslant n_A.$$

令秘密向量 $v=(b,x_2,x_3,...,x_{n_A})\in(Z_p)^{n_A}$, 则有:

$$\lambda_i=v\cdot M_A(i)=bM_{A_{i,1}}+x_2M_{A_{i,2}}+...+x_{n_A}M_{A_{i,n_A}},$$

其中,$M_A(i)$是 M_A 的第 i 行,i=1,…,l_A.令:

$$X=g^b,\left(U_i=(g^b)^{aM_{A_{i,1}}}\left(\prod_{j=2}^{n_A}(g^a)^{x_2M_{A_{i,j}}}\right)h_{\rho_A(i)}^{-r_i},D_i=g^{r_i}\right),1\leqslant i\leqslant l_A(\text{令集合}\{U,D\}=\{(U_i,D_i),1\leqslant i\leqslant l_A\}).$$

A 发送消息 $EPK_A=(X,\{U,D\},M_A,\rho_A)$给 B.

B 随机选取 $er_1',...,er_{l_B}',ex_2',ex_3',...,ex_{n_B}'\in Z_p$, 计算:

$$r_i'=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},er_i'),1\leqslant i\leqslant l_B,$$
$$x_k'=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},ex_k'),2\leqslant k\leqslant n_B.$$

令秘密向量 $v'=(c,x_2',x_3',...,x_{n_B}')$, 计算:

$$\lambda_i'=v'\cdot M_B(i),$$

其中,$M_B(i)$是矩阵 M_B 的第 i 行,i=1,…,l_B.B 计算:

$$Y=g^c,\left(V_i=(g^c)^{aM_{B_{i,1}}}\left(\prod_{j=2}^{n_B}(g^a)^{x_2M_{B_{i,j}}}\right)h_{\rho_B(i)}^{-r_i'},E_i=g^{r_i'}\right),1\leqslant i\leqslant l_B(\text{令集合}\{V,E\}=\{(V_i,E_i),1\leqslant i\leqslant l_B\}).$$

B 发送消息 $EPK_B=(Y,\{V,E\},M_B,\rho_B)$给 A.

在事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$ 中,攻击者必然输入正确的$\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B$ 查询 H 预言机,因此,攻击者可以求解出 $g^{bc}=\sigma_3$,得到:

$$\Pr[S\text{ 解决 CDH 问题}]\geqslant p_3/(N^2L).$$

(5) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_4$

在事件 E_4 中,测试会话 sid^*存在匹配会话 $\overline{sid^*}$,A 查询 $EphemeralReveal(sid^*)$和 $EphemeralReveal(\overline{sid^*})$, 但不允许查询满足访问结构$(M_B,\rho_B)$的长期私钥和满足访问结构$(M_A,\rho_A)$的长期私钥,也不允许查询系统主私钥.

由于 H_1 是随机预言机,因此,A 只能以可以忽略的概率得到正确的$\{s_A,r_i,x_j(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)\}$和$\{s_B,r_i',x_j'(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)\}$.与 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$ 事件中$\mathcal{S}$的模拟过程相似,得到模拟者$\mathcal{S}$的成功率:

$$\Pr[S\text{ 解决 CDH 问题}]\geqslant p_4/(N^2L).$$

(6) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_5$

在事件 E_5 中,测试会话 sid^*存在匹配会话 $\overline{sid^*}$,A 查询满足访问结构(M_B,ρ_B)的属性集对应的长期私钥和 $EphemeralReveal(\overline{sid^*})$, 不允许查询满足访问结构$(M_A,\rho_A)$的属性集对应的长期私钥和 $EphemeralReveal(sid^*)$,也不允许查询 $MasterReveal$.由于 H_1 是随机预言机,因此, A 只能以可以忽略的概率得到正确的$\{s_A,r_i,x_j(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)\}$和 $s_B,r_i',x_j'(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)$. 与 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$ 事件中$\mathcal{S}$的模拟过程相似,得到模拟者$\mathcal{S}$的成功率:

$$\Pr[S\text{ 解决 CDH 问题}]\geqslant p_5/(N^2L).$$

(7) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_6$

在事件 E_6 中,测试会话 sid^*存在匹配会话 $\overline{sid^*}$,A 查询 $EphemeralReveal(sid^*)$和满足访问结构(M_A,ρ_A)的属性集对应的长期私钥,不查询满足访问结构(M_B,ρ_B)的属性集对应的长期私钥和 $EphemeralReveal(\overline{sid^*})$, 不查询 $MasterReveal$.由于 H_1 是随机预言机,因此, A 只能以可以忽略的概率得到正确的$\{s_A,r_i,x_j(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)\}$和 $s_B,r_i',x_j'(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)$. 与 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$ 事件中 S 的模拟过程相似,模拟者 S 的成功率:

$$\Pr[S\text{ 解决 CDH 问题}]\geqslant p_6/(N^2L).$$

针对上述 7 个事件的分析结果,得到以下两个结论.

结论 1. $\Pr[S\text{ 解决 GCPBDHE 困难问题}]\geqslant\max\{p_0,p_1,p_2\}/(N^2L)$.

结论 2. $\Pr[S\text{ 解决 CDH 困难问题}]\geqslant\max\{p_3,p_4,p_5,p_6\}/(N^2L)$.

假设攻击者 A 攻击成功,则下面不等式成立:

$$\Pr[Suc]\geqslant 1/2+\varepsilon \tag{6}$$

由公式(5)和公式(6)得到: $\sum_{i=0}^{6}p_i\geqslant\varepsilon$.

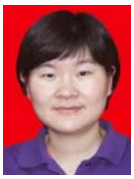
又由于 $7*\max\{p_i,i=0,1,...,6\}\geqslant\sum_{i=0}^{6}p_i$, 因此得到:$\max\{p_i,i=0,1,\ldots,6\}\geqslant\varepsilon/7$.

由于 $\Pr[S\text{ 解决 GCPBDHE 困难问题}]\geqslant\max\{p_0,p_1,p_2\}/(N^2L)$,若 $\max\{p_i,i=0,1,\ldots,6\}\in\{p_0,p_1,p_2\}$,则 $\Pr[S\text{ 解决 GCPBDHE 困难问题}]\geqslant\varepsilon/(7N^2L)$,这与 GCPBDHE 假设是矛盾的;

由于 $\Pr[S\text{ 解决 CDH 困难问题}]\geqslant\max\{p_3,p_4,p_5,p_6\}/(N^2L)$,若 $\max\{p_i,i=0,1,\ldots,6\}\in\{p_3,p_4,p_5,p_6\}$,则 $\Pr[S\text{ 解决 CDH 困难问题}]\geqslant\varepsilon/(7N^2L)$,这与 CDH 假设是矛盾的.

根据上述分析,若 GCPBDHE 假设和 CDH 假设同时成立,并且 H_1,H 是随机预言机,本文提出的 ABAKE 协议在 ABeCK 模型下具有选择安全性.

下面粗略分析模拟者 S 的计算复杂度.为了描述方便,记调用一次 H_1 预言机的计算复杂度为 T_{H_1},DBDH 预言机的计算复杂度为 T_{DBDH},消息 EPK 的计算复杂度为 T_{EPK},对运算的计算复杂度为 T_e,用户长期私钥的计算复杂度为 T_{SK},用户临时私钥以及系统主私钥的计算复杂度相对较小,忽略不计.由于每个事件中 S 的计算复杂度的具体表达式都非常复杂,因此,我们这里只给出了一个粗略的上界,即:事件(1)中, S 的计算复杂度小于 $N^2L(T_{H_1}+2T_{DBDH})+4T_e$;在事件(2)~事件(7)中, S 的计算复杂度都小于 $N^2L(T_{H_1}+2T_{DBDH}+T_{EPK})+N\cdot T_{SK}$,在假设 T_{H_1},T_{DBDH},T_{EPK},T_e 和 T_{SK} 都是多项式时间的条件下, S 的计算复杂度也是多项式时间的.



高海英(1978－),女,河南沈丘人,博士,副教授,主要研究领域为密码理论.