一种高效的基于属性的认证密钥协商协议

陈燕俐 杜英杰 杨 庚
(南京邮电大学计算机学院 南京 210003)

摘 要 提出了一种新的基于密文策略的属性加密方案,其访问结构采用线性秘密共享矩阵(LSSS),可以描述任意访问结构;解密过程仅需要3个双线性运算,解密计算复杂度与属性集合大小无关,具有较高的计算效率。在标准模型下给出了方案的安全性证明。同时基于该属性加密方案,提出了一个高效的基于属性的认证密钥协商协议(ABAKA),该协议结合NAXOS技术,有效抵制了用户密钥的泄露。在ABeCK安全模型下给出了协议的安全性证明。最后的性能分析和实验结果验证了协议具有较高的计算效率。

关键词 属性加密,密文策略,密钥协商,NAXOS
中图法分类号 TP309 **文献标识码** A

Efficient Attribute-based Authenticated Key Agreement Protocol

CHEN Yan-li DU Ying-jie YANG Geng
(School of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract A novel ciphertext-policy attribute-based encryption scheme was proposed. Employing Linear Secret Sharing Schemes (LSSS), any access structure can be expressed. The decryption procedure needs only three bilinear maps resulting in more efficient computation irrespective of attributes set. The CP-ABE was proven to be selectively secure in the standard model under chosen plaintext attack. Based on the efficient scheme above, an efficient Attribute-based Authenticated Key Agreement Protocol (ABAKA) was proposed. Combined with NAXOS technique, the ABAKA can resist the leakage of the users' key. The proof was given in the ABeCK model. Finally the paper gave the analysis and experiment result of the computation overhead.

Keywords Attribute-based encryption, Ciphertext-policy, Key agreement, NAXOS

1 引言

随着网络技术的发展,信息的安全传输日益受到人们的重视。传统的对称加密的安全性依赖于算法的保密;公钥加密的安全性依赖于数学难题,用户的公私钥相互独立,解密过程是一个单向陷门函数,只有拥有私钥的合法用户才可以解密,具有较高的安全性。结合公钥加密方案和Diffie-Hellman密钥协商[1]技术,用户协商出一个会话密钥,进而建立起了一个安全信道来进行信息的保密传输。

2005年,Sahai和Waters[2]提出了模糊身份加密方案(Fuzzy IBE),开启了属性加密(Attribute-based encryption, ABE)研究的新方向,属性加密把用户身份细化为属性集,保护了用户的隐私,并可实现群组的加密、认证和签名。Bethencourt等[3]首次提出了密文策略的基于属性的加密方案,密文关联一个树形的访问结构,可以实现"与"和"或"操作。Cheung等[4]第一个提出了在标准模型下的可证安全的CP-ABE,但访问结构只实现了"与"和"非"操作,且解密算法中的双线性运算个数与系统全部属性集合大小线性相关。Waters[5]提出的CP-ABE中,访问结构采用线性秘密共享方案(LSSS),能够表示灵活的访问控制策略,例如,"与","或","门限(k,n)",但解密算法中的双线性运算个数依然与解密方属性集个数线性相关。Ge等[6]和Attrapadung等[7]分别提出了固定密文长度的CP-ABE,限定了密文长度,且解密算法中的双线性运算个数为O(1),解密效率较高,但访问结构仅能表示门限。Hohenberger等[8]使用LSSS构造出了一个密钥策略的属性加密方案(KP-ABE),该方案解密过程仅需两个双线性运算。

近几年,属性加密在密钥协商中得到广泛应用。Wang等[9,10]分别在随机预言模型和标准模型中构造了基于属性的密钥协商协议,但没有引入灵活的访问控制结构。Yoneyama[11]基于Waters[5]的加密方案,提出了一个强安全的密钥协商协议,该协议结合NAXOS[12]技术,有效抵制了用户密钥的泄露。随后,Yoneyama[13]提出了一个在标准模型下可证安全的密钥协商协议,该协议通过签名实现认证,可以抵抗选

到稿日期:2013-06-08 返修日期:2013-09-18 本文受国家"九七三"重点基础研究发展规划课题:物联网混杂信息融合与决策研究(2011CB302903),国家自然科学基金项目:云计算环境下的新型访问控制理论与关键技术研究(61272084),江苏省自然科学基金(BK2009426)资助。

陈燕俐(1969—),女,博士生,副教授,主要研究方向为计算机网络、信息安全,E-mail:chenyl@njupt.edu.cn;杜英杰(1987—),男,硕士生,主要研究方向为信息安全;杨 庚(1961—),男,教授,博士生导师,主要研究方向为计算机通信与网络、网络安全、分布与并行计算等。

择密文攻击(CCA)。魏江宏等[14]提出了一个多属性机构环境下的密钥交换协议,但该协议计算效率较低。

本文提出了一个新的密文策略的属性加密方案(CP-ABE),方案的访问结构采用线性秘密共享矩阵(LSSS),可表达任意访问策略,包括与门、或门和门限,访问结构灵活。与其他的 CP-ABE 相比,解密算法仅需 3 个双线性运算,不再与访问结构的属性集个数线性相关,效率较高。在此基础上,结合 NAXOS 技术,提出了一个高效的基于属性的认证密钥协商协议(ABAKA),并在 ABeCK 模型中给出了其安全性证明。该 ABAKA 不仅可以表示任意访问结构,还具有较高的计算效率,适用于计算和存贮资源有限的网络系统,例如无线传感器网络(WSN)。

2 预备知识

2.1 双线性映射

设 G,G_T 是阶为素数 p 的循环乘法群,g 是 G 的一个生成元,双线性映射 $e:G\times G\to G_T$ 描述如下:

(1)双线性:对 $\forall g_1,g_2\in G,a,b\in Z_p$,都有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$;

(2)非退化性:$e(g,g)\neq 1$(单位元);

(3)可计算性:对 $\forall g_1,g_2\in G$,存在一个有效的多项式时间算法来计算 $e(g_1,g_2)$。

2.2 访问结构

假设在实体集 $P=\{P_1,\cdots,P_n\}$ 共享一个秘密,能恢复该秘密的实体子集称为授权子集,不能恢复该秘密的实体子集称为非授权子集。所有的授权子集构成的集族 Λ 称为对该秘密的一个访问结构。一个访问结构 Λ 是单调的,是指 $A\in\Lambda,A\subseteq B\subseteq P$,则 $B\in\Lambda$。

2.3 线性秘密共享方案(LSSS)

一个定义在实体集 P 上的线性秘密共享方案(Linear Secret Sharing Scheme,LSSS)Π 是指:

(1)所有实体的共享组成 Z_p 上的一个向量;

(2)存在一个 $l\times n$ 的 Π 的共享生成矩阵 M 和一个从 $\{1,\cdots,l\}$ 到 P 的映射 ρ,随机选取 $v=(s,v_2,\cdots,v_n)\in Z_p^n$,其中 s 是要共享的秘密,则 Mv^T 就是利用 Π 得到的关于 s 的 l 个共享组成的向量,其中共享 $(Mv^T)_i$ 属于实体 $\rho(i)$,表示为 $\lambda_i=(Mv^T)_i$。

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 Λ 的 LSSS,对授权用户集 $S\in\Lambda$,定义 $I=\{i:\rho(i)\in S\}\subseteq\{1,\cdots,l\}$,存在向量 $w=\{\omega_i\in Z_p\}_{i\in I}$,使得 $\sum_{i\in I}\omega_iM_i=(1,0,\cdots,0)$,从而得到:$\sum_{i\in I}\omega_iM_iv^T=\sum_{i\in I}\omega_i\lambda_i=\sum_{i\in I}(\omega_iM_i)v^T=s$。对于非授权用户集,存在向量 $w\in Z_p^n$,使得 $w(1,0,\cdots,0)^T=-1,wM_i^T=0,i\in I$。

LSSS 可以描述灵活的访问控制结构,例如与门(AND)、或门(OR)、门限(k,n)。考虑一个访问结构:$\Lambda=(P_1\wedge P_2\wedge P_3)\vee(P_1\wedge P_4)$,其共享生成矩阵 M:

$$M=\begin{pmatrix}0,1,0\\1,0,1\\0,1,-1\\1,1,0\end{pmatrix}$$

其中,$\rho(i)=P_i,i=1,2,3,4$。

对于授权集 $S=\{P_1,P_2,P_3\}\in\Lambda$,可以找到向量 $w=(-1,1,1)$,使得 $\sum_{i\in I}\omega_iM_i=(1,0,0)$,其中 $I=\{1,2,3\}$;或者 $S=\{P_1,P_4\}\in\Lambda$,可以找到向量 $w=(-1,1)$,使得 $\sum_{i\in I}\omega_iM_i=(1,0,0)$,其中 $I=\{1,4\}$。基于门限的 LSSS 可以使用 Shamir[15]的门限方案。

2.4 困难假设

2.4.1 CDH 假设

G 是阶为素数 p 的循环乘法群,g 是 G 的生成元,随机选择 $A=g^a,B=g^b\in G$,如果计算 CDH$(X=g^a,Y=g^b)=g^{ab}$ 是困难的,则称 CDH 假设成立。

2.4.2 判定性 *q-parallel* BDHE 假设

G 是阶为素数 p 的循环乘法群,g 是 G 的生成元,随机值 $a,s,b_1,\cdots,b_q\in Z_p$,多元组 $y=g,g^s,g^a,\cdots,g^{a^q},,g^{a^{q+2}},\cdots,g^{a^{2q}},\forall 1\leqslant j\leqslant q,g^{a/b_j},\cdots,g^{a^q/b_j},,g^{a^{q+2}/b_j},\cdots,g^{a^{2q}/b_j},\forall 1\leqslant j,k\leqslant q,k\neq j,g^{asb_k/b_j},\cdots,g^{a^qsb_k/b_j}$。

对于敌手,给定 y,区分 $e(g,g)^{a^{q+1}s}\in G_T$ 和随机值 $R\in G_T$ 依然是困难的,定义一个算法 B 能以优势 ε 解决判定性 *q-parallel* BDHE 困难问题,则有 $|\Pr[B(y,T=e(g,g)^{a^{q+1}s}=0)]-\Pr[B(y,T=R)=0]|\geqslant\varepsilon$。

3 基于密文策略的属性加密方案(CP-ABE)

3.1 Attribute-Based Selective-Security 模型

初始化:敌手宣布想要挑战的访问结构 $\Lambda:(M^*,\rho^*)$,共享生成矩阵 M^* 为 $l^*\times n^*$,且 $l^*,n^*\leqslant q$。

系统建立:挑战者执行 Setup 算法,产生系统公钥 PK 和主密钥 MSK,返回给敌手 PK。

阶段 1　对于属性集 $S=\{S_1,\cdots,S_{q_1}\}\notin\Lambda$,敌手询问 KeyGen(MSK,S),挑战者返回对应的私钥。

挑战:敌手给挑战者两个等长的明文 m_0,m_1。挑战者随机选取 $\beta\in\{0,1\}$,并返回密文 CT $*=$ Encrypt(PK,$(M^*,\rho^*),m_\beta$)。

阶段 2　敌手按照阶段 1 的要求,对于属性集 $S=\{S_{q_1+1},\cdots,S_q\}\notin\Lambda$,继续询问私钥。

猜测:敌手输出对 β 的猜测 β'。

定义 1　CP-ABE 是选择明文安全(CPA)的,只要满足以下条件:在安全性游戏中,对于所有概率多项式时间敌手,其优势是可忽略的,定义优势 $\varepsilon=|\Pr[\beta=\beta']-\frac{1}{2}|$。

3.2 CP-ABE 方案的具体描述

本文的 CP-ABE 方案由 4 个算法组成:系统建立(Setup)、私钥提取(KeyGen)、加密(Encrypt)、解密(Decrypt)。

Setup(U):系统输入用户全集 U,G 是阶为素数 p 的循环乘法群,g 是 G 的生成元。系统随机选取 $h_1,h_2,\cdots,h_U\in G$,随机选取 $\alpha,a\in Z_p$,系统公钥为 $PK=g,g^a,h_1,h_2,\cdots,h_U,e(g,g)^\alpha$。系统主密钥 $MSK=g^\alpha$。

Encrypt(PK,(M,ρ),M):输入系统公钥 PK 和明文 M,(M,ρ)是线性秘密共享方案(LSSS),M 是 $l\times n$ 的矩阵,函数 ρ 把矩阵 M 的行向量标识为某一属性,Γ 表示秘密共享矩阵 M 中关联的不同属性的集合。随机选取向量 $v=(s,y_2,y_3,\cdots,y_n)\in Z_p^n$,$s$ 是秘密共享值。对共享生成矩阵 M 的每一行向量 M_i,计算 $\lambda_i=M_i\cdot v$。随机选取 $r_1,r_2,\cdots,r_l\in Z_p$,密文 CT 计算如下:

$C=M\cdot e(g,g)^{\alpha\cdot s}, C'=g^s$,

$(C_1=g^{a\lambda_1}h_{\rho(1)}^{-r_1}, D_1=g^{r_1}, \forall d\in\Gamma/\rho(1), Q_{1,d}=h_d^{-r_1})$

,…,

$(C_l=g^{a\lambda_l}h_{\rho(l)}^{-r_l}, D_l=g^{r_l}, \forall d\in\Gamma/\rho(l), Q_{l,d}=h_d^{-r_l})$

秘密共享结构为(M,ρ)。需要说明的是:d 表示属性;$\Gamma/\rho(i)$表示如果集合 Γ 中存在属性 $\rho(i)$,则移除。

KeyGen(MSK,S):输入系统主秘钥 MSK 和私钥属性集合 S,随机选取 $t\in Z_p$,私钥 SK 计算如下:

$K=g^{\alpha}g^{\alpha t}, L=g^t, \forall x\in S: K_x=h_x^t$。

Decrypt(CT,SK):输入密文 CT 和用户私钥 SK,如果私钥属性集合 $S\not\subset\Lambda$(即属性不满足访问结构),则解密终止;否则计算如下:

定义集合 $I\subset\{1,2,\cdots,l\}, I=\{i:\rho(i)\in S\}$。存在$\{\omega_i\in Z_p\}_{i\in I}$,使得$\sum_{i\in I}\omega_i M_i=(1,0,\cdots,0)$ 即$\sum_{i\in I}\omega_i\lambda_i=s$。

定义集合 $\Delta=\{x:\exists i\in I,\rho(i)=x\}$,$\Delta\in S,\Delta\in\Gamma$。

定义函数 $f(\Delta)=\prod_{x\in\Delta/\rho(i)}h_x$,计算:

$\widetilde{C}_i=C_i\cdot\prod_{x\in\Delta/\rho(i)}Q_{i,x}=g^{a\lambda_i}f(\Delta)^{-r_i}$

$\widetilde{K}=\prod_{x\in\Delta}K_x=\prod_{x\in\Delta}h_x^t=f(\Delta)^t$

解密如下:

$$e(g,g)^{\alpha\cdot s}=\frac{e(K,C')}{e(\prod_{i\in I}\widetilde{C}_i^{\omega_i},L)\cdot e(\prod_{i\in I}D_i^{\omega_i},\widetilde{K})}$$

$$M=\frac{C}{e(g,g)^{\alpha\cdot s}}$$

正确性验证:

$$\frac{e(K,C')}{e(\prod_{i\in I}\widetilde{C}_i^{\omega_i},L)\cdot e(\prod_{i\in I}D_i^{\omega_i},\widetilde{K})}$$

$$=\frac{e(g^{\alpha}g^{\alpha t},g^s)}{e(\prod_{i\in I}(g^{a\lambda_i\omega_i}f(\Delta)^{-r_i\omega_i}),g^t)\cdot e(\prod_{i\in I}g^{r_i\omega_i},f(\Delta)^t)}$$

$$=\frac{e(g^a,g^s)e(g^{at},g^s)}{e(g^{as},g^t)\cdot e(\prod_{i\in I}f(\Delta)^{-r_i\omega_i},g^t)\cdot e(\prod_{i\in I}g^{r_i\omega_i},f(\Delta)^t)}$$

$$=\frac{e(g^a,g^s)e(g^{at},g^s)}{e(g^{as},g^t)}$$

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

3.3 安全性证明

定义 2 对于任意一个共享生成矩阵 $M_{l^*\times n^*}$,且 $l^*, n^*\leqslant q$,假设存在概率多项式时间敌手,其在安全性游戏中能以优势 ε 攻破本方案,则存在定义一个模拟者能以$\frac{\varepsilon}{2}$的优势解决判定性 q-*parallel*BDHE 假设。

初始化:安全性游戏中,模拟者用 B 标识并执行挑战者的功能,敌手用 A 标识。模拟者欲挑战的 q-*parallel*BDHE 组为 y,T,敌手欲挑战的访问结构为(M^*,ρ^*),注意到,共享生成矩阵 M^* 为 $l^*\times n^*$,且 $l^*, n^*\leqslant q$。

系统建立:模拟者选择一个随机值 $\alpha'\in Z_p$,使得 $\alpha=\alpha'+a^{q+1}$,即:$e(g,g)^{\alpha}=e(g^a,g^{a^q})e(g,g)^{\alpha'}$。对于属性 $x\in U$,定义 $X=\{i:\rho^*(i)=x\}$,h_x 计算如下:

$X=\emptyset, h_x=g^{z_x}$;

$X\neq\emptyset, h_x=g^{z_x}\prod_{i\in X}g^{aM_{i,1}^*/b_i}\cdot g^{a^2M_{i,2}^*/b_i}\cdots g^{a^{n^*}M_{i,n^*}^*/b_i}$;$z_x$ 为 Z_p 上的随机值。

阶段 1 对于敌手要挑战属性集 S(S 不满足秘密共享矩阵 M^*),模拟者回答这种询问并返回私钥。模拟者选取随机值 $r\in Z_p$;构造向量 $w=(\omega_1,\cdots,\omega_{n^*})\in Z_p^{n^*}$,$\omega_1=-1$,$\forall i$,$\rho^*(i)\in S$,都有 $w\cdot M_i^*=0$。

模拟者定义 t,如下:

$t=r+\omega_1 a^q+\cdots+\omega_{n^*}a^{q-n^*+1}$,私钥构造如下:

$L=g^r\prod_{i=1,\cdots,n^*}(g^{a^{q+1-i}})^{\omega_i}=g^t$

注意到 g^{at} 中存在 $g^{-a^{q+1}}$,为了消除 $g^{-a^{q+1}}$,K 计算如下:

$K=g^{\alpha'}g^{ar}\prod_{i=2,\cdots,n^*}(g^{a^{q+2-i}})^{\omega_i}$

对于 K_x $\forall x\in S$,如果 $x\in S$,$\forall i,\rho^*(i)\neq x$,此时有 $K_x=L^{z_x}$;否则,K_x 计算如下:

$$K_x=L^{z_x}\prod_{i\in X}\prod_{j=1,\cdots,n^*}(g^{(a^j/b_i)^r}\cdot\prod_{k=1,\cdots,n^*,k\neq j}(g^{a^{q+1+j-k}/b_i})^{\omega_k})^{M_{i,j}^*}$$

。X 表示:$X=\{i:\rho^*(i)=x\}$。

挑战:敌手把 M_0, M_1 交给模拟者,模拟者进行投币实验:$\beta\in\{0,1\}$,计算 $C=M_\beta T\cdot e(g^s,g^{\alpha'}), C'=g^s$。模拟者选择随机值 $y_2',\cdots,y_{n^*}'$,构造秘密共享向量 $v=(s,sa+y_2',\cdots,sa^{n-1}+y_{n^*}')\in Z_p^{n^*}$。

模拟者定义集合 $R_i=\{k:k\neq i,\rho^*(i)=\rho^*(k)\}$,其中 $i=1,\cdots,n^*$。选取随机值 $r_1',\cdots,r_l',r_i=r_i'+sb_i$,计算如下:

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

$$C_i=h_{\rho^*(i)}^{-r_i'}(\prod_{j=2,\cdots,n^*}(g^a)^{M_{i,j}^*y_j'})\cdot(g^{b_i\cdot s})^{-z_{\rho^*(i)}}\cdot(\prod_{k\in R_i}\prod_{j=1,\cdots,n^*}(g^{a^j s(b_i/b_k)})^{M_{k,j}^*})$$

Γ 表示秘密共享矩阵 M^* 中关联的不同属性的集合。对于 $\forall x\in\Gamma/\rho^*(i)$,计算如下:

$$Q_{i,d}=h_d^{-r_i'}(g^{b_i s})^{-z_d}(\prod_{k\in R_d}\prod_{j=1,\cdots,n^*}(g^{a^j s(b_i/b_k)})^{M_{k,j}^*})$$

阶段 2 类似于阶段 1,敌手继续进行私钥询问,模拟者回答这种询问。

猜测:定义敌手在安全性游戏中获胜的优势为 ε。敌手最后输出一个 β' 作为对 β 的猜测。模拟者进行如下猜测:如果 $\beta=\beta'$,$T=e(g,g)^{a^{q+1}s}$,输出 0,此时模拟者的优势为 $\Pr[B(y,T=e(g,g)^{a^{q+1}s})=0]=\frac{1}{2}+\varepsilon$;否则模拟者选择随机值 $T\in G_T$,输出 1,优势为 $\Pr[B(y,R)=0]=\frac{1}{2}$。模拟者解决判定性 q-*parallel*BDHE 假设的概率为:

$$\frac{1}{2}\cdot(\frac{1}{2}+\varepsilon)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{\varepsilon}{2}$$

3.4 CP-ABE 方案效率分析

n 表示用户属性集个数,N 表示系统建立的阶段属性全集个数,$|G|$表示群 G 上元素大小,本文 CP-ABE 与其他加密方案的比较如表 1 所列。

表 1 各 CP-ABE 方案分析与比较

方案	私钥空间	访问结构	双线性运算个数
BSW[3]	$(2n+1)\|G\|$	“任意”	2n+1
CN[4]	$(N+n+1)\|G\|$	“与”和“非”	N+1
W[5]	$(n+2)\|G\|$	“任意”	2n+1
GZC[6]	$(4n^2-2n)\|G\|$	“门限”	2
本方案	$(n+2)\|G\|$	“任意”	3

Hohenberger[8]仿真表明,相对于群 G, G_T 上的乘法运算(0.0034 毫秒/个),双线性运算 $e:G\times G\to G_T$(8.22 毫秒/个)计算效率较低。表 1 表明:本文提出的 CP-ABE 中整个算法只有 3 个双线性运算,计算效率较高;相比于方案 GZC[6],本

文方案采用 LSSS，可以表示任意访问结构，且用户的私钥空间开销较小。

4 基于属性的认证密钥协商协议(ABAKA)

4.1 Attribute-Based eCK 安全模型

本节介绍适用于基于属性密钥协商协议安全性分析的扩展 eCK 模型，即 ABeCK 模型。

协议参与者：每一个协议参与者 P 都被视为概率多项式时间的图灵机，具有属性集 S_P，并能并行地执行多个会话实例。若由 A 发起的一个与 B 之间的会话产生了消息 $m_1,\cdots,m_n$，则该会话被 A 标识为 $sid=(T,S_A,S_B,m_1,\cdots,m_n)$，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 $(T,S_A,S_B,m_1,\cdots,m_n)$ 的匹配会话是 $(R,S_B,S_A,m_1,\cdots,m_n)$，反之亦然。

安全性游戏在模拟者与攻击者之间展开(模拟者和攻击者分别用 S 和 M 标识)，攻击者具有如下询问权限：

(1)Send(m)：攻击者向协议参与者发送消息 m，激活会话。

(2)SessionReveal(sid)：若会话完成，返回给攻击者会话密钥，否则返回随机值。

(3)EphemeralReveal(sid)：攻击者得到会话的短期私钥。

(4)StaticReveal(S_P)：攻击者得到相应于 S_P 的长期私钥。

(5)MasterReveal：攻击者得到系统的主密钥。

(6)Establish(P,S_P)：攻击者在系统中以 P 的身份用属性集 S_P 注册。对一个协议参与者 P，如果攻击者进行了 Establish(P,S_P)询问，则称 P 是不诚实实体，反之称其为诚实实体。

(7)Test(sid^*)：接受到该询问后，随机选取 $b\in\{0,1\}$，若 $b=0$，返回给攻击者会话密钥，否则返回一个与密钥等长的随机值。该询问只进行一次。最后，攻击者输出 b' 作为对 b 的猜测。若 $b'=b$，并且 sid^* 是新鲜的，则称攻击者赢得了安全性游戏。定义攻击者获胜的优势为 $Adv(M)=|\Pr[M_{wins}-\frac{1}{2}]|$。

会话新鲜性：记 sid^* 是一个诚实实体 A 和 B 之间的已完成会话，若 sid^* 存在匹配会话，记为 $\overline{sid}^*$。会话 sid^* 是新鲜的，是指下面条件均不成立：

(1)攻击者询问 SessionReveal(sid^*)或者 SessionReveal($\overline{sid}^*$)($\overline{sid}^*$ 存在时)；

(2)$\overline{sid}^*$ 存在，攻击者进行任何一种下述询问：

StaticReveal(S)，EphemeralReveal(sid^*)，其中 $S\in\Lambda_B$；

或者

StaticReveal(S)，EphemeralReveal($\overline{sid}^*$)，其中 $S\in\Lambda_A$。

(3)$\overline{sid}^*$ 不存在，攻击者进行任何一种下述询问：

StaticReveal(S)，*EphemeralReveal*(sid^*)，其中 $S\in\Lambda_B$

或者

StaticReveal(S)，其中 $S\in\Lambda_A$。

其中攻击者进行 MasterReveal 询问，等价于同时询问了 StaticReveal(S)(其中 $S\in\Lambda_A$)以及 StaticReveal(S)(其中 $S\in\Lambda_B$)。

4.2 ABAKA 的具体描述

基于属性的认证密钥协议由 3 个算法组成：系统建立、私钥生成、密钥协商。

系统建立：U 是用户属性全集，G 是阶为素数 p 的循环乘法群，g 是 G 的生成元。哈希函数 $H_1:\{0,1\}^*\to Z_p$，$H_2:\{0,1\}^*\to\{0,1\}^k$(对于多元组 $x_1,\cdots,x_n$，$H(x_1,\cdots,x_n)$表示 $x_1,\cdots,x_n$ 串接映射后的哈希值)。系统随机选取 $h_1,h_2,\cdots,h_U\in G$，随机选取 $\alpha,a\in Z_p$，系统公钥为 $PK=g,g^a,h_1,h_2,\cdots,h_U,e(g,g)^\alpha$。系统主密钥 $MSK=g^\alpha$。

私钥生成：输入系统主秘钥 MSK 和私钥属性集合 S，随机选取 $t\in Z_p$，私钥 SK 计算如下：

$K=g^\alpha g^{at}$，$L=g^t$，$\forall x\in S:K_x=h_x^t$。

SK 是用户 U 的长期私钥，表示 SK_U。

密钥协商：输入系统公钥 PK，(M,ρ)是线性秘密共享方案(LSSS)，M 是 $l\times n$ 的共享生成矩阵，函数 ρ 把矩阵 M 的行向量标识为某一属性，Γ 表示秘密共享矩阵 M 中关联的不同属性的集合。对于用户 Alice，Bob，协商如下：

Alice 随机选取短期私钥 $esk_A=\tilde{x}_1,\cdots,\tilde{x}_n\in Z_p^n$，分别计算 $x_1=H_1(\tilde{x}_1,\{SK_A\}),\cdots,x_n=H_1(\tilde{x}_n,\{SK_A\})$，定义向量 $v_A=(x_1,\cdots,x_n)$。对共享矩阵 M_A，使得 Bob 的属性集 S_B 满足 M_A，计算 $\lambda_{Ai}=(M_A)_i\cdot v_A$。随机选取 $r_{A1},\cdots,r_{Al}\in Z_p$，短期公钥 epk_A 计算如下：

$C_A'=g^{r_1}$，

$(C_{A1}=g^{\alpha\lambda_{A1}}h_{\rho_A(1)}^{-r_{A1}},D_{A1}=g^{r_{A1}},\forall d\in\Gamma_A/\rho_A(1),Q_{A1,d}=h_d^{-r_{A1}}),\cdots,$

$(C_{Al}=g^{\alpha\lambda_{Al}}h_{\rho_A(l)}^{-r_{Al}},D_{Al}=g^{r_{Al}},\forall d\in\Gamma_A/\rho_A(l),Q_{Al,d}=h_d^{-r_{Al}})$。

Bob 随机选取短期私钥 $esk_B=\tilde{y}_1,\cdots,\tilde{y}_n\in Z_p^n$，分别计算 $y_1=H_1(\tilde{y}_1,\{SK_B\}),\cdots,y_n=H_1(\tilde{y}_n,\{SK_B\})$，定义向量 $v_B=(y_1,\cdots,y_n)$。对共享矩阵 M_B，使得 Alice 的属性集 S_A 满足 M_B，计算 $\lambda_{Bi}=(M_B)_i\cdot v_B$。随机选取 $r_{B1},\cdots,r_{Bl}\in Z_p$，短期公钥 epk_B 计算如下：

$C_B'=g^{y_1}$，

$(C_{B1}=g^{\alpha\lambda_{B1}}h_{\rho_B(1)}^{-r_{B1}},D_{B1}=g^{r_{B1}},\forall d\in\Gamma_B/\rho_B(1),Q_{B1,d}=h_d^{-r_{B1}}),\cdots,$

$(C_{Bl}=g^{\alpha\lambda_{Bl}}h_{\rho_B(l)}^{-r_{Bl}},D_{Bl}=g^{r_{Bl}},\forall d\in\Gamma_B/\rho_B(l),Q_{Bl,d}=h_d^{-r_{Bl}})$

需要说明的是：d 表示属性；$\Gamma/\rho(i)$表示如果集合 Γ 中存在属性 $\rho(i)$，则移除。

Alice 和 Bob 彼此交换 epk_A,epk_B，如果 S_A 不满足(M_B,ρ_B)或 S_B 不满足(M_A,ρ_A)，协议终止，否则计算如下：

对于 Alice：定义集合 $I_A\subset\{1,2,\cdots,l\}$，$I_A=\{i:\rho_B(i)\in S_A\}$。存在$\{\omega_{Ai}\in Z_p\}_{i\in I_A}$，使得 $\sum_{i\in I_A}\omega_{Ai}(M_B)_i=(1,0,\cdots,0)$，$\sum_{i\in I_A}\omega_{Ai}\lambda_{Bi}=y_1$。

定义集合 Δ_A，如下所示：

$\Delta_A=\{attr:\exists i\in I_A,\rho_B(i)=attr\}$，$\Delta_A\in S_A$，$\Delta_A\in\Gamma_B$。

定义函数 $f(\Delta_A)=\prod_{attr\in\Delta_A/\rho_B(i)}h_{attr}$，计算：

$\tilde{C}_{Bi}=C_{Bi}\cdot\prod_{attr\in\Delta_A/\rho_B(i)}Q_{Bi,attr}=g^{\alpha\lambda_{Bi}}f(\Delta_A)^{-r_{Bi}}$

$\tilde{K}_A=\prod_{attr\in\Delta_A}h_{attr}^{t_A}=f(\Delta_A)^{t_A}$

会话密钥 K_A 计算如下：

$$\delta_1=e(g,g)^{\alpha\cdot y_1}=\frac{e(K_A,C_B')}{e(\prod_{i\in I_A}\tilde{C}_{Bi}^{\omega_{Ai}},L_A)\cdot e(\prod_{i\in I_A}\tilde{D}_{Bi}^{\omega_{Ai}},\tilde{K}_A)}$$

$$\delta_2=(e(g,g)^{\alpha})^{x_1}=e(g,g)^{\alpha x_1}$$

$$\delta_3=(C_B')^{x_1}=g^{y_1x_1}$$

$$K_A=H_2(\delta_1,\delta_2,\delta_3,epk_A,epk_B)$$

对于 Bob：定义集合 $I_B\subset\{1,2,\cdots,l\}$，$I_B=\{i:\rho_A(i)\in S_B\}$。存在$\{\omega_{Bi}\in Z_p\}_{i\in I_B}$，使得 $\sum_{i\in I_B}\omega_{Bi}(M_A)_i=(1,0,\cdots,0)$，$\sum_{i\in I_B}\omega_{Bi}\lambda_{Ai}=x_1$。

定义集合 Δ_B，如下所示：

$\Delta_B=\{attr:\exists i\in I_B,\rho_A(i)=attr\}$，$\Delta_B\in S_B$，$\Delta_B\in\Gamma_A$。

定义函数 $f(\Delta_B)=\prod_{attr\in\Delta_B/\rho_A(i)}h_{attr}$，计算：

$$\tilde{C}_{Ai}=C_{Ai}\cdot\prod_{attr\in\Delta_B/\rho_A(i)}Q_{Ai,attr}=g^{\alpha\lambda_{Ai}}f(\Delta_B)^{-r_{Ai}}$$

$$\tilde{K}_B=\prod_{attr\in\Delta_B}h_{attr}^{t_B}=f(\Delta_B)^{t_B}$$

会话密钥 K_B 计算如下：

$$\delta_1=(e(g,g)^{\alpha})^{y_1}=e(g,g)^{\alpha y_1}$$

$$\delta_2=e(g,g)^{\alpha\cdot x_1}=\frac{e(K_B,C_A')}{e(\prod_{i\in I_B}\tilde{C}_{Ai}^{\omega_{Bi}},L_B)\cdot e(\prod_{i\in I_B}D_{Ai}^{\omega_{Bi}},\tilde{K}_B)}$$

$$\delta_3=(C_A')^{y_1}=g^{x_1y_1}$$

$$K_B=H_2(\delta_1,\delta_2,\delta_3,epk_A,epk_B)$$

验证可得：$K=K_A=K_B$，Alice 和 Bob 协商出会话密钥 K。

4.3 安全性证明

定义 3 在 CDH 假设和判定性 q-*parallel*BDHE 假设下，给定 H_1，H_2 随机预言机，不存在多项式时间算法的敌手以不可忽略的优势赢得安全性游戏。

证明：测试会话的会话密钥 $K=H_2(\delta_1,\delta_2,\delta_3,epk_A,epk_B)$，$K$ 由五元组通过哈希函数映射而成，攻击者把 K 和随机值区分开来，只有通过以下两种方法：

(1)伪装攻击：攻击者询问 H_2，得到五元组的信息。

(2)密钥复制攻击：攻击者成功建立另一个会话作为测试会话，该会话有同样的 K。

在随机预言模型中，H_1，H_2 是理想的，输出均匀且无碰撞的哈希函数；并且根据协议描述可知，不同的会话过程会产生不同的五元组，因此，密钥复制攻击成功的概率是可以忽略的，所以，攻击者只进行如下的伪装攻击。

下面分为匹配会话存在和匹配会话不存在两种情况给予证明。

(1)匹配会话存在

模拟者随机选择实体 A 和实体 B 之间的一对匹配会话，标记为 $comm_A$ 和 $comm_B$，匹配会话分别由 A,B 发送，当任何一个会话被激活时，模拟者产生 $comm_A\leftarrow X_0\in G$，$comm_B\leftarrow Y_0\in G$。攻击者选择其中一个作为测试会话，此时，攻击者能区分被模拟者模拟的安全性游戏与真实安全性游戏的唯一方法是向 H_1 询问$(\{esk_A\},\{sk_A\})$或$(\{esk_B\},\{sk_B\})$，根据新鲜性定义，敌手无法同时揭示$(\{esk_A\},\{sk_A\})$和$(\{esk_B\},\{sk_B\})$，敌手猜测这种询问。敌手询问 H_2（五元组表示为 δ_i，δ_j，$\delta_{i,j}$，epk_i，epk_j），如果攻击者赢得了伪装攻击，那么模拟者可得 $\delta_{i,j}=CDH(X_0,Y_0)$。

(2)匹配会话不存在

模拟者随机选择实体 A 和实体 B 之间的一个会话，设 A 为协议发起方。模拟者用 L_{H_1}，L_{H_2} 记录攻击者对 H_1，H_2 的询问，以 K_i 记录攻击者对会话密钥的揭示。

初始化：安全性游戏中，模拟者欲挑战的 q-*parallel*BDHE 组为 y,T，攻击者欲挑战的访问结构为(M^*,ρ^*)，注意到，共享生成矩阵 M^* 为 $l^*\times n^*$，且 $l^*,n^*\leqslant q$。模拟者选择一个随机值 $\alpha'\in Z_p$，使得 $\alpha=\alpha'+a^{q+1}$，即 $e(g,g)^{\alpha}=e(g^a,g^{a^q})e(g,g)^{\alpha'}$。对于属性 $x\in U$，定义 $X=\{i:\rho^*(i)=x\}$，h_x 计算如下：

$X=\emptyset$，$h_x=g^{z_x}$；

$X\neq\emptyset$，$h_x=g^{z_x}\prod_{i\in X}g^{aM_{i,1}^*/b_i}\cdot g^{aM_{i,2}^*/b_i}\cdots g^{a^{n^*}M_{i,n^*}^*/b_i}$；$z_x$ 为 Z_p 上的随机值。

随机预言机 H_2：攻击者询问 H_2，其中 $K_i=H_2(\delta_i,\delta_j,\delta_{i,j},epk_i,epk_j)$，对于五元组 $L_{H_2}=(\delta_i,\delta_j,\delta_{i,j},epk_i,epk_j)$ 由模拟者维护，对于模拟者，如果有 $\delta_i=e(g^a,g^{a^q})e(g,X_0)^{\alpha'}$ 或 $\delta_j=e(g^a,g^{a^q})e(g,Y_0)^{\alpha'}$，返回 K_i 并记录，否则，随机选取 $K_i\in\{0,1\}^k$ 并返回。

StaticReveal(S_U)：对于攻击者要挑战属性集 S_U（S_U 不满足秘密共享矩阵 M^*），模拟者回答这种询问并返回私钥。模拟者选取随机值 $r\in Z_p$；构造向量 $w=(\omega_1,\cdots,\omega_{n^*})\in Z_p^{n^*}$，$\omega_1=-1$，$\forall i,\rho^*(i)\in S_U$，都有 $w\cdot M_i^*=0$。模拟者定义 t：

$t=r+\omega_1a^q+\cdots+\omega_{n^*}a^{q-n^*+1}$，私钥构造如下：

$$L=g^r\prod_{i=1,\cdots,n^*}(g^{a^{q+1-i}})^{\omega_i}=g^t$$

注意到 g^{α} 中存在 $g^{-a^{q+1}}$，为了消除 $g^{-a^{q+1}}$，K 计算如下：

$$K=g^{\alpha'}g^{\alpha r}\prod_{i=2,\cdots,n^*}(g^{a^{q+2-i}})^{\omega_i}$$

对于 K_x $\forall x\in S_U$，如果 $x\in S_U$，$\forall i,\rho^*(i)\neq x$，此时有 $K_x=L^{z_x}$；否则，K_x 计算如下：

$$K_x=L^{z_x}\prod_{i\in X}\prod_{j=1,\cdots,n^*}(g^{(a^j/b_i)^r}\cdot\prod_{\substack{k=1,\cdots,n^*\\k\neq j}}(g^{a^{q+1+j-k}/b_i})^{\omega_k})^{M_{i,j}^*}$$

X 表示：$X=\{i:\rho^*(i)=x\}$。

Send(m)：模拟者选择随机值 $y_2',\cdots,y_{n^*}'$，构造秘密共享向量 $v=(s,sa+y_2',\cdots,sa^{n-1}+y_{n^*}')\in Z_p^{n^*}$，$s$ 是秘密共享值。

模拟者定义集合 $R_i=\{k:k\neq i,\rho^*(i)=\rho^*(k)\}$，其中 $i=1,\cdots,n^*$。选取随机值 $r_1',\cdots,r_l'$，$r_i=r_i'+sb_i$，计算如下：

$$D_i=g^{r_i'}g^{sb_i}$$

$$C_i=h_{\rho^*(i)}^{-r_i'}(\prod_{j=2,\cdots,n^*}(g^a)^{M_{i,j}^*y_j'})\cdot(g^{b_i\cdot s})^{-z_{\rho^*(i)}}\cdot(\prod_{k\in R_i}\prod_{j=1,\cdots,n^*}(g^{a^js(b_i/b_k)})^{M_{k,j}^*})$$

Γ 表示秘密共享矩阵 M^* 中关联的不同属性的集合。对于 $\forall x\in\Gamma/\rho^*(i)$，计算如下：

$$Q_{i,d}=h_d^{-r_i'}(g^{b_is})^{-z_d}(\prod_{k\in R_d}\prod_{j=1,\cdots,n^*}(g^{a^js(b_i/b_k)})^{M_{k,j}^*})$$

模拟者返回短期公钥 epk_i。

SessionReveal(sid)：攻击者询问 H_2，如果$(\delta_i,\delta_j,\delta_{i,j},epk_i,epk_j)\in L_{H_2}$，此时 $T=e(g,g)^{a^{q+1}s}$，返回 K_i，否则返回随机值。

(下转第 177 页)

cessing,2004,52(12):3409-3416
[18] 张旭淘,贺国光,卢宇. 一种在线实时快速地判定交通流混沌的组合算法[J]. 系统工程,2005,23(9):42-45
[19] 顾圣士,王志谦,程极泰. 太阳黑子数时间序列的分形研究及预测[J]. 应用数学与力学,1999,20(1):81-86
[20] Weigend A S, Huberman B A, Rumelhart D E. Predicting the future: A connectionist approach[J]. International Journal of Neural System,1990,1(3):1993-209
[21] 伍春香,刘琳,王葆元. 三层 BP 网隐层节点数确定方法的研究[J]. 计算机学报,1998(6):2-5
[22] 于青. 关联维数计算的分析研究[J]. 计算机学报,2004(12):1-2
[23] 张德平,汪帅,周吴杰. 基于 EMD 和 GEP 的软件可靠性预测模型[J]. 计算机科学,2013,40(4):164-168

(上接第 154 页)

根据新鲜性定义,攻击者不允许进行 MasterReveal 询问,不允许同时揭示测试会话的长期私钥和短期私钥,攻击者询问 SessionReveal(*sid*),如果攻击者能以不可忽略的优势赢得安全性游戏,那么模拟者就成功解决了判定性 *q-parallel*BDHE 假设。

4.4 效率分析

本文提出的 ABAKA 协议中整个算法仅有 3 个双线性运算,具有较高的计算效率。n 表示用户属性集个数,本文 ABAKA 与其他密钥协商协议的比较如表 2 所列。

表 2 各密钥协商协议的分析与比较

协议	长期私钥空间	安全模型	双线性运算个数
Y[11]	(2n+1)|G|	ABeCK	2n+1
Y[13]	(n+2)|G|	ABCK	2n+2
本协议	(n+2)|G|	ABeCK	3

对本协议与 Y[11] 密钥协商阶段的计算进行比较,仿真如图 1 所示。

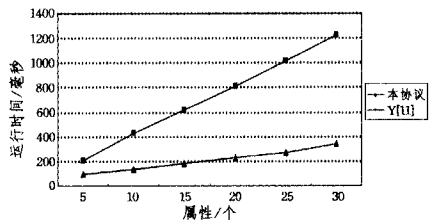

图 1 本协议与 Y[11] 密钥协商阶段的计算效率比较

硬件:Intel T6600@2.2GHz,2GBytes RAM,平台:Windows,代码库:Miracl。

文献[8]指出,群 G,G_T 上的一个乘法运算效率是 0.0034 毫秒,一个双线性运算效率是 8.22 毫秒,双线性运算效率明显较低。表 2 表明:方案 Y[11] 和 Y[13] 中,双线性运算个数与属性个数相关,效率为 $O(n)$,本文提出的 ABAKA 中整个算法只有 3 个双线性运算,效率为 $O(1)$,且用户私钥空间开销较小。图 1 的仿真结果表明:本文提出的 ABAKA 由于双线性运算个数只有 3 个,不再与用户属性个数线性相关,因此具有更高的运算效率。

结束语 本文分析了多种基于属性的加密方案,提出了一种新的高效且具有灵活访问结构的密文策略的属性加密方案,并在该加密方案的基础上提出了一个高效的基于属性的密钥协商协议。该协议采用秘密共享方案,能够表示任意访问结构,且解密效率较高,适用于计算和存贮资源有限的网络系统。但该协议占用较大的密文空间,如何减少密文的长度是今后需要进一步研究的工作。

参 考 文 献

[1] Diffie W, Hellman M. New directions in cryptography [J]. IEEE Transactions on Information Theory,1976,22 (6):644-654
[2] Sahai A, Waters B. Fuzzy identity-based encryption [M]// Advances in Cryptology-EUROCRYPT2005. Springer Berlin Heidelberg,2005:457-473
[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//Proceedings-IEEE Symposium on Security and Privacy. Berkeley,CA,United states,2007:321-334
[4] Cheung L, Newpor C. Provably secure ciphertext policy ABE [C]// Proceedings of the ACM Conference on Computer and Communications Security. Alexandria,VA,United states,2007:456-465
[5] Waters B. Ciphertext-policy attribute-based encryption: An expressive,efficient,and provably secure realization[C]//14th International Conference on Practice and Theory in Public Key Cryptography,PKC 2011. Taormina,Italy,2011:53-70
[6] Ge Ai-jun, Zhang Rui, Chen Cheng, et al. Threshold Ciphertext Policy Attribute-Based Encryption with Constant Size Ciphertexts[C]//17th Australasian Conference on Information Security and Privacy, ACI SP2012. Wollongong, NSW, Australia, 2012,7372:336-349
[7] Attrapadung N, Herranz J, Laguillaumie F, et al. Attribute-based encryption schemes with constant size ciphertexts[J]. Theoretical Computer Science,2012,422:15-38
[8] Hohenberger S, Waters B. Attribute-Based Encryption with Fast Decryption[M]// Public-Key Cryptography PKC2013. Springer Berlin Heidelberg,2013:162-179
[9] Wang Hao, Xu Qiu-liang, Ban Tao. A provably secure two-party attribute-based key agreement protocol[C]// Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP' 09. Fifth International Conference on. IEEE,2009:1042-1045
[10] Wang Hao, Xu Qiu-Liang, Fu Xiu. Two-party attribute-based key agreement protocol in the standard model[C]// Proceedings of the 2009 International Symposium on Information Processing (ISIP 2009). 2009:325-328
[11] Yoneyama K. Strongly secure two-pass attribute-based authenticated key exchange[C]//4th International Conference on Pairing-Based Cryptography, Pairing 2010. Kaga, Japan, 2010, 6487:147-166
[12] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange[C]// 1st International Conference on Provable Security 2007. Wollongong, NSW, Australia, 2007, 4784:1-16
[13] Yoneyama K. Two-party round-optimal session-policy attribute-based authenticated key exchange without random oracles[C]// 14th International Conference on Information Security and Cryptology,ICISC 2011. Seoul,Korea,2012,7259:467-489
[14] 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交换协议[J]. 电子与信息学报,2012,34(2):451-456
[15] Shamir A. How to share a secret[J]. Communications of the ACM,1979,22(11):612-613