一个高效的属性基密钥协商协议

陈 健[1] 王小英[2] 王永涛[3] 李尧森[1]
(防灾科技学院教务处 三河 065201)[1] (防灾科技学院灾害信息工程系 三河 065201)[2]
(中国信息安全测评中心 北京 100085)[3]

摘 要 提出一个高效的属性基密钥协商协议。由于属性基密钥协商协议具有模糊鉴别的特性,近年来成为密钥协商协议的研究热点。基于当前最高效的属性基加密方案的密钥提取形式,构建了一个两方高效的属性基密钥协商协议。新协议实现了较丰富的访问结构且计算效率较高,同时在标准模型下基于判定 q 并行双线性 Diffie-Hellman 指数假定(Decisional q-parallel Bilinear Diffie-Hellman Exponent Assumption)证明了协议的安全性。

关键词 访问结构,属性基加密,密钥协商,模糊鉴别,标准模型
中图法分类号 TP309 文献标识码 A

Efficient Attribute Based Key Agreement Protocol

CHEN Jian[1] WANG Xiao-ying[2] WANG Yong-tao[3] LI Yao-sen[1]
(Institute of Disaster Prevention, Sanhe 065201, China)[1] (Institute of Disaster Prevention, Sanhe 065201, China)[2]
(China Information Technology Security Evaluation Center, Beijing 100085, China)[3]

Abstract We proposed an efficient attribute based key agreement protocol. Due to the property of fuzzy identification on the participants of the protocol, attribute based key agreement protocol has been a hot topic of research in recent years. We presented a concrete construct of a two-party efficient attribute based key agreement protocol, based on the key abstraction of the most efficient attribute based encryption scheme at present. The new protocol achieves more expressive access structure and is effcient. Futhermore, the new protocol was proved secure in the standard model under the decisional q-parallel bilinear diffie-hellman exponent assumption(BDHE).

Keywords Access structure, Attribute based encryption, Key exchange, Fuzzy idenfication, Standard model

属性基加密体制由 Sahai 和 Waters[1] 于 2005 年提出,由于它的诸多特性,例如模糊鉴别、支持对加密数据的灵活访问控制以及实现了一对多保密通信等,近几年得到了广泛的研究。相关研究主要体现在实现更丰富的访问结构以及效率的提高上。属性基加密体制可看作是身份基加密体制同访问结构相结合的产物,根据访问结构的嵌入位置不同,例如嵌入到密钥中或嵌入到密文中,属性基加密体制又划分为密钥策略属性基加密体制和密文策略属性基加密体制。两种属性基加密体制各有优点,均有不同的应用前景。

属性基加密体制体现的核心思想对公钥密码体制的研究具有很强的理论和现实意义。通过将访问结构嵌入到密码体制中,可实现相应具有模糊鉴别特性的密码体制。模糊鉴别特性在带宽或计算受限的环境下具有一定的应用背景,模糊鉴别的程度可自由调节(通过指定的访问结构来控制),具有很强的灵活性,即密码体制中的实体可根据具体情况(需求的模糊鉴别程度、带宽、计算花销等)的不同,依据访问结构灵活实现对密码体制中客体的访问控制。传统的加密体制、签名体制、密钥协商体制等均不具备这样的特性。

属性基密钥协商协议[2-6]在传统密钥协商协议的基础上引入了属性基加密体制的思想,实现了较灵活的模糊鉴别特性。传统两方密钥协商协议假定了相互唯一的意向通信实体,而这在某些特定应用场景[6]并不太适用。属性基密钥协商协议放宽了该条件,仅假定了满足一方指定访问结构的实体即可为该方的意向通信实体。通过指定灵活的访问结构,属性基密钥协商协议可以实现较复杂的访问控制,这是传统交换协议(例如身份基密钥协商协议)难以实现的特性。

目前[2-7]文献中存在一些研究者设计的属性基密钥协商协议,但这些协议不是实现的访问结构比较简单,就是执行效率不高。鉴于上述考虑,本文设计了一个高效且支持复杂访问结构的属性基密钥协商协议

Waters[8]提出一个支持强表达能力的访问结构且高效率的密文策略属性基加密方案,为当前最高效的属性基加密方案。本文基于该方案的密钥提取形式,构建了一个两方高效的属性基密钥协商协议。新协议为消息策略的属性基密钥协商协议,有关消息策略的定义及说明请参见文献[7]。新协议实现了较丰富的访问结构,同时在标准模型下证明了协议的安全性。

本文受河北省人文社会科学类青年基金项目(SQ137005)资助。
陈 健(1979—),男,硕士,讲师,主要研究方向为计算机应用,E-mail:cj-979@163.com;王小英(1979—),女,硕士,讲师,主要研究方向为网络与信息安全、密码学;王永涛(1980—),男,博士,助理研究员,主要研究方向为信息安全、密码学;李尧森(1986—),男,硕士,主要研究方向为高等教育学。

1 基础知识

1.1 双线性对及困难问题假定

本节简要回顾构建协议所使用的双线性对[9]的定义以及协议安全证明所需的相关假定。

定义1 设$\mathbb{G}$,$\mathbb{G}_T$是阶为素数p的两个乘法循环群,设g是群$\mathbb{G}$的一个生成元,假如一个映射$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$,满足下面的条件:

1)双线性性:对于所有的$u,v\in\mathbb{G}$和$a,b\in\mathbb{Z}_p$,映射满足$e(u^a,v^b)=e(u,v)^{ab}$;

2)非退化性:$e(g,g)\neq 1_{\mathbb{G}_T}$;

3)可计算性:对于所有的$u,v\in\mathbb{G}$,存在有效的算法计算$e(u,v)$;

那么称上述映射为一个对称的双线性对。

定义2 判定q并行双线性Diffie-Hellman指数假定(Decisional q-parallel Bilinear Diffie-Hellman Exponent Assumption,decisional q-parallel BDHE)[8]:设随机选取$a,s,b_1,\cdots,b_q\in\mathbb{Z}_p$,$g$群$\mathbb{G}$的一个生成元,该假定指的是,给定

$$\vec{y}=g,g^s,g^a,\cdots,g^{(a^q)},g^{(a^{q+2})},\cdots,g^{(a^{2q})}$$

$$\forall_{1\leqslant j\leqslant q}g^{s\cdot b_j},g^{a/b_j},\cdots,g^{(a^q/b_j)},g^{(a^{q+2}/b_j)},\cdots,g^{(a^{2q}/b_j)}$$

$$\forall_{1\leqslant j,k\leqslant q,k\neq j}g^{a\cdot s\cdot b_k/b_j},\cdots,g^{a^q\cdot s\cdot b_k/b_j}$$

不存在多项式时间的敌手B有不可忽略的优势区分元组$(\vec{y},T=e(g,g)^{a^{q+1}s})$和元组$(\vec{y},T=R)$,其中$R\in\mathbb{G}_T$是随机的。设$\kappa$表示安全参数,敌手B的优势函数$Adv_B^{BDHE}(\kappa)$有如下定义:

$$Adv_B^{BDHE}(\kappa)=|\Pr[B(\vec{y},T=e(g,g)^{a^{q+1}s})=0]-\Pr[B(\vec{y},T=R)=0]|$$

1.2 访问结构

定义3(访问结构定义[10]) 设$\{P_1,P_2,P_3,\cdots,P_n\}$是$n$个参与者的集合。设$\mathbb{A}$表示由参与者集合的子集构成的集合,$B,C$表示参与者集合的子集,对于所有的$B,C$:如果$B\in\mathbb{A}$并且$B\subseteq C$,那么$C\in\mathbb{A}$,则$\mathbb{A}$是一个单调的访问结构。一个访问结构(或者单调的访问结构)$\mathbb{A}$是一个非空的参与者集合的子集(或者单调子集)构成的集合。设D表示参与者的任一子集,如果$D\in\mathbb{A}$,则称其为授权集合,如果$D\notin\mathbb{A}$,则非授权集合。

定义4(线性秘密共享方案,Linear Secret-Sharing Schemes,LSSS[10]) 一个参与者集合P上定义的秘密共享方案Π如果满足以下条件则被称为线性的:

1)各方的秘密份额形成一个$\mathbb{Z}_p$上的向量;

2)存在一个$l\times n$的称为Π的秘密份额生成矩阵M,对$i=1,\cdots,l$,标识M的第i行为$\rho(i)$,其中$\rho(\cdot)$为一个从$i=1,\cdots,l$到P上的一个映射。对于列向量$v=(s,r_2,\cdots,r_n)$,其中$s\in\mathbb{Z}_p$为秘密,$r_2,\cdots,r_n\in\mathbb{Z}_p$为随机值,则$Mv$就是利用$\Pi$得到的关于$s$的$l$个共享份额组成的向量,其中$(Mv)_i$属于参与者$\rho(i)$。

本文协议所实现的访问结构为上述定义中的访问结构,且为消息策略的形式。

1.3 消息策略属性基密钥协商协议形式化定义和安全模型

两方的消息密钥策略属性基密钥协商协议由以下3个算法组成。

Setup:初始化算法,输入为安全参数κ,输出一个系统主公钥mpk和一个系统主密钥msk。

KeyGeneration:输入系统密钥msk,一个用户拥有的属性集合S,算法返回该用户的私钥。

KeyAgreement:一个在两方实体之间交互的协议,用户A选择一个LSSS访问结构(M,ρ),并计算消息M_A,然后发送(广播)该消息;另一个用户B可响应A的密钥协商请求,选择一个LSSS访问结构(M',ρ'),并计算消息M_B发送(广播)。如果用户A拥有的属性集合S_A满足(M',ρ')且用户B的属性集合S_B满足(M,ρ),那么用户A和用户B可以计算一个会话密钥K。

本文安全模型的基础来自Liqun Chen和Caroline Kudla[11],并参考了文献[7]中的表述及修改。有关安全模型的具体细节请参阅文献,这里仅作简单陈述。

设参与者集合为U,用一个预言机$\Pi_{I,J}^n$来模型化集合中的每个参与者的行为,该预言机表示参与者I认为他正在与参与者J执行第n次会话协议。设敌手A被模型化为一个概率多项式时间的图灵机,它对所有参与者的预言机具有访问权限。假定敌手A事先声明一个访问结构T^*作为攻击对象。A被称为一个良性的敌手,如果敌手A只是简单地在参与者之间传递消息。敌手在任何时候可以做的询问包括$Create$询问(根据敌手需要创建一个新参与者)、$Corrupt$询问(返回敌手指定参与者的长期私钥)、$Send$询问(允许敌手向任何一个预言机发送他选择的消息)、$Reveal$询问(根据敌手指定参与者的预言机来返回该预言机持有的会话密钥)。

预言机所处的可能状态包括:接受状态(此时接受了一个会话密钥)、拒绝状态(此时预言机决定不建立会话密钥并中止协议)、特殊状态(记为$*$,表示预言机尚未接受或拒绝会话密钥)、公开状态(预言机回答过$Reveal$询问后处于该状态)和腐化状态(预言机回答了$Corrupt$询问后处于该状态)。攻击最后敌手可针对它选择的适当预言机进行一次$Test$询问;回答该询问,模拟器随机抛一枚公平的硬币μ,根据μ来决定返回该预言机持有的会话密钥是否是一个随机值。敌手最后输出一个μ'作为对μ的猜测。敌手的优势如下定义:

$$Adv_A(\kappa)=|\Pr[\mu'=\mu]-\frac{1}{2}|$$

有关匹配会话以及更详细的模型说明请参阅先前的资料文献,下面给出一个认证密钥协商协议是一个安全的协议的条件。

定义5[12] 如果下述条件满足,则一个协商协议是一个安全的认证密钥协商协议:

1)在存在良性的敌手情况下,两个有匹配会话的预言机$\Pi_{I,J}^n$和$\Pi_{J,I}^t$,总是能处于接受状态并持有相同的会话密钥,且会话密钥均匀随机分布于$\{0,1\}^k$;对于其它敌手有下述条件满足;

2)如果两个预言机$\Pi_{I,J}^n$和$\Pi_{J,I}^t$有匹配会话且都没回答过$Corrupt$询问,那么两个预言机均处于接受状态且持有相同的会话密钥;

3)$Adv_A(\kappa)$是可忽略的。

2 高效的消息策略属性基密钥协商协议

2.1 协议描述

Waters[8]提出一个密文策略属性基加密方案,该方案是当前最高效的加密方案且访问结构表达能力丰富。本文协议

基于 Waters 等[8]的密文策略属性基加密方案中的密钥提取形式设计了一个两方的消息策略的属性基密钥协商协议，协议具体描述如下。

Setup(U)：算法输入系统中的属性数量 U，根据安全参数 κ 生成阶为素数 p 双线性对群 $\mathbb{G}$，一个群 $\mathbb{G}$ 的生成元 g。然后，随机选择 $h_1,\cdots,h_U\in\mathbb{G}$ 与系统中的 U 个属性相对应。此外，随机选择 $a,\alpha\in\mathbb{Z}_p$，如下设置系统主公钥 mpk 和系统主密钥 msk 为：

$$mpk=g,e(g,g)^{\alpha},g^{a},h_1,\cdots,h_U$$

$$msk=g^{\alpha}$$

KeyGeneration(S,msk)：设用户拥有属性集合 S，私钥生成如下，随机选择 $t\in\mathbb{Z}_p$，设置私钥为：

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

KeyAgreement：设用户 A 的属性集合为 S_A，A 预同其他用户协商一个会话密钥，希望该用户的属性集合满足 A 指定的访问结构。A 选择一个 LSSS 访问结构 (M,ρ)，设 M 为一个 $l\times n$ 的生成矩阵，$\rho(\cdot)$ 映射矩阵的行为一个属性。A 选择随机向量 $\vec{v}=(s_1,y_2,\cdots,y_n)$，对于 $i=1,\cdots,l$，计算 $\lambda_i=\vec{v}\cdot M_i$。此外，随机选择 $r_1,\cdots,r_l\in\mathbb{Z}_p$，如下设置消息为：

$$\mathrm{M}_A=\{(M,\rho),C'=g^{s_1},(C_1=g^{a\lambda_1}h_{\rho(1)}^{-r_1},D_1=g^{r_1}),\cdots,$$

$$(C_l=g^{a\lambda_1}h_{\rho(l)}^{-r_l},D_l=g^{r_l})\}$$

设用户 B 的属性集合为 S_B，且满足 A 指定的访问结构，用户 B 预响应 A 的密钥协商请求（A 潜在的密钥协商对象有多个）。同样，用户 B 也可指定一个访问结构来验证 A 是否满足。B 选择一个 LSSS 访问结构 (M',ρ')，B 选择随机向量 $\vec{v}'=(s_2,y'_2,\cdots,y_n')$，对于 $i=1,\cdots,l$，计算 $\lambda_i'=\vec{v}'\cdot M_i'$。此外，随机选择 $r_1',\cdots,r_l'\in\mathbb{Z}_p$，如下设置消息为：

$$\mathrm{M}_B=\{(M',\rho'),C'=g^{s_2},(C_1=g^{a\lambda_1'}h_{\rho'(1)}^{-r_1'},D_1=g^{r_1'}),\cdots,$$

$$(C_l=g^{a\lambda_1'}h_{\rho'(l)}^{-r_l'},D_l=g^{r_l'})\}$$

如果 S_A 满足 (M',ρ') 且 S_B 满足 (M,ρ)，那么 A 和 B 可计算一个会话密钥 K。

A 根据私钥和 M_B 如下计算得到 $K_B=e(g,g)^{\alpha_2}$：设 $I\subset\{1,2,\cdots,l\}$ 并定义 $I=\{i:\rho'(i)\in S_A\}$，设 $\{w_i\in\mathbb{Z}_p\}_{i\in I}$ 为一个常量集合（根据访问结构定义，该集合确实存在）并且满足 $\sum_{i\in I}w_i\lambda_i'=s_2$，可如下计算：

$$\frac{e(C',K)}{\prod_{i\in I}(e(C_i,L)\cdot e(D_i,K_{\rho'(i)}))^{w_i}}$$

$$=\frac{e(g,g)^{\alpha s_2}\cdot e(g,g)^{at s_2}}{\prod_{i\in I}e(g,g)^{at\lambda'_i w_i}}=e(g,g)^{\alpha_2}$$

然后设置会话密钥为 $\mathrm{K}'=K_B(e(g,g)^{\alpha})^{s_1}=e(g,g)^{\alpha(s_1+s_2)}$。同样用户 B 根据私钥和 M_A 计算得到 $K_A=e(g,g)^{\alpha_1}$，再设置会话密钥为 $\mathrm{K}'=K_A\cdot(e(g,g)^{\alpha})^{s_s}=e(g,g)^{\alpha(s_1+s_2)}$。上述计算的 K' 还可以进一步通过一个密钥提取函数来提取会话密钥。例如设 $H:\{0,1\}^*\to\{0,1\}^k$ 为这样的一个函数，则 $\mathrm{K}=H(M_A\parallel M_B\parallel\mathrm{K}')$，其中 $k=|\mathrm{K}|$。

2.2 安全性证明

上述协议的正确性由 Waters[8] 的密文策略属性基加密方案的正确性来保证，很容易证明。这里仅给出协议的安全性证明。协议在选择安全模型下来证明，可支持扩展到完全安全模型。此处不在进一步探讨，可参阅文献来获得完全安全模型下的证明。

定理 1　在标准模型下，设判定 q-parallel BDHE 假定成立，上述协议是一个安全的认证密钥协商协议。

证明：根据安全认证密钥协商协议的定义中规定的要求，只要证明上述协议满足定义中的 3 个条件即可。前两个条件显然成立，这里不在详细讨论。下面给出满足第三个条件的证明。

假设存在一个概率多项式时间敌手 A，它以不可忽略的优势 ε 成功攻击协议。我们构建一个模拟器 B，它有不可忽略的优势 $\varepsilon/2q_o$ 解决判定 q-parallel BDHE 问题。

模拟器 B 输入一个判定 q-parallel BDHE 问题实例 $\vec{y},T$。设参与者集合为 $\{1,2,\cdots,N\}$，对于 $\theta\in\{1,\cdots,N\}$，设 S_θ 表示用户 θ 的属性集合。设 A 在攻击中最多创建 q_o 个预言机，定义符号 $\Pi_{\theta,\sigma}^t$ 为系统所有用户实例的第 t 个用户实例。为每一个预言机，B 维护一个列表 Ω。B 随机选择 $1\leqslant R\leqslant q_o$ 并猜测敌手 A 在此处将做 $Test$ 询问，并记为 $\Pi_{A,B}^R$，其中 $1\leqslant A,B\leqslant N$，并且假设在第 R 个预言机，有 S_A 满足发送给 A 的消息中指定的访问结构。假设敌手 A 选择的挑战访问结构为 (M^*,ρ^*)，其中 M^* 有 n^* 列。

B 模拟系统的 Setup 阶段如下，选择 $a'\in\mathbb{Z}_p$，从 $\vec{y}$ 中取 g,g^a,g^{a^q} 并设置 $e(g,g)^{\alpha}=e(g^a,g^{a^q})e(g,g)^{\alpha'}$。对每一个 $1\leqslant x\leqslant U$，随机选择 $z_x\in\mathbb{Z}_p$，设 X 表示满足 $\rho^*(i)=x$ 的 i 的集合，B 设置 h_x 如下：

$$h_x=g^{z_x}\prod_{i\in X}g^{aM_{i,1}^*/b_i}\cdot g^{a^2M_{i,2}^*/b_i}\cdots g^{a^{n^*}M_{i,n^*}^*/b_i}$$

至此，完成了 Setup 阶段的所有参数的模拟，且参数均为随机分布。然后，B 可以回答如下询问。

$Corrupt(\theta)$：如果 S_θ 满足 (M^*,ρ^*)，模拟器中止，否则按照文献[8]证明中模拟器生成私钥的方式来返回私钥。随机选择 $r\in\mathbb{Z}_p$，找到一个向量 $\vec{w}=(w_1,\cdots,w_{n^*})$ 满足 $w_1=-1$ 且对所有 $\rho^*(i)\in S$ 的 i 满足 $\vec{w}\cdot M_i^*=0$。根据 LSSS 的定义该向量肯定存在　设置

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

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

对于 $\forall x\in S$，如果不存在 i 满足 $\rho^*(i)=x$，则设置 $K_x=L^{z_x}$；设 X 表示满足 $\rho^*(i)=x$ 的 i 的集合，其他的如下生成：

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

最后返回生成的私钥给敌手。

$Create(S)$：B 根据属性集合 S 创建一个新的预言机。然后同模拟 $Corrupt$ 询问一样来生成该预言机的私钥并保存，然后返回“Yes”给 A。

$Send(\Pi_{\theta,\sigma}^t,\mathrm{M})$：设 $K'_{\theta,\sigma}$ 表示 $\Pi_{\theta,\sigma}^t$ 接受的会话密钥，这里仅考虑处理预言机的第一次 $Send$ 询问。如果用户 θ 的属性集合 S_θ 不满足 M 中包含的访问结构，结束会话；如果 M 是抄本中的第二个消息，简单地接受该会话；否则继续处理。

1）当 $t\neq R$ 时，处理如下：模拟器按正常的协商协议执行，选择一个 LSSS 访问结构 (M,ρ)，选择随机向量 $\vec{v}=(s_1,y_2,\cdots,y_n)$，对于 $i=1,\cdots,n^*$，计算 $\lambda_i=\vec{v}\cdot M_i$，随机选择 $r_1,\cdots,r_{n^*}\in\mathbb{Z}_p$，如下设置消息为：

$$\mathrm{M}_\theta=\{(M,\rho),C'=g^{s_1},(C_1=g^{a\lambda_1}h_{\rho(1)}^{r_1},D_1=g^{r_1}),\cdots,$$

$$(C_{n^*}=g^{a\lambda_{n^*}}h_{\rho(n^*)}^{-r_{n^*}},D_{n^*}=g^{r_{n^*}})\}$$

此外，设置 $\mathrm{K}'_{\theta,\sigma}=K_\sigma\cdot(e(g,g)^{\alpha})^{s_1}$，其中 K_σ 可根据用户 θ 的私钥（可通过调用 $Corrupt(\theta)$ 获得）和自敌手收到的 M 来

（下转第 469 页）

节点个数下，3 种算法都具有较好的扩展性，其中 Canopy 算法具有最好的可扩展性。当数据量增大时，Canopy 算法相较 K-means 算法和模糊 K-means 算法速度优势更明显，在 8 个节点数据量为 pub4 时，Canopy 算法时间约为 K-means 算法的 1/15，为模糊 K-means 算法的 1/25，表明 Canopy 非常适合用于海量数据聚类的预处理。4. 随着节点个数不断增加，3 种算法的运行时间随着数据集的增加增长得越缓慢，但随着节点数的增加，模糊 K-means 算法的规模增长性减少幅度明显大于 K-means 算法，说明模糊 K-means 算法能更好地适应大规模并行计算平台。5. 由于 3 种算法都具有较好的加速比、可扩展性和可伸缩性，说明 Mahout 下的 3 种算法能很好地运行于 Hadoop 平台，可以有效地应用于海量数据的聚类。

参 考 文 献

[1] 赵卫中，马慧芳，傅燕翔，等. 基于云计算平台 Hadoop 的并行 k-means 聚类算法设计研究[J]. 计算机科学，2011(10)：166-168，176

[2] Owen S，Anil R，Dunning T，et al. Mahout in action[M]. USA：Manning Publications，2010

[3] 胡俊. 集群环境下聚类算法的并行化研究与实现[D]. 上海：华东师范大学，2010

[4] Ericson C，Pallickara S. On the performance of high dimensional data clustering and classification algorithms[J]. Future Generation Computer Systems，2013(29)：1024-1034

[5] 潘昊斌. 基于云计算的并行 K-means 气象数据挖掘研究与应用[D]. 南京：南京信息工程大学，2013

[6] 怀特. Hadoop 权威指南[M]. 北京：清华大学出版社，2010

[7] 王彦明，奉国和，薛云. 近年来 Hadoop 国外研究综述[J]. 计算机系统应用，2013，22(6)：1-5，28

[8] Apache Hadoop[OL]. http://Hadoop.apache.org

[9] Apache Mahout[OL]. http://Mahout.apache.org

[10] 张明辉. 基于 Hadoop 的数据挖掘算法的分析与研究[D]. 昆明：昆明理工大学，2012

(上接第 446 页)

计算(按协议正常计算即可)，而 s_1 为用户 θ 自己所随机选择的，故可如上设置 $K'_{\theta,\sigma}$。

2)如果 $t=R$，此时应有 $\theta=A$，设置 $C'=g^s$(取自判定 q-parallel BDHE 问题实例 $\vec{y}$)。选择一个 LSSS 访问结构(M,ρ)，直觉上，$\vec{v}$ 应该为：

$$\vec{v}=(s,sa+y_2',sa^2+y_3',\cdots,sa^{n-1}+y'_{n^*})\in Z_p^{n^*}$$

其中，$y_2',\cdots,y'_{n^*}\in Z_p$ 是随机选择的值。选择 $r_1',\cdots,r_l'\in Z_p$，对于 $i=1,\cdots,n^*$，定义 R_i 表示对于 $k\neq i$，有 $\rho^*(i)=\rho^*(k)$ 的一个 k 集合，如下设置 C_i,D_i：

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

$$C_i=h_{\rho^*(i)}^{r_i'}\Big(\prod_{j=2,\cdots,n^*}(g^a)^{M^*_{i,j}y_j'}\Big)(g^{b_i s})^{-z_{\rho^*(i)}}\cdot$$

$$\Big(\prod_{k\in R_i}\prod_{j=1,\cdots,n^*}(g^{a^j s(b_i/b_k)})^{M^*_{k,j}}\Big)$$

返回 $M_\theta=\{(M,\rho),C',(C_1,D_1),\cdots,(C_{n^*},D_{n^*})\}$。模拟器可以设置 $K'_{\theta,\sigma}=K_\sigma\cdot T\cdot e(g^s,g)^{\alpha'}$，其中 K_σ 可根据用户 θ 的私钥(可通过调用 $Corrupt(\theta)$ 获得)和自敌手收到的 M 来计算(按协议正常计算即可)，而 g^s 来自判定 BDHE 问题实例，α' 为模拟器自己随机选择的值，故可如上设置 $K'_{\theta,\sigma}$。

$Reveal(\Pi^t_{\theta,\sigma})$：如果询问的预言机是 $\Pi^R_{A,B}$，或者是它的匹配预言机 $\Pi^{R'}_{B,A}$，则模拟器中止。否则，返回该预言机持有的会话密钥给敌手。

$Test(\Pi^t_{\theta,\sigma})$：敌手最后对预言机询问一次 $Test$。如果敌手询问的不是 $\Pi^R_{A,B}$，模拟器中止。否则，需要预言机 $\Pi^R_{A,B}$ 处于接受状态，并且 $\Pi^R_{A,B}$，或者是它的匹配预言机 $\Pi^{R'}_{B,A}$ 没有回答过 $Reveal$ 询问，以及 A,B 没有回答过 $Corrupt$ 询问。模拟器抛一枚硬币 μ，如果 $\mu=0$，返回 $\Pi^R_{A,B}$ 持有的会话密钥，否则随机返回会话密钥空间里的一个值。

如果敌手输出 $\mu'=\mu$，模拟器输出 0，否则输出 1。根据先前的设置，挑战者有 1/2 的概率设置 $T=e(g,g)^{\alpha^{q+1}s}$，在这种情况下如果模拟器正常模拟且假设没有中止，那么模拟器有不可忽略的优势 $\varepsilon/2q_o$ 判定 q-parallel BDHE 问题。这同判定 q-parallel BDHE 假定成立相矛盾。因此得出结论：不存在概率多项式时间敌手 A，能以不可忽略的优势 ε 成功攻击协议，故文中所设计的协议在标准模型下是一个安全的认证密钥协商协议。

结束语　本文基于 Waters 的密文策略属性基加密方案中的密钥提取形式设计了一个两方的消息策略的属性基密钥协商协议，协议具有较高的效率、标准模型下的可证明安全以及访问结构表达能力强等优点。特别地，选择安全模型下的证明可进一步扩展到支持完全安全模型下的证明。此外，同时满足上述特性的属性基群密钥协商协议是本文的后续研究工作。

参 考 文 献

[1] Sahai A，Waters B. Fuzzy identity based encryption：Advances in Cryptology-Eurocrypt 2005[C]// LNCS Berlin：Springer-Verlag，2005，3494：457-473

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

[3] Wang Hao，Xu Qiu-liang，Fu Xiu. Two-Party attribute-based key agreement protocol in the standard model[C]// the 2009 International Symposium on Information Processing(ISIP'09). Finland：Academy Publisher，2009：325-328

[4] Wang Hao，Xu Qiu-liang，Fu Xiu. Revocable attribute-based key agreement protocol without random oracles[J]. Journal of Networks，2009，4(8)：787-794

[5] 王永涛，宋璟，贺强，等. 一个基于属性的密钥协商协议[J]. 计算机工程，2014，40(2)：134-139

[6] 魏江宏，刘文芬，胡学先. 全安全的属性基认证密钥协商协议[J]. 计算机应用，2012，32(1)：. 38-41

[7] 王永涛，封维端，刘孝男，等. 一个消息策略基于属性的密钥协商协议[J]. 计算机科学，2013，40(9)：106-110

[8] Waters B. Ciphertext-policy Attribute-based Encryption：An Expressive，Efficient，and Provably Secure Realization[C]// PKC，LNCS，vol. 6571，Berlin：Springer-Verlag，2011：53-70

[9] Boneh D，Franklin M. Identity based encryption from the Weil pairing：Advances in Cryptology-Crypto 2001[C]// LNCS，vol. 2139，Berlin：Springer-Verlag，2001：231-229

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

[11] Chen Li-qun，Cheng Zhao-hui，Smart N P. Identity-based Key Agreement Protocols From Pairings. Cryptology ePrint Archive[OL]. http://eprint.iacr.org/2006/199

[12] Bellare M，Rogaway P. Entity authentication and key distribution：Advances in Cryptology-CRYPTO 1993[C]// LNCS，vol. 773，Berlin：Springer-Verlag，1994：232-249