一个消息策略基于属性的密钥协商协议

王永涛¹ 封维端¹ 刘孝男¹ 宋璟¹ 郭振洲²

(中国信息安全测评中心 北京 100085)¹ (沈阳航空航天大学计算机学院 沈阳 110136)²

摘要 提出一个消息策略基于属性的密钥协商协议。基于属性的密钥协商协议具有很多特性,其中主要的特性是模糊鉴别。讨论了模糊鉴别特性在密钥协商协议中的应用,并具体构建了一个两方的消息策略基于属性的密钥协商协议,所实现的消息策略为两值属性上的与门访问结构。此外,基于判定双线性 Diffie-Hellman 假定,在标准模型下证明了协议的安全性。

关键词 消息策略,基于属性加密,密钥协商协议,安全证明,标准模型

中图分类号 TP309.7 **文献标识码** A

Message Policy Attribute Based Key Agreement Protocol

WANG Yong-tao¹ FENG Wei-duan¹ LIU Xiao-nan¹ SONG Jing¹ GUO Zhen-zhou²

(China Information Technology Security Evaluation Center, Beijing 100085, China)¹

(School of Computer, Shenyang Aerospace University, Shenyang 110136, China)²

Abstract We proposed a message policy attribute based key agreement protocol. Attribute based key agreement protocol has many characteristics, the main of which is fuzzy identification. This paper discussed the application of fuzzy identification in key agreement protocol, and constructed a two-party message policy attribute based key agreement protocol, where the message policy is And-gates on two valued attribute. In addition, the new protocol was proved secure in the standard model under the decisional bilinear Diffie-Hellman assumption(DBDH).

Keywords Message policy, Attribute based encryption, Key agreement protocol, Security proof, Standard model

1 引言

在基于属性的密码体制中,加密方案^[1-3]得到了广泛的研究。基于属性加密方案体现出了很多有实际意义的思想,诸如实现一对多通信,根据访问结构来控制解密权限以及隐含的模糊鉴别等。可以考虑将上述思想引入到传统的数字签名和密钥协商概念中来,设计具有这些特性的有意义的方案。基于属性的签名体制、基于属性的密钥协商协议^[4-6]等即是上述思想结合的产物。虽然目前相关的研究并不多见,但这些方案仍然有其潜在的应用背景。本文考虑基于属性密钥协商协议的概念并简单讨论它的一些特性。研究者们大多把基于属性的加密体制看作是基于一身份加密体制的扩展和泛化,因此可以把基于属性密钥协商协议看作是基于一身份密钥协商协议的扩展和泛化。基于上述考虑,设计和构建基于属性的密钥协商协议是很有实际意义的工作,尽管基于属性的密钥协商协议的应用场景并不太清晰。

一个基于属性的密钥协商协议的最大特点可以认为是实现相互模糊鉴别的概念。如果把传统意义上具备完整的鉴别和认证功能的协商协议(概念上称为认证的密钥协商协议)所提供的强鉴别和认证能力(或者称为鉴别和认证程度)由1来

表示,不具备鉴别认证功能的密钥协商协议由0来表示,那么基于属性的密钥协商协议提供的鉴别和认证能力可以认为是介于上述两者之间的,也即是相互模糊鉴别的概念。实际上,在基于属性的密钥协商协议中,两个用户在最终协商成功一个会话密钥后,一方只能确定另一方满足他所指明的条件,而可能满足该条件的用户很多,并不能具体确定是哪个用户,即是相互的模糊鉴别。进一步讲,如果一个用户指明的条件非常苛刻,导致整个系统中只有很少的用户(甚至只有唯一一个用户)满足他指明的条件,那么这时候基于属性的密钥协商协议所提供的鉴别程度对于该用户来说趋近于1(即退化为了基于身份的密钥协商协议);从另一个角度来说,如果一个用户指明的条件比较宽泛,致使系统中几乎全部用户都满足,那么此时,一个基于属性的密钥协商协议相当于对该用户来说没有提供任何鉴别和认证能力(趋近于0)。通过上面的讨论可见,应用一个基于属性的密钥协商协议是非常灵活的,可以由执行协议的用户根据具体需要控制协议的鉴别和认证能力。在某些应用背景下,这一特点可能会很有意义。例如提供最强的鉴别和认证能力,往往意味着需要更多的带宽和计算花费,而不进行任何鉴别和认证又不太合理,这时执行协议的用户可以根据实际情况自行选择需要达到的鉴别程度,这

到稿日期:2012-11-23 返修日期:2013-03-04 本文受国家自然科学基金(61202493,60970111)资助。

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, E-mail: wyt_itsec@aliyun.com; 封维端(1982-),男,博士,副研究员,主要研究方向为信息安全; 刘孝男(1982-),女,博士,助理研究员,主要研究方向为信息安全; 宋璟(1985-),男,硕士,助理研究员,主要研究方向为信息安全; 郭振洲(1978-),男,博士,讲师,主要研究方向为信息安全。

为执行协议提供了很大的灵活性。基于以上的分析,基于属性的密钥协商协议是很有意义的研究内容。实际上,在一个用户的意向通信实体有多个,该用户希望与意向通信实体中的任何一个均能成功协商会话密钥的情况下,使用基于属性的密钥协商协议是最合适的。

在密文策略基于属性加密体制中,访问结构是嵌入到一个密文中的,然而,由于密钥协商协议中不存在密文的概念,因此在基于属性的密钥协商协议中,如果在参与者之间交换的消息是根据某个访问结构计算生成的,或者说访问结构嵌入到交换的消息中,那么本文称它为消息策略基于属性的密钥协商协议。

目前文献中存在的基于属性的密钥协商协议并不多见,例如文献[4-6],需要指出的是有一些协议并非真正基于属性的,而仍然是基于身份的密钥协商协议,并且一些协议实现的访问策略也比较简单。注意到文献[7]提出的交换协议实现了复杂的访问结构,但安全证明基于一个非标准的假设。文献[6]提出了一个基于属性的群密钥协商协议,其它的相关研究还不多见。本文基于 Cheung 等^[3]的密文策略基于属性加密的密钥提取形式,设计了一个两方的消息策略基于属性的密钥协商协议。协议的构建方法具有一定的通用性,因此可以使用同样的方法转化其它的基于属性的加密体制为基于属性的密钥协商协议。此外,本文给出了协议的安全证明。

2 基础知识

近几年,双线性对理论在密码学中,特别是在基于身份的密码体制、基于属性的密码体制中得到了广泛的应用。下面简要回顾双线性对^[8]的定义以及本文使用的判定双线性 Diffie-Hellman 假定^[8]。

定义 1 设 G_1, G_2 是阶为素数 p 的两个乘法循环群,设 g 是群 G_1 的一个生成元,假如一个映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足下面的条件:

- 1) 双线性性:对于所有的 $u, v \in G_1$ 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: $e(g, g) \neq 1_{G_2}$;
- 3) 可计算性:对于所有的 $u, v \in G_1$, 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(判定双线性 Diffie-Hellman 假定, DBDH) 该假定指的是,不存在多项式时间的敌手 $\mathcal{B}$ 有不可忽略的优势区分元组 $(g^a, g^b, g^c, e(g, g)^{abc})$ 和元组 $(g^a, g^b, g^c, e(g, g)^z)$, 其中 $a, b, c, z \in \mathbb{Z}_p^*$ 是随机的。设 κ 表示安全参数, 敌手 $\mathcal{B}$ 的优势函数 $Adv_{\mathcal{B}}^{DBDH}(\kappa)$ 定义如下:

$$Adv_{\mathcal{B}}^{DBDH}(\kappa) = |\Pr[\mathcal{B}(g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[\mathcal{B}(g^a, g^b, g^c, e(g, g)^z) = 1]|$$

定义 3(访问结构定义^[9]) 设 $\{P_1, P_2, P_3, \dots, P_n\}$ 是 n 个参与者的集合。设 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 $B \in A$ 并且 $B \subseteq C$, 那么 $C \in A$, 则说 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) 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 $D \in A$, 则叫做授权集合, 如果 $D \notin A$, 则叫做非授权集合。

在基于属性的密码体制中,上述访问结构中出现的参与者将被属性替换,访问结构 A 将包含所有属性上的授权集合。下面简单描述本文采用的与门访问结构^[3]。

假定系统中的属性有两种取值,例如正属性和负属性(正属性用于表示一个用户拥有该属性,负属性表示用户不拥有该属性)。设 N 表示集合 $\{1, 2, 3, \dots, n\}$, 对于每一个 $i \in N$, 属性 i 如果是正属性,记为 i , 如果是负属性,记为 $\neg i$ 。设 i 表示一个文字量,一个文字量可以取值为正(表示拥有属性 i), 即 $\underline{i} = i$, 也可以取值为负(表示不具有属性 i), 即 $\underline{i} = \neg i$ 。一个与门访问结构记为 $W = \bigwedge_{i \in I} \underline{i}$, 其中 $I \subseteq N$, $\underline{i}$ 为 i 或者 $\neg i$ 。一个属性集合满足一个与门访问结构如下定义: 设属性集合为 S , 它是 N 的一个子集, 集合 S 中的属性认为是正属性, 不在集合 S 中的其它属性认为是负属性。如果 $i \in S$, 且 $i \in I$ 和 $\underline{i} = i$ (或者 $i \notin S$, 且 $i \in I$ 和 $\underline{i} = \neg i$), 表示 i 满足 $\underline{i}$, 记为 1; 如果 $i \in S$, 且 $i \in I$ 和 $\underline{i} = \neg i$ (或者 $i \notin S$, 且 $i \in I$ 和 $\underline{i} = i$), 表示 i 不满足 $\underline{i}$, 记为 0。通过上述的 1 和 0 的赋值, 可以计算与门 W 的值, 如果给定属性集合 S , 使得 W 的值为 1, 那么说属性集合 S 满足与门访问结构 W , 记为 $S \models W$, 否则不满足, 记为 $S \not\models W$ 。给定一个与门访问结构可以划分属性集合, 其中满足该访问结构的属性集合记为授权集合, 不满足该与门访问结构的属性集合记为非授权集合。

3 消息策略基于属性的密钥协商协议形式化定义和安全模型

形式上,一个两方的消息密钥策略基于属性的密钥协商协议由以下 3 个算法组成:

Setup: 该算法输入安全参数 κ , 输出一个系统主公钥 mpk 和一个系统主密钥 msk 。

KeyGeneration: 该算法输入系统主密钥 msk 、一个用户拥有的属性集合 ω , 算法返回该用户的私钥。

KeyAgreement: 这是一个在两个用户之间交互的协商协议, 一个用户 A 选择一个访问结构 $\mathcal{T}_A$, 并根据该访问结构计算一个消息 M_A , 然后发送; 另一个用户 B 响应 A 的密钥协商请求, 即选择一个访问结构 $\mathcal{T}_B$, 根据该访问结构计算一个消息 M_B 并发送。如果用户 A 的属性集合满足 $\mathcal{T}_B$ 且用户 B 的属性集合满足 $\mathcal{T}_A$, 那么用户 A 和用户 B 可以计算一个会话密钥 K 。

本文采用 Liqun Chen 和 Caroline Kudla^[10]在基于身份密钥协商协议下使用的安全模型, 并对其做了简单的修改。

模型中涉及一个参与者集合 U , 集合中的每一个参与者模型化为一个预言机(Oracle), 即 $\Pi_{I,J}^n$, 它表示参与者 I 认为他正在与参与者 J 执行第 n 次会话协议, 该预言机保存一个他接收和发送的消息抄本。每一个参与者持有一个长期的基于属性的私钥, 该私钥是密钥生成中心生成并发送给参与者的。模型中还涉及一个攻击者(敌手) $\mathcal{A}$, 假设他既不是参与者也不是密钥生成中心。 $\mathcal{A}$ 被模型化为一个概率多项式时间的图灵机, 他拥有对所有参与者的预言机的访问权限。 $\mathcal{A}$ 被称为一个良性的(Benign)敌手, 如果敌手 $\mathcal{A}$ 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如下的询问:

Create 询问: 该询问可以根据敌手选择的访问结构(在密钥策略时, 此处为访问结构; 在消息策略时, 此处为属性集合) 创建一个新的参与者, 并创建一个新的预言机来模拟该参与

者;然后返回“*Yes*”给敌手(因为在基于属性密码体制中,访问结构或属性集合即为用户的公钥,所以没有针对该参与者的任何公钥信息返回,仅返回创建成功即可)。

Corrupt 询问:该询问返回敌手指定的参与者的长期基于属性的私钥。

Send 询问:该询问允许敌手向任何一个预言机发送他选择的消息,如 $\Pi_{I,J}^n$,在这种情况下,参与者 I 将认为他收到的消息来自于参与者 J 。敌手也可以发送一个特殊的消息 λ ,这将导致参与者 I 作为发起者开始与参与者 J 执行协议。

Reveal 询问:该询问根据敌手指定的参与者的预言机来返回该预言机持有的会话密钥。

一个预言机可能的状态包括:接受状态(Accepted),此时预言机持有一个会话密钥并接受了该会话密钥;拒绝状态(Rejected),此时预言机决定不建立会话密钥并中止协议;一个特殊状态,记为 $*$,表示预言机还没有做出接受或拒绝的决定;公开状态(Opened),预言机回答过 *Reveal* 询问后处于该状态;腐化状态(Corrupted),如果预言机回答了 *Corrupt* 询问,则处于该状态。此外,有关两个预言机的匹配会话的定义可参考先前的文献[11]。

在攻击的某个时刻,敌手将选择一个预言机,例如 $\Pi_{I,J}^n$,并做一次 *Test* 询问。该预言机要求处于接受状态,且没有回答过 *Reveal* 询问, I, J 没有回答过 *Corrupt* 询问;此外该预言机的匹配预言机没有回答过 *Reveal* 询问。如下回答该询问,预言机随机抛一枚公平的硬币 μ ,如果 $\mu=0$,则返回 $\Pi_{I,J}^n$ 持有的会话密钥,否则随机返回会话密钥空间里的一个值。

攻击的最后一个阶段,敌手将输出一个 μ' 作为对 μ 的猜测。敌手的优势定义如下:

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

定义 4^[10] 如果下述条件满足,一个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 $\Pi'_{J,I}$,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 $\Pi'_{J,I}$ 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) $Adv_{\mathcal{A}}(\kappa)$ 是可忽略的。

最后须指出的是本文协议在一个较弱的模型下来证明,也即选择(Selected)安全模型。在消息策略基于属性的密钥协商协议的证明中,敌手需要先声明一个访问结构 $\mathcal{T}^*$,这意味着敌手 *Corrupt* 询问需要受到限制,即不能询问满足 $\mathcal{T}^*(\omega)=1$ 的属性集合 ω 。这相当于假定了拥有属性集合 ω (以及 ω 的任何属性子集合)的用户私钥没有被腐化。完全安全模型下的协议是进一步的研究工作。

4 一个两方的消息策略基于属性的密钥协商协议

4.1 协议描述

基于 Ling Cheung 等^[3]的密文策略基于属性加密课题中的密钥提取形式设计了一个两方的消息策略基于属性的密钥协商协议,所实现的消息策略为两值属性上的与门访问结构。

设 n 表示系统中一个用户拥有的属性个数的最大值, N 表示集合 $\{1,2,\dots,n\}$ 。此外,设用户拥有一个属性 i ,记为正属性 i ,用户不具有一个属性 i ,记为负属性 $\neg i$ 。本节考虑的密文策略为由正负文字量 i 组成的与门访问结构。该访问结构表示为 $W = \Delta_{i \in I} i$,其中 $I \in N$ 并且每一个 i 表示一个文字量,即 $i = i$ 或者 $i = \neg i$ 。

Setup:系统参数生成如下,首先,根据安全参数 κ 生成双线性对群 G_1 和 G_2 。然后,随机选择 $y, t_1, \dots, t_{3n} \in \mathbb{Z}_p^*$,一个群 G_1 的生成元 g 。设置 $Y = e(g, g)^y$,对于 $k \in \{1, \dots, 3n\}$,设置 $T_k = g^k$ 。最后,设置系统主公钥 mpk 和系统主密钥 msk 为:

$$mpk = \{g, Y, T_1, \dots, T_{3n}\}, msk = \{y, t_1, \dots, t_{3n}\}$$

KeyGeneration(S, msk):该算法为一个拥有属性集合 S 的用户生成私钥,对于 $i \notin S$,认为是一个负属性。对于 $i \in N$,密钥生成中心随机选择 $r_i \in \mathbb{Z}_p$,并设置 $r = \sum_{i=1}^n r_i$ 和 $D = g^{y-r}$ 。

对于每一个 $i \in N$,如果 $i \in S$,设置 $D_i = g^{r_i}$,否则设置 $D_i = g^{r_i/n+i}$;然后对每一个 $i \in N$,设置 $F_i = g^{t_{2n+i}}$ 。用户私钥如下:

$$(D, \{D_i, F_i\}_{i \in N})$$

KeyAgreement:设 Alice 的属性集合为 γ_A ,他想要和一个用户协商一个会话密钥,该用户的属性集合需满足 Alice 指定的访问结构。Alice 随机选择 $s \in \mathbb{Z}_p$ 并指定一个与门访问结构 $W_A = \Delta_{i \in I} i$,如下生成一个消息并发送:设置 $E^{(A)} = g^s$,对于每一个 $i \in I$,如果 $i = i$,设置 $E_i^{(A)}$ 为 T_i ,如果 $i = \neg i$,将其设置为 T_{n+i} 。对于每一个 $i \in N \setminus I$,将其设置为 T_{2n+i} 。消息如下:

$$M_A = (W_A, E^{(A)}, \{E_i^{(A)}\}_{i \in N})$$

设 Bob 的属性集合为 γ_B ,且满足 Alice 指定的与门访问结构,那么 Bob 可以作为 Alice 的一个密钥交换对象来响应 Alice 的密钥交换请求(注意 Alice 潜在的密钥交换对象可能有多个)。由于 Bob 只希望和他所期望的用户群体中的一个来生成会话密钥,因此 Bob 也要指定一个条件来验证 Alice 是否满足。Bob 随机选择 $t \in \mathbb{Z}_p$ 并指定一个与门访问结构 $W_B = \Delta_{i \in I} i$ (注意 W_A 和 W_B 中的 I 可以相同也可以不同),如下计算一个消息并发送:设置 $E^{(B)} = g^t$,对于每一个 $i \in I$,如果 $i = i$,设置 $E_i^{(B)}$ 为 T_i ,如果 $i = \neg i$,将其设置为 T_{n+i} 。对于每一个 $i \in N \setminus I$,将其设置为 T_{2n+i} 。消息如下:

$$M_B = (W_B, E^{(B)}, \{E_i^{(B)}\}_{i \in N})$$

如果 γ_A 满足 W_B ,那么 Alice 和 Bob 可以提取一个会话密钥。Alice 收到消息 M_B ,如下计算得到 $K_B = e(g, g)^{yt}$:

$$\begin{aligned} & e(D, E^{(B)}) \times \prod_{i: i \in \omega} e(D_i, E_i^{(B)}) \times \prod_{i: \neg i \in \omega} e(D_i, E_i^{(B)}) \times \\ & \prod_{i \notin I} e(F_i, E_i^{(B)}) \\ & = e(D, E^{(B)}) \times e(g, g)^n = e(g^{y-r}, g^t) \times e(g, g)^n \\ & = e(g, g)^{yt} \end{aligned}$$

然后设置 $K = K_B \cdot Y^s = e(g, g)^{y(t+s)}$ 。同样, Bob 可以计算 $K_A = e(g, g)^{st}$ 并设置 $K = K_A \cdot Y^s = e(g, g)^{s(t+s)}$ 。基于上述计算的值 K , Alice 和 Bob 可以通过一个密钥提取函数 $H: \{0,1\}^* \rightarrow \{0,1\}^k$ 来生成一个会话密钥: $sk = H(M_A \parallel M_B \parallel K)$,其中 $k = |sk|$ 。

4.2 协议安全性证明

协议的正确性很容易看出,下面证明上述协议是一个安

全的认证密钥协商协议。

定理 1 在标准模型下,假定 DBDH 难解,上述两方消息策略基于属性的密钥协商协议是一个安全的认证密钥协商协议。

证明:前两个条件显然满足,这里证明协议满足第 3 个条件。假设存在一个概率多项式时间敌手 $\mathcal{A}$,它能以不可忽略的优势 ϵ 在游戏中获胜,那么可以创建一个模拟器 $\mathcal{B}$,它以不可忽略的优势解决 DBDH 问题。

挑战者在 $\mathcal{B}$ 的视线之外,抛一枚公平的硬币 ν 。如果 $\nu=0$,挑战者设置 $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{abc})$; 否则设置 $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^z)$, 其中 $a, b, c, z \in \mathbb{Z}_p$ 是随机的。

假如 $\mathcal{A}$ 在攻击中最多创建 q_0 个预言机。定义符号 $\Pi_{\theta, \sigma}^t$ 表示系统所有用户实例的第 t 个用户实例,而不是用户 θ 的第 t 个实例。设参与者集合为 $\{1, 2, \dots, L\}$, 对于 $\theta \in \{1, \dots, L\}$, 设 γ_θ 表示用户 θ 的属性集合。 $\mathcal{B}$ 为每一个预言机维护一个列表 Ω 。 $\mathcal{B}$ 随机选择 $1 \leq R \leq q_0$ 并猜测敌手 $\mathcal{A}$ 在此处将做 *Test* 询问,并记为 $\Pi_{U, V}^R$, 其中 $1 \leq U, V \leq L$ 。假设在第 R 个预言机,有 γ_U 满足发送给 U 的消息中指定的访问结构(根据协议的描述,如果没有上述条件,用户 U 将不能提取一个会话密钥,也即 $\Pi_{U, V}^R$ 不会处于接受状态,此时, $\mathcal{B}$ 在敌手 $\mathcal{A}$ 的帮助下也不能解决 DBDH 问题,此条件是能够成功协商的前提条件)。

模拟器 $\mathcal{B}$ 从敌手收到一个挑战与门访问结构 $W^* = \Delta_{i \in I} i$ 并如下模拟系统的 Setup 阶段。模拟器首先设置参数 $Y = e(A, B) = e(g, g)^{ab}$ 。记 $\{1, \dots, n\}$ 为 N , 对于每一个 $i \in N$, 模拟器随机选择 $\alpha_i, \beta_i, \lambda_i \in \mathbb{Z}_p$, 并设置 $T_i = g^{\alpha_i}, T_{n+i} = B^{\beta_i}, T_{2n+i} = B^{\lambda_i}$, 如果 $i \in I$ 且 $\underline{i} = i; T_i = B^{\alpha_i}, T_{n+i} = g^{\beta_i}, T_{2n+i} = B^{\lambda_i}$, 如果 $i \in I$ 且 $\underline{i} = \neg i$; 对于 $i \notin I$, 设置 $T_i = B^{\alpha_i}, T_{n+i} = B^{\beta_i}, T_{2n+i} = g^{\lambda_i}$ 。然后把公共参数 mpk 等发送给敌手 $\mathcal{A}$ 。注意模拟器 $\mathcal{B}$ 不知道 ab 的值。敌手 $\mathcal{A}$ 可以做下面的询问:

Corrupt(θ): 设 γ_θ 表示用户 θ 的属性集合, 如果 γ_θ 满足 W^* , 模拟器中止, 否则可以按照文献[3]的证明来返回私钥。根据设置必然存在一个 $j \in I$ 满足如下条件, 要么 $j \in \gamma_\theta$ 并且 $\underline{j} = \neg j$, 要么 $j \notin \gamma_\theta$ 并且 $\underline{j} = j$ 。为了简化起见, 这里假设 $\mathcal{B}$ 选择满足条件 $j \notin \gamma_\theta$ 且 $\underline{j} = j$ 的一个 j 。对于每一个 $i \in N$, 选择 $r_i \in \mathbb{Z}_p^*$, 对于 $i \neq j$ 设置 $r_i = r_i b$, 对于 j 设置 $r_j = ab + r_j b$ 。

最后设置 $r = \sum_{i=1}^n r_i = ab + \sum_{i=1}^n r_i b$, 因此

$$D = \prod_{i=1}^n \frac{1}{B^{r_i}} = g^{ab-r}$$

对于 j , 设置

$$D_j = g^{\frac{r_j}{b\beta_j}} = A^{\frac{1}{\beta_j}} g^{\frac{r_j}{\beta_j}}, F_j = A^{\frac{1}{\lambda_j}} g^{\frac{r_j}{\lambda_j}}$$

其它组件设置如下: 当 $i \in \gamma_\theta$ 时, 如果 $i \in I \wedge \underline{i} = i$, 设置 $D_i = B^{\alpha_i}$; 如果 $(i \in I \wedge \underline{i} = \neg i) \vee i \notin I$, 设置 $D_i = g^{\alpha_i}$ 。当 $i \notin \gamma_\theta$ 时, 如果 $(i \in I \wedge \underline{i} = i) \vee i \notin I$, 设置 $D_i = g^{\alpha_i}$; 如果 $i \in I \wedge \underline{i} = \neg i$, 设置 $D_i = B^{\beta_i}$ 。此外, 如果 $i \in I$, 设置 $F_i = g^{\alpha_i}$; 如果 $i \notin I$, 设置 $F_i = B^{\lambda_i}$ 。最后返回生成的私钥给敌手。

Create(γ): 模拟器根据属性集合 γ 创建一个新的参与者(用户), 并用一个新的预言机来模拟该用户。模拟器同模拟

Corrupt 询问一样生成该参与者的私钥并保存, 然后返回 "Yes" 给敌手(因为在基于属性密码体制中, 访问结构或属性集合即为用户的公钥, 所以没有针对该参与者的任何公钥信息返回, 仅返回创建成功即可)。

Send($\Pi_{\theta, \sigma}^t, M$): 这里只考虑返回某一个预言机的第一次 *Send* 询问。如果用户 θ 的属性集合 γ_θ 不满足消息 M 中包含的与门访问结构, 结束会话。如果 M 是抄本中的第 2 个消息, 则简单地接受该会话; 否则继续处理。

1) 当 $t \neq R$ 时, 处理如下:

a) 模拟器随机选择 f_θ 和一个访问结构 $W_\theta = \Delta_{i \in I} i$ 。设置 $E^{(0)} = g^{f_\theta}$; 对于 $i \in I'$ 且 $\underline{i} = i$, 设置 $E_i^{(0)} = (T_i)^{f_\theta}$; 对于 $i \in I'$ 且 $\underline{i} = \neg i$, 设置 $E_i^{(0)} = (T_{n+i})^{f_\theta}$; 对于 $i \notin I'$, 设置 $E_i^{(0)} = (T_{2n+i})^{f_\theta}$ 。模拟器返回:

$$M_\theta = (W_\theta, g^{f_\theta}, \{E_i^{(0)}\}_{i \in N})$$

并设置 $r_{\theta, \sigma} = f_\theta$ 。

b) 有关 $K_{\theta, \sigma}$ 的设置如下: 如果 θ, σ 满足能够协商的前提条件, 即一方的属性集合满足另一方发送的消息中的访问结构, $K_{\theta, \sigma}$ 可以根据协议描述来直接计算, 因为模拟器知道 θ 计算消息时使用的临时秘密值。先执行运算得到一个群元 K_σ , 然后设置 $K_{\theta, \sigma} = K_\sigma \cdot Y^{r_{\theta, \sigma}}$ 。

2) 如果 $t = R$, 此时应有 $\theta = U$, 模拟器选择 ℓ_U 和一个访问结构 $W_U = \Delta_{i \in I'} i$, 此时需要满足 $I' \subseteq I$, 且 I' 中的 $\underline{i}$ 与 I 中的 $\underline{i}$ 取值应相同。模拟器返回:

$$M_U = (W_U, C^U, \{\{C^{i,U}\}_{i \in I' \wedge \underline{i} = i}, \{C^{i,U}\}_{i \in I' \wedge \underline{i} = \neg i}, \{C^{i,U}\}_{i \notin I'}\}_{i \in N})$$

并设置 $r_{U, V} = \perp$ 。此外, 模拟器存储 ℓ_U 。假设属性集合 γ_U 不满足访问结构 W^* , 那么模拟器同 *Corrupt* 询问一样获得 γ_U 的私钥, 然后对消息 M 执行运算, 记得到的计算结果为 K_V 。模拟器可以设置 $K_{U, V}^R = K_V \cdot Z^U$ 。

Reveal($\Pi_{\theta, \sigma}^t$): 如果敌手询问的是 $\Pi_{U, V}^R$ 或者它的匹配预言机 $\Pi_{U, V}^t$, 模拟器中止; 否则, 返回该预言机持有的会话密钥给敌手。

Test($\Pi_{\theta, \sigma}^t$): 在经过上述一系列询问以后, 敌手将对某一个预言机询问一次 *Test*。如果敌手询问的不是 $\Pi_{U, V}^R$, 模拟器中止; 否则, 需要预言机 $\Pi_{U, V}^R$ 处于接受状态, 并且 $\Pi_{U, V}^R$ 或者是它的匹配预言机 $\Pi_{U, V}^t$ 没有回答过 *Reveal* 询问, 以及 U, V 没有回答过 *Corrupt* 询问。模拟器如下回答该询问, 它抛一枚硬币 μ , 如果 $\mu = 0$, 则返回 $\Pi_{U, V}^R$ 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 $\mu' = \mu$, 则模拟器输出 $\nu = 0$, 否则输出 $\nu = 1$ 。根据先前的设置, 挑战者有 1/2 的概率设置 $Z = e(g, g)^{abc}$, 在这种情况下模拟器正常模拟且假设没有中止, 那么模拟器有 $\epsilon/2q_0$ 的优势解决 DBDH 问题。

结束语 本文讨论了基于属性的密钥协商协议的一些特性及可能的应用背景, 提出消息策略基于属性密钥协商协议的概念并设计了一个两方的消息策略的基于属性密钥协商协议, 同时给出了正式的安全证明, 更详细的讨论可参阅文献[12]。进一步的研究将考虑设计一个有效的消息策略基于属性的群密钥协商协议。给出如下思考, 假如在一个系统中, 每一个用户都指明一个协商的条件, 计算一个消息并广播, 那么系统中任何一个用户若满足其他所有用户的协商条件, 就可

以作为一个协商实体来参与协商一个群会话密钥。

参考文献

- [1] Sahai A, Waters B. Fuzzy identity based encryption[A]// Advances in Cryptology-Eurocrypt 2005[C]. LNCS vol. 3494, Berlin: Springer-Verlag, 2005: 457-473
- [2] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine grained access control of encrypted data[A]// the 13th ACM Conference on Computer and Communications Security-CCS 2006[C]. New York: ACM Press, 2006: 89-98
- [3] Cheung L, Newport C. Provably secure ciphertext policy ABE [A]// the 14th ACM Conference on Computer and Communications Security-CCS 2007[C]. New York: ACM Press, 2007: 456-465
- [4] Wang Hao, Xu Qiu-liang, Fu Xiu. Two-Party attribute-based key agreement protocol in the standard model[A]// the 2009 International Symposium on Information Processing- ISIP'09[C]. Finland: Academy Publisher, 2009: 325-328
- [5] Wang Hao, Xu Qiu-liang, Fu Xiu. Revocable attribute-based key agreement protocol without random oracles[J]. Journal of Net-

works, 2009, 4(8): 787-794

- [6] Steinwandt R, Coron A S. Attribute-based group key establishment. Cryptology ePrint archive[OL]. <http://eprint.iacr.org/2010/235>, 2010
- [7] 魏江宏, 刘文芬, 胡学先. 全安全的属性基认证密钥交换协议[J]. 计算机应用, 2012, 32(1): 38-41
- [8] Boneh D, Franklin M. Identity based encryption from the Weil pairing[A]// Advances in Cryptology- Crypto 2001[C]. LNCS, vol. 2139, Berlin: Springer-Verlag, 2001: 231-229
- [9] Beimel A. Secure schemes for secret sharing and key distribution [D]. Haifa: Israel Institute of Technology, 1996
- [10] 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>, 2006
- [11] Bellare M, Rogaway P. Entity authentication and key distribution[A]// Advances in Cryptology-CRYPTO 1993[C]. LNCS, vol. 773, Berlin: Springer-Verlag, 1994: 232-249
- [12] 王永涛. 基于属性密码体制的相关研究[D]. 上海: 上海交通大学, 2011

(上接第 105 页)

可以快速分发到移动网络中的每个目标节点。KCCO-Gossip 算法不是广播发送消息, 因此网络负载低于 Flooding 算法。经典 Gossip 算法对每个目标节点发送消息的概率是一样的, 对于稳定度低的节点来说, 它们可能在没有接收到更新消息时就已经退出或失效, 因此需要更多的周期来达到 100% 的数据分发率, 但其发送的更新消息数较少, 产生的网络负载最低。

结束语 本文为实现移动对等网络覆盖网络资源列表更新, 提出了一种新的数据分发算法, 该算法在移动对等覆盖网络 KCCO 上限定了数据分发的范围, 只对同一 k -派系节点进行更新, 并根据每个节点的动态状态值决定不同的发送消息概率。实验结果表明, 在相同网络节点数的情况下, KCCO-Gossip 算法的数据分发效率明显好于 Gossip 算法, 达到了 Flooding 算法的分发效率。在不同网络节点数的情况下, KCCO-Gossip 算法的网络负载始终低于 Flooding 算法, 用较低的网络代价取得了较高的数据分发效率。

参考文献

- [1] Demers A, Greene D, Hauser C, et al. Epidemic algorithms for replicated database maintenance[C]// the 6th ACM Symposium on Principles of Distributed Computing. 1987: 1-12
- [2] Gabriele G, Ernesto D, Guido L C, et al. Gossiping solutions for distributed consensus on unstructured overlays[C]// The 4th IEEE International Conference on Digital Ecosystems and Technologies. 2010: 246-251
- [3] Da Hora D N, Macedo D F, Oliveira L B, et al. Enhancing peer-to-peer content discovery techniques over mobile ad hoc networks[J]. Computer Communications, 2009, 32(13/14): 1445-1459
- [4] Jin Yang, Simon T, Mueller C, et al. Comparing and refining

Gossip protocols for fault tolerance in wireless P2P systems[C]// The 19th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). 2011: 595-599

- [5] Drabkin V, Friedman R, Kliot G, et al. RAPID: Reliable probabilistic dissemination in wireless Ad-Hoc networks[C]// The 26th IEEE International Symposium on Reliable Distributed Systems. 2007: 13-22
- [6] 刘德辉, 尹刚, 王怀民, 等. Chord 网络环境下的 Gossip 算法[J]. 计算机工程与科学, 2011, 33(9): 48-51
- [7] 汪洋, 陈京文, 黑晓军, 等. 混合内容分发网中社群感知的 Gossip 协议[J]. 北京邮电大学学报, 2010, 33(5): 18-21, 46
- [8] Chen Nao, Hu Rui-min, Zhu Yong-qiong. Gossip-based topology management protocol for self-organizing overlays [J]. China Communications, 2011, 9: 38-46
- [9] Andras K, Vilmos S. Adaptive multihop broadcast protocols for ad hoc networks [C]// The 8th IEEE, IET International Symposium on Communication Systems, Networks and Digital Signal Processing. 2012: 1-6
- [10] Stingl D, Groß C, Rückert J, et al. Peerfactsim. kom: A large scale simulation framework for peer-to-peer systems[C]// the 2011 International Conference on High Performance Computing & Simulation. 2011: 577-584
- [11] Kermarrec A M, Steen M V. Gossiping in distributed Systems [J]. Operating Systems Review, 2007, 41(5): 2-7
- [12] Gavidia D, Voulgaris S, Steen M V. A gossip-based distributed news service for wireless mesh networks[C]// Third International Conference on Wireless On-demand Network Systems & Services (WONS). 2006: 59-67
- [13] Bailey N T J. The mathematical theory of infectious diseases and its applications(second edition)[M]. Hafner Press, 1975
- [14] Johnson D B, Maltz D A. Dynamic source routing in ad hoc wireless networks[J]. Mobile Computing, 1996, 353: 153-181