

## 基于身份认证的密钥交换改进协议

高丽丽, 李顺东

(陕西师范大学计算机科学学院, 西安 710119)

**摘 要:** 基于离散对数的困难性假设, Hölbl 等人提出了 2 个基于身份认证的密钥交换协议 HW1 和 HW2 (Computer Standards & Interfaces, 2009, No. 6)。HW1 协议能够有效抵抗 Tseng 等人提出的攻击 (Journal of Computers, 2002, No. 3), HW2 协议则具有较高的效率, 但 Shim 等人发现 HW1 不能抵抗中间人攻击和伪装攻击, HW2 不能抵抗伪装攻击 (IEEE Communications Letters, 2012, No. 4)。通过分析 Shim 等人提出的攻击方案, 找出这 2 个协议能够被篡改的原因, 分别提出改进的 HW1 和 HW2 协议, 利用 Hash 函数对传输的信息做 Hash 验证, 以防止信息被篡改。对改进协议进行可行性证明和安全性分析, 结果表明, 2 种协议能够有效抵抗中间人攻击和伪装攻击, 具有较高的安全性。

**关键词:** 密钥交换; 基于身份; 中间人攻击; 伪装攻击; Hash 函数; 离散对数问题

**中文引用格式:** 高丽丽, 李顺东. 基于身份认证的密钥交换改进协议[J]. 计算机工程, 2014, 40(11): 113-117.

**英文引用格式:** Gao Lili, Li Shundong. Improved Identity-based Authenticated Key Exchange Protocols[J]. Computer Engineering, 2014, 40(11): 113-117.

## Improved Identity-based Authenticated Key Exchange Protocols

GAO Lili, LI Shundong

(School of Computer Science, Shaanxi Normal University, Xi'an 710119, China)

**[Abstract]** Based on the difficulty of the discrete logarithm assumption, Hölbl et al (Computer Standards & Interfaces, 2009, No. 6) presented two identity-based authenticated key exchange protocols. The first protocol, denoted by HW1, improved Hsieh et al's protocol which makes it immune against Tseng et al's attack (Journal of Computers, 2002, No. 3), while the second protocol, denoted by HW2, improves the efficiency of Tseng's protocol. Shim et al analyzes these two protocols, and then shows that the HW1 can not resist the man-in-the-middle attack and the impersonation attack, and the HW2 can not resist the impersonation attack (IEEE Communications Letters, 2012, No. 4). This paper conducts a detailed analysis on the flaw, and finds the reason of the protocols are tampered, making use of the Hash function, authenticates the information to prevent the information is tampered, it proposes improved protocols based on these two protocols, and analyzes the security of improved protocols. The results suggest that the improved protocols can resist the man-in-the-middle-attack and the impersonation attacks, they are safe and feasible.

**[Key words]** key exchange; identity-based; man-in-the-middle attack; impersonation attack; Hash function; discrete logarithm problem

**DOI:** 10.3969/j.issn.1000-3428.2014.11.022

### 1 概述

网络技术,特别是基于互联网的工具有的不断成熟与发展,传统的事务处理、商业活动以及政府服务等越来越通过网络实施,大大加快了社会信息化的发展,对计算机和网络系统的依赖性也越来越大,信

息系统中的安全问题势必会影响到信息产业的发展。要保证信息的安全性,一个有效的解决办法就是利用密码术。密码学是信息安全的基础和关键,利用密码技术,可以实现信息的保密性、完整性、认证性和抗抵赖性。密码协议是实现网络通信和网络体系、分布式系统和电子商务安全运行的核心组

**基金项目:** 国家自然科学基金资助面上项目“高性能保密计算算法与协议研究”(61070189);国家自然科学基金资助面上项目“云计算与云存储若干关键问题研究”(61272435)。

**作者简介:** 高丽丽(1988-),女,硕士研究生,主研方向:密码学,信息安全;李顺东,教授、博士生导师。

**收稿日期:** 2013-11-18 **修回日期:** 2013-12-17 **E-mail:** fly0323@126.com

成部分,是安全系统的主要保障手段和工具,密钥交换是保密通信的前提和保证,是实施其他密码协议的关键,是公钥基础设施的基础。认证密钥交换协议,作为更可靠的密钥交换协议,在密码学与信息安全领域具有很强的实际意义。

密码学中的一个核心问题是在有敌手控制的网络中如何实现安全可靠的通信,为了解决这个问题,实体之间必须共享一个密钥并利用现有的技术来实现安全通信。密钥交换协议就是这样一个机制,它允许 2 个或多个用户在开放的网络环境中通过协商,建立一个便于保密通信的会话密钥,从而实现安全通信。如果协议能够使参与者确信除了指定的用户之外,其他任何参与者都不能得到会话密钥,则称此类密钥交换协议为认证密钥交换协议,这类协议将认证和密钥交换协议结合在一起,是网络通信中应用最广泛的协议。近年来,不少可认证的密钥交换协议被提出<sup>[14]</sup>,其中也有不少协议被攻破,因此,设计出更为安全的密钥交换协议具有重大意义。

1976 年,Diffie 和 Hellman 提出了公钥密码学的概念<sup>[5]</sup>,同时给出了第一个密钥交换协议,即 Diffie-Hellman 协议。1984 年,Shamir 提出了基于身份的密码学概念<sup>[6]</sup>,在该体制下,终端用户可以任意选取一个身份字符串作为自己的公钥,存在一个可信的密钥生成中心(KGC),秘密持有一个主私钥,将主私钥和用户身份结合生成用户私钥。Hsieh 等人在 2002 年,在 Saeednia 协议的基础上,通过使用模乘运算和模幂运算减少计算花费,提出了一个改进的基于身份认证的密钥协商协议<sup>[7]</sup>。同年,Tseng 等人指出 Hsieh 协议不能抵抗密钥泄露伪装攻击,并给出了攻击方案。在 2007 年,Tseng 对 Hsieh 协议进行了改进,并给出了一个高效的密钥协商协议<sup>[8]</sup>,改进后的协议能够满足所有安全属性。2009 年,Hölbl 等人提出了 2 个基于身份认证的密钥交换协议<sup>[9]</sup>:HW1 协议和 HW2 协议。2012 年,Shim 等人分析了这 2 个协议<sup>[10]</sup>,本文针对这 2 个协议存在的缺陷,利用 Hash 函数对协议进行改进,并对改进后的协议进行安全性分析。

## 2 预备知识

### 2.1 Hash 函数

Hash 函数在密码学中扮演着重要的角色,下面回顾一下 Hash 函数的概念和基本性质<sup>[11]</sup>。

**定义 1 (Hash 函数)** 在密码学中,Hash 函数是一个映射,满足  $h: \{0,1\}^* \rightarrow \{0,1\}^n$ ,其中,  $\{0,1\}^*$  表示任意长度的比特串的集合;  $\{0,1\}^n$  代表长度为  $n$  比特的二进制串集合。消息  $x \in \{0,1\}^*$  的像  $h(x)$  称为  $x$  的 Hash 值。

**定义 2 (碰撞)** 设  $x, x' \in \{0,1\}^*$  是 2 个不同的

消息,如果  $h(x) = h(x')$ ,则称  $x$  和  $x'$  是 Hash 函数  $h$  的一个碰撞。

为了保证 Hash 函数应用的安全性,要求找出 Hash 函数的碰撞在计算上是困难的。依据找出 Hash 函数碰撞的情况,可将 Hash 函数分为 3 类:

(1)单向 Hash 函数:设  $h$  是一个 Hash 函数,给定一个 Hash 值  $y$ ,如果寻找一个消息  $x$ ,使得  $y = h(x)$  是计算上不可行的,则称  $h$  是单向 Hash 函数。

(2)弱抗碰撞 Hash 函数:设  $h$  是一个 Hash 函数,任给一个消息  $x$ ,如果寻找另一个不同的消息  $x'$ ,使得  $h(x) = h(x')$  是计算上不可行的,则称  $h$  是弱抗碰撞 Hash 函数。

(3)强抗碰撞 Hash 函数:设  $h$  是一个 Hash 函数,如果寻找 2 个不同的消息  $x$  和  $x'$ ,使得  $h(x) = h(x')$  是计算上不可行的,则称  $h$  是强抗碰撞 Hash 函数。

一个密码学上的安全 Hash 函数  $h$  应具有以下性质:对任意的消息  $x$ ,计算  $h(x)$  是容易的; $h$  是单向的; $h$  是弱抗碰撞的,或是强抗碰撞的。

### 2.2 eCK 模型

eCK 模型是赋予敌手强攻击力的双方认证密钥交换协议的安全模型,该模型具体描述如下<sup>[12-13]</sup>:

**参与者:**这一模型包含一个参与者集合  $U$ ,每个参与者被模型模拟成概率多项式时间图灵机,可以同时执行多项式次数的协议。假设协议中的 2 个参与者为  $A$  和  $B$ ,则记双方运行的第  $s$  次会话为  $\Pi_{A,B}^s$ 。

**证书管理中心:**eCK 模型需要一个可信第三方证书管理中心(CA)验证每个参与者的长期公钥与其身份的绑定情况,所有通过该验证的参与者(包括敌手)均有资格参与协议。

**敌手:**敌手  $M$  为一个主动攻击者,它被模拟为一个概率多项式时间图灵机。eCK 模型允许敌手任意监听、延迟、重放和修改消息等。

本文通过一个挑战者和敌手  $M$  之间的游戏定义双方认证密钥交换协议的安全性。在该游戏中, $M$  被允许进行以下的预言机查询,并且这些查询是无序的:

(1)Send( $\Pi_{A,B}^s, m$ ): $M$  向  $\Pi_{A,B}^s$  发送消息  $m$ ,  $\Pi_{A,B}^s$  按照协议规范应答消息  $m$ 。另外,通过该查询,敌手可要求参与者(如  $A$ )发起与另一方(如  $B$ )的会话。

(2)Long-term Key Reveal( $A$ ):敌手  $M$  通过此查询获得参与者  $A$  的长期私钥。

(3)Ephemeral Key Reveal( $\Pi_{A,B}^s, A$ ):敌手  $M$  通过此查询获得会话中参与者  $A$  的临时私钥。

(4)Session Key Reveal( $\Pi_{A,B}^s$ ):敌手  $M$  通过此查询获得会话  $\Pi_{A,B}^s$  中计算得到的会话密钥。

(5) Establish Party ( $A$ ): 敌手  $M$  通过此查询可以在 CA 上注册与参与者  $A$  相同的公钥。通过此查询,  $M$  可以发起未知密钥共享攻击。

(6) Test ( $\Pi_{A,B}^s$ )。在游戏的某一时刻,  $M$  可以向一个新鲜的 (见定义 4) 会话 ( $\Pi_{A,B}^s$ ) 进行 Test 查询。此时, ( $\Pi_{A,B}^s$ ) 通过投掷的一枚硬币  $b \in \{0,1\}$  来回答此查询: 若投币结果为 0, 那么返回协商得到的会话密钥; 否则返回会话密钥空间  $\{0,1\}^k$  上的一个随机值。这里,  $k$  表示会话密钥的比特长度。

在游戏最后,  $M$  输出  $b' \in \{0,1\}$  作为对  $b$  的判断, 若  $b = b'$ , 则称敌手  $M$  赢得了此游戏。

基于以上描述, 本文定义以下概念:

**定义 3 (匹配会话)** 如果某次会话  $\Pi_{A,B}^s$  发出的每条消息都相继被传送到另外一个会话  $\Pi_{B,A}^t$ , 并且  $\Pi_{B,A}^t$  的应答消息也被传回到  $\Pi_{A,B}^s$  作为  $\Pi_{A,B}^s$  相应的下一条消息, 则称这 2 个会话是匹配的。

**定义 4 (新鲜性)** 如果参与者  $A$  和  $B$  通过会话  $\Pi_{A,B}^s$  已协商获得一个会话密钥, 且此会话满足:

(1) 敌手没有对参与者  $A$  和  $B$  进行过 Long-term Key Reveal 查询或 Ephemeral Key Reveal 查询。

(2) 敌手没有对  $\Pi_{A,B}^s$  进行过 Session Key Reveal 查询, 则称该会话是新鲜的。

### 3 2 种基于身份认证的密钥交换协议

Hölbl 等人提出了 2 种基于身份认证的密钥交换协议, 即 HW1 协议和 HW2 协议<sup>[7]</sup>, 协议包括 3 个阶段: 系统建立阶段, 私钥生成阶段和密钥交换阶段。

#### 3.1 HW1 协议

**系统建立阶段:** 在这个阶段, 密钥生成中心 KGC 选择一个大素数  $p$ , 一个生成元  $g \in \mathbb{Z}_p^*$ , 一个单向 Hash 函数  $h$ , 一个随机整数  $x_s \in \mathbb{Z}_p^*$ , 计算  $y_s = g^{x_s}$ 。KGC 将系统公共参数设置为  $\{g, h, p, y_s\}$ , 主私钥设置为  $x_s$ 。

**私钥生成阶段:**

对于每一个用户, KGC 首先计算  $I_i = h(ID_i)$ , 其中,  $ID_i$  是用户  $i$  的身份。然后, KGC 选择一个随机数  $k_i \in \mathbb{Z}_p^*$ , 计算用户的公钥  $u_i = g^{k_i} \pmod{p}$  和用户的私钥  $v_i = I_i k_i + x_s u_i \pmod{p-1}$ 。为方便起见, 在以下的运算中省略“mod  $p$ ”。

**密钥交换阶段:**

(1) Alice 选择一个随机数  $r_A \in \mathbb{Z}_p^*$ , 计算  $t_A = g^{r_A}$ , 将  $\{u_A, t_A, ID_A\}$  发送给 Bob。类似地, Bob 选择一个随机数  $r_B \in \mathbb{Z}_p^*$ , 计算  $t_B = g^{r_B}$ , 将  $\{u_B, t_B, ID_B\}$  发送给 Alice。

(2) Alice 计算  $I_B = h(ID_B)$ ,  $x_A = u_B^{I_B} \cdot y_s^{u_B} = g^{k_B I_B} \cdot g^{x_s u_B} = g^{v_B}$  和密钥  $K_{AB} = (x_A \cdot t_B)^{v_A + r_A} = g^{(r_A + v_A)(r_B + v_B)}$ , 类似地, Bob 计算  $I_A = h(ID_A)$ ,  $x_B = u_A^{I_A} \cdot y_s^{u_A} = g^{k_A I_A} \cdot$

$g^{x_s u_A} = g^{v_A}$  和密钥  $K_{BA} = (x_B \cdot t_A)^{v_B + r_B} = g^{(r_A + v_A)(r_B + v_B)}$ , 经过该协议, Alice 和 Bob 共享密钥  $K = K_{AB} = K_{BA} = g^{(r_A + v_A)(r_B + v_B)}$ 。

#### 3.2 HW2 协议

**系统建立阶段:** 在这个阶段, 密钥生成中心 KGC 选择一个大素数  $p$ , 一个生成元  $g \in \mathbb{Z}_p^*$ , 一个单向 Hash 函数  $h$ , 一个随机整数  $x_s \in \mathbb{Z}_p^*$ , 计算  $y_s = g^{x_s}$ 。KGC 将系统公共参数设置为  $\{g, h, p, y_s\}$ , 主私钥设置为  $x_s$ 。

**私钥生成阶段:** 对于每一个用户, KGC 首先计算  $I_i = h(ID_i)$ , 其中,  $ID_i$  是用户  $i$  的身份。然后, KGC 选择一个随机数  $k_i \in \mathbb{Z}_p^*$ , 计算用户的公钥  $u_i = g^{k_i} \pmod{p}$  和用户的私钥  $v_i = k_i + x_s h(ID_i, u_i) \pmod{p-1}$ 。

**密钥交换阶段:**

(1) Alice 选择一个随机数  $r_A \in \mathbb{Z}_p^*$ , 计算  $t_A = g^{r_A}$ , 将  $\{u_A, t_A, ID_A\}$  发送给 Bob。类似地, Bob 选择一个随机数  $r_B \in \mathbb{Z}_p^*$ , 计算  $t_B = g^{r_B}$ , 将  $\{u_B, t_B, ID_B\}$  发送给 Alice。

(2) Alice 计算  $I_B = h(ID_B)$ ,  $x_A = u_B \cdot y_s^{h(ID_B, u_B)} = g^{k_B} \cdot g^{x_s h(ID_B, u_B)} = g^{v_B}$  和密钥  $K_{AB} = (x_A \cdot t_B)^{v_A + r_A} = g^{(r_A + v_A)(r_B + v_B)}$ , 类似地, Bob 计算  $I_A = h(ID_A)$ ,  $x_B = u_A \cdot y_s^{h(ID_A, u_A)} = g^{k_A} \cdot g^{x_s h(ID_A, u_A)} = g^{v_A}$  和密钥  $K_{BA} = (x_B \cdot t_A)^{v_B + r_B} = g^{(r_A + v_A)(r_B + v_B)}$ , 经过该协议, Alice 和 Bob 共享密钥  $K = K_{AB} = K_{BA} = g^{(r_A + v_A)(r_B + v_B)}$ 。

### 4 对协议的攻击

Shim 等对 Hölbl 等基于身份认证的密钥交换协议进行了分析, 提出了中间人攻击和伪装攻击协议<sup>[10]</sup>。

#### 4.1 对 HW1 协议的中间人攻击

敌手 Eve 窃听 Alice 和 Bob 的通信信息, 攻击过程如下:

(1) 当 Alice 发送给 Bob 信息  $\{u_A, t_A, ID_A\}$  时, Eve 窃听该信息, 选取一个随机数  $\alpha$ , 计算  $t'_A = g^{\alpha - v_A}$ , 将  $\{u_A, t'_A, ID_A\}$  发送给 Bob。类似地, 当 Bob 发送给 Alice 信息  $\{u_B, t_B, ID_B\}$  时, Eve 窃听该信息, 选取一个随机数  $\beta$ , 计算  $t'_B = g^{\alpha - v_B}$ , 将  $\{u_B, t'_B, ID_B\}$  发送给 Alice。

(2) Alice 接收到  $\{u_B, t'_B, ID_B\}$  后, 计算密钥  $K_{AB} = (g^{v_B} \cdot t'_B)^{v_A + r_A} = (g^{v_B} \cdot g^{\beta - v_B})^{v_A + r_A} = (g^{v_B} \cdot g^{\beta - v_B})^{v_A + r_A} = (g^\beta)^{v_A + r_A}$ , 类似地, Bob 接收到  $\{u_A, t'_A, ID_A\}$  后, 计算密钥  $K_{BA} = (g^{v_A} \cdot t'_A)^{v_B + r_B} = (g^\alpha)^{v_B + r_B}$ 。

(3) Eve 分别计算密钥  $K_{AB} = (g^{v_A} \cdot t_A)^\beta = g^{\beta(v_A + r_A)}$  和密钥  $K_{BA} = (g^{v_B} \cdot t_B)^\alpha = g^{\alpha(v_B + r_B)}$ 。

最后, Eve 和 Alice 共享密钥  $K_{AB} = g^{\beta(v_A + r_A)}$ ,



Eve 和 Bob 共享密钥  $K_{BA} = g^{(v_B + r_B)}$ 。该协议没有密钥验证过程, Alice 和 Bob 不知道他们的密钥是不同的, Eve 可以解密 Alice 用  $K_{AB}$  加密的消息, 以及 Bob 用  $K_{BA}$  加密的消息。

#### 4.2 对 HW1 协议的伪装攻击

假设敌手 Eve 向 Bob 伪装 Alice, 攻击过程如下:

(1) Eve 选择一个随机数  $t \in \mathbb{Z}_p^*$ , 使得  $t = r_A + v_A$ 。Eve 通过计算  $u_A^t \cdot y_s^{u_A}$  得到  $g^{v_A}$ , 从而得到  $g^{r_A} = g^t \cdot (g^{v_A})^{-1}$ 。Eve 伪装 Alice, 将  $\{u_A, t_A = g^{r_A}, ID_A\}$  发送给 Bob。Bob 将  $\{u_B, t_B, ID_B\}$  发送给 Alice。

(2) Bob 接收到  $\{u_A, t_A = g^{r_A}, ID_A\}$  后, 计算共享密钥  $K_{BA} = (x_B \cdot t_A)^{v_B + r_B} = (g^{v_A} \cdot g^{r_A})^{v_B + r_B} = g^{(r_A + v_A)(r_B + v_B)}$ 。

(3) Eve 截获到  $\{u_B, t_B, ID_B\}$  后, Eve 计算共享密钥  $K_{AB} = (x_A \cdot t_B)^t = g^{(r_A + v_A)(r_B + v_B)}$ 。

最后, Eve 向 Bob 伪装成功, 和 Bob 共享密钥  $K = K_{AB} = K_{BA}$ 。

#### 4.3 对 HW2 协议的伪装攻击

假设敌手 Eve 向 Bob 伪装 Alice, 攻击过程如下:

(1) Eve 选择一个随机数  $\tau \in \mathbb{Z}_p^*$ , 使得  $\tau = r_A + v_A$ 。Eve 通过计算  $u_A \cdot y_s^{h(ID_A, u_A)}$  得到  $g^{v_A}$ , 从而得到  $g^{r_A} = g^\tau \cdot (g^{v_A})^{-1}$ 。Eve 伪装 Alice, 将  $\{u_A, t_A = g^{r_A}, ID_A\}$  发送给 Bob。Bob 将  $\{u_B, t_B, ID_B\}$  发送给 Alice。

(2) Bob 接收到  $\{u_A, t_A = g^{r_A}, ID_A\}$  后, 计算共享密钥:  $K_{BA} = (x_B \cdot t_A)^{v_B + r_B} = (g^{v_A} \cdot g^{r_A})^{v_B + r_B} = g^{(r_A + v_A)(r_B + v_B)}$ 。

(3) Eve 截获到  $\{u_B, t_B, ID_B\}$  后, Eve 计算共享密钥  $K_{AB} = (x_A \cdot t_B)^\tau = g^{(r_A + v_A)(r_B + v_B)}$ 。

最后, Eve 向 Bob 伪装成功, 和 Bob 共享密钥  $K = K_{AB} = K_{BA}$ 。

### 5 改进协议

#### 5.1 改进的 HW1 协议

##### 5.1.1 抗中间人攻击协议

对 HW1 协议, 在密钥交换阶段, 加入密钥验证, 强化密钥交换阶段的安全性。系统建立阶段和私钥生成阶段保持不变, 过程参考 3.1 节。

密钥交换阶段:

(1) Alice 选择一个随机数  $r_A \in \mathbb{Z}_p^*$ , 计算  $t_A = g^{r_A}$ , 将  $\{u_A, t_A, ID_A\}$  发送给 Bob。类似地, Bob 选择一个随机数  $r_B \in \mathbb{Z}_p^*$ , 计算  $t_B = g^{r_B}$ , 将  $\{u_B, t_B, ID_B\}$  发送给 Alice。

(2) Alice 计算  $I_B = h(ID_B)$ ,  $x_A = u_B^t \cdot y_s^{u_B} = g^{k_B I_B} \cdot g^{x_s u_B} = g^{v_B}$  和密钥  $K_{AB} = (x_A \cdot t_B)^{v_A + r_A} = g^{(r_A + v_A)(r_B + v_B)}$ 。类似地, Bob 计算  $I_A = h(ID_A)$ ,  $x_B = u_A^t \cdot y_s^{u_A} = g^{k_A I_A} \cdot g^{x_s u_A} = g^{v_A}$  和密钥  $K_{BA} = (x_B \cdot t_A)^{v_B + r_B} = g^{(r_A + v_A)(r_B + v_B)}$ 。

(3) Alice 计算  $h_A = h(K_{AB}, t_B^r)$ , 将  $h_A$  发送给 Bob。类似地, Bob 计算  $h_B = h(K_{BA}, t_A^r)$ , 将  $h_B$  发送给 Alice。

(4) Alice 和 Bob 分别判断  $h_A$  和  $h_B$  是否相等。若  $h_A = h_B$ , 则 Alice 和 Bob 共享密钥:  $K = K_{AB} = K_{BA} = g^{(r_A + v_A)(r_B + v_B)}$ 。

##### 5.1.2 抗伪装攻击协议

对 HW1 协议, 利用 Hash 函数, 强化密钥交换阶段的安全性。系统建立阶段和私钥生成阶段保持不变, 过程参考 3.1 节。

密钥交换阶段:

(1) Alice 选择一个随机数  $r_A \in \mathbb{Z}_p^*$ , 计算  $t_A = g^{r_A}$ , 将  $\{u_A, t_A, ID_A\}$  发送给 Bob。类似地, Bob 选择一个随机数  $r_B \in \mathbb{Z}_p^*$ , 计算  $t_B = g^{r_B}$ , 将  $\{u_B, t_B, ID_B\}$  发送给 Alice。

(2) Alice 计算  $I_B = h(ID_B)$ ,  $h_{A1} = h(ID_B, t_B^r)$ ,  $h_{A2} = h(ID_A, t_B^r)$ ,  $x_A = u_B^t \cdot y_s^{u_B} = g^{k_B I_B} \cdot g^{x_s u_B} = g^{v_B}$  和密钥  $K_{AB} = (x_A^{h_{A2}} \cdot t_B)^{h_{A1} v_A + r_A} = g^{(r_A + h_{A1} v_A)(r_B + h_{A2} v_B)}$ 。类似地, Bob 计算  $I_A = h(ID_A)$ ,  $h_{B1} = h(ID_A, t_A^r) = h(ID_A, t_B^r) = h_{A2}$ ,  $h_{B2} = h(ID_B, t_A^r) = h(ID_B, t_B^r) = h_{A1}$ ,  $x_B = u_A^t \cdot y_s^{u_A} = g^{k_A I_A} \cdot g^{x_s u_A} = g^{v_A}$  和密钥  $K_{BA} = (x_B^{h_{B2}} \cdot t_A)^{h_{B1} v_B + r_B} = g^{(r_A + h_{A1} v_A)(r_B + h_{A2} v_B)}$ 。

经过该协议, Alice 和 Bob 共享密钥  $K = K_{AB} = K_{BA} = g^{(r_A + h_{A1} v_A)(r_B + h_{A2} v_B)}$ 。

#### 5.2 改进的 HW2 协议

对 HW2 协议, 利用 Hash 函数, 强化密钥交换阶段的安全性。系统建立阶段和私钥生成阶段保持不变, 过程参考 3.2 节。

密钥交换阶段:

(1) Alice 选择一个随机数  $r_A \in \mathbb{Z}_p^*$ , 计算  $t_A = g^{r_A}$ , 将  $\{u_A, t_A, ID_A\}$  发送给 Bob。类似地, Bob 选择一个随机数  $r_B \in \mathbb{Z}_p^*$ , 计算  $t_B = g^{r_B}$ , 将  $\{u_B, t_B, ID_B\}$  发送给 Alice。

(2) Alice 计算  $I_B = h(ID_B)$ ,  $h_{A1} = h(ID_B, t_B^r)$ ,  $h_{A2} = h(ID_A, t_B^r)$ ,  $x_A = u_B \cdot y_s^{h(ID_B, u_B)} = g^{k_B} \cdot g^{x_s h(ID_B, u_B)} = g^{v_B}$  和密钥  $K_{AB} = (x_A^{h_{A2}} \cdot t_B)^{h_{A1} v_A + r_A} = g^{(r_A + h_{A1} v_A)(r_B + h_{A2} v_B)}$ 。类似地, Bob 计算  $I_A = h(ID_A)$ ,  $h_{B1} = h(ID_A, t_A^r) = h(ID_A, t_B^r) = h_{A2}$ ,  $h_{B2} = h(ID_B, t_A^r) = h(ID_B, t_B^r) = h_{A1}$ ,  $x_B = u_A \cdot y_s^{h(ID_A, u_A)} = g^{k_A} \cdot g^{x_s h(ID_A, u_A)} = g^{v_A}$  和密钥  $K_{BA} = (x_B^{h_{B2}} \cdot t_A)^{h_{B1} v_B + r_B} = g^{(r_A + h_{A1} v_A)(r_B + h_{A2} v_B)}$ 。

经过该协议, Alice 和 Bob 共享密钥  $K = K_{AB} = K_{BA} = g^{(r_A + h_{A1} v_A)(r_B + h_{A2} v_B)}$ 。

### 6 安全性分析

#### 6.1 抗中间人攻击协议的安全性分析

改进后的协议利用 Hash 函数进行了密钥验证,

Alice 和 Bob 通过 Hash 值判断  $h_A$  和  $h_B$  是否相等,若两者不相等,则可判断出有中间人攻击该协议。Eve 如果想攻击成功,需找出一个数  $(K'_{AB}, (t'_B)^{'})$  或  $(K'_{BA}, (t'_A)^{'})$ , 使  $h_A = h(K_{AB}, t'_B) = h(K'_{AB}, (t'_B)^{'})$  或  $h_B = h(K_{BA}, t'_A) = h(K'_{BA}, (t'_A)^{'})$ 。

基于 Hash 函数的弱抗碰撞性, Eve 要找到满足条件的数是困难的,故改进后的协议能够抵抗 Shim 等提出的对 HW1 协议的中间人攻击。

## 6.2 抗伪装攻击协议的安全性分析

改进的 HW1 协议,记作 HWP1 协议,在 eCK 模型下证明 HWP1 协议的安全性,改进的 HW2 协议的安全性可用相同的方法得到证明,限于篇幅,本文只给出 HWP1 协议的详细证明过程。

**定义 5** (计算 Diffie-Hellman (CDH) 问题) 设  $G$  是一个  $q$  阶乘法循环群,  $g$  是  $G$  的生成元, 如果已知  $g, g^a, g^b$  ( $a, b$  是正整数), 求  $g^{ab}$  的成功概率  $Pr_{CDH}$  是可忽略的, 则称 CDH 问题是困难的。

**定理** 假设  $H$  是随机预言机, CDH 假设对群  $G$  是成立的, 则 HWP1 协议在 eCK 模型下是安全的。

**证明:** 敌手  $M$  以伪造攻击的方式区分真实的话密钥和随机值。本文将证明, 如果敌手  $M$  以不可忽略的概率赢得游戏, 则可构造一个模拟器  $S$ , 它可利用  $M$  以不可忽略的概率解决 CDH 问题。

给定  $S$  的挑战  $(U, V)$ ,  $S$  将与  $M$  按照 HWP1 协议流程执行查询, 并适当修改诚实的参与者返回的数据, 以期在  $M$  赢得游戏后  $S$  可以解决 CDH 问题。

首先,  $S$  选取由某 2 个参与者 Alice 和 Bob 参与的匹配会话,  $S$  将这 2 个会话中的  $g^{r_A}$  用  $U$  代替,  $g^{r_B}$  用  $V$  代替。假设  $S$  最多可选取  $k$  次会话, 故选择的概率为  $2/k^2$ 。

攻击开始后,  $M$  以  $1/k^2$  的概率选中上述会话中的 Alice 的会话作为 Test 会话。显然, 此时 Bob 的会话称为 Test 会话的匹配会话。若  $M$  成功地进行伪装攻击,  $S$  一定能解决 CDH 问题。

事实上, 共享密钥  $K = g^{(r_A + h_{A1}v_A)(r_B + h_{A2}v_B)}$ , 若  $M$  获得了  $K$ , 它一定可以计算出  $g^{r_A r_B}$ , 通过进行 Hash 运算得到  $h_{A1}, h_{A2}$ 。根据之前的假设,  $K = CDH(U, V)$ 。因此, 若  $M$  成功地进行伪装攻击,  $S$  一定能解决 CDH 问题。

由于 eCK 模型不允许敌手在 Test 会话中的某个参与者同时进行 Long-term Key Reveal 查询和 Ephemeral Key Reveal 查询, 因而敌手查询  $(v_A, r_A)$  或  $(v_B, r_B)$  的概率可以忽略不计, 又 Hash 函数发生碰撞的概率也可以忽略。因此,  $S$  与  $M$  的优势有如下关系:  $Pr_{CDH}(S) \geq \frac{1}{k^2} Pr_{eCK}(M)$ 。

综上, 定理得证。

## 7 结束语

本文通过对 Hölbl 等人基于身份认证的密钥交换协议和 Shim 等人的攻击协议进行研究与分析, 找出 Hölbl 等协议存在的不足, 并对该协议进行改进和安全性分析。分析结果表明, 改进后的协议能够抵抗 Shim 等人提出的攻击, 协议安全、可行。本文主要研究了基于双方的密钥交换协议, 下一步将致力于基于多方的密钥交换协议的研究。

## 参考文献

- [1] Zhao Jianjie, Gu Dawu. Provably Secure Three-party Password-based Authenticated Key Exchange Protocol[J]. Information Sciences, 2012, 184(1): 310-323.
- [2] Chang T Y, Hwang M S, Yang W P. A Communication-efficient Three-party Password Authenticated Key Exchange Protocol[J]. Information Science, 2011, 181(1): 217-226.
- [3] Zhang Shiwu, Cheng Qingfeng, Wang Xuekui. Impersonation Attack on Two Identity-based Authenticated Key Exchange Protocols [C]//Proceedings of 2010 WASE International Conference on Information Engineering. Beidaihe, China: IEEE Press, 2010: 113-116.
- [4] Ni Liang, Chen Gongliang, Li Jianhua, et al. Strongly Secure Identity-based Authenticated Key Agreement Protocols[J]. Computers and Electrical Engineering, 2011, 37(2): 205-217.
- [5] Diffie W, Hellman M E. New Directions in Cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 29-40.
- [6] Shamir A. Identity-based Cryptosystem and Signature Schemes[C]//Advances in Cryptology-Crypto'84. Heidelberg, Germany: Springer, 1984: 47-56.
- [7] Hsien B T, Sun H M, Hwang T, et al. An Improvement of Saeednia's Identity-based Key Exchange Protocol[C]//Proceedings of Information Security Conference. [S.l.]: IEEE Press, 2002: 41-43.
- [8] Tseng Y M, Jan J K, Wang C H. Cryptanalysis and Improvement of an Identity-based Key Exchange Protocol[J]. Journal of Computers, 2002, 14(3): 17-22.
- [9] Hölbl M, Welzer T. Two Improved Two-party Identity-based Authenticated Key Agreement Protocols [J]. Computer Standards & Interfaces, 2009, 31(6): 1056-1060.
- [10] Shim K. Cryptanalysis of Two Identity-based Authenticated Key Agreement Protocols[J]. IEEE Communications Letters, 2012, 16(4): 554-556.
- [11] 李晓航, 王宏霞, 张文芳. 认证理论及应用[M]. 北京: 清华大学出版社, 2009.
- [12] LaMacchia B, Lauter K, Mityagin A. Stronger Security of Authenticated Key Exchange [C]//Proceedings of ProvSec'07. [S.l.]: Springer-verlag, 2007: 1-16.
- [13] 赵建杰, 谷大武. eCK 模型下可证明安全的双方认证密钥协商协议[J]. 计算机学报, 2011, 34(1): 47-54.

编辑 金胡考