文章编号:1672-3961(2013)02-0011-07 DOI:10.6040/j.issn.1672-3961.0.2012.367

标准模型下基于无证书密钥封装的口令认证密钥交换协议

杨珺涵[1],曹天杰[1,2]
(1. 中国矿业大学计算机学院,江苏 徐州 221116;2. 中科院研究生院信息安全国家重点实验室,北京 100039)

摘要:为确保协议的安全性,提出了一种标准模型下可证安全的口令认证密钥交换协议。利用无证书密钥封装机制来传递口令等用户身份验证信息;基于DDH(decision Diffie-Hellman)假设,在标准模型下证明了新协议的安全性。结果显示,该协议是前向安全的,可实现用户间的双向认证,能够有效地抵抗多种攻击。

关键字:无证书密钥封装;标准模型;交换协议;双向认证;口令认证
中图分类号:TP309 **文献标志码**:A

Password-authenticated key exchange protocol based on certificateless key encapsulation in the standard model

YANG Jun-han[1], CAO Tian-jie[1,2]
(1. School of Computer, China University of Mining and Technology, Xuzhou 221116, China;
2. State Key Laboratory of Information Security, Graduate School of the Chinese Academy of Sciences, Beijing 100039, China)

Abstract: To guarantee the security of exchange protocol, a novel password-authenticated key exchange protocol without random oracle model was introduced. Clients' identity information was delivered by the certificateless key encapsulation mechanism. The security of the proposed protocol was proved in the standard model based on decision Diffie-Hellman (DDH) assumption. Security analysis showed that the provided protocol was forward security and achieved mutual authentication, which could resist multiple attacks.

Key words: certificateless key encapsulation; standard model; exchange protocol; mutual authentication; password authentication

0 引言

1992年,Steven M Bellovin和Michael Merritt首次提出了一个两方口令认证密钥交换协议(2PAKE)[1]。2PAKE协议通常使用"用户—服务器"模型,为了相互认证并建立会话密钥,用户和服务器共享一个口令,对于有n个用户的系统来说,若每两个用户都共享一个口令,则每个用户就需要记住n个口令,整个系统需要存储$O(n^2)$个口令,从而限制了协议在实际中的应用。为了解决这个问题,出现了三方口令认证的密钥交换协议(3PAKE)[2-4]。3PAKE协议中所有的用户只需要和一个可信服务器S共享一个简单的口令,通过S的协助,通信双方完成相互认证和会话密钥的交换。

2003年,Sattam S Al-Riyami和Kenneth G Paterson提出了无证书密码学[5-6](Certificateless public-key cryptography, CL-PKC)。在CL-PKC中,

收稿日期:2012-12-20 **网络出版时间**:2013-03-28 16:08
网络出版地址:http://www.cnki.net/kcms/detail/37.1391.T.20130328.1608.002.html
基金项目:信息安全国家重点实验室开放基金资助项目;江苏省2011年度普通高校研究生科研创新计划资助项目(CXZZ11_0295)
作者简介:杨珺涵(1985-),女,河南开封人,博士研究生,主要研究方向为安全协议与可证明安全. E-mail:yang_junhan@163.com
曹天杰(1967-),男,江苏徐州人,工学博士,教授,博导,主要研究方向为密码学与信息安全. Email:cjcao@cumt.edu.cn

用户的公钥是基于其身份信息生成的。用户的私钥则是由可信中心生成的部分私钥和用户生成的秘密值组成的。作为基于身份的公钥密码学的变体，CL-PKC 结合了传统公钥密码学和基于身份的公钥密码学的优点。也就是说，CL-PKC 消除了密钥托管，同时消除了传统公钥基础设施中证书分发、存储、验证和回收的复杂管理过程。

现存的多数基于口令认证的密钥交换协议缺少必要的安全性证明，或者仅在随机预言模型下讨论了协议的安全性，因此，协议的安全性不可保证。本研究提出了一个标准模型下可证安全的口令认证密钥交换协议，该协议利用无证书密钥封装机制来传递口令等用户身份验证信息。基于 DDH（decision Diffie-Hellman）假设，在标准模型下证明了新协议的安全性，证明结果显示，该协议是前向安全[7-8]的，可实现用户间的双向认证，能够有效地抵抗多种攻击，包括离线字典攻击[9]、不可检测的在线字典攻击[10]和口令泄露假冒攻击。

1 预备知识

定义 1.1（可忽略函数） 函数 $\varepsilon(n): N \to R$ 是一个可忽略函数，当且仅当对于任何正多项式 $\mathrm{poly}(\cdot)$，存在正整数 $N_{\mathrm{poly}} > 0$，使得对于所有 $n > N_{\mathrm{poly}}$，都有

$$\left|\frac{1}{\varepsilon(n)}\right| \leqslant \frac{1}{N_{\mathrm{poly}}}。$$

定义 1.2（伪随机函数） 函数 $F_k(): K \times D \to R$ 是一个伪随机函数集合。$f: D \to R$ 是一个均匀函数集合。形式化定义伪随机函数，考虑进行以下两个实验：

$\mathrm{EXp}_F^{\mathrm{prf}-1}(A)$	$\mathrm{Exp}_F^{\mathrm{prf}-0}(A)$
$k \leftarrow K$	$f \leftarrow f(D,R)$
$b \leftarrow A^{F(k)}$	$b \leftarrow A^f$
返回 b	返回 b

定义对于任意概率多项式时间算法 A 能够区分函数 f 和 F 的优势为

$$\mathrm{Adv}^F(A) = |\Pr[\mathrm{Exp}_F^{\mathrm{prf}-1}(A) = 1] - \Pr[\mathrm{Exp}_F^{\mathrm{prf}-0}(A) = 1]|,$$

如果对于任意概率多项式时间算法 A，都有

$$\mathrm{Adv}^F(A) \leqslant \varepsilon(n),$$

那么 F 是一个安全的伪随机函数。其中，$\varepsilon(\cdot)$ 是一个可忽略函数。

定义 1.3（无证书密钥封装机制 Certificateless Key Encapsulation Mechanism，CL-KEM） 无证书密钥封装机制由以下几个算法组成：

（1）主密钥生成算法 KeyGen(1^k)：输入 1^k，$k \in N$ 是安全参数，输出系统主公私钥对（mpk，msk）。向系统中的全体用户公开主公私 mpk，而主私钥 msk 则由密钥生成中心（Key Generator Center，KGC）秘密保存；

（2）部分私钥生成 PartialKeyGen：输入 mpk、msk 和用户的身份 ID，输出用户的部分私钥 d_{ID}；该算法由 KGC 运行；

（3）用户秘密值生成 SecretKeyGen：输入 mpk 和用户身份 ID，输出该用户的秘密值 x_{ID}；

（4）用户公私钥生成 UserKeyGen：输入 mpk 和用户身份 ID，用户的部分私钥 d_{ID} 和用户的秘密值 x_{ID}，输出该用户的公私钥对（upk，usk）

（5）密钥封装 Encap：输入 mpk，upk 和用户身份 ID，输出 $(C, K) \in C_{\mathrm{PK}} \times K_{\mathrm{PK}}$，其中 C 是密钥 K 的封装，K 是在密钥空间 K_{PK} 中随机均匀选取的。

（6）密钥解封 Decap：输入（d_{ID}，x_{ID}，C），输出密钥 K。

定义 1.4（无证书密钥封装安全） 形式化定义无证书密钥封装机制的安全性，考虑以下实验：

$\mathrm{Experiment\ Challenge}_A^{\mathrm{CL\text{-}KEM}}(k)$

$(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathrm{KeyGen}(1^k)$

$\mathrm{ID} \leftarrow \{0,1\}^*$

$(K_1, e^*) \leftarrow \mathrm{Encap}(\mathrm{mpk}, \mathrm{upk}, \mathrm{ID}^*)$

随机选择 $K_0 \leftarrow K^K_{\mathrm{mpk,upk,ID}^*}$

$b \leftarrow \{0,1\}$，$A \leftarrow (K_b, e^*)$

返回 b

定义对于任意概率多项式时间算法 A 能够破解无证书密钥封装机制的优势为 $\mathrm{Adv}^{\mathrm{CL\text{-}KEM}}(A) = |\Pr[\mathrm{exp\ Challenge}_A^{\mathrm{CL\text{-}KEM}}(k) - 1/2|$，如果对于任意概率多项式时间算法 A，都有

$$\mathrm{Adv}^{\mathrm{CL\text{-}KEM}}(A) \leqslant \varepsilon(n),$$

那么无证书密钥封装机制是安全的。其中，$\varepsilon(\cdot)$ 是一个可忽略函数。

假设 1.1（Decisional Diffie-Hellman assumption，DDH 假设） 设大素数 p, q 满足 $q \mid p-1$，且 G_q 是 Z_p^* 的一个阶为 q 的子群，g 是群 G_q 的一个生成元，如果对于任意随机数 $u, v \in Z_p^*$，给定三元组 (g, g^u, g^v)，任何概率多项式时间算法 A 都不能区分 (g, g^u, g^v, g^{uv}) 和 (g, g^u, g^v, Z)，$Z \in Z_p^*$ 是随机数，则称 G_q 上 DDH 假设成立。

2　标准模型

2.1　协议参与方

模型包括一个用户集合 $C \in$ Client 和一个服务器集合 $S \in$ Server。每个用户与服务器共享一个从口令字典 D 中独立均匀选取的用户口令 PW,口令字典 D 的大小为 $|D|$。

协议中的每个参与者被模拟为一组概率多项式时间(Probability polynomial time, PPT)预言机。用预言机 Π_U^i 表示参与者 U 的第 i 个实例。

模型中还包括一个主动攻击者(用 A 表示),攻击者可以具有如下的能力:(1) 能够偷听、阻止和截获网络中传输的消息;(2) 能够存储所获取或者自身生成的消息;(3) 能够伪造并发送消息;(4) 能够假冒合法的主体参与协议的运行;(5) 熟知各种密码算法,具有密码分析的能力;(6) 能够获知各个合法主体的标识符和公钥;(7) 拥有自己的加密和解密密钥;(8) 具有各种攻击的知识和能力;

同时攻击者能力不可能无限大,所受的限制如下:(1) 攻击者不能在不知道密钥的情况下恢复明文;(2) 攻击者不能预知随机数;(3) 攻击者不能从公钥计算出对应的私钥;攻击者也被模拟为一个概率多项式时间 PPT 预言机,并且可以发起多个协议实例的并行运行。

2.2　通信模型

模型将攻击者的能力抽象为对以下所描述的预言机的若干查询,并且这些查询可以是无序和自适应的。攻击者可以发起如下询问。

Execute(Π_U^i))查询:这种查询用于模拟了攻击者被动攻击,如窃听等。查询的输出为协议执行过程中用户之间交互的所有的信息。

Send(Π_U^i, m)查询:这种查询用于模拟攻击者的主动攻击,如删除、修改、伪造、重放或假冒等。按照协议规则回复该查询,查询的输出为实例 Π_U^i 在收到攻击者查询消息 m 后的响应输出。查询消息 m 可能是攻击者重放以前的某个实例消息,也可能是攻击者伪造的消息。若预言机收到的消息为空,表示攻击者让预言机发起一个新的会话。

Reveal(Π_U^i)查询:这种查询模拟了用户 Π_U^i 会话密钥的泄漏,该查询的返回值为被询问用户实例 Π_U^i 的会话密钥。如果一个预言机 Π_U^i 接受所有收到的消息并且已经生成相应的会话密钥,称这个实例是已经接受的。如果预言机 Π_U^i 还不是“已接受”,则返回一个符号. $\perp$ 表示终止。执行了 reveal 查询的实例状态是打开的。

Corrupt(Π_U^i)查询:这种查询用于模拟前向安全和判断协议是否抵抗口令泄露假冒攻击,返回值为被询问预言机 Π_U^i 的口令。回答过 corrupt 查询的预言机的状态称为“已腐化”。

Test(Π_U^i)查询:这种查询用于判断协议的语义安全性。它只能运行一次,并且只能对一个“新鲜”的预言机进行查询。协议在开始之前随机选择一个比特值 $b \in \{0,1\}$,当攻击者进行 Test 查询时,如果 $b=0$,则返回预言机真实的会话密钥;否则,返回一个均匀分布的随机值,攻击者根据返回值以及利用其他查询获得的信息,猜测 b 的值,记为 b'。

2.3　安全性定义

定义 2.1　会话标识符(SID):预言机 Π_U^i 发送的和接收的所有消息的串联。

定义 2.2　搭档预言机:定义预言机 Π_U^i 的意定通信方 PID_U^i 为搭档预言机。

定义 2.3　匹配会话:我们说 $\Pi_{U_1}^{i_1}$ 和 $\Pi_{U_2}^{i_2}$ 匹配会话,当且仅当:

(1) $\Pi_{U_1}^{i_1}$ 和 $\Pi_{U_2}^{i_2}$ 都在接受的状态;

(2) $\Pi_{U_1}^{i_1}$ 和 $\Pi_{U_2}^{i_2}$ 有相同且非空的会话标识符 SID;

(3) $\Pi_{U_2}^{i_1}$ 是 $\Pi_{U_2}^{i_2}$ 的搭档,反之亦然。即 $\mathrm{PID}_{U_2}^{i_2} = \Pi_{U_1}^{i_1}$, $\mathrm{PID}_{U_1}^{i_1} = \Pi_{U_2}^{i_2}$;

(4) 除 $\Pi_{U_1}^{i_1}$ 和 $\Pi_{U_2}^{i_2}$ 外没有其它实例的搭档预言机为 $\Pi_{U_2}^{i_2}$ 和 $\Pi_{U_1}^{i_1}$。

定义 2.4　新鲜预言机。

(1) $\Pi_{U_1}^{i_1}$ 在已接受状态下,无论是否存在一个搭档 $\Pi_{U_2}^{i_2}$;

(2) $\Pi_{U_1}^{i_1}$ 未打开,其搭档预言机 $\Pi_{U_2}^{i_2}$ 也未打开;

(3) $\Pi_{U_1}^{i_1}$ 和 $\Pi_{U_2}^{i_2}$ 没有进行过 Corrupt 查询。

定义 2.5　协议的语义安全性:如果在 Test 查询中,攻击者成功猜对 b 的值,则称攻击者成功。定义攻击者的成功的概率为

$$\Pr[\mathrm{Succ}] = \Pr[b = b'],$$

相应的,攻击者的优势函数为

$$\mathrm{Adv}_D^{\mathrm{PAKE}}(A) = 2\Pr[\mathrm{Succ}] - 1,$$

攻击者优势函数的最大值为

$$\mathrm{Adv}_D^{\mathrm{PAKE}}(t,R) = \max_A\{\mathrm{Adv}_D^{\mathrm{PAKE}}(A)\},$$

如果

$$\mathrm{Adv}_D^{\mathrm{PAKE}}(t,R) \leqslant O\left(\frac{q_s}{|D|}\right) + \varepsilon(n),$$

则称协议是语义安全的。其中,t 表示计算时间;R 表示消耗的资源;q_s 表示 Send 查询即主动攻击的

会话数；$|D|$表示所有口令字典的大小；$\varepsilon(\cdot)$是一个可忽略函数；$O(q_s/|D|)$保证每次 Send 查询，攻击最多排除常数个可能的口令。

为了证明协议能够抵抗在线字典攻击、口令泄露假冒攻击，判断协议是否提供用户间的相互认证是十分必要的。假设存在攻击者 A_{auth}，并且攻击者能够进行 Execute，Send，Reveal，Corrupt 和 Test 询问。

定义 No-Matching$^{A_{\text{auth}}}(k)$表示 $\Pi_{U_1}^{i_1}$（或 $\Pi_{U_2}^{i_2}$）接受了但不存在 $\Pi_{U_2}^{i_2}$（或 $\Pi_{U_i}^{i}$）与它有匹配对话，k 为安全参数。攻击者的优势函数为

$$\text{Adv}_D^{\text{auth}}(A_{\text{auth}}) = \Pr[\text{No-Matching}^{A_{\text{auth}}}(k)],$$

记攻击者优势函数的最大值为：

$$\text{Adv}_D^{\text{auth}}(t,R) = \max_{A_{\text{auth}}}\{\text{Adv}_D^{\text{auth}}(A_{\text{auth}})\}。$$

定义 2.6 用户间的双向认证。三方口令认证密钥交换协议提供用户间的双向认证，满足以下两个条件：

（1）$\Pi_{U_1}^{i_1}$和 $\Pi_{U_2}^{i_2}$是搭档，且两者同时接受；

（2）No-Matching$^{A_{\text{auth}}}(k)$发生的概率是可忽略的，即

$$\text{Adv}_D^{\text{auth}}(t,R) \leqslant \varepsilon(n),$$

其中，t 表示计算时间；R 表示消耗的资源；D 表示口令字典；$\varepsilon(\cdot)$是一个可忽略函数。

3 基于无证书密钥封装的口令认证密钥交换协议

提出了一个基于无证书密钥封装的口令认证密钥交换协议，并在标准模型下证明了该协议的安全性。结果显示该协议具有以下优点：（1）前向安全；（2）双向认证；（3）抵抗字典攻击；（4）抵抗口令泄露假冒攻击。

3.1 协议描述

下面给出文中使用的所有符号定义：

A，B：用户 Alice 和 Bob 的身份标识符；

S：服务器的标识符；

PW_A，PW_B：用户 Alice 和 Bob 的口令；

$h(\cdot)$：安全哈希函数，输出长度为 128 位；

$F_k(\cdot)$：带密钥 k 的伪随机函数；

p，q：足够大的素数，满足 $q|(p-1)$；

G_q：Z_p^*的一个子群，阶为 q；

g：群 G 的一个生成元；

$\oplus$：异或操作；

$\|$：连接操作；

$=?$：验证是否相等操作；

Encap$(\cdot)$：密钥封装；

Decap$(\cdot)$：密钥解封装；

$E(\cdot)$：对称加密；

$D(\cdot)$：对称解密。

除了指数外所有的表达式都是 mod p 的。为了表达上的简便，文中省略了“mod p”。

系统主公私钥对（mpk，msk），可信中心 KGC 运行 PartialKeyGen 算法生成服务器的部分私钥 d_S，服务器运行 SecretKeyGen 算法生成秘密值 x_S，（spk，ssk）是服务器的公私钥对。

假设 Alice 想要和 Bob 进行安全通信，要在 Alice和 Bob 之间建立安全信道，而且该信道有Alice 和 Bob 协商出的会话密钥的支撑。协议具体见图 1。

第一步：服务器选取两个随机数 a，$b \in Z_p^*$，计算 $S_1 = g^a$，$S_2 = g^b$，$S_\text{A} = S_1 \oplus h(\text{PW}_\text{A})$和 $S_\text{B} = S_2 \oplus h(\text{PW}_\text{B})$，并将消息（$A$，$B$，$S$，$S_\text{A}$）和（$A$，$B$，$S$，$S_\text{B}$）分别发送给 Alice 和 Bob。

第二步：Alice 利用口令 PW_A 恢复消息 S_1，然后随机选择 x_1，$x_2 \in Z_p^*$，计算 $X_1 = g^{x_1}$，$X_2 = (S_1)^{x_1}$，$(K_\text{A}, e_\text{A}) \in_R \text{Encap}(\text{spk}, S)$ 和 $X_3 = E_{e_\text{A}}(X_1 \| X_2 \| x_2 \| A \| S \| B)$，并将（$K_\text{A}$，$X_3$，$A$，$S$，$B$）发送给服务器。

同样的，Bob 利用口令 PW_B 恢复消息 S_2，然后，随机选择 y_1，$y_2 \in Z_p^*$，计算 $Y_1 = g^{y_1}$，$Y_2 = (S_2)^{x_1}$，$(K_\text{B}, e_\text{B}) \in_R \text{Encap}(\text{spk}, S)$ 和 $Y_3 = E_{e_\text{B}}(Y_1 \| Y_2 \| y_2 \| B \| S \| A)$，并将（$K_\text{B}$，$Y_3$，$B$，$S$，$A$）发送给服务器。

第三步：服务器解封装得到 $e_\text{A} = \text{Decap}(\text{ssk}, K_\text{A}, S)$，解密 $D_{e_\text{A}}(X_3)$得到 X_1，X_2，x_2。服务器验证 $(X_1)^a$ 是否等于 X_2。如果相等，则服务器认证 Alice，计算 $T_\text{A} = F_{x_2}(X_1 \| Y_1 \| A \| S \| B)$，并将（$S$，$A$，$B$，$Y_1$，$T_\text{A}$）发送给 Alice；否则，终止协议。

同样的，服务器解封装计算得到 $e_\text{B} = \text{Decap}(\text{ssk}, K_\text{B}, S)$，解密 $D_{e_\text{B}}(Y_2)$得到 Y_1，Y_2，y_2。服务器验证 $(Y_1)^b$ 是否等于 Y_2。如果相等，服务器认证 Bob，计算 $T_B = F_{y_2}(Y_1 \| X_1 \| B \| S \| A)$，并将（$S$，$B$，$A$，$X_1$，$T_B$）发送给 Bob；否则，终止协议。

第四步：收到服务器的消息后，Alice 验证收到 T_A 和利用 X_1，x_2和 Y_1 计算得到的 T_A 是否相等。如果相等，Alice 计算会话密钥 $\text{SK} = Y_1^{x_1}$；否则，终止协议。

同样的，收到服务器的消息后，Bob 验证收到 T_B 和利用 Y_1，y_2和 X_1 计算得到的 T_B 是否相等。如果相等，Bob 计算会话密钥 $\text{SK} = X_1^{y_1}$；否则，终止协议。

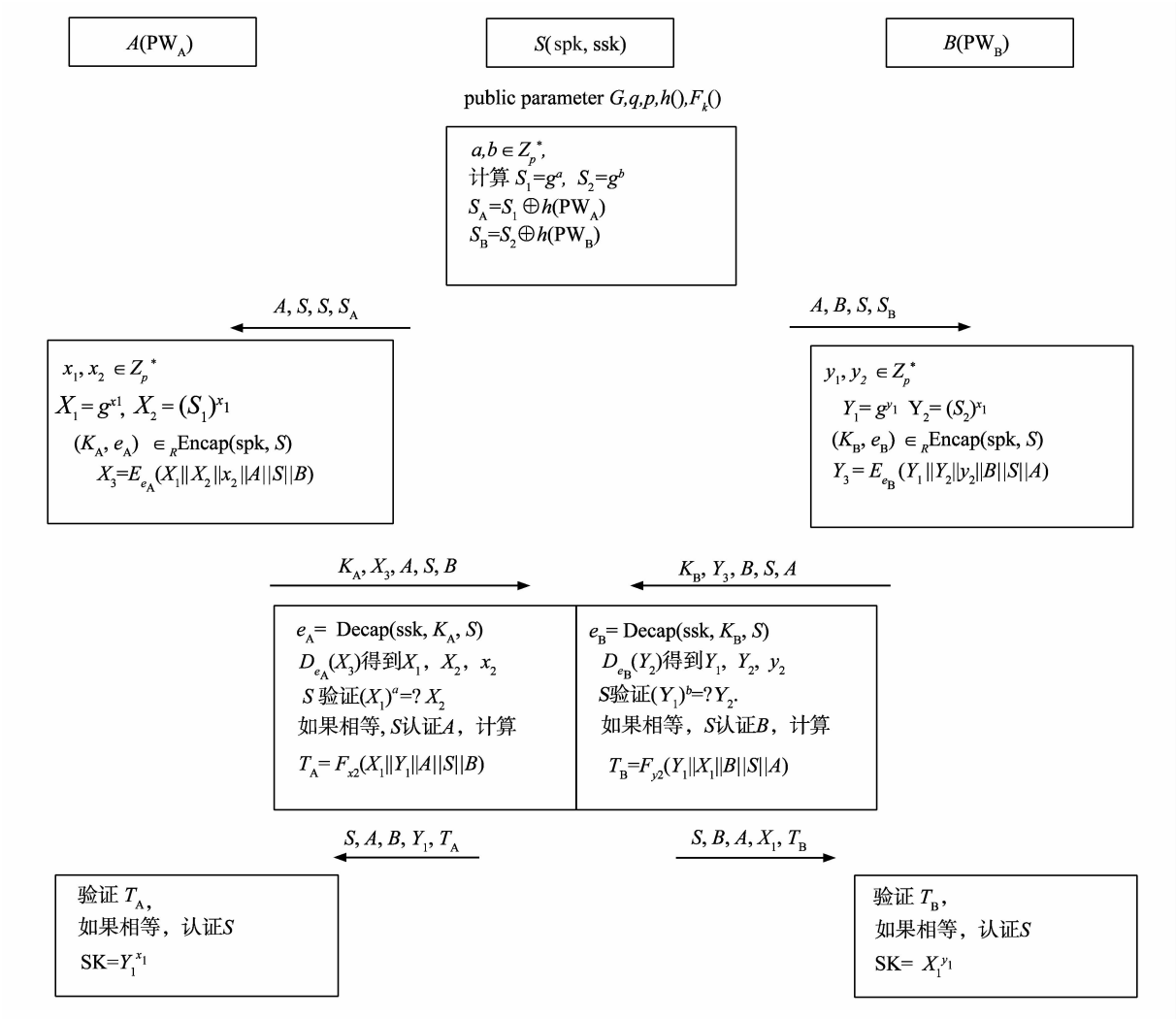

图 1　基于无证书密钥封装的口令认证密钥交换协议

Fig. 1　CL-KEM based password-authenticated key exchange protocol in the standard model

3.2　协议的安全性证明

定理 1　p,q 是大素数且满足 $q \mid p-1$, G_q 是 Z_p^* 的一个阶为 q 的子群, g 是群 G_q 的一个生成元, 群 G 上 DDH 假设成立, CL-KEM 是安全的无证书密钥封装机制, F 是安全的伪随机函数集合, 则基于无证书密钥封装的口令认证密钥交换协议前向安全且抵抗字典攻击。即

$$\mathrm{Adv}_{G,g}^{\text{CL-KEM-PAKE}}(A) \leqslant \frac{q_e}{q-1} + (q_e+q_s)\,\mathrm{Adv}_A^{\text{CL-KEM}} + (q_e+q_s)\,\mathrm{Adv}_A^{F} + q_r \mathrm{Adv}_{G,g}^{\text{DDH}} + q_s\left(\frac{1}{|D|}+\frac{1}{2^n}\right),$$

其中, $|D|$ 表示口令字典的大小, q_e, q_s, q_r, 分别表示攻击者进行 Execute 查询、Send 查询和 Reveal 查询的次数。

定理证明　本研究设计一系列的混合实验, 在所有的实验中, 预言机按协议的描述回答攻击者的查询。实验 0 模拟的是攻击者对协议的一次真实的攻击, 以后的实验中逐步修改预言机的回答方式, 使攻击者在两个相邻实验中成功概率的差值是可以忽略的。

实验 0　是针对协议的真实攻击实验。事件 Succ_0 表示攻击者成功猜出 Test 查询中所使用的比特 b,

$$\mathrm{Adv}_D^{\text{CL-KEM-PAKE}}(A) = 2\Pr[\mathrm{Succ}_0] - 1。$$

实验 1　当攻击者进行 Execute 查询时, 将 K_A, K_B 替换为随机数。运用混合证明技巧, 可得引理 1。

引理 1　$|\Pr[\mathrm{Succ}_1] - \Pr[\mathrm{Succ}_0]| \leqslant q_e \mathrm{Adv}_A^{\text{CL-KEM}}$。

引理证明　假设存在能够区分混合证明实验 $\mathrm{Hybrid}_{1,j-1}$ 和 $\mathrm{Hybrid}_{1,j}$ 的攻击者 $A_{1,j}$。在运行协议 P_j 前均匀的选取一个随机比特值 $b, j \in \{0, q_e\}$, 然后,

(1) 前 $j-1$ 次会话, $A_{1,j}$ 按照实验 1 模拟的环境, 收到一个随机的 CL-KEM 密钥值;

(2) 第 j 次会话, $A_{1,j}$ 选取一个随机值 $Z \in$

Z_p^*；

（3）余下第 $q_e - j$ 次会话，$A_{1,j}$按照实验0模拟的环境，收到一个真实的 CL-KEM 密钥值。

最后，$A_{1,j}$进行 Test 查询，猜测比特值 b'。如果 $b' = b$，$A_{2,j}$输出 1；否则，输出 0。CL-KEM 是安全的，攻击者无法区分两次实验，故有：

$$|\Pr[\mathrm{Succ}_1] - \Pr[\mathrm{Succ}_0]| \leqslant q_e \mathrm{Adv}_A^{\text{CL-KEM}}。$$

实验 2 当攻击者进行 Execute 查询时，将消息 X_3，Y_3 替换为随机数，目前为止，攻击者并为获得任何有用的信息，故有引理2。

引理 2 $|\Pr[\mathrm{Succ}_2] - \Pr[\mathrm{Succ}_1]| \leqslant \dfrac{q_e}{q-1}$。

实验 3 当攻击者进行 Execute 查询时，将消息 T_A，T_B 替换为随机数，运用混合证明技巧，可得引理3。

引理 3 $|\Pr[\mathrm{Succ}_3] - \Pr[\mathrm{Succ}_2]| \leqslant q_e \mathrm{Adv}_A^F$。

引理证明 记混合证明实验3为 $\mathrm{Hybrid}_{3,j}$，$j \in \{0, q_e\}$。假设存在能够区分混合实验 $\mathrm{Hybrid}_{3,j-1}$ 和 $\mathrm{Hybrid}_{3,j}$攻击者 $A_{3,j}$。$A_{3,j}$在运行协议 P_j前均匀的选取一个随机比特值 b，定义实验 $\mathrm{Hybrid}_{3,j}$过程如下：

（1）前 $j-1$ 次会话，$A_{3,j}$按照实验3模拟的环境计算，运用均匀函数计算 T_A，T_B；

（2）第 j 次会话，T_A，T_B 替换为随机值；

（3）余下第 $q_e - j$ 次会话，$A_{3,j}$按照实验2模拟的环境，运用伪随机函数 F 计算 T_A，T_B。

最后，进行 Test 查询，$A_{3,j}$猜测比特值 b'。如果 $b' = b$，$A_{3,j}$输出 1；否则，输出 0。现在分析攻击者 $A_{3,j}$的优势，根据伪随机函数定义，故有：

$$|\Pr[\mathrm{Succ}_3] - \Pr[\mathrm{Succ}_2]| \leqslant q_e Adv_A^F。$$

实验1到实验3显示了攻击者不能通过被动攻击获得任何有用信息。下面开始考虑主动攻击。

实验 4 当攻击者进行 Send 查询时，用随机数替代消息 K_A，K_B，故有引理4。

引理 4 $|\Pr[\mathrm{Succ}_4] - \Pr[\mathrm{Succ}_3]| \leqslant \dfrac{q_s}{2^n}$。

实验 5 当攻击者进行 Send 查询时，用随机数替代消息 X_3，Y_3。运用混合证明技巧，可得引理5。

引理 5 $|\Pr[\mathrm{Succ}_5] - \Pr[\mathrm{Succ}_4]| \leqslant \dfrac{q_s}{|D|} + q_s \mathrm{Adv}_A^{\text{CL-KEM}}$。

引理证明 构造一个攻击者 $A_{5,j}$实施离线字典攻击和在线字典攻击。

（1）$A_{5,j}$在离线的情况下，猜测用户口令，成功的概率为 $q_s/|D|$；（2）$A_{5,j}$猜测用户口令 PW_A'，$\mathrm{PW}_\mathrm{B}' \in \{0,1\}^n$，通过在线字典攻击，成功的概率为 $q_s \mathrm{Adv}_A^{\text{CL-KEM}}$。

故有，

$$|\Pr[\mathrm{Succ}_5] - \Pr[\mathrm{Succ}_4]| \leqslant \frac{q_s}{|D|} + q_s \mathrm{Adv}_A^{\text{cl-kem}}。$$

实验 6 当攻击者进行 Send 查询时，用随机数替代消息 T_A，T_B。由于攻击者不知道 e_A，e_B，故有引理6。

引理 6 $|\Pr[\mathrm{Succ}_6] - \Pr[\mathrm{Succ}_5]| \leqslant q_s \mathrm{Adv}_A^F$。

实验 7 当攻击者进行 Reveal 查询时用随机数代替会话密钥 SK。基于 DDH 假设，可得引理7。

引理 7 $|\Pr[\mathrm{Succ}_7] - \Pr[\mathrm{Succ}_6]| \leqslant q_r \mathrm{Adv}_{g,G}^{\text{DDH}}$。

引理证明 构造一个攻击者 $A_{7,j}$能够解决 DDH 困难问题。在协议运行之前，随机选择一个比特 b，然后

（1）前 $j-1$ 个会话，$A_{7,j}$计算 $\mathrm{SK} = g^r$，其中，$r \in_R Z_p^*$；

（2）第 j 个会话，$A_{7,j}$ 计算 $\mathrm{SK} = Z$，其中，$Z \in_R Z_p^*$；

（3）最后 $q_r - j$ 个会话，$A_{7,j}$计算 $X_1 = g^{x_1}$，$Y_1 = g^{y_1}$，$\mathrm{SK} = g^{x_1 y_1}$，其中，$x_1$，$y_1 \in_R Z_p^*$。

最后，进行 Test 查询，$A_{7,j}$猜测 b'。如果 $b' = b$，$A_{7,j}$输出 1，否则，输出 0。故有，

$$|\Pr[\mathrm{Succ}_7] - \Pr[\mathrm{Succ}_6]| \leqslant q_r \mathrm{Adv}_{g,G}^{\text{DDH}}。$$

由引理1至引理7，可以推导出定理1，有

$$\begin{aligned}\mathrm{Adv}_{G,g}^{\text{CL-KEM-PAKE}}(A) \leqslant{}& \frac{q_e}{q-1} + (q_e + q_s)\mathrm{Adv}_A^{\text{CL-KEM}} + \\ & (q_e + q_s)\mathrm{Adv}_A^F + q_r \mathrm{Adv}_{G,g}^{\text{DDH}} + \\ & q_s\left(\frac{1}{|D|} + \frac{1}{2^n}\right)。\end{aligned}$$

定理 2 p, q 是大素数且满足 $q \mid p-1$，G_q 是 Z_p^* 的一个阶为 q 的子群，g 是群 G_q 的一个生成元，群 G 上 DDH 假设成立，CL-KEM 是安全的无证书密钥封装机制，F 是安全的伪随机函数集合，则基于无证书密钥封装的口令认证密钥交换协议提供双向认证且抵抗口令泄露的假冒攻击。即

$$\begin{aligned}\Pr[\text{No-Matching}^{A_{\text{auth}}}(k)] \leqslant{}& q_s \mathrm{Adv}_A^{\text{CL-LEM}} + q_s \mathrm{Adv}_A^F + \\ & q_s\left(\frac{1}{|D|} + \frac{1}{2^n}\right),\end{aligned}$$

其中，$|D|$ 表示口令字典的大小，q_s 表示攻击者 Send 查询次数。

定理证明：

实验 8 是针对协议的真实攻击。根据定义有：

$$\Pr[\text{No-Matching}^{A_{\text{auth}}}(k)] = \Pr[\mathrm{Succ}_8]。$$

实验 9　当攻击者进行 Send 查询时,用随机数替代消息 K_A, K_B。故有引理 8。

引理 8　$|\Pr[\mathrm{Succ}_9]-\Pr[\mathrm{Succ}_8]|\leqslant\frac{q_s}{2^n}$。

实验 10　当攻击者进行 Send 查询时,用随机数替代消息 X_3, Y_3。运用混合证明技巧,可得引理 9。

引理 9　$|\Pr[\mathrm{Succ}_9]-\Pr[\mathrm{Succ}_8]|\leqslant\frac{q_s}{|D|}+q_s\mathrm{Adv}_A^{\text{CL-KEM}}$。

实验 11　当攻击者进行 Send 查询时,用随机数替代消息 T_A, T_B。基于安全的伪随机函数 F,可得引理 10。

引理 10　$|\Pr[\mathrm{Succ}_{10}]-\Pr[\mathrm{Succ}_9]|\leqslant q_s\mathrm{Adv}_A^F$。

由引理 8 至引理 10,可以推导出定理 2,有:

$$\Pr[\text{No-Matching}^{A_{\text{auth}}}(k)]\leqslant q_s\mathrm{Adv}_A^{\text{CL-LEM}}+q_s\mathrm{Adv}_A^F+q_s\left(\frac{1}{|D|}+\frac{1}{2^n}\right)。$$

4　结论

本研究提出了一个基于无证书密钥封装的口令认证密钥交换协议,并在标准模型下证明了该协议的安全性。结果显示该协议具有以下优点:

(1) 前向安全:即使攻击者知道用户的口令,也不能获得上一轮用户协商出的会话密钥;

(2) 双向认证:通信双方在第三方服务器的帮助下认证对方的身份;

(3) 抵抗字典攻击:攻击者不能猜测或者验证得到用户口令;

(4) 抵抗口令泄露假冒攻击:即使攻击者知道用户的口令,也不能假冒用户。

参考文献:

[1] BELLOVIN S M, MERRITT M. Encrypted key exchange: password-based protocols secure against dictionary attacks [C]//Proceedings of IEEE Symposium on Research in Security and Privacy. Oakland, USA: IEEE, 1992:72-84.

[2] BELLARE M, ROGAWAY P. Provably secure session key distribution-the three party case[C]//Proceedings of Annual ACM Symposium on Theory of Computing. New York, USA: ACM, 1996:57-66.

[3] KWON J O, JEONG I R, LEE D H. Light-weight key exchange with different passwords in the standard model [J]. Journal of Universal Computer Science, 2008, 15 (5):312-332.

[4] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks [C]//Proceedings of Advances in Cryptology-EUROCRYPT2000. Berlin: Springer, 2000:139-155.

[5] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]//Proceedings of Advances in Cryptology-ASIACRYPT 2003. Berlin: Springer, 2003: 452-473.

[6] HUANG Q, WONG S D. Generic certificateless key encapsulation mechanism [C]//Proceedings of Information Security and Privacy: ACISP 2007. Berlin: Springer, 2007:215-229.

[7] ABDALLA M, FOUQUE P A, POINTCHEVAL D. Password-based authenticated key exchange in the three-party setting [C]//Proceedings of PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography. Berlin: Springe, 2005:65-84.

[8] WU S H, ZHU Y F. Three-party password-based authenticated key exchange with forward-security [J]. Chinese Journal of Computers, 2007, 30(10):1833-1841.

[9] GONG L. Optimal authentication protocols resistant to password guessing attacks[C]//Proceedings of 8th IEEE Computer Security Foundations Workshop. Berlin: IEEE, 1995:24-29.

[10] DING Y, HORSTER P. Undetectable on-line password guessing attacks[J]. ACM Operating Systems Review, 1995, 29(4):77-86.

(编辑:陈斌)