

有效的基于混沌映射的三方认证密钥协商协议

李雄¹, 吴凡², 廖俊国¹, 刘玉珍¹

(1. 湖南科技大学计算机科学与工程学院, 湖南 湘潭 411201;

2. 厦门工学院计算机科学与工程系, 福建 厦门 361021)

摘要: 由于良好的密码特性, 混沌映射被用于设计密钥协商协议。在多数基于混沌映射的口令三方密钥协商协议中, 服务器需存储用户口令表, 使这些协议容易遭受口令相关的攻击, 且一旦口令表泄露, 将带来巨大的安全隐患。针对这些安全问题, 提出了一个新的基于混沌映射口令三方认证密钥协商协议, 服务器无需维护用户口令表, 避免了口令相关的攻击。同其他相关协议相比, 所提协议在增强安全性的同时, 大大提高了协议的执行效率。

关键词: 混沌映射; 密钥协商; 认证; 口令

中图分类号: TP 309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00060

Efficient three-party authenticated key agreement protocol based on chaotic map

LI Xiong¹, WU Fan², LIAO Jun-guo¹, LIU Yu-zhen¹

(1. School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China;

2. Department of Computer Science and Engineering, Xiamen Institute of Technology, Xiamen 361021, China)

Abstract: Chaotic map has been used in the design of key agreement protocol due to its excellent properties. In most of password three-party authenticated key agreement protocol based on chaotic map, the server needs to store a sensitive password table. It makes these protocols vulnerable to some password related attacks. Besides, it would be dangerous if the password table was leaked. To resolve the aforementioned problems, a new password three-party authenticated key agreement protocol based on chaotic maps was proposed. The server didn't need to maintain a password table, so the proposed scheme was free from password related attack. Compared with other related protocols, the proposed protocol not only enhances the security, but also improves the efficiency greatly.

Key words: chaotic maps, key agreement, authentication, password

1 引言

随着计算机网络的快速发展和广泛应用, 其

安全问题日益凸显, 如何保护网络会话的安全性变得尤为重要。密钥协商协议可以使2个或多个实体通过公开信道建立共享的会话密钥, 能有效

收稿日期: 2016-05-14; 修回日期: 2016-06-03。通信作者: 李雄, lixiongzhq@163.com

基金项目: 国家自然科学基金资助项目 (No.61300220); 湖南省教育厅一般基金资助项目 (No.15C0545); 福建省高校杰出青年科研人才培育基金资助项目; 福建省中青年骨干教师教育科研基金资助项目 (No. JA14369)

Foundation Items: The National Natural Science Foundation of China(No.61300220), Scientific Research Foundation of Hunan Provincial Education Department (No.15C0545), University Distinguished Young Research Talent Training Program of Fujian Province, The Education Scientific Research Project for Young Teachers of Fujian (No. JA14369)

解决对称密码方案在应用中的密钥分发问题,是信息安全领域的重要基础研究问题。在早期的密钥协商协议^[1,2]中,服务器和用户通过共享长期口令进行密钥协商。因此,攻击者可能从服务器处窃取口令表或通过字典攻击获取用户的口令。在最近的密钥协商协议设计中,研究者极力避免此类问题,并提出了多个两方(服务器—用户)口令密钥协商协议^[3~8]。在这些方案中,用户可以自由选择所持有的口令。而且,为了增强安全性和提供更好的服务,其中一些协议^[3,5,7,8]提供了用户自由选择和更换口令以及保护用户匿名等特性。

上述两方口令密钥协商协议非常适用于“客户—服务器”结构,而不太适用于“客户—客户”结构。在大规模点对点网络环境中,用户所需持有的口令数量与通信实体的数量成比例增加。为克服该问题,多个三方口令密钥协商协议^[9~20]被提出,在这类协议中,通信双方在可信或半可信第三方的协助下生成共享的会话密钥。

混沌系统具有伪随机性、遍历特性,且输出对初始条件非常敏感,当前轨迹的微小变化和扰动就会导致后续状态的显著不同。混沌系统的这些特性正好满足设计密码系统所需的混淆和扩散原则,并被人们广泛应用于设计密码系统,如对称密码算法、散列函数等。最近,研究者们将混沌系统引入密钥协商协议研究中,设计了多个基于切比雪夫混沌映射(chenbyshev chaotic map)的三方密钥协商协议^[9~11,14,16,18,19]。2010年,Wang等^[14]基于混沌映射提出一个三方密钥协商协议,但该协议被Yoon等^[18]指出是不安全的。2013年,Lee等^[10]和Xie等^[16]分别提出基于混沌映射的密钥协商协议。在上述协议中,用户需要与服务器共享长期私钥以完成相互认证和密钥协商。特别在文献[14,16,18]中,用户的身份通过明文方式传输,增加了模仿攻击的风险。2012年,Lai等^[9]基于混沌映射提出一个新的三方密钥协商协议,在该方案中,用户可以自由选择所持有的口令并能保护用户的匿名性。但Zhao等^[19]指出Lai等协议^[9]不能抵抗内部攻击和离线口令猜测攻击,在此基础上他们提出一个新的方案并声称是安全的。经过分析,本文发现Zhao等^[19]的协议不能真正达

成用户和服务器的相互认证。此外,在该方案中,服务器使用2个密钥,在增加不安全因素的同时降低了协议效率。在上述基于混沌映射的口令三方密钥协商协议中,服务器需存储用户口令表,使这些协议容易遭受内部攻击等口令相关的攻击,且一旦口令表泄露,将带来巨大的安全隐患。针对这些安全问题,本文提出一个新的基于混沌映射口令三方认证密钥协商协议,服务器无需维护口令表进行密钥协商。通过分析和比较,本文协议在增强安全性的同时,提高了协议执行效率。

2 预备知识

2.1 切比雪夫混沌映射及困难问题

定义1 切比雪夫多项式。

设 n 是一个整数, x 是区间 $[-1, 1]$ 的一个变量。切比雪夫多项式 $T_n(x):[-1, 1] \rightarrow [-1, 1]$ 定义为 $T_n(x) = \cos(n \arccos(x))$ 。

根据定义1,切比雪夫多项式满足迭代关系 $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$, $n \geq 2$,其中, $T_0(x) = 1$, $T_1(x) = x$ 。

定义2 切比雪夫多项式的混沌特性。

当 $n > 1$ 时, n 维切比雪夫多项式映射 $T_n(x):[-1, 1] \rightarrow [-1, 1]$ 是一个具有不变测度为 $f^*(x) = \frac{1}{\pi}$ 的混沌映射。

定义3 切比雪夫多项式的半群特性。

$$\begin{aligned} T_r(T_s(x)) &= \cos(r \cos^{-1}(\cos(s \cdot \cos^{-1}(x)))) \\ &= \cos(rs \cdot \cos^{-1}(x)) = T_{sr}(x) = T_s(T_r(x)) \end{aligned}$$

其中, r 和 s 是2个正整数, $x \in [-1, 1]$ 。

2008年,Zhang^[21]进一步扩展了定义3,证明了定义在区间 $(-\infty, +\infty)$ 上的切比雪夫多项式仍具有半群特性,即对 $T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) \bmod p$,这里 $n \geq 2$, $x \in (-\infty, +\infty)$, p 是一个大素数,有 $T_r(T_s(x)) = T_{rs}(x) = T_{sr}(x) = T_s(T_r(x)) \bmod p$ 。

定义4 离散对数问题(DLP, the discrete logarithm problem)。

给定2个元素 x 和 y ,找到一个整数 r ,使 $T_r(x) = y$ 。

定义5 Diffie-Hellman问题(DHP, the diffie-hellman problem)。

给定3个元素 x 、 $T_r(x)$ 和 $T_s(x)$,计算 $T_{rs}(x)$ 。

现在一般认为这2个问题是难解的,即不存在多项式时间算法以不可忽略的概率解决上述2

个问题，这也为基于这2个难题设计安全协议提供了可能性。

2.2 安全假设

假设1 敌手能窃听、拦截或篡改公开信道中所有的通信消息，且当用户的智能卡丢失时，敌手能通过能量分析等方法^[22,23]获取用户智能卡中存储的数据。

假设2 服务器S的主密钥 x 、散列函数及对称加解密算法是安全的，即敌手没有多项式时间算法解决这些问题。

假设3 用户的身份标识和口令分别取自2个不同的有限集合，敌手能在多项式时间内猜测其中之一。但根据文献[24, 25]，敌手在多项式时间内同时猜测出身份标识及对应的口令是困难的。

3 新的基于混沌映射的三方密钥协商协议

本节将提出一个新的基于混沌映射的三方口令密钥协商协议。本协议包含3个阶段：初始化阶段、认证与密钥协商阶段以及口令变更阶段。表1给出了本文使用到的符号及其说明。

表1	符号及说明
符号	说明
U_A, U_B	用户A和B
S	远程服务器
ID_A, ID_B	U_A 和 U_B 的身份标识
PW_A, PW_B	U_A 和 U_B 的口令
x	服务器的主密钥
s	一个取自 $(-\infty, +\infty)$ 的随机整数
$a_A, a_B, r_A, r_B, b_A, b_B$	随机数
$h(\cdot)$	单项散列函数
$sk_{AB}(sk_{BA})$	由A(B)生成的会话密钥
$E_k(\cdot)/D_k(\cdot)$	密钥 k 控制下的对称加密/解密算法
$\Rightarrow$	一个安全信道
$\rightarrow$	一个不安全信道
$\oplus$	异或运算符

3.1 初始化阶段

S选择一个随机数 $s \in (-\infty, +\infty)$ 、一个系统主密钥 x 和一个大素数 p 。当用户希望加入系统时，需要向服务器S注册。注册过程以用户A为例说

明，具体如下。

1) $A \Rightarrow S: (ID_A, HPW_A)$

用户A自由选择身份标识 ID_A 和口令 PW_A ，并产生一个随机数 b_A 。A计算 $HPW_A = h(PW_A \| b_A)$ ，并将注册请求 (ID_A, HPW_A) 通过安全信道发送给服务器S。

2) $S \Rightarrow A$: 智能卡

当收到用户A的注册请求消息 (ID_A, HPW_A) ，S产生一个随机数 a_A ，计算 $D_{A1} = h(ID_A \| a_A) \oplus h(x) \oplus HPW_A$ 和 $D_{A2} = h(ID_A \| a_A) \oplus h(x \| a_A)$ ，并将 D_{A1} 、 D_{A2} 、 a_A 和 s 存储在智能卡中。最后，S将智能卡通过安全方式发送给用户A，如通过面对面的方式。

3) $A \Rightarrow$ 智能卡: (D_{A3}, D_{A4})

A计算 $D_{A3} = h(ID_A \| PW_A \| b_A)$ 和 $D_{A4} = h(ID_A \oplus PW_A) \oplus b_A$ ，并将 D_{A3} 和 D_{A4} 存储在智能卡中。

3.2 认证与密钥协商阶段

当用户A和B需要进行安全通信时，可以在服务器的协助下进行相互认证并协商一个共享的密钥。本阶段执行步骤如下，流程如图1所示。

1) $A \rightarrow B: m_1$

A将智能卡插入终端，输入身份标识 ID_A 和口令 PW_A ，智能卡计算 $b_A' = D_{A4} \oplus h(ID_A \oplus PW_A)$ 并检查 $D_{A3} \stackrel{?}{=} h(ID_A \| PW_A \| b_A')$ 。如果不相等，智能卡终止会话；否则，智能卡产生一个随机数 r_A ，计算

$$HPW_A = h(PW_A \| b_A'),$$

$$C_{A1} = D_{A1} \oplus HPW_A \oplus r_A,$$

$$C_{A2} = D_{A2} \oplus r_A,$$

$$C_{A3} = T_{r_A}(s),$$

$$C_{A4} = h(C_{A1} \| C_{A2} \| C_{A3} \| a_A).$$

A将会话请求 $m_1 = \{C_{A1}, C_{A3}, C_{A4}, a_A\}$ 发送给B。

2) $B \rightarrow S: (m_1, m_2)$

跟A相似，B插入智能卡，输入身份标识 ID_B 和口令 PW_B ，智能卡计算 $b_B' = D_{B4} \oplus h(ID_B \oplus PW_B)$ 并检查 $D_{B3} \stackrel{?}{=} h(ID_B \| PW_B \| b_B')$ 。如果它们不相等，智能卡终止会话；否则，B产生一个随机数 r_B ，计算

$$HPW_B = h(PW_B \| b_B'),$$

$$C_{B1} = D_{B1} \oplus HPW_B \oplus r_B,$$

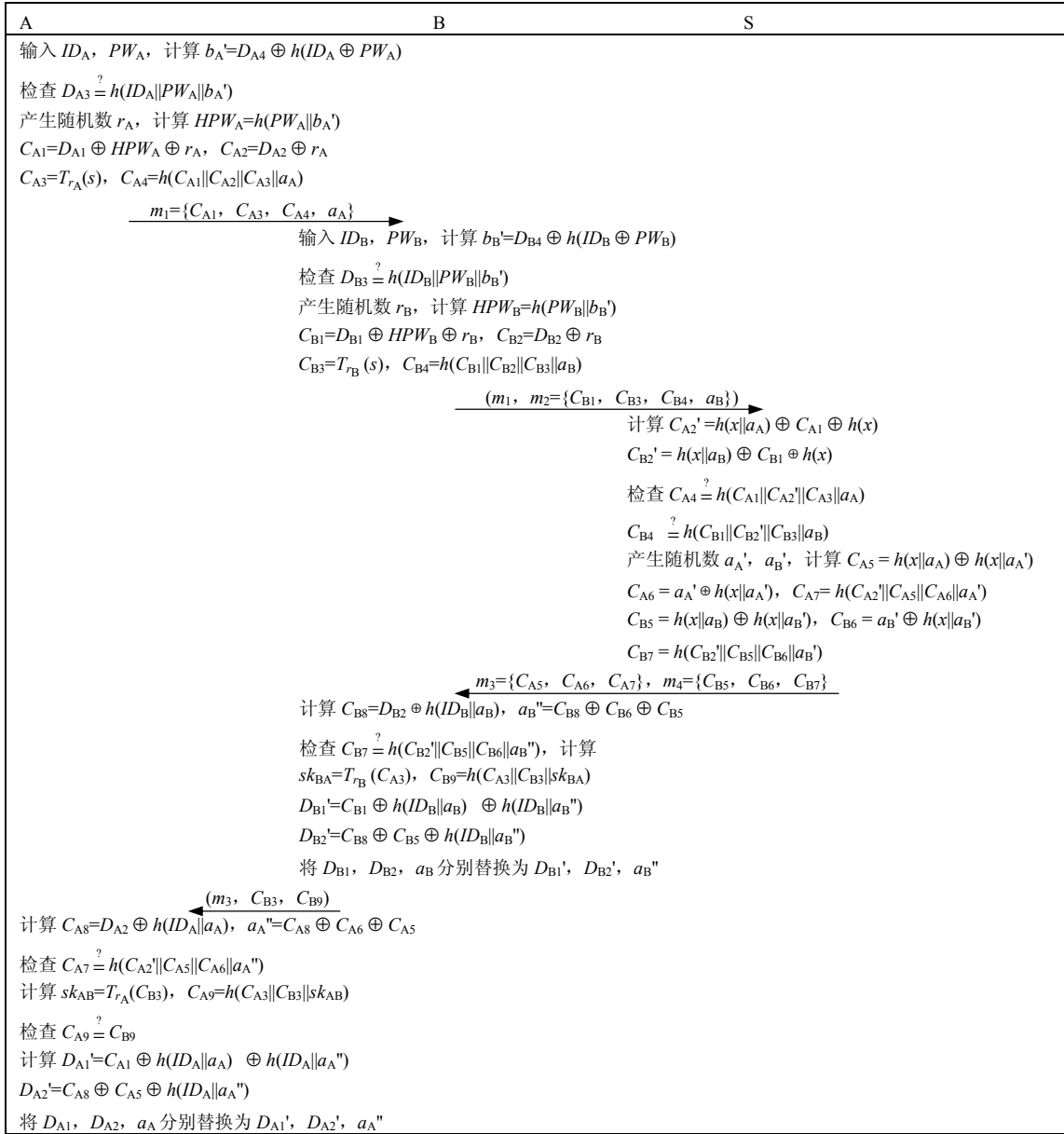


图1 认证与密钥协商阶段流程

$C_{B2} = D_{B2} \oplus r_B$,

$C_{B3} = T_{r_B}(s)$,

$C_{B4} = h(C_{B1} || C_{B2} || C_{B3} || a_B)$.

最后, B 将 $(m_1, m_2 = \{C_{B1}, C_{B3}, C_{B4}, a_B\})$ 发送给服务器 S。

3) S→B: (m_3, m_4)

当收到消息 (m_1, m_2) , S 计算 $C_{A2}' = h(x || a_A) \oplus C_{A1} \oplus h(x)$ 和 $C_{B2}' = h(x || a_B) \oplus C_{B1} \oplus h(x)$ 。然后, 检查 $C_{A4} \stackrel{?}{=} h(C_{A1} || C_{A2}' || C_{A3} || a_A)$ 和 $C_{B4} \stackrel{?}{=} h(C_{B1} || C_{B2}' || C_{B3} || a_B)$ 。如果两者中任意一个不成立, 服务器 S 拒绝会话。否则, S 产生 2 个随机数 a_A' 和 a_B' , 计算

$$C_{A5} = h(x || a_A) \oplus h(x || a_A'),$$

$$C_{A6} = a_A' \oplus h(x || a_A'),$$

$$C_{A7} = h(C_{A2}' || C_{A5} || C_{A6} || a_A'),$$

$$C_{B5} = h(x || a_B) \oplus h(x || a_B'),$$

$$C_{B6} = a_B' \oplus h(x || a_B'),$$

$$C_{B7} = h(C_{B2}' || C_{B5} || C_{B6} || a_B').$$

S 将认证消息 $m_3 = \{C_{A5}, C_{A6}, C_{A7}\}$ 和 $m_4 = \{C_{B5}, C_{B6}, C_{B7}\}$ 发送给 B。

4) B→A: (m_3, C_{B3}, C_{B9})

当收到 S 发送的消息 (m_3, m_4) 后, B 计算 $C_{B8} = D_{B2} \oplus h(ID_B || a_B)$ 和 $a_B'' = C_{B8} \oplus C_{B6} \oplus C_{B5}$, 并检查 $C_{B7} \stackrel{?}{=} h(C_{B2}' || C_{B5} || C_{B6} || a_B'')$ 。如果它们不相等, B

终止会话。否则, B 计算

$$sk_{BA} = T_{r_B}(C_{A3}),$$

$$C_{B9} = h(C_{A3} \| C_{B3} \| sk_{BA}),$$

$$D_{B1}' = C_{B1} \oplus h(ID_B \| a_B) \oplus h(ID_B \| a_B''),$$

$$D_{B2}' = C_{B8} \oplus C_{B5} \oplus h(ID_B \| a_B'').$$

B 将 D_{B1} , D_{B2} 和 a_B 分别替换为 D_{B1}' , D_{B2}' 和 a_B'' , 将 sk_{BA} 作为与 A 共享的会话密钥。最后, B 将消息(m_3 , C_{B3} , C_{B9})发送给 A。

5) 当收到 B 发送的消息(m_3 , C_{B3} , C_{B9}), A 计算 $C_{A8} = D_{A2} \oplus h(ID_A \| a_A)$, $a_A'' = C_{A8} \oplus C_{A6} \oplus C_{A5}$, 并检查 $C_{A7} \stackrel{?}{=} h(C_{A2} \| C_{A5} \| C_{A6} \| a_A'')$ 。如果等式不成立, A 终止会话; 否则, A 计算 $sk_{AB} = T_{r_A}(C_{B3})$, $C_{A9} = h(C_{A3} \| C_{B3} \| sk_{AB})$, 并检查 $C_{A9} \stackrel{?}{=} C_{B9}$ 。如果等式不成立, A 终止会话; 否则 A 计算 $D_{A1}' = C_{A1} \oplus h(ID_A \| a_A) \oplus h(ID_A \| a_A'')$, $D_{A2}' = C_{A8} \oplus C_{A5} \oplus h(ID_A \| a_A'')$ 。最后, A 将 D_{A1} , D_{A2} 和 a_A 分别替换为 D_{A1}' , D_{A2}' 和 a_A'' , sk_{AB} 作为与 B 共享的会话密钥保障后续的安全通信。

3.3 口令变更阶段

当用户需要变更口令时, A 将智能卡插入读卡器, 输入身份标识 ID_A 口令 PW_A 。智能卡计算 $b_A' = D_{A4} \oplus h(ID_A \oplus PW_A)$, 检查 $D_{A3} \stackrel{?}{=} h(ID_A \| PW_A \| b_A')$ 。如果不相等, 智能卡拒绝请求; 否则, A 输入一个新的口令 PW_A^{new} , 智能卡产生一个新的随机数 b_A^{new} , 计算

$$HPW_A = h(PW_A \| b_A'),$$

$$HPW_A^{new} = h(PW_A^{new} \| b_A^{new}),$$

$$D_{A1}^{new} = D_{A1} \oplus HPW_A^{new} \oplus HPW_A,$$

$$D_{A3}^{new} = h(ID_A \| PW_A^{new} \| b_A^{new}),$$

$$D_{A4}^{new} = h(ID_A \oplus PW_A^{new}) \oplus b_A^{new}。$$

最后, A 将 D_{A1} , D_{A3} 和 D_{A4} 分别替换为 D_{A1}^{new} , D_{A3}^{new} 和 D_{A4}^{new} 。

4 安全性分析

本节分析本文所提方案的安全性, 安全性分析表明, 本文方案能够抵抗多种常见的攻击。

4.1 内部攻击

在身份认证方案和基于口令的密钥协商协议中, 由于在注册或初始化阶段用户将身份标识和口令以明文方式发送给服务器, 一旦服务器内部人员获得用户的身份标识和口令, 这类方案容易

遭受内部攻击。在本文方案的初始化阶段, 用户 A 发送(ID_A , HPW_A)给服务器 S 请求注册, 这里 ID_A 是用户 A 选择的身份标识, $HPW_A = h(PW_A \| b_A)$, PW_A 是用户选择的口令, b_A 是用户选择的随机数。这里可以看出, 用户的真实口令通过随机数 b_A 被散列函数所保护, 特权内部攻击者无法获得用户的真实口令, 因此, 本文方案可以抵抗内部攻击。而在其他相关协议^[10,11,16]的注册阶段, 用户直接通过与服务器共享明文口令或直接传输共享的密钥 v_a , 使这些方案容易遭受内部攻击。

4.2 离线口令猜测攻击

以 A 为例分析离线口令猜测攻击。根据第 2.2 节的安全性假设, 攻击者可以从公开信道获取与 A 相关的消息 $\{C_{A1}, C_{A3}, C_{A4}, a_A\}$ 和 $\{C_{A5}, C_{A6}, C_{A7}\}$ 。此外, 还假设攻击者获得用户 A 的智能卡并通过能量分析等方法^[22,23]获得了智能卡中的数据 $\{D_{A1}, D_{A2}, D_{A3}, D_{A4}, a_A, s\}$ 。根据假设 3, 攻击者无法同时猜测出用户的身份标识和口令信息, 所以攻击者无法从 D_{A3} 和 D_{A4} 获得 ID_A , PW_A 和 b_A 。当攻击者从 C_{A1} , C_{A3} , D_{A1} , C_{A5} , C_{A6} , C_{A7} 猜测口令时, 攻击者必须获得 S 的主密钥 x 。所以, 本文协议能够抵抗离线口令猜测攻击。

4.3 模仿攻击

若攻击者希望模仿用户 A, 则其必须能够计算有效的会话请求消息 $m_1 = \{C_{A1}, C_{A3}, C_{A4}, a_A\}$ 。但从第 4.2 节的分析可知, 攻击者无法获得用户的身份标识 ID_A 、口令 PW_A 和随机数 b_A , 所以在未知 ID_A , PW_A 和 b_A 的情况下, 攻击者无法计算正确的消息 C_{A1} 和 C_{A4} 。

同理, 在未知 ID_B , PW_B 和 b_B 的情况下, 攻击者无法伪造用户 B 的会话请求消息 $m_2 = \{C_{B1}, C_{B3}, C_{B4}, a_B\}$ 。此外, 为了模仿用户 B 产生响应信息 C_{B9} , 攻击者必须能计算 $sk_{BA} = T_{r_B}(C_{A3})$, 进而攻击者需要从 C_{B3} 获得随机数 r_B , 而这将面临基于混沌映射的离散对数问题。

综上, 攻击者无法有效进行模仿攻击。

4.4 服务器伪装攻击

为了有效模仿服务器 S, 攻击者必须分别为 A 和 B 计算有效的消息 $m_3 = \{C_{A5}, C_{A6}, C_{A7}\}$ 和

$m_4 = \{C_{B5}, C_{B6}, C_{B7}\}$ 。但在未知 S 主密钥 x 的情况下, 攻击者无法计算 $h(x||a_A)$, $h(x||a_A')$, $h(x||a_B)$ 和 $h(x||a_B')$ 。所以, 本文协议能够避免服务器伪装攻击。

4.5 重放攻击

重放攻击是身份认证和口令密钥协商协议中一种常见的安全威胁, 在这种攻击中, 攻击者通过重放用户以前发送过的消息达到身份认证和密钥协商的目的。在本文方案的每次会话中, 用户 A 和 B 分别产生随机数 r_A 和 r_B 以保证会话的新鲜性。当攻击者重放用户 A 和 B 以前发送过的消息 m_1 和 m_2 时, 为了最终生成会话密钥, 攻击者必须计算出随机数 r_A 或 r_B , 而这将面临解基于混沌映射的 Diffie-Hellman 问题。因此, 随机数机制使每次会话的消息与其他会话的消息都不相同, 而一次会话的随机数只对当次会话有效, 有效地避免了重放攻击。

4.6 用户匿名

用户匿名在电子商务、移动计算等领域具有重要应用, 可以保护用户的购物习惯及用户的移动轨迹等信息。在本文方案中, 用户 A 和用户 B 的真实身份标识 ID_A 和 ID_B 没有包含在公开信道上传输的通信消息中。如对用户 A 来说, 数据 $C_{A1} = h(ID_A||a_A) \oplus h(x) \oplus r_A$ 包含用户的身份标识 ID_A 和随机数 r_A 。但由于无法获得 x 和 r_A , 攻击者无法获得用户 A 的真实身份标识 ID_A 。因此, 本文协议能保护用户匿名。

4.7 相互认证

当从 B 收到消息 m_1 和 m_2 时, S 通过检查 $C_{A4} = h(C_{A1}||C_{A2}||C_{A3}||a_A)$ 和 $C_{B4} = h(C_{B1}||C_{B2}||C_{B3}||a_B)$ 来检验 A 是否拥有 $h(x||a_A)$ 以及 B 是否拥有 $h(x||a_B)$ 。如果等式都成立, S 成功地认证了用户 A 和用户 B 。同时, 本文假设服务器是一个可信第三方, 服务器 S 对用户 A 的认证暗含了用户 B 对用户 A 的认证。此外, 当收到来自 S 的响应消息 (m_3 , m_4) 时, 用户 B 通过检查 $C_{B7} = h(C_{B2}||C_{B5}||C_{B6}||a_B')$ 来认证服务器 S 是否有效。当收到用户 B 的响应消息 (m_3 , C_{B3} , C_{B9}) 时, 用户 A 分别通过检查 $C_{A7} = h(C_{A2}||C_{A5}||C_{A6}||a_A')$ 以及 $C_{A9} = C_{B9}$ 是否成立来验证服务器 S 和用户 B 的有效性。因此, 本文协议能实现参与实体之间的相互认证。

4.8 自由选择 and 变更口令

在基于口令的身份认证和密钥协商协议中, 用户自由选择和变更口令增强了用户的友好性和易用性, 是一种理想的功能特性。在文献[10, 12]等协议中, 用户必须与服务器 S 共享长期私钥进行密钥协商; 而在文献[9]的协议中, 由于用户的个人信息经过服务器的密钥加密后存储在智能卡中, 无法实现自由变更口令。本文协议允许用户自由选择方便自己记忆和使用的口令来进行密钥协商, 在降低安全风险的同时增强了用户易用性。此外, 本文协议允许用户在客户端直接变更口令, 而无需远程服务器的协助, 在增强用户易用性的同时减轻了通信代价。

4.9 前向安全

前向安全是指即使系统主密钥和用户的口令或长期私钥被攻击者获得, 攻击者也无法获得用户密钥泄露之前的协商得到的会话密钥。在本文协议中, 假设攻击者获得了 S 的主密钥 x 以及用户 A 和 B 的口令, 攻击者可以从公开信道的通信消息中获得 $Tr_A(s)$ 和 $Tr_B(s)$, 显然攻击者无法计算用户 A 和用户 B 的会话密钥 $sk_{AB} = Tr_A(Tr_B(s)) = Tr_A r_B(s) = Tr_B(Tr_A(s)) = sk_{BA}$, 因为要获得 r_A 或 r_B , 攻击者将面临解基于混沌映射的离散对数问题, 而直接从 $Tr_A(s)$ 和 $Tr_B(s)$ 计算 $Tr_A r_B(s)$ 将面临解基于混沌映射的 Diffie-Hellman 问题。因此, 本文协议能确保会话密钥的前向安全性。

4.10 已知密钥安全

已知密钥安全是指即使攻击者获得当前会话以前的会话密钥, 也不影响当前会话的安全。在本文方案中, 在每次成功的会话后, 用户 A 和用户 B 共享一个会话密钥 $Tr_A r_B(s)$, 这里的 r_A 和 r_B 是此次会话中分别由用户 A 和用户 B 产生的随机数。由于每一次会话用户 A 和用户 B 都产生新的随机数 r_A 和 r_B , 且 r_A 和 r_B 只对当次会话有效, 所以, 获得当前会话之前的会话密钥无助于攻击者获得当前会话的会话密钥。因此, 本文协议能确保已知密钥安全。

5 同相关方案的比较

本节从安全性和效率出发, 给出了本文方案同其他相关基于混沌映射的三方密钥协商协

表2 安全性比较

安全性分析	文献[10]	文献[16]	文献[9]	文献[19]	文献[11]	本文协议
内部攻击	×	×	×	√	×	√
离线口令猜测攻击	√	√	×	√	√	√
模仿攻击	√	√	N/A	√	√	√
服务器伪装攻击	N/A	N/A	N/A	√	N/A	√
重放攻击	√	√	√	√	√	√
用户匿名	√	×	√	√	√	√
相互认证	√	√	√	×	√	√
自由选择口令	×	×	√	√	√	√
自由变更口令	×	×	×	√	×	√
前向安全	√	√	√	√	√	√
已知密钥安全	√	√	√	√	√	√

议^[9-11,16,19]的比较。

安全性比较如表2所示,√表示具有某种安全特性,×表示不具有某种安全特性,N/A表示未提及或不适用。从表2可以看出,其他相关方案或多或少存在一定的安全缺陷,而本文方案则能抵抗大部分已知攻击。

接下来进行效率比较,为计算各种安全算法的时间消耗量,给出如下说明。

1) 本文使用 MIRACL C/C++函数库完成各种安全算法的实验分析,采用配置为 CPU Intel(R)Core 2 T6570, 2.1 GHz, 4 G 内存, 32 bit Windows7 操作系统的笔记本进行实验,实验程序由 Visual C++ 2008 编写。

2) 为获得切比雪夫混沌多项式的实验结果,本文使用文献[26]中的方法,该方法采用从左至右的方法处理 n 阶切比雪夫多项式的每一比特数据, n 为 1 024 bit。等式 $T_n(s) = 2sT_{n-1}(s) - T_{n-2}(s) \bmod p$ 可以由如下矩阵表示。

$$\begin{bmatrix} T_{n-1}(s) \\ T_n(s) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2s \end{bmatrix} \begin{bmatrix} T_{n-2}(s) \\ T_{n-1}(s) \end{bmatrix} = A \begin{bmatrix} T_{n-2}(s) \\ T_{n-1}(s) \end{bmatrix} = A^{n-1} \begin{bmatrix} T_0(s) \\ T_1(s) \end{bmatrix}$$

$$\text{其中, } A = \begin{bmatrix} 0 & 1 \\ -1 & -2s \end{bmatrix}$$

3) 使用 AES 模拟对称加密/解密算法的运算量。

4) 使用 SHA-1 模拟散列函数的运算量。
各种密码算法执行一次运算的时间消耗量如

表3所示。

表3 密码算法时间消耗

符号	说明	时间消耗/ms
T_C	执行一次切比雪夫多项式的时间	140.745
T_S	执行一次加密/解密的时间	0.168
T_H	执行一次散列函数的时间	0.000 8

本文方案同其他相关方案的性能比较如表4所示。表4列出了每个方案4个方面的运算量,即用户A、用户B、服务器S的时间消耗量和总的时间消耗量。在本文协议中,用户A、用户B、服务器S及总的运算量分别为 $2T_C+8T_H$ 、 $2T_C+8T_H$ 、 $8T_H$ 和 $4T_C+24T_H$,而文献[9,10,16,19]中的协议,用户和服务器需要分别执行3次和2次切比雪夫多项式运算。文献[11]的协议中,用户和服务器分别需要执行2次切比雪夫多项式运算。从表4可以明显看出,本文协议执行一次协议总的时间消耗量为 562.999 2 ms,具有最高的执行效率。特别在服务器端,本文方案所需运算量最小,显然这有利于大规模并发网络中的数据处理。此外,同其他相关方案相比,由于本文方案具有更高的安全特性,因此,本文方案更适用于现实应用中。

6 结束语

针对最近提出的基于混沌映射的三方密钥协商协议存在的安全性问题,本文提出了一个有效

表4

性能比较

时间消耗量/ms	文献[10]	文献[16]	文献[9]	文献[19]	文献[11]	本文协议
A	$3T_C+3T_H$ (422.237 4)	$3T_C+2T_S+5T_H$ (422.575)	$3T_C+6T_H$ (422.239 8)	$3T_C+T_S+5T_H$ (422.407)	$2T_C+2T_S+6T_H$ (281.994 8)	$2T_C+8T_H$ (281.496 4)
B	$3T_C+4T_H$ (422.238 2)	$3T_C+2T_S+5T_H$ (422.575)	$3T_C+6T_H$ (422.407)	$3T_C+T_S+5T_H$ (422.407)	$2T_C+3T_S+T_H$ (281.994 8)	$2T_C+8T_H$ (281.496 4)
S	$2T_C+5T_H$ (281.494)	$2T_C+4T_S+4T_H$ (282.165 2)	$2T_C+2T_S+6T_H$ (281.830 8)	$2T_C+2T_S+6T_H$ (281.830 8)	$2T_C+2T_S$ (281.826)	$8T_H$ (0.006 4)
总和	$8T_C+12T_H$ (1 125.969 6)	$8T_C+8T_S+14T_H$ (1 127.315 2)	$8T_C+2T_S+18T_H$ (1 126.644 8)	$8T_C+4T_S+16T_H$ (1 126.644 8)	$6T_C+8T_S+2T_H$ (845.815 6)	$4T_C+24T_H$ (562.999 2)

的基于混沌映射的三方口令密钥协商协议。同其他相关协议相比,本文协议具有用户匿名、用户自由选择和变更口令等用户友好特性,同时本文方案弥补了相关协议的安全性缺陷,具有更高的安全性。此外,同其他协议相比,本文协议具有更高的计算效率。因此,本文协议更加适用于大规模网络环境下的安全通信。

参考文献:

- [1] KATZ J, OSTROVSKY R, YUNG M. Efficient password-authenticated key exchange using human-memorable passwords[J]. Lecture Notes in Computer Science, 2001(4):475-494.
- [2] RAIMONDO M D, GENNARO R. Provably secure threshold password-authenticated key exchange[J]. Journal of Computer and System Sciences, 2006, 72(9): 507-523.
- [3] GUO C, CHANG C C. Chaotic maps-based password-authenticated key agreement using smart cards[J]. Communications in Nonlinear Science and Numerical Simulation, 2013, 18(6): 1433-1440.
- [4] LEE C C, CHEN C L, WU C Y, et al. An extended chaotic maps-based key agreement protocol with user anonymity[J]. Nonlinear Dynamics, 2012, 69(1/2): 79-87.
- [5] LI C T, LEE C C, WENG C Y. An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments[J]. Nonlinear Dynamics, 2013, 74(4):1133-1143.
- [6] LI X, ZHANG Y. A simple and robust anonymous two-factor authenticated key exchange protocol[J]. Security and Communication Networks, 2013, 6(6): 711-722.
- [7] TAN Z. A chaotic maps-based authenticated key agreement protocol with strong anonymity[J]. Nonlinear Dynamics, 2013, 72(1/2):311-320.
- [8] WU F, XU L L. Security analysis and improvement of a privacy authentication scheme for telecare medical information systems[J]. Journal of Medical Systems, 2012, 37(4): 1-9.
- [9] LAI H, XIAO J, LI L, et al. Applying semigroup property of enhanced chebyshev polynomials to anonymous authentication protocol[J]. Mathematical Problems in Engineering, 2012(6): 589-597.
- [10] LEE C C, LI C T, HSU C W. A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps[J]. Nonlinear Dynamics, 2013, 73(1/2):125-132.
- [11] LIN H Y. Chaotic map-based three-party authenticated key agreement[J]. Security and Communication Networks, 2014, 7(12): 2469-2474.
- [12] LV C, MA M, LI H, et al. An novel three-party authenticated key exchange protocol using one-time key[J]. Journal of Network and Computer Applications, 2013, 36(1): 498-503.
- [13] TSAI H C, CHANG C C. Provably secure three party encrypted key exchange scheme with explicit authentication[J]. Information Sciences, 2013, 238(7):242-249.
- [14] WANG X, ZHAO J. An improved key agreement protocol based on chaos[J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(12): 4052-4057.
- [15] WU S, CHEN K, PU Q, et al. Cryptanalysis and enhancements of efficient three-party password-based key exchange scheme[J]. International Journal of Communication Systems, 2013, 26(5): 674-686.
- [16] XIE Q, ZHAO J, YU X. Chaotic maps-based three-party password-authenticated key agreement scheme[J]. Nonlinear Dynamics, 2013, 74(4): 1021-1027.
- [17] YANG J H, CAO T J. Provably secure three-party password authenticated key exchange protocol in the standard model[J]. Journal of Systems and Software, 2012, 85(2): 340-350.
- [18] YOON E J, JEON I S. An efficient and secure diffie-hellman key agreement protocol based on chebyshev chaotic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(6): 2383-2389.
- [19] ZHAO F, GONG P, LI S, et al. Cryptanalysis and improvement of a three-party key agreement protocol using enhanced chebyshev polynomials[J]. Nonlinear Dynamics, 2013, 74(1/2): 419-427.
- [20] ZHAO J J, GU D W. Provably secure three-party password based authenticated key exchange protocol[J]. Information Sciences, 2012, 184(1): 310-323.
- [21] ZHANG L. Cryptanalysis of the public key encryption based on multiple chaotic systems[J]. Chaos Solitons & Fractals, 2008, 37(3): 669-674.

- [22] MANGARD S, OSWALD E, STANDAERT F X. One for all-all for one: unifying standard differential power analysis attacks[J]. IET Information Security, 2011, 5(2): 100-110.
- [23] MESSERGES T S, DABBISH E A, SLOAN RH. Examining smart-card security under the threat of power analysis attacks[J]. IEEE Transactions on Computers, 2002, 51(5): 541-552.
- [24] KUMARI S, KHAN M K. Cryptanalysis and improvement of ‘a robust smart-card-based remote user password authentication scheme’[J]. International Journal of Communication Systems, 2014, 27(12): 3939-3955.
- [25] WANG D, MA C G, WANG P, et al. Robust smart card based password authentication scheme against smart card security breach[R]. Cryptology ePrint Archive, 2012.
- [26] KOCAREV L, LIAN S G. Chaos-based cryptography: theory, algorithms and applications[M]. Berlin:Springer, 2011.



吴凡（1981-），男，山东济宁人，
厦门理工学院讲师，主要研究方向为信
息安全和网络协议。



廖俊国（1972-），男，湖南衡阳人，
博士，湖南科技大学教授、硕士生导师，
主要研究方向为网络与信息安全。

作者简介：



李雄（1984-），男，土家族，湖南
张家界人，博士，湖南科技大学副教授、
硕士生导师，主要研究方向为信息安全
和密码学。



刘玉珍（1979-），男，山东单县人，
博士，湖南科技大学讲师，主要研究方
向为密码学、智能计算。