基于智能卡的扩展混沌映射异步认证密钥协商协议

王松伟 陈建华

(武汉大学数学与统计学院 武汉 430072)

摘 要 身份认证是确保信息安全的重要手段,混沌映射身份认证协议因其高效性而成为近期研究的热点。2015年,Zhu提出了一个改进的混沌映射协议,声称其可以抵抗冒充攻击、字典攻击,并且提供用户匿名性;然而,Tong等指出Zhu的协议存在离线字典攻击、冒充攻击等问题且无法确保用户匿名性,并提出了一个新的改进协议(简称TC协议)。针对Zhu和TC协议方案,文中指出了其不能确保前向安全性以及容易遭受拒绝服务攻击等安全性缺陷,并提出了一个新的基于智能卡的混沌映射协议方案。安全性分析及同其他相关方案的比较结果表明了所提协议的高安全性和实用性。

关键词 混沌映射,异步,动态身份,认证,密钥协商

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.01.027

Chaotic Mapping Asynchronous Authentication Key Agreement Scheme with Smart-cards

WANG Song-wei CHEN Jian-hua

(School of Mathematics and Statics, Wuhan University, Wuhan 430072, China)

Abstract Identity authentication is an important means to ensure information security. Chaos mapping indentity authentication scheme has become a hot research topic recently because of its high efficieny. In 2015, Zhu proposed an improved chaotic mapping protocol, and claimed that it can oppose impersonation attack and dictionary attack, and it also can provide user anonymity. However, Tong et al. pointed out Zhu's protocol has the problems of offline dictionary attack, impersonation attack and can't guarantee user's anonymity, and proposed a new improvement protocol(short for TC scheme). Aiming at Zhu and TC protocol schemes, this paper pointed out their security defects, for example, the forward security can't be guaranteed and they are easy suffering from denial of service attack. Meanwhile, this paper proposed a new protocol scheme using smart card. The security analysis and the comparison results with other related protocols indicate the high security and practicability of the porposed protocol.

Keywords Chaotic mapping, Asynchronous, Dynamic identity, Authentication, Key agreement

随着互联网的飞速发展,网络已经渗透到我们生活的各个方面,由于互联网是开放的,因此极易引起用户信息泄漏。密码协议在很多互联网领域得到了广泛应用,为保障信息安全发挥了巨大作用[1]。身份认证协议是一类重要的密码协议,1981年Lamport[2]首次提出基于口令的认证协议,1993年Chang等[3]首次提出基于智能卡与口令的身份认证协议。由于混沌映射不需要模指数运算和椭圆曲线点乘运算,对于计算能力和存储能力非常有限的智能卡等设备来说,此类协议相比传统公钥算法有绝对优势[4-6],因此,近年来国内外学者提出了一系列认证协议[7-15]。Xiao等[7]于2005年提出了一个身份认证协议,接着Bergamo等[8]就指出Xiao提出的协议存在安全问题,2007年Xiao等[9]又提出了一个新的认证协议。2010年,Guo等[10]发现Xiao等提出的协议容易遭受冒充服务器攻击。2012年,Xue等[11]提出了一个改进协议,其仍然是基于混沌映射的。但2013年,Tan[12]指出Xue等的改进协议存在中间人攻击且不能保护用户的匿名性。2014年,Lin[16]提出了一个新的认证协议。2015年,Zhu[17]指出Lin的协议容易遭受字典攻击和冒充攻击等,并对协议进行了改进。最近,童彤等发现Zhu的协议不能提供用户匿名性,存在离线字典攻击和冒充攻击等问题[18]。

本文指出了TC协议和Zhu提出的协议均不能提供前向安全性,容易遭受拒绝服务攻击且存在时钟同步问题,并提出了一个新的身份认证协议。

本文的攻击者模型仍然采用经典的Dolev-Yao模型[19],攻击者可以截获公开信道上的信息,对信息进行修改和重放,并且能够采用能量分析方法[20-22]来获得设备中的信息。

1 预备知识

1.1 切比雪夫多项式

切比雪夫多项式是与棣莫弗定理相关的正交多项式序

到稿日期:2017-11-26 返修日期:2018-01-10

王松伟(1989—),男,硕士生,主要研究方向为密码与信息安全,E-mail:wangsw_ecc@163.com;**陈建华**(1963—),男,博士,教授,主要研究方向为数论与密码、椭圆曲线、信息安全,E-mail:chenjh_ecc@163.com(通信作者)。

列，这里是指其第一类多项式[23]。

1.1.1 切比雪夫多项式的定义及性质

定义 1(切比雪夫多项式) 设 n 为正整数，$x\in[-1,1]$，n 阶切比雪夫多项式 $T_n(x)$ 定义为：

$$T_n(x)=\cos(n\times\arccos(x))$$

其等价的递归定义为：

$$T_n(x)=2xT_{n-1}(x)-T_{n-2}(x),n\geqslant 2,T_0(x)=1,T_1(x)=x$$

性质 1(半群性质)

$T_r(T_s(x))=T_s(T_r(x)),r,s\in N,x\in[-1,1]$

证明：

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

性质 2(混沌性质) 当 $n>1$ 时，n 阶切比雪夫多项式映射 $T_n(x):[-1,1]\to[-1,1]$，是混沌映射。

证明请参见文献[24]。

1.1.2 扩展切比雪夫多项式

2008 年，Zhang[25]证明了切比雪夫多项式在区间$(-\infty,+\infty)$上仍然具有半群特性。

定义 2(扩展切比雪夫多项式) n 为正整数，$x\in(-\infty,+\infty)$，n 阶扩展切比雪夫多项式如下：

$$T_n(x)=\cos(n\times\arccos(x))(\mathrm{mod}\ p)$$

其等价的递归定义为：

$$T_n(x)=2xT_{n-1}(x)-T_{n-2}(x)(\mathrm{mod}\ p)$$

其中，$n\geqslant 2,T_0(x)=1,T_1(x)=x,p$ 是一个大素数。显然，半群特性同样适用于扩展切比雪夫多项式，即：

$$T_r(T_s(x))\equiv T_{rs}(x)\equiv T_{sr}(x)\equiv T_s(T_r(x))(\mathrm{mod}\ p)$$

1.1.3 扩展切比雪夫多项式的相关数学难题

多项式时间内求解以下问题是困难的[23]：

定义 3(离散对数问题，CMDLP) 给定 x,p，以及 $y=T_r(x)$，找到一个正整数 r，使得 $T_r(x)\equiv y$。

定义 4(计算 Diffie-Hellman 问题，CMCDHP) 给定 p,x，以及 $T_r(x),T_s(x)$，找到一个正整数 y，使得 $y\equiv T_{rs}(x)(\mathrm{mod}\ p)$。

定义 5(判断 Diffie-Hellman 问题，CMCDHP) 给定 x,p，以及 $T_r(x)(\mathrm{mod}\ p),T_s(x)(\mathrm{mod}\ p),T_z(x)(\mathrm{mod}\ p)$，其中 $r,s,z\geqslant 2,x\in(-\infty,+\infty)$，判断 $T_{rs}(x)\equiv T_z(x)(\mathrm{mod}\ p)$ 是否成立在计算上是困难的。

1.1.4 Bergamo 算法[8]

算法 1 Bergamo 算法

给定 $x\in[-1,1],T_r(x),T_s(x)$，计算 $T_{rs}(x)$。

(1)从集合$\left\{\frac{\pm\arccos(T_r(x))+2k\pi}{\arccos(x)}\mid k\in Z\right\}$中选取一个正整数 $r'=\frac{\arccos(\mathrm{Tr}(x))+2k'\pi}{\arccos(x)},k'\in z$；

(2)计算：

$$\begin{aligned}T_{r'}(x)&=\cos(r'\times\arccos(x))\\&=\cos(\arccos(T_r(x))+2k'\pi)\\&=\cos(\arccos(T_r(x)))\\&=T_r(x)\end{aligned}$$

然后用 r' 计算 $T_{r's}(x)$：

$$T_{r's}(x)=T_{r'}(T_s(x))=T_r(T_s(x))=T_{rs}(x)$$

1.2 时钟同步

在分布式系统中，时钟同步是最重要的技术之一，在身份认证协议中可以采用时戳抵抗重放攻击[26-27]，但其要求较高且成本高。时钟同步的实现可分为软件时钟同步、硬件时钟同步和混合时钟同步[28-29]。

1)硬件时钟同步是指利用一定的硬件设备(如 GPS 接收机、UTC 接收机、专用的时钟信号线路等)进行的局部时钟之间的同步，操作对象往往是计算机的硬件时钟，由外部提供标准时钟同步信号，并以此为标准时间同步整个分布系统；2)软件时钟同步是利用时钟同步算法进行的结点局部时钟之间的同步；3)混合时钟同步是把硬件时钟同步和软件时钟同步的优缺点结合起来。

实现时钟同步需要专用的软件或硬件，并且时戳方法的实现较为困难，其原因是：1)由于网络存在错误，协议必须考虑容错问题；2)由于系统故障和不可预测的网络延迟等问题，很难保持时钟精确同步。

1.3 哈希函数

哈希函数又名单向散列函数或杂凑函数，是指将任意长度信息 m 映射为固定长度信息 $h(m)$ 的一类函数。常见的哈希函数有 MD5，SHA1，SHA256 等。哈希函数有以下 3 条重要性质：

(1)抗原像攻击(单向性)：给定一个哈希值 y，很难找到一个原像值 x，使得 $h(x)=y$ 成立。

(2)抗弱碰撞性：给定一个原像值 x_1，很难找到另一个原像值 x_2，使得 $h(x_1)=h(x_2)$ 成立。

(3)抗强碰撞性：很难找到两个不同的原像值 x_1,x_2，使得 $h(x_1)=h(x_2)$ 成立。

2 TC 协议方案

本节介绍 TC 方案的注册阶段、登录认证阶段，详细内容请参考文献[18]。

注册阶段：

(1)U_a 选取 ID_a、PW_a、随机数 t，计算 $W_a=h(PW_a\parallel t)$，之后通过安全信道给服务器 B 发送注册信息$\{ID_a,W_a\}$。

(2)B 收到$\{ID_a,W_a\}$之后，计算 $h(ID_a)$并在后台数据库中查找该数据，若存在，则表明该 ID 已被注册，通知用户更换 ID 重新开始步骤 1)，否则，计算 $H_a=h(s\parallel ID_a)$，$n_a=h(W_a\parallel ID_a)\oplus H_a$，$K_s=T_s(\sin(H_a))$，随后通过安全通道给 U_a 发送消息$\{n_a,K_s\}$，同时向后台数据库中添加 $h(ID_a)$。

(3)U_a 收到消息后，计算 $N_a=h(ID_a\parallel PW_a)\oplus n_a\oplus h(W_a\parallel ID_a)$，$G_a=h(ID_a\parallel PW_a\parallel N_a)$，并将数据$\{N_a,G_a,K_s\}$存储到移动设备 MD 中。

登录认证阶段：

(4)U_a 向 MD 输入 ID_a 和 PW_a，MD 首先验证 $G_a=?h$

($ID_a \| PW_a \| N_a$)，若成立，则选两个随机整数 k，R，计算 $H_a = N_a \oplus h(ID_a \| PW_a)$，$K_A = T_k(\sin(H_a))$ $K_{AS} = T_k(K_s)$，$H_A = h(H_a \| K_A \| ID_a \| ID_b \| R)$，$C = E_{K_{AS}} h(H_A \| ID_a \| ID_b \| R \| TS)$，其中 TS 为当前时戳。之后 MD 将登录请求信息$\{C, K_A\}$发给 B。

(5)服务器 B 收到用户的消息之后，用私钥 s 计算 $K_{SA} = T_s(K_A)$，然后 B 使用 K_{SA} 解密 C 得到 $H_A \| ID_a \| ID_b \| R \| TS$，检查 TS 的新鲜性，若 TS 过期了，则 B 终止这次会话；否则 B 继续计算 $H_a = h(s \| ID_a)$，$H_A^* = h(H_a \| K_A \| ID_a \| ID_b \| R)$。最后，$B$ 验证等式 $H_A^* = ?\ H_A$，若成立，B 选取随机数 r 并且计算 $V_1 = h(h(R \| r))$，$V_2 = H_a \oplus h(R \| r)$，$SK = h(ID_a \| ID_b \| R \| h(R \| r))$，然后发送消息$\{V_1, V_2\}$给 U_a；若不成立，B 终止会话。

(6)接收到消息$\{V_1, V_2\}$后，MD 验证等式 $V_1 = h(V_2 \oplus H_a)$是否成立，若成立则计算 $h(R \| r) = V_2 \oplus H_a$，$SK = h(ID_a \| ID_b \| R \| h(R \| r))$，并把 SK 作为之后与 B 之间的会话密钥，否则，MD 终止本次会话。

3　TC 协议的安全性分析

3.1　不具有前向安全性

前向安全性指系统的长期密钥泄漏也不会对之前由该密钥建立的会话密钥构成威胁[18]。Zhu 的协议和 TC 协议均不能确保前向安全性：

在 TC 协议的第(4)步和第(5)步，U_a 和 B 相互认证并计算会话密钥 $SK = h(ID_a \| ID_b \| R \| h(R \| r))$。假设攻击者获得了系统密钥 s，且攻击者 M 从公开信道截获消息$\{C, K_A\}$和$\{V_1, V_2\}$，M 首先用私钥 s 计算 $K_{SA} = T_s(K_A)$，然后使用 K_{SA} 解密 C 得到 $H_A \| ID_b \| R \| TS$，即可获 ID_a，ID_b，R，继续计算 $H_a = h(s \| ID_a)$，$h(R \| r) = H_a \oplus V_2$，就可以成功计算出 U_a 和 B 的会话密钥 $SK = h(ID_a \| ID_b \| R \| h(R \| r))$。

因此，TC 协议方案无法实现前向安全性。

Zhu 在文献[17]中表示可以提供前向安全性，但采用上述分析方法很容易得出 Zhu 的方案无法实现会话密钥的前向安全性的结论。

3.2　对于拒绝服务攻击是脆弱的

目前时戳主要通过时钟窗来实现，一方面时间窗应尽量大以包容网络传输延迟，另一方面时钟窗应足够小以尽可能避免重放攻击。由于网络的传输延迟是不可预测的，因此时间窗的大小常常很难掌握。为抵抗重放攻击，Zhu 的协议和 TC 协议均引入了时间戳机制，但却面临时钟同步问题，若出现系统时钟故障、网络延迟等，则会使得用户很容易遭受拒绝服务攻击。

4　提出的新协议

本文提出了一个新的认证协议，该协议包括注册、登录认证、口令修改、智能卡注销及系统主密钥更新 5 个阶段。相关符号的含义如表 1 所列，图 1 给出了注册和登录认证过程。

表 1　协议描述用到的符号说明

Table 1　Symbol description of protocol

符号	含义
U_a，SC	用户，用户的智能卡
S	服务器
M	攻击者
ID_a，CID_i	用户身份，用户动态身份
ID_s	服务器身份
PW_a	用户口令
s	服务器高熵私钥
TS	时戳
SK	共享的会话密钥
k，r	随机整数
R，t，b，b'	随机数
$\oplus$，$\|$	异或运算，级联运算
$h(\cdot)$	安全哈希函数

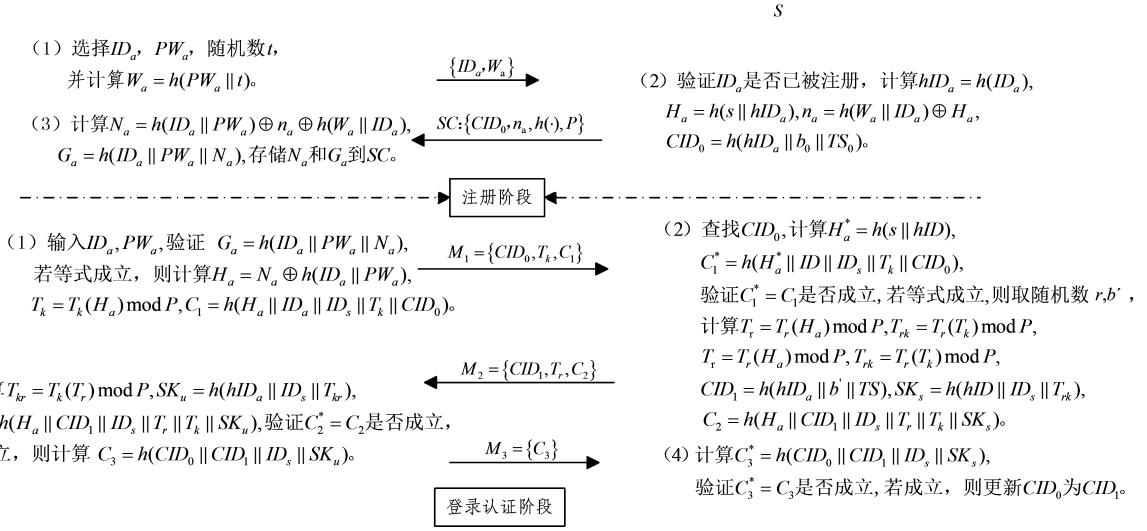

图 1　新协议方案的过程

Fig. 1　Process of new protocol scheme

4.1　注册阶段

(1)U_a 选取自己的 ID_a、口令 PW_a 以及高熵随机数 t 计算 $W_a = h(PW_a \| t)$，并通过安全信道给服务器发送消息$\{ID_a, W_a\}$。

(2)收到$\{ID_a, W_a\}$后,S 计算 $hID_a = h(ID_a)$,然后在用户列表中查找 hID_a,若存在则表明该 ID 已被注册,拒绝用户注册请求,通知用户更换 ID 重新注册;否则,选取随机数 b,计算 $H_a = h(s \| hID_a)$,$n_a = h(W_a \| ID_a) \oplus H_a$,给用户分配动态身份 $CID_0 = h(hID_a \| b \| TS)$,$TS$ 是当前时戳,并将 $\{CID_0, n_a, h(\cdot), P\}$存入 SC,P 为服务器选取的大素数,向用户列表添加(hID_a, CID_0),并将智能卡通过安全信道分发给用户。

(3)用户 U_a 收到智能卡后,输入 ID_a,PW_a,t,并计算 $N_a = h(ID_a \| PW_a) \oplus n_a \oplus h(W_a \| ID_a)$,$G_a = h(ID_a \| PW_a \| N_a)$,用 N_a 替换 SC 中的 n_a,并将 G_a 存储到智能卡 SC。

4.2 登录认证阶段

(1)用户 U_a 插入智能卡并输入 ID_a 和 PW_a,验证 $G_a = h(ID_a \| PW_a \| N_a)$是否成立,若超过 10 次不成立则当天锁定智能卡;若成立则选取随机整数 k,计算 $H_a = N_a \oplus h(ID_a \| PW_a)$,$T_k = T_k(H_a) \bmod P$,$C_1 = h(H_a \| hID_a \| ID_s \| T_k \| CID_0)$,将登录请求信息 $M_1 = \{CID_0, T_k, C_1\}$发送给 S。

(2)S 收到用户的登录请求信息 M_1 之后,首先在用户数据库中查找 CID_0,若查找不到,拒绝用户登录请求,否则取出 CID_0 对应的 hID,计算 $H_a^* = h(s \| hID)$,$C_1^* = h(H_a^* \| hID_a \| ID_s \| T_k \| CID_0)$。然后验证 $C_1^* = C_1$ 是否成立,若成立,S 生成随机数 r, b',计算 $T_r = T_r(H_a) \bmod P$,$T_{rk} = T_r(T_k) \bmod P$,$CID_1 = h(hID_a \| b' \| TS)$,$SK_s = h(hID \| ID_s \| T_{rk})$,$C_2 = h(H_a \| CID_1 \| ID_s \| T_r \| T_k \| SK_s)$,然后将消息 $M_2 = \{CID_1, T_r, C_2\}$发送给用户 U_a。

(3)U_a 收到 M_2 后,计算 $T_{kr} = T_k(T_r) \bmod P$,$SK_u = h(hID_a \| ID_s \| T_{kr})$,$C_2^* = h(H_a \| CID_1 \| ID_s \| T_r \| T_k \| SK_u)$。然后验证 $C_2^* = C_2$ 是否成立,若不成立,则停止协议;否则继续计算 $C_3 = h(CID_0 \| CID_1 \| ID_s \| SK_u)$。然后将消息 $M_3 = \{C_3\}$发给服务器。将 $SK = SK_u$ 作为双方的会话密钥,同时智能卡保存 CID_1 直到下一次认证成功后获得 CID_2,再用 CID_2 更新 CID_0。

(4)收到 M_3 后服务器计算 $C_3^* = h(CID_0 \| CID_1 \| ID_s \| SK_s)$,并验证 $C_3^* = C_3$ 是否成立,若成立,则服务器认证用户成功,将 $SK = SK_s$ 作为双方的会话密钥使用,并更新 CID_0 为 CID_1,否则停止协议。

4.3 口令修改阶段

用户 U_a 若要修改自己的口令,需插入智能卡并输入 ID_a 和 PW_a,验证 $G_a = h(ID_a \| PW_a \| N_a)$是否成立。若超过 10 次不成立则当天锁定智能卡;若成立则用户输入新口令 PW_a',并检验两次输入是否一致,若一致,则计算 $N'_a = N_a \oplus h(ID_a \| PW_a)$,$G'_a = h(ID_a \| PW_a \| N'_a)$,并用 N'_a,G'_a 分别替换 N_a,G_a,口令修改完成。

4.4 注销智能卡阶段

当用户 U_a 的智能卡丢失后,服务器在验证了用户 U_a 的凭据之后,计算 $hID_a = h(ID_a)$,在用户注册列表中找到 hID_a,然后将(hID_a, CID_a)从用户列表中删除。

4.5 系统主密钥更新阶段

用户插入智能卡并输入 ID_a 和 PW_a,执行登录认证阶段协议,完成与服务器的相互认证,并协商会话密钥 SK,在公共信道上建立一条安全私信道,用户选择随机数 R,计算 $N_a' = N_a \oplus R$,服务器通过私信道接收用户信息 CID_a 和 N_a',计算 $N_a^* = N_a' \oplus h(s \| hID_a) \oplus h(s' \| hID_a)$,通过私信道将 N_a^* 发给用户 U_a。用户收到 N_a^* 之后计算 $N_a^{*\prime} = N_a^* \oplus R$,并用 $N_a^{*\prime}$替换 N_a,更新完成。

5 安全性分析

5.1 身份认证协议的安全目标及理想属性

理想的身份认证密钥协商协议应达到表 2 中的理想属性[30]和表 3 中的安全目标。

表 2 身份认证密钥协商协议的理想属性

Table 2 Ideal attributes of identity authentication key agreement protocol

功能特性	描述
U_1	服务器端无校验值
U_2	口令本地自由更新
U_3	相互认证
U_4	前向安全性
U_5	口令输入错误及时检测
U_6	智能卡撤销
U_7	密钥协商
U_8	可修复性
U_9	用户匿名
U_{10}	无时钟同步

表 3 身份认证密钥协商协议的安全目标

Table 3 Security objectives of identity authentication key agreement protocol

安全目标	描述
S_1	抗口令猜测攻击
S_2	抗被盗校验值攻击
S_3	抗冒充攻击
S_4	抗智能卡丢失攻击
S_5	抗重放攻击
S_6	抗平行会话攻击
S_7	抗拒绝服务器攻击
S_8	抗内部攻击
S_9	抗反射攻击
S_{10}	抗未知密钥共享攻击
S_{11}	抗已知会话密钥攻击
S_{12}	抗密钥泄露攻击

5.2 安全性分析假设[31]

安全性分析所需的 3 个安全假设如下。

假设 1 熵值 $S(k)$较小的低强度密码(PW)在多项式时间内能被破解。

假设 2 熵值 $S(k)$较大的高强度密码(服务器的密钥 s)在多项式时间内不能被破解。

假设 3 哈希函数 $y = h(x)$具有已知 x 计算 y 容易,而已知 y 计算 x 几乎不可能的特征。

5.3 新协议的安全性分析

在以上安全假设下,分析本文方案的安全性。新协议中用户的身份是动态变化的,因此这里假设攻击者已经锁定了目标用户,并能在公开信道上截获目标用户与服务器的通信信息,否则由于每次登录身份不同,攻击者的攻击都是无效的。

(1)抵抗 Bergamo 攻击[8]:攻击者必须得到 x,$T_r(x)$和 $T_k(x)$才能发动有效攻击。本协议使用扩展的切比雪夫多项

式，使用了模运算，而且 $x\in(-\infty,+\infty)$ 可以有效避免三角函数的周期性，因此新协议能抵抗 Bergamo 攻击。

(2)抵抗拒绝服务攻击：本协议没有引入时间戳机制，不会因为网络延迟等原因遭受拒绝服务攻击。一般地，用户使用动态身份 CID_i 登录，并收到下一次动态身份 CID_{i+1}，而且每次只有用户登录成功时，双方才更新身份 CID_{i+1}。即使实际上还未更新成功，用户仍可以再次选择使用 CID_i 登录，因此用户一定可以登录到服务器。

(3)用户匿名性：用户 U_a 的身份信息 ID_a 隐藏在 H_a，CID_a，C_1，C_2 这些消息内。首先，攻击者即使获得用户注册列表(hID,CID)，也不能从 hID,CID 中恢复用户的真实身份；其次，用户 U_a 的身份信息在公共信道传送过程中均采用了哈希函数加密保护，即使攻击者在公共信道截获了这些消息，由于哈希函数的单向性，攻击者无法通过 C_1 和 C_2 得到关于 U_a 的任何信息；另外，在公开信道上传送的消息都是与 r，k 和 b'有关的，r，k 和 b'都是随机的，攻击者无法分辨出用户发起的会话；最后，即使攻击者获取了用户智能卡等设备，采用能量分析方法也无法获取 U_a 的身份信息。因此，本协议确保了用户的匿名性。

(4)抗口令猜测攻击：本协议并没有在线对用户口令进行验证，而是验证用户与服务器共享的秘密值，因此本协议不存在在线猜测攻击。攻击者只有采取离线猜测攻击，由于协议能够保护用户匿名性，因此攻击者无法获得用户的 ID_a，即使获得用户的智能卡，并采用能量分析攻击获取了数据$\{CID_0,N_a,G_a,h(\cdot),P\}$(其中 $N_a=h(ID_a\|PW_a)\oplus H_a$，$G_a=h(ID_a\|PW_a\|N_a)$)，其也不可能利用这些数据猜测出口令 PW_a。另一方面，即便攻击者截获了消息 $M_1=\{CID_0,T_k,C_1\}$，$M_2=\{CID_1,T_r,C_2\}$，也无法猜测出口令 PW_a。因此，协议可抵抗口令猜测攻击。

(5)抗内部攻击：在实际应用中，用户可能会使用同一个口令访问很多服务器，这样用户的口令就会泄漏给某个服务器的内部人员，从而存在口令被内部人员利用的风险。在本协议中，用户在注册阶段不需要直接发送口令值，而是发送 $W_a=h(PW_a\|t)$，即用随机数 t 将口令 PW_a 隐藏，对于任何内部人员，W_a 只是一个随机数。因此，本协议可以抵抗内部攻击。

(6)提供相互认证：当服务器 S 收到用户 U_a 的登录请求消息 $M_1=\{CID_0,T_k,C_1\}$ 时，通过验证 $C_1^*=C_1$ 是否成立来检验其是否拥有 $H_a=h(s\|hID_a)$，若等式成立，则 S 成功地认证用户 U_a。当用户 U_a 收到来自 S 的响应消息 $M_2=\{CID_1,T_r,C_2\}$ 时，用户 U_a 通过等式 $C_2^*=C_2$ 是否成立来检验其是否拥有系统私钥，如果等式成立，则 U_a 成功地认证 S。之后用户发送 M_3 给服务器，S 通过验证等式 $C_3^*=C_3$ 是否成立来检验 U_a 是否能够计算出正确的会话密钥 $SK_u=h(hID_a\|ID_s\|T_{kr})$，若等式成立，则表明用户能够计算出会话密钥，协议认证完成，参与认证双方能够确认和对方建立了一个只有双方才知道的会话密钥，因此本协议可以提供相互认证。

(7)抗智能卡丢失攻击：假设攻击者获得了用户的智能卡，并且采用能量分析得到了智能卡中的信息$\{CID_0,N_a,G_a,h(\cdot),P\}$，由以上分析可知，攻击者并不能获得用户的身份信息，也无法验证用户的口令信息。并且当用户发现自己的智能卡丢失以后，用户可以向服务器申请注销，即使攻击者获得了智能卡的身份和口令，也无法登录服务器。因此，协议可抵抗智能卡丢失攻击。

(8)抗重放攻击和冒充攻击：本协议中用户每次均采用动态身份登录，如果攻击者直接重放以前经过双方认证的消息很容易被识破，所以攻击者只有冒充合法用户或服务器尝试构造消息进行攻击。

1)假设攻击者 M 冒充用户，尝试构造 $M_1=\{CID_0,T_k,C_1\}$ 和 $M_3=\{C_3\}$。由于服务器已经更新用户的动态身份 CID_0 为 CID_1，服务器在数据库中查找不到 CID_0 而拒绝用户的请求。因此，这里假设服务器由于其他原因实际还未更新成功。

①重放 CID_0，T_k，C_1，C_3。假设攻击者从公开信道截获了用户 U_a 发送的消息，然后重放消息 CID_0，T_k，C_1 和 C_3，服务器认证收到之后，选择新的随机数 r，并计算新的会话密钥 SK_s，并为用户分配新的动态身份，因此，当攻击者重放 $C_3=h(CID_0\|CID_1\|ID_s\|SK_u)$时无法获得服务器的认证，所以这种攻击无法成功。

②重放 CID_0，T_k，C_1，构造 C_3。若要构造的 $C_3=h(CID_0\|CID_1\|ID_s\|SK_u)$获得了服务器的认证，除非攻击者可以正确猜测出会话密钥 $SK_u=h(hID_a\|ID_s\|T_{kr})$，但是攻击者只有 T_r，T_k，并且无法获得 H_a，即使获得了 H_a，在不知道随机数 k 或 r 的情况下，攻击者不可能计算出 T_{kr}，因为由 T_k，T_r 计算 T_{kr} 面临扩展切比雪夫多项式的 CDHP 难题，若攻击者先由 T_k，T_r 计算出 k 或 r，则将面临扩展切比雪夫多项式的 CDLP 难题。此外，因为哈希函数的保护，攻击者无法从接收到的消息 C_2 中获得 SK_s。因此，这种攻击无法成功。

③重放 CID_0，构造 T_k，C_1，C_3。但是构造 $T_k=T_k(H_a)\bmod P$，$C_1=h(H_a\|ID_a\|ID_s\|T_k\|CID_0)$，需要 H_a，因为 $H_a=N_a\oplus h(ID_a\|PW_a)$，$H_a=h(s\|ID_a)$，则必须获得用户的 ID_a，PW 或服务器密钥 s，而攻击者不可能获得这些信息，所以，攻击无法成功。

2)假设攻击者 M 冒充服务器，尝试构造 $M_2=\{CID_1,T_r,C_2\}$。

①重放 CID_1，T_r，C_2。假设攻击者截获了服务器发给 U_a 的消息，然后重放消息 CID_1，T_r，C_2。由于 $C_2=h(H_a\|CID_1\|ID_s\|SK_s)$，$SK_s=h(hID\|ID_s\|T_{rk})$，$T_{rk}=T_r(T_k)\bmod P$，则 C_2 含有用户登录时选择的随机数 k 的信息 T_k，用户每次登录会选取不同的随机数，则攻击者重放消息 CID_1 和 T_r，C_2 很容易被识破，因此这种攻击无法成功。

②重放 CID_1，构造 T_r，C_2。但是构造 $T_r=T_r(H_a)\bmod P$，$C_2=h(H_a\|CID_1\|ID_s\|SK_s)$，都需要 H_a，因为 $H_a=N_a\oplus h(ID_a\|PW_a)$，$H_a=h(s\|ID_a)$，则必须获得用户的 ID_a，PW 或服务器密钥 s，而攻击者不可能获得这些信息，所以，这种攻击无法成功。

(9)中间人攻击：由以上分析可知，攻击者无法计算相关

消息，简单的消息重放很容易被识破，且攻击者更没有能力同时向用户和服务器发送消息而不被发现，更不可能共享会话密钥，因此，本协议可以抵抗中间人攻击。

(10)完美前向安全性：本协议双方协商的会话密钥为 $SK=h(hID_a \| ID_s \| T_{kr})$，假设攻击者获得系统密钥和用户的口令，通过公开信道截获到会话密钥的两个元素 $T_r=T_r(H_a) \bmod P$，$T_k=T_k(H_a) \bmod P$，然而攻击者在不知道随机数 k 或 r 的情况下，不可能计算出会话密钥，因为由 T_k，T_r 计算 T_{kr} 将面临扩展切比雪夫多项式的 CDHP 难题，若攻击者先由 T_k，T_r 计算出 k 或 r 则将面临扩展切比雪夫多项式的 CMDLP 难题，所以本协议能确保会话密钥具有完美前向安全性。

(11)已知会话密钥安全性：已知会话密钥安全性是指通信双方产生的会话密钥之间应该相互独立。本协议会话密钥 $SK=h(hID_a \| ID_s \| T_{kr})$，其中 $T_{kr} \equiv T_k(T_r) \equiv T_r(T_k) \bmod p$，$k$ 和 r 是用户和服务器选取的随机数，未使用之前的会话密钥，双方计算当前会话密钥时都使用到了一次性随机数 k 和 r，因此即使攻击者获得了用户和服务器某一次的会话密钥 SK，也不能推导出用户和服务器之间下一次的会话密钥 SK'，因为生成每一次会话密钥都使用了不同的随机数 k 和 r，所以本协议提供了已知会话密钥安全性。

6 性能分析

本节将新协议与 Xue 的协议[11]、Lin 的协议[16]、Zhu 的协议[17]和 TC 协议[18]进行比较。

表 4 列出了各协议常见的功能，如果方案不满足某种需求或不能抵抗某种攻击，则用“N”表示，否则用“Y”表示。从表 4 的分析结果来看，本协议方案能抵抗表中的所有攻击，此外，本协议还提供智能卡撤销、系统密钥更新，具有完美前向安全性，并且不需要时钟同步，在功能上明显优于其他认证协议方案。

表 4 本协议与其他协议的功能比较

Table 4 Function comparison among different protocols

功能/方案	Xue[11]	Lin[16]	Zhu[17]	TC[18]	Ours
用户匿名性	N	Y	Y	Y	Y
抗中间人攻击	N	Y	Y	Y	Y
抗用户模仿攻击	Y	N	N	Y	Y
抗服务器模仿攻击	Y	N	Y	Y	Y
抗智能卡丢失攻击	Y	Y	Y	Y	Y
口令猜测攻击	Y	N	N	Y	Y
抗内部攻击	Y	Y	Y	Y	Y
抗重放攻击	Y	Y	Y	Y	Y
相互认证	Y	Y	Y	Y	Y
提供前向安全性	Y	Y	N	N	Y
抗拒绝服务攻击	—	—	Y	Y	Y
完美前向安全性	—	—	N	N	Y
不需要时钟同步	N	N	N	N	Y
智能卡撤销	N	N	N	N	Y
系统密钥更新	N	N	N	N	Y

表 5 对比了几种协议的计算效率，符号含义如下：T_s 表示进行一次对称加密(或解密)所需的时间；T_h 表示计算一次哈希函数所需的时间；T_c 表示计算一次切比雪夫多项式所需的时间。

表 5 本协议与其他协议的性能比较

Table 5 Performance comparison among different protocols

	T_c	T_h	T_s	合计
Xue[11]	4	10	4	$4T_c+10T_h+4T_s \approx 720T_h$
Lin[16]	3	7	0	$3T_c+7T_h+0T_s \approx 532T_h$
Zhu[17]	4	10	2	$4T_c+10T_h+2T_s \approx 715T_h$
TC[18]	3	12	2	$3T_c+12T_h+2T_s \approx 542T_h$
Ours	4	10	4	$4T_c+12T_h+0T_s \approx 712T_h$

由文献[12]可知，$T_c \approx 70T_s \approx 175T_h$，$T_s \approx 2.5T_h$。与以上 3 种运算相比，异或运算所用时间可以忽略不计，另外协议的主要计算在登录和认证阶段，因此表 5 仅用协议这两个阶段所需的运算作为性能比较。从表 5 的结果来看，本方案仅需 $712T_h$，优于 Zhu 和 Xue 的方案，虽比 Lin 的方案和 TC 方案慢，但具有更高的安全性和更全的功能。

为了进一步分析协议的性能，使用硬件为 AMD A6-3400M 1.4GHz 的 CPU 和 2GB 的内存，操作系统为 Ubuntu 的仿真环境，基于 NS-2.26 平台对所提协议进行性能仿真。在协议的注册阶段，能够确保用户注册的 ID 具有唯一性，在协议仿真实现时，选取 SHA-1 作为哈希函数，同时对 TC 协议方案进行仿真模拟，得到了如图 2 所示的结果对比图，其中横坐标为认证次数，纵坐标为认证协议的延迟时间。仿真结果表明，本协议和 TC 协议的表现一样优秀，进一步说明了本协议方案的实用性。总的来说，本协议方案同时具有安全性和高效性，因此所提协议方案更适合于实际应用。

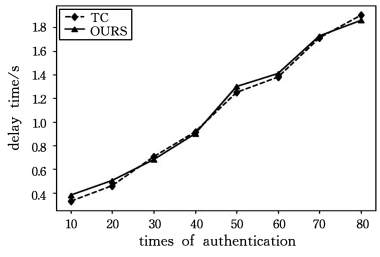

图 2 延迟时间对比

Fig. 2 Comparison of delay time

结束语 混沌映射以其高效性受到研究者的广泛关注。本文以扩展的切比雪夫映射为核心，使用扩展混沌映射数学难题协商会话密钥来确保完美前向安全性，用户使用动态身份登录保护匿名性，采用三次握手技术实现异步认证，同时也避免了时钟同步问题。实验结果表明：新协议不仅满足必要的安全需求以及抵抗各种攻击，还具有较好的计算效率，不仅保证了协议的高效性，也扩大了协议的使用范围，更加适合在实际环境中应用。

参 考 文 献

[1] LIAO X, SHU C. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels[J]. Journal of Visual Communication & Image Representation, 2015, 28: 21-27.

[2] LAMPORT L. Password authentication with insecure communication[J]. Communications of the Acm, 1981, 24(24): 770-772.

[3] CHANG C C, WU T C. Remote password authentication with smart cards[J]. IEE Proceedings E-Computers and Digital Tech-

niques，1993，138(3)：165-168.

[4] KOCAREV L. Chaos-based cryptography：a brief overview[J]. Circuits & Systems Magazine IEEE，2001，1(3)：6-21.

[5] DACHSELT F，SCHWARZ W. Chaos and cryptography [J]. IEEE Transactions on Circuits & Systems I Fundamental Theory & Applications，2002，48(12)：1498-1509.

[6] KOCAREV L，TASEV Z. Public-key encryption based on Chebyshev maps[C]// International Symposium on Circuits and Systems. IEEE，2003：28-31.

[7] XIAO D，LIAO X，WONG K W. An efficient entire chaos-based scheme for deniable authentication[J]. Chaos Solitons & Fractals，2005，23(4)：1327-1331.

[8] BERGAMO P，D'ARCO P，SANTIS A D，et al. Security of public-key cryptosystems based on Chebyshev polynomials[J]. IEEE Transactions on Circuits & Systems I Regular Papers，2005，52(7)：1382-1393.

[9] XIAO D，LIAO X，DENG S. A novel key agreement protocol based on chaotic maps[J]. Information Sciences，2007，177(4)：1136-1142.

[10] GUO X，ZHANG J. Secure group key agreement protocol based on chaotic Hash[J]. Information Sciences，2010，180(20)：4069-4074.

[11] XUE K，HONG P. Security improvement on an anonymous key agreement protocol based on chaotic maps[J]. Communications in Nonlinear Science & Numerical Simulation，2012，17(7)：2969-2977.

[12] TAN Z. A chaotic maps-based authenticated key agreement protocol with strong anonymity[J]. Nonlinear Dynamics，2013，72(1-2)：311-320.

[13] 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.

[14] HE D，CHEN Y，CHEN J. Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol[J]. Nonlinear Dynamics，2012，69(3)：1149-1157.

[15] SHU J. Authentication Key Agreement Protocol Based on Extended Chaos Mapping[J]. Acta Physical Sinica，2014，63(5)：88-92. (in Chinese)
舒剑. 基于扩展混沌映射的认证密钥协商协议[J]. 物理学报，2014，63(5)：88-92.

[16] LIN H Y. Chaotic Map Based Mobile Dynamic ID Authenticated Key Agreement Scheme[J]. Wireless Personal Communications，2014，78(2)：1487-1494.

[17] ZHU H. Cryptanalysis and provable improvement of a chaotic maps-based mobile dynamic ID authenticated key agreement scheme[M]. New Jersey：John Wiley & Sons，Inc.，2015：2981-2991.

[18] TONG T，CHEN J H. Improved Chaotic Maps Based Mobile Authenticated scheme[J]. Application Research of Computers，2017，34(8)：2443-2447. (in Chinese)
童彤，陈建华. 一个改进的基于混沌映射的移动端认证协议[J]. 计算机应用研究，2017，34(8)：2443-2447.

[19] DOLEV D，YAO A. On the Security of Public Key Protocols [J]. IEEE Transactions on Information Theory，1983，29(2)：198-208.

[20] KOCHER P C，JAFFE J，JUN B. Differential Power Analysis [C]// Proceedings of the 19th Annual International Cryptology Conferece on Advances in Crytology. 1999：388-397.

[21] MESSERGES T S，DABBISH E A，SLOAN R H. Examining Smart-Card Security under the Threat of Power Analysis Attacks[J]. IEEE Transactions on Computers，2002，51(5)：541-552.

[22] BRIER E，CLAVIER C，OLIVIER F. Correlation Power Analysis with a Leakage Model[J]. Ches，2004，37(22)：16-29.

[23] ABRAMOWITZ M. Handbook of Mathematical Functions with Formulas，Graphs，and Mathematical Tables[M]. New York：Dover Publications，1974.

[24] JIANG J C，PENG Y H. Chaos of the tchebycheff polynomials [J]. Natural Science Journal of Xiangtan University，1996(3)：37-39. (in Chinese)
蒋建初，彭跃辉. 切比雪夫多项式的混沌性[J]. 湘潭大学自科学报，1996(3)：37-39.

[25] ZHANG L. Cryptanalysis of the public key encryption based on multiple chaotic systems[J]. Chaos Solitons & Fractals，2008，37(3)：669-674.

[26] LIU J F，ZHOU M T. Research and taxonnmy of Replay Attacks on Security Protocol [J]. Application Research of Computers，2007，24(3)：135-139. (in Chinese)
刘家芬，周明天. 对安全协议重放攻击的分类研究[J]. 计算机应用研究，2007，24(3)：135-139.

[27] WANG Z C，YANG S P. Research on Principles and Methods of Designing Authentication Protocols against replay Attack [J]. Computer Engineering and Design，2008，29(20)：5163-5165. (in chinese)
王正才，杨世平. 抗重放攻击认证协议的设计原则和方法研究[J]. 计算机工程与设计，2008，29(20)：5163-5165.

[28] LI M G，SONG H N. Research on Computer Clock Synchronization Technology [J]. Journal of System Simulation，2002，14(4)：477-480. (in Chinese)
李明国，宋海娜. 计算机时钟同步技术研究[J]. 系统仿真学报，2002，14(4)：477-480.

[29] SUN N，XIONG W，DING Y Z. Study and Application of Clock Synchronization[J]. Computer Engineering and Applications，2003，39(27)：177-179. (in chinese)
孙娜，熊伟，丁宇征. 时钟同步的研究与应用[J]. 计算机工程与应用，2003，39(27)：177-179.

[30] WANG D. Research on Password-Based Remote User Authentication scheme using Smart-Cards[D]. Harbin：Harbin Engineering University，2013. (in Chinese)
汪定. 基于智能卡的远程用户口令认证协议研究[D]. 哈尔滨：哈尔滨工程大学，2013.

[31] WANG S B. An Improved Remote User Authentication Scheme [J]. Computer Engineering & Science，2011，33(1)：51-55.