基于扩展混沌映射的三方认证密钥协商协议

闫丽丽，昌 燕，张仕斌

(成都信息工程大学网络空间安全学院 成都 610225)

【摘要】该文基于混沌映射和智能卡技术提出了一个新的三方认证和密钥协商协议。由于该协议在执行过程中无需使用对称、非对称加密算法和时间戳技术，因此降低了协议运行的计算复杂度，提高了运行效率。此外，该协议实现了便捷的用户密钥更新机制，提高了安全性。最后，从安全性和执行效率两方面对所设计协议进行分析，并与相关工作进行了比较，结果显示该协议能够抵御常见攻击，而且具有低传输和计算消耗，更适用于实际应用环境。

关 键 词 认证；混沌映射；密钥协商；智能卡

中图分类号 TP309 **文献标志码** A doi:10.3969/j.issn.1001-0548.2018.06.013

Three-Party Authenticated Key Exchange Scheme Based on Extended Chaotic Maps

YAN Li-li, CHANG Yan, and ZHANG Shi-bin

(Department of Information Security Engineering, Chengdu University of Information and Technology Chengdu 610225)

Abstract In this paper, we propose a novel three-party authentication and key exchange protocol without using a timestamp based on chaotic maps. The proposed protocol requires neither symmetric nor asymmetric cryptosystems. Therefore, the computation complexity of the protocol is reduced and the efficiency of the protocol is improved. In addition, a convenient mechanism for updating user keys is provided, which improves the security of the protocol. Furthermore, the security analysis and performance evaluation are presented in the paper. In comparison with the related protocols, the proposed scheme is secure under certain types of attacks. It also has fewer transmissions and lower computational cost. Accordingly, it is feasible for real world applications.

Key words authentication; chaotic maps; key exchange; smart card

随着无线网络技术的发展，无线通信的应用范围越来越广泛。但是由于无线用户在公开的信道上交换信息，其安全性无法得到保障。而认证和密钥协商协议可以提供数据的隐私保护，保证数据的保密传输。因此，在无线网络应用方面，密钥协商协议的研究变得尤其重要[1]。

1976年，Diffie-Hellman首次提出了密钥协商的概念，随后研究者基于Diffie-Hellman协议做了大量研究。传统的密钥协商协议主要是通过公钥证书的方式实现协议协商过程中的身份认证。基于公钥的密钥协商协议具有许多优点，但是公钥认证和证书管理相当复杂，不适用于资源限制性的网络环境。由于扩展的混沌映射算法具有高效和安全的特性，最近研究者将其应用于安全协议设计上，提出了大量的两方[2-17]和三方认证[18-26]密钥协商协议，本文主要关注三方密钥协商协议。2010年，文献[18]基于混沌算法提出了一个三方密钥协商协议。但该协议存在很多缺陷，如协议采用时间戳，需要严格的时钟同步机制；协议运行需要较多的计算，而且攻击者可以非法篡改传输消息而不被发现[19]。2012年，文献[20]基于混沌算法提出了一个三方认证协议，但该协议不能抵御内部用户发起的攻击[21]。且该协议没有提供用户密钥的更新[25]，而一个密钥使用的时间越长，其安全性必然会变得越来越低。该协议还存在重放攻击，攻击者可以伪装成合法用户，将监听到的信息重新发送给接收者，而接收者却无法发现，而且协议中的智能卡无法检测用户输入的密钥是否正确[25]。2013年，文献[21]提出了一个三方密钥协商协议。但该协议被发现缺少密钥更新功能，而且如果智能卡丢失，攻击者可以提取出智能卡中的信息，伪装成合法用户[25]。2013年，一个基于扩展混沌算法的三方密钥协商协议被提出[22]，但仍然存在

收稿日期：2017－05－26；修回日期：2017－11－22
基金项目：国家自然科学基金(61402058)
作者简介：闫丽丽(1980－)，女，博士，副教授，主要从事无线传感器网络、信息安全及安全协议方面的研究.

诸多问题，如：1) 存在内部用户攻击[25]；2) 攻击者可以实现在协议运行成功的基础上，造成通信双方协商出一个不一致的密钥等[26]；3) 使用了公钥机制，在协议运行前，需要先构造一个公钥基础设施，加重了服务器的负担。2014年，文献[24]提出了一个三方密钥协商协议，该协议不需要智能卡，也不需要公开密钥和对称密钥体制。但是，该协议需要较大的计算量。最近，文献[25]使用扩展的混沌算法，提出了一个基于密钥的三方认证和密钥协商协议。然而，该协议也需要时间戳和对称密钥体系。

本文基于扩展的混沌映射算法，提出了一个三方认证和密钥协商协议。在可信服务器的帮助下，该协议可为通信双方协商一个会话密钥，用于信息的安全传输。该协议无需建立公钥基础设施，整个协议只包含Chebyshev多项式和哈希函数，具有较低的计算消耗，而且可以抵御网络中典型的恶意攻击，适用于资源限制性的网络。

1　相关理论基础

1.1　Chebyshev(切比雪夫)混沌映射

定义 1　n维Chebyshev多项式 $T_n(x):[-1,1]\to[-1,1]$ 定义为 $T_n(x)=\cos(n\arccos(x))$，其中：n为整数，x为实数且 $x\in[-1,1]$。

定义 2　令 $n\in Z$，变量 $x\in[-1,1]$，Chebyshev多项式 $T_n(x):[-1,1]\to[-1,1]$ 的迭代关系式为 $T_n(x)=2xT_{n-1}(x)-T_{n-2}(x)$，$n\geqslant 2$，且 $T_0(x)=1$，$T_1(x)=x$。最初的几个Chebyshev多项式为 $T_2(x)=2x^2-1$，$T_3(x)=4x^3-3x$，$T_4(x)=8x^4-8x^2+1$，…。

当 $n>1$，n维Chebyshev多项式 $T_n(x):[-1,1]\to[-1,1]$ 是一个典型的混沌映射。该映射唯一绝对连续的不变测度为 $f^*(x)=1/(\pi\sqrt{1-x^2})$。$n$维Chebyshev多项式的Lyaounov指数为 $\ln n>0$。当 $n>1$ 时，Chebyshev多项式即为Logistic映射。

定义 3　Chebyshev多项式的半群属性定义为 $T_n(x)\equiv(2xT_{n-1}(x)-T_{n-2}(x))\bmod p$，其中 $n>1$，$x\in(-\infty,+\infty)$，p是一个大素数，由半群性质可知Chebyshev多项式映射可转换为 $T_r(T_s(x))\equiv T_{sr}(x)\equiv T_s(T_r(x))\bmod p$，$s,r\in Z$。

1.2　计算困难问题

扩展的Chebyshev多项式的两个问题被认为是多项式时间难解的。

定义 4　离散对数问题(discrete logarithm problem, DLP)。给定x、y和p，找到一个整数r，使得 $y=T_r(x)\bmod p$ 在计算上不可行。

定义 5　计算Diffie-Hellman问题(computation Diffie-Hellman problem, CDHP)。给定x、$T_r(x)$、$T_s(x)$和p，无法计算 $T_{rs}(x)$。

2　新的三方认证密钥协商协议

该协议包含一个可信服务器S，一个信息发送者U_i和一个响应者U_j。U_i和U_j之间需要在S的帮助下协商一个安全的会话密钥。初始化阶段，U_i和U_j需要到服务器S上注册，获得一个有效的智能卡(smart card)，该注册阶段可在智能卡出厂时，一次设置完成，然后分发给用户使用。本文提出的协议包含注册、登录和密钥协商、密钥更新3个阶段。表1列出了文中需要的变量和符号。

表1　协议中变量和符号说明

变量或符号	说明
ID_i	用户U_i唯一的身份标识
PW_i	用户U_i的密钥
X_s	服务器S的密钥
$\|\|$	将消息串联起来的符号
$\oplus$	异或运算
$\to$	开发的通信网络
$\Rightarrow$	安全的通信网络
$h(),h_1()$	哈希函数，其中h: $\{0,1\}^*\to Z_p^*$
$T_n(x)$	切比雪夫多项式

在协议运行前，由服务器为移动网络生成基本参数：一个大素数p，一个实数 $z\in(-\infty,+\infty)$，一个哈希函数$h()$和服务器的保密密钥X_s。

2.1　注册阶段

用户需在服务器处注册，才能成为网络中的合法用户。用户 U_i 输入其 ID_i 和密钥 PW_i，同时产生一个随机数 N_i。U_i 使用哈希函数 $h_1()$ 计算 $f_i=h_1(\mathrm{PW}_i\|N_i)$，随后将消息$\{\mathrm{ID}_i,f_i\}$通过安全的通道发送给服务器 S。

S 计算 $P_i=h(\mathrm{ID}_i\|X_s)$ 和 $e_i=P_i\oplus f_i$，然后将信息$\{\mathrm{ID}_i, e_i, x, p, h(), \mathrm{SPUB}\}$写入一个 smart card，并将该 smart card 通过一个安全的通信网络发送给 U_i，其中 $\mathrm{SPUB}=T_{X_s}(z)\bmod p$。

用户在收到smart card后，将$h_1()$、N_i 和$h(\mathrm{PW}_i)$加入到smart card中。至此，用户获得了自己的smart card。用户注册的过程如图1所示。

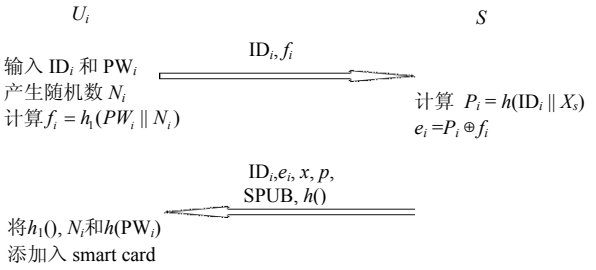

图1 用户注册阶段

2.2 登录和密钥协商阶段

当U_i要与其他移动用户进行通信时，执行如下操作。U_i插入他的smart card，输入密钥PW_i'。smart card计算$h(PW_i')$，并与自己存储的$h(PW_i)$进行比较，如果相等，smart card选择随机数kx和N_1，计算 $f_i = h_1(PW_i \| N_i)$， $P_i = e_i \oplus f_i$， $M_1 = T_{kx}(z) \bmod p$， $M_2 = T_{kx}(SPUB) \bmod p$ 和 $t_1 = h(ID_i \| ID_j \| M_1 \| M_2 \| P_i \| N_1)$。其中$N_1$是一个自增长的随机数，通过一个随机数发生器生成，使得用户每次产生的随机数都比前一次的值大。由于用户和服务器都具有同一个随机数发生器函数，因此它们可以通过使用该随机数抵御重放攻击。

U_i将消息$\{ID_i, ID_j, M_1, t_1, N_1\}$发送给$U_j$。

U_j收到消息后，插入自己的smart card，然后输入PW_j'。由smart card计算是否$h(PW_j) = h(PW_j')$。如果成立，smart card选择一个随机数ky和N_2，计算 $f_j = h_1(PW_j \| N_j)$， $P_j = e_j \oplus f_j$， $M_3 = T_{ky}(z) \bmod p$， $M_4 = T_{ky}(SPUB) \bmod p$ 和 $t_2 = h(ID_i \| ID_j \| M_3 \| M_4 \| P_j \| N_2)$，其中$N_2$是一个自增长的随机数。

U_j 发送消息$\{ ID_i, ID_j, M_1, t_1, N_1, M_3, t_2, N_2\}$给$S$。

S收到消息后计算 $P_i' = h(ID_i \| X_s)$， $P_j' = h(ID_j \| X_s)$， $t_1' = h(ID_i \| ID_j \| M_1 \| M_2' \| P_i' \| N_1)$， $t_2' = h(ID_i \| ID_j \| M_3 \| M_4' \| P_j' \| N_2)$， $M_2' = T_{X_s}(M_1) \bmod p = T_{kx}(T_{X_s}(z)) \bmod p = T_{kx}(SPUB) \bmod p$ 和 $M_4' = T_{X_s}(M_3) \bmod p = T_{ky}(T_{X_s}(z)) \bmod p = T_{ky}(SPUB) \bmod p$。然后，$S$通过判断 $t_1 = t_1'$ 和 $t_2 = t_2'$，来确认U_i和U_j的身份。S将N_1和N_2与对应用户的随机数发生器产生的随机数进行比较，来抵御重放攻击。S计算 $t_3 = h(ID_j \| M_2 \| M_3 \| N_1)$，并发送消息$\{ID_j, M_3, t_3\}$给$U_i$，发送消息$\{ID_i, M_1, t_4\}$给$U_j$.

当U_i收到消息后，根据ID_j获得M_2和N_1，计算 $t_3' = h(ID_j \| M_2 \| M_3 \| N_1)$，通过判断 $t_3 = t_3'$ 来确认S和U_j的身份，如果成立，获得会话密钥 $K = T_{kx}(M_3) \bmod p = T_{kxky}(z) \bmod p$。

当U_j收到消息后，同样根据ID_i获得M_4和N_2，计算 $t_4' = h(ID_i \| M_1 \| M_4 \| N_2)$，并通过判断 $t_4 = t_4'$ 来确认S和U_i的身份，如果成立，获得会话密钥 $K = T_{kx}(M_3) \bmod p = T_{kxky}(z) \bmod p$。协议的登陆和密钥协商过程如图2所示。

2.3 密钥更新阶段

为了保证用户的安全，用户可根据需要更新自己的密钥。在密钥更新阶段，无需服务器的协助，每个合法用户都可以自主地改变密钥。

当用户需要更新密钥时，用户U_i插入他的smart card，输入旧密码PW_i'和一个新密码 PW_i^*。由smart card使用用户输入的旧密码计算$h(PW_i')$，并与其存储的$h(PW_i)$进行比较。如果相等，smart card根据卡里存储的N_i和e_i，计算 $f_i = h_1(PW_i' \| N_i)$ 和 $P_i = e_i \oplus f_i$，并生成一个新的随机数 N_i^*，再计算 $f_i^* = h_1(PW_i^* \| N_i^*)$ 和 $e_i^* = P_i \oplus f_i^*$。最后smart card将N_i替换成 N_i^*，$h(PW_i)$替换成$h(PW_i^*)$，e_i替换成e_i^*，至此完成了密钥的更新。

3 协议的安全性分析

本节将针对典型的攻击方式，采用非形式化的方式分析协议的安全性。

1) 密钥猜测攻击(on-line and off-line password guessing attack)：攻击者可以通过监听的方式，截获U_i、U_j 和S之间传递的信息，并发起密钥猜测攻击。在本协议中，会话密钥 $K = T_{ky}(M_1) \bmod p = T_{kx}(M_3) \bmod p = T_{kxky}(z) \bmod p$，根据定义1.4和1.5，由于kx和ky并不包含在传递的消息内容中，因此即使攻击者获得了M_1和M_3，他也无法计算出会话密钥K。

2) 窃取smart card攻击(stolen smart card attack)：当攻击者窃取到合法用户的smart card后，他可以获得卡中存储的信息$\{ ID_i, e_i, x, p, SPUB, h(), h_1(), N_i, h(PW_i) \}$。但是，攻击者如果想冒充合法用户，他需要输入用户密钥PW_i，由smart card计算$h(PW_i)$，并与存储在智能卡中的值进行比较，只有比较相等smart card才继续执行协商协议。但是由于攻击者无法获得用户密钥PW_i，所以即使攻击者窃取了smart card也无法冒充合法用户。

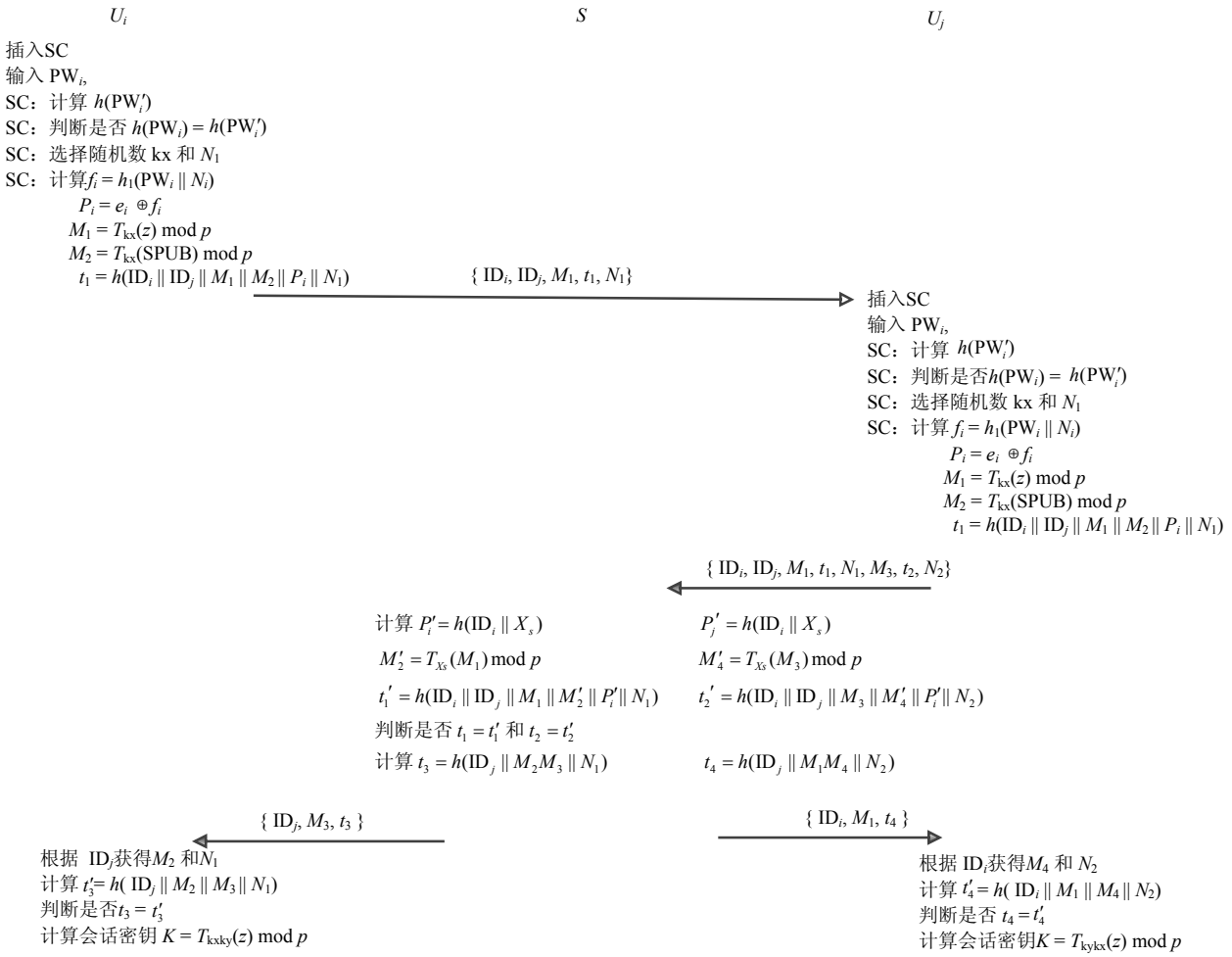

图2　协议登录和密钥协商过程

当用户发现智w能卡丢失后，需要向服务器提出申请，通过服务器重新注册后，生成新的智能卡，旧的智能卡被撤销。

3) 重放攻击(replay attack)：在协议中，所有的消息都包含一个随机数N,而且该随机数是一个自增长的值。协议每执行一次，用户和服务器中对应该用户的随机数发生器都会同步产生一个随机数。如果有重放数据包，数据到到达后，用户和服务器可以通过数据包中的随机数，与自己对应的随机数进行对比，来发现重放攻击。

4) 已知密钥攻击(known-key security)：由于每次通信的会话密钥$K = T_{kykx}(z)$ 都是由本次通信的随机数kx和ky计算获得，即使攻击者知道上次会话或将来会话的某个密钥，也无法推断出本次会话密钥。

5) 伪造和假冒攻击(forgery and impersonation attack)：如果一个攻击者冒充合法用户，他需要发送消息$\{ID_i, ID_j, M_1, t_1, N_1\}$，其中$t_1 = h(ID_i \| ID_j \| M_1 \| M_2 \| P_i \| N_1)$, $P_i = e_i \oplus f_i$ 和 $f_i = h_1(PW_i \| N_i)$ 。但是攻击者无法获得用户密钥PW_i,因此他就无法冒充合法用户。

6) 中间人攻击(man-in-the-middle attack)：从上面分析可以发现，由于攻击者无法实现重放、伪造和假冒攻击，因此他也无法实施中间人攻击。

7) 特权用户攻击(privileged insider attack)：由于在协议中传递的消息不包含U_i和U_j 的密钥，因此协议能够抵御特权用户攻击。

表2列出了本协议与相关协议在安全性方面的比较结果。其中Yes表示，协议具有相应功能，或可以抵御对应攻击。

4　协议的效率分析

本节将本协议的执行效率与相关工作进行对比，结果显示本协议的通信和计算开销都较小。由于异或运算的计算量较少，在进行计算量评估时可忽略不计。表3列出了本协议与相关协议[18-25]在计算开销方面的比较结果，其中T_C、T_S 和T_h分别表示Chebyshev多项式、对称加、解密运算和哈希函数的计算执行时间。

表2 本文协议和相关协议安全性比较

攻击方式	文献[18]	文献[19]	文献[20]	文献[21]	文献[22]	文献[23]	文献[24]	文献[25]	本文协议
双向认证	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
密钥协商	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
密钥更新	No	No	No	No	No	No	Yes	Yes	Yes
密钥猜测攻击	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes
窃取smart card攻击	---	---	Yes	No	---	---	---	Yes	Yes
重放攻击	Yes	Yes	No	Yes	Yes	No	No	Yes	Yes
已知密钥攻击	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
伪造和假冒攻击	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes
中间人攻击	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
特权用户攻击	No	No	No	Yes	No	No	No	Yes	Yes

表3 本文协议和相关协议计算效率比较

协议阶段	文献[18]	文献[19]	文献[20]	文献[21]	文献[22]	文献[23]	文献[24]	文献[25]	本文协议
注册阶段	---	---	$2T_h+T_S+T_C$	$2T_h$	---	---	T_h+T_C	$2T_h+T_S$	$3T_h$
密钥协商	$4T_S+8T_C$	$4T_h+4T_S+4T_C$	$18T_h+2T_S+8T_C$	$18T_h+4T_S+10T_C$	$14T_h+6T_C$	$12T_h+8T_S+6T_C$	$12T_h+8T_C$	$5T_h+14T_S+4T_C$	$14T_h+6T_c$
密钥更新	---	---	---	---	---	---	$10T_h+5T_C$	$2T_h+2T_S$	$4T_h$
总计算消耗	$4T_S+8T_C$	$4T_h+4T_S+4T_C$	$13T_h+3T_S+9T_C$	$20T_h+4T_S+10T_C$	$14T_h+6T_C$	$12T_h+8T_S+6T_C$	$23T_h+14T_C$	$9T_h+17T_S+4T_C$	$21T_h+6T_c$

在3.2 GHz处理器3.0 G RAM环境下，T_h的执行时间是0.2 ms，T_S的执行时间是0.45 ms，T_C的执行时间是32.2 ms[13]，表4列出了本协议和相关协议[18-25]的执行时间。

表4 本协议和相关协议的执行时间

协议	执行时间/ms
文献[18]	260
文献[19]	132
文献[20]	395
文献[21]	329
文献[22]	198
文献[23]	200
文献[24]	457
文献[25]	139
本文协议	198

从上面分析结果可以发现，本协议具有较低的计算开销。与文献[25]提出的协议相比，本协议需要4次通信，而文献[25]中的协议需要8次，而且本协议不需要复杂的网络时钟同步技术。

5 结 束 语

本文基于扩展的混沌算法设计了一个适用于无线网络的三方用户认证和密钥协商协议。在可信第三方服务器的协助下，协议实现了双向用户的认证和密钥协商功能，而且协议提供了便捷的密钥更新机制，提高了用户密钥的安全性。通过安全性分析和效率分析可得出，与现有相关协议相比，本协议具有较高的安全性和较低的通信、计算开销，更适用于无线传感器网络。

参 考 文 献

[1] GUO C, CHANG C C, SUN C Y, et al. Chaotic maps-based mutual authentication and key agreement using smart cards for wireless communications[J]. J Inf Hiding Multimedia Signal Process, 2013, 4(2): 99-109.

[2] ÖZKAYNAK F, YAVUZ S. Designing chaotic s-boxes based on time-delay chaotic system[J]. Nonlinear Dynamics, 2013, 74(3): 551-557.

[3] ALVAREZ G. Security problems with a chaos-based deniable authentication scheme[J]. Chaos Solitons &Fractals, 2005, 26(1): 7-11.

[4] XIAO Di, LIAO Xiao-feng, DENG Shao-jiang. A novel key agreement protocol based on chaotic maps[J]. Information Sciences, 2007, 177(4): 1136-1142.

[5] SONG Han. Security of a key agreement protocol based on chaotic maps[J]. Chaos Solitons & Fractals, 2007, 38(3): 764-768.

[6] XIANG Tao, WONG K W, LIAO Xiao-feng. On the security of a novel key agreement protocol based on chaotic maps[J]. Chaos Solitons & Fractals, 2009, 40(2): 672-675.

[7] XIAO Di, LIAO Xiao-feng, DENG Shao-jiang. Using time-stamp to improve the security of a chaotic maps-based key agreement protocol[J]. Information Sciences, 2008, 178(6): 1598-11602.

[8] HAN S, CHANG E. Chaotic map based key agreement without clock synchronization[J]. Chaos Solitons and Fractals, 2009, 39(3): 1283-1289.

[9] GUO Xian-feng, ZHANG Jia-shu. Secure group key agreement protocol based on chaotic hash[J]. Information Sciences, 2010, 180(20): 4069-4074.

[10] GONG Peng, LI Ping, SHI Wen-bo. A secure chaotic maps-based key agreement protocol without using smart

cards[J]. Nonlinear Dynamics, 2012, 70(4): 2401-2406.
[11] TSENG H, JAN R, YANG W. A chaotic maps-based key agreement protocol that preserves user anonymity[C]// Proceeding of IEEE international conference on communications (ICC09). [S.l.]: IEEE, 2009: 1-6.
[12] NIU Yu-jun, WANG Xing-yuan. An anonymous key agreement protocol based on chaotic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(4): 1986-1992.
[13] XUE Kai-ping, HONG Pei-lin. Security improvement on an anonymous key agreement protocol based on chaotic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(7): 2969-2977.
[14] YOON E. Efficiency and security problems of anonymous key agreement protocol based on chaotic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(7): 2735-2740.
[15] TAN Zuo-wen. A chaotic maps-based authenticated key agreement protocol with strong anonymity[J]. Nonlinear Dynamics, 2013, 72(1-2): 311-320.
[16] LEE C, HSU C A. Secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps[J]. Nonlinear Dynamics, 2013, 71(1-2): 201-211.
[17] GUO Cheng, CHANG Chin-chen. Chaotic maps-based password-authenticated key agreement using smart cards[J]. Communications in Nonlinear Science and Numerical Simulation, 2013, 18(6): 1433-1440.
[18] WANG Xing-yuan, ZHAO Jian-feng. An improved key agreement protocol based on chaos[J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(12): 4052-4057.
[19] YOON E, JEON I. 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.
[20] LAI Hong, XIAO Jing-hua, LI Li-xiang. Applying semigroup property of enhanced Chebyshev polynomials to anonymous authentication protocol[EB/OL]. [2017-02-03]. http://dx.doi-org/10.1155/2012/454823.
[21] ZHAO Feng-jun, GONG Peng, LI Shuai. Cryptanalysis and improvement of a three-party key agreement protocol using enhanced Chebyshev polynomials[J]. Nonlinear Dynamics, 2013, 74(1-2): 419-427.
[22] LEE C, LI C, HSU C. 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.
[23] XIE Qi, ZHAO Jian-min, YU Xiu-yuan. Chaotic maps-based three-party password-authenticated key agreement scheme[J]. Nonlinear Dynamics, 2013, 74(4): 1021-1027.
[24] FARASH M, ATTARI M. An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps[J]. Nonlinear Dynam, 2014, 77(1-2): 399-411.
[25] ISLAM S. Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps[J]. Information Science, 2015, 312(10): 104-130.
[26] FARASH M, ATTARI M, KUMARI S. Cryptanalysis and improvement of a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps[J]. International Journal of Communication Systems, 2017, 30: 1-10.

编 辑 蒋 晓