新型基于 Chebyshev 多项式的身份认证方案*

李旭飞[1,2†]，赵 耿[2]，孙锦慧[1,2]，陶 涛[3]
(1. 西安电子科技大学 通信工程学院，西安 710071；2. 北京电子科技学院，北京 100070；3. 公安部出入境证件核心技术中心，北京 100741)

摘 要：对已有基于 Chebyshev 多项式的身份认证方案进行了安全性方面的分析，引入密态时钟，提出了一种新的身份认证方案。通过对其性能的研究，新的方案是安全有效的。

关键词：Chebyshev 多项式；半群特性；密态时钟；身份认证
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2013)06-1840-03
doi:10.3969/j.issn.1001-3695.2013.06.062

New identity authentication scheme based on Chebyshev polynomials

LI Xu-fei[1,2†], ZHAO Geng[2], SUN Jin-hui[1,2], TAO Tao[3]
(1. *College of Communication Engineering, Xidian University, Xi'an* 710071, *China*; 2. *Beijing Electronic Science & Technology Institute, Beijing* 100070, *China*; 3. *Ministry of Public Security Entry & Exit Certificate Core Technology Center, Beijing* 100741, *China*)

Abstract: This paper studied the security of the proposed identity authentication scheme based on Chebyshev polynomials. It introduced the secret state clock, and proposed a new identity authentication scheme which was secure and practical after analyzing.

Key words: Chebyshev polynomials; semi-group property; secret state clock; identity authentication

身份认证技术是网络安全技术的重要组成部分。用户身份认证可通过多种方式实现，其中口令认证方式由于其实现简单、使用方便而受到了人们广泛的使用。但传统的基于口令的身份认证技术的安全性仅基于对用户口令的保密，任何对口令的存储或传输过程中的攻击都会对合法用户的身份造成威胁。本文提出了一种基于混沌映射的公钥密码算法的身份认证方案，利用混沌系统中 Chebyshev 映射良好的单向性、半群特性等特征，增强了身份认证方案的安全性。

混沌系统由于其对初值和系统参数的敏感性、单向性、运动状态不确定性等特征，近年来成为国内外学者研究的一个热点。其中关于混沌非对称加密的研究也有了一些进展。以 Kocarev 为代表，提出了基于 Chebyshev 映射的公钥加密方案。Kocarev 等人[1]利用 Chebyshev 混沌映射的半群特性，提出了一种构造公钥密码的方案。方案以数学上离散对数求解的难题作为安全保证，以 ElGamal 公钥密码算法为蓝本，提出了基于 Chebyshev 映射的类 ElGamal 公钥密码算法。但很快 Bergamo 等人[2]利用 Chebyshev 多项式的三角函数定义，通过反三角函数进行求逆运算指出了 Kocarev 公钥密码方案的破解方法。而后学者们分别从以下两个角度解决了上述破解方法：

a)以 Xiao 等人[3]为代表的通过在现有的方案中增加 hash 函数来掩盖 Chebyshev 映射输出值以提高算法的安全性。但此方案一经提出，很多学者都指出了其中的漏洞和缺陷。文献[4]提出了中间人攻击的方法，指出攻击者可以分别冒充通信方发送信息从而达到阻断双方通信的目的。文献[5]则从多方面分析了该方案的不安全性，并深刻分析了这种思路的局限性问题。

b)以 Wang 等人[6]为代表的通过将 Chebyshev 多项式扩展到有限域上来解决 Bergamo 攻击的思路。即在文献[1]的基础上，在有限域上提出了算法的改进方案，并提出了相应的身份认证方案。本文从这一角度入手，通过分析现有身份认证方案的缺陷，提出了新的安全性更高的方案。

1 Chebyshev 多项式

1.1 定义

密码学中常用的 Chebyshev 多项式定义如下：

定义 1[1] 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

$$T_n(x)=2xT_{n-1}(x)-T_{n-2}(x)\quad n\geqslant 2 \tag{1}$$

且有 $T_0(x)=1$，$T_1(x)=x$。开始的几个 Chebyshev 多项式为

$$T_2(x)=2x^2-1,T_3(x)=4x^3-3x,T_4(x)=8x^4-8x^2+1$$

n 维 Chebyshev 多项式 $T_n(x):[-1,1]\to[-1,1]$，当 $n\geqslant 2$ 时是一个典型的混沌映射。该映射有一个唯一绝对连续的不变测度为

$$\mu(x)\,\mathrm{d}x=\frac{\mathrm{d}x}{\pi\sqrt{1-x^2}} \tag{2}$$

n 维 Chebyshev 多项式的 Lyapunov 指数 $\lambda=\ln n$。当 $n=2$ 时，Chebyshev 多项式就是著名的 Logistic 映射。

由于 Chebyshev 多项式是代数多项式，因此，可以很容易地把式(1)扩展到实数域 R 和有限域 Z_P 上，这里令 P 为素数。

收稿日期：2012-08-30；**修回日期**：2012-11-06 **基金项目**：国家自然科学基金资助项目(61170037)

作者简介：李旭飞(1988-)，男(通信作者)，陕西兴平人，研究员，硕士，主要研究方向为混沌公钥、声纹识别(xuxu_512@163.com)；赵耿(1964-)，男，四川广元人，教授，博导，博士(后)，主要研究方向为混沌密码、语音处理与语音识别；孙锦慧(1985-)，女，河南开封人，研究员，硕士，主要研究方向为混沌公钥密码、计算机信息安全与保密；陶涛(1984-)，男，陕西咸阳人，副主任科员，硕士，主要研究方向为混沌分组密码.

在有限域 $x \in Z_p$ 上的 Chebyshev 多项式可定义如下:

定义 2[6]　令 $n \in Z^+$,变量 $x \in Z_p$,则多项式 $T_n(x): Z_p \to Z_p$ 的递归关系定义为

$$T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) (\mathrm{mod}\ p) \quad n \geqslant 2 \tag{3}$$

且有 $T_0(x) \equiv 1 (\mathrm{mod}\ p)$, $T_1(x) \equiv x (\mathrm{mod}\ p)$。

同样,当 $n \geqslant 2$ 时,有限域 Chebyshev 多项式也是一个混沌映射。

1.2　性质

1.2.1　半群特性[7]

Chebyshev 多项式的半群特性可表示为

$$T_m(T_n(x)) = T_{m \cdot n}(x) \quad n, m \in Z \tag{4}$$

由半群性质可知,Chebyshev 多项式满足

$$T_m(T_n(x)) = T_{m \cdot n}(x) = T_n(T_m(x)) \quad n, m \in Z \tag{5}$$

把 Chebyshev 多项式扩展到实数域 R 上后,仍满足半群特性,且由于 Chebyshev 多项式是代数多项式,可以得到在有限域 Z_p 上 Chebyshev 多项式的半群特性的表达式为

$$\begin{aligned} &T_n(T_m(x) (\mathrm{mod}\ P)) (\mathrm{mod}\ P) = T_{n \cdot m}(x) (\mathrm{mod}\ P) = \\ &T_m(T_n(x) (\mathrm{mod}\ P)) (\mathrm{mod}\ P) \Rightarrow T_n(T_m(x)) (\mathrm{mod}\ P) = \\ &T_{n \cdot m}(x) (\mathrm{mod}\ P) = T_m(T_n(x)) (\mathrm{mod}\ P) \quad n, m \in Z_p \end{aligned} \tag{6}$$

1.2.2　计算上的单向性[8]

对于有限域 Z_p 上的任意一个 Chebyshev 多项式 $T_n(x)$ 来说,$T_n(x)$ 还可表示为

$$T_n(x) = (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) (\mathrm{mod}\ P) \tag{7}$$

现阶段还没有找到有限域 Chebyshev 多项式的反函数表达式。因此在式(7)中,已知 x 和 n 求 $T_n(x)$ 是比较容易的,但是如果已知 x 和 $T_n(x)$ 求多项式(7)的最高次幂,即 n 的值,是困难的,其求解的困难性可与求离散对数的困难问题类比。在式(7)的最高次幂 n 与所求离散对数的最高次幂相同的情况下,由于多项式(7)中各低次幂项的存在,如 x^{n-1}、x^{n-2} 等,求解式(7)中的最高次幂 n 比求解离散对数 n 更为困难和复杂,而且在 n 未知的情况下,式(7)中的各项系数也是无法确定的。因此,式(7)在计算上有着良好的单向性,即有限域 Z_p 上的 Chebyshev 多项式在计算上也有良好的单向性。由于这种良好的单向性,可将有限域 Chebyshev 多项式应用到密码技术中。

2　已提出的基于 Chebyshev 多项式的身份认证方案

Chebyshev 多项式的半群特性及单向性等特性,可以很好地利用在身份认证当中。以下介绍一个基本的基于 Chebyshev 多项式的身份认证方案[6],实现了服务器方对登录用户合法身份的验证。具体方案如下:

设 $m > 1$ 是一个公开的实数,$F_s^i(\cdot)$ 表示 $F_s(\cdot)$ 迭代 i 次,p 为一整数,且有

$$F_s^i(\cdot) = F(F_s(F_s \cdots F_s(\cdot) \bmod p \cdots)) \bmod p = F_s^i \bmod p$$

服务器方:a)产生一个随机整数 s,选一个整数 p;b)计算并发送 $F_s(m) \bmod p$ 给用户。

用户方:选一个随机整数 u。第 i 个用户认证过程如下:

a)用户计算 $F_u^i(m)$ 和身份证书 $au = F_u^i(F_s(m)) \bmod p$,将这两个值送往服务器。

b)服务器得到 $F_u^i(m)$ 后,计算 $au' = F_s(F_u^i(m)) \bmod p$ 并验证 au 是否等于 au'。如果相等,说明用户是合法的。认证结束。

上述方案基本实现了通信双方的身份认证问题,但无法在实际应用中直接使用。该方案存在以下不足之处:

a)中间人攻击。任何人都可以得到 $F_s(m) \bmod p$,攻击者可以截取第 i 个用户发送的 $F_u^i(m)$,并在第 j 个用户通信时使用 $F_u^i(m)$ 替换正确的 $F_u^j(m)$,这样服务器计算的 au' 与收到的 au 就不相等了,从而阻止了认证。

b)重放攻击。攻击者得到 $F_u^i(m)$ 和 au 就可以冒充第 i 个用户再次与服务器通信,从而得到合法身份。

c)现有的方案没有相互认证能力,即服务器方可以认证用户的合法性,但是用户不能认证服务器的合法性。

3　新型身份认证方案

基于以上方案的缺陷,本文引入了可信第三方。假设 KDC 是网络中可信任的第三方,如果 A 和 B 都有一个到 KDC 的加密连接,那么 KDC 就可以通过加密连接将密钥安全地传递给 A 和 B,该密钥分别为 KDC 与 A、KDC 与 B 的共享密钥。在以下方案中记用户 A 与第三方 KDC 的共享密钥为 SKAU,服务器 B 与第三方 KDC 的共享密钥为 SKBU。认证方案如下:

a)A 将自己的 ID 号与想要登录的服务器 B 的 ID 号发送给服务器 B。

$$A \to B: \mathrm{ID}_A \parallel \mathrm{ID}_B$$

b)B 收到后随机产生大数 x、r,大素数 p 及时钟 T_B,计算 $N = T_r(x) (\mathrm{mod}\ p)$,并用 B 与可信任的第三方 KDC 的共享密钥 SKBU 加密 T_B,然后将 $\mathrm{ID}_B \parallel x \parallel p \parallel N \parallel E_{\mathrm{SKBU}}(T_B)$ 再次用 SKBU加密发送给第三方 KDC。

$$B \to \mathrm{KDC}: E_{\mathrm{SKBU}}(\mathrm{ID}_B \parallel x \parallel p \parallel N \parallel E_{\mathrm{SKBU}}(T_B))$$

c)KDC 收到后解密并用其与 A 的共享密钥 SKAU 加密 $\mathrm{ID}_B \parallel x \parallel p \parallel N \parallel E_{\mathrm{SKBU}}(T_B) \parallel \mathrm{ID}_A$ 发送给用户 A。

$$\mathrm{KDC} \to A: E_{\mathrm{SKAU}}(\mathrm{ID}_B \parallel x \parallel p \parallel N \parallel E_{\mathrm{SKBU}}(T_B) \parallel \mathrm{ID}_A)$$

d)A 收到后随机产生大数 s、a,计算 $M = T_s(x) (\mathrm{mod}\ p)$, $L = a \times T_s(N) (\mathrm{mod}\ p)$,此时,$A$ 可计算出与 B 的共享密钥。

$$k = T_s(N) (\mathrm{mod}\ p) = T_s(T_r(x) (\mathrm{mod}\ p)) (\mathrm{mod}\ p) = T_s(T_r(x)) (\mathrm{mod}\ p)$$

将 $M \parallel L \parallel E_K(E_{\mathrm{SKBU}}(T_B)) \parallel \mathrm{ID}_A$ 发送给 B。

$$A \to B: M \parallel L \parallel E_K(E_{\mathrm{SKBU}}(T_B)) \parallel \mathrm{ID}_A$$

e)B 收到后根据 M 和 $N = T_r(x) (\mathrm{mod}\ p)$,可计算出

$$\begin{aligned} k' &= T_r(M) (\mathrm{mod}\ p) = T_r(T_s(x) (\mathrm{mod}\ p)) (\mathrm{mod}\ p) = \\ &T_r(T_s(x)) (\mathrm{mod}\ p) \end{aligned}$$

$$a' = L \times k'^{-1}$$

B 用 k' 解密 $E_{K'}^{-1}(E_K(E_{\mathrm{SKBU}}(T_B))) = E_{\mathrm{SKBU}}(T_B)'$。若 $E_{\mathrm{SKBU}}(T_B) = E_{\mathrm{SKBU}}(T_B)'$,则说明 $k = k'$,B 即可验证 A 的身份。B 再用 K 加密 $a' \parallel \mathrm{ID}_A \parallel \mathrm{ID}_B$ 发送给 A。若不正确,则认证结束。

$$B \to A: E_K(a' \parallel \mathrm{ID}_A \parallel \mathrm{ID}_B)$$

f)A 收到后用 k 解密。若核对正确,则认证成功,同时 A 也建立了与 B 的会话密钥 k,在以后的通信中可以使用;若核对不正确则认证失败。

4　Chebyshev 多项式的快速算法

实现基于 Chebyshev 多项式的身份认证方案最核心的问题是解决 Chebyshev 多项式 $T_n(x)$ 的快速算法。这一部分将介绍一种基于矩阵的计算方法。由 Chebyshev 多项式的定义 $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$, $T_0 = 1$, $T_1 = x$ 可知,若将上式转换为矩阵的表达形式,则可表示为[9]

$$\begin{bmatrix} T_n \\ T_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix} \begin{bmatrix} T_{n-1} \\ T_n \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix}^n \begin{bmatrix} T_0 \\ T_1 \end{bmatrix} \quad (8)$$

由式(8)可以看出,求 $T_n(x)$ 的关键在于求出矩阵 $\begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix}^n$ 的值。具体算法的流程如图1所示。

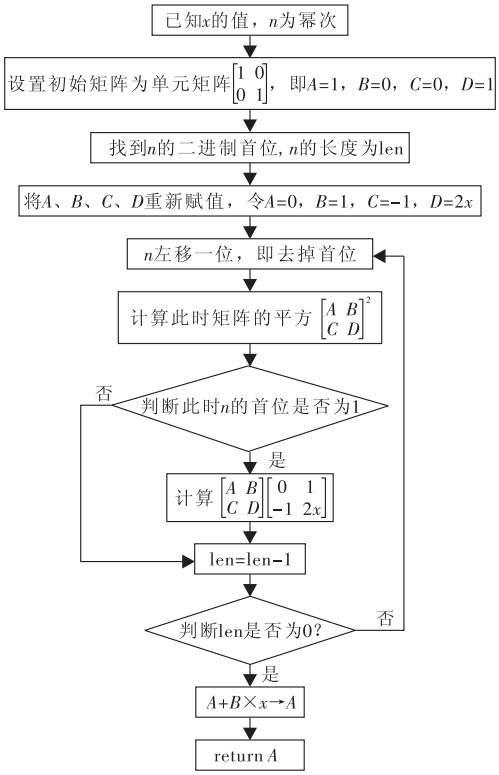

图1 Chebyshev多项式的快速算法

在求出 A 值后,再对 A 取模 p 即可算出最后的 $A = T_n(x) \pmod p$。

在主频为2.33 GHz,内存为2 GB的双核CPU计算机上测试参数长度为64 bit、128 bit、256 bit的计算时间,结果分别为:

a)64 bit参数。计算机随机产生

$x = 8453905564679998682$, $p = 16769903278794126991$,

$n = 439696033179058925$ 时计算结果为 $A = T_n(x) \pmod p = 16901706240345092 84$。计算用时0.003 s。

b)128 bit参数。计算机随机产生

$x = 102158779479527694083239100705255726562$,

$p = 321511324735141979280598970189610924503$,

$n = 160662991214731295155436690005200152 55$ 时计算结果为 $A = T_n(x) \pmod p = 69484568933505346202562653501329232790$。计算用时0.036 s。

c)256 bit参数。计算机随机产生

$x = 513703489214147141290015835041670088670906830026098$
$793778797871112223363633 01$,

$p = 101828224291943527324396992582216290970088536875429$
$754198262756934914318316419$,

$n = 552740850453823414706321146038458925346088945239064$
$648040938990877373407717 62$ 时计算结果为 $A = T_n(x) \pmod p = 459857469706524260550513925281051981573737374475 14$
$937193283861034342479333753$。计算用时0.251 s。

仿真结果证明用矩阵法计算大数值的Chebyshev多项式是可行的,且实现简单、效率很高。

5 身份认证方案的安全性分析

1)相互认证功能 由于可信任第三方的存在,A 和 B 都与可信任第三方拥有各自的共享密钥,保证了它们身份的真实性。由于时钟 T_B 的传送是用KDC和 B 的共享密钥加密的,攻击者无法得到该值。因此在5)中 B 通过解密若能得到时钟 T_B 的密态值 $E_{SKBU}(T_B)$,则可以验证出 A 的身份。同样在6)中 A 通过验证 a 的值也可以最终证实 B 的身份。

2)抵抗重放攻击 由于采用了时钟,即使攻击者截取了上一次通信时的数据,无论是用户 A 还是服务器 B 都可以很容易地判断出数据的有效性。

3)抵抗中间人攻击 中间人攻击是指攻击者可以截取、重放、代替或修改通信双方在通信中的信息,成功获得不应该获得的秘密值,并可能从这些信息中得到一些对通信方来说比较重要的私人信息[10]。本方案利用密态时钟 T_B 干扰了协议的执行,使协议不能正确进行,因此攻击者无法俘获信息。再者,时钟 T_B 只有服务器 B 一方知晓,即使攻击者得到时钟 T_B 的真实值,在认证过程中也很容易穿帮,从而进一步提高了安全性。同时在最后5)6)中 B 通过对密态时钟 $E_{SKBU}(T_B)$ 的验证,A 通过对 a 的验证可以发现信息是否被替代或修改。

4)抵抗惟密文攻击 基于有限域的Chebyshev多项式 $N = T_S(x) \pmod p$ 在公开 (N,x,p) 的情况下,虽然求出 n 的难度等同于求解离散对数问题,但仍然不能抵抗惟密文攻击。即攻击者可以使用穷举搜索找到一个 s' 使得 $N = T_{S'}(x) \pmod p$[11]。但在本方案中,由于用户 B 的公开值 (x,p,N) 都是加密传输的,因此攻击者很难得到真实值。即使 B 由于某种原因不小心泄露了一组 (x,p,N) 值,但时钟 T_B 却是密态的,并且每次通信时都会随机重新生成,攻击者即使得到也无法利用,从而成功地抵抗了惟密文攻击。

5)解决了时钟同步问题[10] 本方案中只使用服务器 B 本身的时钟 T_B,且以密态形式传输,判断标准唯一。因此不存在其他方案中通信双方由于时钟不同步造成的认证失败的问题。

6)解决了密钥分发问题 在本方案中用户 A 和 B 会话密钥的生成是基于Chebyshev多项式的半群特性,在身份认证过程中自动生成的,不需要依靠KDC来分发会话密钥。这样既解决了当用户很多时KDC分发密钥可能会遇到的瓶颈的问题,也解决了用户之间会话的安全性问题。因此,本文提出的方案更具有可操作性。

6 结束语

本文通过研究Chebyshev多项式的性质特点,提出了一种基于Chebyshev映射的公钥密码算法的身份认证方案[12]。这一方案引入了密态时钟,赋予时钟一身两职——认证和同步,克服了以前方案存在的重放攻击、中间人攻击等诸多缺点,在安全性上有了很大的提高。各项性能分析表明新方案是安全有效的。

参考文献:

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

(下转第1846页)

b) 否则协议的安全性依赖于 TLS 协议是否被 A 破坏。同样地可以获得 TLS 协议被 A 破坏的概率上限为

$$\mathrm{Succ}_{CS}^{\mathrm{NoInj}}(A,k) \leqslant \frac{2q^2}{2^{p3(k)}} + \frac{q^2}{2^{p1(k)}} + 4q\mathrm{Adv}_{\mathrm{PRF}}^{\mathrm{prf}}(k) + 3q\mathrm{Adv}_{\mathrm{MAC\text{-}Enc}}^{\mathrm{cuf\text{-}cpa}}(k) + q\mathrm{Adv}_{(\mathrm{asEnc},\mathrm{asDec})}^{\mathrm{ind\text{-}cpa}}(k) + 3q\mathrm{Succ}_{\mathrm{hash}}^{\mathrm{coll}}(k) + q\mathrm{Succ}_{(\mathrm{Sig},\mathrm{Ver})}^{\mathrm{euf\text{-}cma}}(k)$$

最终可以得到以下结论：如果 PRF 是标准伪随机函数，(MAC-Enc，Dec-MAC) 具有 CUF-CPA 安全性，(asEnc，asDec) 具有 IND-CPA 安全性，hash 抗冲突，(Sig，Ver) 具有 EUF-CMA 安全性，那么协议 Π 提供定义 2 中所述安全的认证。事实上这些安全性假设在 TLS 协议规范下是有效的，因为协议规定的 RSA 加密 (PKC#1 或 RSA-OAEP) 已证在 ROM 下具有 IND-CPA 安全性[11]，协议规定的 RSA 签名 (PKCS#1 或 RSA-PSS) 已证在 ROM 下具有 EUF-CMA 安全性[12]；另外 Krawczyk[13] 已证明了 TLS 中的先 MAC 再加密结构具有 CUF-CPA 安全性。

4 结束语

基于浏览器的认证由于其广泛性和脆弱性成为了多种攻击的目标。本文介绍和分析了一种基于浏览器的联合身份管理的认证协议，对用户作最弱的安全性假设：不能理解服务器证书，仅通过容易识别的指示来评估网页，但是能够识别人类可感知认证码，并能够使用某种线下安全认证方法，包括动态密码令牌、外接安全证书等。协议加强浏览器的安全模型，通过实现 SLSO 策略加强对服务器端的认证，同时将安全令牌与客户端公钥证书进行绑定，确保客户端的合法性。最后分析了协议的安全性，证明了协议在 DOM 攻击下能够提供安全的认证。

参考文献：

[1] KORMANN D，RUBIN A. Risks of the passport single sign on protocol [J]. Computer Networks，2000，33(6)：51-58.

[2] GROβ T. Security analysis of the SAML single sign on browser/artifact profile[C]//Proc of the 19th Annual Computer Security Applications Conference. Washington DC：IEEE Computer Society，2003：298.

[3] GAJEK S，SCHWENK J，STEINER M，*et al*. Risks of the CardSpace protocol[C]//Proc of the 12th International Conference on Information Security. Berlin：Springer-Verlag，2009：278-293.

[4] CHEN X，GAJEK S，SCHWENK J. On the insecurity of Microsoft's identity metasystem CardSpace，Horst Görtz Institute for IT Security technical report HGI TR-2008-003 [R]. Bochum：Ruhr-Universität，2008.

[5] BRUEGGER B P，HUHNLEIN D，SCHWENK J. TLS-Federation：a secure and relying-party-friendly approach for federated identity mana-gement[C]//Proc of Special Interest Group on Biometrics and Electronic Signatures. 2008：93-104.

[6] KOHLAR F，SCHWENK J，JENSEN M，*et al*. On cryptographically strong bindings of SAML assertions to transport layer security[J]. International Journal of Mobile Computing and Multimedia Communications，2011，3(4)：20-35.

[7] GAJEK S，JAGER T，MANULIS M，*et al*. A browser-based Kerberos authentication scheme[C]//Proc of the 13th European Symposium on Research in Computer Security. Berlin：Springer-Verlag，2008：115-129.

[8] KARLOF C，SHANKAR U，TYGAR J D，*et al*. Dynamic pharming attacks and locked same-origin policies for Web browsers[C]//Proc of the 14th ACM Conference on Computer and Communications Security. New York：ACM Press，2007：58-71.

[9] GAJEK S，LIAO Li-jun，SCHWENK J. Stronger TLS bindings for SAML assertions and SAML artifacts[C]//Proc of ACM Workshop on Secure Web Services. New York：ACM Press，2008：11-20.

[10] SHOUP V. Sequences of games：a tool for taming complexity in security proofs[EB/OL]. (2004-10-20). http：/eprint. iacr. olrg/2004/332. pdf.

[11] SHOUP V. OAEP reconsidered[J]. Journal of Cryptology，2002，15(4)：223-249.

[12] JONSSON J. Security proofs for the RSA-PSS signature scheme and its variants [EB/OL]. (2001-11-23). http：//eprint. iacr. org/2001/053. pdf.

[13] KRAWCZYK H. The order of encryption and authentication for protecting communications (or：how secure is SSL?)[C]//Proc of the 21st Annual International Cryptology Conference on Advances in Cryptology. London：Springer-Verlag，2001：310-331.

(上接第 1842 页)

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

[3] XIAO Di，LIAO Xiao-feng，DENG Shao-jiang. A novel key agreement protocol based on chaotic maps[J]. Information Science，2007，177(3)：1136-1142.

[4] HAN S. Security of a key agreement protocol based on chaotic maps [J]. Chaos，Solitons，and Fractals，2008，38(3)：764-768.

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

[6] WANG Da-hu，HU Zhi-guo，TONG Zao-jing，*et al*. An identity authentication system based on Chebyshev polynomials[C]//Proc of the 1st International Conference on Information Science and Engineering. 2009：26-28.

[7] ZHAO Geng，LU Fang-fang. Security of several public key algorithms chaos-based proposed recently[C]//Proc of International Conference on Communication. [S. l]：IEEE Press，2006：1573-1576.

[8] 刘亮，刘云，宁红宙. 公钥体系中 Chebyshev 多项式的改进[J]. 北京交通大学学报，2005，29(5)：56-60.

[9] KOCAREV L，MAKRADULI J，AMATO P. Public-key encryption based on Chebyshev polynomials[J]. Circuits，Systems，and Signal Processing，2005，24(5)：497-517.

[10] 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.

[11] 赵耿，闫慧，童宗科. 基于 Chebyshev 多项式的公钥密码算法的研究[J]. 计算机工程，2008，34(24)：137-139.

[12] 郝舒欣，赵耿，徐刚，等. 基于 Chebyshev 多项式的身份认证方案的研究[J]. 计算机应用与软件，2012，29(1)：70-73.