基于有限域上 Chebyshev 多项式的密钥协商方案*

赵 耿[1], 孙锦慧[1,2], 赵 菲[1,2]
(1. 北京电子科技学院, 北京 100070; 2. 西安电子科技大学 通信工程学院, 西安 710071)

摘 要: 利用传统 RSA 算法和有限域上离散对数问题,提出一种新的基于混沌映射的密钥协商方案。该方案基于有限域上 Chebyshev 多项式良好的半群特性,运用 RSA 算法巧妙地隐藏通信双方产生的有限域上的 Chebyshev 多项式值,从而避免了以往的种种主动攻击,保证了密钥协商的安全;同时,该密钥协商方案还实现了身份认证功能。理论分析和软件实现证明了该方案的可行性、正确性和安全性。

关键词: 密钥协商; RSA 算法; Chebyshev 多项式; 混沌映射; 半群特性; 身份认证
中图分类号: TN915 **文献标志码**: A **文章编号**: 1001-3695(2012)10-3794-03
doi:10.3969/j.issn.1001-3695.2012.10.049

Key agreement scheme based on Chebyshev polynomials over finite fields

ZHAO Geng[1], SUN Jin-hui[1,2], ZHAO Fei[1,2]
(1. *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*; 2. *Institute of Telecommunication Engineering*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: This paper proposed an improved chaotic map-based key agreement scheme based on RSA algorithm and discrete logarithm on finite fields. At the base of the good properties of Chebyshev polynomials, the scheme utilized the traditional RSA algorithm to forge the Chebyshev polynomial on finite fields and thus ensured the safe of secret key by preventing the kinds of active attacks. Besides, the scheme had the function of identity authentication. At last the theory analysis and experimental results prove the feasibility, correctness, and security of the scheme.

Key words: key agreement; RSA algorithm; Chebyshev polynomials; chaotic map; semi-group property; identity authentication

最近几十年,混沌分组密码被广泛研究,但混沌公钥密码却很少被研究,密钥协商协议则是更少被人关注。混沌系统具有一些良好的特性,如对初始条件的敏感依赖性、伪随机性和遍历性等。这些特性具有很好的混淆和扩散作用,这正是密码学所需要的。在混沌公钥系统中包含两个密钥,即公钥和私钥,掌握其中一个,通过计算得到另一个是不可行的。通信各方要进行保密通信,必须先进行密钥协商。

Kocarev 等人[1]早已提出了一种基于 Chebyshev 混沌映射的公钥加密体制,这种体制主要是利用 Chebyshev 混沌映射的半群特性。之后,Bergamo 等人[2]很快就发现文献[1]提出的加密体制是不安全的。由于 Chebyshev 多项式的强周期性,敌手在不知道私钥的情况下也可以容易地从一些密文中恢复出明文。Bose[3]于 2005 年提出了一种基于多混沌系统的公钥加密方案,通信双方在公开信道中传输选择函数 $h(x,k)$ 实现密钥协商;文献[4]指出了该加密系统的弱点,并提出了具体的攻击方法。Xiao 等人[5]后来也利用 Chebyshev 混沌映射的半群特性提出了一种新的密钥协商方案,文献[6]针对文献[5]给出了两种攻击方法,文献[7]提出了另外一种改进的密钥协商协议,还增加了身份认证功能。另外,文献[8]提出了一种基于口令的密钥协商协议,但要求时钟同步,后来文献[9]提出了改进版本,在有无时钟同步的情况下都成立。在以上研究的基础上,本文提出了一种新的基于 Chebyshev 混沌映射的密钥协商方案。

1 有限域上 Chebyshev 多项式

1.1 Chebyshev 多项式的定义及其性质

定义 1 n 维 Chebyshev 多项式 $T_n(x):[-1,1]\to[-1,1]$ 定义为

$$T_n(x)=\cos(n\arccos(x)) \tag{1}$$

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

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

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

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

当 $n\geq 2$ 时,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

$$\mu(x)\,\mathrm{d}x=\frac{\mathrm{d}x}{\pi\sqrt{1-x^2}} \tag{3}$$

n 维 Chebyshev 多项式的 Lyapunov 指数为 $\lambda=\ln n$。当 $n=2$ 时,Chebyshev 多项式即为 Logistic 映射。

通过三角变换可以看出,这两种定义是等价的。

Chebyshev 多项式具有一个重要的特性,叫做半群特性,表示为

收稿日期: 2012-03-20; **修回日期**: 2012-04-30 **基金项目**: 国家自然科学基金资助项目(61170037)

作者简介: 赵耿(1964-),男,四川广元人,教授,主要研究方向为混沌密码理论及其应用、计算机信息安全及保密(zg@besti.edu.cn);孙锦慧(1985-),女,硕士研究生,主要研究方向为混沌公钥、信息安全;赵菲(1986-),女,硕士研究生,主要研究方向为网络通信.

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

由半群性质可知 Chebyshev 多项式映射合成可转换为

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

所以有式(6)成立:

$$T_m(T_n(x)) = T_{m\cdot n}(x) = T_n(T_m(x)) \quad n,m\in Z \tag{6}$$

1.2　有限域上 Chebyshev 多项式

由 Chebyshev 多项式的定义可知,Chebyshev 多项式 $T_n(x)$ 的定义域和值域都在$[-1,1]$区间上。由于 Chebyshev 多项式 $T_n(x)$ 是代数多项式,因此,可以很容易地把 Chebyshev 多项式的定义域扩展到实数域和有限域上。

因此,将式(2)扩展到有限域 Z_P 上(P 为素数),则在有限域 $x\in Z_P$ 上,Chebyshev 多项式可定义如下。

定义 3　令 $n\in Z^+$,变量 $x\in Z_P$,则 Chebyshev 多项式 $T_n(x):Z_P\to Z_P$ 的递归关系定义为

$$T_n(x)\equiv(2xT_{n-1}(x)-T_{n-2}(x))\bmod P \quad n\geqslant 2 \tag{7}$$

且有 $T_0(x)\equiv 1(\bmod P)$,$T_1(x)\equiv x(\bmod P)$。

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

由上面的定义可知,有限域 Z_P 上的 Chebyshev 多项式的前几项表示如下:

$$T_0(x)\equiv 1(\bmod P),T_1(x)\equiv x(\bmod P),T_2(x)\equiv(2x^2-1)(\bmod P)$$
$$T_3(x)\equiv(4x^3-3x)(\bmod P),T_4(x)\equiv(8x^4-8x^2+1)(\bmod P),\cdots$$

把 Chebyshev 多项式扩展到实数域 R 上后,式(4)依然成立,即 Chebyshev 多项式在实数域 R 上仍符合半群特性,所以在整数环 Z 上也符合半群特性。

因为 $T_n(x)$ 是代数多项式,所以有式(8)成立。

$$T_n(x)(\bmod P) = T_n(x(\bmod P))(\bmod P) \tag{8}$$

由式(6)和(8)可得到在有限域 Z_P 上 Chebyshev 多项式的半群特性的表达式为

$$T_n(T_m(x)\bmod P)\bmod P = T_m(T_n(x)\bmod P)\bmod P = T_{n\cdot m}(x)\bmod P =$$
$$T_n(T_m(x))\bmod P = T_m(T_n(x))\bmod P = T_{n\cdot m}(x)\bmod P \quad n,m\in Z_P \tag{9}$$

2　基于有限域上 Chebyshev 多项式的密钥协商方案

该密钥协商方案利用 RSA 算法,并结合有限域上 Chebyshev 多项式的半群特性来实现双方之间的密钥交换。该方案的安全性不仅具有大数因式分解的难度,还充分利用了有限域 Z_P 上 Chebyshev 多项式 $T_n(x)$ 计算的单向性。因此该方案还依赖于计算有限域上离散对数的难度。密钥协商的工作流程如图 1 所示。

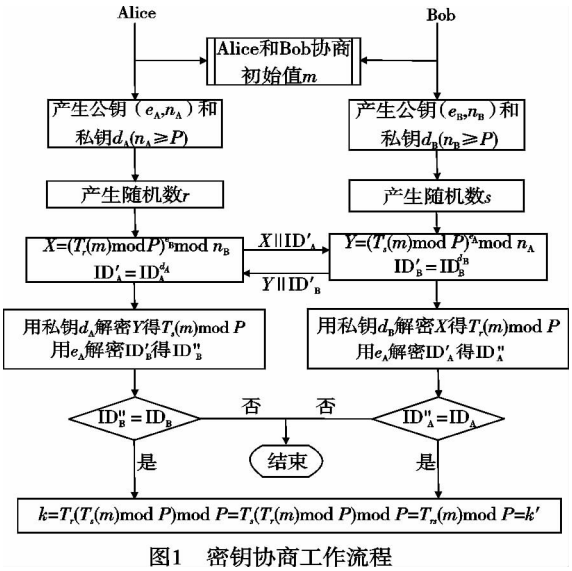

图1　密钥协商工作流程

a) Alice 和 Bob 共同协商一个随机整数 m 作为 Chebyshev 多项式 $T_n(x)$ 的初始值。

b)在有限域 Z_P 上,Alice 利用 RSA 算法产生自己的公钥(e_A,n_A)和私钥 d_A,其中 $n_A\geqslant P$,具体步骤如下:

(a)随机选取两个大素数 p_A 和 q_A,要求两数差值不能过大或过小,比特位相当。

(b)计算模 $n_A=p_Aq_A$ 和 Euler 函数 $\varphi(n_A)$。因为在 RSA 算法中,要求明文取值要小于模数 n_A,在此方案中,有限域上 Chebyshev 多项式的值即相当于 RSA 算法中的明文,而该值属于区间$[0,P]$,故要求 $n_A\geqslant P$。

(c)选取加密密钥 e_A 并用扩展 Euclid 算法求出满足 $e_Ad_A\equiv 1(\bmod \varphi(n_A))$的解密密钥 d_A。

这样就产生了 Alice 的公钥(e_A,n_A)和私钥 d_A。

c)与步骤 b)一样,Bob 利用同样的方法,在有限域 Z_P 中生成自己的公钥(e_B,n_B)和私钥 d_B,并确保 $n_B\geqslant P$。

d) Alice 选取一个随机数 r,计算有限域 Z_P 上 Chebyshev 多项式的值 $T_r(m)\bmod P$,然后利用 Bob 的公钥对其进行加密处理,记做 X,用公式表示为 $X=(T_r(m)\bmod P)^{e_B}\bmod n_B$;用私钥对自己的身份 ID 加密,记做 ID'_A,则 $ID'_A=ID_A^{d_A}\bmod n_A$,然后把 $X\|ID'_A$ 发送给 Bob。

e)与步骤 d)一样,Bob 选取一个随机数 s,计算有限域 Z_P 上 Chebyshev 多项式的值 $T_s(m)\bmod P$,然后利用 Alice 的公钥对其进行加密处理,记做 Y,用公式表示为 $Y=(T_s(m)\bmod P)^{e_A}\bmod n_A$;用私钥对自己的身份 ID 加密,记做 ID'_B,则 $ID'_B=ID_B^{d_B}\bmod n_B$,然后把 $Y\|ID'_B$ 发送给 Alice。

f) Alice 用自己的私钥 d_A 解密 Y 得到 $T_s(m)\bmod P$,用 Bob 的公钥 e_B 解密 ID'_B 得到 ID''_B,用公式表示为

$$T_s(m)\bmod P = Y^{d_A}\bmod n_A = ((T_s(m)\bmod P)^{e_A})^{d_A}\bmod n_A =$$
$$(T_s(m)\bmod P)^{e_Ad_A}\bmod n_A = T_s(m)\bmod P$$
$$ID''_B = (ID'_B)^{e_B}\bmod n_B = (ID_B^{d_B})^{e_B}\bmod n_B = (ID_B)^{d_Be_B}\bmod n_B = ID_B$$

这样 Alice 就确认了 Bob 的身份。

g) Bob 用自己的私钥 d_B 解密 X 得到 $T_r(m)\bmod P$,用 Alice 的公钥 e_A 解密 ID'_A 得到 ID''_A,用公式表示为

$$T_r(m)\bmod P = X^{d_B}\bmod n_B = ((T_r(m)\bmod P)^{e_B})^{d_B}\bmod n_B =$$
$$(T_r(m)\bmod P)^{e_Bd_B}\bmod n_B = T_r(m)\bmod P$$
$$ID''_A = (ID'_A)^{e_A}\bmod n_A = (ID_A^{d_A})^{e_A}\bmod n_A = (ID_A)^{d_Ae_A}\bmod n_A = ID_A$$

这样 Bob 就确认了 Alice 的身份。

h) Alice 和 Bob 即可计算出共享的密钥:

$$k = T_r(T_s(m)\bmod P)\bmod P =$$
$$T_s(T_r(m)\bmod P)\bmod P = T_{rs}(m)\bmod P = k'$$

3　软件实现与可行性分析

3.1　可行性分析

该方案的实现主要涉及两个算法,即 RSA 算法和有限域上 Chebyshev 多项式 $T_n(x)$ 函数值的计算。RSA 算法已得到广泛应用,因此软件实现比较简单;而有限域上 Chebyshev 多项式 $T_n(x)$ 因为阶数较高,误差也会比较大,不能用定义或者递归数列直接计算,必须利用半群特性来降低迭代的次数。

设 Chebyshev 多项式的阶数为

$$s = s_1^{k_1}s_2^{k_2}\cdots s_i^{k_i}$$

那么　$T_s(m)\bmod P = \underbrace{T_{s_1}(\cdots T_{s_1}}_{k_1}\cdots\underbrace{T_{s_i}(\cdots T_{s_i}}_{k_i}(m)))\bmod P$

因此,计算 $T_s(x) \bmod P$ 只需要 $k_1 + k_2 + \cdots + k_i$ 次迭代即可。把 s 分解成 k_i 的乘积很难,但是已知 k_i 构造 s 却很简单。

第二种方法。因为 $T_{2n}(x) \bmod P = T_2(T_n(x)) \bmod P$, $T_{2(n+1)}(x) \bmod P = (2T_{n+1}(x)T_n(x) - x) \bmod P$,所以有

$$T_0 = 1; T_1 = x; T_n(x) = \begin{cases} 2T_{\frac{n}{2}}^2(x) - 1, & n \text{ 是偶数} \\ 2T_{\frac{n-1}{2}}(x)T_{\frac{n+1}{2}}(x) - x & n \text{ 是奇数} \end{cases}$$

由文献[10]可知,当 n 的取值因子越多,其效率会越好。确切地讲,在 2048 bit 下,s、r 的上界是 2^{970}。事实上,新提出方案的安全性不单依赖于多项式求次数问题的困难性,还把安全性转移到 RSA 算法的安全性上,所以完全可以不对 s 和 r 取很大的值,这样就进一步提高了协议的可行性。

3.2 举例说明密钥协商过程

首先,Alice 和 Bob 协商 Chebyshev 多项式的初始值 $m = 13$,有限域 $Z_P = Z_{2281}$,接下来简单的几步便可完成密钥协商。

a) Alice 选取 $p_A = 41$, $q_A = 59$,则 $n_A = p_A q_A = 2419 > p$, $\varphi_A = (p_A - 1)(q_A - 1) = 2320$,选取加密密钥 $e_A = 27$,则 Alice 的公钥为 $(e_A, n_A) = (27, 2419)$,私钥为 $d_A = 1203$。

Bob 选取 $p_B = 37$, $q_B = 67$,则 $n_B = p_A q_A = 2479 > p$, $\varphi_B = (p_B - 1)(q_B - 1) = 2376$,选取加密秘钥 $e_B = 41$,则 Bob 的公钥为 $(e_B, n_B) = (41, 2479)$,私钥为 $d_B = 1217$。

b) Alice 选取随机数 $r = 12$,计算 X 并发给 Bob。Bob 选取随机数 $s = 18$,计算 Y 并发给 Alice。

$$X = (T_r(m) \bmod P)^{e_B} \bmod n_B =$$
$$(T_{12}(13) \bmod 2281)^{41} \bmod 2479 = 1419^{41} \bmod 2479 = 1256$$
$$Y = (T_s(m) \bmod P)^{e_A} \bmod n_A =$$
$$(T_{18}(13) \bmod 2281)^{27} \bmod 2419 = 489^{27} \bmod 2419 = 875$$

c) Alice 用自己的私钥解密 Y 计算得到

$$Y' = Y^{d_A} \bmod n_A = 875^{1203} \bmod 2419 = 489$$

Bob 用自己的私钥解密 X 计算得到

$$X' = X^{d_B} \bmod n_B = 1256^{1217} \bmod 2479 = 1419$$

d) Alice 计算协商密钥:

$$k_A = T_r(T_s(m) \bmod P) \bmod P = T_{12}(489) \bmod 2281 = 2156$$

Bob 计算协商密钥:

$$k_B = T_s(T_r(m) \bmod P) \bmod P = T_{18}(1419) \bmod 2281 = 2156$$

由此可得 $k_A = k_B = k$,这样 Alice 和 Bob 就实现了密钥协商。

4 性能分析

该密钥协商方案是对有限域上 Chebyshev 多项式采用 RSA 算法加/解密,因此该方案的安全性首先是基于大数分解的难题;其次 Chebyshev 多项式 $T_n(x)$ 的阶数 n 是随机产生的,故它的安全性还基于有限域上求离散对数的困难问题。综合可知,该方案有极高的安全性。本文针对新提出的密钥协商方案还作出了以下几方面的性能分析。

1)有效抵抗 Bergamo 等人的攻击

Bergamo 等人的攻击主要基于两点:a)攻击者掌握了 x、$T_r(x)$、$T_s(x)$;b)Chebyshev 多项式的强周期性导致不同次数的 Chebyshev 多项式通过一个共同点。在提出的方案中,攻击者只能得到 x、P;不仅如此,密钥协商中采用 RSA 算法把 $T_r(x)$ 和 $T_s(x)$ 加密隐藏,除了通信双方,其他人无从知道解密密钥。因此,Bergamo 等人的攻击方法能够得到有效的避免。

2)防窜改攻击

在第 d)步,Alice 用 Bob 的公钥对 Chebyshev 多项式值和其身份 ID 加密后传给 Bob,因此,当 Bob 收到并解密后应该得到 Alice 的 ID 号。如果发现结果有误或偏差,说明密文被窜改或更换,Bob 立即停止协商。同理,在第 e)步,Alice 也可以发现密文是否已经被窜改,如果是,则停止协商。

3)身份认证

在第 f)步,Alice 收到 $Y \parallel ID'_B$ 后,用 Bob 的公钥解密得到 Bob 的身份 ID,从而验证正在与 Bob 通信。这是因为只有先用 Bob 私钥加密其身份 ID,然后用 Bob 的公钥解密才能得到,而私钥只有 Bob 自己知道。同理,Bob 可以验证 Alice 的身份。

4)效率分析

该密钥协商方案巧妙地将 Chebyshev 多项式的安全转移到 RSA 算法上,所以完全可以不对 s 和 r 取很大的值,而且整个过程在 Alice 和 Bob 两端分别并行地执行,从而可以大大缩短时间,提高系统运行效率。

5 结束语

本文针对目前提出的基于混沌的密钥协商方案的诸多安全问题,提出了一种新的基于有限域上 Chebyshev 混沌映射的密钥协商方案。由于利用 RSA 算法隐藏了 Chebyshev 多项式的值,使得传统的攻击方法相应地失效。该方案在实现密钥协商的同时增加了身份认证功能,通过实验证明了该方案具有很好的有效性和可行性,对混沌公钥的推广应用具有重要意义。

参考文献:

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

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

[3] BOSE R. Novel public key encryption technique based on multiple chaotic systems [J]. Physical Review Letters, 2005, 95(9): 098702-098705.

[4] WANG Kai, PEI Wen-jiang, ZHOU Li, *et al*. Security of public key encryption technique based on multiple chaotic systems[J]. Physics Letters A, 2006, 360(2): 259-262.

[5] 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.

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

[7] WANG Xing-yuan, ZHAO Jang-feng. An improved key agreement protocol based on chaos[J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(12): 4052-4057.

[8] CHANG E, HAN Song. Using passphrase to construct key agreement, CBS-IS[R]. Perth: Curtin University of Technology, 2006.

[9] HAN Song, CHANG E. Chaotic map based key agreement with/out clock synchronization [J]. Chaos, Solitons & Fractals, 2009, 39(3): 1283-1289.

[10] FAN Lei, XU C X, LI J H. Deniable authentication protocols based on Deffie-Hellman algorithm [J]. IEEE Lectronics Letters, 2002, 38(4): 705-706.