文章编号:1671 - 6833(2014)02 - 0050 - 05

基于有限域上 Chebyshev 多项式的 Diffie-Hellman 密钥协商算法

徐 刚,丁松阳,张墨华

(河南财经政法大学 计算机与信息工程学院,河南 郑州 450002)

摘 要:为了能够利用混沌系统构造出运行速度快、安全性高的密钥协商算法,通过研究一种已提出的基于 Chebyshev 多项式的密钥协商算法,利用有限域上 Chebyshev 多项式的半群性和消息认证码,给出了一种改进的密钥协商算法,该算法能完成通信双方的身份认证和确认会话密钥的一致性;通过对算法的密码分析,该算法能够快速实现、安全性更高.

关键词:Chebyshev 多项式;有限域;Diffie-Hellman 密钥协商算法;消息认证码

中图分类号:TP918.1;TP309.7 **文献标志码**:A doi:10.3969/j.issn.1671 - 6833.2014.02.012

0 引言

混沌系统以其对初始条件的敏感性、伪随机性和遍历性等与密码学类似的特性[1],近年来被研究者广泛应用于现代密码学的研究中,提出了很多基于混沌的密码算法,但是基于混沌的公钥算法、身份认证和密钥协商算法[2-4]则相对较少.

基于混沌的密钥协商(密钥交换)算法使用公钥技术生成会话密钥,能够解决在使用对称加密算法中通信双方的密钥分配问题,也是通信双方在公开信道协商会话密钥的主要方法.生成的会话密钥在特殊的通信中只使用一次,是单独的对称密钥,因此,通信双方对密钥协商算法的安全性和运行效率都有很高的要求.利用混沌系统构造的密钥协商算法不仅具有很高的安全性,而且相比于传统的密钥协商算法运行速度更快,应用范围也更为广泛[4].

Kocarev 和 Tasev[5]在 2003 年利用 Chebyshev 多项式的半群性,提出了一种公钥加密算法;Bose 以安全信道上一系列线性函数为工具,给出了一种多混沌系统的密钥协商算法[6],随后这种算法的弱点被发现并被成功攻破[7],出现了一种改进的多混沌密钥交换算法;2007 年肖迪、廖晓峰等人提出一种新的密钥协商算法[8],但 Han 用两种攻击方法说明该算法是不安全的[9];2010 年文献[10]总结了前期研究成果中普遍存在的问题,如不能提供相互认证、不能抵抗重放或中间人攻击等,并在解决这些问题的基础上,通过时间戳的应用,提出了一种改进的密钥协商算法.

笔者通过对文献[10]提出算法的分析,去掉了其中的冗余计算和时间戳,结合一种有限域 Chebyshev 多项式的快速计算方法,提出了一种改进的 Diffie-Hellman 密钥协商算法,算法利用 Chebyshev 多项式的半群性产生会话密钥,引入消息认证码(Message Authentication Code,MAC)能够使通信的双方确认会话密钥的一致性,并完成相互之间的身份认证,密码分析表明该算法能快速实现,具有很好的安全性.

1 有限域上 Chebyshev 多项式

n 维 Chebyshev 多项式是一种典型的混沌映射,已经被广泛地应用于混沌公钥密码、密钥协商及身份认证等领域中,将这种代数多项式的定义域扩展到有限域上,令 $n \in Z^+$,p 为素数,变量 $x \in F_p$,则多项式 $T_n(x):F_p \to F_p$ 的递归关系为

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

式中:$T_0(x) = 1 \bmod p$;$T_1(x) = x \bmod p$.

经过迭代可得有限域 F_p 上的 Chebyshev 多项式

$$T_0(x) = 1 \bmod p,$$

收稿日期:2013 - 12 - 24;**修订日期**:2014 - 01 - 14

基金项目:国家自然科学基金资助项目(61170037,61309033,11202068);河南省基础与前沿技术研究计划项目(13230 0410438)

作者简介:徐刚(1979 -),男,河南南阳人,河南财经政法大学讲师,博士,主要从事信息安全方面的研究,E-mail:xgtony@ huel. edu. cn.

$T_1(x) = x \bmod p$,

$T_2(x) = (2x^2 - 1) \bmod p$,

$T_3(x) = (4x^3 - 3x) \bmod p$,

$T_4(x) = (8x^4 - 8x^2 + 1) \bmod p \cdots\cdots$

多项式的计算量与计算复杂度会随着迭代次数的递增成倍的增加,用系数矩阵的累乘运算来计算该多项式,可简化代数多项式迭代计算的复杂性,便于编程实现,这种矩阵迭代方法的关系式为

$$\begin{pmatrix} T_n(x) \\ T_{n+1}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix}^n \begin{pmatrix} T_0(x) \\ T_1(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix}^n \begin{pmatrix} 1 \\ x \end{pmatrix} \bmod p$$

或

$$\begin{pmatrix} T_{n-1}(x) \\ T_n(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix}^{n-1} \begin{pmatrix} T_0(x) \\ T_1(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ x \end{pmatrix} \bmod p, \quad (1)$$

这种算法的运算效率,取决于选择合适的方法计算矩阵的 n 次方,递推算法可以解决矩阵的高次方求解问题.

有限域上 Chebyshev 多项式仍是一个混沌映射,到目前为止,数学上仍然没有找到有限域 Chebyshev 多项式的反函数表达式,因此在已知 x 和 n 的情况下求 $T_n(x)$ 很容易,但是已知 x 和 $T_n(x)$ 时求 n 却异常困难,其求解的困难性与求离散对数的困难问题相当.

有限域上 Chebyshev 多项式在计算上具有的良好单向性与半群性,是其能够应用于混沌公钥密码、密钥协商等算法的基础.

2　现有密钥协商算法及其密码分析

文献[10]提出了一种基于 Chebyshev 多项式的密钥协商算法,但其存在的问题使得该算法很容易遭受密码攻击.(说明:此处删除了多余的说明性代号)

2.1　密钥协商算法描述

算法把 Trent 作为可信任的第三方,也可以是密钥分配中心(Key Distribution Center,KDC),会话开始之前,Trent 与会话的双方 Alice、Bob 已约定好各自的对称密码算法及其密钥,密钥协商算法如图 1 所示.

(1)Alice 首先选择一个大整数 r、素数 p 和任意数 x,利用 Cheybeshev 多项式计算 $T_r(x)$,然后 Alice 将 $A \| x \| p \| T_r(x)$ 发送给接收方 Bob,其中"‖"表示这些数据信息的连接.

(2)Bob 收到发来的消息后,发现是 Alice 要开展下一步的会话,Bob 生成一个时间戳 T_B、大整数 s 并计算 $T_s(x)$,Bob 利用其与 Trent 之间的密钥 TB 完成加密 $E_{TB}(A \| x \| p \| T_B \| T_s(x))$,与 B 一起发送给 Trent;这时,Bob 已经得到了与 Alice之间的会话密钥 $K = T_s(T_r(x))$.

(3)Trent 将收到的消息用密钥 TB 解密,确定会话的双方是 Alice 和 Bob,生成两个消息,一个是 Trent 用与 Alice 的密钥 TA 来加密的消息 $B \| x \| p \| T_B \| T_s(x)$,另一个是用密钥 TB 来加密的消息 $A \| T_B$;然后将生成的两个消息 $E_{TA}(B \| x \| p \| T_B \| T_s(x))$ 和 $E_{TB}(A \| T_B)$ 发送给 Alice,其中 T_B 是 Bob 生成的时间戳,用于会话中通信时效性的验证.

(4)Alice 收到消息解密,验证 x,p 是否与第(1)步发送给 Bob 的值相同,若不同则终止通信;若验证正确 Alice 得到了与 Bob 的会话密钥 $K = T_r(T_s(x))$,并给 Bob 发送两条消息:第一个是 Alice 从 Trent 那里得到的 $E_{TB}(A \| T_B)$,第二个是用会话密钥 K 加密的消息 $E_K(T_B \| T_s(x))$.

(5)Bob 得到 $E_{TB}(A \| T_B)$ 和 $E_K(T_B \| T_s(x))$ 后分别用密钥 TB 和 K 解密,验证 T_B 和 $T_s(x)$ 是否是自己在第(2)步给 Alice 发送的消息,若不正确则终止通信;若正确则 Bob 即可与 Alice 用会话密钥 K 进行会话.

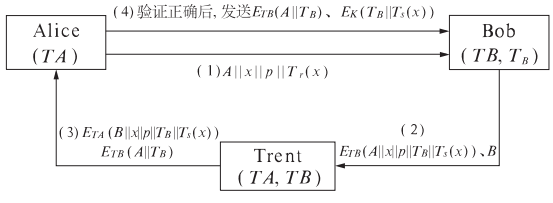

图 1　现有密钥协商算法

Fig. 1　The exist key agreement protocol

2.2　算法存在的问题

对于一个安全的密钥协商算法来说,通信双方相互确认会话密钥的一致性是非常重要的,但该算法 Alice 不能确定 Bob 计算出的会话密钥 K 是否与自己生成的会话密钥一致.

算法在第(2)步中 Bob 首先可计算出会话密钥 $K = T_s(T_r(x))$,并且第(5)步中由于 Bob 收到了 $E_K(T_B \| T_s(x))$ 并能够解密,所以 Bob 可以确定 Alice 的会话密钥 $K = T_r(T_s(x))$ 是正确的,与自己的一致,但算法没有把 Bob 生成的这个会话

密钥也发送给 Alice,Alice 就无法确认 Bob 生成的会话密钥是和自己的也是一致的.

算法的单方面的认证会导致严重的安全问题,若入侵者 Eve 能够干预到算法的通信中,就能实施非法修改的攻击,笔者给出如下一种针对这种算法的攻击方法

(a)在第(1)步中,Eve 拦截 Alice 所发送的消息 $A \| x \| p \| T_r(x)$;Eve 选择一个任意的实数 $\omega \in (-\infty, +\infty)$,计算 $T_\omega(x)$;Eve 用 $A \| x \| p \| T_\omega(x)$ 代替 $A \| x \| p \| T_r(x)$,把修改后的消息发送给 Bob;

(b)Bob 接收到消息 $A \| x \| p \| T_\omega(x)$ 后,计算会话密钥 $K^* = T_s(T_\omega(x))$,然后将消息 $E_{TB}(A \| x \| p \| T_B \| T_s(x))$ 与 B 一起发送给 Trent;

(c)Trent 解密后再将生成的 $E_{TA}(B \| x \| p \| T_B \| T_s(x))$ 和 $E_{TB}(A \| T_B)$ 发送给 Alice;

(d)Alice 得到消息解密后验证 x,p 都是正确的,然后计算出会话密钥 $K = T_r(T_s(x))$,给 Bob 发送两条消息 $E_{TB}(A \| T_B)$ 和 $E_K(T_B \| T_s(x))$;

(e)Bob 用 TB 解密后验证时间戳 T_B 是正确的,但是在用会话密钥 $K^* = T_s(T_\omega(x))$ 解密 $E_K(T_B \| T_s(x))$ 时得到的 $T_s(x)$ 与之前的不一样,Bob 就会终止当前的会话,并认为 Alice 没有生成正确的会话密钥.

通信双方密钥协商失败的主要原因是 Eve 把 $T_r(x)$ 修改为 $T_\omega(x)$,导致 Bob 生成的密钥 K^* 与 Alice 生成的会话密钥不一致,而算法余下的步骤(d)、(e)中,没有为 Bob 提供方法来确认生成的会话密钥与 Alice 会话密钥的一致性,即使会话密钥错误 Bob 也未能及时发现,可见该算法不能抵抗类似的攻击. 另外,算法在运用时间戳时,只需要由 Bob 来验证自己生成的时间戳,且时间戳需要在三方之间不断地传输,不可避免地要占用大量的存储空间,影响整个算法的运行效率. 算法使用对称密码算法的加密和解密各 5 次,存在很多冗余的计算.

3 改进的密钥协商算法

针对以上算法中存在的问题,笔者提出一种改进的密钥协商算法,首先给出一种特征值算法来提高有限域上 Chebyshev 多项式的计算效率;然后利用基于单向 Hash 函数的消息认证码 MAC,验证通信双方会话密钥的一致性并进行身份认证,以抵抗以上类似的攻击,提高安全性;算法舍弃原有算法中的对称密码算法和时间戳的运用,来提高整个算法的运行速度.

3.1 有限域 Chebyshev 多项式的特征值算法

Chebyshev 多项式的计算是密钥协商算法主要的运算,计算的方法、速度及要求的数据存储量都直接影响整个算法的效率,研究者提出了很多种快速实现的方法. 为了提高计算效率,笔者在 Chebyshev 多项式矩阵迭代算法的基础上,利用特征值算法来提高计算的效率,并用该算法证明了有限域 Chebyshev 多项式的半群性.

设 A 的特征值为 $\lambda_1, \lambda_2, \alpha_1, \alpha_2$ 是矩阵 A 的属于 λ_1, λ_2 的特征向量,由式子(1),$\boldsymbol{A} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix}$ 为非奇异矩阵,则 $\boldsymbol{A}$ 的特征多项式为

$$f(\lambda) = |\lambda I - \boldsymbol{A}| = \lambda^2 - 2x\lambda + 1, \tag{2}$$

其中 $|\cdot|$ 是行列式的值;可得特征值

$$\lambda_1 = x + \sqrt{x^2 - 1}, \lambda_2 = x - \sqrt{x^2 - 1},$$

其中 $\sqrt{x^2 - 1} \in F_p$.

对于 $\sqrt{x^2 - 1} \in F_p$ 文献[11]采用 *Legendre* 符号 L 做出了证实,当 $L = \left(\frac{x^2 - 1}{p}\right) = (x^2 - 1)^{\frac{p-1}{2}} = 0$ 或 1 时,$\sqrt{x^2 - 1} \in F_p$ 成立. 此外,选取合适的数 p,如当 $p = 3 \bmod 4$ 或 $p = 5 \bmod 8$,只需经过几步有限域的基本运算,即可完成 $\sqrt{x^2 - 1}$ 的计算.

由特征值计算两个特征向量分别为

$$\alpha_1 = \begin{pmatrix} 1 \\ x + \sqrt{x^2 - 1} \end{pmatrix}, \alpha_2 = \begin{pmatrix} 1 \\ x - \sqrt{x^2 - 1} \end{pmatrix},$$

将两个列向量组成一个矩阵,矩阵 $\boldsymbol{A}$ 的 n 次方可以表示为

$$\begin{aligned} \boldsymbol{A}^n &= (\alpha_1 \alpha_2) \begin{pmatrix} \boldsymbol{\lambda}_1 & 0 \\ 0 & \boldsymbol{\lambda}_2 \end{pmatrix} (\alpha_1 \alpha_2)^{-1} \\ &= \frac{1}{\lambda_2 - \lambda_1} \begin{pmatrix} \boldsymbol{\lambda}_1^n \boldsymbol{\lambda}_2 - \boldsymbol{\lambda}_1 \boldsymbol{\lambda}_2^n & \boldsymbol{\lambda}_2^n - \boldsymbol{\lambda}_1^n \\ \boldsymbol{\lambda}_1^{n+1} \boldsymbol{\lambda}_2 - \boldsymbol{\lambda}_1 \boldsymbol{\lambda}_2^{n+1} & \boldsymbol{\lambda}_2^{n+1} - \boldsymbol{\lambda}_1^{n+1} \end{pmatrix}, \end{aligned} \tag{3}$$

将其代入表达式

$$\begin{aligned} T_n(x) &= T_n\left(\frac{\lambda_1 + \lambda_2}{2} \bmod p\right) \\ &= \frac{\lambda_1^n + \lambda_2^n}{2} \bmod p \\ &= \frac{(x + \sqrt{x^2 - 1})^n + (x - \sqrt{x^2 - 1})^n}{2} \bmod p. \end{aligned} \tag{4}$$

算法利用矩阵特征值与特征向量的特点,结合快速模乘方算法的应用,给出了适合于 Cheby-

shev 多项式的计算方法[12],在选取合适的参数的情况下,比之前多项式计算的常规算法更加快速,便于实现. 采用这种算法,很容易证明有限域 Chebyshev 多项式的半群性:

定理　对任意的 $r,s\in Z^+$ 和 $x\in F_p$,都有等式 $T_r(T_s(x))=T_{rs}(x)=T_{sr}(x)=T_s(T_r(x))$ 成立.

证明　由式(2)可知,$\lambda_1+\lambda_2=2x \bmod p$,$\lambda_1\lambda_2=1 \bmod p$,则

$$T_r(T_s(x))=\frac{\eta_1{}^r+\eta_2{}^r}{2} \bmod p, \tag{5}$$

式中:η_1,η_2 为 $T_r(T_s(x))$ 的特征值,则有 $\eta_1+\eta_2=2T_s(x) \bmod p$,$\eta_1\eta_2=1 \bmod p$,因此,

$$\begin{aligned}&(\eta_1+\eta_1^{-1}) \bmod p=(\eta_1+\eta_2) \bmod p\\&=2T_s(x) \bmod p\ =(2\times\frac{\lambda_1^s+\lambda_2^s}{2}) \bmod p\\&=(\lambda_1^s+\lambda_2^s) \bmod p\\&=(\lambda_1^s+\lambda_1^{-s}) \bmod p.\end{aligned}$$

得 $\eta_1=\lambda_1^s$ 或 λ_1^{-s},代入式(5)得

$$\begin{aligned}&T_r(T_s(x))=T_{rs}(x)=\frac{\eta_1^r+\eta_2^r}{2} \bmod p\\&=\frac{\lambda_1^{rs}+\lambda_2^{rs}}{2} \bmod p,\end{aligned}$$

同理,$T_s(T_r(x))=T_{sr}(x)=\dfrac{\lambda_1^{sr}+\lambda_2^{sr}}{2} \bmod p$,所以 $T_r(T_s(x))=T_{rs}(x)=T_{sr}(x)=T_s(T_r(x))$ 成立.

证毕.

3.2　改进的密钥协商算法

改进的密钥协商算法引入的消息认证码,可以相互确认身份并验证会话双方会话密钥的一致性,改进的算法能既简化算法流程,又降低计算复杂度. 图 2 是改进的密钥协商算法.

(1) Alice 首先选择一个大整数 r、素数 p 和任意数 $x\in(-\infty,+\infty)$,计算 $T_r(x)$,然后 Alice 用密钥 *TA* 加密将 $E_{TA}(A\parallel B\parallel x\parallel p\parallel T_r(x))$ 发送给 Trent.

(2) Trent 解密后再用 *TB* 加密,将消息 $E_{TB}(A\parallel B\parallel x\parallel p\parallel T_r(x))$ 发送给 Bob.

(3) Bob 得到消息后解密,选取一个大整数 s 计算 $T_s(x)$,计算得到会话密钥 $K=T_s(T_r(x))$,用 $A,B,T_r(x)$ 计算用 K 生成的消息认证码 $MAC_B=h_K(A,B,T_r(x))$,Bob 将 $T_s(x)$ 和 MAC_B 发送给 Alice;消息认证码的使用,既能让 Alice 认证 Bob 的身份,又能互相确认会话密钥的正确性.

(4) Alice 收到消息后计算 $K=T_r(T_s(x))$ 和 $MAC'_B=h_K(A,B,T_r(x))$,验证是否与发送过来的 MAC_B 相等,若相等,说明通信的对方是 Bob 并且确认会话密钥 K 是正确的;随后 Alice 生成 $MAC_A=h_K(A,B,T_s(x))$ 发送给 Bob,否则终止会话.

(5) Bob 计算 $MAC'_A=h_K(A,B,T_s(x))$,与收到的 MAC_A 做验证,若相等,Bob 确认 Alice 的身份,并能确认 Alice 的会话密钥的是正确的;若不相等,则会话终止.

完成以上的密钥协商和身份认证后,Alice 和 Bob 就能通过会话密钥 K 来加密传输的消息,进行安全通信.

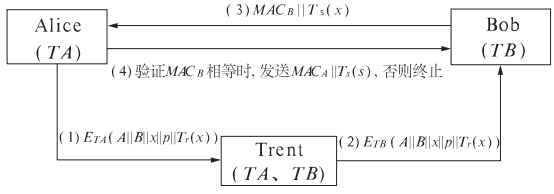

图 2　改进的密钥协商算法

Fig. 2　The improved key agreement protocol

4　安全性能分析

改进的密钥协商算法基于有限域上 Chebyshev 多项式,其求解的困难性与求离散对数的困难问题相当,保证了整个算法的安全性;同时消息认证码的引入,使得通信的双方能够验证会话密钥的一致性和进行相互的身份认证,克服了原有算法的弊端,可以抵抗密码分析.

(1) 重放攻击

重放攻击指攻击者侵入到通信系统里,窃取通信的内容,在下次的通信中冒充原发送者发送给接收者一个已接收过的信息,使接收者误以为是原发送者发送来的信息,来达到欺骗系统、冒充身份的目的.

算法中选取的随机大整数 r 与 s 在系统内的传输,使重放攻击失效. 除了 Alice,只有 Bob 能够将会话密钥和随机数 r,s 嵌入到消息认证码 $MAC_B=h_K(A,B,T_r(x))$ 中,对于 Alice 来说同样如此,所以改进的算法就不需要再使用时间戳抵抗重放攻击.

(2) 中间人攻击

中间人攻击指攻击者在发送方和接收方的通信中,伪装成通信的一个参与者,拦截、替代、修改传输的信息并能不被识破,这种攻击方法对于缺乏相互认证的算法很有效.

改进的密钥协商算法中,发送方和接收方使

用了2个密钥 TA 和 TB,这就使得攻击者无法获取有用的信息入侵到通信中;算法的第(4)步 Alice 可通过验证 MAC_B 判断收到的消息是否被替代或修改,Bob 在第(5)步中验证 MAC_A 来判断,因此,改进的算法能够有效地抵抗中间人攻击.

此外,原算法中使用5次对称密码算法的加密与解密,在改进算法中减少到了2次,改进的密钥协商算法计算量减少,处理速度更快,存储空间要求更小,运用有限域 Chebyshev 多项式算法,密钥的生成和选取也会更加灵活方便.

5 结论

笔者提出了一种改进的密钥协商算法,利用有限域 Chebyshev 多项式算法产生会话密钥,去除了文献[10]中算法中的时间戳和一些冗余计算,使用消息认证码实现相互认证和密钥一致性的验证,密码分析表明算法具有较高的安全性.另外,改进的算法存储空间和计算量都较小,应用在网络中对带宽要求低,可降低整个系统开销,适合用于物联网、云计算等端口间的密钥分配、协商与安全认证.

参考文献:

[1] 方洁,姜长生,邓玮. 混沌修正函数投影同步研究及其在保密通信中的应用[J]. 郑州大学学报:工学版,2011,5: 016.

[2] 陈宇,韦鹏程.基于实数域扩散离散 Chebyshev 多项式的公钥加密算法[J].计算机科学, 2011,38(10):121-122,165.

[3] 陈小松,孙一为.基于 Chebyshev 多项式的公钥系统[J].铁道学报,2013,35(1):77-79.

[4] 李智慧,崔毅东,金跃辉,等.有限域切比雪夫多项式的改进算法[J].北京邮电大学学报,2011,34(6):47-50,77.

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

[6] BOSE R. Novel public key encryption technique based on multiple chaotic systems[J]. Physical review letters, 2005, 95(9): 098702.

[7] WANG Kai, PEI Wen-jiang, ZHOU Liu-hua, et al. Security of public key encryption technique based on multiple chaotic system[J]. Physics letters A, 2006, 360(2): 259-262.

[8] 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.

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

[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] MENEZES A J, VAN OORSCHOT P C, Vanstone S A. Handbook of applied cryptography [M]. New York: CRC Press, 2010.

[12] MULLER S. On the Computation of square roots in finite fields [J]. Designs, Codes and Cryptography, 2004, 31(3): 301-312.

Diffie-Hellman Key Agreement Protocol Based on Chebyshev Polynomials over Finite Field

XU Gang, DING Song-yang, ZHANG Mo-hua

(College of Computer and Information Engineering, Henan University of Economics and Law, Zhengzhou 450002, China)

Abstract: In order to construct high speed and security key agreement protocol using chaotic system, we study one of the existing key agreement protocols based on Chebyshev polynomial, construct an improved key agreement protocol by utilizing the semi-group property of Chebyshev polynomials and message authentication code, which can complete the identity authentication between communication parties and confirm the consistency of the session key. The proposed key agreement protocol is efficient and secure, which is proved by the cryptanalysis.

Key words: Chebyshev polynomials, finite field, Diffie-Hellman key agreement protocol, message authentication code