

基于扩展混沌映射的认证密钥协商协议*

舒剑†

(江西财经大学电子商务系, 南昌 330013)

(电子科技大学计算机科学与工程学院, 成都 611731)

(2013年10月29日收到; 2013年11月21日收到修改稿)

近年来, 基于混沌映射和智能卡的认证密钥协商协议被相继提出. 然而, 防篡改读卡器使得这类协议的实现成本较高并且很难在实际中广泛应用. 另外, 基于混沌映射的数字签名方案需要很高的计算资源, 这使得依赖签名方案的公钥发布存在安全问题. 据此, 本文基于扩展混沌映射提出一种新的无智能卡的认证密钥协商协议. 新协议消除了公钥发布过程. 安全和性能分析表明, 新协议能抵抗各类攻击并且计算复杂度较低. 因此, 新协议更适合在实际环境中应用.

关键词: 混沌映射, 密钥协商, 智能卡, 数字签名

PACS: 05.45.Vx, 05.45.-a

DOI: 10.7498/aps.63.050507

1 引言

密钥协商协议使两方或多方用户生成一个安全的会话密钥. 共享的会话密钥可以为公开网络的安全通信提供保障.

混沌系统具有伪随机、遍历和对初始条件及参数的敏感依赖等特性. 这些性质具有扩散和混淆的作用, 这是设计密码体制所必须的条件, 因而混沌系统被广泛地应用于对称密码体制^[1-3]、哈希函数^[4,5]和流密码^[6,7]的设计. 近年来, 混沌系统被用来设计公钥密码体制^[8-11]. 基于混沌映射, Kocarev 等^[10]在2003年提出一种公钥加密方案. 随后, Xiao 等^[12]提出了一种完全基于混沌机制的可否认认证方案. 然而, Bergamo 等^[8]指出基于混沌映射的公钥密码体制是不安全的, 攻击者可以从通信双方的秘密通信中恢复明文. 为了抵抗文献^[8]中的Bergamo攻击, Xiao 等^[11]基于混沌映射和共享口令提出了一种新的密钥协商协议. Xiang 等^[13]指出文献^[11]中的协议不能抵抗窃取-验证攻击和离线猜测攻击, 因而仍旧不能抵抗Bergamo攻击. 基于混沌映射, Wang 等^[14]利用对称加密方

案提出一种高效的密钥协商协议. 为提高安全性, Tseng 等^[15]提出一种使用智能卡的基于混沌映射的密钥协商协议. Niu 等^[16]指出Tseng等的协议不能抵抗内部攻击者和不具有完美前向安全特性, 同时提出了一种改进方案. 然而, Yoon 等^[17]指出文献^[16]中的协议计算复杂度较高并且不能抵抗拒绝服务攻击. 为提高安全性, 研究者提出了不同的基于智能卡的密钥协商协议^[18-21]. 然而, 基于智能卡的方案需要添加额外的设备——读卡器. 在现实生活中, 防篡改读卡器并不是随处可见. 因此, 设计不使用智能卡的认证协议具有一定的实际意义. 2010年, Guo 等^[22]首先提出了不使用智能卡的基于混沌映射的密钥协商协议, 但协议不能抵抗离线字典猜测攻击. Gong 等^[23]也提出一种不使用智能卡的基于混沌映射的密钥协商协议, 协议的计算复杂度较低. 在基于智能卡的方案中, 服务器将公钥信息写入到用户的智能卡中, 则服务器不需要发布任何公钥信息. 文献中不使用智能卡的方案中, 服务器需要发布公钥信息. 由于基于混沌映射的签名方案难以实现或者实现的代价太高, 使得服务器发布公钥信息存在安全隐患. 基于混沌映射,

* 国家自然科学基金(批准号: 61163053)资助的课题.

† 通讯作者. E-mail: mikeschujian@jxufe.edu.cn

本文提出一种新的认证密钥协商协议. 新方案不使用智能卡, 并且服务器不需要发布公钥信息. 安全性分析和性能分析表明, 新协议适合在实际环境中应用.

2 背景知识

2.1 切比雪夫混沌映射

定义 1 n 是整数, x 是取值在区间 $[-1, 1]$ 的变量, 切比雪夫多项式 $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ 定义为

$$T_n(x) = \cos(n \arccos(x)). \quad (1)$$

由定义 1 可知, 切比雪夫多项式的迭代关系是

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

其中 $T_0(x) = 1$, $T_1(x) = x$.

切比雪夫多项式具有两个重要特性, 分别是半群特性和混沌特性.

1) 半群特性

$$\begin{aligned} T_r(T_s(x)) &= \cos(r \cos^{-1}(s \cos^{-1}(x))) \\ &= \cos(rs \cos^{-1}(x)) = T_{sr}(x) \\ &= T_s(T_r(x)). \end{aligned} \quad (3)$$

2) 混沌特性

当 n 大于 1 时, n 维切比雪夫多项式映射 $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ 是混沌映射, 且具有不变的测度 $f^*(x) = 1/(\pi\sqrt{1-x^2})$.

Zhang^[24] 证明了定义在区间 $(-\infty, +\infty)$ 的切比雪夫多项式 (扩展的切比雪夫多项式) 仍然具有半群特性.

$$T_n(x) \equiv 2xT_{n-1}(x) - T_{n-2}(x) \pmod{P}, \quad (4)$$

其中 $n \geq 2$, $x \in (-\infty, +\infty)$ 且 P 是一个大素数. 显然

$$T_r(T_s(x)) \equiv T_{sr}(x) \equiv T_s(T_r(x)) \pmod{P}, \quad (5)$$

定义在扩展的切比雪夫多项式的两个问题被认为是多项式时间难解的.

定义 2 离散对数问题 (Discrete Logarithm Problem, DLP)^[24].

给定两个元素 x 和 y , 找到一个整数 s , 使得 $T_s(x) = y$.

定义 3 计算 Diffie-Hellman 问题 (computational Diffie-Hellman problem, CDHP)^[24].

给定三个元素 x , $T_r(x)$ 和 $T_s(x)$, 计算 $T_{rs}(x)$.

2.2 Bergamo 攻击

切比雪夫多项式 $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ 定义为 $T_n(x) = \cos(n \arccos(x))$, 其中 n 是整数, x 是取值在区间 $[-1, 1]$ 的变量. Bergamo 等^[5] 指出攻击者得到信息 $(x, T_r(x), T_s(x))$, 就可以计算出 $T_{rs}(x)$, 过程如下.

1) 攻击者根据 $(x, T_r(x))$ 计算

$$r' = \frac{\arccos(T_r(x)) + 2k'\pi}{\arccos(x)} \Big| k' \in z;$$

2) 攻击者计算

$$\begin{aligned} T_{r'}(x) &= \cos(r' \cdot \arccos(x)) \\ &= \cos\left(\left(\frac{\arccos(T_r(x)) + 2k'\pi}{\arccos(x)} \Big| k' \in z\right) \times \arccos(x)\right) \\ &= \cos(\arccos(T_r(x)) + 2k'\pi) \\ &= \cos(\arccos(T_r(x))) \\ &= T_r(x). \end{aligned}$$

由以上可知, 攻击者可以计算出 r' , 使得等式 $T_{r'}(x) = T_r(x)$ 成立. 依据切比雪夫多项式的半群特性, 攻击者很容易计算出 $T_{rs}(x)$.

$$\begin{aligned} T_{r'}(T_s(x)) &= T_{r's}(x) = T_s(T_{r'}(x)) = T_s(T_r(x)) \\ &= T_{sr}(x) = T_{rs}(x). \end{aligned}$$

Bergamo 攻击存在的内在原因是有许多切比雪夫多项式经过了同一个点.

3 新的认证密钥协商协议

协议包括两个阶段: 注册阶段和认证阶段.

注册阶段

用户 U_i 要注册成为一个合法用户, 要执行如下过程.

1) 用户 U_i 自由选择自己的身份 ID_i 和一个低熵的口令 pw_i , 然后通过安全通道发送 (ID_i, pw_i) 给服务器 S .

2) S 计算 $S_i = H(ID_i || pw_i)$, 然后将 (ID_i, S_i) 保存在服务器的列表 L 中.

3) S 将哈希函数 $H()$ 发送给用户 U_i .

认证阶段

用户 U_i 和服务器 S 为了实现双向认证, 如图 1 所示, 要执行如下过程.

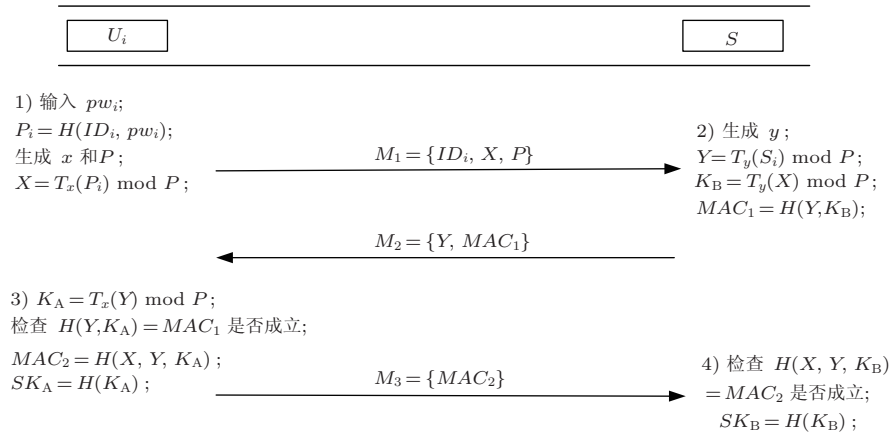


图1 密钥协商过程

1) U_i 输入口令 pw_i , 计算 $P_i = H(ID_i || pw_i)$. U_i 随机选择一个整数 x 和一个大素数 P , 计算 $X = T_x(P_i) \bmod P$. 然后发送消息 $M_1 = \{ID_i, X, P\}$ 给服务器 S .

2) S 收到消息 M_1 后, 根据消息中的 ID_i 从列表 L 中取出 S_i . 然后随机选择一个整数 y , 计算 $Y = T_y(S_i) \bmod P$, $K_B = T_y(X) \bmod P$, $MAC_1 = H(Y, K_B)$. 最后发送消息 $M_2 = \{Y, MAC_1\}$ 给用户 U_i .

3) U_i 收到消息 M_2 后, 计算 $K_A = T_x(Y) \bmod P$, 检验等式 $H(Y, K_A) = MAC_1$ 是否成立. 如果等式不成立, U_i 退出协议; 否则, U_i 认证了 S . U_i 计算 $MAC_2 = H(X, Y, K_A)$, $SK_A = H(K_A)$. 然后发送消息 $M_3 = \{MAC_2\}$ 给 S .

4) S 收到消息 M_3 后, 检验等式 $H(X, Y, K_B) = MAC_2$. 如果等式不成立, S 退出协议; 否则, S 认证了 U_i . S 计算 $SK_B = H(K_B)$. 由于

$$\begin{aligned} K_A &= T_x(Y) \bmod P = T_x(T_y(S_i)) \bmod P \\ &= T_{xy}(S_i) \bmod P = T_y(T_x(S_i)) \bmod P \\ &= T_y(T_x(P_i)) \bmod P = T_y(X) \bmod P = K_B, \end{aligned} \quad (6)$$

$$SK_A = H(K_A) = H(K_B) = SK_B. \quad (7)$$

以上证明了协议的正确性.

4 协议的安全性分析

本小节对新协议的安全性进行分析, 指出协议能抵抗已知的各种攻击.

1) 抵抗 Bergamo 攻击

Bergamo 攻击中, 攻击者必须得到 x , $T_r(x)$ 和 $T_s(x)$ 三个元素, 并且 x 的取值在区间在 -1 和 $+1$ 之间, 才能发动有效攻击. 协议采用扩展的切比雪夫多项式作为安全通信的核心. 由于将模运算引入到扩展切比雪夫多项式的运算中, 定义在区间 $(-\infty, +\infty)$ 的扩展切比雪夫多项式可以有效避免余弦函数的周期性, 因而协议能抵抗 Bergamo 攻击.

2) 协议具有双向认证特性

双向认证性是指通信双方能互相认证对方的身份. 在新协议中, 用户 U_i 用检验消息 MAC_1 的正确性来认证服务器 S , 服务器 S 用检验消息 MAC_2 的正确性来认证用户 U_i . 另外, 任何攻击者都不能伪造合法的消息 MAC_1 和 MAC_2 . 因此, 新协议具有双向认证的特性.

3) 协议能够抵抗重放攻击

在协议中, 如果攻击者伪装成合法用户, 重放消息 M_1 . 在收到消息 M_2 后, 攻击者无法生成本次会话中正确的消息 M_3 . 如果攻击者伪装成服务器, 重放消息 M_2 . 由于和消息 M_2 相对应的消息 M_1 已经改变了, 消息 M_2 无法通过合法用户的验证. 因此, 重放任何消息, 通信方都能检测出来.

4) 协议具有完美的前向安全特性

完美的前向安全性是指用户的长期私钥泄露不会影响以前生成的会话密钥的安全性. 如果用户 U_i 的长期私钥泄露, 攻击者可以得到 $P_i = H(ID_i, pw_i)$. 攻击者可以得到 $T_x(P_i) \bmod P$ 和 $T_y(P_i) \bmod P$. 攻击者要计算出 $T_{xy}(P_i) \bmod P$, 必须解决扩展的切比雪夫多项式 CDHP.

5) 协议能抵抗口令猜测攻击

口令猜测攻击有两种: 在线口令猜测攻击和离线口令猜测攻击. 在线口令猜测攻击中, 攻击者在一次会话中试图猜测用户的口令通过服务器的验证. 离线口令猜测攻击中, 攻击中监听用户与服务器之间的通信, 然后用穷举的方式猜测口令, 并用所监听的信息来验证猜测口令的正确性. 在线猜测口令攻击可以通过限制登陆失败的次数来避免. 协议设计中, 应主要考虑离线口令猜测攻击.

新协议中, 假设攻击者监听用户 U_i 和服务器 S 的通信, 并且得到消息 M_1 , M_2 和 M_3 . 攻击者猜测口令 pw'_i , 计算 $P'_i = H(ID_i, pw'_i)$. 如果攻击者猜测的口令是错误的, 它将得不到任何信息. 即使攻击者猜测的口令是正确的, 它依然要从消息 X 得到随机数 x 或从消息 Y 得到随机数 y , 才能验证猜测口令的正确性. 攻击者要实施有效的离线口令猜测攻击, 必须解决切比雪夫多项式的 DLP.

5 协议的性能分析

本节中, 我们给出新协议与其他相关协议在计算复杂度和安全性方面的比较. 为了方便评价计算

复杂度, 我们定义了如下的符号:

T_C : 执行切比雪夫多项式所需要的时间.

T_H : 执行单向哈希函数所需要的时间.

T_X : 执行异或操作所需要的时间.

从表 1 中可以得出, 新协议比 GZ 协议的计算复杂度更低. 与 GLS 协议相比, 计算复杂度相当, 新协议中用户和服务器都减少了一次异或操作. GZ 协议不能抵抗口令猜测攻击, 因而协议是不安全的. 在 GZ 协议和 GLS 协议中, 通信双方使用切比雪夫多项式 $T_n(r)$ 来建立会话密钥. 由于通信双方必须使用相同的数 r , 服务器要发布信息 r . 服务器发布信息依赖于签名机制, 而基于混沌映射的签名方案难以实现或者实现的代价太高, 则信息 r 存在被替换的风险. 新协议中, 使用通信双方共享的秘密 $H(ID_i || pw_i)$ 作为 r 的值, 服务器不再需要发布信息 r . 虽然服务器与每个合法用户所使用的值 r 并不相同, 服务器可以从自己的列表 L 中直接获得与不同用户通信的数值 r , 并不影响协议的效率. 因此, 新协议更适合在客户-服务器环境中应用.

表 1 与其他协议的比较

	GZ 协议 [22]	GLS 协议 [23]	新协议
计算复杂度 (用户)	$2T_C + 4T_H + 5T_X$	$2T_C + 4T_H + 1T_X$	$2T_C + 4T_H$
计算复杂度 (服务器)	$2T_C + 5T_H + 7T_X$	$2T_C + 3T_H + 1T_X$	$2T_C + 3T_H$
双向认证	是	是	是
完美前向安全	是	是	是
Bergamo 攻击	否	否	否
重放攻击	否	否	否
口令猜测攻击	是	否	否
发布公钥	是	是	否

6 结 论

基于智能卡的认证密钥协商协议, 智能卡和读卡器的使用使得这类协议成本较大. 另外, 基于混沌理论的签名方案还不完善, 使得公钥的发布存在安全隐患. 为解决基于混沌映射密钥协商协议存在的安全问题, 本文基于扩展混沌映射提出一种无智能卡的认证密钥协商协议, 并且新协议不需要服务器发布公钥. 和其他协议相比, 新协议的计算复杂度更低且可以抵抗各类攻击. 因此, 新协议更适合在实际环境中应用.

参考文献

- [1] Wei J, Liao X, Wong K, Xiang T 2006 *Chaos Soliton. Fract.* **30** 1143
- [2] Liu Q, Fang J Q, Zhao G, Liu Y 2012 *Acta Phys. Sin.* **61** 130508 (in Chinese)[刘强, 方锦清, 赵耿, 李永 2012 物理学报 **61** 130508]
- [3] Wang X Y, Bao M M 2013 *Chin. Phys. B* **22** 050508
- [4] Xiao D, Liao X, Deng S 2005 *Chaos Soliton. Fract.* **24** 65
- [5] He T T, Luo X S, Liao Z X, Wei Z C 2012 *Acta Phys. Sin.* **61** 110506 (in Chinese)[何婷婷, 罗晓曙, 廖志贤, 韦正从 2012 物理学报 **61** 110506]
- [6] Wang F L 2011 *Acta Phys. Sin.* **60** 110517 (in Chinese)[王福来 2011 物理学报 **60** 110517]

- [7] Chen T M, Jiang R R 2013 *Acta Phys. Sin.* **62** 040301
(in Chinese)[陈铁明, 蒋融融 2013 物理学报 **62** 040301]
- [8] Bergamo P, Arco P, Santis A, Kocarev L 2005 *IEEE Tran. Circuits.* **52** 1382
- [9] Han S Chang E 2009 *Chaos Soliton. Fract.* **39** 1283
- [10] Kocarev L, Tasev Z 2003 *Proceedings of the 38th International Symposium on Circuits and Systems* Bangkok, Thailand, May 25–28, 2003 p28
- [11] Xiao D, Liao X F, Deng S J 2007 *Inf. Sci.* **177** 1136
- [12] Xiao D, Liao X, Wong K 2005 *Chaos Soliton. Fract.* **23** 1327
- [13] Xiang T, Wong K, Liao X 2009 *Chaos Soliton. Fract.* **40** 672
- [14] Wang X Y, Luan D P 2013 *Chin. Phys. B* **22** 110503
- [15] Tseng H R, Jan R H, Yang W 2009 *Proceedings of the 13th International Conference on Communications* Dresden, Germany, June 14–18, 2009 p1
- [16] Niu Y J, Wang X Y 2011 *Commun. Nonlinear Sci. Numer. Simul.* **16** 1986
- [17] Yoon E J 2012 *Commun. Nonlinear Sci. Numer. Simul.* **17** 2735
- [18] Lee C, Chen C, Wu C, Huang S 2012 *Nonlinear Dyn.* **69** 79
- [19] He D, Chen Y 2012 *Nonlinear Dyn.* **69** 1149
- [20] Xue K, Hong P 2012 *Commun. Nonlinear Sci. Numer. Simul.* **17** 2969
- [21] Zhao F J, Gong P, Li S 2013 *Nonlinear Dyn.* **74** 419
- [22] Guo X, Zhang J 2010 *Inf. Sci.* **180** 4069
- [23] Gong P, Li P, Shi W B 2012 *Nonlinear Dyn.* **70** 2401
- [24] Zhang L 2008 *Chaos Soliton. Fract.* **37** 669

An authenticated key agreement protocol based on extended chaotic maps^{*}

Shu Jian[†]

(Department of Electronic Commerce, Jiangxi University of Finance and Economics, Nanchan 330013, China)

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

(Received 29 October 2013; revised manuscript received 21 November 2013)

Abstract

Recently, many chaotic maps-based authenticated key agreement protocols using smart cards have been proposed. Unfortunately, tamper-resistant card readers make these protocols costly and impractical. In addition, the digital signature scheme based on chaotic maps requires high computational resources. There exists security problem in publishing public keys which depend on signature schemes. In this paper, we will present a novel authenticated key protocol without smart cards while using extended Chebyshev maps. The proposed protocol eliminates the process of publishing the public key. Security and performance analysis show that our protocol can resist various attacks and yet is reasonably efficient. Therefore, our protocol is more suitable for practical applications.

Keywords: chaotic map, key agreement, smart card, digital signature

PACS: 05.45.Vx, 05.45.–a

DOI: 10.7498/aps.63.050507

^{*} Project supported by the National Natural Science Foundation of China (Grant No. 61163053).

[†] Corresponding author. E-mail: mikeshujian@jxufe.edu.cn