基于模糊提取技术的多服务器身份验证协议

郝伟伟[1],吕　磊[2]
(1. 河南省市场监督管理局 信息中心,河南 郑州 450008;
2. 河南工业大学 信息科学与工程学院,河南 郑州 450008)

摘　要:针对屈娟等人采用模糊提取技术、切比雪夫混沌映射算法给出一个身份认证协议进行全面的安全性分析,指出该身份认证协议存在安全隐患或有待商榷的地方等问题,并在此协议基础之上提出一个改进的基于模糊提取技术的多服务器环境下的身份验证协议。文中协议针对安全等级要求不同的隐私信息采用不同的算法进行加密,安全等级要求较高的数据采用模糊提取技术进行加密,其他数据采用逆向遍历组合运算进行加密;模糊提取技术算法属于轻量级的加密算法,逆向遍历组合运算属于超轻量级的加密算法,两种算法组合使用,在确保安全的前提下,亦可减少通信实体的整体计算量。逆向遍历组合运算是一种文中自主设计的超轻量级运算,算法可基于按位运算,同时混入每个加密参量自身固有的属性汉明权重,在减少参数引入的同时,亦可增加攻击者的破解难度。从安全、性能角度综合分析各协议,文中协议可在确保安全的前提下,尽可能降低整体计算量,适用于低成本智能卡中。

关键词:多服务器;模糊提取;身份验证;逆向遍历组合运算;智能卡
中图分类号:TP393.08　　**文献标识码**:A　　**文章编号**:1673-629X(2022)05-0075-05
doi:10.3969/j.issn.1673-629X.2022.05.013

Multi Server Authentication Protocol Based on Fuzzy Extraction Technology

HAO Wei-wei[1],LYU Lei[2]
(1. Information Center,Administration for Market Regulation of Henan Province,Zhengzhou 450008,China;
2. School of Information Science and Technology,Henan University of Technology,Zhengzhou 450008,China)

Abstract:Aiming at the problem that Qu Juan et al. points out that the identity authentication protocol has security risks or problems to be discussed using fuzzy extraction technology and Chebyshev chaotic mapping algorithm to give a comprehensive security analysis of an identity authentication protocol,we propose an improved identity authentication protocol based on fuzzy extraction technology in multi-server environment. In this paper, different algorithms are used to encrypt the privacy information with different security level requirements,the data with higher security level requirements are encrypted by fuzzy extraction technology, and the other data are encrypted by reverse traversal combination operation. Fuzzy extraction algorithm belongs to lightweight encryption algorithm,and reverse traversal combination algorithm belongs to ultra-lightweight encryption algorithm. The combination of the two algorithms can reduce the overall calculation of communication entities on the premise of ensuring security. Reverse traversal combination operation is a kind of ultra-lightweight operation designed by ourselves in this paper. The algorithm can be based on bitwise operation. At the same time,it can mix in the Hamming weight of each encryption parameter's own inherent attribute,which can reduce the introduction of parameters and increase the attacker's cracking difficulty. From the perspective of security and performance,the protocol can reduce the total amount of computation as much as possible on the premise of ensuring security, which is suitable for low-cost smart card.

Key words:multi server;fuzzy extraction;identity authentication;reverse traversal combinatorial operation;smart card

0　引　言

进入新世纪之后,科学技术快速发展,移动网络越来越多地被运用在人们生活中,比如:线上预约挂号看病、线上预约取号办理业务等[1-2]。在上述操作中,用户需要与特定的单位提供的服务器进行登录,比如说:用户甲需要去某家大型医院预约看病,则用户甲必须用自己的身份和口令登录服务器后,才可以进行预约操作[3]。

收稿日期:2021-06-17　　**修回日期**:2021-10-19
基金项目:国家自然科学基金(61705060)
作者简介:郝伟伟(1985-),男,高级工程师,CCF 会员(F9494M),研究方向为电子政务、信息安全、项目管理。

伴随着网络快速发展及运用,越来越多的业务可在网络上事先进行预约,再进行实体门店中办理手续。在传统的单服务器环境下,用户需要在每个服务器环境下进行注册,这样将会使得用户需要记住多个账户和口令信息,不方便用户[4-5]。为解决单服务器环境下存在的不足,多服务器环境下用户只需注册一个账号,便可以访问多个服务器上资源,可使用户免去记忆多个账号和口令负担。用户登录服务器过程中,信息交换通道为无线方式,无线方式具备的开放性特征,使得用户信息存在一定不足。为保证用户隐私信息不受侵犯,需设计身份认证协议以保障二者之间信息传送的安全性。

文中设计一个身份认证协议,该协议既可在单服务器环境下适用,亦可在多服务器环境下适用;为能够确保用户账号和口令的安全性,协议采用模糊提取技术对重要隐私信息进行加密,在确保安全的前提下,引入超轻量级的逆向遍历组合运算对部分消息加密。从不同角度展开多个经典协议分析,表明文中协议在安全性能上优于其他对比协议,能够提供诸如假冒攻击、重放攻击、穷举攻击等常见类型安全防御,且系统整体计算时间开销具备优势。

1 相关工作

文献[6]中提出的身份认证协议只适用于单服务器环境下,无法在当今多服务器环境下使用,因此无法推广,具有一定的局限性。针对文献[7]中设计的身份认证协议,Yeh 等人在文献[8]中进行了安全性分析,指出协议存在无法抵抗用户假冒攻击、服务器假冒攻击和中间人攻击等缺陷,同时作者在文献[8]中设计一个改进的身份认证协议。

文献[9]中协议从多方面对文献[8]中协议进行安全性分析,指出该协议存在内部攻击、用户假冒攻击等缺陷。文献[10-12]中分别设计出不同的协议,其中文献[13]分别对文献[10-12]中的协议进行了安全性分析,指出文献[10]中协议存在无法实现所声称的离线口令猜测攻击,同时该协议也未实现用户匿名性和前向安全性;指出文献[11]中协议存在无法实现抵抗离线口令猜测攻击,同时该协议也无法提供匿名性;指出文献[12]中协议存在不能抵抗所声称的用户仿冒攻击和离线口令猜测攻击,同时协议还无法实现用户不可追踪性。文献[13]中协议存在诸如符号含义不明、多个消息用处不明确等问题,同时协议在智能卡一端设置四种类型哈希函数,使得智能卡实现成本急剧提升,无法推广使用该协议。文献[14]中采用模糊提取技术、切比雪夫混沌映射算法给出一个身份认证协议,但该协议存在诸多正确性有待商榷之处。屈娟等人提出的协议完整过程可参见文献[14],鉴于文中篇幅有限,文中不再详细阐述。对屈娟等人设计协议进行分析,发现如下几处正确性或不足有待商榷:

第一处正确性有待商榷是,屈娟等人提出的协议中多次出现符号 T_1、T_2、T_3,但协议并未给出上述三个符号所表示含义,也未说明上述符号在协议具体实现过程中发挥的作用是什么。故该处符号引入使用正确性有待商榷。

第二处正确性有待商榷是,在协议的“登录阶段”中,用户 U_i 在计算消息 C_{2i} 过程中用到 SID_j 参数,结合上下文分析,SID_j 参数表示服务器 S_j 的身份标识,用户 U_i 是未获取该参数信息的,因此用户 U_i 无法使用该参数进行计算。故该处有关 C_{2i} 计算过程中用到的 SID_j 正确性有待商榷。

第三处不足是,协议中对于信息的加密用到三种不同的加密算法,即模运算、哈希函数运算、切比雪夫运算,使得智能卡一端的计算量较大。对于低成本的智能卡而言,计算能力受到一定制约,同时用到上述三种运算时,现有的智能卡无法实现。故屈娟等人设计协议推广性受到制约。

鉴于现有的诸多经典协议存在无法使用于多服务器环境下或计算量大或存在安全缺陷等问题,文中采用模糊提取技术,同时结合超轻量级的逆向遍历组合运算算法,设计一个改进的身份认证协议。

2 相关知识

文中统一用 $\mathrm{Rtc}(X,Y)$ 符号来表示逆向遍历组合运算,同时 $\mathrm{Rtc}(X,Y)$ 可按照下面方式实现:

X,Y,Z 均是长度为 L 位的二进制字符串,$W(X)$、$W(Y)$ 分别表示 X,Y 的汉明权重。当 $W(X) > W(Y)$ 时,指针 P_x 从 X 右边开始向左边遍历,同时指针 P_y 从 Y 左边开始向右边遍历,若 X 的第 i 位值、Y 的第 j 位值满足 $F_i(X) > F_j(Y)$,则将 X 的第 i 位值 $F_i(X)$ 放于 Z 的第 j 位,否则,将 Y 的第 j 位值 $F_j(Y)$ 放于 Z 的第 j 位,其中 i、j 满足条件 $i+j=L+1$,待遍历完 X 的同时,Y 也遍历完,且可得到逆向遍历组合运算最终结果。

当 $W(X) \leqslant W(Y)$ 时,指针 P_x 从 X 左边开始向右边遍历,同时指针 P_y 从 Y 右边开始向左边遍历,若 X 的第 i 位值、Y 的第 j 位值满足 $F_i(X) > F_j(Y)$,则将 Y 的第 j 位值 $F_j(Y)$ 放于 Z 的第 i 位,否则,将 X 的第 i 位值 $F_i(X)$ 放于 Z 的第 i 位,其中 i、j 满足条件 $i+j=L+1$,待遍历完 X 的同时,Y 也遍历完,且可得到逆向遍历组合运算最终结果。

逆向遍历组合运算可结合下面两个例子进行理解。取 $L=12$、$X=110101101001$、$Y=001001001010$,可得 $W(X)=7$、$W(Y)=4$,满足 $W(X) > W(Y)$ 情况,

依据上述逆向遍历组合运算定义可得 $Z = \mathrm{Rtc}(X,Y) = 101101101011$。再次取 $L = 12$、$X = 100101000010$、$Y = 011010111100$,可得 $W(X) = 4$、$W(Y) = 7$,满足 $W(X) \leqslant W(Y)$ 情况,依据上述逆向遍历组合运算定义可得 $Z = \mathrm{Rtc}(X,Y) = 000111010010$。

3　多服务器环境下身份验证协议

文中设计的身份验证协议共分为五个阶段,依次为服务器注册阶段、用户注册阶段、用户登录阶段、用户与服务器间认证阶段、用户修改口令阶段。

(1)服务器注册。

S_j 表示服务器; ID_{S_j} 表示服务器 S_j 的身份标识; RC 表示注册中心; K_j 表示注册中心密钥。

服务器 S_j 向注册中心 RC 进行注册,发送 ID_{S_j} 给注册中心 RC。注册中心 RC 搜索已存数据是否与 ID_{S_j} 相等。如有,注册中心 RC 告知服务器 S_j 重新选择 ID_{S_j} 再次进行注册;否则,注册中心 RC 计算 $A_j = \mathrm{Rtc}(\mathrm{ID}_{S_j},K_j)$,并将$<A_j, K_j>$发送给服务器 S_j。待服务器 S_j 收到消息,服务器 S_j 注册完成。

(2)用户注册。

U_i 表示用户; ID_{U_i} 表示用户 U_i 的身份标识; PW_{U_i} 表示用户 U_i 设置的口令; SURE 表示确定含义; x 表示用户 U_i 选定的随机数; BIO_i 表示用户 U_i 的生物特征值。用户 U_i 想要访问服务器 S_j 上资源,则用户 U_i 必须先完成注册,只有用户 U_i 成为合法用户后,用户 U_i 才有权限访问服务器 S_j 上资源。

用户 U_i 选择身份标识 ID_{U_i}、设定口令 PW_{U_i},然后将信息发送给注册中心 RC。注册中心 RC 在已存数据中搜索是否有与 ID_{U_i} 相等。如有,注册中心 RC 告知用户 U_i 重新选择 ID_{U_i} 再次进行注册;反之,注册中心 RC 发送 SURE 给用户 U_i,表示注册成功。用户 U_i 收到 SURE 后,选定随机数 x,并将 x 发送给注册中心 RC。注册中心 RC 收到信息,依次计算 $B_i = \mathrm{Rtc}(A_j, x)$、$D_i = B_i \oplus \mathrm{PW}_{U_i}$,并将$<K_j, D_i, \mathrm{Gen}(), \mathrm{Rep}(), \mathrm{Rtc}(X,Y)>$信息写入智能卡中,同时将智能卡发给用户 U_i。用户 U_i 收到智能卡后,先提取用户生物特征值 BIO_i,并将 BIO_i 输入模糊提取函数 Gen() 中,可得到 λ_i、β_i(即 $\mathrm{Gen}(\mathrm{BIO}_i) = (\lambda_i,\beta_i)$),然后计算 $E_i = \mathrm{Rtc}(\mathrm{ID}_{U_i} \oplus \lambda_i, \mathrm{PW}_{U_i} \oplus x)$、$F_i = x \oplus \mathrm{Rtc}(\lambda_{i\_L}, \lambda_{i\_R})$,最后将$<E_i, F_i, \beta_i>$信息写入智能卡中。

待上述操作完成,智能卡中存放信息有$<K_j, D_i, E_i, F_i, \beta_i, \mathrm{Gen}(), \mathrm{Rep}(), \mathrm{Rtc}(X,Y)>$。

(3)用户登录。

y 表示智能卡生成的随机数。

用户 U_i 在访问服务器 S_j 之前,需要一个登录阶段。用户 U_i 插入拥有的智能卡,根据提示,用户 U_i 输入 ID_{U_i}、PW_{U_i},同时通过扫描获取用户生物特征值 BIO_i^*。智能卡将根据用户 U_i 输入的生物特征值 BIO_i^* 恢复出 λ_i(即 $\lambda_i = \mathrm{Rep}(\mathrm{BIO}_i^*, \beta_i)$),智能卡接着计算可得到 $x^* = F_i \oplus \mathrm{Rtc}(\lambda_{i\_L}, \lambda_{i\_R})$,将 x^* 带入可计算得到 $E_i^* = \mathrm{Rtc}(\mathrm{ID}_{U_i} \oplus \lambda_i, \mathrm{PW}_{U_i} \oplus x^*)$,比较 $E_i^* \stackrel{?}{=} E_i$ 是否成立。如不成立,将提示用户 U_i 再次输入 ID_{U_i}、PW_{U_i},三次机会仍无法通过验证,则智能卡将被锁住;反之,且 $x^* = x$,智能卡生成一个随机数 y,接着计算 $B_i = D_i \oplus \mathrm{Rtc}(\mathrm{PW}_{U_i}, x)$、$G_i = y \oplus \mathrm{Rtc}(K_{j\_L}, K_{j\_R})$、$H_i = \mathrm{Rtc}(y \oplus \mathrm{ID}_{U_i}, B_i \oplus E_i)$,并最终将$<E_i, G_i, H_i, x>$信息发送给服务器 S_j。

(4)用户与服务器间认证。

z 表示服务器 S_j 生成的随机数。

待服务器 S_j 收到消息后,将先验证用户合法性。服务器 S_j 计算 $B_i = \mathrm{Rtc}(A_j, x)$、计算 $y^* = G_i \oplus \mathrm{Rtc}(K_{j\_L}, K_{j\_R})$,并将计算所得 B_i、y^* 带入可计算得到 $H_i^* = \mathrm{Rtc}(y^* \oplus \mathrm{ID}_{U_i}, B_i \oplus E_i)$,对比 $H_i^* \stackrel{?}{=} H_i$ 是否成立。如不成立,用户无法通过验证;否则,$y^* = y$,服务器 S_j 生成随机数 z,并依次计算得到 $N_i = z \oplus y$、$K_{S\_U} = \mathrm{Rtc}(z,y)$、$P_i = \mathrm{Rtc}(K_j \oplus z, y \oplus K_{S\_U})$,最后将 $<N_i, P_i>$ 信息发送给智能卡。

智能卡在收到消息后,计算得到 $z^* = N_i \oplus y$,并将 z^* 带入可计算得到 $K_{S\_U}^* = \mathrm{Rtc}(z^*, y)$,再结合 z^*、$K_{S\_U}^*$ 可计算得到 $P_i^* = \mathrm{Rtc}(K_j \oplus z^*, y \oplus K_{S\_U}^*)$,再对比 $P_i^* \stackrel{?}{=} P_i$ 是否成立。如不成立,服务器非法,身份验证协议终止;反之,$z^* = z$、$K_{S\_U}^* = K_{S\_U}$,智能卡再计算 $Q_i = \mathrm{Rtc}(K_{S\_U} \oplus z, y)$,最后将$<Q_i>$信息发送给服务器 S_j。服务器 S_j 收到信息后,计算 $Q_i^* = \mathrm{Rtc}(K_{S\_U} \oplus z, y)$,并对比 $Q_i^* \stackrel{?}{=} Q_i$ 成立与否。如不成立,用户非法,身份验证协议终止;反之,用户合法,将 K_{S_U} 作为服务器 S_j 与用户 U_i 间的共享密钥。

(5)用户修改口令。

用户 U_i 在使用一段时间后,为安全起见,用户 U_i 会修改当初设定的口令。

用户 U_i 插入拥有的智能卡,根据提示,用户 U_i 输入 ID_{U_i}、PW_{U_i},同时通过扫描获取用户生物特征值 BIO_i^*。智能卡将根据用户 U_i 输入的生物特征值 BIO_i^* 恢复出 λ_i(即 $\lambda_i = \mathrm{Rep}(\mathrm{BIO}_i^*, \beta_i)$),智能卡接着计算可得到 $x^* = F_i \oplus \mathrm{Rtc}(\lambda_{i\_L}, \lambda_{i\_R})$,将 x^* 带入可计算得到 $E_i^* = \mathrm{Rtc}(\mathrm{ID}_{U_i} \oplus \lambda_i, \mathrm{PW}_{U_i} \oplus x^*)$,比较 $E_i^* \stackrel{?}{=} E_i$ 是否成立。如不成立,将提示用户 U_i 再次输入 ID_{U_i}、PW_{U_i},三次机会仍无法通过验证,则智能卡将被锁住;反之,且 $x^* = x$,用户 U_i 可进行如下计算: $\mathrm{PW}_{U_i}^{\mathrm{new}} = \mathrm{Rtc}(\mathrm{PW}_{U_i}, x)$、$D_i^{\mathrm{new}} = B_i \oplus \mathrm{PW}_{U_i}^{\mathrm{new}}$、$E_i^{\mathrm{new}} = \mathrm{Rtc}(\mathrm{ID}_{U_i} \oplus$

λ_i,$PW_{U_i}^{new} \oplus x$),并用 D_i^{new}、E_i^{new} 替换智能卡中 D_i、E_i,待替换完成,用户 U_i 修改口令完成。

4 身份验证协议安全性分析

(1)匿名性。

想要实现匿名性,就需要保证用户的身份标识 ID_{U_i} 无法被第三方监听获取或破解获取。文中在用户登录阶段中,发送给注册中心的消息 $H_i = Rtc(y \oplus ID_{U_i}, B_i \oplus E_i)$ 中有出现用户的身份标识 ID_{U_i},但该信息将会经过加密之后再发送,第三方无法破解获取;同时消息 H_i 在加密过程中还会混入随机数 y,使得每轮计算所得消息 H_i 的值都是变动的,从而实现第三方无法追踪用户具体位置。基于上述分析,文中协议可实现匿名性安全需求。

(2)会话密钥协商。

为能够确保后续操作过程中用户隐私信息的安全性,文中协议在认证阶段结束之后,用户与服务器之间将通过协商方式共同生成两者之间的共享密钥 $K_{S\_U} = Rtc(z,y)$。在该共享密钥协商过程中,不仅会用到用户一端产生的随机数 y,而且还会用到服务器一端产生的随机数 x。只有合法的服务器,才可以通过计算得到正确的随机数 y;同理,也只有合法的用户,才可以通过计算得到正确的随机数 x,任何伪装的第三方,都会因缺少关键参数信息,而导致计算过程中错误,无法计算得到正确的随机数 x 或 y。基于上述分析,文中协议可以实现会话密钥协商的安全需求。

(3)假冒攻击。

第三方可以假冒成合法用户,向服务器发送消息。但第三方缺少合法用户拥有的 ID_{U_i}、PW_{U_i}、BIO_i^* 重要参数,使得第三方无法计算得到正确的消息;待服务器收到第三方发送来的消息后,经过简单验证,即可识别出消息来源方是假冒的。第三方也可以假冒成合法服务器,给用户发送消息。第三方需要先能从用户发送来的合法消息中破解出用户产生的随机数,之后第三方用该随机数参与计算后续其他消息。但因第三方无法获取用户隐私信息,使得第三方无法从消息中破解出用户产生的随机数。基于上述分析,无论第三方假冒何方,文中协议都可以抵抗第三方发起的假冒攻击。

(4)前向安全性。

第三方想要从当前会话中窃听获取的消息,推导出之前会话过程中涉及到的隐私信息,但文中协议中第三方无法成功。文中协议中用户与服务器之间的共享密钥都是每次在会话过程中通过商定的方式确定的,且每轮共享密钥商定过程中,都会混入随机数,每轮会话中涉及到的随机数都是随机产生、无规律性、互异性,因此第三方根本无法通过当前消息推导出之前某轮会话用到的随机数。基于上述分析,文中协议可以实现前向安全性需求。

(5)重放攻击。

可以采用窃听的方式,第三方可获取一个完整会话过程中所有消息,并通过下轮会话中重放窃听消息方式,以企图通过合法实体认证,进而获取更多隐私信息,但文中协议第三方无法成功。消息加密过程中加入随机数,每轮会话使用随机数都是不同的,且都是随机产生的,使得前后相隔的两轮会话加密消息值都是不同的。当第三方重放窃听的消息时,当前正在进行的会话中使用到的随机数早已发生变更,第三方重放消息失败。基于上述分析,文中协议可以抵抗第三方发起的重放攻击。

(6)穷举攻击。

可以采用更为直接的方式,即穷举方式穷尽隐私信息可能的所有取值,进而破解出用户关键隐私信息,但文中协议中第三方无法成功。这里仅选择消息 $E_i = Rtc(ID_{U_i} \oplus \lambda_i, PW_{U_i} \oplus x)$ 为例进行分析。在消息 E_i 中,一共有 ID_{U_i}、λ、PW_{U_i}、x 四个参数的值对于第三方来说不知晓;即便是第三方可能通过某些非法途径获取上述四个参数中某些,但也不可能获取四个全部参数,此时第三方仍无法穷尽,因为根据自设计的加密算法定义可知,消息加密过程中还会涉及到参数自身携带的汉明参数值。当第三方无法全部获取四个参数时,则加密过程中涉及到的参数的汉明参数,第三方就无法知晓,则加密破解将失败。基于上述分析,文中协议可以抵抗第三方发起的穷尽攻击。

5 身份验证协议性能分析

本章节主要从用户登录阶段和用户与服务器间相互认证阶段出发,和其他经典协议对比分析两个阶段计算时间开销,分析结果如表 1 所示。

表 1 中各符号含义如下:T_h 表示哈希函数计算一次需要的时间开销;T_pm 表示一次椭圆曲线点乘计算需要的时间开销;T_mod 表示模运算计算一次需要的时间开销;T_re 表示 RSF 加密计算一次需要的时间开销;T_rd 表示 RSA 解密计算一次需要的时间开销;T_c 表示切比雪夫混沌映射计算一次需要的时间开销;T_xor 表示按位异或运算计算一次需要的时间开销;T_rtc 表示逆向遍历组合运算计算一次需要的时间开销。由文献[15]可知,上述除了 T_xor、T_rtc 之外的加密算法计算一次需要的时间开销实现数据依次为 T_h=0.5 ms、T_pm=63.075 ms、T_mod=7.79 ms、T_re=8.7 ms、T_rd=8.7 ms、T_c=21.02 ms。根据现有的文献研究表明,一次轻量级别的计算量相当于几

十次甚至几百次超轻量级的计算量,因此,文中这里取　　T_xor=T_rtc=T_h/1 000=0.000 5 ms。

表 1　协议间性能及安全性分析对比

对比协议	文献[11]	文献[12]	文献[14]	文献[15]	文中协议
匿名性	×	×	✓	✓	✓
会话密钥协商	✓	✓	✓	✓	✓
假冒攻击	✓	×	×	✓	✓
前向安全性					
重放攻击	✓	✓	✓	✓	✓
穷举攻击	✓	✓	✓	×	✓
计算量	15T_h+5T_pm	14T_h+6T_mod	17T_h+3T_re+3T_rd	12T_h+4T_c	6T_xor+14T_rtc
计算时间开销/ms	322.875	53.74	60.7	90	0.01

文献[11-12,14-15]中协议因都是采用轻量级或重量级的加解密算法,因此表 1 中已忽略上述文献中有关超轻量级按位运算时间开销,但因文中协议未采用轻量级的加解密算法,因此未忽略超轻量级位运算时间开销。对表 1 分析可得,文中协议在登录阶段、认证阶段的总计算时间开销远远低于其他对比文献中协议,且文中协议还可以弥补其他协议存在的安全缺陷,使得文中协议具备推广使用的价值。

6　结束语

重点分析了屈娟等人设计协议存在的不妥之处,并结合该协议的优点,提出一种改进的身份验证协议。该协议对每个出现符号均给出详细解释;在保证安全的前提下,采用模糊提取算法实现对重要信息进行加密,同时对次重要信息采用逆向遍历组合运算实现加密;依据逆向遍历组合运算定义,该加密算法可基于按位运算实现,使得计算量得到较大幅度降低。从假冒攻击、重返攻击、后向安全性等多角度分析协议,表明协议可抵抗多种类型的攻击,提供良好的安全性需求;同时详细分析各阶段中协议整体计算量,表明文中协议计算量开销优于其他经典对比协议。

参考文献:

[1] MING Y, YUAN H P. Fully secure anonymous identity based broadcast encryption with group of prime OrderVol [J]. International Journal of Network Security, 2019, 21 (1):7-16.

[2] 刘道微,凌　捷,杨　昕. 一种改进的满足后向隐私的 RFID 认证协议[J]. 计算机科学,2016,43(8):128-130.

[3] JIANG Q, CHEN Z R, LI B Y, et al. Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems[J]. Journal of Ambient Intelligence and Humanized Computing, 2018,9(4):1061-1073.

[4] GUPTA P C, DHAR J. Hash based multi-server key exchange protocol using smart card [J]. Wireless Personal Communications,2016,87(1):225-244.

[5] 王瑞兵,陈建华,张媛媛. 一个匿名的基于生物特征的多服务器的密钥认证协议方案的研究[J]. 计算机应用研究,2016,33(7):2190-2196.

[6] DAS A K. A secure user anonymity preserving three factor remote user authentication scheme for the telecare medicine information systems[J]. Journal of Medicine System,2015, 39(3):1-20.

[7] PIPPAL R S, JAIDHAR C D, TAPASWI S. Robust smart card authentication scheme for multi-server architecture[J]. Wireless Personal Communications,2013,72(1):729-745.

[8] YEH K H. A provably secure multi-server based authentication scheme[J]. Wireless Personal Communications, 2014, 79(3):1621-1634.

[9] MISHR A D. Design and analysis of a provably secure multi-server authentication scheme[J]. Wireless Personal Communications,2016,86(3):1095-1119.

[10] 万　涛,刘遵雄,马建峰,等. 多服务器架构下认证与密钥协商协议[J]. 计算机研究与发展,2016,53(11):2446-2453.

[11] AMIN R. Cryptanalysis and efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card[J]. International Journal of Network Security,2016,18(1):172-181.

[12] REDDY A G, YOON E J, DAS A K, et al. Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment[J]. IEEE Access,2017,5:3622-3639.

[13] 汪　定,李文婷,王　平. 对三个多服务器环境下匿名认证协议的分析[J]. 软件学报,2018,29(7):1937-1952.

[14] 杜浩瑞,陈建华,戚明平,等. 一个前向安全的基于 RSA 的多服务器的认证协议[J]. 计算机科学,2019,46(11A):409-437.

[15] 屈　娟,冯玉明,李艳平,等. 可证明的基于扩展混沌映射的匿名多服务器身份认证协议[J]. 山东大学学报:理学版,2019,54(5):44-51.