文章编号：2095-2163(2022)08-0014-07 中图分类号：TP309 文献标志码：A

基于生物特征的身份认证和密钥协商协议

陈金木，黄朝阳
（厦门海洋职业技术学院 信息工程学院，福建 厦门 361102）

摘 要：生物特征是相互独立且与人体直接相关的重要因素，因此具有不可抵赖的天然特性和便利性。随着网络的高速发展，身份安全认证的需求也在不断增加。为实现人员身份认证的真实性和可靠性提供更好的安全策略，将生物特征信息、抗碰撞哈希函数和智能卡等技术相结合，提出了一种基于生物特征的身份认证和密钥协商协议。采取用户模拟攻击、特权内部攻击和服务器欺骗攻击等方式，对该协议的正确性和安全方面进行剖析。通过分析验证，该协议具备高效的安全性与保密性。

关键词：生物特征；抗碰撞哈希函数；身份认证；智能卡；密钥协商

Biometric based authentication and key agreement protocol

CHEN Jinmu, HUANG Chaoyang
(School of Information Engineering, Xiamen Ocean Vocational College, Xiamen Fujian 361102, China)

【Abstract】 Biological characteristics are mutually independent and directly related to people, which have undeniable natural characteristics and convenience. With the rapid development of the network, there is an ever-increasing demand for identity security authentication. In order to provide a better security strategy for the authenticity and reliability of personnel identity authentication, a biometric based identity authentication and key agreement protocol is proposed by combining biometric information, anti-collision hash function and smart card. The correctness and security of the protocol are analyzed by means of user simulation attack, privileged internal attack and server spoofing attack. Finally, the analysis proves that the protocol has efficient security and confidentiality.

【Key words】 biological characteristics; anti-collision hash function; identity authentication; smart card; key agreement

0 引 言

互联网的高速发展加快了信息时代的前进步伐，手机、电脑的普及方便了人们对信息的获取，人们对信息的时效性比以往也有着更高的要求[1]。现在越来越多的人都会随时随地通过手机等移动设备访问不同类型的应用程序服务器。如：在线购物、电子商务、政务网站等领域，这些服务器的使用频率就会相对较高。然而，在为用户提供这些在线服务的同时，如何保护这些敏感数据是一个较为重要的问题。作为一种防范措施，认证密钥协议被普遍应用于保护信息和抵御威胁上，帮助网络用户在确保个人信息安全的同时享用各种在线服务。密钥协商是在用户及服务商之间建立一个共同的会话密钥，用来确保其在开放网络中的通信安全。

早在 1981 年，文献[2]中就首次提出了基于口令的认证方案，但该方案无法提供密钥协议、且需要维护用户验证列表，这反而为黑客远程入侵造成了可乘之机。文献[3-5]中提出了改进的基于口令和密钥认证方案，但这些只采用口令的密钥交换协议普遍存在一些共同缺点。如：弱口令、容易受到窃取验证表攻击等等。文献[6-8]提出的基于口令和智能卡的身份认证方案，也存在口令被暴力破解、或者木马窃取以及智能卡丢失的风险。文献[9-10]中提出的基于混沌映射的认证密钥协商协议，虽能在一定程度上提高密钥的保密性，但却缺乏实用性。

为进一步提升远程身份认证协议的安全性能，本文提出了一种基于生物特征的身份认证和密钥协商协议，通过在多服务器体系结构下执行，在保证用户享受网络服务的同时，能确保敏感数据的安全性。

1 认证方案设计

本文提出方案由服务器注册、用户注册、登录、认证、密码更改和用户撤销/重新注册等 6 个阶段组成。

基金项目：福建省中青年教师教育科研项目(JAT191316)；2022 年度校级教科研项目(KYZY202201)。

作者简介：陈金木(1985-)，男，学士，实验师、信息系统项目管理师，主要研究方向：信息安全、网络技术。
通讯作者：陈金木 Email：187290818@qq.com

收稿日期：2022-02-18

1.1　前期准备

抗碰撞哈希函数根据任意长度的二进制字符串输出固定长度的二进制字符串，即 $h = h(x):0,1^* \rightarrow 0,1^n$。对于给定的输入 x，求任意输入 $y \neq x$ 使 $h(x) = h(y)$ 在计算上是不可行的。基于生物特征信息 BIO 通过 Gen 过程，输出一个不可预测的二进制字符串 $R \in \{0,1\}^l$ 和一个辅助二进制字符串 $P \in \{0,1\}^*$。借助这个辅助二进制字符串 P 和另一个生物特征信息 BIO^*，通过 Rep 过程进行再生验算。当 $Gen(BIO) \rightarrow \langle R,P \rangle$ 和 $dis(BIO,BIO^*) \leqslant t$ 保持时，恢复一个对应的不可预测二进制串 R，用 $Rep(BIO^*,P) \rightarrow R$ 表示。方案中应用的符号及说明，见表 1。

表 1　符号说明

Tab. 1　Symbols description

符号	说明
RC	注册中心
S_j	服务器 j
U_i	用户 i
SC_i	用户 i 的智能卡
ID_i	用户 i 标识
PW_i	用户 i 的密码
BIO_i	用户 i 的生物特征信息
Gen，Rep	模糊提取器函数
R_i	用户 i 的不可预测二进制字符串
P_i	用户 i 的辅助二进制字符串
SID_j	服务器 j 的标识
PSK，s	预共享密钥，主密钥
$h(\cdot)$	抗碰撞哈希函数
$\|$，$\oplus$	连接操作，异或操作

1.2　方案实现

1.2.1　服务器注册

服务器 S_j 通过安全通道向注册中心 RC 申请进行服务器注册。当收到加入请求消息时，注册中心 RC 授权服务器 S_j，并根据安全信道，应用密钥交换协议（IKEv2）向服务器 S_j 发送预共享密钥 PSK 和主密钥 s。授权服务器 S_j 接收到预共享密钥 PSK 和主密钥 s 后，在认证阶段采用这些共享数据（如 PSK 和 $h(PSK)$），来验证用户 U_i 的合法性。

1.2.2　用户注册

用户 U_i 通过安全通道向注册中心 RC 提交用户注册信息。具体实现步骤如下：

Step 1　用户 U_i 通过传感器输入个人生物特征信息 BIO_i，并利用传感器内置设备绘制用户 U_i 的生物特征 BIO_i。从 $Gen(BIO_i) \rightarrow (R_i,P_i)$ 中提取 (R_i,P_i)，并将用户 U_i 的辅助二进制字符串 P_i 存储在存储器中；接下来，用户 U_i 选择其身份 ID_i 和密码 PW_i，并计算 $RPW_i = h(R_i \| PW_i)$；最后用户 U_i 通过安全通道，向注册中心 RC 提交其注册请求消息 $\{ID_i,RPW_i\}$。

Step 2　获得注册请求消息后，RC 向其内部数据库中添加一个新的条目 $\langle ID_i,N_i = 1 \rangle$。其中，$N_i$ 表示用户 U_i 的注册次数。然后，RC 选择随机数 u_i，并计算 $A_i = h(ID_i \| s)$、$B_i = h(PSK) \oplus u_i$、$C_i = h(PSK \| u_i) \oplus ID_i$ 以及 $V_i = h(ID_i \| RPW_i)$。最后，RC 通过安全通道发送用户 U_i 的智能卡 SC_i，该 SC_i 包括 $\{A_i,B_i,C_i,V_i,h(\cdot)\}$。

Step 3　收到 SC_i 后，U_i 计算 $E_i = B_i \oplus h(R_i)$，并用 E_i 代替 B_i。此后，U_i 将其辅助二进制字符串 P_i 存储到 SC_i 中，并初始化登录和身份验证环境。

1.2.3　登录

在登录阶段，智能卡 SC_i 能够通过应用用户 U_i 的身份、密码和生物特征信息立即发现错误。具体实现步骤如下：

Step 1　U_i 将其 SC_i 插入智能卡阅读器，输入身份 ID_i 和密码 PW_i，并在传感器上印下生物特征 BIO_i^*；传感器绘制用户 U_i 的个人生物特征信息 BIO_i^*，并在辅助二进制字符串 P_i 的帮助下，从 $Rep(BIO_i^*,P_i) \rightarrow R_i$ 中恢复 R_i。

Step 2　SC_i 计算 $RPW_i = h(R_i \| PW_i)$，并验证 $h(ID_i \| RPW_i) = V_i$ 是否有效。如果有效，则 SC_i 进一步计算 $K_i = h(SID_j \| (ID_i \oplus C_i))$。

Step 3　SC_i 产生随机数 N_1，并计算 $M_1 = N_1 \oplus K_i$、$M_2 = ID_i \oplus K_i$、$M_3 = RPW_i \oplus K_i$、$B_i = E_i \oplus h(R_i)$、$D_i = h(N_1 \| RPW_i \| A_i \| T_i)$。其中，$T_i$ 是附加的时间戳。

Step 4　SC_i 通过开放通道，向 S_j 提交其登录请求消息 $\{M_1,M_2,M_3,B_i,D_i,T_i\}$。

1.2.4　认证

在认证阶段，服务器 S_j 确认登录请求消息的来源并进行认证。具体实现步骤如下：

Step 1　S_j 收到用户 U_i 的登录请求消息后，检查 $T_i - T_j \leqslant \Delta T$。其中，$\Delta T$ 表示时间间隔，是 S_j 收到用户 U_i 登录请求消息的时间。若条件成立，S_j 继续执行以下步骤；否则，登录请求将被拒绝。

Step 2　S_j 检索 $u_i = B_i \oplus h(PSK)$、$K_i = h(SID_j \| h(PSK \| u_i))$、$N_1 = K_i \oplus M_1$、$ID_i = K_i \oplus M_2$、$RPW_i = K_i \oplus M_3$、$A_i = h(ID_i \| s)$，以验证

$h(N_1 \| RPW_i \| A_i \| T_i) = D_i$ 是否有效。

Step 3 如果此验证有效，S_j 将生成另一个随机数 N_2，并计算 U_i 和 S_j 之间的会话密钥 $SK_{ij} = h(ID_i \| SID_j \| N_1 \| N_2)$。

Step 4 S_j 计算 $M_4 = N_2 \oplus h(A_i \| RPW_i \| N_1)$ 和 $M_5 = h(SID_j \| N_1 \| N_2 \| ID_i)$，并通过一个开放通道将其身份验证请求消息 $\{M_4, M_5\}$ 发送到用户 U_i。

Step 5 当获得 S_j 的认证请求消息时，SC_i 检索 $N_2 = h(A_i \| RPW_i \| N_1) \oplus M_4$，并检查 $h(SID_j \| N_1 \| N_2 \| ID_i)$ 是否与 M_5 一致。若一致，SC_i 将计算 $SK_{ij} = h(ID_i \| SID_j \| N_1 \| N_2)$ 和 $M_6 = h(SK_{ij} \| N_1 \| N_2)$。然后 SC_i 通过公共信道向 S_j 发送用户的身份验证答复 $\{M_6\}$。

Step 6 S_j 进一步验证 $h(SK_{ij} \| N_1 \| N_2) = M_6$ 是否有效。如果有效，S_j 在之后的通信中将采用此会话密钥 SK_{ij} 与用户 U_i 通信；否则，认证将被中止。

方案中用户注册、登录、认证各阶段具体实现过程如图 1 所示。

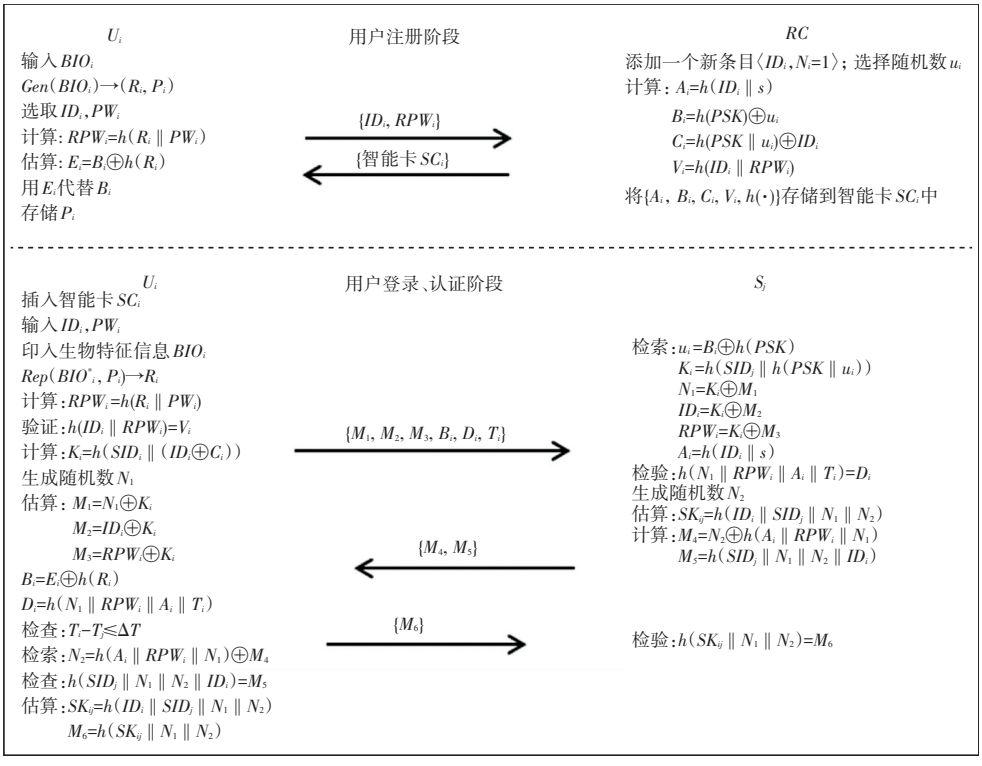

图 1 用户注册、登录、认证实现过程

Fig. 1 User registration phase, login phase and authentication phase

1.2.5 密码更改

在密码更改阶段，用户 U_i 可随意更新个人密码，而不需要服务器或注册中心的任何帮助。具体实现步骤如下：

Step 1 U_i 输入其身份 ID_i 和密码 PW_i，并在传感器上印下生物特征 BIO_i^*；传感器绘制 U_i 的个人生物特征信息 BIO_i^*，并在辅助二进制字符串 P_i 的帮助下，从 $Rep(BIO_i^*, P_i) \rightarrow R_i$ 中恢复 R_i。

Step 2 SC_i 计算 $RPW_i = h(R_i \| PW_i)$，并验证 $h(ID_i \| RPW_i) = V_i$ 是否有效。如果此验证成立，SC_i 将向用户询问新密码；否则，SC_i 将立即终止密码更改。

Step 3 U_i 输入新密码 PW_i^{new}，SC_i 进一步计算 $RPW_i^{new} = h(R_i \| PW_i^{new})$ 和 $V_i^{new} = h(ID_i \| RPW_i^{new})$。

Step 4 SC_i 在没有服务器或注册中心任何帮助的情况下，用 V_i^{new} 代替 V_i。

1.2.6 用户撤销/重新注册

当用户的智能卡被盗或丢失时，用户撤销/重新注册模块将帮助用户撤销其权限或重新注册，使该方案在功能上更加健壮。

当用户需要撤销其特权时，可通过安全通道向注册中心发送撤销请求消息、智能卡和验证消息 $\{RPW_i\}$。若注册中心检查用户有效，则 RC 进一步设置〈$ID_i, N_i = 0$〉来修改相应条目。与用户注册功能类似，在通过安全信道获得重新注册请求消息后，注册中心 RC 执行 1.2.2 节中提到的步骤，并将

$\langle ID_i, N_i = N_i + 1\rangle$ 替换为 $\langle ID_i, N_i\rangle$，帮助用户 U_i 重新注册。

2　方案分析

方案中的认证和密钥协商协议必须满足安全性、功能性和高效率的要求。以下针对本文方案设计，分别从安全性、功能性和效率进行全面分析说明。

2.1　安全性分析

(1)抵抗重放攻击。该方案利用时间戳和随机数来抵抗重放攻击。虽然攻击者通过窃听，得到用户 U_i 先前的登录请求消息 $\{M_1, M_2, M_3, B_i, D_i, T_i\}$，并将其发送给服务器 S_j，但服务器 S_j 可以通过式(1)验证时间戳 T_i 的及时性和随机数 N_1 的正确性，来检查该消息的合法性。公式(1)的数学表达见如下：

$$D_i = h(N_1 \| RPW_i \| A_i \| T_i) \tag{1}$$

其中，时间戳 T_i 和随机数 N_1 对于每个会话都是不同的，因此攻击者会被服务器 S_j 拒绝。

(2)抵抗拒绝服务攻击。当攻击者试图通过窃听和重复发送用户以前的登录请求消息，来削弱或消除服务器的能力时，服务器会验证时间戳 T_i 的新鲜性，同时检查 $D_i = h(N_1 \| RPW_i \| A_i \| T_i)$ 是否成立。此时，服务器会将攻击者视为恶意黑客并终止此会话，以此抵抗拒绝成立服务攻击。

(3)抵抗密码猜测攻击。攻击者利用 SPA 或 DPA 等侧通道攻击，从用户的智能卡中提取敏感数据 A_i、C_i、E_i、V_i 和 P_i。但是，在没有生物特征信息 BIO_i、预共享密钥 PSK、主密钥 s 和随机数 N_1 的情况下，无法验证用户的密码 PW_i 是否正确。在该方案中，是由具有较高熵的不可预测的二进制字符串 R_i 保护用户 U_i 的密码 PW_i。因此，本文协议对密码猜测攻击是安全的。

(4)抵抗智能卡攻击。在没有密码 PW_i 或生物特征信息 BIO_i 的情况下，攻击者发起智能卡攻击，以收集存储在智能卡 SC_i 中的一些敏感数据，并实现服务器 S_j 的身份验证。在该方案中，攻击者能够通过 SPA 或 DPA 获取用户 U_i 中保存在智能卡 SC_i 中的敏感数据 A_i、C_i、E_i、V_i 和 P_i。用户 U_i 和服务器 S_j 之间的会话密钥 SK_{ij} 计算如下：

$$K_i = (SID_j \| (ID_i \oplus C_i)) \tag{2}$$

$$N_1 = K_i \oplus M_1 \tag{3}$$

$$N_2 = h(A_i \| RPW_i \| N_1) \oplus M_4 \tag{4}$$

$$SK_{ij} = h(ID_i \| SID_j \| N_1 \| N_2) \tag{5}$$

攻击者通过一个公共信道获取 M_1 和 M_4 是可行的。但是，检索随机数 N_1 或 N_2 是相当困难的。因此，本文协议能够抵御智能卡攻击。

(5)抵抗用户模拟攻击。在用户模拟攻击中，攻击者试图在没有密码 PW_i 或生物特征信息 BIO_i 的情况下模拟用户 U_i。在该方案中，攻击者即使窃听用户 U_i 先前的登录请求消息 $\{M_1, M_2, M_3, B_i, D_i, T_i\}$ 也无法获取 $h(PSK)$。虽能通过 SPA 或 DPA 从智能卡 SC_i 中提取用户 U_i 的敏感数据，但不能检索随机数 N_1、N_2 或会话密钥 SK_{ij}。因此，本文协议对用户模拟攻击是安全的。

(6)抵抗特权内部攻击。假设攻击者是恶意内部人员，具有访问授权系统的特权，试图模拟用户 U_i。为了达到这一目的，攻击者收集用户 U_i 的注册请求消息 $\{ID_i, RPW_i\}$ 并窃取其智能卡 SC_i，但是却无法获得 $h(PSK)$ 和 B_i。即使从用户 U_i 的智能卡 SC_i 中提取敏感数据，攻击者也无法传递正确的登录请求消息 $\{M_1, M_2, M_3, B_i, D_i, T_i\}$，并无法检索密码 PW_i 或生物特征信息 BIO_i。因此，本文协议能够抵抗特权内部攻击。

(7)抵抗服务器欺骗攻击。假设攻击者是恶意的内部人员，并试图伪装成服务器 S_j，通过收集敏感数据来欺骗用户 U_i。但是由于 $h(PSK)$ 难以检索，使得攻击者无法被用户 U_i 成功认证，并无法获得随机数 N_1 和有效的身份验证请求消息 $\{M_4, M_5\}$。因此，本文协议能够抵抗服务器欺骗攻击。

(8)提供匿名性保护。在该方案登录阶段，用户 U_i 生成其动态身份 $M_2 = ID_i \oplus K_i$。其中，K_i 无法被攻击者从任何请求或回复消息中检索到。因此，攻击者没有能力获取用户 U_i 的身份 ID_i。然而，当接收到用户 U_i 的登录请求消息时，授权服务器 S_j 计算 $u_i = B_i \oplus h(PSK)$，并进一步计算 $K_i = h(SID_j \| h(PSK \| u_i))$，以便用户 U_i 匿名地实现服务器 S_j 的认证。这表明，用户 U_i 的真实身份 ID_i 不会被任何未经授权的参与者泄露。因此，本文协议能够提供有效匿名性。

(9)具备前向保密性。在该方案中即使长期密钥被检索，仍具有前向保密性保护会话密钥。生成会话密钥 SK_{ij} 的计算如下：

$$K_i = h(SID_j \| h(PSK \| u_i)) \tag{6}$$

$$N_1 = K_i \oplus M_1 \tag{7}$$

$$ID_i = K_i \oplus M_2 \tag{8}$$

$$N_2 = h(A_i \| RPW_i \| N_1) \oplus M_4 \tag{9}$$

$$SK_{ij} = h(ID_i \| SID_j \| N_1 \| N_2) \tag{10}$$

虽然攻击者能够计算出长期密钥 $h(PSK)$，但却无法计算一些敏感数据（如：RPW_i、K_i 和 PSK 等），且无法获得随机数 N_1 或 N_2。另外，攻击者也很难检索用户 U_i 和服务器 S_j 之间的会话密钥 SK_{ij}。因此，本文协议能提供前向保密性。

2.2 功能性分析

（1）相互认证功能。方案中，用户 U_i 和服务器 S_j 利用一些敏感数据（如 N_1，N_2，K_i，T_i 和 SK_{ij}）进行认证。特别是，服务器 S_j 检查 $h(N_1 \| RPW_i \| A_i \| T_i) = D_i$ 和 $h(SK_{ij} \| N_1 \| N_2) = M_6$ 是否有效。类似地，用户 U_i 验证 $h(SID_j \| N_1 \| N_2 \| ID_i)$ 是否与 M_5 一致，实现了相互认证功能。

（2）会话密钥协商功能。在身份验证阶段，建立了服务器 S_j 和用户 U_i 之间的会话密钥 $SK_{ij} = h(ID_i \| SID_j \| N_1 \| N_2)$，以保护后续通信。由于 N_1、N_2 在每个认证阶段都会发生变化，因此会话密钥 SK_{ij} 在每个会话期间都是不同的。对于攻击者来说，这将很难检索到会话密钥 SK_{ij}。因此，本文协议具有会话密钥一致性。

（3）用户撤销/重新注册功能。方案中，注册中心通过安全通道获取到用户的撤销/重新注册请求消息时，通过修改 $\langle ID_i, N_i \rangle$ 帮助用户实现用户撤销/重新注册功能。

（4）生物特征信息保护功能。在传统方案中，用户 U_i 将生物特征信息 BIO_i 直接存储在其智能卡 SC_i 中，而没有适当的保护。因此，攻击者能够通过侧通道进行攻击，从丢失或被盗的智能卡 SC_i 中提取用户 U_i 的生物特征 BIO_i。由于不可预测的二进制字符串 R_i 可由抗碰撞哈希函数进行保护，文中利用抗碰撞哈希函数可保护不可预测的二进制字符串 R_i 这个特性机制，来保存用户 U_i 的生物特征信息 BIO_i。因此，攻击者将无法提取用户 U_i 的生物特征信息，使协议达到生物特征信息的保护功能。

2.3 效率分析

本文方案在存储需求、通信开销和计算开销方面的效率分析如下：

（1）存储要求。对于存储需求，可将这些存储在用户 U_i 的智能卡 SC_i 中的消息作为存储开销。如果采用 SHA-1 算法，则 N_1 和 N_2 的字节长度都为 20，用户 U_i 的标识 ID_i 的字节长度为 20，时间戳 T_i 的字节长度为 2，抗碰撞哈希函数输出的字节长度为 20。因此就可以计算所提的方案中存储数据的字节长度，所有保存的消息 $\{A_i, C_i, E_i, V_i, P_i\}$ 共需要 20+20+20+20+20=100（bytes）。

（2）通信开销。为估计通信开销，需要在登录阶段将用户 U_i 的登录请求消息 $\{M_1, M_2, M_3, B_i, D_i, T_i\}$ 提交给服务器 S_j。根据上述假设，该消息的长度为 20+20+20+20+20+2=102（bytes）。服务器 S_j 的认证请求消息 $\{M_4, M_5\}$ 和用户 U_i 的认证应答 $\{M_6\}$ 的通信开销为 20+20+20=60（bytes）。因此，本文协议的总通信开销为 102+60=162（bytes）。

（3）成本计算。考虑到计算复杂度，文中将抗碰撞哈希函数的频率作为计算代价。在 CPU 为 3.7 GHz、RAM 为 4 GB 的环境中，执行抗碰撞哈希函数平均需要0.002 1 ms。在该方案中，分别在登录和认证阶段执行了 3 次和 10 次抗碰撞哈希函数。最终本文协议共需要0.010 9+0.026 8=0.037 7 ms的计算开销。

3 安全与性能验证

为了证明本文协议在相关方面均有良好的表现，特将本文方案与文献[11-14]中各方案在安全性、功能性和效率等方面做了相关比较。比较结果见表 2~表 5。

表 2 本协议与其他协议的安全性比较

Tab. 2 Security comparison between this agreement and other agreements

安全性	文献[11]	文献[12]	文献[13]	文献[14]	本文协议
匿名性保护	×	×	√	√	√
抗重放攻击	√	√	√	√	√
抗拒绝服务攻击	×	√	√	×	√
抗用户模拟攻击	×	×	×	√	√
抗特权内部攻击	×	√	×	√	√
抗密码猜测攻击	√	√	√	√	√
抗智能卡攻击	×	√	√	√	√
抗服务器欺骗攻击	×	×	×	√	√
前向保密性	×	√	×	×	√

表 3　本协议与其他协议的功能性比较

Tab. 3　Functional comparison between this agreement and other agreements

功能性	文献[11]	文献[12]	文献[13]	文献[14]	本文协议
相互认证	√	√	√	√	√
会话密钥协商	√	√	√	√	√
用户撤销/重新注册	×	×	√	√	√
生物特征信息保护	√	√	√	√	√

表 4　本协议与其他协议的通信开销与存储需求比较

Tab. 4　Comparison of communication overhead and storage requirements between this protocol and other protocols　bytes

通信开销存储需求	文献[11]	文献[12]	文献[13]	文献[14]	本文协议
登录阶段通信开销	80	80	102	62	102
身份验证阶段通信开销	80	80	80	62	60
总通信开销	160	160	182	124	162
存储需求	100	80	100	100	100

表 5　本协议与其他协议的计算成本比较

Tab. 5　Comparison of calculated costs between this agreement and other agreements

计算成本	文献[11]	文献[12]	文献[13]	文献[14]	本文协议
登录阶段计算成本	$7T_h$	$3T_h + 1T_p + 2T_s$	$4T_h$	$5T_h$	$5T_h$
登录阶段执行成本	0.016 1 ms	2.242 1 ms	0.015 2 ms	0.012 8 ms	0.010 9 ms
身份验证阶段计算成本	$11T_h$	$5T_h + 3T_p + 3T_s$	$11T_h$	$7T_h + 2T_s$	$13T_h$
身份验证阶段执行成本	0.025 3 ms	6.703 3 ms	0.025 7 ms	0.027 5 ms	0.026 8 ms
总执行成本	0.041 4 ms	8.95 4 ms	0.040 9 ms	0.040 3 ms	0.037 7 ms

从表 2 中可以看出，文献[11]的方案无法抵抗拒绝服务攻击、用户模拟攻击、特权内部攻击、智能卡攻击和服务器欺骗攻击，其方案无法提供匿名性保护和前向保密性。文献[12]的方案无法抵抗用户模拟攻击和服务器欺骗攻击，方案不具有匿名性保护。文献[13]的方案不能防止用户模拟攻击、特权内部攻击和服务器欺骗攻击，其方案也无法实现前向保密性。文献[14]中提出的方案对拒绝服务攻击是不安全的，并且不能提供前向保密性。结果表明，本文协议具有更高的安全性能。

从表 3 中可见，文献[11]、文献[12]中提出的方案均不能提供用户撤销/重新注册。结果表明，本文协议提供了更多的功能属性。

由表 4 可见，在相同的存储需求下，本文协议在通信开销上表现出了令人满意的性能。

表 5 中，T_h 表示抗碰撞哈希函数的计算时间；T_p 表示基于椭圆曲线的点乘计算时间；T_s 表示对称加/解密计算时间；T_c 表示 Chebyshev 混沌映射计算时间。总体可见，本文协议所需的计算成本相对较低。

综上所述，本文协议能抵抗多种常见网络攻击，同时能提供用户匿名性与前向保密性。与其它方案相比，本文提出的方案能进一步降低计算复杂度，并以独特的方式提供更多的功能。在通信开销和存储需求相同的情况下，本方案在计算复杂度方面具有明显的优势。

4　结束语

本文在现有的基于口令及智能卡身份认证协议基础上，通过应用抗碰撞哈希函数、二进制异或运算和级联操作保障协议的安全性能，提出了一种基于生物特征的身份认证和密钥协商协议，协议适用于多服务器体系结构及分布式网络。经过与其它方案的安全与效率对比分析，证明本文方案能抵抗各种攻击并且提供匿名性，更具有安全性和实用性。

参考文献

[1] 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(S2)：409-413，437.

[2] LAMPORT L. Password authentication with insecure communication [J]. Communications of the ACM，1981，24(11)：770-772.

[3] VOSSAERT J，LAPON J，NAESSENS V. Out-of-band password based authentication towards Web services[J]. Lecture Notes in Electrical Engineering，2014，302：181-191.

(下转第 26 页)