一种改进的适用于多服务器架构的匿名认证协议

余宜诚，胡亮，迟令，初剑峰*

(吉林大学 计算机科学与技术，长春 130012)

摘 要：为了保证合法用户与应用服务器双方的通信安全，如何实现会话双方高效安全的相互认证是多服务器架构网络系统急需解决的重要安全问题。针对 Guo 等人提出的三因子认证密钥协商协议无法实现前向安全性且不支持用户的生物特征更新等安全缺陷，引入 Diffie-Hellman 密钥交换技术，提出了改进的匿名认证密钥协商协议。分析表明，改进协议在弥补原方案的安全缺陷的同时，满足多服务器架构网络环境的安全需求，能够抵御各类已知的攻击方法。

关键词：计算机系统结构；认证；多服务器架构；匿名；密钥协商

中图分类号：TP309 **文献标志码：**A

An improved anonymous authentication protocol for multi-server architectures

Yu Yicheng，Hu Liang，Chi Ling，Chu Jianfeng

(*College of Computer Science and Technology, Jilin University, Changchun 130012, China*)

Abstract: In order to ensure the safe communication between legitimate users and application servers, how to achieve efficient and secure mutual authentication between two participants is an important security issue for multi-server architecture. Guo et al.'s proposed three-factor authentication and key agreement protocol cannot achieve perfect forward secrecy and cannot support the update of user's biometric. In order to remedy these flaws, we propose an improved authentication protocol for multi-server architectures by use of Diffie-Hellman key exchange technology. Analysis shows that proposed protocol is able to remedy the security flaws of the original scheme, meet the security requirements of multi-server environment and is able to withstand various possible attacks.

Key words: computer system architecture; authentication; multi-server architecture; anonymous; key agreement

0 引言

随着硬件性能的提高和无线通信技术的发展，移动互联网用户可以随时随地访问网络服务，如网络购物和移动支付。用户对网络服务需求的不断增长使得传统的单服务器架构演变成多服务器架构[1]。在多服务器架构中，用户可以通过无线网络访问不同服务器提供的多种网络服务。

由于公共信道的不安全性，攻击者可以窃听、截取、分析、删除和修改无线网络中传输的数据[2]。因此，为了保护网络中合法用户的隐私、防止非法用户危害网络的安全性，设计一种有效安全的认证协议来保证网络的通信安全是极其必要的。

迄今，研究者们提出了许多适用于多服务器架构的认证协议[3-9]，然而其中大多数协议存在着不同的安全缺陷。2010 年，Yang 等人结合智能卡、用户口令和生物特征提出了一种多服务器架构认证协议[10]，但是 D Mishra 等人指出该协议易受到内部攻击且计算开销较大[11]。2011 年，Sood 等人提出了一种多服务器架构下基于动态身份的认证协议[12]，然而他们的协议无法抵御智能卡丢失攻击和认证表攻击丢失[13]。2014 年，Chuang 等人提出了

收稿日期：年-月-日.（小五号宋体，此处为页脚，和正文分开）
基金项目：国家重点研发专项（2017YFA0604500）；国家科技支撑项目（2014BAH02F00）；国家自然科学基金（61701190）；吉林省青年科学基金项目（20160520011JH）;吉林省省校共建示范项目（SXGJSF2017-4）.
作者简介：余宜诚（1990-），男，博士研究生. 研究方向：网络与信息安全.E-mail:yycitb@vip.qq.com
通信作者：初剑峰（1978-），男，副教授，博士.研究方向：信息安全.E-mail:chujf@jlu.edu.cn

一种多服务器架构下基于可信计算的匿名认证协议[14]。然而 D Mishra 等人分析指出该协议无法抵御智能卡丢失攻击和 DOS 攻击[11]。

2017 年，Guo 等人提出了一种适用于多服务器架构的、具有鲁棒性的三因子认证密钥协商协议，并称其协议高效安全且满足多服务器架构的所有安全需求[15]。然而，通过分析，发现 Guo 等人的协议不具备前向安全性，具有安全隐患，并且协议不支持用户的生物特征更新功能。为此，本文提出了一种新的改进协议克服原有协议的安全缺陷并完善了协议的生物特征更新功能。

1　相关基础知识

1.1 计算性 Diffie-Hellman 问题（CDH 问题）

令 g 为以大素数 q 为阶的循环群 G 的一个生成元；给定 $g, g^a, g^b \in G$（a，b 未知），计算 $g^{ab} \in G$。算法 C 在多项式时间内成功解决 CDH 问题的概率定为义 $Pr[C(g, g^a, g^b) = g^{ab} | a, b \in Z_q^*]$，概率取决于算法 C 的随机选择及 a，b 的随机选取。

CDH 假设：对于任意多项式时间算法 C，解决 CDH 问题的概率可忽略不计。

1.2 网络模型

多服务器网络架构通常由三方参与者组成：用户、服务器及注册中心 *RC*。

注册中心 *RC* 被认为是可信的第三方，负责系统参数的生成。同时，根据用户与服务器的身份标识，*RC* 为用户与服务器生成私钥。用户与服务器通过向 *RC* 注册入网，当用户与服务器完成相互认证之后，用户可以访问服务器提供的移动服务。网络模型如图 1 所示。

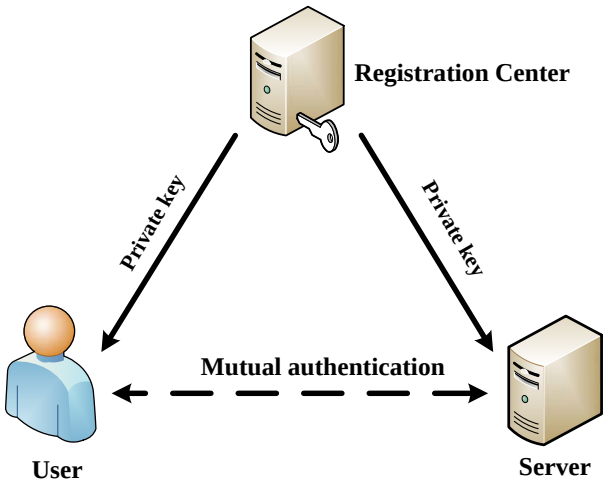

图 1 网络模型

Fig.1 Network model

1.3 安全需求

匿名性：为保护用户的隐私，认证协议应实现用户匿名性，即攻击者无法通过截取的信息提取用户的真实身份。

不可追踪性：为了进一步保护用户的隐私，认证协议应实现不可追踪性，即攻击者无法分辨两个会话是否为同一用户参与。

相互认证：为确保会话参与双方的合法性，认证协议应实现会话双方的相互认证。

会话密钥协商：为确保参与双方未来通信的安全性，认证协议需要实现会话双方协商生成用于未来通信加密的会话密钥。

前向安全性：认证协议应保证，当一方或多方的长期私钥被攻击者捕获，攻击者无法得到此前所建立的会话密钥。

n 因子安全：当攻击者捕获任意 *n*-1 个认证因子（口令、智能卡、生物特征），协议需保证剩余的那个认证因子仍然是安全的。

抵御各类攻击：基于网络环境的性质，协议需要能够抵御内部攻击、离线密码猜测攻击、假冒用户攻击、假冒服务器攻击、智能卡丢失攻击、重放攻击、窃听攻击等多种攻击。

2 Guo 等人的协议的回顾

Guo 等人的协议涉及 3 方参与者：用户 U_i、服务器 S_j、注册中心 *RC*。*RC* 负责系统参数的生成。*RC* 随机生成一个系统密钥 *PSK* 并选择两个安全的 *Hash* 函数 $H(\cdot)$ 和 $h(\cdot)$。最后，*RC* 公布系统参数 $\{H(\cdot), h(\cdot)\}$。

协议由 5 个阶段组成：用户注册阶段、服务器注册阶段、登录阶段、认证阶段以及口令修改阶段。

2.1 服务器注册阶段

当一个新服务器 S_j 想要加入多服务器网络系统时，需要先通过安全信道向注册中心 *RC* 申请注册，

收稿日期：年-月-日.（小五号宋体，此处为页脚，和正文分开）
基金项目：国家重点研发专项（2017YFA0604500）；国家科技支撑项目（2014BAH02F00）；国家自然科学基金（61701190）；吉林省青年科学基金项目（20160520011JH）;吉林省省校共建示范项目（SXGJSF2017-4）.
作者简介：余宜诚（1990-），男，博士研究生. 研究方向：网络与信息安全.E-mail:yycitb@vip.qq.com
通信作者：初剑峰（1978-），男，副教授，博士.研究方向：信息安全.E-mail:chujf@jlu.edu.cn

执行过程如下：

（1）首先 S_j 设定选取代表自己的唯一身份标识 SID_j，并将 SID_j 和其公钥 Pub_j 发送给注册中心 RC。

（2）收到 $\{SID_j, Pub_j\}$ 后，注册中心 RC 通过安全信道将系统密钥 PSK 送给服务器 S_j，并公布 S_j 的公钥 Pub_j。

2.2 用户注册阶段

当一个新用户 U_i 想要访问服务器时，需要先通过安全信道向注册中心 RC 申请注册，执行过程如下：

（1）首先 U_i 选取代表自己的唯一身份标识 ID_i 与口令 PW_i，并输入生物特征 BIO_i；计算 $IDB_i = h(ID_i \| H(BIO_i))$，$PWD_i = h(PW_i \| H(BIO_i))$；最后 U_i 将 $\{h(ID_i), PWD_i, IDB_i\}$ 发送给注册中心 RC。

（2）收到 $\{h(ID_i), PWD_i, IDB_i\}$ 后，注册中心 RC 计算 $V_i = h(h(ID_i) \| PWD_i)$，$W_i = h(h(ID_i) \| PSK) \oplus IDB_i$，并将存储了参数 $\{V_i, W_i, H(\cdot), h(\cdot)\}$ 的智能卡安全地传递给用户 U_i。

2.3 登录阶段

完成注册阶段后，用户 U_i 可使用其智能卡进行登录，执行过程如下：

（1）用户 U_i 将其智能卡插入终端，输入自己的身份标识 ID_i、口令 PW_i 及物特征 BIO_i;；智能卡计算 $PWD_i = h(PW_i \| H(BIO_i))$，并检查等式 $V_i ? = h(h(ID_i) \| PWD_i)$ 是否成立；若等式不成立，智能卡终止协议。

（2）若等式成立，智能卡选择随机数 n_1，获取当前的时间戳 T_1，并计算 $IDB_i = h(ID_i \| H(BIO_i))$，$K = h((W_i \oplus IDB_i) \oplus h(ID_i \| n_1))$，

$M_1 = E_{Pub_j}(ID_i \| n_1)$, $Z_i = h(n_1 \| ID_i \| K \| T_1)$；最后将请求信息 $\{M_1, Z_i, T_1\}$ 通过公共信道发送给服务器 S_j。

2.4 认证阶段

（1）服务器 S_j 收到用户 U_i 的登录请求后，S_j 先验证 $|T_c - T_1| \le \Delta T$ 时间戳的有效性。若有效，S_j 使用其私钥解密 M_1，$(ID_i \| n_1) = E_{Pri_j}(M_1)$，计算

$K = h(h(h(ID_i) \| PSK) \oplus h(ID_i \| n_1))$，并验证等式 $Z_i ? = h(n_1 \| ID_i \| K \| T_1)$ 是否成立；若成立，S_j 接受 U_i 的登录请求；否则，S_j 终止会话。

（3）之后，S_j 生成一个随机数 n_2，获取当前的时间戳 T_2，并计算 $M_2 = n_2 \oplus K$，

$M_3 = h(ID_i \| n_1 \| n_2 \| K \| T_2)$，$SK_{ij} = h(n_1 \| n_2 \| K \| ID_i)$；

S_j 将 $\{M_2, M_3, T_2\}$ 传回 U_i。

（4）U_i 收到 $\{M_2, M_3, T_2\}$ 后，检测 T_2 的有效性后，计算 $n_2 = M_2 \oplus K$，并验证等式 $M_3 ? = h(ID_i \| n_1 \| n_2 \| K \| T_2)$ 是否成立；若成立，U_i 完成对 S_j 的认证，计算 $SK_{ij} = h(n_1 \| n_2 \| K \| ID_i)$，

$M_4 = h(SK_{ij} \| ID_i \| n_2 \| T_3)$，$T_3$ 为当前的时间戳，并将 $\{M_4, T_3\}$ 发送给服务器 S_j。

（5）S_j 收到 $\{M_4, T_3\}$ 后，检测 T_3 的有效性，验证等式 $M_4 ? = h(SK_{ij} \| ID_i \| n_2 \| T_3)$ 是否成立，进一步认证 U_i 身份的合法性。若成立，U_i 和 S_j 计算得到两者间用于未来通信的会话密钥 $SK = h(n_1 \| n_2 \| K \| ID_i)$。

2.5 口令修改阶段

当用户 U_i 想将其口令 PW_i 修改为 PW_{new} 时，执行如下过程：

（1）用户 U_i 将其智能卡插入终端，输入自己的身份标识 ID_i、旧口令 PW_i、新口令 PW_{new} 及生物特征 BIO_i；智能卡计算 $PWD_i = h(PW_i \| H(BIO_i))$，并验证 $V_i ? = h(ID_i \| PWD_i)$ 是否成立；若不成立，智能卡终止协议。

（2）若等式成立，智能卡计算

$PWD_i^* = h(PW_{new} \| H(BIO_i))$，$V_i^* = h(ID_i \| PWD_i^*)$。之后，智能卡将 V_i^* 替换原有的参数 V_i。

3 Guo 等人的协议缺陷

3.1 前向安全性失效

通过对 Guo 等人的协议的分析，我们发现其协议并不能实现协议的前向安全性，即当攻击者 $\mathcal{A}$ 捕获或偶然得到任意服务器 S_j 的长期私钥 Pri_j 和系统密钥 PSK 时，$\mathcal{A}$ 可以通过之前截获的用户 U_i 与服务器 S_j 的登录请求信息及回应信息，推导出之前的会话密钥，攻击过程如下：

（1）假设攻击者 $\mathcal{A}$ 捕获得到服务器 S_j 的长期

收稿日期：年-月-日.（小五号宋体，此处为页脚，和正文分开）
基金项目：国家重点研发专项（2017YFA0604500）；国家科技支撑项目（2014BAH02F00）；国家自然科学基金（61701190）；吉林省青年科学基金项目（20160520011JH）;吉林省省校共建示范项目（SXGJSF2017-4）.
作者简介：余宜诚（1990-），男，博士研究生. 研究方向：网络与信息安全.E-mail:yycitb@vip.qq.com
通信作者：初剑峰（1978-），男，副教授，博士.研究方向：信息安全.E-mail:chujf@jlu.edu.cn

私钥 Pri_j 和系统密钥 PSK。并且 $\mathcal{A}$ 保留有之前截获的用户 U_i 与服务器 S_j 的登录请求信息 $\{M_1, Z_i, T_1\}$ 及回应信息 $\{M_2, M_3, T_2\}$。

（2）$\mathcal{A}$ 根据登录请求信息 $\{M_1, Z_i, T_1\}$，使用 Pri_j 解密 M_1，$(ID_i \| n_1) = E_{Pri_j}(M_1)$ 得到 ID_i 和 n_1，计算得到 $K = h(h(h(ID_i) \| PSK) \oplus h(ID_i \| n_1))$；

（3）$\mathcal{A}$ 根据服务器回应信息 $\{M_2, M_3, T_2\}$，计算得 $n_2 = M_2 \oplus K$，其中 K 由上一步计算得到；

（3）$\mathcal{A}$ 推导出会话密钥 $SK = h(n_1 \| n_2 \| K \| ID_i)$。

3.2 生物特征无法更新

在 Guo 等人的协议中，仅支持用户对其口令的修改。然而实际应用中，当用户的生物特征被攻击者获取或者用户需要转让账户时，都需要对生物特征进行更新，因此协议支持用户对生物特征的更新是必要的。

4 对改进的协议

为弥补 Guo 等人的协议在第 3 节中提到的协议缺陷，本文设计了一个新的改进协议。协议同样涉及三方参与者：用户 U_i、服务器 S_j、注册中心 RC。RC 负责系统参数的生成。RC 选择以大素数 p 为模的循环群，并选择 g 为原根；RC 随机生成一个系统密钥 PSK 并选择两个安全的 $Hash$ 函数 $H(\cdot)$ 和 $h(\cdot)$。最后，RC 公布系统参数 $\{g, p, H(\cdot), h(\cdot)\}$。

协议也同样包含 5 个阶段：服务器注册阶段、用户注册阶段、登录阶段、认证阶段以及口令与生物特征修改阶段。

4.1 服务器注册阶段

当一个新服务器 S_j 想要加入多服务器网络系统时，需要先通过安全信道向注册中心 RC 申请注册，执行过程如下：

（1）首先 S_j 设定选取代表自己的唯一身份标识 SID_j，并将 SID_j 和其公钥 Pub_j 发送给注册中心 RC。

（2）收到 $\{SID_j, Pub_j\}$ 后，注册中心 RC 通过安全信道将系统密钥 PSK 送给服务器 S_j，并公布 S_j 的公钥 Pub_j。

4.2 用户注册阶段

当一个新用户 U_i 想要访问服务器时，需要先通过安全信道向注册中心 RC 申请注册，执行过程如下：

（1）首先 U_i 选取代表自己的唯一身份标识 ID_i 与口令 PW_i，并输入生物特征 BIO_i；计算 $IDB_i = h(ID_i \| H(BIO_i))$，$PWD_i = h(PW_i \| H(BIO_i))$；最后 U_i 将 $\{h(ID_i), PWD_i, IDB_i\}$ 发送给注册中心 RC。

（2）收到 $\{h(ID_i), PWD_i, IDB_i\}$ 后，注册中心 RC 计算 $V_i = h(h(ID_i) \| PWD_i)$，$W_i = h(h(ID_i) \| PSK) \oplus IDB_i$，并将存储了参数 $\{V_i, W_i, H(\cdot), h(\cdot)\}$ 的智能卡安全地传递给用户 U_i。

4.3 登录阶段

完成注册阶段后，用户 U_i 可使用其智能卡进行登录，执行过程如下：

（1）用户 U_i 将其智能卡插入终端，输入自己的身份标识 ID_i、口令 PW_i 及物特征 BIO_i;；智能卡计算 $PWD_i = h(PW_i \| H(BIO_i))$，并检查等式 $V_i ? = h(h(ID_i) \| PWD_i)$ 是否成立；若等式不成立，智能卡终止协议。

（2）若等式成立，智能卡选择随机数 x，获取当前的时间戳 T_1，并计算 $X_i = g^x$，

$IDB_i = h(ID_i \| H(BIO_i))$，$K = h((W_i \oplus IDB_i) \oplus h(ID_i \| X_i))$，

$M_1 = E_{Pub_j}(ID_i \| X_i)$，$Z_i = h(X_i \| ID_i \| K \| T_1)$；最后将请求信息 $\{M_1, Z_i, T_1\}$ 通过公共信道发送给服务器 S_j。

4.4 认证阶段

（1）服务器 S_j 收到用户 U_i 的登录请求后，S_j 先验证 $|T_c - T_1| \leq \Delta T$ 时间戳的有效性。若有效，S_j 使用其私钥解密 M_1，$(ID_i \| X_i) = E_{Pri_j}(M_1)$，计算 $K = h(h(ID_i) \| PSK) \oplus h(ID_i \| X_i))$，并验证等式 $Z_i ? = h(X_i \| ID_i \| K \| T_1)$ 是否成立；若成立，S_j 接受 U_i 的登录请求；否则，S_j 终止会话。

（3）之后，S_j 生成一个随机数 y，获取当前的时间戳 T_2，并计算 $Y_j = g^y$，$M_2 = Y_j \oplus K$，

$M_3 = h(ID_i \| X_i \| Y_j \| K \| T_2)$，

$SK_{ji} = h(X_i \| Y_j \| X_i^y \| K \| ID_i)$；$S_j$ 将 $\{M_2, M_3, T_2\}$ 传回 U_i。

（4）U_i 收到 $\{M_2, M_3, T_2\}$ 后，检测 T_2 的有效性

收稿日期：年-月-日.（小五号宋体，此处为页脚，和正文分开）

基金项目：国家重点研发专项（2017YFA0604500）；国家科技支撑项目（2014BAH02F00）；国家自然科学基金（61701190）；吉林省青年科学基金项目（20160520011JH）;吉林省省校共建示范项目（SXGJSF2017-4）.

作者简介：余宜诚（1990-），男，博士研究生. 研究方向：网络与信息安全.E-mail:yycitb@vip.qq.com

通信作者：初剑峰（1978-），男，副教授，博士.研究方向：信息安全.E-mail:chujf@jlu.edu.cn

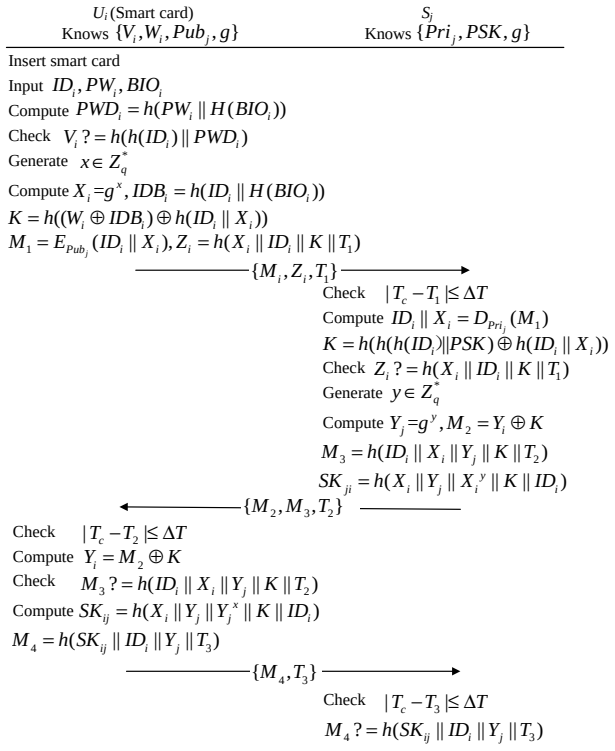

图 2 改进协议的登录与认证阶段

Fig.2 Login and authentication phases of proposed scheme

后，计算 $Y_j = M_2 \oplus K$，并验证等式 $M_3 ? = h(ID_i \| X_i \| Y_j \| K \| T_2)$ 是否成立；若成立，U_i 完成对 S_j 的认证，计算 $SK_{ij} = h(X_i \| Y_j \| Y_j^x \| K \| ID_i)$，$M_4 = h(SK_{ij} \| ID_i \| Y_j \| T_3)$，$T_3$ 为当前的时间戳，并将 $\{M_4, T_3\}$ 发送给服务器 S_j。

（5）S_j 收到 $\{M_4, T_3\}$ 后，检测 T_3 的有效性，验证等式 $M_4 ? = h(SK_{ji} \| ID_i \| Y_j \| T_3)$ 是否成立，进一步认证 U_i 身份的合法性。若成立，U_i 和 S_j 计算得到两者间用于未来通信的会话密钥

$SK_{ij} = h(X_i \| Y_j \| Y_j^x \| K \| ID_i) = h(X_i \| Y_j \| X_i^y \| K \| ID_i) = SK_{ji}$。

改进协议的登录与认证阶段如图 2 所示。

4.5 口令与生物特征修改阶段

当用户 U_i 需要修改其口令或者生物特征时，执行如下过程：

（1）用户 U_i 将其智能卡插入终端，输入自己的身份标识 ID_i、旧口令 PW_i 及旧生物特征 BIO_i；智能卡计算 $PWD_i = h(PW_i \| H(BIO_i))$，并验证 $V_i ? = h(ID_i \| PWD_i)$ 是否成立；若不成立，智能卡终止协议。

（2）若等式成立，用户输入新口令 PW_{new} 和新的生物特征 BIO_{new}，智能卡计算 $IDB_i = h(ID_i \| H(BIO_i))$，$PWD_i^* = h(PW_{new} \| H(BIO_{new}))$，$V_i^* = h(ID_i \| PWD_i^*)$，$W_i^* = W_i \oplus IDB_i \oplus h(ID_i \| H(BIO_{new}))$。之后，智能卡将 V_i^*, W_i^* 替换原有的参数 V_i, W_i。

5 安全性分析

改进方案在继承了原方案优良特性的情况下，有效地弥补了原方案的缺陷。根据下面的安全性分析，可知改进的方案具有匿名性、不可追踪性、前向安全性，能给实现会话密钥协商、三因子安全，且对内部攻击、离线密码猜测攻击、假冒用户攻击、假冒服务器攻击、智能卡丢失攻击、重放攻击、窃听攻击也十分有效。

5.1 匿名性及不可追踪性

用户 U_i 请求登录服务器 S_j 并相互认证的过程中，攻击者仅可以截取到与用户身份 ID_i 有关的数据 $M_1 = E_{Pub_j}(ID_i \| X_i), Z_i = h(X_i \| ID_i \| K \| T_1)$，$M_3 = h(ID_i \| X_i \| Y_j \| K \| T_2)$，$M_4 = h(SK_{ij} \| ID_i \| Y_j \| T_3)$；由于非对称加密 E 以及 $Hash$ 函数 $h(\cdot)$ 的安全性，攻击者无法得到用户的身份 ID_i。同时，由于 X_i、Y_j 分别由随机数 x、y 通过计算 $X_i = g^x, Y_j = g^y$ 得到，$\{M_1, Z_i, M_3, M_4\}$ 在每次登录与认证过程中都是不固定的，攻击者无法判断两个会话是否为同一用户发起，因此无法对用户的访问行为进行追踪。

5.2 前向安全性

前文（4.2 节）中提到了 Guo 等人的协议不具备前向安全性，并叙述了攻击方法。而在改进的方案中，用户 U_i 和服务器 S_j 通过认证得到会话密钥

收稿日期：年-月-日.（小五号宋体，此处为页脚，和正文分开）
基金项目：国家重点研发专项（2017YFA0604500）；国家科技支撑项目（2014BAH02F00）；国家自然科学基金（61701190）；吉林省青年科学基金项目（20160520011JH）;吉林省省校共建示范项目（SXGJSF2017-4）.
作者简介：余宜诚（1990-），男，博士研究生. 研究方向：网络与信息安全.E-mail:yycitb@vip.qq.com
通信作者：初剑峰（1978-），男，副教授，博士.研究方向：信息安全.E-mail:chujf@jlu.edu.cn

$SK_{ij}=h(X_i\|Y_j\|Y_j^x\|K\|ID_i)=h(X_i\|Y_j\|X_i^y\|K\|ID_i)=SK_{ji}$，即使攻击者通过捕获的信息计算推导得到了$\{X_i,Y_j,K,ID_i\}$，要计算$X_i^y$或$Y_j^x$得到会话密钥将是一个 CDH 难题。所以改进协议能够实现前向安全性。

5.3 会话密钥协商

根据协议的描述，显然用户 U_i 和服务器 S_j 通达成了密钥协商，得到了用于未来通信的会话密钥 $SK_{ij}=h(X_i\|Y_j\|Y_j^x\|K\|ID_i)=h(X_i\|Y_j\|X_i^y\|K\|ID_i)=SK_{ji}$。

5.4 三因子安全

假设攻击者捕获或拾到用户的智能卡，通过边信道技术[16]提取其中的数据$\{V_i,W_i,H(\cdot),h(\cdot)\}$；同时攻击者也通过某种方法得到了用户的生物特征$BIO_i$，由于$ID_i$和$PSK$的保护，攻击者无法通过$V_i=h(ID_i)\|h(PW_i\|H(BIO_i)))$，$W_i=h(h(ID_i)\|PSK)\oplus h(ID_i\|H(BIO_i))$得到用户口令$PW_i$。同样地，当攻击者捕获用户的智能卡和口令或者攻击者捕获用户的口令和生物特征，都无法得出剩下的安全因子（生物特征或智能卡信息）。

5.5 抵御各类攻击

在实现以上安全要求的情况下，改进协议能够抵御各类已知的攻击，包括内部攻击、离线密码猜测攻击、智能卡丢失攻击、假冒用户攻击、假冒服务器攻击、重放攻击。

内部攻击：假设*RC*的内部攻击者得到用户数据$\{h(ID_i),PWD_i,IDB_i\}$，由于不知道用户身份ID_i和生物特征BIO_i，内部攻击者无法发起有效的攻击。

离线密码猜测攻击、智能卡丢失攻击：6.4节中说明了改进协议具备三因子安全性，所以即使攻击者得到用户的智能卡和生物特征，也无法实施有效的离线密码猜测攻击和智能卡丢失攻击。

假冒用户攻击：对于用户的登录请求信息，攻击者无法生成合法的K，因此服务器可以通过验证$Z_i\,?=h(X_i\|ID_i\|K\|T_1)$判断伪造的登录信息。

假冒服务器攻击：由于没有服务器私钥和系统密钥PSK，攻击者无法伪造合法的回应信息，用户可以通过验证$M_3\,?=h(ID_i\|X_i\|Y_j\|K\|T_2)$判断伪造的服务器回应信息。

表 1 安全性和功能比较

Table 2 Security and functionality comparison

Security attributes	Guo et al.'s	Ours
User anonymity	Yes	Yes
Un-traceability	Yes	Yes
Perfect forward secrecy	No	Yes
Session key agreement	Yes	Yes
Three-factory security	Yes	Yes
Insider attack resistance	Yes	Yes
Offline password guessing attack resistance	Yes	Yes
Smart card stolen attack resistance	Yes	Yes
User impersonation attack resistance	Yes	Yes
Server impersonation attack resistance	Yes	Yes
Replay attack resistance	Yes	Yes

重放攻击：由于用户与服务器间传递的消息都包含有时间戳信息，因此用户与服务器都能够检测到攻击者的重放攻击。

表 1 给出了改进协议与 Guo 等人的协议的安全性和功能对比的结果。

6 效率比较

本节对改进协议与Guo等人的协议作了安全性能对比，表2给出了协议的安全性能对比结果。

本节还将通过比较改进协议与Guo等人的协议的时间复杂度作效率比较。由于*RC*通常被认为是各方面性能强大的设备，效率比较仅对用户与服务器执行协议的登录与认证阶段的计算开销作比较。相关符号定义如下：

T_h：执行一次*Hash*函数所需时间；

$T_{rsa\text{-}e}$：执行一次*RSA*加密所需时间；

$T_{rsa\text{-}d}$：执行一次*RSA*解密所需时间；

T_e：执行一次幂运算所需时间；

在 Guo 等人的协议中，用户执行了 11 次 *Hash* 函数和 1 次 *RSA* 加密操作，计算开销为$11\times T_h+T_{rsa-e}$；服务器行了 8 次 *Hash* 函数和 1 次 *RSA* 解密操作，计算开销为$8\times T_h+T_{rsa-d}$。而为保证协议能够实现前向安全性，改进的协议中在原方案的基础上，用户与服务器分别执行了两次幂运算；用户和服务器的计算开销分别为$11\times T_h+T_{rsa-e}+2\times T_e$、$8\times T_h+T_{rsa-d}+2\times T_e$。尽管改进的协议在计算开销上高于原协议，但是改进**表 2 计算开销比较**

收稿日期：年-月-日.（小五号宋体，此处为页脚，和正文分开）

基金项目：国家重点研发专项（2017YFA0604500）；国家科技支撑项目（2014BAH02F00）；国家自然科学基金（61701190）；吉林省青年科学基金项目（20160520011JH）;吉林省省校共建示范项目（SXGJSF2017-4）.

作者简介：余宜诚（1990-），男，博士研究生. 研究方向：网络与信息安全.E-mail:yycitb@vip.qq.com

通信作者：初剑峰（1978-），男，副教授，博士.研究方向：信息安全.E-mail:chujf@jlu.edu.cn

Table 2 Computation cost comparison

Participant	Guo et al.'s	Ours
User	$11\times T_h + T_{rsa-e}$	$11\times T_h + T_{rsa-e} + 2\times T_e$
Server	$8\times T_h + T_{rsa-d}$	$8\times T_h + T_{rsa-d} + 2\times T_e$

的协议有效地实现了前向安全性。表2是改进协议与原协议的效率对比结果。

7 结束语

近年来，研究者们提出了许多适用于多服务器架构的身份认证协议。2017 年，Guo 等人提出了一种适用于多服务器架构的、具有鲁棒性的三因子认证密钥协商协议。然而，通过分析，我们发现 Guo 等人的协议不具备前向安全性，具有安全隐患，并且协议不支持用户的生物特征更新功能。为此，本文提出了一种新的改进协议克服原有协议的安全缺陷并完善了协议的生物特征更新功能。通过安全分析可知，改进协议满足多服务器网络环境的安全需求，能够抵御各种已知攻击方法。

参 考 文 献：

[1] Jiang Q, Ma J, Li G, et al. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks[J]. Wireless Personal Communications, 2013, 68(4): 1477-1491.

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

[3] Chandrakar P, Om H. A Secure and Robust Anonymous Three-Factor Remote User Authentication Scheme For Multi-Server Environment Using ECC[J]. Computer Communications, 2017.

[4] Irshad A, Sher M, Ahmad H F, et al. An improved Multi-server Authentication Scheme for Distributed Mobile Cloud Computing Services[J]. TIIS, 2016, 10(12): 5529-5552.

[5] Chatterjee K, De A. A Novel Multi-Server Authentication Scheme for e-commerce Applications Using Smart Card[J]. Wireless Personal Communications, 2016, 91(1): 293-312.

[6] Yeh K H. A provably secure multi-server based authentication scheme[J]. Wireless personal communications, 2014, 79(3): 1621-1634.

[7] Tan Z. A Secure Privacy-Preserving Remote User Authentication Scheme Using Smart Cards for Multi-server Environment[J]. International Information Institute (Tokyo). Information, 2012, 15(4): 1547.

[8] Kim H, Jeon W, Lee K, et al. Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme[J]. Computational Science and Its Applications–ICCSA 2012, 2012: 391-406.

[9] Wang B, Ma M. A smart card based efficient and secured multi-server authentication scheme[J]. Wireless Personal Communications, 2013: 1-18.

[10] Yang D, Yang B. A biometric password-based multi-server authentication scheme with smart card[C]//Computer Design and Applications (ICCDA), 2010 International Conference on. IEEE, 2010, 5: V5-554-V5-559.

[11] Mishra D, Das A K, Mukhopadhyay S. A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards[J]. Expert Systems with Applications, 2014, 41(18): 8129-8143.

[12] Sood S K, Sarje A K, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture[J]. Journal of Network and Computer Applications, 2011, 34(2): 609-618.

[13] Li X, Xiong Y, Ma J, et al. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards[J]. Journal of Network and Computer Applications, 2012, 35(2): 763-769.

[14] Chuang M C, Chen M C. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics[J]. Expert Systems with Applications, 2014, 41(4): 1411-1418.

收稿日期：年-月-日.（小五号宋体，此处为页脚，和正文分开）

基金项目：国家重点研发专项（2017YFA0604500）；国家科技支撑项目（2014BAH02F00）；国家自然科学基金（61701190）；吉林省青年科学基金项目（20160520011JH）;吉林省省校共建示范项目（SXGJSF2017-4）.

作者简介：余宜诚（1990-），男，博士研究生. 研究方向：网络与信息安全.E-mail:yycitb@vip.qq.com

通信作者：初剑峰（1978-），男，副教授，博士.研究方向：信息安全.E-mail:chujf@jlu.edu.cn

[15] Guo H, Wang P, Zhang X, et al. A robust anonymous biometric-based authenticated key agreement scheme for multi-server environments[J]. PloS one, 2017, 12(11): e0187403.

[16] He D, Gao Y, Chan S, et al. An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Networks[J]. Ad hoc & sensor wireless networks, 2010, 10(4): 361-371.

收稿日期：年-月-日.（小五号宋体，此处为页脚，和正文分开）

基金项目：国家重点研发专项（2017YFA0604500）；国家科技支撑项目（2014BAH02F00）；国家自然科学基金（61701190）；吉林省青年科学基金项目（20160520011JH）;吉林省省校共建示范项目（SXGJSF2017-4）.

作者简介：余宜诚（1990-），男，博士研究生. 研究方向：网络与信息安全.E-mail:yycitb@vip.qq.com

通信作者：初剑峰（1978-），男，副教授，博士.研究方向：信息安全.E-mail:chujf@jlu.edu.cn