doi:10.11959/j.issn.1000-436x.2017148

基于生物特征和口令的双因子认证与密钥协商协议

李晓伟[1]，杨邓奇[1]，陈本辉[1,2]，张玉清[3]

（1. 大理大学数学与计算机学院，云南 大理 671000；2. 北京邮电大学网络与交换技术国家重点实验室，北京 100049；
3. 中国科学院大学国家计算机网络入侵防范中心，北京 100049）

摘 要：提出了一个新型的基于生物特征和口令的双因子认证与密钥协商协议。该双因子协议利用用户的生物特征以及口令信息实现安全通信，用户不需要携带智能卡。利用模糊提取技术，服务器不再保存用户生物信息，避免了服务器被攻陷用户敏感信息丢失的风险。通过服务器的公钥保护用户的认证信息，避免了基于口令的认证协议可能遭受的离线字典攻击。基于椭圆曲线计算性 Diffie-Hellman 假设，在随机预言模型下证明了协议的安全性。性能分析表明，所提出的协议具有较高的安全属性。

关键词：认证与密钥协商；生物认证；口令；随机预言模型

中图分类号：TP309 **文献标识码**：A

Two-factor authenticated key agreement protocol based on biometric feature and password

LI Xiao-wei[1], YANG Deng-qi[1], CHEN Ben-hui[1,2], ZHANG Yu-qing[3]

(1. Department of Mathematics and Computer Science, Dali University, Dali 671000, China;
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100049, China;
3. National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: A new two-factor authenticated key agreement protocol based on biometric feature and password was proposed. The protocol took advantages of the user's biological information and password to achieve the secure communication without bringing the smart card. The biometric feature was not stored in the server by using the fuzzy extractor technique, so the sensitive information of the user cannot be leaked when the server was corrupted. The authentication messages of the user were protected by the server's public key, so the protocol can resist the off-line dictionary attack which often appears in the authentication protocols based on password. The security of the proposed protocol was given in the random oracle model provided the elliptic computational Diffie-Hellman assumption holds. The performance analysis shows the proposed protocol has better security.

Key words: authenticated key agreement protocol, biometric authentication, password, random oracle model

1 引言

认证与密钥协商（AKA，authenticated key agreement）协议作为信息安全中的一个重要领域已被应用到众多实际场景中。基于口令的 AKA 协议[1,2]具有便于记忆、便于管理等优点，极大程度地方便用户使用。然而，口令便于记忆，但是熵值较小，很容易遭受字典攻击[3]。为了抵抗单一口令所存在

收稿日期：2016-11-02；**修回日期**：2017-04-18
通信作者：陈本辉，bhchen_dali@163.com
基金项目：国家自然科学基金资助项目（No.61462003, No.71462001, No.61272481, No.61572460）；国家重点研究与发展基金资助项目（No.2016YFB0800703）；网络与交换技术国家重点实验室开放课题基金资助项目（No.SLNST-2016-2-25）；云南省教育厅基金资助项目（No.2016ZZX192）

Foundation Items: The National Natural Science Foundation of China (No.61462003, No.71462001, No.61272481, No.61572460), The National Key Research and Development Project (No.2016YFB0800703), Open Project Program of State Key Laboratory of Networking and Switching Technology (No.SLNST-2016-2-25), Education Foundation of Yunnan Province (No.2016ZZX192)

的字典攻击，许多双因子认证协议被提出。目前，使用较多的是基于口令和智能卡的双因子协议[4~6]。在该类双因子协议中，攻击者不能仅依靠猜测口令来破解 AKA 协议，还需要获得智能卡内信息。该类双因子 AKA 协议有 Juang 等[4]提出的健壮且高效的基于智能卡和口令的 AKA 协议以及 Wang 等[5]提出的具有隐私保护的双因子 AKA 协议。然而，该认证方式也具有一定的局限性。用户需要额外的携带一个智能卡，这对用户来说增加了一定的不便性。同时，智能卡也可能丢失，当智能卡丢失后，用户就不能够再登录到服务器，除非用户重新申请一个智能卡。这对于某些需要处理紧急情况的用户来说是不可接受的。此外，口令和智能卡的丢失也会给该类 AKA 协议带来一定的安全隐患[6]。

生物特征具有不易遗忘、不易丢失、不易伪造以及随身携带等优点，因此，基于生物特征的认证协议既增强了认证协议的安全性又增加了其便捷性。基于此，Li 等[7]结合生物特征到口令和智能卡的 AKA 协议提出了基于三因子的 AKA 协议，该协议除了可以保证 AKA 协议安全外还可以保护用户隐私。Giri 等[8]基于生物特征以及大容量存储装置 USB 提出了效率更高的三因子 AKA 协议。尽管基于生物特征的认证协议具有一定的优势，然而已有的基于生物特征的多因子 AKA 协议本质上仍然采用智能卡来完成协议，没有解决使用智能卡所带来的安全性和便捷性上的问题。本文尝试解决以上问题，提出一个新的基于口令和生物特征的双因子协议。协议具有以下优点。

1) 用户不需要额外携带智能卡，仅依靠短的口令和自己的生物特征就可以完成和服务器的认证与密钥协商。这和已有的基于口令、智能卡的双因子认证与密钥协商协议有着本质的区别。

2) 所提出的协议具备抵抗单一因子丢失的安全属性。即使攻击者获得了用户口令或生物特征中的一个安全因子，它仍然不能破解协议的安全性，即不能破解认证和密钥协商安全属性。

2 模糊提取技术

生物认证中有 2 个需要解决的问题。1) 任意 2 次提取人的生物特征可能得到的信息并不完全一致，这就导致了服务器不可能像口令认证一样对生物特征进行一致性比对。2) 即使解决了上述生物特征比对问题，用户也不希望将自己的生物特征存储在服务器处。因为一旦服务器被攻陷，所有用户的生物特征都将被窃取。模糊提取技术很好地解决了上述 2 个问题[9]。在模糊提取技术中，当输入一个生物特征 B 时，模糊提取技术可以以一种容错的方式输出一个随机的字符串 R。当输入的 B' 和 B 相差不大时，模糊提取器输出的随机字符串 R 不发生改变。服务器只需要存储随机字符 R，而无需存储用户生物特征。在输入生物特征 B' 恢复 R 的过程中，一般需要输入一个辅助的公开信息 P。模糊提取器由以下 2 个算法组成。

1) 随机数生成算法 $Gen(B)\rightarrow\{R,P\}$。输入用户生物特征 B 到 $Gen()$，输出一个长度为 l 的字符串 R，以及一个辅助的字符串 P，其中，l 为安全参数。

2) 随机数恢复算法 $Rep(B',P)\rightarrow R$。输入用户的生物特征 B' 以及辅助字符串 P 到 $Rep()$，若 $dis(B',B)\leqslant\varepsilon$，则 $Rep()$ 的输出为 R，其中，$dis(B',B)\leqslant\varepsilon$ 表示 B' 和 B 的距离不超过一个给定的区间 ε。

3 基于生物特征的认证与密钥协商协议安全模型

本文在 Li 等[10]的基于口令和智能卡的认证与密钥协商协议安全模型提出了一个新的模型，将其中的智能卡丢失询问替换成生物特征丢失询问。模型中包含 3 类实体：用户、服务器以及攻击者。每个用户都拥有其口令和生物特征。攻击者可以控制用户和服务器之间的通信信道。攻击者通过对用户与服务器之间的协议实例 $(\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i})$ 进行询问来试图获取用户和服务器之间产生的会话密钥。具体模型如下。

$Execute(\prod_{\mathrm{U}}^{i},\prod_{\mathrm{S}}^{i})$ 询问。攻击者通过该询问触发用户 U 和服务器 S 完成一次会话，同时攻击者监听该会话的全部过程。

$Send(\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i},m)$ 询问。攻击者可以自己发送任意 m 消息给协议实例 $\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i}$，U 或 S 收到消息后按照协议运行将结果返回给攻击者。该询问实际上是模拟攻击者发起的主动攻击。

$Reveal(\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i})$ 询问。攻击者通过发送该询问给 $\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i}$ 从而得到此次协议运行的会话密钥。

$Password\ reveal(U,PW_{\mathrm{U}})$ 询问。攻击者可以通过该询问得到用户 U 的口令信息。

$Biometric\ reveal(U,B_{\mathrm{U}})$ 询问。攻击者可以通过该询问得到用户 U 的生物特征信息。

$Hash(x)$ 询问。若没有对 x 进行散列询问则选择一个随机数作为 x 的散列值，并存储 $(x,Hash(x))$

到散列列表中；若对 x 已经进行了散列询问，则查看散列列表找到对应的散列值返回。

$Test(\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i})$ 询问。攻击者需要选择一个会话作为测试会话，当选择 $\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i}$ 作为测试会话时，返回结果如下：选择一个随机数 $b\in\{0,1\}$，若 $b=1$ 则返回真实的会话密钥；若 $b=0$，则返回一个随机数。这里需要说明的是测试会话不能是已经被进行 $Reveal(\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i})$ 询问过的会话。

AKA 安全。设攻击者输出的数值为 b'，设攻击者正确猜测 *Test* 询问所返回的数是随机数还是真实的会话密钥的概率为 $Adv_{\mathrm{P}}^{\mathrm{AKA}}$，则攻击者赢得这个游戏的优势可以定义为 $Adv_{\mathrm{P}}^{\mathrm{AKA}}=2\Pr[b=b']-1$。本文称协议 P 为 AKA 安全，如果对于任何多项式时间的攻击者其赢得上述 AKA 游戏的概率为 $Adv_{\mathrm{P}}^{\mathrm{AKA}}=\ 2\Pr[b=b']-1=\dfrac{q_s}{|N|}+neg(k)$。其中，$q_s$ 是攻击者发动 *Send* 询问的次数，$|N|$ 为用户口令空间大小，$neg(k)$ 是一个可忽略的量。

4　新的双因子认证与密钥协商协议

本文简要给出协议的设计思想：双因子 AKA 协议中用户拥有生物特征和口令。生物特征和口令不能直接传输，也不能存储在服务器处。因此，本文首先利用模糊提取技术将用户生物特征进行处理，处理后将其和用户口令的散列值存储在服务器处。该方法避免了服务器被攻陷用户生物特征丢失。其次，本文利用服务器公钥来保证用户传输的认证信息安全性，从而实现认证所需的安全指标。

用户的认证过程包含 2 个部分，首先是用户注册，然后是用户登录过程。协议中所用到的参数如表 1 所示。

表 1　　**文中用到的符号**

符号	描述
k	安全参数
p	大素数
G	椭圆曲线 E 上的点组成的群
P	群 G 的生成元
H	安全的散列函数
MAC	安全的消息认证码
U	用户
S	服务器
PW_{U}	用户口令
B_{U}	用户生物信息
sP,s	服务器 S 的公私钥对

4.1　用户注册

用户 U 要登录到一个服务器 S，获取服务器的服务，那么他首先要在该服务器 S 处进行注册。U 通过一个安全信道发送自己的身份信息 ID_{U}、口令 PW_{U} 以及通过指纹信息提取器或虹膜信息提取器等提取的生物信息 B_{U} 发送给服务器 S。

S 在收到这些信息后，通过模糊提取技术，输入用户的生物特征信息 B_{U} 到 *Gen*() 算法中，输出一个随机的字符串 R_{U} 和一个辅助的字符串 P_{U}，并计算 $W_{\mathrm{U}}=H(R_{\mathrm{U}}\|PW_{\mathrm{U}})$，将 $(ID_{\mathrm{U}},P_{\mathrm{U}},W_{\mathrm{U}})$ 存储于其数据库中，将 B_{U} 和 PW_{U} 删除。

4.2　用户认证

用户 U 和服务器 S 之间的登录—应答过程通过以下步骤来完成，如图 1 所示。

第 1 步　用户 U 首先输入自己的生物信息和口令信息 B_{U} 和 PW_{U} 到识别设备中。该设备向服务器 S 发起一个会话，并发送自己的身份 ID_{U}。

第 2 步　服务器 S 收到 ID_{U} 后搜索其数据库找到和 ID_{U} 对应的数据 P_{U}，发送 P_{U} 给用户。

第 3 步　用户设备收到 P_{U} 后，选取随机数 $a\in Z_p^*$，并计算 $T_{\mathrm{A}}=aP$、$K=H(a\cdot sP\|T_{\mathrm{A}}\|sP)$。然后根据模糊提取技术中的 *Rep* 算法，恢复出 $Rep(B_{\mathrm{U}},P_{\mathrm{U}})\to R_{\mathrm{U}}$，并根据 PW_{U} 和 R_{U} 计算出 $W_{\mathrm{U}}=H(R_{\mathrm{U}}\|PW_{\mathrm{U}})$ 以及 $Auth_{\mathrm{U}}=H(K\|W_{\mathrm{U}})$。此后，U 发送登录信息 $(ID_{\mathrm{U}},T_{\mathrm{A}},Auth_{\mathrm{U}})$ 给服务器。

第 4 步　服务器收到用户发送的信息（ID_{U}，T_{A}，$Auth_{\mathrm{U}}$）后，根据自己的私钥信息 s，计算 $K=H(s\cdot T_{\mathrm{A}}\|T_{\mathrm{A}}\|sP)$。服务器解密其数据库并查看是否有关于 ID_{U} 的数据对 $(ID_{\mathrm{U}},W_{\mathrm{U}})$。如果有，则根据 W_{U} 验证 $Auth_{\mathrm{U}}=H(K\|W_{\mathrm{U}})$ 是否成立。若没有或验证 $Auth_{\mathrm{U}}$ 失败则拒绝登录请求。否则 S 选取随机数 $b,r_{\mathrm{S}}\in Z_p^*$，并计算 $T_{\mathrm{B}}=bP$ 以及 S 的认证信息 $Auth_{\mathrm{S}}=MAC_{\mathrm{K}}(T_{\mathrm{A}}\|T_{\mathrm{B}}\|sP\|r_{\mathrm{S}})$ 以及会话密钥 $sk_{\mathrm{US}}=H(K\|W_{\mathrm{U}}\|abP\|ID_{\mathrm{U}}\|ID_{\mathrm{S}}\|T_{\mathrm{A}}\|T_{\mathrm{B}}\|sP)$。S 发送确认信息 $(ID_{\mathrm{S}},T_{\mathrm{B}},r_{\mathrm{S}},Auth_{\mathrm{S}})$ 给用户 U。

第 5 步　U 在收到 $(ID_{\mathrm{S}},T_{\mathrm{B}},r_{\mathrm{S}},Auth_{\mathrm{S}})$ 后，验证 $Auth_{\mathrm{S}}=MAC_{\mathrm{K}}(T_{\mathrm{A}}\|T_{\mathrm{B}}\|sP\|r_{\mathrm{S}})$ 是否成立。若不成立则拒绝该条消息，请求服务器重新发送确认信息。否则，U 计算用户和服务器之间的会话密钥 $sk_{\mathrm{US}}=H(K\|W_{\mathrm{U}}\|abP\|ID_{\mathrm{U}}\|ID_{\mathrm{S}}\|T_{\mathrm{A}}\|T_{\mathrm{B}}\|sP)$ 以及 U 计算出会话密钥的确认信息 $\sigma_{\mathrm{U}}=H(K\|W_{\mathrm{U}}\|abP\|ID_{\mathrm{U}}\|ID_{\mathrm{S}})$。U 发送确认信息 σ_{U} 给服务器。

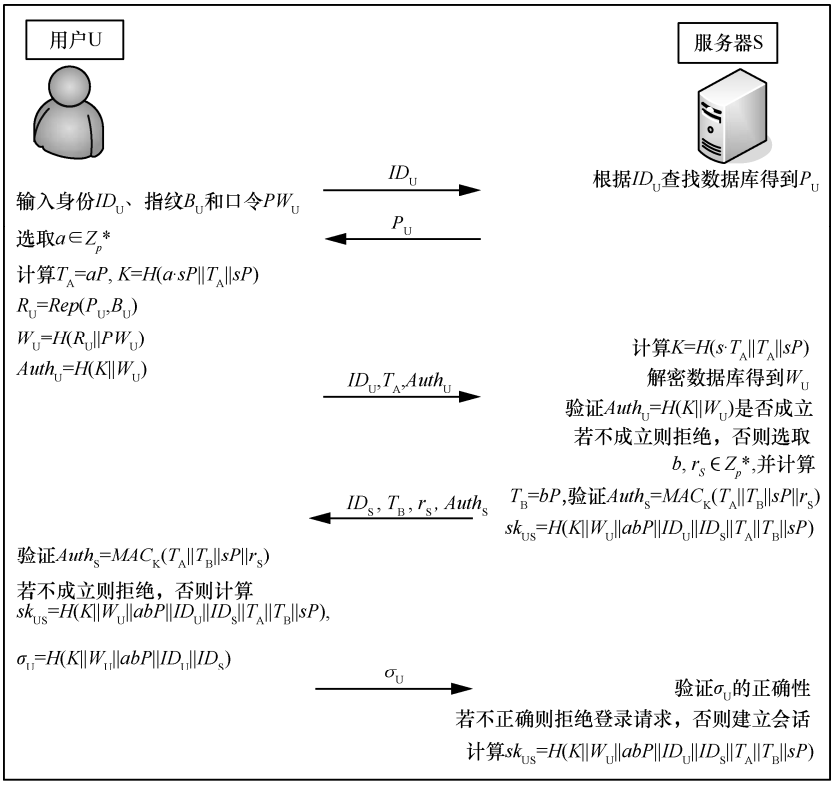


图 1 基于生物特征和口令的双因子认证与密钥协商协

第 6 步 服务器 S 收到 σ_U 后验证 σ_U 的正确性，若 $\sigma_U \neq H(K\|W_U\|abP\|ID_U\|ID_S)$ 则拒绝登录请求，否则 S 计算 U 和 S 之间的会话密钥 $sk_{US}=H(K\|W_U\|abP\|ID_U\|ID_S\|T_A\|T_B\|sP)$ 并建立会话。

5 安全性证明和性能分析

5.1 安全性证明

本文在随机预言模型下证明所提出的协议满足模型中的 AKA 安全定义。本文需要以下数学假设。

ECDH（elliptic curve computational Diffie-Hellman）假设 E 是一条椭圆曲线，其上的点组成阶为 p 的群 G。设 P 为 G 的一个生成元，xP 和 yP 为 G 中的任意 2 个元素。给定 P、aP、bP，任何多项式时间的攻击者都不能以不可忽略的概率计算出 abP。

定理 1 设本文所提出的协议为 P，用户口令空间大小为 $|N|$。设攻击者是一个攻击协议 P 的 AKA 安全属性的攻击者，其在时间 t 内可以进行不高于 q_e 次 Execute 询问，不高于 q_s 次 *Send* 询问，不高于 q_h 次散列询问，则有

$$Adv^{AKA}(t) \leqslant \frac{2q_s}{|N|}+\frac{(q_s+q_e)^2}{2^k}+\frac{q_h^{\,2}}{2^k}+6q_h Adv^{ECDH}(t')+2(q_s+q_e)Adv^{MAC}(t'') \quad (1)$$

其中，$Adv^{AKA}(t)$ 为攻击者破解协议 P 的 AKA 安全属性的概率，$Adv^{ECDH}(t')$ 为攻击者破解 ECDH 问题的概率，$Adv^{MAC}(t'')$ 为攻击者破解 MAC 算法的概率。

证明 这里假设服务器是不可攻陷的，即服务器的密钥 s 只有服务器自己知道。那么攻击者要获得 U 和 S 之间的会话密钥，必然通过以下 3 种方式：1) 攻击者不知道用户口令也不知道用户生物特征破解会话密钥；2) 攻击者知道用户口令但不知道用户生物特征破解会话密钥；3) 攻击者知道用户生物特征但不知道用户口令破解会话密钥。下面本文将分别证明在 3 种情况下，攻击者破解会话密钥的概率均是可忽略的。在证明前，本文首先排除攻击者破解了 MAC 算法的安全性。设攻击者破解 MAC 算法的概率为 $Adv^{MAC}(t'')$，则攻击者在本协议中破解 MAC 算法的概率为 $(q_s+q_e)Adv^{MAC}(t'')$。其中，q_s 为攻击者发送 *Send* 询问的次数，q_e 为攻击者发送 *Execute* 询问的次数。其次，本文排除不同协议实例之间选取相同参数运行协议的概率，即不同协

议之间发生了碰撞，这样的碰撞概率可以利用生日悖论来约束。本文得出发生协议实例碰撞的概率为 $\frac{(q_{\mathrm{s}}+q_{\mathrm{e}})^2}{2^{k+1}}$。同理，本文可以得出散列碰撞的概率为 $\frac{q_{\mathrm{h}}^2}{2^{k+1}}$，其中，$q_{\mathrm{h}}$ 为攻击者进行散列询问的次数。此外，本文还要排除攻击者没有通过和用户以及服务器交互就可以成功猜测出测试会话所返回的数值是真实会话还是随机数，该事件的概率为 $\frac{1}{2}$。若上述前 3 个事件发生，则攻击者破解协议 P 的 AKA 安全属性。这 4 个事件的发生的概率可以限定为

$$\Pr[0]\leqslant(q_{\mathrm{s}}+q_{\mathrm{e}})Adv^{\mathrm{MAC}}(t'')+\frac{(q_{\mathrm{s}}+q_{\mathrm{e}})^2}{2^{k+1}}+\frac{q_{\mathrm{h}}^2}{2^{k+1}}+\frac{1}{2} \quad (2)$$

情况 1　在此情况下，攻击者既不知道用户口令也不知道用户的生物特征。本文按照第 3 节的 AKA 安全模型来模拟协议运行并回答攻击者的相关询问。若攻击者可以以不可忽略的优势区分出会话密钥和随机数，则本文可以利用攻击者来破解 ECDH 问题。具体过程如下。

本文模拟协议 P 的运行并回答攻击者的询问。首先本文初始化所有用户的信息，包括用户的口令和指纹特征。在模拟之前本文加入一个 ECDH 二元组(xP, yP)到测试会话中。其中，xP 用于替换测试会话中的随机数 aP，yP 用于替换服务器私钥 sP。若攻击者可以以不可忽略的优势猜测出测试会话所返回的是随机数还是真实的会话密钥，则本文可以利用攻击者获得 xyP，即破解 ECDH 问题。本文对于非测试会话的模拟是正确的，攻击者不会发现有任何异常。当攻击者选择一个会话 $Execute(ID_{\mathrm{U}})$ 或 $Send(ID_{\mathrm{U}},T_{\mathrm{A}},Auth_{\mathrm{U}})$ 询问时，由于本文不知道服务器私钥(服务器公钥为 yP，不知道对应的 y)，不能直接计算出临时密钥 K 来回答攻击者询问。此时要正确地模拟协议运行，本文需要查看散列列表里是否存储了形如 $(*,T_{\mathrm{A}},yP,Hash(*\|T_{\mathrm{A}}\|yP))$ 这样的数据对，$*$ 表示某个数值。若存储了则将 $Hash(*\|T_{\mathrm{A}}\|yP)$ 作为 K 的值。得到 K 后本文按照协议运行验证 $Auth_{\mathrm{U}}$，并返回 $(ID_{\mathrm{S}},T_{\mathrm{B}},r_{\mathrm{S}},Auth_{\mathrm{S}})$ 给攻击者。若散列列表中没有存储形如 $(*,T_{\mathrm{A}},yP,Hash(*\|T_{\mathrm{A}}\|yP))$ 的消息，则对散列预言机进行 $Hash(\perp\|T_{\mathrm{A}}\|yP)$ 询问，其中，$\perp$ 为空值。散列预言机随机选取一个数 h，令 $h=Hash(\perp\|T_{\mathrm{A}}\|yP)$ 并存储该散列询问及其应答 h 到列表中。此时，本文将 h 作为 K 的值模拟协议运行。此后，若有攻击者对散列函数进行 $Hash(*\|T_A\|yP)$ 询问，则本文将 $\perp$ 空值替换为 $*$ 所代表的值，并将 h 作为 $Hash(*\|T_A\|yP)$ 的值。同理若攻击者冒充服务器对用户的协议实例进行 $Execute(ID_{\mathrm{S}},T_{\mathrm{B}},r_{\mathrm{S}},Auth_{\mathrm{S}})$ 或 $Send(ID_{\mathrm{S}},T_{\mathrm{B}},r_{\mathrm{S}},Auth_{\mathrm{S}})$ 询问时，本文采用相同的方式对散列预言机进行询问，从而可以得到数值 K 并正确模拟协议运行。当攻击者发送 $Execute(\sigma_{\mathrm{U}})$ 或 $Send(\sigma_{\mathrm{U}})$ 询问时回答过程类似。当攻击者进行 $Reveal(\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i})$ 询问时，若协议得出了会话密钥则返回对应的值。若协议没有得出会话密钥则返回空值给攻击者。此时可以发现，在非测试会话中无论攻击者进行了哪种询问，本文都能正确地模拟协议运行。

下面讨论测试会话。当攻击者选择测试会话进行 $Test(\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i})$ 询问时，本文依然按照协议运行得出协议实例，只是在回答用户 $Test(\prod_{\mathrm{U}}^{i}/\prod_{\mathrm{S}}^{i})$ 询问时本文选择一个随机数作为会话密钥返回给攻击者。此时，若攻击者可以确定返回的值是真实的会话密钥还是随机数，则他必然获得了真实会话密钥，$sk_{\mathrm{US}}=H(K\|W_{\mathrm{U}}\|abP\|ID_{\mathrm{U}}\|ID_{\mathrm{S}}\|xP\|bP\|yP)$。也就是说，攻击者必然对散列函数进行了 $H(K\|W_U\|abP\|ID_{\mathrm{U}}\|ID_{\mathrm{S}}\|xP\|bP\|yP)$ 询问。那么本文可以查看散列列表，从而找到对应的 K 值，即获得了 $K=Hash(xyP\|xP\|yP)$，从而可以再次查询散列预言机得到 xyP，也就破解了 ECDH 问题。因此，情况 1 中攻击者破解协议 P 的 AKA 安全属性的概率可以限定为

$$\Pr[\text{情况1}]\leqslant q_{\mathrm{h}}Adv^{\mathrm{ECDH}}(t') \quad (3)$$

情况 2　在此情况下，攻击者知道用户口令信息，即对用户进行了 $Password\ reveal(U,PW_{\mathrm{U}})$ 询问获得了口令 PW_{U}。此时攻击者没有用户的生物特征信息 B_{U}。那么实质上攻击者所能进行的攻击和他没有获得用户口令信息基本一致。因为攻击者获得了口令仍然无法猜测用户的秘密值 W_{U}。因此，在情况 2 下攻击者破解协议 P 的 AKA 安全属性的概率可以限定为

$$\Pr[\text{情况2}]\leqslant q_{\mathrm{h}}Adv^{\mathrm{ECDH}}(t') \quad (4)$$

情况 3　在此情况下，攻击者获得了用户的生物特征信息，即对用户进行了 $biometric\ reveal(U,B_{\mathrm{U}})$ 询问获得了生物特征信息 B_{U}。此时攻击者可以通过以下 2 种方式来对协议进行攻击：1) 在线字典攻击；

2) 离线字典攻击。

若攻击者选择在线字典攻击，即攻击者从口令空间中选取一个候选口令值 PW_{U}' 作为用户的真实口令在线地与服务器进行交互。此时，若攻击者猜测正确，即 $PW_{\mathrm{U}}'=PW_{\mathrm{U}}$，则攻击者正确地冒充了用户，从而可以计算出真实的会话密钥，破解协议 P 的 AKA 安全属性。此情况下，攻击者破解 P 的 AKA 安全属性的概率被限定为

$$\Pr[\text{情况3a}]\leqslant\frac{q_{\mathrm{s}}}{|N|} \tag{5}$$

若攻击者选择离线字典攻击，攻击者同样从口令空间中选取一个候选口令值 PW_{U}' 作为用户的真实口令。此时攻击者不是在线地与服务器进行交互来完成协议而是从已经在诚实用户和服务器之间正确完成的协议中来验证其口令猜测是否正确。在此情况下，攻击者只能通过 $Auth_{\mathrm{U}}$、sk_{US} 以及 σ_{U} 中的任意一个来验证。而此时若攻击者可以从这些值中验证口令是正确的，则攻击者必然进行了 $H(K\|W_{\mathrm{U}}\|\cdots)$ 的散列询问，也就是说，攻击者可以计算出 K 值，那么他必然对散列预言机进行了 $Hash(xyP\|xP\|yP)$ 询问，从而本文可以利用攻击者来破解 ECDH 问题。此情况下，攻击者破解 P 的 AKA 安全属性的概率被限定为

$$\Pr[\text{情况3b}]\leqslant q_{\mathrm{h}}Adv^{\mathrm{ECDH}}(t') \tag{6}$$

根据第 3 节中的模型可知攻击者赢得 AKA 游戏的概率为 $Adv_{\mathrm{p}}^{\mathrm{AKA}}=2\Pr[b=b']-1$，因此，综上式(2)~式(6)可知，攻击者破解协议 P 的 AKA 安全属性的概率为

$$Adv^{\mathrm{AKA}}(t)\leqslant\frac{2q_{\mathrm{s}}}{|N|}+\frac{(q_{\mathrm{s}}+q_{\mathrm{e}})^2}{2^k}+\frac{q_{\mathrm{h}}^2}{2^k}+$$
$$6q_{\mathrm{h}}Adv^{\mathrm{ECDH}}(t')+2(q_{\mathrm{s}}+q_{\mathrm{e}})Adv^{\mathrm{MAC}}(t'') \tag{7}$$

5.2 性能分析

本文从认证与密钥协商协议所常用的 2 个指标来衡量所提出的双因子认证与密钥协商协议的性能，即安全性和计算消耗。表 2 给出了双因子认证与密钥协商协议在安全性方面所应具备的一些安全属性。这些安全属性都包含在上述所提出模型当中，也就是说，在该模型下证明满足安全性定义的协议具有这些安全属性[5]。本文不再具体解释这些安全属性。从表 2 可以看出所提出协议不仅具备安全的认证和密钥协商属性，同时当攻击者获取了双因子中的一个安全因子时，他仍然不能破解协议的安全性。表 3 给出了同较新的且效率较高的基于智能卡的双因子 AKA 协议[5]（即 Wang 等的协议）在计算消耗上的对比。同基于智能卡的双因子 AKA 协议进行对比的原因在于目前使用生物特征和口令的双因子 AKA 协议很少，且没有具体方案。这也正是本文写作的出发点。因此，本文给出 2 类双因子 AKA 协议中的代表协议进行对比。从表 3 中可以看出，虽然所提出协议在计算消耗上比文献[5]中的 AKA 协议略高(指数运算和点乘运算的运算时间是一个量级，远高于表 3 中其他运算的时间)，其原因在于文献[5]中的 AKA 协议不具有前向安全性，其中，e 为指数运算，m 为椭圆曲线点乘运算，h 为散列运算，mac 为 MAC 运算，s 为加/解密运算。若加上前向安全性则用户和服务器也要对应的加上至少一次点乘运算或指数运算。即本文所提出协议的计算效率上本质上和基于智能卡的双因子协议运算量相当。那么综合表 2 和表 3 可以看出，基于生物特征和口令的双因子 AKA 协议和基于智能卡和口令的双因子 AKA 协议相比具有同样的安全属性和计算消耗。而基于生物特征和口令的双因子 AKA 协议中，用户不需要额外携带智能卡，为用户进一步提供了便捷性。同时，也避免了用户智能卡丢失所带来的安全威胁。

表 2 双因子认证与密钥协商协议的安全性指标

安全指标	Wang 等的协议	本文协议
双向认证	是	是
安全的密钥协商	是	是
抗中间人攻击	是	是
抗重放攻击	是	是
抗已知密钥攻击	是	是
抗密钥控制攻击	否	否
抗平行会话攻击	是	是
抗口令丢失攻击	是	是
抗生物特征丢失攻击	是	是
前向安全性	否	是

表 3 计算消耗对比

计算消耗	Wang 等的协议	本文协议
用户的计算消耗	2e+8h+1s	3m+5h+1mac
服务器的计算消耗	2e+4h+1s	3m+5h+1mac

5.3 讨论

本文提出的基于生物特征和口令的双因子认

证与密钥协商协议的安全模型中不允许攻击者攻陷服务器（一般假设服务器不可被攻陷），为了给出更全面的安全性分析，下面讨论服务器被攻陷后对用户和已经结束的会话的影响。

1) 服务器被攻陷对用户的影响。事实上，用户最为担心的是服务器被攻陷后是否会获得用户的口令信息，因为用户使用相同口令登录多个服务器。本文方案中，攻击者攻陷服务器后可以获得用户登录该服务器的凭证 $W_{\mathrm{U}} = H(R_{\mathrm{U}} \| PW_{\mathrm{U}})$。由于攻击者没有用户的生物特征 B_{U}，因此攻击者并不能恢复 R_{U}，则攻击者也不能通过离线字典攻击来猜测用户口令，从而保证了即使服务器被攻陷用户口令也是安全的。除非攻击者也攻陷了用户生物特征，而这在实际应用当中是一种非常强的假设。

2) 服务器被攻陷对已经结束的会话的影响。服务器被攻陷后，服务器的长期密钥 s 以及用户凭证 W_{U} 都将被攻击者所获取。然而，此时攻击者仍然不能获得已经完成的会话秘密信息，即攻击者不能获得已经结束的会话密钥，协议具有前向安全性。因为从会话密钥的构成来看，$sk_{\mathrm{US}} = H(K \| W_{\mathrm{U}} \| abP \| ID_{\mathrm{U}} \| ID_{\mathrm{S}} \| aP \| bP \| sP)$，攻击者可以计算出 K 以及 W_{U}，但是攻击者不能计算出每次会话都重新产生的 Diffie-Hellman 密钥协商值 abP，因为每次会话结束后该值对应的 a 和 b 都将删除，攻击者仍然面对的是解决 ECDH 问题。因此，即使服务器被攻陷已经结束的会话也是安全的。

6　结束语

本文提出了一个基于生物特征和口令的新型双因子认证与密钥协商协议。与基于智能卡和口令的双因子认证、密钥协商协议相比，用户不用携带多个智能卡，从而解决了智能卡丢失所带来的安全性和可用性的问题，为用户提供了便利。同时，在随机预言模型下基于 ECDH 假设给出了所提出方案的形式化证明。综合安全性和效率，所提出的新型双因子认证与密钥协商协议具有一定优势。方案的局限性在于方案依然是依赖服务器的公钥来完成认证与密钥协商，如何在不使用公钥密码的情况下仍然可以保证双因子协议所需的全部安全性将是下一步所要研究的问题。

参考文献：

[1] HALEVI S, KRAWCZYK H. Public-key cryptography and password protocols[C]//The 5th ACM Conference on Computer and Communications Security. 1998:122-131.

[2] BELLOVIN S M, MERRITT M. Encrypted key exchange: password based protocols secure against dictionary attacks[C]//IEEE Security and Privacy. 1992:72-84.

[3] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[J]. Tecnologia Electronica E Informatica, 2000: 139-155.

[4] JUANG W S, CHEN S T, LIAW H T. Robust and efficient password authenticated key agreement using smart cards[J]. IEEE Transaction on Industrial Electronics, 2008, 55(6):2551-2556.

[5] WANG D, WANG N, WANG P, et al. Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity[J]. Information Sciences, 2015, 321(10):162-178.

[6] MISHRA D, DAS A K, CHATURVEDI A, et al. A secure password-based authentication and key agreement scheme using smart cards[J]. Journal of Information Security and Applications, 2015, 23(8): 28-43.

[7] LI X, NIU J, WANG Z, et al. Applying biometrics to design three-factor remote user authentication scheme with key agreement[J]. Security and Communication Networks, 2014, 7(10):1488-1497.

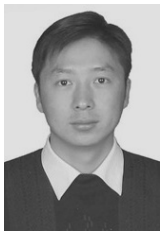
[8] GIRI D, SHERRATT R S, MAITRA T. A novel and efficient session spanning biometric and password based three-factor authentication protocol for consumer USB mass storage devices[J]. IEEE Transactions on Consumer Electronics, 2016, 62(3): 283-291.

[9] DODIS Y, REYZIN L, SMITH A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data[C]//Cryptology Eurocrypt 2004. 2004: 523-540.

[10] 李晓伟, 张玉清, 张格非, 等. 基于智能卡的强安全认证与密钥协商协议[J]. 电子学报, 2014, 42(8):1587-1593.
LI X W, ZHANG Y Q, ZHANG G F, et al. Strongly secure authenticated key agreement protocol using smart card[J]. Acta Electronica Sinica, 2014, 42(8):1587-1593.

作者简介：

李晓伟（1985-），男，吉林通化人，博士，大理大学讲师，主要研究方向为网络安全协议、云安全。



杨邓奇（1979-），男，白族，云南大理人，博士，大理大学副教授，主要研究方向为机器学习、图像识别。

陈本辉（1978-），男，云南大理人，大理大学教授，主要研究方向为神经网络、进化计算、机器学习。

张玉清（1966-），男，陕西宝鸡人，中国科学院大学教授、博士生导师，主要研究方向为网络与信息系统安全。