软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2016,27(6):1511−1522 [doi: 10.13328/j.cnki.jos.005001]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

# 标准模型下隐私保护的多因素密钥交换协议*

魏福山[1,2], 张 刚[2], 马建峰[1], 马传贵[2]

[1](西安电子科技大学 计算机学院,陕西 西安 710071)

[2](数学工程与先进计算国家重点实验室,河南 郑州 450001)

通信作者: 魏福山, E-mail: weifs831020@163.com

**摘 要**: 多因素认证密钥交换协议融合多种不同的认证因素来实现强安全的身份认证和访问控制,在具有高级别安全应用需求的移动泛在服务中具有巨大的应用潜力.现阶段多因素协议的研究成果还不丰富,并且已有协议都是在随机预言模型下可证明安全的.以两方口令认证密钥交换协议、鲁棒的模糊提取器以及签名方案为基本组件提出了一个标准模型下可证明安全的多因素协议.协议中服务器不知道用户的生物模板,因此实现了对生物信息的隐私保护.与已有的随机预言模型下的多因素协议相比,该协议在满足更高安全性的同时具有更高的计算效率和通信效率,因此更满足高级别安全的移动泛在服务的应用需求.

**关键词**: 多因素认证密钥交换协议;标准模型;模糊提取器;签名方案

**中图法分类号**: TP309

中文引用格式: 魏福山,张刚,马建峰,马传贵.标准模型下隐私保护的多因素密钥交换协议.软件学报,2016,27(6):1511−1522. http://www.jos.org.cn/1000-9825/5001.htm

英文引用格式: Wei FS, Zhang G, Ma JF, Ma CG. Privacy-preserving multi-factor authenticated key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1511−1522 (in Chinese). http://www.jos.org.cn/1000-9825/5001.htm

## Privacy-Preserving Multi-Factor Key Exchange Protocol in the Standard Model

WEI Fu-Shan[1,2], ZHANG Gang[2], MA Jian-Feng[1], MA Chuan-Gui[2]

[1](School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

[2](State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

**Abstract**: Multi-factor authenticated key exchange (MFAKE) protocols combine different authentication factors to realize strong secure identity authentication and access control, and have great application potential in mobile ubiquitous services with high-level security requirements. Until now, literatures about MFAKE protocols are rare and far from satisfactory. Moreover, existing multi-factor authenticated key exchange protocols are proven secure only in the random oracle model. The study proposes a MFAKE protocol using two-party password authenticated key exchange protocols, fuzzy extractors and signature schemes as building blocks. The security of this MFAKE protocol is conducted in the standard model. The server does not need to know the biometric template of the user, thus the

* 基金项目: 国家自然科学基金(61309016, 61379150, 61201220, U1135002, U1405255); 国家高技术研究发展计划(863)(2015AA011704); 中国博士后科学基金(2014M562493); 陕西省博士后科学基金; 信息保障技术重点实验室开放课题(KJ-13-02); 高校基本业务费项目(JB161501); 河南省科技攻关重点项目(092101210502, 122102210126)

Foundation item: National Natural Science Foundation of China (61309016, 61379150, 61201220, U1135002, U1405255); National High-Tech R&D Program of China (863) (2015AA011704); China Postdoctoral Science Foundation (2014M562493); Shaanxi Province Postdoctoral Science Foundation; The Funding of Science and Technology on Information Assurance Laboratory (KJ-13-02); Fundamental Research Funds for the Central Universities (JB161501); Key Scientific and Technological Project of He'nan Province (092101210502, 122102210126)

收稿时间: 2015-08-15; 修改时间: 2015-10-09; 采用时间: 2015-12-05; jos 在线出版时间: 2016-01-21

CNKI 网络优先出版: 2016-01-22 10:14:51, http://www.cnki.net/kcms/detail/11.2560.TP.20160122.1014.007.html

biometric privacy of the user is preserved. Compared with existing MFAKE protocols, our protocol achieves stronger security with lower computation and communication costs. Consequently, the proposed protocol is more suitable for mobile ubiquitous services with high-level security requirements.

**Key words**: multi-factor authenticated key exchange protocol; standard model; fuzzy extractor; signature scheme

随着云计算等新一代信息技术的迅猛发展,用户可以通过移动终端便捷地享受到几乎无所不在的服务.在云计算框架中,所有的资源以服务的形式交租给用户,用户可以按照需求获取相应的服务.伴随云储存和外包计算的兴起,越来越多的用户将个人数据外包于云服务器端.但是,数据所有权和管理权的分离使得用户数据面临泄露和被篡改的风险,同时网络的开放性和计算环境的不可控性易导致用户的密钥泄露,给云计算中用户的数据安全带来了巨大的安全威胁.为了保护用户的个人隐私信息以及敏感数据的安全性,必须采用高强度的认证对用户进行鉴权以实现高级别安全的访问控制,并进一步在认证的基础上建立共享的会话密钥来实现用户与云服务器之间的保密通信.当前,在云计算环境中采用了包括口令、对称密钥、公钥证书、指纹、虹网膜等多种认证方式用于实现用户鉴权.上述认证方式可以归类为 3 类与用户相关的认证因素:第 1 类认证因素是用户所能够记忆的秘密(something the user knows),例如人脑可以记忆的低熵口令;第 2 类认证因素是用户所拥有的设备(something the user has),比如用户持有的智能卡、硬件令牌和 USB KEY 等;第 3 类认证因素是用户自身独一无二的生物特征(something the user is),比如用户的指纹、虹膜等.研究者对如何利用某一类认证因素实现安全认证进行了大量的研究并取得了单因素认证协议的丰富成果.但是,每类认证因素都存在无法通过密码技术克服的缺陷.敌手可以利用虚假网站进行“网络钓鱼”或者通过间谍软件窃取用户的口令,而用户无法察觉;用户所持有的密码设备可能丢失或被窃取,攻击者可以通过逆向工程恢复出其中储存的密钥进而复制用户的密码设备;用户的生物特征容易被攻击者复制,复制的生物信息不仅可以在远程登录中通过服务器的验证,更为致命的是被复制的生物特征难以撤销.针对单因素认证协议存在的安全缺陷,密码学家提出了将多种认证因素结合以实现强安全的多因素认证密钥交换协议(multi-factor authenticated key exchange protocols,以下简称多因素协议).多因素协议的安全目标是只有攻击者同时获得用户所有的认证因素才能够通过认证,具有很高的安全强度.因此,多因素协议特别适用于云计算中具有高级别安全需求的移动泛在服务,一经提出就引起了广泛的关注,成为当前安全协议研究领域的一个热点问题.

目前对双因素认证协议的研究已较为成熟,本文主要关注采用 3 认证因素的多因素协议.2006 年,Spantzel 等人[1]结合口令、生物特征以及公钥加密设计了具有隐私保护功能的多因素协议;该协议通过零知识证明来实现生物特征认证,因此效率较低并且没有严格的安全性证明.2008 年,著名密码学家 Pointcheval 等人[2]建立了多因素协议的第一个可证明安全模型,然后利用 ElGamal 加密算法的同态性对生物模板进行逐比特加密以实现生物特征与公钥的绑定,并在此基础上设计了一个在随机预言模型下可证明安全的多因素协议.该协议为很多后续多因素协议的研究奠定了基础.2009 年,Fan 等人[3]设计了基于口令、智能卡和生物特征的多因素协议,该协议通过 3 轮交互实现了对生物特征的隐私保护.2010 年,Stebila 等人[4]以 BPR 2000 口令模型[5]为基础,提出了新的多因素协议安全模型,并设计了使用长期口令、一次口令和生物特征的多因素协议.同年,Liu 等人[6]将 Pointcheval 的多因素协议设计方法从两方推广到了三方,并且在随机预言模型下基于 CDH 假设证明了其安全性.2011 年,Huang 等人[7]提出了利用口令、智能卡和生物特征设计多因素协议的通用框架,通过模糊提取器(fuzzy extractor)[8]将“智能卡-口令”双因素认证协议与生物特征结合构造多因素协议,但其框架的效率有待提高.2012 年,Hao 等人[9]发现 Pointcheval 的多因素协议存在安全缺陷.攻击者只需要得到用户的口令就可以伪装服务器获得用户的生物模板,进而利用口令和生物模板获得用户的私钥,即攻击者仅获得口令就攻破了多因素协议的安全性.Hao 等人的攻击也适用于 Liu 等人设计的三方多因素协议[6].Hao 等人还指出必须对 Pointcheval 等人协议的设计思路进行大幅度的修改才能设计出抵抗上述攻击的多因素协议.2012 年,Yang 等人[10]提出了结合生物特征、智能卡和口令的多因素协议,在实现生物特征隐私性的同时还具有较低的通信效率,较适用于无线网络环境.密码学家 Manulis 等人[11]研究了多因素协议的模块化设计和分析方法,提出了多因素协议的安全模型,并且利用基于标签的认证(tag-based authentication)提出了多因素协议的通用构造框架.该框架将基于口

令、公钥以及生物特征的单因素协议作为子协议构造多因素协议.但是,该框架实际上是将 3 个子协议并行独立运行,计算效率和通信效率都较低.2014 年,Huang 等人[12]研究了针对脆弱通信环境的多因素协议设计方法,提出了可以在低速率通信连接的情形下加速认证进程的认证协议;此外,他们还提出了在无法连接到中心服务器的情形下的 Stand-alone 认证协议.He 等人针对之前的协议所存在的安全攻击,提出了多服务环境下的多因素认证协议[13],以及针对 USB 存储设备的多因素认证协议[14].Yu 等人[15]在 Huang 等人协议[7]的基础上设计了多因素认证协议的通用框架,通过模糊保险箱(fuzzy vault)将“智能卡-口令”双因素协议与生物特征进行结合得到安全的多因素协议,并给出了可证明安全的具体实例.

当前多因素的研究主要集中在对现有的多因素认证协议进行安全性分析并进行改进,陷入了攻击-改进-攻击-改进的恶性循环,而对于安全模型的研究以及多因素协议的形式化安全证明等方面还没有得到足够的重视,并且为数不多的具有安全性证明的多因素协议都是在随机预言模型下可证明安全的.针对目前多因素研究中存在的不足,我们以两方口令认证密钥交换协议[16]、模糊提取器[17]和签名方案[18]为基本组件设计了一个多因素协议,并且基于所采用密码学组件的安全性在标准模型下证明了协议的安全性.与已有的随机预言模型下的多因素协议相比,我们的多因素协议在具有更强的安全性的同时还具有较高的通信效率和计算效率,因此我们多因素协议更符合高级别安全的移动泛在服务的应用需求.

本文第 1 节回顾预备知识和多因素协议安全模型.第 2 节给出我们所设计的多因素协议并且在标准模型下证明其安全性.第 3 节给出多因素协议与其他相关协议的安全性和效率比较.最后第 4 节总结全文.

## 1 预备知识

### 1.1 模糊提取器

模糊提取器最早由 Dodis 等人[8]在 2004 年提出,主要用于解决生物模板认证的问题.模糊提取器允许从一个生物模板 $W$ 中产生一个生物密钥和一个公开参数,之后可以利用公开参数和与模板 $W$ 相近的另一个生物模板 $W'$恢复出生物密钥.下面我们回顾关于模糊提取器的相关定义[19].

**定义 1(度量空间(metric space))**. 度量空间$(\mathcal{M},d)$是一个定义了距离函数 $d$: $\mathcal{M}\times\mathcal{M}\to Z^{+}\cup\{0\}$的有限集合$\mathcal{M}$,其中距离函数 $d$ 满足下述性质:

正定性: $d(x,y)\geqslant 0$, 且 $d(x,y)=0$ 当且仅当 $x=y$;

对称性: $d(x,y)=d(y,x)$;

三角不等式: $d(x,z)\leqslant d(x,y)+d(y,z)$.

在生物认证中,我们通常假设生物模板在适当的距离函数定义下构成了一个度量空间.汉明距离是生物认证中最常用的距离函数.在定义模糊提取器时通常不需要具体说明所使用的距离函数,因为大多数距离函数都满足模糊提取器的定义需求.

**定义 2(统计距离(statistical distance))**. 设 $X_1$ 和 $X_2$ 是定义在有限集$\mathcal{S}$上的两个随机变量.定义 $X_1$ 和 $X_2$ 之间的统计距离为 $SD(X_1,X_2)=\frac{1}{2}\sum_{s\in\mathcal{S}}|\Pr[X_1=s]-\Pr[X_2=s]|$. 如果两个随机变量 $X_1$ 和 $X_2$ 之间的统计距离至多为$\varepsilon$,我们称 $X_1$ 和 $X_2$ 是$\varepsilon$接近的.

**定义 3(最小熵(min-entropy))**. 一个随机变量 $X$ 的最小熵定义为 $H_{\infty}(X)=-\log(\max_x \Pr[X=x])$.

**定义 4(鲁棒的模糊提取器(robust fuzzy extractor))**. 一个定义在度量空间$(\mathcal{M},d)$上的$(m,l,t,\varepsilon)$模糊提取器由两个有效的随机算法$(Gen,Rep)$组成,其中生物密钥产生算法 $Gen$ 的输入为一个生物模板 $W\in\mathcal{M}$,输出为一个生物密钥 $R\in\{0,1\}^{l}$和一个公共参数 $P\in\{0,1\}^{*}$.生物密钥复制算法 $Rep$ 的输入为另一个生物模板 $W'\in\mathcal{M}$以及公共参数 $P\in\{0,1\}^{*}$,输出为一个$\{0,1\}^{l}$的比特串,并且算法满足以下条件:

(1) 正确性:如果 $d(W,W')\leqslant t$ 并且$(R,P)$是 $Gen(W)$的输出,那么 $Rep(W',P)=R$;

(2) 安全性:对于$\mathcal{M}$上最小熵为 $m$ 的所有随机变量,即使在公开 $P$ 的条件下,$R$ 与$\{0,1\}^{l}$上的均匀分布之间的统计距离至多为$\varepsilon$;

(3) 鲁棒性:对于敌手伪造的公共参数 $P'\neq P$,算法 $Rep(W',P)\neq\perp$的概率是可忽略的,即对于敌手伪造的公共参数 $P'$,算法 $Rep(W',P')$将以极大的概率停止运行.

### 1.2 安全模型

本节对 Pointcheval 等人提出的多因素协议安全模型[2]进行扩展.我们将在第 2 节给出所设计的多因素协议在此模型下的安全证明.

多因素协议的参与者包括用户和服务器两类.为了简便起见通常假设认证服务器 $S$ 是唯一的.每个参与者可以激活多个协议实例并且并行运行多个会话实例.我们用 $\prod_U^i$ 表示参与者 $U$ 的第 $i$ 个会话实例.定义实例 $\prod_U^i$ 的会话标识 $sid_U^i$ 为 $\prod_U^i$ 发送和接受的所有消息(除了最后一条消息)的级联.我们用伙伴标识 $pid_U^i$ 表示实例 $\prod_U^i$ 想要与之通信的意定通信方的身份.此外,我们还定义布尔函数 $acc_U^i$ 用于表示会话结束时实例 $\prod_U^i$ 是否接受协议运行.

每个用户 $C$ 拥有一个由认证因素组成的多元组 $t_C=(\mathcal{W}_C,sk_C,pw_C)$, 其中,$\mathcal{W}_C$ 是其生物模板的概率分布,$sk_C$ 是用户 $C$ 所持有的高熵密钥,$pw_C$ 是用户 $C$ 从口令字典空间$\mathcal{D}$中随机选择的低熵口令.认证服务器 $S$ 持有一个认证因素的列表 $t_S=\langle t_S[C]\rangle$ ,其中每条记录 $t_S[C]$ 对应于某一个用户且 $t_S[C]$ 是由 $t_C$ 通过变换得到.认证服务器 $S$ 也拥有高熵的私钥 $sk_S$,其对应的公钥 $pw_S$ 在整个系统内是公开的,即每个用户都知道服务器的公钥 $pw_S$.

**定义 5(伙伴(partnering))**. 两个实例 $\prod_U^i$ 和 $\prod_{U'}^j$ 被称为伙伴,如果以下条件能够满足:

(1) $sid_U^i=sid_{U'}^j\neq null$; (2) $acc_U^i=acc_{U'}^j=1$; (3) $pid_U^i=U'$ 并且 $pid_{U'}^j=U$.

多因素协议的攻击者$\mathcal{A}$是一个概率多项式时间的攻击者.攻击者$\mathcal{A}$控制了用户和认证服务器之间的通信信道,可以窃听所有消息并且任意修改或伪造消息.攻击者$\mathcal{A}$的攻击能力通过以下的谕示询问来模拟:

$Execute(\prod_C^i,\prod_S^j)$: 此询问模拟攻击者$\mathcal{A}$被动窃听用户实例 $\prod_C^i$ 和服务器实例 $\prod_S^j$ 之间通信消息的能力.在会话结束后,攻击者$\mathcal{A}$将得到本次会话所有交互的消息.

$Send(\prod_U^i,m)$: 此询问模拟攻击者$\mathcal{A}$对于实例 $\prod_U^i$ 的主动攻击.攻击者$\mathcal{A}$冒充其余的参与者给实例 $\prod_U^i$ 发送消息 $m$,并得到实例 $\prod_U^i$ 接收到消息 $m$ 后执行协议所返回的消息.

$Reveal(\prod_U^i)$: 此询问模拟已知密钥攻击或会话密钥丢失.攻击者$\mathcal{A}$通过此询问可以获得用户实例 $\prod_U^i$ 所持有的会话密钥.

$Corrupt(S)$:此询问模拟对认证服务器的入侵攻击,将导致认证服务器被腐化.攻击者$\mathcal{A}$将得到认证服务器 $S$ 的私钥 $sk_S$ 以及所持有的认证因素列表 $t_S=\langle t_S[C]\rangle$.

$Corrupt(C)$:对于用户的腐化询问有 3 类:

- $Corrupt(C,sk_C,pw_C)$: 攻击者$\mathcal{A}$通过此腐化询问将得到用户 $C$ 的私钥 $sk_C$ 以及口令 $pw_C$;
- $Corrupt(C,pw_C,W_C)$: 攻击者$\mathcal{A}$通过此腐化询问将得到用户 $C$ 的口令 $pw_C$ 以及一个有效的生物模板 $W_C$;
- $Corrupt(C,sk_C,W_C)$: 攻击者$\mathcal{A}$通过此腐化询问将得到用户 $C$ 的私钥 $sk_C$ 以及一个有效的生物模板 $W_C$.

$Test(\prod_U^i)$: 此询问不模拟攻击者$\mathcal{A}$的实际攻击能力,而是用于衡量协议会话密钥的语义安全.对于参与者实例 $\prod_U^i$, 如果该实例没有生成会话密钥,那么返回无定义的符号$\perp$;否则进行一次均匀的抛币,如果抛币结果是 1,则返回实例 $\prod_U^i$ 的真实会话密钥,如果抛币结果是 0,那么返回一个与会话密钥等长的随机数.攻击者$\mathcal{A}$需要猜测抛币的结果,即猜测其获得的是真实的会话密钥还是随机数.

模型中需要限制攻击者$\mathcal{A}$只能对新鲜的会话实例 $\prod_U^i$ 进行 $Test(\prod_U^i)$ 询问,否则攻击者$\mathcal{A}$将轻易的赢得上述攻击游戏.我们称一个用户 $C$ 被完全腐化(fully corrupted)当且仅当攻击者$\mathcal{A}$得到该用户的所有认证因素,即攻击者$\mathcal{A}$得到用户 $C$ 的私钥 $sk_C$,口令 $pw_C$ 以及一个有效的生物模板 $W_C$.我们称认证服务器 $S$ 被腐化当且仅当攻击者$\mathcal{A}$进行了 $Corrupt(S)$查询.

**定义 6(新鲜性(freshness))**. 一个实例 $\prod_U^i$ 被称为是新鲜的,如果以下条件能够满足:

(1) 在实例 $\prod_U^i$ 接受协议运行并产生会话密钥之前,无论是参与者 $U$ 还是实例 $\prod_U^i$ 的伙伴都没有被完全腐化;(2) 攻击者$\mathcal{A}$没有对实例 $\prod_U^i$ 或者其伙伴实例(假如存在的话)进行 *Reveal* 查询.

注意,上述的新鲜性定义刻画了前向安全,因为我们仅限制在会话密钥产生之前会话的参与者没有被完全腐化,在会话密钥产生之后即使用户和认证服务器都被完全腐化也不会改变会话的新鲜性.

多因素协议的安全目标包括会话密钥安全和认证安全.在定义会话密钥安全的时候,给定攻击者$\mathcal{A}$所有谕示询问的能力,但是限定攻击者$\mathcal{A}$只能对新鲜的会话进行 *Test* 询问.攻击者的目标是猜测模拟 *Test* 询问时抛币的结果.如果攻击者$\mathcal{A}$成功猜测到抛币的结果,则认为$\mathcal{A}$成功,记此事件为 *Succ*.给定一个多因素协议$\mathcal{P}$,攻击者$\mathcal{A}$破坏协议$\mathcal{P}$会话密钥安全的优势定义为 $Adv_{\mathcal{P},\mathcal{D}}^{mfake}(\mathcal{A})=2\cdot\Pr[Succ]-1$.

**定义 7(会话密钥安全(session key security))**. 给定一个多因素协议$\mathcal{P}$,如果对于任意的概率多项式时间的攻击者$\mathcal{A}$,其破坏协议$\mathcal{P}$会话密钥安全的优势 $Adv_{\mathcal{P},\mathcal{D}}^{mfake}(\mathcal{A})$ 至多比 $kq_{send}/|\mathcal{D}|$ 大一个可忽略的量,则称多因素协议$\mathcal{P}$满足会话密钥安全,其中 $q_{send}$ 是敌手进行主动攻击的次数,$|\mathcal{D}|$表示字典空间的规模,$k$ 为常数.

一个多因素协议在满足会话密钥安全的同时还应该提供认证安全从而验证参与者身份的有效性.认证安全保证了除非某个会话参与者被攻击者$\mathcal{A}$完全腐化,否则攻击者$\mathcal{A}$无法仿冒该参与者.我们称攻击者$\mathcal{A}$破坏了多因素协议$\mathcal{P}$的用户认证安全,假如存在一个服务器实例 $\prod_S^i$ 接受了伙伴标识为用户 $C$ 的某次会话运行,但是用户 $C$ 被没有被攻击者$\mathcal{A}$完全腐化.我们用 $Succ_{CAuth}^{mfake}(\mathcal{A})$ 来表示攻击者$\mathcal{A}$破坏协议$\mathcal{P}$用户认证安全的优势.

**定义 8(用户认证安全(client authentication security))**. 给定一个多因素协议$\mathcal{P}$,如果对于任意的概率多项式时间的攻击者$\mathcal{A}$,其破坏协议$\mathcal{P}$用户认证安全的优势 $Succ_{CAuth}^{mfake}(\mathcal{A})$ 至多比 $kq_{send}/|\mathcal{D}|$ 大一个可忽略的量,则称多因素协议$\mathcal{P}$满足用户认证安全,其中 $q_{send}$ 是敌手进行主动攻击的次数,$|\mathcal{D}|$表示字典空间的规模,$k$ 为常数.

我们可以采用与用户认证安全类似的方式来定义服务器认证安全.为了简便起见,我们略去了服务器认证安全的定义.如果一个多因素协议$\mathcal{P}$同时满足用户认证安全和服务器认证安全,则称协议$\mathcal{P}$实现了双向认证.需要说明的是与原模型不同,这里定义的双向认证的安全强度更高,并且刻画了密钥泄漏仿冒(key compromise impersonation,简称 KCI)攻击.具体来说,我们的定义允许攻击者$\mathcal{A}$对认证服务器完全腐化,然后仿冒某个用户 $C$ 来欺骗服务器,如果欺骗成功则认为攻击者$\mathcal{A}$破坏了服务器认证安全,这里唯一的限制是用户 $C$ 没有被完全腐化.攻击者$\mathcal{A}$可以完全腐化某个参与者然后进行反向的冒充,如果冒充成功则认为攻击者$\mathcal{A}$成功,因此扩展模型中的认证安全涵盖了密钥泄漏仿冒攻击.

## 2 标准模型下的多因素协议

### 2.1 协议描述

我们的协议是在共同参考串(common reference string)模型下[16]设计的.在共同参考串模型下,系统中所有的参与者可以访问由一个可信第三方选择的公开参数.本文中共同参考串模型下的系统公开参数包括 $G_q,q,g,h,pk,\mathcal{UH},PRF,H$,其中,$G_q$ 是一个阶为大素数 $q$ 的循环群,$g,h$ 为随机选择的 $G_q$ 的两个生成元,且 $h$ 关于 $g$ 的离散对数是难解的;$pk$ 是定义在群 $G_q$ 上的一个自适应选择密文安全(adaptive choose ciphertext secure,简称 CCA 安全)的公钥加密算法 $E$ 的公钥,需要说明的是在系统中任何人都不知道 $pk$ 对应的私钥;$UH:G_q\to\{0,1\}^l$ 是一个从通用哈希函数簇$\mathcal{UH}$中随机选择的通用哈希函数;*PRF* 是一个伪随机函数簇,用 $PRF_s(a)$表示密钥种子为 $s$、输入为 $a$ 时的函数输出;$H:\{0,1\}^*\to\{0,1\}^l$ 是一个防碰撞的哈希函数,其中,$l$ 是安全参数.

在注册阶段,用户 C 从字典空间$\mathcal{D}$中随机选择其口令 $pw_C$.不失一般性,我们假设 $pw_C\in Z_q^*$. 用户 $C$ 采样一个生物模板 $W_C$ 并通过模糊提取器的生物密钥产生算法计算 $Gen(W_C)=(R_c,P_C)$, 其中,$R_c$ 是产生的生物密钥,$P_C$ 是用来恢复 $R_c$ 的公开字符串.此外,用户 $C$ 拥有用于签名的公私钥对$(pk_C,sk_C)$.用户 $C$ 将$(pw_C,R_C,P_C,pk_C)$通过安全的信道发送给服务器 $S$,服务器 $S$ 收到该消息后将关于用户 $C$ 的记录保存在其数据库中.服务器 $S$ 同样拥有用于签名的公私钥对$(pk_S,sk_S)$,其中系统中的所有用户都知道服务器 $S$ 的公钥 $pk_S$.

我们所设计的多因素协议在密钥交换阶段共有 3 轮消息交互,详细步骤如图 1 所示,具体的流程如下.

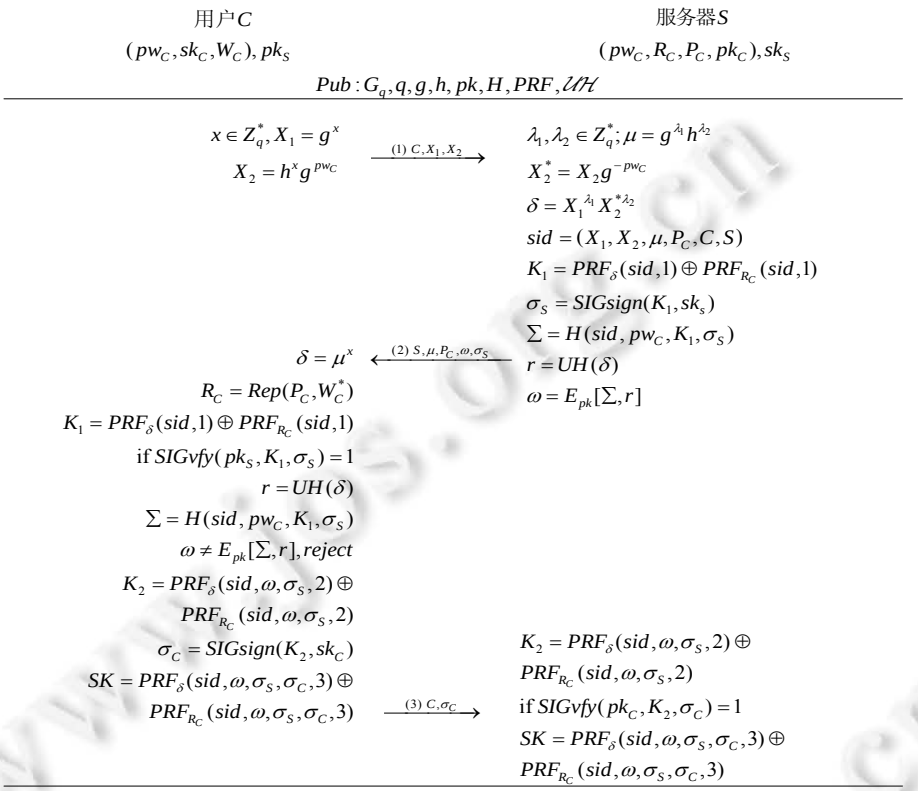


Fig.1 An MFAKE protocol in the standard model

图 1 标准模型下的多因素协议

第 1 轮:用户 $C$ 选择一个随机数 $x \in Z_q^*$, 然后利用其口令 $pw_C$ 计算 $X_1 = g^x$ 以及 $X_2 = h^x g^{pw_C}$. 用户 $C$ 发送消息$(C,X_1,X_2)$给服务器 $S$.

第 2 轮:服务器 $S$ 接收到消息$(C,X_1,X_2)$后,首先选择两个随机数 $\lambda_1,\lambda_2 \in Z_q^*$, 然后计算 $\mu = g^{\lambda_1} h^{\lambda_2}$, $X_2^* = X_2 g^{-pw_C}$ 以及 $\delta = X_1^{\lambda_1} X_2^{*\lambda_2}$. 这里,$\delta$是标准模型下两方口令密钥交换协议计算得到的会话密钥.服务器 $S$ 利用当前的会话标识 $sid = (X_1, X_2, \mu, P_C, C, S)$ 计算 $K_1 = PRF_\delta(sid,1) \oplus PRF_{R_C}(sid,1)$, 其中,$\delta$和 $R_c$ 分别是伪随机函数簇的密钥种子,而$(sid,1)$为伪随机函数的输入.服务器 $S$ 然后利用其私钥 $sk_S$ 对 $K_1$ 进行签名并得到签名$\sigma_S$= $SIGsign(K_1, sk_S)$. 服务器 $S$ 将$\delta$作为输入计算通用哈希函数的输出 $r = \mathcal{UH}(\delta)$ 并计算消息摘要 $\sum = H(sid, pw_C, K_1, \sigma_S)$. 最后,服务器 $S$ 将 $r$ 作为随机输入对消息摘要Σ利用 CCA 安全的加密算法 $E$ 的公钥 $pk$ 进行加密并计算密文 $\omega = E_{pk}[\sum, r]$, 最终发送消息 $(S, \mu, P_C, \omega, \sigma_S)$ 给用户 $C$.

第 3 轮:用户 $C$ 接收到消息 $(S, \mu, P_C, \omega, \sigma_S)$ 后,首先利用$\mu$计算两方口令认证密钥交换协议的秘密值 $\delta = \mu^x$; 用户 $C$ 然后采样一个生物模板 $W_C^*$ 并利用模糊提取器的生物密钥复制算法计算 $R_C = Rep(P_C, W_C^*)$. 用户 $C$ 计算 $K_1 = PRF_\delta(sid,1) \oplus PRF_{R_C}(sid,1)$ 并验证签名 $\sigma_S$ 是否有效.如果签名无效则拒绝协议运行,否则用户 $C$ 计算 $r$= $\mathcal{UH}(\delta)$并利用 $r$ 作为随机输入计算密文 $E_{pk}[\sum, r]$, 其中, $\sum = H(sid, pw_C, K_1, \sigma_S)$. 如果 $E_{pk}[\sum, r]$ 与服务器 $S$ 发送的密文$\omega$不相等,那么用户 $C$ 终止本次会话;否则用户 $C$ 计算 $K_2 = PRF_\delta(sid, \omega, \sigma_S, 2) \oplus PRF_{R_C}(sid, \omega, \sigma_S, 2)$ 并利用其私钥 $sk_C$ 对 $K_2$ 计算签名 $\sigma_C = SIGsign(K_2, sk_C)$. 用户 $C$ 最后计算会话密钥 $SK = PRF_\delta(sid, \omega, \sigma_S, \sigma_C, 3) \oplus PRF_{R_C}(sid, \omega, \sigma_S, \sigma_C, 3)$, 发送消息$(C,\sigma_C)$给服务器 $S$ 并接受本次会话.

服务器 $S$ 接收到消息$(C,\sigma_C)$后,计算 $K_2 = PRF_{\delta}(sid,\omega,\sigma_S,2) \oplus PRF_{R_C}(sid,\omega,\sigma_S,2)$ 并验证签名$\sigma_C$的有效性.如果签名$\sigma_C$无效,则服务器 $S$ 终止本次会话;否则,服务器 $S$ 计算会话密钥 $SK = PRF_{\delta}(sid,\omega,\sigma_S,\sigma_C,3) \oplus PRF_{R_C}(sid,\omega,\sigma_S,\sigma_C,3)$ 并接受本次会话.

注 1:在协议的第 2 轮消息中要求服务器 S 同时发送签名$\sigma_S$和密文$\omega$的原因在于,我们需要通过$\omega$来证明服务器 $S$ 知道口令;$\sigma_S$尽管是对会话密钥验证值的签名,但恶意攻击者在不知道口令的情况下,可以直接随机选择 $y \in Z_q^*$ 并且令$\mu=g^y$从而与用户计算出共同的秘密值 $g^{xy}$.

注 2:为了协议简便起见,我们的协议中并没有给出模糊提取器和签名的具体算法,任何在标准模型下可证明安全的签名算法以及在标准模型下鲁棒的模糊提取器都可以满足我们所提出的多因素协议的要求.

注 3:根据文献[8]中模糊提取器的构造方法,服务器在拥有$(R_C,P_C)$时无法恢复出用户的生物模板 $W_C$,因此我们的协议可以实现对用户生物信息的隐私保护.关于模糊提取器构造的更多细节,参见文献[8].

### 2.2 安全性证明

本节给出多因素协议的安全性证明.通过定理 1 证明多因素协议的会话密钥安全和认证安全.

**定理 1**. 设$\mathcal{P}$是第 2.1 节的多因素协议,$\mathcal{A}$是进行了 $q_{send}$ 次主动攻击的概率多项式时间的攻击者.假设 DDH 假设在循环群 $G_q$ 中成立,协议中所使用的公钥加密算法 $E$ 是 CCA 安全的,签名算法对于适应性选择消息是存在性不可伪造的,并且$\mathcal{P}$中所使用的是一个鲁棒的模糊提取器,那么敌手$\mathcal{A}$攻击本文的多因素协议的会话密钥安全和认证安全的优势的上界分别为

$$Adv_{\mathcal{P},\mathcal{D}}^{mfake}(\mathcal{A}) \leqslant \frac{q_{send}}{|\mathcal{D}|} + neg(l),$$

$$Succ_{CAuth}^{mfake}(\mathcal{A}) \leqslant \frac{q_{send}}{|\mathcal{D}|} + neg(l),$$

$$Succ_{SAuth}^{mfake}(\mathcal{A}) \leqslant \frac{q_{send}}{|\mathcal{D}|} + neg(l),$$

其中,$neg(l)$表示关于安全参数 $l$ 的一个可忽略函数.

证明:我们通过混合实验的方式来证明定理 1.混合实验从真实的攻击游戏开始,然后逐步修改每个混合实验中的模拟规则,直到攻击者的攻击优势为 0 的混合实验结束.对两个相邻的混合实验,我们将计算攻击者在这两个混合实验中优势差距的上界,最终计算出攻击者攻击多因素协议的优势上界.我们用$\Delta i$ 表示混合实验 $Exp_i$ 与 $Exp_{i+1}$ 的差别.对于混合实验 $Exp_i$,我们定义以下的事件:

$S_i^{mfake}$:此事件用于刻画多因素协议的会话密钥安全,此事件表示攻击者$\mathcal{A}$正确猜测到 *Test* 查询中的随机抛币结果,即攻击者$\mathcal{A}$赢得了会话密钥安全的攻击游戏;

$A_i^{CAuth}$:此事件用于刻画多因素协议的用户认证安全,此事件表示攻击者$\mathcal{A}$成功仿冒了一个没有被完全腐化的用户并且令服务器接受了仿冒的会话运行,即攻击者$\mathcal{A}$破坏了多因素协议的用户认证安全;

$A_i^{SAuth}$:此事件用于刻画多因素协议的服务器认证安全,此事件表示攻击者$\mathcal{A}$成功仿冒了未被完全腐化的服务器实例并与某个用户建立了会话,即攻击者$\mathcal{A}$破坏了多因素协议的服务器认证安全.

混合实验 $Exp_0$:此混合实验模拟了针对多因素协议攻击游戏的真实运行.根据定义有:

$$Adv_{\mathcal{P},\mathcal{D}}^{mfake}(\mathcal{A}) = 2\Pr[S_0^{mfake}] - 1,$$

$$Succ_{CAuth}^{mfake} = \Pr[A_0^{CAuth}],$$

$$Succ_{SAuth}^{mfake} = \Pr[A_0^{SAuth}].$$

混合实验 $Exp_1$:从此混合实验开始,我们将对攻击者$\mathcal{A}$通过 *Execute* 询问实施的被动攻击的会话模拟规则进行修改.首先令用户 $C$ 在计算第 1 轮的消息的时候不使用其真实的口令 $pw_C$,而是选择口令空间之外的一个虚假口令 $pw_C^*$, 即用户 $C$ 正常计算 $X_1=g^x$,但是令 $X_2 = h^x g^{pw_C^*}$. 相应地,服务器 $S$ 在接收到消息$(C,X_1,X_2)$时,同样

采用虚假口令 $pw_C^*$ 进行会话模拟.我们可以将真实口令 $pw_C$ 和虚假口令 $pw_C^*$ 看做针对 ElGamal 加密算法的两个挑战消息,因此混合实验 $Exp_0$ 和 $Exp_1$ 的差别至多是攻击者 $\mathcal{A}$ 攻破 ElGamal 加密算法的 CPA 安全性的优势,而 ElGamal 加密算法的 CPA 安全性又可以归约到 DDH 假设.我们有:

$$\Delta_0 \leqslant neg(l).$$

混合实验 $Exp_2$:在此混合实验中,我们继续修改对 *Execute* 询问的模拟规则.我们令服务器 $S$ 在接收到消息 $(C,X_1,X_2)$时,正常计算 $\mu = g^{\lambda_1}h^{\lambda_2}$,但是不计算 $X_2^*$,而是直接从循环群 $G_q$ 中随机选择 $\delta$.根据文献[16]中证明的结论知,当密文 $(X_1,X_2)$不是对真实口令 $pw_C$ 的有效密文时,$\delta$的分布与循环群 $G_q$ 上的均匀分布是统计不可区分的.我们有:

$$\Delta_1 \leqslant neg(l).$$

混合实验 $Exp_3$:在此混合实验中,我们继续修改对 *Execute* 询问的模拟规则.进一步令服务器 $S$ 在计算 $r=\mathcal{UH}(\delta)$时不通过通用哈希函数计算,而是直接从相应的值域中随机选择.在上一个混合实验中,我们已经从循环群 $G_q$ 中随机选择 $\delta$的取值.根据通用哈希函数的性质可知,当其输入为随机值时,通用哈希函数簇的输出与其值域中的均匀分布是统计不可区分的.我们有:

$$\Delta_2 \leqslant neg(l).$$

混合实验 $Exp_4$:在此混合实验中,继续修改对 *Execute* 询问的模拟规则.令服务器 $S$ 在计算Σ时,不输入真实的口令,即令 $\sum = h(sid,K_1,\sigma_S)$. 为了保证模拟的一致性,要求用户 $C$ 在验证密文 $\omega = E_{pk}[\sum,r]$ 的有效性时,采用与服务器 $S$ 相同的方式计算Σ.混合实验 $Exp_4$ 与上一个混合实验的差别仅仅在于密文 $\omega$ 是对 $h(sid,pw_C,K_1,\sigma_S)$ 的加密还是对 $h(sid,K_1,\sigma_S)$ 的加密.由于公钥加密算法 $E$ 是 CCA 安全的,因此混合实验 $Exp_3$ 和 $Exp_4$ 的差别至多是攻击者 $\mathcal{A}$ 破坏公钥加密算法 $E$ 的 CCA 安全性的攻击优势.实际上,这里只需要用到公钥加密算法 $E$ 的 CPA 安全性,因为对此混合实验的模拟不需要用到解密预言机.我们有:

$$\Delta_3 \leqslant neg(l).$$

混合实验 $Exp_5$:在此混合实验中,我们最后一次修改对 *Execute* 询问的模拟规则.令服务器 $S$ 在计算 $K_1,K_2$ 以及 $SK$ 时,不通过伪随机函数簇 *PRF* 计算,而是直接从相应的值域中随机选择上述秘密值.为了保证模拟的一致性,要求用户 $C$ 采用服务器 $S$ 选定的 $K_1,K_2$ 以及 $SK$ 的值.由于 $\delta$ 是从循环群 $G_q$ 中随机选择的,而由模糊提取器的性质可知生物密钥 $R_C$ 的分布与均匀分布是统计不可区分的,因此由伪随机函数簇 *PRF* 的定义可知,攻击者 $\mathcal{A}$ 区分两个混合实验 $Exp_4$ 和 $Exp_5$ 的概率是可忽略的.我们有:

$$\Delta_4 \leqslant neg(l).$$

到目前为止,我们已经完成了对被动会话的模拟修改,使得在被动会话中不会泄露任何关于口令的信息(被动会话的模拟都采用虚假口令或者避免包含真实的口令),并且会话密钥是随机选择的.由于生物密钥和签名私钥都是高熵密钥,因此我们在被动会话中并没有修改对这两类密钥的模拟规则.通过上述模拟,攻击者 $\mathcal{A}$ 通过 *Execute* 询问将不会得到口令的任何信息,并且攻击者 $\mathcal{A}$ 区分会话密钥的优势为 0.需要强调的是我们仅仅修改了被动会话的模拟规则,对攻击者 $\mathcal{A}$ 通过 *Send* 询问进行的主动攻击依然根据多因素协议的描述来模拟.但是对于攻击者 $\mathcal{A}$ 通过 *Send* 询问进行的主动攻击,假如攻击者 $\mathcal{A}$ 只是如实传递消息而不对消息进行任何修改,对于这一类主动攻击的会话的模拟规则与对于 *Execute* 询问的模拟规则相同.此外,从下一个实验开始,我们在产生公开参数 $h$ 和公钥 $pk$ 时记录相应的密钥作为陷门信息.上述修改不会改变攻击者 $\mathcal{A}$ 的视图.

混合实验 $Exp_6$:从此混合实验开始,我们将对攻击者 $\mathcal{A}$ 通过 *Send* 询问进行的主动攻击的模拟规则进行修改.对于某个用户 $C$,如果攻击者 $\mathcal{A}$ 对该用户进行了 $Corrupt(C,pw_C,W_C)$询问,即攻击者腐化了用户 $C$ 的口令和生物模板,此时我们修改服务器 $S$ 对攻击者 $\mathcal{A}$ 针对用户 $C$ 进行的 *Send* 询问的模拟规则.当服务器 $S$ 接收到攻击者 $\mathcal{A}$ 发送的 $Send(S,(C,X_1,X_2))$ 询问后,按照协议的描述进行模拟并返回相应的消息.在攻击者 $\mathcal{A}$ 发送的 $Send(S,(C,\sigma_C))$询问时,服务器 $S$ 不验证签名的有效性并直接拒绝本次协议运行.混合实验 $Exp_6$ 和 $Exp_5$ 是完全相同的,除非攻击者 $\mathcal{A}$ 伪造了一个有效的签名,但是被服务器 $S$ 拒绝.由于协议中所采用的签名方案是对适应性选择攻击存

在性不可伪造的,攻击者$\mathcal{A}$区分两个混合实验$Exp_6$和$Exp_5$的概率至多是破坏签名体制不可伪造性的优势.则有:

$$\Delta_5 \leqslant neg(l).$$

混合实验$Exp_7$:在此混合实验中,我们继续对攻击者$\mathcal{A}$通过$Send$询问进行的主动攻击的模拟规则进行修改.对于某个用户$C$,如果攻击者$\mathcal{A}$对该用户进行了$Corrupt(C,pw_C,W_C)$询问,即攻击者腐化了用户$C$的口令和签名私钥.当服务器$S$接收到攻击者$\mathcal{A}$发送的$Send(S,(C,X_1,X_2))$询问后,按照协议的描述进行模拟,但是在计算$K_1$,$K_2$以及$SK$时不通过伪随机函数簇$PRF$计算,而是在相应的值域中随机选择.其余的模拟规则与协议描述完全相同.进一步,在攻击者$\mathcal{A}$发送的$Send(S,(C,\sigma_C))$询问时,服务器$S$不验证签名的有效性并直接拒绝本次协议运行.混合实验$Exp_7$和$Exp_6$是完全相同的,除非攻击者$\mathcal{A}$成功猜测到$K_2$的值并进行了签名,但是该签名被服务器$S$拒绝.此时攻击者$\mathcal{A}$拥有用户$C$的签名密钥,但是生物密钥对于攻击者$\mathcal{A}$是完全随机的,由伪随机函数簇$PRF$的性质得知攻击者$\mathcal{A}$成功猜测到随机值$K_2$的概率是可忽略的,因此我们有:

$$\Delta_6 \leqslant neg(l).$$

混合实验$Exp_8$:在此混合实验中,我们继续对攻击者$\mathcal{A}$通过$Send$询问进行的主动攻击的模拟规则进行修改.对于某个用户$C$,如果攻击者$\mathcal{A}$对该用户进行了$Corrupt(C,sk_C,W_C)$询问,即攻击者腐化了用户$C$的生物模板和签名私钥.当服务器$S$接收到攻击者$\mathcal{A}$发送的$Send(S,(C,X_1,X_2))$询问后,利用记录的$h$所对应的私钥对密文$(X_1,X_2)$进行解密,如果解密得到的是真实的口令,我们将结束整个攻击游戏的模拟并且宣布攻击者$\mathcal{A}$获胜.显然,上述修改只是增加了一种攻击者$\mathcal{A}$获胜的方式,攻击者$\mathcal{A}$获胜的优势将会增加.我们有:

$$\Pr[S_8^{mfake}] \geqslant \Pr[S_7^{mfake}],$$
$$\Pr[A_8^{CAuth}] \geqslant \Pr[A_7^{CAuth}],$$
$$\Pr[A_8^{SAuth}] \geqslant \Pr[A_7^{SAuth}].$$

混合实验$Exp_9$:在此混合实验中,我们继续对攻击者$\mathcal{A}$通过$Send$询问进行的主动攻击的模拟规则进行修改.对于某个用户$C$,如果攻击者$\mathcal{A}$对该用户进行了$Corrupt(C,sk_C,W_C)$询问,即攻击者腐化了用户$C$的生物模板和签名私钥.当服务器$S$接收到攻击者$\mathcal{A}$发送的$Send(S,(C,X_1,X_2))$询问后,利用记录的$h$所对应的私钥对密文$(X_1,X_2)$进行解密,如果解密得到的不是正确的口令,我们将从循环群$G_q$中随机选择$\delta$,剩余的模拟则按照协议描述执行.当攻击者$\mathcal{A}$发送$Send(S,(C,\sigma_C))$,我们令服务器$S$不验证签名的有效性并直接拒绝本次协议运行.由于$(X_1,X_2)$不是真实口令的有效密文,因此$\delta$值将在$G_q$中均匀分布,因此攻击者$\mathcal{A}$能够猜测到随机值$\delta$并且正确计算$K_2$的概率是可忽略的.我们有:

$$\Delta_8 \leqslant neg(l).$$

混合实验$Exp_{10}$:在此混合实验中,我们最后一次修改对攻击者$\mathcal{A}$通过$Send$询问进行的主动攻击的模拟规则进行修改.对于某个用户$C$,如果攻击者$\mathcal{A}$仿冒未被腐化的服务器$S$进行了$Send(C,start)$询问,用户$C$随机选择$X_1$,$X_2$并将消息$(C,X_1,X_2)$返回给攻击者.当用户$C$接收到攻击者$\mathcal{A}$返回的$Send(C,(S,\mu,P_C,\omega,\sigma_S))$询问时,我们令用户$C$直接拒绝本次会话运行.显然,由于服务器$S$未被腐化,因此攻击者$\mathcal{A}$无法得到服务器$S$的签名私钥$sk_S$,与混合实验$Exp_6$中的分析类似,混合实验$Exp_9$与$Exp_8$的差别至多是攻击者$\mathcal{A}$攻破签名方案的存在性不可伪造的优势.我们有:

$$\Delta_9 \leqslant neg(l).$$

在混合实验$Exp_{10}$中,攻击者$\mathcal{A}$通过$Execute$询问进行的被动会话中都不包含真实口令的信息,并且会话密钥是随机选择的;对于攻击者$\mathcal{A}$通过$Send$询问进行的主动攻击,只有在攻击者$\mathcal{A}$不知道口令并且在第1条消息中正确猜测到口令的情况下才令攻击者$\mathcal{A}$赢得攻击游戏,其余的所有主动攻击都将被拒绝.而攻击者$\mathcal{A}$正确猜测口令的概率为$\frac{q_{send}}{|\mathcal{D}|}$.因此,我们有:

$$\Pr[S_{10}^{mfake}] \leqslant \frac{q_{send}}{|\mathcal{D}|},$$

$$\Pr[A_{10}^{CAuth}] \leqslant \frac{q_{send}}{|\mathcal{D}|},$$

$$\Pr[A_{10}^{SAuth}] \leqslant \frac{q_{send}}{|\mathcal{D}|}.$$

综上,定理 1 得证. □

## 3 协议性能比较

据我们所知,Pointcheval 等人的协议[2]是目前仅有的一个采用口令、高熵密钥和生物信息实现认证的多因素协议.本节将对多因素协议与 Pointcheval 等人的协议(简称 PZ 协议)从效率和安全性两个方面进行比较.

在效率方面,我们主要从计算代价和通信代价两个方面来衡量.我们采用标准模型下可证明安全的签名方案[18]、标准模型下 CCA 安全的 DHIES 公钥加密算法[20]以及标准模型下可证明安全的鲁棒的模糊提取器[17]来对多因素协议进行实例化.通信代价主要通过通信带宽和通信轮数来衡量.用户和服务器的身份可由 32 比特的字符串表示,循环群中的元素可由 160 比特长的字符串表示,哈希函数、通用哈希函数以及伪随机函数的输出长度都设为 160 比特.模糊提取器中的公开参数 $P_C$ 的长度为 62 464 比特.由于 PZ 协议采用了逐比特加密的方式来认证生物模板,通常假设生物模板的长度为 1 024 比特,而其中的认证标签的长度为 4 比特.计算代价方面,我们只考虑较为耗时的模幂运算(记为 e)并将公钥加密和签名方案的代价通过模幂运算的个数来衡量.由模糊提取器的高效性可知,*Gen* 算法和 *Rep* 算法的计算代价和哈希函数的计算代价相当,因此我们略去该部分运算的代价.DHIES 算法加密时需要 2 个模幂运算,而签名算法在签名时需要 1 个模幂运算,验证签名时需要 1 个模幂运算和 1 个双线性对运算.注意,形如 $g^x h^y$ 的模幂运算的乘积利用并行加速算法可以通过 1 个模幂运算的代价求得,并且 1 个双线性对的运算代价约等价于 4 个模幂运算.从表 1 可以看出,我们的标准模型下的多因素协议无论是在计算效率还是通信效率方面都远高于 PZ 协议.但是需要说明的是,PZ 协议之所以效率低主要是假设生物模板是公开的,并且采用了逐比特加密的方式来认证生物信息.

**Table 1** Complexity comparison with Pointcheval et al.'s MFAKE protocol

**表 1** 与 Pointcheval 等人多因素协议的复杂性比较

| 比较的协议 | 通信代价 | | 计算代价 | | |
|---|---|---|---|---|---|
| | 通信带宽(bits) | 通信轮数 | 用户 | 服务器 | 总代价 |
| PZ 协议[2] | 172 416 | 4 | 1 026e | 2 025e | 3 051e |
| 我们的协议 | 63 840 | 3 | 11e | 11e | 22e |

表 2 总结了多因素协议在标准模型下是安全的,而 PZ 协议是在随机预言模型下可证明安全的.我们的协议具有双向认证并且真正实现了多因素安全,而 PZ 协议仅实现了用户向服务器的单向认证,这也是 PZ 协议被 Hao 等人[9]所攻击的根本原因.尽管 Pointcheval 等人声称 PZ 协议中服务器储存对生物模板进行逐比特加密的密文,从而实现了对用户生物模板的隐私保护,但 Hao 等人攻击表明该结论是错误的.此外,多因素协议还可以抵抗密钥泄漏仿冒攻击,因此比 PZ 协议具有更强的安全性.需要说明的是 PZ 协议中假设生物模板是公开的,而我们的协议中假设生物模板是秘密的.虽然目前研究者对于生物模板究竟应该被假设为公开合理还是假设为秘密合理争论不定,尚未形成统一的意见[9,11],但是生物模板是公开的假设下多因素协议的设计难度更大.这是我们的协议相比 PZ 协议的一个不足之处.

**Table 2** Security comparison with Pointcheval et al.'s MFAKE protocol

**表 2** 与 Pointcheval 等人多因素协议的安全性比较

| 比较的协议 | 安全模型 | 多因素安全 | 双向认证 | KCI 攻击 | 生物隐私保护 | 生物模板假设 |
|---|---|---|---|---|---|---|
| PZ 协议[2] | 随机预言模型 | 否 | 否 | 不抵抗 | 否 | 公开 |
| 我们的协议 | 标准模型 | 是 | 是 | 抵抗 | 是 | 隐私 |

## 4 结束语

本文以模糊提取器为工具设计了一个具有隐私保护功能的多因素认证密钥交换协议,并且在标准模型下基于 DDH 假设证明了其安全性.我们的协议真正实现了多因素协议的安全目标并且具有前向安全;此外,在认证过程中服务器不需要得到用户的生物模板,因此更好地保护了用户的隐私.安全性和效率比较表明我们的多因素协议不仅具有更高的安全性,同时具备更高的计算和通信效率.

**致谢** 在此,我们向匿名的审稿老师的工作表示感谢.

**References**:

[1] Spantzel A, Squicciarini A, Bertino E. Privacy preserving multi-factor authentication with biometrics. In: Proc. of the 2nd ACM Workshop on Digital Identity Management (DIM 2006). New York: ACM, 2006. 63−72. [doi: 10.1145/1179529.1179540]

[2] Pointcheval D, Zimmer S. Multi-Factor authenticated key exchange. In: Bellovin M, *et al*., eds. Proc. of the Applied Cryptography and Network Security (ACNS 2008). LNCS 5037, Berlin: Springer-Verlag, 2008. 277−295. [doi: 10.1007/978-3-540-68914-0_17]

[3] Fan CI, Lin YH. Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. IEEE Trans. on Information Forensics and Security, 2009,4(4):933−945. [doi: 10.1109/TIFS.2009.2031942]

[4] Stebila D, Udupi P, Chang S. Multi-Factor password-authenticated key exchange. In: Proc. of the CRPIT 2010. New York: ACM, 2010. 56−66.

[5] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attack. In: Preneel B, ed. Proc. of the EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 139−155. [doi: 10.1007/3-540-45539-6_11]

[6] Liu Y, Wei FS, Ma CG. Multi-Factor authenticated key exchange protocol in the three-party setting. In: Lai XJ, *et al*., eds. Proc. of the 6th China Int'l Conf. on Information Security and Cryptology (Inscrypt 2010). LNCS 6584, Berlin: Springer-Verlag, 2011. 255−267. [doi: 10.1007/978-3-642-21518-6_18]

[7] Huang XY, Yang X, Chonka A, Zhou JY, Deng RH. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Trans. on Parallel and Distributed Systems, 2011,22(8):1390−1396. [doi: 10.1109/TPDS.2010.206]

[8] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Cachin C, Camenisch J, eds. Advances in Cryptology–EUROCRYPT 2004. LNCS 3027, Berlin: Springer-Verlag, 2004. 523−540. [doi: 10.1007/978-3-540-24676-3_31]

[9] Hao F, Clarke D. Security analysis of a multi-factor authenticated key exchange protocol. In: Bao F, Samaratieds P, Zhou JY, eds. Proc. of the Applied Cryptography and Network Security (ACNS 2012). LNCS 7341, Berlin: Springer-Verlag, 2012. 1−11. [doi: 10.1007/978-3-642-31284-7_1]

[10] Yang DX, Yang B. A novel multi-factor authenticated key exchange scheme with privacy preserving. Journal of Internet Services and Information Security, 2012,1(2/3):44−56.

[11] Fleischhacker N, Manulis M, Sadrazodi A. Modular design and analysis framework for multi-factor authentication and key exchange. In: Chen LQ, Mitchell C, eds. Proc. of the Security Standardisation Research (SSR 2014). LNCS 8893, Berlin: Springer-Verlag, 2014. 190−214. [doi: 10.1007/978-3-319-14054-4_12]

[12] Huang XY, Xiang Y, Bertino E, Zhou J, Xu L. Robust multi-factor authentication for fragile communications. IEEE Trans. on Dependable and Secure Computing, 2014,11(6):568−581. [doi: 10.1109/TDSC.2013.2297110]

[13] He DB, Wang D. Robust biometrics-based authentication scheme for multi-server environment. IEEE Systems Journal, 2015,9(3):816−823. [doi: 10.1109/JSYST.2014.2301517]

[14] He DB, Kumar N, Lee JH, Sherratt RS. Enhanced three-factor security protocol for consumer USB mass storage devices. IEEE Trans. on Consumer Electronics, 2014,60(1):30−37. [doi: 10.1109/TCE.2014.6780922]

[15] Yu J, Wang G, Mu Y, Gao W. An efficient generic framework for three-factor authentication with provably secure instantiation. IEEE Trans. on Information Forensics and Security, 2014,9(12):2302−2313. [doi: 10.1109/TIFS.2014.2362979]

[16] Jiang SQ, Gong G. Password based key exchange with mutual authentication. In: Handschuh H, Hasan A, eds. Proc. of the SAC 2004. LNCS 3357, Berlin: Springer-Verlag, 2004. 267−279. [doi: 10.1007/978-3-540-30564-4_19]

[17] Dodis Y, Katz J, Reyzin L, Reyzin L, Smith A. Robust fuzzy extractors and authenticated key agreement from close secrets. In: Dwork C, ed. Advances in Cryptology—CRYPTO 2006. LNCS 4117, Berlin: Springer-Verlag, 2006. 232−250. [doi: 10.1007/11818175_14]

[18] Boneh D, Boyen X. Short signatures without random oracles. In: Cachin C, Camenisch J, eds. Advances in Cryptology—EUROCRYPT 2004. LNCS 3027, Berlin: Springer-Verlag, 2004. 56−73. [doi: 10.1007/978-3-540-24676-3_4]

[19] Boyen X, Dodis Y, Katz J, Ostrovsky R, Smith A. Secure remote authentication using biometric data. In: Cramer R, ed. Advances in Cryptology—EUROCRYPT 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 147−163. [doi: 10.1007/11426639_9]

[20] Abdalla M, Bellare M, Rogaway P. The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: David N, ed. Proc. of the CT-RSA 2001. LNCS 2020, Berlin: Springer-Verlag, 2001. 143−158. [doi: 10.1007/3-540-45353-9_12]

**魏福山**(1983－),男,甘肃武威人,博士,讲师,主要研究领域为安全协议,无线网络安全认证.

**张刚**(1975－),男,讲师,主要研究领域为无线网络安全.

**马建峰**(1963－),男,教授,博士生导师,CCF会士,主要研究领域为计算机系统安全,移动/无线安全,系统可生存性,可信计算.

**马传贵**(1962－),男,教授,博士生导师,主要研究领域为信息安全.