UCAP：云计算中一种 PCL 安全的用户认证协议

李学峰[1,2]，张俊伟[2]，马建峰[2]
（1. 青海广播电视大学教育信息技术与资源建设中心，青海 西宁 810008；2. 西安电子科技大学计算机学院，陕西 西安 710071）

摘 要：云计算利用网络使 IT 服务变得弹性可变，如果用户需要登录到云端来使用服务与应用，系统需要确保使用者的身份合法，才能为其服务。为此，提出一种面向云计算协议组合逻辑（PCL, protocol composition logic）安全的用户认证协议（UCAP）。UCAP 引入了可信第三方，使用基于对称加密密钥的认证方法，确保参与认证双方的相互认证，实现协议会话的认证性和密钥机密性。协议主要分成 2 个阶段：初始认证阶段，由可信第三方生成根会话密钥后，认证双方相互认证；重认证阶段，不需要可信第三方的参与，认证双方快速生成子会话密钥并实现相互认证。在协议组合逻辑模型下给出所提协议的形式化描述并利用顺序组合证明方法分析了所提协议的安全属性。同其他相关协议比较及实验分析表明，UCAP 在不影响安全性的前提下，提高了用户认证的通信与计算效率，不但在重认证阶段不依赖可信第三方，而且整个过程不依赖可信第三方同步时钟。

关键词：云计算；用户认证；协议组合逻辑；机密性；相互认证
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2018147

UCAP: a PCL secure user authentication protocol in cloud computing

LI Xuefeng[1,2], ZHANG Junwei[2], MA Jianfeng[2]
1. Education Information Technology and Resource Construction Center, Qinghai Radio & Television University, Xining 810008, China
2. School of Computer Science & Technology, Xidian University, Xi'an 710071, China

Abstract: As the combine of cloud computing and Internet breeds many flexible IT services, cloud computing becomes more and more significant. In cloud computing, a user should be authenticated by a trusted third party or a certification authority before using cloud applications and services. Based on this, a protocol composition logic (PCL) secure user authentication protocol named UCAP for cloud computing was proposed. The protocol used a symmetric encryption symmetric encryption based on a trusted third party to achieve the authentication and confidentiality of the protocol session, which comprised the initial authentication phase and the re-authentication phase. In the initial authentication phase, the trusted third party generated a root communication session key. In the re-authentication phase, communication users negotiated a sub session key without the trusted third party. To verify the security properties of the protocol, a sequential compositional proof method was used under the protocol composition logic model. Compared with certain related works, the proposed protocol satisfies the PCL security. The performance of the initial authentication phase in the proposed scheme is slightly better than that of the existing schemes, while the performance of the re-authentication phase is better than that of other protocols due to the absence of the trusted third party. Through the analysis results, the proposed protocol is suitable for the mutual authentication in cloud computing.

Key words: cloud computing, user authentication, protocol composition logic, confidentiality, mutual authentication

收稿日期：2017−07−05；**修回日期**：2018−07−01
通信作者：张俊伟，jwzhangxd@126.com
基金项目：国家自然科学基金资助项目（No.61472310, No.61372075）；国家高技术研究发展计划（“863 计划”）基金资助项目（No.2015AA016007）；青海社会科学规划课题基金资助项目（No.16034）
Foundation Items: The National Natural Science Foundation of China (No.61472310, No.61372075), The National High Technology Research and Development Program of China (863 Program) (No.2015AA016007), The Social Science Planning Project of Qinghai (No.16034)

1　引言

基于互联网技术的云计算模型被视为下一代 IT 技术，它以资源租用、应用托管、服务外包为核心，迅速成为计算机技术发展的热点[1]。云计算的开放性和复杂性决定了其安全性面临着比传统信息系统更为严峻的挑战[2-3]。作为安全需求的第一道防线，身份认证也面临着新的挑战与威胁，这就需要一个有效的身份认证协议。

面对云计算安全威胁，需要采用加强身份认证机制，即相互认证等多种办法，来保护云计算环境下的用户数据。

云安全联盟（CSA, cloud security alliance）在《云计算安全指南（3.0）》中提出了身份认证即服务的概念，它包括云服务中的身份、权限及授权或访问管理中任何一部分的管理工作，身份认证即服务也是安全即服务的一项重要内容。当用户试图访问云计算服务时，借助身份提供商（IdP, identity provider）的协助，完成与云服务提供商（CSP, cloud service provider）的认证。因此，通过可信第三方（TTP, trusted third party）协助用户与 CSP 相互认证，对 CSP 来说降低了安全成本，对用户来说能够明确他们所获得的安全服务，同时使 CSP 遵守清晰、一致的服务标准。

基于密码技术的认证协议从协议设计的角度可分为无信任管理中心和有信任管理中心这 2 类。在无信任管理中心认证协议中，一般有基于口令[4-5]、基于用户生物特征[6]、基于双方持有秘密[7]的认证协议；在有信任管理中心的认证协议中，一般可以分为基于对称密钥的认证协议[8-9]和基于非对称密钥的认证协议[10-11]。通过分析可知，上述协议虽然存在一些不足，但采用有信任管理中心基于对称加密的身份认证机制是一个可取的办法。

使用 TTP 协助通信双方相互认证，为避免重放攻击，一般要求通信双方与 TTP 时钟保持同步，但在分布式云环境下，由于变化的和不可预见的网络时延的特性，很难做到较好的时钟同步。因此，需要避免时钟同步的缺陷。

当用户与 CSP 完成认证后，为了保证双方会话的安全性，协议应能快速更新会话密钥。为减少运行开销且更好地适用云环境公开通信的应用需求，更新会话密钥时不需要 TTP 的参与。

另外，在云计算环境下所设计的协议需要保证其在独立计算情况下是安全的，在网络环境下的运行也是安全的。基于逻辑的协议组合（PCL, protocol composition logic）[12]模型是形式化证明协议安全属性正确性的一种有效方法。目前，PCL 已经用于证明基于 Differ-Hellman 的密钥交换和签名的 STS 协议族[12]（如 IKEv2 协议等）、Needham-Schroeder 协议族[13]（如 Kerberos V5 协议[14]）以及 WLAN 安全标准[15]（如 IEEE802.11i 协议[16]和 4G 无线安全接入方案[17]）等。

根据上述云计算身份认证和协议安全性的需求，本文提出的用户身份认证协议具有以下特点：1) 满足协议组合安全；2) 基于对称加密的相互认证；3) 可信第三方协助认证；4) 不依赖时钟同步；5) 支持快速密钥更新，更新时不涉及 TTP。

2　相关工作及 PCL 模型

2.1　相关工作

近年来，许多学者针对云环境下身份认证的问题做了大量工作。文献[8-9]基于对称密码体制，解决了用户认证问题，但该协议依赖时钟同步，如果 TTP 或票据服务器任何一个服务终止，用户将无法继续认证，且用户身份认证的计算开销和通信开销较大。文献[18]采用基于公钥的密码体制解决了用户与 CSP 之间的身份认证问题，但公钥证书的管理和维护会消耗巨大的计算资源。文献[19]面向云存储提出基于口令的三方认证密钥交换协议，解决了数据接收方和数据发送方的认证，但由于采用的混沌映射系统复杂性高，序列性质不易控制。文献[20-21]面向云计算数据存储提出了基于椭圆曲线的认证机制，与 RSA 方案相比，该机制有效降低了计算成本。文献[22-23]面向云计算提出了基于分层身份管理的认证思想，解决了证书管理问题。文献[24]面向云计算提出了基于身份的用户认证协议，虽然加强了用户的安全属性，但认证过程仍需指数运算。

上述文献不能完全满足前述云计算环境下身份认证协议的特点。因此，本文基于身份认证即服务的思想提出一种基于对称加密的、由可信第三方协助的、支持快速密钥更新的、可组合的身份认证协议（UCAP）。该协议包含初始认证和重认证这 2 个阶段。初始认证阶段：TTP 分发相互认证实体的根会话密钥；重认证阶段：不需要 TTP 的参与，快

速生成子会话密钥。本文给出了 UCAP 的系统模型和方案描述，在 PCL 模型下描述了协议 Cord 演算、前提条件、不变量，并使用顺序组合证明方法证明了协议的认证性和机密性。最后与其他文献方案进行比较，结果显示：与文献[17,19]相比，UCAP 不依赖同步时钟；与文献[17,19,21,24]相比，UCAP 具有较高的计算效率、通信效率，且能快速生成子会话密钥。

2.2 PCL 系统

PCL 是一种支持协议属性证明的 Floyd-Hoare 类型的逻辑推导模型，它由 Cord 演算、协议逻辑（包括语法和语义逻辑）、证明系统组成[12,14]。

协议组合逻辑是逻辑地证明网络协议的安全属性，使用 Cord 来描述协议行为。PCL 提供了组合证明方法（compositional proof method）和抽象改进方法（abstraction and refinement methodology）这 2 类可组合安全证明方法[12]。本文使用的术语、行为和串等相关语法、PCL 逻辑语法、协议动作公理可参考文献[12]。

2.3 PCL 组合证明方法

安全证明包含个体行为，保证属性的局部论证和忠实的遵循协议诚实主体的全局论证。多数协议证明使用式 $\theta[P]_X\phi$，它表示从状态 θ 为真的状态开始，在线程 X 执行 P 动作之后，ϕ 也为真。协议组合逻辑 PCL 采用标准逻辑概念，提出认证属性是协议动作之间的时间匹配关系，只推理诚实主体的动作即可证明攻击下协议的安全性，并通过逻辑公理和模块化推理方法支持复杂安全协议的组合推理，可以用来证明安全协议的认证性和机密性等安全属性。顺序组合证明方法的主要思想是：首先分析子协议的安全性，并将前一步的证明分解为 2 个部分，一部分使用诚信准则（honest rule）证明协议的不变量，另一部分不使用 honest rule，将不变量作为假设证明协议；接着在更弱的前提下，协议的安全属性应该能够得到保证；然后应用顺序规则，将二者进行顺序组合；最后证明组合后的不变量对 2 个子协议都成立。由此可以得出，子协议的安全性在顺序组合下得到保证。

3 系统模型及安全目标

3.1 系统模型

本文方案的协议模型如图 1 所示，模型主要由用户、云服务提供商和可信第三方组成。

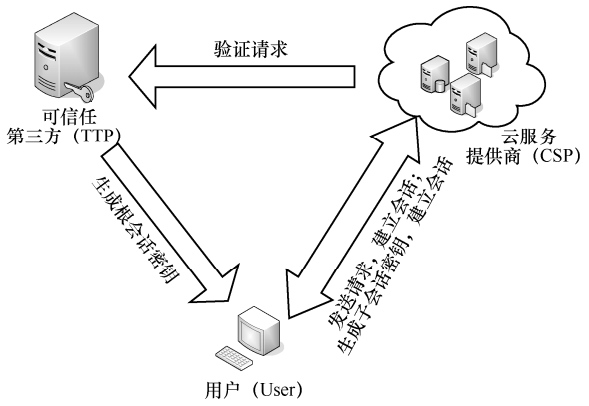

图 1 本文方案的协议模型

1) 用户（User）：用户需要与云服务提供商进行数据交换或需要云服务提供商提供服务，可能是一个用户或一个企业。在获取会话密钥后，经过安全传输，用户可以访问服务提供商提供的相关服务。

2) 云服务提供商（CSP）：CSP 负责提供云解决方案，在与用户协商会话密钥后，与用户建立会话，并提供相关服务。

3) 可信第三方（TTP）：TTP 是一个可信实体，它总是行为诚实的，并将得到用户和云服务提供商的信任，即它按照协议规范做出反应，而不会参与任何破坏其他主体安全的活动，在 TTP 的帮助下，用户和云服务提供商这 2 个主体之间即便完全不认识，也可以实现相互认证和安全传输。TTP 主要负责生成参与主体的会话密钥。

本文引入的 TTP 从密码学协议设计角度上看，是逻辑存在的，在现实部署中，TTP 可以租用，也可以由 CSP 自身维护，本文所指 TTP 在其他文献中可能称为 PKG（private key generator）、KGC（key generate center）或 KDC（key distribution center）。

3.2 敌手模型

1) TTP 是可信的，并且不会泄露密钥，也不会泄露与其他用户间的共享长期密钥。

2) 信道被敌手控制，整个网络通信环境是不可信的，敌手可以对数据流进行修改或伪造。

3) 假设敌手不能攻破底层的密码算法而获取相关密钥。

4) 假设敌手不能攻陷 TTP。

3.3 安全目标

总体来说，本文有以下安全目标：1) 确保长期共享密钥和会话密钥的机密性和认证性；2) 确保会话密钥的机密性；3) 确保会话密钥的时限性。

用户、CSP 预先与 TTP 安装了长期共享密钥，

在初始认证阶段有以下安全目标。

1) 用户、CSP 与 TTP 进行身份认证以确保其认证性。

2) TTP 生成并分发根会话密钥，会话密钥具有机密性，即会话密钥除 TTP 外仅由用户、CSP 共享。

3) 会话密钥具有机密性。

在重认证阶段有以下安全目标。

1) 用户与 CSP 进行相互认证以确保认证性。

2) CSP 验证确保密钥时限性。

3) 用户与 CSP 更新子会话密钥。

4) 确保更新后的会话密钥具有机密性。

4　方案描述

UCAP 涉及 3 个主体：用户、CSP、TTP，分别用 A、B、S 来表示，其中，S 分别和 A、B 共享长期会话密钥 E_{A_S}、E_{B_S}。在云计算环境中，A 与 B 进行安全传输时，必须要通过 B 的许可才可以进行下一个动作，在本协议模型中，A 和 B 为参与者，他们与 S 分别共享长期密钥 K_{A_S}、K_{B_S}，并约定一种对称加密机制，$E_K(\cdot)$表示使用密钥 K 执行对称加密操作。这时，需要参与云计算的每一方在 S 注册并与 S 共享长期会话密钥。

本协议可分为 2 个阶段，初始认证阶段（密钥生成、认证阶段）和重认证阶段。具体描述如下。

4.1　初始认证阶段

假设 A 和 B 与 S 的长期共享密钥由 S 进行管理，并且使用统一的对称加密算法，例如 AES 或 DES 等。

1) A 将自己的标识和加密信息发送给预期接收的对象 B，此时的加密信息是将用户产生的随机数 R_A 以及 A 和 B 的标识用 A 与 S 的长期共享密钥 E_{A_S} 进行加密。

$$A \to B:\{ID_A \| E_{A\_S}\{R_A \| ID_A \| ID_B\}\} \tag{1}$$

2) B 把从 A 接收到的加密信息连同自己产生的时间戳 T_B、A 的标识、会话密钥有效期限 EXP 和 S 共享的长期共享密钥进行加密，再将加密结果和 B 的标识、A 的标识以及 B 产生的随机数一起发送给可信第三方机构 S。

$$B \to S:\{ID_B \| ID_A \| E_{B\_S}\{E_{A\_S}\{R_A \| ID_A \| ID_B\} \| T_B \| EXP\} \| R_B\} \tag{2}$$

3) S 在接收到来自 B 的消息后解密，然后生成 2 个消息并保留 B 产生的随机数 R_B，第一个消息由 B 的标识、A 与 B 间的会话密钥 K、A 的随机数 R_A、B 的时间戳 T_B 以及会话密钥有效期限 EXP 组成，用 S 和 A 的长期共享密钥（E_{A_S}）对所有第一个消息进行加密；第二个消息由 A 的标识、A 与 B 间的会话密钥 K、B 的时间戳 T_B 以及会话密钥有效期 EXP 组成，用 S 和 B 的长期共享密钥对所有第二个消息进行加密，然后将这 2 个消息连同 B 的随机数一起发送给 A。

$$S \to A:\{E_{A\_S}\{K \| ID_B \| R_A \| T_B \| EXP\} \| E_{B\_S}\{K \| ID_A \| T_B \| EXP\} \| R_B\} \tag{3}$$

4) A 解密第一个消息，提取 A 与 B 间的会话密钥 K，并确认 R_A 的值是否与 1)中的值一样。A 发送 2 个消息给 B，第一个消息是从 S 接收到的用 E_{B_S} 加密的消息，第二个消息是用 A 与 B 间的会话密钥 K 加密的 B 的随机数 R_B。

$$A \to B:\{E_{B\_S}\{K \| ID_B \| T_B \| EXP\} \| E_K\{R_B\}\} \tag{4}$$

5) 随后，B 用它的密钥解密消息，提取 A 与 B 间的会话密钥 K、密钥有效期 EXP，并确认 R_B 的值是否与 2)中的值一致。

如果时间戳和随机数都匹配，A 和 B 就会相信对方的身份，并共享一个会话密钥 K。协议中的时间戳仅相对于 B 的时间，所以不需要同步时钟，B 只需要检查自己产生的时间戳即可。

4.2　重认证阶段

4.1 节中的 4)产生的第一个消息“$\{E_{B\_S}\{K \| ID_A \| T_B \| EXP\}\}$”可以视为一个“票据密钥”，在 EXP 确定的时间内，用户 A 能够用从 S 接收到的第一个消息与云服务提供商 B 进行重认证。

假设 A 和 B 完成了上述的协议，然后终止连接，如需重认证则不必依赖 S，且能够在 3 步之内重认证。

1) A 将 S 在 4.1 节的 3)中发给它的“票据密钥”和一个新的随机数与 A 的标识发送给云服务提供商 B。

$$A \to B:\{ID_A \| R'_A \| E_{B\_S}\{ID_A \| K \| T_B \| EXP\}\} \tag{5}$$

2) B 接收到信息后，解密信息，提取 A 与 B 间的会话密钥 K，首先核对 ID_A 是否一致，然后生成新的会话密钥 K'（$K' = Has(R'_B \| K \| R'_A)$）并生成一个新的随机数。这时，$B$ 将它的身份标识、新的随机数以及用新生成的会话密钥加密的消息一同发送给 A。

$$B \to A:\{ID_B \| R'_B \| E_{K'}\{R'_A \| ID_A \| \mathrm{ID_B} \| R'_B\}\} \quad (6)$$

3) A 接收到信息后，核对 ID_B 是否一致，用新产生的会话密钥 K'（$K' = Has(R'_B \| K \| R'_A)$）加密云服务提供商的新随机数、双方身份标识，并把它发给 B。

$$A \to B:\{E_{K'}\{R'_B \| ID_A \| ID_B \| R'_A\}\} \quad (7)$$

重认证过程可以多次重复，直到 EXP 过期为止，另外，新的随机数也防止了重放攻击。

5 基于 PCL 的协议安全性分析

5.1 UCAP 形式化描述

为了描述 UCAP，约定在 UCAP 对称密钥系统下的 $K = \bar{K}$。$\{m\}_{\bar{K}}$ 表示对消息 m 的解密，$\Diamond\phi$ 表示在过去的某一状态下 ϕ 成立，$\ominus\phi$ 表示在之前的状态下 ϕ 成立。

分别以 A、B、S 角色执行动作 Cord 的描述，如表 1 所示。

5.2 前提条件、安全属性和不变量

5.2.1 前提条件

UCAP 方案包括 A、B、S 这 3 个主体，且 A、B 与 S 分别有共享会话密钥 B_S 和 A_S，UCAP 的 2 个阶段的前提条件如表 2 所示。

5.2.2 安全属性

UCAP 中 S 用来分配 A 与 B 间的会话密钥 K 及会话票据，其安全属性包括认证性和机密性。UCAP 的 2 个阶段的安全属性如表 3 所示。

5.2.3 不变量

在 UCAP 中，利用 PCL 中的诚实准则，基于 A、B、S 角色的协议动作顺序以及 A 与 B 的会话密钥 K 的不变量描述如表 4 所示。

表 1 **A、B、S 角色执行动作 Cord 的描述**

第一阶段：初始认证阶段	第二阶段：重认证阶段
$UCAP_{1A} = [< (vR_A)\hat{A},\hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S} > (\hat{S},\ \hat{A},\{z,w,R_B\})$ $(z/\{K,ID_B,R_A,T_B,EXP\}_{\overline{A\_S}}) < \hat{A},\hat{B},w,u(u/\{R_B\}_{\overline{K}}) >]_A$	$UCAP_{2A} = [< (vR'_A)\hat{A},\hat{B},ID_A,\{ID_A,K,T_B,EXP\}_{B\_S} >$ $(\hat{B},\hat{A},\{ID_B,R'_B,u'\})(u'/\{R'_A,ID_A,ID_B,R'_B\}_{\overline{K'}}),$ $< (\hat{A},\hat{B},\{R'_B,ID_A,ID_B,R'_A\}_{K'},(K'/Has(K,R'_A,R'_B)) >]_A$
$UCAP_{1B} = [(ID_A,x),< (vR_B)\hat{B},\hat{S},ID_B,ID_A\{x,T_B,ID_A,EXP\}_{B\_S},R_B >$ $(\hat{A},\hat{B},w,u)(w/\{K,ID_A,T_B,EXP\}_{\overline{B\_S}})(u/\{R_B\}_{\overline{K}})]_B$	$UCAP_{2B} = [(\hat{A},\hat{B},w)(vR'_B)(w/\{K,A,T_B,ID_AEXP\}_{\overline{K}}),$ $< (\hat{B},\hat{A},\{ID_B,R'_B,\{R'_A,ID_A,ID_B,R'_B\}_{K'}\}) >,$ $(\hat{A},\hat{B},\{u''\}(K'/Has(K',R'_A,R'_B))(u''/\{R'_B,ID_A,ID_B,R'_A\}_{\overline{K'}}))]_B$
$UCAP_{1S} = [(\hat{B},\hat{S},\{ID_B,y,R_B,EXP\})(x/\{R_A,ID_A,ID_B\}_{\overline{A\_S}})$ $(y/\{x,T_B\}_{\overline{B\_S}})(ID_B/\hat{B}) < (vK)\hat{S},\ \hat{A},\{z,w,R_B\} >]_S$	

表 2 **UCAP 的前提条件**

第一阶段 $UCAP_1$ 的前提条件	第二阶段 $UCAP_2$ 的前提条件
$\theta_{UCAP_1} = Has(A,A\_S) \wedge Has(B,B\_S) \wedge Has(S,A\_S) \wedge Has(S,B\_S)$	$\theta_{UCAP_2} = Has(A,B\_S) \wedge Has(B,B\_S) \wedge Has(B,K) \wedge Has(A,K)$

表 3 **UCAP 安全属性**

第一阶段 $UCAP_1$ 的安全属性	第二阶段 $UCAP_2$ 的安全属性
$\phi_{UCAP_{1\_auth}} = Honest(\hat{A}) \wedge Honest(\hat{B}) \wedge\ Honest(\hat{S}) \supset \exists B.ActionInOrder($ $Send(A,\{\hat{A},\hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S}\}),$ $Receive(B,\{\hat{A},\hat{B},A,\{R_A,ID_A,ID_B\}_{A\_S}\}),$ $Send(B,\{\hat{B},\hat{S},ID_B,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},ID_A,R_B),$ $Receive(S,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B),$ $Send(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S}\},R_B),$ $Receive(A,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_B,T_B,EXP\}_{B\_S}\},R_B),$ $Send(A,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\}),$ $Receive(B,\{\hat{A},\hat{B},\{\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\})$	$\phi_{UCAP_{2\_auth}} = Honest(\hat{A}) \wedge Honest(\hat{B})) \supset \exists B.ActionInOrder($ $Send(A,\{\hat{A},\hat{B},ID_A,R'_A,\{ID_A,K,T_B,EXP\}_{B\_S}\}),$ $Receive(B,\{\hat{A},\hat{B},ID_A,R'_A,\{ID_A,K,T_B,EXP\}_{B\_S}),$ $Send(B,\{\hat{B},\hat{A},ID_B,R'_B,\{R'_A,ID_A,ID_B,R'_B\}_{K'}\}),$ $Receive(A,\{\hat{B},\hat{A},ID_B,R'_B,\{R'_A,ID_A,ID_B,R'_B\}_{K'}\}),$ $Send(A,\{\hat{A},\hat{B},\{R'_B,ID_A,ID_B,R'_A\}_{K'}),$ $Receive(B,\{\hat{A},\hat{B},\{R'_B,ID_A,ID_B,R'_A\}_{K'})$
$\phi_{UCAP_{1\_sec}} = Honest(\hat{A}) \wedge\ Honest(\hat{B}) \wedge Honest(\hat{S}) \supset$ $(Has(Z,K)) \wedge Z \neq \hat{S} \supset\ (Z = \hat{A} \vee Z =\ \hat{B}) \wedge Has(\hat{A},K) \wedge\ Has(\hat{B},K)$	$\phi_{UCAP_{2\_sec}} = Honest(\hat{A}) \wedge Honest(\hat{B}) \supset (Has(Z,K)) \supset$ $(Z = \hat{A} \vee Z =\ \hat{B}) \wedge Has(\hat{A},K') \wedge\ Has(\hat{B},K')$

表 4　　**UCAP 的不变量**

第一阶段 $UCAP_1$ 的不变量	第二阶段 $UCAP_2$ 的不变量
$\Gamma_{UCAP,1} == Honest(\hat{A}) \supset ((\Diamond Send(A,x_0) \wedge Contains(x_0,\{R_A,ID_A,ID_B\}_{A\_S}) \wedge \neg\neg\Diamond Fresh(\hat{A},R_A)) \supset ((x_0=\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S}\}, \{R_B\}_K,\{R_A,ID_A,ID_B\}_{A\_S}) \wedge After(\mathrm{Re}ceive(A,\{\hat{S},\hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S}, \{K,ID_A,T_B,EXP\}_{B\_S}\},R_B)), Send(A,\{\hat{A},\hat{B},\{K,ID_B,T_B,EXP\}_{B\_S}\},\{R_B\}_K))$	$\Gamma_{UCAP,5} == Honest(\hat{A}) \supset ((\Diamond Send(A,x'_0) \wedge Contains(x_0,\{ID_A,K,T_B,EXP\}_{B\_S}) \wedge \neg\Diamond Fresh(A,R'_A)) \supset ((x_0=\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S}\} \wedge After(Receive(A,\{\hat{B},\ \hat{A},R'_A\{K,\ \hat{A},T_B,EXP\}_{B\_S}\})), Send(A,\{\hat{A},\hat{B},\{R'_B,ID_A,ID_B,R'_A\}_{K'}))$
$\Gamma_{UCAP,2} = Honest(\hat{B})(\exists B \Diamond Send(B,y_0) \wedge Contains(y_0,\{\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S})) \supset ((y_0=\{\hat{A},\hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S},\{\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B) \wedge\Diamond Fresh(B,R_B) \wedge \Diamond Fresh(B,T_B) \wedge After(Receive(B,\{\hat{A},\hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S}\})), Send(B,\{\hat{B},\hat{S},ID_B,ID_A,\{\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B\}))$	$\Gamma_{UCAP,6} = Honest(\hat{B})(\exists B \Diamond Send(B,y_0) \wedge Contains(y_0,\{R'_A,ID_A,ID_B,R'_B\}_{K'})) \supset ((y_0=\{R'_A,ID_A,ID_B,R'_B\}_{K'}) \wedge \Diamond Fresh(B,R'_B) \wedge After(Receive(B,\{\hat{A},\hat{B},\{ID_A,K,T_B,EXP\}_{B\_S}\})), Send(B,\{\hat{B},\hat{A},\{\{R'_B,ID_A,ID_B,R'_A\}_{K'}\}))$
$\Gamma_{UCAP,3} = Honest(\hat{S})(\Diamond Send(S,z_0) \wedge Contains(z_0,\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S})) \wedge \ominus Fresh(S,K) \supset ((z_0=\{\hat{B},\hat{S},ID_B,\{\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B\}, \{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\} \wedge After(Receive(S,\{\hat{B},\hat{S},ID_B,ID_A,\{\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B\})), Send(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}))$	$\Gamma_{UCAP,7} = (Has(X',K) \supset \neg((Send(X',m) \wedge Contains(m,K')) \wedge Has(\hat{A},K') \wedge Has(\hat{B},K'))$
$\Gamma_{UCAP,4} = (Has(X,K) \supset \neg((Send(X,m) \wedge Contains(m,K)) \wedge Has(\hat{A},K) \wedge Has(\hat{B},K) \wedge Has(\hat{S},A\_S) \wedge Has(\hat{S},B\_S))$	$\Gamma_{UCAP_2} = \Gamma_{UCAP,5} \wedge \Gamma_{UCAP,6} \wedge \Gamma_{UCAP,7}$
$\Gamma_{UCAP_1} = \Gamma_{UCAP,1} \wedge \Gamma_{UCAP,2} \wedge \Gamma_{UCAP,3} \wedge \Gamma_{UCAP,4}$	

5.3　安全性证明

在 UCAP 第一阶段、第二阶段中，根据 *A*、*B*、*S* 的 Cord 演算、前提条件、不变量，分别基于 *A*、*B*、*S* 的角色进行安全性证明，由于篇幅限制，本节只给出基于角色 *A* 的证明过程，详细证明过程参见附录 I 和附录 II，基于 *B*、*S* 角色的证明过程类似于角色 *A* 的证明过程。

定理 1　若 θ_{UCAP_1} 为真，如果在基于 *A*、*B*、*S* 角色的执行 $UCAP_{1A}$、$UCAP_{1B}$、$UCAP_{1S}$ 后公式 $\phi_{RNS_{1.\mathrm{auth}}}$ 为真，则 UCAP 具有认证性，即 $UCAP_1 \vdash \theta_{UCAP_1}\left[UCAP_{1A}\right]_A \phi_{UCAP_{1.\mathrm{auth}}}$。

定理 2　若 θ_{UCAP_1} 为真，如果在基于 *A*、*B*、*S* 角色的执行 $UCAP_{1A}$、$UCAP_{1B}$、$UCAP_{1S}$ 后公式 $\phi_{UCAP_{1.\mathrm{sec}}}$ 为真，则 UCAP 具有机密性，即 $UCAP_1 \vdash \theta_{UCAP_1}\left[UCAP_{1A}\right]_A \phi_{UCAP_{1.\mathrm{sec}}}$。

定理 1 和定理 2 得证，因此协议 $UCAP_1$ 具有机密性和认证性，即式 $UCAP_1 \vdash \theta_{UCAP_1}\left[UCAP_1\right] \cdot \phi_{UCAP_{1.\mathrm{auth}}} \wedge \phi_{UCAP_{1.\mathrm{sec}}}$ 成立。

由于篇幅限制，定理 1 和定理 2 的证明过程见附录 I 和附录 II。

定理 3　若 θ_{UCAP_2} 为真，如果在基于 *A*、*B* 角色执行 $UCAP_{2A}$、$UCAP_{2B}$ 后公式 $\phi_{UCAP_{2.\mathrm{auth}}}$ 为真，则 UCAP 具有认证性，即 $UCAP_2 \vdash \theta_{UCAP_2}\left[UCAP_{2A}\right]_A \cdot \phi_{UCAP_{2.\mathrm{auth}}}$。

定理 4　若 θ_{UCAP_2} 为真，如果在基于 *A*、*B* 角色执行 $UCAP_{2A}$、$UCAP_{2B}$ 后公式 $\phi_{RNS_{2.\mathrm{sec}}}$ 为真，则 UCAP 具有认证性，即 $UCAP_2 \vdash \theta_{UCAP_2}\left[UCAP_{2A}\right]_A \phi_{UCAP_{2.\mathrm{sec}}}$。

定理 3 和定理 4 得证，因此协议 $UCAP_2$ 具有机密性和认证性，即式 $UCAP_2 \vdash \theta_{UCAP_2}\left[UCAP_{2A}\right]_A \cdot \phi_{UCAP_{2.\mathrm{auth}}} \wedge \phi_{UCAP_{2.\mathrm{sec}}}$ 成立。

定理 3 和定理 4 的证明过程与定理 1 和定理 2 的证明过程类似。

5.4　组合安全性

UCAP 由 $UCAP_1$ 和 $UCAP_2$ 的协议顺序组合而成，UCAP 的证明使用 PCL 中顺序组合的安全性证明方法。

定理 5 根据云用户的进程，通过组合 $UCAP_1$ 和 $UCAP_2$，UCAP 可以保证 A 和 B 之间共享密钥的安全性，即 $UCAP \vdash \theta_{UCAP}[UCAP_1, UCAP_2]_A \cdot \phi_{UCAP_1} \wedge \phi_{UCAP_2}$，其中，$\phi_{UCAP_1} = \phi_{UCAP_{1.auth}} \wedge \phi_{UCAP_{1.sec}}$，$\phi_{UCAP_2} = \phi_{UCAP_{2.auth}} \wedge \phi_{UCAP_{2.sec}}$。

证明 协议顺序组合的安全性证明如下。

1) 由 $UCAP_1$ 和 $UCAP_2$ 安全性证明可得，$UCAP_1$ 和 $UCAP_2$ 可以满足安全需求，即 $UCAP_1 \vdash \Gamma_{UCAP_1}$，$\Gamma_{UCAP_1} \vdash \varphi_{UCAP_1}$，$\varphi_{UCAP_1} = [UCAP_{1A}]_A \phi_{UCAP_1}$；$UCAP_2 \vdash \Gamma_{UCAP_2}$，$\Gamma_{UCAP_2} \vdash \varphi_{UCAP_2}$，$\varphi_{UCAP_2} = [UCAP_{2A}]_A \phi_{UCAP_2}$。

2) 在更弱的前提假设 $\Gamma_{UCAP_1} \cup \Gamma_{UCAP_2}$ 下，协议的安全属性依然可以保证，即 $\Gamma_{UCAP_1} \cup \Gamma_{UCAP_2} \vdash \varphi_{UCAP_1}$，$\Gamma_{UCAP_1} \cup \Gamma_{UCAP_2} \vdash \varphi_{UCAP_2}$。

3) 由于 φ_{UCAP_2} 的后置条件（post-condition）满足 φ_{UCAP_1} 的前提条件（pre-condition），即 $\varphi_{UCAP_2} \supset \varphi_{UCAP_1}$，因此应用顺序规则 S_1，而这可以顺序组合。假设 φ_{UCAP_2} 和 φ'_{UCAP_1} 分别为 $[UCAP_{2A}]_A \psi$ 和 $\psi[UCAP_{1A}]_A \varphi_{UCAP_1} \wedge \varphi_{UCAP_2}$，其中，$\psi = \varphi_{UCAP_2}$，可以得到 $\Gamma'_{UCAP_1} = \Gamma_{UCAP_2}$，$\Gamma_{UCAP_1} \cup \Gamma_{UCAP_2} \vdash [UCAP_{1A}, UCAP_{2A}]_A \varphi_{UCAP_1}$。

4) 不变量 $\Gamma_{UCAP_1} \cup \Gamma_{UCAP_2}$ 对于 $UCAP_1$ 和 $UCAP_2$ 均成立，即 $UCAP_1 \vdash \Gamma_{UCAP_1} \cup \Gamma_{UCAP_2}$，$UCAP_2 \vdash \Gamma_{UCAP_1} \cup \Gamma_{UCAP_2}$，可得 $UCAP \vdash \Gamma_{UCAP_1} \cup \Gamma_{UCAP_2}$。

由上述步骤可得，$UCAP_1$ 和 $UCAP_2$ 的安全性在顺序组合后仍然可以得到保证，即 $UCAP \vdash [UCAP_{1A}, UCAP_{2A}]_A \varphi_{UCAP_1} \wedge \varphi_{UCAP_2}$。

证毕。

其他参与方的证明过程与 A 的证明过程类似，通过证明可以得出，UCAP 方案在第一阶段和第二阶段具有相应的安全属性，顺序组成形成 UCAP 整体方案时也具有相应的安全属性。接下来，通过定性与定量相结合的方法来对相关协议进行比较。

6 相关协议比较

为了有效地说明新协议 UCAP 的性能优势，从理论和实验这 2 个层面对上述协议参与方进行了对比分析，分别如表 5~表 7 和图 2 所示。为统一比较，将文献中所提协议进行命名，其中，文献[8]记为 Kerberos，文献[19]记为 3PAKE，文献[21]记为 EPP，文献[24]记为 IDP。

表 5 从协议功能上对本文所提 UCAP 与其他相关协议进行了总结，具体符号含义如下。

F_1：TTP 参与。

F_2：依赖时钟同步。

F_3：快速生成会话密钥，更新时不涉及 TTP。

F_4：基于对称的认证机制。

F_5：相互认证。

F_6：密钥建立。

F_7：已知会话密钥安全性。

F_8：抵抗重放攻击。

表 5 协议功能及安全性比较

协议	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
3PAKE	Y	Y	N	N	Y	N	Y	Y
EPP	Y	N	N	N	Y	N	Y	Y
IDP	Y	N	N	N	Y	N	N	Y
Kerberos	Y	Y	N	Y	Y	Y	N	Y
UCAP	Y	N	Y	Y	Y	Y	Y	Y

表 6 从协议性能上对本文所提 UCAP 与其他相关协议进行了总结，其中，C 为混沌映射操作、H 为 Hash 操作、E/D 为对称加/解密操作、Ep/Dp 为公钥加/解密操作、Ec 为椭圆曲线密钥交换算法、G 为概率生成操作、R 为确定性复制操作、M 为模运算，IC 为初始认证、RC 为重认证，CN 为通信轮次。

表 6 协议性能比较

协议	用户		CSP		TTP		总计		CN	
	IC	RC	IC	RC	IC	RC	IC	RC	IC	RC
Kerberos	3D+3E	3D+3E	2E	2E	3D+3E	3D+3E	6D+8E	6D+8E	6	6
3PAKE	4C+2H	4C+2H	4C+2H	4C+2H	5C	5C	13C+4H	13C+4H	5	5
EPP	Ec+3H+Kp+Dp	Ec+3H+Kp+Dp	Ec+3H+Kp+Dp	Ec+3H+Kp+Dp	2Ec+6H+2Kp+2Dp	2Ec+6H+2Kp+2Dp	4Ec+12H+4Kp+4Dp	4Ec+12H+4Kp+4Dp	5	5
IDP	12H+2M+1G+1R+2E+D	12H+2M+1G+1R+2E+D	8H+D+E	8H+D+E	6H+M+G+R	6H+M+G+R	26H+3M+2G+2R+3E+2D	26H+3M+2G+2R+3E+2D	7	7
UCAP	D+2E	E	2D+E	2D+E+H	2D+2E	—	5D+5E	2D+2E+H	4	3

表 7 从协议计算时延上将 UCAP 和其他相关协议进行了对比。实验时，在单机上测试协议计算、认证时延，而不考虑发送消息时的传输时延。本机硬件环境为：CPU 为 i5，内存为 4 GB；软件环境为：系统为 Windows7；测试语言为 C++。

表 7　协议计算时延对比（单位为 ms）

协议	用户	CSP	TTP	总计
Kerberos	366	188	366	920
3PAKE	236	236	190	662
EPP	696	696	1 392	2 784
IDP	792	458	324	1 574
UCAP	155	171	122	448

图 2 在不同 CPU 主频下对 Kerberos、3PAKE、UCAP 的认证时延进行了比较。

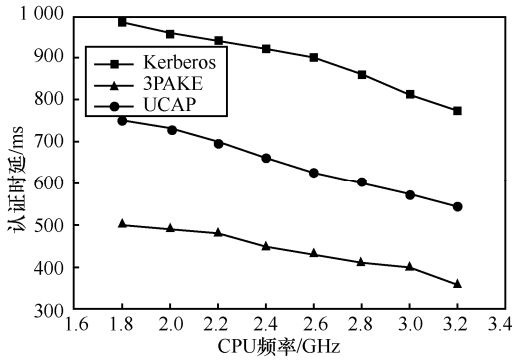

图 2　不同 CPU 主频下的认证时延

从表 5~表 7 和图 2 可以看出，与当前主流的用户认证协议相比，在完成相同任务的情况下，新协议 UCAP 的应用场景、通信效率和计算效率具有优势，具体分析如下。

1) 应用场景

如表 5 所示，所比较协议均需要 TTP 参与，3PAKE 和 Kerberos 协议需要和 TTP 同步时钟。在快速生成会话密钥时不需要 TTP 参与，只有 UCAP 可以实现，符合云环境下公开通信的应用要求。

2) 通信效率

如表 6 所示，在 IC 阶段的通信轮次上，UCAP 最少，3PAKE、EPP、Kerberos 协议居中，IDP 最高。从总体上看计算开销，UCAP 最低，Kerberos 协议次之，EPP 和 IDP 较高。从用户角度看，UCAP 计算开销最低，Kerberos 协议次之，IDP 最高。从 TTP 角度看，UCAP 与 3PAKE 协议计算开销相当，TTP 最高。从 CSP 角度看，Kerberos 协议计算开销最低，UCAP 次之。从用户、CSP、TTP 这 3 个角色看，根据云计算的特点，CSP 应承载更多的计算开销，用户次之，TTP 最少。除 IDP、Kerberos 协议外，其余协议均能满足上述特点。在 RC 阶段，除 UCAP 外，其余协议均需要 TTP 参与来完成密钥更新。UCAP 在密钥更新过程中，仅需 3 轮通信即可完成密钥更新，在通信效率上，与其他协议相比也具有较为明显的优势。

3) 计算效率

如表 7 所示，新协议的计算负载要明显低于其他协议，UCAP 较 Kerberos 协议在用户、CSP、TTP 端的计算时延分别下降了 57.65%、9.04%和 66.67%，较 3PAKE 协议在用户、CSP、TTP 端的计算时延分别下降了 34.32%、27.54%、35.79%。新协议 UCAP 各参与方的整体计算时延较 Kerberos、3PAKE、EPP、IDP 协议降低了 51.41%、32.48%、83.94%、71.60%。由于协议 EPP、IDP 的计算时延较长，图 2 仅对 Kerberos、3PAKE、UCAP 各参与方的整体认证时延进行了比较。从图 2 可以看出，随着 CPU 主频的提高，3 个协议的认证时延整体下降，但新协议 UCAP 具有更低的认证时延。因此，基于对称密钥算法在实现通信双方相互认证的基础上，提高了认证双方的计算效率。

4) 安全性分析

① 在相互认证方面，UCAP、3PAKE、Kerberos、IDP、EPP 均能实现相互认证，从 4.2 节的式(5)~式(7)中可以发现，在重认证阶段，UCAP 也可实现相互认证。② 在密钥建立方面，UCAP 在初始认证阶段，A 和 B 与 S 共享长期密钥，A 和 B 可分别获取根会话密钥；在重认证阶段，A 和 B 可通过 $K' = Has(R'_B \| K \| R'_A)$ 生成子会话密钥，因此协议 UCAP 支持密钥建立。③ 在已知会话密钥安全性方面，UCAP 在初始认证和重认证阶段都生成新的随机数，并各自提取或计算出会话密钥，敌手很难获取根会话密钥和子会话密钥。④ 在抵抗重放攻击方面，UCAP 在重认证阶段产生新的随机数，可以有效抵抗重放攻击。

综上所述，新协议 UCAP 在不失安全性的前提下，在应用场景、通信效率与计算效率方面性能优势明显。

7 结束语

在云计算环境中，安全问题是一项极具挑战的问题[25]。针对参与云计算用户认证的安全问题，本文在研究认证协议的基础上，面向云环境提出了一种安全的用户认证协议。该协议基于 TTP 分发根会话密钥、CSP 分发生成子会话密钥的思想，使用对称密钥算法将协议方案分为 2 个阶段，第一阶段通过 TTP 实现用户认证及根会话密钥的分发，第二阶段不涉及 TTP 实现用户认证及子会话密钥的生成，并且 2 个阶段均不依赖 TTP 同步时钟。在 PCL 模型下对 UCAP 进行协议组合证明，证明结果表明，所提协议在 PCL 模型下具有密钥机密性和会话认证性。最后通过相关协议比较的结果表明：UCAP 在不失安全性的前提下，降低了通信双方的计算开销，提高了通信效率，并且不依赖 TTP 同步时钟，子会话密钥的生成及用户重认证不需要 TTP 的参与，符合云环境下公开通信的需求。因此，在云计算环境中本文所提方案具有一定的应用价值。

附录 I

定理 1 证明过程如下。

AN_3,AA_2,AP_1

$$\theta_{UCAP_1}[UCAP_{1A}]_A \Diamond (Send(A,\{\hat{A},\hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S}\})) \wedge \ominus Fresh(A,R_A) \tag{8}$$

式(8), $\Gamma_{UCAP,2}$,AF_3

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{B}) \supset (Receive(B,\{\hat{A},\ \hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S}\})) \wedge After(Receive(B,\{\hat{A},\hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S}\}),\ (Send(B,\{\hat{B},\hat{S},ID_B,ID_A \{\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S}\},R_B)) \tag{9}$$

式(8), $\Gamma_{UCAP,3-4}$,AF3

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{S}) \supset (Receive(S,\{\hat{B},\hat{S},ID_B,ID_A,\{\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B\})),\wedge After(Receive(S,\{\hat{B},\hat{S},ID_B,ID_A,\{\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B\})), (Send(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\},R_B\})) \tag{10}$$

式(8),AA_1,P_1

$$\theta_{UCAP_1}[UCAP_{1A}]_A \Diamond (Receive\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}) \tag{11}$$

DEC,REC

$$\theta_{UCAP_1}[UCAP_{1A}]_A \Diamond (Receive\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}) \supset Has(A,K) \wedge Has(A,\{K,ID_A,R_A,T_B\}_{B\_S}) \tag{12}$$

式(9)~式(11),AF_1, ARP

$$\theta_{UCAP_1}[UCAP_{1A}]_A ActionInOrder(Send(A,\{\hat{A},\hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S}\})), Receive(B,\{\hat{A},\hat{B},ID_A,\{R_A,ID_A,ID_B\}_{A\_S}\}), Send(B,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B), Receive(S,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B), Send(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}), Receive(A,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}), Send(A,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\}), Receive(B,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\})) \tag{13}$$

式(9),式(10), 式(13),CP_3

$$Receive(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}) \supset \exists S\ \exists z_0 Send(S,z_0) \wedge Contains(z_0,\{B,\{\hat{B},\hat{S},ID_B,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S}\},R_B) \wedge After(Send(S,z_0),Receive(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\})) \tag{14}$$

式(14),PROJ,DEC, CP_3

$$Receive(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}) \supset Has(S,A\_S) \wedge Has(S,B\_S) \tag{15}$$

$$Computes(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}) \supset Has(S,A\_S) \wedge Has(S,B\_S) \tag{16}$$

Γ_{UCAP}

$$Honest(B) \wedge Honest(S) \supset B \neq \hat{S} \tag{17}$$

式(12)~式(16)

$$Honest(B) \wedge Honest(S) \supset \exists B \exists y_0.Send(B,y_0) \wedge Contains(y_0,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S}) \wedge Computes(B,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S}) \wedge B=\hat{B} \quad (18)$$

式(13),式(18),$G_{1\text{-}3}$

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{B}) \supset \exists B.Fresh(B,R_B,T_B) \wedge Send(B,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B) \wedge After(Receive,(B,\{R_A,ID_A,ID_B\}_{A\_S})), (Send(B,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B)) \quad (19)$$

式(13),式(19),AF_2

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{B}) \wedge Honest(\hat{S}) \supset After (Send(B,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B)), (Receive(B,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B)) \quad (20)$$

式(8),式(9),AF_2

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{S}) \supset After (Send(S,\{\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\})), (Receive(A,\{\{K,ID_B,R_A,T_B,EXP\}_{A\_S}\},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\})) \quad (21)$$

$\Gamma_{UCAP,3}$

$$Honest(\hat{S}) \supset ActionInOrder(Receive(S,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B)), (Send(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,IDA,T_B,EXP\}_{B\_S}\},R_B)) \quad (22)$$

Γ_{UCAP}

$$Honest(\hat{A}) \wedge Honest(\hat{S}) \supset A \neq \hat{S} \quad (23)$$

式(18),式(23),CP_3

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{S}) \wedge Honest(\hat{B}) \supset Receive (S,\{\hat{B},\hat{S},ID_B,ID_A,\{R_A,ID_A,ID_B\}_{A\_S},T_B\}_{B\_S},R_B) \supset \exists X \exists x_0. Computes(X,\{R_A,ID_A,ID_B\}_{A\_S}) \wedge Send(X,x_0) \wedge Contains(x_0,\{R_A,ID_A,ID_B\}_{A\_S}) \supset Has(A,K) \supset (X=\hat{B} \vee X=\hat{S}) \quad (24)$$

式(24)

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{S}) \wedge Honest(\hat{B}) \supset \exists X \exists x_0.Computes(X,\{R_A,ID_A,ID_B\}_{A\_S}) \wedge Send(X,x_0) \wedge Contains(x_0,\{R_A,ID_A,ID_B\}_{A\_S}) \wedge After(Send(X,x_0), Receive(A,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\})) \quad (25)$$

式(25), $\Gamma_{UCAP,1}$

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{S}) \supset After (Send(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\})), (Receive(A,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\})) \quad (26)$$

AA_1,P_1

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{B}) \supset Receive(B,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\}) \quad (27)$$

式(26),式(27),CP_3

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{B}) \supset \exists X \exists x_0.Contains(X,x_0) \supset Receive(B,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\}) \quad (28)$$

DEC,PROJ, Γ_{UCAP}

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \supset Receive(A,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}) \supset Has(A,\{K,\hat{B},R_A,T_B\}_{A\_S}) \supset Has(A,K) \quad (29)$$

$$Computes(Y,\{R_B\}_K) \supset Has(Y,K) \supset (Y=\hat{A} \vee Y=\hat{S} \vee Y=\hat{B}) \quad (30)$$

Γ_{UCAP}

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{S}) \wedge Honest(\hat{B}) \supset Y \neq \hat{A} \wedge Y \neq \hat{S} \quad (31)$$

式(31), Γ_{UCAP}

$$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{S}) \wedge Honest(\hat{B}) \supset \exists B.After(Send(A,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\}), Receive(B,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\})) \quad (32)$$

式(13),式(19)~式(24),式(32)　$\theta_{UCAP_1}[UCAP_{1A}]_A Honest(\hat{A}) \wedge Honest(\hat{S}) \wedge Honest(\hat{B}) \supset \phi_{UCAP_1.\text{auth}}$　(33)

证毕。

根据式(33)可得，UCAP 具有认证性，即 $UCAP_1 \vdash \theta_{UCAP_1}\left[UCAP_{1A}\right]_A \phi_{UCAP_1.\text{auth}}$。定理 1 得证。

附录 II

定理 2 证明过程如下。

P_3　$Has Alone(S,\{B\_S, A\_S\}) \wedge Fresh(\hat{S},K)\theta_{UCAP_1}[UCAP_{1A}]_A$　(34)

$Has Alone(\hat{A},\{A\_S\})\theta_{UCAP_1}[UCAP_{1A}]_A \ \ HasAlone(\hat{A},\{A\_S\})$　(35)

$\Gamma_{UCAP,3}$, AF_2　$Honest(\hat{S}) \supset \Diamond Send(S,z_0) \wedge Contains(z_0,\{\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S}\})$　(36)

式(34)~式(36), AF_1, ARP　$HasAlone(\hat{S},\{B\_S,A\_S\}) \wedge \ Fresh(\hat{S},K)\theta_{UCAP}[RNSA]_A Honest(\hat{S})\exists S.ActionInOrder(Send(S,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}),Receive(A,\{\hat{S},\ \hat{A},\{K,ID_B,R_A,T_B,EXP\}_{A\_S},\{K,ID_A,T_B,EXP\}_{B\_S},R_B\}),Send(A,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\}),Receive(B,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\})$　(37)

$\Gamma_{UCAP,1}$　$Honest(\hat{A}) \wedge \Diamond Send(\{A,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\}\})\exists x_0.(x_0 = \{R_B\}_K) \wedge HasAlone(\hat{A},x_0)$　(38)

$\Gamma_{UCAP,2}$　$Honest(\hat{B}) \wedge Receive(\{B,\{\hat{A},\hat{B},\{K,ID_A,T_B,EXP\}_{B\_S},\{R_B\}_K\}\})\exists y_0.(y_0 = \{R_B\}_K) \wedge HasAlone(\hat{B},y_0)$　(39)

式(37)~式(39), Computes　$Computes(Z,K) \supset (Z = \hat{A} \vee Z = \hat{B})$　(40)

式(40)　$Honest(\hat{A}) \wedge Honest(\hat{B}) \supset \ Has(Z,K) \wedge Z \neq \hat{S} \supset (Z = \hat{A} \vee Z = \hat{B}) \wedge Has(\hat{A},K) \wedge Has(\hat{B},K)$　(41)

根据式(41)可得，UCAP 具有机密性，即 $UCAP_1 \vdash \theta_{UCAP_1}\left[UCAP_{1A}\right]_A \phi_{UCAP_1.\text{sec}}$。定理 2 得证。

证毕。

定理 3 和定理 4 的证明过程类似于定理 1 和定理 2。

参考文献：

[1] 林闯, 苏文博, 孟坤, 等. 云计算安全: 架构, 机制与模型评价[J]. 计算机学报, 2013, 36(9): 1765-1784.
LIN C, SU W B, MENG K, et al. Cloud computing security: architecture , mechanism and modeling[J]. Chinese Journal of Computers, 2013, 36(9): 1765-1784.

[2] KANDUKURI B R, RAKSHIT A. Cloud security issues[C]//IEEE International Conference on Services Computing. 2009: 517-520.

[3] XIAO Z, XIAO Y. Security and privacy in cloud computing[J]. IEEE Communications Surveys & Tutorials, 2013, 15(2): 843-859.

[4] BOYKO V, MACKENZIE P, PATEL S. Provably secure password-authenticated key exchange using Diffie-Hellman[C]// International Conference on the Theory and Applications of Cryptographic Techniques. 2000: 156-171.

[5] MACKENZIE P, PATEL S, SWAMINATHAN R. Password-authenticated key exchange based on RSA[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2000: 599-613.

[6] BERTINO E, PACI F, FERRINI R, et al. Privacy-preserving digital identity management for cloud computing[J]. Bulletin of the Technical Committee on Data Engineering, 2009, 32(1): 21-27.

[7] BRAINARD J, JUELES A, KALISKI B S, et al. A new two-server approach for authentication with short secret[C]//The 12th Conference USENIX Security. 2003: 201-214.

[8] KOHL J, NEUMAN C. The Kerberos network authentication service (v5)[R]. 1993.

[9] HOJABRI M. Innovation in cloud computing: implementation of Kerberos version5 in cloud computing in order to enhance the security issues[C]//2013 International Conference on Information Communica-

tion and Embedded Systems (ICICES). 2013: 452-456.

[10] ZISSIS D, LEKKAS D. Addressing cloud computing security issues[J]. Future Generation Computer Systems, 2012, 28(3): 583-592.

[11] BINU S, MISBAHUDDIN M, RAJ P. A mobile based remote user authentication scheme without verifier table for cloud based services[C]//The Third International Symposium on Women in Computing and Informatics. 2015: 502-509.

[12] DATTA A. Security analysis of network protocols: compositional reasoning and complexity-theoretic foundations[D]. Stanford University, 2005.

[13] ZHNG J, MA J F, YANG C. Protocol derivation system for the needham-schroeder family[J]. Security and Communication Networks, 2015, 8(16): 2687-2703.

[14] DATTA A, DEREK A, MITCHELL J C, et al. Protocol composition logic (PCL)[J]. Electronic Notes in Theoretical Computer Science, 2007, 172: 311-358.

[15] ZHANG H, CHEN L. An efficient authentication protocol of WLAN and its security proof[C]//The 2008 International Conference on Communications and Networking. 2008: 1133-1137.

[16] HE C, SUNDARARAJAN M, DATTA A, et al. A modular correctness proof of IEEE 802.11i and TLS[C]//The 12th ACM conference on Computer and communications security. 2005: 2-15.

[17] 王丽丽, 冯涛, 马建峰. 协议组合逻辑安全的 4G 无线网络接入认证方案[J]. 通信学报, 2012, 33(4): 77-84.
WANG L L, FENG T, MA J F. Secure access authentication scheme for 4G wireless network based on PCL[J]. Journal on Communications, 2012, 33(4): 77-84.

[18] URIEN P, MARIE E, KIENNERT C. An innovative solution for cloud computing authentication: grids of EAP-TLS smart cards[C]//2010 Fifth International Conference on Digital Telecommunications (ICDT). 2010: 22-27.

[19] LI C T, LEE C W, SHEN J J. A secure three-party authenticated keyexchange protocol based on extended chaotic maps in cloud storage service[C]//The 2015 International Conference on Information Networking (ICOIN). 2015: 31-36.

[20] ZISSIS D, LEKKAS D. Addressing cloud computing security issues[J]. Future Generation Computer Systems, 2012, 28(3): 583-592.

[21] YIN X C, LIU Z G, LEE H J. An efficient and secured data storage scheme in cloud computing using ECC-based PKI[C]//2014 16th International Conference on Advanced Communication Technology(ICACT). 2014: 523-527.

[22] YAN L, RONG C, ZHAO G. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography[C]//IEEE International Conference on Cloud Computing. 2009: 167-177.

[23] GOEL A, GUPTA G, BHUSHAN M, et al. Identity management in hybrid cloud[C]//2015 International Conference on Green Computing and Internet of Things (ICGCIoT). 2015: 1096-1100.

[24] YANG J H, LIN P Y. An ID-based user authentication scheme for cloud computing[C]// 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal (IIH-MSP). 2014: 98-101.

[25] QIAN L, LUO Z, DU Y, et al. Cloud computing: an overview[M]//Springer Berlin Heidelberg, 2009: 626-631.

[作者简介]

李学峰（1975−），男，安徽宿州人，青海广播电视大学副教授，“西部之光”访问学者（在西安电子科技大学访学），主要研究方向为密码学、协议设计与形式化分析等。

张俊伟（1982−），男，陕西西安人，博士，西安电子科技大学副教授，主要研究方向为密码学、网络安全等。

马建峰（1963−），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为信息安全、密码学与无线网络安全等。