通用可组合的网关口令认证密钥交换协议

胡学先[1),2),3)] 张启慧[1)] 张振峰[2)] 刘凤梅[3)]

[1)](中国人民解放军信息工程大学 郑州 450002)

[2)](中国科学院软件研究所可信计算与信息保障实验室 北京 100190)

[3)](信息保障技术重点实验室 北京 100072)

摘 要 网关口令认证密钥交换(GPAKE)协议是一类特殊的三方协议,其中客户和认证服务器共享有低熵口令,客户和网关在服务器的协助下生成高熵的会话密钥.由于通信架构更贴近实际,GPAKE 协议研究近年来受到了较多的关注.然而,已有 GPAKE 协议都是在传统"孤立"的安全模型中进行分析和设计的,没有考虑协议的可组合安全,也没有考虑用户将相关口令用于不同协议时的影响.为了保证 GPAKE 协议在更接近实际应用的复杂环境下的安全性,该文在通用可组合(UC)框架下研究 GPAKE 协议的安全性定义,给出了 GPAKE 的理想功能,对会话密钥安全、防止恶意网关猜测客户口令以及保持会话密钥相对于服务器的私密性等安全目标进行了刻画,保证了协议在复杂应用环境中的可组合安全性,还考虑了用户将服从任意分布的、甚至是与其他协议相关的口令用于 GPAKE 协议的情况.另外,利用 UC 安全两方 PAKE 协议、消息认证码为组件,给出了 GPAKE 协议的一个通用构造,使其能够被实例化得到多个具体的协议,并证明了该通用构造是 UC 安全的,即能够 UC 安全实现 GPAKE 理想功能.

关键词 可证明安全;通用可组合;口令认证;密钥交换;网关协议

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2017.01109

Universally Composable Gateway-Oriented Password-Authenticated Key Exchange Protocol

HU Xue-Xian[1),2),3)] ZHANG Qi-Hui[1)] ZHANG Zhen-Feng[2)] LIU Feng-Mei[3)]

[1)](*The PLA Information Engineering University*, *Zhengzhou* 450002)

[2)](*Trusted Computing and Information Assurance Laboratory*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100190)

[3)](*Science and Technology on Information Assurance Laboratory*, *Beijing* 100072)

Abstract Gateway-oriented password-authenticated key exchange (GPAKE) protocol is an important cryptographic primitive executed among a client, a gateway and an authentication server, where a password is only shared between the client and the server, but a session key which has high-entropy is exchanged between the client and the gateway. Because of their convenience in practice, GPAKE protocols have attracted much attention in recent years. However, almost all existing GPAKE protocols are analyzed only in 'stand-alone' security models, in which some basic security goals, such as protocol composability and security when related passwords are used by one user within different protocols, are not considered. To overcome these deficiencies, we consider the security definition of GPAKE in the well-known Universal Composability (UC) framework. We first formulate an ideal functionality within the UC framework for GPAKE protocols, which captures the requirements of semantic security of session keys, resistance to password-guessing attacks mounted by malicious gateway, key privacy with respect to the honest-but-curious server, as

收稿日期:2016-05-07;在线出版日期:2016-09-29.本课题得到国家"九七三"重点基础研究发展规划项目基金(2013CB338003,2012CB315905)、国家自然科学基金(61502527,U1536205,61379150,61572485)、中国博士后科学基金 (2014M552524)、信息保障技术重点实验室开放基金(KJ-14-004)资助.**胡学先**,男,1982 年生,博士,讲师,中国计算机学会(CCF)会员,主要研究方向为可证明安全协议和模型.E-mail:xuexian_hu@hotmail.com.**张启慧**,女,1983 年生,博士研究生,讲师,主要研究方向为信息安全.**张振峰**,男,1972 年生,博士,研究员,主要研究领域为公钥密码和基于格的密码学.**刘凤梅**,女,1974 年生,博士,研究员,主要研究领域为密码理论与应用.

well as protocol composable security. Moreover, since in the formulation of the GPAKE functionality we let the environment choose passwords for all parties, our definition captures the cases that related passwords are used by different parties, or by the same parties for different protocols, even when the passwords are selected from arbitrary probability distribution. In addition, by utilizing cryptographic primitives such as UC secure 2-party protocols and message authentication codes, we put forward a general construction of GPAKE protocol, which can be instantiated to several concrete protocols. We then prove the security of our construction rigorously in the UC framework, i. e., the construction can securely realize the GPAKE functionality.

Keywords provable security; universal composability framework; password authentication; key exchange; gateway-oriented protocol

1 引 言

口令认证密钥交换(Password Authenticated Key Exchange,PAKE)协议使得客户和服务器仅使用一个低熵口令作为初始凭证,便可通过公开信道安全地生成共享的高熵会话密钥.它避免了一般密钥交换协议要求网络中额外部署有公钥基础设施(Public Key Infrastructure,PKI)或要求客户拥有能安全保存高熵对称密钥的专用硬件设备等假设,因其方便实用的特性而受到了普遍关注.近年来,密码学者在 PAKE 协议安全分析和协议设计方面提出了诸多成果[1-7],国际标准组织还颁布了 ISO/IEC 11770-4,IEEE Std 1363.2,RFC5054,ISO/IEC 20009-4 等标准,极大地推动了 PAKE 协议的发展.

多数典型的 PAKE 协议主要考虑"客户-服务器"应用框架下的认证和密钥交换问题,将服务器看成是网络中的一个单独实体.而很多应用中,所谓的服务器并不是一个主机,而是分为前端接入网关和后端认证服务器两个相对独立的部分,其中网关是客户登录系统前的安全接入设备,但是客户仅与认证服务器共享有认证凭证.网关口令认证密钥交换(Gateway-oriented Password-Authenticated Key Exchange,GPAKE)协议是面向这种"客户-网关-服务器"通信架构的一类特殊的三方 PAKE 协议,其中每个客户都和认证服务器共享有唯一的低熵口令,网关和认证服务器之间有预先构建的认证信道,客户和网关在认证服务器的帮助下进行认证的密钥交换.相比于传统的"客户-服务器"模型,GPAKE 协议的通信模型更贴近实际,在很多现实系统中都具有较大的应用需求.

在 2005 年的亚密会上,Abdalla 等人[8]首次提出了 GPAKE 的概念,给出了 GPAKE 安全模型,并设计了一个可证明安全的 GPAKE 协议.随后,密码学者们对 GPAKE 的安全模型和协议设计、分析展开了一系列的研究.Byun 等人[9]2006 年指出 Abdalla 等人[8]所提出的 GPAKE 协议易于遭受不可察觉在线字典攻击(Undetectable On-line Dictionary Attack,UODA),意味着恶意网关能够不断重复地对客户口令实施在线猜测、验证,而服务器检测不到这些行为是恶意攻击.为了防止 UODA 攻击,Byun 等人[9]试图通过添加消息认证码来对原始协议进行改进.不过,Shim[10]在 2008 年发现 Byun 等人[9]所提出的改进协议的认证消息错误地包含了口令信息,使得攻击者可以对附加认证码的消息进行重放实施 UODA 攻击.同年,Abdalla 等人[11]提出了一个更强的安全模型,通过允许对测试会话的拥有方进行腐化(Corrupt)刻画了会话密钥的前向安全性,该模型还用一个攻击游戏同时涵盖了 GPAKE 所需要实现的多个安全目标.Yoon 和 Yoo[12]在 2010 年发现 Shim 提出的协议[10]实际上无法正确执行,存在设计方面的严重错误.作为改进,Yoon 等人提出了一个称为最优 GPAKE(简记为 O-GPAKE)的协议.随后,Wei 等人[13-14]在已有的 GPAKE 和三方 PAKE 安全模型的基础上,提出了更强的 GPAKE 安全模型,并进一步在他们的安全模型中分析了 O-GPAKE 协议的安全性不足[15].

然而,已有的 GPAKE 安全模型都是对传统"孤立"的 PAKE 安全模型(如 BPR[1]、ROR 模型[3])扩展得到的,仅仅孤立地考虑被分析 GAPKE 协议的安全性,而没有考虑协议在和其他相关协议并发运行时的安全性.如同 Canetti 等人[4,16-17]指出,这些传统"孤立"的 PAKE 安全模型存在如下不足:(1)没有考虑协议的可组合性:不能保证 GPAKE 协议和

其他相关协议并发运行、被用作一个系统子模块时的安全性；(2)没有考虑用户口令的相关性：没有考虑用户将相关口令用于不同协议时的影响，也不能刻画用户依据偏好分布选取口令时的安全性.

为了保证 GPAKE 协议在更接近实际应用的复杂环境下的可组合安全性，本文中我们利用通用可组合(Universal Composability，UC)框架对 GPAKE 协议的安全定义和协议设计进行研究. 首先，针对 GPAKE 协议的会话密钥语义安全、防止恶意网关猜测客户口令以及保持会话密钥相对于服务器的私密性等安全目标，在 UC 框架下构造了 GPAKE 的理想功能，形式化地定义了 GPAKE 的安全性，保证了 GPAKE 在复杂应用环境中的可组合性；另外，利用 UC 安全两方 PAKE 协议、消息认证码为组件，给出了 GPAKE 协议的一个通用构造，并证明了该构造是 UC 安全的，即能够 UC 安全地实现所提出的 GPAKE 理想功能.

2　GPAKE 协议安全定义

2.1　通用可组合框架简介

为了克服传统可证明安全理论中没有考虑协议组合安全的不足，IBM 公司的密码学家 Canetti 在 2001 年创造性地提出了通用可组合(Universal Composability，UC)安全框架[18]，利用统一的分析框架解决密码学任务的组合执行问题. 随后，该安全框架被广泛地用于两方和多方计算[19]、承诺方案[20]、签名方案[21]、不经意传输[22]、密钥交换协议[23]、可信网络连接协议[24]、安全定位协议[25]、群组通信机制[26]等密码体制的安全分析和设计中，为安全协议提供了更强的安全性保障.

UC 框架涉及到两种不同的协议运行模型：现实模型(Real-life Model)和理想模型(Ideal Model). 现实模型是对真实协议运行过程的抽象，主要涉及 3 类参与方：π 表示需要被分析的协议，被抽象为交互式图灵机；$\mathcal{Z}$ 表示所分析协议所处的运行环境，也被抽象为一个实体，用于模型化除被分析的协议之外的所有其他协议(例如，调用当前协议的上层协议等)；$\mathcal{A}$ 表示概率多项式时间(Probabilistic Polynomial Time，PPT)攻击者，控制着所有协议用户之间的通信网络. 理想模型是为了刻画密码任务的安全目标而定义的，主要涉及到下述参与方：$\mathcal{Z}$ 表示所分析协议所处的运行环境；理想功能 $\mathcal{F}$ 是一个特殊的实体，刻画了密码任务应该实现的功能和最大允许的信息泄露，并且通过安全信道直接与(虚拟的)协议参与方进行交互；理想攻击者 $\mathcal{S}$ 不能直接控制协议用户之间的通信，仅仅能通过和 $\mathcal{F}$ 交互来获取一些不会影响最终安全目标的信息，从形式上确保了理想模型中密码任务的安全性.

通过定义协议模拟和协议实现，UC 框架以统一的方式给出了协议安全性的定义，即要求现实模型中的协议和理想模型中的理想功能具有几乎相同的功能、实现了相似的密码学目标. 具体地说，给定现实模型中的协议 π 和理想模型中的理想功能 $\mathcal{F}$，如果对任意的 PPT 攻击者 $\mathcal{A}$，都有一个相应的理想攻击者 $\mathcal{S}$，使得任意的环境 $\mathcal{Z}$ 都不能以不可忽略的概率区分两种模型中的协议运行——即不能区分它是‘在与现实模型中的协议 π 和攻击者 $\mathcal{A}$ 进行交互’还是‘在于理想模型中的理想功能 $\mathcal{F}$ 和攻击者 $\mathcal{S}'$ 进行交互，那么称现实模型中的协议 π 为 UC 模拟/实现了理想模型中的理想功能 $\mathcal{F}$，也称为 UC 安全的’.

进一步，Canetti[18]证明了如果协议 π 为 UC 模拟/实现了理想功能 $\mathcal{F}$，Π 是调用了理想功能 $\mathcal{F}$ 的任何(混合)密码协议，那么将 $\mathcal{F}$ 替换成 π 后所得到的协议 Π' 实现了和 Π 相同的功能. 这个结论保证了协议的可组合安全性，被称为组合定理. 随后，面向不同协议实例之间可能共同享有相同的子协议或共同参考串 CRS 的情形，Canetti 和 Rabin[27]对 UC 框架进行了改进，定义了拥有共同状态的 UC 框架(JUC)，通过引入多会话扩展的概念定义了新的组合算子、给出了新的组合定理，在不同协议之间共有子协议的条件下保证了组合安全性.

2.2　GPAKE 协议的理想功能

面向“客户-网关-服务器”的特殊通信架构，针对 GPAKE 协议需要保证会话密钥语义安全、防止恶意网关猜测客户口令、以及保持会话密钥相对于服务器的私密性等安全目标，本节在 UC 框架下给出了 GPAKE 的理想功能 $\mathcal{F}_{\text{GPAKE}}$，形式化地定义 GPAKE 的安全性. 所构造的 GPAKE 理想功能以 UC 框架下两方 PAKE[4,28-29]、传统三方 PAKE[30-31]的理想功能为基础和出发点，同时考虑到 GPAKE 协议与两方或传统三方 PAKE 协议的不同：需要添加从客户到服务器的显式认证，以防止想知道用户口令的恶意网关实施离线字典攻击.

2.2.1　GPAKE 协议的理想功能构造

假设 k 是安全参数，Pid 是由 3 个参与方身份

构成的有序集合，形如 $Pid=\{P_c,P_g,P_s\}$，GPAKE 理想功能 $\mathcal{F}_{\text{GPAKE}}$ 按照如下定义对理想攻击者 $\mathcal{S}$ 和协议用户 $P_1,P_2,\cdots$ 的询问进行响应.

(1) 协议初始化部分：

① 当理想功能 $\mathcal{F}_{\text{GPAKE}}$ 收到来自某个协议参与方 P_i 的询问(NewSession，sid，Pid，P_i，pw_i，$role$)时，其中 $P_i\in Pid$，$role\in\{client,server\}$，则执行：

如果这是第 1 个 NewSession 询问，或这是第 2 个或第 3 个 NewSession 询问、Pid 和已有记录中的 Pid 相同，且目前不存在角色为 $role$ 的记录，则增加记录(sid，Pid，P_i，pw_i，$role$)，将该记录标记为 fresh，然后向攻击者 $\mathcal{S}$ 发送消息(sid，Pid，P_i，$role$)；

② 当理想功能收到来自参与方 P_i 的询问(NewSession，sid，Pid，P_i，$gateway$)时，执行：

如果这是第 1 个 NewSession 询问，或这是第 2 个或第 3 个 NewSession 询问、Pid 和已有记录中的 Pid 相同，且目前不存在角色为 $gateway$ 的记录，则增加记录(sid，Pid，P_i，$gateway$)，将该记录标记为 fresh，然后向攻击者 $\mathcal{S}$ 发送消息(sid，Pid，P_i，$gateway$).

(2) 口令测试部分：

当理想功能接收到攻击者 $\mathcal{S}$ 发送的询问消息(TestPwd，sid，P_i，pw_i')时，如果已经存在被标记为 fresh 的记录(sid，Pid，P_i，pw_i，$role$)，则执行：

如果 $pw_i=pw_i'$，将该记录标记由 fresh 更新为 compromised，向攻击者发送 *correct guess*；

如果 $pw_i\neq pw_i'$，将该记录标记由 fresh 更新为 interrupted，并向攻击者发送 *wrong guess*.

(3) 密钥生成部分：

① 当理想功能收到来自攻击者 $\mathcal{S}$ 的询问(GetReady，sid，Pid，P_s，$server$)时，如果此时存在被标记为 fresh 的记录(sid，Pid，P_s，pw_s，$server$)，则执行：

如果存在被标记为 fresh 的记录(sid，Pid，P_c，pw_c，$client$)，满足 $pw_c=pw_s$，则记录(sid，Pid，P_s，pw_s，$server$，ready)，并向 P_s 发送(sid，Pid，completed)；

否则，记录(sid，Pid，P_s，pw_s，$server$，error)，并向 P_s 发送(sid，Pid，error)；

② 当收到来自攻击者 $\mathcal{S}$ 的询问(NewKey，sid，Pid，P_g，sk_g，$gateway$)时，如果此时存在记录(sid，Pid，P_g，$gateway$)，则执行：

如果某个参与方 $P_i\in Pid$ 已经被腐化，或记录(sid，Pid，P_s，pw_s，$server$)已为 compromised，则将(sid，Pid，sk_g)发送给 P_g；

否则，则选择一个随机密钥 $sk_g'\in\{0,1\}^k$，记录(sid，Pid，P_g，$gateway$，sk_g')，并将(sid，Pid，sk_g')发送给参与方 P_g；

③ 当收到来自攻击者 $\mathcal{S}$ 的询问(NewKey，sid，Pid，P_c，sk_c，$client$)时，如果此时存在记录(sid，Pid，P_c，pw_c，$client$)，则执行：

如果该记录的标记为 compromised，或某个参与方 $P_i\in Pid$ 已经被腐化，则将(sid，sk_c)发送给参与方 P_c；

如果该记录的标记为 fresh，且存在记录(sid，Pid，P_s，pw_s，$server$，ready)和(sid，Pid，P_g，$gateway$，sk_g')，则将(sid，Pid，sk_g')发送给 P_c；

否则，选择一个随机的密钥 $sk_c'\in\{0,1\}^k$，将(sid，Pid，sk_c')发送给参与方 P_c.

2.2.2 理想功能构造说明

GPAKE 理想功能 $\mathcal{F}_{\text{GPAKE}}$ 的构造分为 3 个部分：协议初始化、口令测试以及密钥生成. 在协议初始化部分，参与方通过向理想功能发送 NewSession 询问显式地参与协议；在口令测试部分，攻击者通过向理想功能发送 TestPwd 消息进行口令猜测，模型化了现实攻击者实施的在线字典攻击；在密钥生成部分，理想功能基于参与方所处的不同状态采用不同的策略生成最终的会话密钥. 如果攻击者实施在线字典攻击猜测口令错误，相应的参与方将生成独立随机的会话密钥；如果猜测正确，攻击者将可以获知相应参与方的会话密钥. 在没有遭受在线字典攻击时，诚实的客户和网关将生成相同的会话密钥，并且对服务器是未知的，刻画了会话密钥的语义安全和相对于服务器的私密性.

和已有的 UC 框架下的两方 PAKE 协议理想功能类似，我们让环境为客户和服务器提供口令作为输入，而不是让理想功能依据给定概率分布随机地生成口令. 如同 Abdalla 等人[28]所指出，让环境选择口令有如下好处：(1) 能够模型化参与方将相同口令用在不同安全协议中的情况；(2) 能够刻画口令依据任意概率分布(即不一定是均匀分布)随机选取时协议的安全性；(3) 使得理想功能以自然的方式刻画会话密钥的前向安全性.

另外，理想功能还刻画了客户和服务器之间的显式认证：只有当客户是诚实的、且和服务器拥有相同的口令时，服务器才可能进入 completed 状态，网关才可能生成和客户相同的会话密钥；否则服务器就将返回错误消息 error，网关也将会与服务器生成

独立的密钥，防止了恶意网关猜测用户口令.

3　UC 安全的 GPAKE 协议

本节给出我们设计的 UC 安全的网关口令认证密钥交换协议框架，简称为 UC-GPAKE 协议. 类似于文献[9,31-32]，UC-GPAKE 协议构造采用了模块化的设计思想，将 UC 安全的两方 PAKE 理想功能作为其子模块；此外，还用到了针对选择消息攻击存在性不可伪造(CMA-EUF)安全的消息认证码(MAC)机制、Diffie-Hellman 密钥交换等组件.

3.1　密码学组件

3.1.1　UC 安全的两方 PAKE

2005 年，Canetti 等人[4]首次给出了两方 PAKE 的理想功能，在 UC 框架下对传统“客户-服务器”架构下的 PAKE 的安全目标进行了刻画. 随后，Abdalla 等人[28]和 Groce 等人[33]分别对其进行了改进，提出了能实现单向认证和双向认证的理想功能. 为了将尽可能多的两方 PAKE 协议用作 GPAKE 协议的子模块，我们选用了安全性定义最为基础的不带认证的理想功能 $\mathcal{F}_{\text{2PAKE}}$[4]作为协议组件，其具体构造如图 1 所示.

(1) 假设 k 是安全参数. 理想功能 $\mathcal{F}_{\text{2PAKE}}$ 将按照如下方式对理想攻击者 $\mathcal{S}$ 和协议参与方 $P_1, P_2, \cdots$ 的询问进行响应.

(2) 当收到某个用户 P_i 发送的询问(NewSession, $sid, P_i, P_j, pw, role$)时，

① 向攻击者 $\mathcal{S}$ 发送消息(NewSession, $sid, P_i, P_j, role$)；

② 如果该询问是首个 NewSession 询问，或是第 2 个 NewSession 询问且理想功能中已存在记录(P_j, P_i, pw')，则记录(P_i, P_j, pw)并将其标记为 fresh.

(3) 当收到攻击者 $\mathcal{S}$ 发送的询问(TestPwd, sid, P_i, pw')时，如果此时存在记录(P_i, P_j, pw)且其标记为 fresh，则

① 如果 $pw = pw'$，将该标记更改为 compromised，并发送 correct guess 给攻击者；

② 如果 $pw \neq pw'$，将该标记更改为 interrupted，并发送 wrong guess 给攻击者.

(4) 当接收到攻击者 $\mathcal{S}$ 发送的询问(NewKey, sid, P_i, sk), $sk \in \{0,1\}^k$ 时，如果该询问是关于用户 P_i 的第 1 个 NewKey 询问且理想功能中已经存在相关记录(P_i, P_j, pw)，则：

① 如果该记录的标记为 compromised，或 P_i, P_j 中至少 1 个被腐化，则向 P_i 发送(sid, sk)；

② 如果该记录的标记为 fresh，且存在记录(P_j, P_i, pw')，满足 $pw = pw'$，已向用户 P_j 发送过密钥 sk' 且(P_j, P_i, pw')在接收到密钥时的标记为 fresh，发送(sid, sk')给 P_i；

③ 在所有其他情况下，选择一个新的随机值 $sk' \in \{0,1\}^k$ 并向 P_i 发送(sid, sk').

最终，将记录(P_i, P_j, pw)标记更新为 completed.

图 1　两方 PAKE 的理想功能 $\mathcal{F}_{\text{2PAKE}}$

理想功能 $\mathcal{F}_{\text{2PAKE}}$ 构造的出发点是经典密钥交换协议的理想功能，在此基础上综合考虑了低熵口令易于遭受字典攻击的固有安全缺陷. 理想功能设计的核心思想是：当进行密钥协商的两个实体都没有被腐化、攻击者没有对任何一方实施主动攻击时，则理想功能选择一个新鲜的随机值作为两个实体共享的会话密钥，且该密钥对于攻击者是未知的；然而，如果攻击者腐化了某一个实体，或是通过主动攻击猜测得到了某个实体所拥有的口令，则让攻击者拥有知晓(甚至决定)相应会话密钥的能力，即认为攻击者完全攻破协议的安全目标；另外，如果攻击者采取了主动攻击，但是没有成功猜对口令的情况下，通信双方应该生成相互(不匹配的)独立随机会话密钥.

3.1.2　消息认证码机制[34]

一个消息认证码机制 MAC=(Key, Mac, Ver)包含 3 个 PPT 算法：密钥生成算法 Key 的输入为安全参数 1^k，输出为一个随机密钥 $K \in Key(1^k)$；MAC 生成算法 Mac 的输入为密钥 K 和消息 m，输出为相应的认证码 $\delta = Mac_K(m)$；验证算法 Ver 的输入为密钥 K、消息 m 和认证码 δ，当 δ 是消息 m 的合法有效的认证码时，输出为 1，否则输出为 0. MAC 机制定义还应该满足正确性要求，即对任意的密钥 K 和消息 m 都有 $Ver_K(m, Mac_K(m)) = 1$.

消息认证码的安全性定义如下. 首先，任意选择随机的 MAC 密钥 $K \in Key(1^k)$，并假设攻击者 $\mathcal{A}_{mac}$ 能够询问 MAC 生成谕示 $\mathcal{O}_{mac}(m) = Mac_K(m)$ 和验证谕示 $\mathcal{O}_{ver}(m, \delta) = Ver_K(m, \delta)$. 设攻击者 $\mathcal{A}_{mac}$ 在进行了多项式次询问后，输出消息和 MAC 值对 (x^*, δ^*)，如果 $\mathcal{A}_{mac}$ 从未就消息 x^* 询问过谕示 $\mathcal{O}_{mac}$，但是成立 $Ver_k(x^*, \delta^*) = 1$，则认为攻击者攻击成功，将该事件记为 $Succ_{mac}$. 将 $Succ_{mac}$ 发生的概率定

义为 $\mathcal{A}_{mac}$ 的优势，即 $Adv_{MAC}^{EUF}(\mathcal{A}_{mac})=\Pr\{Succ_{mac}\}$，并相应的定义优势函数

$$Adv_{MAC}^{EUF}(t,q_{mac},q_{ver})=\max_{\mathcal{A}_{mac}}\{Adv_{MAC}^{EUF}(\mathcal{A}_{mac})\},$$

其中最大值所涉及到的 $\mathcal{A}_{mac}$ 需要满足条件：(1)计算时间不超过 t；(2)询问 MAC 生成和验证谕示的次数分别不超过 q_{mac}，q_{ver}. 如果对任意 PPT 的攻击者，$Adv_{MAC}^{EUF}(t,q_{mac},q_{ver})$ 都是可忽略的，则称消息认证码 MAC=(Key,Mac,Ver)在选择消息攻击下是存在性不可伪造(CMA-EUF)安全的.

3.1.3 DDH 困难性假设[35]

设 $G=\langle g\rangle$ 是素数 q 阶循环群，群 G 上的 DDH (Decisional Diffie-Hellman)问题是指：区分 Diffie-Hellman 三元组集合 $\{(g^x,g^y,g^{xy}):x,y\in Z_q\}$ 和随机三元组集合 $\{(g^x,g^y,g^z):x,y,z\in Z_q\}$ 上的均匀分布. 假设 $\mathcal{A}_{ddh}$ 是一个 PPT 攻击者(也被称为区分器)，定义 $\mathcal{A}_{ddh}$ 的优势为 $Adv_G^{\mathrm{DDH}}(\mathcal{A}_{ddh})=|2\Pr[Succ]-1|$，其中 $Succ$ 表示事件“攻击者猜对所给三元组的概率分布”. DDH 困难性假设是指对所有计算时间不超过 t 的 PPT 攻击者 $\mathcal{A}_{ddh}$，其优势 $Adv_G^{ddh}(\mathcal{A}_{ddh})$ 都是可忽略函数.

3.2 UC-GPAKE 协议构造

假设 $\mathcal{F}_{\mathrm{2PAKE}}$ 是两方 PAKE 协议的理想功能，MAC=(Key,Mac,Ver)是一个 CMA-EUF 安全的消息认证码，$G=\langle g\rangle$ 是阶为素数 q 的循环群. 假设客户 P_c 和接入网关 P_g 试图在认证服务器 P_s 的帮助下协商生成共享的会话密钥，运行 UC-GPAKE 协议的具体步骤如下：

(1)当客户 P_c 被环境 $\mathcal{Z}$ 发送的消息(即子程序输入)(NewSession,sid,Pid,P_c,pw_c,$client$)激活后，首先检查确保 Pid 是形如 $Pid=\{P_c,P_g,P_s\}$ 的有序集合，且客户身份 P_c 与该集合中的身份信息 P_c 相一致. 然后，客户 P_c 定义 $sid'=sid\parallel P_c\parallel P_s$，并向两方 PAKE 的理想功能 $\mathcal{F}_{\mathrm{2PAKE}}$ 发送询问消息(NewSession,sid',P_c,P_s,pw_c,$client$). 当服务器 P_s 被激活后，定义相同的 sid' 并执行类似的操作步骤. 特别地，如果不存在会话标识为 sid' 的两方 PAKE 理想功能 $\mathcal{F}_{\mathrm{2PAKE}}$，则激活一个新的理想功能实例.

(2)当网关 P_g 来自环境 $\mathcal{Z}$ 的消息(NewSession,sid,Pid,P_i,$gateway$)激活后，首先检查确保 Pid 是形如 $Pid=\{P_c,P_g,P_s\}$ 的有序集合，且网关身份 P_g 与该集合中的身份信息 P_g 相一致. 然后，网关进入等待状态.

(3)当客户 P_c 收到来自于会话标识为 sid' 的两方 PAKE 理想功能 $\mathcal{F}_{\mathrm{2PAKE}}$ 实例的子程序输出(sid',sk')时，选择随机数 $x\in\mathbb{Z}_q^*$，计算 $X=g^x$ 以及 $\delta_{cs}=Mac_{sk'}(sid,Pid,P_c,X)$，然后发送消息($sid$,$Pid$,$X$,$\delta_{cs}$)给网关 P_g；当服务器 P_s 收到来自于会话标识为 sid' 的两方 PAKE 理想功能 $\mathcal{F}_{\mathrm{2PAKE}}$ 实例的子程序输出(sid',sk')时，记录(sid',sk')并进入等待状态.

(4)网关 P_g 收到来自客户 P_c 的(sid,Pid,X,δ_{cs})后，选择随机数 $y\in\mathbb{Z}_q^*$，计算 $Y=g^y$，然后通过认证信道发送消息(sid,Pid,X,Y,δ_{cs})给服务器 P_s.

(5)服务器 P_s 收到来自于网关 P_g 的消息(sid,Pid,X,Y,δ_{cs})后，利用从理想功能 $\mathcal{F}_{\mathrm{2PAKE}}$ 处获得的 sk' 验证 δ_{cs}：如果 $Ver_{sk'}((sid,Pid,P_c,X),\delta_{cs})=0$，表明关于 MAC 认证码合法性验证未通过，则服务器向环境 $\mathcal{Z}$ 输出(sid,Pid,error)，向网关 P_g 发送(sid,Pid,error)，然后终止协议运行；若 $Ver_{sk'}((sid,Pid,P_c,X),\delta_{cs})=1$，意味着 MAC 验证通过，则服务器利用临时密钥 sk' 计算 $\delta_{sc}=Mac_{sk'}(sid,Pid,P_s,Y,X)$，随后向环境 $\mathcal{Z}$ 发送输出(sid,Pid,completed)，并通过认证信道给网关发送消息(sid,Pid,X,Y,δ_{sc}).

(6)若网关 P_g 收到来自 P_s 的消息(sid,Pid,error)，即从 P_s 获知验证不通过，则选择随机的会话密钥 $sk_{gc}\in\{0,1\}^k$；否则，若网关 P_g 从服务器处收到消息(sid,Pid,X,Y,δ_{sc})，表明客户之前发送的消息通过了服务器的验证，则计算 $sk_{gc}=X^y$，向环境输出(sid,Pid,sk_{gc})，然后发送消息(sid,Pid,Y,δ_{sc})给客户 P_c.

(7)客户 P_c 收到来自于 P_g 的消息(sid,Pid,Y,δ_{sc})后，首先利用 sk' 验证 MAC 认证码 δ_{sc}，如果验证不通过则选择随机的会话密钥 $sk_{cg}\in\{0,1\}^k$；如果验证通过，则计算 $sk_{cg}=Y^x$. 最后，向环境输出(sid,Pid,sk_{cg}).

注 1. 在 UC-GPAKE 协议中，服务器的主要作用是协助网关验证客户的合法性，因此当客户发送的消息中 MAC 认证码验证不通过时，服务器不仅向环境输出(sid,Pid,error)，还进一步通知网关验证未通过的结果；对于客户(或网关)，我们采用了和理想功能定义相一致的做法，如果有任何验证不通过，则客户(或网关)直接选择独立随机的比特串作为会话密钥. 只有当所有验证都通过的情况下，双方才能计算得到相同的会话密钥.

注 2. 类似于传统“孤立”模型下已有 GPAKE 协议构造[8,13]，UC-GPAKE 协议假设网关和服务器

间有能提供安全认证服务的信道.在理想模型中,认证信道可通过调用认证通信理想功能[18]作为子模块实现,提供网关和服务器之间的传递消息的数据源和完整性认证;在现实模型中,可假设在协议初始化阶段网关和服务器之间共享高熵的对称密钥,然后利用安全 MAC 机制对所传输的消息进行认证.注意到网关和认证服务器都具有较强的计算能力,上述假设是容易实现的.

3.3　协议实例化

UC-GPAKE 协议是一种混合协议,它将两方 PAKE 理想功能 $\mathcal{F}_{2\text{PAKE}}$ 作为一个基本组件,在实际应用中可以被替换成为任何能够 UC 实现 $\mathcal{F}_{2\text{PAKE}}$ 理想功能的两方 PAKE 协议[4,28,36].当作为组件的两方 PAKE 协议是随机谕示(RO)模型下可证明安全的,所得到的 UC-GPAKE 协议将是 RO 模型下可证明安全的;当所采用的两方 PAKE 协议是标准模型下可证明安全的协议时,所得到的 UC-GPAKE 协议实例也将是标准模型下可证明安全的协议.

本节中,我们利用 Abdalla 等人[28]给出的 RO 模型下 UC 安全的两方 PAKE 协议进行实例化,得到了一个高效的 UC-GPAKE 协议,具体步骤如图 2 所示.其中实线表示参与方之间的通信是通过不安全信道进行的,虚线表示网关和服务器之间的通信是通过预先存在的认证信道进行的.

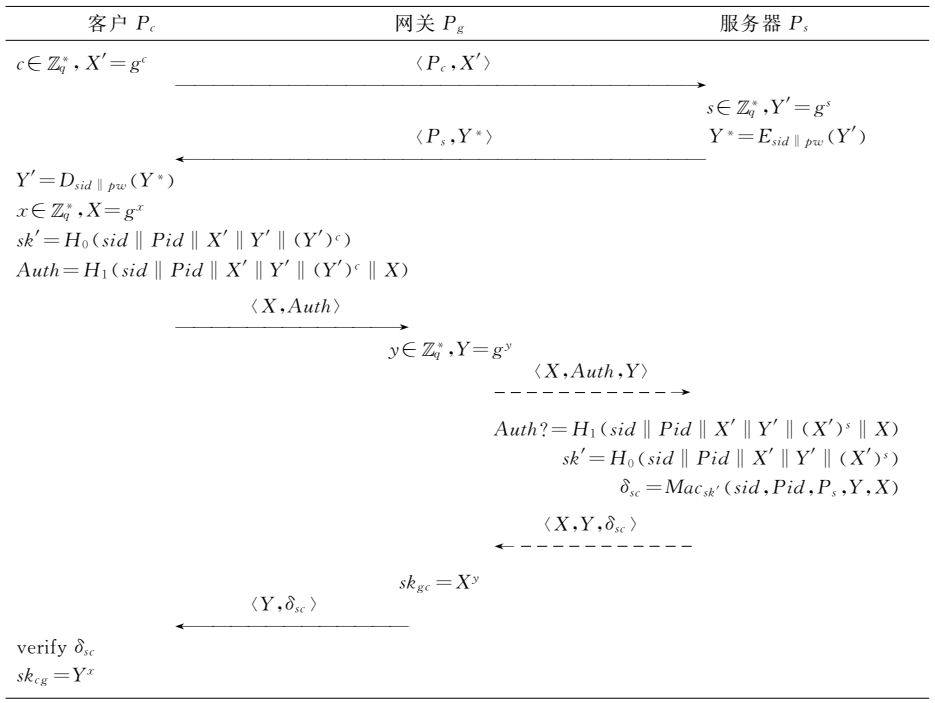

图 2　UC-GPAKE 协议实例化

在第 4 节中,我们将通过严格的安全性规约证明 UC-GPAKE 协议的安全性,这将涵盖本节中协议实例的安全性.为了更为直观地说明协议的安全属性,下面对协议的设计原理和安全性进行简要的分析.协议的前 4 条消息实现了客户 P_c 和服务器 P_s 之间的两方口令认证密钥交换,生成了共享的临时会话密钥 sk',并实现了服务器 P_s 对客户 P_c 的单向认证.由于作为底层组件的两方 PAKE 中包含有从客户到服务器的认证消息,所以在实例化过程中通过复用该消息简化了消息的传输次数.具体地说,我们在 Abdalla 等人给出协议[28]的 $Auth$ 计算过程中添加了 $X=g^x$,在实现临时密钥确认的同时实现了对 X 的认证,避免了使用 MAC 认证码对 X 认证(见 3.2 节步骤 3)所带来的额外计算.另外,通过使用 sk' 作为 MAC 密钥生成认证码 δ_{sc},协议还实现了从客户 P_c 对服务器 P_s 的显式认证,从而 UC-GPAKE 协议提供了客户和服务器之间的显式双向认证,达到了防止恶意网关攻击的目的.

协议的第 3 条至第 6 条消息构成了客户 P_c 和网关 P_g 之间的 Diffie-Hellman 密钥交换,并在服务器 P_s 的协助下使用 MAC 机制保证了消息传输的认证性,从而直观地保证了会话密钥相对于外部攻击者的语义安全性.另外,由于客户 P_c 和网关 P_g 分别掌握有私密信息 x,y 且对服务器保密,服务器将无法获知最终生成的会话密钥 $sk_{cg}=sk_{gc}=g^{xy}$ 的信息,协议还保证了会话密钥相对于服务器的

私密性.

3.4 协议比较

本节将 UC-GPAKE 协议的安全性和效率和其他协议进行比较. 鉴于 UC-GPAKE 协议是基于两方 PAKE 协议的模块化设计,所以在比较协议效率时我们利用 3.3 节所给出的实例化后的协议. 表 1 列出了实例化后的 UC-GPAKE 协议和已有的 GPAKE 协议之间的详细比较结果.

表 1 UC-GPAKE 协议的安全性和效率比较

	安全模型	抗 UODA	M-Auth	通信轮数	客户	网关	服务器
ACFP[8]	ROR Model	No	No	4	2E	2E	2E
AIP[11]	ROR$^+$ Model	No	No	4	4E	3E	3E
YY[12]	ROR Model	Yes	Yes	7	4E	2E	4E
WMZ[13]	ROR$^+$ Model	Yes	Yes	6	3E	2E	2E
Ours	UC-Framework	Yes	Yes	6	4E	2E	2E

在表格中,"安全模型"表示协议安全证明所依赖的安全模型,其中 ROR Model 表示 Abdalla 等人提出的适用于 GPAKE 协议分析和安全证明的 Real-Or-Random 模型[8],ROR Model$^+$ 表示 Abdalla 等人 2008 年在 Real-Or-Random 模型基础上进一步改进提出的增强模型[11],UC-Framework 表示通用可组合框架."抗 UODA"表示协议是否能够抵抗不可察觉在线字典攻击(UODA),"M-Auth"表示协议是否提供客户和服务器之间的显式双向认证,"通信轮数"表示协议运行所需传递消息的轮数,"客户"、"网关"、"服务器"分别表示 3 个参与方的计算复杂度,只计算最为耗时的模指数运算,其中 E 表示一次模指数运算所需的计算时间.

如表 1 所指出,在安全性方面 UC-GPAKE 协议要强于已有的 GPAKE 协议,它能保证在复杂应用环境的组合安全性,并且能提供双向认证、防止 UODA 攻击. 注意到部分早期的协议[8,11]不能抵抗 UODA 攻击,且都是在传统"孤立"的安全模型中可证明安全的,并不能保证组合安全性. 在协议效率方面,鉴于文献[8,11]中的协议存在安全性缺陷,只需与安全的协议进行比较. UC-GPAKE 协议具有和 Wei 等人[13]的协议相同的通信轮数,在网关和服务器端拥有相同的计算复杂度,表现优于文献[12]中的协议. 不过,由于我们考虑了更强的安全性,在客户端的计算效率方面还是有一定的损失,和文献[12]一样需要计算 4 次模指数运算.

4 协议的安全性证明

本节证明 UC-GPAKE 协议满足 UC 框架下 GPAKE 的安全定义. 因为协议构造需要用到公共参考串,其安全性证明实际上是在 JUC 框架下进行的,即需证明所构造的 UC-GPAKE 协议实现了理想功能 $\mathcal{F}_{\text{GPAKE}}$ 的多会话扩展 $\mathcal{F}_{\text{GPAKE}}$. 另外,由于 UC-GPAKE 协议构造使用了两方 PAKE 协议的理想功能 $\mathcal{F}_{\text{2PAKE}}$ 作为子模块,因而定理证明是在混合模型中进行的.

定理 1. 假设 $\mathcal{F}_{\text{2PAKE}}$ 是两方 PAKE 协议的理想功能,MAC$=(Key,Mac,Ver)$ 是一个 CMA-EUF 安全的消息认证码,$G=\langle g\rangle$ 是阶为素数 q 的循环群,且群 G 上的 DDH 问题是困难的,则 3.2 节中所构造的 UC-GPAKE 协议是UC安全的,即在 $\mathcal{F}_{\text{2PAKE}}$-混合模型中 UC 实现了理想功能 $\mathcal{F}_{\text{GPAKE}}$ 的多会话扩展 $\mathcal{F}_{\text{GPAKE}}$.

注 1. 如果遵循 JUC 框架中多会话扩展定义,理想功能 $\mathcal{F}_{\text{GPAKE}}$ 的不同实例将具有完全一样的会话标识 SID,它们通过额外定义不同的子会话标识 $SSID$ 来予以区分. 下述证明中,我们将省略相同的 SID,仅使用具有区分意义的 $SSID$.

证明. 根据 UC 框架中协议模拟/实现的定义,定理 1 的结论是指:对任意 PPT 攻击者 $\mathcal{A}$,都存在理想攻击者 $\mathcal{S}$,使得任意 PPT 环境 $\mathcal{Z}$ 都不能以不可忽略的概率区分它是'在与真实 UC-GPAKE 协议用户以及攻击者 $\mathcal{A}$ 进行交互'还是'在与理想功能 $\mathcal{F}_{\text{GPAKE}}$ 以及理想攻击者 $\mathcal{S}$ 进行交互'. 因此,证明过程主要包含构造理想攻击者(即模拟者)和证明不可区分性两个部分,4.1 节给出模拟者 $\mathcal{S}$ 的详细构造,4.2 节证明环境对理想模型和现实模型中协议运行的不可区分性.

4.1 构造模拟者 $\mathcal{S}$

模拟者 $\mathcal{S}$ 的构造主要通过调用攻击者 $\mathcal{A}$ 来实现. 总体上讲,模拟者 $\mathcal{S}$ 将利用与理想功能 $\mathcal{F}_{\text{GPAKE}}$ 动态交互所获得的信息,为攻击者 $\mathcal{A}$ 构造一个模拟的协议运行环境,在其中模拟除 $\mathcal{A}$ 之外的所有实体,然后模拟者 $\mathcal{S}$ 尽可能地模仿攻击者 $\mathcal{A}$ 的行为而进行动作. 模拟的难点在于,$\mathcal{S}$ 需要在不知道用户真实口令

的情形下回答攻击者$\mathcal{A}$的询问. 相应采取的解决办法是让$\mathcal{S}$充分地利用与$\mathcal{F}_{\text{GPAKE}}$交互的能力，从中直接或间接地获得口令的信息.

模拟者$\mathcal{S}$的具体构造如下. 在被激活后，模拟者$\mathcal{S}$调用攻击者$\mathcal{A}$，为$\mathcal{A}$提供运行协议所需公共参考串(包括群G以及其生成元g)，然后按照如下方式模拟$\mathcal{F}_{\text{2PAKE}}$-混合模型中的所有参与方和两方 PAKE 的理想功能$\mathcal{F}_{\text{2PAKE}}$：

(1) 如果模拟者$\mathcal{S}$收到了来自理想功能$\mathcal{F}_{\text{GPAKE}}$的消息$(ssid, Pid, P_i, role)$，其中$Pid=\{P_c, P_g, P_s\}$，$role\in\{client, server\}$，以会话标识为$ssid$、用户标识为$P_i\in\{P_c, P_s\}$、角色为$role$激活一个新的实例，简记为$(ssid, P_i)$. 令$P_j$为集合$\{P_c, P_s\}\backslash\{P_i\}$中的身份信息，$ssid'=ssid\parallel P_c\parallel P_s$，以会话标识为$ssid'$的理想功能$\mathcal{F}_{\text{2PAKE}}$身份向攻击者$\mathcal{A}$发送消息$(\text{NewSession}, ssid', P_i, P_j, role)$，在$\mathcal{S}$的内部状态中记录$(P_i, P_j, \perp)$并将该记录标记为 fresh；

(2) 如果模拟者$\mathcal{S}$收到了来自理想功能$\mathcal{F}_{\text{GPAKE}}$的消息$(ssid, Pid, P_g, gateway)$，以会话标识为$ssid$、用户标识为$P_g$、角色为$gateway$激活一个新的网关实例，记为$(ssid, P_g)$，然后进入等待状态；

(3) 当模拟者$\mathcal{S}$所模拟的理想功能$\mathcal{F}_{\text{2PAKE}}$收到来自于$\mathcal{A}$的口令测试询问$(\text{TestPwd}, ssid', P_i, pw')$时，模拟者$\mathcal{S}$利用该消息中所包含的口令$pw'$向理想功能$\mathcal{F}_{\text{GPAKE}}$发出询问$(\text{TestPwd}, ssid, P_i, pw')$. 如果$\mathcal{F}_{\text{GPAKE}}$返回消息“correct guess”，则表示攻击者$\mathcal{A}$猜测到了正确的口令，模拟者$\mathcal{S}$将记录$(P_i, P_j, \perp)$更新为(P_i, P_j, pw')，并将其状态更新为 compromised；如果$\mathcal{F}_{\text{GPAKE}}$返回消息“wrong guess”，模拟者$\mathcal{S}$将记录$(P_i, P_j, \perp)$的状态更新为 interrupted；

(4) 当模拟者$\mathcal{S}$所模拟的理想功能$\mathcal{F}_{\text{2PAKE}}$收到来自于$\mathcal{A}$的密钥生成询问$(\text{NewKey}, ssid', P_i, sk)$时，其中$P_i\in\{P_c, P_s\}$，记$P_j$为集合$\{P_c, P_s\}\backslash\{P_i\}$中的身份信息，如果$(P_i, P_j, *)$是 compromised 或某个用户被腐化，则直接发送$(ssid', sk)$给用户P_i；如果$(P_i, P_j, \perp)$是 fresh，其同时存在记录$(P_j, P_i, \perp)$，已经给用户P_j发送过密钥sk'且发送密钥时该会话是 fresh，那么模拟者$\mathcal{S}$向理想功能$\mathcal{F}_{\text{GPAKE}}$发送询问$(\text{GetReady}, ssid, Pid, P_s, server)$. 如果$\mathcal{S}$收到$\mathcal{F}_{\text{GPAKE}}$返回的消息$(ssid, Pid, \text{completed})$，则表明$P_i, P_j$拥有相同的口令，此时将用户$P_j$拥有的密钥$sk'$发送给用户$P_i$. 在所有其他情况下，选择一个新的随机值$sk'$，并将其发送给用户$P_i$.

(5) 当所模拟的客户P_c或服务器P_c得到来自于理想功能$\mathcal{F}_{\text{2PAKE}}$的临时密钥后，模拟者$\mathcal{S}$就可以按照真实协议规范模拟所有参与方的剩余动作，即生成并发送消息，或接收验证消息并生成最终的密钥. 需要注意的是，此时用户间发送的消息都需要经过攻击者$\mathcal{A}$转发. 另外，如果模拟的用户或服务器生成了会话密钥，则模拟者$\mathcal{S}$就利用相应的密钥发出 NewKey 询问.

4.2　证明不可区分性

本节证明不可区分性，即任意 PPT 环境$\mathcal{Z}$都只能以最多可忽略的概率区分它是‘在与真实 UC-GPAKE 协议用户以及攻击者$\mathcal{A}$进行交互’还是‘在与理想功能$\mathcal{F}_{\text{GPAKE}}$以及理想攻击者$\mathcal{S}$进行交互’. 为此，我们根据环境$\mathcal{Z}$所提供的口令输入以及攻击者的不同行为分情况进行讨论. 容易验证，任何参与方的腐化都将导致攻击者能够攻击成功，因此下述讨论仅仅分析攻击者没有发出腐化请求的情况.

(1) 情形 1. 环境$\mathcal{Z}$为协议中的客户和服务器提供了相同的口令$pw_c=pw_s$，协议运行中攻击者$\mathcal{A}$没有发出 TestPwd 询问.

当环境$\mathcal{Z}$在与现实攻击者$\mathcal{A}$以及 UC-GPAKE 协议进行交互时，根据 3.2 节中的协议构造可知，作为子程序的理想功能$\mathcal{F}_{\text{2PAKE}}$将为客户$P_c$和服务器$P_s$提供相同的临时密钥$sk'$. 注意到 MAC 机制是一个 CMA-EUF 安全的消息认证码，故当临时密钥sk'安全的情况下，攻击者$\mathcal{A}$只能以最多可忽略的概率伪造 MAC 认证码. 因此，除了可忽略的概率外，客户和网关将生成相同的 Diffie-Hellman 实例输出作为会话密钥$sk_{cg}=sk_{gc}=g^{xy}$.

当环境$\mathcal{Z}$在与理想攻击者$\mathcal{S}$以及理想功能$\mathcal{F}_{\text{GPAKE}}$进行交互时，根据 4.1 节中模拟者$\mathcal{S}$的构造可知，理想环境中$\mathcal{S}$向理想功能$\mathcal{F}_{\text{GPAKE}}$发出 GetReady 询问时将获知双方的口令是相同的. 此时，理想功能将为网关P_g选择均匀随机的会话密钥sk'_g，并随后将该密钥发送给客户P_c.

综上所述，当攻击者$\mathcal{A}$没有成功伪造 MAC 认证码时，现实环境中客户和网关将采用 Diffie-Hellman 实例的输出g^{xy}作为最终的会话密钥，理想环境中的客户和网关将采用均匀选取的随机数$sk'_g=g^z$作为最终的会话密钥. 当 DDH 问题困难性假设成立时，可知环境$\mathcal{Z}$至多以可忽略的概率区分两种会话密钥，从而至多以可忽略的概率区分它是在与真实协议还是理想协议进行交互.

(2) 情形 2. 环境$\mathcal{Z}$为协议中的客户和服务器提

供了相同的口令 $pw_c = pw_s$，协议运行中攻击者$\mathcal{A}$发出了 TestPwd 询问(不妨设是针对用户 P_c).

首先考虑攻击者$\mathcal{A}$猜对了 P_c 口令的情形. 在现实环境中，$\mathcal{A}$将可以获知 P_c 的临时密钥 sk'，随后冒充网关向用户 P_c 发送攻击者选定的任意消息 $Y = g^y$，从而可获知 P_c 生成的最终密钥 $sk_{cg} = X^y$；在理想环境中，模拟者$\mathcal{S}$发出的 TestPwd 询问也将猜测正确，此时$\mathcal{S}$通过 NewKey 询问使得理想环境中的 P_c 生成和模拟环境中的 P_c 相同的会话密钥，两者是不可区分的.

其次考虑攻击者$\mathcal{A}$没有猜对 P_c 口令的情形. 在现实环境中，除了可忽略的概率外，$\mathcal{A}$发送给用户 P_c 的消息将无法验证通过，此时 P_c 将选择独立随机的密钥 sk_{cg}；而在理想环境中，$\mathcal{S}$发出的 TestPwd 询问将也猜测错误，使得理想环境中的 P_c 也将生成独立随机的会话密钥，两种情形是不可区分的.

(3) 情形 3. 环境$\mathcal{Z}$为协议中的客户和服务器提供了不同的口令 $pw_c \neq pw_s$.

在现实环境中，客户 P_c 和服务器 P_s 将生成不同的临时密钥. 根据 3.2 节中的协议构造可知，除了可忽略的概率外，P_c 和 P_s 之间的验证将无法通过，从而 P_c 和 P_g 生成的会话密钥均是独立随机的. 在理想环境中，$\mathcal{S}$向理想功能 $\mathcal{F}_{\text{GPAKE}}$ 发出 GetReady 询问将返回一个 error 消息. 根据理想功能的定义可知，P_c 和 P_g 将分别选择独立随机的值作为会话密钥. 此时，理想环境和现实环境也是不可区分的. 证毕.

5 结束语

通过在通用可组合(UC)框架下构造网关口令认证密钥交换(GPAKE)协议的理想功能，给出了 GPAKE 协议的一个新的安全性定义，不仅对 GPAKE 的基本安全目标进行了刻画，还保证了协议在复杂应用环境中的可组合安全性；利用 UC 框架下两方 PAKE 理想功能、消息认证码为组件，给出了 GPAKE 协议的一个通用构造，并证明了该构造能够 UC 安全实现所提出的 GPAKE 理想功能. 进一步利用 Abdalla 等人给出的 RO 模型下 UC 安全的两方 PAKE 协议[28]进行实例化，得到了一个高效的 UC-GPAKE 协议实例.

致 谢 审稿专家对论文提出了宝贵意见，在此表示感谢!

参 考 文 献

[1] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attack//Proceedings of the EUROCRYPT 2000. Bruges, Belgium, 2000: 139-155

[2] Katz J, Ostrovsky R, Yung M. Practical password-authenticated key exchange provably secure under standard assumptions//Proceedings of the EUROCRYPT 2001. Innsbruck, Austria, 2001: 475-494

[3] Abdalla M, Fouque P, Pointcheval D. Password-based authenticated key exchange in the three-party setting//Proceedings of the PKC 2005. Les Diablerets, Switzerland, 2005: 65-84

[4] Canetti R, Halevi S, Katz J, et al. Universally composable password-based key exchange//Proceedings of the EUROCRYPT 2005. Aarhus, Denmark, 2005: 404-421

[5] Benhamouda F, Blazy O, Chevalier C, et al. New techniques for SPHFs and efficient One-Round PAKE Protocols//Proceedings of the CRYPTO 2013. Santa Barbara, USA, 2013: 449-475

[6] Abdalla M, Benhamouda F, Mackenzie P. Security of the J-PAKE password- authenticated key exchange protocol//Proceedings of the 2015 IEEE Symposium on Security and Privacy (S&P). San Jose, USA, 2015: 571-587

[7] Xu J, Hu X X, Zhang Z F. Round-optimal password-based group key exchange protocols in the standard model//Proceedings of the Applied Cryptography and Network Security. New York, USA, 2015: 42-61

[8] Abdalla M, Chevassut O, Fouque P A, et al. A simple threshold authenticated key exchange from short secrets//Proceedings of the ASIACRYPT 2005. Chennai, India, 2005: 566-584

[9] Byun J W, Lee D H, Lim J I. Security analysis and improvement of a gateway-oriented password-based authenticated key exchange protocol. IEEE Communications Letters, 2006, 10(9): 683-685

[10] Shim K A. Cryptanalysis and enhancement of modified gateway-oriented password-based authenticated key exchange protocol. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, 91(12): 3837-3839

[11] Abdalla M, Izabachene M, Pointcheval D. Anonymous and transparent gateway-based password-authenticated key exchange//Proceedings of the Cryptology and Network Security 2008. Hong Kong, China, 2008: 133-148

[12] Yoon E J, Yoo K Y. An optimized gateway-oriented password-based authenticated key exchange protocol. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, 2010, 93(4): 850-853

[13] Wei F S, Ma C G, Zhang Z F. Gateway-oriented password-authenticated key exchange protocol with stronger security//Proceedings of the Provable Security 2011. Xi'an, China,

2011：366-379

[14] Wei Fu-Shan，Zhang Zhen-Feng，Ma Chuan-Gui. A framework for gateway-oriented password-authenticated key exchange in the standard model. Chinese Journal of Computers，2012，35(9)：1833-1844(in Chinese)
(魏福山，张振峰，马传贵. 标准模型下网关口令认证密钥交换协议的通用框架. 计算机学报，2012，35(9)：1833-1844)

[15] Wei F S，Zhang Z F，Ma C G. Analysis and enhancement of an optimized gateway-oriented password-based authenticated key exchange protocol. IEICE Transactions on Fundamentals of Electronics，Communications and Computer Sciences，2013，96(9)：1864-1871

[16] Abdalla M. Password-based authenticated key exchange：An overview//Proceedings of the Provable Security 2014. Hong Kong，China，2014：1- 9

[17] Hu Xue-Xian，Zhang Zhen-Feng，Liu Wen-Fen. Universal composable password authenticated key exchange protocol in the standard model. Journal of Software，2011，22(11)：2820-2832(in Chinese)
(胡学先，张振峰，刘文芬. 标准模型下通用可组合的口令认证密钥交换协议. 软件学报，2011，22(11)：2820-2832)

[18] Canetti R. Universally composable security：A new paradigm for cryptographic protocols//Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science (FOCS). Las Vegas，USA，2001：136-145

[19] Canetti R，Lindell Y，Ostrovsky R，et al. Universally composable two-party and multi-party secure computation//Proceedings of the 34th annual ACM Symposium on Theory of Computing. Montreal，Canada，2002：494-503

[20] Canetti R，Fischlin M. Universally composable commitments//Proceedings of the CRYPTO 2001. Santa Barbara，USA，2001：19-40

[21] Canetti R. Universally composable signature，certification，and authentication//Proceedings of the 17th IEEE Computer Security Foundations Workshop. Pacific Grove，USA，2004：219-233

[22] Green M，Hohenberger S. Universally composable adaptive oblivious transfer//Proceedings of the ASIACRYPT 2008. Melbourne，Australia，2008：179-197

[23] Canetti R，Krawczyk H. Universally composable notions of key exchange and secure channels//Proceedings of the EUROCRYPT 2002. Amsterdam，The Netherlands，2002：337-351

[24] Zhang J W，Ma J F，Moon S J. Universally composable secure TNC model and EAP-TNC protocol in IF-T. Science China Information Sciences，2010，53(3)：465-482

[25] Zhang J W，Ma J F，Yang C，et al. Universally composable secure positioning in the bounded retrieval model. Science China Information Sciences，2015，58(11)：1-15

[26] Tian You-Liang，Ma Jian-Feng，Peng Chang-Gen，Ji Wen-Jiang. Universally composable mechanism for group communication. Chinese Journal of Computers，2012，35(4)：645-653(in Chinese)
(田有亮，马建峰，彭长根，姬文江. 群组通信的通用可组合机制. 计算机学报，2012，35(4)：645-653)

[27] Canetti R，Rabin T. Universal composition with joint state//Proceedings of the CRYPTO 2003. Santa Barbara，USA，2003：265-281

[28] Abdalla M，Catalano D，Chevalier C，et al. Efficient two-party password-based key exchange protocols in the UC framework//Proceedings of the CT-RSA 2008. San Francisco，USA，2008：335-351

[29] Zhang L，Zhang Z F，Hu X X. UC-secure two-server password-based authentication protocol and its applications//Proceedings of the AsiaCCS 2016. Xi'an，China，2016：153-164

[30] Deng M L，Ma J F，Le F L. Universally composable three party password-based key exchange protocol. China Communications，2009，6(3)：150-154

[31] Hu X X，Zhang Z F，Zhang Q H. Universally composable three party password authenticated key exchange with contributiveness. International Journal of Communication Systems，2015，28(6)：1100-1111

[32] Wang W J，Hu L. Efficient and provably secure generic construction of three-party password- based authenticated key exchange protocols//Proceedings of the INDOCRYPT 2006. Kolkata，India，2006：118-132

[33] Groce A，Katz J. A new framework for efficient password-based authenticated key exchange//Proceedings of the 17th ACM Conference on Computer and Communications Security. Chicago，USA，2010：516-525

[34] Katz J，Lindell Y. Introduction to Modern Cryptography. 2nd Edition. American：Chapman & Hall/CRC Press，2014

[35] Boneh D. The decision Diffie-Hellman problem//Proceedings of the Algorithmic number theory 1998. Oregon，USA，1998：48-63

[36] Abdalla M，Benhamouda F，Blazy O，et al. SPHF-friendly non-interactive commitments//Proceedings of the ASIACRYPT 2013. Bangalore，India，2013：214-234

HU Xue-Xian，born in 1982，Ph. D.，lecturer. His current research interests include provably secure protocols and security models.

ZHANG Qi-Hui，born in 1983，Ph. D. candidate，lecturer. Her current research interest is information security.

ZHANG Zhen-Feng，born in 1972，Ph. D.，professor. His current research interests include public key cryptography and lattice-based cryptography.

LIU Feng-Mei，born in 1974，Ph. D.，professor. Her current research interests include cryptography theory and application.

Background

This work is supported by the National Basic Research and Program (973 Program) of China (Grant Nos. 2013CB338003, 2012CB315905), the National Natural Science Foundation of China (Grant Nos. 61502527, U1536205, 61379150, 61572485), the China Postdoctoral Science Foundation Funded Project (Grant No. 2014M552524), and the Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-14-004).

Password-authenticated key exchange (PAKE) is an important type of key exchange, which allows parties to authenticate each other and establish a high-entropy key based on shared low-entropy credential called passwords. Because of their convenience, PAKE protocols have been extensively explored and widely standardized in recent years.

A gateway-oriented password authenticated key exchange (GPAKE) is a special kind of three-party PAKE protocol among a client, a gateway, and an authentication server. The aim of the protocol is to exchange an authenticated session key between the client and the gateway with the help of the authentication server, where the authentication is conducted by means of a low-entropy password. The password is known to both the client and the server, but not to the gateway. With the incensement of protocol's participants, more security properties and goals should be considered when GPAKE protocols are analyzed and designed. Indeed, much research focus on the problem of extended the existing security models to contain some new security goals.

However, almost all existing GPAKE protocols with provable security are analyzed in variants of the BPR model and the ROR model. These game-based models restrict attention to a "stand-alone" setting, in which only the instances of a single protocol are considered in isolation, whereas no other protocols are allowed to be executed in the same network at the same time. As pointed out by Canetti, when placing the protocols in a more complex context, security can no longer be guaranteed by these stand-alone models. Some progress has been achieved in respect to UC-secure PAKE protocols during the last decade. Nevertheless, little, if any, effort has been made in strengthening GPAKE with UC security.

To overcome this deficiency, we consider the security definition of GPAKE in the well-known Universal Composability (UC) framework. We first formulate an ideal functionality for GPAKE, which captures the requirements of semantic security, resistant to attacks mounted by malicious gateway, key privacy with respect to the server, as well as composable security. In addition, we put forward a general construction of GPAKE protocol, and prove its security in the UC framework.