# 标准模型下网关口令认证密钥交换协议的通用框架

魏福山[1) ] 张振峰[2)] 马传贵[1)]

[1)](信息工程大学信息工程学院信息研究系 郑州 450002)

[2)](中国科学院软件研究所信息安全国家重点实验室 北京 100190)

**摘 要** 网关口令认证密钥交换协议允许用户和网关在服务器的协助下建立起一个共享的会话密钥.网关口令协议适用于无线通信环境,如GSM和3GPP等.已有的网关口令认证密钥交换协议大多缺乏严格的安全证明,或者是在随机预言模型下证明安全的.该文采用模块化的设计方法提出了在标准模型下构造网关口令协议的通用框架.通用框架可以实现双向认证并且能够抵抗不可检测在线字典攻击,因此具有更强的安全性.利用DDH假设、二次剩余假设和$N$次剩余假设对通用框架进行实例化可以得到不同的标准模型下可证明安全的网关口令协议.

**关键词** 口令认证;网关;平滑投射Hash函数;标准模型

**中图法分类号** TP309 **DOI号**: 10.3724/SP.J.1016.2012.01833

# A Framework for Gateway-Oriented Password-Authenticated Key Exchange in the Standard Model

WEI Fu-Shan[1)] ZHANG Zhen-Feng[2)] MA Chuan-Gui[1)]

[1)](*Department of Information Research, Institute of Information Engineering, Information Engineering University, Zhengzhou* 450002)

[2)](*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

**Abstract** Protocols for gateway-oriented password-based authenticated key exchange (GPAKE) allow a client and a gateway to establish a common session key with the help of an authentication server. GPAKE protocols are suitable for mobile communication environments such as GSM and 3GPP. To date, only a few GPAKE protocols are known. Most of them are either proven secure in the random oracle model or only have heuristic security arguments. In this paper, we use a modular approach to propose a general framework for constructing GPAKE protocols in the standard model. Our framework is more secure than related GPAKE protocols in the sense that it can achieve mutual authentication and resist undetectable on-line dictionary attacks. Another advantage of the framework is that we can obtain various efficient GPAKE protocols under the DDH assumption, the Quadratic-residuosity assumption and the $N$-residuosity assumption.

**Keywords** password-based authentication; gateway; smooth projective hash function; standard model

## 1 引 言

### 1.1 口令认证密钥交换协议

口令认证密钥交换(PAKE)协议允许通信方仅使用一个低熵、人脑可记忆的口令来建立一个安全的会话密钥.PAKE协议广泛地应用于用户认证和安全通信等实际应用场合,如网上银行和远程用户登录.最早的PAKE协议是由Bellovin和Merritt[1]提出的EKE协议.EKE协议具有广泛的影响力,是

收稿日期:2012-05-14;最终修改稿收到日期:2012-07-30.本课题得到国家"八六三"高技术研究发展计划项目基金(2009AA01Z417)、国家自然科学基金(91118006,61170278)资助.**魏福山**,男,1983年生,博士,讲师,研究方向为安全协议和无线网络的安全认证.E-mail:weifs831020@163.com.**张振峰**,男,1972年生,博士,研究员,博士生导师,研究领域为安全协议的设计与密码系统安全模型的建立.**马传贵**(通信作者),男,1962年生,博士,教授,博士生导师,研究领域为密码协议和无线通信.E-mail:chuanguima@sina.com.

后续很多口令协议研究的基础[2-5].但是上述口令协议只有启发式的安全讨论,缺乏严格的证明.PAKE协议的安全模型是近期才提出的,之后研究者设计了在随机预言模型或者理想加密模型下可证明安全的PAKE协议[6-7].

到目前为止,在标准模型下设计PAKE协议的方法还不多.Katz等人[8]提出了第一个标准模型下可证明安全的PAKE协议,即著名的KOY协议.KOY协议是在共同参考串(Common Reference String)模型下设计的,需要假设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.尽管共同参考串模型比仅用口令来设计协议的假设要强,但是对于实际应用中的PAKE协议来说不算一个缺陷,因为在具体应用中可以将公共参数嵌入到用户芯片中.KOY协议后来被Gennaro和Lindell进行了概括,他们给出了标准模型下PAKE协议的一个GL通用框架[9],KOY协议可以看作GL通用框架的一个特例.几乎所有标准模型下可证明安全的PAKE协议都可以看作是对KOY/GL框架的扩展[10-12].唯一的例外是由Jiang等人[13]利用DDH假设设计的标准模型下安全的PAKE协议.最近,Groce等人对Jiang等人的协议进行了概括和提升,设计了一个效率很高的标准模型下PAKE协议的通用框架[14].

### 1.2 相关工作

在很多实际应用中,服务提供商是由两个实体组成的.一个是与用户直接进行会话的网关,另外一个是用于验证用户身份的后端服务器.为了刻画这种实际的应用场景,Abdalla等人[15]提出了网关口令认证密钥交换(GPAKE)协议的概念.GPAKE协议使得用户和网关在服务器的协助下建立起一个安全的会话密钥.用户和服务器共享一个口令用于认证,但是会话密钥是在用户和网关之间建立的.除了会话密钥的语义安全性之外,GPAKE协议的安全需求还包括针对服务器的密钥私密性和针对恶意网关的口令保护.密钥私密性是指会话密钥对于一个知道所有用户口令的、诚实而好奇的服务器来说是不可区分的;口令保护是指恶意网关通过执行协议不能从服务器端得到用户口令的任何信息.Byun等人[16]后来发现Abdalla等人的GPAKE协议不能抵抗不可检测在线字典攻击.一个恶意的网关可以反复对用户的口令进行猜测并且在服务器端得到验证,直到猜测出正确的口令为止.他们还通过对用户发送的密钥材料进行MAC认证的方法提出了一个改进的协议.但是在2008年,Shim[17]指出Byun等人的改进协议实际上依然不能抵抗不可检测在线字典攻击,Shim通过采用对称加密算法来掩盖口令信息的方法给出了一个改进的S-GPAKE协议.在2010年,Yoon等人[18]指出S-GPAKE协议效率较低并存在设计中的错误.他们提出了一个被称为最优的O-GPAKE协议,但该协议缺乏严格的安全证明.最近,Abdalla等人[19]在最早的GPAKE协议的基础上设计了一个匿名的GPAKE协议,他们提出了一个允许对用户进行腐化的更强的安全模型.但是由于匿名性的原因,该协议依然不能抵抗不可检测在线字典攻击.

### 1.3 我们的工作

本文提出了第一个标准模型下可证明安全的GPAKE协议的通用框架.我们采用了可以实现平滑投射Hash函数的CPA安全的公钥加密算法以及CCA安全的带标签(Labeled)的公钥加密算法.我们的通用框架具有以下三个方面的优势:首先,通用框架是在标准模型下证明安全的,即不需要随机预言或者理想加密的假设;其次,通用框架可以实现双向认证并且可以抵抗不可检测在线字典攻击.Abdalla等人[15,19]认为他们的协议可以通过用户向服务器增加认证消息的方法来抵抗不可检测在线字典攻击.但是,用户发送给服务器的认证消息应该包含一个仅由用户和服务器知道的秘密值,并且不能泄露用户口令的任何信息给网关.在Abdalla等人[15,19]的协议中很难找到满足上述需求的秘密值.尽管文献[17-18]中的协议被声称可以抵抗不可检测在线字典攻击,但是这些协议缺乏严格的安全证明并且效率较低;最后,我们的通用框架采用了一般的密码学组件,如公钥加密体制和平滑投射Hash函数簇等.我们可以采用DDH假设、二次剩余假设和$N$次剩余假设对通用框架进行有效的实例化从而得到不同的GPAKE协议.特别的,如果我们采用CPA安全的ElGamal加密算法和CCA安全的Cramer-Shoup加密算法对通用框架进行实例化,将得到一个标准模型下高效的GPAKE协议.与同类的协议相比,我们的协议在相同的效率下具有更高的安全性.

第2节回顾GPAKE协议的安全模型;第3节介绍通用框架用到的一些基础构件;第4节介绍GPAKE协议的通用框架并且给出框架的安全性证明;第5节采用CPA安全的ElGamal加密算法和CCA安全的Cramer-Shoup加密算法对通用框架进

行实例化，并进一步进行效率比较；第 6 节对全文进行总结.

## 2　安全模型

本节简单介绍由 Abdalla 等人在 2005 年提出的 GPAKE 协议的安全模型，对于安全模型的详细介绍参见文献[15].

### 2.1　安全模型

**协议参与方**. GPAKE 协议的参与者由用户 $C\in\mathcal{C}$、网关 $G\in\mathcal{G}$ 以及服务器 $S\in\mathcal{S}$ 组成. 用 $\mathcal{U}$ 表示所有参与者组成的集合，即集合 $\mathcal{U}=\mathcal{C}\cup\mathcal{G}\cup\mathcal{S}$. 用 $U\in\mathcal{U}$ 表示 GPAKE 协议中的任意一个参与者.

**通信模型**. 在 GPAKE 协议中，通常假设用户和网关之间的通信是不安全的，通信被敌手完全控制，敌手可以对用户和网关之间传递的消息进行窃听、删除、修改和延迟发送等操作. 但是网关和服务器之间的信道是认证的私人信道，即敌手无法窃听网关和服务器之间发送的消息，也不能对网关和服务器之间发送的消息进行修改. 另外，用户无法和服务器直接进行通信，用户和服务器之间的消息必须经过网关进行传递.

**长期密钥**. 每个用户 $C\in\mathcal{C}$ 都拥有一个与服务器共享的用于认证的口令 $pw_C$. 每个服务器 $S\in\mathcal{S}$ 都持有一个口令列表 $pw_S=\langle pw_C\rangle_{C\in S}$，其中每条记录对应一个在服务器 $S$ 处进行注册的用户 $C$ 的口令 $pw_C$. $pw_C$ 和 $pw_S$ 分别称为用户 $C$ 和服务器 $S$ 的长期密钥.

**敌手能力**. 敌手的攻击能力通过预言询问来刻画. 在协议执行的过程中，敌手可以针对某个参与者产生多个并行的会话实例. 用 $U^i$ 来表示用户 $U$ 的第 $i$ 次会话实例. 敌手可以进行的预言询问有以下几种：

(1) $Execute(C^i,G^j)$ 询问. 此询问模拟敌手进行的被动攻击. 其中敌手对用户实例 $C^i$ 和网关实例 $G^j$ 之间进行的一次协议执行过程进行窃听. 对此询问的回答是将本次协议执行过程中用户和网关之间传输的所有消息返回给敌手；

(2) $Send(U^i,m)$ 询问. 此询问模拟敌手进行的主动攻击. 其中敌手伪造一个消息 $m$ 并且将消息 $m$ 发送给用户实例或者网关实例 $U^i$. 敌手将得到实例 $U^i$ 在接收到消息 $m$ 后根据协议描述返回的消息；

(3) $Test(U^i)$ 询问. 此询问不刻画敌手的攻击能力，只是用来衡量参与者实例 $U^i$ 的会话密钥的语义安全性. 如果实例 $U^i$ 的会话密钥没有定义，那么返回一个未定义的符号 $\perp$. 否则，如果 $b=1$ 就将真实的会话密钥返回给敌手，如果 $b=0$ 则返回一个与会话密钥等长的随机数，其中 $b$ 是在攻击游戏开始运行之前选择的随机比特；

(4) $TestPair(C^i,G^j)$ 询问. 此询问不刻画敌手的攻击能力，而是用来定义会话密钥对于服务器的密钥私密性. 如果用户实例 $C^i$ 和网关实例 $G^j$ 之间没有建立共享的会话密钥，那么返回一个未定义的符号 $\perp$. 否则，如果 $b=1$ 就将真实的会话密钥返回给敌手，如果 $b=0$，则返回一个与会话密钥等长的随机数，其中 $b$ 是在攻击游戏开始运行之前选择的随机比特.

### 2.2　安全定义

本小节给出安全模型中的安全性定义. 如果一个实例生成会话密钥并且完成协议运行，则称该实例接受. 我们通过会话标识和伙伴标识来定义伙伴. 一般定义会话标识为协议执行结束后所有消息的级联. 一个实例 $U_1^i$ 的伙伴标识则为其想要与之通信的实例 $U_2^j$.

**定义 1**(伙伴). 用户实例 $C^i$ 和网关实例 $G^j$ 被称为伙伴，如果：(1) $C^i$ 和 $G^j$ 都接受；(2) $C^i$ 和 $G^j$ 有相同的会话标识；(3) $C^i$ 的伙伴标识为 $G^j$，反之亦然；(4) 除了 $C^i$ 和 $G^j$ 外，不存在其它接受实例的伙伴标识为 $C^i$ 或 $G^j$.

敌手只能对新鲜的实例进行 $Test$ 询问，否则敌手可以轻易赢得攻击游戏. 新鲜性定义就是为了防止敌手可以通过平凡的方式赢得攻击游戏.

**定义 2**(新鲜性). 一个用户实例 $C^i$ 或者网关实例 $G^j$ 是新鲜的，如果该实例接受协议运行并且生成了会话密钥.

在 Abdalla 等人的安全模型中有 3 个安全目标，包括语义安全性、密钥私密性和口令保护. 其中会话密钥的语义安全性保证了一个外部敌手不能够区分真实的会话密钥和与会话密钥等长的随机数；针对服务器的密钥私密性要求用户和网关之间建立的会话密钥对于诚实而好奇的服务器是不可区分的；针对网关的口令保护是指恶意网关通过协议运行不能得到用户口令的任何信息. 下面我们分别给出这三个安全目标的严格定义.

考虑一个对 GPAKE 协议 $\mathcal{P}$ 进行攻击的敌手 $\mathcal{A}$，给敌手提供 $Execute$，$Send$ 询问以及对新鲜会话进行多次 $Test$ 询问的能力. 敌手的目标是猜测 $Test$ 询问中所使用的随机比特 $b$. 我们用 $Succ$ 来表示敌

手成功猜测到 $b$ 这一事件.

**定义 3**(语义安全). 当口令是从字典空间 $\mathcal{D}$ 中随机选择的时候,定义敌手 $\mathcal{A}$ 攻破 GPAKE 协议 $\mathcal{P}$ 的语义安全的优势为

$$Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-ror}}(\mathcal{A})=2\cdot Pr[Succ]-1,$$

定义 GPAKE 协议 $\mathcal{P}$ 的语义安全的优势函数为

$$Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-ror}}(t,R)=\max\{Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-ror}}(\mathcal{A})\},$$

上式中的最大值遍历所有计算时间至多为 $t$,消耗的资源(询问不同预言的次数)至多为 $R$ 的敌手.

如果一个 GPAKE 协议 $\mathcal{P}$ 语义安全的优势函数 $Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-ror}}(t,R)$ 至多比 $kn/|\mathcal{D}|$ 大一个可忽略的量,那么称 GPAKE 协议 $\mathcal{P}$ 是语义安全的,其中 $n$ 是敌手进行主动攻击的次数,$|\mathcal{D}|$ 表示字典空间的规模,$k$ 是一个常数. 一般 $k=1$ 是最优的结果,因为每次敌手进行主动攻击至少可以排除一个错误的口令.

考虑一个对 GPAKE 协议 $\mathcal{P}$ 进行攻击的敌手 $\mathcal{A}$,给敌手提供所有用户的口令,*Execute* 询问以及对伙伴会话进行 *TestPair* 询问的能力. 敌手的目标是猜测 *TestPair* 询问中所使用的随机比特 $b$. 我们用 *Succ* 来表示敌手成功猜测到 $b$ 这一事件.

**定义 4**(密钥私密性). 当口令是从字典空间 $\mathcal{D}$ 中随机选择的时候,定义敌手 $\mathcal{A}$ 攻破 GPAKE 协议 $\mathcal{P}$ 的密钥私密性的优势为

$$Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-kp}}(\mathcal{A})=2\cdot Pr[Succ]-1,$$

定义 GPAKE 协议 $\mathcal{P}$ 的密钥私密性的优势函数为

$$Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-kp}}(t,R)=\max\{Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-kp}}(\mathcal{A})\},$$

上式中的最大值遍历所有计算时间至多为 $t$,消耗的资源(询问不同预言的次数)至多为 $R$ 的敌手.

称一个 GPAKE 协议 $\mathcal{P}$ 实现了密钥私密性,如果其密钥私密性安全的优势函数 $Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-kp}}(t,R)$ 是相对于安全参数的一个可忽略函数.

考虑一个恶意的网关 $\mathcal{A}$ 猜测用户的口令,然后通过与服务器执行协议来验证口令是否正确. 如果一个错误的猜测没有被服务器检测到,则认为恶意的网关 $\mathcal{A}$ 成功. 我们用 $Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-uoda}}(\mathcal{A})$ 来表示恶意的网关 $\mathcal{A}$ 成功的优势.

**定义 5**(口令保护). 称一个 GPAKE 协议 $\mathcal{P}$ 实现了对恶意网关的口令保护,如果恶意的网关 $\mathcal{A}$ 成功的优势 $Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-uoda}}(\mathcal{A})$ 至多比 $kn/|\mathcal{D}|$ 大一个可忽略的量,其中 $n$ 是敌手进行主动攻击的次数,$|\mathcal{D}|$ 表示字典空间的规模,$k$ 是一个常数.

## 3 密码学组件

本节介绍在通用框架设计和证明中需要用到的密码学组件. 首先给出带标签的公钥加密体制的定义,然后介绍平滑投射 Hash 函数的概念.

### 3.1 带标签的公钥加密体制

带标签的加密体制(Labeled Encryption)最初是由 ISO18033-2 标准正式提出的[20],与通常的加密体制的定义不同的地方在于,在带标签的加密体制中,加密算法和解密算法都有一个额外的被称为标签的参数,并且解密算法只有在输入的标签跟加密时的标签相同时才能正确解密.

一个带标签的公钥加密体制 $LPKE=(LKG,Enc,Dec)$ 一般由以下 3 个算法组成:参数生成算法 $LKG$:输入安全参数 $n$,通过参数生成算法 $LKG(1^n)$ 产生带标签的公钥加密体制的公私钥对 $(pk,sk)$;加密算法 $Enc$:输入为消息 $m$,标签 $l$,加密时的公钥 $pk$ 以及随机输入 $r$,通过加密算法 $c=Enc_{pk}^{l}(m;r)$ 产生对应的密文 $c$;解密算法 $Dec$:输入为密文 $c$,标签 $l$ 以及解密的私钥 $sk$,通过解密算法 $m=Dec_{sk}^{l}(c)$ 恢复出明文 $m$.

下面给出带标签的公钥加密体制的不可区分 CCA 安全性的定义. 定义带标签的公钥加密体制不可区分 CCA 安全的攻击游戏与定义一般公钥加密体制不可区分 CCA 安全的攻击游戏类似. 攻击游戏开始,首先对敌手进行第 1 阶段的解密培训,此时敌手可以选择密文/标签对 $(c,l)$ 要求解密预言机进行解密服务. 在挑战密文生成阶段,当敌手进行挑战密文询问的时候,除了要输入两个等长的消息 $(m_0,m_1)$ 外,还需要提供一个标签 $l$ 作为额外的输入. 当敌手接收到挑战密文 $C^*$ 的时候,需要判断挑战密文 $C^*$ 是由消息 $m_0$ 和标签 $l$ 加密产生,还是由消息 $m_1$ 和标签 $l$ 加密产生的. 此时敌手可以继续进行第 2 阶段的解密培训,敌手除了密文/标签对 $(c^*,l)$ 外,可以对任意的密文/标签对进行解密询问. 最终,敌手输出其对挑战密文的猜测. 敌手的优势函数的定义与普通的公钥加密体制中敌手的优势定义相同. 如果敌手的优势是关于安全参数的可忽略的函数,那么我们说带标签的公钥加密体制是不可区分 CCA 安全的,简称为 CCA 安全. 对于带标签的公钥加密体制的详细定义可参见文献[20-21].

### 3.2 平滑投射 Hash 函数簇

平滑投射 Hash 函数簇可以看作是有两类密钥的 Hash 函数,其中一类密钥称为全局密钥,可以用来计算平滑投射函数整个定义域上所有输入的对应输出,还有一类密钥称为投射密钥,由全局密钥通过投射函数计算得到,投射密钥只能计算平滑投射函

数定义域的一个子集对应的函数值. 平滑投射 Hash 函数之所以被广泛应用于口令协议的设计当中，主要原因是对于投射密钥能够计算的那个特定子集上面的输出，可以通过全局密钥和投射密钥两种不同的方式来计算出相同的函数值，这样使得协议执行的双方在实现认证的同时还能产生共同的秘密值作为会话密钥. 而对于特定子集之外的函数值，仅仅知道投射密钥不会泄露该函数值的任何信息. 实际上，投射密钥和特定子集之外的函数值是统计独立的.

现在给出基于 CPA 安全的公钥加密体制构造的平滑投射 Hash 函数簇的严格定义以及相应的性质. 给定一个 CPA 安全的公钥加密体制$(Gen, Enc, Dec)$和一个消息空间$\mathcal{D}$(对应于通用框架中的口令空间). 设$(pk, sk)$是由密钥生成函数$Gen(1^n)$在输入安全参数 $n$ 时产生的，我们用 $\Omega$ 表示对于公钥 $pk$ 的有效的密文集合. 定义集合 $X=\{(\omega,m)\mid \omega\in\Omega; m\in\mathcal{D}\}$，集合 $L_m=\{(\omega,m)\mid Dec_{sk}(\omega)=m\}\subset X$ 以及集合 $L=\bigcup_{m\in\mathcal{D}} L_m$. 注意，对于每个密文 $\omega$ 至多存在一个消息 $m\in\mathcal{D}$ 使得$(\omega,m)\in L$.

一个平滑投射 Hash 函数是由一个有效的采样算法来定义的. 在给定公钥 $pk$ 的情况下，输出以下的函数组$(K,\mathcal{H}=\{H_k: X\to(0,1)^n\}_{k\in K}, S, \alpha: K\times\Omega\to S)$满足：

(1) 存在有效的算法可以对密钥空间 $K$ 进行均匀采样 $k\in K$；对于给定的全局密钥 $k\in K$ 和定义域中的元素 $x\in X$，存在有效的算法计算平滑投射函数的输出 $H_k(x)$；给定任意的全局密钥 $k\in K$ 和密文空间中的任意元素 $\omega\in\Omega$，存在有效的算法计算投射密钥 $\alpha(k,\omega)$.

(2) 对于 $x=(\omega,m)\in L$，函数值 $H_k(x)$ 完全由 $\alpha(k,\omega)$ 确定. 即存在一个有效的算法 $H'$ 在输入 $s=\alpha(k,\omega)$ 和 $\bar{x}=(\omega,m,r)$ 满足 $H'(s,\bar{x})=H_k(x)$，其中 $r$ 是对消息 $m$ 进行加密时的随机输入，即 $\omega=Enc_{pk}(m;r)$.

(3) 对于任意的 $x=(\omega,m)\in X\backslash L$，下面的两个分布$\{k\leftarrow K; s=\alpha(k,\omega), v\leftarrow\{0,1\}^n: (s,v)\}$以及$\{k\leftarrow K; s=\alpha(k,\omega): (s, H_k(x))\}$是统计不可区分的.

上面定义中的第 2 条性质被称为平滑投射 Hash 函数的正确性，第 3 条性质一般被称为平滑性. 对于平滑投射 Hash 函数的详细定义可参见文献[14].

# 4　网关口令协议的通用框架

本节给出网关口令协议的通用框架，并对其安全性进行证明.

## 4.1　通用框架描述

GPAKE 协议的通用框架是在共同参考串模型下设计的. 在共同参考串模型中，假设所有的用户都可以获取从一个预先给定的分布中选择的公共参数. 在我们的构造中用到了一个 CPA 安全的公钥加密体制 $\Sigma=(Gen, Enc, Dec)$ 和一个 CCA 安全的带标签的公钥加密体制 $\Sigma'=(Gen', Enc', Dec')$，并且要求可以通过 CPA 安全的加密体制 $\Sigma$ 定义平滑投射 Hash 函数簇$(K,\mathcal{H}=\{H_k: X\to(0,1)^n\}_{k\in K}, S, \alpha: K\times\Omega\to S)$. 设安全参数为 $n$，设 $G_q$ 是一个阶为大素数 $q$ 的循环群，$g$ 为 $G_q$ 的一个生成元. 我们设计的 GPAKE 协议的通用框架中所使用的共同参考串的公共参数包括两个加密体制对应的公钥 $pk$，$pk'$ 以及对群 $G_q$ 的描述$(G_q, g, q)$. 需要说明的是，在共同参考串模型中，任何人都不知道加密体制的公钥 $pk, pk'$ 对应的私钥 $sk, sk'$.

GPAKE 协议的通用框架的参与者由用户、网关和服务器组成. 假设用户和服务器之间共享一个从口令字典空间$\mathcal{D}$中选择的口令 $pw$，并且网关和服务器之间存在认证通道. GPAKE 协议的通用框架的描述在图 1 中给出，具体的执行步骤如下：

1. 用户 $C$ 选择一个随机数 $x\in Z_q^*$ 并计算 $X=g^x$. 然后用户从$\{0,1\}^n$中选择一个随机数 $r$，计算利用 CPA 安全的加密体制 $\Sigma$ 对口令 $pw$ 进行加密的密文 $\omega=Enc_{pk}(pw;r)$，最后发送消息$(C, X, \omega)$给网关 $G$.

2. 网关 $G$ 接收到消息$(C, X, \omega)$后，随机选择 $y\in Z_q^*$ 并且计算 $Y=g^y$，然后将 $Y$ 连同接收到的消息一起发送给服务器 $S$.

3. 服务器 $S$ 接收到网关发送的消息$(C, X, Y, \omega)$后，首先随机选择全局密钥 $k\in K$，并计算投射密钥 $s=\alpha(k,\omega)$. 然后服务器利用口令 $pw$ 和全局密钥 $k$ 计算平滑投射 Hash 函数的值 $H_k(\omega, pw)$，并且将结果分为三个随机比特串 $r'\|\tau_1\|\tau_2$，其中 $\tau_1$ 和 $\tau_2$ 的长度至少为 $n$，并且 $r'$ 有足够的长度作为 CCA 加密体制 $\Sigma'$ 的随机输入. 服务器定义标签 $label=C\|G\|S\|\omega\|s\|X\|Y$ 并且用带标签的加密体制计算对口令 $pw$ 加密的密文 $\omega'=Enc_{pk'}^{label}(pw;r')$，其中 $r'$ 是随机输入. 最后，服务器发送消息$(s, \omega', \tau_1)$给网关.

4. 网关接收到消息$(s, \omega', \tau_1)$后，储存 $\tau_1$ 用来验证用户的合法性，然后将消息$(G, s, \omega', Y)$发送给用户.

5. 用户 $C$ 接收到消息$(G, s, \omega', Y)$后，首先通过投射密钥 $s$，口令 $pw$ 以及在第一轮生成密文 $\omega$ 时的随机输入 $r$ 来计算平滑投射 Hash 函数的值，即用户计算 $r'^*\|\tau_1^*\|\tau_2^*=H'(s,\omega,pw,r)$，然后验证 $\omega'$ 是否等于 $Enc_{pk'}^{label}(pw;r'^*)$. 如果验证通过，那么用户接受协议并且计算会话密钥 $K=Y^x=g^{xy}$；否则，用户终止协议运行. 最后，用户发送

$(C,\tau_1^*,\tau_2^*)$给网关.

6. 网关接收到消息$(C,\tau_1^*,\tau_2^*)$后,首先验证$\tau_1$是否等于$\tau_1^*$.如果验证通过,则说明用户是合法的,那么网关接受协议运行并生成会话密钥$K=X^y=g^{xy}$;否则,网关拒绝协议运行并终止.最后,网关发送消息$(C,\tau_2^*)$给服务器.服务器通过消息$(C,\tau_2^*)$来检测恶意网关进行的在线字典攻击.具体地,服务器验证$\tau_2$是否等于$\tau_2^*$.如果验证通过,说明接入认证请求确实是一个诚实的用户发送的;否则,接入请求很可能来自一个恶意网关对用户的在线仿冒攻击,服务器将采取进一步的措施以保护用户口令.

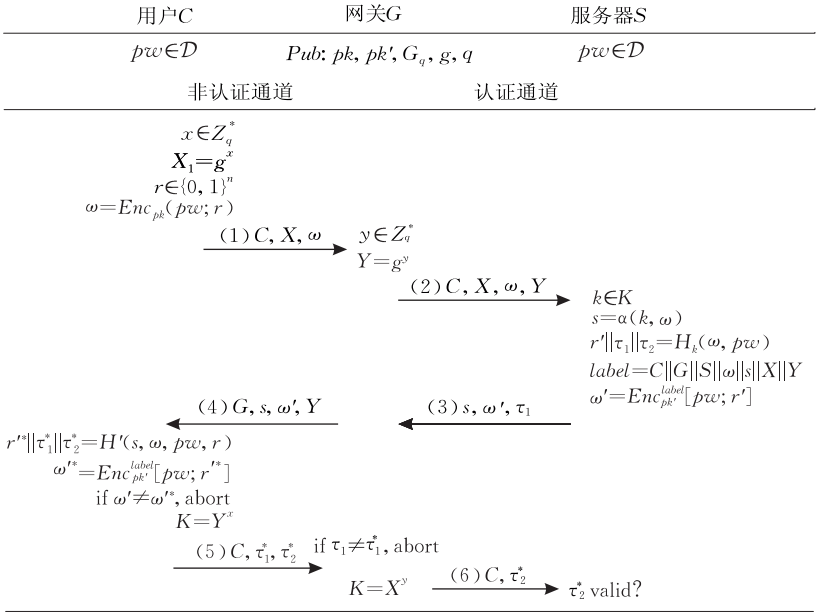


图 1 GPAKE 协议的通用框架

## 4.2 安全性证明

本小节给出对 GPAKE 协议的通用框架的安全性证明,证明主要基于 DDH 假设、框架中所使用的公钥加密体制 $\Sigma$ 的 CPA 安全性以及公钥加密体制 $\Sigma'$ 的 CCA 安全性.下面给出 DDH 假设的定义.

**DDH 假设**. 假设$G_q$为阶为素数$q$的循环群,$g$为$G_q$的一个生成元.假设$\mathcal{A}_{ddh}$是一个概率多项式时间的敌手,模拟者首先随机选择$u,v,w\in Z_q$,并且计算$U=g^u$,$V=g^v$和$W=g^w$,然后随机选择一个比特$b\in\{0,1\}$,如果$b=1$,那么将$(g^u,g^v,g^{uv})$给敌手,否则将$(g^u,g^v,g^w)$给敌手.敌手需要猜测随机比特$b$的值,如果敌手猜测正确就认为敌手成功,记此事件为$Succ$.定义敌手的优势为$Adv(\mathcal{A}_{ddh})=|2\cdot Pr[Succ]-1|$.如果对于任意的概率多项式敌手,上述优势都是可忽略的,那么称循环群$G_q$中DDH假设成立.

**定理 1**(语义安全). 假设$\mathcal{A}$是一个运行时间为$t$,并且进行了$q_{send}$次$Send$询问的概率多项式敌手.如果DDH假设在群$G_q$中成立、公钥加密体制$\Sigma$是CPA安全的并且公钥加密体制$\Sigma'$是CCA安全的,那么敌手$\mathcal{A}$破坏GPAKE协议通用框架语义安全的优势至多为

$$Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-ror}}(\mathcal{A})\leq\frac{q_{Send}}{|\mathcal{D}|}+neg(n),$$

其中$neg(n)$表示关于安全参数$n$的一个可忽略函数.

证明. 我们定义一系列混合实验.从每一个实验开始,我们首先用随机数替代被动攻击中的会话密钥,然后修改主动攻击中的会话,使得敌手猜测口令错误的主动会话都会被拒绝接受.到最后一个实验,所有的会话密钥完全随机并且与用户的口令完全独立,因此敌手无法区分真实的会话密钥和与会话密钥等长的随机数,也无法获得任何关于用户口令的任何信息.我们总共定义了11个混合实验,我们用$P_0,P_1,\cdots,P_{10}$来表示这些混合实验,用事件$Success$表示敌手正确猜测出了在$Test$询问中所使用的随机数$b$,并且用$Adv(\mathcal{A},P_i)$表示敌手$\mathcal{A}$在第$i$个混合实验中的优势.

实验$P_0$. 此实验模拟在标准模型下的真实协议运行.在实验中敌手$\mathcal{A}$可以多次访问$Execute$、$Send$和$Test$询问.根据定义有

$$Adv(\mathcal{A})=Adv(\mathcal{A},P_0).$$

实验$P_1$. 在这个实验中,我们修改对$Execute$询问的模拟.对于敌手进行的$Execute(C^i,G^j)$询问,我们计算$\omega=Enc_{pk}(pw_0;r)$,其中$pw_0$是不在口

令空间中的虚假口令. 相应的，在用户端计算 $r'^{*}$，$\tau_1^{*}$ 和 $\tau_2^{*}$ 的时候，直接将这几个值取为由服务器计算的 $r'$，$\tau_1$ 和 $\tau_2$ 的值. 其余的模拟与上一个实验完全相同. 显然，这个实验将被动会话中用户端对口令加密的密文替换为对一个虚假口令加密的密文. 实验 $P_1$ 和实验 $P_0$ 的差别至多是敌手攻破公钥加密体制 $\Sigma$ 的 CPA 安全性的优势.

给定一个可以区分实验 $P_1$ 和实验 $P_0$ 的敌手 $\mathcal{A}$，我们现在来构造一个可以攻击公钥加密体制 $\Sigma$ 的 CPA 安全性的概率多项式敌手 $\mathcal{B}$. 给定公钥 $pk$，敌手 $\mathcal{B}$ 选择其余的公开参数并为所有的用户选择口令，然后为敌手 $\mathcal{A}$ 模拟整个实验. 对于 $Execute(C^i,G^j)$ 询问，敌手 $\mathcal{B}$ 用口令 $pw$ 和虚假口令 $pw_0$ 作为两条消息进行挑战密文的询问. 当敌手 $\mathcal{B}$ 接收到挑战密文 $\omega$，就将挑战密文添加到用户发送给网关的第一条消息中，其余的模拟跟实验 $P_1$ 中完全相同. 在实验结束时，如果敌手 $\mathcal{A}$ 认为他在实验 $P_0$ 中，那么敌手 $\mathcal{B}$ 就判定挑战密文 $\omega$ 是对口令 $pw$ 的加密；反之挑战密文则是对虚假口令 $pw_0$ 的加密. 敌手 $\mathcal{B}$ 攻击公钥加密体制 $\Sigma$ 的 CPA 安全性的优势与敌手 $\mathcal{A}$ 区分实验 $P_1$ 和实验 $P_0$ 的概率完全相同，由公钥加密体制 $\Sigma$ 的 CPA 安全性，我们有

$$|Adv(\mathcal{A},P_1)-Adv(\mathcal{A},P_0)|\leq neg(n).$$

实验 $P_2$. 在这个实验中，我们继续修改对 $Execute$ 询问的模拟. 服务器在接收到用户 $C$ 发送的消息 $(C,X,Y,\omega)$ 后，随机选择 $k\in K$ 并计算 $s=\alpha(k,\omega)$，但是服务器随机选择适当长度的比特串作为 $r'$、$\tau_1$ 和 $\tau_2$ 的值. 相应地，根据模拟规则将用户端的 $r'^{*}$、$\tau_1^{*}$ 和 $\tau_2^{*}$ 的值直接取为由服务器选择的 $r'$、$\tau_1$ 和 $\tau_2$ 的值. 其余的模拟和上一个实验相同. 由平滑投射 Hash 函数的平滑性易知实验 $P_2$ 和实验 $P_1$ 的差别至多是关于安全参数 $n$ 的一个可忽略函数. 注意到我们在计算 $\omega$ 的时候用的是虚假口令 $pw_0$，因此 $(\omega,pw_0)\notin L$，根据平滑性可知，即使敌手知道投射密钥 $s$，平滑投射 Hash 函数的输出 $H_k(\omega,pw_0)$ 与其值域中的均匀分布仍然是统计不可区分的. 因此，我们有

$$|Adv(\mathcal{A},P_2)-Adv(\mathcal{A},P_1)|\leq neg(n).$$

实验 $P_3$. 在这个实验中，我们继续修改对 $Execute$ 询问的模拟. 当服务器计算密文 $\omega'$ 的时候，我们令 $\omega'=Enc_{pk'}^{label}(pw_0;r')$，其中所使用的随机输入 $r'$ 是根据实验 $P_2$ 的模拟规则随机选择的. 同时，我们取消用户端对 $\omega'$ 的验证，要求用户直接接受协议运行并产生会话密钥. 实验 $P_3$ 和实验 $P_2$ 的差别至多是敌手攻破公钥加密体制 $\Sigma'$ 的 CCA 安全性的优势. 实际上，我们这里用到的只是公钥加密体制 $\Sigma'$ 的 CPA 安全性. 通过跟实验 $P_1$ 类似的分析可以知道：

$$|Adv(\mathcal{A},P_3)-Adv(\mathcal{A},P_2)|\leq neg(n).$$

实验 $P_4$. 在这个实验中，我们最后一次修改对 $Execute$ 询问的模拟. 当我们计算 $Execute$ 询问的会话密钥的时候，直接从 $G_q$ 中随机选择一个元素 $K$，而不是通过 $K=X^y$ 或者 $K=Y^x$ 的方式计算. 实验 $P_5$ 和实验 $P_4$ 中敌手优势的差距跟攻破 DDH 假设的优势相同.

现在我们给出上面结论的证明. 给定一个 DDH 实例 $(U,V,W)$，我们为了模拟对 $Execute(C^i,G^j)$ 询问的回答，首先随机选择 $a_1,a_2,b_1,b_2\in Z_q^{*}$，然后在模拟 $Execute(C^i,G^j)$ 询问的时候我们令 $X=U^{a_1}g^{a_2}$ 以及 $Y=V^{b_1}g^{b_2}$，其余的模拟都跟实验 $P_3$ 完全相同. 最后，我们定义会话密钥为 $K=W^{a_1b_1}\cdot U^{a_1b_2}\cdot V^{a_2b_1}\cdot g^{a_2b_2}$. 显然，如果 $(U,V,W)$ 是一个 Diffie-Hellman 三元组，那么模拟的规则与实验 $P_3$ 完全相同；如果 $(U,V,W)$ 是一个随机的三元组，那么模拟的规则与实验 $P_4$ 一致. 如果存在敌手可以区分实验 $P_4$ 和实验 $P_3$，那么我们可以以相同的优势攻破 DDH 假设，因此我们有

$$|Adv(\mathcal{A},P_4)-Adv(\mathcal{A},P_3)|\leq neg(n).$$

注意在实验 $P_4$ 中，对于 $Execute$ 询问产生的会话密钥以及协议的消息跟口令完全无关，因此敌手不可能通过 $Execute$ 询问得到口令的任何信息，同时由于会话密钥是随机选择的，敌手在猜测由 $Execute$ 询问产生的会话密钥的时候也不会有任何优势.

实验 $P_5$. 从这个实验开始，我们修改对 $Send$ 询问的模拟. 为了符号上的方便，我们令 $Send_0(C^i,G^j)$ 表示要求用户实例 $C^i$ 开始执行协议的初始激活消息；令 $Send_1(G^j,C\|X\|\omega)$ 表示用户发送给网关实例 $G^j$ 的第一条消息；令 $Send_2(C^i,G\|s\|\omega'\|Y)$ 表示协议中网关接收到消息 $C\|X\|\omega$ 后发送给用户实例 $C^i$ 的消息；令 $Send_3(G^j,C\|\tau_1^{*}\|\tau_2^{*})$ 表示用户发给网关实例 $G^j$ 的最后一条消息. 另外如果一条消息是由诚实的参与者生成的，那么我们说该消息是由实例生成的；否则，我们称消息是由敌手产生的.

在实验 $P_5$ 开始，当我们在产生 CRS 参数中公钥加密体制 $\Sigma$ 和 $\Sigma'$ 的公钥 $pk$，$pk'$ 的时候，我们记录其对应的私钥 $sk$，$sk'$.

当敌手产生的消息$G\|s\|\omega'\|Y$并进行$Send_2(C^i, G\|s\|\omega'\|Y)$询问时，假设$C\|X\|\omega$是对于$Send_0(C^i, G^j)$询问的回答，我们首先检查$s\|\omega'$是否是由某一个实例产生的，如果不是则利用私钥$sk'$和标签$label=C\|G\|S\|\omega\|s\|X\|Y$对敌手发送的密文$\omega'$进行解密，看解密得到的消息是否等于$pw$. 如果不相等，那么拒绝协议，并且停止用户实例$C^i$的运行；如果相等，那么我们停止协议运行并且宣布敌手成功. 实验$P_5$和实验$P_4$唯一的区别在于当敌手伪造的消息$G\|s\|\omega'\|Y$中的密文$\omega'$可以被解密为$pw$的情况，在这种情况下我们认为敌手攻破了协议的语义安全性，所以敌手的攻击优势增大. 因此，我们有

$$|Adv(\mathcal{A}, P_4)| \leq Adv(\mathcal{A}, P_5).$$

实验$P_6$. 在这个实验中，我们修改对$Send_0$和$Send_2$询问的模拟. 对于敌手发送的$Send_0(C^i, G^j)$询问，我们现在计算$\omega=Enc_{pk}(pw_0; r)$，其中$pw_0$是不在口令空间中的虚假口令. 为了保证敌手视图的一致性，对于一个$Send_2(C^i, G\|s\|\omega'\|Y)$询问，如果确实存在一个网关实例$G^j$跟$Send_1(G^j, C\|X\|\omega)$询问匹配，也就是说$G\|s\|\omega'\|Y$是由网关实例$G^j$在接收到消息$C\|X\|\omega$后产生的，那么我们要求用户实例$C^i$在不对消息$G\|s\|\omega'\|Y$进行验证的情况下就接受，并且将$r'^*\|\tau_1^*\|\tau_2^*$定义为网关实例$G^j$在接收到$C\|X\|\omega$后计算出的$r'\|\tau_1\|\tau_2$. 敌手区分实验$P_6$和实验$P_5$的优势和攻破公钥加密体制$\Sigma$的CPA安全性的优势相同. 从实验$P_1$进行的类似分析可知：

$$|Adv(\mathcal{A}, P_6) - Adv(\mathcal{A}, P_5)| \leq neg(n).$$

实验$P_7$. 在这个实验中，我们修改对$Send_1$询问的模拟进行一个简单的改动. 对于敌手产生的$Send_1(G^j, C\|X\|\omega)$询问，注意到从实验$P_5$开始我们就记录了私钥$sk, sk'$，因此可以用公钥加密体制$\Sigma$对应于公钥$pk$的私钥$sk$对$\omega$进行解密，如果解密的明文是$pw$，那么我们停止模拟并且宣布敌手成功；如果不是，那么按照上一个实验的模拟规则进行. 除此之外，所有的模拟和实验$P_6$完全一致. 显然，在这个实验里面，我们只是增加敌手成功的方式，因此有

$$|Adv(\mathcal{A}, P_6)| \leq Adv(\mathcal{A}, P_7).$$

实验$P_8$. 在这个实验中，我们继续修改对$Send_1$询问的模拟. 对于敌手产生的$Send_1(G^j, C\|X\|\omega)$询问，我们用公钥加密体制$\Sigma$对应于公钥$pk$的私钥$sk$对$\omega$进行解密，如果解密的明文是$pw$，那么我们停止模拟并且宣布敌手成功；如果解密后的明文不是$pw$，那么我们随机选择适当长度的比特串作为$r'$、$\tau_1$和$\tau_2$的值. 特别的，如果敌手继续发送了$Send_3(G^j, C\|\tau_1^*\|\tau_2^*)$询问，有$\tau_1^*=\tau_1$并且$\tau_2^*=\tau_2$，那么网关实例$G^j$接受协议运行并且生成会话密钥$K$. 实验$P_8$和实验$P_7$的差别至多是关于安全参数$n$的一个可忽略函数. 注意到敌手计算$\omega$的时候对口令猜测错误，根据平滑性可知，即使敌手知道投射密钥$s$，平滑投射Hash函数的输出与其值域中的均匀分布仍然是统计不可区分的. 因此，我们有

$$|Adv(\mathcal{A}, P_8) - Adv(\mathcal{A}, P_7)| \leq neg(n).$$

实验$P_9$. 在这个实验中，我们最后一次修改对$Send_1$询问的模拟. 对于敌手发送的$Send_1(G^j, C\|X\|\omega)$询问，当计算密文$\omega'$的时候，我们令$\omega'=Enc_{pk'}^{label}(pw_0; r')$，其中所使用的随机输入$r'$是根据实验$P_8$的模拟规则随机选择的. 敌手在实验$P_9$和实验$P_8$中的优势之差至多为敌手攻破公钥加密体制$\Pi'$的CCA安全性的优势.

如果存在敌手$\mathcal{A}$可以区分实验$P_9$和实验$P_8$，那么我们可以构造一个概率多项式敌手$\mathcal{B}$攻击公钥加密体制$\Pi'$的CCA安全性. 给定公钥$pk'$，敌手$\mathcal{B}$按照实验$P_8$中的模拟规则选择所有的口令和安全参数，并为敌手$\mathcal{A}$模拟整个实验运行. 注意，这里敌手$\mathcal{B}$不知道公钥加密体制$\Pi'$的公钥$pk'$对应的私钥$sk'$，但是知道公钥加密体制$\Pi$的公钥$pk$对应的私钥$sk$. 与实验$P_8$中的模拟规则不同的地方在于，当接收到敌手发送的$Send_1(G^j, C\|X\|\omega)$询问，当计算密文$\omega'$的时候，敌手$\mathcal{B}$令$label=C\|G\|S\|\omega\|s\|X\|Y$，并产生一个虚假的口令$pw_0$，然后将口令$pw$和虚假的口令$pw_0$作为挑战的消息连同$label$一起发送给加密体制的预言机. 当敌手$\mathcal{B}$收到加密预言机返回的挑战密文$\omega'$后，就把$\omega'$加入到返回给敌手$\mathcal{A}$的消息中. 为了使模拟完美，敌手$\mathcal{B}$需要判断敌手$\mathcal{A}$是否通过询问$Send_1$或者$Send_2$已经成功. 敌手$\mathcal{B}$对于$Send_1$询问的判断很容易，因为敌手$\mathcal{B}$知道私钥$sk$. 但是对于$Send_2$询问需要借助于公钥加密体制$\Sigma'$中的解密预言机来判断敌手$\mathcal{A}$是否成功. 容易验证敌手$\mathcal{B}$不需要向解密预言机询问标签/密文对$(label, \omega')$的解密服务，因此敌手$\mathcal{B}$可以完美模拟整个实验. 在实验的最后，如果敌手$\mathcal{A}$认为其处在实验$P_8$中，那么敌手$\mathcal{B}$就判定挑战密文$\omega'$是对口令$pw$的加密；反之，如果敌手$\mathcal{A}$认为其处在实验$P_9$中，那么敌手$\mathcal{B}$就判定挑战密文$\omega'$是对虚假口令$pw_0$的加密. 这样敌手$\mathcal{B}$可以攻破公钥加密体制$\Sigma'$的CCA安全性，因此我们有

$$|Adv(\mathcal{A}, P_9) - Adv(\mathcal{A}, P_8)| \leq neg(n).$$

实验 $P_{10}$. 在最后的实验中，我们考虑敌手通过 *Send* 询问进行的被动攻击，也就是说敌手虽然进行了 *Send* 询问，但是只是诚实传递消息，没有对消息进行任何改动. 对于这样的会话，模拟的规则和实验 $P_5$ 中模拟 *Execute* 询问产生的被动会话相同. 跟实验 $P_4$ 中的分析类似，我们有

$$|Adv(\mathcal{A},P_{10})-Adv(\mathcal{A},P_9)|\leq neg(n).$$

现在我们考虑敌手在实验 $P_{10}$ 中成功的几种可能的方式：

情况 1. 对于敌手产生的消息进行的询问 $Send_1(G^j,C\|X\|\omega)$，敌手伪造的密文 $\omega$ 可以解密得到正确的口令 $pw$.

情况 2. 对于敌手产生的消息进行的询问 $Send_2(C^i,G\|s\|\omega'\|Y)$，敌手伪造的密文 $\omega'$ 可以解密得到正确的口令 $pw$.

情况 3. 对于敌手进行的询问 $Send_3(G^j,C\|\tau_1^*\|\tau_2^*)$，有 $\tau_1=\tau_1^*$ 以及 $\tau_2=\tau_2^*$，但是 $\tau_1^*$ 和 $\tau_2^*$ 不是由与网关实例 $G^j$ 匹配的用户实例产生的.

情况 4. 敌手成功猜测到 *Test* 询问中使用的随机比特 $b$.

情况 3 发生的概率是可忽略的，因为 $\tau_1$ 和 $\tau_2$ 是随机选择的并且与敌手的视图完全独立. 我们用事件 *PwdGuess* 表示情况 1 或者情况 2 发生. 由于敌手的视图与所有的口令都是独立的，直到情况 1 或者情况 2 发生，因此我们有

$$Pr[PwdGuess]\leq\frac{q_{Send}}{|\mathcal{D}|}.$$

如果事件 *PwdGuess* 不发生，那么敌手 $\mathcal{A}$ 只能通过情况 4 成功. 但是所有的会话密钥都是随机选择的，并且与敌手的视图完全独立，因此敌手通过情况 4 成功的概率是 $\frac{1}{2}$. 忽略情况 3，我们有

$$\begin{aligned}Pr[Success]&\leq Pr[Success\wedge PwdGuess]+\\&\quad Pr[Success\wedge\overline{PwdGuess}]\\&\leq Pr[PwdGuess]+Pr[Success|\overline{PwdGuess}]\cdot\\&\quad(1-Pr[PwdGuess])\\&=\frac{1}{2}+\frac{1}{2}\cdot Pr[PwdGuess]\\&\leq\frac{1}{2}+\frac{1}{2}\cdot\frac{q_{Send}}{|\mathcal{D}|}.\end{aligned}$$

综上，定理 1 得证. 证毕.

**定理 2**(密钥私密性). 假设 $\mathcal{A}$ 是一个运行时间为 $t$，并且进行了 $q_{Execute}$ 次 *Execute* 询问的概率多项式敌手. 如果 DDH 假设在群 $G_q$ 中成立，那么敌手 $\mathcal{A}$ 破坏 GPAKE 协议通用框架的密钥私密性的优势至多为

$$Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-kp}}(\mathcal{A})\leq 2\cdot Adv_{G_q}^{\text{DDH}}(O(t)).$$

证明. 假设 $\mathcal{A}_{kp}$ 是运行时间至多为 $t$，进行了 $q_{Execute}$ 次 *Execute* 询问和 $q_{Test}$ 次 *TestPair* 询问的概率多项式敌手. 下面我们通过调用 $\mathcal{A}_{kp}$ 来构造一个可以解决 DDH 问题的敌手 $\mathcal{A}_{\text{DDH}}$.

设 DDH 实例 $(U,V,W)$ 是给 $\mathcal{A}_{\text{DDH}}$ 的输入. $\mathcal{A}_{\text{DDH}}$ 首先根据协议中口令空间 $\mathcal{D}$ 的分布为所有的用户选择口令，另外选择框架中所有的 CRS 公共参数. $\mathcal{A}_{\text{DDH}}$ 随机选择一个随机比特 $b$ 用于模拟 *TestPair* 询问. 然后 $\mathcal{A}_{\text{DDH}}$ 将所有的口令告诉敌手 $\mathcal{A}_{kp}$ 并且开始模拟协议的运行.

为了模拟 $Execute(C^i,G^j)$ 询问，$\mathcal{A}_{\text{DDH}}$ 首先随机选择 $a_1,a_2,b_1,b_2\in Z_q^*$，然后在模拟用户的时候令 $X=U^{a_1}g^{a_2}$，然后在模拟网关的时候令 $Y=V^{b_1}g^{b_2}$. $\mathcal{A}_{\text{DDH}}$ 根据协议的描述正常模拟协议剩余的步骤直到计算 Diffie-Hellman 密钥 $K$ 为止，$\mathcal{A}_{\text{DDH}}$ 设置 Diffie-Hellman 密钥 $K=W^{a_1b_1}\cdot U^{a_1b_2}\cdot W^{a_2b_1}\cdot g^{a_2b_2}$.

为了模拟 $TestPair(C^i,G^j)$ 询问，$\mathcal{A}_{\text{DDH}}$ 首先检查敌手 $\mathcal{A}_{kp}$ 是否进行过相同的询问. 如果是，则返回与上次相同的回答；否则，$\mathcal{A}_{\text{DDH}}$ 检查 $C^i$ 和 $G^j$ 是否是伙伴，如果不是，则返回错误的符号 $\perp$. 在 $C^i$ 和 $G^j$ 是伙伴的情况下，如果随机比特 $b=0$，那么 $\mathcal{A}_{\text{DDH}}$ 返回真实的会话密钥 $K$ 给敌手 $\mathcal{A}_{kp}$，如果随机比特 $b=1$，那么 $\mathcal{A}_{\text{DDH}}$ 返回一个 $G_q$ 中的随机元素给敌手 $\mathcal{A}_{kp}$.

下面我们分析 $\mathcal{A}_{\text{DDH}}$ 攻破 DDH 假设的成功概率，首先如果 DDH 实例 $(U,V,W)$ 是一个 Diffie-Hellman 三元组，那么上面对协议的模拟是完美的，因此 $\mathcal{A}_{\text{DDH}}$ 输出 1 的概率为 $\frac{1}{2}+\frac{1}{2}Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-kp}}(\mathcal{A}_{kp})$. 如果 DDH 实例 $(U,V,W)$ 是一个随机的三元组，那么无论 $b$ 为 0 或者 1，返回给敌手 $\mathcal{A}_{kp}$ 的都是与其视图独立的随机数，因此不会泄露关于 $b$ 的任何信息，此时 $\mathcal{A}_{\text{DDH}}$ 输出 1 的概率为 $\frac{1}{2}$.

综上，定理 2 得证. 证毕.

**定理 3**(口令保护). 假设 $\mathcal{A}$ 是一个运行时间为 $t$，并且进行了 $q_{Send}$ 次 *Send* 询问的概率多项式敌手，那么敌手 $\mathcal{A}$ 对 GPAKE 协议通用框架进行不可检测在线字典攻击成功的优势至多为

$$Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-uoda}}(\mathcal{A})\leq\frac{q_{Send}}{|\mathcal{D}|}+neg(n).$$

证明. 考虑一个恶意网关 $\mathcal{A}$ 冒充诚实用户并

且发送消息$(C,X,\omega,Y)$给服务器.根据协议描述,此时服务器应该随机选择$k\in K$并计算投射密钥$s=\alpha(k,\omega)$,然后计算平滑投射 Hash 函数的值$H_k(\omega,pw)$,并且将结果分为三个随机比特串$r'\|\tau_1\|\tau_2$.服务器定义标签$label=C\|G\|S\|\omega\|s\|X\|Y$并且用带标签的加密体制$\Sigma'$计算对口令$pw$加密的密文$\omega'=Enc_{pk'}^{label}(pw;r')$,最后服务器发送消息$(s,\omega',\tau_1)$给恶意网关.恶意网关需要返回消息$\tau_2^*$满足$\tau_2=\tau_2^*$,否则服务器将会检测到恶意网关的在线口令猜测攻击.

如果恶意网关在产生密文$\omega$的时候正确猜测到了口令,那么可以正确计算出$\tau_2^*$的值.反之,如果口令猜测错误,根据平滑投射函数的平滑性可知,即使敌手知道投射密钥$s$,平滑投射 Hash 函数的输出与其值域中的均匀分布仍然是统计不可区分的.因此恶意网关能够正确返回$\tau_2^*$的概率是$2^{-n}$.

因此,恶意网关$\mathcal{A}$对 H-GPAKE 协议进行不可检测在线字典攻击成功的概率至多为

$$Adv_{P,\mathcal{D}}^{\text{ake-uoda}}(\mathcal{A})\leq\frac{q_{Send}}{|\mathcal{D}|}+neg(n).$$

## 5 性能分析

在本节,我们首先用具体的公钥加密体制对通用框架进行实例化,然后与其它的网关口令协议进行效率与安全性方面的比较.

如果令 ElGamal 加密算法为框架中的 CPA 安全的加密体制,Cramer-Shoup 加密算法为框架中的 CCA 安全的加密体制,那么我们得到标准模型下安全高效的网关口令协议[22].在计算代价方面,由于模指数运算和公钥加密是计算代价最高的运算,因此我们只考虑模指数运算(用$e$表示)和 CCA 公钥加密运算(用$E$表示),而忽略其余的运算(如 Hash 函数运算、模乘、对称加密和 MAC 等).在通信代价方面,我们从传输的消息所占用的通信带宽和通信轮数两个方面来比较.为了比较通信带宽,我们假设参与者的身份可以用 32 比特的字符串表示,循环群$G_q$中的点可以由 160 比特的字符串表示,假设对称加密算法、Hash 函数和 MAC 的输出都是 160 比特.由于文献[16-18]中的协议假设用户和服务器之间需要执行安全的两方 PAKE 协议,因此我们用文献[6]中安全高效的两方 PAKE 协议对这些协议进行实例化.计算效率和通信效率的比较结果见表 1.在安全性方面,我们主要从是否可以抵抗不可检测在线字典攻击、是否实现双向认证、安全性证明的模型以及安全性证明所基于的困难性假设四个方面进行衡量.我们用 UODA 表示不可检测在线字典攻击,用 MA 表示双向认证,用 PCDDH 表示基于口令的选择基判定性 DDH 假设[19],用 ROM 表示随机预言模型,Standard 表示标准模型.安全性比较的结果见表 2.

**表 1 标准模型下网关口令协议的效率比较**

| 比较的协议 | 计算复杂度 | | | 通信复杂度 | |
|---|---|---|---|---|---|
| | 用户 | 网关 | 服务器 | 通信带宽/bits | 消息轮数 |
| ACFP 协议[15] | $2e$ | $2e$ | $2e$ | 1216 | 4 |
| AIP 协议[19] | $4e$ | $3e$ | $3e$ | 2208 | 4 |
| BLL 协议[16] | $4e$ | $2e$ | $4e$ | 2240 | 8 |
| Shim 协议[17] | $4e$ | $2e$ | $4e$ | 1920 | 8 |
| YY 协议[18] | $4e$ | $2e$ | $4e$ | 2752 | 9 |
| 我们的协议 | $4e+1E$ | $2e$ | $2e+1E$ | 3360 | 6 |

**表 2 标准模型下的网关口令协议的安全性比较**

| 比较的协议 | UODA | MA | 安全性证明 | 困难性假设 |
|---|---|---|---|---|
| ACFP 协议[15] | N | N | ROM | DDH,PCDDH |
| AIP 协议[19] | N | N | ROM | DDH,PCDDH |
| BLL 协议[16] | N | N | Unproven | |
| Shim 协议[17] | Y | N | Unproven | |
| YY 协议[18] | Y | Y | Unproven | |
| 我们的协议 | Y | Y | Standard | DDH |

在计算代价方面,注意形如$g^xh^y$这样的运算可以通过一个模指数的运算代价求得.从表 1 可见,对于网关的计算量,我们的协议和其余的 GPAKE 协议相同.但是在我们的协议中,用户需要 8 个模指数运算(其中 4 个是 Cramer-Shoup 加密算法的代价),服务器需要计算 6 个模指数运算(其中 4 个是 Cramer-Shoup 加密算法的代价),因此我们的协议计算复杂度高于其它的协议.在通信带宽方面,我们的协议仍然是效率最低的.但是注意到,大部分的计算代价和通信带宽都来自协议中用到的 CCA 安全的公钥加密体制,仅 CCA 加密体制就占到了 8 个指数运算和 1280 比特的传输带宽.然而目前在设计标准模型下可证明安全的 PAKE 协议时,CCA 安全的公钥加密体制几乎是必不可少的.事实上,标准模型下可证明安全的协议计算复杂度和通信复杂度一般是随机预言模型下的同类协议的 3 倍左右.考虑到我们的协议是标准模型下可证明安全的,因此这样的计算代价和通信代价是可以接受的,并且具有相当的优势.在协议的通信轮数方面,我们的协议需要 6 轮交互,效率只比 ACFP 协议和 AIP 协议低.注意到 ACFP 协议和 AIP 协议都不能抵抗不可检测在线字典攻击,为了使其能够抵抗该攻击,至少需

要增加两轮通信(用户给网关发送对服务器的验证信息,再由网关转发给服务器).

在安全性方面,我们的协议可以抵抗不可检测在线字典攻击并且实现了双向认证,其余的协议都没有能够达到相同的安全强度.虽然文献[18]中的协议也声称具有同样的安全性,但是缺乏严格的证明,其安全性无法令人信服.我们的协议是唯一的一个在标准模型下可证明安全的 GPAKE 协议,并且安全性证明基于标准的 DDH 假设.

## 6　总　结

本文在共同参考串模型下基于平滑投射 Hash 函数簇设计了网关口令认证密钥交换协议一个高效的通用框架,并且在标准模型中证明了其安全性.通用框架采用了模块化的设计思路,可以利用不同的密码学组件进行具体的实例化;在安全性方面,通用框架可以实现双向认证并且能够抵抗不可检测在线字典攻击,还采用了模块化的安全证明思路;利用 DDH 假设、二次剩余假设和 $N$ 次剩余假设对通用框架进行实例化可以得到不同的标准模型下高效的网关口令协议.

## 参　考　文　献


[1] Bellovin S M, Merritt M. Encrypted key exchange: Password-based protocols secure against dictionary attacks//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, USA, 1992: 72-84

[2] Steiner M, Tsudic G, Waidner M. Refinement and extension of encrypted key exchange. ACM Operation System Review, 1995, 29(3): 22-30

[3] Jablon D P. Strong password-only authenticated key exchange. ACM Computer Communication Review, 1996, 26(5): 5-26

[4] Lucks S. Open key exchange: How to defeat dictionary attacks without encrypting public keys//Proceedings of the 5th International Workshop on Security Protocols 1997. Paris, France, 1997. LNCS 1361. Berlin: Springer-Verlag, 1997: 79-90

[5] Patel S. Number theoretic attacks on secure password schemes//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, USA, 1997: 236-247

[6] Bellare M, Pointcheval D, Rogway P. Authenticated key exchange secure against dictionary attacks//Proceedings of the Advances in Cryptology -Eurocrypt 2000. Bruges, Belgium, 2000: 139-155

[7] Boyko V, Mackenzie P D, Patel S. Provably secure password-authenticated key exchange using Diffie-Hellman//Proceedings of the Advances in Cryptology-Eurocrypt 2000. Bruges, Belgium, 2000: 156-171

[8] Katz J, Ostrovsky R and Yung M. Practical password authenticated key exchange provably secure under standard assumptions//Proceedings of the Advances in Cryptology-Eurocrypt 2001, Innsbruck, Austria, 2001: 475-494

[9] Gennaro R, Lindell Y. A framework for password-based authenticated key exchange. ACM Transactions on Information and System Security, 2006, 9(2): 181-234

[10] Gennaro R. Faster and shorter password-authenticated key exchange//Proceedings of the Theory of Cryptography Conference-TCC 2008. New York, USA, 2008: 589-606

[11] Abdalla M, Chevalier C, Pointcheval D. Smooth projective hashing for conditionally extractable commitments//Proceedings of the Advances in Cryptology-Crypto 2009. California, USA, 2009: 671-689

[12] Katz J, Vaikuntanathan V. Password-based authenticated key exchange based on lattices//Proceedings of the Advances in Cryptology-Asiacrypt 2009. Tokyo, Japan, 2009: 636-652

[13] Jiang S, Gong G. Password based key exchange with mutual authentication//Proceedings of the Selected Areas in Cryptography-SAC 2004. Waterloo, Canada, 2004: 267-279

[14] 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 — ACM CCS 2010. Chicago, USA, 2010: 516-525

[15] Abdalla M, Chevassut O, Fouque P A, Pointcheval D. A simple threshold authenticated key exchange from short secrets//Proceedings of the Advances in Cryptology-Asiacrypt 2005. Chennai, India, 2005: 566-584

[16] 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

[17] Shim K A. Cryptanalysis and enhancement of modified gateway-oriented password-based authenticated key exchange protocol. IEICE Transactions on Fundamentals, 2008, E91-A(12): 3837-3839

[18] Yoon E J, Yoo K Y. An optimized gateway-oriented password-based authenticated key exchange protocol. IEICE Transactions on Fundamentals, 2010, E93-A(4): 850-853

[19] Abdalla M, Izabachene M, Pointcheval D. Anonymous and transparent gateway-based password-authenticated key exchange//Proceedings of the 7th International Conference on Cryptology and Network Security. Hong Kong, China, 2008: 133-148

[20] Shoup V. ISO 18033-2: An emerging standard for public-key encryption. http://shoup.net/iso/std6.pdf, Final Committee Draft. 4, 2004

[21] Bellare M, Boldyreva A, Micali S. Public-key encryption in a multi-user setting: Security proofs and improvements//Proceedings of the Advances in Cryptology-Eurocrypt 2000. Bruges, Belgium, 2000: 259-274

[22] Wei F S, Zhang Z F, Ma C G. Gateway-oriented password-based authenticated key exchange protocol in the standard model. The Journal of Systems and Software, 2012, 85(3): 760-768

**WEI Fu-Shan**, born in 1983, Ph. D., lecturer. His current research interests include secure protocols and authentication in wireless networks.

**ZHANG Zhen-Feng**, born in 1972, Ph. D., professor, Ph. D. supervisor. His current research interests include provably-secure protocols and security models.

**MA Chuan-Gui**, born in 1962, Ph. D., professor, Ph. D. supervisor. His current interests include cryptology protocols and wireless communications.

**Background**

This work is supported by three grants from the National High Technology Research and Development Program (863 Program) of China (Grant No. 2009AA01Z417) and the National Natural Science Foundation of China (Grant Nos. 91118006, 61170278).

Key exchange protocols are fundamental for establishing secure communication channels over public insecure networks. Gateway-oriented password-based authenticated key exchange protocols (GPAKE) take into account the presence of firewalls when clients communicate with authentication servers using passwords. It brings the PAKE problem closer to practice. GPAKE allows a client and a gateway to establish a common session key with the help of an authentication server. GPAKE protocols are suitable for mobile communication environments such as GSM (Global System for Mobile Communications) and 3GPP (The Third Generation Partnership Project). Due to its practical importance, researchers pay more and more attention to GPAKE protocols.

Existing GPAKE protocols either are proven secure in the random oracle model, or have no security reductions. Moreover, all known GPAKE protocols either are vulnerable to undetectable on-line dictionary attacks, or are claimed to be secure against the undetectable on-line dictionary attack without rigorous proofs. In order to improve research on GPAKE protocols in the standard model, we propose the first general framework for GPAKE protocols in this paper, and prove its security under standard assumptions. The design and the proof of the framework are conducted using high-level cryptographic tools. The framework can be instantiated under the DDH assumption, the Quadratic residuosity assumption and the N-residuosity assumption to obtain various efficient GPAKE protocols in the standard model. We formally prove that our general framework for GPAKE protocols in the standard model can resist the undetectable on-line dictionary attack. Our framework only needs 6 message flows to resist on-line dictionary attacks, which is quite efficient. Although it has higher computation and communication costs than related schemes, the complexity costs are acceptable consider the fact that our framework can be proven secure in the standard model.