具有强匿名性的网关口令认证密钥交换协议

魏福山 马传贵

(信息工程大学信息工程学院信息研究系 郑州 450002)

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,其中用户和服务器之间的认证通过低熵的口令来完成.已有的网关口令认证密钥交换协议对用户的匿名性研究不足.该文基于 Diffie-Hellman 密钥交换提出了具有强匿名性的网关口令认证密钥交换协议,并且在随机预言模型下基于标准的 DDH 假设证明了协议的安全性.新协议可以抵抗不可检测在线字典攻击并且计算效率高,安全性和计算效率都优于已有的同类协议.

关键词 口令认证;网关;匿名性;随机预言模型;DDH 假设

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2012.01823

An Efficient Gateway-Oriented Password-Based Authenticated Key Exchange Protocol with Strong User Anonymity

WEI Fu-Shan MA Chuan-Gui

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

Abstract Gateway-oriented password-based authenticated key exchange (GPAKE) protocol allows a client and a gateway to establish a common session key with the help of an authentication server, where the authentication between the client and the server is done via a low-entropy password. The approach of designing GPAKE protocols with user anonymity is far from maturity and perfection. This paper presents a GPAKE protocol with strong user anonymity based on the Diffie-Hellman key exchange, and then proves its security under the standard DDH assumption in the random oracle model. The new protocol can resist the undetectable on-line dictionary attack and is quite efficient in terms of computation. Compared with other related protocols, the new protocol is more secure and efficient.

Keywords password authentication; gateway; anonymity; random oracle model; DDH assumption

1 引 言

在很多实际的应用中,如网上银行、移动支付和无线漫游接入等,服务提供商由前置的网关和后端的验证服务器组成.网关是提供协议转换、网间连接、信息过滤和安全功能的设备,负责用户的接入并且为用户提供保密的数据传输,在网络连接中必不可少.服务器则负责用户的注册、安全鉴权和计费等功能.为了刻画这种实际的应用需求,Abdalla 等人[1]在 2005 年的亚密会上提出了网关口令认证密钥交换(GPAKE)协议的概念.GPAKE 协议是一

收稿日期:2012-05-14;最终修改稿收到日期:2012-07-30.**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. **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.

个三方口令协议,使得用户和网关在服务器的协助下建立一个认证的会话密钥.服务器和用户之间共享口令用于认证用户身份,但是会话密钥是在用户和网关之间建立的.由于 GPAKE 协议的模型贴近实际,在很多场景中都具有巨大的应用潜力,因此成为轻量级口令协议研究的一个热点问题.

2005 年,Abdalla 等人[1]提出了 GPAKE 协议的安全模型,设计了第一个在随机预言模型下安全的 GPAKE 协议并且将该协议进一步推广到门限的形式.但是在 2006 年,Byun 等人[2]指出 Abdalla 等人所设计的 GPAKE 协议易遭受不可检测在线字典攻击[3].一个恶意的网关可以反复对用户的口令进行在线的猜测,然后从服务器端得到验证,直到猜测出正确的口令为止,而服务器检测不到这种恶意的攻击.Byun 等人提出了一个改进的协议,要求用户和服务器在执行 GPAKE 协议之前运行一次安全的两方口令协议,预先建立一个用于认证消息的共享密钥,并且通过给用户发送的消息增加消息认证码的方式来保护口令.但是在 2008 年,Shim 发现[4] Byun 等人的改进协议实际上依旧不能抵抗不可检测在线字典攻击,敌手可以重放增加认证码的消息从而对用户的口令进行在线的猜测.Shim 采用类似于 Byun 等人的改进方式,要求用户和服务器执行一次安全的两方口令协议从而建立起共享的加密密钥,利用对称加密体制掩盖口令的信息并提出了 S-GPAKE 协议.同年,Abdalla 等人[5]提出了一个可以利用私密信息检索(Private Information Retrieval)协议[6-7]实现用户匿名性的 GPAKE 协议.他们同时提出了一个更强的安全模型,该模型允许对参与者进行腐化从而实现了前向安全性.2010 年,Yoon 等人[8]指出 Shim 提出的 S-GPAKE 协议存在设计上的错误,协议无法正常执行,并且计算效率较低.他们对 Shim 设计的协议进行改进,提出了称为最优的 O-GPAKE 协议.2011 年,Wei 等人利用 RSA 体制设计了 GPAKE 协议[9],并进一步对该协议进行了改进,提出了效率更高并且可以利用私密信息检索协议实现用户匿名性的 GPAKE 协议[10].此外,他们还分别在随机预言模型和标准模型下提出了可以抵抗不可检测在线字典攻击的 GPAKE 协议[11-12].

GPAKE 协议适用于移动通信环境,如 GSM 和 3GPP 等.由于移动通信网络不能像传统的有线网络那样通过物理隔离来保护用户隐私信息的数据包,并且敌手更易于窃取用户认证时所提交的身份信息和服务器对用户身份标识的询问,增加了对用户隐私信息保护的难度.实现用户匿名性在保护用户的个人隐私的同时还可以减少对用户仿冒攻击的几率,因此研究具有匿名性的 GPAKE 协议有非常重要的现实意义.但是,具有匿名性的 GPAKE 协议的研究成果很少,目前只有由 Abdalla 等人[5]和 Wei 等人[10]分别基于 Diffie-Hellman 密钥交换和 RSA 体制提出的两个匿名 GPAKE 协议.已有的匿名 GPAKE 协议都采用网关和服务器共同执行私密信息检索协议的方法来实现用户的匿名性,只能保证用户身份对服务器的匿名性,网关和攻击者都可以得到用户的真实身份,匿名性较弱;此外,已有的匿名 GPAKE 协议的计算效率较低,需要进一步地提高,并且 Abdalla 等人的匿名 GPAKE 协议[5]还存在安全漏洞,不能抵抗不可检测在线字典攻击.

针对已有的匿名 GPAKE 协议存在的不足,本文采用匿名认证协议的设计思想,基于 Diffie-Hellman 密钥交换设计了一个具有强匿名性的 GPAKE 协议,并且在随机预言模型下利用标准的 DDH 假设证明了协议的安全性.与已有的匿名 GPAKE 协议相比,新协议可以抵抗不可检测在线字典攻击并且实现了用户和服务器之间的双向认证,因此具有更强的安全性;在匿名性方面,新协议实现了对用户身份的强匿名保护,无论是攻击者、网关还是服务器都无法得到用户的真实身份;最后,在与已有同类协议具有相同通信效率的情况下,新协议在计算效率方面具有明显的优势.因此,本文所提出的匿名 GPAKE 协议具有更强的安全性和更高的效率,更符合移动通信环境的应用需求.

第 2 节回顾 GPAKE 协议的安全模型;第 3 节介绍具有强匿名性的 GPAKE 协议并且给出协议的安全性证明;第 4 节给出与已有匿名 GPAKE 协议的性能比较;第 5 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[1].

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.

Abdalla 等人[13]的安全模型采用了 ROR(Real-Or-Random)模型的定义方式. 敌手可以进行多次 *Test* 询问，所有 *Test* 询问的回答都由一个随机比特来决定. 即敌手得到的可能全部是真实的会话密钥或者全部是与会话密钥等长的随机数. 在 FTG(Find-Then-Guess)模型中常见的 *Reveal* 询问在 ROR 模型中不存在，但是由于 FTG 模型中只允许敌手进行一次 *Test* 询问，ROR 模型实际上比 FTG 模型强. 关于 ROR 模型和 FTG 模型的更多比较，参见文献[13].

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 3 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.

对于协议的匿名性,我们采用文献[14]中的定义方法. 称一个 GPAKE 协议是匿名的,如果在用户和网关建立会话密钥的过程中,用户除了证明自己是合法的成员外,不泄露任何身份信息给网关和服务器.

定义 6(匿名性). 对于两个用户 C_i 和 C_j,分别用 $P(C_i,G,S)$和 $P(C_j,G,S)$表示两个用户执行协议的消息抄本. 称一个 GPAKE 协议$\mathcal{P}$实现了用户匿名性,如果有

$$Dist[P(C_i,G,S)]=Dist[P(C_j,G,S)],$$

其中$Dist[P(C,G,S)]$表示 $P(C,G,S)$的概率分布.

3 具有强匿名性的 AGPAKE 协议

3.1 协议描述

设 G_q是一个阶为大素数 q 的循环群,g,h 为随机选择的G_q的两个生成元,且 h 关于 g 的离散对数是难解的;设 $H,H_i:\{0,1\}^*\rightarrow\{0,1\}^l(i=0,1,2,3)$是相互独立的 Hash 函数,其中 l 是安全参数. 假设系统中总共有 n 个用户,每个用户 C_i分别与服务器共享一个口令 pw_i. 不失一般性,假设口令已经映射为 Z_q^* 中的元素. 协议的参与者有用户、网关和服务器,网关和服务器之间是安全的认证通道. 协议的描述见图 1,具体的步骤如下.

1. 用户 C_i 选择随机数 $x,r_1\in Z_q^*$,计算 $X=g^x$ 以及 $R_1=g^{r_1}h^{pw_i}$,最后用户发送消息(C,X,R_1)给网关 G,其中 C 是系统中所有用户的身份.

2. 网关G接收到消息(C,X,R_1)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,R_1,Y)后,随机选择 $r_2\in Z_q^*$ 和 $MS\in\{0,1\}^l$,然后计算 $R_2=g^{r_2}$. 对于每一个用户 $C_j(1\leq j\leq n)$,服务器首先计算 $R_{1,j}=R_1/h^{pw_j}$ 和 $K_j=(R_{1,j})^{r_2}$,然后利用 K_j 对 MS 进行掩盖,即计算 $Z_j=H(j,K_j)\oplus MS$. 最后服务器利用随机数 MS 计算认证值 $V_{S_1}=H_1(ID_1\|ID_2\|MS)$和 $V_{S_2}=H_2(ID_1\|ID_2\|MS)$,其中 $ID_1=(C,G,X,R_1,Y)$,$ID_2=(R_2,\{Z_j\}_{1\leq j\leq n})$. 服务器发送消息$(ID_2,V_{S_1},V_{S_2})$给网关.

4. 网关 G 接收到消息(ID_2,V_{S_1},V_{S_2})后,先储存 V_{S_2}用于验证用户身份,然后转发消息(G,Y,ID_2,V_{S_1})给用户.

5. 用户 C_i 接收到消息(G,Y,ID_2,V_{S_1})后,首先从$\{Z_j\}_{1\leq j\leq n}$找到对应于自己的 Z_i,然后计算 $K_i=R_2^{r_1}$ 和$MS'=Z_i\oplus H(i,K_i)$. 用户 C_i 利用 MS'验证 V_{S_1} 是否有效. 如果无效则拒绝协议,否则计算认证值 $V'_{S_2}=H_2(ID_1\|ID_2\|MS')$和 $V'_{S_3}=H_3(ID_1\|ID_2\|MS')$以及 Diffie-Hellman 密钥 $K=Y^x$. 最后用户 C_i计算会话密钥 $sk=H_0(ID_1\|ID_2\|K)$,发送消息(C,V'_{S_2},V'_{S_3})给网关并且接受协议运行.

6. 网关接收到消息(C,V'_{S_2},V'_{S_3})后,首先验证用户 C_i 发送的 V'_{S_2}是否等于所储存的 V_{S_2}. 如果验证通过,则网关接受协议运行并计算 Diffie-Hellman 密钥 $K=X^y=g^{xy}$ 以及会话密钥 $sk=H_0(ID_1\|ID_2\|K)$;否则,网关拒绝协议运行并终止. 最后,网关发送消息(C,V'_{S_3})给服务器,服务器验证 V'_{S_3}是否有效. 如果验证通过,说明认证请求确实是一个诚实的用户发送的;否则,认证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.

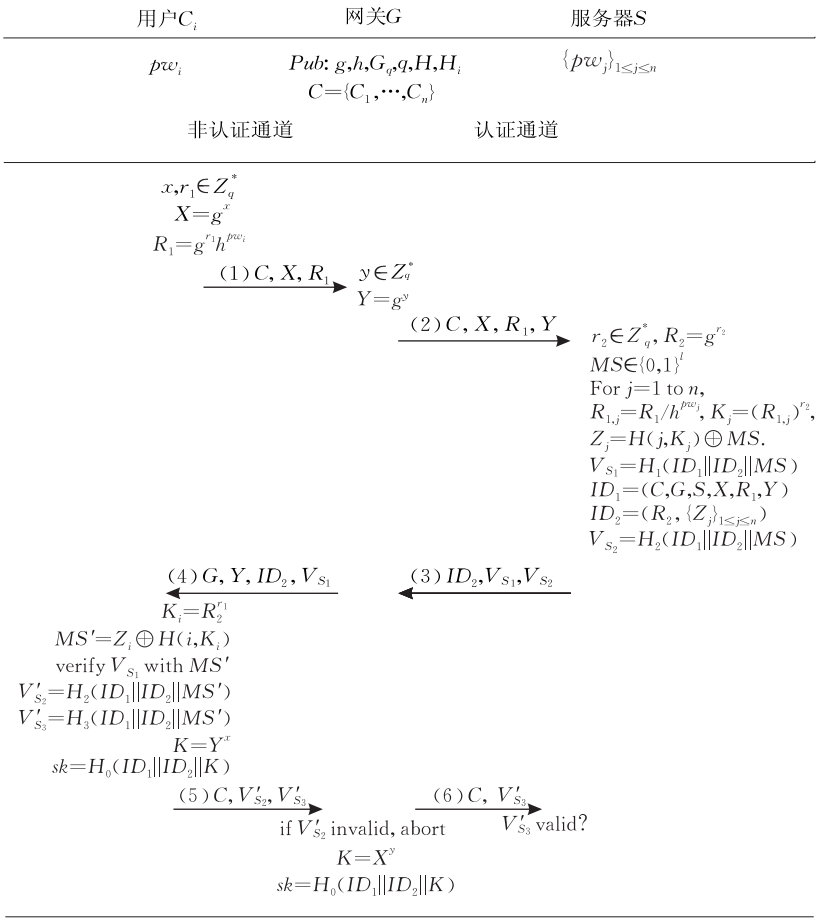

图 1　匿名的 AGPAKE 协议

3.2　安全性证明

本小节给出匿名的 AGPAKE 协议的安全性证明. 协议的安全性基于 DDH 假设，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，那么敌手 $\mathcal{A}$ 破坏 AGPAKE 协议的语义安全的优势至多为

$$Adv_{\mathcal{P},\mathcal{D}}^{\text{ake-ror}}(\mathcal{A})\le\frac{3q_{Send}}{|\mathcal{D}|}+neg(l),$$

其中 $neg(l)$ 表示关于安全参数 l 的一个可忽略函数.

证明.　我们采用混合实验的方法来证明协议的语义安全性，证明思路是通过一系列攻击实验对模拟规则逐渐进行改变，直到敌手的优势为可忽略的函数为止. 我们用事件 $Succ$ 表示敌手正确猜测出了在 $Test$ 询问中所使用的随机比特 b，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：此实验模拟在随机预言模型下的真实协议运行，在试验中敌手 $\mathcal{A}$ 可以多次进行 $Execute$、$Send$ 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，我们通过维持哈希列表来模拟随机预言函数 $H_i(i=0,1,2,3)$ 以及 H. 另外我们还模拟私有的随机预言函数 $H'_i(i=0,1,2,3)$ 以及 H'，这 5 个私有的随机预言函数将在后面的实验中用到. 随机预言函数的模拟规则如下.

(1) H_i 查询列表 $\wedge_{H_i}(i=0,1,2,3)$. 对于每一次随机预言询问 $H_i(m)$，如果列表 $\wedge_{H_i}$ 中存在记录 (i,m,r)，则返回 r；否则，随机选择 $r\in\{0,1\}^l$，将 r 返回给询问者，并且将记录 (i,m,r) 添加到列表 $\wedge_{H_i}$.

(2) H_i'查询列表 $\wedge_{H_i'}$ ($i=0,1,2,3$). 对于每一次随机预言询问 $H_i'(m)$,如果列表 $\wedge_{H_i'}$ 中存在记录 (i,m,r),则返回 r;否则,随机选择 $r\in\{0,1\}^l$,将 r 返回给询问者,并且将记录 (i,m,r) 添加到列表 $\wedge_{H_i'}$.

(3) H 查询列表 $\wedge_H$. 对于每一次随机预言询问 $H(m)$,如果列表 $\wedge_H$ 中存在记录 (m,r),则返回 r;否则,随机选择 $r\in\{0,1\}^l$,将 r 返回给询问者,并且将记录 (m,r) 添加到列表 $\wedge_H$.

(4) H'查询列表 $\wedge_{H'}$. 对于每一次随机预言询问 $H'(m)$,如果列表 $\wedge_{H'}$ 中存在记录 (m,r),则返回 r;否则,随机选择 $r\in\{0,1\}^l$,将 r 返回给询问者,并且将记录 (m,r) 添加到列表 $\wedge_{H'}$.

除了模拟随机预言函数外,我们还根据协议描述模拟所有的 *Execute*、*Send* 和 *Test* 询问. 由模拟的规则可知

$$Adv(\mathcal{A},P_0)=Adv(\mathcal{A},P_1).$$

实验 P_2:为了方便后面的分析,在此实验中我们排除一些发生碰撞的会话. 具体来说,如果会话中消息抄本发生碰撞,或者随机预言函数的输出发生碰撞,那么我们取消该次会话的运行. 由生日攻击原理可知,实验 P_2 和实验 P_1 是不可区分的,因此有

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

实验 P_3:从此实验开始,我们修改对 *Execute* 询问的模拟. 具体来说,我们在被动会话中将 Hash 函数 H 以及 H_1,H_2,H_3 分别替换为实验 P_1 中定义的私有随机预言函数 H' 和 H_1',H_2',H_3',并且随机选择随机预言函数中的输入 K_j 以及 MS. 我们现在来证明实验 P_3 和实验 P_2 是不可区分的.

敌手如果想要区分实验 P_3 和实验 P_2,由于在 H_1,H_2,H_3 中的输入只有 MS 是秘密的值,其余的都是公开值,因此对于某一次被动会话,敌手如果正确恢复出 MS 则可以区分实验 P_3 和实验 P_2. 由于 $Z_j=H(j,K_j)\oplus MS$,因此对于任意的 $1\leq j\leq n$,敌手需要计算出一个正确的 K_j 才可以正确恢复出 MS. 但是因为会话是被动的,并且 R_1 对应于用户 C_i,因此实际上敌手需要恢复出正确的 K_i. 用事件 *PassiveAskH* 表示敌手正确计算出 K_i 并且向随机预言函数 H 进行了相应的询问,显然如果 *PassiveAskH* 事件发生,那么敌手可以区分实验 P_3 和实验 P_2;用 *PassiveAskH*$_i$ 表示在 *PassiveAskH* 事件没有发生的情况下,敌手用正确的 MS 向随机预言函数 H_1, H_2, H_3 进行相应的询问. 如果 *PassiveAskH* 没有发生,那么敌手不可能知道正确的 MS,因此事件 *PassiveAskH*$_i$ 的概率是可忽略的. 我们现在来证明,*PassiveAskH* 发生的概率至多为敌手破解 CDH 问题的优势,即敌手区分实验 P_3 和实验 P_2 的优势是可忽略的.

给定一个 CDH 实例 (U,V),我们定义一个额外的实验 P_3'. 在实验 P_3' 中,当我们模拟 *Execute* 询问时,令用户 C_i 计算 $R_1=U^{a_1}g^{a_2}\times h^{pw_i}$,服务器计算 R_2 时令 $R_2=V^{b_1}g^{b_2}$,其中 $a_1,a_2,b_1,b_2\in Z_q^*$. 其余的模拟规则和实验 P_3 完全相同. 注意虽然实验 P_3 和实验 P_3' 的模拟规则不同,但是分布却完全相同. 如果事件 *PassiveAskH* 发生,我们可以从 $\wedge_H$ 列表中提取 $K_i=CDH(U^{a_1}g^{a_2},V^{b_1}g^{b_2})=CDH(U,V)^{a_1b_1}\cdot U^{a_1b_2}\cdot V^{a_2b_1}\cdot g^{a_2b_2}$,由于 a_1,a_2,b_1,b_2 已知,因此可以得到 $CDH(U,V)=(K_i/(U^{a_1b_2}\cdot V^{a_2b_1}\cdot g^{a_2b_2}))^{-a_1b_1}$,从而得到了 CDH 问题的解. 由 CDH 问题的困难性假设可知事件 *PassiveAskH* 发生的概率是可忽略的.

由上面的分析可知实验 P_3 和实验 P_2 是不可区分的,因此有

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

实验 P_4:在这个实验中,我们继续修改对 *Execute* 询问的模拟. 我们修改用户和网关的会话密钥的计算方式,即使用私有的随机预言函数 H_0' 来计算会话密钥 sk. 这样的修改使得被动会话中会话密钥 sk 完全与随机预言函数 H_0 以及 Diffie-Hellman 密钥 K 无关. 由于在上一个实验中,我们令用户和服务器之间的认证值完全与 MS 无关,因此在此实验中可以简化模拟规则,在模拟被动会话时直接从 G_q 中随机选择 R_1 和 $R_{1,j}$ 以及 K_j 的值.

在实验 P_4 中,所有的被动会话中的认证值和会话密钥都是随机选择的,并且口令在被动会话中也完全没有用到,因此敌手在区分被动会话的会话密钥时没有任何优势,也不能通过被动会话得到口令的任何信息. 需要说明的是,在主动攻击的会话中,模拟规则依然和真实的实验一样. 通过和实验 P_3 类似的分析可知实验 P_4 和实验 P_3 是不可区分的,敌手区分这两个实验的优势至多是破解 CDH 问题的优势,因此有

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

实验 P_5:在这个实验中,我们处理敌手 $\mathcal{A}$ 通过 *Send* 询问进行的被动攻击,也就是说敌手只是诚实转发消息,不对消息进行任何改动. 具体来说,对于这些貌似主动实际还是被动的特殊会话,我们用私有的随机预言函数来计算认证值以及会话密钥,修改的规则和实验 P_4 中对被动会话的处理完全相同,并且通过类似的分析有

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

实验 P_6：在这个实验中，我们开始处理敌手$\mathcal{A}$通过 *Send* 询问进行的主动攻击. 对于敌手的$(C^i,G^j,start)$询问，我们首先随机选择 $R_1\in G_q^*$，随机选择 $x\in Z_q^*$ 并计算 $X=g^x$，然后返回消息(C,X,R_1)给敌手，并且当敌手返回消息(G,Y,ID_2,V_{S_1})的时候，我们令用户实例拒绝接受并且终止协议运行. 实验 P_6 与实验 P_5 是不可区分的，除非对于$(C^i,G^j,start)$询问返回的消息(C,X,R_1)，敌手向随机预言函数 H 询问输入为(i,K_i)的值，其中 $K_i=(R_1/h^{pw_i})^{r_2}$ 并且 $R_2=g^{r_2}$，我们记此事件为 $AskHWithC$. 显然有 $|Adv(\mathcal{A},P_6)-Adv(\mathcal{A},P_5)|\leq Pr[AskHWithC_6]$.

实验 P_7：在这个实验中，我们最后一次处理敌手$\mathcal{A}$通过 *Send* 询问进行的主动攻击. 对于敌手的 $Send(G^j,(C,X,R_1))$询问，我们返回消息(G,Y,ID_2,V_{S_1})，其中 V_{S_1} 是通过私有的随机预言函数H_1'计算得到的，其秘密输入为一个随机选择的 MS. 另外，$Z_j(1\leq j\leq n)$的值我们也随机选择. 当敌手返回消息$(C,V_{S_2'},V_{S_3'})$的时候，我们令网关实例直接拒绝并且终止协议运行. 注意到 K_j 在模拟中没有用到，因此我们可以简化协议的模拟，取消对 K_j 的计算. 显然，实验 P_7 与实验 P_6 是不可区分的，除非敌手计算出某一个正确的 K_j 值，然后恢复出正确的 MS，最后对随机预言函数 H_1,H_2,H_3 进行询问. 敌手区分的关键在于计算出一个正确的 K_j 值并且向随机预言函数 H 询问(j,K_j)，我们记此事件为 $AskHWithG$. 显然有 $|Adv(\mathcal{A},P_7)-Adv(\mathcal{A},P_6)|\leq Pr[AskHWithG_7]$.

在实验P_7中，我们现在来计算事件 $AskHWithC_7$ 和 $AskHWithG_7$ 的概率，并且在此基础上进一步计算敌手破坏协议语义安全的优势.

首先注意到在实验 P_7 中，我们在模拟的时候完全没有用到口令的任何信息，口令可以在模拟的最后阶段来选择. 所有被动会话的会话密钥都是随机选择的，而敌手进行主动攻击的会话都会被拒绝接受. 根据上面的分析可知，敌手在实验 P_7 区分真实的会话密钥和随机数不会有任何优势，因此有 $Succ_7=1/2$. 事件 $AskHWithC_7$ 实际上对应着敌手冒充网关欺骗诚实用户的攻击，由于敌手产生的认证值 V_{S_1} 唯一对应着一个 MS，相应的唯一对应于一个口令值 pw_i，由于我们在实验 P_3 中已经排除了随机预言函数的碰撞，因此有

$$Pr[AskHWithC_7]\leq\frac{q_{Send}}{|\mathcal{D}|}.$$

类似的，事件 $AskHWithG_7$ 对应于敌手冒充用户来欺骗网关的攻击，类似于事件 $AskHWithC_7$ 的分析，我们有

$$Pr[AskHWithG_7]\leq\frac{q_{Send}}{|\mathcal{D}|}.$$

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 AGPAKE 协议的密钥私密性的优势至多为

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

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. $\mathcal{A}_{\text{DDH}}$ 首先根据口令空间$\mathcal{D}$的分布为所有的用户选择口令. $\mathcal{A}_{\text{DDH}}$ 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，$\mathcal{A}_{\text{DDH}}$ 首先随机选择四个随机数 $a_1,a_2,b_1,b_2\in Z_q^*$，然后选择 $r_1\in Z_q^*$，计算 $X=U^{a_1}g^{a_2}$ 和 $R_1=g^{r_1}h^{pw_i}$. $\mathcal{A}_{\text{DDH}}$ 然后将消息(C,X,R_1)发送给网关. 网关接收到消息(C,X,R_1)后，计算 $Y=V^{b_1}g^{b_2}$ 并且发送(C,X,R_1,Y)给服务器. $\mathcal{A}_{\text{DDH}}$ 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 $K=W^{a_1b_1}\cdot U^{a_1b_2}\cdot W^{a_2b_1}\cdot g^{a_2b_2}$，$\mathcal{A}_{\text{DDH}}$ 按照协议的描述完成剩余的模拟.

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 $b=1$，那么 $\mathcal{A}_{\text{DDH}}$ 返回真实的会话密钥 sk 给敌手 $\mathcal{A}_{kp}$，如果随机比特 $b=0$，那么 $\mathcal{A}_{\text{DDH}}$ 返回一个与会话密钥等长的随机数给敌手 $\mathcal{A}_{kp}$.

如果 DDH 实例(U,V,W)是一个 Diffie-Hellman 三元组，那么上面的模拟是完美的，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$\mathcal{A}_{kp}$的都是随机数,因此不会泄露关于 b 的任何信息,此时$\mathcal{A}_{\mathrm{DDH}}$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 AGPAKE 协议进行不可检测在线字典攻击成功的优势至多为

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

证明. 考虑一个恶意网关$\mathcal{A}$冒充诚实用户并且发送接入请求给服务器.根据协议的描述,服务器应该随机选择 $r_2\in Z_q^*$ 和 $MS\in\{0,1\}^l$,然后计算 $R_2=g^{r_2}$.对于每一个用户 $C_j(1\leq j\leq n)$,还需要计算 $R_{1,j}=R_1/h^{pw_j}$ 和 $K_j=(R_{1,j})^{r_2}$ 以及 $Z_j=H(j,K_j)\oplus MS$.最后服务器利用随机数 MS 计算认证值 $V_{S_1}=H_1(ID_1\|ID_2\|MS)$和 $V_{S_2}=H_2(ID_1\|ID_2\|MS)$,其中 $ID_1=(C,G,X,R_1,Y)$,$ID_2=(R_2,\{Z_j\}_{1\leq j\leq n})$.服务器发送消息$(ID_2,V_{S_1},V_{S_2})$给网关.恶意网关为了欺骗成功,需要相应地返回一个认证值 $V_{S_3'}=H_3(ID_1\|ID_2\|MS)$.

如果恶意网关$\mathcal{A}$对用户的口令猜测错误,那么计算出的 K_i 是错误的,相应的也无法正确恢复出 MS 的值.除非敌手能够在不询问 $H_3(ID_1\|ID_2\|MS)$的条件下猜测出 V_{S_3},否则服务器在接收到认证值 $V_{S_3'}$ 后将会拒绝.但是由于 H_3 为随机预言函数,因此在不询问 $H_3(ID_1\|ID_2\|MS)$而正确猜测到 $V_{S_3'}$ 的值的概率是可忽略的.如果恶意网关$\mathcal{A}$对用户的口令猜测正确,那么很容易根据协议描述计算出正确的 $V_{S_3'}$.但是注意到恶意网关$\mathcal{A}$从服务器发出的消息(ID_2,V_{S_1},V_{S_2})至多排除一个口令,因此恶意网关$\mathcal{A}$猜测口令正确的概率至多为$\frac{q_{Send}}{|\mathcal{D}|}$.

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

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

定理 4(匿名性). 匿名的 AGPAKE 协议实现了用户身份的匿名性,并且一个恶意服务器至多以 $1/n$ 的概率破坏用户的匿名性.

证明. 对于用户 $C_i(1\leq i\leq n)$发送的第一条消息(C,X,R_1),因为 x,r_1 是从 Z_q^* 中随机选择的,因此(C,X,R_1)在集合 $C\times G_q\times G_q$ 上是均匀分布的;由于所有的 $Z_j(1\leq j\leq n)$中使用相同的 MS,因此用户C_i发送的消息(C,V'_{S_2},V'_{S_3})不会泄露用户身份的信息.对于两个用户 C_i 和 C_j,显然有 $Dist[P(C_i,G,S)]=Dist[P(C_j,G,S)]$,因此 AGPAKE 协议实现了用户身份的匿名性.

考虑一个恶意的服务器试图通过协议运行获得用户身份.在用户发送消息(C,X,R_1)给服务器后,服务器如果真实地执行协议,由于 R_1 是随机的,并且由于所有的 $Z_j(1\leq j\leq n)$中都使用相同的 MS,那么服务器不可能有任何优势区分用户的身份.根据协议的描述,服务器只能通过用户返回的消息$(C,V_{S_2'},V_{S_3'})$来对用户身份进行猜测,注意到认证值 $V_{S_2'},V_{S_3'}$ 中只有一个秘密输入 MS,因此服务器只有针对不同的用户 C_i 选择不同的秘密值 MS_i 才能区分用户,但是协议中要求服务器在返回消息的时候计算出一个认证值 V_{S_1},但是此时服务器不知道用户身份的任何信息,因此服务器只能以 $1/n$ 的概率来猜测用户的身份并且返回相应的认证值 V_{S_1}.由于用户将对认证值 V_{S_1} 进行验证,那么服务器猜测的认证值 V_{S_1} 将以$\frac{n-1}{n}$的概率无法通过验证,用户将拒绝协议运行.因此恶意服务器破坏协议中用户匿名性的优势至多为 $1/n$. 证毕.

4 性能分析

本节给出本文提出的协议与已有的匿名 GPAKE 协议在计算效率和安全性方面的比较.我们分别用 AIP 协议和 WMC 协议来表示文献[5]和文献[10]中的协议.假设系统中总共有 n 个用户.在计算复杂性方面,只考虑模指数运算而忽略其余的运算(如哈希函数、模乘等运算),用 e_{dh} 表示 Diffie-Hellman 模指数运算,用 e_{rsa} 表示 RSA 的模指数运算.一般认为在相同的参数规模下,这两种模指数运算具有近似的计算代价.在通信复杂性方面,从协议的通信轮数来比较.在安全性方面,主要从是否可以抵抗不可检测在线字典攻击、匿名性的强弱、是否实现双向认证以及安全性证明基于的困难性假设几方面进行衡量.用 UODA 表示不可检测在线字典攻击,用 PCDDH 表示基于口令的选择基判定性 DDH 假设[5],用 RSA 表示 RSA 假设.AGPAKE 协议效率和安全性比较的结果见表 1 和表 2.

表 1　AGPAKE 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	消息轮数
AIP 协议[5]	$4e_{dh}$	$3e_{dh}$	$3ne_{dh}$	4
WMC 协议[10]	$4e_{rsa}$	$2e_{rsa}$	$2ne_{rsa}$	8
AGPAKE 协议	$4e_{dh}$	$2e_{dh}$	$(n+1)e_{dh}$	6

表 2　AGPAKE 协议的安全性比较

比较的协议	UODA	匿名性	双向认证	困难性假设
AIP 协议[5]	否	弱	否	DDH,PCDDH
WMC 协议[10]	是	弱	是	RSA
AGPAKE 协议	是	强	是	DDH

从上面的比较可以看出，在计算代价方面，AGPAKE 协议在用户端和网关端的计算量和已有协议大致相同，但是在服务器端 AGPAKE 协议只需要 $n+1$ 个指数运算，远少于 AIP 协议和 WMC 协议中所需要的指数运算. 通常在服务器进行注册的用户个数 n 都比较大，因此 AGPAKE 协议的计算效率与已有的匿名 GPAKE 协议相比具有明显的优势. 在通信轮数方面 AGPAKE 协议比 WMC 协议少两轮. 但比 AIP 协议多了两轮. 在安全性方面，AGPAKE 协议可以抵抗不可检测在线字典攻击、实现了双向认证并且具有强匿名性，具有最强的安全性. AIP 协议不能抵抗不可检测在线字典攻击并且匿名性较弱，如果 AIP 协议想要达到与 AGPAKE 协议相同的安全性，至少还需要增加两轮通信. 最后，AGPAKE 协议还有一个优势，即安全性基于标准的 DDH 假设，而 AIP 协议还需要用到非标准的 PCDDH 假设.

5　结　语

本文研究如何设计具有强匿名性、安全高效的 GPAKE 协议. 利用匿名认证协议的思想，基于 Diffie-Hellman 密钥交换设计了一个具有强匿名性、安全高效的 GPAKE 协议. 与已有协议相比，新协议可以实现用户身份对恶意敌手、网关和服务器的强匿名保护，可以抵抗不可检测在线字典攻击，并且实现了双向认证，因此具有更强的安全性；此外，新协议在相同通信效率的条件下，在计算效率方面具有明显的优势.

参　考　文　献

[1] 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. LNCS 3788. Berlin: Springer-Verlag, 2005: 566-584

[2] 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

[3] Ding Yun, Horster P. Undetectable on-line dictionary attacks. ACM Operating System, 1995, 29(3): 77-86

[4] 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

[5] 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. LNCS5339. Berlin: Springer-Verlag, 2008: 133-148

[6] Chor B, Goldreich O, Kushilevitz E, Sudan M. Private information retrieval. Journal of ACM, 1998, 45(6): 965-981

[7] Gertner Y, Ishai Y, Kushilevitz E, Malkin T. Protecting data privacy in private information retrieval schemes//Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC), ACM Press, 1998: 151-160

[8] 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

[9] Wei Fu-Shan, Ma Chuan-Gui, Cheng Qing-Feng. Gateway-oriented password authenticated key exchange based on RSA. Chinese Journal of Computers, 2011, 34(1): 38-46(in Chinese)
(魏福山，马传贵，程庆丰. 基于 RSA 的网关口令认证密钥交换协议. 计算机学报，2011，34(1)：38-46)

[10] Wei F S, Ma C G, Cheng Q F. Anonymous gateway-oriented password authenticated key exchange based on RSA. EURASIP Journal on Wireless Communications and Networking, 2011: 162

[11] Wei F S, Ma C G, Zhang Z F. Gateway-oriented password-based authenticated key exchange with stronger security//Proceedings of the Advances in ProvSec 2011. Xi′an, China, 2011. LNCS6980. Berlin: Springer-Verlag, 2011: 366-379

[12] 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

[13] Abdalla M, Fouque P A, Pointcheval D. Password-based authenticated key exchange in the three-party setting//Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, 2005. LNCS3386. Berlin: Springer-Verlag, 2005: 65-86

[14] Shin S H, Kobara K, Imai H. Threshold anonymous password-authenticated key exchange secure against insider attacks. IEICE Transactions on Fundamentals, 2011, E94-D(11): 2095-2110

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

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 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) 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 (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.

Client anonymity is an important research issue in GPAKE protocols. Many of the privacy problems that arise out of Internet use can be solved using anonymous Internet connections such that a client's actions are unlinkable. Implementing anonymity of clients not only protects their personal information but also reduces the chances of attacks based on impersonation. However, the design of anonymous GPAKE protocols is much less understood. The approach of designing GPAKE protocols with client anonymity is far from maturity and perfection. Currently, there are few research papers on anonymous GPAKE protocols. Existing solutions either are inefficient or have security weaknesses. There is a need for significant theoretical progresses for anonymous GPAKE protocols.

Research issues of this paper focus on how to design strongly secure and efficient GPAKE protocols with client anonymity. We first investigate anonymous 2-party PAKE protocols, and choose an efficient solution as our start point to design our protocol. Then we presents a GPAKE protocol with strong client anonymity based on the Diffie-Hellman key exchange, and proves its security under the standard DDH assumption in the random oracle model. The new protocol can resist the undetectable on-line dictionary attack and is quite efficient in terms of computation. As far as we know, our protocol is more efficient and secure than other related protocols.