软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(9):2389−2399 [doi: 10.13328/j.cnki.jos.004861]

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

标准模型下高效的三方口令认证密钥交换协议*

魏福山[1,2,3], 马建峰[1], 李光松[3], 马传贵[3]

[1](西安电子科技大学 计算机学院,陕西 西安 710071)

[2](密码科学技术国家重点实验室,北京 100878)

[3](数学工程与先进计算国家重点实验室,河南 郑州 450001)

通讯作者: 魏福山, E-mail: weifs831020@163.com

摘 要: 三方口令认证密钥交换协议允许两个分别与服务器共享不同口令的用户在服务器的协助下建立共享的会话密钥,从而实现了用户间端到端的安全通信.现阶段,多数的三方口令认证密钥交换协议都是在随机预言模型下可证明安全的.但在实际应用中,利用哈希函数对随机预言函数进行实例化的时候会给随机预言模型下可证明安全的协议带来安全隐患,甚至将导致协议不安全.以基于 ElGamal 加密的平滑投射哈希函数为工具,在共同参考串模型下设计了一种高效的三方口令认证密钥交换协议,并且在标准模型下基于 DDH 假设证明了协议的安全性.与已有的同类协议相比,该协议在同等的安全假设下具有更高的计算效率和通信效率,因此更适用于大规模的端到端通信环境.

关键词: 三方口令协议;标准模型;平滑投射哈希函数;DDH 假设

中图法分类号: TP309

中文引用格式: 魏福山,马建峰,李光松,马传贵.标准模型下高效的三方口令认证密钥交换协议.软件学报,2016,27(9):2389−2399. http://www.jos.org.cn/1000-9825/4861.htm

英文引用格式: Wei FS, Ma JF, Li GS, Ma CG. Efficient three-party password-based authenticated key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2016,27(9):2389−2399 (in Chinese). http://www.jos.org.cn/1000-9825/4861.htm

Efficient Three-Party Password-Based Authenticated Key Exchange Protocol in the Standard Model

WEI Fu-Shan[1,2,3], MA Jian-Feng[1], LI Guang-Song[3], MA Chuan-Gui[3]

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

[2](State Key Laboratory of Cryptology, Beijing 100878, China)

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

Abstract: Three-party password authenticated key exchange (3PAKE) protocols allow two clients to establish a common session key via the help of an authentication server. Each client only needs to share a password with the server. The derived session key can be later used to achieve end-to-end secure communications. Most of the existing 3PAKE protocols are proven secure in the random oracle model.

* 基金项目: 国家自然科学基金(61309016, 61379150,61201220, U1135002, U1405255); 国家高技术研究发展计划(863) (2015AA016007); 中国博士后科学基金(2014M562493); 陕西省博士后科学基金; 信息保障技术重点实验室开放课题(KJ-13-02); 高校基本业务费项目(JB161501); 河南省科技攻关重点项目(092101210502, 122102210126)

Foundation item: National Natural Science Foundation of China (61309016, 61379150, 61201220, U1135002, U1405255); National High-Tech R&D Program of China (863) (2015AA016007); China Postdoctoral Science Foundation (2014M562493); Shaanxi Province Postdoctoral Science Foundation; The Funding of Science and Technology on Information Assurance Laboratory (KJ-13-02); Fundamental Research Funds for the Central Universities (JB161501); Key Scientific and Technological Project of He'nan Province (092101210502, 122102210126)

收稿时间: 2014-12-29; 修改时间: 2015-03-30; 采用时间: 2015-05-14

However, these protocols may turn out to be insecure in real applications when the random oracle function is instantiated with a concrete hash function. In this paper, an efficient 3PAKE protocol is proposed using smooth projective hash function based on ElGamal public key encryption. The security of the proposed protocol is conducted in the standard model under the DDH assumption. Compared with other related protocols, this protocol is quite efficient in terms of computation and communication costs under the same security assumption, and as a result, it is more suitable for large-scale end-to-end communication environments.

Key words: three-party password key exchange protocol; standard model; smooth projective hash function; DDH assumption

随着云计算技术的迅速发展,用户可以通过互联网享受到各种便捷的服务,越来越多的用户将个人数据外包存储于云服务器端.但是,数据所有权和管理权的分离使得用户数据面临泄露和被篡改的风险.为了保护用户的数据安全和个人隐私,需要安全的认证机制来实现对服务器的访问控制.认证密钥交换协议可以在认证用户身份的同时建立安全的共享密钥,进而实现安全的通信,因此在访问控制中有非常重要的应用.密钥交换协议的认证机制主要包括公钥、对称密钥和口令.口令由于其简单易记、使用便捷和代价低廉等优势成为当前网络中应用最广泛的认证机制.自 Bellovin 和 Merritt 提出著名的加密密钥交换协议(encrypted key exchange protocol)以来[1],口令认证密钥交换协议(简称 PAKE 协议)得到了广泛的关注,很多两方 PAKE 协议被提出[2−6].

两方 PAKE 协议适用于用户-服务器的认证框架,但是不满足大规模端到端通信的应用需求.假如某个用户想与 n 个不同的其他用户分别通过口令进行安全通信,那么就需要记忆 n 个不同的口令,这对于人脑来说是难以承受的负担.为了利用口令实现大规模的端到端通信,Lin 等人提出了针对用户-服务器-用户框架下的三方 PAKE 协议[7,8].三方 PAKE 协议允许分别与服务器共享口令的两个用户在服务器的协助下建立安全的共享密钥.与两方 PAKE 协议相比,三方 PAKE 不仅要抵抗在线字典攻击和离线字典攻击,还需要考虑一种特有的不可检测在线字典攻击,因此设计难度更大.2005 年,Abdalla 等人对可证明安全的三方 PAKE 协议开展了研究[9].他们首先提出了著名的 ROR(Real-Or-Random)模型,然后设计了一种利用两方 PAKE 协议构造三方 PAKE 的通用构造方法,并在 ROR 模型下证明了其安全性.同年,Abdalla 等人又设计了一个高效的三方 PAKE 协议,并且在随机预言模型下给出了安全性证明[10].但是在 2006 年,Wang 等人指出,Abdalla 等人提出的三方 PAKE 协议[9,10]都不能抵抗不可检测在线字典攻击.Wang 等人通过增加消息认证码的方式对 Abdalla 等人的协议进行了改进[11].此后,有大量在随机预言模型下可证明安全的三方 PAKE 协议被相继提出[12−18].

随机预言模型作为安全证明的一种重要模型,对于协议的安全性具有重要的检验作用.但是随机预言函数在现实中并不存在,随机预言模型下可证明安全的协议在实际应用时只能通过具有良好密码学性质的哈希函数来替代随机预言函数,但这样的替代可能会给协议带来安全隐患.例如,Canetti 等人给出了一个在随机预言模型下安全,但通过哈希函数对随机预言函数进行实例化时却不安全的签名方案[19].与随机预言模型相比,标准模型不需要将协议中使用的哈希函数理想化为真随机函数,是更为自然的协议分析模型.因此,尽管随机预言模型下可证明安全的协议通常具有更高的效率,人们还是更青睐标准模型下可证明安全的协议.2009 年,Kwon 等人[20]提出了首个标准模型下可证明安全的三方 PAKE 协议,并且基于 HDH 假设证明了协议的安全性.2012 年,Yang 等人[21]提出了标准模型下可证明安全的三方 PAKE 协议,然后在 DDH 假设下证明了协议的安全性.但是文献[20,21]中的协议都假设服务器拥有公钥,用户需要储存并验证服务器的公钥,因此用户不能仅仅通过记忆口令实现认证,违背了口令协议便捷性的优势.2014 年,Nam 等人[22]利用两方 PAKE 协议设计了一个可证明安全的三方 PAKE 协议,但是该协议计算效率和通信效率都很低.到目前为止,标准模型下可证明安全的三方 PAKE 协议还很少,已有的协议或者假设服务器拥有公钥[20,21],或者效率较低[22].针对已有协议存在的不足,我们以基于 ElGamal 加密的平滑投射哈希函数为工具设计了一个安全高效的三方 PAKE 协议,并且在标准模型下,基于 DDH 假设证明了协议的安全性.与已有的协议相比,我们的协议不需要假设服务器拥有公钥,并且具有较高的通信效率和计算效率,因此更符合大规模端到端通信的应用需求.

本文第 1 节回顾预备知识和证明所需的安全模型.第 2 节给出我们所设计的标准模型下的三方 PAKE 协议并证明其安全.第 3 节给出我们的协议与其他相关协议的安全性和效率比较.最后,第 4 节总结全文.

1 预备知识

1.1 平滑投射哈希函数

平滑投射哈希函数(smooth projective hash function)最早由 Cramer 和 Shoup[23]在设计 CCA 安全的公钥加密算法时提出.之后,平滑投射哈希函数作为一个密码学基本组件被广泛用于构造安全的 PAKE 协议、非延展的承诺体制以及不经意传输协议等.设 X 是平滑投射哈希函数的定义域,NP 语言 L 是 X 的一个真子集.平滑投射哈希函数最重要的性质是对于子集 L 中的元素 x,函数的输出可以分别通过全局密钥和公开的投射密钥这两种方式来计算.全局密钥可以用于计算整个定义域 X 上的所有函数输出;而投射密钥只对子集 L 中的元素有效,并且计算函数输出时还需要 $x\in L$ 的一个证据 w.

一个平滑投射哈希函数由以下 5 个算法($SPHFSetup$;$HashKG$;$ProjKG$;$Hash$;$ProjHash$)组成:

- $SPHFSetup(1^k)$:输入安全参数 k,产生方案的全局参数 $param$ 以及对 NP 语言 L 的描述;
- $HashKG(L;param)$:输入全局参数 $param$ 和 NP 语言 L,生成全局密钥 hk;
- $ProjKG(hk;L;param;x)$:根据全局密钥 hk 和 NP 语言 L 中的元素 x 计算投射密钥 hp;
- $Hash(hk;L;param;x)$:根据全局密钥 hk 和元素 x 计算函数输出;
- $ProjHash(hp;L;param;x;w)$:根据投射密钥 hp、元素 x 以及证据 w 计算函数输出.

一个平滑投射哈希函数应该满足以下性质:

- 正确性:给定 $x\in L$ 以及证据 w,那么对于所有的全局密钥 hk 以及相应的投射密钥 hp,我们有:
$$Hash(hk;L;Param;x)=ProjHash(hp;L;Param;x;w);$$
- 平滑性:对于所有的 $x\in X\backslash L$,分布 $\Delta_0=\{(L,param,x,hp,v):v=Hash(hk,L,param,x)\}$ 和 $\Delta_1=\{(L,param,x,hp,v):v\in\{0,1\}^k\}$ 是统计不可区分的;
- 伪随机性:对于 $x\in L$,在无证据 w 的条件下,分布 $\Delta_0=\{(L,param,x,hp,v):v=Hash(hk,L,param,x)\}$ 和 $\Delta_1=\{(L,param,x,hp,v):v\in\{0,1\}^k\}$ 是计算不可区分的.

1.2 安全模型

本节简单回顾 Kwon 等人提出的三方 PAKE 协议的安全模型[20],我们将在第 2 节给出所设计协议在此模型下的安全性证明.

三方 PAKE 协议的参与者集合有两类,分别是用户集 $\mathcal{U}$ 和服务器集 $\mathcal{S}$.每个用户 $U\in\mathcal{U}$ 拥有一个与服务器共享的、从口令空间 D 中随机选择的口令 pw_U.服务器持有一个口令向量 $pw_S=\langle pw_U\rangle_{U\in\mathcal{U}}$,其中每一项对应于在服务器端注册的某个用户的口令.每个用户可以并行地执行协议的多个会话实例,用 U^i 表示用户 U 的第 i 个实例.我们通过谕示询问来模拟攻击者的能力.

- $Execute(U_1^{i_1},S^j,U_2^{i_2})$:此询问模拟攻击者的被动攻击能力.攻击者通过此询问,可以获得用户实例 $U_1^{i_1}$ 和 $U_2^{i_2}$ 以及服务器实例 S^j 的协议运行的所有交互的消息;
- $Reveal(U^i)$:此询问模拟已知密钥攻击或会话密钥丢失.攻击者通过此询问,可以获得用户实例 U^i 持有的会话密钥;
- $SendClient(U^i,m)$:此询问模拟攻击者对于用户实例 U^i 的主动攻击.攻击者冒充服务器给用户实例 U^i 发送消息 m,并得到用户实例 U^i 接收到消息 m 后返回的消息;
- $SendServer(S^j,m)$:此询问模拟攻击者对于服务器实例 S^j 的主动攻击.攻击者冒充用户给服务器实例 S^j 发送消息 m,并得到服务器实例 S^j 接收到消息 m 后返回的消息;
- $Corrupt(U)$:此询问用于刻画前向安全.攻击者通过此询问,可以获得用户 U 的口令并且控制用户 U;
- $Test(U^i)$:此询问不模拟攻击者的实际攻击能力,而是用于刻画协议会话密钥的语义安全.对于用户实例 U^i,如果该实例没有生成会话密钥,那么返回无定义的符号 $\perp$;否则进行一次均匀的抛币:
  - 如果抛币结果是 1,则返回实例 U^i 的真实会话密钥;
  - 如果抛币结果是 0,那么返回一个与会话密钥等长的随机数;

攻击者需要猜测抛币的结果,即猜测其获得的是真实的会话密钥还是随机数;

- *TestPair*(U_1^i,U_2^j) :此询问不模拟攻击者的实际攻击能力,而是用于刻画协议会话密钥针对服务器的密钥私密性.若用户实例 U_1^i 和 U_2^j 不共享会话密钥,那么返回无定义的符号⊥;否则进行一次均匀的抛币:
  - 如果抛币结果是 1,则返回真实会话密钥;
  - 如果抛币结果是 0,那么返回一个与会话密钥等长的随机数.

  攻击者需要猜测抛币的结果,即猜测其获得的是真实的会话密钥还是随机数.

如果一个用户实例 U^i 接受协议运行并生成会话密钥,那么我们称该实例接受(accepted).如果攻击者对一个接受的实例 U^i 进行了 *Reveal*(U^i)查询,我们称该实例被打开(opened).我们定义会话标示 *sid* 为两个用户在协议完成时所交互消息中的共享消息的级联.我们称两个用户实例 U_1^i 和 U_2^j 是伙伴,如果以下条件成立:(1) 实例 U_1^i 和 U_2^j 都接受;(2) 实例 U_1^i 和 U_2^j 的会话标示 *sid* 相同;(3) 实例 U_1^i 的意定通信方是 U_2^j,反之亦然;(4) 除了 U_1^i 和 U_2^j 之外,没有任何接受实例的意定通信方是 U_1^i 或者 U_2^j.我们称一个诚实用户的实例 U_1^i 是新鲜的,如果以下的条件成立:(1) 实例 U_1^i 接受;(2) 攻击者没有对实例 U_1^i 或其伙伴实例(如果存在的话)进行 *Reveal* 查询;(3) 在实例 U_1^i 结束协议运行之前,攻击者没有对用户 U_1 及其伙伴(如果存在的话)进行 *Corrupt* 查询.

为了考虑协议会话密钥的语义安全性,我们给攻击者 $\mathcal{A}$ 所有谕示询问的能力,但限定攻击者只能对新鲜的会话进行一次 *Test* 询问.记 *Test* 询问中的抛币结果为 *b*,如果攻击者正确猜测到 *b* 的值,则认为攻击者成功,记该事件为 *Succ*.攻击者 $\mathcal{A}$ 破坏协议 $\mathcal{P}$ 的语义安全性的优势定义为 $Adv_{\mathcal{P},\mathcal{D}}^{ake-fs}(\mathcal{A})=2\cdot\Pr[Succ]-1$.类似地,我们定义攻击者破坏协议 $\mathcal{P}$ 的语义安全性的优势函数为 $Adv_{\mathcal{P},\mathcal{D}}^{ake-fs}(t,R)=\max\{Adv_{\mathcal{P},\mathcal{D}}^{ake-fs}(\mathcal{A})\}$,其中,最大值遍历所有攻击时间为多项式时间、所使用资源为 *R* 的攻击者 $\mathcal{A}$.我们称三方 PAKE 协议 $\mathcal{P}$ 是语义安全的,如果 $Adv_{\mathcal{P},\mathcal{D}}^{ake-fs}(t,R)$ 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* 为常数.

由于三方 PAKE 协议中用户之间的会话密钥是由服务器协助生成的,为了降低对服务器的信任程度,需要考虑会话密钥对于诚实而好奇的服务器的密钥私密性.即:服务器在没有进行主动攻击的条件下,会话密钥对于服务器来说仍然是不可区分的.考虑一个知道所有用户口令的攻击者 $\mathcal{A}$,我们给攻击者 $\mathcal{A}$ 所有谕示询问的能力,但是攻击者 $\mathcal{A}$ 不能对测试会话 *TestPair*(U_1^i,U_2^j) 进行主动攻击.类似地,我们可以定义攻击者 $\mathcal{A}$ 破坏协议 $\mathcal{P}$ 的会话私密性的优势 $Adv_{\mathcal{P},\mathcal{D}}^{kp}(\mathcal{A})=2\cdot\Pr[Succ]-1$ 以及优势函数 $Adv_{\mathcal{P},\mathcal{D}}^{kp}(t,R)=\max\{Adv_{\mathcal{P},\mathcal{D}}^{kp}(\mathcal{A})\}$.我们称三方 PAKE 协议实现了针对服务器的密钥私密性,如果优势函数 $Adv_{\mathcal{P},\mathcal{D}}^{kp}(t,R)$ 是关于安全参数的一个可忽略的函数.

2 标准模型下的三方 PAKE 协议

2.1 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;*pk* 是定义在群 G_q 上的一个 CCA 加密算法 *E* 的公钥.需要说明的是:在系统中,任何人都不知道 *pk* 对应的私钥.我们用 $E_{pk}[m,r]$ 表示用公钥 *pk* 对消息 *m* 进行加密,其中,*r* 是加密时所用的随机数.我们用 $Enc_k(m)$ 和 $Dec_k(m)$ 分别表示使用对称加密算法对消息 *m* 利用密钥 *k* 进行加密和解密操作.$UH:G_q\to\{0,1\}^{3n}$ 是从通用哈希函数簇 $\mathcal{UH}$ 中随机选择的通用哈希函数,$H:\{0,1\}^*\to\{0,1\}^n$ 是防碰撞的哈希函数,其中,*n* 是安全参数.用户 *A* 和服务器 *S* 共享口令 pw_A,用户 *B* 和服务器 *S* 共享口令 pw_B.为了简便起见,我们假设口令空间被映射到 Z_q^* 中,即,$pw_A, pw_B\in Z_q^*$.协议共有 3 轮消息交互,具体的流程如下:

第 1 轮.用户 *A* 选择一个随机数 $x\in Z_q^*$,然后计算 $X_1=g^x$ 以及 $X_2=h^x g^{pw_A}$.这里,X_1 和 X_2 实质上是利用 ElGamal 加密算法对口令 pw_A 进行加密后的密文.用户 *A* 发送消息(A,X_1,X_2)给服务器 *S*.类似的,用户 *B* 选择一个随机数 $y\in Z_q^*$,计算 $Y_1=g^y$ 以及 $Y_2=h^y g^{pw_B}$,并且发送消息(B,Y_1,Y_2)给服务器 *S*.

第 2 轮.服务器 *S* 接收到来自用户 *A* 和 *B* 的消息后,首先选择两个随机数 $\lambda_1,\lambda_2\in Z_q^*$,然后计算 $\mu=g^{\lambda_1}h^{\lambda_2}$,

$X_2'=X_2g^{-pw_A}$,$Y_2'=Y_2g^{-pw_B}$,$\sigma_A=X_1^{\lambda_1}X_2'^{\lambda_2}$ 和 $\sigma_B=Y_1^{\lambda_1}Y_2'^{\lambda_2}$.这里,$\lambda_1$ 和 λ_2 为基于 ElGamal 加密算法的平滑投射函数的全局密钥,μ是对应的投射密钥.σ_A 和 σ_B 则是服务器分别与用户 A 和 B 共享的平滑投射哈希函数的输出.此外,服务器 S 还选择随机数 $z\in Z_q^*$ 并计算 $X_1^*=X_1^z$ 以及 $Y_1^*=Y_1^z$.服务器 S 计算通用哈希函数的输出 $r_A||\tau_{A1}||\tau_{A2}=UH(\sigma_A)$和 $r_B||\tau_{B1}||\tau_{B2}=UH(\sigma_B)$.这里,$r_A$ 和 r_B 分别用于 CCA 加密算法的随机输入,τ_{A1} 和 τ_{B1} 分别用作利用对称加密算法加密随机化后的密钥材料 X_1^* 以及 Y_1^* 时的密钥,而 τ_{A2} 和 τ_{B2} 则用于实现用户向服务器的认证.服务器 S 计算密文 $C_A=Enc_{\tau_{A1}}(Y_1^*)$ 和 $C_B=Enc_{\tau_{B1}}(X_1^*)$,并用 r_A 和 r_B 作为随机输入,对 $\Sigma_A=H(X_1,X_2',C_A,\mu,A,B,S)$ 和Σ_B=$H(Y_1,Y_2',C_B,\mu,A,B,S)$ 分别进行加密得到密文ω_A 和ω_B.最后,服务器 S 分别发送消息(S,C_A,μ,ω_A)和(S,C_B,μ,ω_B)给用户 A 和 B.

第 3 轮.用户 A 接收到消息(S,C_A,μ,ω_A)后,首先利用投射密钥μ计算平滑投射哈希函数的输出$\sigma_A=\mu^x$,并计算通用哈希函数的输出 $r_A'||\tau_{A1}'||\tau_{A2}'=UH(\sigma_A)$; 用户 A 首先利用 τ_{A1}' 解密 C_A 得到 Y_1^*,并验证 ω_A 是否等于 $E_{pk}[\Sigma_A,r_A']$,如果不相等,则拒绝并结束协议运行;否则,用户 A 计算会话密钥 $K=Y_1^{*x}$ 并发送消息 (A,τ_{A2}') 给服务器 S.用户 B 和用户 A 执行类似的操作,为了简便起见,这里略去该部分描述.

最后,服务器 S 接收到消息 (A,τ_{A2}') 和 (B,τ_{B2}') 后,验证 τ_{A2}' 和 τ_{B2}' 是否有效:如果有效,则服务器 S 接受协议运行;如果无效,则说明前面的接入请求来自敌手对某个用户进行的仿冒攻击.如果服务器没有收到消息 (A,τ_{A2}') 或 (B,τ_{B2}'), 则同样认为前面的接入请求来自敌手对某个用户进行的仿冒攻击,服务器将采取进一步的措施(如限制用户认证次数等)以保护用户口令(如图 1 所示).

注:两个用户 A 和 B 在发送最后一轮消息时,已经建立了共享的会话密钥用于后续的安全通信.第 3 轮消息的目的在于用户向服务器证明其合法身份,从而达到双向认证和抵抗不可检测在线字典攻击的目的.

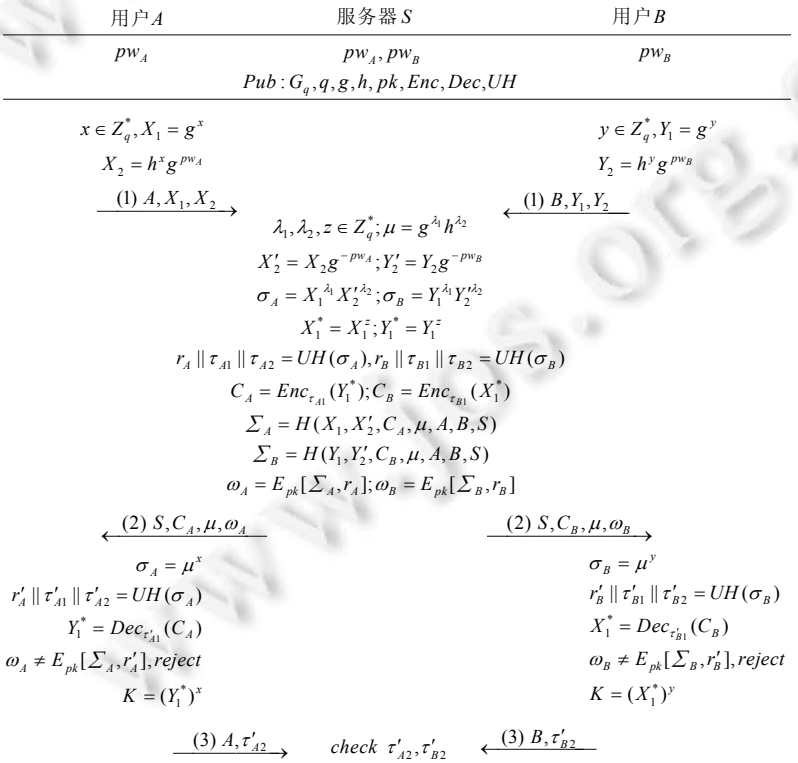

Fig.1 An efficient 3PAKE protocol in the standard model

图 1 标准模型下高效的三方口令协议

2.2 安全性证明

本节给出我们所设计的三方 PAKE 协议的语义安全性的证明.

定理 1. 假设$\mathcal{A}$是一个运行时间为 t,并且进行了 q_{send} 次主动攻击的概率多项式敌手.假设 DDH 假设在循环群 G_q 中成立,协议中所使用的对称加密算法满足对于单次加密的 CPA 安全性,并且公钥加密算法 E 是 CCA 安全的,那么敌手$\mathcal{A}$攻击本文的三方 PAKE 协议的语义安全的优势至多为

$$Adv_{\mathcal{P},\mathcal{D}}^{ake-fs}(\mathcal{A}) \leqslant \frac{q_{send}}{|\mathcal{D}|} + neg(n),$$

其中,$neg(n)$表示关于安全参数 n 的一个可忽略函数.

证明:本定理的证明由一系列混合实验组成:第 1 个实验从真实的攻击游戏开始,然后逐步对攻击游戏中的模拟规则进行修改,并估计两个相邻实验之间敌手优势差距的上界,直到敌手的攻击优势为 0 的实验结束.我们首先修改被动攻击的模拟规则,使得被动攻击中不泄露任何口令信息并且会话密钥完全随机,然后逐步修改主动攻击中的模拟规则,使得只有敌手正确猜测口令的条件下才有可能赢得攻击游戏.我们用 $Adv(\mathcal{A},P_i)$表示敌手$\mathcal{A}$在第 i 个混合实验中的优势.

实验 P_0:这个实验模拟了攻击游戏在标准模型下的真实运行.根据敌手优势的定义有:

$$Adv_{\mathcal{P},\mathcal{D}}^{ake-fs}(\mathcal{A}) = Adv(\mathcal{A},P_0).$$

实验 P_1:从这个实验开始,我们开始修改对敌手进行的被动攻击 *Execute* 询问的模拟规则.对于敌手$\mathcal{A}$进行的 $Execute(A^{i_1},S^j,B^{i_2})$ 询问,我们令用户 A 正常计算 $X_1=g^x$,但是在计算 X_2 时,使用在口令空间之外随机选择的一个虚假口令 pw_A^*,即, $X_2 = h^x g^{pw_A^*}$. 类似地,用户 B 也用虚假口令 pw_B^* 计算 $Y_2 = h^y g^{pw_B^*}$.服务器 S 在模拟时直接令 $X_2' = h^x$ 和 $Y_2' = h^y$,并计算 $\sigma_A = X_1^{\lambda_1} h^{x\lambda_2}$ 和 $\sigma_B = Y_1^{\lambda_1} h^{y\lambda_2}$. 其余的模拟规则与真实的攻击游戏完全相同.显然,如果存在敌手能够以不可忽略的概率区分实验 P_1 和实验 P_0,那么我们可以构造算法以相同的优势攻破 ElGamal 加密算法的 CPA 安全性.这个规约非常直观,因此这里不再赘述.由 ElGamal 加密算法的 CPA 安全性,我们有:

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

实验 P_2:在这个实验中,我们继续修改对敌手进行的 *Execute* 询问的模拟规则.对于敌手$\mathcal{A}$进行的 $Execute(A^{i_1},S^j,B^{i_2})$ 询问,我们在实验 P_1 修改的基础上进一步从循环群 G_q 中随机选择σ_A和σ_B的值.由于在实验 P_1 中,对于 *Execute* 询问的模拟使用的是虚假的口令,因此由基于 ElGamal 加密算法的平滑投射哈希函数的平滑性保证了σ_A和σ_B的分布与 G_q 上的均匀分布是统计不可区分的.根据平滑投射哈希函数的平滑性,敌手区分实验 P_1 和实验 P_2 的优势是可忽略的.我们有:

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

实验 P_3:在这个实验中,我们继续修改对敌手进行的 *Execute* 询问的模拟规则.对于敌手$\mathcal{A}$进行的 $Execute(A^{i_1},S^j,B^{i_2})$ 询问,我们令服务器 S 随机选择适当长度的 $r_A\|\tau_{A1}\|\tau_{A2}$ 和 $r_B\|\tau_{B1}\|\tau_{B2}$,而不是通过通用哈希函数簇计算.相应地,我们令用户端的相应值与 $r_A\|\tau_{A1}\|\tau_{A2}$ 和 $r_B\|\tau_{B1}\|\tau_{B2}$ 一致.由通用哈希函数簇的性质可知:当其输入为 G_q 中的随机值时,通用哈希函数簇的输出与其值域中的均匀分布式统计不可区分的,因此有:

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

实验 P_4:在这个实验中,我们继续修改对敌手进行的 *Execute* 询问的模拟规则.对于敌手$\mathcal{A}$进行的 $Execute(A^{i_1},S^j,B^{i_2})$ 询问,我们进一步令服务器在计算 CCA 加密算法 E 的密文 ω_A 和 ω_B 时,将输入中的 X_2' 和 Y_2' 用 G_q 中的两个随机值来替代.由于在实验 P_3 中,我们随机选择了加密时所用的随机输入 r_A 和 r_B,因此,实验 P_4 和上一个实验的差别至多是敌手攻破加密算法 E 的 CCA 安全的优势.其实,这里仅用到 CCA 加密算法 E 的 CPA 安全性.与实验 P_1 的分析类似,我们有:

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

实验 P_5:在这个实验中,我们最后一次修改对敌手进行的 *Execute* 询问的模拟规则.首先,在产生公共参数中的 h 时,我们随机选择 $s \in Z_q^*$ 并令 $h=g^s$.此外,对于敌手$\mathcal{A}$进行的 $Execute(A^{i_1},S^j,B^{i_2})$ 询问,我们选择 G_q 中的一个随

机值作为会话密钥,而不是通过 $K=Y_1^{*x}$ 或者 $K=X_1^{*y}$ 来计算.实验 P_5 和上一个实验的差距至多是敌手攻破 DDH 假设的优势.给定一个 DDH 实例(U,V,W),我们利用 DH 问题的自归约性来证明上述结论.为了模拟 $Execute(A^{i_1},S^j,B^{i_2})$ 询问,我们首先随机选择 $a_1,a_2,b_1,b_2\in Z_q^*$, 然后令 $X_1=U^{a_1}g^{a_2}$ 以及 $Y_1=U^{b_1}g^{b_2}$. 由于我们令 $h=g^s$,因此可以按照实验 P_4 的规则正常模拟 *Execute* 询问的剩余步骤.最后计算会话密钥的时候,定义会话密钥 $K=(W^{a_1b_1}\cdot U^{a_1b_2}\cdot V^{a_2b_1}\cdot g^{a_2b_2})^z$.显然,如果 $W=CDH(U,V)$,那么上述模拟与实验 P_4 完全一致;如果 $W\neq CDH(U,V)$,那么上述模拟与实验 P_5 一致.如果存在敌手可以以不可忽略的优势区分实验 P_4 和 P_5,那么我们可以以同样的优势攻破 DDH 假设.我们有:

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

从实验 P_5 中,我们已经完成了对 *Execute* 询问的模拟规则的修改.敌手不能通过 *Execute* 询问获得用户口令的任何信息,因为在 *Execute* 询问的模拟中我们使用了虚假的无效口令,因此在 *Execute* 询问的会话模拟中不包含真实口令的任何信息;此外,由于 *Execute* 询问的会话密钥是随机选择的,因此敌手通过 *Execute* 询问进行攻击的优势是可忽略的.从下一个实验开始,我们对敌手进行的主动攻击的模拟规则进行修改.

在下一个实验开始之前,我们先进行一些预备工作.如果一条消息是诚实的参与者生成的,即使敌手转发了该消息,依然称该消息是实例产生的;否则,称该消息是敌手产生的.我们用 $Send_0(A,B,S)$表示敌手要求用户开始执行协议的初始激活消息;用 $SendClient_i(U,m)$表示敌手在某个会话的第 i 轮通信中冒充服务器给用户 U 发送消息 m,用 $SendServer_i(S,m)$表示敌手在某个会话的第 i 轮通信中冒充用户给用户 S 发送消息 m.在产生公开参数时,除了令 $h=g^s$ 外,我们还在产生公开参数中加密算法 E 的公钥 pk 的同时,记录其对应的私钥 sk.

实验 P_6:从这个实验开始,我们对敌手进行的主动攻击 *Send* 询问的模拟规则进行修改.对于敌手伪造服务器的消息并对诚实用户 A(对于用户 B 的模拟类似)进行的 $SendClient_2(A^{i_1},C_A\|\mu\|\omega_A)$ 询问,假设(A,X_1,X_2)是用户 A 上一轮通信中对应于 $Send_0(A^{i_1},B^{i_2},S^j)$ 的回答,我们直接用密钥 sk 对 ω_A 解密,并验证解密得到的消息是否等于 $H(X_1,X_2',C_A,\mu,A,B,S)$,其中, $X_2'=X_2g^{-pw_A}$.如果上述验证通过,则认为敌手攻击成功并结束攻击游戏的模拟;如果验证不通过,则拒绝该消息并停止对用户实例 A^{i_1} 的模拟.注意:对于敌手简单重放而没有进行修改的消息,这里的模拟规则与实验 P_5 相同.实验 P_6 和 P_5 相比,只是增加了敌手成功的一种方式,因此,敌手在实验 P_6 的优势将会增加.我们有:

$$|Adv(\mathcal{A},P_5)|\leqslant Adv(\mathcal{A},P_6).$$

实验 P_7:在这个实验中,我们对敌手进行的 $Send_0(A^{i_1},B^{i_2},S^j)$ 询问的模拟进行修改.对于未被腐化的用户 A(或 B)接收到 $Send_0(A^{i_1},B^{i_2},S^j)$ 后,类似于实验 P_1,我们在计算消息(A,X_1,X_2)(或消息(B,Y_1,Y_2))时采用虚假的口令 pw_A^* (或 pw_B^*).为了保证模拟的一致性,如果敌手在 $SendClient_2(A^{i_1},C_A\|\mu\|\omega_A)$ 的询问中只是简单转发了服务器产生的消息,那么我们令用户 A 将服务器在模拟时产生的 $r_A\|\tau_{A1}\|\tau_{A2}$ 作为自己通用哈希函数的输出;否则类似于实验 P_6,我们对消息中密文 ω_A 进行解密来判断敌手是否成功.实验 P_7 和 P_6 的差别和敌手攻破 DDH 假设的优势相等.与实验 P_1 的分析类似,我们有:

$$|Adv(\mathcal{A},P_7)-Adv(\mathcal{A},P_6)|\leqslant neg(n).$$

实验 P_8:在这个实验中,我们对敌手冒充诚实用户 A 进行的 $SendServer_1(S^j,A\|X_1\|X_2)$询问的模拟进行修改(敌手冒充诚实用户 B 的模拟类似).我们直接利用 h 对应于 g 的离散对数 s 对 X_2 进行解密,如果解密得到正确的口令,那么结束整个攻击游戏,得模拟并认为敌手成功.与实验 P_6 类似,敌手在这个实验里面只是增加了一种赢得攻击游戏的方式,因此敌手的优势将增加:

$$|Adv(\mathcal{A},P_7)|\leqslant Adv(\mathcal{A},P_8).$$

实验 P_9:在这个实验中,我们对敌手冒充诚实用户 A 进行的 $SendServer_1(S^j,A\|X_1\|X_2)$询问的模拟继续进行修改(敌手冒充诚实用户 B 的模拟类似).我们利用 s 对 X_2 进行解密后,如果得到正确的口令,则认为敌手赢得了攻击游戏;如果解密得到的不是正确的口令,那么从循环群 G_q 中随机选择σ_A 的值.由于敌手对于诚实用户 A 的口令猜测错误,因此根据平滑投射哈希函数的平滑性,有:

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

实验 P_{10}:在这个实验中,我们对敌手冒充诚实用户 A 进行的 $SendServer_1(S^j,A||X_1||X_2)$询问的模拟继续进行修改(敌手冒充诚实用户 B 的模拟类似).我们利用 s 对 X_2 进行解密后,如果得到正确的口令,则认为敌手赢得攻击游戏;否则在实验 P_9 的模拟规则的基础上,进一步随机选择 $r_A||\tau_{A1}||\tau_{A2}$.由通用哈希函数簇的性质可知:当输入为 G_q 的随机值的时候,通用哈希函数簇的输出与其值域中的均匀分布是统计不可区分的.因此,我们有:

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

实验 P_{11}:在这个实验中,我们对敌手冒充诚实用户 A 进行的 $SendServer_1(S^j,A||X_1||X_2)$询问的模拟最后一次进行修改(敌手冒充诚实用户 B 的模拟类似).在实验 P_{10} 模拟规则的基础上,我们在在计算 CCA 加密算法的密文 ω_A 时,采用在 G_q 中随机选择的值来替代 X_2',从而保证在敌手没有猜测到正确口令的主动攻击中得不到关于用户口令的任何信息.实验 P_{11} 与实验 P_{10} 的差别至多是敌手攻破公钥加密算法 E 的 CCA 安全的优势.

与实验 P_4 的分析类似,但是这里我们需要用到公钥加密算法 E 的 CCA 安全性.原因在于:根据我们对敌手进行的 $SendClient_2(A^h,C_A\|\mu\|\omega_A)$ 的模拟规则,需要利用 CCA 攻击游戏中的解密谕示帮助我们解密消息中密文 ω_A,从而判断敌手是否成功.根据公钥加密算法 E 的 CCA 安全性,我们有:

$$|Adv(\mathcal{A},P_{11})-Adv(\mathcal{A},P_{10})|\leqslant neg(n).$$

实验 P_{12}:在这个实验中,我们对敌手冒充诚实用户 A 进行的 $SendServer_3(S^j,A\|\tau'_{A2})$ 询问的模拟进行修改(敌手冒充诚实用户 B 的模拟类似).如果敌手伪造的 τ'_{A2} 与我们随机选择的 τ_{A2} 相等,那么我们认为敌手成功.

显然,如果敌手在 $SendServer_1(S^j,A||X_1||X_2)$在猜测到正确的口令,我们已经令敌手获胜;如果敌手发送 $SendServer_3(S^j,A\|\tau'_{A2})$,说明敌手在第 1 轮消息中没有猜到正确的口令.根据模拟规则,我们将从值域中随机选择 $r_A||\tau_{A1}||\tau_{A2}$,因此,敌手正确猜测到 τ_{A2} 的概率是可忽略的.我们有:

$$|Adv(\mathcal{A},P_{12})-Adv(\mathcal{A},P_{11})|\leqslant neg(n).$$

实验 P_{13}:在这个实验中,我们最后一次对敌手冒充诚实用户 A 进行的 *Send* 询问的模拟进行修改.如果敌手没有发送 $SendServer_3(S^j,A\|\tau'_{A2})$, 但是敌手从服务器在第 2 轮发送的消息$(S,C_A,\mu,\omega_A)$利用对称加密算法的密文 C_A 得到了 Y_1^*,那么我们认为敌手成功.显然,在这个实验里面,敌手多了一种获胜的方式.但是,由于我们所使用的对称加密对于单次加密是CPA安全的,而我们随机选择通用哈希函数簇的输出,因此随机选择的输出(即对称加密算法的密钥)发生碰撞的概率是可忽略的.根据对称加密的 CPA 安全性,我们有:

$$|Adv(\mathcal{A},P_{13})-Adv(\mathcal{A},P_{12})|\leqslant neg(n).$$

现在我们来分析敌手在这个实验里面赢得攻击游戏的几种方式:

- 方式 1:对于敌手产生的 $SendServer_1(S^j,A||X_1||X_2)$询问(对于敌手冒充用户 B 的模拟类似),如果对 X_2 解密后发现敌手猜测口令正确,则认为敌手赢得攻击游戏;
- 方式 2:对于敌手伪造服务器的消息并对诚实用户 A 进行的 $SendClient_2(A^h,C_A\|\mu\|\omega_A)$ 询问(对于敌手冒充用户 B 的模拟类似),如果对密文 ω_A 解密后发现该密文包含了正确的口令信息,则认为敌手赢得攻击游戏;
- 方式 3:敌手在没有正确猜测到口令的条件下,通过 $SendServer_3(S^j,A\|\tau'_{A2})$ 询问正确猜测到了 τ_{A2} 的值,同样认为敌手获胜;
- 方式 4:敌手没有通过上述的 3 种方式获胜,但是从密文 C_A 中得到了 Y_1^*,那么我们认为敌手获胜;
- 方式 5:敌手成功猜测到 *Test* 询问中所使用的随机比特.

显然,敌手通过方式 3 和方式 4 获胜的概率是可忽略的.我们用 *PwGuess* 表示事件敌手通过方式 1 或方式 2 正确猜测到口令;用 *Success* 表示事件敌手通过方式 5 猜测到 *Test* 询问中所使用的随机比特而获胜.由于我们在模拟协议运行时,在敌手没有猜测到正确口令的条件下不会在模拟中用到任何口令的信息,因此有:

$$\Pr[PwGuess]\leqslant\frac{q_{send}}{|\mathcal{D}|}.$$

如果事件 *PwGuess* 不发生,那么由于敌手通过方式 3 和方式 4 获胜的概率是可忽略的,因此敌手只能通过方式 5 赢得攻击游戏.但是,由于在敌手进行的主动攻击中,诚实用户的实例由于敌手在第 2 轮无法产生正确的消息(S,C_A,μ,ω_A)从而拒绝接受;而在被动的会话中,所有的会话密钥是随机选择的,因此敌手通过方式 5 成功的概率是$\frac{1}{2}$.忽略方式 3 和方式 4,我们有:

$$\begin{aligned}\Pr[Success] &= \Pr[Success \wedge PwGuess] + \Pr[Success \wedge \overline{PwGuess}]\\ &\leqslant \Pr[PwGuess] + \Pr[Success \mid \overline{PwGuess}] \cdot (1 - \Pr[PwGuess])\\ &= \frac{1}{2} + \frac{1}{2} \cdot \Pr[PwGuess]\\ &\leqslant \frac{1}{2} + \frac{1}{2} \cdot \frac{q_{send}}{|\mathcal{D}|}.\end{aligned}$$

综合上面所有的等式结果,定理 1 得证. □

定理 2. 假设$\mathcal{A}_{kp}$是一个运行时间为 t 并且进行了 $q_{execute}$ 次被动攻击的概率多项式敌手.假设 DDH 假设在循环群 G_q 中成立,那么敌手$\mathcal{A}_{kp}$攻击本文的三方 PAKE 协议的密钥私密性的优势至多为

$$Adv_{\mathcal{P},\mathcal{D}}^{ake-kp}(\mathcal{A}) \leqslant q_{execute} Adv_{G_q}^{DDH}(O(t)),$$

其中, $Adv_{G_q}^{DDH}(O(t))$ 表示在多项式时间内破解 DDH 假设的优势.

证明:假设$\mathcal{A}_{kp}$是一个运行时间为 t 并且进行了 $q_{execute}$ 次被动攻击的概率多项式敌手.如果$\mathcal{A}_{kp}$可以破坏协议的密钥私密性,那么我们可以通过敌手$\mathcal{A}_{kp}$的能力来解决 DDH 问题.

给定 DDH 问题的一个实例(U,V,W),我们首先根据口令空间$\mathcal{D}$的分布为所有用户选择口令并相应的选择所有的公共参数,并且将所有用户的口令告诉敌手$\mathcal{A}_{kp}$.在攻击游戏模拟阶段,我们令模拟者随机猜测 $q_{execute}$ 次被动攻击中的一次会话作为敌手$\mathcal{A}_{kp}$ 的测试会话,对于其余的会话都正常模拟.显然,猜测正确测试会话的概率为 $1/q_{execute}$.对于猜测的测试会话,我们令 $X_1=U,Y_1=V$,并且随机令服务器选择 z,计算 $X_1^* = X_1^z, Y_1^* = Y_1^z$.其余的模拟按照协议的描述执行.如果$\mathcal{A}_{kp}$ 没有选择预先选定的会话作为测试会话,则跳出本次攻击游戏的模拟;否则,当敌手$\mathcal{A}_{kp}$ 对测试会话进行 *TestPair* 询问时,我们返回 $K=W^z$ 作为回答.显然:如果(U,V,W)是 Diffie-Hellman 三元组,那么返回的是真实的会话密钥;否则,返回的是一个与会话密钥等长的随机数.此时,敌手$\mathcal{A}_{kp}$ 赢得攻击游戏的优势等同于解决 DDH 假设的优势.由于模拟者猜测正确测试会话的概率为 $1/q_{execute}$,因此定理得证. □

3 协议性能比较

在本节,我们对本文的协议和已有的标准模型下的三方口令认证密钥交换协议[20−22]从效率和安全性两个方面进行比较.

在计算代价方面,我们主要考虑计算代价较高的模幂运算(用 e 表示)和公钥加解密运算,而忽略其余的运算(诸如哈希函数、对称加密和 MAC 等).我们采用标准模型下 CCA 安全的 DHIES 公钥加密算法来对参与比较的协议中所使用的 CCA 安全的加密体制进行实例化[24],从而将公钥加解密的计算代价转化为模幂运算的个数.DHIES 算法加密时需要两个模幂运算,解密时需要一个模幂运算.由于形如 g^xh^y 的两个模幂运算的乘积可以通过一个模幂运算的代价求得,因此对于此类运算,我们只计为一个模幂运算.在通信代价方面,三方口令认证密钥交换协议多用于无线通信环境,而在无线环境下,协议的交互轮数远比通信带宽重要,因此我们主要考虑协议的执行轮数.由于文献[22]采用了模块化的设计思路,通过安全的两方 PAKE 协议来构造三方 PAKE 协议,因此我们用目前标准模型下效率最高的 Jiang 等人的两方 PAKE 协议[5]对该协议进行实例化.在安全性方面,由于参与比较的协议都提供了相同的安全属性,因此我们主要从服务器是否具有公钥证书和证明所基于的困难性假设来进行比较,其中,ODH 代表 DHIES 算法的安全性所基于的 Oracle Diffie-Hellman 假设.

从表 1 可以看出:我们的协议在计算代价方面低于 NRK 协议[22],与 YC 协议[21]的计算代价相当,而计算代价高于 KJL 协议[20],但是我们的协议在通信轮数方面要明显低于 NRK 协议.虽然 NRK 协议可以通过标准模型

下一轮的 PAKE 进行实例化从而降低轮数,但是目前,标准模型下最高效的一轮的 PAKE 中,每个参与者需要至少 12 个模幂运算[25],这将会极大增加协议的计算代价.KJL 协议虽然只需要两轮通信,并且计算效率高于我们的协议,但是该协议假设服务器拥有公钥证书,并不是完全基于口令认证的;并且,用户需要知道服务器的公钥,这将给用户的使用带来不便.

Table 1 Cost comparison with existing protocols for 3PAKE in the standard model

表 1 标准模型下三方口令协议的性能比较

比较的协议	通信轮数	计算代价			服务器公钥证书	困难性假设
		用户	服务器	总代价		
KJL 协议[20]	2	4e	2e	10e	是	DDH, ODH
YC 协议[21]	3	5e	8e	18e	是	DDH
NRK 协议[22]	6	9e	12e	30e	否	DDH
我们的协议	3	6e	9e	21e	否	DDH,ODH

4 结束语

本文以基于 ElGamal 加密的平滑投射哈希函数为工具设计了一种安全高效的三方 PAKE 协议,并且在标准模型下,基于 DDH 假设证明了其安全性.我们的协议实现了用户和服务器之间的双向认证并且具有前向安全性.与同类的协议相比,新协议完全基于口令实现用户认证,并且具有较高的通信和计算效率.因此,我们的协议更适用于大规模端到端通信的应用环境.

References:

[1] Bellovin SM, Merritt M. Encrypted key exchange: Password-Based protocols secure against dictionary attacks. In: Proc. of the IEEE Symp. on Research in Security and Privacy. Los Alamitos: IEEE Computer Society, 1992. 72−84. [doi: 10.1109/RISP.1992.213269]

[2] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attack. In: Preneel B, ed. Proc. of the EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 140−156. [doi: 10.1007/3-540-45539-6_11]

[3] Boyko V, MacKenzie P, Patel S. Provably secure password-authenticated key exchange using Diffie-Hellman. In: Preneel B, ed. Proc. of the EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 156−171. [doi: 10.1007/3-540-45539-6_12]

[4] Katz J, Ostrovsky R, Yung M. Efficient password-authenticated key exchange using human-memorable passwords. In: Pfitzmann B, ed. Proc. of the EUROCRYPT 2001. LNCS 2045, Berlin: Springer-Verlag, 2001. 475−494. [doi: 10.1007/3-540-44987-6_29]

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

[6] Canetti R, Halevi S, Katz J, Lindell Y, MacKenzie P. Universally composable password-based key exchange. In: Cramer R, ed. Proc. of the EUROCRYPT 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 404−421. [doi: 10.1007/11426639_24]

[7] Lin CL, Sun HM, Hwang T. Three-Party encrypted key exchange: Attacks and a solution. ACM SIGOPS Operation System Review, 2000,34(4):12−20. [doi: 10.1145/506106.506108]

[8] Lin CL, Sun HM, Steiner M, Hwang T. Three-Party encrypted key exchange without server public-keys. IEEE Communications Letters, 2000,5(12):497−499. [doi: 10.1109/4234.974498]

[9] Abdalla M, Fouque PA, Pointcheval D. Password-Based authenticated key exchange in the three-party setting. In: Vaudenay S, ed. Proc. of the PKC 2005. LNCS 3386, Berlin: Springer-Verlag, 2005. 65−84. [doi: 10.1007/978-3-540-30580-4_6]

[10] Abdalla M, Pointcheval D. Interactive Diffie-Hellman assumptions with applications to password-based authentication. In: Patrick AS, ed. Proc. of the FC 2005. LNCS 3570, Berlin: Springer-Verlag, 2005. 341−356. [doi: 10.1007/11507840_31]

[11] Wang WJ, Hu L. Efficient and provably secure generic construction of three-party password-based authenticated key exchange protocols. In: Barua R, ed. Proc. of the INDOCRYPT 2006. LNCS 4329, Berlin: Springer-Verlag, 2006. 118−132. [doi: 10.1007/11941378_10]

[12] Yoneyama K. Efficient and strongly secure password-based server aided key exchange. In: Chowdhury DR, ed. Proc. of the INDOCRYPT 2008. LNCS 5365, Berlin: Springer-Verlag, 2008. 172−184. [doi: 10.1007/978-3-540-89754-5_14]

[13] Zhao JJ, Gu DW. Provably secure three-party password-based authenticated key exchange protocol. Information Sciences, 2012, 184(1):310−323. [doi: 10.1016/j.ins.2011.07.015]

[14] Huang HF. A simple three-party password-based key exchange protocol. Int'l Journal of Communication Systems, 2009, 22(7): 857−862. [doi: 10.1002/dac.1002]

[15] Yoon EJ, Yoo KY. Cryptanalysis of a simple three-party password-based key exchange protocol. Int'l Journal of Communication Systems, 2011,24(4):532−542. [doi: 10.1002/dac.1168]

[16] Wu SH, Chen KF, Zhu YF. Enhancements of a three-party password-based authenticated key exchange protocol. Int'l Arab Journal of Information Technology, 2013,10(3):215−221.

[17] Lee TF, Hwang T. Simple password-based three party authenticated key exchange without server public keys. Information Sciences, 2010,180(9):1702−1714. [doi: 10.1016/j.ins.2010.01.005]

[18] Chang TY, Hwang MS, Yang WP. A communication-efficient three party password authenticated key exchange protocol. Information Sciences, 2011,181(1):217−226. [doi: 10.1016/j.ins.2010.08.032]

[19] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. Journal of the ACM, 2004,51(4):557−594. [doi: 10.1145/1008731.1008734]

[20] Kwon JO, Jeong IR, Lee DH. Light-Weight key exchange with different passwords in the standard model. Journal of Universal Computer Science, 2009,15(5):1042−1064. [doi: 10.3217/jucs-015-05-1042]

[21] Yang JH, Cao TJ. Provably secure three-party password authenticated key exchange protocol in the standard model. The Journal of Systems and Software, 2012,85:340−350. [doi: 10.1016/j.jss.2011.08.024]

[22] Nam JH, Raymond Choo KK, Kim J, Paik J, Won D. Password-Only authenticated three-party key exchange with provable security in the standard model. The Scientific World Journal, 2014, Article ID 825072. [doi: 10.1155/2014/825072]

[23] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public key encryption. In: Kundsen LR, ed. Proc. of the EUROCEYPT 2002. LNCS 2332, Berlin: Springer-Verlag, 2002. 45−64. [doi: 10.1007/3-540-46035-7_4]

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

[25] Benhamouda F, Blazy O, Chevalier C, Pointcheval D, Vergnaud D. New techniques for SPHFs and efficient one-round PAKE protocols. In: Canetti R, ed. Proc. of the CRYPTO 2013. LNCS 8042, Berlin: Springer-Verlag, 2013. 449−475. [doi: 10.1007/978-3-642-40041-4_25]

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

李光松(1977－),男,博士,副教授,主要研究领域为无线网络安全.

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

马传贵(1962－),男,博士,教授,博士生导师,主要研究领域为信息安全.