软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(10):3238−3250 [doi: 10.13328/j.cnki.jos.005805]

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

改进的三方口令验证元认证密钥交换协议*

张启慧[1], 胡学先[1], 刘文芬[2], 魏江宏[1]

[1](中国人民解放军战略支援部队信息工程大学,河南 郑州 450001)

[2](桂林电子科技大学 计算机与信息安全学院,广西 桂林 541004)

通讯作者: 胡学先, E-mail: huxuexian@tca.iscas.ac.cn

摘 要: 在三方口令认证密钥交换(三方 PAKE)协议中,每个用户仅仅需要和服务器共享一个口令,就可以在服务器的协助下与他人进行安全的密钥交换.由于有效地减少了用户管理口令的负担,三方 PAKE 协议在大规模用户集的安全通信中受到了较多关注.然而,已有的三方 PAKE 协议大多关注的是服务器利用明文存储用户口令的情形,没有考虑服务器口令文件泄露所造成的巨大威胁.在服务器端存放的是相应于用户口令的验证元的情形下,研究三方 PAKE 协议的分析和设计.首先分析了一个最近提出的基于验证元的三方 PAKE 协议,指出该协议易于遭受离线字典攻击,因此未能达到所宣称的安全性;其次,在分析已有协议设计缺陷的基础上,提出了一个新的基于验证元的三方 PAKE 协议,并在标准模型下证明了所设计的协议的安全性,与已有协议的比较表明,新提出的协议在提供了更高安全性的同时具有可接受的计算和通信效率.

关键词: 密钥交换协议;口令认证;验证元;离线字典攻击;标准模型

中图法分类号: TP309

中文引用格式: 张启慧,胡学先,刘文芬,魏江宏.改进的三方口令验证元认证密钥交换协议.软件学报,2020,31(10):3238−3250. http://www.jos.org.cn/1000-9825/5805.htm

英文引用格式: Zhang QH, Hu XX, Liu WF, Wei JH. Improved verifier-based three-party password-authenticated key exchange protocol. Ruan Jian Xue Bao/Journal of Software, 2020,31(10):3238−3250 (in Chinese). http://www.jos.org.cn/1000-9825/5805.htm

Improved Verifier-based Three-party Password-authenticated Key Exchange Protocol

ZHANG Qi-Hui[1], HU Xue-Xian[1], LIU Wen-Fen[2], WEI Jiang-Hong[1]

[1](PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China)

[2](School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: With the aid of three-party password-authenticated key exchange (3PAKE) protocol, two users, each of which shares a low-entropy password with the trusted server, could agree on a common session key securely. Since 3PAKE protocols reduce the burden of password management dramatically when the total number of users is very large, they have attracted much attention recently. However, most of the existing 3PAKE protocols are designed in the scenario where a user stores her/his plain password in the password file of the server, henceforth no protection would be provided once the password file is leaked. This study investigates the analysis and design of verifier-based 3PAKE protocols, where the server holds a verifier of a password other than the plain password. Firstly, it is shown that a recently proposed verifier-based 3PAKE protocol is not secure, which is vulnerable to off-line dictionary attack. Then, aiming to overcome the existed deficits, a new verifier-based 3APKE protocol is proposed and its security is proved in the standard model. Comparisons show that the proposed new scheme takes the advantage of security as well as enjoys practical efficiency.

Key words: key exchange protocol; password authentication; verifier-based; off-line dictionary attack; standard model

* 基金项目: 国家自然科学基金(61502527, 61702549, 61862011); 广西密码学与信息安全重点实验室研究课题(GCIS201704)

Foundation item: National Natural Science Foundation of China (61502527, 61702549, 61862011); Guangxi Key Laboratory of Cryptography and Information Security (GCIS201704)

收稿时间: 2018-08-20; 修改时间: 2018-10-12; 采用时间: 2018-12-11

当今,以移动互联网、云计算、大数据为代表的信息技术日新月异,使人们的日常生活不断网络化,资产不断数字化,构造安全的身份认证和密钥交换(AKE)协议逐渐成为保障用户数字化资产安全的关键.在所有的认证方式中,口令认证由于简单易用、方便部署,成为目前应用最为普遍的一种[1].

早在 1992 年,Bellovin 等人[2]就开创性地提出第一个真正意义上能够抵抗离线字典攻击的两方口令认证密钥交换(PAKE)协议,其中,用户和服务器利用共享的低熵口令进行认证并生成高熵的会话密钥.PAKE 协议仅仅要求用户记住一个较短的口令,避免了传统的基于对称密钥的 AKE 协议对存储初始对称密钥的专用硬件的需求,也无需网络中配有复杂的公钥基础设施,非常方便实际使用.随后,为进一步提高两方 PAKE 协议的安全性和效率,密码学家针对两方 PAKE 协议的设计与分析进行了深入的探索,基于可证明安全理论构建了适用于 PAKE 的安全模型[3−6],分别设计了在随机预言模型下安全的两方 PAKE 协议[3,4,7,8]和在标准模型下安全的两方 PAKE 协议[9−14].国际标准化组织(ISO)等机构还颁布了 ISO/IEC 11770-4、IEEE Std 1363.2 等系列相关安全标准,进一步推动了 PAKE 协议的广泛应用.

两方 PAKE 协议比较适合“用户-服务器”架构下的两方通信,却不适合用在大规模用户相互通信的场合.此时,任何两个需要相互通信的用户都需要预先共享一个口令,从而导致每个用户需要记住多个口令才能支持安全通信.为了降低这一情形下用户记忆和管理口令的负担,三方 PAKE 协议随即被提出,其中每个用户仅仅需要和服务器共享一个口令,就可以在服务器的协助下与他人进行安全的密钥交换.由于这类协议在大规模通信中较为实用,密码学家基于不同假设构造了一系列实用的三方 PAKE 协议[15,16],并在安全模型下严格地证明了协议的安全性[17−21].

尽管两方、三方 PAKE 协议已经得到深入而广泛的研究,密码学家提出了诸多安全、高效的构造方案,满足了不同场合的安全应用,然而,多数已有口令协议关注的是服务器利用明文存储用户口令的情形,没有考虑服务器口令文件泄露所造成的巨大威胁.而现实中关于服务器端存储的口令文件被泄露的案例却是层出不穷[22],亟待在 PAKE 协议设计中增加减弱服务器文件泄露造成危害的措施.针对服务器文件泄露问题,常见的解决方案有验证元[23−25]、泄露检测[26]、慢哈希[27]、口令硬化[28]等技术.作为防止服务器文件泄露所造成攻击的技术的典型代表,验证元技术是指服务器端使用口令的变换值而非口令本身进行认证,使得攻击者在获得服务器口令文件后至少需要进行离线字典攻击才能获得原始的口令,有效地减弱了服务器口令文件泄露所造成的危害.

针对基于验证元的三方 PAKE 协议,杨等人[29]提出了首个标准模型下的协议构造.他们利用带标签的公钥加密体制、平滑投射哈希函数等组件构造了一个基于验证元的三方 PAKE 协议,并在标准模型下分析了所提出协议的安全性.本文中,我们分析指出该协议并未达到所声称的安全性,难以抵抗离线字典攻击.其次,在分析已有协议缺陷的基础上,通过借鉴标准模型下 PAKE 协议设计的新技术,我们利用改进的平滑投射哈希函数构造了一个新的基于验证元的三方 PAKE 协议,并在广泛接受的安全模型中对其进行了严格的安全性证明.最后,还将所提出的基于验证元的三方 PAKE 协议与已有协议进行了安全性和效率比较,结果表明,新提出的协议在提供了更高安全性的同时具有可接受的计算和通信效率.

1 相关密码学组件和假设

1.1 公钥加密体制

一个公钥加密体制含有 3 个算法 $PKE=(KG,Enc,Dec)$,其中,密钥生成算法 KG 在输入安全参数 k 时,输出公私钥对 $(pk,sk)\leftarrow KG(1^k)$, 加密算法 Enc 在输入公钥 pk、明文 m 以及随机数 r 时,输出对应的密文 $c\leftarrow Enc(pk,m;r)$, 解密算法 Dec 在输入私钥 sk、合法密文 c 时,输出对应的明文 $m\leftarrow Dec(sk,c)$, 如果输入的密文不合法,解密算法输出$\perp$.

如果公钥加密算法能够抵御选择密文攻击(CCA),则称它是 CCA 安全的.在 CCA 攻击中,攻击者 $\mathcal{A}$ 除了能够获得加密公钥 pk 外,还具有访问解密预言 $O_{dec}(c)=Dec(sk,c)$的能力.攻击者 $\mathcal{A}$ 自适应地选择两个明文 m_0 和 m_1, 模拟者选择随机的比特 $b\in\{0,1\}$并计算挑战密文 $c^*=Enc(pk,m)$.如果攻击者在不向解密预言询问 c^*的条件下,输

出猜测 b',则定义攻击者的优势 $Adv_{PKE}^{CCA}(\mathcal{A})$ 以及相应的优势函数分别为

$$Adv_{PKE}^{CCA}(\mathcal{A})=\left|2\Pr\{b'=b\}-1\right|, Adv_{PKE}^{CCA}(t,q_{dec})=\max_{\mathcal{A}}\{Adv_{PKE}^{CCA}(\mathcal{A})\},$$

其中,最大值函数跑遍所有计算时间至多为 t,询问解密预言的次数至多为 q_{dec} 的 CCA 攻击者.在上述定义中,如果不提供给攻击者访问解密预言的能力,而仅仅让其获得公钥 pk,则相应的攻击是选择明文攻击(CPA),此时安全的加密算法被称为 CPA 安全的.

在 PAKE 协议设计中,我们需要用到公钥加密体制的一种变体,称为带标签(label)的公钥加密体制,其定义类似于传统的公钥加密体制,不过,要求加密算法和解密算法能够接受将标签 l 作为一个额外的公开输入(形如 $c\leftarrow Enc(pk,m;l;r)$),且仅当解密算法输入和加密算法完全一样的标签时才能解密得到正确的明文.关于带标签的公钥加密体制的 CCA 安全性,其定义与传统公钥加密算法类似,不同之处在于,攻击者询问解密预言时要同时提供密文和标签,攻击者在选择挑战明文 m_0、m_1 时也需要同时提供一个挑战标签 l^*.

1.2 平滑投射哈希函数

平滑投射哈希函数最初是由密码学家 Cramer 和 Shoup[30]提出的,随后被 Katz 等人[31]和 Benhamouda 等人[13]加以改进用于通信高效的 PAKE 协议构造.粗略地说,它是一种双密钥的哈希函数,给定集合 X 以及语言 $L\subset X$,对任意的词语 $c\in L$,其相应的哈希值可以用两种方式计算:利用哈希密钥 hk 和 c,或利用投射密钥 hp 和相应于 $c\in L$ 的证据 w.具体而言,一个平滑投射哈希函数 $SPHF=(HashKG,ProjKG,Hash,ProjH)$ 由 4 个算法组成,其中密钥生成算法 $HashKG$ 在输入安全参数 k 时输出哈希密钥 $hk\leftarrow HashKG(1^k)$, 投射密钥生成算法 $ProjKG$ 在输入哈希密钥 hk、语言 L 以及相应的元素 $c\in X$ 时输出相应的投射密钥 $hp\leftarrow ProjKG(hk,L,c)$, 哈希函数 $Hash$ 在输入哈希密钥 hk、语言 L 以及任意元素 $c\in X$ 时输出哈希值 $h\leftarrow Hash(hk,L,c)$, 投射哈希函数 $ProjH$ 在输入投射密钥 hp、语言 L、词语 $c\in L$ 以及相应证据 w 时输出哈希值 $h\leftarrow ProjH(hp,L,c,w)$.

平滑投射哈希函数应该满足正确性和平滑性两个特性.正确性是指,对任意合法的词语 $c\in L$ 以及相应证据 w, $Hash(hk,L,c)$=$ProjH(hp,L,c,w)$ 成立;平滑性是指,对任意的不属于给定语言的元素 $c\notin L$, 即使在已知 hp 的条件下, $Hash(hk,L,c)$ 也和完全随机选取的输出是统计不可区分的.当安全参数为 k 时,记 $\varepsilon_{SPHF}(k)$为这两个分布的统计距离的一个可忽略的上界.

1.3 口令哈希机制

Benhamouda 等人[25]形式化地给出了口令哈希机制的严格定义,用来描述基于验证元的口令协议中验证元的生成方式.一个口令哈希机制 PHS 通常由 5 个算法组成,其中参数生成算法 $PSetup$ 在输入安全参数 k 以及口令比特位数 n 时输出公开参数 $param\leftarrow PSetup(1^k,1^n)$, 预盐值生成算法 $PPHSalt$ 在输入参数 $param$ 时输出随机的预盐值 $s_P\leftarrow PPHSalt(param)$, 预哈希值生成算法 $PPreHash$ 在输入参数 $param$、预盐值 s_P 和口令 π 时输出预哈希值 $P\leftarrow PPreHash(param,s_P,\pi)$, 预盐值 s_P 和预哈希值 P 主要是客户端使用;盐值生成算法 $PSalt$ 在输入参数 $param$ 时输出随机的盐值 $s_H\leftarrow PSalt(param)$, 验证元生成算法 $PHash$ 在输入参数 $param$、盐值 s_H 和口令 π 时输出哈希值 $H\leftarrow PHash(param,s_H,\pi)$, 盐值 s_H 和哈希值 H 被服务器端用作验证元.

为了保证服务器口令文件泄露后让攻击者尽可能难地获得用户的口令,需要保证加盐操作后攻击者只有对每个验证元进行独立的离线字典攻击才能获得相应的口令,为此,Benhamouda 等人[25]给出了紧单向性(tight one-wayness)的定义.为了让口令哈希机制能够适配 PAKE 协议设计中的平滑投射哈希等操作,文献[25]还给出了一个基于代数运算的口令哈希机制.

1.4 DDH假设

设 q 是素数,G 是 q 阶乘法循环群, $g\in G$ 是其中的一个生成元.判定型 Diffie-Hellman(DDH)假设是指,对所有概率多项式时间的攻击者 $\mathcal{A}$,其成功区分 $\{(g^x,g^y,g^{xy}):x,y\in Z_q\}$ 和 $\{(g^x,g^y,g^z):x,y,z\in Z_q\}$ 上的均匀分布的优势都是可忽略的.定义相应的优势函数为 $Adv_G^{ddh}(t)=\max_{\mathcal{A}}\{Adv_G^{ddh}(\mathcal{A})\}$, 则 DDH 假设成立意味着 $Adv_G^{ddh}(t)$ 是安全参数的可忽略函数.

2 安全模型

本节介绍用于分析三方 PAKE 协议的安全模型,该模型首先由 Abdalla 等人提出[5],随后,文献[29,32]对其进行了改进.此外,在定义攻击者优势时,考虑到真实口令分布并不服从均匀分布,而是服从严重偏态的 Zipf 分布[33],我们采用了类似于文献[34]的方式对其进行了改进.

协议参与方.三方 PAKE 协议的参与方包含两个集合:所有用户组成的集合$\mathcal{U}$以及可信服务器组成的集合$\mathcal{S}$.其中,用户集合$\mathcal{U}$又分为诚实用户集合$\mathcal{C}$和恶意用户集合$\mathcal{E}$,恶意用户集合形式化了意图攻击其他用户的恶意用户.不失一般性,常常假设服务器集合仅包含一个元素$\mathcal{S}=\{S\}$.

长期密钥.用户集合$\mathcal{U}$中的每一个用户 $U\in\mathcal{U}$都拥有一个口令 π_U,服务器拥有口令列表 $pw_S=\langle pw_S[U]\rangle_{U\in\mathcal{U}}$,其中, $pw_S[U]=\{s_U,H_U\}$ 由口令 π_U 相对应的盐值 s_U 和口令哈希值 H_U 组成.

协议运行模型.假设每个用户或服务器都可能同时运行多个会话,记 U_i 表示用户 U 的第 i 个会话,S^j 表示服务器 S 的第 j 个会话.概率多项式时间(PPT)攻击者 $\mathcal{A}$ 完全控制通信网络,可以随意窃听、修改、伪造、延迟、删除消息.形式化地讲,攻击者具有询问下述预言的能力.

- *Execute*$(U_1^{i_1},S^j,U_2^{i_2})$: 模型化攻击者对协议的被动窃听攻击.让用户会话 $U_1^{i_1}$、$U_2^{i_2}$ 和服务器会话 S^j 诚实运行协议,然后输出用户和服务器之间交换的所有消息.
- *SendClient*(U^i,m):模型化攻击者对用户会话的主动攻击.攻击者将消息 m 发送给用户会话 U^i,然后输出会话 U^i 在收到消息 m 后的响应消息.
- *SendServer*(S^j,m):模型化攻击者对服务器会话的主动攻击.攻击者将消息 m 发送给服务器会话 S^j,然后输出会话 S^j 在收到消息 m 后的响应消息.
- *Reveal*(U^i):模型化会话密钥泄露或丢失.攻击者发给该询问,即可获得会话 U^i 的所拥有的会话密钥.
- *Corrupt*(U):模型化敌手腐化用户攻击.攻击者发出该询问,即可获得用户 U 的口令以及用户 U 中所有会话的内部状态.
- *Corrupt*(S):模型化敌手腐化服务器攻击.攻击者发出该询问,即可获得服务器 S 中存储的口令列表 $pw_S=\langle pw_S[U]\rangle_{U\in\mathcal{U}}=\langle\{s_U,H_U\}\rangle_{U\in\mathcal{U}}$.
- *Test*(U^i):用以刻画会话密钥的安全性.如果用户会话 U^i 已经生成会话密钥,则抛掷一枚均匀的硬币 $b\in\{0,1\}$.若 b=1,输出会话 U^i 的真实会话密钥;若 b=0,输出与会话密钥等长度的随机比特串.

对每个用户会话 U^i,记 sid_U^i 为会话标识, pid_U^i 为其意定通信会话.如果一个会话顺利完成且已生成会话密钥,则称其为已经接受(accepted).

匹配会话.称两个会话 $U_1^{i_1}$ 和 $U_2^{i_2}$ 是匹配的,如果:(1) $U_1^{i_1}$ 和 $U_2^{i_2}$ 都已接受;(2) $U_1^{i_1}$ 和 $U_2^{i_2}$ 有相同的会话标识 *sid*;(3) $U_1^{i_1}$ 和 $U_2^{i_2}$ 互为意定通信方;(4) 除会话 $U_1^{i_1}$ 和 $U_2^{i_2}$ 外没有其他会话的意定通信方为 $U_2^{i_2}$ 或 $U_1^{i_1}$.

新鲜会话.称一个会话 U^i 是新鲜的,如果:(1) U^i 已接受;(2) 攻击者未对 U^i 或其匹配会话发起 *Reveal* 询问;(3) 在会话 U^i 接受之前,攻击者未对用户 U 以及服务器发起过 *Corrupt* 询问.

语义安全.在协议运行过程中,PPT 攻击者 $\mathcal{A}$ 能以任意顺序发出 *Execute*、*SendClient*、*SendServer*、*Reveal* 和 *Corrupt* 询问,但只能针对某个新鲜的用户会话发出一次 *Test* 询问.最终, $\mathcal{A}$ 输出一个比特 b'作为 *Test* 中的随机比特 b 的猜测,若 $b'=b$,则认为攻击者攻击成功,并记该事件为 *Succ*.假设所攻击的协议为 P,相应口令字典为 D,我们定义攻击者 $\mathcal{A}$ 的优势为 $Adv_{P,D}^{ake}(\mathcal{A})=2\Pr[Succ]-1$.若对所有发起主动攻击的次数至多为 q_{send} 的 PPT 攻击者 $\mathcal{A}$,其优势 $Adv_{P,D}^{ake}(\mathcal{A})$ 只比 $C'\cdot q_{send}^{s'}$ 大一个可忽略量,则称协议 P 是语义安全的,其中,C'和 s'是相应于字典 D 的 Zipf 参数[33].例如,当利用天涯论坛泄露的口令集作为口令分布的模型时,可以得到 C'=0.062239 和 s'=0.155478[34].

会话密钥私密性.为了防止诚实但好奇的(Honest-but-Curious)服务器获知最终的会话密钥,需特别考虑一个知道所有用户口令的攻击者 $\mathcal{A}$,并假设 $\mathcal{A}$ 能够询问 *Execute*、*SendClient*、*Reveal* 和 *Corrupt* 预言以及下述 *TestPair* 预言.

● $TestPair(U_1^{i_1},U_2^{i_2})$: 如果 $U_1^{i_1}$ 和 $U_2^{i_2}$ 没有生成相同的会话密钥,则返回⊥;否则,抛掷一枚均匀的硬币 $b\in\{0,1\}$.若 b=1,输出 $U_1^{i_1}$ 和 $U_2^{i_2}$ 共享的会话密钥;若 b=0,输出与会话密钥等长度的随机比特串.

最终,$\mathcal{A}$输出一个比特 b'作为 TestPair 中的随机比特 b 的猜测,若 b'=b,则认为攻击者攻击成功,并记为 Succkp.相应地定义攻击者$\mathcal{A}$的优势为 $Adv_{P,D}^{kp}(\mathcal{A})=2\Pr[Succ_{kp}]-1$. 若对所有的 PPT 攻击者$\mathcal{A}$,其优势是安全参数的可忽略函数,则称协议 P 相对于诚实但好奇的服务器能够保证会话密钥的私密性.

3 一个基于验证元的 3PAKE 协议的安全缺陷

本节我们首先回顾杨等人[29]提出的基于验证元的三方 PAKE 协议(简记为 Yang-V3PAKE 协议)的详细步骤,然后提出了针对 Yang-V3PAKE 协议的离线字典攻击.

3.1 杨等人提出的协议

Yang-V3PAKE 协议采用了文献[24]中给出的口令哈希机制的具体构造,其中,参数生成算法 *PSetup* 输出为 (p,G,g,h),G 是阶为素数 p 的循环群,g、h 是其中两个独立生成元.预哈希值生成算法 *PPreHash* 的输出为 $P=g^{s_P\cdot\pi}$, 哈希算法 *PHash* 的输出为 $H=(H_1,H_2)=(g^{s_P},P\cdot h^{s_H})$.

假设用户 A 和用户 B 想要在服务器 S 的协助下进行安全的密钥交换,其中,A 和 B 分别拥有口令 π_A 和 π_B,服务器 S 拥有相应验证元 (s_{H_A},H_{1A},H_{2A}) 和 (s_{H_B},H_{1B},H_{2B}), 则 Yang-V3PAKE 协议的具体步骤如下.

(1) 服务器 S 选择两个随机数 $s_A,s_B\in_R\mathbb{Z}_p$, 分别计算 $T_A=h^{s_A},T_A^*=T_A(H_{2A}h^{-s_{H_A}})$ 和 $T_B=h^{s_B}$, $T_B^*=T_B(H_{2B}h^{-s_{H_B}})$, 然后发送消息 (T_A^*,H_{1A}) 给用户 A,发送消息 (T_B^*,H_{1B}) 给用户 B;

(2) 用户 A 收到消息 (T_A^*,H_{1A}) 后,运行平滑投射哈希密钥生成算法 *HashKG*,生成哈希密钥 $hk=(\eta_1,\eta_2,\theta,\mu,\gamma)$, 计算 $\omega_A=h^{\mu},\omega_A^*=h^{\mu}H_{1A}^{\pi_A},T_A=T_A^*/H_{1A}^{\pi_A},\omega_{AS}=T_A^{\mu}$, 并利用 ω_{AS} 计算 MAC 认证值 $\sigma_{AS}=MAC_{\omega_{AS}}(A\|B\|S\|\omega_A^*)$, 然后选择随机数 $r_A\in_R\mathbb{Z}_p$ 计算 $e=h^{r_A}H_{1A}^{\pi_A}$ 并向服务器发送消息 $(e,\omega_A^*,\sigma_{AS})$; 类似地,用户 B 收到消息 (T_B^*,H_{1B}) 后,选择随机哈希密钥 $hk'=(\eta_1',\eta_2',\theta',\mu',\gamma')$ 和随机数 $r_B\in_R\mathbb{Z}_p$, 计算 $\omega_B,\omega_B^*,T_B,\omega_{BS},\sigma_{BS},e'$, 并向服务器发送消息 $(e',\omega_B^*,\sigma_{BS})$.

(3) 服务器 S 接收到消息 $(e,\omega_A^*,\sigma_{AS})$ 和 $(e',\omega_B^*,\sigma_{BS})$ 后,首先计算 $\omega_A=\omega_A^*/(H_{2A}h^{-s_{H_A}})$, $\omega_{AS}=\omega_A^{s_A}$ 和 $\omega_B=\omega_B^*/(H_{2B}h^{-s_{H_B}})$,$\omega_{BS}=\omega_B^{s_B}$, 然后验证 σ_{AS},σ_{BS} 的有效性.当验证都通过时,服务器计算 $e_{AS}=[e/(H_{2A}h^{-s_{H_A}})]^{s_B}\cdot H_{2B}h^{-s_{H_B}}$, $e_{BS}=[e'/(H_{2B}h^{-s_{H_B}})]^{s_A}\cdot H_{2A}h^{-s_{H_A}}$,生成 MAC 值 $\lambda_{AS}=MAC_{\omega_{AS}}(A\|B\|S\|e_{AS})$, $\lambda_{BS}=MAC_{\omega_{BS}}(A\|B\|S\|\ e_{BS})$, 接着向用户 A 和 B 分别发送消息 $(e_{AS},e_{BS},\lambda_{AS})$ 和 $(e_{BS},e_{AS},\lambda_{BS})$.

(4) 用户 A 收到消息 $(e_{AS},e_{BS},\lambda_{AS})$ 后,首先验证 MAC 值 λ_{AS} 是否有效.验证通过后,计算 $hp_1=g_1^{\eta_1}g_2^{\theta}c^{\gamma}\omega_{AS}$, $hp_2=g_1^{\eta_2}d^{\gamma}$, $l=(A,B,hp)$,$u_1=g_1^{r_A}$,$u_2=g_2^{r_A}$,$v=(cd^{\xi})^{\gamma_A}$,$\xi=H_k(l,u,e_{AS})$, 然后,用户 A 给用户 B 发送消息 $hp=(hp_1,hp_2)$, $C_{AS}=(u_1,u_2,e_{AS},v)$;类似地,用户 B 收到消息 $(e_{BS},e_{AS},\lambda_{BS})$ 且 λ_{BS} 验证通过后,相应的计算并发送消息 $hp'=(hp_1',hp_2')$, $C_{BS}=(u_1',u_2',e_{BS},v')$ 给用户 A.

(5) 用户 A 和 B 收到对方发送的消息后,分别计算 $sk_A=(u_1')^{\eta_1+\xi'\eta_2}(u_2')^{\theta}(e_{BS}/H_{1A}^{\pi_A})^{\mu}(v')^{\gamma}(hp_1'hp_2'^{\xi})^{r_A}$,$sk_B=u_1^{\eta_1'+\xi\cdot\eta_2'}u_2^{\theta'}(e_{AS}/H_{1B}^{\pi_B})^{\mu'}v^{\gamma'}(hp_1hp_2^{\xi'})^{r_B}$, 根据平滑投射哈希函数的性质可以保证 sk_A=sk_B.

文献[29]声称,Yang-V3PAKE 协议能够提供会话密钥的语义安全性、前向安全性、针对服务器的密钥私密性,还能够抵抗不可测在线字典攻击和服务器泄露攻击.根据安全模型的定义,协议满足语义安全性是指攻击者成功的优势至多为 $O(q_s/2^{\beta})+negl(k)$, 其中,q_s 为攻击者进行在线字典攻击的次数,这意味着攻击者不能针对协议实施离线字典攻击.

3.2 对Yang-V3PAKE协议的攻击和分析

本小节首先给出对 Yang-V3PAKE 协议的离线字典攻击.我们注意到,文献[29]中假设攻击者 $\mathcal{A}$ 完全控制着

通信信道,可以窃听、插入、修改消息,或是创建、重发、转发消息.其次,Yang-V3PAKE 协议中服务器发送了第1轮消息,用户在收到消息后就利用口令对其进行运算计算得到第2轮的回复消息,且该回复消息中包含一个可用于验证的 MAC 值.

假设用户 A 和用户 B 想要在服务器 S 的协助下进行安全的密钥交换,用户 A 和 B 的真实口令分别为 π_A 和 π_B.攻击者 $\mathcal{A}$ 按照如下方式对用户 A 的口令进行离线字典攻击.

(1) 攻击者 $\mathcal{A}$ 选择随机数 r_1 和 r_2,计算 $T_A^*=h^{r_1},H_{1A}=h^{r_2}$, 然后攻击者 $\mathcal{A}$ 冒充服务器 S 向用户 A 发送消息 T_A^*,H_{1A}.

(2) 用户 A 收到消息 (T_A^*,H_{1A}) 后,将利用其真实口令 π_A 进行下述运算.首先,运行平滑投射哈希密钥生成算法 $HashKG$ 生成哈希密钥 $hk=(\eta_1,\eta_2,\theta,\mu,\nu)$, 然后利用口令 π_A 计算 $\omega_A=h^{\mu},\omega_A^*=h^{\mu}H_{1A}^{\pi_A}=h^{\mu+r_2\pi_A}$, $T_A=T_A^*/H_{1A}^{\pi_A}=h^{\eta_1-r_2\pi_A},\omega_{AS}=T_A^{\mu}=h^{\mu(\eta_1-r_2\pi_A)}$, 并利用 ω_{AS} 计算 MAC 认证值 $\sigma_{AS}=MAC_{\omega_{AS}}(A\|B\|S\|\omega_A^*)$, 然后选择随机数 $r_A\in_R\mathbb{Z}_p$ 计算 $e=h^{r_A}H_{1A}^{\pi_A}$ 并向服务器 S 发送消息 $(e,\omega_A^*,\sigma_{AS})$.

(3) 攻击者 $\mathcal{A}$ 拦截得到上述消息,逐个地穷举所有可能的口令 $\tilde{\pi}_A$,然后利用这个猜测的口令计算 $\tilde{\omega}_{AS}=(\omega_A^*\cdot h^{-r_2\tilde{\pi}_A})^{(\eta_1-r_2\tilde{\pi}_A)}$, $\tilde{\sigma}_{AS}=MAC_{\tilde{\omega}_{AS}}(A\|B\|S\|\omega_A^*)$, 并检验 $\tilde{\sigma}_{AS}=\sigma_{AS}$ 是否成立,如果等式成立,则输出 $\tilde{\pi}_A$ 当作用户 A 的口令.

若攻击者猜测正确 $\tilde{\pi}_A=\pi_A$,则可得 $\tilde{\omega}_{AS}=(\omega_A^*\cdot h^{-r_2\tilde{\pi}_A})^{(\eta_1-r_2\tilde{\pi}_A)}=(h^{\mu+r_2\pi_A-r_2\tilde{\pi}_A})^{(\eta_1-r_2\tilde{\pi}_A)}=\omega_{AS}$,从而恰好成立 $\tilde{\sigma}_{AS}=\sigma_{AS}$, 证实了上述离线字典攻击的合理性.类似地,攻击者也可以对用户 B 的口令 π_B 实施离线字典攻击进行猜测.且对于每个猜测的口令,攻击者实施上述攻击所需的计算量为 7 次模指数运算、2 次模多指数运算以及 2 次 MAC 计算,是一个固定的值.因此,攻击者可以针对 Yang-V3PAKE 协议进行有效的离线字典攻击.由于抵抗离线字典攻击是口令认证协议的基本安全目标,也是语义安全性等定义的基础,因此,Yang-V3PAKE 协议并没有达到其宣称的安全性.

4 改进的基于验证元的 3PAKE 协议

鉴于 Yang-V3PAKE 协议是首个在标准模型下设计的基于验证元的三方 PAKE 协议,但是该协议并没有满足三方 PAKE 的安全需求,本节中我们提出一个新的改进的基于验证元的三方 PAKE 协议,并在标准模型下对所构造的协议进行严格的安全性证明.

4.1 协议描述

本节给出我们改进的基于验证元的 3PAKE 协议的详细设计,记为 I-V3PAKE 协议,该协议用到了文献[11,21]中的 PAKE 的设计技术以及文献[25]中针对验证元的验证技术.

I-V3PAKE 协议用到了 CPA 安全的 ElGamal 公钥加密体制 $PKE'=(KG',Enc',Dec')$ 和一个 CCA 安全的带标签的公钥加密体制 $PKE=(KG,Enc,Dec)$. 记 ElGamal 公钥加密体制 PKE' 所对应的公钥为 $pk'=(g,h)$, 明文 m 所对应的 ElGamal 密文为 $c\leftarrow Enc'(pk',m;r)=(u=g^r,e=h^r\cdot m)$, 记公钥加密体制 PKE 所对应的公钥为 pk.尽管协议设计使用了公钥加密体制,但是并没有依赖公钥基础设施(PKI),只需如同文献[11]一样,将这两种加密算法的公钥 pk' 和 pk 当作协议运行环境设置中的公共参考串(CRS).

协议采用了如下代数口令哈希机制 PHS,其中, $s_P=\perp,P=g^{F(\pi)},s=s_H\in_R\{0,1\}^k,H=s^{F(\pi)},F(\cdot)$ 是从口令空间到指数集 Z_q 上的变换.定义语言

$$L_{s,H}=\{(u,e):\exists r,\exists\pi,u=g^r,e=h^rg^{F(\pi)},H=s^{F(\pi)}\} \tag{1}$$

并记 $L_A=L_{s_A,H_A},L_B=L_{s_B,H_B}$. 我们还利用文献[25]的技术构造了适应语言 $L_{s,H}$ 的平滑投射哈希函数 SPHF,来实现在用户和服务器之间临时密钥交换的同时,适应用户拥有口令而服务器拥有验证元的条件.其中,哈希密钥为 $hk=(x,y,z)$,投射密钥为 $hp=(hp_1,hp_2),hp_1=g^xh^y,hp_2=g^ys^z$, 利用哈希密钥和投射密钥计算哈希值的方式分别为

$Hash(hk,L_{s,H},c=(u,e))=u^x e^y H^z, ProjH(hp,L_{s,H},c,(r,\pi))=hp_1^r hp_2^{F(\pi)}$.

假设用户 A 和用户 B 想要在服务器 S 的协助下进行安全的密钥交换,其中,A 和 B 分别拥有口令 π_A 和 π_B,服务器 S 拥有相应验证元 $(s_A,H_A=s_A^{F(\pi_A)})$ 和 $(s_B,H_B=s_B^{F(\pi_B)})$,则 I-V3PAKE 协议的具体步骤如下.

(1) 用户 A 选择随机数 $r_A\in\mathbb{Z}_p$,计算口令的预哈希值 $P_A=g^{F(\pi_A)}$ 对应的 ElGamal 密文 $c_{AS}=(u_A=g^{r_A},e_A=h^{r_A}\cdot P_A)$,然后发送消息 $\langle A,B,c_{AS}\rangle$ 给服务器 S;类似地,用户 B 选择随机数 $r_B\in\mathbb{Z}_p$,计算口令的预哈希值 $P_B=g^{F(\pi_B)}$ 对应的 ElGamal 密文 $c_{BS}=(u_B=g^{r_B},e_B=h^{r_B}\cdot P_B)$,然后发送消息 $\langle B,A,c_{BS}\rangle$ 给服务器 S.

(2) 服务器 S 收到消息后,先为用户 A 选择随机数 $hk_A=(x_A,y_A,z_A)$,计算 $hp_{1A}=g^{x_A}h^{y_A}$, $hp_{2A}=g^{y_A}s^{z_A}$, $tk_A\|mk_A$=$Hash(hk_A,L_A,c_A)=u_A^{x_A}e_A^{y_A}H_A^{z_A}$,设置 $l_A=A\|B\|S\|c_{AS}\|hp_{1A}\|hp_{2A},M_A=s_A\|H_A$,并用 tk_A 作为加密的随机数计算 $c_{SA}=Enc(pk,M_A;l_A;tk_A)$,并发送消息 $\langle s_A,hp_{1A},hp_{2A},c_{SA}\rangle$ 给用户 A;类似地,为用户 B 选择随机数 $hk_B=(x_B,y_B,z_B)$,计算 $hp_{1B}=g^{x_B}h^{y_B},hp_{2B}=g^{y_B}s^{z_B},tk_B\|mk_B$=$Hash(hk_B,L_B,c_B)=u_A^{x_A}e_A^{y_A}H_A^{z_A}$,设置 $l_B=B\|A\|S\|c_{BS}\|hp_{1B}\|hp_{2B}$, $M_B=s_B\|H_B$,并用 tk_B 作为加密的随机数计算 $c_{SB}=Enc(pk,M_B;l_B;tk_B)$,同时发送消息 $\langle s_B,hp_{1B},hp_{2B},c_{SB}\rangle$ 给用户 B.

(3) 用户 A 收到 $\langle hp_{1A},hp_{2A},c_{SA}\rangle$ 后,首先计算 $tk_A\|mk_A$=$ProjH((hp_{1A},hp_{2A}),L_A,c_A,(r_A,\pi_A))=hp_{1A}^{r_A}\cdot hp_{2A}^{F(\pi_A)}$,然后利用 tk_A 作为随机数重新计算 $c'_{SA}=Enc(pk,M_A;l_A;tk_A)$,并验证与其接收到的 c_{SA} 是否相等.如果验证不相等,则立即结束会话;如果验证通过,则用户 A 选择随机数 $x\in\mathbb{Z}_p$,计算 $X=g^x,\sigma_{AS}=MAC(mk_A,A\|B\|S\|X)$,然后向服务器 S 发送消息 $\langle X,\sigma_{AS}\rangle$;类似地,用户 B 收到消息 $\langle hp_{1B},hp_{2B},c_{SB}\rangle$ 后,计算 $tk_B\|mk_B$ 并验证 c_{SB},验证通过后选择随机数 $y\in\mathbb{Z}_p$,计算 $Y=g^y,\sigma_{BS}=MAC(mk_B,B\|A\|S\|Y)$,然后向服务器 S 发送消息 $\langle Y,\sigma_{BS}\rangle$.

(4) 服务器 S 收到消息后,首先用密钥 mk_A 和 mk_B 验证 MAC 值 σ_{AS} 和 σ_{BS} 是否正确,验证通过后计算 $\sigma_{SA}=MAC(mk_A,A\|B\|S\|X\|Y),\sigma_{SB}=MAC(mk_B,B\|A\|S\|Y\|X)$,然后向用户 A 发送消息 $\langle Y,\sigma_{SA}\rangle$,向用户 B 发送消息 $\langle X,\sigma_{SB}\rangle$.

(5) 用户 A 和 B 在收到来自服务器的消息后,分别利用密钥 mk_A 和 mk_B 验证 MAC 值 σ_{SA} 和 σ_{SB} 是否正确,验证失败,则结束会话.然后,用户 A 计算会话密钥为 $sk_{AB}=Y^x$,用户 B 计算会话密钥为 $sk_{BA}=X^y$.

在用户和服务都诚实运行协议的情况下,对与用户 A 相关的语言 $L_A=L_{s_A,H_A}$ 而言,下式成立:

$$\begin{aligned}Hash(hk_A,L_A,c_A)&=u_A^{x_A}e_A^{y_A}H_A^{z_A}\\&=g^{r_Ax_A}(h^{r_A}g^{H(\pi_A)})^{y_A}s^{H(\pi_A)z_A}\\&=(g^{x_A}h^{y_A})^{r_A}(g^{y_A}s^{z_A})^{F(\pi_A)}\\&=(hp_{1A})^{r_A}(hp_{2A})^{F(\pi_A)}\\&=ProjH((hp_{1A},hp_{2A}),L_A,c_A,(r_A,\pi_A))\end{aligned}\tag{2}$$

可知用户 A 和服务器 S 将计算得到相同的 $tk_A\|mk_A$,保证了 c_{SA}、σ_{AS}、σ_{SA} 的正确性;类似地,用户 B 和服务器 S 将计算得到相同的 $tk_B\|mk_B$,保证了 c_{SB}、σ_{BS}、σ_{SB} 的正确性.因此,协议中验证都将通过,最终 A 和 B 将生成相同的会话密钥 $sk_{AB}=Y^x=g^{xy}=X^y=sk_{BA}$.

注 1.在 I-V3PAKE 协议中,我们利用具有良好代数性质的口令哈希机制和特别构造的平滑投射哈希函数实现了对口令和验证元的验证.一方面,用户在利用投射密钥计算哈希值 $ProjH(hp,L_{s,H},c,(r,\pi))=hp_1^r hp_2^{F(\pi)}$ 时需要用到 $F(\pi)$,验证了用户确实拥有 $F(\pi)$ 和 π,另一方面,语言 $L_{s,H}=\{(u,e):\exists r,\exists\pi,u=g^r,e=h^r g^{F(\pi)},H=s^{F(\pi)}\}$ 的定义方式保证了 $e=h^r g^{F(\pi)}$ 中的 $g^{F(\pi)}$ 部分相对于 g 的指数与 H 相对于 s 的指数是相等的,即证实了服务器确实拥有与用户相匹配的验证元.

注 2.I-V3PAKE 协议能够抵御针对 Yang-V3PAKE 协议[29]的离线字典攻击.具体地,如果攻击者仿照第 3.2 节中提到的攻击方法将 I-V3PAKE 协议的第 1 轮消息替换成伪造的消息,则只要攻击者未猜对用户 $U\in\{A,B\}$ 的口令,将由于 ElGamal 密文 $(u,e)\notin L_{s,H}$ 使得服务器计算得到的 $tk_U\|mk_U$ 对攻击者来说是完全随机的,从而攻击者无法通过验证 c_{SU} 来判别其猜测口令的正确性.

4.2 协议比较

本节给出 I-V3PAKE 协议与其他典型的三方 PAKE 协议在功能、安全性、效率方面的比较,具体结果见表 1.在表 1 中,“验证元”“标准模型”“抗离线字典攻击”“C2S 认证”“Key Privacy”分别表示所考虑的三方 PAKE 协议是否支持验证元、是否在标准模型下可证明安全、是否提供抗离线字典攻击、用户到服务器的显式认证以及会话密钥针对服务器的私密性,“计算效率 $A/B/S$”表示用户 A、B 和服务器 S 分别所需的计算模指数运算的次数.如同文献[32],我们采用标准模型下 CCA 安全的 DHIES 公钥加密算法[35]来实例化协议中的公钥加密算法 PKE.另外,注意到形如 $g^x h^y$ 的多指数运算可以通过快速算法在约等于单个指数的计算时间内完成[32],因而在计算效率中只算作一次指数运算.

从表 1 中的结果可以看出,目前只有文献[29]和我们的 I-V3PAKE 协议是基于验证元的,且是在标准模型下设计的,但是文献[29]中的协议不能抵抗离线字典攻击,因而安全性不能满足实用要求.尽管文献[32,36]中的协议也是在标准模型下可证明安全的,但是这两个协议都不是基于验证元的,因此不能抵御服务器泄露攻击.另外,从通信和计算效率上看,我们的 I-V3PAKE 协议在额外的通过验证元方式保护口令的条件下,还具备与文献[29,32,36]较为接近的通信和计算复杂度,甚至 I-V3PAKE 协议的计算效率要更优于文献[29].因此,I-V3PAKE 协议不仅提供了更强的安全性保障,同时具有可接受的计算和通信效率.

Table 1 Comparisons between I-V3PAKE protocol and other verifier-based 3PAKE protocols

表 1 I-V3PAKE 协议与其他典型三方 PAKE 协议的比较

协议	验证元	标准模型	抗离线字典攻击	C2S 认证	Key privacy	通信轮数	计算效率 $A/B/S$
[5]	N	N	Y	N	N	2	1/1/2
[37]	N	N	Y	N	N	3	3/3/4
[36]	N	Y	Y	Y	Y	3	6/6/10
[32]	N	Y	Y	Y	Y	3	6/6/9
[29]	Y	Y	N	Y	Y	4	20/20/6
Ours	Y	Y	Y	Y	Y	4	7/7/10

5 安全性证明

本节在前述安全模型中证明 I-V3PAKE 协议的安全性,首先证明 I-V3PAKE 协议满足语义安全性,然后证明协议中诚实用户所生成的会话密钥相对于诚实而好奇的服务器具有私密性.

定理 1. 如果公钥加密体制 $PKE=(KG,Enc,Dec)$ 是 CCA 安全的,ElGamal 公钥加密体制 $PKE'=(KG',Enc',Dec')$ 是 CPA 安全的,$L_{s,H}$ 是按照式(1)定义的与公钥加密体制 PKE′及口令哈希机制 PHS 相关联的语言,SPHF 是相应于语言 $L_{s,H}$ 的平滑投射哈希函数,MAC 是安全的消息认证码,则 I-V3PAKE 协议是语义安全的.

证明:假设 $\mathcal{A}$ 是针对 I-V3PAKE 协议语义安全性的攻击者,其计算时间至多为 t,访问 *Send* 和 *Execute* 预言的次数至多为 q_{send},q_{exe}.下面通过构造游戏序列 $G_0,G_1,...,G_8$ 来估计攻击者的优势,起始游戏是安全模型所定义的与真实协议交互的游戏.

游戏 G_0:这个游戏对应于安全模型中语义安全定义时的真实攻击,记此时攻击者的优势为

$$Adv^{ake}_{P,D}(\mathcal{A})=Adv_0(\mathcal{A}) \tag{3}$$

游戏 G_1:从这个游戏开始,我们先逐步修改对 *Execute* 询问的模拟方式.游戏 G_1 中,在模拟 *Execute* 询问时,首先将用户端利用 *ProjH* 的计算全部替换成对应的 Hash 计算.由于 *Execute* 中用户和服务器都是诚实的,因而上述替换可行;又根据平滑投射哈希函数的正确性定义,可知在游戏 G_1 中攻击者具有和在游戏 G_0 中相同的优势,即 $Adv_1(\mathcal{A})=Adv_0(\mathcal{A})$.

游戏 G_2:在模拟 *Execute* 时,对任意用户 $U\in\{A,B\}$, 我们将用户第 1 条消息中的密文 $c_{US}=Enc'(pk',P_U;r_U)=(u_U=g^{r_U},e_U=h^{r_U}\cdot P_U)$ 替换成 $c_{US}=Enc'(pk',P_0;r_U)=(u_U=g^{r_U},e_U=h^{r_U}\cdot P_0)$, 其中,$P_0$ 是一个虚拟口令 π_0(即不属于口令字典中的一个值)所对应的预哈希.根据 ElGamal 公钥加密体制 PKE′的 CPA 安全性,可知 P_0 和 P_U 的密文是不可区分的,从而利用标准的混合(hybrid)证明技术将 q_{exe} 个 *Execute* 预言中的密文逐个替换可知,攻击者在游

戏 G_2 与在游戏 G_1 中的优势差是可忽略的,即

$$|Adv_2(\mathcal{A})-Adv_1(\mathcal{A})|\leqslant 2q_{exe}\cdot Adv^{CPA}_{PKE'}(t+O(q_{send}+q_{exe})) \tag{4}$$

其中,式(4)考虑到了 CPA 攻击者在模拟协议运行时,只有在模拟 *Send* 和 *Execute* 类预言时才需要进行额外的计算,在模拟 *Reveal* 和 *Corrupt* 询问时只需要返回对应状态,从而其计算时间至多为 $t+O(q_{send}+q_{exe})$.

游戏 G_3:在模拟 *Execute* 询问时,我们将 $tk_U\|mk_U=Hash(hk_U,L_U,c_U),U\in\{A,B\}$ 替换成随机选择的等长比特串.由于游戏 G_2 已将 c_{US} 替换成 P_0 的密文,从而有 $c_{US}\notin L_A,c_{US}\notin L_B$,根据平滑投射哈希函数的平滑性质,可知攻击者在游戏 G_3 与在游戏 G_2 中的优势差可忽略,即记 $\varepsilon_{SPHF}(k)$为平滑投射哈希函数在输入非语言元素时的输出哈希值与均匀分布之间的统计距离的一个可忽略的上界,则有

$$|Adv_3(\mathcal{A})-Adv_2(\mathcal{A})|\leqslant 2q_{exe}\cdot\varepsilon_{SPHF}(k) \tag{5}$$

游戏 G_4:在模拟 *Execute* 询问时,我们将 $c_{SA}=Enc(pk,M_A;l_A;tk_A),c_{SB}=Enc(pk,M_B;l_B;tk_B)$ 中的 M_A 和 M_B 替换成 $M_A=s_A\|H_{0,A},M_B=s_B\|H_{0,B}$, 其中, $H_{0,A}=s_A^{\pi_0},H_{0,B}=s_B^{\pi_0}$ 是对应于不属于字典的一个虚拟口令 $\pi_0\notin D$. 由于 tk_A 和 tk_B 在游戏 G_3 中已被替换成完全随机的比特串,因此根据加密体制 $PKE=(KG,Enc,Dec)$ 的 CCA 安全性,可知攻击者在游戏 G_4 与在游戏 G_3 中的优势差是可忽略的,因此,

$$|Adv_4(\mathcal{A})-Adv_3(\mathcal{A})|\leqslant 2q_{exe}\cdot Adv^{CCA}_{PKE}(t+O(q_{send}+q_{exe})) \tag{6}$$

需要说明的是,在游戏 G_4 中并没有询问加密体制 PKE 的解密预言,从而实际上只用到了 PKE 体制的 CPA 安全性.但是,在下面的游戏 G_{10} 中需要询问解密预言,因此需要 PKE 是 CCA 安全的.

游戏 G_5:在模拟 *Execute* 询问时,我们直接将最终的会话密钥 sk_{AB}=sk_{BA} 替换成随机值.利用 DDH 自规约技术,我们证明攻击者在实验 G_4 和 G_5 中的优势差至多为攻击者区分 DDH 三元组的优势.给定 DDH 三元组(X_0,Y_0,Z_0),当用户 A 需要生成消息 X和σ_{AS} 时,我们选择随机的 $a,x\in\mathbb{Z}_p$, 并计算 $X=X_0^a g^x$, 当用户 B 需要生成消息 Y和σ_{BS} 时,选择随机的 $b,y\in\mathbb{Z}_p$, 并计算 $Y=Y_0^b g^y$, 当双方需要生成密钥时,计算 $sk_{AB}=sk_{BA}=Z_0^{ab}Y^{xb}X^{ya}g^{xy}$. 可以看出,当三元组($X_0$,$Y_0$,$Z_0$)满足 $Z_0=DH(X_0,Y_0)$ 时,上述游戏和游戏 G_4 完全一样;当 $Z_0\neq DH(X_0,Y_0)$ 时,上述游戏和游戏 G_5 是一样的.在 DDH 问题困难假设下,可知

$$|Adv_5(\mathcal{A})-Adv_4(\mathcal{A})|\leqslant 2\cdot Adv^{ddh}_G(t+O(q_{send}+q_{exe})) \tag{7}$$

至此,我们已将 *Execute* 模拟中的与口令相关的消息和会话密钥替换成为随机值,从而攻击者不能从中获得用户口令的信息.下面将开始修改对敌手主动攻击类询问的模拟.为了表述简单,下面用 $SendClient_0(U^i)$表示攻击者激活用户的初始消息, $SendClient_d(U^i,m),d\in\{2,4\}$ 表示在第 d 轮通信中给用户会话 U^i 发送消息 m, $SendServer_d(S^j,m),d\in\{1,3\}$ 表示在第 d 轮通信中给服务器会话 S^j 发送消息 m.在公开参数产生阶段,我们还让模拟者记录对应于公钥 pk'和 pk 的私钥 sk'和 sk.

游戏 G_6:本游戏修改针对用户 A 的 $SendClient_2(A^i,\langle hp_{1A},hp_{2A},c_{SA}\rangle)$ 的回答方式,对用户 B 按照类似的方式进行处理(下同).先检查$\langle hp_{1A},hp_{2A},c_{SA}\rangle$是否来源于某个诚实模拟的 $SendServer_1(S^j,*)$ 的回复,如果答案是否定,则直接解密 c_{SA} 得到 s'_A和H'_A 并检查与用户 A 的口令 π_A 是否匹配.若成立 $(s'_A)^{F(\pi_A)}=H'_A$, 则直接认为攻击者 $\mathcal{A}$ 攻击成功并结束模拟.如果验证不通过,则让 A^i 拒绝该消息并结束该会话的模拟.容易看出,上述修改增加了攻击者成功的途径,因此有 $Adv_5(\mathcal{A})\leqslant Adv_6(\mathcal{A})$.

游戏 G_7:本游戏继续修改针对用户 A 的询问 $SendClient_2(A^i,\langle hp_{1A},hp_{2A},c_{SA}\rangle)$ 响应的模拟.若消息$\langle hp_{1A},hp_{2A},c_{SA}\rangle$确实来源于某个诚实模拟的 $SendServer_1(S^j,*)$ 的回复,则不再按照协议规范为 A^i 计算 $tk_A\|mk_A$,而是直接将 A^i 中的 $tk_A\|mk_A$ 设置成与 S^j 中一样的值.此时,由于会话 A^i 和 S^j 都是诚实模拟的,故上述修改并不改变攻击者的优势,即 $Adv_6(\mathcal{A})=Adv_7(\mathcal{A})$.

游戏 G_8:本游戏修改针对用户的激活消息 $SendClient_0(A^i)$ 响应的模拟方式.类似于游戏 G_2,我们将其中的 $c_{AS}=(u_A=g^{r_A},e_A=h^{r_A}\cdot P_A)$ 替换成虚拟口令所对应的 P_0 的密文.由于加密体制 PKE′是 CPA 安全的,从而攻击者在游戏 G_8 与在游戏 G_7 中的优势差是可忽略的,即

$$|Adv_8(\mathcal{A})-Adv_7(\mathcal{A})|\leqslant 2q_{send}\cdot Adv^{CPA}_{PKE'}(t+O(q_{send}+q_{exe})) \tag{8}$$

游戏 G_9:本游戏修改服务器在收到消息 $SendServer_1(S^j,\langle A,B,c_{AS}\rangle)$ 的响应方式.直接利用私钥 sk'对密文 c_{AS} 进行解密,并验证其中的 P_A 与用户口令 π_A 是否匹配.如果匹配,则直接认为攻击成功,停止模拟;如果不匹配,则按照完全随机的方式选择 $tk_A\|mk_A$.可以看出,第 1 部分修改仅仅是增加了攻击者成功的途径,而第 2 部分修改的合理性则由平滑投射哈希函数的随机性保证,从而可得

$$Adv_8(\mathcal{A})\leqslant Adv_9(\mathcal{A})+2q_{send}\cdot\varepsilon_{SPHF}(k) \tag{9}$$

游戏 G_{10}:本游戏继续修改服务器在收到消息 $SendServer_1(S^j,\langle A,B,c_{AS}\rangle)$的响应方式.类似于游戏 G_4,我们将 $c_{SA}=Enc(pk,M_A;l_A;tk_A),c_{SB}=Enc(pk,M_B;l_B;tk_B)$ 替换成消息 $M_A=s_A\|H_{0,A},M_B=s_B\|H_{0,B}$ 的密文,其中, $H_{0,A}=s_A^{\pi_0},H_{0,B}=s_B^{\pi_0}$. 由于 tk_A 和 tk_B 已被替换成完全随机的比特串,因此根据加密体制 PKE 的 CCA 安全性(由于游戏 G_6 需要解密能力),可知

$$|Adv_9(\mathcal{A})-Adv_{10}(\mathcal{A})|\leqslant 2q_{send}\cdot Adv^{CCA}_{PKE}(t+O(q_{send}+q_{exe})) \tag{10}$$

游戏 G_{11}:本游戏修改针对 $SendClient_d(A^i,m),d\in\{2,4\}$ 的模拟.类似于游戏 G_5,利用 DDH 自规约技术在给定三元组(X_0,Y_0,Z_0)的情形下,修改用户会话 A 和 B 生成 X、Y、sk_{AB}、sk_{BA} 的方式,即当用户 A 需要计算 X 时,选择随机的 $a,x\in\mathbb{Z}_p$ 并计算 $X=X_0^a g^x$, 当用户 B 需要计算 Y 时,选择随机的 $b,y\in\mathbb{Z}_p$ 并计算 $Y=Y_0^b g^y$, 当双方需要生成密钥时,计算 $sk_{AB}=sk_{BA}=Z_0^{ab}Y^{xb}X^{ya}g^{xy}$. 此时,攻击者区分真实的会话密钥 sk_{AB}=sk_{BA} 和完全随机值的优势不超过攻击者攻破 DDH 假设的优势,即

$$|Adv_{10}(\mathcal{A})-Adv_{11}(\mathcal{A})|\leqslant 2\cdot Adv^{ddh}_{G}(t+O(q_{send}+q_{exe})) \tag{11}$$

综上可得,攻击者的优势满足 $Adv^{ake}_{P,D}(\mathcal{A})=Adv_0(\mathcal{A})\leqslant Adv_{11}(\mathcal{A})+negl(k)$. 下面分析攻击者在游戏 G_{11} 中成功的方式.

(1) 攻击者冒充用户 A(B 类似)发送了消息$\langle A,B,c_{AS}\rangle$,且密文 c_{AS} 确实是与口令 π_A 相对应的密文;

(2) 攻击者冒充服务器向用户 A(B 类似)发送了消息$\langle hp_{1A},hp_{2A},c_{SA}\rangle$,且其中的 c_{SA} 确实是与口令 π_A 相对应的验证元(s_A,H_A)的密文;

(3) 在 MAC 安全的情况下,攻击者成功地伪造了用户 A(B 类似)所使用的 MAC 认证值;

(4) 攻击者成功地猜对了 *Test* 询问中所使用的比特 b.

记计算时间至多为 t 的攻击者针对协议所采用的 MAC 机制的优势函数为 $Adv^{CMA\text{-}EUF}_{MAC}(t)$, 由于 MAC 密钥在游戏 G_3 和 G_9 中已被替换成随机值,则攻击者通过情形(3)成功的概率至多是 $2(q_{send}+q_{exe})\cdot Adv^{CMA-EUF}_{MAC}(t+O(q_{send}+q_{exe}))$. 若用 *PwdGuess* 表示事件"上述情形(1)或情形(2)发生",注意到在上述游戏 G_{11} 中攻击者已经不能从会话消息获取到口令的任何信息,从而攻击者只能通过暴力穷举或字典攻击[22]猜测用户所使用的正确口令.

当协议中所有用户口令构成的集合服从 Zipf 定律时,可知攻击者成功的概率至多为 Pr[*PwdGuess*]$\leqslant C'\cdot q_{send}^{s'}$, 其中,$C'$和 s'是相应的 Zipf 参数.另外,如果事件 *PwdGuess* 不出现,注意到协议会话密钥都已经被替换成随机值,可知攻击者通过情形(4)成功的概率至多为 1/2.因此可得 $Adv_{11}(\mathcal{A})\leqslant C'\cdot q_{send}^{s'}$. 综合上式以及式(3)~式(11)可得,

$$\begin{aligned}Adv^{ake}_{P,D}(\mathcal{A})=Adv_0(\mathcal{A})\leqslant C'\cdot q_{send}^{s'}+2(q_{send}+q_{exe})\cdot[Adv^{CPA}_{PKE'}(t+O(q_{send}+q_{exe}))+\varepsilon_{SPHF}(k)+\\ Adv^{CCA}_{PKE}(t+O(q_{send}+q_{exe}))+Adv^{CMA\text{-}EUF}_{MAC}(t+O(q_{send}+q_{exe}))]+4\cdot Adv^{ddh}_{G}(t+O(q_{send}+q_{exe})).\end{aligned}$$

从而有 $Adv^{ake}_{P,D}(\mathcal{A})$ 至多比 $C'\cdot q_{send}^{s'}$ 大一个可忽略量,可知 I-V3PAKE 协议是语义安全的. □

定理 2. 若 DDH 假设成立,则 I-V3PAKE 协议相对于诚实而好奇的服务器可保证会话密钥的私密性.具体地说,假设 $\mathcal{A}_{kp}$ 是安全模型中针对会话密钥私密性的攻击者,其运行时间至多为 t,发出的 *Execute* 和 *Send* 询问次数至多为 q_{exe},q_{send},则有

$$Adv^{kp}_{P,D}(\mathcal{A}_{kp})\leqslant 2\cdot Adv^{ddh}_{G}(t+O(q_{exe}+q_{send})).$$

证明:给定会话密钥私密性攻击者 $\mathcal{A}_{kp}$,我们按照如下方式构造针对 DDH 问题的攻击者 $\mathcal{A}_{ddh}$.DDH 攻击者 $\mathcal{A}_{ddh}$ 收到输入的三元组(X_0,Y_0,Z_0),首先为所有用户选择口令,为 *TestPair* 询问选择随机比特 $b\in\{0,1\}$,诚实地模拟协议运行并基本按照规范回答攻击者 $\mathcal{A}_{kp}$ 发出的 *Execute* 和 *SendClient* 询问,不同之处在于,在询问响应中将最终 X、Y、sk_{AB}、sk_{BA} 相关的部分予以修改:按照类似于定理 1 证明中游戏 G_5 和 G_{11} 利用随机自规约方式将三元组(X_0,Y_0,Z_0)嵌入到协议运行中.

最后,$\mathcal{A}_{ddh}$ 观察 $\mathcal{A}_{kp}$ 的输出比特 b',如果 $b'=b$,则 $\mathcal{A}_{ddh}$ 输出 1,若 $b'\neq b$,则 $\mathcal{A}_{ddh}$ 输出 0.那么可以估计 $\mathcal{A}_{ddh}$ 成功的概率为

$$\begin{aligned}\Pr\{\mathcal{A}_{ddh}\text{ wins}\}&=\frac{1}{2}(\Pr\{b'=b|\text{Real}(X_0,Y_0,Z_0)\}+\Pr\{b'\neq b|\text{Rand}(X_0,Y_0,Z_0)\})\\&=\frac{1}{2}\left(\frac{1}{2}+\frac{1}{2}Adv_{P,D}^{kp}(\mathcal{A}_{kp})+\left(1-\frac{1}{2}\right)\right)\\&=\frac{1}{2}+\frac{1}{4}Adv_{P,D}^{kp}(\mathcal{A}_{kp}).\end{aligned}$$

其中,*Real*(·)和 *Rand*(·)分别表示输入的三元组是真实的 DDH 三元组和随机的三元组.当(X_0,Y_0,Z_0)是随机三元组时,随机自规约保证了最终会话密钥是独立随机的;当(X_0,Y_0,Z_0)是真实的 DDH 三元组时,给攻击者 $\mathcal{A}_{kp}$ 提供的模拟环境与真实攻击相同.最后,注意到 $\mathcal{A}_{ddh}$ 对每个 *Execute* 和 *SendClient* 询问的模拟都只需要常数时间,即可得定理结论. □

6 结束语

本文对基于验证元三方 PAKE 协议进行了研究.首先,指出目前唯一的在标准模型下设计的基于验证元的三方 PAKE 协议存在安全缺陷,易于遭受离线字典攻击.其次,基于 ElGamal 公钥加密体制、口令哈希机制以及支持验证元的平滑投射哈希函数等密码学组件,构造了一个新的基于验证元的三方 PAKE 协议,并在标准模型下证明了该协议满足语义安全、会话密钥私密性等安全属性,与已有协议的比较表明新协议不仅提供了更高的安全性,而且具有可接受的计算和通信效率.

References:

[1] Bonneau J, Herley C, van Oorschot PC, Stajano F. The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. In: Proc. of IEEE Symp. on Security and Privacy (S&P). IEEE, 2012. 553–567.

[2] Bellovin SM, Merritt M. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In: Proc. of the Symp. on Security and Privacy (S&P). IEEE, 1992. 72–84.

[3] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks. In: Preneel B, ed. Proc. of the EUROCRYPT 2000. Berlin, Heidelberg: Springer-Verlag, 2000. 139–155.

[4] Boyko V, MacKenzie P, Patel S. Provably secure password-authenticated key exchange using Diffie-Hellman. In: Preneel B, ed. Proc. of the EUROCRYPT 2000. Berlin, Heidelberg: Springer-Verlag, 2000. 156–171.

[5] Abdalla M, Fouque PA, Pointcheval D. Password-based authenticated key exchange in the three-party setting. In: Vaudenay S, ed. Proc. of the Public Key Cryptography-PKC 2005. Berlin, Heidelberg: Springer-Verlag, 2005. 65–84.

[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. Berlin, Heidelberg: Springer-Verlag, 2005. 404–421.

[7] Abdalla M, Catalano D, Chevalier C, Pointcheval D. Efficient two-party password-based key exchange protocols in the UC framework. In: Malkin T, ed. Proc. of the CT-RSA 2008. Berlin, Heidelberg: Springer-Verlag, 2008. 335–351.

[8] Abdalla M, Benhamouda F, MacKenzie P. Security of the J-PAKE password-authenticated key exchange protocol. In: Proc. of the Symp. on Security and Privacy (S&P). IEEE, 2015. 571–587.

[9] Katz J, Ostrovsky R, Yung M. Efficient password-authenticated key exchange using human-memorable passwords. In: Pfitzmann B, ed. Proc. of the EUROCRYPT 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 475–494.

[10] Gennaro R, Lindell Y. A framework for password-based authenticated key exchange. In: Biham E, ed. Proc. of the EUROCRYPT 2003. Berlin, Heidelberg: Springer-Verlag, 2003. 524–543.

[11] Jiang S, Gong G. Password based key exchange with mutual authentication. In: Handschuh H, Hasan A, eds. Proc. of the Selected Areas in Cryptography. Berlin, Heidelberg: Springer-Verlag, 2005. 267–279.

[12] Hu XX, Zhang ZF, Liu WF. Universal composable password authenticated key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2011,22(11):2820−2832 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3910.htm [doi: 10.3724/SP.J.1001.2011.03910]

[13] Benhamouda F, Blazy O, Chevalier C, Pointcheval D, Vergnaud D. New techniques for SPHFs and efficient one-round PAKE protocols. In: Canetti R, Garay JA, eds. Proc. of the CRYPTO 2013. Berlin, Heidelberg: Springer-Verlag, 2013. 449–475.

[14] Hu XX, Zhang J, Zhang ZF, Xu J. Universally composable anonymous password authenticated key exchange. Science China Information Sciences, 2017,60(5):52107.

[15] Chang CC, Chang YF. A novel three-party encrypted key exchange protocol. Computer Standards & Interfaces, 2004,26(5): 471–476.

[16] Lu RX, Cao ZF. Simple three-party key exchange protocol. Computers & Security, 2007,26(1):94–97.

[17] Deng ML, Ma JF, Le FL. Universally composable three party password-based key exchange protocol. China Communications, 2009,6(3):150–155.

[18] Chang T, Hwang M, Yang W. A communication-efficient three-party password authenticated key exchange protocol. Information Sciences, 2011,181:217–226.

[19] Xiong H, Chen Y, Guan Z, Chen Z. Finding and fixing vulnerabilities in several three-party password authenticated key exchange protocols without server public keys. Information Sciences, 2013,235:329–340.

[20] Hu XX, Zhang ZZ, Zhang QH. Universally composable three-party password-authenticated key exchange with contributiveness. Int'l Journal of Communication Systems, 2015,28(6):1100–1111.

[21] Zhang QH, Hu XX, Wei JH, Liu WF. Universally composable three-party password authenticated key exchange. In: Sun X, Chao HC, eds. Proc. of the Int'l Conf. on Cloud Computing and Security. Cham: Springer-Verlag, 2017. 123–137.

[22] Wang D, Zhang Z, Wang P, Huang XY. Targeted online password guessing: An underestimated threat. In: Proc. of the 2016 ACM SIGSAC Conf. on CCS. ACM, 2016. 1242–1254.

[23] Gentry C, MacKenzie P, Ramzan Z. A method for making password-based key exchange resilient to server compromise. In: Dwork C, ed. Proc. of the CRYPTO 2006. Berlin, Heidelberg: Springer-Verlag, 2006. 142–159.

[24] Kiefer F, Manulis M. Zero-knowledge password policy checks and verifier-based PAKE. In: Kutyłowski M, Vaidya J, eds. Proc. of the European Symp. on Research in Computer Security. Cham: Springer-Verlag, 2014. 295–312.

[25] Benhamouda F, Pointcheval D. Verifier-based password-authenticated key exchange: New models and constructions. IACR Cryptology ePrint Archive, 2013, https://eprint.iacr.org/2013/833.pdf

[26] Wang D, Cheng H, Wang P, Huang XY. A security analysis of honeywords. In: Proc. of the Network and Distributed Systems Security (NDSS) Symp. San Diego: The Internet Society, 2018. 1–16.

[27] Andrade ER, Simplicio MA, Barreto PS, Santos PCF. Lyra2: Efficient password hashing with high security against time-memory trade-offs. IEEE Trans. on Computers, 2016,65(10):3096–3108.

[28] Lai RW, Egger C, Schröder D, Chow SM. Phoenix: Rebirth of a cryptographic password-hardening service. In: Proc. of the 26th USENIX Security Symp. (USENIX Security 17). 2017. 899–916.

[29] Yang XY, Hou MB, Wei XC. Verifier-based three-party password authenticated key exchange protocol. Journal of Computer Research and Development, 2016,53(10):2230–2238 (in Chinese with English abstract).

[30] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen LR, ed. Proc. of the EUROCRYPT 2002. Berlin, Heidelberg: Springer-Verlag, 2002. 45–64.

[31] Katz J, Vaikuntanathan V. Round optimal password based authenticated key exchange. In: Ishai Y, ed. Proc. of the Theory of Cryptography Conf. Berlin, Heidelberg: Springer-Verlag, 2011. 293–310.

[32] 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 with English abstract). http://www.jos.org.cn/1000-9825/4861.htm [doi: 10.13328/j.cnki.jos.004861]

[33] Wang D, Cheng HB, Wang P, Huang XY, Jiang GP. Zipf's law in passwords. IEEE Trans. on Information Forensics and Security, 2017,12(11):2776−2791.

[34] Wang D, Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. on Dependable and Secure Computing, 2018,15(4):708−722.

[35] Abdalla M, Bellare M, Rogaway P. The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: Naccache D, ed. Proc. of the CT-RSA 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 143−158.

[36] Yang JH, Cao TJ. Provably secure three-party password authenticated key exchange protocol in the standard model. Journal of Systems and Software, 2012,85(2):340−350.

[37] Wu SH, Zhu YF. Three-party password-authenticated key exchange with forward security. Chinese Journal of Computers, 2007,30(10):1833−1841 (in English with Chinese abstract).

附中文参考文献:

[12] 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. http://www.jos.org.cn/1000-9825/3910.htm [doi: 10.3724/SP.J.1001.2011.03910]

[29] 杨晓燕,侯孟波,魏晓超.基于验证元的三方口令认证密钥交换协议.计算机研究与发展,2016,53(10):2230−2238.

[32] 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 [doi: 10.13328/j.cnki.jos.004861]

[37] 吴树华,祝跃飞.一个前向安全的基于口令认证的三方密钥交换协议.计算机学报,2007,30(10):1833−1841.

张启慧(1983－),女,讲师,博士生,主要研究领域为安全协议,大数据安全.

刘文芬(1965－),女,博士,教授,博士生导师,主要研究领域为大数据安全.

胡学先(1982－),男,博士,副教授,主要研究领域为安全协议,大数据安全.

魏江宏(1987－),男,博士,讲师,主要研究领域为属性基密码,大数据安全.