可证明安全的抗量子高效口令认证密钥交换协议

尹安琪[1)] 汪 定[2),3)] 郭渊博[1)] 陈 琳[1)] 唐 迪[1)]

[1)](信息工程大学电子技术学院 郑州 450001)

[2)](南开大学网络空间安全学院 天津 300350)

[3)](天津市网络与数据安全技术重点实验室(南开大学) 天津 300350)

摘 要 基于格的口令认证密钥交换(Password-Authenticated Key Exchange,PAKE)协议在后量子时代具有广泛的应用前景.降低通信轮次可以有效提高执行效率,也是格上 PAKE 协议的重要优化方向.现有基于格的低轮次 PAKE 协议的构建方法主要有两种:一种是基于非交互式零知识(Non-Interactive Zero-Knowledge,NIZK)证明,但在标准模型下如何在格上实现 NIZK 证明仍然是公开问题;另一种虽然宣称基于不可区分适应性选择密文攻击(Indistinguishability under Adaptive Chosen-Ciphertext Attack,IND-CCA2)的安全模型,但实际上只采用了不可区分性选择密文攻击(Indistinguishability under Chosen-Ciphertext Attack,IND-CCA1)安全的公钥加密(Public Key Encryption,PKE)方案,该类 PAKE 协议在现实应用时需要利用签名/验签等技术才能保证安全性.这两种方法都会增加计算和通信开销.为此,本文利用带误差学习(Learning with Errors,LWE)问题的加法同态属性,提出了一种格上 IND-CCA2 安全的非适应性平滑投影哈希函数(Smooth Projective Hash Function,SPHF),该函数支持一轮 PAKE 协议的构造;并确定了所基于的 PKE 方案中相关参数的大小,从而消除了 LWE 问题的不完全加法同态属性对 SPHF 正确性的影响.尽所知,这是格上第一个直接基于 IND-CCA2 安全模型的非适应性 SPHF,且该 SPHF 具有相对独立的研究价值,可应用于证据加密、零知识证明和不经意传输等领域.基于此,本文构建了一种格上可证明安全的高效 PAKE 协议.该协议可以抵御量子攻击;只需要一轮通信,因而具有最优的通信轮次;是基于标准模型,所以避免了使用随机预言机的潜在安全威胁,特别是使用随机预言机可能导致格上 PAKE 协议遭受离线口令猜测攻击和量子攻击;在实际应用时,该协议也不需要利用 NIZK 证明和签名/验签等技术来保证安全性,这有效提高了执行效率.本文还利用人人网 474 万口令数据验证了基于 CDF-Zipf 定律的 PAKE 协议安全模型可以更加准确地评估 PAKE 协议所提供的安全强度;最后基于该安全性模型,本文在标准模型下对所提出的 PAKE 协议进行了严格的安全性证明.实验结果表明,与其它相关协议相比,本文协议具有最优的整体执行效率和最低的通信开销.

关键词 抗量子;非适应性平滑投影哈希函数;高效;加法同态;口令认证密钥交换协议;可证明安全

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2022.02321

Provably Secure Quantum Resistance Efficient Password-Authenticated Key Exchange Protocol

YIN An-Qi[1)] WANG Ding[2),3)] GUO Yuan-Bo[1)] CHEN Lin[1)] TANG Di[1)]

[1)](*College of Electronic Technology, Information Engineering University, Zhengzhou* 450001)

[2)](*College of Cyber Science, Nankai University, Tianjin* 300350)

[3)](*Tianjin Key Laboratory of Network and Data Security Technology (Nankai University), Tianjin* 300350)

Abstract Password-Authenticated Key Exchange(PAKE) protocol has a wide application prospect in the coming post-quantum era. Scaling down the number of communication rounds is capable of effectively improving the execution efficiency, and this is a rather important direction for optimi-

收稿日期:2021-11-10;在线发布日期:2022-07-20.本课题得到国家自然科学基金(62172240)和京津冀基础研究合作专项(21JCZXJC00100)资助.**尹安琪**,博士,主要研究方向为口令认证密钥交换协议和格密码理论.E-mail:yinanqi0222@foxmail.com.**汪 定**(通信作者),博士,教授,博士生导师,主要研究领域为口令安全和密码协议.E-mail:wangding@nankai.edu.cn.**郭渊博**,博士,教授,博士生导师,主要研究领域为网络防御、机器学习和人工智能安全等.**陈 琳**,博士,副教授,主要研究方向为网络安全、安全专用芯片设计.**唐 迪**,硕士,主要研究方向为网络安全.

zing PAKE protocols over lattices. Up to now, there are mainly two technical routes in the existing literature guiding the construction of low-round PAKE schemes over lattices. One is based on Non-Interactive Zero-Knowledge (NIZK) proofs, but how to implement NIZK proofs in the standard model over lattices is still an open question for these derivative schemes; the other one is nominally designed as Indistinguishability under Adaptive Chosen-Ciphertext Attack (IND-CCA2) secure based protocol, nevertheless it applies only an Indistinguishability under Chosen-Ciphertext Attack (IND-CCA1) secure based Public Key Encryption (PKE) scheme in implementation, which relies on the introduction of signature/verification algorithms or other techniques to ensure its security in implementation. Moreover, these two methods will introduce extra computation and communication costs. Therefore, taking advantage of the additive homomorphic property of the Learning with Errors(LWE) problem, this paper proposes an IND-CCA2 secure word-independent Smooth Projective Hash Function(SPHF) over lattices, which also supports the construction of one-round PAKE protocols. And this paper identifies the exact values of parameters of the PKE scheme that the proposed SPHF predicates on, ultimately eliminate the influence of the incomplete additive homomorphic property of the LWE problem on the correctness of the SPHF. As far as we know, so mentioned function is the first IND-CCA2 secure word-independent SPHF over lattices. Besides, the proposed SPHF possesses independent research value and great application potential in multiple practice fields such as witness encryption, zero-knowledge proof, oblivious transmission and so on. On this basis, this paper innovatively designs an efficient provably secure PAKE protocol. This protocol is resistant to quantum attack; it only requires one-round communication, achieving the optimal communication round; it is based on the standard model, thus capable of avoiding the potential security threats of utilizing random oracles, especially in situations where the utilize of random oracles may cause lattice-based PAKE protocols to suffer offline password guessing attacks and quantum attacks. In practical applications, the proposed protocol does not reflect dependence on the utilization of NIZK proofs, signature/verification algorithms or other techniques to ensure its security, which will effectively improve the execution efficiency. In addition, this paper utilizes a dataset containing 4.74 million unique username—password pairs of Renren to verify that the PAKE security analysis model based on the CDF-Zipf law is indubitable feasible to more accurately evaluate the security guarantee that a real PAKE protocol can provide. Finally, in the standard model and based on this more realistic security analysis model, this paper provides a strict proof of the security of above mentioned protocol. Controlled experimental results show that the proposed PAKE protocol has the most optimal efficiency and the lowest communication cost compared with other related protocols, which drops in line with our expectations.

Keywords quantum resistance; word-independent smooth projective hash function; efficient; additive homomorphism; password-authenticated key exchange; provably secure

1 引 言

利用口令认证密钥交换协议,协议参与方只需持有低熵口令,就可以通过公开的非安全信道,协商高熵的会话密钥[1].在实际应用中,PAKE 协议的执行不依赖智能卡、传感器等硬件设备,也不需要指纹、虹膜等涉及个人隐私的生物特征,这大大提高了安全系统的可部署性[2].但随着量子计算技术的快速发展,基于大整数分解、离散对数等传统困难问题的 PAKE 协议[3-7]将面临严重的安全威胁.

基于格上困难问题的密码体制不仅能够抵御量

子攻击[8]，还具有高渐进效率的优势[9]，而且在全同态加密[10]等领域具有广泛应用. 此外，在格上已经实现了从最坏情况困难问题到平均情况困难问题的安全性归约[11]，这使格密码体制可以随机选取困难实例. 但与基于传统困难问题的 PAKE 协议相比，目前格上 PAKE 协议的研究投入明显不足，普遍存在计算效率较低、通信开销较大等问题. 优化协议的通信轮次不仅可以降低计算和通信开销，还可以降低其被攻击的风险，并且有助于简化对协议的安全性分析. 因此，优化协议的通信轮次一直是格上 PAKE 协议的重要优化方向，并取得了一些阶段性成果[12-15].

构造格上低轮次（即一轮和两轮）PAKE 协议所需的 PKE 应具备 IND-CCA2 安全性，这也是目前实际应用的安全标准[16]. NIZK 证明技术是构造上述 PKE 的有效技术[17-18]，但在标准模型下实现格上的 NIZK 证明仍然为公开问题[14]，且使用此类证明会大大增加 PAKE 协议的计算、通信和存储开销. 一些基于格的 PAKE 协议（如文献[19-20]）虽然避免了 NIZK 证明的使用，但只采用了 IND-CCA1 安全的 PKE，这导致此类协议在实际应用时需要利用签名/验签等技术来保证安全性，这同样增加了 PAKE 协议各方面的开销.

在格上，构造高效的一轮 PAKE 协议主要有以下困难：(1) 在不使用额外密码学原语的前提下保证 PAKE 协议的安全性，以简化协议架构并提高执行效率. 目前格上的低轮次 PAKE 协议需要使用 NIZK 证明（如文献[13-15]）或签名/验签（如文献[19]）等密码学原语；(2) 在设计 SPHF 的同时实现 IND-CCA2 安全性和非适应性. 非适应性 SPHF 是构建一轮 PAKE 协议的有效数学工具，但在格上还不存在 IND-CCA2 安全的此类 SPHF. 且现有的直接基于 IND-CCA2 安全模型的 PKE 较少，一般有基于带标签的[21-22]和多密文分量的[14]两种. 目前，基于前者构建的 SPHF 要求标签固定（如文献[13]），基于后者构建的 SPHF 只使用了单个密文分量（如文献[14-15]），都不具备 IND-CCA2 安全性. 且基于后者的 SPHF 是适应性的，最多支持两轮 PAKE 协议的构造；(3) 确定所基于的 PKE 中相关参数的大小，以保证 SPHF 的正确性. LWE 问题只具备不完全加法同态属性，因此直接基于多密文分量构建 SPHF 不能保证其正确性.

因此，本文主要研究在避免使用非交互式零知识证明、签名/验证等技术的前提下，设计格上直接基于 IND-CCA2 安全模型的非适应性平滑投影哈希函数，并进一步提出格上可证明安全的抗量子高效口令认证密钥交换协议.

1.1　相关工作

本文主要研究 SPHF 与 PAKE 协议，下面从这两个方面介绍相关工作.

SPHF 可分为适应性和非适应性两类，其中后者在计算投影密钥时不依赖密文，是构建一轮 PAKE 协议的关键. 与基于传统困难问题构建 SPHF[4-7]相比，基于格困难问题构建 SPHF 比较困难[23]. 为此，文献[21]提出在格上利用近似 SPHF 实现 PAKE 协议的技术路线，并给出了第一个基于格的近似 SPHF. 在此基础上，文献[24]也提出了一种基于格的近似 SPHF. 然而，上述 SPHF 都是适应性的，最多支持两轮 PAKE 协议的构建. 文献[13]利用带标签的 IND-CCA2 安全的 PKE 分别构建了一种适应性和一种非适应性 SPHF，其中后者要求标签固定，所以只具备不可区分性选择明文攻击（Indistinguishability under Chosen-Plaintext Attack，IND-CPA）安全性. 文献[19]改进了文献[13]中的非适应性方案，从而得到了一种 IND-CCA1 安全的非适应性 SPHF. 文献[14]基于 IND-CCA2 安全的 PKE 构建了一种基于格的 SPHF；但一方面，该 SPHF 只使用了多密文分量中的一个，因而不具备 IND-CCA2 安全性，这导致所得到的 PAKE 协议无法避免使用 NIZK 证明；另一方面，该 SPHF 是适应性的，不支持一轮 PAKE 协议的构造. 文献[25]提出了一种格上 IND-CCA1 安全的精确 SPHF，这使格上 PAKE 协议的安全性不再局限于 BPR（Bellare-Pointcheval-Rogaway）模型[26]. 然而，上述方案都没有解决直接基于 IND-CCA2 安全模型构建格上非适应性 SPHF 的问题.

早期的 PAKE 协议一般是基于 KOY/GL[5-6]或者 JG/GK[4,7]架构，这两种架构都需要三轮通信，但后者可实现相互认证. 为减小协议的开销，文献[14-15,20]等研究了 PAKE 协议的两轮实现问题. 文献[27]进一步提出了可证明安全的一轮 PAKE 协议，但 NIZK 证明的使用影响了执行效率的提升. 文献[13]在格上实例化了文献[27]中的 PAKE 协议，从而得到了格上首个一轮 PAKE 协议. 文献[28]研究了在无可信中心的应用场景下设计格上安全 PAKE 协议的问题. 但上述两个方案均需使用 NIZK 证明. 文献[19]改进了文献[13]中的一轮 PAKE 协议，所提出的方案避免了 NIZK 证明的使用，却引入了签名/验签算法，这依然影响执行效率的提升. 近期，还有很多文献研究基于理想格的

PAKE 协议[29-31]，这进一步提高了格上 PAKE 协议的执行效率. 上述基于格的 PAKE 协议多采用 IND-CPA 或者 IND-CCA1 安全的 PKE 方案，因此在实际应用时需要使用 NIZK 证明[13-15]或签名/验签等技术[19]来保证安全性. 个别 PAKE 协议[14-15]即使采用了 IND-CCA2 安全的 PKE 方案，也无法避免 NIZK 证明的使用，且需要两轮通信，这都降低了协议的执行效率且增大了通信与存储开销.

1.2 主要贡献

本文的主要贡献有三：

(1) 利用 LWE 问题的加法同态属性，本文提出了一种格上基于多密文分量的非适应性 SPHF，可支持一轮 PAKE 协议的构建. 鉴于 LWE 问题只具备不完全加法同态属性，本文还确定了所基于的公钥加密算法中相关参数的大小，以保证 SPHF 的正确性. 尽所知，这是格上第一个 IND-CCA2 安全的非适应性 SPHF，且具有相对独立的研究价值，还可应用于证据加密、零知识证明和不经意传输等领域.

(2) 基于所提出的非适应性 SPHF，本文构建了一种格上可证明安全的高效 PAKE 协议. 该协议可以抵御量子攻击；只需要一轮通信，具有最优的通信轮次，因此降低了通信开销；且不需要使用 NIZK 证明和签名/验签等密码学原语来保证安全性，从而提高了执行效率.

(3) 本文借鉴文献[19-20]的做法，假设口令分布服从 CDF-Zipf 定律[32]，因而所采用的 PAKE 协议安全模型更加现实；并通过 474 万人人网口令数据验证了该模型可以更加准确地评估 PAKE 协议面临的真实风险. 在标准模型下，根据所采用的更加现实的安全模型，本文对所提出的协议进行了严格的安全性证明，从而避免了使用随机预言机的潜在安全威胁，特别是它可能导致 PAKE 协议遭受离线口令猜测攻击.

1.3 组织结构

本文在第 2 节介绍构建格上非适应性平滑投影哈希函数和一轮口令认证密钥交换协议所需的预备知识；第 3 节给出本文的口令认证密钥交换协议安全模型；第 4 节提出一种格上 IND-CCA2 安全的非适应性平滑投影哈希函数，并对其进行正确性与平滑性证明；第 5 节提出一种格上可证明安全的抗量子高效口令认证密钥交换协议，并对其进行正确性与安全性证明；第 6 节对所提出的协议进行仿真，并与相关协议进行对比；第 7 节总结全文，并指出下一步的研究方向.

2 预备知识

令 q 为素数或某素数 $b(b\geq 2)$ 的幂，矩阵用加粗的大写字母表示，向量用加粗的小写字母表示. 本文用到的符号及其含义见表 1.

表 1 符号定义

符号	含义
κ	安全参数
$\|/\|\|$	矩阵或向量的横/纵向级联
$negl(\cdot)$	可忽略函数
q	LWE 问题的模数
$\boldsymbol{A}^{\mathrm{T}}$	矩阵 $\boldsymbol{A}$ 的转置
$\leftarrow/\xleftarrow{r}$	取样/随机取样
$\|\mathcal{D}\|$	集合 $\mathcal{D}$ 的大小
$\|\boldsymbol{x}\|$	向量 $\boldsymbol{x}$ 的欧几里得范数
$\perp$	非法标识
$\lceil\cdot\rceil/\lfloor\cdot\rfloor$	向上/向下取整
$\langle\cdot,\cdot\rangle$	内积运算
$Ham(\cdot,\cdot)$	汉明距离函数
$\boldsymbol{0}$	零向量

2.1 LWE 困难问题

本小节主要介绍判定性 LWE 问题的定义，并给出格和离散高斯分布的概念.

格[33]. 格 Λ 可定义为 $\{\Lambda_{\boldsymbol{A}}=\boldsymbol{As}\,|\,\boldsymbol{s}\in\mathbb{Z}^n\}$，其中 $\boldsymbol{A}\in\mathbb{R}^{m\times n}$ 是格 Λ 的基矩阵，$\boldsymbol{A}$ 的列向量线性无关.

离散高斯分布[34]. 设高斯函数的中心为 $\boldsymbol{c}\in\mathbb{Z}^m$，平滑参数为 s. 另设高斯权重函数为 $\rho_{s,\boldsymbol{c}}$，其表达式为 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/s^2)$. 对于格 $\Lambda\in\mathbb{Z}^m$，令 $\rho_{s,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$，定义格 Λ 上的离散高斯分布如下. 特别地，若 $\boldsymbol{c}=\boldsymbol{0}$，可将 $\boldsymbol{c}$ 省略.

$$D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)} \tag{1}$$

判定性 $\mathrm{LWE}_{n,q,\chi,m}$ 问题[35]. 对于正整数 m,n,q $(q\geq 2, m=poly(n), q\leq 2^{poly(n)})$，任意离散高斯分布 $\chi=D_{\Lambda,s}(\Lambda\in\mathbb{Z}_q^m, s\in(0,1), s\cdot q\geq 2\sqrt{n})$，存在以下分布：(1) $\{(\boldsymbol{A},\boldsymbol{b})\,|\,\boldsymbol{A}\xleftarrow{r}\mathbb{Z}_q^{m\times n},\boldsymbol{b}\xleftarrow{r}\mathbb{Z}_q^{m\times 1}\}$；(2) $\{(\boldsymbol{A},\boldsymbol{b})\,|\,\boldsymbol{A}\xleftarrow{r}\mathbb{Z}_q^{m\times n},\boldsymbol{s}\xleftarrow{r}\mathbb{Z}_q^{m\times 1},\boldsymbol{e}\xleftarrow{r}\chi^{m\times 1},\boldsymbol{b}=\boldsymbol{As}+\boldsymbol{e}(\mathrm{mod}\,q)\}$. 判定性 $\mathrm{LWE}_{n,q,\chi,m}$ 问题定义为区分以上两个分布的问题.

安全性归约[35]. 若参数 $s\cdot q\geq 2\sqrt{n}, q\leq 2^{poly(n)}$，判定性 $\mathrm{LWE}_{n,q,\chi,m}$ 问题至少与最坏情况下具有多项式困难因子的最短线性无关向量问题一样困难.

2.2 格上 IND-CCA2 安全的公钥加密方案

构建 IND-CCA2 安全的 PKE 方案一般有两种

方法.一种是在随机预言机模型下,利用 IND-CPA 安全的 PKE 构建;但使用随机预言机的安全性存疑[36],因为在实际应用时需要用具体的哈希函数代替随机预言机.另一种是在标准模型下,利用 NIZK 证明技术、哈希证明系统、BCHK 转换技术(又分为 BCHK-Sig 与BCHK-Mac 技术)和陷门技术[16]构建.文献[22]利用 BCHK-Sig 技术设计了一种 IND-CCA1 安全的公钥加密算法,称为 MP(Micciancio-Peikert)方案.目前在基于格的 SPHF 和 PAKE 协议[13,19-20]中,MP 方案是应用最广泛的 PKE 方案之一.但基于 MP 方案构建的 PAKE 协议或者 SPHF,在实际应用时需要使用一次性签名等技术来保证 IND-CCA2 安全性,这增加了计算、通信与存储开销.

文献[16]利用 BCHK-Mac 技术在格上构造了一种 IND-CCA2 安全的公钥加密算法,该算法具有较高的执行效率,本文将其记作 Σ 方案.本文基于 Σ 方案展开研究,下面给出 Σ 方案的定义.

设 κ 为安全参数,令 $m,n,\bar{m},b,k$ 为正整数,且满足 $n,\bar{m}>0$,$m=\bar{m}+n\cdot k$,$b\geq 2$,$k=\lceil \log_b q\rceil$,$2\leq d\leq\sqrt{q}$,$n\cdot\log_2 d\geq 3\kappa$.令 $\mathbb{F}(2^\kappa)$ 表示阶为 2^κ 的有限域,$H:\{0,1\}^*\to\mathbb{F}(2^\kappa)/\{0\}$ 为抗碰撞哈希函数;并令 $(encoded,decoded)$ 为编/解码算法,$FRD:\mathbb{F}(2^\kappa)\to\mathbb{Z}_q^{n\times n}$ 为全秩差编码算法;那么 $\Sigma(KeyGen,Enc,Dec)$ 的定义如下:

$KegGen(1^\kappa)$:首先随机选取 $\boldsymbol{A}\xleftarrow{r}\mathbb{Z}_q^{n\times\bar{m}}$,$\boldsymbol{R}\xleftarrow{r}(D_{\mathbb{Z}^{\bar{m}},\omega(\sqrt{\log n})})^{nk}$,然后计算矩阵 $\boldsymbol{B}=-\boldsymbol{A}\boldsymbol{R}$,最后返回 Σ 方案的公私钥对 $(pk,sk)=((\boldsymbol{A},\boldsymbol{B}),\boldsymbol{R})$.

$Enc(pk,p\in\mathbb{F}(2^\kappa))$:$\boldsymbol{s}\xleftarrow{r}D_{\mathbb{Z}^n,\alpha q}$,$\boldsymbol{e}_1\xleftarrow{r}D_{\mathbb{Z}^{\bar{m}},\alpha q}$,$\boldsymbol{e}_2\xleftarrow{r}D_{\mathbb{Z}^{nk},\gamma}$($\gamma=\sqrt{\|\boldsymbol{e}_1\|^2+\bar{m}(\alpha q)^2}\cdot\omega(\sqrt{\log n})$),$x,y,z\xleftarrow{r}\mathbb{F}(2^\kappa)$;令 $\boldsymbol{v}=x\|y\|z\in(\mathbb{F}(2^\kappa))^3$,并计算

$$\begin{cases}\tilde{\boldsymbol{s}}=\boldsymbol{s}+encode_d(\boldsymbol{v})\\ \boldsymbol{c}_1=\boldsymbol{A}^{\mathrm{T}}\tilde{\boldsymbol{s}}+\boldsymbol{e}_1\\ \boldsymbol{c}_2=(\boldsymbol{B}+FRD(tag)\boldsymbol{G}_b)^{\mathrm{T}}\tilde{\boldsymbol{s}}+\boldsymbol{e}_2\\ c_3=x+p\\ c_4=\tau y+z\end{cases}\tag{2}$$

其中 $tag=H(\boldsymbol{c}_1)\in\mathbb{F}(2^\kappa)$,$\tau=H(\boldsymbol{c}_2,c_3)\in\mathbb{F}(2^\kappa)$;最后,返回密文 $\boldsymbol{C}=(\boldsymbol{c}_1,\boldsymbol{c}_2,c_3,c_4)\in\mathbb{Z}_q^{\bar{m}}\times\mathbb{Z}_q^{nk}\times\mathbb{F}(2^\kappa)\times\mathbb{F}(2^\kappa)$.

上述 $\tilde{\boldsymbol{s}}$ 与密文 $\boldsymbol{C}$ 是绑定的,$\tilde{\boldsymbol{s}}$ 又称为明密文对 $(\boldsymbol{C},p)$ 的证据.本研究不需要使用解密算法(Dec),所以不再对其进行介绍,解密过程可参见文献[16].

2.3　平滑投影哈希函数

平滑投影哈希函数的概念最初由 Cramer 等人[37]提出;文献[21]根据格上的应用需求对此概念进行修改,本文采用文献[21]中的相关概念.

设口令 pw 的集合为 $\mathcal{D}$,IND-CCA2 安全的公钥加密方案的公钥为 pk;令 $\mathcal{C}_{pk}$ 表示与 pk 对应的 $(label,\boldsymbol{C})$ 对的集合,其中 $label$ 表示有效标签,$\boldsymbol{C}$ 表示与 pk 相对应的密文.对于给定的 pk,定义集合 $\mathcal{X}$ 和 $\{\mathcal{L}_{pw}\}_{pw\in\mathcal{D}}$ 如下[21]:

(1) $\mathcal{X}:=\{(label,\boldsymbol{C},pw)\mid(label,\boldsymbol{C})\in\mathcal{C}_{pk}\ \&\&\ pw\in\mathcal{D}\}$;

(2) $\mathcal{L}_{pw}:=\{(label,\mathrm{Enc}(pk,pw\|label),pw\in\mathcal{D})\}$.

$\mathcal{X}$ 表示三元组 $(label,\boldsymbol{C},pw)$ 的集合,本文称三元组 $(label,\boldsymbol{C},pw)$ 为一个单词,用 $\boldsymbol{W}$ 表示.单词 $(label,\boldsymbol{C},pw)$ 的第一个元素为有效标签 $label$,第三个元素为口令 $pw\in\mathcal{D}$,第二个元素为与 $pw\|label$ 相对应的合法密文.令 $\mathcal{L}=\{\mathcal{L}_{pw}\mid pw\in\mathcal{D}\}$,易知 $\mathcal{L}\subset\mathcal{X}$.

平滑投影哈希函数[21].平滑投影哈希函数可以通过取样算法定义:给定公钥 pk 和集合 $\mathcal{X}$、$\mathcal{L}$、$\mathcal{L}_{pw}$,输出 $(\mathcal{K},\mathcal{G},\mathcal{H}=\{Hash(\boldsymbol{W},HK\in\mathcal{K}):\mathcal{X}\to\mathcal{G}\},\mathcal{S},ProjKG:\mathcal{K}\to\mathcal{S})$.其中 $\mathcal{K}$ 为哈希密钥 HK 的集合;$\mathcal{G}$ 为某集合;$\mathcal{H}$ 为带密钥的哈希函数簇,其定义域为 $\mathcal{X}$,值域为 $\mathcal{G}$;$\mathcal{S}$ 为投影密钥 HP 的集合;$ProjKG$ 为投影函数.平滑投影哈希函数必须满足以下条件:

(1) 存在以下三种高效算法:哈希密钥的取样算法,$HK\xleftarrow{r}\mathcal{K}$;哈希函数,$Hash(\boldsymbol{W},HK\in\mathcal{K}):\mathcal{X}\to\mathcal{G}$;投影函数,$ProjKG:\mathcal{K}\to\mathcal{S}$;

(2) 近似正确性:对于 $\forall\boldsymbol{W}\in\mathcal{L}$,存在高效算法 $ProjHash$ 以投影密钥 $HP\leftarrow ProjKG(HK,pk)$ 和 $(\boldsymbol{W}=(label,\boldsymbol{C},pw),r)$ 为输入,满足 $Pr(Ham(Hash(\boldsymbol{W},HK),ProjHash(HP,\boldsymbol{W},r))>\varepsilon\cdot l)=negl(\kappa)$,其中 l 表示哈希值的长度.即哈希值 $Hash(\boldsymbol{W},HK)$ 的计算方式有两种,一种是通过哈希密钥 HK 计算,另一种是通过投影密钥 HP 和 $\boldsymbol{W}\in\mathcal{L}$ 的证据 r 计算.

(3) 平滑性:对于任意函数 $f:S\to\mathcal{X}/\mathcal{L}$,以下两个分布在统计上不可区分:① $\{(HP,Hash((label,f(HP)\in\mathcal{X}/\mathcal{L},pw),HK))\mid HK\leftarrow\mathcal{K},HP\leftarrow ProjKG(HK,pk)\}$;② $\{(HP,g)\mid HK\leftarrow\mathcal{K},HP\leftarrow ProjKG(HK,pk),g\xleftarrow{r}\mathcal{G}\}$.即对于 $\forall\boldsymbol{W}=(label,f(HP),pw)\in\mathcal{X}/\mathcal{L}$,投影密钥 HP 不能漏泄哈希值 $Hash$ 的任何信息.

上述投影密钥的计算不依赖密文,所以上述

SPHF 是非适应性 SPHF[27]. 下面介绍一个有关 SPHF 的定理及其安全性证明中所涉及的实验.

定理 1[27]. 对于任意 pk、$(label, pw)$ 和 $i, j \in [1, l]$，即使 HK 以及 $\boldsymbol{C}$ 重用，以下分布仍不可区分：(1) $\{(\{HP_i\}, \{\boldsymbol{C}_i\}, \{Hash((label, \boldsymbol{C}_j, pw), HK_i)\}) \mid HK_i \leftarrow \mathcal{K}, HP_i \leftarrow ProjKG(HK_i, pk), \boldsymbol{C}_j \leftarrow (label, Enc(pk, pw \| label))\}$；(2) $\{(\{HP_i\}, \{\boldsymbol{C}_i\}, \{g_{i,j}\}) \mid HK_i \leftarrow \mathcal{K}, HP_i \leftarrow ProjKG(HK_i, pk), g_{i,j} \xleftarrow{r} \mathcal{G}\}$.

令 $l = l(\kappa)$，$\mathcal{M}$ 为敌手，并令随机比特 $b \in \{0, 1\}$，攻击定理 1 的实验(也称为游戏)如下：

(1) 给定 $\{pk, sk\} \leftarrow Gen(1^\kappa)$，令 $(\mathcal{K}, \mathcal{G}, \mathcal{H} = \{Hash(\boldsymbol{W}, HK \in \mathcal{K}): \mathcal{X} \rightarrow \mathcal{G}\}, \mathcal{S}, ProjKG: \mathcal{K} \rightarrow \mathcal{S})$ 表示公钥为 pk 的 SPHF，向敌手 $\mathcal{M}$ 返回公钥 pk.

(2) 取样 $HK_i \xleftarrow{r} \mathcal{K}$ $(i \in [1, l])$，计算 $HP_i \leftarrow ProjKG(HK_i, pk)$，向敌手 $\mathcal{M}$ 返回 $\{HP_i \mid i \in [1, l]\}$.

(3) 敌手 $\mathcal{M}$ 可以向加密预言机发送 $(label, pw)$，加密预言机向 $\mathcal{M}$ 返回：选择 $b \xleftarrow{r} \{0, 1\}$，若 $b = 0$，返回 $(\boldsymbol{C} = Enc(pk, pw), \{Hash((label, \boldsymbol{C}, pw), HK_i)\})$；否则，返回 $(\boldsymbol{C} = Enc(pk, pw), \{g_{i,j} \xleftarrow{r} \mathcal{G}\})$.

(4) 敌手 $\mathcal{M}$ 可以访问解密预言机，$\mathcal{M}$ 发送 $(label, \boldsymbol{C})$，解密预言机返回 $(label, pw)$.

(5) 最后，敌手 $\mathcal{M}$ 输出猜测比特 b'，若 $b' = b$，称敌手 $\mathcal{M}$ 攻击成功，并记该事件为 $\text{Success}_{\mathcal{M}}$.

引理 1[27]. 令 $\Sigma(KeyGen, Enc, Dec)$ 是 IND-CCA2 安全的公钥加密算法，令 $(\mathcal{K}, \mathcal{G}, \mathcal{H} = \{Hash(\boldsymbol{W}, HK \in \mathcal{K}): \mathcal{X} \rightarrow \mathcal{G}\}, \mathcal{S}, ProjKG: \mathcal{K} \rightarrow \mathcal{S})$ 是 SPHF，对于任意 $l = l(\kappa)$ 以及概率多项式时间(Probabilistic Polynomial Time，PPT)的敌手 $\mathcal{M}$，存在可忽略函数 $negl(\kappa)$ 满足

$$Pr(\text{Success}_{\mathcal{M}}) \leq 1/2 + negl(\kappa) \tag{3}$$

3 PAKE 协议安全模型

本节采用的 PAKE 协议安全性分析模型基于 BPR 模型[26]. 下文中关于伙伴关系、正确性、新鲜性和敌手优势等的定义可参见文献[26].

假设协议在公开的非安全信道上执行，协议参与方包括用户、服务器以及敌手/攻击者. 敌手可以执行仿冒、篡改、重放、窃听、中间人等攻击[38]. 并设口令空间为 $\mathcal{D}$，口令空间的大小为 $\|\mathcal{D}\|$.

每个协议参与方可与其他参与方(并行地)执行多次协议. BPR 模型用实例建模协议的执行，并用 Π 表示实例，如 Π_u^i 表示用户 u 的第 i 个实例. 一个实例只能使用一次且拥有一个本地状态变量 $(sid_u^i, pid_u^i, sk_u^i, acc_u^i, term_u^i)$. sid_u^i 表示实例 Π_u^i 的会话标识，sid_u^i 为接收和发送的消息统一编号；pid_u^i 表示实例 Π_u^i 自认为的通信伙伴的标识；sk_u^i 表示实例 Π_u^i 的会话密钥；acc_u^i 和 $term_u^i$ 都是二值变量，若实例 Π_u^i 最终被接受，那么 $acc_u^i = 1$，若实例 Π_u^i 最终被中止，那么 $term_u^i = 1$.

BPR 模型通过以下不同的预言机建模敌手与用户或者服务器之间的各种交互. 这些交互实际上是敌手与各实例之间的交互.

Execute(u, i, s, j)：若实例 Π_u^i 和 Π_s^j 都未使用过，该预言机执行这两个实例间的协议，并向敌手返回执行副本. 该预言机建模了敌手的被动窃听攻击.

Send(u, i, msg)：该预言机建模敌手对协议执行的主动攻击. 敌手向实例 Π_u^i 发送消息 msg 后，该预言机根据协议定义执行协议，同时更新实例 Π_u^i 的状态变量，最后向敌手返回协议的输出消息. 特别地，敌手可以通过 Send(u, i, s) 初始化实例 Π_u^i(未使用过的实例)与服务器 s 之间的协议，此时 Send(u, i, s) 返回协议的首条传输消息.

Reveal(u, i)：该预言机输出会话密钥 sk_u^i. Reveal 建模会话密钥泄漏攻击，比如会话密钥的非法擦除、计算机泄漏攻击和密码分析等.

Test(u, i)：该预言机不建模真实世界中的敌手攻击，只用于定义安全协议. 该预言机选择随机比特 b，若 $b = 1$，则向敌手返回真实会话密钥；否则，返回与之等长的随机串. 只允许敌手对未被访问过 Reveal 的实例执行一次 Test 询问.

下面介绍几个用于定义敌手优势以及安全 PAKE 协议的概念.

伙伴关系. 设用户 u 与服务器 s 是协议参与双方，称实例 Π_u^i 与 Π_s^j 互为伙伴关系如果：(1) $sid_u^i = sid_s^j \neq \text{NULL}$；且(2) $pid_u^i = s$ 且 $pid_s^j = u$.

正确性. 设用户 u 与服务器 s 是协议参与双方，称 PAKE 协议是正确的，如果：(1) 实例 Π_u^i 与 Π_s^j 互为伙伴关系；且(2) $acc_u^i = acc_s^j = 1$；且(3) $sk_u^i = sk_s^j$. 即正确性要求互为伙伴关系的实例都处于接受状态，并且协商了一致的会话密钥.

新鲜性. 设实例 Π_u^i 与 Π_s^j 互为伙伴关系，称 Π_u^i 是新鲜的，如果敌手(1)未访问过 Reveal(u, i)，且(2)未访问过 Reveal(s, j).

设实例 Π_u^i 与 Π_s^j 互为伙伴关系，并设敌手对实例 Π_u^i 进行 Test(u, i) 询问后给出的猜测比特为 b'.

若敌手未访问过 Reveal(u,i)和 Reveal(s,j)，且 $b'=b$，称敌手攻击成功.

敌手优势. 设敌手$\mathcal{A}$是攻击协议 Π 的 PPT 敌手，并设敌手$\mathcal{A}$可以执行多次 Execute、Send、Reveal 询问，但只能对新鲜实例执行一次 Test 询问. 记“敌手攻击成功”事件为 Success，那么，敌手$\mathcal{A}$攻击协议 Π 的优势 $Adv_{\mathcal{A},\Pi}$ 定义为

$$Adv_{\mathcal{A},\Pi}=2Pr(\text{Success})-1=2Pr(b'=b)-1 \quad (4)$$

根据敌手优势的定义，若敌手的获胜概率为 $Pr(\text{Success})=1/2+negl(\kappa)$，则敌手优势为 $Adv_{\mathcal{A},\Pi}=negl(\kappa)$，其中 $negl(\kappa)$为关于安全参数 κ 的可忽略函数. 此时，PAKE 协议具备语义安全性：PPT 敌手不能区分真实的会话密钥及与之等长的随机串，即 PAKE 协议可以保证会话密钥的机密性.

用户实际使用的口令空间较小，敌手总可以通过穷尽口令空间的方式来执行在线仿冒攻击，因此 PAKE 协议无法避免在线口令猜测攻击[5]. 一般情况下，若此类攻击是敌手的最佳攻击方式，就称 PAKE 协议是安全的. 下面正式给出本文中安全口令认证密钥交换协议的定义.

定义 1.　安全口令认证密钥交换协议. 设 κ 是安全参数，$\mathcal{A}$是攻击协议 Π 的 PPT 敌手，且$\mathcal{A}$最多执行 $Q(\kappa)$次在线口令猜测攻击. 另设口令空间为 $\mathcal{D}$，且口令分布服从 CDF-Zipf 定律. 称协议 Π 是安全的口令认证密钥交换协议，如果对于任意的 PPT 敌手$\mathcal{A}$，存在可忽略函数 $negl(\kappa)$满足

$$Adv_{\mathcal{A},\Pi}(\kappa)\leq C'\cdot Q(\kappa)^{s'}+negl(\kappa) \quad (5)$$

其中 $Q(\kappa)\leq\|\mathcal{D}\|$，$C'=0.0415632$ 和 $s'=0.180224$ 为基于人人网口令数据集的 CDF-Zipf 拟合参数.

图 1 以 474 万人人网口令数据为例，展示了不同口令分布假设下敌手优势与真实敌手优势之间的差距. 这种差距越小表示该敌手优势越接近真实敌手优势，也说明该口令分布假设对应的安全模型能够更加准确地评估 PAKE 协议面临的真实风险.

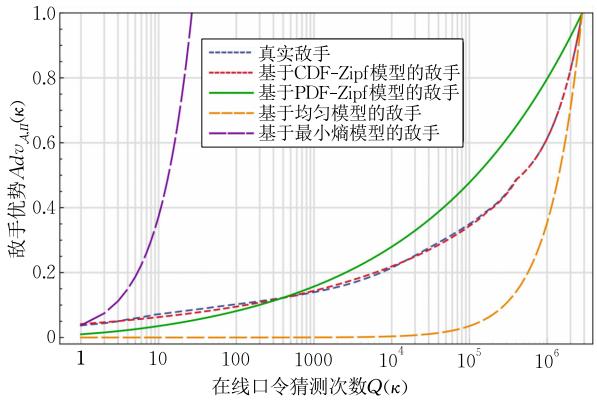

图 1　不同口令分布假设下敌手优势的对比：真实敌手优势、基于 CDF-Zipf 口令分布模型的敌手优势、基于 PDF-Zipf 口令分布模型的敌手优势、基于口令均匀分布模型的敌手优势、基于最小熵口令分布模型的敌手优势

现有的 PAKE 协议安全模型大多假设口令服从均匀分布[5-8,13-14]，此时，敌手优势的上限为 $Q(\kappa)/\|\mathcal{D}\|+negl(\kappa)$. 一般情况下，口令空间的大小($\|\mathcal{D}\|$)的数量级为 10^6，敌手执行在线口令猜测攻击的次数上限($Q(\kappa)$)的数量级为 10^3[2,39]. 那么，当 $Q(\kappa)$的数量级为 10^3时，基于口令均匀分布假设的敌手优势将小于 1%；根据图 1，这大大低估了真实敌手的优势，因此基于口令均匀分布模型的 PAKE 协议安全性分析模型也大大低估了 PAKE 协议所面临的真实风险. 图 1 还显示，与基于其他口令分布模型的敌手优势(如基于 PDF-Zipf 口令分布模型和基于最小熵口令分布模型的敌手优势)相比，基于 CDF-Zipf 口令分布模型的敌手优势与真实敌手优势之间的差距明显更小. 综上，本文借鉴文献[19-20]的做法，所采用的 PAKE 协议安全模型更加现实，因而可以更加准确地评估 PAKE 协议所提供的安全强度.

4　非适应性平滑投影哈希函数

本节主要研究基于格的 IND-CCA2 安全的非适应性平滑投影哈希函数. 为使所提出的非适应性 SPHF 支持一轮 PAKE 协议的构造，本节在设计投影函数时应避免使用密文. 同时，为使所提出的非适应性 SPHF 具备 IND-CCA2 安全性，以及所得到的一轮 PAKE 协议可以避免 NIZK 证明和签名/验签等技术的使用，本节利用 LWE 问题的加法同态属性，设计基于多密文分量的非适应性 SPHF. 本节还确定了所基于的公钥加密算法中相关参数的大小，以消除 LWE 问题的不完全加法同态属性对 SPHF 正确性的影响. 最后，本节对所提出的非适应性 SPHF 进行了正确性与平滑性证明.

本节基于第 2.2 节中 IND-CCA2 安全的 Σ 方案设计非适应性 SPHF. 设 Σ 的公钥为 $pk_\Sigma=(\boldsymbol{A},\boldsymbol{B})$，公共本原矩阵为 $\boldsymbol{G}_b$，并设哈希密钥的长度为 l. 另设所提出的格上非适应性平滑投影哈希函数为($\mathcal{K},\mathcal{G},\mathcal{H}=\{Hash(\boldsymbol{W},HK\in\mathcal{K}):\mathcal{X}\to\mathcal{G}\},\mathcal{S},ProjKG:\mathcal{K}\to\mathcal{S}$)$_{\text{WI}}$，记作 WI-SPHF，具体如下：

$HashKG(q,n,k,l,1^\kappa)$：首先输入算法参数$(q,n,k,l,1^\kappa)$，然后选择哈希密钥$hk_i \xleftarrow{r} \mathbb{Z}^{\bar{m}}(1\leq i\leq l)$，最后输出哈希密钥$HK=(hk_1,hk_2,\cdots,hk_l)$；

$ProjKG(HK=(hk_1,hk_2,\cdots,hk_l),pk_\Sigma=(\boldsymbol{A},\boldsymbol{B}),\boldsymbol{G}_b)$：首先输入哈希密钥$HK=(hk_1,hk_2,\cdots,hk_l)$、$\Sigma$方案的公钥$pk_\Sigma=(\boldsymbol{A},\boldsymbol{B})$和公共本原矩阵$\boldsymbol{G}_b$，然后计算$hp_i=(\boldsymbol{A}+(\boldsymbol{B}+FRD(tag)\boldsymbol{G}_b)\,|\,\boldsymbol{0})\cdot hk_i$，最后输出投影密钥$HP=(hp_1,hp_2,\cdots,hp_l)$；

$Hash(\boldsymbol{W}=(label,(\boldsymbol{c}_1,\boldsymbol{c}_2,c_3,c_4),p),HK=(hk_1,hk_2,\cdots,hk_l))$：首先输入单词$\boldsymbol{W}=(label,(\boldsymbol{c}_1,\boldsymbol{c}_2,c_3,c_4),p)$和哈希密钥$HK=(hk_1,hk_2,\cdots,hk_l)$；然后计算

$$\begin{cases} z_i=(\boldsymbol{c}_1+\boldsymbol{c}_2\,\|\,\boldsymbol{0})^{\mathrm{T}}hk_i(\mathrm{mod}q)\\ t_i=(z_i+c_3+c_4)(\mathrm{mod}q)-q/2\\ h_i=1+RD(2t_i/q)(\mathrm{mod}2)\end{cases}\tag{6}$$

其中$i\in[1,l]$，$RD(x)$表示对x进行四舍五入计算；最后输出哈希值$h=(h_1,h_2,\cdots,h_l)$；

$ProjHash(HP=(hp_1,hp_2,\cdots,hp_l),\boldsymbol{W}=(label,(\boldsymbol{c}_1,\boldsymbol{c}_2,c_3,c_4),p),\tilde{\boldsymbol{s}})$：首先输入投影密钥$HP=(hp_1,hp_2,\cdots,hp_l)$、单词$\boldsymbol{W}=(label,(\boldsymbol{c}_1,\boldsymbol{c}_2,c_3,c_4),p)$及$\boldsymbol{W}\in\mathcal{L}$的证据$\tilde{\boldsymbol{s}}$；然后计算

$$\begin{cases} z_i'=hp_i^{\mathrm{T}}\cdot\tilde{\boldsymbol{s}}\\ t_i'=(z_i'+c_3+c_4)(\mathrm{mod}q)-q/2\\ h_i'=1+RD(2t_i'/q)(\mathrm{mod}2)\end{cases}\tag{7}$$

最后，输出投影哈希值$ph=(ph_1,ph_2,\cdots,ph_l)$.

为消除LWE问题的不完全加法同态属性对WI-SPHF正确性的影响，现确定Σ方案中相关参数的大小. 根据式(6)、式(7)及Σ方案的定义可知，

$$|z_i-z_i'|=|(\boldsymbol{e}_1+\boldsymbol{e}_2)\cdot hk_i|\tag{8}$$

根据SPHF的正确性定义可知，Σ方案中的误差分布应该满足式(9).

$$|(\boldsymbol{e}_1+\boldsymbol{e}_2)\cdot hk_i|\leq\frac{\varepsilon}{2}\cdot\frac{q}{4}\tag{9}$$

又$\boldsymbol{e}_1$和$\boldsymbol{e}_2$取自截断离散高斯分布，根据2.2节截断高斯分布的定义有$\boldsymbol{e}_1\leq\alpha q\sqrt{\bar{m}\kappa}$，$\boldsymbol{e}_2\leq\gamma\sqrt{nk\cdot\kappa}$. 进一步，根据$\Sigma$方案和WI-SPHF的定义有$|hk_i|\leq s\sqrt{\bar{m}}$. 那么，根据式(9)可得

$$(\alpha q\sqrt{\bar{m}\kappa}+\gamma\sqrt{nk\cdot\kappa})s\sqrt{\bar{m}}\leq\frac{\varepsilon\cdot q}{8}\tag{10}$$

根据第2.3节的预备知识，SPHF必须具备正确性与平滑性. 正确性保证了由哈希密钥计算的哈希值与由投影密钥计算的投影哈希值相等，从而确保了PAKE协议的正确性. 平滑性保证了当单词$\boldsymbol{W}=(label,\boldsymbol{C},p)\in\mathcal{X}/\mathcal{L}$时，即使已知投影密钥，哈希值与随机数仍不可区分. 即投影密钥不能泄漏哈希值的任何信息，这保证了SPHF的安全性. 本文通过证明定理2来证明本节所提出的WI-SPHF是平滑投影哈希函数，即满足正确性与平滑性要求.

定理2. WI-SPHF是基于公钥加密方案Σ的平滑投影哈希函数.

证明. 详见附录I.

5 可证明安全的抗量子高效口令认证密钥交换协议

为提高PAKE协议的执行效率并降低通信、存储开销，本节以降低通信轮次和简化协议架构为目标，研究在避免使用NIZK证明和签名/验签等技术的前提下，格上PAKE协议的一轮实现问题. 本节还在标准模型下，基于第3节给出的更加现实的PAKE协议安全模型，对所提出的PAKE协议进行了严格的安全性证明，从而避免了使用随机预言机带来的安全隐患[36]，特别是这可能导致PAKE协议遭受离线口令猜测攻击.

5.1 协议设计

基于第4节提出的非适应性平滑投影哈希函数，本小节提出了一种抗量子的高效PAKE协议. 协议双方在计算投影密钥时不需要等待对方传输的密文，可以同步传输消息，并在一轮通信内完成协议的执行. 在计算通信轮次时，现有的相关研究都忽略了“用户请求”消息[14-15,19,27]，因此本文也未计入此初始消息.

假设协议在用户u与服务器s之间展开，二者共享相同的口令($pw_u=pw_{s,u}$). 协议所需的密码学原语、协议初始化阶段和执行流程如下：

密码学原语. (1) 格上IND-CCA2安全的公钥加密方案Σ；(2) 基于Σ方案的非适应性平滑投影哈希函数，$(\mathcal{K},\mathcal{G},\mathcal{H}=\{Hash(\boldsymbol{W},HK\in\mathcal{K}):\mathcal{X}\to\mathcal{G}\},\mathcal{S},ProjKG:\mathcal{K}\to\mathcal{S})_{\mathrm{WI}}$，记作WI-SPHF.

协议初始化阶段. 协议双方在该阶段建立共享信息，又称为公共参考序列(Common Reference String, CRS). 设$pk_\Sigma=(\boldsymbol{A},\boldsymbol{B})$和$\boldsymbol{G}_b$分别为$\Sigma$方案的公钥和公共本原矩阵(相关定义见第2.2节)，那么$CRS=((\boldsymbol{A},\boldsymbol{B}),\boldsymbol{G}_b)$.

协议执行流程. 所提出的可证明安全的抗量子高效PAKE协议如算法I所示.

算法 I.　可证明安全的抗量子高效 PAKE 协议.

用户端 $u(pw_u)$		服务器端 $s(pw_{s,u})$
1. $x_u, y_u, z_u \xleftarrow{r} \mathbb{F}(2^\kappa)$, $\bar{\boldsymbol{s}}_u \xleftarrow{r} D_{\mathbb{Z}^{\bar{m}},aq}$, $\boldsymbol{e}_{1u} \xleftarrow{r} D_{\mathbb{Z}^{\bar{m}},aq}$, $\boldsymbol{e}_{2u} \xleftarrow{r} D_{\mathbb{Z}^{nk},\gamma}$		1. $x_s, y_s, z_s \xleftarrow{r} \mathbb{F}(2^\kappa)$, $\bar{\boldsymbol{s}}_s \xleftarrow{r} D_{\mathbb{Z}^{\bar{m}},aq}$, $\boldsymbol{e}_{1s} \xleftarrow{r} D_{\mathbb{Z}^{\bar{m}},aq}$, $\boldsymbol{e}_{2s} \xleftarrow{r} D_{\mathbb{Z}^{nk},\gamma}$
2. $HK_u \leftarrow HashKG(q,n,k,l,1^\kappa)$		2. $HK_s \leftarrow HashKG(q,n,k,l,1^\kappa)$
3. $HP_u \leftarrow ProjKG(HK_u, pk_\Sigma, \boldsymbol{G}_b)$		3. $HP_s \leftarrow ProjKG(HK_s, pk_\Sigma, \boldsymbol{G}_b)$
4. $label_u := u \Vert s \Vert HP_u$		4. $label_s := s \Vert u \Vert HP_s$
5. $\boldsymbol{c}_{1u} = \boldsymbol{A}^{\mathrm{T}} \bar{\boldsymbol{s}}_u + \boldsymbol{e}_{1u}$		5. $\boldsymbol{c}_{1s} = \boldsymbol{A}^{\mathrm{T}} \bar{\boldsymbol{s}}_s + \boldsymbol{e}_{1s}$
6. $\boldsymbol{c}_{2u} = (\boldsymbol{B} + FRD(tag_u)\boldsymbol{G}_b)^{\mathrm{T}} \bar{\boldsymbol{s}}_u + \boldsymbol{e}_{2u}$		6. $\boldsymbol{c}_{2s} = (\boldsymbol{B} + FRD(tag_s)\boldsymbol{G}_b)^{\mathrm{T}} \bar{\boldsymbol{s}}_s + \boldsymbol{e}_{2s}$
7. $c_{3u} = x_u + H(pw_u \Vert label_u)$		7. $c_{3s} = x_s + H(pw_s \Vert label_s)$
8. $c_{4u} = \tau_u y_u + z_u$		8. $c_{4s} = \tau_s y_s + z_s$
	$u \Vert \boldsymbol{C}_u = (\boldsymbol{c}_{1u}, \boldsymbol{c}_{2u}, c_{3u}, c_{4u}) \Vert HP_u$ →	
	$s \Vert \boldsymbol{C}_s = (\boldsymbol{c}_{1s}, \boldsymbol{c}_{2s}, c_{3s}, c_{4s}) \Vert HP_s$ ←	
1. $h_u \leftarrow Hash(\boldsymbol{W}_s, HK_u)$		1. $h_s \leftarrow Hash(\boldsymbol{W}_u, HK_s)$
2. $ph_u \leftarrow ProjHash(HP_s, \boldsymbol{W}_u, \bar{\boldsymbol{s}}_u)$		2. $ph_s \leftarrow ProjHash(HP_u, \boldsymbol{W}_s, \bar{\boldsymbol{s}}_s)$
3. $sk_u = h_u \cdot ph_u$		3. $sk_s = h_s \cdot ph_s$
4. 删除除 pw_u 和 sk_u 外的存储信息		4. 删除除 $pw_{s,u}$ 和 sk_s 外的存储信息

协议双方首先同步计算并发送口令的加密值；然后，调用本文提出的非适应性平滑投影哈希函数，WI-SPHF：(1) 以己方的哈希密钥和对方的密文来计算己方的哈希值；(2) 并以对方的投影密钥、己方的密文和己方密文的证据来计算对方的哈希值，即己方的投影哈希值；最后，通过把两个哈希值(己方的哈希值和己方的投影哈希值)相乘得到一致的会话密钥. 协议的具体执行过程如下.

用户 u 调用 WI-SPHF 来计算哈希密钥 $HK_u \leftarrow HashKG(q,n,k,l,1^\kappa)$ 和投影密钥 $HP_u \leftarrow ProjKG(HK_u, pk_\Sigma, \boldsymbol{G}_b)$；并根据 Σ 方案的定义计算密文 $\boldsymbol{C}_u = (\boldsymbol{c}_{1u}, \boldsymbol{c}_{2u}, c_{3u}, c_{4u})$；最后，用户 u 向服务器 s 发送消息 $u \Vert \boldsymbol{C}_u = (\boldsymbol{c}_{1u}, \boldsymbol{c}_{2u}, c_{3u}, c_{4u}) \Vert HP_u$.

服务器 s 调用 WI-SPHF 来计算哈希密钥 $HK_s \leftarrow HashKG(q,n,k,l,1^\kappa)$ 和投影密钥 $HP_s \leftarrow ProjKG(HK_s, pk_\Sigma, \boldsymbol{G}_b)$；并根据 Σ 方案的定义计算密文 $\boldsymbol{C}_s = (\boldsymbol{c}_{1s}, \boldsymbol{c}_{2s}, c_{3s}, c_{4s})$；最后服务器 s 向用户 u 发送消息 $s \Vert \boldsymbol{C}_s = (\boldsymbol{c}_{1s}, \boldsymbol{c}_{2s}, c_{3s}, c_{4s}) \Vert HP_s$. 该计算过程与上述用户的计算过程同步进行.

用户 u 收到服务器 s 发送的消息后，利用服务器的密文 $\boldsymbol{C}_s = (\boldsymbol{c}_{1s}, \boldsymbol{c}_{2s}, c_{3s}, c_{4s})$ 和用户的哈希密钥 HK_u，计算用户的哈希值 $h_u = Hash(\boldsymbol{W}_s, HK_u)$；利用服务器发送的投影密钥 HP_s 和用户的 $\bar{\boldsymbol{s}}_u$ 计算用户的投影哈希值 $ph_u \leftarrow ProjHash(HP_s, \boldsymbol{W}_u, \bar{\boldsymbol{s}}_u)$(即服务器的哈希值)；最后，计算会话密钥 $sk_u = h_u \cdot ph_u$，并删除除 pw_u 和 sk_u 外的所有本地存储信息.

服务器 s 收到用户 u 发送的消息后，根据 u 的密文 $\boldsymbol{C}_u = (\boldsymbol{c}_{1u}, \boldsymbol{c}_{2u}, c_{3u}, c_{4u})$ 和服务器的哈希密钥 HK_s，计算 s 的哈希值 $h_s = Hash(\boldsymbol{W}_u, HK_s)$；根据 u 发送的投影密钥 HP_u 和服务器的 $\bar{\boldsymbol{s}}_s$ 计算服务器的投影哈希值 $ph_s \leftarrow ProjHash(HP_u, \boldsymbol{W}_s, \bar{\boldsymbol{s}}_s)$(即用户的哈希值)；最后，计算会话密钥 $sk_s = h_s \cdot ph_s$，并删除除 $pw_{s,u}$ 和 sk_s 外的所有本地存储信息.

5.2　协议正确性分析与安全性证明

(1) 协议正确性分析

协议正确性是指，若根据算法 I 的流程执行协议，协议双方将得到相同的会话密钥. 为方便描述，下文直接称算法 I 所示的协议为协议 I. 下证协议 I 是正确的，即证 $sk_s = sk_u$.

根据 WI-SPHF 的正确性，式(11)中的二式以不可忽略的概率成立.

$$\begin{cases} h_u = Hash(\boldsymbol{W}_s, HK_u) \\ \quad = ProjHash(HP_u, \boldsymbol{W}_s, \bar{\boldsymbol{s}}_s) = ph_s \quad \text{(a)} \\ h_s = Hash(\boldsymbol{W}_u, HK_s) \\ \quad = ProjHash(HP_s, \boldsymbol{W}_u, \bar{\boldsymbol{s}}_u) = ph_u \quad \text{(b)} \end{cases} \tag{11}$$

那么，根据式(11)可以得到式(12).

$$\begin{aligned} sk_u &= h_u \cdot ph_u \\ &= Hash(\boldsymbol{W}_s, HK_u) \cdot ProjHash(HP_s, \boldsymbol{W}_u, \bar{\boldsymbol{s}}_u) \\ &= ProjHash(HP_u, \boldsymbol{W}_s, \bar{\boldsymbol{s}}_s) \cdot Hash(\boldsymbol{W}_u, HK_s) \\ &= ph_s \cdot h_s = h_s \cdot ph_s = sk_s \end{aligned} \tag{12}$$

根据式(12)及 PAKE 协议的正确性要求可知，协议 I 是正确性的.

(2) 协议安全性证明

本节通过证明定理 3 来证明所提出的协议是安全的口令认证密钥交换协议(即满足定义 1).

定理 3.　若 Σ 是 IND-CCA2 安全的公钥加密方案，且第 4.1 节提出的函数 WI-SPHF，$(\mathcal{K}, \mathcal{G}, \mathcal{H} = \{Hash(\boldsymbol{W}, HK \in \mathcal{K}) : \mathcal{X} \to \mathcal{G}\}, \mathcal{S}, ProjKG : \mathcal{K} \to \mathcal{S})_{\mathrm{WI}}$，是非适应性平滑投影哈希函数，那么协议 I 是安全的口令认证密钥交换协议.

证明.　详见附录 II.

6 协议仿真与性能分析

本节对本文协议及相关协议进行仿真，并从执行效率、通信开销、存储开销、安全性等方面评估本文协议.

6.1 协议仿真与协议效率评估

为实现公平对比，本文统一采用 python 语言，在 Intel(R)Core(TM)i5-4590 平台上，对本文协议及五个相关协议进行仿真. 该平台的内存大小为 8 GB，频率为 3.3 GHz，操作系统为 Win7. 为方便进行执行效率等的对比，本节设 $\kappa=128$ bit，$m=6400$ bit，$\overline{m}=3328$ bit，$n=256$ bit，$n_1=128$ bit，$n_2=127$ bit，$q=4096$ bit. 上述参数规模符合 Σ 方案的参数设置要求(见第 2.2 节). 各密码学原语的仿真时间如表 2 所示. 表 3 则给出了不同协议的仿真时间对比.

表 2 密码学原语仿真时间

密码原语	名称	仿真时间/s	名称	仿真时间/s
加密算法	MP	0.320750	KV	0.889398
	GPV	0.135338	SPKE	14.313541
	Reg	0.043393	Σ	0.315670
SPHF	MP	0.001067	KV	0.449303
	GPV	0.009486	SPKE	0.001102
	Reg	0.005781	Σ	0.315677
纠错算法	ECC	0.001612	ECC^{-1}	0.001682

表 3 协议仿真时间对比

方案	用户端/s	服务器端/s
KV1.PAKE[21]	1.046087	1.046087
ZY.PAKE[14]	14.314656	14.314656
BF.PAKE[13]	0.321819	0.321817
LW1.PAKE[19]	0.321817	0.321817
LW2.PAKE[20]	0.326531	0.044460
本文协议	0.317650	0.317650

注：KV1.PAKE[21]、BF.PAKE[13]、LW1.PAKE[19] 和 LW2.PAKE[20] 的实际计算开销还应包含由签名/验签算法引入的额外部分.

表 3 显示本文协议在用户端具有最高的执行效率，主要原因是所提出的非适应性 SPHF 和所基于的公钥加密算法都具有较高的执行效率. 在服务器端，本文协议在表 3 中的执行效率低于 LW2.PAKE 协议[20]. 这是因为 LW2.PAKE[20] 是两轮协议，在服务器端可以采用 IND-CPA 安全的公钥加密算法，其计算开销要小于一轮协议所需的 IND-CCA2 安全的公钥加密算法. 但 LW2.PAKE 协议[20] 在用户端的执行效率同时低于本文协议在用户端和服务器端的执行效率，且比本文协议多一轮的通信延时，因此本文协议的实际整体执行效率最高.

表 3 还显示，ZY.PAKE 协议[14] 在用户端和服务器端都具有最低的执行效率，这是因为该协议所采用的 SPKE 方案本就具有较大的计算开销(见表 2)，而 NIZK 证明的使用进一步增大了整体开销. 此外，由于在实际应用时，除表 3 中的数据外，KV1.PAKE[21]、BF.PAKE[13]、LW1.PAKE[19] 和 LW2.PAKE[20] 协议的计算开销还包含由签名/验签等算法引入的额外部分，本文协议在执行效率上的优势将大于表 3 中数据.

图 2 进一步给出了在不同会话密钥长度下，不同协议在用户端与服务器端的执行时间对比. 由图 2 可知，即使所需会话密钥的长度增大，本文协议在用户端的效率仍然最高. 在服务器端，本文协议的执行效率虽然在图 2 中低于 LW2.PAKE 协议[20]，但在实际应用时仍最高，原因同前所述. 且随着会话密钥长度的增大，本文协议在执行效率上的优势将更加明显. 当会话密钥长度为 128 bit 时，本文协议的执行效率约是 LW2.PAKE 协议[20] 的 4.25 倍，这得益于所提出的高效非适应性 SPHF. 此外，本文协议的执行效率曲线具有最小的斜率，即若会话密钥位宽增大，本文协议执行时间的增速最缓.

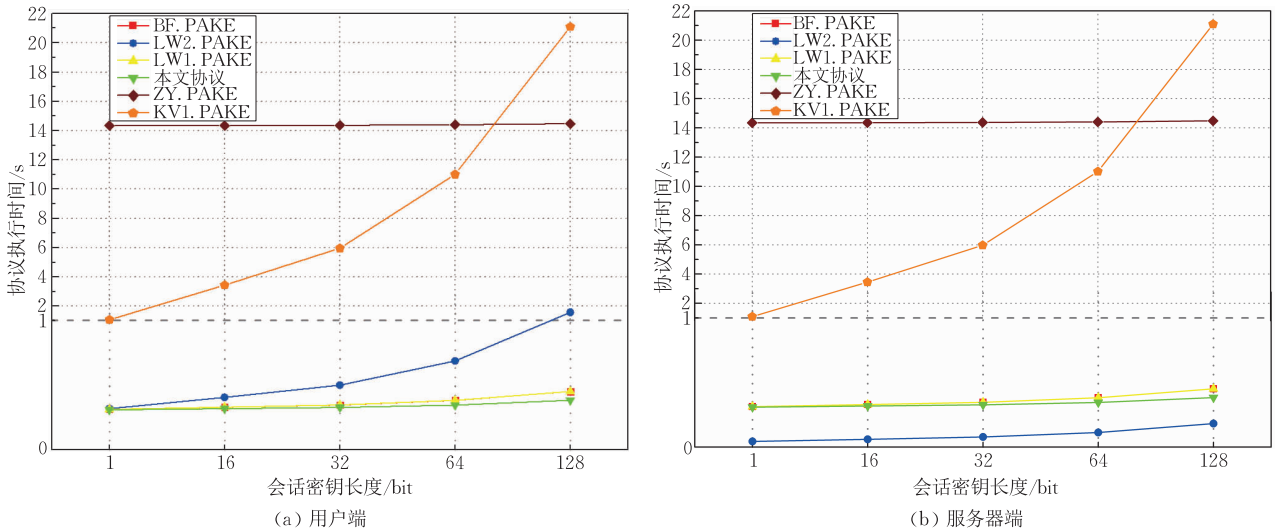

图 2 不同会话密钥长度下协议的执行效率对比

综上，有以下结论：(1) 本文协议具有最优的执行效率，且随着会话密钥长度的增加，协议执行时间的增速最低且增幅最小，即本文协议还具有较好的密钥长度可扩展性；(2) 虽然平滑投影哈希函数是构造口令认证密钥交换协议的关键组件，但口令认证密钥交换协议的计算开销还包含其所基于的公钥加密算法的开销，因此为提高执行效率，在设计时要全面考虑上述两个因素.

6.2　协议通信、存储开销评估

本小节在评估通信开销时，主要评估通信轮次、通信复杂度和通信数据量. 通信轮数和次数分别指通信双方之间的双向和单向通信数量. 如果是异步消息传输，二者相等；如果是同步消息传输，通信次数是通信轮数的两倍. 表 4 给出了不同协议之间的通信开销对比.

表 4　通信开销对比

方案	通信轮(次)	通信复杂度	通信开销/bit
KV1.PAKE[21]	3(3)	$O((kn_1+m-n_2)\log q)$	59 769 984
ZY.PAKE[14]	2(2)	$O((m+kn)\log q)$	1 001 600
BF.PAKE[13]	1(2)	$O((m+kn)\log q)$	940 032
LW1.PAKE[19]	1(2)	$O((m+kn)\log q)$	940 032
LW2.PAKE[20]	2(2)	$O((m+kn)\log q)$	940 032
本文协议	1(2)	$O((\bar{m}+kn)\log q)$	938 496

注：KV1.PAKE[21]、BF.PAKE[13]、LW1.PAKE[19] 和 LW2.PAKE[20] 协议的实际通信开销还包含由验签算法的公钥和签名引入的额外部分.

根据表 4，本文协议只需要一轮通信，具有最优的通信轮次和通信开销. 在实际通信时，与 KV1.PAKE[21]、BF.PAKE[13]、LW1.PAKE[19] 和 LW2.PAKE[20] 协议相比，本文协议在通信开销上的优势将更加明显. 因为除表中的数据外，上述四个协议的实际通信开销还包含由验签公钥和签名等引入的额外部分. 即使如此，本文协议在表 4 中的通信开销依然最小，这得益于本文协议较小的通信复杂度，特别是关键参数 $\bar{m}$ 要小于 m. 表 4 还说明，减小通信轮次一般能大大减小通信开销，这进一步验证了本文研究一轮 PAKE 协议的意义.

表 5 给出了不同 PAKE 协议之间的存储开销对比情况，包括存储复杂度与存储空间占用的对比. 本文协议是对称协议，在用户端和服务器端具有相同的存储复杂度和存储开销，且二者均大于除 KV1.PAKE[21] 外的其他协议，这主要是本文协议所基于的公钥加密算法的公钥较大所致. 但在实际应用时，本文协议在存储开销上的劣势会减小，因为除表 5 中的数据外，KV1.PAKE[21]、BF.PAKE[13]、LW1.PAKE[19] 和 LW2.PAKE[20] 协议的存储开销还包含由签名/验签算法的公钥和签名等引入的额外部分.

6.3　协议安全性及其他评估

本小节对比评估了不同 PAKE 协议的安全性假设、安全模型，以及能否抵御量子攻击、是否需要使用 NIZK 证明和签名/验签算法，如表 6 所示.

表 5　存储开销对比

方案	存储复杂度		存储开销	
	用户端	服务器端	用户端/bit	服务器端/bit
KV1.PAKE[21]	$O((mn(n+k))\log q)$	$O((mn(n+k)\log q)$	17 734 832 768	17 734 832 768
ZY.PAKE[14]	$O((mn+k(n_1+m)+n_2)\log q)$	$O((mn+k(n_1+m)+n_2)\log q)$	50 006 656	50 006 656
BF.PAKE[13]	$O((mn+k(n+m)\log q)$	$O((mn+k(n+m)\log q)$	30 514 560	30 514 560
LW1.PAKE[19]	$O((mn+k(n+m)\log q)$	$O((mn+k(n+m)\log q)$	30 514 560	30 514 560
LW2.PAKE[20]	$O((mn+k(n+m))\log q)$	$O((mn+k(n+m))\log q)$	30 440 844	30 517 644
本文协议	$O((n(\bar{m}+m+nk)+k\bar{m})\log q)$	$O((n(\bar{m}+m+nk)+k\bar{m})\log q)$	137 789 312	137 789 312

注：KV1.PAKE[21]、BF.PAKE[13]、LW1.PAKE[19] 和 LW2.PAKE[20] 的实际存储开销还应包含由签名/验签算法的公钥和签名等引入的额外部分.

表 6　协议安全性及其他对比

方案	是否抗量子	签名/验签	NIZK 证明	安全模型	安全性假设	
					用户端	服务器
KV1.PAKE[21]	是	是	否	标准模型	IND-CCA2	IND-CCA2
KV2.PAKE[27]	否	是	是	标准模型	IND-CCA2	IND-CCA2
ZY.PAKE[14]	是	否	是	随机预言机	IND-CCA2	IND-CCA2
BF.PAKE[13]	是	是	是	随机预言机	IND-CCA2	IND-CCA2
LW1.PAKE[19]	是	是	否	标准模型	IND-CCA2	IND-CCA2
LW2.PAKE[20]	是	是	否	标准模型	IND-CCA2	IND-CPA
本文协议	是	否	否	标准模型	IND-CCA2	IND-CCA2

根据表 6，只有本文提出的一轮 PAKE 协议同时避免了签名/验签算法和 NIZK 证明的使用. 与 KV2.PAKE 协议[27]相比，本文协议可以抵御量子攻击. 与格上首个一轮 PAKE 协议（BF.PAKE 协议[13]）相比，本文协议与 LW1.PAKE 协议[19]是基于标准模型的，避免了随机预言机潜在的安全威胁，特别是使用随机预言机还可能导致 PAKE 协议遭受离线口令猜测攻击；且 LW1.PAKE 协议[19]与本文协议不需要使用 NIZK 证明，这大大提高了执行效率. 而相比于 LW1.PAKE 协议[19]，本文协议不需要额外的签名/验签等算法就能保证 IND-CCA2 安全性，进一步提高了 PAKE 协议的执行效率.

表 6 还说明，更少的通信轮次意味着 PAKE 协议所采用的公钥加密算法需要具备更高的安全性，即 PAKE 协议需要基于安全性更强的安全模型. 比如，一轮 PAKE 协议在用户端和服务器端都需要使用 IND-CCA2 安全的公钥加密算法. 而两轮 PAKE 协议只需要在客户端使用 IND-CCA2 安全的公钥加密算法，在服务器端其对公钥加密算法的安全性需求可以降低到 IND-CPA（如 LW2.PAKE[26]）.

7 结束语

本文利用 LWE 问题的加法同态属性，提出了一种格上 IND-CCA2 安全的非适应性 SPHF. 该 SPHF 支持一轮 PAKE 协议的构建，并解决了直接基于 IND-CCA2 安全模型构建格上非适应性 SPHF 的问题. 鉴于 LWE 问题只具备不完全加法同态属性，本文还确定了所基于的公钥加密算法中相关参数的大小，以保证 SPHF 的正确性. 尽所知，这是格上第一个 IND-CCA2 安全的非适应性 SPHF. 在此基础上，本文在标准模型下构建了一种格上可证明安全的高效 PAKE 协议，避免了使用随机预言机潜在的安全威胁. 该协议可以抵御量子攻击；只需要一轮通信，具有最优的通信轮次；在实际应用时，不需要使用 NIZK 证明和签名/验签等技术来保证安全性，从而提高了执行效率.

此外，为准确评估 PAKE 协议面临的真实风险，本文采用了一种更加现实的 PAKE 协议安全模型，并据此对所提出的协议进行了严格的安全性证明. 实验结果表明，对比其他相关协议，本文协议以一定的存储开销牺牲，实现了最优的执行效率和最低的通信开销. 此外，随着会话密钥长度的增加，协议执行时间的增速最低且增幅最小，即本文协议还具有较好的密钥长度可扩展性. 若将本文协议在理想格上实例化，将进一步提高执行效率，这也是下一步的研究内容.

参 考 文 献

[1] Shin J S, Jo M, Hwang J Y, et al. A verifier-based password-authenticated key exchange using tamper-proof hardware. The Computer Journal, 2021, 64(8): 1293-1302

[2] Wang Ding. Research on Key Issues in Password Security [Ph.D. dissertation]. Peking University, Beijing, 2017 (in Chinese)
(汪定. 口令安全关键问题研究[博士学位论文]. 北京大学，北京，2017)

[3] Nahar M N, Alsadoon A, Prasad P, et al. An enhanced one-time password with biometric authentication for mixed reality surgical tele-presence. Multimedia Tools and Applications, 2021, 80(7): 10075-10100

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

[5] Katz J, Ostrovsky R, Yung M. Efficient and secure authenticated key exchange using weak passwords. Journal of the ACM, 2009, 57(1): 1-39

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

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

[8] Regev O. Lattice-based cryptography//Proceedings of the 26th Annual International Cryptology Conference. Santa Barbara, California, USA, 2006: 131-141

[9] Peikert C. A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 2016, 10(4): 283-424

[10] Yousuf H, Lahzi M, Salloum S A, et al. Systematic review on fully homomorphic encryption scheme and its application. Recent Advances in Intelligent Systems and Smart Applications, 2021, 295: 537-551

[11] Brakerski Z, Döttling N. Hardness of LWE on general entropic distributions//Proceedings of the 2020 EUROCRYPT. Zagreb, Croatia, 2020: 551-575

[12] Li Z, Wang D, Morais E. Quantum-safe round-optimal password authentication for mobile devices. IEEE Transactions on Dependable and Secure Computing, 2022, 19(3): 1885-1899

[13] Benhamouda F, Blazy O, Ducas L, et al. Hash proof systems over lattices revisited//Proceedings of the 2018 Public Key Cryptography. Rio de Janeiro, Brazil, 2018: 644-674

[14] Zhang J, Yu Y. Two-round PAKE from approximate SPH and instantiations from lattices//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China, 2017: 37-67

[15] Yin A, Guo Y, Song Y, et al. Two-round password-based authenticated key exchange from lattices. Wireless Communications and Mobile Computing, 2020, 2020: 8893628

[16] Zhang J, Yu Y, Fan S Q, et al. Improved lattice-based CCA2-secure PKE in the standard model. Science China Information Sciences, 2020, 63(8): 182101

[17] Sahai A. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security//Proceedings of the 40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039). New York, USA, 1999: 543-553

[18] Naor M, Yung M. Public-key cryptosystems provably secure against chosen ciphertext attacks//Proceedings of the 22nd Annual ACM Symposium on Theory of Computing. Baltimore, USA, 1990: 427-437

[19] Li Z, Wang D. Achieving one-round password-based authenticated key exchange over lattices. IEEE Transactions on Services Computing, 2022, 15(1): 308-321

[20] Li Z, Wang D. Two-round PAKE protocol over lattices without NIZK//Proceedings of the International Conference on Information Security and Cryptology. Fuzhou, China, 2018: 138-159

[21] Katz J, Vaikuntanathan V. Smooth projective hashing and password-based authenticated key exchange from lattices//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Tokyo, Japan, 2009: 636-652

[22] Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cambridge, UK, 2012: 700-718

[23] Peikert C, Vaikuntanathan V, Watres B. A framework for efficient and composable oblivious transfer//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2008: 554-571

[24] Ding Y, Fan L. Efficient password-based authenticated key exchange from lattices//Proceedings of the 2011 Seventh International Conference on Computational Intelligence and Security. Sanya, China, 2011: 934-938

[25] Blazy O, Chevalier C, Ducas L, et al. Exact smooth projective hash function based on LWE. IACR Cryptology ePrint Archive, 2013/821. https://eprint.iacr.org/2013/821, 2013, 12, 06

[26] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Bruges, Belgium, 2000: 139-155

[27] Katz J, Vaikuntanathan V. Round-optimal password-based authenticated key exchange//Proceedings of the 2011 Theory of Cryptography. Providence, USA, 2011: 293-310

[28] Yoneyama K. Password-based authenticated key exchange without centralized trusted setup//Proceedings of the International Conference on Applied Cryptography and Network Security. Lausanne, Switzerland, 2014: 19-36

[29] Li Z, Xie T, Zhang J, et al. Post quantum authenticated key exchange protocol based on ring learning with errors problem. Journal of Computer Research and Development, 2019, 56(12): 2694-2701

[30] Karbasi A H, Shahpasand S. A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks. Peer-to-Peer Networking and Applications, 2020, 13(5): 1423-1441

[31] Agarkar A A, Agrawal H. Lightweight R-LWE-based privacy preservation scheme for smart grid network. International Journal of Information and Computer Security, 2019, 11(3): 233-254

[32] Wang D, Cheng H, Wang P, et al. Zipf's law in passwords. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2776-2791

[33] Micciancio D, Goldwasser S. Complexity of Lattice Problems: A Cryptographic Perspective. Boston: Kluwer Academic Publishers, 2002

[34] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions//Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. Victoria, Canada, 2008: 197-206

[35] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 2009, 56(6): 1-40

[36] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. Journal of the ACM, 2004, 51(4): 557-594

[37] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption//Proceedings of the 2022 EUROCRYPT. Amsterdam, Netherland, 2002: 45-64

[38] Guo Y, Zhang Z, Guo Y. Anonymous authenticated key agreement and group proof protocol for wearable computing. IEEE Transactions on Mobile Computing, 2020, DOI: 10.1109/TMC.2020.3048703

[39] Bonneau J. The science of guessing: Analyzing an anonymized corpus of 70 million passwords//Proceedings of the 2012 IEEE Symposium on Security and Privacy. San Francisco, USA, 2012: 538-552

附录 I.

证明. (1)正确性证明

下证对于任意合法单词,即对于 $\forall \boldsymbol{W}=(label,\boldsymbol{C},p)\in\mathcal{L}$,式(I.1)成立.

$$Pr[h=ph]\gg 1-negl(\kappa) \tag{I.1}$$

要保证式(I.1)成立,只要保证 $h=ph$ 统计上成立即可.上述条件等价于对于 $i\in[1,l]$,$h_i=ph_i$ 统计上成立.根据式(6)和式(7),要证明式(I.1)成立,只需证明式(I.2)成立.

$$Pr[z_i=z_i']\gg 1-negl(\kappa) \tag{I.2}$$

下面根据所提出的 WI-SPHF 证明上式成立.

$$\begin{aligned}
z_i&=(\boldsymbol{c}_1+\boldsymbol{c}_2\parallel\boldsymbol{0})^{\mathrm{T}}\cdot hk_i(\mathrm{mod}\,q)\\
&=((\boldsymbol{A}^{\mathrm{T}}\tilde{\boldsymbol{s}}+\boldsymbol{e}_1)+((\boldsymbol{B}+FRD(tag)\boldsymbol{G}_b)^{\mathrm{T}}\tilde{\boldsymbol{s}}+\boldsymbol{e}_2)\parallel\boldsymbol{0})^{\mathrm{T}}\cdot\\
&\quad hk_i(\mathrm{mod}\,q)\\
&=((\boldsymbol{A}+(\boldsymbol{B}+FRD(tag)\boldsymbol{G}_b)\mid\boldsymbol{0})^{\mathrm{T}}\tilde{\boldsymbol{s}})^{\mathrm{T}}hk_i+\\
&\quad(\boldsymbol{e}_1+\boldsymbol{e}_2\parallel\boldsymbol{0})^{\mathrm{T}}\cdot hk_i(\mathrm{mod}\,q)\\
&\approx\tilde{\boldsymbol{s}}^{\mathrm{T}}((\boldsymbol{A}+(\boldsymbol{B}+FRD(tag)\boldsymbol{G}_b)\mid\boldsymbol{0})^{\mathrm{T}}\cdot hk_i)\\
&=\tilde{\boldsymbol{s}}^{\mathrm{T}}\cdot hp_i(\mathrm{mod}\,q)=hp_i^{\mathrm{T}}\cdot\tilde{\boldsymbol{s}}(\mathrm{mod}\,q)=z_i'
\end{aligned} \tag{I.3}$$

综上,第 4 节提出的 WI-SPHF 具备正确性.

(2)平滑性证明

平滑投影哈希函数的平滑性要求投影密钥不能泄漏哈希值的任何信息,即对于 $\forall \boldsymbol{W}=(label,\boldsymbol{C},p)\in\mathcal{X}/\mathcal{L}$,式(I.4)中的两个分布在统计上不可区分.

$$\begin{cases}
\{(HP,h)\mid HK\leftarrow HashKG,HP\leftarrow ProjKG,\\
h\leftarrow Hash(\boldsymbol{W},HK)\}\ \text{(a)}\\
\{(HP,h)\mid HK\leftarrow HashKG,HP\leftarrow ProjKG,\\
h\xleftarrow{r}\{0,1\}^l\}\ \text{(b)}
\end{cases} \tag{I.4}$$

根据式(I.3)可知,$z_i=((\boldsymbol{A}+(\boldsymbol{B}+FRD(tag)\boldsymbol{G}_b)\mid\boldsymbol{0})^{\mathrm{T}}\tilde{\boldsymbol{s}})^{\mathrm{T}}\cdot hk_i+(\boldsymbol{e}_1+\boldsymbol{e}_2\parallel\boldsymbol{0})^{\mathrm{T}}\cdot hk_i(\mathrm{mod}\,q)$.又投影密钥 $hp_i=(\boldsymbol{A}+(\boldsymbol{B}+FRD(tag)\boldsymbol{G}_b)\mid\boldsymbol{0})\cdot hk_i$,那么,根据 $\tilde{\boldsymbol{s}}$ 的随机性可知 hp_i 不能泄漏 z_i 的任何信息.因此,在已知投影密钥 HP 的情况下,哈希值 $h=(h_1,h_2,\cdots,h_l)$ 是 $\{0,1\}^l$ 上的随机分布,即式(I.4)中的两个分布在统计上不可区分.所以,所提出的 WI-SPHF 具备平滑性.

综上,第 4 节所提出的 WI-SPHF 是基于 Σ 方案的非适应性平滑投影哈希函数,即定理 2 成立. 证毕.

附录 II.

证明. 假设敌手 $\mathcal{A}$ 是攻击协议 I 的 PPT 敌手,并将协议的执行看作模拟器与敌手 $\mathcal{A}$ 之间的交互实验.模拟器根据协议的定义选择公共参数,并为用户选择口令,为敌手 $\mathcal{A}$ 模拟协议的执行.以下证明通过逐渐改变原始协议的定义,得到了一系列的改动协议.记敌手 $\mathcal{A}$ 攻击这些改动协议的实验分别为 Exp0,Exp1,…,其中 Exp0 表示 $\mathcal{A}$ 攻击真实协议的实验.本节首先证明了 $\mathcal{A}$ 在两个相邻实验中的优势差是可忽略的,然后界定了 $\mathcal{A}$ 在最后一个实验中的优势上限,从而得到了 $\mathcal{A}$ 攻击真实协议的优势上限.最后,本文通过证明 $\mathcal{A}$ 攻击真实协议的优势满足定义 1 来证明定理 3 成立.

实验 Exp1. 该实验对 Exp0 中的 Execute 预言机进行以下修改:(1)将 $\boldsymbol{C}_u$ 与 $\boldsymbol{C}_s$ 分别替换为非法口令 pw' 的加密值 $\boldsymbol{C}_u'$ 与 $\boldsymbol{C}_s'$(pw' 服从 CDF-Zipf 分布);(2)将客户端和服务器端会话密钥 sk_u^i 和 sk_s^j 的计算方式都替换为 $sk_u^i=sk_s^j=Hash(\boldsymbol{W}_s,HK_u)\cdot Hash(\boldsymbol{W}_u,HK_s)$.

引理 2. 如果 Σ 方案是 IND-CCA2 安全的公钥加密方案,那么式(II.1)成立.

$$|Adv_{\mathcal{A},\mathrm{I},1}(\kappa)-Adv_{\mathcal{A},\mathrm{I},0}(\kappa)|\leq negl(\kappa) \tag{II.1}$$

证明. 利用标准的混合证明法来证明引理 2.设敌手 $\mathcal{B}$ 是攻击公钥加密方案 Σ 的 PPT 敌手,且攻击优势为 $Adv_{\mathcal{B},\Sigma}(\kappa)$.$\mathcal{B}$ 利用 $\mathcal{A}$ 攻击 Σ 方案,为 $\mathcal{A}$ 模拟整个协议攻击实验.

敌手 $\mathcal{B}$ 在回复敌手 $\mathcal{A}$ 的 Execute 询问时,$\mathcal{B}$ 向自己的挑战预言机发送 (pw,pw').收到挑战密文 $\boldsymbol{C}'$ 后,$\mathcal{B}$ 向 $\mathcal{A}$ 返回消息 $(u\|\boldsymbol{C}'\|HP_u)$.在实验的最后,若敌手 $\mathcal{A}$ 攻击协议成功,则 $\mathcal{B}$ 输出 1;否则,$\mathcal{B}$ 输出 0.记"$\boldsymbol{C}'$ 由真实口令生成且 $\mathcal{B}$ 输出 1"为事件 $\mathrm{EV}_{\mathcal{B},\Sigma}(pw)$,记"$\boldsymbol{C}'$ 由非法口令生成且 $\mathcal{B}$ 输出 1"为事件 $\mathrm{EV}_{\mathcal{B},\Sigma}(pw')$.那么,$\mathrm{EV}_{\mathcal{B},\Sigma}(pw)$ 发生的概率与 $\mathcal{A}$ 在 Exp0 中攻击成功的概率相等,即 $Pr(\mathrm{EV}_{\mathcal{B},\Sigma}(pw)=1)=Pr(\mathrm{Success}_{\mathrm{Exp0}})$.同理可得,$Pr(\mathrm{EV}_{\mathcal{B},\Sigma}(pw')=1)=Pr(\mathrm{Success}_{\mathrm{Exp1}})$.综上,式(II.2)成立.

$$\begin{aligned}
&|Adv_{\mathcal{A},\mathrm{I},1}(\kappa)-Adv_{\mathcal{A},\mathrm{I},0}(\kappa)|\\
&=|(2Pr(\mathrm{Success}_{\mathrm{Exp1}})-1)-(2Pr(\mathrm{Success}_{\mathrm{Exp0}})-1)|\\
&=|2Pr(\mathrm{EV}_{\mathcal{B},\Sigma}(pw)=1)-2Pr(\mathrm{EV}_{\mathcal{B},\Sigma}(pw')=1)|\\
&=2Adv_{\mathcal{B},\Sigma}(\kappa)
\end{aligned} \tag{II.2}$$

根据 Σ 方案的 IND-CCA2 安全性知,$Adv_{\mathcal{B},\Sigma}(\kappa)\leq negl(\kappa)$.所以,将 $\boldsymbol{C}_u$ 与 $\boldsymbol{C}_s$ 分别替换为 pw' 的加密值 $\boldsymbol{C}_u'$ 与 $\boldsymbol{C}_s'$ 后,$|Adv_{\mathcal{A},\mathrm{II},1}(\kappa)-Adv_{\mathcal{A},\mathrm{I},0}(\kappa)|\leq negl(\kappa)$.而将会话密钥的计算方式替换为 $sk_u^i=sk_s^j=Hash(\boldsymbol{W}_s,HK_u)\cdot Hash(\boldsymbol{W}_u,HK_s)$ 只是概念上的变化,不会带来敌手优势的改变.根据以上证明,式(II.1)成立.

实验 Exp2. 该实验对 Exp1 中的 Execute 进行以下修改:将用户 u 和服务器 s 的会话密钥 sk_u^i 和 sk_s^j 都替换为与真实会话密钥等长的同一随机数,即令 $sk_u^i=sk_s^j\xleftarrow{r}\{0,1\}^l$.

引理 3. 若第 4 节提出的 WI-SPHF,$(\mathcal{K},\mathcal{G},\mathcal{H}=\{Hash(\boldsymbol{W},HK\in\mathcal{K}):\mathcal{X}\rightarrow\mathcal{G}\},\mathcal{S},ProjKG:\mathcal{K}\rightarrow\mathcal{S})_{\mathrm{WI}}$,是非适应性平滑投影哈希函数,那么

$$|Adv_{\mathcal{A},\mathrm{I},2}(\kappa)-Adv_{\mathcal{A},\mathrm{I},1}(\kappa)|\leq negl(\kappa) \tag{II.3}$$

证明. 实验 Exp1 已经将 pw 替换为 pw'(pw' 服从 CDF-Zipf 分布),即 $\boldsymbol{W}_s=(label_s,\boldsymbol{C}_s',pw_{s,u})\in\mathcal{X}/\mathcal{L}$.根据平滑投影哈希函数的平滑性,$Hash(\boldsymbol{W}_s,HK_u)$ 与随机数不可区分,同理 $Hash(\boldsymbol{W}_u,HK_s)$ 与随机数不可区分.因此,式(II.3)成立.

下面对 Send 进行修改.为便于说明,本文将 Send 分为两种.第一种是 Send0(u,i,s),其初始化 u 与 s 之间的一次

协议执行，即实例 Π_u^i 的执行. 该预言机令 $pid_u^i=s$，并向敌手返回协议中 u 向 s 发送的消息. 第二种是 Send1(u,i,msg)，其表示敌手向 u 发送消息 msg. Send1 不向敌手返回任何消息，但根据协议的定义计算会话密钥. Send1(u,i,msg)中的 msg 可能由之前的 Send0$(u,*,s)$产生，也可能由 $\mathcal{A}$ 产生. 此外，本文假设无效的 msg 会被丢弃，所以下述证明不再讨论 msg 无效时的情况.

实验 Exp3. 该实验对 Exp2 中的 Send1 进行以下修改：(1)若 msg 由敌手产生，则用 Σ 方案的私钥对 msg 解密以得到 $pw_{\mathcal{A}}$：(a)若 $pw_{\mathcal{A}}=pw_u$，则直接宣布敌手 $\mathcal{A}$ 获胜，并终止实验；(b)若 $pw_{\mathcal{A}}\neq pw_u$，则随机选择会话密钥，即令 $sk_u^i\xleftarrow{r}\{0,1\}^l$. (2)若 msg 由之前的 Send0 产生，则令会话密钥 $sk_u^i=sk_s^j=Hash(\boldsymbol{W}_s,HK_u)\cdot Hash(\boldsymbol{W}_u,HK_s)$.

引理 4. 若第 4 节提出的 WI-SPHF，$(\mathcal{K},\mathcal{G},\mathcal{H}=\{Hash(\boldsymbol{W},HK\in\mathcal{K}):\mathcal{X}\to\mathcal{G}\},\mathcal{S},ProjKG:\mathcal{K}\to\mathcal{S})_{\text{WI}}$，是非适应性平滑投影哈希函数，那么

$$|Adv_{\mathcal{A},\text{I},3}(\kappa)-Adv_{\mathcal{A},\text{I},2}(\kappa)|\leqslant negl(\kappa)\qquad(\text{II}.4)$$

证明. 上述情况(a)只可能增加敌手优势. 对于上述情况(b)，因为 $pw_{\mathcal{A}}\neq pw_u$，所以 $\boldsymbol{W}_s=(label_s,\boldsymbol{C}_s,pw_{\mathcal{A}})\in\mathcal{X}/\mathcal{L}$. 根据平滑投影哈希函数的平滑性，$Hash(\boldsymbol{W}_s,HK_u)$与随机数不可区分，那么客户端和服务器端的会话密钥 sk_u^i 和 sk_s^j($sk_u^i=sk_s^j=Hash(\boldsymbol{W}_s,HK_u)\cdot Hash(\boldsymbol{W}_u,HK_s)$)也都与随机数不可区分. 因此，上述情况(b)带来的敌手优势的变化可以忽略. 而上述情况(2)只是改变了会话密钥的定义方式，这不会影响会话密钥的取值. 因此，上述情况(2)不会影响敌手优势. 根据以上证明可知式(II.4)成立.

实验 Exp4. 该实验对 Exp3 中的 Send1 进行以下修改. 若 msg 由之前的 Send0 产生：(1)若存在实例 Π_s^j 与 Π_u^i 互为伙伴关系，令 $sk_u^i=sk_s^j$；(2)若不存在实例 Π_s^j 与 Π_u^i 互为伙伴关系，用户 u 随机选择会话密钥，即令 $sk_u^i\xleftarrow{r}\{0,1\}^l$.

引理 5. 若 Σ 是 IND-CCA2 安全的公钥加密方案，那么式(II.5)成立.

$$|Adv_{\mathcal{A},\text{I},4}(\kappa)-Adv_{\mathcal{A},\text{I},3}(\kappa)|\leqslant negl(\kappa)\qquad(\text{II}.5)$$

证明. 利用标准的混合证明法对引理 5 进行证明. 令敌手 $\mathcal{M}$ 是攻击定理 1 的概率多项式时间敌手. 给定系统公钥 pk_Σ 以及 $\{HP_i\}_{i=1}^l$，敌手 $\mathcal{M}$ 为敌手 $\mathcal{A}$ 模拟整个协议攻击实验. 首先，敌手 $\mathcal{M}$ 为用户 u 选择口令 $pw_u=pw_{s,u}$(口令服从 CDF-Zipf 分布)，并向 $\mathcal{A}$ 提供 pk_Σ 和其他公共参数.

在回复敌手 $\mathcal{A}$ 的 Execute 询问时，$\mathcal{M}$ 向 Σ 方案的加密预言机发送非法口令 pw'(pw'服从 CDF-Zipf 分布)，并将会话密钥设置为随机数.

在回复敌手 $\mathcal{A}$ 的第 i 个 Send0 询问时，敌手 $\mathcal{M}$ 令 $label_u=u\|s\|HP_i$，并向其自己的加密预言机发送$(label_u,pw_u)$. 敌手 $\mathcal{M}$ 收到$(\boldsymbol{C}_i,\{h_{j,i}\}_{i=1}^l)$后，向敌手 $\mathcal{A}$ 返回消息$(HP_i,\boldsymbol{C}_i)$.

$\mathcal{M}$ 在回复 $\mathcal{A}$ 的 Send1$(u,k,msg=(HP_{\mathcal{A}},\boldsymbol{C}_{\mathcal{A}}))$询问时，若服务器 s 端存在实例 Π_s^j 与 Π_u^i 互为伙伴关系，那么令 $sk_u^i=sk_s^j$. 否则，令 $pid_u^i=s$，令 Send0(u,k,s)为 $\mathcal{A}$ 的第 i 个 Send0 预言机询问，并进行以下修改：(1)若 msg 由之前的预言机 Send0(u,x,s)产生，即 $msg=(HP_x,\boldsymbol{C}_x)$，那么令 $sk_u^k=h_{i,x}\cdot h_{x,i}$；(2)若 msg 由敌手 $\mathcal{A}$ 产生，那么 $\mathcal{M}$ 令 $label'=s\|u\|HP_{\mathcal{A}}$，并向自己的解密预言机发送$(label',\boldsymbol{C}_{\mathcal{A}})$. $\mathcal{M}$ 收到解密预言机返回的$(label',pw_{\mathcal{A}})$后，若 $pw_{\mathcal{A}}=pw_u$，$\mathcal{M}$ 宣布 $\mathcal{A}$ 获胜；否则，随机选择 sk_u^i. 实验的最后，若敌手 $\mathcal{A}$ 攻击成功，那么敌手 $\mathcal{M}$ 输出 1.

设 b 为定理 1 中的随机比特. 若 $b=0$，则 $\mathcal{M}$ 为 $\mathcal{A}$ 模拟的实验与 Exp3 相同，否则与 Exp4 相同. 这里还要说明 $h_{i,x}$ 和 $h_{x,i}$ 的随机性. 二者可能重用的情况只有敌手 $\mathcal{A}$ 访问 Send1$(u,*,msg=(HP_x,\boldsymbol{C}_x))$这一种情况. 此时，实例 Π_s^j 与 Π_u^i 互为伙伴关系，会话密钥的计算不再使用 $h_{i,x}$ 和 $h_{x,i}$，所以二者是随机的. 因此，若定理 1 成立且 Σ 是 IND-CCA2 安全的公钥加密方案，那么式(II.5)成立.

实验 Exp5. 该实验对实验 Exp4 中的 Send0 进行以下修改：将用户 u 和服务器 s 的密文 $\boldsymbol{C}_u$ 与 $\boldsymbol{C}_s$ 分别替换为非法口令 pw'的加密值 $\boldsymbol{C}_u'$ 与 $\boldsymbol{C}_s'$(pw'服从 CDF-Zipf 分布).

引理 6. 若 Σ 方案是 IND-CCA2 安全的公钥加密方案且定理 1 成立，那么式(II.6)成立.

$$|Adv_{\mathcal{A},\text{I},5}(\kappa)-Adv_{\mathcal{A},\text{I},4}(\kappa)|\leqslant negl(\kappa)\qquad(\text{II}.6)$$

该证明与 Exp1 中的证明类似，不再赘述.

下证所提出的协议 I 是安全的口令认证密钥交换协议(满足定义 1)，即证

$$Adv_{\mathcal{A},\text{I}}(\kappa)\leqslant C'\cdot Q(\kappa)^{s'}+negl(\kappa)\qquad(\text{II}.7)$$

根据式(II.1)到式(II.6)，要证式(II.7)成立，只需证

$$Adv_{\mathcal{A},\text{I},5}(\kappa)\leqslant C'\cdot Q(\kappa)^{s'}+negl(\kappa)\qquad(\text{II}.8)$$

设敌手 $\mathcal{A}$ 最多可执行 $Q(\kappa)$ 次在线口令猜测，并记敌手 $\mathcal{A}$ 猜测出正确的口令为事件 GPW，记敌手 $\mathcal{A}$ 未猜测出正确的口令为事件 NGPW. 那么

$$\begin{aligned}Pr(\text{Success}_{\text{Exp}_5})&=Pr(\text{Success}_{\text{Exp}_5}|\text{GPW})\cdot Pr(\text{GPW})+\\&\quad Pr(\text{Success}_{\text{Exp}_5}|\text{NGPW})\cdot Pr(\text{NGPW})\\&\leqslant Pr(\text{Success}_{\text{Exp}_5}|\text{GPW})\cdot Pr(\text{GPW})+\\&\quad Pr(\text{Success}_{\text{Exp}_5}|\text{NGPW})\\&=Pr(\text{Success}_{\text{Exp}_5}|\text{NGPW})+\\&\quad(1-Pr(\text{Success}_{\text{Exp}_5}|\text{NGPW}))\cdot\\&\quad Pr(\text{GPW})\end{aligned}\qquad(\text{II}.9)$$

又在实验 Exp5 中，会话密钥是随机的，且口令分布服从 CDF-Zipf 定律，所以有

$$Pr(\text{GPW})\leqslant C'\cdot Q(\kappa)^{s'}+negl(\kappa)\qquad(\text{II}.10)$$

若敌手 $\mathcal{A}$ 未猜测出正确的口令，那么 $\mathcal{A}$ 只能通过 Test 中的比特猜测获胜，所以有

$$Pr(\text{Success}_{\text{Exp}_5}|\text{NGPW})=1/2+negl(\kappa)\qquad(\text{II}.11)$$

根据式(II.9)、(II.10)、(II.11)和敌手优势的定义有

$$\begin{aligned}Adv_{\mathcal{A},\text{I},5}(\kappa)&=2Pr(\text{Success}_{\text{Exp}_5})-1\\&\leqslant 2(Pr(\text{Success}_{\text{Exp}_5}|\text{NGPW})+\\&\quad(1-Pr(\text{Success}_{\text{Exp}_5}|\text{NGPW}))\cdot Pr(\text{GPW}))-1\\&\leqslant C'\cdot Q(\kappa)^{s'}+negl(\kappa)\end{aligned}\qquad(\text{II}.12)$$

式(II.12)证明了式(II.8)成立，所以有式(II.7)成立. 综上，定理 3 成立. 证毕.

YIN An-Qi, Ph. D. Her research interests include password-authenticated key exchange protocol and lattice-based cryptography.

WANG Ding, Ph. D., professor, Ph. D. supervisor. His research interests focus on password security and cryptographic protocols.

GUO Yuan-Bo, Ph. D., professor, Ph. D. supervisor. His research interests include cyber defense, machine learning, and artificial intelligence security.

CHEN Lin, Ph. D., associate professor. Her research interests include cyber security and the design of secure specific chip.

TANG Di, M. S. His research interests focus on cyber security.

Background

Currently, password-authenticated key exchange (PAKE) protocols based on traditional difficult problems are not resistant to quantum attacks. Lattice-based cryptosystem is a typical quantum-resistant cryptosystem, and it has been certified by NIST as the most promising cryptosystem in the post-quantum era. The lower-round PAKE protocol is generally more efficient. However, existing low-round lattice-based PAKE schemes are not able to avoid the utilization of additional cryptographic primitives, such as non-interactive zero-knowledge (NIZK) proofs, signature/verification algorithms or other techniques, hindering the improvement of execution efficiency. Besides, word-independent smooth projection hash function (SPHF) is an important mathematical tool to construct low-round PAKE protocols. But there is no such SPHF with IND-CCA2 secure over lattices. In addition, the current security analysis model of PAKE protocol generally assumes that passwords obey a uniform distribution, which leads to an underestimation of the security risks faced by a real PAKE protocol.

Therefore, utilizing the additive homomorphic property of the Learning with Errors (LWE) problem, this paper proposes an IND-CCA2 secure word-independent SPHF over lattices and identifies the parameters of the public key encryption (PKE) scheme it predicates on to eliminate the influence of the incomplete additive homomorphic property on the correctness of the proposed SPHF. As far as we know, this is the first lattice-based word-independent SPHF with IND-CCA2 secure. On this basis, this paper designs an efficient and provably secure PAKE protocol in the standard model. This quantum-resistant protocol achieves the optimal communication round without the utilization of, NIZK proofs and signature/verification algorithms. We also eliminate the utilization of the random oracle, thus capable of avoiding the potential security threats of utilizing random oracles, especially in situations where the utilize of random oracles may cause lattice-based PAKE protocols to suffer offline password guessing attacks and quantum attacks. And this paper presents a more practical PAKE protocol security model, based on which, a strict security proof is provided for the proposed protocol. The experimental results show that the proposed protocol has the most optimal efficiency and the lowest communication cost compared with other related protocols.

This work has been supported by the National Natural Science Foundation of China (Grant No. 62172240) and the Basic Research Program of Beijing-Tianjin-Hebei, China (Grant No. 21JCZXJC00100). Our research group has devoted a lot of effort to password-based authentication schemes and password security. We have published some papers in the respectable journals, such as computer networks, security and communication networks, International Journal of Communication Systems and so on.