基于格的口令认证密钥交换协议综述

郭渊博，尹安琪
（信息工程大学密码工程学院，河南 郑州 450001）

摘 要：量子计算技术的快速发展使基于传统困难问题的口令认证密钥交换（PAKE）协议在后量子时代面临严重的安全威胁。基于格的密码体制因高效性、高安全性，以及支持全同态加密和多线性映射等更强的密码服务功能，被美国 NIST 认证为后量子时代最具潜力的密码体制。首先系统地梳理格上 PAKE 协议的研究进展，主要包括格上集中式的两方、三方 PAKE 协议和分布式 PAKE 协议，然后分别对相关典型方案进行了对比分析，最后展望了格上 PAKE 协议的未来发展趋势。

关键词：口令认证密钥交换；格；可证明安全；抗量子
中图分类号：TP393
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022190

Research on password-authenticated key exchange protocol over lattices

GUO Yuanbo, YIN Anqi
Department of Cryptogram Engineering, Information Engineering University, Zhengzhou 450001, China

Abstract: With the rapid development of quantum computing technology, password-authenticated key exchange (PAKE) protocol based on conventional difficult problems will face serious security threats in the post-quantum era. Lattice-based cryptosystem has been certified by NIST as the most promising cryptosystem in the post-quantum era due to its high efficiency, high security and support for stronger cryptographic service functions (such as fully homomorphic encryption and multi-linear mapping). Firstly, the research progress of lattice-based PAKE protocol was systematically sort out, mainly including the centralized two-party, three-party PAKE protocol and the distributed PAKE protocol over lattices. Then, the relevant typical schemes were compared and analyzed, respectively. Finally, the future research directions PAKE protocol over lattices were prospected.

Keywords: password-authenticated key exchange, lattice, provably secure, quantum resistance

0 引言

近年来，随着 5G、云计算、大数据、人工智能等高新技术的飞速发展，人类的生产、生活也随之走向深度的信息化、网络化、数字化。以“互联网+”为代表的新型发展生态已经成为中国社会发展的国家战略。由于网络的开放性与匿名性，互联网在快速发展的同时衍生出一系列安全问题，网络空间俨然成为国家安全的“第五疆域”[1]。身份认证系统是保护网络资产过程中的重要关卡[2]，一旦其被攻破，信息和网络系统内所有的安全措施就形同虚设。

基于口令的身份认证技术不存在高熵密钥的管理问题（相比基于智能卡、U 盾等信任物体的身份认证技术），也不存在用户不可撤销的隐私泄露问题（相比基于指纹、虹膜等生物特征的身份认证技术），大大降低了认证成本并提高了安全系统的便利性、可部署性。然而，与已经得到深入、广泛研究的高熵密钥认证方式相比，口令认证的研究成果相对不足。口令

收稿日期：2022−07−22；**修回日期：**2022−09−13
基金项目：国家自然科学基金资助项目（No.61501515, No.61601515）
Foundation Item: The National Natural Science Foundation of China (No.61501515, No.61601515)

认证作为一种低熵认证方式，虽然曾一度因各种安全问题被认为必将消亡，但迄今为止，口令认证仍是各类信息和安全系统中应用最广泛的认证方式之一[3]。由于口令认证是唯一不需要进行硬件部署的认证方式，在绝大多数网站中，基于口令的单因子认证方式无可替代[1]。口令在工业界的作用也从未淡化，其不仅在传统的电子政务、商务、医疗等领域继续发挥优势，还向交通、税务、广电、能源、水利、教育等多领域不断扩展[4]。虽然在 2022 年 MIT Technology Review“十大突破性技术”[5]掀起了“终结口令”的第二次浪潮，但汪定等[3]指出，无口令身份认证方案目前存在兼容性差、可扩展性低、成本高和存在隐私泄露等风险，并特别指出无口令身份认证方案降低了用户对身份的控制权，因而有 52%的被调研者并不接受此类认证方式。因此，学术界与工业界逐渐达成共识，在可预见的未来，口令认证仍将是用户最主要的认证方式之一[1,3,5]。

现阶段，口令认证的相关研究聚焦于设计适用于不同应用场景的安全高效的口令认证密钥交换（PAKE, password-authenticated key exchange）协议。PAKE 协议使只拥有低熵口令的协议参与方可以通过非安全信道协商用于安全通信的高熵密钥[6]。研究者先后提出了一系列PAKE协议[7-13]，如著名的 SPR[7]、PAK[8]、PPK[9]、KOY/GL[10-11]和 JG/GK[12-13]协议。上述协议都是基于传统困难问题的，但早在 1994 年 Shor[14]就证明，存在量子算法可以解密所有基于大整数分解和离散对数等传统困难问题的密码体制，且量子计算机已经诞生[15]，其量产化和实用化只是时间问题。因此，基于传统困难问题的 PAKE 协议在即将到来的量子时代不再安全。

为应对量子攻击，密码学者已经开始研究各种抗量子的密码体制。除了以 AES、DES 为代表的对称密码体制外，现有公认的抗量子密码体制主要分为以下 5 类[16-17]：基于哈希的密码体制[18]、基于编码的密码体制[19]、基于多变量的密码体制[20]、基于格的密码体制[21]和基于同源的密码体制。其中，基于格的密码体制有以下优势：1) 密码学者已经完成了格上部分困难问题从平均情况下困难性到最坏情况下困难性的归约证明[22]，因此基于格的密码体制不仅具有更强的安全性，在应用时还支持困难实例的随机选取[22]，这也是此类密码体制独有的优势；2) 格上的运算一般具有线性渐近复杂度，如小整数的矩阵、向量的模乘/加，而基于大整数分解和离散对数等传统困难问题的密码体制需要采用大整数模/幂运算，相比之下基于格的密码体制具有高效性[23]；3) 格上有多个困难问题被证明是困难的，如最短向量问题、最近向量问题、带差错学习问题，这为基于格的密码体制提供了丰富的密码学原语选择空间[16]；4) 鉴于格的简单代数和几何结构，基于格的密码体制易于通过软件和硬件实现[17]；5) 密码服务功能较强，在全同态加密[24]、多线性映射[17]等领域具有广泛的应用前景。因此，基于格的密码体制被美国国家标准与技术研究院（NIST）认为是后量子时代最具潜力的密码体制[25]。

然而与已经得到深入研究和广泛应用的传统密码体制相比，关于基于格的密码体制的研究相对不足。当前，相关研究主要集中在加密算法和哈希函数 2 个领域，关于格上 PAKE 协议的研究成果还比较有限。随着网络和信息技术的快速发展，各方对大规模通信系统中的身份认证方案需求日盛；但格上相关方案的执行效率较低，且个别方案仅实现了密钥传输。另一方面，目前格上 PAKE 协议的研究多关注如何提高单服务器 PAKE 协议的执行效率，此类协议固有的缺陷是无法抵抗服务器泄露攻击；个别可抵抗此类攻击的相关方案未实现唯口令设置和密钥交换，且执行效率低下。

早期协议的研究基于启发式安全性分析，这使协议研究一度陷入了“提出→攻击→改进→攻击→改进”的循环[1]。因此，可证明安全逐渐成为必要的设计目标。PAKE 协议的研究也由此衍生出以下 2 条技术路线：在随机预言机模型（ROM, random oracle model）/理想加密模型下最优化 PAKE 协议的性能[9,26-28]；在标准模型下，构造可证明安全的高效 PAKE 协议[13,29-33]。相比之下，在标准模型下构造可证明安全的 PAKE 协议更加困难。然而，在格 PAKE 方案中使用随机预言机比在一般方案中更具安全威胁，主要原因如下：随机预言机的安全性本身存疑，因为在实际应用时随机预言机需要被具体的哈希函数替代[34]；对于 PAKE 协议而言，使用随机预言机还可能导致协议遭受离线口令猜测攻击；格密码方案的主要应用场景为后量子时代，量子敌手可以在量子态下访问随机预言机[35-36]，这进一步加剧了使用随机预言机对格 PAKE 方案的安全威胁。因此，在格 PAKE 方案中应尽量避免使用随机预言机，这

使基于格假设构造 PAKE 方案更加困难。

PAKE 协议还面临离线口令猜测攻击、在线口令猜测攻击和各种新型口令猜测攻击的威胁[1]。抵抗离线口令猜测一直是 PAKE 协议设计的重点与难点[13,37]。当前，口令泄露问题日益突出，2021 年，仅 RockYou2021 数据集就泄露了 84 亿条口令记录。知名网站（Yahoo、163 等）、社交媒体（Facebook、Instagram 等）、营销服务提供商（大众、奥迪等）也都发生过口令泄露问题，且口令泄露在短期内往往难以被发现，这进一步加剧了口令泄露的危害。相比之下，在进行在线口令猜测时，攻击者无法获得用户口令文件且可执行的猜测次数受限，因此无论是在学术界还是在工业界，在线口令猜测一直被认为是易于防范的[11,36]。但事实是用户与服务器商正遭受日趋严重的在线口令猜测攻击，如 Github 和 iCloud 等知名网站都遭受过此类攻击。Wang 等[38]指出当前的研究大大低估了真实攻击者在线口令猜测的成功率。此外，随着网络化、信息化、数字化的深入发展，还涌现出一系列新型口令猜测攻击，如基于深度学习的[39]和基于云计算增强的[40]口令猜测攻击等，这导致 PAKE 协议面临更加严重甚至未知的安全威胁。另一方面，《“十四五”规划和 2035 年远景目标纲要》明确指出要“加强重要领域数据资源、重要网络和信息系统安全保障”；并且，在 2019 年 10 月 26 日、2021 年 6 月 10 日和 2021 年 8 月 20 日，《中华人民共和国密码法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》相继问世，这对口令认证技术提出了更高的要求。

面对即将产业化的量子计算机、不断更新的口令攻击手段，以及国家对网络和信息系统的高安全需求，本文对目前格上 PAKE 协议的研究现状进行分析与总结，以期为相关领域研究人员提供更清晰的现状梳理和为未来研究方向提供借鉴。

1 预备知识

本节主要介绍后续综述所需的基本概念、格上困难问题、公钥加密体制、平滑投影哈希函数（SPHF, smooth projective hash function）和 PAKE 协议的安全性分析模型等。首先给出必要的符号说明，其中，矩阵和向量分别用加粗的大写和小写字母表示，如矩阵 $\boldsymbol{A}$ 和向量 $\boldsymbol{a}$；其他参数含义如表 1 所示。

表 1 参数含义

参数	含义
κ	安全参数
$\leftarrow / \xleftarrow{r}$	取样/随机取样
$\|\|\boldsymbol{a}\|\|$	向量 $\boldsymbol{a}$ 的模
$\|\|C\|\|$	集合 C 的大小
ε	错误比例参数
β	平滑参数
pw	口令
D	口令空间
$\mathrm{Ham}(\cdot,\cdot)$	汉明距离函数
$\boldsymbol{0}$	零向量/零矩阵

1.1 基本概念

定义 1 格[41]。设矩阵 $\boldsymbol{A}\in\mathbb{R}^{m\times n}$，且 $\boldsymbol{A}$ 的列向量线性无关。格 Λ 可定义为

$$\{\Lambda_{\boldsymbol{A}}=\boldsymbol{A}s \mid s\in\mathbb{Z}_q^n\} \tag{1}$$

其中，$\boldsymbol{A}$ 为格 Λ 的基矩阵，m 为格 Λ 的维数，n 为格 Λ 的秩。

定义 2 理想格[42]。设 k 为正整数，$n=2^k$，多项式 $f(x)=x^n+1\in\mathbb{Z}[x]$，另设多项式环为 $R=\mathbb{Z}[x]/<f(x)>$，环 R 中的元素为 $<g(x)>=\{g(x)=h(x)\bmod f(x)\mid h(x)\in\mathbb{Z}[x],\ \deg(x)<n\}$，且 $g(x)$ 的系数是 $\mathbb{Z}^n$ 中的元素。令 I 是环 R 的理想，则 I 中所有元素的系数构成 $\mathbb{Z}^n$ 的一个子格，称对应于理想 I（$I\subseteq R=\mathbb{Z}[x]/<f(x)>$）的一个子格（关于 $\mathbb{Z}^n$ 的子格）为 $f-$理想格。

定义 3 离散高斯分布[43]。设高斯函数的中心为 c，平滑参数为 β（$\beta\in(0,1)$）。另设随机向量 $\boldsymbol{x}$ 和高斯权重函数 $\rho_{\beta,c}$，$\rho_{\beta,c}$ 的表达式为

$$\rho_{\beta,c}(\boldsymbol{x})=\frac{1}{\beta}\exp\left(\frac{-\pi\|\boldsymbol{x}-c\|^2}{\beta^2}\right) \tag{2}$$

对于格 $\Lambda\in\mathbb{Z}^m$，令

$$\rho_{\beta,c}(\Lambda)=\sum_{x\in\Lambda}\rho_{\beta,c}(\boldsymbol{x}) \tag{3}$$

进一步，定义格 Λ 上的离散高斯分布为

$$D_{\Lambda,\beta,c}(\boldsymbol{x})=\frac{\rho_{\beta,c}(\boldsymbol{x})}{\rho_{\beta,c}(\Lambda)} \tag{4}$$

特别地，若 $c=0$，可将 $D_{\Lambda,\beta,c}$ 简记为 $D_{\Lambda,\beta}$。

下文中的错误概率分布采用截断离散高斯分布[37]，即 $D_{\Lambda,\beta}$ 的定义域为 $\|\boldsymbol{x}\|<\beta\sqrt{n}$。根据 Katz 等[37]研究，在统计上，截断高斯分布与非截断高斯分布

相近，因此下文直接称截断高斯分布为高斯分布。本文用 $\overline{\psi}_{\beta q}$ 表示 $\mathbb{Z}_q$ 上的某分布，取样方法为 $y \leftarrow D_{\Lambda,\beta}$，输出 $\lceil qy \rfloor (\mathrm{mod}\, q)$ [37]。

定义 4　判定性带误差学习（DLWE, decisional learning with error）问题[44]。对于正整数 m、n、q（$m = \mathrm{poly}(n)$，$2 \leqslant q \leqslant 2^{\mathrm{poly}(n)}$）以及任意离散高斯分布 $\chi = D_{\Lambda,\beta}$　（$\Lambda \in \mathbb{Z}_q^m$，$\beta \in (0,1)$，$\beta q \geqslant 2\sqrt{n}$），DLWE 问题定义为区分以下 2 个分布的问题：1) $\{(A,b) | A \xleftarrow{r} \mathbb{Z}_q^{m\times n}, b \xleftarrow{r} \mathbb{Z}_q^{m\times 1}\}$；2) $\{(A,b) | A \xleftarrow{r} \mathbb{Z}_q^{m\times n}, s \xleftarrow{r} \mathbb{Z}_q^{n\times 1}, e \xleftarrow{r} \chi^{m\times 1}, b = As + e (\mathrm{mod}\, q)\}$。DLWE 问题的安全性归约[45]如下：若参数 $\beta q \geqslant 2\sqrt{n}$，$q \leqslant 2^{\mathrm{poly}(n)}$，$\mathrm{DLWE}_{n,q,\chi,m}$ 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（SIVP, shortest independent vector problem）一样困难。

典型 DLWE 问题的参数设置为 $n = \Omega(\kappa)$，$q \leqslant 2^{\mathrm{poly}(n)}$，$m = O(n \log q)$，误差分布为 $\chi = D_{\mathbb{Z},\beta}$，其中 $\beta = \dfrac{q}{\mathrm{ploy}(n)}$。在该参数设置下，攻破 DLWE 问题至少需要 $2^{\Omega(n)}$ 次攻击。减小参数 β 会导致 DLWE 问题的安全性降低，比如当 $\beta = \dfrac{q}{2^{\Omega(n)}}$ 时，攻破 DLWE 问题只需要 $\mathrm{ploy}(n)$ 次攻击。文献[42]以合理的安全性牺牲为代价（即减小误差分布的参数 β）来实现安全性证明等应用目标。

定义 5　强 DLWE 问题[42]。设安全参数为 κ，令 $f(n)$ 为正整数 n 的亚指数函数，若 $\beta = \dfrac{q}{f(n)}$，$n = \Omega(\kappa^2)$，那么攻破 LWE 问题至少需要亚指数次攻击，此时称 LWE 问题为强 LWE 问题。

定义 6　环 LWE（RLWE, ring LWE）问题[46]。设 n，q（$q \geqslant 2$）为正整数，且 $q \equiv 1 (\mathrm{mod}\, 2n)$，多项式环 $R_q = \mathbb{Z}_q[x] / < f(x) >$，其中 $f(x) \in \mathbb{Z}_q[x]$；另设错误分布为 $\overline{\psi}_{\beta q}$，对于 $s \in R_q$，存在以下 2 个分布：1) $\{(a,b) | a \xleftarrow{r} R_q, b = as + e\} \in R_q \times R_q$；2) $\{(a,b) | a \xleftarrow{r} R_q, b \xleftarrow{r} R_q\} \in R_q \times R_q$。RLWE 问题定义为区分以上 2 个分布的问题。

1.2　公钥加密体制

公钥加密是指由对应的唯一一对密钥（包括公钥和私钥）组成的加密算法。根据安全性的不同，公钥加密方案可分为选择明文攻击下不可区分性（IND-CPA, indistinguishability under chosen- plaintext attack）安全和选择密文攻击下不可区分性（IND-CCA, indistinguishability under chosen- ciphertext attack）安全 2 种；进一步，根据攻击者或敌手能力的不同，IND-CCA 安全又可以分为 IND-CCA1 安全（在现有文献中，有时直接称 IND-CCA1 安全为 IND-CCA 安全）和适应性选择密文攻击下不可区分（IND-CCA2, indistinguishability under adaptive chosen-ciphertext attack）安全。下面，正式给出 3 种安全性的定义。

定义 7　IND-CPA 安全。设 κ 为安全参数，对于给定的公钥加密方案 $\mathrm{PKE} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$，令任意概率多项式时间（PPT, probabilistic polynomial time）敌手 $\mathcal{A}$ 执行以下游戏（也称为实验）。

1) 系统建立：模拟器运行密钥生成算法生成公私钥对 $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{KeyGen}(1^\kappa)$，并向 PPT 敌手 $\mathcal{A}$ 公开公钥 pk。

2) 询问阶段：$\mathcal{A}$ 向模拟器（也可以是挑战预言机）进行多项式有界次的加密询问。

3) 挑战阶段：$\mathcal{A}$ 选择 2 个等长的不同明文 m_1, m_2，并向模拟器发送 (m_1, m_2)；模拟器选择随机比特 $b \xleftarrow{r} \{0,1\}$，计算挑战密文 $c^* \leftarrow \mathrm{Enc}(m_*, \mathrm{pk})$，并向 $\mathcal{A}$ 发送 c^*。

4) 猜测阶段：$\mathcal{A}$ 收到挑战密文 c^* 后，输出关于 b 的猜测比特 b'。

若 $b' = b$，则称敌手成功，并定义此时的敌手优势为

$$\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{IND\text{-}CPA}}(\kappa) = |2\Pr(b' = b) - 1| \tag{5}$$

若对于任意 PPT 敌手 $\mathcal{A}$，存在可忽略函数 $\mathrm{negl}(\kappa)$，使此时的敌手优势满足 $\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{IND\text{-}CPA}}(\kappa) \leqslant \mathrm{negl}(\kappa)$，则称公钥加密方案 $\mathrm{PKE} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ 是 IND-CPA 安全的。

定义 8　IND-CCA2 安全。设 κ 为安全参数，对于给定的公钥加密方案 $\mathrm{PKE} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$，令任意 PPT 敌手 $\mathcal{A}$ 执行以下游戏。

1) 系统建立：模拟器运行密钥生成算法生成公私钥对 $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{KeyGen}(1^\kappa)$，并向 PPT 敌手 $\mathcal{A}$ 公开公钥 pk。

2) 询问阶段 1：$\mathcal{A}$ 向模拟器进行多项式有界次的加/解密询问。

3) 挑战阶段：$\mathcal{A}$ 选择 2 个等长的不同明文

m_1, m_2，并向模拟器发送(m_1, m_2)；模拟器选择随机比特$b \xleftarrow{r} \{0,1\}$，计算挑战密文$c^* \leftarrow \mathrm{Enc}(m_*, \mathrm{pk})$，并向$\mathcal{A}$发送$c^*$。

4) 询问阶段 2：$\mathcal{A}$收到挑战密文c^*后，向模拟器进行多项式有界次的加/解密询问。

5) 猜测阶段：$\mathcal{A}$输出b的猜测比特b'。

若$b'=b$，则称敌手成功，并定义此时的敌手优势为

$$\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{IND\text{-}CCA2}}(\kappa) = |2\Pr(b'=b)-1| \tag{6}$$

若对于任意 PPT 敌手$\mathcal{A}$，存在可忽略函数$\mathrm{negl}(\kappa)$，满足$\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{IND\text{-}CCA2}}(\kappa) \leqslant \mathrm{negl}(\kappa)$，则称$\mathrm{PKE}=(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$是 IND-CCA2 安全的。

定义 9 IND-CCA1 安全。设κ为安全参数，对于给定的公钥加密方案$\mathrm{PKE}=(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$，若对于任意 PPT 敌手$\mathcal{A}$，赢得下述游戏的优势$\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{IND\text{-}CCA1}}$满足$\mathrm{Adv}_{\mathrm{PKE},\mathcal{A}}^{\mathrm{IND\text{-}CCA1}}(\kappa) \leqslant \mathrm{negl}(\kappa)$，则称$\mathrm{PKE}=(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$是 IND-CCA1 安全的。

该游戏与定义 8 中游戏的不同之处在于，其不能执行“询问阶段 2”，即敌手$\mathcal{A}$收到模拟器发送的挑战密文c^*后，不能再向模拟器进行加/解密询问。

1.3 平滑投影哈希函数

平滑投影哈希函数是一种隐式证明方法，其概念最初由 Cramer 等[47]提出，Katz 等[33]根据格上的应用需求对此概念进行修改，本文采用 Katz 等[33]的相关定义。平滑投影哈希函数是构造唯口令 PAKE 协议的有效数学工具，除此之外，还可应用于零知识证明、不经意传输和证据加密等领域。

设口令为 pw，pw 的集合为D，并设公钥加密方案的公钥为 pk；令C_{pk}表示与 pk 对应的 (label, C) 对的集合，其中，label 表示有效标签，C 表示与 pk 相对应的密文。对于给定的 pk，定义集合 X 和$\{L_{\mathrm{pw}}\}_{\mathrm{pw}\in D}$如下[32]：1) X:={(label, C, pw) | (label, C)$\in C_{\mathrm{pk}}$ && pw$\in D$}；2) L_{pw}:={(label, Enc(pk, pw || label), pw$\in D$)}。

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

下面，正式给出 SPHF 的定义。

定义 10 平滑投影哈希函数[37]。首先给出近似 SPHF 的概念。设汉明距离函数为 Ham，错误比例参数为ε；哈希密钥为 kh，哈希密钥的长度为 l，kh 的集合为 KH；投影密钥为 kp，kp 的集合为 KP；Hash 表示哈希函数，其定义域为 X、值域为$\mathbb{Z}_q$；由 Hash 构成的哈希函数簇用$\mathcal{H}$表示；ProjKG 表示定义域为 KH、值域为 KP 的投影函数。近似 SPHF 可由取样算法定义，输入公钥 pk 和集合 L、X，输出 (K, G, $\mathcal{H}$={Hash(W, kh): $X \rightarrow \{0,1\}^n$}, S, ProjKG(kh): KH $\rightarrow$ KP)，且满足以下条件。

1) 存在以下高效算法：取样算法$\mathrm{kh} \xleftarrow{r} \mathrm{KH}$、哈希函数 Hash($W$, kh) 和投影函数 ProjKG。

2) 近似正确性：对于$\forall W=(\mathrm{label}, C, \mathrm{pw}) \in L$，哈希值有 2 种计算方式，其一为通过哈希密钥计算$h=\mathrm{Hash}(W, \mathrm{kh})$；其二为由投影密钥 kp 计算，即存在投影哈希函数 ProjHash，满足以投影密钥 kp、单词 W 和$W \in L$ 的证据 r 为输入，以投影哈希值 ph 为输出，且哈希值 h 与投影哈希值 ph 近似相等，即式(7)成立。

$$\Pr(\mathrm{Ham}(h, \mathrm{ph}) \geqslant \varepsilon l) = \mathrm{negl}(\kappa) \tag{7}$$

3) 平滑性：对于$\forall W=(\mathrm{label}, C, \mathrm{pw}) \in X/L$、$\mathrm{kh} \xleftarrow{r} \mathrm{KH}$和$\mathrm{kp}=\mathrm{ProjKG}(\mathrm{kh})$，式(8)中的 2 个分布在计算上不可区分。

$$\begin{cases} (\mathrm{kp}, \mathrm{Hash}(W, \mathrm{kh})) \\ (\mathrm{kp}, v \leftarrow \{0,1\}^*) \end{cases} \tag{8}$$

特别地，若错误比例参数$\varepsilon=0$，则上述近似平滑投影哈希函数为平滑投影哈希函数。此外，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[48]。

近似 SPHF 只能实现近似正确性，Benhamouda 等[48]给出了通过纠错码算法实现正确性放大从而得到 SPHF 的通用技术，现介绍该技术。

令$\{\mathrm{HashKG}', \mathrm{ProjKG}', \mathrm{Hash}', \mathrm{ProjHash}'\}$为近似 SPHF，值域为$\{0,1\}^v$；令 ECC 为纠错码算法，可以纠正$\varepsilon$比例的错误，那么下述$\{\mathrm{HashKG}, \mathrm{ProjKG}, \mathrm{Hash}, \mathrm{ProjHash}\}$是 SPHF。

$\mathrm{kh} \leftarrow \mathrm{HashKG}(\mathrm{params})$：输入$\mathrm{kh}_1 \leftarrow \mathrm{hashKG}'(\mathrm{params})$，在 ECC 的定义域中随机选择$\mathrm{kh}_2$，输出哈希密钥$\mathrm{kh} := (\mathrm{kh}_1, \mathrm{kh}_2)$。

$\mathrm{kp} \leftarrow \mathrm{ProjKG}(\mathrm{params}, \mathrm{kh}, W)$：计算$\mathrm{kp}_1 \leftarrow \mathrm{ProjKG}(\mathrm{params}, \mathrm{kh}_1, W)$，并计算$c=\mathrm{ECC}(\mathrm{kh}_2)$、$h' \leftarrow \mathrm{Hash}'(\mathrm{params}, \mathrm{kh}_1, W)$和$\mathrm{kp}_2 = c \oplus h'$，最后输出$\mathrm{kp} := (\mathrm{kp}_1, \mathrm{kp}_2)$。

$h \leftarrow \mathrm{Hash}(\mathrm{params}, \mathrm{kh}, W)$：输出 $h = \mathrm{kh}_2$。

$\mathrm{ph} \leftarrow \mathrm{ProjHash}(\mathrm{params}, \mathrm{kp}, W, r)$：计算 $\mathrm{ph}' \leftarrow \mathrm{ProjHash}(\mathrm{params}, \mathrm{kp}_1, W, r)$，并输出 $\mathrm{ph} = \mathrm{ECC}^{-1}(\mathrm{ph}' \oplus \mathrm{kp}_2)$。

鉴于存在标准技术能够将近似平滑投影哈希函数转换为平滑投影哈希函数，为方便描述，下文中直接省略“近似”二字。

1.4　PAKE 协议安全性分析模型

早期协议，也包括 PAKE 协议的安全性分析是启发式的，这使协议的研究陷入了“设计→攻击→改进→攻击→改进”的循环，因此可证明安全逐渐成为安全协议设计的必要目标。协议的安全性分析模型一般定义了协议的通信环境（包括敌手模型）和安全性等，是研究可证明安全方案的重要基础，下面介绍 PAKE 协议的安全性分析模型。

Bellare 等[49]提出的安全性分析模型一般称为 BR 模型，是第一个针对实例认证和密钥交换的标准安全性分析模型，该模型面向的是对称两方协议。Bellare 等[50]基于 BR 模型提出了一种针对三方协议的安全性分析模型。Blake-Wilson 等[51]进一步提出了一种针对非对称协议的安全性分析模型。Mackenzie[52]和 Bellare 等[26]提出了面向口令认证的安全性分析模型，其中 Bellare 等[26]提出的安全性分析模型是目前应用最广泛的 PAKE 协议安全性分析模型之一，一般称为 BPR 模型，下面介绍该模型。

假设 PAKE 协议在公开网络上展开，参与方包括合法用户 $u \in \mathrm{User}$、合法服务器 $s \in \mathrm{Sever}$ 和非法敌手 $\mathcal{A} \in \mathrm{Adversary} = \{\mathcal{A}, \mathcal{B}, \mathcal{M}, \cdots\}$。假设敌手可以执行仿冒、篡改、重放、窃听、中间人等攻击[53]。另设口令空间为 D，其大小为 $\|D\|$。

在 BPR 模型中，协议的执行用实例 Π 建模。每个参与方可执行多次协议，且允许协议的并行执行。用户 u 的第 i 次协议执行，即第 i 个实例表示为 Π_u^i。BPR 模型规定一个实例只能使用一次，且每个实例维持一个本地状态变量，如 Π_u^i 的本地状态变量为 $(\mathrm{sid}_u^i, \mathrm{pid}_u^i, \mathrm{sk}_u^i, \mathrm{acc}_u^i, \mathrm{term}_u^i)$。其中，$\mathrm{sid}_u^i$ 表示 Π_u^i 的会话标识，并对 Π_u^i 接收和发送的消息进行统一编号；pid_u^i 表示 Π_u^i 的伙伴标识，是 Π_u^i 单方确信的通信对象标识符；sk_u^i 表示 Π_u^i 协商的会话密钥；acc_u^i 是二值变量，若 $\mathrm{acc}_u^i = 1$，Π_u^i 被接受，否则，Π_u^i 被丢弃；term_u^i 也是二值变量，若 $\mathrm{term}_u^i = 1$，Π_u^i 被中止，否则，Π_u^i 未被中止。

在 BPR 模型中，敌手与合法参与方（包括用户和服务器）之间通过以下预言机进行交互，实际上是敌手与各实例的交互。

Execute(u, i, s, j)。该预言机执行实例 Π_u^i 和实例 Π_s^j 之间的协议，并向敌手返回协议的传输副本。Execute 预言机建模了敌手执行的被动窃听攻击。

Send(u, i, msg)。敌手向 Π_u^i 发送该预言机询问后，该预言机根据协议的定义执行协议，包括设置本地状态变量 $(\mathrm{sid}_u^i, \mathrm{pid}_u^i, \mathrm{sk}_u^i, \mathrm{acc}_u^i, \mathrm{term}_u^i)$，最后该预言机将协议的输出消息返回给敌手。特别地，若敌手发送 Send(u, i, s) 预言机询问，那么敌手可以启动 Π_u^i 与服务器 s 端某实例之间的一次协议的执行，但要求 Π_u^i 未被使用过。Send(u, i, s) 预言机根据协议的定义将第一条传输消息返回给敌手，并建模了主动敌手攻击。

Reveal(u, i)。若敌手发送该预言机询问，该预言机将 Π_u^i 的会话密钥 sk_u^i 返回给敌手，并建模会话密钥泄露攻击，如会话密钥的非法擦除、服务器泄露攻击和密码分析等。

Test(u, i)。该预言机用于定义安全协议，不对真实世界中的任何敌手能力进行建模。若敌手发送 Test 预言机询问，该预言机随机选择比特 b，若 $b = 1$，则将真实的会话密钥 sk_u^i 返回给敌手；否则，向敌手返回与 sk_u^i 等长的随机字符串。BPR 模型规定敌手能且只能对未被访问过的 Reveal 预言机实例执行一次 Test 预言机询问。

下面，给出 BPR 模型中伙伴关系、正确性、新鲜性、敌手优势和安全的 PAKE 协议等定义。

定义 11　伙伴关系[26]。设协议参与方包括用户 u 与服务器 s，若 $\mathrm{sid}_u^i = \mathrm{sid}_s^j \neq \mathrm{NULL}$，$\mathrm{pid}_u^i = s$ 且 $\mathrm{pid}_s^j = u$，则称 u（实例 Π_u^i）与 s（实例 Π_s^j）互为伙伴关系。

定义 12　正确性[26]。设协议参与方包括用户 u 与服务器 s，若实例 Π_u^i 与 Π_s^j 互为伙伴关系，且 $\mathrm{acc}_u^i = \mathrm{acc}_s^j = 1$，$\mathrm{sk}_u^i = \mathrm{sk}_s^j$，则称 PAKE 协议是正确的，即协议正确性要求互为伙伴关系的实例都处于接受状态，且协商了一致的会话密钥。

定义 13　新鲜性[26]。设用户 u 与服务器 s 是伙伴关系，如果敌手未访问过 Reveal(u, i)预言机，且未访问过 Reveal(s, j) 预言机，则称实例 Π_u^i 是新鲜的实例。

设用户 u 与服务器 s 是伙伴关系，并设 PPT 敌

手执行 Test(u,i) 预言机询问后给出了猜测比特 b'。若敌手未访问过 Reveal(u,i) 和 Reveal(s, j) 预言机，且 $b'=b$，称敌手攻击成功。

定义 14 敌手优势[26]。设$\mathcal{A}$表示攻击协议 Π 的 PPT 敌手，且$\mathcal{A}$可对一个实例执行多项式次 Execute、Send、Reveal 预言机询问，但能且只能对新鲜的实例执行一次 Test 预言机询问。用 Success 表示“敌手攻击成功”事件，定义$\mathcal{A}$攻击协议 Π 的优势 $\mathrm{Adv}_{\mathcal{A},\Pi}$ 为

$$\mathrm{Adv}_{\mathcal{A},\Pi}=2\Pr(\mathrm{Success})-1 \tag{9}$$

设 κ 是安全参数，$\mathrm{negl}(\kappa)$ 是关于 κ 的可忽略函数。理想情况下，鉴于 b 的随机性，敌手攻击成功的概率为 $\Pr(\mathrm{Success})=\frac{1}{2}+\mathrm{negl}(\kappa)$。根据式(9)，此时敌手优势为 $\mathrm{Adv}_{\mathcal{A},\Pi}=\mathrm{negl}(\kappa)$，那么敌手$\mathcal{A}$在统计上不能区分真实的会话密钥和与之等长的随机字符串。因此，会话密钥是安全的，这表示 PAKE 协议具备语义安全性。

人脑的记忆能力有限，用户倾向于选择短的、低熵的口令，且用户经常在多个网站使用相同或相近的口令，因而用户实际使用的口令空间较小。鉴于此，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，这导致 PAKE 协议无法避免在线口令猜测攻击[54]。一般情况下，若此类攻击是敌手的最佳攻击方式，则称 PAKE 协议是安全的。

定义 15 安全的 PAKE 协议。设 κ 是安全参数，$\mathcal{A}$是攻击协议 Π 的 PPT 敌手，且$\mathcal{A}$执行在线口令猜测攻击的次数上限为 $Q(\kappa)$。假设口令服从均匀分布，并用 D 表示口令空间，$\|D\|$ 表示口令空间的大小，则称协议 Π 是安全的口令认证密钥交换协议，如果对于所有的 PPT 敌手$\mathcal{A}$，存在可忽略函数 $\mathrm{negl}(\kappa)$ 满足

$$\mathrm{Adv}_{\mathcal{A},\Pi}(\kappa)\leqslant\frac{Q(\kappa)}{\|D\|}+\mathrm{negl}(\kappa) \tag{10}$$

2 基于格的两方 PAKE 协议

现阶段，在基于格的 PAKE 协议领域中，有关两方 PAKE 协议的成果最为丰富。两方 PAKE 协议的典型应用场景如图 1 所示，参与方包括一个用户和一个认证服务器，其中用户持有口令 pw，认证服务器通常存储口令或口令的哈希值、与口令相关的令牌等。根据认证服务器是否直接存储口令，格上的两方 PAKE 协议大致可以分为对称和非对称两类。

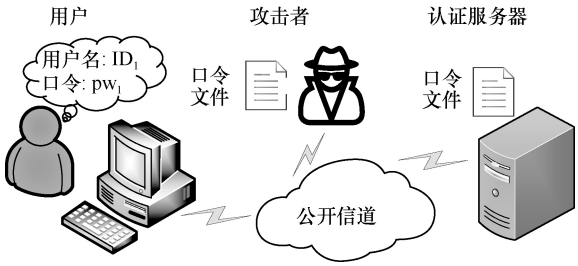

图 1 两方 PAKE 协议的典型应用场景

2.1 对称两方 PAKE 协议

对称 PAKE 协议在服务器端直接存储了用户口令，用于对用户进行认证。在格上实现对称 PAKE 协议的技术路线一般为基于格上的公钥加密算法，通过设计基于格的 SPHF 实现格上的两方 PAKE 协议。该技术路线的技术难点在于构建基于格的 SPHF，这是因为 LWE 问题只具备不完全加法同态性，直接基于格上困难问题设计的 SPHF 难以满足正确性要求。为此，Katz 等[37]提出了近似 SPHF 的概念，并首次给出了在格上实现 PAKE 协议的可行方法，该方法也成为构造格上 PAKE 协议的典型方法，即利用基于格的近似 SPHF 和纠错码技术来实现（精确）SPHF 的功能，进而实现基于格的 PAKE 协议。Katz 等[37]由此提出了第一个基于格的 SPHF 和 PAKE 协议。该协议属于 KOY/GL 架构[10-11]，因而是基于标准安全模型的，且该协议需要 3 轮通信，在用户和服务器端都需要基于 IND-CCA2 安全的公钥加密算法。

JG/GK 架构[12-13]是另一种基于标准安全模型的典型 PAKE 架构，Ding 等[55]基于此架构提出了一种基于格的高效 PAKE 协议。与 Katz 等[37]的方案相比，该协议虽然也需要 3 轮通信，但实现了互认证，且该协议在用户端只需要使用 IND-CPA 安全的公钥加密算法，因而提高了用户端的性能。Ding 等[55]曾断言，除非基于格的精确 SPHF 更加高效，否则没有必要设计格上的精确 SPHF。但在 2013 年，Blazy 等[56]提出了一种基于 LWE 问题的精确 SPHF，并指出精确 SPHF 至少可以使 PAKE 协议的构造不局限于 BPR 安全模型。

借鉴基于传统困难问题的 PAKE 协议的研究路线，减少通信轮（次）和弱化协议所基于的安全性假设依然是格上 PAKE 协议的重要优化方向。Zhang 等[57]首先提出了一种基于格的可拆分公钥加密算法，并基于此提出了一种基于格的非适应性 SPHF，这 2 种构造除用于实现 PAKE 协议外，还具有相对

独立的研究价值；然后，基于 Abdalla 等[58]的通用两轮 PAKE 协议架构，Zhang 等[57]提出了一种格上的两轮两方 PAKE 协议。

Zhang 等[57]提出的两轮 PAKE 架构需要使用模拟健全的非交互式零知识（SS-NIZK, simulation sound non-interactive zero-knowledge）证明，因此执行效率较低，且目前格上还不存在标准模型下的 SS-NIZK 证明，所以 Zhang 等[57]的方案需要使用随机预言机。为此，同样基于 Abdalla 等[58]提出的通用两轮 PAKE 协议架构，Benhamouda 等[48]提出了格上第一个不需要使用 SS-NIZK 证明的两轮 PAKE 协议。在此基础上，Li 等[44]利用 MP 公钥加密方案[59]，也提出了一种格上不需要 SS-NIZK 证明的两轮 PAKE 协议。该协议通过弱化协议所基于的安全性假设（在服务器端只需要基于 IND-CPA 的安全模型）降低了协议各方面的开销。尹安琪等[60]通过安全性证明指出，Li 等[44]将两轮 PAKE 协议中服务器端的安全性假设降低到 IND-CPA 不能保证协议的安全性；进一步，尹安琪等[60]提出了一种格上可证明安全的两轮 PAKE 协议，该协议将用户端的安全性假设降低到 IND-CPA，因而降低了用户端的计算、通信和存储等开销。2018 年，基于 Katz 等[33]提出的通用一轮 PAKE 架构，Benhamouda 等[48]利用其所提出的格上非适应性 SPHF 和 SS-NIZK 证明，给出了一种格上一轮 PAKE 协议的实现方法，但没有给出具体的协议构造和安全性证明。Li 等[61]基于 Benhamouda 等[48]的研究，利用 MP 公钥加密方案[59]，提出了一种高效的基于格的 SPHF，并基于此实现了一种格上的一轮 PAKE 协议。

为进一步提高格上 PAKE 协议的执行效率和降低协议各方面的开销，格上 PAKE 协议的另一个研究方向是基于理想格上困难问题（如 RLWE 困难问题）来构造协议。2010 年，Lyubashevsky 等[62]提出了 LWE 问题在环上的变体——RLWE 问题，并将 RLWE 问题的困难性规约到理想格上困难问题中最难实例的求解。基于 RLWE 问题的加密体制很好地克服了基于欧氏格的密码体制（如 LWE 问题）中密钥过长的缺陷，并且可以通过快速傅里叶变换算法提高加/解密运算速度。2013 年，叶茂等[63]提出了一种基于理想格的 SPHF，该 SPHF 可用于构造基于理想格的 PAKE 协议，从而提高协议性能。2019 年，利用 Lyubashevsky 等[62]基于 RLWE 问题的公钥加密方案，Karbasi 等[64]提出了一种基于理想格的 SPHF，并基于此在 KOY/GL 架构[10,65]下构造了一种基于理想格的 PAKE 协议。

表 2 对比了不同对称 PAKE 协议的性能对比。通信轮（次）特指服务器与用户之间的通信轮（次），其中，通信轮数是指通信双方之间双向通信的数量，次数是指通信双方之间单向通信的数量；如果是异步通信，通信轮数等于通信次数，如果是同步通信，通信次数是通信轮数的 2 倍。

根据表 2，格上 PAKE 协议的通信轮次由 Katz 等[37]、Ding 等[55]方案的 3 轮架构，逐渐发展到 Zhang 等[57]的两轮架构和 Benhamouda 等[48]和 Li 等[61]的一轮架构，从而得到了具有最优通信轮次的 PAKE 协议。更少的通信轮（次）通常代表更低的通信开销和更低的通信风险，一直是格上 PAKE 协议的重要优化方向。但低轮（次）的 PAKE 协议一般无法实现显式认证，只能实现隐式认证。

目前，格上的部分低轮（次）PAKE 协议（包

表 2　　不同对称 PAKE 协议的性能对比

协议名称	通信轮(次)数	抗量子	安全模型		计算类型	随机预言机	SS-NIZK	认证方式
			用户端	服务器端				
文献[37]	3 轮(3 次)	√	IND-CCA2	IND-CCA2	小整数模乘/加	×	×	显式认证
文献[55]	3 轮(3 次)	√	IND-CPA	IND-CCA2	小整数模乘/加	×	×	显式互认证
文献[57]	2 轮(2 次)	√	IND-CCA2	IND-CCA2	小整数模乘/加	√	√	隐式认证
文献[44]	2 轮(2 次)	√	IND-CCA2	IND-CPA	小整数模乘/加	×	×	隐式认证
文献[60]	2 轮(2 次)	√	IND-CPA	IND-CCA2	小整数模乘/加	×	×	隐式认证
文献[33]	1 轮(2 次)	×	IND-CCA2	IND-CCA2	大整数模幂	√	√	隐式认证
文献[48]	1 轮(2 次)	√	IND-CCA2	IND-CCA2	小整数模乘/加	√	√	隐式认证
文献[61]	1 轮(2 次)	√	IND-CCA2	IND-CCA2	小整数模乘/加	√	√	隐式认证

括 Zhang 等[57]的两轮方案和 Benhamouda 等[48]、Li 等[61]一轮 PAKE 方案等）需要使用 SS-NIZK 证明来保证安全性，这种昂贵的密码学原语会影响协议性能的提升，且在格上还不存在基于标准模型的 SS-NIZK 证明，因此上述方案都需要使用随机预言机。随机预言机不仅在实际应用时需要被具体的哈希函数替代，还可能导致 PAKE 遭受离线口令猜测攻击。此外，量子敌手可以在量子态下访问随机预言机，这进一步增大了在格密码方案中使用随机预言机的危害。因此，应该在格 PAKE 方案中尽量避免随机预言机的使用。Li 等[44]和尹安琪等[60]提出的格上两轮 PAKE 方案同时避免了 SS-NIZK 证明和随机预言机的使用，相比之下安全性更高。

Katz 等[37]的 3 轮 PAKE 方案、Zhang 等[57]的两轮 PAKE 方案，以及 Benhamouda 等[48]和 Li 等[61]的一轮 PAKE 方案在用户端和服务器端都需要基于 IND-CCA2 的安全模型。而 Ding 等[55]的 3 轮 PAKE 协议、尹安琪等[60]的两轮 PAKE 协议将格上 PAKE 协议在用户端所基于的安全模型降低到 IND-CPA 安全，Li 等[44]的两轮 PAKE 方案将服务器端所基于的安全模型降低到 IND-CPA 安全。一般而言，基于更强安全模型的密码方案具有更大的计算和存储等开销，因此，与一轮 PAKE 协议相比，两轮 PAKE 协议虽然在通信轮（次）上存在劣势，但在用户端或服务器端可能具有更高的执行效率。

此外，与基于传统困难问题的 PAKE 方案（如 Katz 等[33]的方案）相比，基于格的 PAKE 方案不仅可以抵抗量子攻击，且格上的基本运算是小整数的模乘/加等具有线性渐近复杂度的运算，比传统 PAKE 方案的大整数模幂运算更加高效。

2.2 非对称两方 PAKE 协议

对称 PAKE 方案在服务器端存储了用户的口令，因此存储的或真实的口令一旦泄露，攻击者就可以轻易仿冒合法用户，即此类方案无法抵抗服务器泄露攻击。非对称 PAKE 协议是解决该问题的一种有效方法，因为此类协议只需要在服务器端存储与口令相关的哈希值或验证器或者令牌，用户不需要向服务器端发送真实的口令。

目前，在格上实现非对称 PAKE 方案的常用方法是基于格上困难问题实例化传统的基于传统困难问题（一般是数论困难问题）的非对称 PAKE 协议。基于传统困难问题的典型非对称 PAKE 方案包括 SPR[7]、PAK[8]、PPK[9]方案。2017 年，Ding 等[66]利用 RLWE 困难问题，分别在格上实例化了 PAK 和 PPK 协议[8-9]，从而得到了抗量子的非对称两轮和 3 轮 PAKE 协议，这 2 个协议在服务器端存储了口令的哈希值，Ding 等[66]还在 ROM 下严格证明了这 2 个协议的安全性。同年，Gao 等[67]利用 RLWE 困难问题在格上实例化了 SPR 方案[7]，从而得到了一种抗量子的 SPR 协议，并在通用可组合（UC, universally composable）模型下证明了方案的安全性；该协议只需要在服务器端存储一个与口令相关的验证器，并且该验证器不会泄露口令的任何信息。因为不需要存储口令或者口令的哈希值，该方案的安全性得到了进一步的提高。2021 年，舒琴等[68]利用 Peikert 式误差调和机制，在 UC 模型下提出了一种更加高效的可证明安全的非对称 PAKE 协议。

Li 等[54]在 2020 年指出现有的非对称 PAKE 方案，更确切地说是方案中使用的口令哈希方案（PHS, password hashing scheme），要么基于 ROM（使用随机预言机的局限性见本文的引言部分），要么基于传统困难问题（此类方案无法抵抗量子攻击）。为此，利用基于格的 SPHF，Li 等[54]提出了第一个基于格的 PHS，并在此基础上提出了一种标准模型下可证明安全的格上非对称 PAKE 协议，该协议在服务器端存储了口令的哈希值，可以有效抵抗服务器泄露攻击和量子攻击。

现阶段，随着人们对个人隐私关注度的提高，很多用户期望在认证过程中隐藏个人身份信息，匿名认证方案可以有效解决该问题。2018 年，Feng 等[69]基于 RLWE 问题的困难性，首次提出了一种基于理想格的匿名 PAKE 方案，使用户可以在不泄露身份信息的前提下，通过公开信道实现身份认证和密钥交换。Dabra 等[70]在 2021 年指出 Feng 等[69]的方案简单、高效，但不能抵抗信号泄露攻击、电子欺骗攻击、操纵攻击和用户匿名违规攻击。基于 Ding 等[71]零知识认证协议中直接公钥验证的思想，Dabra 等[70]提出了一种新的基于理想格的匿名 PAKE 方案，并在 ROR（real-or-random）模型下证明了方案的安全性。该方案可以抵抗信号泄露等攻击，包括注册、登录、认证和口令更新等功能。进一步，Ding 等[72]在 2022 年指出，若主密钥重用，Dabra 等[70]的方案仍不能抵抗信号泄露攻击；为此，他们利用 Ding 等[73]随机密钥交换方案中的思想，对 Dabra 等[70]的方案进行改

进，从而提出了一种改进的理想格上的匿名 PAKE 方案，并对方案进行了严格的安全性证明，该协议保证了方案在主密钥重用的情况下也能抵抗信号泄露攻击。

上述方案虽然可以解决服务器端的口令泄露问题，但无法解决用户端的口令泄露问题。多因子认证方式是解决该问题的有效方法，若将口令身份认证看作网络和信息系统的第一道防线，那么为解决该问题可以引入第二道防线——智能卡。2021 年，基于 RLWE 问题的困难性，Wang 等[74]利用 Alkim 等[75]提出的格上密钥交换方案首次提出了抗量子的双因子 PAKE 方案，该方案在随机预言机模型下是可证明安全的，且可以抵抗密钥重用攻击、信号泄露攻击和密钥不匹配攻击。

表 3 对比了非对称 PAKE 协议的性能。为对用户进行认证，Ding 等[66]、Gao 等[67]和 Li 等[54]的方案在服务器端存储了口令的哈希值，而舒琴等[68]、Feng 等[69]、Dabra 等[70]和 Ding 等[71]的方案在服务器端存储了与口令相关的验证器。相比之下，存储口令的验证器要比存储与口令直接相关的哈希值更加安全。Li 等[54]虽然也在服务器端存储了口令的哈希值，但他们提出了一种抗量子的口令哈希方案，因而提高了相应 PAKE 方案的安全性。Ding 等[66]、Gao 等[67]、Feng 等[69]方案的安全性是基于随机预言机的，本文在引言部分总结了使用随机预言机的潜在安全威胁。Dabra 等[70]、Ding 等[71]方案的安全性是基于 ROR 模型[76]的，Li 等[54]的非对称 PAKE 方案是基于标准模型的，这两类方案都避免了随机预言机的使用，因而具有更高的实际安全性。舒琴等[68]的方案在 UC 模型下仍然是可证明安全的，在表 3 所有的协议中具有更强的实际安全性。

Feng 等[69]、Dabra 等[70]和 Ding 等[72]的匿名非对称 PAKE 方案使用户可以在不公开个人身份信息的前提下进行身份认证和密钥交换，因而保护了用户的个人隐私。Feng 等[69]的方案不能抵抗信号泄露攻击，Dabra 等[70]的方案在主密钥重用的情况下也不能抵抗此类攻击，而 Ding 等[72]的方案在主密钥重用的情况下依然可以抵抗此类攻击。

3　基于格的三方 PAKE 协议

现有格上 PAKE 协议的研究多针对两方应用场景，即多为两方 PAKE 协议，此类方案要求每 2 个用户之间都共享一个口令或口令的哈希值等，因而此类方案在应用于大规模通信系统时会产生繁重的口令管理问题。另一方面，由于人脑的记忆能力有限，用户可记忆口令的数目和长度有限，一般只能记忆 5~7 个短的、低熵的口令[77]；若用户重复使用口令，将带来严重的安全问题。三方 PAKE 协议可以有效解决该问题，其典型应用场景如图 2 所示。协议参与方包括多个用户和一个认证服务器，每个用户只需要与可信服务器共享一个口令，就可以实现与任意其他用户（同样与可信服务器共享口令的用户）进行身份认证与密钥交换。

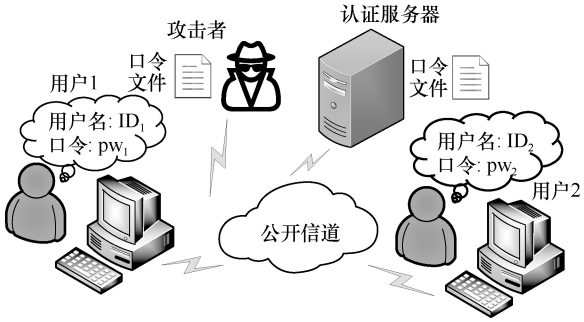

图 2　三方 PAKE 协议的典型应用场景

虽然存在通用的技术可以基于两方 PAKE 协议实现三方 PAKE 协议[76]，但会增加协议的通信轮（次），并且无法实现显式认证。因此，2013 年，叶茂等[78]

表 3　非对称 PAKE 协议的性能对比

协议名称	服务器端认证数据类型	口令哈希函数是否抗量子	困难问题	信号泄露攻击		匿名性	安全模型
				主密钥不重用	主密钥重用		
文献[66]	口令的哈希值	×	RLWE	—	—	×	随机预言机
文献[67]	口令的哈希值	×	RLWE	—	—	×	随机预言机
文献[68]	验证器/令牌	×	RLWE	—	—	×	UC 模型
文献[54]	口令的哈希值	√	LWE	—	—	×	标准模型
文献[69]	验证器/令牌	×	RLWE	×	×	√	随机预言机
文献[70]	验证器/令牌	×	RLWE	√	×	√	ROR 模型[78]
文献[71]	验证器/令牌	×	RLWE	√	√	√	ROR 模型[78]

在 JG/GK[12-13]架构的基础上，首次提出了基于格的三方 PAKE 协议，并在标准模型下证明了协议的安全性。在该协议中，每个用户与认证服务器都可以在 3 轮通信内实现显式的互认证。2017 年，Xu 等[79]基于 RLWE 问题，在随机预言机模型下提出了一种格上的三方 PAKE 协议，并严格证明了协议的安全性；与叶茂等[78]的方案相比，该方案的通信轮（次）更多，但由于环上的运算可以通过快速傅里叶变换加速，因此该协议具有较小的计算开销。2018 年，于金霞等[80]利用 Zhang 等[57]提出的两方 PAKE 协议，提出了一种基于格的两轮三方 PAKE 协议，但未克服 Zhang 等[57]的方案仅能实现密钥传输的问题，因而用户所得到的会话密钥仅由服务器端确定。2020 年，Yin 等[81]提出了一种新的可证明安全的格上两轮三方 PAKE 协议，与于金霞等[80]的方案相比，该方案中的会话密钥由认证双方同时确定，提高了密钥协商的公平性。

表 4 对比了不同三方 PAKE 协议的性能。与 Abdalla 等[76]的传统三方 PAKE 协议相比，叶茂等[78]、于金霞等[80]、Xu 等[79]、Yin 等[81]的三方 PAKE 协议基于格上困难问题，因而可以抵抗量子攻击。此外，Abdalla 等[74]的方案使用了大整数模/幂运算，与格上的小整数向量/矩阵运算相比，开销较大。Xu 等[79]的三方 PAKE 协议不仅需要用户与可信服务器进行通信，还需要用户之间进行通信。相比之下，叶茂等[78]、于金霞等[80]和 Yin 等[81]的三方 PAKE 协议只需要用户与服务器进行通信就能实现身份认证与密钥交换。Xu 等[79]方案的优势是基于 RLWE 困难问题，因而计算开销较小。

叶茂等[78]的格上三方 PAKE 协议需要 3 轮通信，而于金霞等[80]和 Yin 等[81]的方案需要两轮通信，减小了协议的通信轮（次）。叶茂等[78]的三方 PAKE 协议的通信数据类型包括密文、投影密钥和消息认证码，该方案的密文复杂度、投影密钥大于尹安琪等[80]的三方 3PAKE 协议。Yin 等[81]、于金霞等[80]的三方 PAKE 协议采用了可拆分公钥加密体制，只需要验证密文有效性就可以实现 IND-CCA2 安全，避免了消息认证码的传输。Xu 等[79]、于金霞等[80]、Yin 等[81]的格上三方 PAKE 协议需要使用随机预言机，但叶茂等[78]的方案是基于标准模型的，因而安全性更高。

4 基于格的分布式 PAKE 协议

第 2 节和第 3 节中的 PAKE 协议都属于集中式认证方案，用户认证信息（口令、口令的哈希值或与口令相关的令牌）都存储在单个服务器上。若服务器端直接存储了口令，则 PAKE 协议将面临服务器泄露攻击的威胁；若在服务器端简单存储了口令的哈希值，则协议仍面临离线字典攻击的威胁。虽然在服务器端存储口令相关的验证器可以有效抵抗上述攻击，但相关研究成果较少。而敌手执行此类攻击的收益率很大，因为只需入侵存在安全漏洞的单个服务器，就有可能获取数以千万计的口令数据。例如在 2021 年，仅 RockYou2021 数据集就泄露了约 84 亿条口令记录。分布式认证为解决服务器端的口令泄露问题提供了另一种解决方案。

图 3 给出了分布式 PAKE 协议的典型应用场景。在一次协议执行中，参与方包括一个用户和多个认证服务器，其中用户持有口令，多个认证服务器分布式地存储口令份额，对用户的认证由多个认证服务器协同完成。敌手入侵部分服务器（一般是小于相应阈值数目的服务器）不会泄露口令的任何信息。目前，格上的相关研究成果较少。2021 年，Roy 等[82]通过基于格的秘密共享算法提出了格上首个分布式 PAKE 协议，该协议可以抵抗量子攻击和服务器攻击，但需要基于 PKI 模型，因而用户在进行认证时除了需要记忆口令外，还需要存储和管理系统公钥。Roy 等[82]的方案是一种阈值方案，不适用于服务器数目小于阈值的应用场景，如两服务器场景。2022 年，尹安琪等[83]通过设计基于格的两方 SPHF，提出了格上第一个两服务器 PAKE 协议，并

表 4 不同三方 PAKE 协议的性能对比

方案	抗量子	困难问题	通信轮数	计算类型	密钥交换	认证方式	安全模型	私钥
文献[75]	×	DH	4	大整数模/幂	√	隐式认证	ROR 模型	√
文献[78]	√	LWE	3	小整数向量/矩阵	√	显式互认证	标准模型	×
文献[79]	√	RLWE	3	小整数向量/矩阵	√	显式互认证	随机预言机	×
文献[80]	√	LWE	2	小整数向量/矩阵	×	显式互认证	随机预言机	×
文献[81]	√	LWE	2	小整数向量/矩阵	√	显式互认证	随机预言机	×

在标准模型下证明了该协议的安全性。该协议实现了唯口令设置，因而可部署性更强。目前，格上分布式 PAKE 协议的相关研究成果较少，对比之下，基于传统困难问题的分布式 PAKE 方案的研究成果相对丰富，大致可分为以下 3 类：基于 PKI 模型的方案[84-85]、基于身份的方案[86-87]和唯口令的方案[88]。在这 3 类方案中，除用户口令外，前两类分别需要用户管理系统公钥和服务器身份等信息。

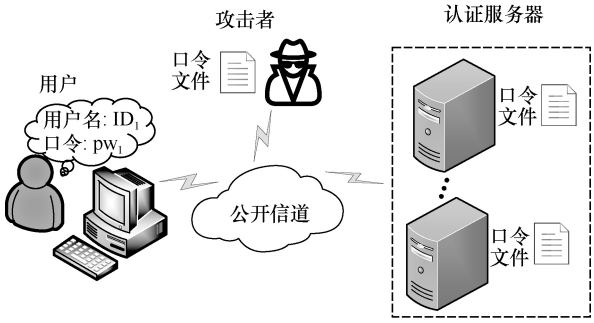

图 3　分布式 PAKE 协议的典型应用场景

表 5 给出了不同分布式 PAKE 协议的性能对比。Katz 等[89]、Yi 等[86]、Yi 等[87]和 Raimondo 等[88]的协议基于 DDH 困难问题，无法抵抗量子攻击；Roy 等[82]和尹安琪等[83]的分布式 PAKE 协议基于格上的困难问题，可以抵抗量子攻击。

Roy 等[82]的方案基于 PKI 模型，用户在进行身份认证时除了需要记忆口令外，还需要存储服务器公钥；Yi 等[86]、Yi 等[87]的方案是基于身份的，用户需要额外管理服务器身份信息；Katz 等[89]、Raimondo 等[88]和尹安琪等[83]的方案实现了唯口令设置，因而其所对应的安全系统具有更强的可部署性。Katz 等[89]、Yi 等[86]、Yi 等[87]和尹安琪等[83]的分布式 PAKE 方案是两服务器认证方案，适合两服务器应用场景；Roy 等[82]、Raimondo 等[88]的分布式 PAKE 协议是阈值方案，适合服务器数目大于相应阈值的应用场景。

在用户和服务器之间，Katz 等[89]、Yi 等[87]、Roy 等[82]和 Raimondo 等[88]的方案需要 3 轮通信，Yi 等[86]的方案需要两轮通信，尹安琪等[83]的协议则需要一轮通信，通信轮（次）不断得到优化。多服务器 PAKE 方案[82,88]与两服务器 PAKE 方案[83,86-87,89]相比一般需要更多的通信次数。在表 5 的协议中，除尹安琪等[83]的协议外，其他协议[82,86-89]都需要使用签名/验签算法。Raimondo 等[88]、Katz 等[89]和尹安琪等[83]（被动敌手攻击下的协议）避免了零知识证明的使用，有助于协议性能的提升；此外，Roy 等[82]的方案在每次协议执行时都需要多次使用秘密共享算法，这会进一步增加协议各方案的开销。

在 Roy 等[82]的协议中，会话密钥由一方确定，相比之下，表 5 中其他方案[83,86-88]的会话密钥由认证双方同时确定，这使密钥协商更加公平。Yi 等[86]、Yi 等[87]的协议是否需要使用随机预言机取决于其所基于的密码学原语，而 Katz 等[89]、Raimondo 等[88]、Roy 等[82]和尹安琪等[83]的协议基于标准模型，所以直接避免了随机预言机的使用。

5　未来研究方向

根据以上分析可知，现阶段格上 PAKE 协议的研究已经取得了一定的成果。但由于起步较晚且投入相对不足，现有格上 PAKE 协议的相关技术还存在诸多局限性，也面临许多挑战，在未来的研究工作中，可以更多地关注以下几个方面。

1) 量子随机预言机模型（QROM, quantum random oracle model）中可证明安全的 PAKE 方案。

表 5　　**不同分布式 PAKE 协议的性能对比**

方案		量子攻击	唯口令	密码学原语		服务器数目	通信轮(次)数	随机预言机	密钥协商方式
				签名/验签	SS-NIZK				
文献[82]		√	×	√	√	N	3(6N)	×	密钥传输
文献[83]	被动	√	√	×	×	2	1(4)	×	密钥交换
	主动	√	√	×	√	2	1(4)	×	密钥交换
文献[86]		×	×	√	√	2	2(4)	—	密钥传输
文献[87]		×	×	√	√	2	3(6)	—	密钥传输
文献[88]		×	√	√	×	N	3(6N)	×	密钥交换
文献[89]		×	√	√	×	2	3(6)	×	密钥交换

基于 ROM 的方案与基于标准模型的方案相比，一般在执行效率上具有显著优势。目前，基于 ROM 的格 PAKE 方案在证明安全性时一般只考虑具有经典访问权限的敌手，但相关方案被实例化后，随机预言机也被具体的哈希函数替代，此时量子敌手可以对随机预言机进行量子访问——QROM。因此，在经典 ROM 下，可证明安全的方案可能无法抵抗量子敌手的攻击。而在 QROM 下证明方案的安全性比在经典模型下更加困难：一是量子敌手可以在输入的指数叠加上查询随机预言机，因而在 QROM 下高效地模拟随机预言机是困难的；二是经典的 ROM 证明技术对 QROM 来说并不适用。因此，为保证格 PAKE 方案的高效性和安全性，需要研究在 QROM 中可证明安全的相关方案。

2) 基于格的分布式口令更新方案。在基于口令的相关方案中，口令更新是一个基本的且重要的问题。但据本文所知，目前还不存在基于格的分布式口令更新方案。Raimondo 等[88]提出了基于传统困难问题的门限口令更新方案，但无法抵抗量子攻击。虽然存在基于格的成熟技术可以解决单服务器设置下的口令更新问题[69]，但利用此类方案无法直接构造分布式口令更新方案：一是在两服务器或多服务器设置下，存在 2 个或多个服务器身份（在单服务器设置下，只有一个服务器身份）；二是此时服务器并不存储用户口令的哈希值。因此，设计实现基于格的分布式口令更新方案，从而使基于口令的分布式身份认证系统的功能更加完善，是一个有挑战且有重要现实意义的研究方向。

3) 基于格的口令哈希方案。口令哈希方案是构造非对称 PAKE 方案的重要数学组件。口令哈希方案可以对口令进行哈希处理，并将其与用户名等其他重要信息一起存储在服务器上，以便在用户端登录时服务器可以验证用户端注册的口令[54]。当前的口令哈希函数要么基于经典 ROM，因而不具备 QROM 下的可证明安全性；要么基于传统困难问题，无法抵抗量子攻击。据本文所知，目前格上只存在一种标准模型下的口令哈希方案[54]，该方案在计算效率上还存在优化空间。若要使格上 PAKE 方案更加安全实用，一是可以在 QROM 下构造高效的（或在标准模型下构造更加有效的）格上口令哈希方案，二是要使方案能够满足口令隐藏性、保熵性、预哈希保熵性，且能抵抗原像攻击、二次原像攻击等。鉴于工业领域中非对称 PAKE 协议应用的广泛性，基于格的口令哈希方案是一个具有重要现实意义的研究方向。

6 结束语

基于格的 PAKE 协议可以抵抗量子攻击，不存在高熵密钥的管理问题，也不涉及用户不可撤销的隐私泄露问题，因而所对应的安全系统具有较强的可部署性。口令认证是应用最广泛的身份认证技术之一，而基于格的 PAKE 协议在后量子时代也将具有重要的意义。本文对现有的基于格的 PAKE 协议进行了研究综述，主要介绍了基于格的两方 PAKE 协议（包括对称和非对称 PAKE 协议）、三方 PAKE 协议和分布式 PAKE 协议，并分别对比了不同类型 PAKE 方案的安全性、通信轮（次）、认证方式等，最后展望了基于格的 PAKE 协议的未来研究方向。

参考文献：

[1] 汪定. 口令安全关键问题研究[D]. 北京: 北京大学, 2017.
WANG D. Research on key issues in password security[D]. Beijing: Peking University, 2017.

[2] 张效林, 谷大武, 张驰. 移动平台典型应用的身份认证问题研究[J]. 网络与信息安全学报, 2020, 6(6): 137-151.
ZHANG X L, GU D W, ZHANG C. Issues of identity verification of typical applications over mobile terminal platform[J]. Chinese Journal of Network and Information Security, 2020, 6(6): 137-151.

[3] 汪定, 邹云开, 陶义, 等. 基于循环神经网络和生成式对抗网络的口令猜测模型研究[J]. 计算机学报, 2021, 44(8): 1519-1534.
WANG D, ZOU Y K, TAO Y, et al. Password guessing based on recurrent neural networks and generative adversarial networks[J]. Chinese Journal of Computers, 2021, 44(8): 1519-1534.

[4] 郭宓文. 密码, 让百姓生活更安全[N]. 人民日报, 2021.
GUO B W. Password, let people live more secure[N]. The People's Daily, 2021.

[5] MIT Technology Review 2022 年"全球十大突破性技术"解读[J]. 中国科学基金, 2022(3): 432-446.
Interpretation of 2022 MIT technology review's top 10 breakthrough technologies[J]. Bulletin of National Natural Science Foundation of China, 2022(3): 432-446.

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

[7] WU T D. The secure remote password protocol[C]//Proceedings of Internet Society 1997 Symposium on Network and Distributed System Security. Piscataway: IEEE Press, 1997: 97-111.

[8] MACKENZIE P. The PAK suite: protocols for password-authenticated key exchange[R]. DIMACS Technical Report 2002-46, 2002.

[9] BOYKO V, MACKENZIE P, PATEL S. Provably secure password-authenticated key exchange using diffie-Hellman[C]// Advances in Cryptology — EUROCRYPT 2000. Berlin: Springer, 2000: 156-171.

[10] KATZ J, OSTROVSKY R, YUNG M. Efficient password-

authenticated key exchange using human-memorable passwords[C]// Lecture Notes in Computer Science. Berlin: Springer, 2001: 475-494.

[11] GENNARO R, LINDELL Y. A framework for password-based authenticated key exchange1[J]. ACM Transactions on Information and System Security (TISSEC), 2006, 9(2): 181-234.

[12] JIANG S, GONG G. Password based key exchange with mutual authentication[C]//International Workshop on Selected Areas in Cryptography. Berlin: Springer, 2004: 267-279.

[13] GROCE A, KATZ J. A new framework for efficient password-based authenticated key exchange[C]//Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM Press, 2010: 516-525.

[14] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1994: 124-134.

[15] ROSS O H M. A review of quantum-inspired metaheuristics: going from classical computers to real quantum computers[J]. IEEE Access, 2019, 8: 814-838.

[16] 牟雁飞. 基于格的数字签名和认证协议研究[D]. 上海: 复旦大学, 2014.
MOU Y F. Research in lattice-based digital signature and identification protocols[D]. Shanghai: Fudan University, 2014.

[17] 张彦华. 基于格的若干密码方案的设计与分析[D]. 西安: 西安电子科技大学, 2017.
ZHANG Y H. Design and analysis of several lattice-based cryptographic schemes[D]. Xi'an: Xidian University, 2017.

[18] MERKLE R C. Protocols for public key cryptosystems[C]// Proceedings of 1980 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 1980: 122.

[19] 宋永成, 黄欣沂, 伍玮, 等. 基于编码的数字签名综述[J]. 网络与信息安全学报, 2021, 7(4): 1-17.
SONG Y C, HUANG X Y, WU W, et al. Survey of code-based digital signatures[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 1-17.

[20] PATARIN J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms[C]// Advances in Cryptology — EUROCRYPT '96. Berlin: Springer, 1996: 33-48.

[21] NEJATOLLAHI H, DUTT N, RAY S, et al. Post-quantum lattice-based cryptography implementations[J]. ACM Computing Surveys, 2019, 51(6): 1-41.

[22] ASIF R. Post-quantum cryptosystems for Internet-of-things: a survey on lattice-based algorithms[J]. IoT, 2021, 2(1): 71-91.

[23] SEYHAN K, NGUYEN T N, AKLEYLEK S, et al. Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey[J]. Cluster Computing, 2022, 25(3): 1729-1748.

[24] ALAYA B, LAOUAMER L, MSILINI N. Homomorphic encryption systems statement: trends and challenges[J]. Computer Science Review, 2020, 36: 100235.

[25] ALAGIC G, ALPERIN-SHERIFF J, APON D, et al. Status report on the second round of the NIST post-quantum cryptography standardization process[R]. NIST, 2020.

[26] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2000: 139-155.

[27] BRESSON E, CHEVASSUT O, POINTCHEVAL D. Security proofs for an efficient password-based key exchange[C]//Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003: 241-250.

[28] MACKENZIE P, PATEL S, SWAMINATHAN R. Password-authenticated key exchange based on RSA[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2000: 599-613.

[29] ABDALLA M, BENHAMOUDA F, POINTCHEVAL D. Disjunctions for hash proof systems: New constructions and applications[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 69-100.

[30] ABDALLA M, CHEVALIER C, POINTCHEVAL D. Smooth projective hashing for conditionally extractable commitments[C]// Advances in Cryptology - CRYPTO 2009. Berlin: Springer, 2009: 671-689.

[31] BENHAMOUDA F, BLAZY O, CHEVALIER C, et al. New techniques for SPHFs and efficient one-round PAKE protocols[C]// Advances in Cryptology – CRYPTO 2013, Berlin: Springer, 2013: 449-475.

[32] CANETTI R, HALEVI S, KATZ J, et al. Universally composable password-based key exchange[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 404-421.

[33] KATZ J, VAIKUNTANATHAN V. Round-optimal password-based authenticated key exchange[C]//Theory of Cryptography. Berlin: Springer, 2011: 293-310.

[34] MITTELBACH A, FISCHLIN M. The theory of hash functions and random oracles[M]. Cham: Springer International Publishing, 2021.

[35] BONEH D, DAGDELEN Ö, FISCHLIN M, et al. Random oracles in a quantum world[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2011: 41-69.

[36] CHIESA A, MANOHAR P, SPOONER N. Succinct arguments in the quantum random oracle model[C]//Theory of Cryptography Conference. Berlin: Springer, 2019: 1-29.

[37] KATZ J, VAIKUNTANATHAN V. Smooth projective hashing and password-based authenticated key exchange from lattices[C]// Advances in Cryptology – ASIACRYPT 2009. Berlin: Springer, 2009: 636-652.

[38] WANG D, WANG P. On the implications of Zipf's law in passwords[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2016: 111-131.

[39] YANG K Y, HU X X, ZHANG Q H, et al. VAEPass: a lightweight passwords guessing model based on variational auto-encoder[J]. Computers & Security, 2022, 114: 102587.

[40] FUN T S, AHMEDY F, FOO Z M, et al. Enhanced password-based authentication mechanism in cloud computing with extended honey encryption (XHE): a case study on diabetes dataset[C]//Advances in Computer, Communication and Computational Sciences. Berlin: Springer, 2021: 65-74.

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

[42] BANERJEE A, PEIKERT C, ROSEN A. Pseudorandom functions and

lattices[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 719-737.

[43] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]//Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2008: 197-206.

[44] LI Z, WANG D. Two-round PAKE protocol over lattices without NIZK[C]//International Conference on Information Security and Cryptology. Berlin: Springer, 2018: 138-159.

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

[46] 叶茂. 基于格的口令认证密钥交换协议和相关加密算法研究[D]. 郑州: 信息工程大学, 2013.
YE M. Research on password-based authenticated key exchange protocols and associated encryption algorithms from lattices[D]. Zhengzhou: Information Engineering University, 2013.

[47] CRAMER R, SHOUP V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2002: 45-64.

[48] BENHAMOUDA F, BLAZY O, DUCAS L, et al. Hash proof systems over lattices revisited[C]//IACR International Workshop on Public Key Cryptography. Berlin: Springer, 2018: 644-674.

[49] BELLARE M, ROGAWAY P. Entity authentication and key distribution[C]//Annual International Cryptology Conference. Berlin: Springer, 1993: 232-249.

[50] BELLARE M, ROGAWAY P. Provably secure session key distribution: the three party case[C]//Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1995: 57-66.

[51] BLAKE-WILSON S, JOHNSON D, MENEZES A. Key agreement protocols and their security analysis[C]//Crytography and Coding. Berlin: Springer, 1997: 30-45.

[52] MACKENZIE P. Secure network authentication with password identification[R]. IEEE P1363 Working Group, 1999.

[53] GUO Y M, ZHANG Z F, GUO Y J. Anonymous authenticated key agreement and group proof protocol for wearable computing[J]. IEEE Transactions on Mobile Computing, 2022, 21(8): 2718-2731.

[54] LI Z P, WANG D, MORAIS E. Quantum-safe round-optimal password authentication for mobile devices[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(3): 1885-1899.

[55] DING Y, FAN L. Efficient password-based authenticated key exchange from lattices[C]//Proceedings of 2011 Seventh International Conference on Computational Intelligence and Security. Piscataway: IEEE Press, 2011: 934-938.

[56] BLAZY O, CHEVALIER C, DUCAS L, et al. Exact smooth projective hash function based on LWE[J]. Cryptology ePrint Archive, 2013: 173107.

[57] ZHANG J, YU Y. Two-round PAKE from approximate SPH and instantiations from lattices[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2017: 37-67.

[58] ABDALLA M, BENHAMOUDA F, POINTCHEVAL D. Public-key encryption indistinguishable under plaintext-checkable attacks[J]. IET Information Security, 2016, 10(6): 288-303.

[59] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 700-718.

[60] 尹安琪, 曲彤洲, 郭渊博, 等. 格上基于密文标准语言的可证明安全两轮口令认证密钥交换协议[J]. 电子学报, 2022, 50(5): 1140-1149.
YIN A Q, QU T Z, GUO Y B, et al. Provably secure two-round PAKE based on ciphertext standard language over lattices[J]. Acta Electronica Sinica, 2022, 50(5): 1140-1149.

[61] LI Z P, WANG D. Achieving one-round password-based authenticated key exchange over lattices[J]. IEEE Transactions on Services Computing, 2022, 15(1): 308-321.

[62] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 1-23.

[63] 叶茂, 胡学先, 刘文芬. 基于理想格的近似平滑投射 Hash 函数[J]. 信息工程大学学报, 2013, 14(1): 13-21.
YE M, HU X X, LIU W F. Approximate smooth projective hash functions from ideal lattices[J]. Journal of Information Engineering University, 2013, 14(1): 13-21.

[64] ATANI R E, ATANI S E, KARBASI A H. A new ring-based SPHF and PAKE protocol on ideal lattices[J]. The ISC International Journal of Information Security, 2019, 11(1): 75-86.

[65] KATZ J, OSTROVSKY R, YUNG M. Efficient and secure authenticated key exchange using weak passwords[J]. Journal of the ACM, 2009, 57(1): 1-39.

[66] DING J, ALSAYIGH S, LANCRENON J, et al. Provably secure password authenticated key exchange based on RLWE for the post-quantum world[C]// Topics in Cryptology – CT-RSA 2017. Berlin: Springer, 2017: 183-204.

[67] GAO X, DING J, LIU J, et al. Post-quantum secure remote password protocol from RLWE problem[C]//International Conference on Information Security and Cryptology. Berlin: Springer, 2017: 99-116.

[68] 舒琴, 王圣宝, 路凡义, 等. 基于理想格的通用可组合两方口令认证密钥交换协议[J]. 电子与信息学报, 2021, 43(6): 1756-1763.
SHU Q, WANG S B, LU F Y, et al. Universally composable two-party password-based authenticated key exchange from ideal lattices[J]. Journal of Electronics & Information Technology, 2021, 43(6): 1756-1763.

[69] FENG Q, HE D B, ZEADALLY S, et al. Ideal lattice-based anonymous authentication protocol for mobile devices[J]. IEEE Systems Journal, 2019, 13(3): 2775-2785.

[70] DABRA V, BALA A J, KUMARI S. LBA-PAKE: lattice-based anonymous password authenticated key exchange for mobile devices[J]. IEEE Systems Journal, 2021, 15(4): 5067-5077.

[71] DING J, SARASWATHY R, ALSAYIGH S, et al. How to validate the secret of a ring learning with errors (RLWE) key[J]. Cryptology ePrint Archive, 2018: 2018/081.

[72] DING R Y, CHENG C, QIN Y. Further analysis and improvements of a lattice-based anonymous PAKE scheme[J]. IEEE Systems Journal, 2022, 16(3): 5035-5043.

[73] GAO X W, DING J T, LI L, et al. Practical randomized RLWE-based key exchange against signal leakage attack[J]. IEEE Transactions on Computers, 2018, 67(11): 1584-1593.

[74] WANG Q X, WANG D, CHENG C, et al. Quantum2FA: efficient quantum-resistant two-factor authentication scheme for mobile devices[J]. IEEE Transactions on Dependable and Secure Computing, 2021, doi: 10.1109/TDSC.2021.3129512.

[75] ABDALLA M, FOUQUE P A, POINTCHEVAL D. Password-based authenticated key exchange in the three-party setting[C]// Public Key Cryptography - PKC 2005. Berlin: Springer, 2005: 65-84.

[76] ALKIM E, DUCAS L, PöPPELMANN T, et al. NewHope without reconciliation[J]. Cryptology ePrint Archive, 2016: 2016/1157.

[77] KEITH M, SHAO B, STEINBART P J. The usability of passphrases for authentication: an empirical field study[J]. International Journal of Human-Computer Studies, 2007, 65(1): 17-28.

[78] 叶茂, 胡学先, 刘文芬. 基于格的三方口令认证密钥交换协议[J]. 电子与信息学报, 2013, 35(6): 1376-1381.
YE M, HU X X, LIU W F. Password authenticated key exchange protocol in the three party setting based on lattices[J]. Journal of Electronics & Information Technology, 2013, 35(6): 1376-1381.

[79] XU D, HE D, CHOO K-K R, et al. Provably secure three-party password authenticated key exchange protocol based on ring learning with error[J]. Cryptology ePrint Archive, 2017: 173311.

[80] 于金霞, 廉欢欢, 汤永利, 等. 格上基于口令的三方认证密钥交换协议[J]. 通信学报, 2018, 39(11): 87-97.
YU J X, LIAN H H, TANG Y L, et al. Password-based three-party authenticated key exchange protocol from lattices[J]. Journal on Communications, 2018, 39(11): 87-97.

[81] YIN A Q, GUO Y B, SONG Y M, et al. Two-round password-based authenticated key exchange from lattices[J]. Wireless Communications and Mobile Computing, 2020, 2020: 8893628.

[82] ROY P S, DUTTA S, SUSILO W, et al. Password protected secret sharing from lattices[C]//International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2021: 442-459.

[83] 尹安琪, 郭渊博, 汪定, 等. 可证明安全的抗量子两服务器口令认证密钥交换协议[J]. 通信学报, 2022, 43(3): 14-29.
YIN A Q, GUO Y B, WANG D, et al. Provably secure quantum resistance two-server password-authenticated key exchange protocol[J]. Journal on Communications, 2022, 43(3): 14-29.

[84] GONG L, LOMAS M A, NEEDHAM R M, et al. Protecting poorly chosen secrets from guessing attacks[J]. IEEE Journal on Selected Areas in Communications, 1993, 11(5): 648-656.

[85] HALEVI S, KRAWCZYK H. Public-key cryptography and password protocols[J]. ACM Transactions on Information and System Security, 1999, 2(3): 230-268.

[86] YI X, HAO F, BERTINO E. ID-based two-server password-authenticated key exchange[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2014: 257-276.

[87] YI X, RAO F Y, TARI Z, et al. ID2S password-authenticated key exchange protocols[J]. IEEE Transactions on Computers, 2016, 65(12): 3687-3701.

[88] RAIMONDO D M, GENNARO R. Provably secure threshold password-authenticated key exchange[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2003: 507-523.

[89] KATZ J, MACKENZIE P, TABAN G, et al. Two-server password-only authenticated key exchange[C]//International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2005: 1-16.

[作者简介]

郭渊博（1975− ），男，陕西周至人，博士，信息工程大学教授、博士生导师，主要研究方向为网络空间安全、数据挖掘、机器学习和人工智能安全等。

尹安琪（1995− ），女，山东临沂人，信息工程大学博士生，主要研究方向为安全协议设计及格密码理论。