专题: 量子信息处理

量子身份认证研究进展*

王兴福[1)] 郑艳艳[2)†] 顾世浦[3)] 张琦[1)] 钟伟[4)] 杜明明[3)]
李喜云[1)] 沈淑婷[3)] 张安蕾[1)] 周澜[1)] 盛宇波[3)‡]

1) (南京邮电大学理学院, 南京 210023)

2) (延安大学物理与电子信息学院, 延安 716000)

3) (南京邮电大学电子与光学工程学院、柔性电子 (未来技术) 学院, 南京 210023)

4) (南京邮电大学通信与信息工程学院, 南京 210003)

(2025 年 7 月 12 日收到; 2025 年 9 月 5 日收到修改稿)

量子通信具有感知窃听的功能, 这是其区别于经典通信而独有的优势, 能够为信息安全提供新的保障. 在实际应用中, 量子通信具有绝对安全性的前提是所有通信方均是合法通信方, 然而, 这在实际通信环境中难以保证, 为量子保密通信带来安全性隐患. 因此, 在通信之前对通信方进行身份认证具有重要意义. 量子身份认证利用量子力学基本原理在通信方之间实现单向或双向身份认证, 并能确保身份认证码的绝对安全, 在量子通信领域具有重要的研究价值. 本文系统地梳理了量子身份认证协议的研究历程, 根据所需的不同量子资源对基于单光子、纠缠态、连续变量、混合型变量的量子身份认证协议进行介绍, 又根据身份认证过程中使用的量子协议类型, 介绍了基于量子密钥分发、量子安全直接通信、量子隐形传态以及乒乓协议框架的量子身份认证协议, 并分析各类协议在效率、安全性及实用化方面的优缺点. 最后, 详细地介绍了最新的量子身份认证协议——基于 GHZ 态的多方同步身份认证协议以及具有身份认证功能的极化-空间超编码的三方量子安全直接通信协议, 并对量子身份认证的未来发展方向以及在量子通信领域的应用潜力进行展望. 本综述可为未来量子身份认证的实用化发展提供理论支持.

关键词: 量子身份认证, 量子保密通信, 量子纠缠

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.7498/aps.74.20250920

CSTR: 32037.14.aps.74.20250920

1 引 言

在数字化浪潮中, 信息交互的广泛性与复杂性对信息安全体系提出了更高要求. 传统公钥密码学依赖大整数分解或离散对数等难题构建的安全屏障[1–3], 正面临量子计算的巨大冲击. 量子计算机通过量子并行性与 Shor 算法[4] 等机制, 可在短时间内破解经典加密体系, 使得金融交易、政务通信、医疗数据等核心领域的信息防护体系面临系统性风险. 在此背景下, 量子通信依托量子态叠加、量子纠缠、量子不可克隆原理、不确定性原理等量子力学的基本原理[5,6], 为构建新型安全通信提供了理论根基. 量子通信包含量子密钥分发 (quantum key distribution, QKD)[7–9]、量子隐形传态 (quantum teleportation, QT)[10–13]、量子秘密共享 (quantum secret sharing, QSS)[14–17]、量子安全直接通信 (quantum secure direct communication,

* 国家自然科学基金 (批准号: 12175106, 92365110) 资助的课题.

† 通信作者. E-mail: yyz@yau.edu.cn

‡ 通信作者. E-mail: shengyb@njupt.edu.cn

QSDC)[18–20] 等重要分支, 理论上具有绝对安全性. 在过去三十年中, 量子通信技术在理论和实验方面都取得了巨大进展[21–53]. 在实际操作中, 任何安全通信协议的成功实施都需要以身份认证为前提, 即必须事先检验实际通信方的身份是否合法. 只有合法的通信方之间才能进一步进行通信. 因此, 构建量子安全认证体系已成为量子保密通信研究的重要课题之一.

量子身份认证 (quantum identity authentication, QIA) 是量子认证的一个重要分支. QIA 允许通信方基于量子力学的基本原理证明自己的身份, 并能确保身份认证码的绝对安全, 通常作为登录量子通信系统的第一步. QIA 是一种有效防止窃听者 (Eve) 在通信中冒充合法用户窃取传递的密钥和信息 (扮演攻击) 的方法. 只有当实际通信方均是合法用户时, 量子通信协议的无条件安全性才能得到保证[54–61]. 早期的 QKD 协议本质上考虑使用经典身份认证协议. 直到 1995 年, Crépeau 和 Salvail[62] 提出了首个基于不经意传输 (oblivious transfer, OT) 的协议. 在该协议提出之后, 出现了一系列关于 QIA 的工作. 1998 年 Zeng 和 Wang[63] 提出了一种 QKD 协议, 该协议允许同时分发密钥和验证通信者的身份. 1999 年, Dušek 等[54] 结合经典识别过程和 QKD 协议提出了两种量子相互认证协议. 这些协议均是通过结合经典认证协议和 QKD 协议提出的, 特别强调一次性密码. 严格来说, 这些协议是混合型的协议. 在伴随量子通信技术的进步的同时, 量子身份认证协议也同步演变和发展.

从应用维度看, QIA 的价值贯穿国家战略至民生领域. 在国家安全层面, 有效防范敌对方的渗透与信息战攻击, 为军事指挥、外交密电、关键基础设施管控等场景提供身份核验保障; 在社会经济领域, 支撑金融系统的大额交易认证、智能电网的隐私数据交互以及电子政务的机密公文传输, 遏制诈骗与数据泄漏风险; 在公共服务方面, 保障远程医疗的诊疗信息安全、跨境物流的电子单证可信性, 推动数字化服务的高效落地; 对于个体用户而言, 其通过保护生物特征、财产账户等隐私数据, 构建了数字身份主权的新型防护范式. 因此, QIA 的研究具有重要的应用价值.

此外, 在许多前沿的多用户量子任务中, QIA 更是发挥着不可或缺的基础安全作用. 例如, 在量子群组密钥分发 (group QKD)[64] 中, 需要首先对所有组成员身份进行认证, 以确保生成的密钥在合法用户间安全共享; 在量子数字签名 (quantum digital signature, QDS)[65] 方案中, 签名方的身份真实性是防止伪造和抵赖的前提; 在基于量子安全多方计算 (quantum secure multi-party computing, QSMPC) 或量子区块链的共识机制中[66], 参与节点的身份认证是防止恶意节点入侵、确保计算与共识结果可信的关键一环; 在量子中继网络中, 对中继节点的身份认证更是构建可信量子通道的基础. 因此, 对 QIA 的研究是推动这些高级量子应用从理论走向实践的必经之路.

本文的其余部分组织如下. 第 2 节从使用的量子资源和量子协议两个方面对现有的 QIA 协议进行分类, 并着重介绍一些关注度高的 QIA 协议. 第 3 节介绍一个最新的 QIA 协议和具有身份认证功能的极化-空间超编码的三方量子安全直接通信协议. 最后, 第 4 节对 QIA 进行了总结和展望.

2 量子身份认证的分类

根据不同的标准可以对量子身份认证进行分类. 本文将从以下两个方面对量子身份认证进行分类介绍, 即根据 QIA 所使用的量子资源和所使用的量子协议. 由于文献数量众多, 我们只对一些代表性工作进行介绍, 有望能清晰地展现各类型协议的执行过程和使用场景.

2.1 根据量子资源分类

根据 QIA 协议中使用的核心量子资源类型, 将 QIA 协议分类如下: 基于单光子、纠缠态、连续变量 (continuous variable, CV) 和混合型变量的 QIA 协议.

2.1.1 基于单光子的协议

利用单光子 (极化光子、相位编码光子等) 作为核心资源, 通过量子态的测量或单粒子操作实现认证. 其特点是资源需求低, 兼容现有量子光学器件 (如单光子探测器); 实验实现简单, 适用于低资源环境 (如量子物联网). 协议的安全性依赖单光子的不可克隆性, 可能需结合经典加密增强.

2009 年 Zhang[67] 提出了一种仅需单光子操作的单向 QIA 协议, 首次引入经典公钥基础设施的

核心思想, 降低了实现复杂度. 2017 年 Hong 等[68]提出了一种单光子态编码优化 QIA 协议, 因为允许使用单个量子比特对两位认证密钥序列进行认证, 该协议对资源的需求相对较低, 并且效率较高. Zawadzki[69] 在 2019 年指出 Hong 等的 QIA 协议存在安全缺陷, 并对该协议提出了改进, 通过哈希函数与动态会话密钥, 进行编码优化与流程精简. 后来在 2021 年 González-Guillén 等[70] 指出 Zawadzki 的协议容易受到密钥空间缩减攻击, 并设计首个针对哈希-量子混合认证协议的攻击策略, 通过实验验证密钥空间几何缩减效应. 有趣的是, Calsi 和 Kohl[71] 在 2024 年再次指出 Hong 等的 QIA 协议存在一个额外漏洞, 该漏洞源于诱骗态生成与管理策略的缺陷, 并展示了一个能有效解决该问题的简易缓解协议. 对已提出的协议, 分析其漏洞, 并设计出无此漏洞的改进协议, 这种密码分析过程在密码学领域非常普遍, 也可视为推动 QIA 发展的一个典型例子. 2023 年 Rao 和 Jayaraman[72] 提出了一种保留预共享密钥信息的新型 QIA 协议, 仅使用单光子与经典信道完成双向认证, 通过动态基矢生成与相位反冲检测, 显著降低预共享密钥泄漏风险.

简述 Rao 和 Jayaraman[72] 的 QIA 协议如下.

步骤 1 协议初始化. Alice 和 Bob 预先共享 n 位密钥 $K=\{k_1,k_2,\cdots,k_n\}$, Alice 随机选择起始位置 i 和距离 r ($1\leqslant i,\ r\leqslant n$), 认证密钥长度 $m=10\%\times n$. Alice 通过经典信道向 Bob 发送 $(i,\ r)$, Bob 随机生成认证密钥 $B_K=\{B_{k1},B_{k2},\cdots,B_{kn}\}$, 两个诱骗态序列 D_{AK}, D_{BK}.

步骤 2 Bob 量子通信阶段. Bob 基于预共享密钥动态生成基矢: $x_t=k_{i-r}\oplus k_{i+r}$, $y_t=k_{i-r}\oplus k_i$, $z_t=k_i\oplus k_{i+r}$ ($t\leqslant m$). 若 $x_t=0$, Bob 将量子态编码为 $|0\rangle$ 或 $|1\rangle$; 若 $x_t=1$, 则编码为 $|+\rangle$ 或 $|-\rangle$. 分别用基矢 y_t 和 z_t 编码诱骗态 D_{AK} 和 D_{BK}. 将序列 QB_{kt}, $QD_{\mathrm{A}kt}$ 和 $QD_{\mathrm{B}kt}$ 通过量子信道发送给 Alice. Alice 使用相同规则生成 x_t, y_t, z_t, 并分别测量 QB_{kt}, $QD_{\mathrm{A}kt}$, $QD_{\mathrm{B}kt}$, 对应存储 B'_{kt}, $D'_{\mathrm{A}kt}$, $D'_{\mathrm{B}kt}$.

步骤 3 诱骗态验证. Alice 公布诱骗态, 通过经典信道发送 D'_{AK} 给 Bob. 比较 D'_{AK} 与 Bob 的原始 D_{AK}, 若错误率大于 QBER, 终止协议, 否则继续.

步骤 4 Alice 量子通信阶段. Alice 随机生成认证密钥 $A_K=\{A_{k1},A_{k2},\cdots,A_{kn}\}$, 动态生成基矢 $D'_{\mathrm{B}kt}\oplus B'_{kt}$, 并用该基矢编码 A_{kt} 为 QA_{kt}, 发送给 Bob. Bob 用相同基矢 $D_{\mathrm{B}kt}\oplus B_{kt}$ 测量 QA_{kt}, 并存储 A'_{kt}.

步骤 5 经典信道身份认证. Alice 公布 A_K, Bob 公布 B_K, 交叉验证是否满足 $A_K=A'_K$ 且 $B_K=B'_K$. 若匹配, 身份认证成功, 进行安全通信; 若不匹配, 则终止协议并重启.

从以上协议可以看出, 协议利用单光子的极化特性进行编码和测量, 强调实用性与效率, 但存在密钥管理漏洞.

2.1.2 基于量子纠缠的 QIA 协议

此类 QIA 协议使用量子纠缠作为核心资源, 通过纠缠特性 (如非局域关联性、不可分割性) 来保障安全性. 其特点是需高精度制备和维持多粒子纠缠态, 实验复杂度较高; 适用于需要高安全性的长距离或多方身份认证场景.

Zeng 和 Zhang[55] 在 2000 年提出了一种基于贝尔态的 QIA 协议. 该协议是量子密码学中首个身份验证与密钥分发一体化协议, 密钥分发通过之前的 Einstein-Podolsky-Rosen(EPR)QKD 协议实现, 身份认证过程通过对称密码协议实现. 尽管受限于当时的量子存储技术, 但其设计思想为后续无信任中心的 QIA 协议奠定了基础. 2006 年, Lee 等[73]提出了利用第三方 Trent 生成 Greenberger-Horne-Zeilinger(GHZ) 态, 执行用户身份认证的 QIA 协议, 首次将用户认证与消息传输结合. 发送方 Alice 无需同接收方 Bob 预先共享密钥, 可以直接向 Bob 发送秘密消息, 且无需 Alice 与 Bob 间的直接量子信道, 适用于受限网络环境. 有趣的是, 在 2007 年 Zhang 等[74] 认为 Lee 的协议假设 Trent 完全可信且不窃取秘密信息, 但未限制 Trent 获取消息的能力. Trent 可通过拦截-测量-重发攻击和单量子比特测量攻击窃取消息, 因此协议存在安全漏洞. 他们将原协议中的比特翻转操作 X 替换为泡利 Z 操作 (相位翻转), 这样的改进不影响计算基的测量结果, 也不破坏协议功能, 但改变叠加态的相位, 使得 Trent 无法通过简单操作还原编码信息.

2014 年, Chang 等[75] 提出了一种基于五粒子团簇态和量子一次性密码的受控量子安全直接通信协议, 旨在实现多方权限控制与高效信息传输. 协议中, 光子 1, 2 用于信息编码, 光子 3, 5 供接收方 Bob 解密, 光子 4 作为控制器 Charlie 的权限标

识. 通过动态酉操作 (I/U) 调制光子 4 的状态 (依据 Bob 的身份码), 确保控制器无法独立获取明文.

2020 年, Zhang 等[76] 提出了一种基于贝尔态和纠缠交换的 QIA 协议, 旨在解决传统协议中存在的第三方信任问题与单向认证局限. 引入半诚实第三方 Charlie 负责制备贝尔态、分发粒子并验证结果, 但无法获取用户的共享密钥. 区别于传统协议中完全可信或不可信的第三方, Charlie 不参与密钥相关操作, 显著降低其窃取密钥的可能性, 支持双向认证且无需用户间额外通信, 效率更高. 2023 年, Dutta 和 Pathak[77] 提出了一种融合受控量子通信与 Bell 态操控技术的 QIA 协议, 在资源效率、安全性和功能性上均优于部分经典协议. 其核心创新在于双向认证机制、第三方半诚实假设下的鲁棒性, 以及对低复杂度量子资源的有效利用, 同时可抵御多种量子攻击.

简述 Zeng 和 Zhang[55] 的 QIA 协议如下.

步骤 1 初始阶段 (通过可信中心建立共享密钥 K_1). Alice 和 Bob 向可信信息中心 (TIC) 注册身份标识 $\mathrm{ID_A}$ 和 $\mathrm{ID_B}$, TIC 分别与 Alice 和 Bob 建立量子信道. TIC 制备两个单态 EPR 对, 可表示为

$$|\Phi_{\mathrm{ac}}\rangle = \sqrt{\frac{1}{2}}\left(|\uparrow_{\mathrm{a}}\downarrow_{\mathrm{c}}\rangle - |\downarrow_{\mathrm{a}}\uparrow_{\mathrm{c}}\rangle\right),$$

$$|\Phi_{\mathrm{bc}}\rangle = \sqrt{\frac{1}{2}}\left(|\uparrow_{\mathrm{b}}\downarrow_{\mathrm{c}}\rangle - |\downarrow_{\mathrm{b}}\uparrow_{\mathrm{c}}\rangle\right),$$

也可写为

$$|\Phi_{\mathrm{ac}}\rangle = \sqrt{\frac{1}{2}}\left(|\nearrow_{\mathrm{a}}\searrow_{\mathrm{c}}\rangle - |\searrow_{\mathrm{a}}\nearrow_{\mathrm{c}}\rangle\right),$$

$$|\Phi_{\mathrm{bc}}\rangle = \sqrt{\frac{1}{2}}\left(|\nearrow_{\mathrm{b}}\searrow_{\mathrm{c}}\rangle - |\searrow_{\mathrm{b}}\nearrow_{\mathrm{c}}\rangle\right).$$

其中, $|\uparrow\rangle$, $|\downarrow\rangle$ 是 $\hat{S}_z$ 的本征态, $|\nearrow\rangle$, $|\searrow\rangle$ 是 $\hat{S}_x$ 的本征态. TIC 发送粒子 a 给 Alice, 粒子 b 给 Bob, 自己保留粒子 c. Alice 和 Bob 独立随机选择测量基 ($\hat{S}_z$ 或 $\hat{S}_x$) 测量各自粒子. 测量后, 粒子处于四个态 $|\uparrow\rangle$, $|\downarrow\rangle$, $|\nearrow\rangle$, $|\searrow\rangle$ 之一. TIC 对剩余粒子进行总自旋测量, 若结果 $s=1$, 则丢弃; 若结果 $s=0$, 则保留, 说明粒子处于单态, Alice 和 Bob 的结果必然相反. Alice 和 Bob 公布测量基, 但不公布结果. 若使用相同基, 测量结果相反, 转换为密钥比特; 若使用不同基, 则丢弃结果. 最终生成共享密钥 K_1. 该过程中 TIC 无法获取 K_1, 因为投影测量 $s=0$ 不泄漏信息.

步骤 2 验证阶段 (身份验证+新密钥分发). 将密钥 K_1 转换为测量基序列 M_{K1}, 可约定密钥 0 对应直角基, 密钥 1 对应对角基, 或者反过来 (如 $K_1=001101$, $M_{K1}=\odot\odot\oplus\oplus\odot\oplus$). Alice 制备 EPR 对为四个贝尔态之一, 如 ($|\psi_{\mathrm{ab}}\rangle=\sqrt{1/2}(|\uparrow_{\mathrm{a}}\downarrow_{\mathrm{b}}\rangle - |\downarrow_{\mathrm{a}}\uparrow_{\mathrm{b}}\rangle)$), 保留粒子 a, 发送粒子 b 给 Bob. Alice 随机选择基测量粒子 a, 则 Bob 粒子 b 的状态发生塌缩. Bob 对粒子 b 进行两种基测量: 身份验证基 M_{K1}(由 K_1 确定的固定基) 和密钥分发基 M(随机选择, 用于生成新密钥). Bob 将 M_{K1} 基的测量结果 m 和位置编号 N_{i} 用 K_1 加密后, 发送密文 y 给 Alice. Alice 用 K_1 解密, 比对自身测量结果: 若匹配, 则 Bob 身份真实. Alice 将解密结果 m'发送给 Bob 验证, 若 $m'=m$, 则 Alice 身份真实. 身份验证通过后, 双方用剩余粒子 (M 基测量结果) 执行标准 EPR 协议, 生成新密钥 K. 丢弃旧共享密钥 K_1, 从新密钥 K 中提取部分比特作为下次共享密钥 K_2.

2.1.3 基于连续变量的 QIA 协议

此类 QIA 协议利用 CV 量子态 (如压缩态、相干态) 的统计特性或纠缠特性实现身份认证. 其特点是利用光场的连续参数 (如相位、振幅) 编码信息, 在短距离城域网中效率优于离散变量协议. 同时, 此类协议的实验复杂度较低 (无需单光子探测), 但需高精度调制技术. 适用于光纤量子通信网络中的高效身份认证和与经典光通信系统融合的混合量子网络.

2016 年, Ma 等[78] 首次将 CV 量子态引入身份认证框架, 提出了一种基于 CV 的 QIA 协议. 该协议利用双模压缩态与相干态实现用户身份的动态验证与密钥更新. 有趣的是, 在相对较短的距离内, CV QKD 协议比其离散变量 QKD 协议表现更好[79–81]. 因此, 对于城域网, 配备 CV QIA 的 CV QKD 有望实现更高效安全的密钥分发. 2024 年, Chen 等[82] 提出了一种基于 CV 系统的双向 QIA 协议, 利用双模压缩光场的纠缠特性实现合法用户间的相互身份验证. 通过引入诱骗态序列与参数 F (表征纠缠度), 协议不仅能够抵御高斯克隆攻击, 还可实时检测窃听者的存在, 为量子通信网络中的身份认证提供了高安全性的解决协议. 比较而言, Ma 等[78] 的协议需要贝尔态测量与位移操作, 实验复杂度较高, 而后者依赖双模压缩态的直接传输, 实验复杂度较低.

简述 Ma 等[78] 的 QIA 协议如下.

Alice 和 Bob 预先共享初始认证密钥 $K_{\rm a}$. Alice 对两个初始真空态 $|0\rangle$ 应用双模压缩算子, 生成两个纠缠模 $\hat{a}_1$ 和 $\hat{a}_2$, 并将 $\hat{a}_2$ 发送给 Bob. Alice 将二进制初始密钥 $K_{\rm a}$ 转换为十进制数 $k_{\rm a}$, 并随机选取两个十进制数 $y_{\rm a}$ 和 $z_{\rm a}$. Alice 分别对真空态应用位移算子 $\hat{D}(\alpha_3)$ 和 $\hat{D}(\alpha_{3\rm D})$, 获得两个分别在 $\hat{a}_3$ 模和 $\hat{a}_{3\rm D}$ 模的纠缠态, 分别用于密钥更新和身份认证. Alice 每次随机选择 $\hat{a}_3$ 或 $\hat{a}_{3\rm D}$ 与 $\hat{a}_1$ 进行联合贝尔态测量, 得到 $X_{\rm u}$ 和 $P_{\rm u}$, 并将其公开给 Bob. Bob 对 $\hat{a}_2$ 应用酉变换 $\hat{D}(u=\sqrt{2}(X_{\rm u}+{\rm i}P_{\rm u}))$, 随机选择基 ($X$ 或 P) 测量, 得到序列 ξ. Alice 公开诱骗态的时间区间, Bob 从 ξ 中提取诱骗态对应结果 $\xi_{3\rm D}$, 剩余为 ξ_3 (用于密钥更新). Bob 将二进制初始密钥 $K_{\rm a}$ 转为十进制数 k'_a, 计算 $z_{\rm b}=\xi_{3\rm D}-\varphi k'_{\rm a}$, 并公开. 通过定义保真度 $H=\langle[z_{\rm b}-\lambda z_{\rm a}]^2\rangle_{\rm min}$ 进行判断: 若 $H=0$, 则 Bob 身份合法, 无窃听; 若 $H>0$, 存在 Eve 或 Bob 非法, 通信中止. 身份验证通过后, Alice 和 Bob 从 ξ_3 提取新密钥 (与 $y_{\rm a}$ 相关).

2.1.4 基于混合型变量的 QIA 协议

基于混合型变量的 QIA 协议结合多种量子资源 (如单光子+纠缠态) 或量子与经典资源 (如哈希函数+量子态), 利用量子物理特性抵御量子攻击, 经典密码学增强协议的鲁棒性. 其特点是平衡资源效率与安全性, 降低对单一量子源的依赖. 然而, 此类协议需协调量子与经典操作的同步性, 可能引入新攻击. 此类 QIA 协议适用于资源受限的量子-经典混合网络 (如边缘计算节点) 和需要兼容现有密码学基础设施的过渡阶段应用.

2009 年, Liu 等[83] 提出了一种改进的确定性安全量子通信 (deterministic secure quantum communication, DSQC) 协议, 结合四量子比特簇态与单光子身份认证机制, 核心创新在于利用四维簇态的纠缠特性, 将每簇态的编码容量提升至 2 比特, 显著优化了经典信息的传输容量与协议安全性. 2020 年, Zhu 等[84] 通过融合身份认证与密钥协商 (quantum key agreement, QKA), 提出了一种无需纠缠的高效 QIA-QKA 协议. 该协议利用单光子编码+动态密钥更新, 实现量子与经典的结合. 传统协议将 QIA 与 QKA 分离, 导致资源冗余. 他们采用单光子编码及动态密钥更新机制, 仅需 2 轮通信, 复杂度低. 协议可抵抗中间人攻击、重放攻击、冒充攻击等, 并支持前向安全性 (动态密钥更新), 在安全性、效率和实用性上均优于传统协议. 另外, 2006 年 Wang 等[85] 提出混合 GHZ 态+经典哈希函数的协议和 2014 年 Yuan 等[86] 提出混合单粒子态+乒乓技术 (量子态动态传输) 的协议也可视为混合型协议.

简述 Liu 等[83] 的协议如下.

步骤 1 Alice 和 Bob 预先共享一个长度为 d 的二进制种子密钥 SK, 经扩展函数 G 生成长度为 k 的扩展密钥 EK, 要求 EK 满足随机性 (0 和 1 出现概率各为 1/2).

步骤 2 将 EK 均分为 Alice 身份密钥 $EK_{\rm A}$ 和 Bob 身份密钥 $EK_{\rm B}$. 进一步将分为基序列信息 $EK_{\rm A1}$ 和比特值序列信息 $EK_{\rm A2}$; $EK_{\rm B}$ 同理分割. 当 Alice 向 Bob 发送消息时, 使用 $EK_{\rm A}$ 认证 Alice 身份.

步骤 3 Alice 制备 N 个四粒子团簇态, 随机处于两个态之一

$$|\varphi\rangle=\frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{a_1a_2b_1b_2},$$

$$|\varphi'\rangle=\frac{1}{2}(|1001\rangle+|1010\rangle+|0101\rangle-|0110\rangle)_{a_1a_2b_1b_2}.$$

将序列命名为序列 $P=\{P_1(a_1,\ a_2),\ P_1(b_1,\ b_2),\ P_2(a_1,\ a_2),\ P_2(b_1,\ b_2),\ \cdots,\ P_{\rm N}(a_1,\ a_2),\ P_{\rm N}(b_1,\ b_2)\ \}$.

步骤 4 Alice 对每个团簇态的粒子 b_2 施加酉操作 I, σ_x, ${\rm i}\sigma_y$, σ_z. 原团簇态被转换为 8 种可能态之一

$$|\varphi_1\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{a_1a_2}|\varphi^+\rangle_{b_1b_2}+|11\rangle_{a_1a_2}|\varphi^-\rangle_{b_1b_2}\right),$$

$$|\varphi'_1\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}+|10\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}\right),$$

$$|\varphi_2\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}+|11\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}\right),$$

$$|\varphi'_2\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle_{a_1a_2}|\varphi^-\rangle_{b_1b_2}+|10\rangle_{a_1a_2}|\varphi^+\rangle_{b_1b_2}\right),$$

$$|\varphi_3\rangle=-\frac{1}{\sqrt{2}}\left(|00\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}+|11\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}\right)$$

$$|\varphi'_3\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle_{a_1a_2}|\varphi^+\rangle_{b_1b_2}+|10\rangle_{a_1a_2}|\varphi^-\rangle_{b_1b_2}\right),$$

$$|\varphi_4\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{a_1a_2}|\varphi^-\rangle_{b_1b_2}+|11\rangle_{a_1a_2}|\varphi^+\rangle_{b_1b_2}\right),$$

$$|\varphi'_4\rangle=-\frac{1}{\sqrt{2}}\left(|01\rangle_{a_1a_2}|\psi^+\rangle_{b_1b_2}+|10\rangle_{a_1a_2}|\psi^-\rangle_{b_1b_2}\right).$$

步骤 5 从粒子序列中提取粒子 a_1 和 a_2 形成

序列 $P_{\rm A}=\{P_1(a_1,\ a_2),\ P_2(a_1,\ a_2),\ \cdots,\ P_N(a_1,\ a_2)\}$, 剩余粒子 b_1 和 b_2 形成序列 $P_{\rm B}=\{P_1(b_1,\ b_2),\ P_2(b_1,\ b_2),\ \cdots,\ P_N(b_1,\ b_2)\}$.

步骤 6 Alice 根据 $EK_{\rm A1}$ 制备光子检测序列 S, 并随机插入序列 $P_{\rm B}$, 发送混合序列给 Bob.

步骤 7 Alice 公开 S 光子在 $P_{\rm B}$ 中的位置, Bob 根据 $EK_{\rm A1}$ 选择 Z 基或 X 基测量 S 中的光子, 并将测量结果与 $EK_{\rm A2}$ 对比, 计算错误率. 若错误率超过阈值, 则终止通信; 否则继续进行下一步.

步骤 8 Alice 对 $P_{\rm A}$ 中的每个粒子 a_1 和 a_2 进行 Z 基测量, Bob 对 $P_{\rm B}$ 中的每个粒子 b_1 和 b_2 进行贝尔基测量, Alice 公开测量结果, Bob 根据该结果和自己的测量结果, 查表解码消息.

表 1 中, 我们对基于不同量子资源的 QIA 协议的优势和局限性进行了总结和比较. 对上述协议而言, 在实验成熟度方面, 单光子协议 (如 Hong2017[68]) 因技术成熟度较高, 已接近实用化. 连续变量协议 (如 Chen2024[82]) 在光纤通信中更具优势, 但需解决信道损耗问题. 在安全性方面, 纠缠态协议理论上提供“无条件安全性”, 但实际安全性受限于设备缺陷 (如纠缠源不可信), 需考虑设备无关 (device-independent) 假设的适用性. 单光子协议需防范光子数分离攻击 (PNS 攻击), 常需诱骗态技术补充. 在未来, 混合型协议可能成为量子网络的主流, 兼顾资源效率与安全性. 连续变量 QIA 与经典光通信的深度融合是重要研究方向.

2.2 根据量子协议分类

根据 QIA 协议中使用的量子协议和通信类型, 将文中提到的 QIA 协议分类如下: 基于 QKD 框架的 QIA 协议、基于 QSDC 框架的 QIA 协议、基于 QT 框架的 QIA 协议、基于 QSS 框架的 QIA 协议以及基于乒乓协议框架的 QIA 协议.

2.2.1 基于 QKD 框架的 QIA 协议

基于 QKD 框架的 QIA 协议将身份认证功能嵌入密钥分发过程, 确保通信双方身份的合法性. 在 QKD 生成密钥的同时, 通过量子态操作或预共享密钥验证身份. 利用贝尔态分发 (如 EPR 对) 或单光子编码等技术, 必要时可借助第三方可信任机构辅助验证. 多用于量子通信网络中的初始身份绑定 (如量子卫星通信) 和需要高安全性的长期密钥分发场景.

基于 QKD 框架的 QIA 协议使用最为广泛, 2000 年, Zeng 和 Zhang[55] 提出的 QIA 协议就是基于 QKD 框架. 同年, Ljunggren 等 [56] 通过引入第三方可信机构 Trent 作为仲裁者, 提出了一种基于授权的 QIA 协议. 当引入第三方后, 可能会出现各种问题, 故在该协议中假设第三方是诚实的. 此外, 第三方的量子能力也是影响认证成功与否的关键. 2001 年, Curty 和 Santos[87] 提出了一种基于量子资源的经典消息认证协议 (CS01 协议), 该协议首次提出仅需共享一个量子比特 (如纠缠态中的单粒子) 作为认证密钥, 即可安全验证二进制经典消息的完整性和发送者身份, 显著地降低了传统方法对长密钥的依赖, 提升了资源效率. 通过设计特定的幺正操作, 将经典消息编码为量子态, 结合纠缠资源生成认证标签, 实现了量子物理特性 (如不可克隆性) 对经典信息的保护, 突破了传统哈希函数与加密算法的局限性. 相较于经典消息认证码 (MAC) 需至少两比特密钥确保安全性, 该协议在单量子比特下即实现信息论安全, 为低资源环境 (如量子物联网) 的认证需求提供了高效解决协议.

简述 Curty 和 Santos[87] 的协议如下.

表 1 根据量子资源分类的 QIA 协议

Table 1. QIA scheme based on quantum resources classification.

量子源类型	核心资源	优势	局限性	信道损耗/噪声容忍度
单光子	极化/相位编码单光子	低资源消耗、易于实现、与现有QKD技术兼容度高	需高效单光子探测器, 抗噪声能力较弱, 需防范光子数分离(PNS)攻击	中等. 对信道损耗敏感, 需使用诱骗态; 散粒噪声会影响误码率
纠缠态	贝尔态、GHZ态、团簇态	高安全性、抗窃听能力强、具备理论上的无条件安全性	实验复杂度高, 依赖稳定纠缠源, 传输距离受纠缠分效率限制	较低. 纠缠分发效率极易受信道损耗和退相干效应影响, 保真度下降快
连续变量	双模压缩态、相干态	城域网效率高, 兼容经典光通信设备, 探测效率高	需高精度调制, 安全性依赖高斯假设, 易受到非高斯攻击	较高. 可采用经典光通信的放大和纠错技术, 但对过量噪声非常敏感
混合型	纠缠态+单光子/经典算法	灵活性强, 平衡效率与安全性, 降低对单一量子源的依赖, 适用复杂场景	安全性需双重验证, 协议设计复杂度高, 需协调量子与经典操作的同步性	可调节. 取决于所采用的具体量子资源组合, 设计上可针对噪声进行优化

步骤 1 初始化. Alice 和 Bob 预先共享一个两量子比特的最大纠缠态 $|\psi\rangle_{\mathrm{AB}}=1/\sqrt{2}\,(|01\rangle_{\mathrm{AB}}-|10\rangle_{\mathrm{AB}})$, Alice 持有粒子 A, Bob 持有粒子 B. 双方公开幺正操作 $U_{\mathcal{E}}$, 消息态空间$\mathcal{E}$是一个四维希尔伯特空间, 包含正交基 $\{|\varphi_0\rangle,|\varphi_1\rangle,|\varphi_2\rangle,|\varphi_3\rangle\}$, $|\varphi_0\rangle,|\varphi_1\rangle$ 分别对应经典信息 0 和 1, 且满足正交性 $\langle\varphi_i|\varphi_j\rangle=\delta_{ij}$, $|\varphi_2\rangle,|\varphi_3\rangle$ 为辅助态, 用于错误检测.

步骤 2 认证编码过程. Alice 发送消息 $i\in\{0,1\}$时, 制备消息态 $|\varphi_i\rangle\in\varepsilon$ (例如 $|\varphi_0\rangle=|00\rangle,|\varphi_1\rangle=|11\rangle$), 对共享密钥粒子 A 和消息态执行幺正操作: $E_{\mathrm{A}\varepsilon}=|0\rangle\langle 0|_{\mathrm{A}}I_{\varepsilon}+|1\rangle\langle 1|_{\mathrm{A}}U_{\varepsilon}$. 若 A 处于 $|0\rangle$, 执行恒等操作; 若 A 处于 $|1\rangle$, 执行 U_{ε} 操作. Alice 发送编码后的消息态给 Bob. 保留密钥粒子 A.

步骤 3 验证解码过程. Bob 接收到消息态后, 对共享密钥粒子 B 和消息态执行解码操作: $D_{\mathrm{B}\varepsilon}=|0\rangle\langle 0|_{\mathrm{B}}\otimes U_{\varepsilon}'+|1\rangle\langle 1|_{\mathrm{B}}\otimes I_{\varepsilon}$. 若 B 处于 $|1\rangle$, 执行恒等操作; 若 B 处于 $|0\rangle$, 执行解码 U_{ε}' 操作. Bob 在消息空间$\mathcal{E}$上对正交基 $\{|\varphi_k\rangle\,|k=0,1,2,3\}$ 进行投影测量. 若测得 $|\varphi_0\rangle$ 则接受消息为 0, 若测得 $|\varphi_1\rangle$ 则接受消息为 1, 即认证通过; 若测得 $|\varphi_2\rangle$ 或 $|\varphi_3\rangle$ 则拒绝消息, 即认证失败.

2.2.2 基于 QSDC 框架的 QIA 协议

QSDC 可以直接通过量子信道传输秘密信息而无需密钥. 通过这种方式, 已认证用户可以采用 QSDC 直接将他们的身份码发送给认证者. 基于 QSDC 框架的 QIA 协议利用量子态的基矢选择或相位参数, 将身份认证信息直接嵌入量子态编码中, 采用极化光子、贝尔态编码、动态密钥更新等技术, 结合诱骗态检测窃听, 实现安全通信与认证一体化. 多用于实时量子安全通信 (如军事指挥系统) 和资源受限的量子物联网设备认证.

2010 年, Liu 等 [88] 提出了一种结合极化光子与贝尔态的 QSDC 改进协议, 通过动态身份认证机制优化了传统协议的实现复杂度与安全性. 相较于依赖 GHZ 态或多光子纠缠的现有协议, 该协议利用极化光子的制备与测量简易性, 将认证过程整合至传统 QSDC 框架内, 硬件成本降低约 30%. 2015 年, Chang 等 [89] 提出了一种改进型 QSDC 协议, 通过单光子序列实现高效通信与动态身份认证. 该协议的核心创新在于将身份标识嵌入光子偏振基矢选择中, 并利用经典异或 (XOR) 加密增强抗攻击能力, 同时优化了传统协议中纠缠态资源依赖与传输效率问题. 相较于依赖纠缠态的 QSDC 协议 (如 Wang 等 [85]2006 年协议需两次光子传输), 该协议通过单次光子传输完成通信, 信道利用率提升约 40%. 此外, 单光子制备与测量技术兼容现有量子光学器件, 实验实现成本降低 30%.

2020 年, QSDC 拓展了新的应用场景, Zhou 等 [90] 提出了一种新型的测量设备无关的 QSDC (MDI-QSDC) 协议, 旨在解决传统 QSDC 中由测量设备缺陷引发的安全漏洞. 通过引入不可信的第三方 (Charlie) 执行 Bell 态测量 (Bell state measurement, BSM), 该协议不仅消除了测量端潜在的攻击风险, 还将通信距离提升至传统 QSDC 的两倍 (例如从 100 km 扩展至 200 km). 随后在 2022 年, Das 和 Paul[91] 提出了一种结合用户身份认证的 MDI-QSDC 协议, 并扩展至量子对话和确定性安全量子通信场景, 为量子密码学提供了新的安全解决协议. 首次将用户认证与 MDI 技术结合, 构建高效且安全的量子通信框架. 2024 年, Li 等 [92] 提出了一种基于单光子的 MDI-QSDC 协议, 首次将身份认证与单光子资源结合, 解决了现有 MDI-QSDC 协议依赖纠缠光子对且缺乏身份验证的缺陷. 协议通过预共享身份标识、诱骗态检测及 BSM, 实现了通信双方的双向身份认证与安全信息直传, 采用离散变量 (单光子) 与 BSM 技术成熟, 资源制备简单, 易于集成现有量子网络设施, 适配光纤通信等实际场景.

简述 Li 等 [92] 的协议如下.

步骤 1 初始化阶段. Alice 和 Bob 约定四个局域酉操作与比特的映射关系: 操作 $\sigma_{00}=I$, $\sigma_{01}=\sigma_x$, $\sigma_{10}=\mathrm{i}\sigma_y$, $\sigma_{11}=\sigma_z$, 分别对应 00, 01, 10, 11 比特. Alice 持有 $\mathrm{ID_A}$, Bob 持有 $\mathrm{ID_B}$, 二者私有且定期更新.

步骤 2 Bob 向 Alice 认证身份. Bob 制备一组 EPR 对序列, 每个 EPR 对随机抽取一个光子, 根据 $\mathrm{ID_B}$ 制备极化光子: $\mathrm{ID_B}$ 比特为 0 制备直角基 ($|0\rangle$ 或 $|1\rangle$), $\mathrm{ID_B}$ 比特为 1 制备对角基 ($|+\rangle$ 或 $|-\rangle$). 将极化光子随机插入 EPR 光子序列, 发送混合序列给 Alice. Alice 使用滤波器 (防不可见光子) 和光子数分离器 (防延迟光子) 检测特洛伊木马攻击, 存储序列. Bob 公开极化光子位置. Alice 随机选择基测量这些光子, 公开测量基和结果. Bob 计算错误率: 若错误率大于阈值, 则终止; 否则, Bob 公开制备基. Alice 修正测量基, 提取 $\mathrm{ID_B'}$. Alice 比较

ID'_B 与 ID_B, 若匹配, 则 Bob 身份合法.

步骤 3 Alice 发送机密信息. Alice 根据机密消息, 对序列中非极化光子施加相应酉操作, 并根据 ID_A 制备极化光子 (规则同 Bob), 随机插入序列, 回传给 Bob.

步骤 4 Alice 向 Bob 认证身份. Alice 公开极化光子位置, Bob 测量光子并公开测量基和结果. Alice 计算错误率, 若低于阈值, 则公开正确基. Bob 修正测量基, 提取 ID'_A, 与 ID_A 比较, 若匹配则 Alice 身份合法, 继续解码.

步骤 5 Bob 解码信息. Bob 对接收到的 EPR 光子和本地保留的配对光子进行贝尔态联合测量, 根据测量结果和酉操作映射 (步骤 1) 解码机密消息, 每个 EPR 对得到 2 比特. Alice 和 Bob 使用经典纠错协议修正传输错误.

步骤 6 身份标识更新. 从已传输的机密消息中截取部分比特, 更新 ID_A 和 ID_B, 供下次通信使用.

2.2.3 基于 QT 框架的 QIA 协议

基于 QT 框架的 QIA 协议利用量子隐形传态传输身份信息或认证密钥, 通过 EPR 对或 GHZ 态分配量子资源, 采用纠缠交换、BSM 和量子态远程制备等技术, 保障通信过程的无条件安全性, 实现跨节点认证. 多用于量子中继网络中的跨节点身份认证和城域量子通信 (如银行数据中心互联).

2005 年, Zhou 等 [93] 提出了一种基于量子隐形传态和纠缠交换的跨中心 QIA 协议. 该协议通过 EPR 纠缠对的完整性传输未知量子态, 确保信息传输的无条件安全性. 而且, 通过操作未直接交互的量子系统, 从而扩展了量子通信距离. 然而, 这种方法需要保证用于纠缠交换的中间设备需要被完全信任, 否则会带来新的安全问题. 2016 年 Ma 等 [78] 的连续变量协议也是与 QT 相结合的.

简述 Zhou 等 [93] 的协议如下.

注册阶段: 用户在归属认证中心 CA 注册身份. 用户归属的客户端服务器 U_{1i} 和认证中心 CA_1 预先共享一个 EPR 对 (光子 2, 3): $|\psi^-\rangle_{23} = (1/\sqrt{2})(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3)$. U_{1i} 持有光子 2, CA_1 持有光子 3. U_{1i} 根据用户身份信息制备单光子量子态 $|\varphi\rangle_1 = \alpha|0\rangle + \beta|1\rangle$, 称为认证密钥. U_{1i} 对光子 1 (身份态) 和光子 2 进行贝尔基联合测量, 得到 4 种可能结果之一 (如 $|\psi^+\rangle_{12}$), 并将测量结果通过经典信道告知 CA_1. CA_1 根据收到的测量结果, 对持有的光子 3 施加相应酉操作, 重建出原始身份态 $|\varphi\rangle$. U_{1i} 测量结果和 CA_1 所需操作对应如下:

$$|\psi^-\rangle_{12} \to U = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$|\psi^+\rangle_{12} \to U = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$|\varphi^-\rangle_{12} \to U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$|\varphi^+\rangle_{12} \to U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

CA_1 将用户身份信息以量子态形式存入数据库, 并通知 U_{1i} 注册成功.

认证阶段: 用户跨中心请求服务. 用户在 U_{2j} 输入用户名、CA 编号 (CA_1) 及身份信息. U_{2j} 将 CA 编号通过经典信道发送给 CA_2. CA_2 根据 CA 编号将请求转发给 CA_1. CA_2 对本地光子 ca_2 和 ca_{2j} 进行贝尔基联合测量, 实现纠缠交换. 测量结果为 4 种贝尔态之一 (如 $|\psi^+\rangle_{ca_2ca_{2j}}$), 此时 CA_1 的光子 ca_1 与 U_{2j} 的光子 u_{2j} 形成纠缠态 (如 $|\psi^+\rangle_{ca_1u_{2j}}$). CA_2 将测量结果通过经典信道告知 CA_1. CA_2 向 U_{2j} 发送操作指令, 通知其准备进行隐形传态. U_{2j} 根据用户输入的身份信息制备单光子态 $|\varphi\rangle_S$, 并对身份态光子 S 和光子 u_{2j} (纠缠交换后与 CA_1 纠缠) 进行贝尔基联合测量, 将结果通过经典信道发送给 CA_2, 然后 CA_2 转发给 CA_1. CA_1 结合两次收到的信息 (CA_2 的纠缠交换结果和 U_{2j} 的贝尔测量结果), 对持有的光子施加相应酉操作, 重建出身份态 $|\varphi\rangle$, 并将其与数据库中存储的该用户认证密钥 K 进行比对. 若匹配则认证成功, CA_1 通知 CA_2 授权服务, CA_2 根据 CA_1 的授权结果, 向用户提供相应服务.

2.2.4 基于纠缠交换框架的 QIA 协议

基于纠缠交换框架的 QIA 协议利用 GHZ 态或团簇态的全局纠缠特性, 实现多方协作式身份认证, 需多用户或第三方共同验证身份. 此类协议采用 GHZ 态分发、诱骗光子插入和经典哈希函数辅助等技术, 利用量子纠缠的非局域关联性, 确保攻击者无法伪造部分参与方的身份. 多用于多方量子会议系统 (如量子区块链共识机制 [66]) 和高安全等级的多机构联合认证 [94](如政府机密系统).

2006 年, Wang 等 [85] 提出了一种基于纠缠交换的多方 QIA 协议, 旨在通过可信第三方 (Trent)

同时认证多个用户的身份. 该协议结合 GHZ 态的量子纠缠特性与经典哈希函数, 试图在提升效率的同时保证无条件安全性. 2009 年, Yang 等[95] 利用 GHZ 态的纠缠特性与诱骗光子技术, 提出了一种多方同时进行的 QIA 协议, 能有效地检测双 CNOT 攻击等复杂攻击. 该协议与 2006 年 Wang 等[85] 的协议类似, 但需要的量子资源更少, 且用户仅需单量子比特测量 (SQM), 显著降低了资源消耗与操作复杂度. 尽管仍依赖可信第三方, 其高效性与安全性为大规模量子网络中的身份认证提供了重要参考.

简述 Wang 等[85] 的协议如下.

步骤 1 可信第三方 Trent 制备 N 个三粒子 GHZ 态, 初始态均为 $|\psi_1\rangle=\dfrac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{TA_1A_2}$, 自己保留 T 序列, 将 A_1 和 A_2 序列分别发送给 Alice_1 和 Alice_2.

步骤 2 Trent 随机选择部分 GHZ 态作为抽样集, 并随机选择 Z 基 ($|0\rangle$, $|1\rangle$) 或 X 基 ($|+\rangle$, $|-\rangle$) 测量, 公开抽样位置和测量基. Alice_1 和 Alice_2 对相应位置的 A_1 和 A_2 粒子用相同基测量, 并公布测量结果. 根据错误率决定是否继续.

步骤 3 Trent 将剩余 GHZ 态随机分为 M 组, 每组含两个 GHZ 态 (T, T'; A_1, A_1'; A_2, A_2').

步骤 4 Alice_1 和 Alice_2 根据认证密钥 AK_i 对组内粒子施加酉操作. 若比特为 0, 则施加 $\boldsymbol{I}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$; 若比特为 1, 则施加 $\mathrm{i}\sigma_y=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$.

步骤 5 Trent 对每组中的 T 和 T' 粒子随机独立施加 I 或 $\mathrm{i}\sigma_y$ 操作.

步骤 6 Alice_1 和 Alice_2 分别测量每组中的 (A_1, A_1') 和 (A_2, A_2') 粒子对, 并公布结果. Trent 测量 (T, T') 粒子对, 不公布结果. 他根据三方测量结果反推用户操作, 并将反推的密钥比特与预共享的进行比对, 若一致则认证通过. 例如, 若测得 $\left(|\psi^-\rangle_{TT'},|\psi^-\rangle_{A_1A_1'},|\psi^+\rangle_{A_2A_2'}\right)$, 则对应操作组合 $\mathrm{i}\sigma_y\otimes\mathrm{i}\sigma_y\otimes I$, 即 Alice_1 操作 $\mathrm{i}\sigma_y$, 密钥比特 1; Alice_2 操作 I, 密钥比特 0. 该协议也可扩展至多方 (r 个用户), 仅需 Trent 制备 $(r+1)$-粒子 GHZ 态.

2.2.5 基于乒乓协议框架的 QIA 协议

此类 QIA 协议基于量子信道的“请求-响应”机制 (乒乓协议), 量子态在发送方与接收方之间多次传输, 动态更新认证密钥, 采用单光子乒乓传输、CNOT 门操作和动态基矢选择等技术实现身份验证. 量子态传输的不可逆性, 导致攻击者的操作会破坏量子态关联, 从而确保认证过程的安全性. 多用于动态网络环境中的临时身份认证 (如移动量子终端) 和需要频繁更新密钥的短期通信场景.

2006 年, Zhang 等[96] 首次结合乒乓协议 (ping-pong protocol) 和量子控制非门 (CNOT), 提出了一种单向的 QIA 协议, 实现了高效、安全的量子认证与动态密钥更新一体化. 该协议对诸如假冒欺诈攻击和替换欺诈攻击等个体攻击具有安全性. 该协议仅支持单向认证, 即 Alice 被视为可靠的认证机构, 而 Bob 被视为需要验证身份的用户, 双向认证需进一步扩展. 严格地从技术上来讲, 到目前为止所提出的许多协议在这个意义上都是单向的, 当然也可以简单认为通过两次使用相同的过程就可以进行双向认证, 但实现上并不能完全等同, 所以通常不会明确提及. 2014 年, Yuan 等[86] 提出了一种基于单粒子态和乒乓技术的量子身份认证协议, 无需依赖纠缠态即可实现用户身份验证与认证密钥的动态更新. 协议利用单粒子在双向量子信道中的传输特性, 结合异或操作和基矢选择机制, 确保密钥更新与身份验证同步完成. 通过单粒子态与乒乓技术的创新结合, 为量子身份认证提供了高效且安全的解决协议, 其无纠缠依赖与动态密钥更新机制具有重要理论价值.

简述 Zhang 等[96] 的 QIA 协议如下.

可靠认证中心 Alice 验证用户 Bob 的身份. Alice 和 Bob 预先共享一个经典二进制认证密钥 $K_a=\{k_1,k_2,\cdots,k_{2n}\}$.

步骤 1 Alice 制备一个 EPR 纠缠对 $|\Psi\rangle=\dfrac{1}{\sqrt{2}}(|0_\text{h}0_\text{t}\rangle+|1_\text{h}1_\text{t}\rangle)$, 粒子 h 保留, 将粒子 t 通过量子信道发送给 Bob.

步骤 2 Bob 收到粒子 t 后, 根据密钥的当前两位 $k_{2i-1}k_{2i}$ $(1\leqslant i\leqslant n)$ 制备一个信息粒子 m: $|\varphi_m\rangle=|k_{2i-1}\oplus k_{2i}\rangle$, 然后对粒子 t 和 m 施加量子受控非门 (CNOT). 若 $k_{2i-1}=0$, 使用 Z 基 CNOT 门 C_0: $C_0=|0\rangle\langle0|\otimes I+|1\rangle\langle1|\sigma_x$; 若 $k_{2i-1}=1$, 使用 X 基CNOT 门 C_1: $C_1=|+\rangle\langle+|\otimes I+|-\rangle\langle-|\sigma_x$, 操作后生成三粒子纠缠态 $|\Phi_\text{w}\rangle=C_\text{p}(|\Psi\rangle\otimes|\varphi_\text{m}\rangle)$. Bob 保留粒子 t, 并将信息粒子 m 发回 Alice.

步骤 3 Alice 收到粒子 m 后, 对保留的粒子 h 和收到的粒子 m 施加相同的 CNOT 门 C_p(根据密

表 2 基于量子框架分类的 QIA 协议

Table 2. QIA schemes based on quantum framework classification.

分类	信道需求	核心优势	主要局限	适用场景
QKD框架	低损耗	高安全性, 密钥与认证同步	依赖预共享密钥或可信第三方	长期密钥分发的安全通信
QSDC框架	高稳定性	高效信息传输与认证一体化	对量子信道质量要求高	实时安全通信(如军事指挥)
隐形传态框架	中继节点	跨节点认证, 无条件安全性	实验复杂度高, 需可信中继	量子中继网络与城域互联
纠缠交换框架	多方同步	多方协作抗合谋攻击	量子资源消耗大, 依赖可信第三方	多方联合认证(如区块链共识)
乒乓协议框架	双向信道	动态密钥更新, 抗窃听能力强	仅支持单向认证, 需双向信道	移动终端临时认证

钥 k_{2i-1} 选择基): $|\Phi'_{\rm w}\rangle = C_{\rm p}|\Psi_{\rm w}\rangle = |\Psi\rangle \otimes |\varphi_{\rm m}\rangle$, 此时粒子 m 恢复为初始态 $|\varphi_m\rangle = |k_{2i-1} \oplus k_{2i}\rangle$.

步骤 4 Alice 在 σ_z 基下测量粒子 m, 合法 Bob 的测量结果必为 $k_{2i-1} \oplus k_{2i}$. 若结果匹配, 返回步骤 1 进行下一组密钥位的验证. 若所有 n 组密钥均通过, 则 Bob 身份认证成功.

步骤 5 每认证一组密钥位 $k_{2i-1}k_{2i}$ 后, 更新该密钥.

表 2 中, 我们对基于不同量子框架的 QIA 协议的优势、局限性以及适用场景进行了总结和比较.

3 最新的 QIA 协议

随着量子通信的发展, QIA 协议也是不断发展的, 以下介绍 1 个最新的 QIA 协议以及具有 QIA 功能的三方 QSDC 协议.

3.1 基于 GHZ 态的多方 QIA 协议 [97]

如图 1 所示, Alice 为验证方, 她事先与 N 个目标通信方 $\rm Bob'_1$, $\rm Bob'_2$, $\cdots$, $\rm Bob'_N$, 分别通过 BB84 协议共享一组认证密钥序列 K'_1, K'_2, $\cdots$, K'_N. 密钥各不相同, 分别为一系列长度相同的二进制比特串, 每个目标通信方只知道自己与 Alice 的共享密钥序列, 而 Alice 知道所有目标通信方的密钥序列.

步骤 1 Alice 制备一系列相同的 N+1 光子极化 GHZ 态, 取出所有 GHZ 态中的光子 1, 组成序列 $S_{\rm A}$, 并把序列 $S_{\rm A}$ 的光子存储到量子存储器中. Alice 将所有 GHZ 态中的光子 2 组成序列 $S_{\rm B1}$, 将所有 GHZ 态中的光子 3 组成序列 $S_{\rm B2}$……依次操作, 将所有 GHZ 态中的光子 N+1 组成序列 $S_{\rm BN}$.

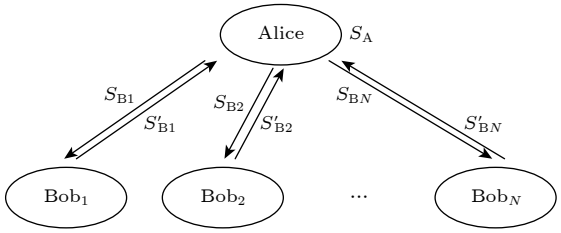

图 1 多方 QIA 协议原理图

Fig. 1. Schematic diagram of multi-party quantum identity authentication.

步骤 2 Alice 随机制备大量直角基 (Z) 或对角基 (X) 单光子, 作为安全检测光子. Alice 将这些光子分别随机插入到序列 $S_{\rm B1}$, $S_{\rm B2}$, ···, $S_{\rm BN}$ 中, 再通过 N 条量子信道将序列 $S_{\rm B1}$, $S_{\rm B2}$, ···, $S_{\rm BN}$ 分别发送给实际通信方 (待证明方) $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$.

步骤 3 待证明方接收到光子后, Alice 公开各条光子序列中安全性检测光子的位置和制备基, $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 分别提取出安全性检测光子, 进行第一轮安全性检测, 并公布测量结果. Alice 根据结果估算每条量子信道的错误率, 若均低于事先设定的阈值, 说明所有量子信道中的光子传输过程均安全, 则进行下一步.

步骤 4 Alice 对序列 $S_{\rm A}$ 的光子进行 Z 基测量, $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 根据各自的认证密钥 K_1, K_2, $\cdots$, K_N, 分别对剩余光子进行编码操作, 得到序列 $S'_{\rm B1}$, $S'_{\rm B2}$, $\cdots$, $S'_{\rm BN}$. 接着, 随机地在光子序列中插入足够数量的安全性检测光子. 操作完成后, 分别将光子序列再发送回验证方 Alice.

步骤 5 待 $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 公开序列中安全性检测光子的位置和制备基后, Alice 进行第二轮安全性检测. 确认安全后, Alice 分别对返回序列中的剩余光子进行 Z 基测量, 根据测量结果, Alice 可推断出 $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 的操作, 从而读出 $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 传递的认证密钥序列 K_1, K_2, $\cdots$, K_N. 通过与目标通信方的认证密钥 K'_1, K'_2, $\cdots$, K'_N 进行比对, 从而验证 $\rm Bob'_1$, $\rm Bob'_2$, $\cdots$, $\rm Bob'_N$ 的身份.

该协议中, 包含两轮安全性检测. 在待证明方 $\rm Bob_1$, $\rm Bob_2$, $\cdots$, $\rm Bob_N$ 和验证方 Alice 收到光子序

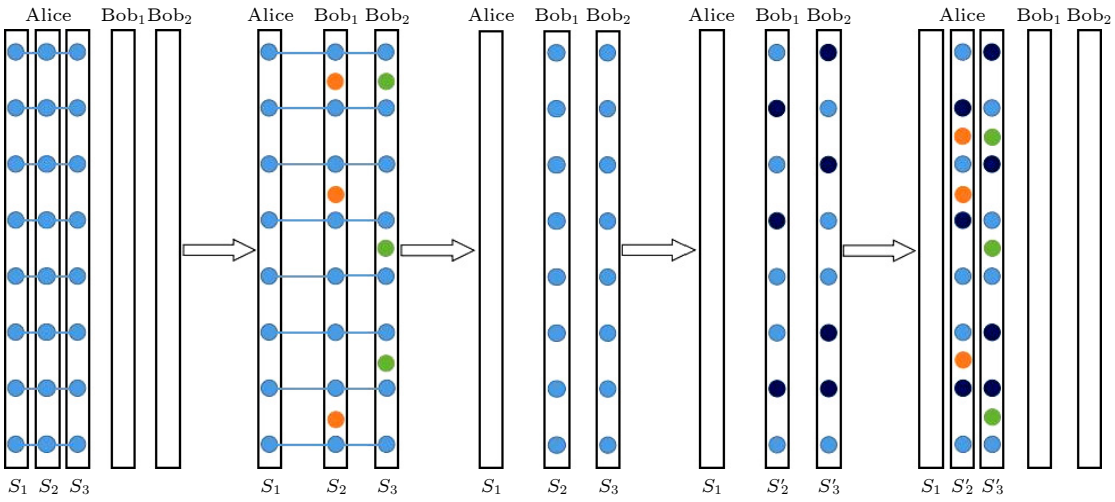

图 2 三方 QIA 协议步骤图

Fig. 2. Schematic diagram of the three-partite QIA protocol.

列后, 均必须确认量子通道的安全性, 才能进行下一步的操作.

为了更清楚地描述协议, 以三用户 QIA 为例说明. 三用户 QIA 协议步骤图如图 2 所示, 其中两个用户 Bob_1, Bob_2 需要向 Alice 认证身份, 该过程忽略安全性检测. Alice 与合法用户 Bob_1', Bob_2' 预先共享的密钥序列 $K_1=\{K_{11}, K_{12}, K_{13}, \cdots, K_{1L}\}$, $K_2=\{K_{21}, K_{22}, K_{23}, \cdots, K_{2L}\}$作为 Bob_1, Bob_2 的身份认证码序列, L 足够大. Alice 制备大量处于相同的量子态的 3 光子 GHZ 态, 属于 8 个 GHZ 态之一. 如果选取其中之一的量子态 $|\varphi_2^+\rangle=\dfrac{1}{\sqrt{2}}(|\mathrm{HVH}\rangle+|\mathrm{VHV}\rangle)_{123}$ 进行制备, 量子态的数量等于认证密钥序列的长度. 验证方 Alice 取出所有 GHZ 态中的光子 1, 2 和 3, 分别组成序列 S_1, 序列 S_2 和序列 S_3. 在待证明方 Bob_1 和 Bob_2 编码前, Alice 对序列 S_{A} 的光子进行 Z 基测量. 假设测量结果是 $|H\rangle$, 则 Bob_1 和 Bob_2 分别为 $|V\rangle$ 和 $|H\rangle$. 然后, Bob_1 和 Bob_2 根据各自密钥 K_1 和 K_2 进行编码操作, 将认证密钥信息加载到纠缠光子上, 编码操作包含两种幺正操作$\{I, \sigma_x\}$. $I=|H\rangle\langle H|+|V\rangle\langle V|$ (不变操作) 代表密钥 0, $\sigma_x=|H\rangle\langle V|+|V\rangle\langle H|$ (比特翻转操作) 代表密钥 1. 对返回的光子序列, Alice 再次进行单光子测量. 如果 Alice 测量 Bob_1 光子结果是 $|H\rangle$ ($|V\rangle$), 她可知 Bob_1 的操作是 $\sigma_x(I)$, 则可推断密钥为 1(0). 同时, 如果 Alice 测量 Bob_2 光子结果是 $|H\rangle$ ($|V\rangle$), 她可知 Bob_1 的操作是 $I(\sigma_x)$, 则可推断密钥为 0(1). 经过逐个判断, Alice 可推断出密钥序列, 如果与预先共享的密钥序列相同, 则可确认其身份, 否则为非法用户.

该协议能够抵御来自认证用户的内部攻击, 以及外部的拦截-测量-重发攻击.

3.2 具有身份认证功能的三方 QSDC 协议[98]

下面介绍身份认证在通信协议中的一个实例, 一种具有身份认证功能的三方 QSDC 协议. 该协议基于极化-空间自由度超编码单光子. 其协议步骤图如图 3 所示. 该协议先通过身份认证, 使信息接收方确定两个信息发送方的身份. 身份确定后, 两个信息发送方分别在极化自由度和空间自由度对单光子进行编码. 编码完成后, 编码单光子重新发送给信息接收方. 信息接收方通过测量, 可同时得到两个发送方传递的秘密信息.

在通信前, Alice 与目标通信方 Bob_1 和 Bob_2 分别共享一组随机密钥序列 K_1 和 K_2 作为 Bob_1 和 Bob_2 的身份码序列.

步骤 1 Alice 随机制备大量极化-空间超编码单光子作为信息传输光子, 组成序列 S_1, 再根据 Bob_1 和 Bob_2 的身份码制备足够多身份认证光子和大量安全检测光子, 随机插入序列 S_1 中, 组成序列 S_1'.

步骤 2 Alice 将序列 S_1' 发给第一个实际通信方 Bob_1', Bob_1' 接收到所有光子后. Alice 公布安全检测光子的位置和量子态, Bob_1' 进行第一轮安全性检测. 若安全性检测未通过, 则终止通信; 若安全性检测通过, 则进行下一步.

步骤 3 Alice 公布用于 Bob_1' 的身份认证光子的位置, Bob_1' 根据自己的身份码选择测量基对其

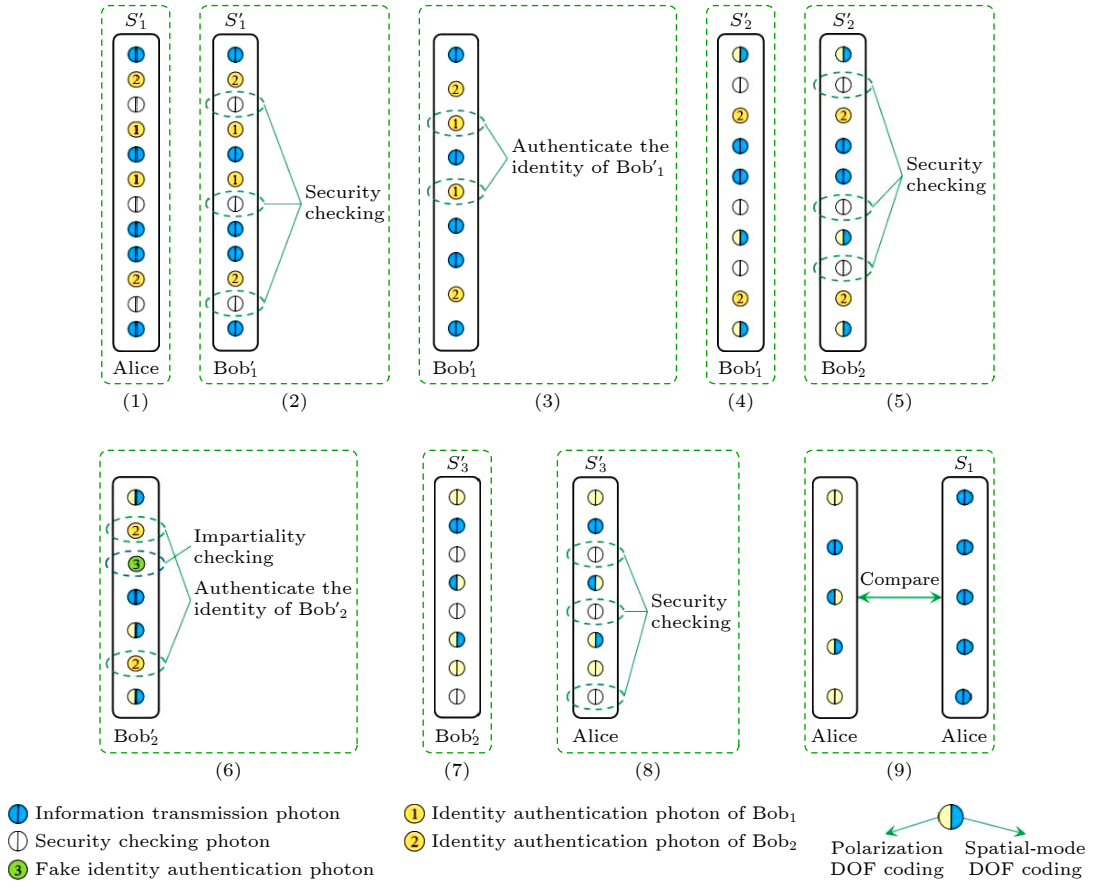

图 3 具有身份认证功能的三方量子安全通信协议示意图

Fig. 3. Schematic diagram of a three-party quantum secure communication scheme with identity authentication function.

进行测量并公开测量结果. Alice 根据公开结果与制备的初始态比较, 进行身份认证. 若身份认证未通过, 则认为第一个实际通信方 Bob'_1 为非法用户, 通信取消; 若身份认证通过, 则认为 Bob'_1 即为目标通信方 Bob_1, 进行下一步骤.

步骤 4 Alice 公布用于 Bob'_2 的身份认证光子的位置, 其余的光子即为信息传输光子, Bob'_1 在其极化自由度上编码, 组成序列 S_2, 并在序列 S_2 中随机插入足够数量的安全检测光子, 组成序列 S'_2.

步骤 5 Bob'_1 将序列 S'_2 发给 Bob'_2, 并公布序列 S'_2 中的安全检测光子的位置和量子态, Bob'_2 进行第二轮安全性检测. 若安全性检测未通过, 则终止通信; 若安全性检测通过, 则进行下一步.

步骤 6 Bob'_2 根据自己的身份码选择测量基对其进行测量并公开测量结果. Alice 根据公开的结果与制备的初始态比较, 进行身份认证.

步骤 7 若身份认证通过, Bob'_2 在信息传输光子空间自由度上编码, 并随机插入足够数量的安全检测光子, 组成序列 S'_3.

步骤 8 Bob'_2 将序列 S'_3 发给 Alice, 并公布序列 S'_3 中的安全检测光子的位置和量子态, Alice 提取出安全检测光子进行第三轮安全性检测.

步骤 9 若安全性检测通过, Alice 对每个信息传输光子的两个自由度进行测量, 再与原始序列 S_1 中对应的信息传输光子的量子态进行比较, 由此解码 Bob'_1 和 Bob'_2 的编码信息.

接下来仅对身份认证部分进行详细说明. Alice 根据 Bob_1 和 Bob_2 的身份码制备一系列在极化自由度上编码的单光子作为身份认证光子, 其制备规则如下: 当 Bob_1 的身份码或 Bob_2 的身份码为“0”时, Alice 利用直角基 (Z 基) 制备 $|H\rangle$ 或 $|V\rangle$ 态的光子; 当 Bob_1 的身份码或 Bob_2 的身份码为“1”时, Alice 利用对角基 (X 基) 制备 $|+\rangle = \dfrac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ 或 $|-\rangle = \dfrac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ 态的光子. 对 Bob'_1 进行身份认证流程如下: Alice 公布用于 Bob'_1 的身份认证光子的位置, Bob'_1 从量子存储器中提取出对应的光子, 根据自己的身份码选择测量基对其在极化自

由度进行测量并公开测量结果. Bob_1' 测量规则如下: 当 Bob_1' 的身份码为“0”时, Bob_1' 利用直角基 (Z 基) 测量身份认证光子并公布结果; 当 Bob_1' 的身份码为“1”时, Bob_1' 利用对角基 (X 基) 测量身份认证光子并公布结果. Alice 根据公开结果与制备的初始态比较, 若测量结果与 Alice 制备的初始态一致, 则认为 Bob_1' 的身份码正确; 若测量结果与 Alice 制备的初始态不一致, 则认为 Bob_1' 的身份码错误.

大多数基于纠缠态的 QIA 协议需要量子存储器, 以上两个协议也是如此. 近年来, 量子存储器已经取得了显著的实验进展 [99–103]. 例如, 2017 年, 研究人员报道了一种基于介观钕系集成与光子晶体腔耦合的高保真纳米光子量子存储器 [101]. 2021 年, Liu 等 [102] 实现了吸收式量子存储器之间的预示纠缠分发. 2022 年, 采用单晶片单程配置的自旋波固态量子存储器被成功演示, 该器件对单光子级弱相干脉冲的存储过程保真度达到 91.9%±2.4%[103]. 这些突破性进展表明, 量子存储器可能在不久的将来得以实现.

3.3 两个协议的创新性与优势分析

以上两个协议是本课题组提出的最新方案, 其在协议设计和性能上相较于现有方案具有一定的创新性和优势.

1) 基于 GHZ 态的多方同步身份认证协议创新性与优势:

创新性: 该协议的核心创新在于利用了 GHZ 态“全有或全无”的纠缠特性, 设计了一种多方同步身份认证机制. 验证方 (Alice) 通过单次量子态分发和一轮经典比对, 即可同时验证多个用户 (Bob_1, Bob_2, ···, Bob_N) 的身份, 无需进行多次双边认证, 极大提升了多用户场景下的认证效率.

安全性优势: 协议包含两轮诱骗态安全检测, 能有效抵御信道中的拦截-重发攻击和测量攻击. 更重要的是, 由于 GHZ 态的全局关联性, 任何单个认证用户 (如 Bob_i) 都无法在不被察觉的情况下与外部攻击者 Eve 合谋来伪造另一个用户 (Bob_j) 的身份, 从而有效地抵御了来自认证用户内部的合谋攻击, 这是许多双边认证协议难以实现的.

资源效率与实用性: 协议基于离散变量偏振编码, 与现有 QKD 技术兼容性高. 虽然需要量子存储器, 但随着量子存储技术的快速发展 [99–103], 该协议为未来量子网络中的集中式身份管理系统提供了一个可行的解决方案.

2) 具有身份认证功能的三方 QSDC 协议创新性与优势:

创新性: 该协议的创新点在于实现了身份认证与安全通信在单光子自由度上的深度集成. 利用单个光子的极化自由度和空间自由度分别进行身份认证信息和机密信息的编码 (超编码), 在一个协议框架内依次完成了两个发送方的身份认证和双信息的传输, 实现了“认证即通信”的一体化设计.

安全性优势: 协议流程中嵌入了三轮安全性检测, 确保了光子在各参与方之间传输的全程安全. 身份认证过程依赖于预共享密钥和量子态不可克隆原理, 通信过程则利用了量子超编码和测量技术, 共同构成了端到端的安全保障.

资源效率优势: 与需要制备复杂纠缠态或进行多次量子态传输的方案相比, 该协议主要依赖单光子源和线性光学操作, 降低了对复杂量子资源的需求. 它将两个独立的通信过程 (认证+通信) 融合, 提高了信道利用率和整体协议的效率, 特别适用于对传输效率有要求的有限量子资源场景.

综上所述, 本课题组提出的两个协议分别从多用户认证效率和认证-通信融合架构两个角度进行了创新探索, 在安全性、效率和实用性方面相较于同类协议展现出一定的优势, 为 QIA 在实际量子网络中的应用提供了新的思路.

4 总结与展望

QIA 作为量子通信的重要环节, 本文系统地梳理了 QIA 协议的技术演进脉络, 从早期基于 QKD 的混合认证协议到近年来低资源依赖、高实用性的创新协议, 本文通过分类比较, 全面分析了不同协议的理论基础、实现路径及安全边界, 为 QIA 的理论发展与应用提供了参考.

各类型认证协议各有优缺点. 单光子协议在配合诱骗态监测的条件下, 具备较高的实用化潜力, 但需防范光子数分离攻击; 纠缠态协议虽具备理论上的无条件安全性, 却受限于多粒子纠缠态的制备与维持难度; 连续变量协议在城域网中展现效率优势, 但其安全性依赖高斯假设; 混合型协议通过量子-经典协同设计平衡效率与安全性, 成为复杂网

络环境下的优选架构.

此外, 各类 QIA 协议对实际量子信道中的损耗与噪声的容忍度是其走向实用化的关键指标. 如表 1 所列, 不同类型的协议面临不同的挑战: 离散变量单光子协议需要克服损耗带来的低计数率问题, 并利用诱骗态技术对抗信道噪声 (如 PNS 攻击); 纠缠态协议的核心挑战在于如何长距离、高保真地分发和维持纠缠, 对信道退相干极为敏感; 连续变量协议虽探测效率高, 但必须严格控制系统的过量噪声 (excess noise). 未来, 发展噪声自适应的 QIA 协议、探索与测量设备无关 (MDI) 框架相结合的认证方案、以及设计更强的抗噪声编码和解码方法, 将是提升 QIA 实用性和鲁棒性的重要研究方向.

未来研究需重点关注以下方向: 1) 低资源依赖协议, 进一步优化单光子与连续变量协议, 降低对高精度量子器件的需求; 2) 协议轻量化与集成化, 结合测量设备无关 (MDI) 技术实现身份认证与安全通信的一体化设计; 3) 混合架构的鲁棒性增强, 探索量子-经典混合认证框架的动态密钥管理机制, 抵御量子计算攻击; 4) 实际环境适应性, 针对信道损耗、设备缺陷等现实约束, 发展噪声容忍与后量子安全增强技术. 此外, QIA 与量子物联网、区块链等新兴技术的深度融合, 将为数字身份主权与跨域安全协作提供全新范式. 随着量子通信网络的规模化部署, 高效、普适且抗量子攻击的认证协议将成为构建下一代安全信息生态的核心支柱.

参考文献

[1] Goldenberg L, Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239
[2] Scarani V, Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[3] Liestyowati D 2020 *J. Phys.: Conf. Ser.* **1477** 052062
[4] Shor P W 1994 *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* Santa Fe, USA, November 20–22, 1994 p124
[5] Zhao Q C 2004 *Quantum Computation and Quantum Information (I) — Quantum Computation* (Beijing: Tsinghua University Press) (in Chinese) [赵千川 2004 量子计算和量子信息 (一)——量子计算部分 (北京: 清华大学出版社)]
[6] Zhang Y D 2010 *Advanced Quantum Mechanics* (2nd ed.) (Beijing: Peking University Press) (in Chinese) [张永德 2010 高等量子力学 第 2 版 (北京: 北京大学出版社)]
[7] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, India, December 10–12, 1984 p175
[8] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[9] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[10] Bennett C H, Brassard G, Crépeau C, Jozsa R 1993 *Phys. Rev. Lett.* **70** 1895
[11] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H, Zeilinger A 1997 *Nature* **390** 575
[12] Pandey R K, Pathak A, Venugopalan A 2021 *Quantum Inf. Process.* **20** 322
[13] Li J X, Wang Z M, Shi S S, Li Y N, Shang R M, Gu Y J 2022 *Europhys. Lett.* **140** 58001
[14] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[15] Cleve R, Gottesman D, Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[16] Wang T Y, Wei Z L, Gao F 2021 *Quantum Inf. Process.* **20** 7
[17] Ju X X, Zhong W, Sheng Y B, Zhou L 2022 *Chin. Phys. B* **31** 100302
[18] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302
[19] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317
[20] Deng F G, Long G L 2004 *Phys. Rev. A* **69** 052319
[21] Eusebi A, Mancini S 2009 *Quantum Inf. Comput.* **9** 950
[22] Hu J Y, Li C L, Zhang C, Liu B, Guo G C 2016 *Light Sci. Appl.* **5** e16144
[23] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S, Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[24] Zhu F, Zhang W, Sheng Y B, Guo G C 2017 *Sci. Bull.* **62** 1519
[25] Hu X M, Zhang C, Zhang C J, Liu B H, Huang Y F, Han Y J, Li C F, Guo G C 2019 *Quantum Eng.* **1** e13
[26] Xu F H, Curty M, Qi B, Qian L, Lo H K 2020 *Rev. Mod. Phys.* **92** 025002
[27] Chen Y A, Zhang Q, Chen T Y, Pan J W 2021 *Nature* **589** 214
[28] Yin Z Q, Li F L, Chen Y A, Pan J W 2021 *Fundam. Res.* **1** 93
[29] Kwek L C, Cao L, Luo Y, Wang Y, Sun S H, Liu X, Lai J, Oh C H 2021 *AAPPS Bull.* **31** 15
[30] Wang X F, Sun X J, Liu Y X, Wang W, Kan B X, Dong P, Zhao L L 2021 *Quantum Eng.* **3** e73
[31] Hajji H, El Baz M 2021 *Quantum Inf. Process.* **20** 4
[32] Zhang C Y, Li C L, Xu J S, Li C F, Guo G C 2021 *Quantum Inf. Process.* **20** 146
[33] Jin A R, Li Y, Zhang Y, Pan J W 2021 *Phys. Rev. Appl.* **16** 034017
[34] Wang S, Chen W, Yin Z Q, Li H W, He D Y, Li Y H, Zhou Z, Guo G C, Han Z F 2022 *Nat. Photonics* **16** 154
[35] Liu B, Xia S, Xiao D, Huang W, Xu B J, Li Y 2022 *Sci. China-Phys. Mech. Astron.* **65** 240312
[36] Liang K X, Li Z Q, Liu J, Wang Q L 2022 *Phys. Rev. Appl.* **18** 054077
[37] Zeng P, Zhou H, Zhang W, Xu B J, Liu B, Gao Z 2022 *Nat. Commun.* **13** 3903
[38] Zhu H T, Zhang C M, Pei C X, Li H W 2022 *PRX Quantum* **3** 020353
[39] Zhou L, Sheng Y B, Long G L 2020 *Sci. Bull.* **65** 12
[40] Qi R Y, Sun Z, Lin Z, Niu J L, Hao P L, Song L J, Gao F 2019 *Light Sci. Appl.* **8** 22
[41] Long G L, Zhang H R 2021 *Sci. Bull.* **66** 1267
[42] Liu X, Li Z J, Luo D, Huang C F, Ma D, Geng M M, Wang J W, Wei K J L 2021 *Sci. China-Phys. Mech. Astron.* **64** 120311
[43] Cao Z W, Yao F W, Xiao X Q 2021 *Phys. Rev. Appl.* **16** 024012
[44] Zhang H R, Sun Z, Qi R Y, Yin L G, Long G L, Lu J H 2022 *Light Sci. Appl.* **11** 83
[45] Liu X, Luo D, Lin G S, Chen Z H, Huang C F, Li S Z, Zhang C X, Zhang Z R, Wei K J 2022 *Sci. China-Phys.*

Mech. Astron. **65** 120311
[46] Sheng Y B, Zhou L, Long G L 2022 *Sci. Bull.* **67** 367
[47] Zhou L, Sheng Y B 2022 *Sci. China-Phys. Mech. Astron.* **65** 250311
[48] Ying J W, Zhou L, Zhong W, Sheng Y B 2022 *Chin. Phys. B* **31** 120303
[49] Niu J L, Liu X C 2022 *Eurphys. Lett.* **139** 38001
[50] Wu J W, Long G L, Hayashi M 2022 *Phys. Rev. Appl.* **17** 064011
[51] Das N, Paul G 2022 *Europhys. Lett.* **138** 48001
[52] Cao Z W, Yao F W, Xiao X Q 2023 *Laser Phys. Lett.* **20** 045201
[53] Zhou L, Sheng Y B, Long G L 2023 *Phys. Rev. Appl.* **19** 014036
[54] Dŭsek M, Haderka O, Hendrych M, Gisin N 1999 *Phys. Rev. A* **60** 149
[55] Zeng G H, Zhang W P 2000 *Phys. Rev. A* **61** 022303
[56] Ljunggren D, Bourennane M, Karlsson A 2000 *Phys. Rev. A* **62** 022305
[57] Shi B S, Jiang Y K, Guo G C 2001 *Phys. Lett. A* **281** 83
[58] Zhang H G, Ji Z X, Wang H Z, Wu W Q 2019 *Chin. Commun.* **10** 1
[59] Tsai C W, Hwang T, Kuo L J 2011 *Commun. Theor. Phys.* **56** 1023
[60] Li J X, Zhang Y S, Guo G C 2021 *Europhys. Lett.* **133** 20004
[61] Dutta A, Pathak A 2022 *Quantum Inf. Process.* **21** 369
[62] Crépeau C, Salvail L 1995 *Quantum Oblivious Mutual Identification* (Berlin: Springer) p133
[63] Zeng G H, Wang X B 1998 arXiv: quant-ph/9812022
[64] Zhu D X, Zhao Z L, Zhang H J, Zhou Z Q, Li Y B, Zhao J, Song L J, Zheng J 2025 *J. King Saud Univ. Comput. Inf. Sci.* **37** 57
[65] Zhao W, Shi R H, Shi J J, Huang P, Guo Y, Huang D 2021 *Phys. Rev. A* **103** 012410
[66] Li Q, Wu J J, Quan J Y, Shi J J, Zhang S C 2022 *IEEE Trans. Inf. Forensics Secur.* **17** 3264
[67] Zhang X L 2009 *Chin. Sci. Bull.* **54** 2018
[68] Hong C H, Heo J, Jang J G, Kwon D 2017 *Quantum Inf. Process.* **16** 236
[69] Zawadzki P 2019 *Quantum Inf. Process.* **18** 7
[70] González-Guillén C E, González Vasco M I, Johnson F, Pérez del Pozo Á L 2021 *Entropy* **23** 389
[71] Calsi D L, Kohl P 2024 *Quantum Inf. Process.* **23** 357
[72] Rao B D, Jayaraman R 2023 *Quantum Inf. Process.* **22** 92
[73] Lee H, Lim J, Yang H J 2006 *Phys. Rev. A* **73** 042305
[74] Zhang Z J, Liu J, Wang D, Shi S H 2007 *Phys. Rev. A* **75** 026301
[75] Chang Y, Xu C X, Zhang S B, Yan L 2014 *Chin. Sci. Bull.* **59** 2541
[76] Zhang S S, Chen Z K, Shi R H 2020 *Int. J. Theor. Phys.* **59** 236
[77] Dutta A, Pathak A 2023 *Quantum Inf. Process.* **22** 13
[78] Ma H Q, Huang P, Bao W S, Zeng G H 2016 *Quantum Inf. Process.* **15** 2605
[79] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen, C S, Andersen U L 2015 *Nat. Photonics* **9** 397
[80] Xu F H, Curty M, Qi B, Qian L, Lo H K 2015 *Nat. Photonics* **9** 772
[81] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S, Andersen U L 2015 *Nat. Photonics* **9** 773
[82] Chen Z P, Yao F W, Xiao X Q 2024 *Laser Phys. Lett.* **21** 115201
[83] Liu W J, Chen H W, Li Z Q, Liu Z H, Hu W B 2009 *Chin. Phys. B* **18** 4105
[84] Zhu H F, Wang L W, Zhang Y L 2020 *Quantum Inf. Process.* **19** 381
[85] Wang J, Zhang Q, Tang C J 2006 *Chin. Phys. Lett.* **23** 2360
[86] Yuan H, Liu Y M, Pan G Z 2014 *Quantum Inf. Process.* **13** 2535
[87] Curty M, Santos D J 2001 *Phys. Rev. A* **64** 062309
[88] Liu D, Pei C X, Quan D X, Zhao N 2010 *Chin. Phys. Lett.* **27** 050306
[89] Chang Y, Zhang S B, Yan L L, Han G H 2015 *Chin. Phys. B* **24** 050307
[90] Zhou Z R, Sheng Y B, Niu P H, Yin L G, Long G L, Hanzo L 2020 *Sci. China-Phys. Mech. Astron.* **63** 230362
[91] Das N, Paul G 2022 *Quantum Inf. Process.* **21** 260
[92] Li G D, Liu J C, Wang Q L, Sun W Q 2024 *IEEE Commun. Lett.* **28** 473
[93] Zhou N R, Zeng G H, Zeng W J, Zhu F C 2005 *Opt. Commun.* **254** 380
[94] Xin X J, He F, Qiu S J, Li C Y, Li F G 2024 *Chin. J. Phys.* **92** 664
[95] Yang Y G, Wen Q Y 2009 *Chin. Phys. B* **18** 3233
[96] Zhang Z S, Zeng G H, Zhou N R, Xiong J 2006 *Phys. Lett. A* **356** 199
[97] Wang X F, Gu S P, Sheng Y B, Zhou L 2023 *Europhys. Lett.* **142** 68002
[98] Zhang Q, Du M M, Zhong W, Sheng Y B, Zhou L 2024 *Ann. Phys. (Berlin)* **536** 2300407
[99] Nicolas A, Veissier L, Giner L, Giacobino E, Maxein D, Laurat J 2014 *Nat. Photonics* **8** 234
[100] Sukachev D D, Sipahigil A, Nguyen C T, Bhaskar M K, Evans R E, Jelezko F, Lukin M D 2017 *Phys. Rev. Lett.* **119** 223602
[101] Zhong T, Kindem J M, Bartholomew J G, Rochman J, Craiciu I 2017 *Science* **357** 1392
[102] Liu X, Hu J, Li Z F, Li X, Li P Y, Liang P J, Zhou Z Q, Li C F, Guo G C 2021 *Nature* **594** 41
[103] Jin M, Ma Y Z, Zhou Z Q, Li C F, Guo G C 2022 *Sci. Bull.* **67** 676

SPECIAL TOPIC—Quantum information processing

Latest research progress of quantum identity authentication*

WANG Xingfu [1)] ZHENG Yanyan [2)†] GU Shipu [3)] ZHANG Qi [1)]
ZHONG Wei [4)] DU Mingming [3)] LI Xiyun [1)] SHEN Shuting [3)]
ZHANG Anlei [1)] ZHOU Lan [1)] SHENG Yubo [3)‡]

1) (*College of Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*)

2) (*School of Physics and Electronic Information, Yan'An University, Yan'an* 716000, *China*)

3) (*College of Electronic and Optical Engineering & College of Flexible Electronics* (*Future Technology*), *Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*)

4) (*School of Communications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 12 July 2025; revised manuscript received 5 September 2025)

Abstract

The absolute security of quantum communication protocols relies on a critical premise: all participating parties are legitimate users. Ensuring the legitimacy of participant identities is paramount in complex real-world communication environments. Quantum identity authentication (QIA), in which fundamental principles of quantum mechanics are used to achieve unilateral or mutual authentication between communicating parties, constitutes an indispensable core component for building a comprehensive quantum secure communication system. It holds significant research value in the field of quantum communication.

This review employs a comparative classification method to systematically outline the research trajectory of QIA protocols. By categorizing protocols based on the required quantum resources and the types of quantum protocols employed, the advantages and disadvantages of various categories are analyzed in terms of efficiency, security, and practicality. Single-photon protocols require low resources, and they are easy to implement, and compatible with existing optical components, but require high-efficiency single-photon detectors and exhibit weak noise resistance. Entangled-state protocols offer high security and strong resistance to eavesdropping, particularly suitable for long-distance or multi-party authentication. However, they greatly depend on the preparation and maintenance of high-precision, stable multi-particle entanglement sources, resulting in high experimental complexity. Continuous-variable (CV) protocols achieve high transmission efficiency in short-distance metropolitan area networks and are compatible with classical optical communication equipment, making experiments relatively straightforward. Yet, they require high-precision modulation technology and are sensitive to channel loss. Hybrid protocols aim to balance resource efficiency and security while reducing reliance on a single quantum source, but their design is complex and may introduce new attack vectors. Quantum key distribution (QKD) framework protocols embed identity authentication in the key distribution process, making them suitable for scenarios requiring long-term secure key distribution, although they often depend on pre-shared keys or trusted third parties. Quantum secure direct communication (QSDC) framework protocols integrate authentication with secure direct information transmission, offering high efficiency for real-time communication, but requiring high channel quality. Measurement-device-independent QSDC (MDI-QSDC)

* Project supported by the National Natural Science Foundation of China (Grant Nos. 12175106, 92365110).

† Corresponding author. E-mail: yyz@yau.edu.cn

‡ Corresponding author. E-mail: shengyb@njupt.edu.cn

represents a key development direction that can resist attacks on measurement devices. Quantum teleportation (QT) framework protocols achieves cross-node authentication and unconditional security, making it suitable for quantum relay networks despite its high experimental complexity. The entanglement swapping framework protocol can resist conspiracy attacks and is suitable for multi-party joint scenarios, but it consumes a lot of resources and relies on trusted third party. Ping-pong protocol framework supports dynamic key updates and exhibits strong resistance to eavesdropping, making it suitable for temporary authentication on mobile terminals, although it typically only supports unilateral authentication and requires a bidirectional channel.

Subsequently, this review details the latest QIA protocols of our research group, including a multi-party synchronous identity authentication protocol based on Greenberger-Horne-Zeilinger (GHZ) states, and a tripartite QSDC protocol with identity authentication capabilities utilizing polarization-spatial super-coding. The GHZ-based multi-party synchronous authentication protocol leverages the strong correlations inherent in GHZ states to achieve simultaneous authentication among multiple parties. Through a carefully designed two-round decoy-state detection mechanism, it effectively resists both external eavesdropping and internal attacks originating from authenticated users, thereby enhancing the efficiency and security of identity management in large-scale quantum networks. The core innovation of the polarization-spatial super-coding tripartite QSDC protocol lies in its deep integration of the authentication process with information transmission by utilizing the spatial degrees of freedom of single photons. This design accomplishes the identity verification of two senders and the transmission of secret information within a single protocol run, ensuring end-to-end security through a three-stage security check. This "authentication-as-communication" paradigm significantly improves the overall efficiency and practicality of the protocol. Its successful implementation also relies on advancements in quantum memory technology.

Finally, the review outlines future research directions for quantum identity authentication and explores its potential applications in quantum communication. The QIA research needs to focus on reducing resource dependency, exploring more efficient protocol designs, further enhancing protocol integration and robustness, prioritizing the development of protocols adaptable to real-world environments, and actively investigating integration with novel scenarios. This comprehensive review aims to provide theoretical research foundations and technical support for the practical development of future quantum identity authentication.

Keywords: quantum identity authentication, quantum secure communication, quantum entanglement

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.7498/aps.74.20250920

CSTR: 32037.14.aps.74.20250920

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

量子身份认证研究进展

王兴福 郑艳艳 顾世浦 张琦 钟伟 杜明明 李喜云 沈淑婷 张安蕾 周澜 盛宇波

Latest research progress of quantum identity authentication

WANG Xingfu ZHENG Yanyan GU Shipu ZHANG Qi ZHONG Wei DU Mingming LI Xiyun SHEN Shuting ZHANG Anlei ZHOU Lan SHENG Yubo

引用信息 Citation: Acta Physica Sinica, 74, 210302 (2025) DOI: 10.7498/aps.74.20250920
CSTR: 32037.14.aps.74.20250920
在线阅读 View online: https://doi.org/10.7498/aps.74.20250920
当期内容 View table of contents: http://wulixb.iphy.ac.cn
