软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(11):5376−5391 [doi: 10.13328/j.cnki.jos.006738]

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

基于测量设备无关的可认证身份量子投票方案*

柯唯阳, 石润华

(华北电力大学 控制与计算机工程学院, 北京 102206)

通信作者: 石润华, E-mail: rhshi@ncepu.edu.cn

摘　要: 为解决量子通信过程中的身份认证及协议的可实现性问题, 提出一种基于测量设备无关的带身份认证服务器的量子安全直接通信协议, 并依据该协议提出一种量子投票方案. 所提方案利用测量设备无关的量子密钥分配, 完备的量子加密, 以及经典的一次一密等技术, 不仅理论上确保方案的无条件安全性, 而在实际上也避免外部攻击者对测量设备漏洞的攻击. 此外, 所提方案使用 BB84 态的弱相干脉冲作为量子资源, 仅实施单粒子操作, 以及识别 Bell 态的测量. 因此, 基于现有技术, 所提方案具有良好的可实现性. 同时所提方案扩展了身份认证功能, 引入比特承诺, 使得监票人可以验证投票信息的完整性和正确性. 仿真结果和分析表明, 所提方案是正确的并具有理论上无条件的安全性, 即信息理论安全. 相较于现有的量子投票方案, 所提方案具有更好的可行性.

关键词: 量子投票; 量子安全直接通信; 测量设备无关; 身份认证

中图法分类号: TP309

中文引用格式: 柯唯阳, 石润华. 基于测量设备无关的可认证身份量子投票方案. 软件学报, 2023, 34(11): 5376–5391. http://www.jos.org.cn/1000-9825/6738.htm

英文引用格式: Ke WY, Shi RH. Measurement-device-independent Quantum Voting Scheme with Identity Authentication. Ruan Jian Xue Bao/Journal of Software, 2023, 34(11): 5376–5391 (in Chinese). http://www.jos.org.cn/1000-9825/6738.htm

Measurement-device-independent Quantum Voting Scheme with Identity Authentication

KE Wei-Yang, SHI Run-Hua

(School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China)

Abstract: This study proposes a measurement-device-independent (MDI) quantum secure direct communication (QSDC) protocol with an identity authentication server to solve the problems concerning identity authentication and protocol feasibility during quantum communication and further puts forward a quantum voting scheme on the basis of the proposed MDI-QSDC protocol. This scheme takes advantage of various technologies, such as MDI quantum key distribution, perfect quantum encryption, and the classical one-time pad. In this way, it not only ensures its unconditional security in theory but also avoids the attack of the vulnerabilities of the measurement equipment by outside attackers in practice. Furthermore, this scheme takes the weak coherent pulses in the BB84 state as quantum resources and only performs single-particle operations and the measurements for identifying Bell states. As a result, this scheme is highly feasible for the present technologies. In addition, it extends the identity authentication function and enables the scrutineer to verify the integrity and correctness of voting information by adopting the Bit Commitment. Simulation results and analysis show that the proposed scheme is correct and has unconditional security in theory, i.e., information-theoretic security. Compared with the existing quantum voting schemes, the proposed scheme is more feasible.

Key words: quantum voting; quantum secure direct communication (QSDC); measurement-device-independent (MDI); identity authentication

电子投票因其具有高效率、低成本等优势, 已广泛应用于选举及决策等日常场景中. 在众多电子投票协议中, 最具代表性的是 1992 年由 Fujioka 等人提出的 FOO 协议[1]. 电子投票协议通常使用公钥加密 (public key

* 基金项目: 国家自然科学基金 (61772001)
收稿时间: 2022-03-09; 修改时间: 2022-05-31; 采用时间: 2022-07-17; jos 在线出版时间: 2023-06-16
CNKI 网络首发时间: 2023-06-19

encryption) 技术以保证传输过程中的安全性, 常见的公钥加密算法包括基于大数分解问题的 RSA 算法和基于离散对数问题的 ElGamal 算法[2], 其安全性由数学问题求解的复杂性所保证. 然而随着量子计算机的发展, 其计算能力相较于传统计算机具有显著的优势, 2019 年 10 月, 谷歌 (Google) 基于其 53 量子比特芯片宣称其首先实现了量子霸权 (quantum supremacy)[3,4], 2020 年 12 月, 中国科学技术大学 76 个光子的量子计算原型机“九章”完成对“高斯玻色取样”问题的快速求解, 其计算速度相较于超级计算机具有显著的优势[5]. 量子计算机的出现使得现有基于计算复杂性的经典密码学算法不再安全, 部分学者为解决量子计算这一威胁开展了对后量子密码 (post-quantum cryptography) 这一领域的研究[6,7]. 量子密码学 (quantum cryptography) 因其安全性受量子力学原理所保证[8,9], 具有理论上无条件的安全性, 也受到了学者的广泛关注. 量子密码学的研究范畴很广, 包括量子密钥分配 (quantum key distribution, QKD), 量子安全直接通信 (quantum secure direct communication, QSDC), 量子秘密分享 (quantum secret share, QSS), 量子认证 (quantum authentication), 量子投票 (quantum voting) 等. 其中, QKD 指基于量子力学基本原理的安全密钥分发方式, 是一种理论上无条件安全的通信方式, 根据使用的量子资源不同可以分为基于单粒子系统的 QKD、基于纠缠粒子系统的 QKD 及单粒子和纠缠粒子混合系统的 QKD[10]. 在众多 QKD 协议中最具代表性的是 1984 年由 Bennett 等人提出的 BB84 协议[11]. QSDC 指利用量子力学方法直接传输经典信息的量子通信方法, 不需要预先产生密钥来加密信息, QSDC 根据使用的量子资源不同可以分为基于单光子和基于纠缠态两种类型[12,13], 根据应用场景的不同又包含量子广播通信 (QBC) 和受控量子安全直接通信 (CQSDC)[14], 最早的 QSDC 算法由 Bostro 等人在 2002 年提出, 又称 Ping-Pong 协议[15].

随着量子密码的迅猛发展, 出现了多种基于量子密码的电子投票 (简称量子投票) 方案. 2006 年, Hillery[16]提出了移动式和分配式两种量子投票模型, 2007 年, Vaccaro 等人[17]提出了量子投票需要满足的基本原则, 并提出了比较投票 (comparative ballot) 的量子投票方案. 随后其他学者也提出了他们的量子投票方案, 根据使用的量子资源的不同, 部分学者利用纠缠态资源和多粒子测量来实现投票信息的传输[18,19], 具有较好的效率. 然而其使用的量子资源和量子操作较为困难, 因此不具有较好的可实现性; 部分学者利用单光子作为量子资源来编码投票信息[20,21], 其优点是具有较好的可行性. 此外, 部分学者也尝试使用不同的量子密码学工具提出了他们的量子投票协议. 2016 年, Wang 等人[22]基于量子安全多方求和的思想, 提出了一种自计票的量子投票协议. 2018 年, 秦加奇等人[23]提出了一种基于受控量子安全直接通信的量子投票协议. 2020 年, Zhang 等人[24]利用量子签名技术[25]对投票信息进行编码, 提出了一种基于盲签名和组签名的量子投票协议, 2021 年, Shi 等人[26]根据中国剩余定理提出了一种移动式量子投票协议. 现有的量子投票方案从理论上满足电子投票中的多种安全需求, 但其可实现性尚不及经典的电子投票, 大部分投票方案利用多量子纠缠及 Bell 态测量来编码投票信息, 并利用 QKD 进行密钥分配. 其所使用的量子资源及量子操作较难实现, 并且在进行 QKD 的过程中没有考虑到实际设备的不完美, 这可能导致在实际应用中受到外部攻击者的攻击[27−31].

2012 年, Lo 等人[32]提出了测量设备无关 (measurement-device-independent, MDI) 的量子密钥分配方案 (quantum key distribution, QKD), 该方案使用弱相干脉冲 (weak coherent pulses, WCPs) 作为量子资源, 利用不可信的第三方代理进行测量, 避免了攻击者对于测量端的攻击, 并随后于 2015 年提出了基于测量设备无关的密码学[33]. 许多学者基于其思想提出了多种协议, 2019 年 Zhou 等人[34]提出了一种基于 MDI 的 QSDC 方案, 同年, Cui 等人[35]提出了一种基于测量设备无关的 Hyper-encoding 方案, 2021 年, Rong 等人[36]提出了一种半量子的安全直接通信方案, Choi 等人[37]提出了一种基于测量设备无关的身份认证方案. 现有的基于 MDI 的 QSDC 方案通过在消息的发送者和接收者之间建立一条安全的、经过身份认证的经典信道来实现消息发送者和接收者之间的身份认证. 受限于这种基于认证经典信道的方式, 当多个用户之间使用 QSDC 方案进行通信时, 则需要在每个用户之间都建立一条认证的经典信道, 增加了系统的开销. 因此基于其研究成果, 在本文中我们提出了一种基于测量设备无关的带身份认证服务器的 QSDC 协议, 该协议引入身份认证服务器为消息的发送者分配秘密的身份信息, 同时辅助消息的发送者执行所述 QSDC 协议, 并且秘密信息可通过公开的信道进行传输, 无需消息接收方和发送方之间认证的经典信道. 进而依据该协议提出了一种可认证身份的、完备的量子投票方案, 该方案结合比特承诺机制和所述 QSDC 协议中秘密的身份信息, 使得监票人可以验证投票信息的正确性及完整性进而验证投票者的身份.

具有匿名、可验证、不可二次投票等较为完备的安全属性. 最后, 我们利用 IBM Qiskit 进行了仿真验证. 相较于现有的量子投票方案, 我们方案的优势体现在: (1) 仅使用 WCPs 作为量子资源, 必要的操作和测量仅为单光子操作及 Bell 态识别, 因而具有良好的可实现性. (2) 利用 MDI-QKD 的原理, 可以抵抗攻击者对测量设备漏洞的攻击. (3) 引入身份认证和比特承诺, 使得监票人可以验证投票信息的正确性.

本文的主要贡献如下.

(1) 借鉴 MDI-QKD 的思想设计了一个 MDI-QSDC 协议, 结合完备的量子加密以及经典的后处理技术, 保证了投票人把投票信息安全的传输给计票人/监票人.

(2) 引入身份认证服务器, 结合比特承诺机制, 在量子执行过程中的一个环节嵌入秘密的身份信息, 最后通过打开承诺验证用户的合法性和真实性. 即一次认证确保整个协议中参与方的真实性, 不需要多轮验证, 从而提高效率. 同时, 认证过程不需要借助经典的认证通道.

本文第 1 节介绍本文所需的基础知识. 第 2 节介绍本文提出的基于 MDI 的带身份认证服务器的 QSDC 协议. 第 3 节介绍基于第 2 节所述协议的量子投票方案. 第 4 节对所述协议的安全性和正确性进行证明. 第 5 节对所述协议的性能进行分析与比较, 最后总结全文.

1 预备知识

为了更好地理解后面所设计的协议, 我们首先对 MDI-QKD 所采用的量子资源及实现原理进行简要介绍. 在 QKD 理论中多是采用理想的单光子, 但现实中受限于实际设备, QKD 协议中多用近似的单光子源. 主流的近似单光子源方案包括确定性单光子源和概率性单光子源[38]. 这里我们重点介绍概率性单光子源中的弱相干态光源 (weak coherent source, WCS).

1.1 弱相干态光源

弱相干态光源是由激光经过调制后得到的概率性单光子源, 其光场满足泊松分布, 光子数态密度矩阵如下[39]:

$$\rho_{\mu}=\sum_{n}\frac{\mu^{n}}{n!}\mathrm{e}^{-\mu}|n\rangle\langle n| \tag{1}$$

其中, μ 为平均光子数, $|n\rangle$ 表示 n 光子态, $|\rangle$ 和 $\langle|$ 分别表示右矢和左矢. 这里的光子数态又称为 Fock 态[40], 其含义为光子数算符的本征值所对应的电磁场中包含的光子的个数. 在此引入光子数算符 $\hat{n}=a^{+}a$, 由 $\hat{n}$ 和哈密顿量算符 H 的对易关系及光子数算符 H 的本征方程可以推出下列方程:

$$a|n\rangle=\sqrt{n}|n-1\rangle \tag{2}$$

$$a^{+}|n\rangle=\sqrt{n+1}|n+1\rangle \tag{3}$$

其中, n=0 的状态 $|0\rangle$ 称为真空态, 将 a 称为光子湮灭算符, a^{+}称为光子产生算符. 由公式 (3) 的递推关系可得:

$$|n\rangle=\frac{(a^{+})^{n}}{\sqrt{n!}}|0\rangle \tag{4}$$

1.2 测量设备无关的密钥分配 (MDI-QKD)

MDI-QKD 原理图如图 1 所示, 其原理是利用分束器 (beam splitter, BS) 实现 HOM 型干涉[41], 极化分束器 (polarizing beam splitter, PBS) 用于分离处于不同极化状态的光子, 诱骗态强度调制器 (decoy intensity modulator, Decoy-IM) 用于调制诱骗态, 极化调制器 (polarization modulator, Pol-M) 用于调制光子的极化状态. 当入射的两个光子为全同光子时, 两个光子从分束器两侧同时射出的概率相干相消, 即两个光子将从同一出口射出. 根据这一分束器的光学性质, 使得入射光子的光子态和输出端的探测器响应情况具有对应关系, 从而在不泄露密钥信息的前提下实现 Alice 和 Bob 之间的密钥分配.

光学分束器的原理如图 2 所示, 其输入端和输出端的光子产生算符具有如下的关系[42].

$$a_{|i\rangle}^{+}=\frac{1}{\sqrt{2}}\left(c_{|i\rangle}^{+}+d_{|i\rangle}^{+}\right) \tag{5}$$

$$b^{+}_{|i\rangle}=\frac{1}{\sqrt{2}}\left(c^{+}_{|i\rangle}-d^{+}_{|i\rangle}\right) \tag{6}$$

其中, 下标$|i\rangle$表示在产生算符作用后会产生一个处于状态$|i\rangle$的光子, $|i\rangle\in\{|0\rangle,|1\rangle\}$.

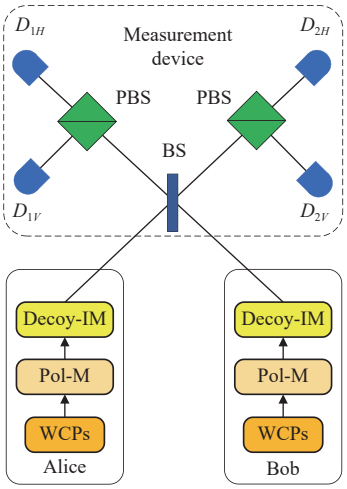

图 1 测量设备无关的密钥分配

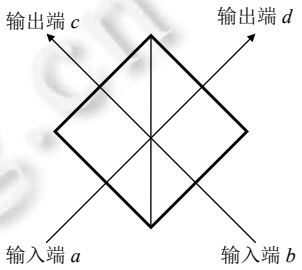

图 2 光学分束器

当 a、b 两端输入处于相同极化状态的光子时 ($|00\rangle_{ab}$或$|11\rangle_{ab}$), 其通过光学分束器后的状态可以用产生算符和 Fock 态的形式表示为:

$$|00\rangle_{ab}=a^{+}_{|0\rangle}b^{+}_{|0\rangle}|0,0\rangle_{a,b}=\frac{1}{2}\left(c^{+}_{|0\rangle}+d^{+}_{|0\rangle}\right)\left(c^{+}_{|0\rangle}-d^{+}_{|0\rangle}\right)|0,0\rangle_{c,d} \tag{7}$$

$$|11\rangle_{ab}=a^{+}_{|1\rangle}b^{+}_{|1\rangle}|0,0\rangle_{a,b}=\frac{1}{2}\left(c^{+}_{|1\rangle}+d^{+}_{|1\rangle}\right)\left(c^{+}_{|1\rangle}-d^{+}_{|1\rangle}\right)|0,0\rangle_{c,d} \tag{8}$$

当 a、b 两端输入处于不同极化状态的光子时 ($|01\rangle_{ab}$或$|10\rangle_{ab}$), 其通过光学分束器后的状态可以用产生算符和 Fock 态的形式表示为:

$$|01\rangle_{ab}=a^{+}_{|0\rangle}b^{+}_{|1\rangle}|0,0\rangle_{a,b}=\frac{1}{2}\left(c^{+}_{|0\rangle}+d^{+}_{|0\rangle}\right)\left(c^{+}_{|1\rangle}-d^{+}_{|1\rangle}\right)|0,0\rangle_{c,d} \tag{9}$$

$$|10\rangle_{ab}=a^{+}_{|1\rangle}b^{+}_{|0\rangle}|0,0\rangle_{a,b}=\frac{1}{2}\left(c^{+}_{|1\rangle}+d^{+}_{|1\rangle}\right)\left(c^{+}_{|0\rangle}-d^{+}_{|0\rangle}\right)|0,0\rangle_{c,d} \tag{10}$$

其中, $|ij\rangle_{ab}$表示 a 端输入的光子处于极化状态$|i\rangle$, b 端输入的光子处于极化状态$|j\rangle$, $|0,0\rangle_{a,b}$和$|0,0\rangle_{c,d}$分别表示在 a、b 端和 c、d 端 Fock 态的真空态.

当 a、b 端输入的光子处于 Bell 态时, 其通过光学分束器后的状态为:

$$\left|\varphi^{+}\right\rangle_{ab}=\frac{1}{\sqrt{2}}\left(|00\rangle_{ab}+|11\rangle_{ab}\right)=\frac{1}{2}\left(c^{+}_{|0\rangle}c^{+}_{|0\rangle}-d^{+}_{|0\rangle}d^{+}_{|0\rangle}-c^{+}_{|1\rangle}c^{+}_{|1\rangle}+d^{+}_{|1\rangle}d^{+}_{|1\rangle}\right)|0,0\rangle_{c,d} \tag{11}$$

$$\left|\varphi^{-}\right\rangle_{ab}=\frac{1}{\sqrt{2}}\left(|00\rangle_{ab}-|11\rangle_{ab}\right)=\frac{1}{2}\left(c^{+}_{|0\rangle}c^{+}_{|0\rangle}-d^{+}_{|0\rangle}d^{+}_{|0\rangle}+c^{+}_{|1\rangle}c^{+}_{|1\rangle}-d^{+}_{|1\rangle}d^{+}_{|1\rangle}\right)|0,0\rangle_{c,d} \tag{12}$$

$$\left|\psi^{+}\right\rangle_{ab}=\frac{1}{\sqrt{2}}\left(|01\rangle_{ab}-|10\rangle_{ab}\right)=\frac{1}{\sqrt{2}}\left(c^{+}_{|0\rangle}c^{+}_{|1\rangle}-d^{+}_{|1\rangle}d^{+}_{|0\rangle}\right)|0,0\rangle_{c,d} \tag{13}$$

$$\left|\psi^{-}\right\rangle_{ab}=\frac{1}{\sqrt{2}}\left(|01\rangle_{ab}+|10\rangle_{ab}\right)=\frac{1}{\sqrt{2}}\left(c^{+}_{|0\rangle}d^{+}_{|1\rangle}-c^{+}_{|1\rangle}d^{+}_{|0\rangle}\right)|0,0\rangle_{c,d} \tag{14}$$

根据 c、d 端探测器响应的特异性, 我们可以区分 4 种 Bell 态中的 2 种. 当 c 端测量极化状态$|0\rangle$的探测器和测量极化状态$|1\rangle$的探测器同时响应, 或者当 d 端测量极化状态$|0\rangle$的探测器和测量极化状态$|1\rangle$的探测器同时响应, 表示此时 a、b 端输入的状态为$|\psi^{+}\rangle_{ab}$; 当 c 端测量极化状态$|0\rangle$的探测器和 d 端测量极化状态$|1\rangle$的探测器同时响应, 或者当 c 端测量极化状态$|1\rangle$的探测器和 d 端测量极化状态$|0\rangle$的探测器同时响应, 表示此时 a、b 端输入

的状态为 $|\psi^-\rangle_{ab}$.

因此, 当第三方测量端的识别结果为 $|\psi^+\rangle$ 和 $|\psi^-\rangle$ 时记为识别成功, 其余情况记为识别失败.

在 MDI-QKD 协议中, 密钥分配双方 Alice 和 Bob 随机制备处于 BB84 状态下的 WCPs, 并将 WCPs 发送给第三方测量代理 Charlie 进行 Bell 态识别, 由 Charlie 公布 Bell 态识别的结果. 随后, Alice 和 Bob 通过认证的可信经典信道公开对基, 选择 Charlie 识别结果成功且处于相同基 (Z 基或 X 基) 的 WCPs 对用于密钥分配.

根据表 1, 可以得出如表 2 所示的 MDI-QKD 协议的编码表, 密钥分配双方 Alice 和 Bob 根据事先的约定, 由一人执行比特翻转, 即可保证通信双方手中的密钥一致, 并且第三方测量代理 Charlie 无法通过他的 Bell 态识别结果获取通信双方手中密钥的信息.

表 1 MDI-QKD 初始状态与测量结果

WCP1	WCP2	Measurement result			
		$\|\varphi^+\rangle$	$\|\varphi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
$\|0\rangle$	$\|0\rangle$	√	√	—	—
$\|0\rangle$	$\|1\rangle$	—	—	√	√
$\|1\rangle$	$\|0\rangle$	—	—	√	√
$\|1\rangle$	$\|1\rangle$	√	√	—	—
$\|+\rangle$	$\|+\rangle$	√	—	√	—
$\|-\rangle$	$\|-\rangle$	√	—	√	—
$\|+\rangle$	$\|-\rangle$	—	√	—	√
$\|-\rangle$	$\|+\rangle$	—	√	—	√

表 2 MDI-QKD 协议的编码表

Alice & Bob	Charlie output	
	$\|\psi^+\rangle$	$\|\psi^-\rangle$
Z basis ($\|0\rangle$ $\|1\rangle$)	Bit flip	Bit flip
X basis ($\|+\rangle$ $\|-\rangle$)	No bit flip	Bit flip

2 基于 MDI 的带身份认证服务器的 QSDC 协议

2.1 协议的模型及定义

现有的 QSDC 方案包括消息的发送者和接收者两个参与方, 通常是由消息的发送者制备相关的量子资源; 我们提出的基于 MDI 的可认证身份的 QSDC, 其中有一个消息的发送者, 一个接收者, 此外还存在一个专门的身份认证服务器 (也可扩展为可控的 QSDC 中的控制方) 和半诚实的第三方测量代理. 首先发送者在认证服务器注册, 保留认证凭证 (个人 ID 及用于身份认证的密钥 k); 随后由消息的接收者制备相关的量子资源, 消息的发送者在身份认证服务器和第三方测量代理的辅助下, 利用单量子操作对秘密信息进行编码, 并可最终由接收者所解密. 其原理图如图 3 所示, 其中, M 表示调制器 (即图 1 MDI-QKD 协议中的 Pol-M 和 Decoy-IM), Y 表示单量子泡利 Y 门 (Pauli-Y gate) 操作, H 表示哈德玛门 (Hadamard gate) 操作. 我们的 QSDC 协议定义如下 4 个参与方.

(1) 消息的发送者 Client: 接收由 Server 发来的 WCPs, 并根据自己随机生成的随机数 $r_1[j]$, $k_1[j]$ 对收到的 WCPs 执行 $U_Y^{r_1[j]}H^{k_1[j]}$ 操作.

(2) 身份认证服务器 AS (authentication service): 负责验证 Client 身份的合法性并向合法的 Client 分配用于身份认证的信息. 接收由 Server 发来的 WCPs, 并根据自己随机生成的随机数 $r_2[j]$, $k_2[j]$ 对收到的 WCPs 执行 $U_Y^{r_2[j]}H^{k_2[j]}$ 操作.

(3) 第三方测量代理 Agent: 负责对 Client 和 AS 执行完操作后的 WCPs 对进行 Bell 态识别.

(4) 消息的接收者 Server: 负责制备 WCPs 对并发送给 Client 和 AS, 并根据 Client 和 AS 公开的信息及 Agent 的 Bell 态识别结果计算 Client 发送的隐私信息 x.

假定图 3 中量子资源的制备、单量子门操作和 Bell 态识别均是在安全可控的实验室中进行的 (即图 3 虚线框中的部分), 而传输的量子信道是公开的, 可能是不安全的, 敌手 Eve 可以在信道上采用窃听或截获重发的方式获取协议执行的量子资源. 第三方测量端 Agent 可能是不诚实的, 他可能会公布错误的 Bell 态识别结果.

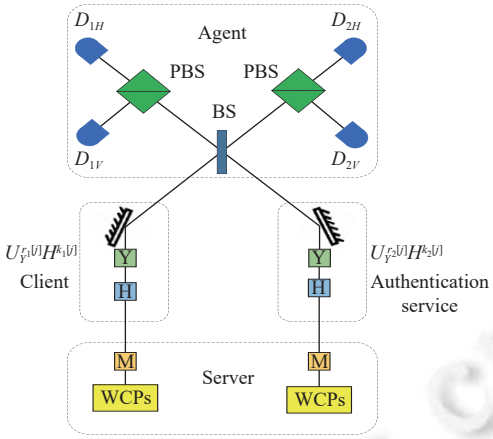

图 3 协议原理图

2.2 协议流程

● 协议初始化阶段

Step 0. 由 AS 验证 Client 身份的合法性, 若合法, 则通过面对面或其他安全的通信方式 (例如 QKD) 共享一个长度为 n 的用于执行协议的密钥 k.

● 协议具体内容

Step 1. Server 随机制备 t 个 ($t \approx 8n$) 处于 BB84 态 ($|0\rangle,|1\rangle,|+\rangle,|-\rangle$) 下的 WCPs 对 (weak coherent pulses pair), 将其中一个 WCPs 发给 Client, 并将另外一个 WCPs 发给 AS, 并保证发给 Client 和 AS 的 WCPs 对处于相同的基下 (Z 基或 X 基), 但其所处的状态可能不同.

Step 2. Client 和 AS 分别对各自收到的 t 个 WCPs 执行 $U_Y^{r_1[j]}H^{k_1[j]}$ 和 $U_Y^{r_2[j]}H^{k_2[j]}$ 操作, 并将执行过操作后的 WCPs 发给 Agent 进行 Bell 态识别. 其中, $r_1[j]$, $k_1[j]$ 为 Client 随机选取的随机数; $r_2[j]$, $k_2[j]$ 为 AS 随机选取的随机数; $r_1[j]$、$k_1[j]$、$r_2[j]$、$k_2[j] \in \{0, 1\}$. 以 Client 为例, 当 $r_1[j]=1$ 时, 表示对 Server 发来的 WCPs 执行单量子泡利 Y 门 (Y) 操作, 当 $k_1[j]=1$ 时, 表示对 Server 发来的 WCPs 执行哈德玛门 (H) 操作, 当 $r_1[j]=0$ 或 $k_1[j]=0$ 时, 表示对 Server 发来的 WCPs 不执行操作, 即 $H^0=Y^0=I$.

Step 3. Agent 在收到 Client 和 AS 发来的 WCPs 后, 对其进行 Bell 态识别, 并公布 Bell 态识别的结果是否成功及成功时的 Bell 态 (若成功识别, 则公布具体的 Bell 态, 否则公布识别失败).

Step 4. Client 和 AS 分别公布各自随机选择的 t 个随机数 $k_1[j]$ 及 $k_2[j]$, $j \in \{1, 2,\ldots, t\}$ 并选出满足 $k_1[j]=k_2[j]$ 的 WCPs 对 (约 $4n$ 对), 即 Client 和 AS 执行完 $U_Y^{r_1[j]}H^{k_1[j]}$ 操作和 $U_Y^{r_2[j]}H^{k_2[j]}$ 后, 发送给 Agent 进行 Bell 态识别的 WCPs 仍为同种基 (Z 基或 X 基).

Step 5. 从满足 Step 4 要求的 WCPs 对中选出 Agent 的 Bell 态识别结果成功的 WCPs 对 (约 $2n$ 对), Client 和 AS 共同从选出的 $2n$ 对 WCPs 对中随机选择 n 对用于传输长度为 n 的秘密信息 x, 并用剩余的 n 对进行诚实性及窃听检测.

Step 6. 对用于诚实性及窃听检测的 n 对 WCPs, Client 和 AS 公布与之相对应的 $r_1[j]$ 和 $r_2[j]$, Server 公布与之相对应的 WCPs 对的初始状态, 参与协议的任何一方都可以根据公开的信息及 Agent 的 Bell 态识别结果计算误码率. 若误码率高于阈值, 则证明存在外部窃听或测量代理 Agent 存在不诚实行为, 终止执行后续协议; 若误码率低于阈值, 则继续执行.

Step 7. 根据选出的用于传输长度为 n 的秘密信息 x 的 n 对 WCPs 及 Client 和 AS 在 Step 2 随机选取的随机数 $r_1[j]$ 和 $r_2[j]$, Client 和 Authentication Service 可以得到一个长度为 n 的用于加密的二进制序列 $r_1=\{r_{11},r_{12},\ldots,r_{1j},\ldots,r_{1n}\}$, $r_2=\{r_{21},r_{22},\ldots,r_{2j},\ldots,r_{2n}\}$, Client 和 AS 分别计算 $m'_{aj}=k_j\oplus r_{1j}\oplus x_j$, $m'_{bj}=k_j\oplus r_{2j}$, 并公布计算后的 n 位结果

$m'_a=\{m'_{a1},m'_{a2},\ldots,m'_{an}\}$、$m'_b=\{m'_{b1},m'_{b2},\ldots,m'_{bn}\}$. 其中 k_j 为 Step 0 中共享的密钥 k 的第 j 位.

Step 8. Server 计算 $m'_a\oplus m'_b=\{m'_{a1}\oplus m'_{b1},m'_{a2}\oplus m'_{b2},\ldots,m'_{an}\oplus m'_{bn}\}$, 其中 $m'_{aj}\oplus m'_{bj}=x_j\oplus r_{1j}\oplus r_{2j}$, $j\in\{1,2,\ldots,n\}$. 根据 MDI-QKD 的原理及表 3、表 4, Server 可以得到 $r_{1j}\oplus r_{2j}$ 的结果, 从而得到秘密信息 x_j 的值.

表 3 当 $k_1[j]=k_2[j]=0$ 时的可能组合

Initial state	Agent output			
	$\|\psi^+\rangle$		$\|\psi^-\rangle$	
	$\|W_A\rangle_j=\|W_B\rangle_j$	$\|W_A\rangle_j\neq\|W_B\rangle_j$	$\|W_A\rangle_j=\|W_B\rangle_j$	$\|W_A\rangle_j\neq\|W_B\rangle_j$
$\|0\rangle\ \|1\rangle$	$r_{1j}\oplus r_{2j}=1$	$r_{1j}\oplus r_{2j}=0$	$r_{1j}\oplus r_{2j}=1$	$r_{1j}\oplus r_{2j}=0$
$\|+\rangle\ \|-\rangle$	$r_{1j}\oplus r_{2j}=0$	$r_{1j}\oplus r_{2j}=1$	$r_{1j}\oplus r_{2j}=1$	$r_{1j}\oplus r_{2j}=0$

表 4 当 $k_1[j]=k_2[j]=1$ 时的可能组合

Initial state	Agent output			
	$\|\psi^+\rangle$		$\|\psi^-\rangle$	
	$\|W_A\rangle_j=\|W_B\rangle_j$	$\|W_A\rangle_j\neq\|W_B\rangle_j$	$\|W_A\rangle_j=\|W_B\rangle_j$	$\|W_A\rangle_j\neq\|W_B\rangle_j$
$\|0\rangle\ \|1\rangle$	$r_{1j}\oplus r_{2j}=0$	$r_{1j}\oplus r_{2j}=1$	$r_{1j}\oplus r_{2j}=1$	$r_{1j}\oplus r_{2j}=0$
$\|+\rangle\ \|-\rangle$	$r_{1j}\oplus r_{2j}=1$	$r_{1j}\oplus r_{2j}=0$	$r_{1j}\oplus r_{2j}=1$	$r_{1j}\oplus r_{2j}=0$

3 基于 MDI 的可认证身份量子投票方案

3.1 投票方案的模型及定义

基于 MDI 的可认证身份量子投票属于分布式的电子投票, 有一个计票人, 一个监票人, 一个身份认证服务器, 一个公告板, 一个第三方测量代理, 和 n 个投票人. 每一位投票人对 n 个候选者进行投票, 同意编码为二进制的 1, 不同意编码为二进制的 0, 并最终得到长度为 n 的二进制投票信息. 在投票过程中, 投票人 Alice 首先在公告板上公布自己的比特承诺信息, 随后在 AS 的辅助下, 利用基于 MDI 的带身份认证服务器的 QSDC 协议将自己的投票信息发送给计票人 Bob, 将用于比特承诺的随机数发送给监票人 David, 最终通过计票人 Bob 在公告板上公布的信息计算投票结果. 其模型图如图 4 所示.

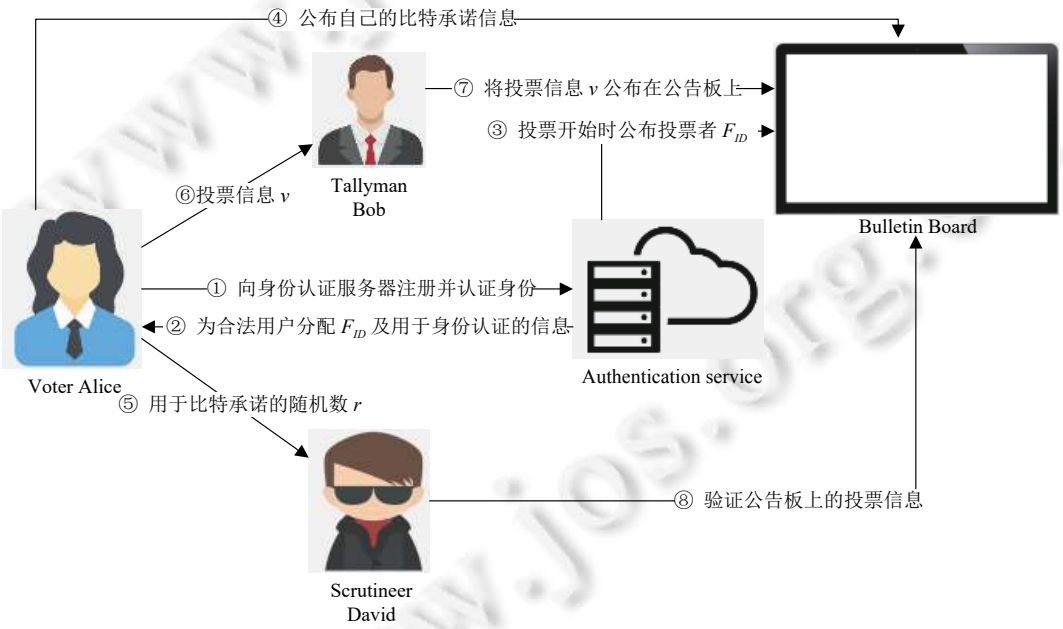

图 4 量子投票模型

3.2 方案流程

我们的量子投票方案定义如下 5 名参与者.

(1) 投票人 Alice: 投票信息的拥有者, 负责为 n 位候选人进行投票.

(2) 身份认证服务器 (AS): 负责认证投票者身份的合法性, 并分配投票所需的秘密的身份信息, 是一个诚实的参与者.

(3) 代理 Charlie: 半诚实的第三方测量代理.

(4) 计票人 Bob: 半诚实的计票人, 负责统计投票人的投票结果并公布在公告板上.

(5) 监票人 David: 半诚实的监票人, 负责验证投票信息的正确性.

假定存在一个公开的安全的哈希函数 h 和一个只可写入不可篡改的电子公告板, 并且计票人和监票人之间是不串谋的. 我们的投票方案包含如下几个步骤, 具体细节如下.

● 初始化阶段

Step 0. Alice 发送个人 ID 给 AS, 向 AS 申请注册并由 AS 验证其身份的合法性以及是否是第 1 次进行投票. 若满足要求, 则通过面对面或其他安全的方式 (例如 QKD) 为 Alice 分配一个用于投票的假名 F_{ID} 及密钥 K_{ID}, Alice 和 AS 利用安全的哈希函数 h 计算用于与计票人 David 进行通信的身份验证信息 $y_i=h(K_{ID})$ 以及用于与监票人 David 进行通信的身份验证信息 $y_i'=h(h(K_{ID}))$, AS 将 Alice 的个人信息 (ID, F_{ID}, K_{ID}) 保存在身份认证服务器中. 若不满足要求, 则拒绝 Alice 的投票请求.

● 投票阶段

Step 1. 投票人 Alice 随机选择一个秘密的随机数 r, 并按照自己的投票意愿生成一个长度为 n 的 0、1 向量 v 作为投票信息, 投票者利用哈希函数 h 计算比特承诺信息 $v'=h(v\oplus h(v\oplus r))$ 并将 v' 公布在公告板上.

Step 2. 投票人 Alice (作为 Client 方) 利用基于 MDI 的带身份认证服务器的 QSDC 协议, 在 AS 的辅助下, 使用假名 F_{ID} 和身份认证信息 $y_i'=h(h(K_{ID}))$ 与监票人 David (作为 Server 方) 进行通信, 将自己用于比特承诺的随机数 r 发送给监票人 David.

Step 3. 投票人 Alice (作为 Client 方) 利用基于 MDI 的带身份认证服务器的 QSDC 协议, 在 AS 的辅助下, 使用假名 F_{ID} 和身份认证信息 $y_i=h(K_{ID})$ 与计票人 Bob (作为 Server 方) 进行通信, 将自己的投票信息 v 发送给计票人 Bob, 由 Bob 将 Alice 的投票信息 (即 F_{ID} 和 v) 公布在公告板上.

● 验票阶段

Step 4. 监票人 David 利用 Alice 发来的随机数 r 和 Bob 公布在公告板上的信息 v 计算 $h(v\oplus h(v\oplus r))$ 并与 Alice 的比特承诺信息 v' 进行比对. 如果不相等, 则指明投票者或者计票人存在不诚实的行为, 拒绝此次投票. 需要注意的是, 在理想情况下, 若与比特承诺信息不一致, 则只能是计票人作弊, 此时用户可以公开 v 和 r 用来提交仲裁, 因为即使用户和监票人串谋也不能修改 v 或 r 来通过比特承诺值的比对 (注: 目前哈希函数能够抵抗量子计算机的攻击).

● 计票阶段

Step 5. 待所有投票者结束投票后, 所有投票人可根据公告板上正确的投票信息得出最终的投票结果.

4 正确性及安全性分析

由于所述的量子投票方案是利用基于 MDI 的带身份认证服务器的 QSDC (相当于可控的 QSDC) 协议进行秘密信息的传输, 因此当所述 QSDC 协议是正确并具有理论上无条件安全性的前提下, 所述投票方案的通信过程也是正确且理论上无条件安全的, 在第 4.1 节和第 4.2 节中将证明所述 QSDC 协议的正确性及安全性, 在第 4.3 节中, 对所述投票方案的安全属性进行分析. 分析结果表明, 所述投票协议的通信过程满足理论上的无条件安全, 即信息理论安全, 并且满足合法性、可验证性、匿名性、完整性、不可二次投票等完备的投票安全属性.

4.1 正确性

定理 1. 当协议中的所有参与者都诚实执行协议的条件下, 所述协议是正确的.

不失一般性, 本文的正确性分析仅考虑第 j 个 WCPs 对, 假设在协议开始时由 Server 制备的 WCPs 对的初始状态为 $|W_A\rangle_j$ 和 $|W_B\rangle_j$, 并保证 $|W_A\rangle_j,|W_B\rangle_j\in\{|0\rangle,|1\rangle\}$ 或 $|W_A\rangle_j,|W_B\rangle_j\in\{|+\rangle,|-\rangle\}$, 随后, Server 将 $|W_A\rangle_j$ 发送给 Client, 将 $|W_B\rangle_j$ 发送给 AS. 在 Client 和 AS 执行完各自的操作后, WCPs 的状态将变为:

$$|W_A\rangle_j' = U_Y^{r_1[j]}H^{k_1[j]}|W_A\rangle_j \tag{15}$$

$$|W_B\rangle_j' = U_Y^{r_2[j]}H^{k_2[j]}|W_B\rangle_j \tag{16}$$

根据协议, 我们对满足 $k_1[j]=k_2[j]$ 的 WCPs 对进行后处理并根据相对应的 $r_1[j]$ 和 $r_2[j]$ 对秘密信息进行编码, 根据 H 门和 Y 门 (不考虑全局相位 i) 的单量子门操作易得:

$$H|0\rangle = |+\rangle, H|1\rangle = |-\rangle \tag{17}$$

$$H|+\rangle = |0\rangle, H|-\rangle = |1\rangle \tag{18}$$

$$Y|0\rangle = |1\rangle, Y|1\rangle = -|0\rangle \tag{19}$$

$$Y|+\rangle = |-\rangle, Y|-\rangle = -|+\rangle \tag{20}$$

由于 $|W_A\rangle_j$ 和 $|W_B\rangle_j$ 的初始状态为同种基态, Y 门操作不改变 WCPs 对的基态, 所以当 $k_1[j]=k_2[j]$ 时, $|W_A\rangle_j'$ 和 $|W_B\rangle_j'$ 仍为同种基态.

根据 MDI-QKD 的原理, 第三方测量代理 Agent 通过探测器的状态仅可以识别 $|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right)$ 和 $|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle-|10\rangle\right)$, 当输入的 Bell 态为 $|\varphi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)$ 和 $|\varphi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle-|11\rangle\right)$ 时, Agent 无法区分这两种状态, 因而该次 Bell 态识别的结果失败.

根据协议, 第三方测量端 Agent 可能收到的 WCPs 对的状态可以表示为如下的几种情况:

$$|00\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^+\rangle+|\varphi^-\rangle\right) \tag{21}$$

$$|01\rangle = \frac{1}{\sqrt{2}}\left(|\psi^+\rangle+|\psi^-\rangle\right) \tag{22}$$

$$|10\rangle = \frac{1}{\sqrt{2}}\left(|\psi^+\rangle-|\psi^-\rangle\right) \tag{23}$$

$$|11\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^+\rangle-|\varphi^-\rangle\right) \tag{24}$$

$$|++\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^+\rangle+|\psi^+\rangle\right) \tag{25}$$

$$|+-\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^-\rangle-|\psi^-\rangle\right) \tag{26}$$

$$|-+\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^-\rangle+|\psi^-\rangle\right) \tag{27}$$

$$|--\rangle = \frac{1}{\sqrt{2}}\left(|\varphi^+\rangle-|\psi^+\rangle\right) \tag{28}$$

因此, 我们可以根据 Agent 的 Bell 态识别结果以及 Server 制备的 WCPs 对的初始状态推断出 Client 和 AS 执行的操作情况, 其中 Bell 态识别结果失败表示 Agent 的 Bell 态识别结果既不是 $|\psi^+\rangle$ 也不是 $|\psi^-\rangle$, 可能的组合情况如表 5 所示.

根据表 5, 可以总结出表 3 中的结果. 同样当 $k_1[j]=k_2[j]=1$ 时, 可以总结出表 4 中的结果. 根据 WCPs 的初始状态和 Agent 的测量结果, Server 可以推断出 $r_{1j}\oplus r_{2j}$ 的值.

由于 Server 可以根据 Client 和 AS 公开的信息计算 $m'_{aj}\oplus m'_{bj} = x_j\oplus r_{1j}\oplus r_{2j}$, 所以通过 $r_{1j}\oplus r_{2j}$ 的值, Server 可以得到秘密信息 x_j 的值, 因而所述的基于 MDI 的带身份认证服务器的 QSDC 协议具有正确性.

4.2 安全性

根据文献 [43], 若对于任何一个输入态, 其输出态均为最大混合态时, 该量子加密协议满足信息论安全 (informational-theoretical security), 在所述协议中, 其输入态及输出态为:

$$\rho_{\text{out}} = \sum\nolimits_k p_k U_k \rho_{\text{in}} U_k^\dagger = \frac{1}{2^t} I \tag{29}$$

其中, ρ_{in} 表示所有可能输入状态的密度矩阵, U_k 表示对于输入状态施加的操作算子, $U_k^{\dagger}$ 为 U_k 的厄米矩阵 (Hermitian matrix). 不失一般性, 我们仅考虑协议中的第 j 个 WCPs, 根据协议可得:

$$\rho_{\text{in}}\left(WCP_j\right)=\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right) \tag{30}$$

表 5 当 $k_1[j]=k_2[j]=0$ 时可能的组合情况

$\|W_A\rangle_j$	$\|W_B\rangle_j$	$r_1[j]$	$r_2[j]$	Agent output	$\|W_A\rangle_j$	$\|W_B\rangle_j$	$r_1[j]$	$r_2[j]$	Agent output	$\|W_A\rangle_j$	$\|W_B\rangle_j$	$r_1[j]$	$r_2[j]$	Agent output	$\|W_A\rangle_j$	$\|W_B\rangle_j$	$r_1[j]$	$r_2[j]$	Agent output
$\|0\rangle$	$\|0\rangle$	0	0	Fail	$\|1\rangle$	$\|0\rangle$	0	0	$\|\psi^+\rangle/\|\psi^-\rangle$	$\|+\rangle$	$\|+\rangle$	0	0	Fail / $\|\psi^+\rangle$	$\|-\rangle$	$\|+\rangle$	0	0	Fail / $\|\psi^-\rangle$
$\|0\rangle$	$\|0\rangle$	0	1	$\|\psi^+\rangle/\|\psi^-\rangle$	$\|1\rangle$	$\|0\rangle$	0	1	Fail	$\|+\rangle$	$\|+\rangle$	0	1	Fail / $\|\psi^-\rangle$	$\|-\rangle$	$\|+\rangle$	0	1	Fail / $\|\psi^+\rangle$
$\|0\rangle$	$\|0\rangle$	1	0	$\|\psi^+\rangle/\|\psi^-\rangle$	$\|1\rangle$	$\|0\rangle$	1	0	Fail	$\|+\rangle$	$\|+\rangle$	1	0	Fail / $\|\psi^-\rangle$	$\|-\rangle$	$\|+\rangle$	1	0	Fail / $\|\psi^+\rangle$
$\|0\rangle$	$\|0\rangle$	1	1	Fail	$\|1\rangle$	$\|0\rangle$	1	1	$\|\psi^+\rangle/\|\psi^-\rangle$	$\|+\rangle$	$\|+\rangle$	1	1	Fail / $\|\psi^+\rangle$	$\|-\rangle$	$\|+\rangle$	1	1	Fail / $\|\psi^-\rangle$
$\|0\rangle$	$\|1\rangle$	0	0	$\|\psi^+\rangle/\|\psi^-\rangle$	$\|1\rangle$	$\|1\rangle$	0	0	Fail	$\|+\rangle$	$\|-\rangle$	0	0	Fail / $\|\psi^-\rangle$	$\|-\rangle$	$\|-\rangle$	0	0	Fail / $\|\psi^+\rangle$
$\|0\rangle$	$\|1\rangle$	0	1	Fail	$\|1\rangle$	$\|1\rangle$	0	1	$\|\psi^+\rangle/\|\psi^-\rangle$	$\|+\rangle$	$\|-\rangle$	0	1	Fail / $\|\psi^+\rangle$	$\|-\rangle$	$\|-\rangle$	0	1	Fail / $\|\psi^-\rangle$
$\|0\rangle$	$\|1\rangle$	1	0	Fail	$\|1\rangle$	$\|1\rangle$	1	0	$\|\psi^+\rangle/\|\psi^-\rangle$	$\|+\rangle$	$\|-\rangle$	1	0	Fail/ $\|\psi^+\rangle$	$\|-\rangle$	$\|-\rangle$	1	0	Fail / $\|\psi^-\rangle$
$\|0\rangle$	$\|1\rangle$	1	1	$\|\psi^+\rangle/\|\psi^-\rangle$	$\|1\rangle$	$\|1\rangle$	1	1	Fail	$\|+\rangle$	$\|-\rangle$	1	1	Fail / $\|\psi^-\rangle$	$\|-\rangle$	$\|-\rangle$	1	1	Fail / $\|\psi^+\rangle$

且 $r_1[j],r_2[j],k_1[j],k_2[j]\in R\{0,1\}$, 当 Alice 和 AS 执行完所有操作后, 其输出态为:

$$\begin{aligned}\rho_{\text{out}}\left(WCP_j\right)=&\frac{1}{4}\left[U_Y^0H^0\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]+\frac{1}{4}\left[U_Y^0H^1\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]\\&+\frac{1}{4}\left[U_Y^1H^0\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]+\frac{1}{4}\left[U_Y^1H^1\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]\\=&\frac{1}{4}\left[\left(\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|\right)\right]+\frac{1}{4}\left[\left(\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|-\rangle\langle -|+\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|1\rangle\langle 1|\right)\right]\\&+\frac{1}{4}\left[\left(\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|0\rangle\langle 0|+\frac{1}{4}|-\rangle\langle -|+\frac{1}{4}|+\rangle\langle +|\right)\right]+\frac{1}{4}\left[\left(\frac{1}{4}|-\rangle\langle -|+\frac{1}{4}|+\rangle\langle +|+\frac{1}{4}|1\rangle\langle 1|+\frac{1}{4}|0\rangle\langle 0|\right)\right]\\=&\frac{1}{4}\left[|0\rangle\langle 0|+|1\rangle\langle 1|+|+\rangle\langle +|+|-\rangle\langle -|\right]=\frac{1}{4}\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\right]\\=&\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\frac{1}{2}I\end{aligned} \tag{31}$$

根据上述证明, 我们可以得出在 Client 及 AS 对发来的 WCPs 执行单量子门操作后, 其输出的状态为最大混合态 (totally mixed state), 因此任何人不能得到 Client 和 AS 随机选择的秘密比特的信息, 即该加密方式为量子完备加密 (quantum perfect encryption), 满足信息论的安全性. 接下来, 将证明所述的投票方案可以抵抗外部攻击者的截获重发攻击 (intercept-and-resend attacks)、CNOT 攻击 (CNOT attacks) 及纠缠测量攻击 (entangle-and-measure attacks), 并且可以检测代理 Charlie 的诚实性即内部参与者的攻击.

4.2.1 外部攻击

由于所述协议使用的量子信道是公开的, 可能是不安全的, 这使得量子资源在传输过程中可能会受到来自全能的敌手 Eve 的外部攻击, 以下将分析 3 种常见的外部攻击并证明所述协议是安全的.

(1) 截获重发攻击

根据协议, 只有知道 WCPs 对的初始状态才可以解密得到秘密信息 x. 因此, Eve 可能在量子线路上截获 Server 发来的 WCPs 对并对其进行测量, 随后根据测量结果制备一个处于同种状态的 WCPs 对并重新发送. 由于 Server 在制备 WCPs 对的时候是随机从 Z 基及 X 基中选择的, 因此外部攻击者 Eve 在选择测量基进行窃听的过

程中将会有 50% 的概率引入错误, 使得系统存在 25% 的误码率. 这将会在窃听检测及诚实性检测阶段被发现且窃听者 Eve 通过窃听检测的概率为 $\left(\frac{3}{4}\right)^n$, 当 n 足够大的时候, 所述协议可以抵抗截获重发攻击[44−46].

(2) CNOT 攻击

Eve 可能会使用 CNOT 操作来获取量子资源的信息, 我们假定 Eve 制备了一个辅助粒子序列 (用下标 e 表示) 作为 CNOT 操作的目标粒子, 并将协议传输的粒子 (用下标 a 表示) 作为 CNOT 操作的控制粒子, 在经过 CNOT 操作后, Eve 通过对辅助粒子进行测量以获取目标粒子的状态. 不失一般性, 不妨设辅助粒子的初始状态为 $|0\rangle$, 则经过 CNOT 操作后的系统将演化为如下的状态:

$$|0\rangle_a|0\rangle_e \xrightarrow{\text{CNOT}} |0\rangle_a|0\rangle_e \tag{32}$$

$$|1\rangle_a|0\rangle_e \xrightarrow{\text{CNOT}} |1\rangle_a|1\rangle_e \tag{33}$$

$$|+\rangle_a|0\rangle_e = \frac{1}{\sqrt{2}}(|00\rangle_{ae}+|10\rangle_{ae}) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle_{ae}+|11\rangle_{ae}) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle_{ae}+|{-}{-}\rangle_{ae}) \tag{34}$$

$$|-\rangle_a|0\rangle_e = \frac{1}{\sqrt{2}}(|00\rangle_{ae}-|10\rangle_{ae}) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle_{ae}-|11\rangle_{ae}) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle_{ae}+|{-}{+}\rangle_{ae}) \tag{35}$$

由公式 (32)–公式 (35) 可知, 在 Eve 知道传输粒子使用何种测量基 (Z 基或 X 基) 的前提下, 当协议传输的粒子处于 $|0\rangle$ 或 $|1\rangle$ 时, Eve 可以获取正确的传输粒子信息, 而当协议传输的粒子处于 $|+\rangle$ 或 $|-\rangle$ 时, Eve 将无法区分这两种状态. 进一步, 由于传输粒子的状态是随机从 Z 基和 X 基中选择的, Eve 在选择测量基的过程中可能会引入错误, 这将导致获取错误的传输粒子信息. 因此, 所述协议可以抵抗 CNOT 攻击.

(3) 纠缠测量攻击

在文献 [47] 中, 提出了一种与 CNOT 攻击相似的纠缠测量攻击, Eve 通过制备一个辅助粒子序列 χ 和特殊的酉操作 E, 使得传输粒子在酉操作 E 的作用下与辅助粒子 χ 纠缠. 经过酉操作后的系统状态如公式 (36)–公式 (39) 所示:

$$E|0\rangle|\chi\rangle = \alpha|0\rangle|\chi\rangle_1+\beta|1\rangle|\chi\rangle_2 \tag{36}$$

$$E|1\rangle|\chi\rangle = \alpha|1\rangle|\chi\rangle_1+\beta|0\rangle|\chi\rangle_2 \tag{37}$$

$$E|+\rangle|\chi\rangle = |+\rangle(\alpha|\chi\rangle_1+\beta|\chi\rangle_2) \tag{38}$$

$$E|-\rangle|\chi\rangle = |-\rangle(\alpha|\chi\rangle_1-\beta|\chi\rangle_2) \tag{39}$$

其中, α 和 β 满足归一化条件 $|\alpha|^2+|\beta|^2=1$, $\{|\chi\rangle_1,|\chi\rangle_2\}$ 是由酉操作 E 决定的纯化正交态. 显然, Eve 可以通过使用 $\{|\chi\rangle_1,|\chi\rangle_2\}$ 对辅助粒子 χ 进行测量来获取传输粒子的状态. 当传输粒子的状态处于 $|+\rangle$ 或 $|-\rangle$ 时, 纠缠测量攻击将不会影响传输粒子的状态. 当传输粒子的状态处于 $|0\rangle$ 或 $|1\rangle$ 时, 纠缠测量攻击将会改变传输粒子的状态, 这将使得系统的误码率增加, 并在窃听检测及诚实性检测阶段被发现, 因此所述协议可以抵抗纠缠测量攻击.

4.2.2 内部参与者攻击

在所述协议中, 引入了半诚实的测量代理 Agent 进行 Bell 态的识别, Agent 可能会公布错误的 Bell 态识别的结果, 这将使得用于 QSDC 协议的编码信息出现错误, 为此需要对 Agent 的诚实性进行检测.

在所述协议的后处理过程中会从满足要求的 $2n$ 个粒子中选出 n 个用于窃听和诚实性检测, 这 n 个粒子可以视为是诱骗态粒子, Client/AS 会公布对应的随机数信息, Server 公布初始 WCPs 对的状态. 如果测量代理 Agent 没有诚实的执行协议并公布错误的测量结果, 将会在窃听检测及诚实性检测阶段被发现, 因而所述协议可以检测代理 Agent 的诚实性.

在所述协议中, 使用量子完备加密对量子资源进行编码, 该过程满足信息论的安全性. Client 和 AS 利用后处理提取出用于加密秘密信息的随机数, 并公布加密后的密文信息, 可以视为是经典的一次一密, 其安全性受一次一密 (one-time pad) 加密保护[48], 满足无条件安全性. 在初始化阶段, 所述协议利用 MDI-QKD 的原理, 通过引入第三方 Agent 进行 Bell 态识别, 避免了测量端的漏洞, 其安全性受 MDI-QKD 保护, 满足理论上的无条件安全性, 因此所述 QSDC 协议满足理论上无条件的安全性.

4.3 投票方案的安全需求

(1) 合法性

只有合法的投票者可以进行投票. 在所述投票方案中, 合法的投票者 Alice 会在初始化阶段获得一个用于投票的假名 F_{ID} 及用于身份认证的密钥 K_{ID}. 在保证投票者合法性的同时, 利用 K_{ID} 对投票信息进行编码, 使得只有合法投票者的投票信息才能被计票人成功的接收, 同时监票人可以根据比特承诺机制, 在验票阶段再次验证投票者身份的合法性.

(2) 匿名性

在投票过程中, 投票者使用假名 F_{ID} 进行投票, 由于身份认证服务器是可信的, 他不会向其他人泄露投票者的真实身份信息, 因此除身份认证服务器 AS 外, 其他的投票者及参与者均不能利用公开的信息及假名 F_{ID} 得出 Alice 的个人信息.

由于只有计票人 Bob 知道 WCPs 的初始状态, 从而计算得到 Alice 的投票结果, 其他的投票者均不能在计票人 Bob 公布投票结果前利用公开的信息得出 Alice 的投票信息.

(3) 完整性及可验证性

在所述投票方案中, 包括验票阶段及监票人 David, 计票人 Bob 在投票阶段后会将 Alice 的投票信息公布在公告板上, 由 Alice 验证自己的投票信息是否被正确统计, 同时监票人 David 可以利用投票人 Alice 选择的随机数 r 和公告板上的比特承诺信息验证投票信息的正确性和完整性, 进而验证了投票人 Alice 的身份.

(4) 不可二次投票

在初始化阶段, 只有合法且没有在公告板上投过票的投票者才会被身份认证服务器 AS 分配一个用于投票的假名, 因此没有投票者可以进行二次投票.

(5) 准确性及公开计票

在计票阶段, 每一位投票者的投票信息均被统计在公告板上, 因此所有合法的选票都会被统计, 同时, 由于计票过程是公开的, 每一位投票者都可以通过自计票的方式计算投票的结果.

5 性能评估及比较

5.1 资源消耗及效率

所述投票方案在投票阶段, Bob 和 David 分别制备 t ($t \approx 8n$) 个 WCPs 对, 其通信复杂度为 O(n). 此外, 在不考虑初始化阶段密钥分配资源的情况下, 所述投票方案使用 $2t$ 个 WCPs 对传递了 n 位的投票信息, 其效率为 $\frac{n}{32n}=\frac{1}{32}$. 表 6 列出了所述方案与其他现有量子投票方案的对比, 相较于现有的量子投票方案, 所述方案的通信效率较低, 但使用的量子资源及量子操作更为简单, 并且考虑了测量设备安全和身份认证, 具备更好的可行性及安全性.

表 6 与现有量子投票方案的对比

比较项	文献[19]	文献[18]	本文
Quantum resources	4 particles cluster state	6 particles entangled state	WCPs
Quantum operation	Bell state measurement	GHZ state measurement、Pauli operation	Bell state analyze、Pauli operation
Measurement device security	No	No	Yes
Communication efficiency	$\frac{n}{2Q}$ ($Q >> n$)	$\frac{1-\varepsilon}{2}$ ($0<\varepsilon<1$)	$\frac{1}{32}$
Eavesdropping detection	Yes	Yes	Yes
Honesty detection	No	No	Yes
Scrutineer	Yes	Yes	Yes

5.2 仿真实验

基于开源的量子计算框架 IBM Qiskit, 我们对所述量子投票方案的正确性进行了验证. 实验证明, 所述方案的输出结果处于均匀的叠加态.

如图 5 所示, 我们的仿真线路图可以分为 3 个部分, Bob/David 制备 WCPs、Alice & AS 选择随机数执行 H、Y 操作、Charlie 执行 Bell 态识别. Bob/David 根据 q_0、q_2、q_5、q_7 的测量结果以及受控量子门使得 q_1 和 q_6 处于同基的 BB84 态, Alice (AS) 根据 q_3 (q_8) 和 q_4 (q_9) 的测量结果以及受控量子门决定是否对 q_1 和 q_6 执行 H、Y 操作.

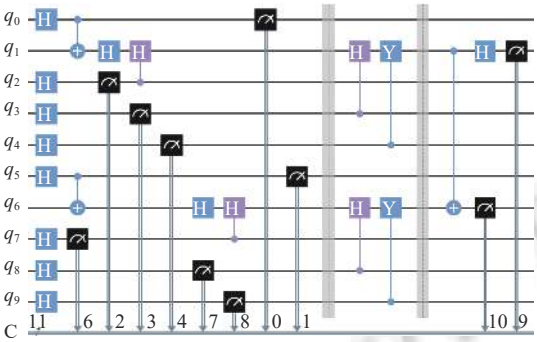

图 5 量子投票仿真线路图

根据该线路, 我们设计了两个实验来验证所述协议的正确性, 其输出结果均处于均匀的叠加态. 实验线路如图 6 和图 7 所示.

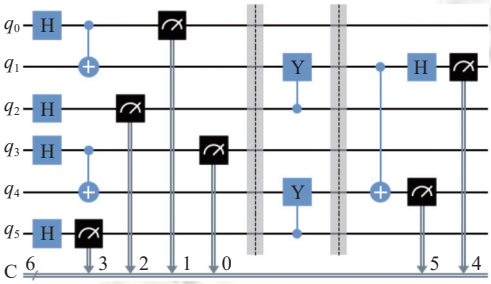

图 6 输入均为 Z 基时的仿真线路图

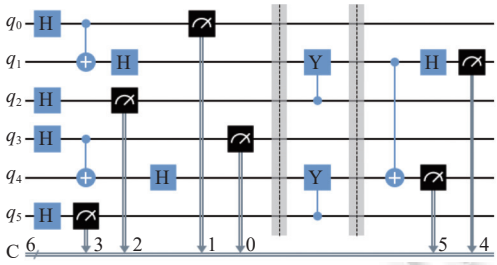

图 7 输入均为 X 基时的仿真线路图

由于 Qiskit 仿真平台无法模拟光学元件的 Bell 态识别过程, 在仿真线路中使用等效的 Bell 态识别线路来代替实际第三方测量端的 Bell 态识别结果, 通过 q_1 和 q_4 的测量结果即可识别出输入的是哪一种 Bell 态 (00 代表 $|\varphi^+\rangle$, 10 代表 $|\varphi^-\rangle$, 01 代表 $|\psi^+\rangle$, 11 代表 $|\psi^-\rangle$) 分别对图 6 和图 7 进行 1 000 次仿真, 其统计结果如表 7 所示, 输出结果处于 4 种 Bell 态的均匀叠加态.

表 7 仿真结果 (Charlie)

Input state	00	01	10	11
Z basis	256	253	243	248
X basis	239	257	235	269

6 总 结

在本文中, 基于 MDI-QKD 提出了一种带身份认证服务器的 QSDC (即可控身份的 QSDC) 协议, 并基于此协议提出了一种带身份认证的量子投票方案. 该方案考虑到了现有测量设备的不完美, 避免了测量端的漏洞, 具有更好的安全性. 其次, 相较于其他的量子投票方案需要制备纠缠态, 所述的方案仅需使用 BB84 态的 WCPs 作为量子资源, 并且只应用了 Bell 态识别及单量子门操作, 对于现有的技术和设备具有较好的可行性. 最后, 所述的投票方案引入了身份认证及监票人, 使得所述的方案满足电子投票协议中的多种安全性需求, 且监票人可以利用承诺机

制验证投票信息的正确性, 因此所述方案具有较好的应用前景. 然而, 所述方案是基于理想的无噪声条件, 没有考虑到实际噪声对于量子态的干扰, 在今后的工作中将会通过引入纠错等方式, 使得我们的方案可以免疫噪声的干扰. 此外, 所述投票方案将投票结果直接公布在公告板上, 没有保护到候选人的隐私, 并且现有的投票协议只能够验证投票信息的正确性, 无法抵抗投票人抵赖投票信息的不诚实行为. 在今后的工作中将通过引入量子安全多方求和及签名等方式, 使得我们的投票方案能够满足更多的安全需求.

References:

[1] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections. In: Proc. of the 1992 Workshop on the Theory and Application of Cryptographic Techniques. Gold Coast: Springer, 1992. 244–251. [doi: 10.1007/3-540-57220-1_66]

[2] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985, 31(4): 469–472. [doi: 10.1109/TIT.1985.1057074]

[3] Brooks M. Beyond quantum supremacy: The hunt for useful quantum computers. Nature, 2019, 574(7776): 19–21. [doi: 10.1038/d41586-019-02936-3]

[4] Arute F, Arya K, Babbush R, Bacon D, *et al*. Quantum supremacy using a programmable superconducting processor. Nature, 2019, 574(7779): 505–510. [doi: 10.1038/s41586-019-1666-5]

[5] Long GL. The development and prospect of quantum computer. Frontiers, 2021(7): 44–56 (in Chinese with English abstract). [doi: 10.16619/j.cnki.rmltxsqy.2021.07.005]

[6] Wu WB, Liu Z, Yang H, Zhang JP. Survey of side-channel attacks and countermeasures on post-quantum cryptography. Ruan Jian Xue Bao/Journal of Software, 2021, 32(4): 1165−1185 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6165.htm [doi: 10.13328/j.cnki.jos.006165]

[7] Yu HF, Fu SF. Post-quantum blind signature scheme based on multivariate cryptosystem. Ruan Jian Xue Bao/Journal of Software, 2021, 32(9): 2935−2944 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6019.htm [doi: 10.13328/j.cnki.jos.006019]

[8] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Reviews of Modern Physics, 2002, 74(1): 145–195. [doi: 10.1103/RevModPhys.74.145]

[9] Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature, 1982, 299(5886): 802–803. [doi: 10.1038/299802a0]

[10] Chen XB. Research on quantum secure communication and its circuit simulation [Ph.D. Thesis]. Beijing: Beijing University of Post and Telecommunications, 2009 (in Chinese with English abstract).

[11] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proc. of the 1984 Int'l Conf. on Computers, Systems & Signal Processing. Bangalore: IEEE, 1984. 175–179.

[12] Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. Physical Review A, 2002, 65(3): 032302. [doi: 10.1103/PhysRevA.65.032302]

[13] Lucamarini M, Mancini S. Secure deterministic communication without entanglement. Physical Review Letters, 2005, 94(14): 140501. [doi: 10.1103/PhysRevLett.94.140501]

[14] Chang Y. The theoretical research on quantum secure communication protocol [Ph.D. Thesis]. Chengdu: University of Electronic Science and Technology of China, 2016 (in Chinese with English abstract).

[15] Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Physical Review Letters, 2002, 89(18): 187902. [doi: 10.1103/PhysRevLett.89.187902]

[16] Hillery M. Quantum voting and privacy protection: First steps. Int'l Society of Optical Engineering, 2006, 41(5): 1117−1119. [doi: 10.1117/2.1200610.0419]

[17] Vaccaro JA, Spring J, Chefles A. Quantum protocols for anonymous voting and surveying. Physical Review A, 2007, 75(1): 012333. [doi: 10.1103/PhysRevA.75.012333]

[18] Xue P, Zhang X. A simple quantum voting scheme with multi-qubit entanglement. Scientific Reports, 2017, 7(1): 7586. [doi: 10.1038/s41598-017-07976-1]

[19] Niu XF, Zhang JZ, Xie SC, Chen BQ. An improved quantum voting scheme. Int'l Journal of Theoretical Physics, 2018, 57(10): 3200–3206. [doi: 10.1007/s10773-018-3837-9]

[20] Zhang S, Wang SL, Wang Q, Shi RH. Quantum anonymous voting protocol with the privacy protection of the candidate. Int'l Journal of Theoretical Physics, 2019, 58(10): 3323–3332. [doi: 10.1007/s10773-019-04205-5]

[21] Li YR, Jiang DH, Zhang YH, Liang XQ. A quantum voting protocol using single-particle states. Quantum Information Processing, 2021, 20(3): 110. [doi: 10.1007/s11128-021-03048-6]

[22] Wang QL, Yu CH, Gao F, Qi HY, Wen QY. Self-tallying quantum anonymous voting. Physical Review A, 2016, 94(2): 022333. [doi: 10.1103/PhysRevA.94.022333]

[23] Qin JQ, Shi RH, Zhang R. Quantum voting protocol based on controlled quantum secure direct communication. Chinese Journal of Quantum Electronics, 2018, 35(5): 558–566 (in Chinese with English abstract).

[24] Zhang X, Zhang JZ, Xie SC. A secure quantum voting scheme based on quantum group blind signature. Int'l Journal of Theoretical Physics, 2020, 59(3): 719–729. [doi: 10.1007/s10773-019-04358-3]

[25] Zhang KJ, Sun Y, Song TT, Zuo HJ. Cryptanalysis of the quantum group signature protocols. Int'l Journal of Theoretical Physics, 2013, 52(11): 4163–4173. [doi: 10.1007/s10773-013-1729-6]

[26] Shi RH, Qin JQ, Liu B, Zhang MW. Anonymous quantum voting protocol based on Chinese remainder theorem. The European Physical Journal D, 2021, 75(1): 20. [doi: 10.1140/epjd/s10053-020-00014-2]

[27] Makarov V, Hjelme DR. Faked states attack on quantum cryptosystems. Journal of Modern Optics, 2005, 52(5): 691–705. [doi: 10.1080/09500340410001730986]

[28] Qi B, Fung CHF, Lo HK, Ma XF. Time-shift attack in practical quantum cryptosystems. Quantum Information & Computation, 2007, 7(1): 73–82.

[29] Makarov V. Controlling passively quenched single photon detectors by bright light. New Journal of Physics, 2009, 11(6): 065003. [doi: 10.1088/1367-2630/11/6/065003]

[30] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics, 2010, 4(10): 686–689. [doi: 10.1038/nphoton.2010.214]

[31] Weier H, Krauss H, Rau M, Fürst M, Nauerth S, Weinfurter H. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. New Journal of Physics, 2011, 13(7): 073024. [doi: 10.1088/1367-2630/13/7/073024]

[32] Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. Physical Review Letters, 2012, 108(13): 130503. [doi: 10.1103/PhysRevLett.108.130503]

[33] Xu FH, Curty M, Qi B, Lo HK. Measurement-device-independent quantum cryptography. IEEE Journal of Selected Topics in Quantum Electronics, 2015, 21(3): 148–158. [doi: 10.1109/JSTQE.2014.2381460]

[34] Zhou ZR, Sheng YB, Niu PH, Yin LG, Long GL, Hanzo L. Measurement-device-independent quantum secure direct communication. Science China Physics, Mechanics & Astronomy, 2020, 63(3): 230362. [doi: 10.1007/s11433-019-1450-8]

[35] Cui ZX, Zhong W, Zhou L, Sheng YB. Measurement-device-independent quantum key distribution with hyper-encoding. Science China Physics, Mechanics & Astronomy, 2019, 62(11): 110311. [doi: 10.1007/s11433-019-1438-6]

[36] Rong ZB, Qiu DW, Mateus P, Zou XF. Mediated semi-quantum secure direct communication. Quantum Information Processing, 2021, 20(2): 58. [doi: 10.1007/s11128-020-02965-2]

[37] Choi JW, Kang MS, Park CH, Yang HJ, Han SW. Measurement-device-independent mutual quantum entity authentication. Quantum Information Processing, 2021, 20(4): 152. [doi: 10.1007/s11128-021-03093-1]

[38] Zhou XY. Research on performance optimization and realization of practical measurement-device-independent quantum key distribution [Ph.D. Thesis]. Nanjing: Nanjing University of Posts and Telecommunications, 2020 (in Chinese with English abstract).

[39] Zhang CH. Design and implementation of new quantum cryptographic schemes [Ph.D. Thesis]. Nanjing: Nanjing University of Posts and Telecommunications, 2020 (in Chinese with English abstract).

[40] Zhang ZM. Quantum Optics. Beijing: Science Press, 2015. 14, 65 (in Chinese).

[41] Hong CK, Ou ZY, Mandel L. Measurement of subpicosecond time intervals between two photons by interference. Physical Review Letters, 1987, 59(18): 2044–2046. [doi: 10.1103/PhysRevLett.59.2044]

[42] Wang C. Practical research of measurement-device-independent quantum key distribution [Ph.D. Thesis]. Hefei: University of Science and Technology of China, 2018 (in Chinese with English Abstract).

[43] Boykin PO, Roychowdhury V. Optimal encryption of quantum bits. Physical Review A, 2003, 67(4): 042317. [doi: 10.1103/PhysRevA.67.042317]

[44] Mayers D. Unconditional security in quantum cryptography. Journal of the ACM, 2001, 48(3): 351–406. [doi: 10.1145/382780.382781]

[45] Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters, 2000, 85(2): 441–444. [doi: 10.1103/PhysRevLett.85.441]

[46] Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283(5410): 2050–2056. [doi: 10.1126/science.283.5410.2050]

[47] Wang ZY. Quantum secure direct communication and quantum sealed-bid auction with EPR pairs. Communications in Theoretical Physics, 2010, 54(6): 997. [doi: 10.1088/0253-6102/54/6/08]

[48] Vernam GS. Cipher printing telegraph systems for secret wire and radio telegraphic communications. Trans. of the American Institute of Electrical Engineers, 1926, 45: 295–301. [doi: 10.1109/t-aiee.1926.5061224]

附中文参考文献:

[5] 龙桂鲁. 量子计算机的研发进展与未来展望. 人民论坛·学术前沿, 2021(7): 44–56. [doi: 10.16619/j.cnki.rmltxsqy.2021.07.005]
[6] 吴伟彬, 刘哲, 杨昊, 张吉鹏. 后量子密码算法的侧信道攻击与防御综述. 软件学报, 2021, 32(4): 1165−1185. http://www.jos.org.cn/1000-9825/6165.htm [doi: 10.13328/j.cnki.jos.006165]
[7] 俞惠芳, 付帅风. 抗量子计算的多变量盲签名方案. 软件学报, 2021, 32(9): 2935−2944. http://www.jos.org.cn/1000-9825/6019.htm [doi: 10.13328/j.cnki.jos.006019]
[10] 陈秀波. 量子安全通信及其线路模拟的研究 [博士学位论文]. 北京: 北京邮电大学, 2009.
[14] 昌燕. 量子安全通信协议理论研究 [博士学位论文]. 成都: 电子科技大学, 2016.
[23] 秦加奇, 石润华, 张瑞. 基于受控量子安全直接通信的量子投票协议. 量子电子学报, 2018, 35(5): 558–566.
[38] 周星宇. 实用化测量设备无关量子密钥分配协议的改进与实现研究 [博士学位论文]. 南京: 南京邮电大学, 2020.
[39] 张春辉. 新型量子密码的方案设计与实验验证 [博士学位论文]. 南京: 南京邮电大学, 2020.
[40] 张智明. 量子光学. 北京: 科学出版社, 2015. 14, 65.
[42] 王超. 测量设备无关量子密钥分配的实用化研究 [博士学位论文]. 合肥: 中国科学技术大学, 2018.

柯唯阳(1996－), 男, 硕士, 主要研究领域为测量设备无关的密码学, 量子投票协议.

石润华(1974－), 男, 博士, 教授, 博士生导师, 主要研究领域为经典密码协议及其应用, 量子密码协议及其应用.