激光与光电子学进展

免疫集体噪声的半量子盲签名协议

王俊辉**，李云霞，郭瀚，魏家华*
空军工程大学信息与导航学院，陕西 西安 710077

摘要 量子盲签名作为量子密码的重要组成部分，近年来备受关注，半量子协议为量子盲签名走向实用化提供了可行性方法。结合半量子概念和抵抗集体噪声的逻辑粒子，提出了免疫集体噪声的半量子盲签名协议。在协议中，只有签名方Charlie具备完整的量子能力，这使得该协议对量子资源的依赖大幅降低。通过安全性分析可以证明：本协议能够抵抗内部攻击、纠缠测量攻击和截断重发攻击等，实现了部分密钥的可复用性，同时能够扩展到量子签名网络，实现跨区域的量子签名。

关键词 量子密码；量子盲签名；半量子；集体噪声
中图分类号 O431.2 **文献标志码** A **DOI**：10.3788/LOP202259.1927001

Semi-Quantum Blind Signature Against Collective Noise

Wang Junhui**, Li Yunxia, Guo Han, Wei Jiahua*
Institute of Information and Navigation, Air Force Engineering University, Xi'an 710077, *Shaanxi, China*

Abstract As an important part of quantum cryptography, quantum blind signature has attracted more and more attention in recent years. Semi-quantum protocol provides a feasible method for the practical application of quantum blind signature. In this paper, a semi-quantum blind signature protocol against collective noise is proposed by combining the semi-quantum and logical qubits resisting collective noise. In the protocol, only the signer Charlie has the complete quantum capability, which makes the demand for quantum resources of the protocol drop drastically. Through security analysis, the protocol can resist internal attack, entanglement-measurement attack and intercept-resend attack. The protocol implements reusability of keys and the scheme can be extended to quantum signature networks to realize cross-center quantum signature.

Key words quantum cryptography; quantum blind signature; semi-quantum; collective noise

1 引 言

自1984年Bennett等[1]提出BB84协议以来，量子密码学以其无条件、安全性吸引了诸多学者关注和研究。随后，其他类似的协议也相继被提出，如量子密钥分发[2-5]、量子安全直接通信[6-8]、量子秘密共享[9-11]等。同时，量子签名(Quantum signature，QS)协议也引起了广泛关注。

量子签名技术主要用于验证消息真实性、完整性和不可否认性，并实现通信双方的消息认证。2002年，曾贵华等[12]利用Greenberger-Horne-Zeilinger(GHZ)三重态的相干性，提出了第一个仲裁量子签名协议，这标志着量子签名的开端。随后，大量的量子签名协议被提出并不断完善。基于不同功能需求，新型的量子签名被提出，相继诞生了量子代理签名、量子盲签名和量子群签名等。

量子盲签名作为量子签名技术的重要分支，可以在签名者不知道具体消息的情况下进行签名。2009年，Wen等[13]首次提出了基于Einstein-Podolsky-Rosen(EPR)纠缠粒子的量子弱盲签名方案。2012年，Yin等[14]提出了基于χ型态的量子盲签名方案。Tian等[15]提出了一个基于量子隐形传态的量子广播多重量子盲签名方案，Zhang等[16]针对其可能遭受的签名伪造行为，进行了协议优化。2017年，Zhang等[17]指出现有仲裁量子签名不安全，即签名接收者可能通过存在性攻击否认所收到的签名，并给出了改进思路，为增强量子盲签名的安全性提供了依据。2019年，Chen等[18]利用非正交单光子，提出了一个不需要

收稿日期：2021-08-31；**修回日期**：2021-09-10；**录用日期**：2021-09-27
基金项目：国家自然科学基金(61971436,61803382)
通信作者：*weijiahua@126.com；** jhwang0630@126.com

纠缠的量子盲签名协议。Wang 等[19]提出基于 Bell 态和 GHZ 态的量子盲签名协议，该协议具有较高的量子签名效率。Liang 等[20]和 Liu 等[21]分别基于四粒子纠缠态和五粒子纠缠态提出了盲代理签名协议。Zhang 等[22]和 Yang 等[23]分别基于六粒子纠缠态和七粒子纠缠态提出了盲代理签名的改进协议。2020 年，Li 等[24]和 Niu 等[25]分别基于量子行走和量子密集编码原理提出了新的盲签名协议。

随着量子签名的发展，实用性的量子签名协议成为了研究热点。首先，环境和设备不完美等因素，会使传输的签名或信息出现偏差，即量子噪声对量子签名的影响不可忽略；其次，量子设备制造难度大、价格昂贵和不易携带等特性为量子签名的实用化造成了阻碍。为克服量子噪声影响，可将量子信道噪声模型转化为集体噪声[26-27]，由几个经历相同噪声的物理比特组成去相干子空间（Decoherence free subspace，DFS），对噪声进行补偿，以达到抵抗集体噪声的目的。2010 年，Yang 等[28]提出了抵抗集体振幅阻尼噪声的量子仲裁签名方案，Zhang 等[29]于 2016 年提出了抵抗集体退相位噪声和集体旋转噪声的量子盲签名方案。Boyer 等[30]于 2007 年提出的“半量子（Semi-quantum，SQ）”概念为量子设备价格昂贵和不易携带的问题提供了解决方案。2019 年，Zhao 等[31]基于 W 态提出了双向半量子签名方案。Chen 等[32]基于四粒子簇态实现了 2 个经典方仲裁签名方案。本文结合半量子概念和抵抗集体噪声的逻辑粒子，提出了在集体噪声干扰下的容错半量子盲签名协议。

2 基本原理

2.1 半量子密钥分发协议

半量子密钥分发（Semi-quantum key distribution，SQKD）协议最早由 Boyer 等[30]于 2007 年提出，该协议在 BB84 的基础上弱化了一方量子能力，可以实现量子方 Alice 与经典方 Bob 安全共享密钥。其中，经典方是指参与方具备以下 4 种量子能力中的几种：1）能够制备 Z 基$\{|0\rangle,|1\rangle\}$量子比特；2）能够执行 Z 基测量；3）对量子态不做任何改变，直接返回量子态；4）对量子比特重新排序。2009 年，Boyer 等[33]提出了使用 4 个单量子$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$实现的 SQKD 协议。2014 年，Yu 等[34]利用 Bell 态实现 SQKD，2015 年，Krawec[35]利用不可信量子第三方实现两个经典方的 SQKD。2016 年，Krawec[36]系统地证明了 SQKD 协议的安全性，并指出 SQKD 满足无条件安全性。随后，各种半量子密钥分发协议被提出[37-38]，其他类似协议也相继被提出，如半量子安全直接通信[39]，半量子签名[31-32]等。

2.2 集体噪声

集体退相位噪声和集体旋转噪声是 2 种常见的集体噪声模型。集体退相位噪声算符可表示为

$$\boldsymbol{U}_{\mathrm{dp}}=\begin{pmatrix}1 & 0\\ 0 & \exp(\mathrm{i}\omega)\end{pmatrix},\tag{1}$$

式中：ω为集体退相位噪声参数。在集体退相位信道中，量子态$|1\rangle$变为$\exp(\mathrm{i}\omega)|1\rangle$，而量子态$|0\rangle$保持不变。逻辑量子态$|0\rangle_{\mathrm{dp}}=|01\rangle$和$|1\rangle_{\mathrm{dp}}=|10\rangle$均由 2 个粒子组成，且集体退相位噪声对这 2 个逻辑量子态影响相同，即具备抵抗集体退相位噪声能力。

利用逻辑量子态$|0\rangle_{\mathrm{dp}}$和$|1\rangle_{\mathrm{dp}}$组建逻辑 Bell 态$\left|\phi^{+}\right\rangle_{1234}^{\mathrm{dp}}$，可表示为

$$\begin{aligned}\left|\phi^{+}\right\rangle_{1234}^{\mathrm{dp}}&=\frac{1}{\sqrt{2}}\left(|0\rangle_{\mathrm{dp}}|0\rangle_{\mathrm{dp}}+|1\rangle_{\mathrm{dp}}|1\rangle_{\mathrm{dp}}\right)_{1234}=\\&\frac{1}{\sqrt{2}}\left(|0101\rangle+|1010\rangle\right)_{1234}=\\&\frac{1}{\sqrt{2}}\left(\left|\phi^{+}\right\rangle\left|\phi^{+}\right\rangle+\left|\phi^{-}\right\rangle\left|\phi^{-}\right\rangle\right)_{1324},\end{aligned}\tag{2}$$

式中：$\left|\phi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle\pm|11\rangle\right)$。由式（2）可知，对逻辑 Bell 态$\left|\phi^{+}\right\rangle_{1234}^{\mathrm{dp}}$中粒子 1 和粒子 3 执行 Bell 测量，并对粒子 2 和粒子 4 执行 Bell 测量可以得到相同的结果，且同时为$\left|\phi^{+}\right\rangle$或同时为$\left|\phi^{-}\right\rangle$。

集体旋转噪声的模型为

$$\begin{aligned}\boldsymbol{U}_{\mathrm{r}}|0\rangle&=\cos\theta|0\rangle+\sin\theta|1\rangle,\\\boldsymbol{U}_{\mathrm{r}}|1\rangle&=-\sin\theta|0\rangle+\cos\theta|1\rangle,\end{aligned}\tag{3}$$

式中：θ为集体旋转噪声参数。逻辑量子态$|0\rangle_{\mathrm{r}}$和$|1\rangle_{\mathrm{r}}$能够容忍集体旋转噪声，其中$|0\rangle_{\mathrm{r}}=\left|\phi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)$，$|1\rangle_{\mathrm{r}}=\left|\phi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle-|10\rangle\right)$。同理，利用逻辑量子态$|0\rangle_{\mathrm{r}}$和$|1\rangle_{\mathrm{r}}$组建逻辑 Bell 态$\left|\phi^{+}\right\rangle_{1234}^{\mathrm{r}}$可抵抗集体旋转噪声

$$\begin{aligned}\left|\phi^{+}\right\rangle_{1234}^{\mathrm{r}}&=\frac{1}{\sqrt{2}}\left(|0\rangle_{\mathrm{r}}|0\rangle_{\mathrm{r}}+|1\rangle_{\mathrm{r}}|1\rangle_{\mathrm{r}}\right)_{1234}=\\&\frac{1}{2\sqrt{2}}\left(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle+|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle\right)_{1234}=\\&\frac{1}{\sqrt{2}}\left(\left|\phi^{+}\right\rangle\left|\phi^{+}\right\rangle+\left|\psi^{-}\right\rangle\left|\psi^{-}\right\rangle\right)_{1324}。\end{aligned}\tag{4}$$

由式(4)可知,对逻辑量子态$\left|\phi^{+}\right\rangle_{1234}^{r}$中的粒子1和粒子3进行Bell测量,对粒子2和粒子4也进行Bell测量,则两者测量结果相同,且为$\left|\phi^{+}\right\rangle$或$\left|\phi^{-}\right\rangle$。

3　免疫集体噪声的半量子盲签名协议

免疫集体噪声的量子盲签名包含三方:消息发送方Alice,签名方Charlie和签名接受及验证方Bob,其中Alice和Bob为经典方,Charlie为量子方。经典方Alice和Bob允许进行的量子操作有:1)对接收到的量子态进行Z基$\{|0\rangle,|1\rangle\}$测量,并返还测量结果给发送方;2)对接收到的量子态不经过任何操作直接进行转发,返还给发送方;3)制备Z基量子态。本协议与其他盲签名协议类似,分为初始化阶段、签名阶段和验证阶段。协议的流程示意图如图1所示。

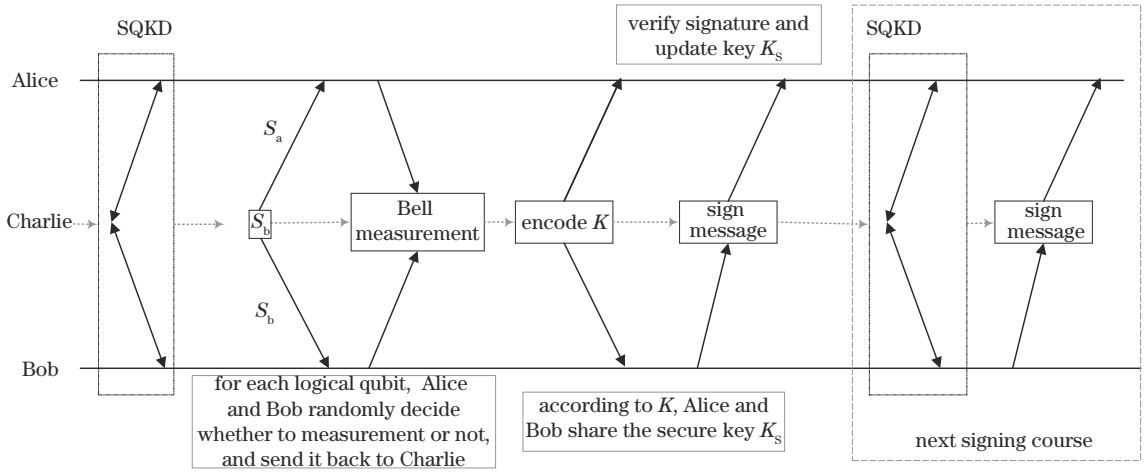

图1　抵抗集体噪声的版量子签名流程示意图

Fig. 1　Schematic of semi-quantum blind signature against collective noise

3.1　初始化阶段

1)消息转化:Alice将待签名的消息转化为二进制消息序列$M=\{m_1,m_2,\cdots,m_n\}$,其中$m_i\in\{0,1\}$,$i\in[1,2,\cdots,n]$,n为二进制消息M的长度;

2)密钥共享:Alice和Charile以及Bob和Charlie分别通过SQKD技术[35]共享密钥K_A和K_B,且该SQKD技术已被证明是安全的[36];

3)量子态制备和分发:签名方Charlie准备$8n$个量子态$\left|\phi^{+}\right\rangle_{1234}^{L}$,其中$L$表示dp或r,即表示抵抗集体退相位噪声或集体旋转噪声所需准备的量子态。Charlie将所有量子态分为S_1、S_2、S_3和S_4,其中对应位置的S_1和S_2构成一个逻辑量子比特序列S_a,对应位置的S_3和S_4构成一个逻辑量子比特序列S_b。Charlie将序列S_a和S_b分别发给Alice和Bob;

3.2　签名阶段

1)Alice生成随机数序列$M_A=\{0,1\}^{8n}$,对于$M_A^i=1$,其中$M_A^i\in M_A$,$i\in[1,2,\cdots,8n]$,表示对第i个接收到的逻辑量子比特进行Z基测量,并将测量后粒子返还给Charlie,若$M_A^i=0$则不进行任何操作后转发给Charlie。同理,Bob生成随机数序列$M_B=\{0,1\}^{8n}$,并依据M_B对量子态操作,随后转发给Charlie。Charlie在接收完所有逻辑量子比特后,构成量子态序列$\left|\phi'\right\rangle_{1234}^{L}$,并对每个$\left|\phi'\right\rangle_{1234}^{i}\in\left|\phi'\right\rangle_{1234}^{L}$中的粒子1和粒子3以及粒子2和粒子4各进行一次Bell测量,得到$\left|\varphi\right\rangle_{13}$和$\left|\varphi\right\rangle_{24}$。若$L$为dp(r),则Charlie依据测量结果和表1(表2)规则得到序列K。若信道中存在窃听则会出现表1(表2)中未出现的情况。Charlie将序列K通过经典信道广播。

表1　集体退相位噪声下Bell测量结果与序列K的对应关系

Table 1　Relation between Bell measurement results and K under collective-dephasing noise

$\left\|\varphi\right\rangle_{13}$ Bell measurement result	$\left\|\varphi\right\rangle_{24}$ Bell measurement result	K
$\left\|\phi^{+}\right\rangle$	$\left\|\phi^{+}\right\rangle$	0
$\left\|\phi^{+}\right\rangle$	$\left\|\phi^{-}\right\rangle$	1
$\left\|\phi^{-}\right\rangle$	$\left\|\phi^{-}\right\rangle$	0
$\left\|\phi^{-}\right\rangle$	$\left\|\phi^{+}\right\rangle$	1

信道窃听检测:Alice和Bob通过经典信道广播M_A和M_B。Alice和Bob验证对$\forall M_A^i=M_B^i=0$,都满足$K=0$,否则放弃协议。实际使用时,验证$M_A^i=M_B^i=0$时,$K\neq0$所占比例,若大于给定门限,则放弃协议,否则进行下一步。

2)取前n个$M_A^i=M_B^i=1$的位置i,并依据第i个逻辑量子比特测量结果编码得到K_S,其编码规则如表3(L表示dp)和表4(L表示r)所示。

3)消息盲化:Alice计算$m_A=M\oplus K_S\|r_1\|H(M,r_1)$,其中$r_1\in\{0,1\}^{k_1}$为Alice制备的随机数序

表 2 集体旋转噪声下 Bell 测量结果与序列 K 的对应关系

Table 2 Relation between Bell measurement results and K under collective-rotation noise

$\|\varphi\rangle_{13}$ Bell measurement result	$\|\varphi\rangle_{24}$ Bell measurement result	K	$\|\varphi\rangle_{13}$ Bell measurement result	$\|\varphi\rangle_{24}$ Bell measurement result	K
$\|\phi^+\rangle$	$\|\phi^+\rangle$	0	$\|\psi^+\rangle$	$\|\psi^+\rangle$	1
$\|\phi^+\rangle$	$\|\phi^-\rangle$	1	$\|\psi^+\rangle$	$\|\psi^-\rangle$	1
$\|\phi^-\rangle$	$\|\phi^-\rangle$	1	$\|\psi^-\rangle$	$\|\psi^-\rangle$	0
$\|\phi^-\rangle$	$\|\phi^+\rangle$	1	$\|\psi^-\rangle$	$\|\psi^+\rangle$	1

表 3 集体退相位噪声下 K_S 编码规则

Table 3 Rules of encoding K_S with collective-dephasing noise

Result of logical qubits with Z basis	K_S
$\|01\rangle$	0
$\|10\rangle$	1

表 4 集体旋转噪声下 K_S 编码规则

Table 4 Rules of encoding K_S with collective-rotation noise

Result of logical qubits with Z basis	K_S
$\|00\rangle$	0
$\|01\rangle$	1
$\|10\rangle$	1
$\|11\rangle$	0

列，哈希函数 $H(\cdot):\{0,1\}^*\rightarrow\{0,1\}^{n-k_1}$，$\|$ 为并集符号。然后，Alice 依据表 5 制备量子态 s_A，并通过 Alice 与 Charlie 共享的密钥 K_A 加密得到 $S_A=E_{K_A}(s_A)$，Alice 将 S_A 发送给 Charlie。

表 5 Alice 制备量子态 s_A 规则

Table 5 Rules of Alice preparation of qubits s_A

m_A	s_A
0	$\|01\rangle$
1	$\|10\rangle$

4）签名发送：Charlie 接收到 S_A 后，用 K_A 解密得到 s'_A，随后通过 s'_A 得到 m'_A，其规则为表 5 的逆过程，从而得到 $(M\oplus K_S)'$、r'_1 和 H'，Charlie 生成签名 $S_C=E_{K_B}\left[(M\oplus K_S)'\|r_1'\|H'\right]$，并将其发送给 Bob。

3.3 验证阶段

1）Bob 接收到 S_A 后通过 K_B 解密得到 $(M\oplus K_S)''$、r_1'' 和 H''，Bob 计算 $(M\oplus K_S)''\oplus K_S$ 得到 M'。Bob 计算 $H(M',r_1'')$ 是否与 H' 一致，若一致，则接受签名，否则中止协议。

2）Bob 和 Alice 更新 K_S。Alice 和 Bob 将 K_S 更新为 $K_S\otimes r_1''\|H''$，方便下次消息的发送。

4 安全性分析及协议特性

该签名方案在量子信道中采用抵抗集体退相位噪声或集体旋转噪声的逻辑粒子进行传输，因此该方案能够抵抗集体退相位噪声或集体旋转噪声，实现了 2 个经典方在量子签名方的协助下进行半量子盲签名。该半量子盲签名（SQBS）协议满足不可抵赖性、不可伪造性和盲性，并具备可扩展性和密钥的可复用性。

4.1 不可抵赖性

Alice 不能抵赖发送了消息，Alice 用 Alice 与 Charlie 共享的密钥 K_A 对消息进行了加密，而 Charlie 解密时需要用到 K_A，且 Alice 对消息 M 的加密用到了 K_S，Alice 不能否认其发送了消息。Charlie 签名时用到 K_B，不能否认其进行了签名，Bob 解密用到 K_B 和 K_S 间接证明了 Alice 和 Charlie 的参与。

4.2 不可伪造性

主要分析了协议在遭受参与者攻击和外部攻击时的安全性能，其中外部攻击包含纠缠测量攻击和截断重发攻击。相比于外部攻击，参与者更了解协议相关信息，参与者攻击对协议的安全性有着更大的威胁。假设 Bob 试图伪造 Alice 的签名，但 Bob 不能在不被察觉的情况下获得任何有关 K_A 的信息，因此，Bob 不能伪造 Alice 的签名。假设 Charlie 尝试伪造消息 M，并将其签名结果发送给 Bob，则 Charlie 窃听的目标是获取 K_S 的有关信息。不失一般性，考虑集体退相位噪声下的协议。

1）内部攻击

Charlie 试图通过 S_a 和 S_b 获取 K_S 相关信息。假设 Charlie 是半可信的，即 Charlie 基于协议规定进行 Bell 测量，并传输正确的编码序列 K。根据协议，Charlie 在宣布 Bell 测量结果前，不能得知 Alice 和 Bob 是否对逻辑量子比特进行 Z 基测量，即 Charlie 不能确定 Alice 和 Bob 都进行 Z 基测量的比特位置。因此，Charlie 不能获得任何有关 K_S 的信息。

假设 Charlie 是不可信的，即 Charlie 可以通过其他任何量子态以欺骗 Alice 和 Bob，而不被发现。存在 2 种情况，Charlie 通过单逻辑粒子代替 $|\phi^+\rangle_{dp}$ 或 Charlie 通过辅助粒子纠缠的方式代替 $|\phi^+\rangle_{dp}$。若 Charlie 直接发送单逻辑粒子给 Alice 和 Bob，而不是逻辑量子态 $|\phi^+\rangle_{dp}$，即假设 Charlie 发送序列 $S_a=\{|0\rangle_{dp},|0\rangle_{dp},|1\rangle_{dp},|1\rangle_{dp}\}$，$S_b=\{|0\rangle_{dp},|1\rangle_{dp},|0\rangle_{dp},|1\rangle_{dp}\}$，无论 Alice 和 Bob 是否测量，Alice 返回 S_a，Bob 返回 S_b，Charlie 不能通过返回序列确定 Alice 和 Bob 是否进行

了测量，也不能通过信道窃听检测，即 Charlie 的欺骗行为一定会被发现。因此，Charlie 通过直接发送单逻辑粒子的方案不能获取任何有关 K_S 的信息。

若 Charlie 在初始化阶段 3）用 $\left|\varphi\right\rangle_{123456}^{dp}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{dp}\left|0\right\rangle_{dp}\left|0\right\rangle_{dp}+\left|1\right\rangle_{dp}\left|1\right\rangle_{dp}\left|1\right\rangle_{dp}\right)_{123456}$ 代替 $\left|\phi^+\right\rangle_{1234}^{dp}$，即通过增加辅助粒子 5 和粒子 6 的方式，得到有关 Alice 和 Bob 测量的信息，从而获取 K_S。若 Alice 和 Bob 都未对接收到的逻辑粒子进行测量，此时系统的状态为

$$\begin{aligned}\left|\varphi\right\rangle_{123456}^{dp}=&\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{dp}\left|0\right\rangle_{dp}\left|0\right\rangle_{dp}+\left|1\right\rangle_{dp}\left|1\right\rangle_{dp}\left|1\right\rangle_{dp}\right)_{123456}=\\&\frac{1}{2\sqrt{2}}\left[\left|\phi^+\right\rangle_{13}\left|\phi^+\right\rangle_{24}\left(\left|01\right\rangle_{56}+\left|10\right\rangle_{56}\right)+\left|\phi^+\right\rangle_{13}\left|\phi^-\right\rangle_{24}\left(\left|01\right\rangle_{56}-\left|10\right\rangle_{56}\right)+\right.\\&\left.\left|\phi^-\right\rangle_{13}\left|\phi^+\right\rangle_{24}\left(\left|01\right\rangle_{56}-\left|10\right\rangle_{56}\right)+\left|\phi^-\right\rangle_{13}\left|\phi^-\right\rangle_{24}\left(\left|01\right\rangle_{56}+\left|10\right\rangle_{56}\right)\right],\end{aligned}\tag{5}$$

由于 $\left|\phi^-\right\rangle_{13}\left|\phi^+\right\rangle_{24}$ 或 $\left|\phi^+\right\rangle_{13}\left|\phi^-\right\rangle_{24}$ 出现的概率为 50%，即出现错误的概率为 50%；若 Alice 和 Bob 至少有一个对接受的逻辑量子比特进行测量，则总系统的状态为

$$\left|\varphi\right\rangle_{123456}^{dp}=\left|0\right\rangle_{dp}\left|0\right\rangle_{dp}\left|0\right\rangle_{dp}=\frac{1}{2}\left(\left|\phi^+\right\rangle_{13}\left|\phi^+\right\rangle_{24}\left|01\right\rangle_{56}-\left|\phi^+\right\rangle_{13}\left|\phi^-\right\rangle_{24}\left|01\right\rangle_{56}+\left|\phi^-\right\rangle_{13}\left|\phi^+\right\rangle_{24}\left|01\right\rangle_{56}-\left|\phi^-\right\rangle_{13}\left|\phi^-\right\rangle_{24}\left|01\right\rangle_{56}\right),\tag{6}$$

或

$$\left|\varphi\right\rangle_{123456}^{dp}=\left|1\right\rangle_{dp}\left|1\right\rangle_{dp}\left|1\right\rangle_{dp}=\frac{1}{2}\left(\left|\phi^+\right\rangle_{13}\left|\phi^+\right\rangle_{24}\left|10\right\rangle_{56}+\left|\phi^+\right\rangle_{13}\left|\phi^-\right\rangle_{24}\left|10\right\rangle_{56}-\left|\phi^-\right\rangle_{13}\left|\phi^+\right\rangle_{24}\left|10\right\rangle_{56}-\left|\phi^-\right\rangle_{13}\left|\phi^-\right\rangle_{24}\left|10\right\rangle_{56}\right)。\tag{7}$$

由式(6)和式(7)可得，Charlie 可通过对粒子 1、粒子 3 以及粒子 2、粒子 4 进行 Bell 测量，对粒子 5、粒子 6 进行 Z 基测量，可得到 Alice 和 Bob 的测量结果。

综上所述，Charlie 通过增加辅助粒子的方式获取 K_S 相关信息，必将给 Alice 和 Bob 都未进行测量逻辑粒子这一情况带来错误。

2）纠缠测量攻击

第三方 Eve 想利用提前准备的辅助光子 $\left|E_i\right\rangle$ 并使辅助量子与信道中传输光子相结合，随后，对传输的逻辑量子比特进行幺正操作 U_E，通过对辅助光子的测量得到有用信息。Eve 在传输的量子态 $\{\left|0\right\rangle_{dp},\left|1\right\rangle_{dp}\}$ 上的纠缠测量攻击为

$$\begin{aligned}U_E\left|0\right\rangle_{dp}\left|E_i\right\rangle&=U_E\left|01\right\rangle\left|E_i\right\rangle=a_{00}\left|00\right\rangle\left|e_0e_0\right\rangle+a_{01}\left|01\right\rangle\left|e_0e_1\right\rangle+a_{10}\left|10\right\rangle\left|e_1e_0\right\rangle+a_{11}\left|11\right\rangle\left|e_1e_1\right\rangle,\\U_E\left|1\right\rangle_{dp}\left|E_i\right\rangle&=U_E\left|10\right\rangle\left|E_i\right\rangle=b_{00}\left|00\right\rangle\left|e_0'e_0'\right\rangle+b_{01}\left|01\right\rangle\left|e_0'e_1'\right\rangle+b_{10}\left|10\right\rangle\left|e_1'e_0'\right\rangle+b_{11}\left|11\right\rangle\left|e_1'e_1'\right\rangle,\end{aligned}\tag{8}$$

式中：$\left|e_0e_0\right\rangle$、$\left|e_0e_1\right\rangle$、$\left|e_1e_0\right\rangle$ 和 $\left|e_1e_1\right\rangle$ 属于 Eve 探针的 Hilbert 空间，且满足

$$\begin{aligned}&\left|a_{00}\right|^2+\left|a_{01}\right|^2+\left|a_{10}\right|^2+\left|a_{11}\right|^2=1,\\&\left|b_{00}\right|^2+\left|b_{01}\right|^2+\left|b_{10}\right|^2+\left|b_{11}\right|^2=1,\\&a_{01}=b_{10},\ a_{10}=b_{01},\end{aligned}\tag{9}$$

由式(8)和式(9)可知，Charlie 发送的诱骗态量子 $\{\left|0\right\rangle_{dp},\left|1\right\rangle_{dp}\}$ 经过纠缠测量攻击后，被 Alice(Bob)检测到的概率为

$$\begin{aligned}P_d(\left|0\right\rangle_{dp})&=1-\left(\left|a_{01}\right|^2+\left|a_{10}\right|^2\right),\\P_d(\left|1\right\rangle_{dp})&=1-\left(\left|b_{01}\right|^2+\left|b_{10}\right|^2\right)。\end{aligned}\tag{10}$$

被检测的概率为零，即 $P_d\left(\left|0\right\rangle_{dp}\right)=0$，$P_d\left(\left|1\right\rangle_{dp}\right)=0$，也就是满足 $a_{00}=a_{11}=b_{00}=b_{11}=0$，将其代入式(8)可得

$$\begin{aligned}U_E\left|0\right\rangle_{dp}\left|E_i\right\rangle&=U_E\left|01\right\rangle\left|E_i\right\rangle=\sqrt{\alpha}\left|01\right\rangle\left|e_0e_1\right\rangle+\sqrt{1-\alpha}\left|10\right\rangle\left|e_1e_0\right\rangle,\\U_E\left|1\right\rangle_{dp}\left|E_i\right\rangle&=U_E\left|10\right\rangle\left|E_i\right\rangle=\sqrt{1-\alpha}\left|01\right\rangle\left|e_0'e_1'\right\rangle+\sqrt{\alpha}\left|10\right\rangle\left|e_1'e_0'\right\rangle,\end{aligned}\tag{11}$$

式中：$\alpha=\left|a_{01}\right|^2$，$\beta=\left|b_{01}\right|^2$。根据协议，Charlie 准备逻辑量子态 $\left|\phi^+\right\rangle_{1234}^{dp}$，并将两逻辑量子比特分别发送给 Alice 和 Bob，Alice(Bob)选择是否测量并转发给 Charlie，U_F 为逻辑量子态从 Alice(Bob)返回 Charlie 过程中 Eve 的窃听操作

$$U_FU_E\left|0\right\rangle_{dp}\left|E_i\right\rangle=\sqrt{\alpha}\left(\sqrt{\beta}\left|01\right\rangle\left|\varepsilon_0\varepsilon_0\right\rangle+\sqrt{1-\beta}\left|10\right\rangle\left|\varepsilon_0\varepsilon_1\right\rangle\right)+\sqrt{1-\alpha}\left(\sqrt{\beta}\left|10\right\rangle\left|\varepsilon_1\varepsilon_0\right\rangle+\sqrt{1-\beta}\left|01\right\rangle\left|\varepsilon_1\varepsilon_1\right\rangle\right),\tag{12}$$

$$U_{\mathrm{F}}U_{\mathrm{E}}|1\rangle_{\mathrm{dp}}|E_i\rangle=\sqrt{1-\alpha}\left(\sqrt{\beta}|01\rangle|\varepsilon_0'\varepsilon_0'\rangle+\sqrt{1-\beta}|10\rangle|\varepsilon_0'\varepsilon_1'\rangle\right)+\sqrt{\alpha}\left(\sqrt{\beta}|10\rangle|\varepsilon_1'\varepsilon_0'\rangle+\sqrt{1-\beta}|01\rangle|\varepsilon_1'\varepsilon_1'\rangle\right),\tag{13}$$

式中：$\langle\varepsilon_i\varepsilon_j|\varepsilon_i\varepsilon_j\rangle=1$，$\langle\varepsilon_i'\varepsilon_j'|\varepsilon_i'\varepsilon_j'\rangle=1$，且 $i,j\in\{0,1\}$。最后，Eve通过测量辅助量子以提取有用信息。

总量子系统经过Eve的 U_{E} 和 U_{F} 操作后，可以表示为

$$\begin{aligned}U_{\mathrm{F}}U_{\mathrm{E}}|\psi\rangle=\frac{1}{\sqrt{2}}\Big[&\left(\left(\sqrt{\alpha}\sqrt{\beta}|01\rangle_{12}|\varepsilon_0\varepsilon_0\rangle+\sqrt{\alpha}\sqrt{1-\beta}|10\rangle_{12}|\varepsilon_0\varepsilon_1\rangle\right)|01\rangle_{34}+\right.\\&\left(\sqrt{1-\alpha}\sqrt{\beta}|10\rangle_{12}|\varepsilon_1\varepsilon_0\rangle+\sqrt{1-\alpha}\sqrt{1-\beta}|01\rangle_{12}|\varepsilon_1\varepsilon_1\rangle\right)|01\rangle_{34}+\\&\left(\sqrt{\alpha}\sqrt{\beta}|10\rangle_{12}|\varepsilon_1'\varepsilon_0'\rangle+\sqrt{\alpha}\sqrt{1-\beta}|01\rangle_{12}|\varepsilon_1'\varepsilon_1'\rangle\right)|10\rangle_{34}+\\&\left.\left(\sqrt{1-\alpha}\sqrt{\beta}|01\rangle_{12}|\varepsilon_0'\varepsilon_0'\rangle+\sqrt{1-\alpha}\sqrt{1-\beta}|10\rangle_{12}|\varepsilon_0'\varepsilon_1'\rangle\right)|10\rangle_{34}\right],\end{aligned}\tag{14}$$

则Charlie发现Eve窃听的概率 $P_{\mathrm{d}}=\left|\sqrt{\alpha}\sqrt{1-\beta}\right|^2+\left|\sqrt{1-\alpha}\sqrt{\beta}\right|^2$，要使 P_{d} 最小化，则 $\alpha=\beta=1$ 或 $\alpha=\beta=0$。当 $\alpha=\beta=1$ 时，式(14)可改写为

$$U_{\mathrm{F}}U_{\mathrm{E}}|\psi\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle_{12}|\varepsilon_0\varepsilon_0\rangle|01\rangle_{34}+|10\rangle_{12}|\varepsilon_1'\varepsilon_0'\rangle|10\rangle_{34}\right),\tag{15}$$

密度矩阵为

$$\begin{aligned}\boldsymbol{\rho}_1=\frac{1}{2}\Big(&|01\rangle|\varepsilon_0\varepsilon_0\rangle|01\rangle\langle01|\langle\varepsilon_0\varepsilon_0|+|10\rangle|\varepsilon_1'\varepsilon_0'\rangle|10\rangle\langle10|\langle\varepsilon_1'\varepsilon_0'|+\\&|01\rangle|\varepsilon_0\varepsilon_0\rangle|01\rangle\langle10|\langle\varepsilon_1'\varepsilon_0'|+|10\rangle|\varepsilon_1'\varepsilon_0'\rangle|10\rangle\langle01|\langle\varepsilon_0\varepsilon_0|\Big),\end{aligned}\tag{16}$$

Eve利用测量基 $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ 取出总系统密度矩阵中的逻辑量子态，得到附加粒子的密度矩阵

$$\boldsymbol{\rho}_1'=|\varepsilon_0\varepsilon_0\rangle\langle\varepsilon_0\varepsilon_0|+|\varepsilon_1'\varepsilon_0'\rangle\langle\varepsilon_1'\varepsilon_0'|,\tag{17}$$

用测量基 $\{|\varepsilon_0\varepsilon_0\rangle,|\varepsilon_1'\varepsilon_0'\rangle\}$ 测量该系统，其密度矩阵可写为

$$\boldsymbol{\rho}_1'=\begin{pmatrix}1&0\\0&1\end{pmatrix}。\tag{18}$$

同理，当 $\alpha=\beta=0$ 时，系统的密度矩阵为 $\boldsymbol{\rho}_2'=\begin{pmatrix}1&0\\0&1\end{pmatrix}$。则Eve可以得到的最大信息量为辅助量子的冯诺依曼熵 $S_{\mathrm{Eve}}=-\sum_{k=0}^{1}\lambda_k\log_2\lambda_k=0$，其中 $\lambda_0=\lambda_1=1$ 为密度矩阵 $\boldsymbol{\rho}_i'$，$(i=1,2)$ 的特征值。综上所述，Eve在不被发现的情况下，不能通过纠缠测量攻击获得有用信息。窃听者Eve想要得到Alice和Bob的测量结果，就需引入错误，从而被检测到。

3）截断重发攻击

第三方Eve可以通过截断Alice和Bob发送给Charlie的量子态，并对其进行测量，最后选择合适的量子态并重新发送给Charlie，并期待依据测量结果获取 K_{S} 相关信息。Eve采用Z基 $\{|0\rangle_{\mathrm{dp}},|1\rangle_{\mathrm{dp}}\}$ 测量，若Alice和Bob都没有对发送给Charlie的量子态进行任何操作，则Eve测量结果为 $\{|0\rangle_{\mathrm{dp}}|0\rangle_{\mathrm{dp}},|1\rangle_{\mathrm{dp}}|1\rangle_{\mathrm{dp}}\}$ 中的一种；若Alice和Bob至少有一个对发送给Charlie的量子态进行测量，则Eve测量结果仍为 $\{|0\rangle_{\mathrm{dp}}|0\rangle_{\mathrm{dp}},|1\rangle_{\mathrm{dp}}|1\rangle_{\mathrm{dp}}\}$ 中的一种。Eve不能通过截断操作获得任何关于Alice和Bob测量的信息，其重发量子态只能从纠缠态 $|\phi^+\rangle^{\mathrm{dp}}$ 和测量值之间随机挑选，则Charlie没有发现Eve窃听的概率为 $\frac{1}{2^{8n}}$。因此，Eve只能通过猜测得到 K_{S}，正确得到 K_{S} 的概率为 $1-\frac{1}{8}\times\frac{1}{2^n}=1-\frac{1}{2^{n+3}}$，被Charlie发现窃听的概率为 $1-\frac{1}{2^{8n}}$，且当 n 足够大时，得到被发现窃听的概率为1。

4.3 协议特点

1）可扩展性

上述免疫集体噪声的半量子盲签名协议可以在签名方Charlie的协助下完成2个经典方的签名验证，可推广到量子签名网上，如图2所示。图中QuS A、QuS B和QuS C为量子签名服务器，Cell A、Cell B和Cell C分别为QuS A、QuS B和QuS C能够服务的区域，user Ai为A区经典方用户，user Bi和user Ci分别为B区和C区经典方用户。同一区域中不同经典方签名，具体步骤为上述协议所述；不同区域经典方用户之间进行签名，可通过量子签名服务器进行中继，其中继方式为量子隐形传态。不失一般性，假设user A1与user B1传递消息并签名，则其与同一区域量子签名的差异有：i）初始化阶段中QuS A与user A1共享密钥 K_{A1}，QuS B与user B1共享密钥 K_{B1}，QuS A制备量子态 $|\phi^+\rangle_{1234}^L$，将粒子1和粒子2发送给QuS B，留下粒子3和粒子4；

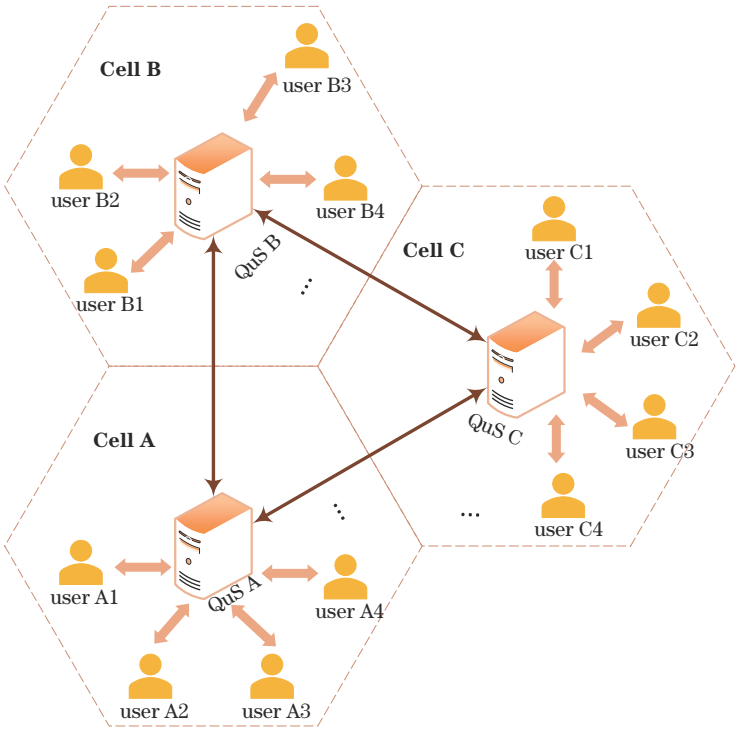

图 2　半量子签名网络示意图

Fig. 2　Schematic of semi-quantum blind signature network

ii)签名阶段中 user A1将盲化后消息发送给 QuS A。QuS A将盲化消息序列$|01\rangle_{56}$或$|10\rangle_{56}$与粒子3和粒子4进行 Bell 测量得到$|\varphi\rangle_{35}$和$|\varphi\rangle_{46}$，并将测量结果发送给 QuS B，QuS B 测量粒子1和粒子2，则 QuS B 接收序列与测量结果对应关系如表6所示。最后，经 QuS B将消息签名发送给 user B1，并判断是否接受签名。

表6　QuS B接收结果与QuS A测量结果对应规则

Table 6　Rules of QuS B receiving message with measurement of QuS A

QuS A measurement result $\|\varphi\rangle_{35}$	QuS A measurement result $\|\varphi\rangle_{46}$	QuS B measurement result $\|\varphi\rangle_{12}$	QuS B
$\|\phi^+\rangle_{35}$ or $\|\phi^-\rangle_{35}$	$\|\phi^+\rangle_{46}$ or $\|\phi^-\rangle_{46}$	$\|01\rangle$	$\|01\rangle$
$\|\psi^+\rangle_{35}$ or $\|\psi^-\rangle_{35}$	$\|\psi^+\rangle_{46}$ or $\|\psi^-\rangle_{46}$	$\|10\rangle$	$\|01\rangle$
$\|\phi^+\rangle_{35}$ or $\|\phi^-\rangle_{35}$	$\|\phi^+\rangle_{46}$ or $\|\phi^-\rangle_{46}$	$\|10\rangle$	$\|10\rangle$
$\|\psi^+\rangle_{35}$ or $\|\psi^-\rangle_{35}$	$\|\psi^+\rangle_{46}$ or $\|\psi^-\rangle_{46}$	$\|01\rangle$	$\|10\rangle$

2) 密钥的可复用性

密钥K_S是实现盲签名的主要手段，通过前一次签名更新下一次所需的K_S，高效运行，提高协议效率。

5　结　　论

提出了免疫集体退相位噪声或集体旋转噪声的半量子盲签名协议，包含经典方消息拥有者 Alice，量子方签名者 Charlie 和经典方消息接收者和签名验证者 Bob，可以实现2个经典方在集体退相位噪声或集体旋转噪声的情况下进行盲签名。本方案可以减少量子资源的消耗，同时在量子方的协助下实现无量子计算能力方的签名。安全性分析表明，本方案能够抵抗现有攻击手段，满足不可抵赖性和不可伪造性等量子签名方案基本特点，即使在签名方 Charlie 不可信的情况下，Charlie 也不能成功伪造 Alice 消息。当第三方 Eve 试图通过纠缠测量攻击窃取K_S相关信息，从而得到消息M，若使 Charlie 发现攻击的概率为0，则 Eve 通过辅助量子得到的最大信息熵为零。即 Eve 获取的最大信息量$S_{Eve}>0$，则必有 Charlie 检测到攻击的概率$P_d>0$。当 Eve 采用截断重发策略进行攻击时，被检测到的概率为$1-\left(\frac{1}{2}\right)^{8n}$，且$n$越大，Charlie 发现窃听的概率趋近于1。另外，本协议可以通过量子隐形传态的方式组网扩展成量子签名网络，实现跨区域的量子签名。

参　考　文　献

[1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.

[2] Acín A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks[J]. Physical Review Letters, 2007, 98(23): 230501.

[3] Yin Z Q, Wang S, Chen W, et al. Reference-free-independent quantum key distribution immune to detector side channel attacks[J]. Quantum Information Processing, 2014, 13(5): 1237-1244.

[4] 虞味, 周媛媛. 基于预报单光子源的相位匹配被动诱骗态量子密钥分配[J]. 光学学报, 2021, 41(2): 0227001.
Yu W, Zhou Y Y. Phase-matched passive-decoy-state quantum key distribution based on heralded single photon source[J]. Acta Optica Sinica, 2021, 41(2): 0227001.

[5] 何业锋, 白倩, 李丽娜, 等. 基于多晶体指示源的测量设备无关量子密钥分配协议[J]. 光学学报, 2021, 41(16): 1627001.
He Y F, Bai Q, Li L N, et al. Measurement-device-independent quantum key distribution protocols based on multiple crystal heralded source[J]. Acta Optica Sinica, 2021, 41(16): 1627001.

[6] Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. Physical Review A, 2003, 68(4): 042317.

[7] 龙桂鲁, 王川, 李岩松, 等. 量子安全直接通信[J]. 中国科学: 物理学 力学 天文学, 2011, 41(4): 332-342.
Long G L, Wang C, Li Y S, et al. Quantum secure direct communication[J]. Scientia Sinica (Physica, Mechanica & Astronomica), 2011, 41(4): 332-342.

[8] Zhou Z R, Sheng Y B, Niu P H, et al. Measurement-device-independent quantum secure direct communication [J]. Science China Physics, Mechanics & Astronomy, 2019, 63(3): 230362.

[9] Tavakoli A, Herbauts I, Żukowski M, et al. Secret sharing with a single d-level quantum system[J]. Physical Review A, 2015, 92(3): 030302.

[10] Wang X J, An L X, Yu X T, et al. Multilayer quantum secret sharing based on GHZ state and generalized Bell basis measurement in multiparty agents[J]. Physics Letters A, 2017, 381(38): 3282-3288.

[11] Ye C Q, Ye T Y, He D, et al. Multiparty semi-quantum secret sharing with d-level single-particle states[J]. International Journal of Theoretical Physics, 2019, 58(11): 3797-3814.

[12] Zeng G H, Keitel C H. Arbitrated quantum-signature scheme[J]. Physical Review A, 2002, 65(4): 042312.

[13] Wen X J, Niu X M, Ji L P, et al. A weak blind signature scheme based on quantum cryptography[J]. Optics Communications, 2009, 282(4): 666-669.

[14] Yin X R, Ma W P, Liu W Y. A blind quantum signature scheme with χ -type entangled states[J]. International Journal of Theoretical Physics, 2012, 51(2): 455-461.

[15] Tian Y, Chen H, Ji S F, et al. A broadcasting multiple blind signature scheme based on quantum teleportation[J]. Optical and Quantum Electronics, 2014, 46(6): 769-777.

[16] Zhang W, Qiu D W, Zou X F, et al. Analyses and improvement of a broadcasting multiple blind signature scheme based on quantum GHZ entanglement[J]. Quantum Information Processing, 2017, 16(6): 150.

[17] Zhang L, Sun H W, Zhang K J, et al. The security problems in some novel arbitrated quantum signature protocols[J]. International Journal of Theoretical Physics, 2017, 56(8): 2433-2444.

[18] Chen F L, Wang Z H, Hu Y M. A new quantum blind signature scheme with BB84-state[J]. Entropy, 2019, 21(4): 336.

[19] 王俊辉, 李云霞, 蒙文, 等. 基于两粒子和三粒子最大纠缠态的量子盲签名协议[J]. 激光与光电子学进展, 2021, 58(7): 0727002.
Wang J H, Li Y X, Meng W, et al. Protocol of quantum blind signature based on two-qubit and three-qubit maximally entangled states[J]. Laser & Optoelectronics Progress, 2021, 58(7): 0727002.

[20] Liang X Q, Wu Y L, Zhang Y H, et al. Quantum multi-proxy blind signature scheme based on four-qubit cluster states[J]. International Journal of Theoretical Physics, 2019, 58(1): 31-39.

[21] Liu G, Ma W P, Cao H, et al. A novel quantum group proxy blind signature scheme based on five-qubit entangled state[J]. International Journal of Theoretical Physics, 2019, 58(6): 1999-2008.

[22] Zhang J L, Zhang J Z, Xie S C. Improvement of a quantum proxy blind signature scheme[J]. International Journal of Theoretical Physics, 2018, 57(6): 1612-1621.

[23] Yang Y Y, Xie S C, Zhang J Z. An improved quantum proxy blind signature scheme based on genuine seven-qubit entangled state[J]. International Journal of Theoretical Physics, 2017, 56(7): 2293-2302.

[24] Li X Y, Chang Y, Zhang S B, et al. Quantum blind signature scheme based on quantum walk[J]. International Journal of Theoretical Physics, 2020, 59(7): 2059-2073.

[25] Niu X F, Ma W P, Chen B Q, et al. A quantum proxy blind signature scheme based on superdense coding[J]. International Journal of Theoretical Physics, 2020, 59(4): 1121-1128.

[26] Wang X B. Fault tolerant quantum key distribution protocol with collective random unitary noise[J]. Physical Review A, 2005, 72(5): 050304.

[27] Li X H, Deng F G, Zhou H Y. Efficient quantum key distribution over a collective noise channel[J]. Physical Review A, 2008, 78(2): 022321.

[28] Yang Y G, Wen Q Y. Arbitrated quantum signature of classical messages against collective amplitude damping noise [J]. Optics Communications, 2010, 283(16): 3198-3201.

[29] Zhang M H, Li H F. Fault-tolerant quantum blind signature protocols against collective noise[J]. Quantum Information Processing, 2016, 15(10): 4283-4301.

[30] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob[C]//2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM′07), January 2-6, 2007, Guadeloupe, French Caribbean. New York: IEEE Press, 2007: 10.

[31] Zhao X Q, Chen H Y, Wang Y Q, et al. Semi-quantum Bi-signature scheme based on W states[J]. International Journal of Theoretical Physics, 2019, 58(10): 3239-3251.

[32] Chen L Y, Liao Q, Tan R C, et al. Offline arbitrated semi-quantum signature scheme with four-particle cluster state[J]. International Journal of Theoretical Physics, 2020, 59(12): 3685-3695.

[33] Boyer M, Gelles R, Kenigsberg D, et al. Semiquantum key distribution[J]. Physical Review A, 2009, 79(3): 032341.

[34] Yu K F, Yang C W, Liao C H, et al. Authenticated

semi-quantum key distribution protocol using Bell states[J]. Quantum Information Processing, 2014, 13(6): 1457-1465.

[35] Krawec W O. Mediated semiquantum key distribution[J]. Physical Review A, 2015, 91(3): 032323.

[36] Krawec W O. Security of a semi-quantum protocol where reflections contribute to the secret key[J]. Quantum Information Processing, 2016, 15(5): 2067-2090.

[37] Li C M, Yu K F, Kao S H, et al. Authenticated semi-quantum key distributions without classical channel[J]. Quantum Information Processing, 2016, 15(7): 2881-2893.

[38] He J J, Li Q, Wu C H, et al. Measurement-device-independent semiquantum key distribution[J]. International Journal of Quantum Information, 2018, 16(2): 1850012.

[39] Rong Z B, Qiu D W, Mateus P, et al. Mediated semi-quantum secure direct communication[J]. Quantum Information Processing, 2021, 20(2): 58.