

一种可抵抗双重CNOT攻击的半量子秘密共享方案

任少轩, 娄小平, 杨艺清

(湖南师范大学 信息科学与工程学院, 湖南 长沙 410081)

摘要: 半量子秘密共享的目的是允许拥有全量子能力的信息发布者将秘密信息分成两个部分, 分别交给两个仅具备经典能力的参与者进行管理, 只有当两位参与者共同协作时才能获得原始的秘密信息。为此, 提出一种半量子秘密共享方案, 使用Bell态纠缠粒子作为信息传输的媒介, 协议中的经典参与者无需具备测量和制备新粒子的能力, 只需通过粒子进行泡利操作就能实现秘密共享。安全性分析表明, 该协议不仅能抵抗拦截重发攻击、测量重发攻击、纠缠测量攻击、特洛伊木马攻击, 还可抵抗双重CNOT攻击, 效率达到25%, 相较于以往同类型的半量子私有比较协议更安全、高效, 并在IBM量子云平台上对该方案过程进行了实验验证, 证明了该方法的正确性。

关键词: 量子通信; 半量子秘密共享; 双重CNOT; 测量能力; IBM量子云平台

DOI: 10.11907/rjdk.241438

开放科学(资源服务)标识码(OSID):

中图分类号: TN918

文献标识码: A

文章编号: 1672-7800(2025)006-0128-08



A Semi-quantum Secret Sharing Scheme Against Double CNOT Attack

REN Shaoxuan, LOU Xiaoping, YANG Yiqing

(College of Computer Science and Engineering, Hunan Normal University, Changsha 410081, China)

Abstract: Purpose of semi quantum secret sharing is to allow information publishers with full quantum capabilities to divide secret information into two parts and hand them over to two participants with only classical capabilities for management. Only when the two participants work together can they obtain the original secret information. To this end, a semi quantum secret sharing scheme is proposed, which uses Bell state entangled particles as a medium for information transmission. The classical participants in the protocol do not need to have the ability to measure and prepare new particles, and only need to perform Pauli operations on the particles to achieve secret sharing. Security analysis shows that this protocol can not only resist interception resend attacks, measurement resend attacks, entanglement measurement attacks, Trojan horse attacks, but also resist dual CNOT attacks, with an efficiency of 25%. Compared with previous similar semi quantum private comparison protocols, it is more secure and efficient. The process of this scheme has been experimentally verified on the IBM quantum cloud platform, proving the correctness of this method.

Key Words: quantum communication; semi-quantum secret sharing; double CNOT; measurement capability; IBM quantum cloud platform

0 引言

随着信息技术迅速发展, 传统密码学虽已广泛应用于各领域, 但信息安全问题日益严峻, 使经典密码学面临着

前所未有的挑战^[1-5]。经典密码学的安全性主要依赖于数学的复杂性, 理论上任何经典密码都可能在足够的时间后被破解。与此相反, 量子密码学将量子态作为信息载体, 利用量子力学定理和法则保证其安全性, 所有计算都严格遵循物理定律, 无法通过数学方法破解, 因此量子密码学

收稿日期: 2024-05-09

扫描二维码阅读全文:

基金项目: 湖南省自然科学基金面上项目(2024JJ5273)

作者简介: 任少轩(1999-), 女, 湖南师范大学信息科学与工程学院硕士研究生, 研究方向为软件工程、量子信息; 娄小平(1982-), 女, 博士, CCF高级会员, 湖南师范大学信息科学与工程学院教授、硕士生导师, 研究方向为信息安全技术、经典密码学、量子信息、安全通信协议等; 杨艺清(1973-), 男, 博士, 湖南师范大学信息科学与工程学院副教授, 研究方向为信息安全技术、网络技术。本文通讯作者: 杨艺清。



绝对安全^[6,7]。正因如此,量子密码学引起了研究者的广泛关注,并取得了显著进展,涌现出众多半量子密码协议,例如半量子密钥分发协议(Semi Quantum Key Distribution Protocol, SQKD)、半量子私有比较(Semi Quantum Private Comparison, SQPC)、半量子安全直接通信(Semi Quantum Secure Direct Communication, SQSDC)、半量子秘密共享(Semi Quantum Secret Sharing, SQSS)等^[8-20]。

Li 等^[21]将半量子概念引入 QSS 中,提出了第一个半量子秘密共享协议。Yin 等^[22]提出基于 Bell 状态的 SQSS 协议,但存在安全漏洞,恶意参与者可通过拦截重发攻击来获取 Alice 的秘密,当方案扩展到多方时最后一个参与者能独立获得 Alice 的秘密。Li 等^[23]提出了一种 SQSS 协议,参与者无需具备测量能力,且具有全量子能力的 Alice 不需要访问量子存储器,但恶意参与者可在不被检测到的情况下,通过执行双重 CNOT 攻击窃取另一个参与者的部分秘密信息。Tian 等^[24]提出的一种高效的半量子秘密共享协议中也存在同样的漏洞,窃听者能通过双重 CNOT 攻击窃取到秘密。Hu 等^[25]在高维量子系统中基于乘积态提出一个更简单、有效的 SQSS 协议,该协议使用高维量子系统,具有更高的安全性且能共享更多信息。

研究表明,大部分协议均要求经典参与者具备测量和制备新粒子的能力,一些方案还可能存在安全漏洞,无法有效应对恶意窃听者的拦截重发攻击和双重 CNOT 攻击^[26-29]。为此,本文提出一种基于 Bell 态的半量子秘密共享方案,参与者无需具备测量和制备新粒子的能力,仅通过泡利操作即可实现秘密共享。更重要的是,该方案在安全性上具有明显优势,不仅能有效抵御多种常见的攻击,还能够抵挡双重 CNOT 攻击,相较于其他协议更安全、更高效。

1 泡利算子

Bell 态是两个量子比特中最大的纠缠态,可写成 $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ 。其中, α, β 分别表示坍塌成 $|0\rangle$ 和 $|1\rangle$ 的概率值,且 $|\alpha|^2 + |\beta|^2 = 1$,由此存在以下 4 种状态:

$$\begin{cases} |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{cases} \quad (1)$$

泡利算子是常用的单量子门,通常指的是 4 个常用的泡利矩阵:

$$\sigma_0 \equiv I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_1 \equiv X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\sigma_2 \equiv Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_3 \equiv Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (2)$$

对 $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ 执行 4 种泡利算子后得到的结果如表 1 所示。

Table 1 Result of the Pauli operations on the Bell state

表 1 在 Bell 态上执行泡利算子的结果

初始 Bell 态	泡利算子	经过泡利算子后的 Bell 态
$ \phi^+\rangle(\phi^+\rangle)$	I	$ \phi^+\rangle(\phi^+\rangle)$
	X	$ \psi^+\rangle(\psi^+\rangle)$
	Y	$ \psi^-\rangle(\psi^+\rangle)$
	Z	$ \phi^-\rangle(\phi^+\rangle)$
$ \psi^+\rangle(\psi^+\rangle)$	I	$ \psi^+\rangle(\psi^+\rangle)$
	X	$ \phi^+\rangle(\phi^+\rangle)$
	Y	$ \phi^-\rangle(\phi^+\rangle)$
	Z	$ \psi^-\rangle(\psi^+\rangle)$

2 协议描述

本文提出一种使用 Bell 态的 SQSS 协议,信息发布者 Alice 想要与两个经典的参与者 Bob 和 Charlie 分享秘密信息。Alice 拥有完整的量子能力,而 Bob、Charlie 只能执行以下操作:①CTRL:经典参与者不受干扰地直接反射 Alice 发送的粒子;② U_m 操作:经典参与者从 4 个泡利算子中随机选择一个执行,然后将得到的粒子发送给 Alice。

随后,记录上述两个经典参与者与 Alice 发送的粒子进行操作所对应的 $m_b^i(m_c^i)$,其中 $i = 0, 1, \dots, n$,如表 2 所示。例如,Bob 执行 U_{00} 操作,那么他将执行的是泡利算子 I ,同时记录 $m_b^i = 00$ 。

Table 2 Operation of two classic participants on the particles sent by Alice

表 2 两个经典参与者对 Alice 发送的粒子的操作

Bob/Charlie 的选择	记录对应的 m_b^i/m_c^i
I	00
X	01
Y	11
Z	10

图 1 为 SQSS 协议的框架,包括以下 5 个步骤:

步骤一:首先,Alice 制备 $4n$ 长度的 Bell 态序列,粒子都从 $\{|\phi^+\rangle, |\psi^+\rangle\}$ 中随机选择。Alice 将纠缠对的第一个粒子形成序列 $S_B = \{p_b^1, p_b^2, \dots, p_b^{4n}\}$,将第二个粒子形成序列 $S_C = \{p_c^1, p_c^2, \dots, p_c^{4n}\}$,每个 (p_b^i, p_c^i) 为一对纠缠对;其次,将序列 S_B 和 S_C 重新排序得到 S'_B, S'_C ,需要注意的是排序后的 p_b^i 与 p_c^i 不在同一个位置上;最后,Alice 将序列 S'_B 发送给 Bob,将序列 S'_C 发给 Charlie。

步骤二:当 Bob/Charlie 收到粒子后,Alice 在公共信道

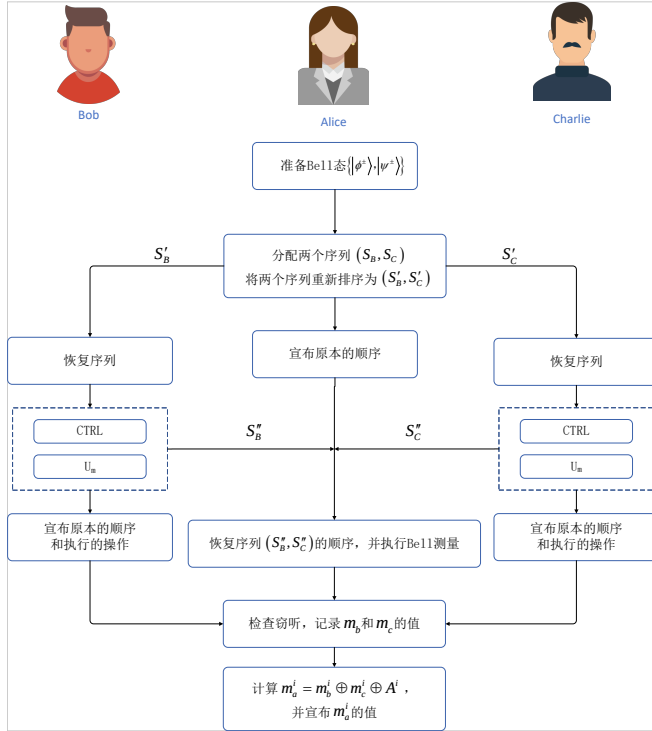


Fig. 1 Process of the proposed protocol

图1 本文所提协议的流程

上宣布序列 S'_B/S'_C 的原始顺序。在 Bob/Charlie 恢复序列 S'_B/S'_C 的顺序后,对每个粒子随机选择 CTRL 或 U_m 操作,然后重新排序序列中的所有粒子得到 S''_B/S''_C ,并将 S''_B/S''_C 发送回 Alice。

步骤三: Alice 从 Bob 和 Charlie 收到粒子后,要求他们公布粒子的原始顺序及执行的操作。值得注意的是,他们只宣布选择的是 CTRL 还是 U_m ,不会宣布具体执行哪个泡利算子。在 Bob 和 Charlie 宣布了最初的顺序后 Alice 恢复顺序,并对两个序列中相同位置的粒子进行 Bell 测量。

步骤四: Alice 根据 Bob、Charlie 的选择执行相应操作,此时会有 4 种情况,如表 3 所示。

Table 3 Operations of 3 participants in 4 different situations

表3 3名参与者在4种情况下的操作

案例	Bob 的选择	Charlie 的选择	Alice 的操作
1	CTRL	CTRL	窃听检测
2	CTRL	U_m	记录相应的 m_c^i
3	U_m	CTRL	记录相应的 m_b^i
4	U_m	U_m	窃听检测

(1) 当 Bob 与 Charlie 同时选择 CTRL 时, Alice 将测量结果与初始 Bell 态进行比较,通过错误率推断是否存在窃听者。例如, Alice 最初准备的是 $|\phi^+\rangle$, 如果没有窃听者,测量结果也应为 $|\phi^+\rangle$ 。

(2) 当 Bob 选择 CTRL 操作, Charlie 选择 U_m 操作时, Alice 根据表 1 将测量结果与初始 Bell 态进行比较以知晓 Charlie 执行的操作,再根据表 2 得到 m_c^i 值。

(3) 当 Bob 选择 U_m 操作, Charlie 选择 CTRL 操作时, Alice 根据表 1 将测量结果与初始 Bell 态进行比较即可知晓

Bob 执行的操作,再根据表 2 得到 m_b^i 的值。

(4) 当 Bob 与 Charlie 同时选择 U_m 操作时, Alice 通知他们执行相应例子上的哪个泡利算子,并将测量结果与初始 Bell 态进行比较,通过错误率推断是否有窃听者。例如,如果 Alice 最初准备的是 $|\phi^+\rangle$, Bob 选择了泡利算子 X , Charlie 选择了泡利算子 I , 如果没有窃听者那么测量结果应为 $|\psi^+\rangle$; 如果错误率高于预定义的阈值则终止该协议,否则后续步骤。

步骤五: Alice 计算 $m_a^i = m_b^i \oplus m_c^i \oplus A^i$, A^i 为 Alice 的秘密信息, m_a^i 为由 $m_b^i \oplus m_c^i \oplus A^i$ 生成的随机数,随后将 m_a^i 的值公布给 Bob 和 Charlie。Bob 与 Charlie 可通过计算等式 $A^i = m_b^i \oplus m_c^i \oplus m_a^i$ 得到 A^i 。

3 实例结果与分析

首先,假设 Alice 要分享的秘密信息为 $A = \{0, 1, 0, 1\}$, 制备了一个由 4 个 Bell 态组成的序列 $S = \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$; 其次, Alice 将纠缠对中的第一个粒子形成序列 $S_B = \{|\phi^+\rangle_b, |\phi^-\rangle_b, |\psi^+\rangle_b, |\psi^-\rangle_b\}$, 将纠缠对中第二个粒子形成序列 $S_C = \{|\phi^+\rangle_c, |\phi^-\rangle_c, |\psi^+\rangle_c, |\psi^-\rangle_c\}$; 再次,重新排序序列得到 $S'_B = \{|\phi^-\rangle_b, |\phi^+\rangle_b, |\psi^-\rangle_b, |\psi^+\rangle_b\}$, $S'_C = \{|\psi^+\rangle_c, |\psi^-\rangle_c, |\phi^+\rangle_c, |\phi^-\rangle_c\}$; 最后, Alice 将序列 S'_B 发送给 Bob, 将序列 S'_C 发送给 Charlie, 在 Bob 与 Charlie 收到粒子并恢复顺序后分别进行 {CTRL, Y, Y, CTRL} 和 {CTRL, I, CTRL, Z} 操作。此时将存在 4 种案例:

(1) 当 Bob 与 Charlie 都选择 CTRL 时。Alice 最初用 $|00\rangle$ 制备 $|\phi^+\rangle$, 在收到 Bob 与 Charlie 发来的粒子后恢复原始顺序,对相同位置的粒子执行 Bell 测量,量子电路如图 2 所示,测量结果如图 3 所示。其中,图 3 中第一、二数值分别代表图 2 第一、二个粒子所在端的结果(图 5、图 7、图 9 同理)。由图 3 可见结果为 00, 表示 Bell 测量结果为 $|\phi^+\rangle$, 说明过程中没有窃听者;反之则有窃听者。

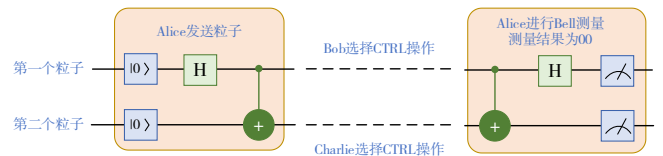


Fig. 2 Quantum circuit when Bob and Charlie choose CTRL operation

图2 当 Bob 与 Charlie 选择 CTRL 操作时的量子电路

(2) 当 Bob 选择泡利算子 Y , Charlie 选择泡利算子 I 时。Alice 最初用 $|10\rangle$ 制备 $|\phi^-\rangle$, Bob 对收到的粒子执行 U_{11} 操作(泡利算子 Y), Charlie 对粒子执行 U_{00} 操作(泡利算子 I),

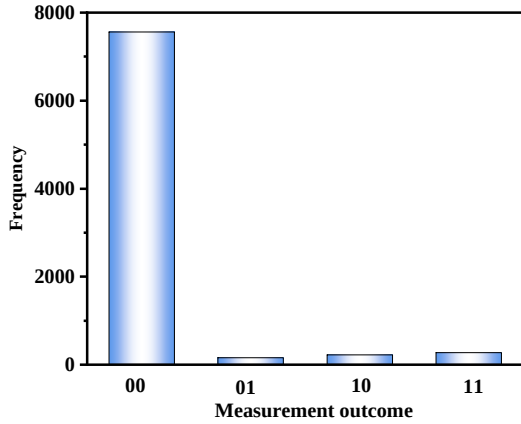


Fig. 3 Simulation results of figure 2

图3 图2的模拟结果

Alice 要求他们宣布具体执行的是何种泡利算子。与此同时, Alice 恢复序列的原始顺序后使用 Bell 态测量他们发送来的粒子, 量子电路图如图 4 所示, 测量结果如图 5 所示。由图 5 可见测量结果为 01, 表示 Bell 测量结果为 $|\psi^+\rangle$ 。Alice 在知晓 Bob 和 Charlie 的选择后, 根据表 1 可推算出理论上的测量结果, 并与实际测量结果进行比较, 结果相同即可证明没有窃听者, 不同则说明有窃听者。

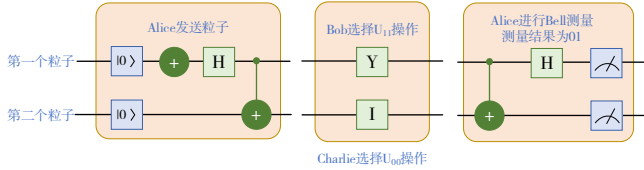
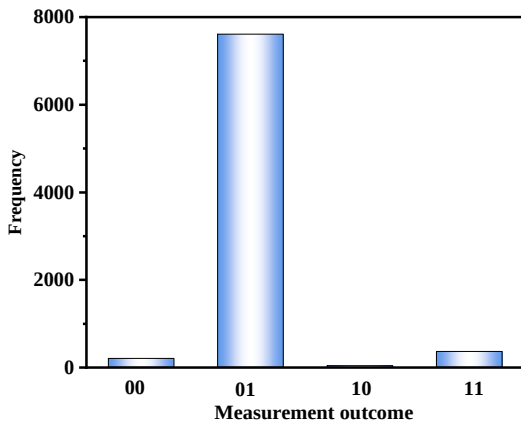
Fig. 4 Quantum circuit when both Bob and Charlie choose U_m operation图4 当 Bob 与 Charlie 选择 U_m 操作时的量子电路

Fig. 5 Simulation results of figure 4

图5 图4的模拟结果

(3) 当 Bob 选择泡利算子 Y, Charlie 选择 CTRL 时。Alice 最初用 $|01\rangle$ 制备 $|\psi^+\rangle$, Bob 对 Alice 发送来的粒子执行 U_{11} 操作(泡利算子 Y)并根据表 1 记录 $m_b^1 = 11$, Charlie 则执行 CTRL 操作。Alice 恢复序列原始顺序后, 使用 Bell 态测量他们发送的粒子, 量子电路图如图 6 所示, 测量结果如

图 7 所示。由图 7 可见结果为 10, 表示测量结果为 $|\phi^-\rangle$, 此时 Bob 执行 U_m 操作(不具体说明执行了哪个泡利算子), Charlie 执行 CTRL 操作。Alice 已知初始 Bell 态和经过操作后的 Bell 态, 可根据表 1 推算出 Bob 执行 Y 操作, 再根据表 2 可得 $m_b^1 = 11$ 。

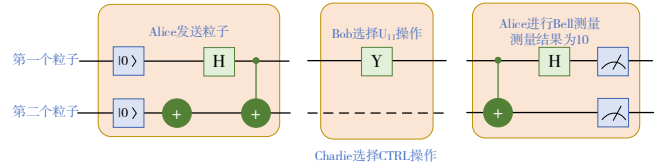
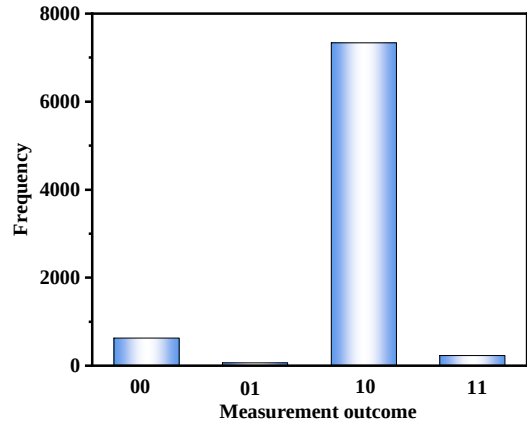
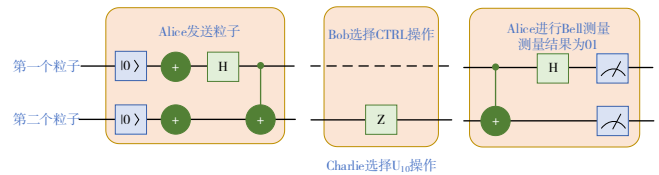
Fig. 6 Quantum circuit when Bob chooses U_m operation and Charlie chooses CTRL operation图6 当 Bob 选择 U_m 操作、Charlie 选择 CTRL 操作时的量子电路

Fig. 7 Simulation results of figure 6

图7 图6电路的模拟结果

(4) 当 Bob 选择 CTRL, Charlie 选择泡利算子 Z 时。Alice 最初用 $|11\rangle$ 制备 $|\psi^-\rangle$, Bob 执行 CTRL 操作, Charlie 对 Alice 发送来的粒子进行 U_{10} 操作(泡利算子 Z)并根据表 1 记录 $m_c^1 = 10$ 。Alice 恢复序列原始顺序后, 对他们发送的粒子进行 Bell 测量, 量子电路图如图 8 所示, 测量结果如图 9 所示。由图 9 可见结果为 01, 表示测量结果为 $|\psi^+\rangle$, 此时 Bob 执行 CTRL 操作, Charlie 执行 U_m 操作(不具体说明执行了哪个泡利算子)。Alice 已知初始 Bell 态和经过操作后的 Bell 态, 可根据表 1 推算出 Charlie 执行 Z 操作, 再根据表 2 可得 $m_c^1 = 10$ 。

Fig. 8 Quantum circuit when Bob chooses CTRL operation and Charlie chooses U_m operation图8 当 Bob 选择 CTRL 操作、Charlie 选择 U_m 操作时的量子电路

在确定没有窃听者后, 将进行后续操作。此时, Alice 已知 $m_b^1 = 11$ 、 $m_c^1 = 10$, 想要分享的秘密为 $A^1 = 10$, 即计算 $m_a^1 = m_b^1 \oplus m_c^1 \oplus A^1 = 11$ 。Alice 将 m_a^1 的值公布给 Bob 和

Charlie后,通过计算 $A^1 = m_b^1 \oplus m_c^1 \oplus m_a^1 = 10$ 可得 Alice 想要分享的秘密信息。

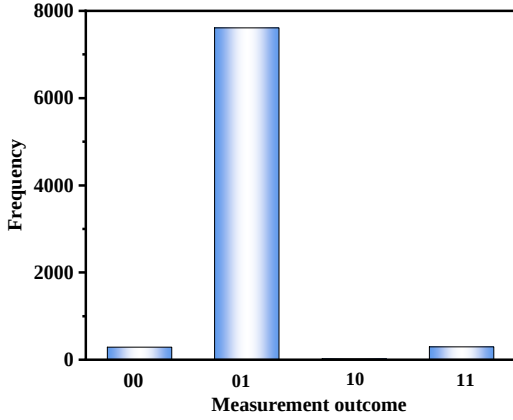


Fig. 9 Simulation results of figure 8

图9 图8的模拟结果

4 安全性分析

一个不诚实的参与者还能充当一个窃听者,相较于外部窃听者能知道更多信息,具有更强的窃听能力。因此,本文重点讨论 SQSS 协议在具有不诚实的内部参与者的情况下的安全性。假设 Charlie 想知道 Bob 的手中的信息,他可能会发起一些著名的攻击,例如拦截重发攻击、测量重发攻击、纠缠测量攻击、双重 CNOT 攻击和特洛伊木马攻击。

4.1 拦截重发攻击

步骤一中假设不诚实的参与者 Charlie 拦截了 Alice 发送给 Bob 的序列,然后制备一个新的序列发送给 Bob。步骤二中 Charlie 拦截了 Bob 发送给 Alice 的序列,并将步骤一中拦截的序列发送给 Alice。

然而,在这种攻击下 Charlie 将不可避免地会在步骤四中被发现。他将在案例 1 和案例 4 的窃听检测中被检测到,原因为他不知道 Bob 如何重新排列序列 S_B^* ,此时协议将在步骤四结束,且 Bob 不会得到任何关于 Alice 秘密信息的有用信息。

4.2 测量重发攻击

假设在步骤一中 Charlie 拦截了 Alice 发送给 Bob 的粒子并进行 Z 基测量(测量一个量子比特是否处于 $|0\rangle$ 状态或 $|1\rangle$ 状态),Charlie 根据测量结果准备一个新序列发送给 Bob。然而,在这种攻击下 Charlie 将不可避免地会在步骤四中被检测到。在案例 1 中假设 Alice 准备的是 $|\phi^+\rangle$,当 Charlie 测量重发攻击后 Alice 准备的粒子将坍缩, Bob 和 Charlie 都选择 CTRL 操作。Charlie 进行测量重发攻击时, Alice 使用 Bell 态测量的结果为 $|\phi^+\rangle$ 或 $|\phi^-\rangle$,即每个被替换粒子的检测概率为 1/2。

类似地,在案例 4 中假设 Alice 准备的是 $|\phi^+\rangle$,当 Bob 与 Charlie 同时执行泡利算子 I 时,Charlie 进行测量重发攻击后 Alice 准备的粒子将坍缩。此时, Alice 使用 Bell 态测量的结果可能为 $|\phi^+\rangle$ 或 $|\phi^-\rangle$,即每个被替换粒子的检测概率为 1/2。

综上,总检出率为 $1/2 \times 1/2 + 1/2 \times 1/2 = 1/2$, Charlie 被检测到的概率为 $P_2 = 1 - (1/2)^{4N}$,当 N 足够大时该攻击的检测概率将达到 100%,此时该协议将在步骤四结束,攻击者不会得到任何关于 Alice 秘密信息的有用信息。

4.3 纠缠测量攻击

假设一个恶意的参与者 Charlie 想要通过纠缠测量攻击获得另一个参与者的秘密,将在步骤一中对 Alice 发送给 Bob 的粒子执行么正操作 U 。

$$U(|0\rangle|\varepsilon\rangle_c) = p_0|0\rangle|\varepsilon_{00}\rangle_c + p_1|1\rangle|\varepsilon_{01}\rangle_c \quad (3)$$

$$U(|1\rangle|\varepsilon\rangle_c) = q_0|0\rangle|\varepsilon_{10}\rangle_c + q_1|1\rangle|\varepsilon_{11}\rangle_c \quad (4)$$

式中: $|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle$ 是由 $U, |p_0|^2 + |p_1|^2 = 1$ 和 $|q_0|^2 + |q_1|^2 = 1$ 唯一确定的纯状态。

本文使用 $|B\rangle_b$ 表示 Alice 发送给 Bob 的粒子,用 $|C\rangle_c$ 表示 Alice 发送给 Charlie 的粒子,用 $|\varepsilon\rangle_c$ 表示 Charlie 的辅助粒子。假设, Alice 准备的 Bell 态为 $|\psi^+\rangle$,当 Bob 与 Charlie 同时选择 CTRL 时他们的粒子仍处于纠缠状态,若此时 Charlie 执行 U 操作状态将会变为:

$$\begin{aligned} U(|\psi^+\rangle|\varepsilon\rangle_c) &= \frac{1}{\sqrt{2}} \left[\left(p_0|0\rangle|\varepsilon_{00}\rangle_c + p_1|1\rangle|\varepsilon_{01}\rangle_c \right)_b |1\rangle_c + \left(q_0|0\rangle|\varepsilon_{10}\rangle_c + q_1|1\rangle|\varepsilon_{11}\rangle_c \right)_b |0\rangle_c \right] \\ &= \frac{1}{\sqrt{2}} \left[\left(p_0|01\rangle_{bc}|\varepsilon_{00}\rangle_c + p_1|11\rangle_{bc}|\varepsilon_{01}\rangle_c \right) + \left(q_0|00\rangle_{bc}|\varepsilon_{10}\rangle_c + q_1|10\rangle_{bc}|\varepsilon_{11}\rangle_c \right) \right] \\ &= \frac{1}{2} \left[p_0(|\psi^+\rangle + |\psi^-\rangle)|\varepsilon_{00}\rangle_c + p_1(|\phi^+\rangle - |\phi^-\rangle)|\varepsilon_{01}\rangle_c \right. \\ &\quad \left. + q_0(|\phi^+\rangle + |\phi^-\rangle)|\varepsilon_{10}\rangle_c + q_1(|\psi^+\rangle - |\psi^-\rangle)|\varepsilon_{11}\rangle_c \right] \\ &= \frac{1}{2} \left[|\psi^+\rangle(p_0|\varepsilon_{00}\rangle_c + q_1|\varepsilon_{11}\rangle_c) + |\psi^-\rangle(p_0|\varepsilon_{00}\rangle_c - q_1|\varepsilon_{11}\rangle_c) \right. \\ &\quad \left. + p_1(|\phi^+\rangle - |\phi^-\rangle)|\varepsilon_{01}\rangle_c + q_0(|\phi^+\rangle + |\phi^-\rangle)|\varepsilon_{10}\rangle_c \right] \end{aligned} \quad (5)$$

Alice 在步骤三中执行 Bell 测量,测量结果为 $|\psi^+\rangle$ 。为

为了使 Charlie 攻击不被发现,他的辅助粒子就应该处于一个

独立状态, 那么必须满足以下条件:

$$U(|\psi^+\rangle|\varepsilon\rangle_c) = \frac{1}{2} \left[|\psi^+\rangle(p_0|\varepsilon_{00}\rangle_c + q_1|\varepsilon_{11}\rangle_c) + |\psi^-\rangle(p_0|\varepsilon_{00}\rangle_c - q_1|\varepsilon_{11}\rangle_c) \right] \\ + p_1(|\phi^+\rangle - |\phi^-\rangle)|\varepsilon_{01}\rangle_c + q_0(|\phi^+\rangle + |\phi^-\rangle)|\varepsilon_{10}\rangle_c \\ = |\psi^+\rangle|\varepsilon\rangle_c \quad (6)$$

根据式(6)可得:

$$p_0 = q_1 = 1, p_1 = q_0 = 0 \quad (7)$$

$$|\varepsilon_{00}\rangle_c = |\varepsilon_{11}\rangle_c \quad (8)$$

将式(7)一式(8)代入式(5)可得:

$$U(|\psi^+\rangle|\varepsilon\rangle_c) = |\psi^+\rangle|\varepsilon_{00}\rangle_c \quad (9)$$

通过上述证明, 要使 Charlie 攻击不被发现就需要在攻击中不能引入错误, 即其辅助粒子与 Bob 的粒子不能相互纠缠, 因此所提协议可抵御恶意参与者的纠缠测量攻击。

4.4 特洛伊木马攻击

在本文的 SQSS 协议中, 假设不诚实的参与者 Charlie 想要执行特洛伊木马攻击。首先, Charlie 拦截 Alice 发送给 Bob 的粒子, 将不可见的光子附加到每个粒子上; 其次, 将被操纵的粒子发送给 Bob 以获得 Bob 的粒子顺序。

SQSS 协议可在所有设备前添加波长滤波器 (Wavelength Filter, WF) 设备与光子数分配器 (Photon number allocator, PNA) 防护该攻击, 以有效防止特洛伊木马程序攻击。

4.5 双重 CNOT 攻击

假设 Charlie 是一个具备完全量子能力的恶意参与者, 试图在步骤一中拦截 Alice 发给 Bob 的序列 S_B , Charlie 生成一个量子比特 $|0\rangle_E$ 作为他的辅助粒子。同时, 假设本文所提协议中 Alice 制备的 Bell 态为:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (10)$$

Charlie 执行第一次 CNOT 操作的计算公式为:

$$U_{CNOT} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11| \quad (11)$$

式中: 从 Bob 截获的量子位 S_B^i 为控制量子位; 辅助粒子 $|0\rangle_E$ 为目标量子位。

Charlie 将 S_B^i 重新发给 Bob 并保留辅助粒子, 根据 Bob 的量子态, 在第一次 CNOT 攻击后整个量子位系统为:

$$U_{CNOT}(|\phi^+\rangle_{BC} \otimes |0\rangle_E) = \frac{1}{\sqrt{2}}(|00\rangle_{BC}|0\rangle_E + |11\rangle_{BC}|1\rangle_E) \quad (12)$$

式中: B 表示 Alice 发给 Bob 的量子; C 表示 Alice 发给 Charlie 的粒子; E 表示 Charlie 的辅助粒子。

在步骤二中, Bob 对粒子随机选择执行 CTRL 或 U_m 操作, Charlie 拦截 Bob 发给 Alice 的序列 S_B^i , 并再次对该序列及其辅助粒子执行第二次 CNOT 操作。此时, 将发生两种情况, 即 Bob 选择 CTRL 操作或 U_m 操作。

(1) 当 Bob 选择 CTRL 模式时, Bob 直接毫无干扰地反射 Alice 发来的粒子。具体地, Charlie 执行第二次 CNOT 操作后, 整个系统的全局状态被转变为:

$$U_{CNOT} \left[\frac{1}{\sqrt{2}}(|00\rangle_{BC}|0\rangle_E + |11\rangle_{BC}|1\rangle_E) \right] = \frac{1}{\sqrt{2}}(|00\rangle_{BC}|0\rangle_E + |11\rangle_{BC}|0\rangle_E) = |\phi^+\rangle_{BC} \otimes |0\rangle_E \quad (13)$$

(2) 当 Bob 选择 U_m 模式时, Bob 会对 Alice 发来的粒子执行以下 4 种操作中的一种。具体地, Charlie 执行第二次 CNOT 操作后, 整个系统的全局状态被转变为:

当 Bob 执行泡利算子 I 时, 计算公式为:

$$|\phi^+\rangle_{BC} = \frac{1}{\sqrt{2}}(|00\rangle_{BC} + |11\rangle_{BC}) \xrightarrow{I} \frac{1}{\sqrt{2}}(|00\rangle_{BC} + |11\rangle_{BC}) = |\phi^+\rangle_{BC} \quad (14)$$

$$U_{CNOT} \left[\frac{1}{\sqrt{2}}(|00\rangle_{BC}|0\rangle_E + |11\rangle_{BC}|1\rangle_E) \right] = \frac{1}{\sqrt{2}}(|00\rangle_{BC}|0\rangle_E + |11\rangle_{BC}|0\rangle_E) = |\phi^+\rangle_{BC} \otimes |0\rangle_E \quad (15)$$

当 Bob 执行泡利算子 X 时, 计算公式为:

$$|\phi^+\rangle_{BC} = \frac{1}{\sqrt{2}}(|00\rangle_{BC} + |11\rangle_{BC}) \xrightarrow{X} \frac{1}{\sqrt{2}}(|01\rangle_{BC} + |10\rangle_{BC}) = |\psi^+\rangle_{BC} \quad (16)$$

$$U_{CNOT} \left[\frac{1}{\sqrt{2}}(|01\rangle_{BC}|0\rangle_E + |10\rangle_{BC}|1\rangle_E) \right] = \frac{1}{\sqrt{2}}(|01\rangle_{BC}|0\rangle_E + |10\rangle_{BC}|0\rangle_E) = |\psi^+\rangle_{BC} \otimes |0\rangle_E \quad (17)$$

当 Bob 执行泡利算子 Y 时, 计算公式为:

$$|\phi^+\rangle_{BC} = \frac{1}{\sqrt{2}}(|00\rangle_{BC} + |11\rangle_{BC}) \xrightarrow{Y} \frac{1}{\sqrt{2}}(|01\rangle_{BC} - |10\rangle_{BC}) = |\psi^-\rangle_{BC} \quad (18)$$

$$U_{CNOT} \left[\frac{1}{\sqrt{2}}(|01\rangle_{BC}|0\rangle_E - |10\rangle_{BC}|1\rangle_E) \right] = \frac{1}{\sqrt{2}}(|01\rangle_{BC}|0\rangle_E - |10\rangle_{BC}|0\rangle_E) = |\psi^-\rangle_{BC} \otimes |0\rangle_E \quad (19)$$

当 Bob 执行泡利算子 Z 时, 计算公式为:

$$|\phi^+\rangle_{BC} = \frac{1}{\sqrt{2}}(|00\rangle_{BC} + |11\rangle_{BC}) \xrightarrow{Z} \frac{1}{\sqrt{2}}(|00\rangle_{BC} - |11\rangle_{BC}) = |\phi^-\rangle_{BC} \quad (20)$$

$$U_{CNOT} \left[\frac{1}{\sqrt{2}}(|00\rangle_{BC}|0\rangle_E - |11\rangle_{BC}|1\rangle_E) \right] = \frac{1}{\sqrt{2}}(|00\rangle_{BC}|0\rangle_E - |11\rangle_{BC}|0\rangle_E) = |\phi^-\rangle_{BC} \otimes |0\rangle_E \quad (21)$$

根据式(13)一(21)可知, Charlie 在双重 CNOT 攻击后其辅助粒子状态始终为 $|0\rangle$, 且不知道 Bob 的操作, 无法从辅助粒子中获得任何有用信息, 因此 Charlie 的双重 CNOT

攻击对本文协议无效。

综上,常见的几种攻击对本文协议无效,验证了该协议的有效性。

5 比较分析

本文提出的SQSS协议采用文献[30]提出的效率自然定义方法,可计算出量子比特效率 $\eta = c/(q + b)$ 。其中, c 为秘密共享的比特数量; q 为传输的量子比特数量; b 为经

典参与者Bob与Charlie使用经典信道占用的比特数量。

Alice还准备了 $4N$ 个Bell态粒子(共 $8N$ 个量子比特),并将他们发送给两个参与者。由于参与者无需制备新粒子,所以 $b = 0$,每个量子比特可分享两比特的信息。因此,本文协议的量子位效率 $\eta = c/(q + b) = 2N/(8N + 0) = 25\%$ 。同理,可计算出文献[19]、[23]的量子效率分别为6.25%和8.33%,而文献[22]、文献[25]的协议由于使用了诱饵粒子来保证其协议的安全性,因此其量子效率将随着诱饵粒子数量增多而降低,故量子效率低于25%,具体结果如表4所示。

Table 4 Comparison of various SQSS protocols

表4 各种SQSS协议比较

方法	量子资源	参与者需要测量能力	参与者需要制备新粒子的能力	是否安全	量子效率/%
文献[22]	Bell态	需要	需要	不安全	<25.00
文献[23]	乘积态	不需要	需要	不安全	8.33
文献[19]	W态	需要	需要	安全	6.25
文献[25]	乘积态	需要	需要	安全	<25.00
本文方法	Bell态	不需要	不需要	安全	25.00

由表4可知,本文协议相较于相似的SQSS协议而言,在量子比特效率、经典参与者的能力和安全性等方面都具有明显优势。首先,在量子比特效率方面,本文所提协议的量子位效率最高;其次,经典参与者的测量与制备粒子的能力对所提协议而言并非必须,因此灵活性更强;再次,所提协议能抵抗4种常见的攻击及双重CNOT攻击,而文献[22,23]分别无法抵挡恶意窃听者的拦截重发攻击和双重CNOT攻击。

6 结语

本文提出一种可抵抗4种常见的攻击及双重CNOT攻击的半量子秘密共享协议,经典参与者无需具备测量和制备粒子的能力,减少了经典参与者对量子器件的需求,灵活性和通用性更优秀。

实验表明,所提协议相较于现有协议更简单、高效,在安全性方面存在明显优势,不仅能抵抗常见的4种攻击,还能抵抗恶意窃听者的双重CNOT攻击。此外,本文还利用IBM量子云平台对协议进行仿真实验,进一步验证了该方案的安全可行性。

参考文献:

- [1] SUN H, QIN J H, LI W P, et al. Reversible information hiding based on secret sharing of multiple hiding devices in medical images[J]. Software Guide, 2023, 22(3): 78-88.
孙昊,秦健豪,李文沛,等. 医学图像的多隐藏器秘密共享可逆信息隐藏[J]. 软件导刊, 2023, 22(3): 78-88.
- [2] SONG Q Q, XU H, YANG D L, et al. Federation chain-based authentication method for IoT devices [J]. Software Guide, 2022, 21 (10) :

212-216.

宋晴晴,徐辉,杨冬蕾,等. 基于联盟链的物联网设备身份认证方法[J]. 软件导刊, 2022, 21(10): 212-216.

- [3] LU H, ZHU Y, CHEN C E, et al. Efficient key generation on lattice cryptography for privacy protection in mobile IoT crowdsourcing[J]. IEEE Internet of Things Journal, 2023, 11(2): 1893-1909.

- [4] LI L, ZHU J W, YANG C Y, et al. An overview on traitor tracking technology based on attribute-based encryption[J]. Software Guide, 2023, 22 (12): 238-244.

李莉,朱江文,杨春艳,等. 基于属性加密的叛逆者追踪技术研究综述[J]. 软件导刊, 2023, 22(12): 238-244.

- [5] BIDOUX L, BRIAUD P, BROS M, et al. RQC revisited and more cryptanalysis for rank-based cryptography[J]. IEEE Transactions on Information Theory, 2023, 70(3): 2271-2286.

- [6] HUO W, YU Y, YANG K, et al. Privacy-preserving cryptographic algorithms and protocols: a survey on designs and applications[J]. Scientia Sinica (Information Sciences), 2023, 53(9): 1688-1733.

霍炜,郝昱,杨糠,等. 隐私保护计算密码技术研究进展与应用[J]. 中国科学(信息科学), 2023, 53(9): 1688-1733.

- [7] MA Z C. The cyber security challenge in the quantum era and its countermeasures [J]. Information and Communications Technology and Policy, 2019(10): 37-42.

马彰超. 量子时代的网络安全挑战及其应对研究[J]. 信息通信技术与政策, 2019(10): 37-42.

- [8] YE Q Q, LI J, CHEN X B, et al. Security and application of semi-quantum key distribution protocol for users with different quantum capabilities [J]. EPJ Quantum Technology, 2023, 10(1): 21.

- [9] GU J, HWANG T. Double C-NOT attack on a single-state semi-quantum key distribution protocol and its improvement [DB/OL]. <https://arxiv.org/abs/2009.12535>.

- [10] YE Q Q, LI J, CHEN X B, et al. An efficient semi-quantum key distri-

- bution protocol and its security proof[J]. IEEE Communications Letters, 2022, 26(6): 1226–1230.
- [11] GONG L H, LI M L, CAO H, et al. Novel semi-quantum private comparison protocol with Bell states[J]. Laser Physics Letters, 2024, 21(5): 55209.
- [12] YANG C W, HUANG Y Y, LIN J, et al. Efficient and secure semi-quantum private comparison protocol using three-particle GHZ-like states against participant attack[J]. Modern Physics Letters A, 2024, 39(10): 2450037.
- [13] SUN Z Y. Improvement of measure-resend semi-quantum private comparison scheme using GHZ states[J]. Quantum Information Processing, 2022, 61(3): 877–887.
- [14] HE Z B, LOU X P. Security analysis and improvement in a semi-quantum private comparison without pre-shared key[J]. Quantum Information Processing, 2023, 22(3): 150.
- [15] WANG P, CHEN X, SUN Z. Semi-quantum secure direct communication against collective-dephasing noise[J]. Quantum Information Processing, 2022, 21(10): 352.
- [16] ZHANG X, ZHOU R G. An efficient and novel semi-quantum deterministic secure quantum communication protocol[J]. International Journal of Theoretical Physics, 2022, 61(4): 94.
- [17] YANG Y F, DUAN L Z, QIU T R, et al. Multi-party semi-quantum secure direct communication using Greenberger-Horne-Zeilinger states[J]. Quantum Information Processing, 2022, 21(9): 324.
- [18] ZHOU Z, WANG Y, DOU Z, et al. $A(t, n)$ threshold protocol of semi-quantum secret sharing based on single particles[J]. Frontiers in Physics, 2023, 11: 1225059.
- [19] TSAI C W, YANG C W, LEE N Y. Semi-quantum secret sharing protocol using w-state[J]. Modern Physics Letters A, 2019, 34(27): 1950213.
- [20] HE F, XIN X, LI C, et al. Security analysis of the semi-quantum secret-sharing protocol of specific bits and its improvement[J]. Quantum Information Processing, 2024, 23(2): 51.
- [21] LI Q, CHAN W H, LONG D Y. Semiquantum secret sharing using entangled states[J]. Physical Review A, 2010, 82(2): 22303.
- [22] YIN A H, WANG Z F, FU F B. A novel semi-quantum secret sharing scheme based on bell states[J]. Modern Physics Letters B, 2017, 31(13): 1750150.
- [23] LI Z L, LIU C D, PENG Y, et al. Limited resource semiquantum secret sharing[J]. Quantum Information Processing, 2018, 17(10): 285.
- [24] TIAN Y, LI J, CHEN X B, et al. An efficient semi-quantum secret sharing protocol of specific bits[J]. Quantum Information Processing, 2021, 20(6): 217.
- [25] HU W W, ZHOU R G, LUO J. Semi-quantum secret sharing in high-dimensional quantum system using product states[J]. Chinese Journal of Physics, 2022, 70(1): 1701–1712.
- [26] CHEN Y, ZOU X, WANG X, et al. Two intercept-and-resend attacks on a bidirectional quantum secure direct communication and its improvement[J]. Quantum Information Processing, 2023, 22(9): 346.
- [27] HE Z, LOU X. Security analysis and improvement in a semi-quantum private comparison without pre-shared key[J]. Quantum Information Processing, 2023, 22(3): 150.
- [28] SUN Z. Improvement of measure-resend semi-quantum private comparison scheme using GHZ states[J]. International Journal of Theoretical Physics, 2022, 61(3): 91.
- [29] LI Q, LI P, XIE L, et al. Security analysis and improvement of a semi-quantum private comparison protocol with three-particle G-like states[J]. Quantum Information Processing, 2022, 21(4): 127.
- [30] CABELLO A. Quantum key distribution in the holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635–5638.

(责任编辑: 刘嘉文)