DOI: 10.3969/j.issn.1007-5461.2024.01.013

一种基于GHZ态的半量子双方身份认证协议

李 想[1,2,3]， 张可佳[1,2,3*]

(1 黑龙江大学数学科学学院， 黑龙江 哈尔滨 150080;
2 黑龙江省复杂系统理论与计算重点实验室， 黑龙江 哈尔滨 150080;
3 黑龙江大学密码与网络安全研究院， 黑龙江 哈尔滨 150080)

摘 要: 半量子身份认证在保障通讯安全方面发挥着至关重要的作用。通过引入一个量子第三方对密钥进行集中管理, 提出一种新的基于Greenberger-Home-Zeilinger (GHZ) 态的半量子双方身份认证协议。首先, 对参与者的量子能力进行限制, 两个认证者都只具有半量子的能力, 协议使用更少的量子资源。其次, 协议中两个半量子参与者只需要执行简单的测量操作和异或操作。安全性分析发现, 利用该协议进行量子通信时，假冒攻击、截获重发攻击和纠缠附加攻击等攻击都无法引起合法身份信息的泄露, 表明该协议可以有效防止非法的不诚实参与者获得合法身份, 具有较好的安全性和实用性。

关 键 词: 量子通信; 半量子认证; 身份认证; 双方认证; GHZ态

中 图 分 类 号 : O431.2 **文 献 标 识 码 :** A **文章编号:** 1007-5461(2024)01-00135-08

A semi-quantum mutual identity authentication protocol based on GHZ state

LI Xiang[1,2,3], *ZHANG Kejia*[1,2,3*]

(1 School of Mathematical Sciences, Heilongjiang University, Harbin 150080, China;
2 Heilongjiang Provincial Key Laboratory of the Theory and Computation of Complex Systems, Harbin 150080, China;
3 Institute for Cryptology & Network Security, Heilongjiang University, Harbin 150080, China)

Abstract: Semi-quantum identity authentication plays a crucial role in ensuring communication security. By introducing a quantum third party to centrally manage keys, a new semi-quantum two-party authentication protocol based on Greenberger-Home-Zeilinger (GHZ) state is proposed. Firstly, the quantum capabilities of the participants are limited, both authenticators have only semi-quantum capabilities, and the protocol uses fewer quantum resources. Secondly, the two semi-quantum participants in the protocol only need to perform simple measurement operations and XOR operations. Through further security analysis, it is found that attacks such as impersonation attack, intercept-resend attack and entangle-measure attack cannot cause the leakage of legitimate identity information when using this

基金项目: 国家自然科学基金 (61802118, 62271234), 黑龙江省自然科学基金 (YQ2020F013), 黑龙江省高校基本科研业务费项目
作者简介: 李 想 (1998 -), 女, 山东平阴人, 研究生, 主要从事量子密码协议方面的设计与分析。E-mail: 2190985@s.hlju.edu.cn
导师简介: 张可佳 (1987 -), 黑龙江大庆人, 博士, 教授, 硕士生导师, 主要从事量子密码、量子计算方面的研究。E-mail: zhangkejia@hlju.edu.cn
收稿日期: 2022-04-28; **修改日期:** 2022-06-20
*通信作者。

protocol for quantum communication, indicating that the protocol can effectively prevent an illegal and dishonest participant from obtaining a legitimate identity, and has better security and practicality.

Key words: quantum communication; semi-quantum authentication; identity authentication; mutual authentication; GHZ state

0 引 言

随着通讯信息化和互联网技术的日益进步, 全球已进入大数据时代。人们在生活起居和交通出行等各方面都离不开计算机网络。但是, 在享受着信息化便利的同时, 随之而来的私人信息泄露、非法数据传输等各类安全问题也频繁出现, 所以如何保护信息安全受到各界人士的广泛关注。在此背景下, 作为一个多领域交叉学科, 密码学发挥了不可替代的作用。算力的迅速增强使基于计算数学复杂度的经典密码学存在不安全隐患, 而量子密码学的安全性由海森堡不确定性原理、量子相干性等量子力学原理保证, 比其他密码系统具有更高的安全性优势。

作为量子密码学的分支, 量子身份认证是基于量子物理特性而实现的, 可以有效抵抗量子计算的攻击。量子身份认证是双方进行安全通信的前提, 是网络安全的第一道防线。1999 年, Dušek 等[1]通过将量子密钥分发和经典识别过程相结合, 首次设计了一个安全的身份认证系统; 2000 年, Zeng 等[2]提出了一种量子密钥分发协议, 在完成量子密钥分发的同时进行量子身份认证; 2002 年, Mihara 等[3]提出了三种具体的量子认证方案, 通过使用纠缠态和引入可信仲裁完成了两次量子认证, 并将量子密码系统与普通认证相结合, 提出了一种量子消息认证方案。近年来, 关于量子身份认证的研究主要从降低实现条件方面展开[4−9], 研究人员相继提出了经典第三方[4]、无可信第三方[5]和无需纠缠[6, 7]的量子身份认证方案。

然而, 现有大多数量子身份认证协议的前提条件是所有通信者都具有完整量子能力, 这在现实生活中是不现实的。为了解决量子硬件成本昂贵及量子设备携带不便等问题, 2007 年, Boyer 等[8]首先提出了经典参与方的 BB84 类量子密钥分配协议, 随后提出了半量子密钥分发 (SQKD) 协议设计思想[9]。半量子概念的提出进一步推动了密码学的实用性进程, 近些年有关半量子通信的协议层出不穷。除了 SQKD[10−12]以外, 半量子安全直接通信(SQSDC)[13, 14]和半量子秘密共享 (SQSS)[15−17]等研究方向也被相继提出。2019 年, Zhou 等[18]通过结合半量子思想和经典身份认证, 首次提出了两种单光子半量子身份认证协议, 该协议可以抵抗中间人攻击。在 Zhou 等的第一个协议中, 经典用户可以在没有认证的经典信道下验证量子用户的身份; 在他们的第二个协议中, 量子用户可以在没有经典测量能力的情况下验证经典用户的身份。同年, Wen 等[19]提出了一种基于类 GHZ 态和 W 态的半量子消息和身份认证协议, 该协议实现了经典用户和量子用户之间的相互身份认证。此外, 消息认证阶段还可以作为一个独立的消息认证协议来使用。2021 年, Jiang 等[20]提出了一种基于 Bell 态的两方同时身份认证协议, 该协议只需要执行单量子测量和 XOR 操作即可完成身份验证, 并不需要第三方或复杂的操作, 且该协议针对四种常见的攻击是安全的。

在上述相关的量子通信协议基础上, 本文提出了一种新的基于 GHZ 态的半量子双方同时身份认证协议。在协议中, 第三方在量子认证通信过程中需要制备量子资源并且进行密钥的管理和分发, 参与者根据自己的密钥对量子态进行操作从而完成认证。另外, 本文介绍了协议中用到的一些基础知识, 包括半量子身份认证协议应该满足的一些基本条件和协议的流程, 并分析了协议的安全性。

1　预备知识

1.1　GHZ纠缠态

在所提出的半量子双方认证协议中, 三粒子GHZ态是量子通信中常用的纠缠资源。量子第三方Trent随机生成N个8种GHZ态, 其形式为

$$\begin{cases} |\psi_1\rangle_{\mathrm{ABT}}=\dfrac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right)_{\mathrm{ABT}},\ |\psi_2\rangle_{\mathrm{ABT}}=\dfrac{1}{\sqrt{2}}\left(|000\rangle-|111\rangle\right)_{\mathrm{ABT}} \\ |\psi_3\rangle_{\mathrm{ABT}}=\dfrac{1}{\sqrt{2}}\left(|100\rangle+|011\rangle\right)_{\mathrm{ABT}},\ |\psi_4\rangle_{\mathrm{ABT}}=\dfrac{1}{\sqrt{2}}\left(|100\rangle-|011\rangle\right)_{\mathrm{ABT}} \\ |\psi_5\rangle_{\mathrm{ABT}}=\dfrac{1}{\sqrt{2}}\left(|010\rangle+|101\rangle\right)_{\mathrm{ABT}},\ |\psi_6\rangle_{\mathrm{ABT}}=\dfrac{1}{\sqrt{2}}\left(|010\rangle-|101\rangle\right)_{\mathrm{ABT}} \\ |\psi_7\rangle_{\mathrm{ABT}}=\dfrac{1}{\sqrt{2}}\left(|110\rangle+|001\rangle\right)_{\mathrm{ABT}},\ |\psi_8\rangle_{\mathrm{ABT}}=\dfrac{1}{\sqrt{2}}\left(|110\rangle-|001\rangle\right)_{\mathrm{ABT}} \end{cases}. \tag{1}$$

1.2　半量子定义

本研究所提出的半量子身份认证协议中有三类参与者: Trent、Alice、Bob。其中Trent是具有完整量子能力的参与者, 他可以准备量子资源并对其进行相应的量子操作, 即测量和存储不同基下的量子比特。而用户 Alice和Bob则被限制仅能执行以下四种特定的 "半量子" 操作[9]: 1) 测量: 在计算基 Z 基上测量并重发量子比特; 2) 制备: 在$\{|0\rangle, |1\rangle\}$基中制备一个新的量子比特; 3) 反射: 将从Trent收到的量子比特不受任何干扰地返回给他; 4) 重新排序: 对接收到的量子序列进行重新排序, 并使用延迟线圈暂时存储量子比特。

2　半量子双方身份认证协议

本节将介绍半量子双方同时身份认证协议的具体细节。Alice和Bob作为通信中的合法参与者, 在诚实第三方Trent的帮助下完成认证流程。半量子身份认证过程如图1所示, 协议包括注册和认证两个部分。

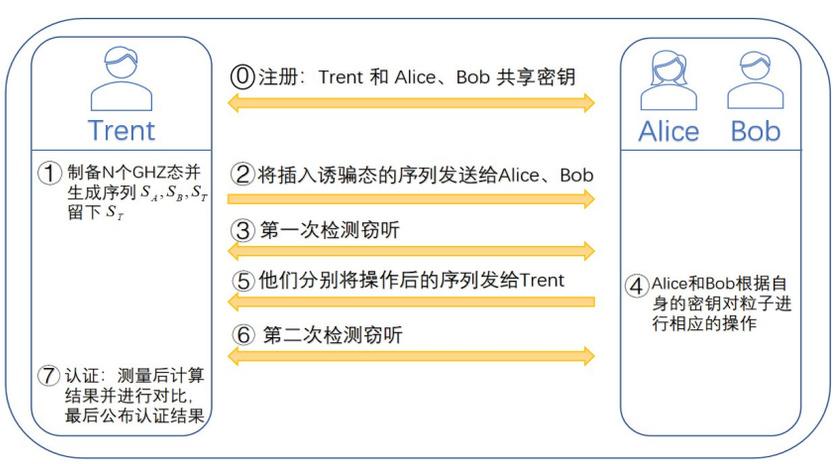

图1　半量子双方认证协议流程

Fig. 1　Process of semi-quantum mutual authentication protocol

2.1　注册

在身份认证流程开始之前, 为了使Alice和Bob成为拥有合法身份的用户, Alice和Bob需要在第三方Trent注册身份。具体地, Alice和Bob需要分别与Trent共享一个秘密的身份标识串K_{AT}和K_{BT}, 形式为

$$\begin{cases} K_{\mathrm{AT}}=\left\{K_{\mathrm{A}_1},K_{\mathrm{A}_2},\cdots,K_{\mathrm{A}_N}\right\} \\ K_{\mathrm{BT}}=\left\{K_{\mathrm{B}_1},K_{\mathrm{B}_2},\cdots,K_{\mathrm{B}_N}\right\} \end{cases}, \tag{2}$$

其中K_{A_i}, $K_{\mathrm{B}_i}\in\{0,1\}$, $i=1,2,\cdots,N$。

2.2 认证

2.2.1 准备

首先, Trent随机生成一个N个GHZ态序列的量子系统, 形式为

$$\begin{cases} \left|\Psi_1\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|S_{\mathrm{A}_{11}}S_{\mathrm{B}_{21}}S_{\mathrm{T}_{31}}\right\rangle+\left|(S_{\mathrm{A}_{11}}\oplus1)(S_{\mathrm{B}_{21}}\oplus1)(S_{\mathrm{T}_{31}}\oplus1)\right\rangle\right)_{\mathrm{A}_1\mathrm{B}_1\mathrm{T}_1} \\ \left|\Psi_2\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|S_{\mathrm{A}_{12}}S_{\mathrm{B}_{22}}S_{\mathrm{T}_{32}}\right\rangle+\left|(S_{\mathrm{A}_{12}}\oplus1)(S_{\mathrm{B}_{22}}\oplus1)(S_{\mathrm{T}_{32}}\oplus1)\right\rangle\right)_{\mathrm{A}_2\mathrm{B}_2\mathrm{T}_2} \\ \vdots \\ \left|\Psi_N\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|S_{\mathrm{A}_{1N}}S_{\mathrm{B}_{2N}}S_{\mathrm{T}_{3N}}\right\rangle+\left|(S_{\mathrm{A}_{1N}}\oplus1)(S_{\mathrm{B}_{2N}}\oplus1)(S_{\mathrm{T}_{3N}}\oplus1)\right\rangle\right)_{\mathrm{A}_N\mathrm{B}_N\mathrm{T}_N} \end{cases}, \tag{3}$$

式中下标$\mathrm{A}_i\mathrm{B}_i\mathrm{T}_i(i=1,2,\cdots,N)$表示第$i$个量子态。Trent将这些GHZ态分成三个序列$S_{\mathrm{A}}$、$S_{\mathrm{B}}$、$S_{\mathrm{T}}$, 并从$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$中随机选择生成$4N$个诱骗态, 分别将$2N$个诱骗态各自插入到序列$S_{\mathrm{A}}$和$S_{\mathrm{B}}$中, 则序列$S_{\mathrm{A}}$变为$S'_{\mathrm{A}}$, 序列$S_{\mathrm{B}}$变为$S'_{\mathrm{B}}$。随后Trent记录下所有诱骗态的初始位置并保留$S_{\mathrm{T}}$在自己手中, 将序列$S'_{\mathrm{A}}$发送给Alice, 将序列$S'_{\mathrm{B}}$发送给Bob。

2.2.2 第一次窃听检测

Trent确认Alice和Bob已经收到S'_{A}和S'_{B}序列后, 分别宣布各自序列中$2N$个诱骗态中的初始位置。而后, Alice和Bob使用量子延迟线圈储存S'_{A}和S'_{B}序列, 他们将序列中的前N个诱骗态随机执行以下操作: 1) 将收到的诱骗态不受任何干扰地返回给Trent; 2) 用Z基测量诱骗态并且制备与测量结果相同的态, 然后传输新的量子态给Trent。

一旦确认Trent收到了诱骗态, Alice和Bob将分别公布对应的N个诱骗态序列的位置、测量结果和操作。然后Trent对不同类型的诱骗态执行不同的窃听检测策略: 对于直接反射回来的粒子, Trent用初始的测量基来测量并得到测量结果R, 并将R与其初始态的测量结果进行比较; 对于被测量的粒子, Trent用Z基测量粒子并检查结果是否与公开的测量结果一致。最后, Trent计算总错误率。如果这些粒子的总错误率在可以接受的阈值内, 协议继续;否则, 他们将放弃继续进行身份验证。

2.2.3 测量和操作

Alice和Bob分别将序列S'_{A}和S'_{B}恢复为序列S''_{A}和S''_{B}, 且他们用Z基测量非诱骗态粒子并将结果记为R_{A}和R_{B}。然后Alice和Bob通过秘密身份密钥K_{AT}和K_{BT}执行以下操作: 如果身份认证密钥的比特值是0, Alice和Bob将制备与测量结果相同的量子态;如果身份认证密钥的比特值是1, Alice和Bob将制备与测量结果相反的量子态。相应的转换规则如表1所示。通过第一次窃听检测后, 序列S''_{A}和S''_{B}中仍有N个诱骗态。Alice和Bob对剩余的N个诱骗态执行与2.2.2相同的窃听检测操作, 并将新的序列S'''_{A}和S'''_{B}发送给Trent。

表1 测量结果的转换规则

Table 1 Conversion rules of measurement result

身份认证密钥比特	测量结果→转换结果
0	$\|0\rangle \to \|0\rangle$
	$\|1\rangle \to \|1\rangle$
1	$\|0\rangle \to \|1\rangle$
	$\|1\rangle \to \|0\rangle$

2.2.4 第二次窃听检测

与第一次窃听检测作用相同, 第二次窃听检测也是为了保证协议的安全性, 防止量子态在传输过程中被非法窃听。首先, Alice 和 Bob 确认 Trent 已经收到序列 S_{A}''' 和 S_{B}''' 后, 宣布 N 个诱骗态的位置、测量结果和操作; 类似地 Trent 计算错误率, 如果错误率超过安全阈值, 协议即刻终止, 否则认证协议继续进行。

2.2.5 认证

在通过第二次窃听检测后, Trent 保留余下的量子态并生成 $\bar{S}_{\mathrm{A}}$ 和 $\bar{S}_{\mathrm{B}}$ 序列, 随后在 $\bar{S}_{\mathrm{A}}$、$\bar{S}_{\mathrm{B}}$ 和 S_{T} 序列的相应位置上执行Z基测量。Trent 通过表2的转换规则将测量结果转换为经典结果 $\bar{R}_{\mathrm{A}}$、$\bar{R}_{\mathrm{B}}$ 和 R_{T}, 表示为

$$\begin{cases} \bar{R}_{\mathrm{A}} = \left[R_{\mathrm{A}_1}, R_{\mathrm{A}_2}, \cdots, R_{\mathrm{A}_N} \right] \\ \bar{R}_{\mathrm{B}} = \left[R_{\mathrm{B}_1}, R_{\mathrm{B}_2}, \cdots, R_{\mathrm{B}_N} \right] \\ R_{\mathrm{T}} = \left[R_{\mathrm{T}_1}, R_{\mathrm{T}_2}, \cdots, R_{\mathrm{T}_N} \right] \end{cases}. \tag{4}$$

表2 测量结果的转换方式

Table 2 Conversion rules of measurement results

测量结果	经典结果
$\|0\rangle$	0
$\|1\rangle$	1

Trent 计算 $Q_{\mathrm{A}_j} = R_{\mathrm{A}_j} \oplus S_{\mathrm{A}_{1j}}$ 和 $Q_{\mathrm{B}_j} = R_{\mathrm{B}_j} \oplus S_{\mathrm{B}_{2j}} \left(j = 1, 2, \cdots, N \right)$, 其中 $\oplus$ 为异或操作。如果 $Q_{\mathrm{A}_j} = Q'_{\mathrm{A}_j}$ 且 $Q_{\mathrm{B}_j} = Q'_{\mathrm{B}_j}$, 则 Alice 和 Bob 相互身份认证成功, 两人都是具有合法身份的参与者;否则, 协议中有非法通信者存在。最后, Trent 向 Alice 和 Bob 公布认证是否成功。

3 安全性分析

在量子信号的传输过程中, Eve 是一个具有量子能力的窃听者, 他希望通过攻击协议来非法获取秘密信息, 从而实现身份认证。

3.1 假冒攻击

本研究提出的双方身份认证协议中, 第三方 Trent 是资源提供者, 而 Alice 和 Bob 是被认证的用户。

一方面, Eve 想假冒 Trent 来获取秘密信息。Eve 可以忠实地遵循协议步骤, 但他试图提取密钥。首先, Eve 会随机生成量子纠缠态并将纠缠粒子分配给 Alice 和 Bob。2.2.4 节中, Trent 收到 Alice 和 Bob 根据密钥操作后的粒子后, 由于他不知道 Trent 插入的 N 个诱骗态具体是什么, 所以他会随机执行基于Z基和X基的测量。这些测量基有四个测量结果 $\left\{ |0\rangle, |1\rangle, |+\rangle, |-\rangle \right\}$。此外, 在 $2N$ 序列中仅选择正确的 N 位置的概率很低, 所以他失败的概率是 $P_1 = 1 - \frac{1}{2} \times \frac{1}{4^N} = 1 - \frac{1}{8^N}$。由图2(a)可知 Eve 攻击失败的概率 P_1 趋于 1。

另一方面, 假设Eve通过假冒Alice或Bob进行假冒攻击。当Eve进行到步骤2.2.3时, 由于不知道预共享密钥K_{AT}、K_{BT}, 他只能对量子比特随机执行表1中的操作, 选择正确操作或错误操作的概率为$\frac{1}{2}$, 同时Eve得到正确转换结果的概率为$\frac{1}{2^N}$。由图2(b)可知Eve攻击失败的概率$P_2=1-\frac{1}{2}\times\frac{1}{2^N}$趋于1。因此, 该协议可以有效抵抗假冒攻击。

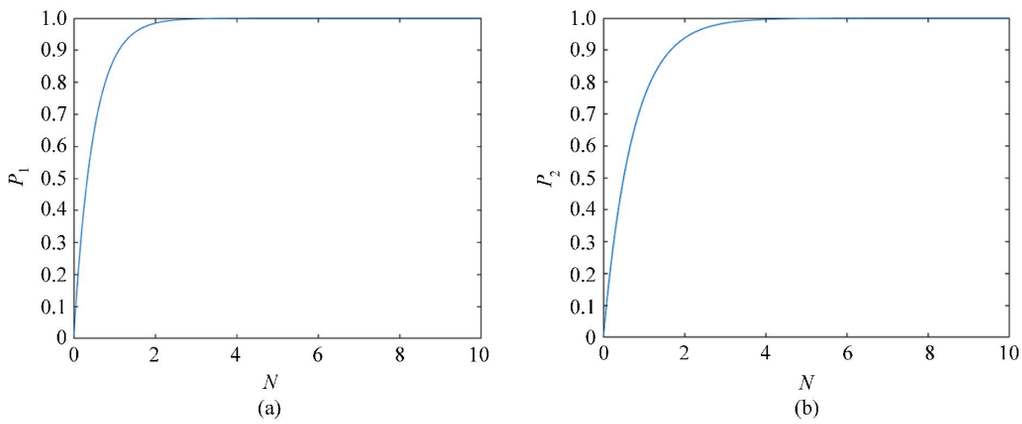

图2 Eve被检测出的概率 (a) P_1 及 (b) P_2

Fig. 2 (a) Probability P_1 and (b) P_2 of Eve being detected

3.2 截获重发攻击

实际上, Eve作为外部攻击者只能从第三方Trent那里获得Alice和Bob的秘密身份。首先, 他无法通过访问Trent获得任何有关Alice和Bob身份的相关信息, 因为第三方对此协议绝对诚实。此外, 他也无法通过截获重发攻击获得Alice和Bob的真实身份。

在2.2.1节中, Trent在序列S_A和S_B中分别插入$2N$个诱骗态, 用于两次窃听检测。然而, 由于Eve并不知道Trent发送给Alice和Bob的序列中诱骗态的初始位置和初始状态, 因此即便Eve是量子参与者, 能够在Z基和X基上执行测量操作, 他也无法确定具体的量子态;也很难在$3N$长的量子序列中仅选择正确的N位置。此时, 他成功获取正确信息的概率是$\frac{1}{3}\times\frac{1}{4^N}=\frac{1}{12^N}$。如图3所示, 当$N$足够大时, 概率$P_3=1-\frac{1}{12^N}$近似为1。因此, 检测不到Eve的非法行为的几率很小。

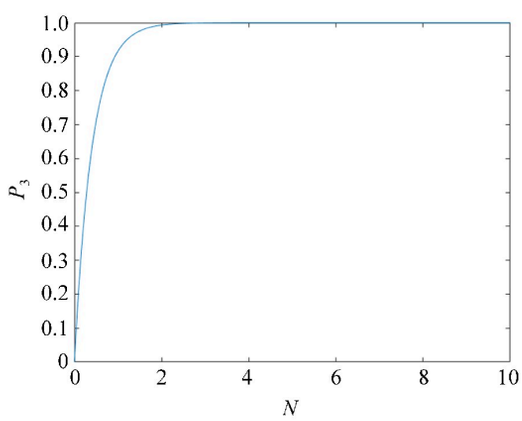

图3 Eve被检测出的概率P_3

Fig. 3 Probability P_3 of Eve being detected

3.3 纠缠附加攻击

本节讨论一些非法用户在信息交互过程中是否可以通过纠缠附加攻击获得秘密信息。当量子序列从Trent发送到Alice和Bob时, 假设Eve对于诱骗态和辅助态组成的系统执行U_{E}操作, 那么可以得到

$$\begin{cases} U_{\mathrm{E}}|0\rangle|e\rangle = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle \\ U_{\mathrm{E}}|1\rangle|e\rangle = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle \end{cases}, \tag{5}$$

$$\begin{aligned} &U_{\mathrm{E}}|+\rangle|e\rangle = \frac{1}{\sqrt{2}}\Big[|0\rangle\Big(a|e_{00}\rangle + c|e_{10}\rangle\Big) + |1\rangle\Big(b|e_{01}\rangle + d|e_{11}\rangle\Big)\Big] = \\ &\frac{1}{2}\Big[|+\rangle\Big(a|e_{00}\rangle + b|e_{01}\rangle + c|e_{10}\rangle + d|e_{11}\rangle\Big) + |-\rangle\Big(a|e_{00}\rangle - b|e_{01}\rangle + c|e_{10}\rangle - d|e_{11}\rangle\Big)\Big], \end{aligned} \tag{6}$$

$$\begin{aligned} &U_{\mathrm{E}}|-\rangle|e\rangle = \frac{1}{\sqrt{2}}\Big[|0\rangle\Big(a|e_{00}\rangle - c|e_{10}\rangle\Big) + |1\rangle\Big(b|e_{01}\rangle - d|e_{11}\rangle\Big)\Big] = \\ &\frac{1}{2}\Big[|+\rangle\Big(a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle\Big) + |-\rangle\Big(a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle\Big)\Big], \end{aligned} \tag{7}$$

式中$|e_{00}\rangle$、$|e_{01}\rangle$、$|e_{10}\rangle$、$|e_{11}\rangle$属于Eve的辅助粒子所在的空间, 且$|a|^2+|b|^2+|c|^2+|d|^2=1$。然后Eve让量子序列继续参与协议流程, 并试图通过测量辅助量子态来获取Alice和Bob的操作信息。为了在不引入任何错误的情况下通过窃听检测, 她执行的操作会准确区分辅助态, 那么则有

$$\begin{cases} b=c=0 \\ a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle = 0 \\ a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle = 0 \end{cases}. \tag{8}$$

然而$b=c=0$, 意味着$a|e_{00}\rangle = d|e_{11}\rangle$。由此可见, 如果Eve能够逃避窃听检测, 那么他就无法区分辅助态。因此, 所提出协议可以抵抗纠缠附加攻击。

此外, 类似特洛伊木马等攻击方式, Alice和Bob只需要放置波长滤波器和光子数分离器就可避免, 因此本协议并没有特别提及。

4 结　论

提出了一个基于GHZ态的半量子双方同时身份认证协议, 包括一个量子方和两个半量子方。在量子第三方的帮助下, 半量子双方可以完成同时身份认证。安全性分析表明, 该协议可以有效地防止非法参与者或攻击者获取合法身份信息。

参考文献:

[1] Dušek M, Haderka O, Hendrych M, *et al*. Quantum identification system [J]. *Physical Review A*, 1999, 60(1): 149-156.

[2] Zeng G H, Zhang W P. Identity verification in quantum key distribution [J]. *Physical Review A*, 2000, 61(2): 022303.

[3] Mihara T. Quantum identification schemes with entanglements [J]. *Physical Review A*, 2002, 65(5): 052326.

[4] Li X, Zhang K J, Zhang L, *et al*. A new quantum multiparty simultaneous identity authentication protocol with the classical third-party [J]. *Entropy*, 2022, 24(4): 483.

[5] Kang M S, Heo J, Hong C H, *et al*. Controlled mutual quantum entity authentication with an untrusted third party [J]. *Quantum Information Processing*, 2018, 17(7): 159.

[6] Zawadzki P. Quantum identity authentication without entanglement [J]. *Quantum Information Processing*, 2019, 18(1): 7.

[7] Zhu H F, Wang L W, Zhang Y L. An efficient quantum identity authentication key agreement protocol without entanglement [J]. *Quantum Information Processing*, 2020, 19(10): 381.

[8] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob [J]. *Physical Review Letters*, 2007, 99(14): 140501.

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

[10] Zou X F, Qiu D W, Li L Z, *et al*. Semiquantum-key distribution using less than four quantum states [J]. *Physical Review A*, 2009, 79(5): 052312.

[11] Krawec W O. Restricted attacks on semi-quantum key distribution protocols [J]. *Quantum Information Processing*, 2014, 13 (11): 2417-2436.

[12] Zhou N R, Zhu K N, Zou X F. Multi-party semi-quantum key distribution protocol with four-particle cluster states [J]. *Annalen Der Physik*, 2019, 531(8): 1800520.

[13] Yang C W. Efficient and secure semi-quantum secure direct communication protocol against double CNOT attack [J]. *Quantum Information Processing*, 2019, 19(2): 50.

[14] Gu J, Lin P H, Hwang T. Double C-NOT attack and counterattack on 'Three-step semi-quantum secure direct communication protocol' [J]. *Quantum Information Processing*, 2018, 17(7): 182.

[15] Li Q, Chan W H, Long D Y. Semi-quantum secret sharing using entangled states [J]. *Physical Review A*, 2010, 82(2): 022303.

[16] Tsai C W, Chang Y C, Lai Y H, *et al*. Cryptanalysis of limited resource semi-quantum secret sharing [J]. *Quantum Information Processing*, 2020, 19(8): 224.

[17] Xie C, Li L Z, Qiu D W. A novel semi-quantum secret sharing scheme of specific bits [J]. *International Journal of Theoretical Physics*, 2015, 54(10): 3819-3824.

[18] Zhou N R, Zhu K N, Bi W, *et al*. Semi-quantum identification [J]. *Quantum Information Processing*, 2019, 18(6): 1-17.

[19] Wen X J, Zhao X Q, Gong L H, *et al*. A semi-quantum authentication protocol for message and identity [J]. *Laser Physics Letters*, 2019, 16(7): 075206.

[20] Jiang S Q, Zhou R G, Hu W W. Semi-quantum mutual identity authentication using Bell states [J]. *International Journal of Theoretical Physics*, 2021, 60(9): 3353-3362.