第 43 卷 第 5 期/2023 年 3 月/光学学报 研究论文

光学学报

基于量子行走的电子支付协议

何业锋，杨梦玫*，李智，刘妍，田哲铭

西安邮电大学网络空间安全学院，陕西 西安 710121

摘要 目前，量子行走已广泛应用于量子计算和量子模拟中，并可应用于量子隐形传态中。提出了一种基于量子行走的电子支付协议。在协议中，买家基于可信第三方平台，将部分购物信息通过量子行走传送给银行和商家，完成一次网络购物。此协议将量子行走与电子支付相结合，使参与方仅需制备单光子便可以得到所需的纠缠资源，便于量子态的制备和实现。同时，协议不仅满足购物清单对银行保密，还实现了购买者的部分私人信息对商家保密，提高了隐私保护能力。最后的安全性分析表明，该协议可以抵御内部和外部攻击，对于当前技术是安全可行的。

关键词 量子光学；量子密码；量子行走；电子支付；隐形传态；单粒子

中图分类号 TN918 **文献标志码** A **DOI**：10.3788/AOS221642

1 引 言

随着电子商务和计算机的发展，网络购物越来越方便，越来越多的人开始通过网络平台进行购物。1983年，Chaum[1]提出电子现金的概念，随后人们提出了许多基于签名技术的电子支付协议。然而，随着量子算法的发展，基于数学困难问题所提出的经典电子支付协议越来越不安全，为抵御量子算法的攻击，人们开始研究量子电子支付协议。2010年，Wen等[2]率先提出了一种基于量子签名技术的电子支付协议，此协议在利用量子特性保证无条件安全性的同时，还通过量子盲签名和量子群签名技术来保证参与者和协议内部结构的匿名性。2013年，为便于银行间支付，Wen等[3]将量子代理盲签名技术应用于电子支付协议。2014年人们提出基于量子盲签名的离线电子支付方案[4]，并将可控量子隐形传态技术与电子支付相结合[5]。此外，人们还陆续提出了基于量子多重代理盲签名[6-8]、量子稠密编码[9]等技术的电子支付协议。2019年，Zhang等[10]提出了一种基于区块链和量子签名的电子支付协议，其通过量子代理盲签名技术保护电子支付系统的匿名性，并通过区块链技术防止卖家的不诚实行为。此后，Gou等[11]对Zhang等的协议进行改进，降低了量子资源的复杂性。但是，以上方案多为利用量子纠缠态进行操作，制备和测量相对复杂。2020年，Jiang等[12]提出了一种基于局域不可区分正交直积(X-LIOP)态的可信第三方电子支付协议，此协议通过制备比纠缠态更易产生的乘积态粒子，提高了协议的有效性。次年，Lin等[13]对Jiang等的协议进行改进，通过修改协议模型，降低了其对第三方平台的依赖性，并将4粒子X-LIOP态改为3粒子X-LIOP态，降低了量子资源的复杂性，使协议更易实现。除签名技术，人们还提出了基于量子通信的电子支付协议[14-17]。

量子行走(QW)源于对量子扩散现象的研究，其概念最早由Aharonov等[18]在1993年提出。近年来，QW被证明是量子信息处理任务中一种很有前途的资源，被广泛地应用在搜索算法[19-20]、隐形传态[21-26]等技术中。基于QW的量子隐形传态技术无需提前制备纠缠态资源，单光子便可以通过QW自发产生必要的纠缠资源，这可以降低制备和测量粒子资源的难度，消除复杂的量子操作，提高协议的有效性。依据QW隐形传态的思想，人们陆续提出了一些基于QW的量子签名技术[22-25]、量子秘密共享方案[26]等，扩展了QW的应用领域。

本文将QW与量子电子支付相结合，提出了一个新的量子电子支付协议。新协议的参与方只需要制备单光子序列便可以通过QW隐形传态得到所需的纠缠资源，与其他电子支付协议相比，量子资源的制备和测量更加简单，同时改变了传统量子电子支付协议中只针对银行进行信息保密的情况，将购买者的部分私人信息如真实姓名、银行账户、电话等信息对商家进行保密，以提升协议的匿名性。

2 基础知识

2.1 一维量子行走

QW是以量子作为载体对经典随机行走进行的模

收稿日期：2022-08-25；**修回日期**：2022-09-26；**录用日期**：2022-10-14；**网络首发日期**：2022-10-24

基金项目：国家自然科学基金(61802302)、陕西省自然科学基础研究计划(2021JM-462)

通信作者：*meng_mei1999@outlook.com

拟，它根据量子的特性来模拟混沌非线性的动态行走行为，从而建立加密的量子传输信道。

量子行走空间是包含位置空间和硬币空间两个主要量子空间的复合 Hilbert 空间，可以表示为 $H=H_P\otimes H_C$，其中，H_P 为位置空间，H_C 为硬币空间，行走的位置跨度为 $\{|n\rangle:n\in\mathbf{Z}\}$，行走的硬币方向为 $\{|0\rangle,|1\rangle\}$。QW 的每一步都可以描述为 $W^{(l)}=E^{(l)}(I\otimes C)$，$E^{(l)}=S\otimes|0\rangle\langle 0|+S^{+}\otimes|1\rangle\langle 1|$，其中：$S$ 为移位算子，表示粒子向前（后）移动 1 位或若干位；C 为硬币算子。当量子行走光子当前所处于的状态为 $|0\rangle$ 态时，硬币粒子从 $|n\rangle$ 态前进到 $|n+1\rangle$ 态；而当量子行走光子当前所处于的状态为 $|1\rangle$ 态时，硬币粒子从 $|n\rangle$ 态后退到 $|n-1\rangle$ 态。

2.2　基于量子行走的量子隐形传态

通过两步量子行走，移位算子可以使位置空间和硬币空间相互纠缠，这种纠缠可用于构建量子信道和进行量子隐形传态。

假设 Alice 想要发送量子态 $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$ 给 Bob，其中 $|\alpha|^2+|\beta|^2=1$。为完成传送，Alice 制备粒子 A_P、A_1 和 B，其中：A_P 为位置空间的状态，初始态为 $|0\rangle$；A_1 表示 coin1，包含要发送的量子态 $|\varphi\rangle$；B 表示 coin2，初始态为 $|0\rangle$。

此时，通过两步行走即可完成信息传输任务。第一步量子行走为 $W^{(1)}=E^{(1)}(I_P\otimes C_1\otimes I_2)$，其中，$E^{(1)}=S\otimes|0\rangle_1\langle 0|\otimes I_2+S^{+}\otimes|1\rangle_1\langle 1|\otimes I_2$，$C_1$ 为 A_1（coin1）上的硬币操作，其对应的操作符为身份操作（恒等操作），S^{+} 为移位算符 S 的伴随算符。第二步量子行走为 $W^{(2)}=E^{(2)}(I_P\otimes I_1\otimes H)$，其中，$E^{(2)}=S\otimes I_1\otimes|0\rangle_2\langle 0|+S^{+}\otimes I_1\otimes|1\rangle_2\langle 1|$，$H$ 为 B（coin2）上的 Hadamard 操作，即 $H|0\rangle=|+\rangle$，$H|1\rangle=|-\rangle$，$H|+\rangle=|0\rangle$，$H|-\rangle=|1\rangle$。

经过两步量子行走后，Alice 将粒子 B 发送给 Bob。然后，Alice 使用 X 基 $\left(X=\{|+\rangle,|-\rangle\}\right)$ 测量粒子 A_1，对测量结果按照如表 1 所示的方法进行编码，将编码结果记为 λ_1；Alice 再使用 Q 基 $\left(Q=\{|-2'\rangle,|-1\rangle,|0\rangle,|1\rangle,|2'\rangle\}\right.$ $\left.\text{其中}|-2'\rangle=\frac{1}{\sqrt{2}}(|-2\rangle-|2\rangle,|2'\rangle=\frac{1}{\sqrt{2}}(|-2\rangle+|2\rangle)\right]$ 测量粒子 A_P，结果记为 λ_2。然后 Alice 将 λ_1 和 λ_2 告诉 Bob，Bob 再对粒子 B 执行如表 2 所示的 Pauli 操作，得到 A_1 的量子态。

在量子行走系统中，一般的初始态为 $|\Phi\rangle^{(0)}=|0\rangle_P\otimes\left(\alpha|0\rangle+\beta|1\rangle\right)_1\otimes|0\rangle_2$，系统中所有粒子态均按照 A_P、A_1 和 B 的顺序书写，其具体演化过程可以参考文献[22-24]。经过演化算子 $W^{(1)}$ 后，系统的初始态 $|\Phi\rangle^{(0)}$ 演化为 $|\Phi\rangle^{(1)}=\left(a|100\rangle+b|-110\rangle\right)_{P12}$，此时粒子 A_P 和粒子 A_1 已经纠缠在一起，其复合态由 $\left(a|0\rangle+b|1\rangle\right)_1\otimes|0\rangle_P$ 变为 $\left(a|10\rangle+b|-11\rangle\right)_{P1}$。经过演化算子 $W^{(2)}$ 后，$|\Phi\rangle^{(1)}$ 演化为 $|\Phi\rangle^{(2)}=\left(a|200\rangle+a|001\rangle+b|010\rangle+b|-211\rangle\right)_{P12}/\sqrt{2}$，此时硬币空间的粒子 A_1 和 B 纠缠在一起，Alice 使用 X 基测量 A_1，根据量子力学原理，量子态 A_P 和 B 塌缩为 $|+\rangle_1\left(a|20\rangle+a|01\rangle+b|00\rangle+b|-21\rangle\right)_{P2}+|-\rangle_1\times\left(a|20\rangle+a|01\rangle-b|00\rangle-b|-21\rangle_{P2}\right)/\sqrt{2}$。第 2 步 QW 后，当 A_1 的测量结果是 $|+\rangle$ 时，A_P 和 B 的纠缠态为 $\left(a|20\rangle+a|01\rangle+b|00\rangle+b|-21\rangle\right)_{P2}$，最终得到的一般态为 $|2'\rangle_P\left(a|0\rangle+b|1\rangle\right)_2/2+|-2'\rangle_P\left(a|0\rangle-b|1\rangle\right)_2/2+|0\rangle_P\left(a|1\rangle+b|0\rangle\right)_2/\sqrt{2}$。当 A_1 的测量结果是 $|-\rangle$ 时，A_P 和 B 的纠缠态为 $\left(a|20\rangle+a|01\rangle-b|00\rangle-b|-21\rangle\right)_{P2}$，然后 Alice 测量 A_P，得到最终的一般态为 $|2'\rangle_P\left(a|0\rangle-b|1\rangle\right)_2/2+|-2'\rangle_P\left(a|0\rangle+b|1\rangle\right)_2/2+|0\rangle_P\left(a|1\rangle-b|0\rangle\right)_2/\sqrt{2}$。

表 1　Alice 测量结果编码

Table 1　Coding of Alice's measurement results

Q-basis	λ_2	X-basis	λ_1
$\|1\rangle$	1	$\|+\rangle$	1
$\|2'\rangle$	−1	$\|-\rangle$	−1
$\|0\rangle$	0		
$\|-1\rangle$	−1		
$\|-2'\rangle$	−1		

表 2　修正 Pauli 操作

Table 2　Revise Pauli operation

A_1	A_P	Revise operation
1(−1)	1(−1)	I
1(−1)	−1(1)	σ_z
1	0	σ_x
−1	0	$\sigma_z\sigma_x$

3　基于量子行走的电子支付协议

3.1　协议模型

本协议中主要包含 5 个参与方：买家 Alice、Alice 的开户银行 Bob1，卖家 Charlie，Charlie 的开户银行 Bob2，以及可信的第三方平台 Trent（购物软件或网站，如淘宝、京东等）。协议模型如图 1 所示：1）Alice 在平台上选购商品，生成购物信息，并将其告知 Trent；2）Trent 收到 Alice 的购物信息后，对其进行处理，并将购物金额部分发送给 Bob1；3）Alice 对所需要支付的购物金额进行确认；4）Bob1 将相应金额转给 Trent，由

Trent暂时保管；5）Trent收到转账后，告诉Charlie相关信息，但将买家的私人信息对Charlie保密；6）Charlie收到Trent的消息，确认Alice的订单内容无误后，发出其所购买商品；7）Alice收到商品并确认无误后，告诉Trent；8）Trent将先前Bob1转账金额转入Bob2中Charlie的账户，交易结束。

为方便描述，将协议的流程分为初始阶段、购买阶段、支付阶段和验证阶段4部分，整个协议的量子态传输过程如图2所示。

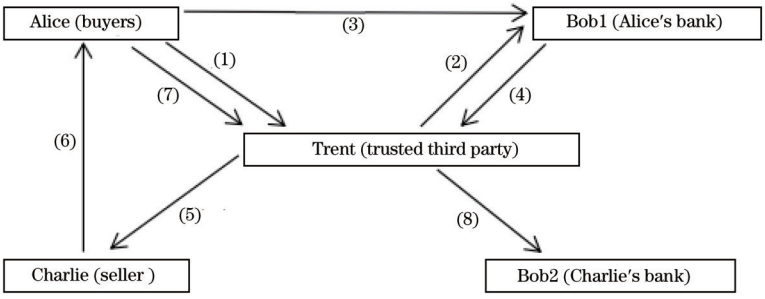

图1　协议模型

Fig. 1　Protocol model

3.2　初始阶段

初始阶段主要包括密钥分发、购买信息处理和购买信息的分发三部分内容。

3.2.1　密钥分发

Alice和Charlie首先在Trent处注册。各参与方之间用已有量子密钥分发（QKD）协议[27-30]实现双方之间的密钥共享。其中，Alice和Trent共享密钥K_{AT}，Alice和Bob1共享密钥K_{AB1}，Charlie和Trent共享密钥K_{CT}，Bob1和Trent共享密钥K_{TB1}。

3.2.2　购买信息处理及分发

Alice在Charlie处选购商品后，生成购物信息M，其中包括所购买商品的名称、金额、购买时间、买家信息等内容。然后将M分为购物金额M_1和其他内容M_2两部分。在电子支付协议中，M_2需要盲化。

1）Alice告诉Trent她所购买的商品。Alice使用密钥K_{AT}对M_1和M_2进行加密，得到$S_{AT}=E_{K_{AT}}(M_1,M_2)$，并将其发送给Trent。

2）Trent对Alice的购买信息进行处理。Trent使用密钥K_{AT}解密S_{AT}，得到M_1和M_2，再对M_2进行编码，得到$M_2'=|a_1b_1c_1\rangle|a_2b_2c_2\rangle\cdots|a_nb_nc_n\rangle$。其编码过程如下：Trent将Alice的个人信息编码成序列I，再将详细明目编码为等长序列II，其中I构成M_2的奇数位，II构成偶数位，得到$M_2=(m_1,m_2,\cdots,m_n)\left(m_i\in\{00,01,10,11\}\right)$。然后，Trent随机生成字符串$L=(L_1,L_2,\cdots,L_n)\left(L_i\in\{0,1\}\right)$，按照表3所示规则，对$M_2$进行编码。当$L_i=0$时，选$Z$基，令$a_i\oplus b_i=m_i^{(1)}$，$b_i\oplus c_i=m_i^{(2)}$；当$L_i=1$时，选$X$基，即：当$|a_i\rangle=|+\rangle$时，$a_i'=0$；$|a_i\rangle=|-\rangle$时，$a_i'=1$。$b_i$、$c_i$类似，令$a_i'\oplus b_i'=m_i^{(1)}$，$b_i'\oplus c_i'=m_i^{(2)}$。

当m_i为00时，$|a_ib_ic_i\rangle$满足$|a_i\rangle\oplus|b_i\rangle=0$且$|b_i\rangle\oplus|c_i\rangle=0$。当$L_i=0$时，可以被编码为$|000\rangle$或$|111\rangle$；当$L_i=1$时，$|a_ib_ic_i\rangle$为$|+++\rangle$或$|---\rangle$。

然后，Trent将所得的M_2'分成3个量子序列，即$A=|a_1,a_2,\cdots,a_n\rangle$、$B=|b_1,b_2,\cdots,b_n\rangle$和$C=|c_1,c_2,\cdots,c_n\rangle$。

最后，Trent将A发送给Alice，B发送给Bob1，C自己保留。

3.3　购买阶段

购买阶段主要包括Trent告诉Bob1购物金额和Alice确认付款金额两部分内容。

1）Trent将Alice的购买金额告诉Bob1。Trent使用密钥K_{TB1}对购物金额M_1进行加密，得到$S_{TB1}=E_{K_{TB1}}(M_1)$，并将其发送给Bob1。

2）Bob1收到S_{TB1}后，将其中付款金额告诉Alice。Alice确认无误后，通过QW量子隐形传态将量子序列A的量子态发送给Bob1，作为确认凭证，其传输过程如下：

（1）Alice生成单光子序列A_1和A_P，通过两步量子行走，使A、A_1和A_P相互纠缠。Alice再将行走后的A_P记为$\bar{A}_P$，并在其中随机地插入诱骗粒子串$t\left(t\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}\right)$用于窃听检测。将插入诱骗粒子后的量子序列记为$\bar{A}_P'$，并发送给Bob1。Alice确认Bob1收到$\bar{A}_P'$后，公开她在$\bar{A}_P'$中插入的诱骗粒子的位置和初始态等信息，Bob1对其进行测量并计算错误率，若错误率低于预先设定的阈值，则认为传输过程中无窃听，执行下一步；否则，立即终止协议。

（2）Alice用X基测量$|a_i\rangle$，用Q基测量$|A_{1i}\rangle$，分别得到λ_1和λ_2。Alice再使用密钥K_{AB1}对λ_1和λ_2进行加密，得到$S_{AB1}=E_{K_{AB1}}(\lambda_1,\lambda_2)$，并将其发送给Bob1。

3.4　支付阶段

支付阶段主要包括Bob1完成对Trent的转账，Trent验证Bob1的转账信息并暂时保管Bob1的转账，以及将此消息告诉Charlie并通知其发货三部分内容。

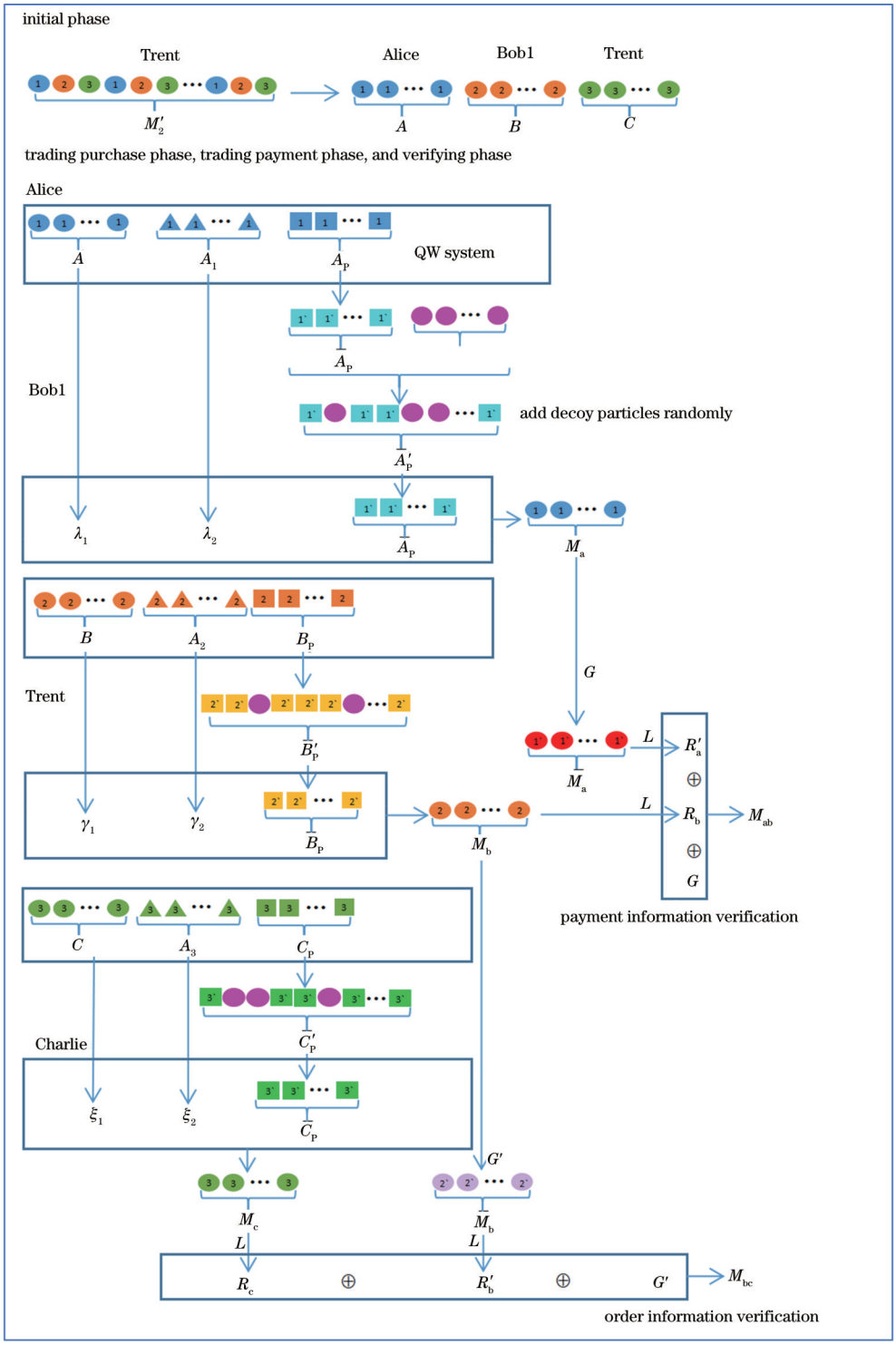

图 2　量子态传输原理图

Fig. 2　Schematic diagram of quantum-state transmission

3.4.1　Bob1 对 Trent 转账

Bob1 解密 S_{AB1}，得到 λ_1 和 λ_2，再根据 λ_1 和 λ_2 的值对 A_P 进行修正 Pauli 操作（表 2），使 $\bar{A}_P$ 的态序列与 A 的态序列相等，将操作后的序列记为 M_a。

1）Bob1 将 Alice 已确认交易金额的消息告知 Trent。首先，Bob1 生成随机字符串 $G\left[G=\left(g_1,g_2,\cdots,g_n\right),g_i\in\{0,1\}\right]$，再利用 G 对 M_a 执行 Pauli 操作：若 $g_i=0$，则 Bob1 对 $M_a^{(i)}$ 执行 I 操作；否则，执行 σ_x 操作。然后，Bob1 将所得序列记为 $\bar{M}_a$，并将 $\bar{M}_a$ 和 G 发送给 Trent。

2）Bob1 将相应金额转给 Trent，并用与 Alice 类似的方法将 B 对应的量子态传送给 Trent，作为自己的转账凭证，其传输过程如下：

（1）Bob1 生成单光子序列 A_2、B_P，通过两步量子

表 3 购买信息的编码规则

Table 3 Coding rules for purchase information

L_i	m_i	$\lvert a_i b_i c_i\rangle$
0	00	$\lvert 000\rangle$ or $\lvert 111\rangle$
	01	$\lvert 001\rangle$ or $\lvert 110\rangle$
	10	$\lvert 011\rangle$ or $\lvert 100\rangle$
	11	$\lvert 010\rangle$ or $\lvert 101\rangle$
1	00	$\lvert +++\rangle$ or $\lvert ---\rangle$
	01	$\lvert ++-\rangle$ or $\lvert --+\rangle$
	10	$\lvert +--\rangle$ or $\lvert --+\rangle$
	11	$\lvert +-+\rangle$ or $\lvert -+-\rangle$

行走，使 B、A_2 和 B_P 相互纠缠。然后，Bob1 将行走后的 B_P 记为 $\bar{B}_P$，在其中随机地插入诱骗粒子串 $s\left(s\in\{\lvert 0\rangle,\lvert 1\rangle,\lvert +\rangle,\lvert -\rangle\}\right)$，并将所得序列发送给 Trent。Bob1 确认 Trent 收到序列后，公开他在其中插入的诱骗粒子的位置和初始态等信息，Trent 对其进行测量并计算错误率。若错误率低于预先设定的阈值，则认为传输过程中无窃听，执行下一步；否则，立即终止协议。

(2) Bob1 使用 X 基测量 $\lvert b_i\rangle$，使用 Q 基测量 $\lvert A_{2i}\rangle$，将测量结果分别记为 γ_1 和 γ_2。Bob1 再使用密钥 K_{TB1} 对 γ_1 和 γ_2 进行加密，得到 $S_{B1T}=E_{K_{TB1}}(\gamma_1,\gamma_2)$，并将其发送给 Trent。

3.4.2 Trent 验证 Bob1 的信息并通知 Charlie 发货

Trent 首先根据 L 对收到的 $\bar{M}_a$ 进行测量，若 $L=0$ 则使用 Z 基，否则使用 X 基，将测量结果记为 R'_a。然后，Trent 通过修正 Pauli 操作使 $\bar{B}_P$ 与 B 的态序列相等，将所得序列记为 M_b。最后，Trent 根据 L 对 M_b 进行测量，将测量结果记为 R_b。

1) Trent 验证 Alice 是否已对 Bob1 的转账信息进行确认。Trent 执行 $R'_{ai}\oplus R_{bi}\oplus G$ 操作，将所得结果记为 M_{ab}，然后将 M_{ab} 与 I 进行比较，若二者相等，认为 Bob1 的转账金额已经过 Alice 确认，可执行下一步；否则，提示确认有误，并终止协议。

2) Trent 告诉 Charlie 买家已经付款，需尽快发货。首先，Trent 生成随机字符串 G'，再利用 G' 对 M_b 执行 Pauli 操作得到 $\bar{M}_b$，并将 $\bar{M}_b$ 与 G' 一起发送给 Charlie。然后，Trent 将 C 对应的量子态发送给 Charlie，作为自己的认证凭证，其传输过程如下：

(1) Trent 生成单光子序列 A_3、C_P，通过两步量子行走，使 C、A_3 和 C_P 相互纠缠。

(2) Trent 将行走后的 C_P 记为 $\bar{C}_P$，再在其中随机插入诱骗粒子串 $r\left(r\in\{\lvert 0\rangle,\lvert 1\rangle,\lvert +\rangle,\lvert -\rangle\}\right)$，并将所得量子序列记为 $\bar{C}'_P$ 发送给 Charlie。Charlie 收到后，Trent 公开他在 $\bar{C}'_P$ 中插入的诱骗粒子的位置和初始态等信息，由 Charlie 对其进行测量并计算错误率。若错误率低于预先设定的阈值，执行下一步；否则，立即终止协议。随后，Trent 分别使用 X 基和 Q 基对 $\lvert c_i\rangle$ 和 $\lvert A_{3i}\rangle$ 进行测量，分别得到 ξ_1 和 ξ_2。Trent 再使用密钥 K_{CT} 对 ξ_1 和 ξ_2 进行加密，得到 $S'_{TC}=E_{K_{CT}}\{\xi_1,\xi_2\}$，并将其发送给 Charlie。

(3) Trent 使用密钥 K_{CT} 对 L、II 和 M_1 进行加密，得到 $S_{TC}=E_{K_{CT}}\{L,II,M_1\}$，并发送给 Charlie。

3.5 验证阶段

首先，Charlie 根据 L 选择适当测量基对 $\bar{M}_b$ 进行测量，将测量结果记为 R'_b。然后，Charlie 丢弃 $\bar{C}'_P$ 中的诱骗粒子，得到 $\bar{C}_P$，再通过解密 S'_{TC}，得到 ξ_1 和 ξ_2，根据 ξ_1 和 ξ_2 使 $\bar{C}_P$ 与 C 的态序列相等，并将所得序列记为 M_c。然后，Charlie 根据 L 对 M_c 进行测量，将测量结果记为 R_c。

Charlie 验证 Alice 的购买信息。Charlie 执行 $R'_{bi}\oplus R_{ci}\oplus G'$ 操作，将所得结果记为 M_{bc}，再将 M_{bc} 与 II 进行比较，若二者相等，认为 Alice 订单无误，执行下一步，否则，拒绝订单并终止协议。

确认订单后，Charlie 为 Alice 发货。Alice 收到货并确认无误后，确认订单，Trent 将 Bob1 转的钱转入 Charlie 登记的账户(Bob2)中，交易结束。

4 安全性与性能分析

4.1 外部攻击

假设 Eve 为外部攻击者，她试图未经许可获取或伪造秘密信息 M_2。若要完成此目的，她需要知道序列 I 和序列 II 的相关信息，或者得到协议中的全部粒子相关信息。

首先，由于序列 I 和序列 II 在协议中是分开传输的，且传输时分别使用密钥 K_{TB1} 和 K_{CT} 进行加密，因此 Eve 要想得到 I 和 II 的相关信息，她就必须要得到 K_{TB1} 和 K_{CT} 的相关信息，而 K_{TB1} 和 K_{CT} 是通过 QKD 协议进行分发的，由 QKD 协议保证其安全性，而 QKD 协议已被证明是绝对安全的，因此 Eve 无法通过此方法得到秘密信息 M_2。

其次，Eve 若想得到协议中粒子的相关信息，她可以通过以下三种攻击策略来进行攻击。

4.1.1 截获-重发攻击和测量-重发攻击

由于在粒子串传送时添加了诱骗粒子，因此外部攻击者 Eve 无法通过截获-重发攻击和测量-重发攻击对秘密信息进行有效窃取。

假设 Eve 截获 Alice 通过量子行走系统发送给 Bob1 的粒子串 A_P，然后对其进行伪造，将另一串粒子重新发送给 Bob1，由于 Eve 对 A'_P 中所插入的诱骗粒子的相关信息一无所知，因此 Bob1 在进行窃听检测时会发现错误率高于阈值，从而导致协议终止。

同理，若 Eve 对所截获粒子串进行测量，再将测量结果发送给 Bob1，同样会导致错误率升高，协议终止。

并且，即使Eve侥幸通过窃听检测，她的行为也使测量结果发生改变，无法通过之后的验证，因此Eve无法通过此攻击策略窃取秘密信息。

4.1.2　纠缠测量攻击

由于信息在量子信道中传输时，需要被编码为粒子串，并用离散时间量子行走系统进行加密，因此外部攻击者Eve无法通过纠缠测量攻击获取秘密信息。

假设Eve为获取隐形传态中所传输的粒子信息，她截获Alice发送给Bob1的粒子串A_{P}，并用自己准备的粒子e与$A_{\mathrm{P}i}$相互纠缠。此时，A_{P}中的每个诱骗粒子状态变化如下：

$$E\otimes|0e\rangle=a|0e_{00}\rangle+b|1e_{01}\rangle, \tag{1}$$

$$E\otimes|1e\rangle=b'|0e_{10}\rangle+a'|1e_{11}\rangle, \tag{2}$$

$$E\otimes|+e\rangle=\frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle+b|1e_{01}\rangle+b'|0e_{10}\rangle+a'|1e_{11}\rangle\right), \tag{3}$$

$$E\otimes|-e\rangle=\frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle+b|1e_{01}\rangle-b'|0e_{10}\rangle-a'|1e_{11}\rangle\right), \tag{4}$$

式中：E为Eve对其中每个粒子所进行的操作，矩阵形式为$\boldsymbol{E}=\begin{pmatrix}a & b'\\ b & a'\end{pmatrix}$。由$E$算符决定的4个纯状态$\left\{|e_{00}\rangle、|e_{01}\rangle|e\rangle_{10}、|e\rangle_{11}\right\}$满足归一化条件$\sum_{\alpha,\beta\in\{0,1\}}\left\langle e_{\alpha,\beta}\middle|e_{\alpha,\beta}\right\rangle=1$。根据$\boldsymbol{EE}^{*}=1$，$a$、$b$、$a'$和$b'$满足$|a|^2+|b|^2=1$、$|a'|^2+|b'|^2=1$和$ab^{*}=(a')^{*}b'$，因此可得$|a|^2=|a'|^2$和$|b|^2=|b'|^2$。如果Eve攻击的粒子处于纠缠态，此行为必然会引入错误，通过计算概率$P_E=|b|^2=1-|a|^2=|b'|^2=1-|a'|^2$，可以检测到窃听者的存在。如果Eve不想引入误差，则总粒子必须与Eve的辅助粒子以直积态的形式相关，然而，在直积态中，辅助粒子e与粒子$A_{\mathrm{P}i}$之间不存在相关性，因此Eve无法通过纠缠测量攻击得到任何有用信息。

由于Eve通过以上方法均无法获得有用的相关信息，因此，她的行为无法获得秘密信息M_2或对其进行伪造，即使进行了伪造也无法通过相关的验证。

4.2　内部攻击

协议中的内部参与者Bob1和Charlie无法推测出Alice的完整秘密信息M_2，也无法否认自己发送的信息或伪造其他参与者的信息。

1）Bob1和Charlie均无法获得完整的M_2。在此协议中，Trent将M_2编码在粒子串A、B和C中，Bob1只知道他拥有的粒子串B的信息和根据L测量得到的Alice发送给他的粒子串A的信息，而C对他来说是未知的粒子串。假设Bob1有50%的概率成功猜测出粒子串C中粒子c_i的状态，则Bob1成功推断出完整购物清单M_2内容的概率为$P_i=\binom{N}{k}\left(\frac{1}{2}\right)^{k}\left(\frac{1}{2}\right)^{N-k}$，其中$N$为$M_2$的长度，$k$为Bob1猜测正确的粒子数。因此，概率$P_i$满足二项分布，其二项式系数为$\binom{N}{k}=\frac{N!}{k!(N-k)!}$。对于不同的$N$，如图3所示，当$N\to\infty$时，$P_i\to0$。因此Bob1无法得到粒子串$C$，也就无法得到完整的$M_2$。同理可知，Charlie也无法得到完整的$M_2$。

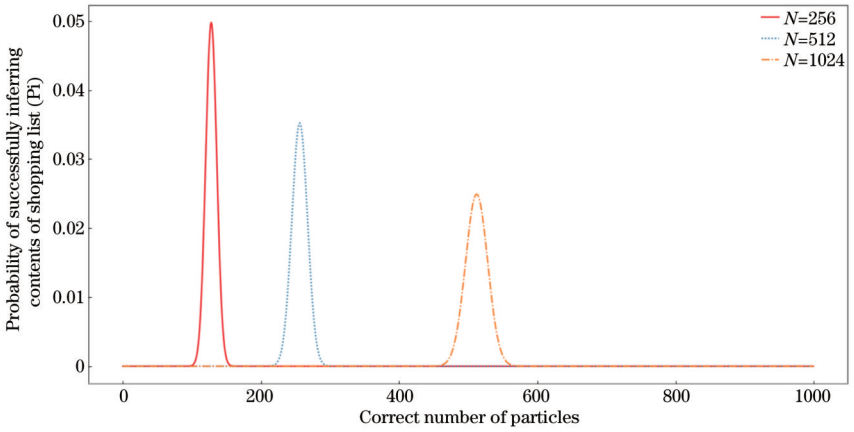

图3　Bob1推断出购物清单内容的概率

Fig. 3　Probability of Bob1 inferring the contents of the shopping list

2）Bob1无法否认自己发出的信息。假设Bob1想要否认他所发送的认证信息M_{a}'。由于Trent在验证时需要字符串G，而G是由Bob1利用共享密钥K_{TB1}加密后发送给Trent的，而K_{TB1}的安全性可以由QKD协议进行保证，因此Bob1无法否认他所发出的消息M_{a}'。

此外，也可以通过统计数据的方式对Bob1否认的概率进行定量评估。假设对于单粒子，Bob1否认的概率为50%，则否认其认证信息的概率P满足二项分布，二项式系数为$\binom{N}{k}=\frac{N!}{k!(N-k)!}$，其中$k$表示Bob1

否认的粒子数，N表示Trent收到的消息长度。因此，当$N\to\infty$时，$P\to 0$。也就是说，Bob1无法否认他所发出的消息M_a'。

3）Charlie无法对自己验证的信息进行否认。假设Charlie想要否认他验证的消息M_b'和C_P。如果Charlie否认他收到了Trent所发送的消息M_b'，那么当他验证消息的完整性时，需要的G'只能由他解密得到，因此，Trent可以揭露Charlie的不诚信行为。如果Charlie想要在验证后否认此信息的正确性，即在$M_{bc}=II$的情况下声明$M_{bc}\neq II$。此行为对Charlie甚至是协议的任一参与方都没有好处，因为此行为意味着协议过程中存在窃听行为，协议终止。

同时，Charlie也不能否认他收到的量子序列C_P。协议中，Trent将C_P发送给Charlie并使用K_{CT}对测量结果ξ_1和ξ_2进行加密，此消息只能由Charlie解密得到，如果Charlie否认他收到的信息，他将无法完成验证阶段。因此，Charlie无法否认他所验证的信息M_b'和C_P。

4）Alice无法伪造Bob1的信息M_a'，同时Bob1和Charlie也无法伪造Trent的信息M_b'。在协议中，Alice的目的是让Bob1将相应金额转给Trent，由于Alice不知道Bob1处理M_a时所使用的字符串G的相关信息，因此Alice无法伪造M_a'。同理，Bob1由于不知道Trent处理M_b时所使用的字符串G'的相关信息，从而无法伪造M_b'。

Charlie的目的是验证Alice的购买信息并售卖商品，因此即使Charlie可以伪造M_b'，他伪造出的M_b'也无法通过验证。若他将伪造的序列记为M_{bc}'，同时篡改II的信息为II'，令$M_{bc}'=II'$，则同样拥有II的Alice和Trent可以揭穿他的行为，因此Charlie无法伪造M_b'。

4.3 性能分析

近年来，区块链技术的研究，为电子支付协议提供了新思路，促进了其发展。量子电子支付协议在设计上也越来越追求更加简单的量子态制备方式和测量方法，在早期基于量子盲签名技术和量子代理盲签名技术的电子支付协议的设计基础上，尝试将制备的纠缠态粒子（常见的有Bell态和GHZ态）用相对更容易制备的其他量子态代替。为此，将本文所提出的协议与近年来提出的较为典型且安全的基于区块链技术的量子电子支付协议[11]和相比于纠缠态更易制备和测量的基于乘积态粒子的量子电子支付协议[13]进行比较，相关信息如表4所示。从表4可知，本文协议并未用到乘积态或纠缠态粒子，而是使用单粒子序列，再通过量子行走技术获取所需的纠缠态资源，并且本文协议所采用的测量操作为单粒子测量，因此粒子制备和测量难度更低。

表4 相关协议比较

Table 4 Comparison of relevant protocols

Protocol	Protocol in Ref. [11]	Protocol in Ref. [13]	Our protocol
Quantum resource	3-particle entangled states, single-particle states	3-particle partial X-LIOP states	Single-particle states
Trusted third party	No	Yes	Yes
Measurements	Bell-state measurements, Single-particle measurements	Single-particle measurements	Single-particle measurements

5 结 论

基于一维量子行走的隐形传态，提出了一种新的量子电子支付协议。与已有的量子电子支付协议相比，此协议不仅保留了支持第三方平台和银行间支付等功能，还将量子行走与电子支付相结合，使协议的参与方在初始阶段无需制备纠缠态粒子，而是采用单粒子降低了粒子制备和测量的困难性。目前研究人员已完成很多量子行走实验，因此本协议兼具实用性和安全性。同时，此协议将买家的购物信息进行二次划分，不仅将所购买商品的信息对银行进行保密，也将买家的私人信息，包括其真实姓名、银行账户等内容对商家进行盲化处理，由于这部分信息在物流方面没有过多的要求，故隐藏此信息对商家发货并没有产生不良影响。当商家确实需要买家的这部分信息时，可以向拥有此信息的第三方平台提出申请，在经过平台审核和买家同意后获知相关内容，从而完成相关操作。因此，对商家隐藏买家私人信息可以提高协议的匿名性，使协议内容更加贴合用户需求。安全性分析表明，此协议能够抵御内部攻击和外部攻击，在当前技术下是安全可行的。

参 考 文 献

[1] Chaum D. Blind signatures for untraceable payments[M]// Chaum D, Rivest R L, Sherman A T. Advances in cryptology. Boston: Springer, 1983: 199-203.

[2] Wen X J, Nie Z. An E-payment system based on quantum blind and group signature[C]//2010 Second International Symposium on Data, Privacy, and E-Commerce, September 13-14, 2010, Buffalo, NY, USA. New York: IEEE Press, 2010: 50-55.

[3] Wen X J, Chen Y Z, Fang J B. An inter-bank E-payment protocol based on quantum proxy blind signature[J]. Quantum Information Processing, 2013, 12(1): 549-558.

[4] Khodambashi S, Zakerolhosseini A. A quantum blind signature scheme for electronic payments[C]//2014 22nd Iranian Conference on Electrical Engineering (ICEE), May 20-22, 2014, Tehran, Iran. New York: IEEE Press, 2014: 879-884.

[5] Zhou R G, Li W, Huan T T, et al. An online banking system based on quantum cryptography communication[J]. International Journal of Theoretical Physics, 2014, 53(7): 2177-2190.
[6] Shao A X, Zhang J Z, Xie S C. An E-payment protocol based on quantum multi-proxy blind signature[J]. International Journal of Theoretical Physics, 2017, 56(4): 1241-1248.
[7] Niu X F, Zhang J Z, Xie S C, et al. A third-party E-payment protocol based on quantum multi-proxy blind signature[J]. International Journal of Theoretical Physics, 2018, 57(8): 2563-2573.
[8] Tiliwalidi K, Zhang J Z, Xie S C. A multi-bank E-payment protocol based on quantum proxy blind signature[J]. International Journal of Theoretical Physics, 2019, 58: 3510-3520.
[9] 何业锋, 陈思昊, 强雨薇, 等. 一种基于量子稠密编码的电子支付协议[J]. 光学学报, 2021, 41(10): 1027001.
He Y F, Chen S H, Qiang Y W, et al. Electronic payment protocol based on quantum dense coding[J]. Acta Optica Sinica, 2021, 41(10): 1027001.
[10] Zhang J L, Hu M S, Jia Z J, et al. A novel E-payment protocol implented by blockchain and quantum signature[J]. International Journal of Theoretical Physics, 2019, 58(4): 1315-1325.
[11] Gou X L, Shi R H, Gao W, et al. A novel quantum E-payment protocol based on blockchain[J]. Quantum Information Processing, 2021, 20(5): 192.
[12] Jiang D H, Hu Q Z, Liang X Q, et al. A trusted third-party E-payment protocol based on locally indistinguishable orthogonal product states[J]. International Journal of Theoretical Physics, 2020, 59(5): 1442-1450.
[13] Lin M M, Xue D W, Wang Y, et al. A new quantum payment protocol based on a set of local indistinguishable orthogonal product states[J]. International Journal of Theoretical Physics, 2021, 60(4): 1237-1245.
[14] Chou Y H, Lin F J, Zeng G J. An efficient novel online shopping mechanism based on quantum communication[J]. Electronic Commerce Research, 2014, 14(3): 349-367.
[15] Huang W, Yang Y H, Jia H Y. Cryptanalysis and improvement of a quantum communication-based online shopping mechanism [J]. Quantum Information Processing, 2015, 14(6): 2211-2225.
[16] Shukla C, Thapliyal K, Pathak A. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue[J]. Quantum Information Processing, 2017, 16(12): 295.
[17] Thapliyal K, Pathak A. Quantum e-commerce: a comparative study of possible protocols for online shopping and other tasks related to e-commerce[J]. Quantum Information Processing, 2019, 18(6): 191.
[18] Aharonov Y, Davidovich L, Zagury N. Quantum random walks [J]. Physical Review A, 1993, 48(2): 1687-1690.
[19] Lovett N B, Everitt M, Trevers M, et al. Spatial search using the discrete time quantum walk[J]. Natural Computing, 2012, 11 (1): 23-35.
[20] Tanaka H, Sabri M, Portugal R. Spatial search on Johnson graphs by continuous-time quantum walk[J]. Quantum Information Processing, 2022, 21(2): 74.
[21] Wang Y, Shang Y, Xue P. Generalized teleportation by quantum walks[J]. Quantum Information Processing, 2017, 16 (9): 221.
[22] Shi J J, Chen H, Zhou F, et al. Quantum blind signature scheme with cluster states based on quantum walk cryptosystem [J]. International Journal of Theoretical Physics, 2019, 58(4): 1337-1349.
[23] 冯艳艳, 施荣华, 石金晶, 等. 基于量子游走的仲裁量子签名方案[J]. 物理学报, 2019, 68(12): 120302.
Feng Y Y, Shi R H, Shi J J, et al. Arbitrated quantum signature scheme based on quantum walks[J]. Acta Physica Sinica, 2019, 68(12): 120302.
[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] Zheng T, Chang Y, Yan L L, et al. Semi-quantum proxy signature scheme with quantum walk-based teleportation[J]. International Journal of Theoretical Physics, 2020, 59(10): 3145-3155.
[26] Chen X X, Lou X P. An efficient verifiable quantum secret sharing scheme via quantum walk teleportation[J]. International Journal of Theoretical Physics, 2022, 61: 99.
[27] Bennett C H, Brassard G. An update on quantum cryptography [M]//Blakley G R, Chaum D. Advances in cryptology. Lecture notes in computer science. Heidelberg: Springer, 1984, 196: 475-480.
[28] 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.
[29] 何业锋, 赵艳坤, 李春雨, 等. 标记配对相干态下有限探测器死时间的测量设备无关量子密钥分配[J]. 光学学报, 2020, 40 (24): 2427001.
He Y F, Zhao Y K, Li C Y, et al. Measurement-device-independent quantum key distribution of finite detector's dead time in heralded pair coherent state[J]. Acta Optica Sinica, 2020, 40(24): 2427001.
[30] 何业锋, 李丽娜, 白倩, 等. 基于W态的多方测量设备无关量子密钥分配性能分析[J]. 激光与光电子学进展, 2021, 58(11): 1127002.
He Y F, Li L N, Bai Q, et al. Performance analysis of multi-party measurement-device-independent quantum key distribution based on W states[J]. Laser & Optoelectronics Progress, 2021, 58(11): 1127002.

E-Payment Protocols Based on Quantum Walk

He Yefeng, Yang Mengmei*, Li Zhi, Liu Yan, Tian Zheming

School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, *Shaanxi, China*

Abstract

Objective In recent years, with the rapid development of e-commerce and computer, online shopping is more and more popular. In the meantime, the development of quantum algorithms makes the traditional e-payment protocols based on

difficult mathematical problems more and more insecure, so the e-payment protocols based on quantum algorithms come into being. At present, most of the proposed quantum e-payment protocols use entangled states for quantum electronic signature protocols. However, the preparation and measurement of entangled states are very difficult, so in the case of ensuring the security of the protocols, using quantum states featuring more convenient preparation and measurement, instead of entangled states, has become a research direction of e-payment. Quantum walk is a technology that can produce the necessary entanglement resources spontaneously only by using the single-particle states without preparing entanglement resources in advance. This technology has been widely used in quantum computing and quantum simulation and is of certain practical value. At the same time, as people pay more attention to personal privacy, only users′ shopping lists being confidential to banks have been unable to meet people′s privacy needs. Therefore, in order to solve the above problems, we modify a classic e-payment agreement model and make the hidden users′ identity information not affect the normal delivery and merchants. Furthermore, we combine the quantum walk with quantum e-payment and propose a quantum e-payment protocol to ensure that entanglement resources can be obtained without preparing entangled states in advance and guarantee that the buyers′ bank accounts and real identity information can be kept confidential to merchants.

Methods Quantum walk is an extension of random walk in the quantum field. It takes the quantum as the carrier to simulate the chaotic nonlinear dynamic walk behavior. According to the characteristics of the quantum walk, the encrypted quantum communication channels are established accordingly. The quantum walk mainly contains the complex Hilbert space of two main quantum spaces, namely, coin space and position space. The protocol is based on the one-dimensional quantum walk teleportation, and through the two-step quantum walk, the shift operator can make the position space and coin space entangle with each other, so as to construct quantum channels for information transmission. The biggest advantage of quantum walk technology is that it can obtain the entanglement resources through the single photon operation. The measurement and preparation of the protocol are simpler compared with directly operating entangled states, and the randomness of the quantum walk makes the transmission more secure. In addition, by dividing the shopping information of buyers into the identity information accessible to the banks and making the shopping list open to the merchants, the banks and the merchants in the protocol will not know the information obtained by the other party so that the privacy of the buyers is greatly protected.

Results and Discussions Firstly, in order to further protect the users′ privacy, we modify a classic electronic payment agreement model (Fig. 1). In this model, we reduce the workload of buyers and give the processing and distribution of information to third-party platforms. While keeping the buyers′ shopping lists confidential to the banks, the buyers′ identity information is also unavailable to the merchants. So this protocol makes the merchants and the banks only have the information that they need and know nothing of the information obtained by the other party. Secondly, quantum walk technology is applied to various stages of the protocol including the trading purchase phase, trading payment phase, and verifying phase (Fig. 2). By applying quantum walk technology, the complexity of quantum resource preparation and measurement in the protocol is reduced. Finally, the security analysis of this protocol is conducted (Fig. 3), and the result shows that neither the internal nor external attackers of this protocol can obtain the secret information in the protocol, and this protocol can resist both internal and external attacks.

Conclusions This protocol, compared with the existing quantum e-payment protocols, not only retains the third-party platforms and the inter-bank payment function but also combines the quantum walk and electronic payment. It makes the participants of the protocol in the initial stage free from preparing particles in entangled states and makes them only prepare the single-particle states which can get the required entanglement resources. This move reduces the complexity of quantum state preparation and measurement. At the same time, the shopping information of the buyers is divided, with the information of the purchased goods confidential to the banks and the buyers′ private information unavailable to the merchants. In addition, when the merchants really need this part of the information of the buyers, they can apply to third-party platforms for the information. Being reviewed by the platforms and approved by the buyers, the merchants can know the information they want, so as to complete the corresponding operation. Finally, security analysis shows that this protocol can resist internal and external attacks and is safe and feasible under current technology.

Key words quantum optics; quantum cryptography; quantum walk; electronic payment; teleportation; single particles