第 41 卷 第 10 期/2021 年 5 月/光学学报 研究论文

光学学报

一种基于量子稠密编码的电子支付协议

何业锋[1,2]，陈思昊[1*]，强雨薇[1]，李丽娜[1]，白倩[1]

[1]西安邮电大学网络空间安全学院，陕西 西安 710121；

[2]桂林电子科技大学广西密码学与信息安全重点实验室，广西 桂林 541004

摘要 针对电子支付系统的安全性和实用性需求，考虑到基于可控隐形传态的传统电子支付协议存在步骤繁杂、签名过程琐碎等问题，提出了一种基于量子稠密编码的电子支付协议。该协议运用量子密钥分配、单粒子测量、Bell 测量和幺正变换等量子操作，依次进行了消息盲化、授权、签名和验证，从而完成了电子支付过程。新协议以三粒子纠缠态作为量子传输信道，能用较少的资源完成不同银行之间的交易。利用稠密编码代替可控隐形传态，可以实现仅传送一个量子位就传输 2 bit 经典消息。安全性分析结果表明，该协议能实现购买信息的盲化，满足不可否认性、不可伪造性和无条件安全性。

关键词 量子光学；量子密码学；电子支付；稠密编码；幺正变换

中图分类号 TN918 **文献标志码** A **doi**：10.3788/AOS202141.1027001

Electronic Payment Protocol Based on Quantum Dense Coding

He Yefeng[1,2], Chen Sihao[1*], Qiang Yuwei[1], Li Lina[1], Bai Qian[1]

[1] *School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*;

[2] *Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*

Abstract In view of the security and practicability requirements of an electronic payment system as well as the problems of complicated steps and trivial signature processes and others in the traditional electronic payment protocol based on controlled teleportation, we propose an electronic payment protocol based on quantum dense coding. The proposed protocol uses quantum operations such as quantum key distribution, single particle measurement, Bell measurement, and unitary operator to perform message blinding, authorization, signature and verification processes in order, and thus completes the whole electronic payment process. In the new protocol, the three-particle entangled state is used as the quantum channel, which can use less resources to complete transactions among different banks. Moreover, by using dense coding instead of controlled teleportation, it is possible to transmit two-bit classical messages with only one qubit. The security analysis shows that the protocol can guarantee the blindness of the purchase information, and satisfy the undeniability, unforgeability and unconditional security.

Key words quantum optics; quantum cryptography; electronic payment; dense coding; unitary operator

OCIS codes 270.5568; 270.5565; 270.5585

1 引 言

目前，随着互联网的高速发展和网络技术的推陈出新，不受时间和空间限制的电子商务成为了人们日常生活中的一部分。因此，为电子商务选择一种合适的电子支付模型具有十分重要的意义。1982 年，Chaum 等[1]首次提出了电子现金的概念，从此电子现金得到了广泛的研究，研究者提出了许多电

收稿日期：2020-11-17；**修回日期**：2020-12-10；**录用日期**：2020-12-30

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项目(2021JM-462)、广西密码学与信息安全重点实验室研究课题(GCIS201923)

* **E-mail**：515358140@qq.com

子现金支付协议[2-3]。然而，随着量子计算的发展，大部分电子现金支付协议的安全性就受到了严重威胁。由于量子密码学的安全性是基于量子力学原理的，因此量子签名在电子支付中的应用受到了广泛的关注。

2010 年，Wen[4]提出了基于量子盲签名和群签名的电子支付系统，引入了两个可信中心，提高了系统的安全性。在 2013 年，Wen 等[5]以量子代理盲签名为基础，构建了一个可用于不同银行间的跨行支付系统。但 Cai 等[6]发现，这个系统中的量子信道存在着安全漏洞，外部入侵者能发起拒绝服务攻击，内部的不诚信商人能更改购物信息，因此提出了改进措施。2018 年，Niu 等[7]提出了基于多代理盲签名的电子支付协议，该协议不仅支持移动电子支付，还支持不同银行间的交易。2019 年，Zhang 等[8]首次基于区块链和量子签名，提出了一种新型的电子支付协议。该协议引入了区块链，具有分散、不可篡改和安全可靠的特性，不需要引入第三方中介，即可避免接受者的不诚实行为，提高了协议的安全性。2020 年，Xie 等[9]提出了一种银行间的量子电子支付协议，该协议利用四粒子团簇态良好的纠缠性和测量规则，能更好地节省资源。然而，这些协议都是基于可控量子隐形传态[10-11]实现的，利用粒子的纠缠交换特性对消息进行签名或盲签名。大多数协议的步骤繁杂，签名过程琐碎。

量子稠密编码是量子信息学的重要应用，由 Bennet 等[12]在 1992 年提出，若通信双方事先共享一个纠缠态，只发送一个量子比特就可以传输 2 bit 经典信息，显然量子信道的经典容量扩大了。本文提出了一种基于量子稠密编码的电子支付协议，该协议通过单粒子和 Bell 基测量来实现，简单易操作，且具有高效性。

2 量子稠密编码

本文提出的电子支付协议是基于量子稠密编码。如果 Alice 想把经典比特 00，01，10，11 发送给 Bob，她可以在 Charlie 的协助下完成下面的协议。

1) Alice 首先制备三粒子纠缠态 $|\xi\rangle_{123}$，形式为

$$|\xi\rangle_{123}=\frac{1}{2}(|000\rangle+|110\rangle+|011\rangle+|101\rangle)_{123},\tag{1}$$

式中：脚标 1、2、3 分别表示纠缠态 $|\xi\rangle_{123}$ 的第 1、2、3 个粒子。然后，Alice 把粒子 2 发给 Charlie，粒子 3 发给 Bob，而将粒子 1 留在自己手中。

2) Alice 根据自己要发送的经典比特，对粒子 1 进行相应的幺正变换。当经典比特为 00，01，10，11 时，分别对粒子 1 进行 $\boldsymbol{I}$、$\boldsymbol{\sigma}_x$、$\mathrm{i}\boldsymbol{\sigma}_y$、$\boldsymbol{\sigma}_z$ 操作，其中 $\boldsymbol{I}$ 为恒等操作，$\boldsymbol{\sigma}_x$、$\boldsymbol{\sigma}_y$ 和 $\boldsymbol{\sigma}_z$ 分别为 Pauli 矩阵的 x、y、z 分量。此时，$|\xi\rangle_{123}$ 分别变为

$$\begin{cases}|\xi_{\boldsymbol{I}}\rangle_{123}=\dfrac{1}{2}(|000\rangle+|110\rangle+|011\rangle+|101\rangle)_{123}\\ |\xi_{\boldsymbol{\sigma}_x}\rangle_{123}=\dfrac{1}{2}(|100\rangle+|010\rangle+|111\rangle+|001\rangle)_{123}\\ |\xi_{\mathrm{i}\boldsymbol{\sigma}_y}\rangle_{123}=\dfrac{1}{2}(-|100\rangle+|010\rangle-|111\rangle+|001\rangle)_{123}\\ |\xi_{\boldsymbol{\sigma}_z}\rangle_{123}=\dfrac{1}{2}(|000\rangle-|110\rangle+|011\rangle-|101\rangle)_{123}\end{cases}。\tag{2}$$

然后，Alice 再把执行幺正变换后的粒子 1 发给 Bob。

3) Charlie 用$\{|0\rangle,|1\rangle\}$基去测量粒子 2，将测量结果通过公开信道发给 Bob。测量粒子 2 后，粒子 1 和粒子 3 的可能状态变化为

$$\begin{cases}\langle 0_2|\xi_{\boldsymbol{I}}\rangle=\dfrac{1}{2}(|00\rangle+|11\rangle)_{13}\\ \langle 0_2|\xi_{\boldsymbol{\sigma}_x}\rangle=\dfrac{1}{2}(|10\rangle+|01\rangle)_{13}\\ \langle 0_2|\xi_{\mathrm{i}\boldsymbol{\sigma}_y}\rangle=\dfrac{1}{2}(-|10\rangle+|01\rangle)_{13}\\ \langle 0_2|\xi_{\boldsymbol{\sigma}_z}\rangle=\dfrac{1}{2}(|00\rangle-|11\rangle)_{13}\\ \langle 1_2|\xi_{\boldsymbol{I}}\rangle=\dfrac{1}{2}(|10\rangle+|01\rangle)_{13}\\ \langle 1_2|\xi_{\boldsymbol{\sigma}_x}\rangle=\dfrac{1}{2}(|00\rangle+|11\rangle)_{13}\\ \langle 1_2|\xi_{\mathrm{i}\boldsymbol{\sigma}_y}\rangle=\dfrac{1}{2}(|00\rangle-|11\rangle)_{13}\\ \langle 1_2|\xi_{\boldsymbol{\sigma}_z}\rangle=\dfrac{1}{2}(-|10\rangle+|01\rangle)_{13}\end{cases}。\tag{3}$$

4) Bob 对收到的粒子 1 和粒子 3 进行 Bell 基测量。基于量子纠缠态理论[13-14]，Bob 能根据自己的测量结果和 Charlie 的测量结果，获知 Alice 的幺正变换和经典比特信息。具体对应关系如表 1 所示，其中$|\varphi^+\rangle$，$|\varphi^-\rangle$，$|\psi^+\rangle$和$|\psi^-\rangle$为一组完备正交基，又称 Bell 基。

3 量子支付协议

如图 1 所示，我们的协议有四个参与者：Alice 是消费者，Charlie 是商家，Bob 1 是消费者所在的银行，Bob 2 是商家所在的银行。

表 1 测量结果与 Alice 的操作之间的关系

Table 1 Relationship between measured results and Alice′s operations

Classic bit	Unitary operator	Charlie′s measurement result	Bob′s measurement result
00	$\boldsymbol{I}$	$\|0\rangle_2$	$\|\varphi^+\rangle$
00	$\boldsymbol{I}$	$\|1\rangle_2$	$\|\psi^+\rangle$
01	$\boldsymbol{\sigma}_x$	$\|0\rangle_2$	$\|\psi^+\rangle$
01	$\boldsymbol{\sigma}_x$	$\|1\rangle_2$	$\|\varphi^+\rangle$
10	$\mathrm{i}\boldsymbol{\sigma}_y$	$\|0\rangle_2$	$\|\psi^-\rangle$
10	$\mathrm{i}\boldsymbol{\sigma}_y$	$\|1\rangle_2$	$\|\varphi^-\rangle$
11	$\boldsymbol{\sigma}_z$	$\|0\rangle_2$	$\|\varphi^-\rangle$
11	$\boldsymbol{\sigma}_z$	$\|1\rangle_2$	$\|\psi^-\rangle$

假设客户 Alice 需要通过电子支付向商家 Charlie 购物，而 Alice 和 Charlie 分别在不同的两家银行 Bob 1 和 Bob 2 处开户。Alice 发一条购物信息给 Charlie，同时请求 Bob 1 付款。Bob 1 收到请求后授权 Bob 2 对购物信息进行代理签名，同时扣除 Alice 账户上的金额。Bob 2 接到 Bob 1 的授权后，对购物信息进行签名，同时在商家的账户上存入相应的金额。最后 Charlie 验证 Bob 2 的签名有效后发送货物给 Alice，交易完成。

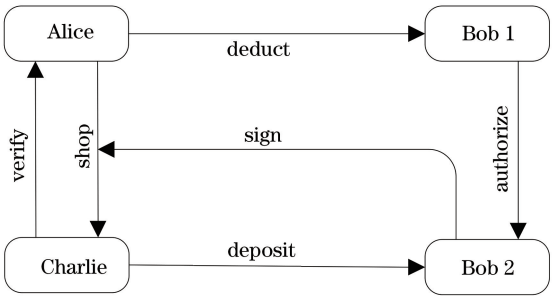

图 1 电子支付框架图

Fig. 1 Block diagram of electronic payment

3.1 初始阶段

1) Alice 的购物信息 M 分为两部分：M_1（n bit）和 M_2（n bit）。其中包括消费者的私人购物信息、商品的价格、消费者和商家所在银行的消息。为了保护隐私，需要对详细的购物账单信息进行盲化处理。

2) 消费者与商家建立共享会话密钥 K_{AC}；消费者与自己所在银行建立共享会话密钥 K_{AB1}；商家与自己所在银行建立共享会话密钥 K_{CB2}；两家银行之间建立共享会话密钥 K_{B1B2}。以上密钥分配可以通过无条件安全的量子密钥分配（QKD）协议[15-17]或测量设备无关 QKD 协议[18-20]实现，例如著名的 BB84 或者 B92 等协议。

3) 消费者 Alice 在准备购物时，首先制备 n 个三粒子纠缠态 $|\xi\rangle_{123}$[形式如(1)式所示]，分别将 n 个纠缠态中的粒子 1，2，3 组成粒子序列 L_1，L_2，L_3，将粒子序列 L_2 发给消费者所在银行 Bob 1，将粒子序列 L_3 发给商家所在银行 Bob 2，粒子序列 L_1 留在自己手中。

3.2 消息盲化阶段

1) Alice 将自己所购物品的详细账单信息 M_1 转化为二进制信息 $M_1'=\{M_1'(i),i=1,2,\cdots,n\}$，并且 $M_1'(i)\in\{00,01,10,11\}$，其中 i 为随机数。

2) Alice 根据 $M_1'(i)$ 的值，对粒子序列 L_1 中的第 i 个粒子进行幺正变换，当 $M_1'(i)$ 为 00，01，10，11 时，Alice 分别使用幺正变换 $\boldsymbol{I}$、$\boldsymbol{\sigma}_x$、$\mathrm{i}\boldsymbol{\sigma}_y$、$\boldsymbol{\sigma}_z$，执行幺正变换后的粒子序列记为 L_1'。因此实现了消息 M_1 的盲化。Alice 从集合$\{|1\rangle,|0\rangle,|+\rangle,|-\rangle\}$中随机选出足够多的诱骗光子，随机插入到粒子序列 L_1' 中，得到新的粒子序列 L_1''。

3)Alice 利用与 Charlie 共享的密钥 K_{AC} 和一次一密算法，对 M_1' 进行加密处理，得到 $C_1=E_{K_{\mathrm{AC}}}(M_1')$，并将 C_1 和粒子序列 L_1'' 一起发送给 Charlie。

3.3 授权和签名阶段

1) Alice 利用与 Bob 1 共享的密钥 K_{AB1} 对 M_2 进行加密处理，得到 $C_2=E_{K_{\mathrm{AB1}}}(M_2)$，并把 C_2 发给 Bob 1 以通知支付。

2) Bob 1 收到 C_2 之后，解密得到 M_2。当他收到了购买请求后，用$\{|1\rangle,|0\rangle\}$基去测量粒子序列 L_2 中的每个粒子，将测量结果记录为 $\beta_{\mathrm{B1}}=\{\beta(i)_2,i=1,2,\cdots,n\}$，$\beta(i)_2\in\{|1\rangle,|0\rangle\}$。并将 β_{B1} 转化为经典信息 $\beta'_{\mathrm{B1}}=\{\beta(i)'_2,i=1,2,\cdots,n\}$，$\beta(i)'_2\in\{1,0\}$，其中符号“1”对应$|1\rangle$态，符号“0”对应$|0\rangle$态。然后用与 Bob 2 共享的密钥 K_{B1B2} 加密 β'_{B1}，得到 $S_{\mathrm{B1}}=E_{K_{\mathrm{B1B2}}}(\beta'_{\mathrm{B1}})$，并将$(M_2,S_{\mathrm{B1}})$发给 Bob 2 以作为代理授权信息。

3) Bob 2 收到 S_{B1} 之后，解密得到 β'_{B1}。然后 Bob 2 产生随机经典字符串 $r=\{r(i),i=1,2,\cdots,n\}$，$r(i)\in\{00,01,10,11\}$。根据 $r(i)$ 的值对粒子序列 L_3 中的第 i 个粒子进行幺正变换。当 $r(i)$ 为 00，01，10，11 时，分别执行幺正变换 $\boldsymbol{I}$、$\boldsymbol{\sigma}_x$、$\mathrm{i}\boldsymbol{\sigma}_y$、$\boldsymbol{\sigma}_z$。执行幺正变换后的粒子序列记为 L_3'。Bob 2 从集合$\{|1\rangle,|0\rangle,|+\rangle,|-\rangle\}$中随机选出足够多的诱骗光子，随机插入到粒子序列 L_3' 中，得到新的粒子序列 L_3''。然后 Bob 2 用与 Charlie 共享的密钥 K_{CB2} 加密 β'_{B1} 和 r，得到代理盲签名 $S_{\mathrm{B2}}=E_{K_{\mathrm{B1B2}}}(\beta'_{\mathrm{B1}},r)$，并把$(M_2,S_{\mathrm{B2}})$和 L_3'' 发给 Charlie。

3.4 验证阶段

1) Charlie 用密钥 K_{AC} 解密 Alice 发来的 C_1，得到 M_1'。用密钥 K_{CB2} 解密 Bob 2 发来的 $S_{B2}=E_{K_{B1B2}}(\beta_{B1}',r)$，得到 β_{B1}' 和 r。

2) 在 Charlie 收到 Alice 和 Bob 2 发来的粒子序列 L_1'' 和 L_3'' 后，Alice 和 Bob 2 分别公布诱骗光子的位置与相应的测量基{|1⟩，|0⟩}或{|+⟩，|−⟩}，Charlie 用正确的测量基去测量相应的诱骗光子，并将测量结果分别告诉 Alice 和 Bob 2。Alice 和 Bob 2 分别比较测量结果和诱骗光子的初始状态，并计算错误率。如果错误率低于预先规定的限门值，则继续协议的下一步。如果错误率超过了预先规定的限门值，则停止此协议并重新开始。

3) Charlie 从 L_1'' 和 L_3'' 中去掉诱骗光子后，得到序列 L_1' 和 L_3'。然后对 L_1' 和 L_3' 中的每一对对应的粒子进行 Bell 基测量，并记录测量结果为 $\beta_C=\{\beta(i)_{13},i=1,2,\cdots,n\}$，$\beta(i)_{13}\in\{|\varphi^+\rangle,|\varphi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$。

4) 如果 M_1'、β_{B1}'、r、β_C 符合表2中的对应关系，

表 2 M_1'、β_{B1}'、r、β_C 之间的关系

Table 2 Relationship among M_1', β_{B1}', r and β_C

M_1'	β_{B1}'	r	β_C
00	0	00	$\|\varphi^+\rangle$
00	0	01	$\|\psi^+\rangle$
00	0	10	$\|\psi^-\rangle$
00	0	11	$\|\varphi^-\rangle$
00	1	00	$\|\psi^+\rangle$
00	1	01	$\|\varphi^+\rangle$
00	1	10	$\|\varphi^-\rangle$
00	1	11	$\|\psi^-\rangle$
01	0	00	$\|\psi^+\rangle$
01	0	01	$\|\varphi^+\rangle$
01	0	10	$\|\varphi^-\rangle$
01	0	11	$\|\psi^-\rangle$
01	1	00	$\|\varphi^+\rangle$
01	1	01	$\|\psi^+\rangle$
01	1	10	$\|\psi^-\rangle$
01	1	11	$\|\varphi^-\rangle$
10	0	00	$\|\psi^-\rangle$
10	0	01	$\|\varphi^-\rangle$
10	0	10	$\|\varphi^+\rangle$
10	0	11	$\|\psi^+\rangle$
10	1	00	$\|\varphi^-\rangle$
10	1	01	$\|\psi^-\rangle$
10	1	10	$\|\psi^+\rangle$
10	1	11	$\|\varphi^+\rangle$
11	0	00	$\|\varphi^-\rangle$
11	0	01	$\|\psi^-\rangle$
11	0	10	$\|\psi^+\rangle$
11	0	11	$\|\varphi^+\rangle$
11	1	00	$\|\psi^-\rangle$
11	1	01	$\|\varphi^-\rangle$
11	1	10	$\|\varphi^+\rangle$
11	1	11	$\|\psi^+\rangle$

Charlie 就确认代理签名是有效的，否则拒绝。

4 安全性分析与讨论

在本节中，我们说明协议满足盲性、不可伪造性、不可否认性和无条件安全性，并对协议的性能进行了分析。

4.1 消息的盲性

在交易过程中，若外部攻击者 Eve 想要获得 Alice 的详细账单信息 M_1，根据协议的执行过程，我们发现他只能从加密信息 C_1 和粒子序列 L_1'' 入手。由于 C_1 是 M_1' 的密文，且协议中采用的加密算法是无条件安全的，所以 Eve 从 C_1 中得不到 M_1' 的内容。若 Eve 截获 L_1''，由于不知道诱骗光子的位置和原粒子的初始量子态，因此无法通过测量得到 M_1' 的内容。另外，交易中的内部成员 Bob 1 和 Bob 2 也不知道 M_1' 的内容，因此方案具备盲性。

4.2 不可否认性

下面说明本协议可以抵抗消费者 Alice 和商人 Charlie 的否认行为。根据 3.3 节可知，为了通知支付，Alice 需要把 $C_2=E_{K_{AB1}}(M_2)$ 发送给 Bob 1。一旦发生争议，Bob 1 可以使用 K_{AB1} 解密得到 M_2，从而识别 Alice 的否认行为。这就意味着消费者 Alice 无法否认他的购买信息。根据 3.4 节可知，Charlie 若否认代理签名有效，那么此时协议就会终止。若 Charlie 否认收到货款，由于银行是可信的，这种行为会被驳回。因此，Charlie 无法进行否认行为。

4.3 不可伪造性

在本协议中，银行 Bob 1 和 Bob 2 是可信的。下面说明攻击者 Eve 无法伪造消息和签名。假设 Eve 想冒充 Alice 给 Bob 1 或 Charlie 发送消息，由于 Eve 不知道 Alice 与 Bob 1 以及与 Charlie 之间的共享密钥 K_{AB1} 和 K_{AC}，根据一次一密算法的无条件安全性，可知 Eve 的攻击无法成功。假设 Eve 想要伪造 Bob 1 的代理授权 S_{B1}，由于 Eve 不知道 Bob 1 与 Bob 2 共享的密钥 K_{B1B2}，同样根据一次一密算法的无条件安全性可知，Bob 1 的代理授权不可能被伪造。类似地，Bob 2 的签名 S_{B2} 也不能被伪造。

4.4 无条件安全性

本协议的无条件安全性是由量子密钥分配、一次一密加密算法和安全的量子传输信道来保证的。首先，在初始阶段，消费者、商家、消费者所在银行和商家所在银行两两建立共享会话密钥，都采用的是量子密钥分配协议或测量设备无关 QKD 协议，这些协议都是基于量子力学基本原理的，已经被证明

是无条件安全的。其次，在发送经典信息 C_1，C_2、S_{B1} 和 S_{B2} 时，利用共享会话密钥并结合一次一密加密算法进行传输，一次一密算法的无条件安全性保证了加密消息是无条件安全的。最后，Alice 和 Bob 2 对发送给 Charlie 的粒子序列 L_1 和 L_3 进行变换，并随机从集合{|1⟩，|0⟩，|+⟩，|−⟩}中选择诱骗态插入到这两个序列中，Charlie 收到这两个序列后可以与发送者合作，利用诱骗态检测信道的安全性，防止测量-重发攻击、截获重发攻击和纠缠-测量攻击等[21]，保证发送粒子序列这个过程是安全的。因此量子传输信道是无条件安全的。

4.5 性能分析

本协议与文献[7-9]的比较如表 3 所示。从表 3 可知，相比于其他协议中用到的量子资源，如六粒子纠缠态和四粒子团簇态，本文协议中所需的量子资源仅为三粒子纠缠态，消耗更少的资源且容易制备和操作。用稠密编码代替可控隐形传态，可以实现仅传送一个量子位就传输 2 bit 经典消息。本协议与文献[7-9]相比，操作更简单；与文献[7-8]相比，次数减少。幺正变换操作由两个参与者执行，减少了操作的难度和强度。在现有技术和实验条件下，本文所提出的协议更容易实现。

表 3 本协议与其他协议的对比

Table 3 Comparison between proposed protocol and others

Method	Quantum resource	Measurement	Controlled teleportation	Unitary operator
Protocol in Ref. [7]	Genuinely entangled six-qubit state	Three Bell state measurement	Yes	Once
Protocol in Ref. [8]	Six-qubit entangled state	One single particle measurement, one GHZ state measurement, and one Bell state measurement	Yes	Once
Protocol in Ref. [9]	Four-particle cluster state	Two Bell state measurement	Yes	Once
Proposed protocol	Three-particle entangled state	One single particle measurement, and one Bell state measurement	No	Twice

5 结 论

提出了一种基于量子稠密编码的电子支付协议。安全性分析结果表明，此协议满足盲性、不可否认性、不可伪造性和无条件安全性。与之前的工作相比，所提协议是基于三粒子纠缠态，仅使用 Bell 基测量、单粒子测量和幺正变换就可以实现，简单易操作。协议用稠密编码代替可控隐形传态，实现了操作的高效性。

参 考 文 献

[1] Chaum D, Rivest R L, Sherman A T, et al. Blind signatures for untraceable payments[C]//Advances in Cryptology: Proceedings of CRYPTO ′82, August 23-25, 1982, Santa Barbara, California, USA. New York: Plenum Press, 1982: 199-203.

[2] Maitland G, Boyd C. Fair electronic cash based on a group signature scheme[M]//Qing S H, Okamoto T, Zhou J Y, et al. Information and communications security. Lecture notes in computer science. Heidelberg: Springer, 2001, 2229: 461-465.

[3] Canard S, Traoré J. On fair E-cash systems based on group signature schemes[M]//Naini R S, Seberry J. Information security and privacy. Lecture notes in computer science. Heidelberg: Springer, 2003, 2727: 237-248.

[4] Wen X J. An E-payment system based on quantum group signature[J]. Physica Scripta, 2010, 82(6): 065403.

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

[6] Cai X Q, Wei C Y. Cryptanalysis of an inter-bank E-payment protocol based on quantum proxy blind signature [J]. Quantum Information Processing, 2013, 12(4): 1651-1657.

[7] Niu X F, Zhang J Z, Xie S C, et al. A practical E-payment protocol based on quantum multi-proxy blind signature [J]. Communications in Theoretical Physics, 2018, 70(5): 529-533.

[8] 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.

[9] Xie S C, Niu X F, Zhang J Z, et al. An improved quantum E-payment system[J]. International Journal of Theoretical Physics, 2020, 59(2): 445-453.

[10] Li Y H, Li X L, Nie L P, et al. Controlled quantum secure direct communication by using a five-atom cluster state in cavity QED[J]. International Journal of Theoretical Physics, 2015, 54(10): 3728-3732.

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

[12] Bennett C H, Wiesner S J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states[J]. Physical Review Letters, 1992, 69(20): 2881-2884.

[13] Wang T Y, Ma J F, Cai X Q, et al. The postprocessing of quantum digital signatures [J]. Quantum Information Processing, 2017, 16: 19.

[14] Niu X F, Zhang J Z, Xie S C, et al. A practical E-payment protocol based on quantum multi-proxy blind signature[J]. Communications in Theoretical Physics, 2018, 70(5): 529-533.

[15] Su H Y. Simple analysis of security of the BB84 quantum key distribution protocol [J]. Quantum Information Processing, 2020, 19(6): 169.

[16] Lo H K, Chau H F, Ardehali M, et al. Efficient quantum key distribution scheme and a proof of its unconditional security [J]. Journal of Cryptology, 2005, 18(2): 133-165.

[17] Inamori H, Lütkenhaus N, Mayers D, et al. Unconditional security of practical quantum key distribution[J]. The European Physical Journal D, 2007, 41(3): 599-627.

[18] He Y F, Zhao Y K, Guo J R, et al. Statistical fluctuation analysis of quantum key distribution protocols based on heralded pair coherent state[J]. Acta Optica Sinica, 2020, 40(7): 0727002.
何业锋, 赵艳坤, 郭佳瑞, 等. 基于标记配对相干态的量子密钥分配协议的统计涨落分析[J]. 光学学报, 2020, 40(7): 0727002.

[19] He Y F, Li C Y, Guo J R, et al. Passive measurement-device-independent quantum key distribution based on heralded pair coherent states [J]. Chinese Journal of Lasers, 2020, 47(9): 0912002.
何业锋, 李春雨, 郭佳瑞, 等. 基于标记配对相干态的被动测量设备无关量子密钥分配[J]. 中国激光, 2020, 47(9): 0912002.

[20] He Y F, Guo J R, Li C Y, et al. Fluctuation analysis of key distribution protocol based on heralded single-photon source and orbital angular momentum [J]. Chinese Journal of Lasers, 2020, 47(4): 0412001.
何业锋, 郭佳瑞, 李春雨, 等. 基于指示单光子源和轨道角动量的密钥分配协议的波动分析[J]. 中国激光, 2020, 47(4): 0412001.

[21] He Y F. Two-party quantum key agreement protocols based on four-particle entangled states[J]. Journal of University of Electronic Science and Technology of China, 2017, 46(2): 340-345.
何业锋. 基于四粒子纠缠态的两方量子密钥协商协议[J]. 电子科技大学学报, 2017, 46(2): 340-345.