doi:10.11959/j.issn.1000-436x.2015248

有序双重的量子盲签名协议

王辉，石润华，仲红，崔杰，张顺，汪开婷
（安徽大学 计算机科学与技术学院，安徽 合肥 230601）

摘 要：考虑现实生活中跨行交易的情形，需要两方银行对同一账单进行签名，首次提出了一个基于量子相干性和量子纠缠性的有序双重量子盲签名协议。消费者先将消息盲化，两方银行先后对盲化消息进行有序签名。协议的优势是验证方只需要进行粒子测量，并不需要实施量子酉变换。此外，与其他主流的单重量子盲签名方案相比，验证签名时的效率和正确率有明显的提高。
关键词：量子信息；量子签名；盲签名；双重签名
中图分类号：TN918.1 **文献标识码**：A

Sequential double quantum blind signature protocol

WANG Hui, SHI Run-hua, ZHONG Hong, CUI Jie, ZHANG Shun, WANG Kai-ting
（School of Computer Science and Technology, Anhui University, Hefei 230601, China）

Abstract: Considering the fact that both party banks need to sign on the same bill because of the inter-bank E-payment in real life. A sequential double blind signature protocol based on the quantum coherence and quantum entanglement was proposed for the first time. Consumer blinded the message at first and each bank signed the blinded message one by one. The advantage of this protocol is that it only requires particle measurements for the verification without any quantum unitary operation. In addition, the proposed protocol obtains the higher efficiency and accuracy in the phase of signature verification, compared with other single quantum blind signature schemes.
Key words: quantum information; quantum signature; blind signature; double signature

1 引言

数字签名是对现实生活中手写签名的数字模拟，给电子文档进行签名的方法，它是信息安全的核心技术之一，也是安全电子商务和安全电子政务所依赖的技术之一。随着数字签名技术的深入应用，继而出现了新需求，在签名的同时还需要保护签名消息的隐私性，即盲签名。1983 年，Chaum[1]第一次提出了盲签名的概念。盲签名因其既有盲性的特点，又可以有效保护所签署消息的具体内容，所以在电子商务和电子选举等领域有着广泛的应用。

现实情况下，在数字签名中有时可能需要 2 个或 2 个以上的签名者对同一个消息的签名，实现多重数字签名。在 1996 年，Wu 等[2]提出了一种基于数学上素因子分解的有序多重数字签名方案，在有序多重数字签名中，签名者们对同一消息先后进行签名，并将最终的签名结果发送给验证者，验证者能够验证最后多重签名的正确性。当在实际应用中，消息的隐私还需要保密时，有

收稿日期：2014-11-10；**修回日期**：2015-05-12
基金项目：国家自然科学基金资助项目(61173187, 61173188, 11301002)；高等学校博士学科点专项科研基金资助项目(20133401110004)；安徽省自然科学基金资助项目(11040606M141, 1408085QF107)；安徽大学博士科研启动基金资助项目(33190187)；安徽大学“信息安全”新专业基金资助项目(17110099)
Foundation Items: The National Natural Science Foundation of China(61173187, 61173188, 11301002); Special Research Foundation of the Doctoral Program of Higher Education (20133401110004); The Natural Science Foundation of Anhui Province(11040606M141, 1408085QF107); Doctoral Research Project of Anhui University(33190187); Anhui University “Information security” New Professional Project(17110099)

序多重盲签名就是很好的选择。由此可以将多重数字签名和盲签名结合形成具有特殊用途的跨行支付签名方案。

传统的经典盲签名方案大多数是基于数学计算复杂度问题[3~6]，如大整数因子分解、离散对数。随着现代计算机的计算能力不断提高，特别是量子计算机的出现，这些经典的算法或协议将变得不安全。而基于量子物理特性的量子签名方案具有无条件安全性，量子密码技术的原理是基于量子力学性质，其安全性建立在量子不可克隆等定理的基础上。例如著名的 BB84 协议已经被证明是无条件安全的。自从 2001 年曾贵华教授首次提出利用 GHZ 三粒子纠缠态的仲裁签名方案[7,8]以来，对量子签名的研究引起越来越多学者们的关注。2001 年，Gottesman 等提出了一个基于量子单向函数的签名协议，其方案可以实现多个用户对同一消息的签名验证；Lee 等[9]提出了基于自动恢复原始消息的仲裁量子签名方案；2005 年，Lv 等[10]提出了一个基于 GHZ 三体纠缠态粒子和量子稳固码的量子签名方案；2007 年，Wen 提出了能够支持多个用户对同一消息进行的多重量子签名方案[11,12]，以及基于纠缠交换的量子有序多重数字签名方案[13]；2009 年，Wen 等[14]又提出了一个基于量子密码术的弱盲签名方案；2013 年，Wen 等[15]提出了一个跨行电子支付的量子代理盲签名方案。

随着越来越多的学者对量子签名的深入研究，涌现出许多量子签名方案和对量子签名的讨论[16~21]。然而，在已提出的上述签名方案中大多数是用于单用户签名，有的方案在验证时还需要仲裁的干预，签名的步骤冗余、量子酉变换较多，从而导致签名过程的繁琐，限制了量子签名的应用性。基于电子支付中的现实性需求，本文提出了一种量子有序双重盲签名协议，该签名协议实现了两方对同一消息的盲签名，在签名过程上较为简捷，验证方也不需要进行量子酉操作，减少了资源的消耗。另外，验证方面比现有方案在复杂度上有了较大的改进，验证的效率和验证的正确率有了明显的提升。协议中，由于转账支付是基于不同银行之间交易的事实，两方银行需要对顾客的账单信息进行有序盲签名，但并不知道所签名消息的具体内容，利用量子隐形传态的非局域性和量子纠缠交换特性，使可能处于遥远距离的顾客、银行和商家建立量子信息联系，达到盲签名的目的，协议并非基于传统经典的数学计算复杂度问题，其安全性由量子力学特性来保证。

2 基本原理

量子计算中 2 种基本单量子比特测量基。设 $\{|0\rangle,|1\rangle\}$ 是一组标准正交基，称为 B_Z，令

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$
$$|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{1}$$

则 $\{|+\rangle,|-\rangle\}$ 也构成一组正交基，称为 B_X。显然容易看出 2 组测量基 B_Z 和 B_X 之间是非正交的，也就是说如果用其中一组测量基去测量处于另外一组测量基状态的粒子，测量结果是随机不确定的。此外，由式(1)可以得到

$$|0\rangle=\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle)$$
$$|1\rangle=\frac{1}{\sqrt{2}}(|+\rangle-|-\rangle) \tag{2}$$

2.1 Bell 态和 GHZ 态

Bell 态是用于描述 2 个量子比特系统的 4 种最大纠缠态，4 种 Bell 态定义如下

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)$$
$$|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle) \tag{3}$$

Bell 态又称为 EPR 态或 EPR 对。容易推出 Bell 态又可写成

$$|\phi^{+}\rangle=\frac{1}{\sqrt{2}}(|++\rangle+|--\rangle)$$
$$|\phi^{-}\rangle=\frac{1}{\sqrt{2}}(|+-\rangle+|-+\rangle)$$
$$|\psi^{+}\rangle=\frac{1}{\sqrt{2}}(|++\rangle-|--\rangle)$$
$$|\psi^{-}\rangle=\frac{1}{\sqrt{2}}(|+-\rangle-|-+\rangle) \tag{4}$$

GHZ 三体纠缠态是三粒子系统的最大纠缠态，假设 3 个粒子分别由三方所拥有，根据 $B_Z=\{|0\rangle,|1\rangle\}$ 作为基矢量，GHZ 态可以表示如下

$$|\varphi\rangle=\frac{1}{\sqrt{2}}(|0_1 0_2 0_3\rangle+|1_1 1_2 1_3\rangle) \tag{5}$$

其中，下标 1、2、3 分别表示有三方拥有的 3 个粒子。

将式(1)和式(2)代入式(5)后，得到 GHZ 态表示如下

$$|\varphi\rangle=\frac{1}{2}(|+\rangle_1|+\rangle_2|+\rangle_3+|+\rangle_1|-\rangle_2|-\rangle_3+|-\rangle_1|-\rangle_2|+\rangle_3+|-\rangle_1|+\rangle_2|-\rangle_3) \quad (6)$$

式(6)说明粒子 1、2、3 之间存在着量子关联性，由于 GHZ 态的纠缠特性，当测量前 2 个粒子后，第 3 个粒子必然会坍塌，如果使用适当的测量基对其进行测量，则可以确定第 3 个粒子的状态，因此可以联合 2 个粒子的测量结果来判定剩下一个粒子的量子态。例如，当粒子 1 和粒子 2 采取 $B_X=\{|+\rangle,|-\rangle\}$ 测量，测量结果假设为 $|+\rangle$ 和 $|-\rangle$，那么粒子 3 在基 $B_X=\{|+\rangle,|-\rangle\}$ 下进行测量必然得到 $|-\rangle$；然而，如果粒子 3 选择在基 $B_Z=\{|0\rangle,|1\rangle\}$ 下进行测量，那么可以得到 $|0\rangle$ 和 $|1\rangle$ 的几率各为 50%，结果是随机的。

量子关联性的所有情形如表 1 所示。

表 1　　GHZ 态中粒子的量子关联性

粒子 1	粒子 2	粒子 3
$\|+\rangle$	$\|+\rangle$	$\|+\rangle$
	$\|-\rangle$	$\|-\rangle$
$\|-\rangle$	$\|+\rangle$	$\|-\rangle$
	$\|-\rangle$	$\|+\rangle$

2.2　量子隐形传态

量子隐形传态是一种基于量子特性的通信方式。它传输的是量子态所携带的量子信息，在量子纠缠的帮助下，待传输的量子态不需要任何载体的携带，而在另一个地方可以恢复量子态信息。

假设 *Alice* 和 *Bob* 分别拥有式(7)中一组 *EPR* 纠缠态的 2 个粒子

$$|\phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB} \quad (7)$$

此外 *Alice* 拥有要发送的消息粒子 *M* 态为

$$|\xi\rangle_M=(\alpha|0\rangle+\beta|1\rangle)_M \quad (8)$$

其中，$|\alpha|^2+|\beta|^2=1$。

如果 *Alice* 随机将自己手中一个处于 EPR 态的粒子做酉变换 σ_x，那么变换后的 EPR 粒子纠缠态为

$$|\psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{AB} \quad (9)$$

那么消息粒子 *M* 与两粒子纠缠 EPR 态所构成的组合态将是下列 2 种之一

$$|\Psi_1\rangle_{Mabc}=|\xi\rangle_M\otimes|\phi^+\rangle_{AB}=(\alpha|0\rangle+\beta|1\rangle)_M\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB} \quad (10)$$

$$|\Psi_2\rangle_{MAB}=|\xi\rangle_M\otimes|\psi^+\rangle_{AB}=(\alpha|0\rangle+\beta|1\rangle)_M\otimes\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{AB} \quad (11)$$

此时，*Alice* 要将粒子 *M* 的消息发送给接收者 *Bob*，那么可以把手中的 2 个粒子进行联合 Bell 测量，将粒子 *M* 的状态信息传送到 *Bob* 所拥有的粒子上。

式(10)和式(11)以另外一种方式表示为

$$\begin{aligned}|\Psi_1\rangle=\frac{1}{2}[&|\phi^+\rangle_{MA}(\alpha|0\rangle+\beta|1\rangle)_B+\\&|\phi^-\rangle_{MA}(\alpha|0\rangle-\beta|1\rangle)_B+\\&|\psi^+\rangle_{MA}(\alpha|1\rangle+\beta|0\rangle)_B+\\&|\psi^-\rangle_{MA}(\alpha|1\rangle-\beta|0\rangle)_B]\end{aligned} \quad (12)$$

$$\begin{aligned}|\Psi_2\rangle=\frac{1}{2}[&|\phi^+\rangle_{MA}(\alpha|1\rangle+\beta|0\rangle)_B+\\&|\phi^-\rangle_{MA}(\alpha|1\rangle-\beta|0\rangle)_B+\\&|\psi^+\rangle_{MA}(\alpha|0\rangle+\beta|1\rangle)_B+\\&|\psi^-\rangle_{MA}(\alpha|0\rangle-\beta|1\rangle)_B]\end{aligned} \quad (13)$$

其中，$|\phi^\pm\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),|\psi^\pm\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$。

最后，消息接收方 *Bob* 只需要对自己手中的粒子进行相应的酉变换即可恢复原始粒子 *M* 的信息，所有的情形如表 2 所示。

表 2　　为恢复消息 *Bob* 进行的酉变换

Alice 对粒子所做变换	*Alice* 测量结果	*Bob* 需要的酉变换
I	$\|\phi^+\rangle$	I
	$\|\phi^-\rangle$	σ_z
	$\|\psi^+\rangle$	σ_x
	$\|\psi^-\rangle$	$i\sigma_y$
σ_x	$\|\phi^+\rangle$	σ_x
	$\|\phi^-\rangle$	$i\sigma_y$
	$\|\psi^+\rangle$	I
	$\|\psi^-\rangle$	σ_z

从表 2 可以看出，*Bob* 只需要根据 *Alice* 先前对 EPR 粒子所做的变化和之后对粒子 *M* 和 EPR 粒子进行联合 Bell 基测量，从而对自己的粒子进行相对应的量子酉变换，就可恢复原始粒子 *M* 所携带的信息，即 $\alpha|0\rangle+\beta|1\rangle$。

3 协议描述

在本协议中，有 *Alice*、*Bob*、*Trent*1 和 *Trent*2 四方，*Alice* 为消息的持有方，*Trent*1 和 *Trent*2 为签名方，*Bob* 为签名验证方。不妨假设他们的角色如下。

Alice：顾客。她要向商家 *Bob* 通过银行电子支付系统支付账单，账单的具体内容是不愿意让银行看到的，所以她要对账单信息 *M*（*n* bit）进行盲化 *M'*，再请求银行方面进行签名，后期协助 *Bob* 对签名进行审计。

Bob：商家。商家接收顾客 *Alice* 发来的账单信息和银行方面关于支付账单的签名，并验证签名的有效性。

*Trent*1：银行方。*Alice* 的开户银行，负责接受 *Alice* 的跨行转账请求对电子现金进行签名，并通知要转账的银行。

*Trent*2：银行方。*Bob* 的开户银行，负责收到电子现金的转账信息，并对账单进行签名。

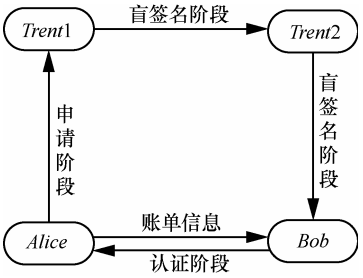


图 1 基于盲签名的跨行支付系统框架

3.1 初始化

1) 密钥分配：*Alice* 和 *Bob* 拥有用于他们之间通信的共享密钥 K_{AB}（*n* bit），*Alice* 和 *Trent*1 之间拥有共享密钥 K_{AT1}（*n* bit），*Bob* 和 *Trent*2 之间拥有共享密钥 K_{BT2}（3*n* bit），*Trent*1 和 *Trent*2 之间拥有共享密钥 K_{T1T2}（*n* bit），密钥分发可以通过量子密码的方法获得，如著名的 BB84 协议或 BBM92 协议。

2) 量子信道建立和粒子制备分发：*Trent*2 制备 *Q*(*Q*>*N*)对 GHZ 纠缠态粒子对，将每对 GHZ 对中的 2 个粒子分别发送给 *Trent*1 和 *Bob*，自己保留一个粒子。*Trent*2 随机选取 *Q*−*N* 对来检测信道，首先 *Trent*2 选用基 B_X 测量自己手中的 *Q*−*N* 个粒子，并将测量结果公布，随后 *Trent*1 也用基 B_X 测量自己手上对应的 *Q*−*N* 个粒子，并将结果公布，最后 *Bob* 在收到两方的测量结果后，同样用基 B_X 测量自己手上对应的粒子，如果三方之间的测量结果满足式(6)，则安全信道被建立。*Trent*1 制备 *Q*(*Q* > *N*)对 *EPR* 纠缠态粒子对，将每对 *EPR* 对中的 2 个粒子分别发送给 *Alice* 和 *Trent*2。检测信道的原理使用如上类似的方法。

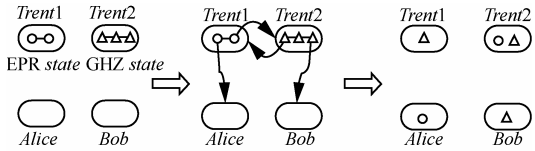


图 2 粒子分发方案

3) 签名申请：当消费者 *Alice* 要进行转账时，则向 *Trent*1 进行申请，并告知其转账的目的银行 *Trent*2。

3.2 盲签名阶段

1) 消息盲化

Step1 *Alice* 收到粒子后，根据自己的账单消息将其转化为经典比特序列 $M=\{m(1),m(2),\cdots,m(i),\cdots,m(n)\}$，$m(i)\in\{0,1\}$。

Step2 *Alice* 根据比特序列将手中粒子作为目标粒子进行 CNOT 门的相应变换，若 $m(i)=0$，则置控制粒子为 $|0\rangle$，若 $m(i)=1$，则置控制粒子为 $|1\rangle$。

Step3 *Alice* 将所有手中的粒子通过量子信道发送给 *Bob*，并将账单消息的比特序列通过密钥 K_{AB} 加密得到 $E_{K_{AB}}(M)$ 发送给 *Bob*。

这里，由于使用密钥 K_{AB} 和消息 *M* 均为 *n* 比特，因此采用一次一密的加密算法保证了无条件安全，随后的加密方法也使用了类似的原理。

2) 盲签名

Step1 *Trent*1 收到 *Alice* 的转账申请后，对手中的粒子进行基 $B_X=\{|+\rangle,|-\rangle\}$ 下的测量并记录下测量结果。

Step2 *Trent*1 将测量结果编码为经典比特序列 $T1=\{t1(1),t1(2),\cdots,t1(i),\cdots,t1(n)\}$，其中 $t1(i)\in\{0,1\}$，0 代表测量结果的 $|+\rangle$，1 代表 $|-\rangle$。然后 *Trent*1 将 *T*1 用密钥 K_{AT1} 进行加密得到 $E_{K_{AT1}}(T1)$，至此，*Trent*1

完成他对消息 M 的签名步骤，最后用密钥 K_{T1T2} 加密 $E_{K_{AT1}}(T1)$ 得到 $E_{K_{T1T2}}(E_{K_{AT1}}(T1))$，并将其发送给 *Trent*2 作为通知转账信息。

Step3 为了提供事后的验证依据，*Trent*1 还需将自己的测量结果 $T1$ 进行量子指纹函数[17]的变换

$$\left|f(T1)\right\rangle=\frac{1}{\sqrt{m}}\sum_{i=1}^{m}\left|i\right\rangle\left|E_i(T1)\right\rangle \tag{14}$$

接着，*Trent*1 用共享密钥 K_{AT1} 执行量子加密算法[18]，加密后的状态记 $E_{K_{AT1}}(\left|f(T1)\right\rangle)$，并将其通过量子信道发送给 *Alice*。

Step4 *Trent*2 收到通知转账信息 $E_{K_{T1T2}}(E_{K_{AT1}}(T1))$ 后，解密得到 *Trent*1 的签名 $E_{K_{AT1}}(T1)$，接着 *Trent*2 将自己手中的粒子对进行 *Bell* 基测量并记录测量结果。

Step5 随后 *Trent*2 将测量结果进行编码 $T2=\{t2(i),t2(i),\cdots,t2(i),\cdots,t2(n)\}$，其中，$t2(i)\in\{00,01,10,11\}$，00 代表测量结果的 $\left|\phi^+\right\rangle$，01 代表 $\left|\phi^-\right\rangle$，10 代表 $\left|\psi^-\right\rangle$，11 代表 $\left|\psi^-\right\rangle$。最后 *Trent*2 用密钥 K_{BT2} 加密 $E_{K_{AT1}}(T1)$ 和 $T2$ 得到 $E_{K_{BT2}}(E_{K_{AT1}}(T1),T2)$，并将其发送给 *Bob*，即为 *Trent*1 和 *Trent*2 对消息的盲签名。

3.3 签名验证阶段

Step1 *Bob* 收到签名 $E_{K_{BT2}}(E_{K_{AT1}}(T1),T2)$ 后解密得到 $E_{K_{AT1}}(T1)$ 和 $T2$，随后 *Bob* 公布序列 $E_{K_{AT1}}(T1)$，此时 *Alice* 先将其解密后，再根据恢复的 $T1$ 用式(14)进行量子指纹函数变换，得到 $\left|f(T1')\right\rangle$，接着将其与之前从 *Trent*1 接收到的 $\left|f(T1)\right\rangle$ 进行比较，若相等则通知 *Bob* 信息无误通过审计，并将 $T1$ 发送给 *Bob*，如不相等则审计不通过，通知 *Bob* 拒绝签名。

Step2 若 *Bob* 收到 *Alice* 签名通过审计的消息，则将手中的粒子对进行 *Bell* 基测量并记录测量结果。

Step3 *Bob* 将测量结果进行编码 $B=\{b(i),b(i),\cdots,b(i),\cdots,b(n)\}$，其中，$b(i)\in\{00,01,,10,11\}$，00 代表测量结果的 $\left|\phi^+\right\rangle$，01 代表 $\left|\phi^-\right\rangle$，10 代表 $\left|\psi^-\right\rangle$，11 代表 $\left|\psi^-\right\rangle$。然后 *Bob* 将三方的测量结果进行对比验证，验证规则如表 3 和表 4 所示。

表 3　验证规则 1

*Trent*1 测量及编码序列 $T1$	*Trent*2 测量及编码序列 $T2$	*Bob* 测量及编码序列 B
$\left\|+\right\rangle$,0	$\left\|\phi^+\right\rangle$,00	$\left\|\phi^+\right\rangle$,00
	$\left\|\phi^-\right\rangle$,01	$\left\|\phi^-\right\rangle$,01
	$\left\|\psi^+\right\rangle$,10	$\left\|\psi^+\right\rangle$,10
	$\left\|\psi^-\right\rangle$,11	$\left\|\psi^-\right\rangle$,11
$\left\|-\right\rangle$,1	$\left\|\phi^+\right\rangle$,00	$\left\|\phi^-\right\rangle$,01
	$\left\|\phi^-\right\rangle$,01	$\left\|\phi^+\right\rangle$,00
	$\left\|\psi^+\right\rangle$,10	$-\left\|\psi^-\right\rangle$,11
	$\left\|\psi^-\right\rangle$,11	$-\left\|\psi^+\right\rangle$,10

表 4　验证规则 2

*Trent*1 测量及编码序列 $T1$	*Trent*2 测量及编码序列 $T2$	*Bob* 测量及编码序列 B
$\left\|+\right\rangle$,0	$\left\|\phi^+\right\rangle$,00	$\left\|\psi^+\right\rangle$,10
	$\left\|\phi^-\right\rangle$,01	$-\left\|\psi^-\right\rangle$,11
	$\left\|\psi^+\right\rangle$,10	$\left\|\phi^+\right\rangle$,00
	$\left\|\psi^-\right\rangle$,11	$-\left\|\phi^-\right\rangle$,01
$\left\|-\right\rangle$,1	$\left\|\phi^+\right\rangle$,00	$-\left\|\psi^-\right\rangle$,11
	$\left\|\phi^-\right\rangle$,01	$\left\|\psi^+\right\rangle$,10
	$\left\|\psi^+\right\rangle$,10	$\left\|\phi^-\right\rangle$,01
	$\left\|\psi^-\right\rangle$,11	$-\left\|\phi^+\right\rangle$,00

Step4 若三方测量结果通过表 3 和表 4 中规则验证。则 *Bob* 可以依次将自己编码序列恢复为原始消息：如果测量结果和编码满足表 3 的规则，则记录比特 0，如果测量结果和编码满足表 4 的规则，则记录比特 1，记录完成后为 $M'=\{m'(1),m'(2),\cdots,m'(i),\cdots,m'(n)\}$，$m'(i)\in\{0,1\}$。此时 *Bob* 将之前从 *Alice* 得到的原始消息 M 进行对比验证，若 $M=M'$，则确认签名为有效签名，否则拒绝签名。

4 协议分析

4.1 签名的盲性

在本协议的盲签名阶段中，签名者 *Trent*1 和 *Trent*2 进行签名时无法知道消息拥有者 *Alice* 的账单信息。因为 *Alice* 仅仅只是根据账单信息 M 对自己手中粒子进行 CNOT 门变换，使用的相应变换规则也不公开，而且账单信息 M 除了使用一次一密的加密算法后直接发送给 *Bob* 外，并不对任何人泄露。

因此 *Trent*1 是不可能由自己的粒子态或其他方法得知 *Alice* 的消息，而 *Trent*2 虽然拥有 EPR 态的另一组粒子，但也不可能由自己的粒子得到任何信息，因为 *Alice* 对粒子进行的 CONT 门操作并不影响 *Trent*2 手中的粒子，而且一旦 *Trent*2 对粒子进行测量的话，那么就会发生不可逆的坍塌，随后的签名也就将无法继续。所以 *Trent*1 和 *Trent*2 都不可能知道 *Alice* 的账单信息。因此签名具有盲性。

4.2 协议的安全性

4.2.1 经典安全性

信息和签名的安全。在本文的协议中，支付信息和签名信息都具有GHZ三体纠缠态粒子间的关联性，因此一旦被攻击者截获和篡改都会通不过验证。此外，所有针对经典信息的加密算法都是采用一次一密的加密算法，因此签名也是无条件安全的。

1) 不可伪造

首先，攻击者不可能伪造签名。第一，假设攻击者攻击了 *Trent*1 并且获得 *T*1，但由于没有 *Trent*2 手中处于 EPR 态和 GHZ 态的粒子，它将无法进行后续的签名，如果伪造了签名，那么在最后 *Bob* 的验证阶段一定不会通过；第二，假设攻击者攻击了 *Trent*2 并获得 *T*2，但由于无法获取 *T*1，所以即使伪造了编码签名也可不可能通过最后 *Alice* 的审计。

其次，*Trent*1 和 *Trent*2 不可能伪造签名。第一，*Trent*1 不可能伪造签名，如果 *Trent*1 伪造了测量编码序列并进行相应的操作，那么虽然可以通过最后 *Alice* 的审计，但依然无法通过 *Bob* 的对比验证，这是因为处于量子 EPR 态和 GHZ 态粒子纠缠相关性决定的；第二，*Trent*2 不可能在没有接收到 *Trent*1 转账通知的情况下进行签名，因为签名中必须包含 *Trent*1 的加密测量编码序列 *T*1，*T*1 使用 *Trent*1 和 *Alice* 之间的共享密钥加密，所以对 *Trent*1 和 *Alice* 可见对 *Trent*2 不可见，而且最后序列 *T*1 要通过 *Bob* 的对比验证；第三，假如 *Trent*2 在收到 *Trent*1 的加密序列的情况下利用伪造的测量编码来进行伪造签名，那么签名可以通过先期 *Alice* 的审计，但依然无法通过最后的验证，因为最后的验证仍然是通过 GHZ 三体纠缠态粒子之间的关联性进行对比检验，如果 *Trent*2 不是进行正确的测量编码，那么编码后的序列将通不过表 3 和表 4 的验证规则。

2) 不可抵赖

*Trent*2 不可能抵赖签名。首先，*Trent*2 在签名之前收到 *Trent*1 的加密序列，序列中包含 *Trent*1 的测量编码；其次，*Bob* 也将收到来自 *Trent*2 的签名，而且此签名用两者共享的密钥加密，实际上，在这个文件中就已经有了 *Trent*2 的记录，签名中包含自己的测量编码结果，一旦发生争执，*Bob* 可向 *Alice* 发出申请，*Trent*2 任何抵赖签名的行为都会被 *Trent*1 质疑，因为 *Trent*1 只将加密序列发送给了 *Trent*2。

4.2.2 量子安全性

本方案采用的是一次一密加密算法（QTP），而这些密钥的获得都采用著名的 BB84 或 BBM92 密钥分配协议（QKD）。如果攻击者采取中间人的攻击方式进行消息的篡改或签名的冒充是不可能的。

1) 假设攻击者可能会在信道采取中间人截获和重发的攻击策略进行攻击，在实际情形下，信道也会有一定的噪声，但这些都会对处于纠缠的量子态产生扰动而被发现，可采用初始化时建立量子信道的方法检测信道的安全性。如果三方的测量结果没有相干性，则信道中可能存在攻击者窃听，所以通信三方可事先约定阈值 c，假设测量 i 组纠缠态粒子，其中没有量子相干性的粒子组数为 j，当 $\frac{j}{i}<c$ 时，则可认为测量的错误是由一般的噪声产生，可以在本方案的适用范围内。

2) 假设攻击者 *Eve* 会想办法通过自己的一些量子操作来获得部分签名信息，假设消息比特是 0 的情况下，若 *Eve* 使用纠缠共享粒子方法攻击，则可以把攻击者 *Eve* 与签名粒子纠缠态的总系统表示为

$$|\Psi\rangle=(\alpha_1|00\rangle+\beta_1|11\rangle)_{12}\otimes (\alpha_2|000\rangle+\beta_2|111\rangle)_{456}|\eta\rangle_e \tag{15}$$

事实上，攻击者 *Eve* 将会进行一些量子操作来降低自己被三方检测出来的概率，如果它将 CNOT 门 C_{6e} 作用到这个总量子纠缠系统，那么得到的系统状态为

$$C_{6e}|\Psi\rangle=(\alpha_1\alpha_2|00\,000\rangle_{12\,456}+\beta_1\alpha_2|11\,000\rangle_{12\,456})|\eta\rangle_e+(\alpha_1\beta_2|00\,111\rangle_{12\,456}+\beta_1\beta_2|11111\rangle_{12\,456})|\eta\oplus 1\rangle_e \tag{16}$$

如果攻击者 *Eve* 为了将出现没有用的量子信息概率降低到可以被接受的门限范围 δ 之内，那么它还应该使量子态 $|\eta\rangle$ 满足

$$(\alpha_1^2\beta_2^2+\beta_1^2\beta_2^2)(\langle\eta|\eta\rangle)\geqslant 1-\delta \tag{17}$$

在这样的情况下，攻击者 *Eve* 能够获取到纠缠系统的正确信息概率为

$$P_e = (\alpha_1^2\beta_2^2 + \beta_1^2\beta_2^2)(\langle\eta|\eta\rangle) \tag{18}$$

根据量子信息论，此时 *Eve* 和纠缠粒子之间的交互信息量可以表示为

$$I(E,|\Psi\rangle) = 1 - H(P_e) \tag{19}$$

其中，$H(P_e)$ 表示二元 Shannon 熵，并且有 $H(x) = -x\mathrm{lb}x - (1-x)\mathrm{lb}(1-x)$，当 *Eve* 为了最大程度地获取量子系统的信息时，门限范围值 δ 应该无限接近于 $\frac{1}{2}$，那么 *Eve* 被发现到的概率也接近等于 $\frac{1}{2}$，这已经足以让正常用户能够检测到攻击者 *Eve* 的侵入行为。

3) 假设攻击者 *Eve* 可能会攻击签名者随机的检测粒子信息，那么它单方猜测成功的概率应为 $\frac{1}{2}$，被检测到的概率为 $\frac{1}{2}$。由于在前面介绍，检测光子是随机在量子粒子对中选取的，所以对攻击者来说，正确获取检测光子位置的概率为 $\frac{1}{Q}$，这对于 *Eve* 来说也是相当困难的。

另外，可以根据粒子的基本信息计算出二元 von Neumann 信息熵

$$S(\rho_\psi) = -tr(\rho_\psi \mathrm{lb}\rho_\psi) \tag{20}$$

其中，$\rho_\psi = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$，当 $|\alpha| = |\beta| = \frac{1}{\sqrt{2}}$ 时，二元 von Neumann 信息熵有最大值 $S(\rho_\psi) = \mathrm{lb}2 = 1\ \mathrm{bit}$，这表示纠缠量子态的不确定程度，也就是说当攻击者 *Eve* 即使获得一部分系统量子信息也无法恢复出原始消息。

通过建立安全的量子信道，利用对纠缠态粒子组的变换和测量，实现了盲化信息和签名，这种粒子之间的关联性是基于量子态物理特性的安全，是不受空间和时间限制的，因此具有无条件安全性。

4.3　性能分析

分析本协议的量子代理盲签名效率需要考虑盲签名阶段和签名验证阶段的代价和复杂度。协议中认为 *Trent*1 和 *Trent*2 是相互独立，不能联合欺骗的，所以一旦其中一方有不诚实行为，将会破坏粒子之间的纠缠关系，*Bob* 可以通过粒子的纠缠态特性验证签名是很容易揭发欺骗行为，因此只需验证表 3 和表 4 的几种对应关系，复杂度较低。

特别地，与 Wen 等人提出的量子单重盲签名方案[15]相比，验证过程的效率得到了明显的提高：在随机概率的情形下，Wen 等每次验证要先进行预比较，然后进行编码的验证比较，验证过程总共要进行两重循环比较，验证开支较大，而本协议的验证规则是一重比较，没有对签名验证毫无用处的预比较环节，而是直接进行签名的编码验证比较，验证开支有了明显的降低。

另外，Wen 协议中用于验证签名正确性的对应比较关系为 8 种，占对应关系总数的 $\frac{1}{2}$，而本协议中所有的对应关系皆用于验证签名，占随机概率情形下总数的 100%，因此在随机概率的情况下，本协议验证签名的正确率比前者要高，在验证上没有误判率。表 5 比较了本文和其他 2 个量子单重盲签名协议的特点。

表 5　　协议对比

特点	文献[16]协议	文献[15] 协议	本文协议
量子资源	*n* 对 EPR 态和 *2n* 对六粒子纠缠态	*n* 对三粒子纠缠态	*n* 对 GHZ 态和 *n* 对 EPR 态
签名用户数量	1 个	1 个	2 个
验证方酉变换	需要	不需要	不需要
签名长度	4*n* bit 经典比特	3*n* bit 经典比特	3*n* bit 经典比特
消息恢复功能	有	无	有
验证开支	一重比较	两重比较	一重比较
签名验证比特正确率	100%	50%	100%

5　结束语

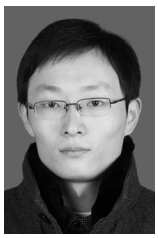
结合现实情况下电子商务的需求，本文提出了一个基于量子有序多重盲签名的跨行支付协议。协议基于量子 GHZ 态和 EPR 态的相干性及量子纠缠交换的物理特性，与以往一些提出的量子签名相比，本协议不依赖于仲裁，所以有着较高的安全性和通信效率。特别是首次提出了两方签名者对同一消息的有序双重盲签名，对于实际情形下的跨行电子支付有一定的应用背景。此外，验证方仅仅需要进行粒子测量，不必进行任何量子酉变换，并且通过测量结果可以恢复出原始消息，验证时也只需要进行经典比特的比对验证，与一些经典的量子单重盲签名方案相比，除了增加了签名用户数量，在验证效率和验证正确率上也有着明显的优势。

参考文献：

[1]　CHAUM D. Blind signatures for untraceable payments[A]. Advances

in Cryptology[C]. Springer US, 1983. 199-203.
[2] TZONGCHEN W, SHULIN C, TZONG-Sun W. Two-based multisi gnature protocols for sequential and broadcasting architecture[J]. Computer Communications, 1996, 19(9/10): 851-856.
[3] CHIEN H Y, JAN J K, TSENG Y M. RSA-based partially blind signature with low computation[A]. Parallel and Distributed Systems, Proceedings Eighth International Conference on[C]. 2001. 385-389.
[4] TRAORE J. Group signatures and the irrelevance to privacy-protecting off-line electronic cash systems[A]. Australasian Conference on Information Security and Privacy[C]. Springer-Verlag，1999.228-243.
[5] JEONG I R, LEE D H, LIM J I. Efficient transferable cash with group signatures[M]. Springer Berlin Heidelberg, 2001.462-474.
[6] MAITLAND G, BOYD C. Fair Electronic Cash Based on a Group Signature Scheme[M]. Springer Berlin Heidelberg, 2001.461-465.
[7] ZENG G, MA W, WANG X, *et al*.Signature scheme based on quantum cryptography[J].Acta Electronica Sinica, 2001, 29(8):1098-1100.
[8] ZENG G, KEITEL C H. Arbitrated quantum-signature scheme[J]. Physical Review A, 2002, 65(4): 042312.
[9] LEE H, HONG C, KIM H, *et al*. Arbitrated quantum signature scheme with message recovery[J]. Physics Letters A, 2004, 321(5): 295-300.
[10] LV X, FENG D G. An arbitrated quantum message signature scheme[M]. Springer Berlin Heidelberg, 2005.1054-1060.
[11] WEN X J, LIU Y, SUN Y. Quantum multi-signature protocol based on teleportation[J]. Zeitschrift fur Naturforschung A, 2007, 62(3/4): 147-151.
[12] WEN X J, LIU Y. Secure authentic digital signature scheme using quantum fingerprinting[J]. Chinese Journal of Electronics, 2008, 17(2): 340-344.
[13] WEN X J, LIU Y. A realizable quantum sequential multi-signature scheme[J]. Acta Electronica Sinica, 2007, 35(6): 1079-1083.
[14] 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.
[15] 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.
[16] CAO H J, ZHU Y Y, LI P F. A quantum proxy weak blind signature scheme[J]. International Journal of Theoretical Physics, 2014, 53(2): 419-425.
[17] BUHRMAN H, CLEVE R, WATROUS J, *et al*. Quantum fingerprinting[J]. Physical Review Letters, 2001, 87(16): 167902.
[18] NAN R Z, GUI H Z. A realizable quantum encryption algorithm for qubits[J]. Chinese Physics, 2005, 14(11): 2164.
[19] YANG C W, HWANG T, LUO Y P. Enhancement on quantum blind signature based on two-state vector formalism"[J]. Quantum Information Processing, 2013, 12(1): 109-117.
[20] ZOU X F, QIU D W. Attack and improvements of fair quantum blind signature schemes[J]. Quantum Information Processing, 2013, 12(6): 2071-2085.
[21] KHODAMBASHI S, ZAKEROLHOSS EINI A. A sessional blind signature based on quantum cryptography[J]. Quantum Information Processing, 2014, 13(1): 121-130.

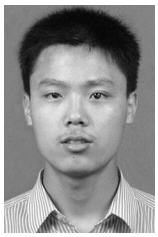
作者简介：



王辉（1989-），男，安徽合肥人，安徽大学硕士生，主要研究方向为信息安全和量子密码。

石润华[通信作者]（1974-），男，安徽安庆人，安徽大学教授，主要研究方向为可证明安全的量子密码、保护隐私的多方协作计算和无线网络安全。E-mail:shrh@ahu.edu.cn。

仲红（1965-），女，安徽宿州人，安徽大学教授，主要研究方向为网络与信息安全。



崔杰（1983-），男，河南淮阳人，安徽大学讲师，主要研究方向为网络与信息安全。

张顺（1982-），男，安徽安庆人，安徽大学讲师，主要研究方向为信息计算复杂性、高振荡问题易处理性和量子框架计算。

汪开婷（1992-），女，安徽芜湖人，安徽大学硕士生，主要研究方向为信息安全和密码学。