基于弱非线性实现量子信息签名*

丁东[1)2)] 闫凤利[2)†]

1) (华北科技学院基础部, 北京 101601)

2) (河北师范大学物理科学与信息工程学院, 石家庄 050024)

(2012 年 5 月 28 日 收到; 2012 年 8 月 7 日 收到修改稿)

基于弱非线性及对称量子密码体系提出了一个量子信息签名方案. 信息发送方可以发送消息给接收方并且能够判断信息是否被敌手修改或换掉. 一旦验证签名成功, 依赖于一个忠实的公证人, 通信双方对信息的发送或接收都不能否认.

关键词: 量子隐形传态, 弱非线性, 信息签名

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.62.010302

1 引 言

近年来, 量子信息学迅速发展, 特别是在量子密码术 [1,2]、量子稠密编码 [3]、量子隐形传态 [4]、量子签名 [5−7] 等方面. 与量子密码术一样, 基于量子力学原理的量子签名相对传统的经典签名具有独特的优势, 进而具有非常重要的研究价值. 在实际应用中, 量子签名可以保证信息的真实性, 并且还可以有效地防止通信双方中的任何一方抵赖 [8,9].

用光学方案实现量子纠缠 [10−12] 已取得了很大的进展, 特别地, 基于 cross-Kerr 非线性介质 [13,14], 人们可以构造量子非破坏性测量 [15−20], 用于产生具有偏振和空间自由度纠缠的 hyperentanglement[21,22]. 除了直接用于构造 entangler[17], 量子非破坏性测量技术还可以用于实现可控的量子隐形传态 [23], 从而降低了用光学方法实现联合 Bell 基测量的难度. 然而, cross-Kerr 介质本身的非线性非常弱 [24,25], 即使通过电磁感应透明技术也只是改进到 $\theta \approx 10^{-2}$ 数量级 [26,27]. 所以, 在非线性相互作用过程中如果同时引入相位角 θ 和 $-\theta$ 必然存在实现上的困难 [18], 这个问题可以通过引入一个额外的相位门并巧妙地设计量子线路 [28,29] 得以解决.

本文提出一个基于弱非线性实现量子信息签名方案, 在各参与方都诚实的前提下, 方案可以有效地验证所传输信息的真实性, 如果信息签名成功, 通信双方中的任何一方都不可以否认已经发送或者接收了该信息, 或者说对通信的合法性加以保护.

2 物理原理

2.1 量子非破坏性测量

量子非破坏性测量可以用 cross-Kerr 非线性介质实现, 该介质对由信号光子和相干态 (探针光束) 组成的复合系统进行演化, 其 Hamiltonian 为 [30]

$$H = \hbar\chi \hat{a}_{\mathrm{s}}^{\dagger}\hat{a}_{\mathrm{s}}\hat{a}_{\mathrm{p}}^{\dagger}\hat{a}_{\mathrm{p}}, \tag{1}$$

其中, $\hat{a}_{\mathrm{s}}^{\dagger}$, $\hat{a}_{\mathrm{s}}$(或 $\hat{a}_{\mathrm{p}}^{\dagger}$, $\hat{a}_{\mathrm{p}}$) 为信号光子 (或相干态) 的产生和湮灭算子, χ 是介质的耦合强度. 具体地说, 如果信号光子 (信号模) 处于态 $|\varphi\rangle_{\mathrm{s}} = a|0\rangle_{\mathrm{s}} + b|1\rangle_{\mathrm{s}}$, 相干态 (探针模) 为 $|\alpha\rangle_{\mathrm{p}}$, 那么经过 cross-Kerr 非线性介质作用后整个系统将演化为

$$|\psi\rangle_{\mathrm{sp}} = a|0\rangle_{\mathrm{s}}|\alpha\rangle_{\mathrm{p}} + b|1\rangle_{\mathrm{s}}\left|\alpha \mathrm{e}^{\mathrm{i}\theta}\right\rangle_{\mathrm{p}}, \tag{2}$$

* 国家自然科学基金 (批准号: 10971247)、河北省自然科学基金 (批准号: A2012205013, A2010000344) 和中央高校基本科研业务费专项资金 (批准号: 2011B025) 资助的课题.

† 通讯作者. E-mail: flyan@hebtu.edu.cn

这里 $\theta=\chi t$ (t 表示相互作用时间). 注意到系统演化后的结果是信号模没有发生变化, 而与信号光子相联系的相干态在信号模存在光子的情况下产生了一个相位变化. 所以, 通过对相干态的测量可以判断信号模是否有光子存在, 同时投影信号光子态到不同的子空间.

2.2 基于量子非破坏性测量的可控量子隐形传态

首先, 我们简要地介绍一下周建等 [23] 提出的可控量子隐形传态方案. 在该方案中, 信息发送方 Alice 欲传送一个未知的单光子态

$$|\varphi\rangle_i=a|H\rangle_i+b|V\rangle_i,\quad |a|^2+|b|^2=1 \tag{3}$$

给信息接收方 Bob, 量子信道为三光子 GHZ 态

$$|\psi\rangle_{\mathrm{ABC}}=\frac{1}{\sqrt{2}}(|HHH\rangle+|VVV\rangle)_{\mathrm{ABC}}, \tag{4}$$

其中, 通信双方 Alice, Bob 及控制方 Charlie 分别拥有光子 A, B 及 C. 首先, Alice 将自己拥有的两个光子 (欲传送的未知单光子和三光子 GHZ 态中的一个光子) 作为信号模, 同时引入相干态 $|\alpha\rangle$ 作为探针模, 利用 cross-Kerr 非线性介质及 X-quadrature 测量构造两光子的 parity-gate[17], 根据 Alice 公布的测量结果及适当的相位门操作, 最终使复合系统投影到两个可区分的子空间. 随后, Alice 和 Charlie 在算子 $\hat{\sigma}_x$ 的本征基矢下各自对自己拥有的光子实施测量并公布测量结果. Bob 根据 Alice 和 Charlie 公布的测量结果对自己拥有的光子进行适当的单光子幺正变换就可以得到 Alice 所传送的未知单光子态. 显然, 如果控制方 Charlie 不公布测量结果, Bob 就不能采取适当的幺正变换恢复出传送的单光子态, 从而实现第三方可控的量子隐形传态.

为了避免在弱非线性相互作用过程中引入较大的相位角 (相对于较小的相位角 θ, 考虑到 $-\theta$ 很大), 我们采用 double cross-phase modulation 方法 [19,20,29] 对非线性相互作用及测量过程做适当改进, 实验装置如图 1 所示. 图中, 偏振光束分束器 (PBS) 的作用是使水平偏振光通过, 而垂直偏振光被反射; 50 : 50 独立于偏振的分束器 (BS) 对入射光的演化满足:

$$\hat{a}_{\mathrm{in}}^{\dagger}=\frac{1}{\sqrt{2}}\left(\hat{a}_{\mathrm{out}}^{\dagger}-\hat{b}_{\mathrm{out}}^{\dagger}\right),$$

$$\hat{b}_{\mathrm{in}}^{\dagger}=\frac{1}{\sqrt{2}}\left(\hat{a}_{\mathrm{out}}^{\dagger}+\hat{b}_{\mathrm{out}}^{\dagger}\right),$$

其中 $\hat{a}_{\mathrm{in}}^{\dagger}$, $\hat{b}_{\mathrm{in}}^{\dagger}$ ($\hat{a}_{\mathrm{out}}^{\dagger}$, $\hat{b}_{\mathrm{out}}^{\dagger}$) 分别代表两个不同的输入 (输出) 模的产生算子. θ 表示信号模光子与相干态通过 cross-Kerr 非线性介质相互作用产生的相位变化, $-\theta$ 表示一个单光子相位门. 一个投影测量 ($|n\rangle\langle n|$) 及经典反馈信息 ($\phi(n)$) 用于投影复合系统到两个可区分的子空间.

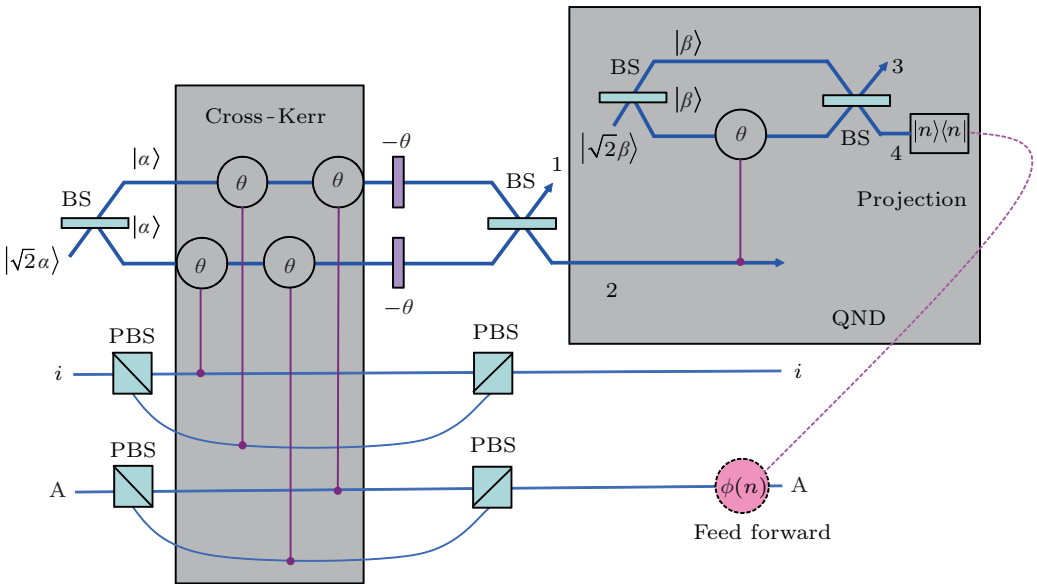

图 1 量子非破坏性测量装置

具体地, 以三光子 GHZ 态

$$|\psi\rangle_{\mathrm{ABC}}=\frac{1}{\sqrt{2}}(|HHV\rangle+|VVH\rangle)_{\mathrm{ABC}} \tag{5}$$

为例, Alice 将自己拥有的光子 i 和 A 作为信号模与相干态 $|\alpha\rangle|\alpha\rangle$ 经 cross-Kerr 非线性介质发生相互作用. 然后, 将相干态经 BS 作用, 整个复合系统演化过程为

$$\begin{aligned}
&|\varphi\rangle_i|\psi\rangle_{\mathrm{ABC}}|\alpha\rangle|\alpha\rangle\\
\rightarrow&\frac{1}{\sqrt{2}}(a|HHHV\rangle+b|VVVH\rangle)_{i\mathrm{ABC}}|\alpha\rangle|\alpha\rangle\\
&+\frac{1}{\sqrt{2}}\Big(a|HVVH\rangle_{i\mathrm{ABC}}\Big|\alpha\mathrm{e}^{-\mathrm{i}\theta}\Big\rangle\Big|\alpha\mathrm{e}^{\mathrm{i}\theta}\Big\rangle\\
&+b|VHHV\rangle_{i\mathrm{ABC}}\Big|\alpha\mathrm{e}^{\mathrm{i}\theta}\Big\rangle\Big|\alpha\mathrm{e}^{-\mathrm{i}\theta}\Big\rangle\Big)\\
\rightarrow&\frac{1}{\sqrt{2}}(a|HHHV\rangle+b|VVVH\rangle)_{i\mathrm{ABC}}|0\rangle\Big|\sqrt{2}\alpha\Big\rangle\\
&+\frac{1}{\sqrt{2}}\Big(a|HVVH\rangle_{i\mathrm{ABC}}\Big|-\mathrm{i}\sqrt{2}\alpha\sin\theta\Big\rangle\\
&+b|VHHV\rangle_{i\mathrm{ABC}}|\mathrm{i}\sqrt{2}\alpha\sin\theta\rangle\Big)\Big|\sqrt{2}\alpha\cos\theta\Big\rangle.
\end{aligned}\tag{6}$$

再引入足够强的相干态 $|\beta\rangle|\beta\rangle$, 经 BS 作用后对光路 4 进行间接光子数分辨测量 $|n\rangle\langle n|$ 实现量子非破坏性测量. 当投影测量结果为 $n=0$ 时, 得到四光子态

$$|\psi\rangle_{i\mathrm{ABC}}=a|HHHV\rangle_{i\mathrm{ABC}}+b|VVVH\rangle_{i\mathrm{ABC}}; \tag{7}$$

当投影测量结果为 $n\neq 0$ 时, 根据反馈的具体测量值 n 对光子 A 做一个适当的相位转换 $\phi(n)=n\pi/2$ 得到四光子态

$$|\psi\rangle_{i\mathrm{ABC}}=a|HVVH\rangle_{i\mathrm{ABC}}+b|VHHV\rangle_{i\mathrm{ABC}}. \tag{8}$$

表 1 测量结果及所对应的幺正操作

光子 i 和 A 测量结果	光子 C 测量结果	用于恢复量子态而对 B 的幺正操作
$\|+\rangle_i\|+\rangle_{\mathrm{A}}$ 或 $\|-\rangle_i\|-\rangle_{\mathrm{A}}$	$\|+\rangle_{\mathrm{C}}$	$\hat{I}$
$\|+\rangle_i\|-\rangle_{\mathrm{A}}$ 或 $\|-\rangle_i\|+\rangle_{\mathrm{A}}$	$\|-\rangle_{\mathrm{C}}$	
$\|+\rangle_i\|+\rangle_{\mathrm{A}}$ 或 $\|-\rangle_i\|-\rangle_{\mathrm{A}}$	$\|-\rangle_{\mathrm{C}}$	$\hat{\sigma}_z$
$\|+\rangle_i\|-\rangle_{\mathrm{A}}$ 或 $\|-\rangle_i\|+\rangle_{\mathrm{A}}$	$\|+\rangle_{\mathrm{C}}$	

值得注意的是, (8) 式所示的态可以通过对光子 A, B 以及 C 的偏振进行翻转得到态 (7). 接下来, 以 (7) 式为例, 注意到 $\hat{\sigma}_x|\pm\rangle=\pm|\pm\rangle$, 其中, $|\pm\rangle=\frac{1}{\sqrt{2}}(|H\rangle\pm|V\rangle)$ 是算子 $\hat{\sigma}_x$ 的两个本征态, Alice 在算子 $\hat{\sigma}_x$ 的本征基矢下对光子 i 和 A 实施测量, Charlie 在算子 $\hat{\sigma}_x$ 的本征基矢下对光子 C 实施测量. 如果 Alice 和 Charlie 公布测量结果, 在仅差一个幺正变换的情况下 Bob 就得到了要传送的未知量子态 $|\varphi\rangle_i=a|H\rangle_i+b|V\rangle_i$. 测量结果及所对应的用于恢复量子态而对 B 的幺正操作见表 1.

3 量子签名方案

方案中涉及通信双方, 即信息发送方 Alice, 信息接收方 Bob 和公证人 Charlie. 为了实现发送消息

$$M=\{M_i\},\quad M_i=0,1 \tag{9}$$

给 Bob 并对消息进行有效地签名, Alice 首先利用她和 Bob 之间的密钥 K_{ab} 加密消息的一个备份, 得到消息的密文 $S_{\mathrm{ab}}=K_{\mathrm{ab}}(\{M_i\})$, 然后根据要发送的消息制备单光子态集合

$$\begin{aligned}
&|\phi\rangle=\{|\phi\rangle_i\},\\
&|\phi\rangle_i=c_i(|H\rangle_i+m_i|V\rangle_i),\\
&m_i=-1,1,0,
\end{aligned}\tag{10}$$

其中 $|H\rangle$ 和 $|V\rangle$ 分别代表光子的水平和垂直偏振态, $m_i=-1$, 1 分别对应经典信息 0 和 1, $m_i=0$ 表示用于安全性检测的样品粒子不对应经典信息, c_i 为归一化常数.Alice 首先发送密文 S_{ab} 给 Bob, Bob 利用 K_{ab} 解密 S_{ab} 得到明文 M 作为原始未被签名的信息. 然后, 利用三光子最大纠缠态 GHZ 态作为量子信道, 在通信双方 Alice 和 Bob 以及公证人 Charlie 的共同参与下, Bob 得到消息 M', 最后 Bob 对 M 和 M' 逐一比对, 若结果完全一致, 信息签名成功, 否则签名失败, 选择放弃本次通信. 为了防止事后通信双方抵赖, 方案中引入忠实的公证人 Charlie, 因为有 Charlie 及包含个人信息的密钥的存在, 一旦签名成功, 通信双方中的任何一方都不可以否认已经发送或者接收了该信息.

3.1 密钥分发及密文的发送

通过目前已经成熟的密钥分配方案 [1], Alice 和 Bob 各自获得与 Charlie 之间的密钥 K_{ac} 和 K_{bc} 及 Alice 和 Bob 之间的密钥 K_{ab}. Alice 利用密钥 K_{ab} 加密消息的一个备份, 得到消息的密文 S_{ab} 并发送给 Bob.

3.2 制备量子信道

当 Alice 要给 Bob 传送未知量子态时, 双方分

别利用密钥 K_{ac} 和 K_{bc} 通过经典信道向 Charlie 提出申请. Charlie 收到申请后, 首先利用密钥 K_{ac} 和 K_{bc} 确认 Alice 和 Bob 的身份, 然后, 利用高效的三光子 GHZ 态产生装置 [29], 制备三光子最大纠缠态 $|\psi\rangle_{ABC}$, 并将光子 A 和 B 分别分发给 Alice 和 Bob, 自己拥有光子 C. Alice 和 Bob 收到光子后三方进行必要的安全性检测 [31,32].

3.3 量子信息签名

以第 i 个未知单光子态为例, 我们给出依赖于忠实的公证人的量子签名过程. 为了便于理解, 我们这里只给出 $m_i=-1,1$ 情况, 对于 $m_i=0$, 即用于安全性检测的样品粒子情况将在安全性分析部分讨论.

1) Alice 首先将自己拥有的光子 i (将要传送的某个未知量子态) 和光子 A (三光子 GHZ 态中的一个) 作为信号模通过 cross-Kerr 非线性介质与相干探针束 $|\alpha\rangle|\alpha\rangle$ 发生相互作用 [19,20]. Alice 先对探针束进行间接光子数分辨测量 $|n\rangle\langle n|$ 投影复合系统 [29], 并通过经典信道广播测量结果, 即 $n=0$ 或 $n\neq 0$. 根据 Alice 的投影测量结果, Alice, Bob 和 Charlie 分别选择对光子 A, B 和 C 进行操作 $\hat{I}$ (对应 $n=0$) 或 $\hat{\sigma}_x$ (对应 $n\neq 0$), 使四光子处于 (7) 式所示的态. 接下来, Alice 在算子 $\hat{\sigma}_x$ 的本征基矢下分别对光子 i 和 A 实施测量, 测量结果记为 $\{|x\rangle_i|y\rangle_A\}$, 其中 $|x\rangle,|y\rangle=|+\rangle,|-\rangle$ 分别对应算子 $\hat{\sigma}_x$ 的两个本征态.

2) Alice 利用和 Charlie 之间的密钥 K_{ac} 对测量结果 (比如以二进制数 0 和 1 分别表示测量结果 $|+\rangle_i|+\rangle_A$ (或 $|-\rangle_i|-\rangle_A$) 和 $|+\rangle_i|-\rangle_A$ (或 $|-\rangle_i|+\rangle_A$)) 进行加密, 获得签名 $S_a=K_{ac}(\{|x\rangle_i|y\rangle_A\})$, 并随后公布 S_a.

3) Charlie 利用和 Alice 之间的密钥 K_{ac} 从 S_a 中得到 Alice 的测量结果. 接着, Charlie 也在算子 $\hat{\sigma}_x$ 的本征基矢下对自己的光子 C 实施测量, 测量结果记为 $|k\rangle_C$, 其中 $|k\rangle=|+\rangle,|-\rangle$.

4) Charlie 整理所有的测量结果并给出 Bob 所需要的操作信息, 最后, 利用和 Bob 之间的密钥 K_{bc} 加密该操作信息得到 $S_c=K_{bc}\left(\left\{\hat{I},\hat{\sigma}_z\right\}\right)$, 并公布 S_c.

3.4 签名的验证

1) Bob 利用他和 Alice 之间的密钥 K_{ab} 解密 S_{ab} 得到消息的明文 $M=\{M_i\}$.

2) Bob 利用他和 Charlie 之间的密钥 K_{bc} 解密 S_c, 得到公证人 Charlie 发送的与幺正操作对应的信息. 根据该信息 Bob 对光子 B 执行相应的幺正变换后, 也在算子 $\hat{\sigma}_x$ 的本征基矢下实施测量得到消息 $M'=\{M_i'\}$.

3) Bob 比对 $M=\{M_i\}$ 和 $M'=\{M_i'\}$, 如果两者完全符合则签名成功, 否则验证签名失败, 放弃所接收到的消息. 最后, Bob 公布签名成功与否, 一旦签名成功, 通信双方 Alice 和 Bob 事后单方或双方予以抵赖行为必受到忠实的公证人 Charlie 的监督.

3.5 安全性分析

对于经典信道的安全性, 我们采用对称的量子密钥体系 K_{ab}, K_{ac} 和 K_{bc} 加以保证. 量子密钥的分发采用已经成熟的量子密钥分配方案, 比如 BB84 协议 [1]. 量子信道的安全性由三粒子 GHZ 态的纠缠特性保证 [31,32]. 本方案中, 我们在消息序列中随机地加入了一定数量的样品粒子, $m_i=0$, 即 $|\phi\rangle_i=|H\rangle_i$, 样品粒子的位置在 Bob 对光子 B 测量之前公布. 对于样品粒子, 和其他光子一样根据 Alice 和 Bob 的测量信息进行相应的幺正变换, 但结果惟一地得到态 $|V\rangle_i$, 所以, 此时 Bob 只要对光子 B 在 $\{|H\rangle,|V\rangle\}$ 正交基下测量, 通过检验测量结果是否惟一地得到 $|V\rangle_i$ 来判断通信过程是否安全. 样品粒子所对应的消息没有实际意义, 可简单地与经典消息 0 对应, 并在安全性检测之后丢弃. 另外, 考虑到通信过程中不可避免地会存在信道噪声, 所以在实际应用中允许出现一定的出错率, 只要出错率不高于估计的阈值就可以认为错误是由信道噪声引起的, 即信道是安全的.

4 结 论

量子通信中可能存在信息被篡改或通信双方可能发生抵赖的情况, 所以传输信息的真实性及通信的不可抵赖性具有很高的研究价值. 本文给出了基于弱非线性及对称量子密码体系的量子信息签名方案, 总的思想是通信双方首先通过经典信道传输原始信息, 再在公证人的参与下经量子通道对原始信息进行签名验证. 一方面, 在通信各方都诚实可信的前提下, 利用经典信息和量子信道接收方可以对传输过程中可能被恶意篡改的信息的真伪进行检验. 另一方面, 由于公证人的存在及信息发送方 Alice 和信息接收方 Bob 各自的私人密钥在经典

通信中的使用, 结果使得只要签名成功, 事后通信双方都不能对信息的发送或接收予以否认, 从而保证了通信的合法性. 目前基于 cross-Kerr 非线性介质及相干探针束的量子非破坏性测量技术正处于迅猛发展阶段 [33,34], 本文提出简单可行的方案还可以类似地应用到其他的一些量子通信方案中去.

华侨大学信息科学与工程学院林青副教授和河北师范大学数学与信息科学学院高亭教授曾与作者们进行过有益的讨论, 谨向他们致谢.

[1] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* Bangalore, India (New York: IEEE) p175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[4] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[5] Zeng G H, Keitel C H 2002 *Phys. Rev.* A **65** 042312
[6] Curty M, Lütkenhaus N 2008 *Phys. Rev.* A **77** 046301
[7] Zeng G H 2008 *Phys. Rev.* A **78** 016301
[8] Yan F L, Ding D 2008 *Commun. Theor. Phys.* **50** 1109
[9] Ding D 2011 *Journal of Hebei Normal University* (Natural Science Edition) **35** 34 (in Chinese) [丁东 2011 河北师范大学学报 (自然科学版) **35** 34]
[10] Bouwmeester D, Pan J W, Daniell M, Weinfurter H, Zeilinger A 1999 *Phys. Rev. Lett.* **82** 1345
[11] Pan J W, Daniell M, Gasparoni S, Weihs G, Zeilinger A 2001 *Phys. Rev. Lett.* **86** 4435
[12] Du K, Qiao C F 2011 http://www.arxiv.org/pdf/quant-ph/1108.1475
[13] Hau L V, Harris S E, Dutton Z, Behroozi C H 1999 *Nature* **397** 594
[14] Schmidt H, Imamoglu A 1996 *Opt. Lett.* **21** 1936
[15] Braginsky V B, Khalili F Ya 1996 *Rev. Mod. Phys.* **68** 1
[16] Barrett S D, Kok P, Nemoto K, Beausoleil R G, Munro W J, Spiller T P 2005 *Phys. Rev.* A **71** 060302 (R)
[17] Nemoto K, Munro W J 2004 *Phys. Rev. Lett.* **93** 250502
[18] Kok P 2008 *Phys. Rev.* A **77** 013808
[19] He B, Ren Y H, Bergou J A 2009 *Phys. Rev.* A **79** 052323
[20] Lin Q, He B 2009 *Phys. Rev.* A **80** 042310
[21] Simon C, Pan J W 2002 *Phys. Rev. Lett.* **89** 257901
[22] Sheng Y B, Deng F G 2010 *Phys. Rev.* A **82** 044305
[23] Zhou J, Yang M 2011 *Chinese Journal of Quantum Electronics* **28** 350 (in Chinese) [周建, 杨名 2011 量子电子学报 **28** 350]
[24] Boyd R W 1999 *J. Mod. Opt.* **46** 367
[25] Kok P, Lee H, Dowling J P 2002 *Phys. Rev.* A **66** 063814
[26] Lukin M D, Imamoğlu A 2000 *Phys. Rev. Lett.* **84** 1419
[27] Munro W J, Nemoto K, Beausolei R G, Spiller T P 2005 *Phys. Rev.* A **71** 033819
[28] Munro W J, Nemoto K, Spiller T P 2005 *New J. Phys.* **7** 137
[29] Ding D, Yan F L 2012 http://www.arxiv.org/pdf/quant-ph/1204.0438
[30] Imoto N, Haus H A, Yamamoto Y 1985 *Phys. Rev.* A **32** 2287
[31] Hillery M, Buzek V, Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[32] Yan F L, Gao T, Chitambar E 2011 *Phys. Rev.* A **83** 022319
[33] Jeong H, Kim M S, Ralph T C, Ham B S 2004 *Phys. Rev.* A **70** 061801 (R)
[34] Ourjoumtsev A, Brouri R T, Laurat J, Grangier P 2006 *Science* **312** 83

Implementation of the scheme of a quantum information signature based on weak nonlinearity*

Ding Dong[1)2)] Yan Feng-Li[2)†]

1) (*Department of Basic Curriculum, North China Institute of Science and Technology, Beijing* 101601, *China*)

2) (*College of Physics Science and Information Engineering, Hebei Normal University, Shijiazhuang* 050024, *China*)

(Received 28 May 2012; revised manuscript received 7 August 2012)

Abstract

A quantum information signature protocol based on weak nonlinearity and the symmetrical quantum cryptography is proposed. A sender can send classical messages and can judge whether the messages have been modified or replaced by an adversary. When the authentication of messages is completed, the fact of the communication can neither be disavowed by the sender nor be denied by the receiver because of the existence of an honest arbitrator.

Keywords: quantum teleportation, weak nonlinearity, information signature

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.62.010302

* Project supported by the National Natural Science Foundation of China (Grant No. 10971247), the Hebei Natural Science Foundation of China (Grant Nos. A2012205013, A2010000344), and the Fundamental Research Funds for the Central Universities of Ministry of Education of China (Grant No. 2011B025).

† Corresponding author. E-mail: flyan@hebtu.edu.cn