信道噪声对量子信息分离的影响

白晨明[1] 李永明[2]

(陕西师范大学数学与信息科学学院 西安 710119)[1] (陕西师范大学计算机科学学院 西安 710119)[2]

摘 要 文献[7]给出了一个三者之间利用四粒子团簇态作为量子信道实现单粒子量子态的量子信息分离的方案。在此方案的基础上,分析了经典噪声信道对这个量子信息分离方案的影响。通过利用二元对称信道以及二元删除信道,得到了信息分离成功概率与经典信道噪声系数之间的关系。除此之外,还研究了量子噪声信道对此方案的影响。在振幅阻尼信道或者去极化信道上进行量子信息分离的过程中,量子纠缠信道将会发生退相干,从而导致量子信息分离质量的下降。文中给出了量子信息分离保真度与噪声系数以及所传送量子态系数之间的关系刻画。

关键词 量子信息分离,二元对称信道,二元删除信道,量子信道

中图法分类号 O431 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.4.011

Effect of Channel Noise on Quantum Information Splitting

BAI Chen-ming[1] LI Yong-ming[2]

(School of Mathematics and Information Science, Shaanixi Normal University, Xi'an 710119, China)[1]

(School of Computer Science, Shaanixi Normal University, Xi'an 710119, China)[2]

Abstract In the literature[7], Muralidharan et al have proposed quantum information splitting of single-qubit state by using four cluster state. Based on this scheme, we analyzed the classical noise channel that has a profound influence on the quantum information splitting. Through the binary symmetric channel and the binary erasure channel, we obtained the relationship between information splitting success probability and the classical channel noise coefficient. In addition, we also investigated the effect of this scheme by the quantum noise channel. In the process of quantum information splitting by amplitude damping channel or depolarzing channel, quantum entanglement channel's decoherence will occur, thus leading to the decline of the quality of quantum information splitting. In this paper, we characterized the relationship among the fidelity, the noise coefficient and the original quantum state.

Keywords Quantum information splitting, Binary symmetric channel, Binary erasure channel, Quantum channel

1 引言

在量子信息学中,量子纠缠是最引人注目的,它在许多方面有着广泛且重要的应用,譬如量子隐形传态[1]、量子秘密共享[2]等。量子信息分离[2]也是在以纠缠为通道的基础上实现的,与经典秘密分享相对应,量子信息分离建立在量子论的基础上。自从 Hillery 等人[2]首先提出了量子信息分离的思想后,Karlsson 小组[3]和 Cleve 小组[4]也分别提出不同的量子秘密共享和量子信息分离的方案,他们方案中的粒子首先与其他的粒子纠缠,并传送量子信息,由此量子信息的分离吸引了更多的研究者。目前,许多研究者已经给出了一些很好的方案[5-20]。然而,这些方案大都是将理想的最大纠缠态等纯态作为量子信道,很少有人考虑此量子信道经过量子噪声干扰会出现什么情况。除此,方案中有两次经典的通信,即 Alice 和 Charlie分别将测量的结果告诉 Bob,很少有方案考虑这些经典通信是否会受到经典噪声的影响。

本文提出通过给定一个三者之间基于四粒子团簇态作为量子信道,对单粒子量子态进行量子信息分离的方案。在这个方案中,分析了基于经典噪声二元对称信道以及二元删除信道对经典通信的影响,得出了量子信息分离成功概率与噪声系数之间的具体表达式。除此之外,还考虑了量子纠缠信道经受量子噪声影响的情况。特别地,对在振幅阻尼信道上量子纠缠态发生退相干以及在去极化信道上量子纠缠态发生局部退相干对量子信息分离的重要影响进行了分析,得到了量子信息分离过程中接收者获得的量子态与原始信息态间的保真度与噪声系数以及原始量子态系数之间的关系。

2 量子信息分离

在文献[7]中,Muralidharan 已经提出了利用四粒子团簇态对单粒子进行信息分离。此方案的关键步骤如下。

第一步:设想 Alice、Bob 和 Charlie 共享的量子信道是一个四粒子团簇态,如式(1)所示,信息的发送者 Alice 拥有第 1 粒子,信息的接收者 Bob 拥有 4 粒子,剩下的粒子归信息的控制方 Charlie 拥有。

$$|\phi\rangle_{1234}=\frac{1}{2}(|0000\rangle+|0110\rangle+|1001\rangle-|1111\rangle) \quad (1)$$

到稿日期:2015-06-10 返修日期:2015-08-10 本文受国家自然科学基金(11271237,61228305)资助。

白晨明(1990—),男,硕士生,主要研究方向为量子计算与量子信息;李永明(1966—),男,教授,博士生导师,主要研究方向为非经典计算理论、计算智能、模型检测以及量子计算与量子信息,E-mail:liyongm@snnu.edu.cn。

Alice 想要将一个单比特量子态在 Charlie 的协助下发送给 Bob，即为 $|\varphi\rangle_A=x|0\rangle+y|1\rangle$，其中 x,y 是复数，且满足 $|x|^2+|y|^2=1$。整个系统的初始态可以表达为：

$$|\phi\rangle_{A1234}=|\varphi\rangle_A\otimes|\phi\rangle_{1234}$$
$$=\frac{1}{2}(x|00000\rangle+x|00110\rangle+x|01001\rangle-x|01111\rangle+y|10000\rangle+y|10110\rangle+y|11001\rangle-y|11111\rangle) \quad (2)$$

第二步：Alice 首先对自己手中的 A 和 1 粒子进行 Bell 测量，测量后粒子塌缩，Bob 与 Charlie 将会获得一个纠缠态。此时，Alice 将测量结果通过经典信道告知 Bob 与 Charlie。

第三步：在得到 Alice 的测量结果之后，Charlie 对自己手中的 2 和 3 粒子在基$\{|00\rangle,|11\rangle\}$下进行测量，并将测量结果利用经典信道告知 Bob。Bob 根据 Alice 与 Charlie 的测量结果，对自己手中的粒子 4 进行适当的酉变换，以恢复 Alice 所发送的量子态 $|\varphi\rangle_A=x|0\rangle+y|1\rangle$。具体情形如表 1 所列。

表 1　Alice 与 Charlie 的测量，塌缩后的态以及 Bob 的酉操作

Alice 的测量	测量后的塌缩态	Charlie 的测量	测量后的塌缩态	酉操作
$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$(x|000⟩+x|110⟩+y|001⟩−y|111⟩)	$\|00\rangle_{23}$	x|0⟩+y|1⟩	U_0
		$\|11\rangle_{23}$	x|0⟩−y|1⟩	U_1
$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$(x|000⟩+x|110⟩−y|001⟩+y|111⟩)	$\|00\rangle_{23}$	x|0⟩−y|1⟩	U_1
		$\|11\rangle_{23}$	x|0⟩+y|1⟩	U_0
$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$(x|001⟩−x|111⟩+y|000⟩+y|110⟩)	$\|00\rangle_{23}$	x|1⟩+y|0⟩	U_2
		$\|11\rangle_{23}$	−x|1⟩+y|0⟩	U_3
$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$(x|001⟩−x|111⟩−y|000⟩−y|110⟩)	$\|00\rangle_{23}$	x|1⟩−y|0⟩	$-U_3$
		$\|11\rangle_{23}$	−x|1⟩−y|0⟩	$-U_2$

这里的酉操作如下：

$U_0=|0\rangle\langle0|+|1\rangle\langle1|$，$U_1=|0\rangle\langle0|-|1\rangle\langle1|$

$U_2=|0\rangle\langle1|+|1\rangle\langle0|$，$U_3=|0\rangle\langle1|-|1\rangle\langle0|$

3　经典噪声信道对量子信息分离的影响

在第 2 节的量子信息分裂的方案中，Alice 和 Charlie 分别通过经典信道将自己的测量结果告诉了 Bob。在先前的文献中，人们都默认经典信道是无噪声的信道。然而，经典信道如果为噪声信道，必将给量子信息分离造成影响。因此，先介绍两种较为常见的经典噪声信道[21]作为上述方案中的经典通道，一种称为二元对称信道(BSC)，其简单的模型如图 1 所示；另一种称为二元删除信道(BEC)，其模型如图 2 所示。

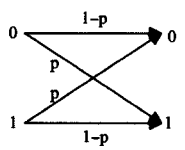


图 1　二元对称信道

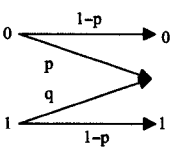


图 2　二元删除信道

假设 Alice 在进行 Bell 态测量之后，将得到的 4 种测量结果分别编码为 00，01，10，11，Charlie 将测量的结果分别编码为 0，1，他们在传输这些经典信息的过程中受到了经典噪声的干扰，而接收者 Bob 并不知道。因此，考虑这些经典噪声信道或为二元对称信道，或为二元删除信道。为了简化模型，假设两种噪声系数 p 是相同的。在信息分离过程中，Alice 与 Charlie分别独立给 Bob 传输信息，所以可能会有下面 4 种干扰情况：

(1)Alice 给 Bob 传输信息受到 BSC 干扰，Charlie 给 Bob 传输信息受到 BSC 干扰；

(2)Alice 给 Bob 传输信息受到 BSC 干扰，Charlie 给 Bob 传输信息受到 BEC 干扰；

(3)Alice 给 Bob 传输信息受到 BEC 干扰，Charlie 给 Bob 传输信息受到 BSC 干扰；

(4)Alice 给 Bob 传输信息受到 BEC 干扰，Charlie 给 Bob 传输信息受到 BEC 干扰。

接下来，设想 Alice 测量后得到的结果编码为 00，Charlie 测量后得到的结果编码为 0，以情况(1)、情况(2)为例具体分析经典噪声对量子信息分离的影响，如表 2、表 3 所列。情况(3)、情况(4)可以类似分析。

表 2　在情况(1)下，经典噪声对量子信息分离的影响

Alice 测量结果	Charlie 测量结果	Bob 粒子 4 的态	Bob 接到 Alice 的测量结果	Bob 接到 Chaelie 的测量结果	Bob 酉操作	分离结果
00	0	x|0⟩+y|1⟩	00	0	U_0	T
				1	U_1	F
			01	0	U_1	F
				1	U_0	T
			10	0	U_2	F
				1	U_3	F
			11	0	$-U_3$	F
				1	$-U_2$	F

表 3　在情况(2)下，经典噪声对量子信息分离的影响

Alice 测量结果	Charlie 测量结果	Bob 粒子 4 的态	Bob 接到 Alice 的测量结果	Bob 接到 Chaelie 的测量结果	Bob 酉操作	分离结果
00	0	x|0⟩+y|1⟩	00	0	U_0	T
				—	—	—
			01	0	U_1	F
				—	—	—
			10	0	U_2	F
				—	—	—
			11	0	$-U_3$	F
				—	—	—

通过对表 2、表 3 的分析可知，在情况(1)下，经典信道受噪声干扰之后，四粒子团簇态作为纠缠信道的量子信息分离的成功概率为 $P=(1-p)^3+p^2(1-p)$；在情况(2)下，量子信息分离的成功概率为 $P=(1-p)^3$，如图 3 所示。从图中可知，在情况(1)下成功的概率大于情况(2)下的成功概率，也即当经典通信时抵抗情况(1)噪声的能力强于抵抗情况(2)噪声的能力。

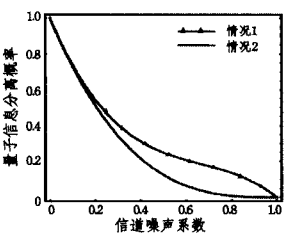


图 3　量子信息分离成功概率与经典噪声系数之间的关系

4　量子噪声信道对量子信息分离的影响

第 3 节分析了经典噪声信道对量子信息分离的影响，得

到了分离成功概率与信道噪声系数之间的关系；此节将分析量子噪声信道对量子信息分离的影响。对于量子信道，其算子和的形式为：

$$\varepsilon(\rho)=\sum_i K_i\rho K_i^{\dagger} \tag{3}$$

这里，$\sum_i K_i^{\dagger}K_i=I$，$K_i$ 为 Kraus 算子，并且 ρ 为任意量子态的密度矩阵，ε 表示作用在 ρ 上的量子运算。

文献[22]介绍了许多量子噪声信道，比如比特翻转信道、去极化信道以及振幅阻尼信道。然而，振幅阻尼信道以及去极化信道都描述了量子系统能量的耗散，是噪声信道的理想模型，而且能够抓住出现在量子系统中噪声的许多非常重要的特性。因此，下面主要研究振幅阻尼信道和去极化信道对量子信息分离的影响。

4.1 振幅阻尼信道对量子信息分离的影响

振幅阻尼信道可以表示成形式(3)，其中 $i=0,1$，且 $K_0=\begin{pmatrix}1 & 0\\ 0 & \sqrt{1-p}\end{pmatrix}$，$K_1=\begin{pmatrix}0 & \sqrt{p}\\ 0 & 0\end{pmatrix}$。除此，还可以将振幅阻尼信道上系统状态与环境的演化描述为下面的变换形式：

$$U_{AE}=\begin{cases}|0\rangle_A|0\rangle_E\rightarrow|0\rangle_A|0\rangle_E\\ |1\rangle_A|0\rangle_E\rightarrow\sqrt{1-p}\,|1\rangle_A|0\rangle_E+\sqrt{p}\,|0\rangle_A|0\rangle_E\end{cases} \tag{4}$$

其中，p 为振幅阻尼系数，A 代表系统，E 代表环境系统。在下面讨论过程中，为了书写方便，将系统下标省略，同时为简化模型，假设量子纠缠信道是对称的。

下面具体分析振幅阻尼信道对量子信息分离的影响。

根据第 2 节量子信息分离方案，采用四粒子团簇态 $|\phi\rangle_{1234}=\frac{1}{2}(|0000\rangle+|0110\rangle+|1001\rangle-|1111\rangle)$ 作为纠缠信道。然而，该信道经过振幅阻尼信道与环境演化为：

$$\begin{aligned}|\tilde{\phi}\rangle_{1234}=&\frac{1}{2}[|0000\rangle|0000\rangle+(1-p)|0110\rangle|0000\rangle+\\ &\sqrt{p(1-p)}|0100\rangle|0010\rangle+\sqrt{p(1-p)}|0010\rangle\\ &|0100\rangle+p|0000\rangle|0110\rangle+(1-p)|1001\rangle\\ &|0000\rangle+\sqrt{p(1-p)}|1000\rangle|0001\rangle+\sqrt{p(1-p)}\\ &|0001\rangle|1000\rangle+p|0000\rangle|1001\rangle-((1-p)^2\\ &|1111\rangle|0000\rangle+\sqrt{p(1-p)^3}|1110\rangle|0001\rangle+\\ &\sqrt{p(1-p)^3}|1101\rangle|0010\rangle+p(1-p)|1100\rangle\\ &|0011\rangle+\sqrt{p(1-p)^3}|1011\rangle|0100\rangle+p(1-p)\\ &|1010\rangle|0101\rangle+p(1-p)|1001\rangle|0100\rangle+\\ &\sqrt{p^3(1-p)}|1000\rangle|0111\rangle+\sqrt{p(1-p)^3}|0111\rangle\\ &|1000\rangle+p(1-p)|0110\rangle|1001\rangle+p(1-p)\\ &|0101\rangle|1010\rangle+\sqrt{p^3(1-p)}|0100\rangle|1011\rangle+p(1-\\ &p)|0011\rangle|1100\rangle+\sqrt{p^3(1-p)}|0010\rangle|1101\rangle+\\ &\sqrt{p^3(1-p)}|0001\rangle|1110\rangle+p^2|0000\rangle|1111\rangle)] \end{aligned}\tag{5}$$

将 $|\tilde{\phi}\rangle_{1234}$ 作为量子信道对 $|\varphi\rangle_A=x|0\rangle+y|1\rangle$ 进行量子信息分离，则整体系统的初始状态为 $|\tilde{\phi}\rangle_{A1234}=|\varphi\rangle_A\otimes|\tilde{\phi}\rangle_{1234}$，然后按照第 2 节给出的第二步与第三步进行操作。下面讨论其中一种情况，其他情况可以类似分析。

设想 Alice 用 $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ 测量，Charlie 用 $|00\rangle$ 测量，最后 Bob 可以得到的量子态为：

$$\begin{aligned}|\phi\rangle_4=&x|0\rangle|0000\rangle+px|0\rangle|0110\rangle+\sqrt{p(1-p)}\,x|1\rangle\\ &|1000\rangle+px|0\rangle|1001\rangle-\sqrt{p^3(1-p)}\,x|1\rangle|1110\rangle-\\ &p^2x|0\rangle|1111\rangle+(1-p)y|1\rangle|0000\rangle+\sqrt{p(1-p)}\\ &y|0\rangle|0001\rangle-p(1-p)y|1\rangle|0110\rangle-\sqrt{p^3(1-p)}\\ &y|0\rangle|1111\rangle\end{aligned}\tag{6}$$

对环境求偏迹，得到粒子 4 的密度矩阵为：

$$\rho_4=\frac{1}{L}\begin{pmatrix}|x|^2(1+2p^2+p^4)+|y|^2(p-p^2+p^3-p^4) & xy^*(1-p-p^2+p^3)\\ x^*y(1-p-p^2+p^3) & |x|^2(p-p^2+p^3-p^4)+|y|^2(1-2p+2p^2-2p^3+p^4)\end{pmatrix} \tag{7}$$

其中，L 是归一化因子，且 $L=|x|^2(1+p+p^2+p^4)+|y|^2(1-p+p^2-p^3)$。

上式中，令 $p=0$，则得到无噪声情况下粒子 4 量子态的密度矩阵为：

$$\rho_0=\begin{pmatrix}|x|^2 & xy^*\\ x^*y & |y|^2\end{pmatrix} \tag{8}$$

此时，ρ_0 正好为 Alice 想要发送的量子态 $|\varphi\rangle_A$ 的密度矩阵。由于振幅阻尼信道的影响，在量子信息分离过程中 Bob 得到的量子态与 Alice 发送的原始态之间存在一定的差异，其保真度为：

$$\begin{aligned}F(\rho_4,|\varphi\rangle_A)=&\langle\varphi_A|\rho_4|\varphi\rangle_A\\ =&\frac{1}{L}(|x|^2(1+2p^2+p^4)+|x|^2|y|^2(2-\\ &4p^2+4p^3-2p^4)+|y|^2(1-2p+2p^2-\\ &2p^3+p^4))\end{aligned}\tag{9}$$

因此，对于满足 $|x|^2+|y|^2=1$ 的任意 x 和 y，当 $p>0$ 时，$F(\rho_4,|\varphi\rangle_A)\leqslant 1$，即由于振幅阻尼信道的影响，Bob 得到的量子态与原始信息的保真度有所下降，如图 4 所示。

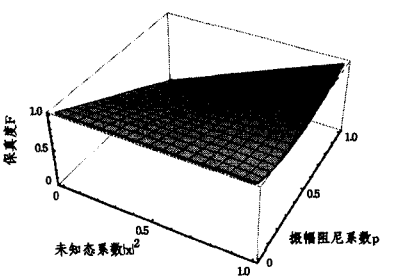


图 4 保真度、振幅阻尼系数和未知态系数之间的关系

4.2 去极化信道对量子信息分离的影响

去极化信道也是一类重要的量子信道，量子系统在这个噪声后的状态可表示为 $\varepsilon(\rho)=pI/2+(1-p)\rho$。

另外，可以将去极化信道表示成以下变换的形式：

$$U_{AE}=\begin{cases}|0\rangle_A|0\rangle_E\rightarrow\sqrt{1-\frac{p}{2}}\,|0\rangle_A|0\rangle_E+\sqrt{\frac{p}{2}}\,|1\rangle_A|1\rangle_E\\ |1\rangle_A|0\rangle_E\rightarrow\sqrt{1-\frac{p}{2}}\,|1\rangle_A|0\rangle_E+\sqrt{\frac{p}{2}}\,|0\rangle_A|1\rangle_E\end{cases} \tag{10}$$

其中，p 为噪声系数，A 代表系统，E 代表环境系统。在以下讨论过程中，为了书写方便，将系统下标省略。

为简化模型以及方便计算，假设去极化信道仅对量子纠缠信道引起了局部退相干。利用4.1节中的方法仅对两种情况进行分析，其他情况可以进行类似的分析。

(1)四粒子团簇态$|\phi\rangle_{1234}$在去极化信道下仅粒子1和粒子2发生局部退相干

采用4.1节中的方法，设想Alice用$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$测量，

$$\rho_4'=\frac{1}{L}\begin{pmatrix}(1-\frac{p}{2})^2|x|^2+\frac{p}{2}(1-\frac{p}{2})|y|^2 & xy^*(1-\frac{p}{2})^2+\frac{p}{2}(1-\frac{p}{2})x^*y\\ x^*y(1-\frac{p}{2})^2+\frac{p}{2}(1-\frac{p}{2})xy^* & (1-\frac{p}{2})^2|y|^2+\frac{p}{2}(1-\frac{p}{2})|x|^2\end{pmatrix} \tag{11}$$

其中，L是归一化因子，且$L=1-\frac{p}{2}$。

经过去极化信道的局部影响，在量子信息分离过程中Bob得到的量子态与Alice发送的原始态之间保真度为：

$$F_{1,2}(\rho_4',|\varphi\rangle_A)=1-\frac{p}{2}+p|x|^2|y|^2+\frac{p}{2}[(x^*y)^2+(xy^*)^2]$$

而量子态$|\varphi\rangle_A=x|0\rangle+y|1\rangle$又可以表示成$|\varphi\rangle_A=\cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$，其中$\theta\in[0,\pi]$，$\varphi\in[0,2\pi]$。

因此，保真度又可以表示为：

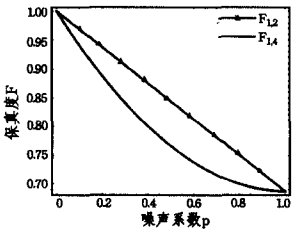
$$F_{1,2}(\rho_4',|\varphi\rangle_A)=1-\frac{p}{2}+\frac{p\sin^2\theta(1+\cos2\varphi)}{4} \tag{12}$$

(2)四粒子团簇态$|\phi\rangle_{1234}$在去极化信道下仅粒子1和粒子4发生局部退相干

与(1)类似，经过去极化信道的局部影响，在量子信息分离过程中Bob得到的量子态与Alice发送的原始态之间的保真度为：

$$F_{1,4}(\rho_4'',|\varphi\rangle_A)=1-p+\frac{p^2}{2}+\frac{\sin^2\theta(1+\cos2\varphi)(2p-p^2)}{4} \tag{13}$$

图5以$\theta=\pi$，$\varphi=\pi$为例，给出了在局部的去极化信道的影响下，两种情况保真度的对比曲线。可以看出，纠缠信道被去极化信道干扰粒子1和粒子4后，获得的保真度低于干扰粒子1和粒子2后的保真度，也即说明了在去极化信道下干扰粒子1和粒子4要比干扰粒子1和粒子2对量子信息分离影响大。



$F_{1,2}$、$F_{1,4}$分别表示对粒子1和粒子2与粒子1和粒子4进行了去极化干扰后得到的保真度

图5 在局部去极化信道的影响下，两种情况保真度的对比曲线

结束语 经典的二元对称信道以及二元删除信道都是重要的经典噪声信道。针对这两种信道对量子信息分离的影响，本文分析了量子信息分离成功概率与信道噪声系数之间的关系。另外，还研究了量子噪声信道对量子信息分离的影响。振幅阻尼信道和去极化信道是两类重要的量子噪声信道，在这两种信道上量子纠缠态将发生退相干现象，从而对量子信息分离产生影响。通过具体分析，得到了接收者获得的量子态和初始态保真度与噪声系数之间的关系。而本文的方法同样也可以推广到其他噪声信道上或者其他的量子信息分离方案中。

Charlie用$|00\rangle$测量，可以得出Bob获得的粒子4的量子态：

$$|\phi\rangle_4=(1-\frac{p}{2})x|0\rangle|0000\rangle+\sqrt{\frac{p}{2}(1-\frac{p}{2})}x|1\rangle|1000\rangle+\sqrt{\frac{p}{2}(1-\frac{p}{2})}y|0\rangle|1000\rangle+\sqrt{\frac{p}{2}(1-\frac{p}{2})}y|1\rangle|0000\rangle$$

对环境求偏迹，得到粒子4的密度矩阵为：

参 考 文 献

[1] Bennett C H, Brassard G, Crepeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. Physical Review Letters, 1993, 70: 1895-1899

[2] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing [J]. Physical Review A, 1999, 59: 1829

[3] Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting[J]. Physical Review A, 1999, 59: 162-168

[4] Cleve R, Gottesman D, Lo H K. How to share a quantum secret [J]. Physical Review Letters, 1999, 83: 648

[5] Zheng Shi-Biao. Splitting quantum information via W states[J]. Physical Review A, 2006, 74(5): 9-15

[6] Zhang Qun-yong, Zhan You-bang, Zhang Ling-ling, et al. Schemes for splitting quantum information via tripartite entangled states[J]. International Journal of Theoretical Physics, 2009, 48: 3331-3338

[7] Muralidharan S, Panigrahi P K. Quantum-information splitting using multipartite cluster states[J]. Physical Review A, 2008, 78(6): 5175-5179

[8] Wang Xin-wen, Xia Li-xin, Wang Zhi-yong, et al. Hierarchical quantum-information splitting [J]. Optics Communications, 2010, 283: 1196-1199

[9] Wang Xin-wen, Zhang Deng-yu, Tang Shi-qing, et al. Multiparty hierarchical quantum-information splitting[J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2011, 44(3): 35505-35508

[10] Li Yuan-hua, Liu Jun-chang, Nie Yi-you. Quantum teleportation and quantum information splitting by using a genuinely entangled six-qubit state [J]. International Journal of Theoretical Physics, 2010, 49(10): 2592-2599

[11] Yin Xiao-feng, Liu Yi-min, Zhang Wen, et al. Simplified four-qubit cluster state for splitting arbitrary single-qubit information [J]. Communications in Theoretical Physics, 2010, 53: 49-53

[12] Li Shu-wen, Jiang Min, Jiang Frank, et al. Multi-qudit information splitting with multiple controllers[J]. Quantum Information Processing, 2014, 13: 1057-1066

[13] Shukla C, Pathak A. Hierarchical quantum communication[J]. Physical Review A, 2013, 377: 1337-1344

[14] Nie Yi-you, Li Yuan-hua, Liu Jun-chang. Quantum information

splitting of an arbitrary three-qubit state by using two four-qubit cluster states[J]. Quantum Information Processing, 2011, 10(3): 297-305

[15] Li Dong-fen, Wang Rui-jin, Zhang Feng-li, et al. Quantum information splitting of arbitrary two-qubit state by using four-qubit cluster state and Bell-state[J]. Quantum Information Processing, 2015, 14: 1103-1116

[16] Kang Shuang-yong, Chen Xiu-bo, Yang Yi-xian. Asymmetric Quantum Information Splitting of an Arbitrary N-qubit State via GHZ-like State and Bell States[J]. International Journal of Theoretical Physics, 2014, 53: 1848-1861

[17] Saha D, Panigrahi P K. N-qubit quantum teleportation information splitting and superdense coding through the composite GHZ-Bell channel[J]. Quantum Information Processing, 2012, 11(2): 615-628

[18] Li Dong-fen, Wang Rui-jin, Zhang Feng-li. Quantum information splitting of arbitrary three-qubit state by using four-qubit cluster state and GHZ-state[J]. International Journal of Theoretical Physics, 2015, 54: 1142-1153

[19] Bai Ming-qiang, Mo Zhi-wen. Hierarchical quantum information splitting with eight-qubit cluster states[J]. Quantum Information Processing, 2013, 12: 1053-1064

[20] Muralidharan S, Jain S, Panigrahi P K. Splitting of quantum information using N-qubit linear cluster states[J]. Optics Communications, 2011, 284(4): 1082-1085

[21] Thomas M C, Thomas J A. Elements of information theory[M]. United States of America, 2006: 187-189

[22] Nielsen M A, Chuang I L. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2000: 356-386

(上接第 52 页)

因此，可以计算得到

$$e(P,P)^{abc}=e(aP,bcP)=e(aP,bQ_B)=e(Q_A,S_B)=\left(\frac{e(W,Q_B)}{R}\right)^{(h+r_2)^{-1}}$$

这与计算 CBDH 问题相矛盾，所以我们提出的方案是不可伪造的。

5.4 效率分析

下面将本文方案与 FeiTang 的方案[10]和 Hafizul Islam 的方案[11]做性能上的比较，并将结果列于表 1 中。表 1 中的 P 表示双线性映射中的对操作。

表 1 比较结果

方案	签名阶段	验证阶段	模拟阶段	总和
本文方案	1P	3P	1P	5P
FeiTang	3P	4P	4P	11P
Hafizul Islam	3P	1P	2P	6P

FeiTang 等人提出的方案中，签名阶段使用了 3 次双线性对的计算，验证和模拟阶段各使用了 4 次双线性对的计算，共需要计算双线性对 11 次；Hafizul Islam 等人的方案在签名阶段、验证阶段、模拟阶段共使用了 6 次双线性对的计算；本文的方案共使用 5 次双线性对。双线性对的计算是极其耗时的，所以本文的方案比文献[9,11]中的方案更有效。

结束语 指定验证者签名由于其具有的特殊性质，已经被广泛地应用在生活的各个领域。本文首先提出了基于身份的强指定验证者签名方案的定义和安全模型，然后构造了一个基于身份的强指定验证者签名方案，并证明了该方案的正确性、不可传递性和不可伪造性。基于 GBDH 假设，证明了方案对适应性选择消息攻击是存在不可伪造的。最后分析了方案的计算代价，结果表明本文的方案具有较高的效率。

参 考 文 献

[1] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications[M]// Advances in Cryptology (EUROCRYPT'96). Springer Berlin Heidelberg, 1996: 143-154

[2] Saeednia S, Kremer S, Markowitch O. An efficient strong designated verifier signature scheme[M]// Information Security and Cryptology (ICISC 2003). Springer Berlin Heidelberg, 2004: 40-54

[3] Susilo W, Zhang F, Mu Y. Identity-based strong designated verifier signature schemes[M]// Information Security and Privacy. Springer Berlin Heidelberg, 2004: 313-324

[4] Kancharla P K, Gummadidala S, Saxena A. Identity based strong designated verifier signature scheme[J]. Informatica, 2007, 18(2): 239-252

[5] Kang B, Boyd C, Dawson E. Identity-based strong designated verifier signature schemes: attacks and new construction[J]. Computers & Electrical Engineering, 2009, 35(1): 49-53

[6] Kang B, Boyd C, Dawson E D. A novel identity-based strong designated verifier signature scheme[J]. Journal of Systems and Software, 2009, 82(2): 270-273

[7] Zhang J, Mao J. A novel ID-based designated verifier signature scheme[J]. Information Sciences, 2008, 178(3): 766-773

[8] Islam S H, Biswas G P. An efficient and secure strong designated verifier signature scheme without bilinear pairings[J]. J. Appl. Math. Info, 2013, 31(3/4): 425-441

[9] Tang F, Lin C, Li Y, et al. Identity-based strong designated verifier signature scheme with full non-delegatability[C]// 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2011: 800-805

[10] Tian H, Chen X, Zhang F, et al. A non-delegatable strong designated verifier signature in ID-based setting for mobile environment[J]. Mathematical and Computer Modelling, 2013, 58(5): 1289-1300

[11] Hafizul I S K, Biswas G P. Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings[J]. Journal of King Saud University-Computer and Information Sciences, 2013, 25(1): 51-61

[12] Schnorr C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174

[13] Joux A. A one round protocol for tripartite Diffie-Hellman[M]// Algorithmic Number Theory. Springer Berlin Heidelberg, 2000: 385-393

[14] Smart N P. Identity-based authenticated key agreement protocol based on Weil pairing[J]. Electronics Letters, 2002, 38(13): 630-632