文章编号：2095-4980(2017)06-0921-07

集体噪声信道下容错的量子密钥分配协议

高　昊，陈晓光，钱松荣

（复旦大学 通信科学与工程系，上海 200433）

摘　要：近年来，量子通信成为一个比较活跃的研究领域。由于理论上的无条件安全性以及实际应用中的可行性，量子密钥分配是量子通信中非常重要的组成部分。而集体噪声信道下的量子密钥分配协议一直被广泛研究。本文提出一种改进的集体噪声信道下容错的量子密钥分配协议，以及一种可行的密钥协商方案。本协议的量子比特效率达到 28.57%，是所有针对集体噪声容错的量子密钥分配协议中最好的，由此提高了量子密钥分配时的效率。

关键词：量子通信；量子密钥分配；集体噪声；量子比特效率

中图分类号：TN929.11　　**文献标志码：A**　　**doi：**10.11805/TKYDA201706.0921

Fault-tolerant Quantum Key Distribution protocols under collective noise channel

GAO Hao，CHEN Xiaoguang，QIAN Songrong

(Department of Communication Science & Engineering，Fudan University，Shanghai 200433，China)

Abstract：Recently, quantum communication has become a very popular research field. Quantum Key Distribution(QKD) plays an important role in the field of quantum communication, based on its unconditional security in terms of theory and feasibility in applications. Among all kinds of QKD protocols, QKD protocols resisting collective noise are widely studied. In this paper, an improved fault-tolerant QKD protocol resisting collective noise is proposed and a feasible plan for information reconciliation is presented. The proposed protocol's qubit efficiency has achieved 28.57%, which is the best among all the fault-tolerant QKD protocols against collective noise, indicating that the proposed protocol can improve the transmission efficiency of quantum key distribution.

Keywords：quantum communication；Quantum Key Distribution；collective noise；qubit efficiency

量子密钥分配协议的设计是用来让通信双方 Alice 和 Bob 建立一个共享的安全密钥，即使面对一个全能的窃听者，这个密钥也是绝对安全的。1984 年 Bennett 和 Brassard 提出了著名的量子密钥分配的概念，并提出了第一个量子密钥分配协议(BB84 协议)[1]。自此，针对量子密钥分配展开了大量研究，并取得了一系列的研究成果。不过许多已有的量子密钥分配方案[1-2]都是基于量子信道为理想信道这一假设所进行的讨论。实际上通信双方需要通过光纤来传输光子，而在传输过程中，量子信道中会有噪声影响。因此，在量子协议的执行过程中，很难区分由噪声引起的错误以及由窃听者所产生的错误。也就是说，窃听者可以让通信双方误以为这些错误均是由噪声导致的。目前集体噪声是量子密码学中被广泛讨论的一个问题。

2004 年，集体噪声信道下容错的量子密钥分配方案被 WANG 提出[3]。之后，YANG[4]和 CHANG 等[5]也提出了类似的容错量子密钥分配方案。但他们的方案中都没有注意到：即使他们的方案是容错的，还是需要有密钥协商这一过程，而且他们方案的量子比特效率都不够高。本文使用 Bell 态对集体噪声信道下容错的量子密钥分配方案进行改进，从而提高了量子比特效率，并提出了一种可行的密钥协商方案。

1　预备知识

1.1　集体噪声

集体噪声主要可被分为 2 种：集体相移噪声和集体旋转噪声。

收稿日期：2017-05-11；修回日期：2017-07-02

当偏振光子$|0\rangle$或$|1\rangle$穿过集体相移噪声信道时，会产生如下变化：$|0\rangle \to |0\rangle$或者$|1\rangle \to \mathrm{e}^{\mathrm{i}\theta}|1\rangle$；当偏振光子$|0\rangle$或$|1\rangle$穿过集体旋转噪声信道时，会产生如下变化：$|0\rangle \to \cos\theta|0\rangle + \sin\theta|1\rangle$或者$|1\rangle \to -\sin\theta|0\rangle + \cos\theta|1\rangle$。其中$|0\rangle$和$|1\rangle$分别代表水平态和垂直态，而$\theta$被视作随时间波动的噪声系数。

1.2 免消相干子空间

量子态受到环境噪声的干扰而造成信息丢失的过程称为消相干过程。针对特定的消相干模型，可以找到系统 Hilbert 空间的一个子空间，使该子空间的态不受其影响，保证态的演化过程仍然是幺正的，这样的子空间称为免消相干子空间(Decoherence-Free Subspace，DFS)。这种方法主要用来消除集体噪声的影响[4,6]。

1.2.1 抵抗集体相移噪声

由集体相移噪声的性质可知，子空间$\{|0_{\mathrm{dp}}\rangle, |1_{\mathrm{dp}}\rangle\}$和$\{|+_{\mathrm{dp}}\rangle, |-_{\mathrm{dp}}\rangle\}$可以构成一个 DFS 来消除集体相移噪声的影响，其中$|0_{\mathrm{dp}}\rangle = |01\rangle$，$|1_{\mathrm{dp}}\rangle = |10\rangle$，$|+_{\mathrm{dp}}\rangle = \frac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle + |1_{\mathrm{dp}}\rangle)$，$|-_{\mathrm{dp}}\rangle = \frac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle - |1_{\mathrm{dp}}\rangle)$。

因此如方程(1)中所示，Bell 态$|\Psi^+\rangle$和$|\Psi^-\rangle$可以不受集体相移噪声的影响。

$$\begin{cases} |\Psi^+\rangle_{12} = \dfrac{1}{\sqrt{2}}(|01\rangle_{12} + |10\rangle_{12}) = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle_{12} + |1_{\mathrm{dp}}\rangle_{12}) \\ |\Psi^-\rangle_{12} = \dfrac{1}{\sqrt{2}}(|01\rangle_{12} - |10\rangle_{12}) = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle_{12} - |1_{\mathrm{dp}}\rangle_{12}) \end{cases} \tag{1}$$

如方程(2)中所示，四粒子 GHZ 态$|G_1\rangle, |G_2\rangle, |G_3\rangle$和$|G_4\rangle$可以通过纠缠量子比特$|0_{\mathrm{dp}}\rangle$和$|1_{\mathrm{dp}}\rangle$来构造。其中$|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$和$|\Psi^-\rangle$分别代表 4 个 Bell 态，如参考文献[4,7−8]中所述，为了区分四粒子 GHZ 态，必须分别对量子比特(1st,3rd)和(2nd,4th)进行 Bell 基测量。显然四粒子 GHZ 态$|G_1\rangle, |G_2\rangle, |G_3\rangle$和$|G_4\rangle$也可以不受集体相移噪声的影响。

$$\begin{cases} |G_1\rangle_{1234} = \dfrac{1}{\sqrt{2}}(|01\rangle_{12}|01\rangle_{34} + |10\rangle_{12}|10\rangle_{34}) = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle_{12}|0_{\mathrm{dp}}\rangle_{34} + |1_{\mathrm{dp}}\rangle_{12}|1_{\mathrm{dp}}\rangle_{34}) = \dfrac{1}{\sqrt{2}}(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24} - |\Phi^-\rangle_{13}|\Phi^-\rangle_{24}) \\ |G_2\rangle_{1234} = \dfrac{1}{\sqrt{2}}(|01\rangle_{12}|01\rangle_{34} - |10\rangle_{12}|10\rangle_{34}) = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle_{12}|0_{\mathrm{dp}}\rangle_{34} - |1_{\mathrm{dp}}\rangle_{12}|1_{\mathrm{dp}}\rangle_{34}) = \dfrac{1}{\sqrt{2}}(|\Phi^-\rangle_{13}|\Phi^+\rangle_{24} - |\Phi^+\rangle_{13}|\Phi^-\rangle_{24}) \\ |G_3\rangle_{1234} = \dfrac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34} + |10\rangle_{12}|01\rangle_{34}) = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle_{12}|1_{\mathrm{dp}}\rangle_{34} + |1_{\mathrm{dp}}\rangle_{12}|0_{\mathrm{dp}}\rangle_{34}) = \dfrac{1}{\sqrt{2}}(|\Psi^+\rangle_{13}|\Psi^+\rangle_{24} - |\Psi^-\rangle_{13}|\Psi^-\rangle_{24}) \\ |G_4\rangle_{1234} = \dfrac{1}{\sqrt{2}}(|01\rangle_{12}|10\rangle_{34} - |10\rangle_{12}|01\rangle_{34}) = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle_{12}|1_{\mathrm{dp}}\rangle_{34} - |1_{\mathrm{dp}}\rangle_{12}|0_{\mathrm{dp}}\rangle_{34}) = \dfrac{1}{\sqrt{2}}(|\Psi^-\rangle_{13}|\Psi^+\rangle_{24} - |\Psi^+\rangle_{13}|\Psi^-\rangle_{24}) \end{cases} \tag{2}$$

1.2.2 抵抗集体旋转噪声

由集体旋转噪声的性质可知，子空间$\{|0_{\mathrm{r}}\rangle, |1_{\mathrm{r}}\rangle\}$和$\{|+_{\mathrm{r}}\rangle, |-_{\mathrm{r}}\rangle\}$可以构成一个 DFS 来消除集体旋转噪声的影响，其中$|0_{\mathrm{r}}\rangle = |\Phi^+\rangle$，$|1_{\mathrm{r}}\rangle = |\Psi^-\rangle$，$|+_{\mathrm{r}}\rangle = \frac{1}{\sqrt{2}}(|0_{\mathrm{r}}\rangle + |1_{\mathrm{r}}\rangle)$，$|-_{\mathrm{r}}\rangle = \frac{1}{\sqrt{2}}(|0_{\mathrm{r}}\rangle - |1_{\mathrm{r}}\rangle)$。

可以不受集体旋转噪声影响的四粒子类 GHZ 态$|L_1\rangle, |L_2\rangle, |L_3\rangle$和$|L_4\rangle$如式(3)所示。如参考文献[4,7−8]中所述，为区分四粒子类 GHZ 态$|L_1\rangle, |L_2\rangle, |L_3\rangle$和$|L_4\rangle$，必须分别对量子比特(1st,3rd)和(2nd,4th)进行 Bell 基测量。

$$\begin{cases} |L_1\rangle_{1234} = \dfrac{1}{2\sqrt{2}}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle + |0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle)_{1234} = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{r}}\rangle_{12}|0_{\mathrm{r}}\rangle_{34} + |1_{\mathrm{r}}\rangle_{12}|1_{\mathrm{r}}\rangle_{34}) \\ |L_2\rangle_{1234} = \dfrac{1}{2\sqrt{2}}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle - |0101\rangle + |0110\rangle + |1001\rangle - |1010\rangle)_{1234} = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{r}}\rangle_{12}|0_{\mathrm{r}}\rangle_{34} - |1_{\mathrm{r}}\rangle_{12}|1_{\mathrm{r}}\rangle_{34}) \\ |L_3\rangle_{1234} = \dfrac{1}{2\sqrt{2}}(|0001\rangle - |0010\rangle + |1101\rangle - |1110\rangle + |0100\rangle + |0111\rangle - |1000\rangle - |1011\rangle)_{1234} = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{r}}\rangle_{12}|1_{\mathrm{r}}\rangle_{34} + |1_{\mathrm{r}}\rangle_{12}|0_{\mathrm{r}}\rangle_{34}) \\ |L_4\rangle_{1234} = \dfrac{1}{2\sqrt{2}}(|0001\rangle - |0010\rangle + |1101\rangle - |1110\rangle - |0100\rangle - |0111\rangle + |1000\rangle + |1011\rangle)_{1234} = \dfrac{1}{\sqrt{2}}(|0_{\mathrm{r}}\rangle_{12}|1_{\mathrm{r}}\rangle_{34} - |1_{\mathrm{r}}\rangle_{12}|0_{\mathrm{r}}\rangle_{34}) \end{cases} \tag{3}$$

2　改进后的协议

2.1 针对集体相移噪声的协议

第 1 步：Alice 准备好 n 个五粒子态 $A_i=\{q_1^i,q_2^i,q_3^i,q_4^i,q_5^i\}(i=1,2,\cdots,n)$，其中 $\{q_1^i,q_2^i\}$ 为 Bell 态 $|\Psi^+\rangle_{12}=\frac{1}{\sqrt{2}}(|01\rangle_{12}+|10\rangle_{12})$，$\{q_3^i,q_4^i\}$ 随机地选择 $|00\rangle$ 或 $|11\rangle$，$\{q_5^i\}=|0\rangle$。接着，Alice 以 $\{q_1^i,q_2^i\}$ 为控制比特，$\{q_3^i,q_4^i,q_5^i\}$ 为目标比特执行 CNOT 操作($CNOT=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$)，见式(4)。经过这一操作后，原来的五粒子态变为 $\{q_1^i,q_2^i,q_3^{i'},q_4^{i'},q_5^{i'}\}$，接着准备序列 $SA=\{A_1',A_2',\cdots,A_n'\}$，其中 $A_i'=\{q_5^{i'},q_2^i,q_3^{i'},q_4^{i'}\}$。然后 Alice 随机从 $\{|0_{dp}\rangle,|1_{dp}\rangle|+_{dp}\rangle,|-_{dp}\rangle\}$ 中挑选诱骗态 $\{d_1^i,d_2^i\}$，将诱骗态随机地插入到 A_i' 中形成传输序列 SA'，并将诱骗态插入的位置信息记录下来[9]。

$$\begin{cases}CNOT(1,3)CNOT(2,4)CNOT(1,5)|\Psi^+\rangle_{12}\otimes|00\rangle_{34}\otimes|0\rangle_5=\frac{1}{\sqrt{2}}\left(|0101\rangle_{5234}|0\rangle_1+|1010\rangle_{5234}|1\rangle_1\right)\\CNOT(1,3)CNOT(2,4)CNOT(1,5)|\Psi^+\rangle_{12}\otimes|11\rangle_{34}\otimes|0\rangle_5=\frac{1}{\sqrt{2}}\left(|0110\rangle_{5234}|0\rangle_1+|1001\rangle_{5234}|1\rangle_1\right)\end{cases}\tag{4}$$

第 2 步：Alice 将生成的传输序列 SA' 传给 Bob，并对 $\{q_1^i\}$ 进行 X 基测量，结合初始状态 $\{q_3^i,q_4^i\}$ 生成对应的原始密钥(可参见方程(5)和表 1，在进行测量后，方程(4)变成方程(5))。

第 3 步：Bob 接收到整个传输序列 SA' 后，告知 Alice 这一事实。

第 4 步：Alice 将诱骗态的位置信息，应采用的正确的测量基以及相应的测量结果通过公开信道告知 Bob。

第 5 步：Bob 获取到诱骗态在序列 SA' 中的位置信息后，Bob 用 Alice 告知的测量基测量 $\{d_1^i,d_2^i\}$，根据 Alice 告知 Bob 的测量结果检查诱骗态的正确性，若测量结果不一致则代表有窃听者的存在，那么终止本次协议并重新开始；若没有发现窃听者，则 Bob 用 Bell 基分别测量序列 SA' 中的 $\{q_5^{i'},q_3^{i'}\}$ 和 $\{q_2^{i'},q_4^{i'}\}$，根据测量结果生成对应的原始密钥(可参见方程(5)和表 1，在进行测量后，方程(4)变为了(5))。

$$\begin{cases}CNOT(1,3)CNOT(2,4)CNOT(1,5)|\Psi^+\rangle_{12}\otimes|00\rangle_{34}\otimes|0\rangle_5=\frac{1}{\sqrt{2}}\left(|G_1\rangle_{5234}|+\rangle_1+|G_2\rangle_{5234}|-\rangle_1\right)\\CNOT(1,3)CNOT(2,4)CNOT(1,5)|\Psi^+\rangle_{12}\otimes|11\rangle_{34}\otimes|0\rangle_5=\frac{1}{\sqrt{2}}\left(|G_3\rangle_{5234}|+\rangle_1+|G_4\rangle_{5234}|-\rangle_1\right)\end{cases}\tag{5}$$

第 6 步：进行密钥协商和保密放大的工作，来获取绝对匹配且绝对安全的密钥。

表 1 测量结果及所对应的密钥比特

Table1 Measurement results and the corresponding key bits

Bob's measurement result	Alice's measurement result	the initial state of $\{q_3^i,q_4^i\}$	key bits
$\|G_1\rangle$	$\|+\rangle$	$\|00\rangle$	00
$\|G_2\rangle$	$\|-\rangle$	$\|00\rangle$	01
$\|G_3\rangle$	$\|+\rangle$	$\|11\rangle$	10
$\|G_4\rangle$	$\|-\rangle$	$\|11\rangle$	11

2.2 针对集体旋转噪声的协议

第 1 步：Alice 准备好 n 个五粒子态 $A_i=\{q_1^i,q_2^i,q_3^i,q_4^i,q_5^i\}(i=1,2,\cdots,n)$，其中 $\{q_1^i,q_2^i\}$ 为 Bell 叠加态 $|+_r\rangle_{12}=\frac{1}{\sqrt{2}}(|\Phi^+\rangle_{12}+|\Psi^-\rangle_{12})$，$\{q_3^i,q_4^i\}$ 随机地选择 $|\Phi^+\rangle$ 或 $|\Psi^-\rangle$，$\{q_5^i\}=|0\rangle$。接着，Alice 以 $\{q_1^i,q_2^i\}$ 为控制比特，$\{q_3^i\}$ 为目标比特执行 CPhase 操作($CPhase=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}$)；以 $\{q_1^i,q_2^i\}$ 为控制比特，$\{q_4^i,q_5^i\}$ 为目标比特执行 CNOT 操作，见方程(6)。经过这一操

作后，原来的五粒子态变为了 $\{q_1^i, q_2^i, q_3^{i'}, q_4^{i'}, q_5^{i'}\}$，接着准备序列 $SA=\{A_1', A_2', \cdots, A_n'\}$，其中 $A_i'=\{q_1^i, q_2^i, q_3^{i'}, q_4^{i'}\}$。然后 Alice 随机从 $\{|0_r\rangle, |1_r\rangle |+_r\rangle, |-_r\rangle\}$ 中挑选诱骗态 $\{d_1^i, d_2^i\}$，将诱骗态随机地插入到 A_i' 中形成传输序列 SA'，并将诱骗态插入的位置信息记录下来[9]。

$$\begin{cases} CPhase(1,3)(2,3)CNOT(1,4)(2,4)CNOT(1,5)(2,5)|+_r\rangle_{12}\otimes|\Phi^+\rangle_{34}\otimes|0\rangle_5=\dfrac{1}{\sqrt{2}}(|\Phi^+\rangle_{12}|\Phi^+\rangle_{34}|0\rangle_5+|\Psi^-\rangle_{12}|\Psi^-\rangle_{34}|1\rangle_5) \\ CPhase(1,3)(2,3)CNOT(1,4)(2,4)CNOT(1,5)(2,5)|+_r\rangle_{12}\otimes|\Psi^-\rangle_{34}\otimes|0\rangle_5=\dfrac{1}{\sqrt{2}}(|\Phi^+\rangle_{12}|\Psi^-\rangle_{34}|0\rangle_5+|\Psi^-\rangle_{12}|\Phi^+\rangle_{34}|1\rangle_5) \end{cases} \tag{6}$$

第 2~第 6 步：与针对集体相移噪声协议中的第 2~第 6 步基本相同，唯一的不同点在于解码方程与解码表(如方程(7)和表 2 所示，在进行测量后，方程(6)变为方程(7))。

$$\begin{cases} CPhase(1,3)(2,3)CNOT(1,4)(2,4)CNOT(1,5)(2,5)|+_r\rangle_{12}\otimes|\Phi^+\rangle_{34}\otimes|0\rangle_5=\dfrac{1}{\sqrt{2}}(|L_1\rangle_{1234}|+\rangle_1+|L_2\rangle_{1234}|-\rangle_1) \\ CPhase(1,3)(2,3)CNOT(1,4)(2,4)CNOT(1,5)(2,5)|+_r\rangle_{12}\otimes|\Psi^-\rangle_{34}\otimes|0\rangle_5=\dfrac{1}{\sqrt{2}}(|L_3\rangle_{1234}|+\rangle_5+|L_4\rangle_{1234}|-\rangle_5) \end{cases} \tag{7}$$

3 安全性证明

窃听者攻击一个量子密钥分配协议的方式大致可分为集体攻击、个体攻击和特洛伊木马攻击 3 种，下面就这 3 种攻击方式分别进行阐述，以证明本量子密钥分配协议在集体噪声信道下的无条件安全性。

表 2 测量结果及所对应的密钥比特

Table2 Measurement results and the corresponding key bits

Bob's measurement result	Alice's measurement result	the initial state of $\{q_3^i, q_4^i\}$	key bits
$\|L_1\rangle$	$\|+\rangle$	$\|\Phi^+\rangle$	00
$\|L_2\rangle$	$\|-\rangle$	$\|\Phi^+\rangle$	01
$\|L_3\rangle$	$\|+\rangle$	$\|\Psi^-\rangle$	10
$\|L_4\rangle$	$\|-\rangle$	$\|\Psi^-\rangle$	11

3.1 集体攻击

集体攻击是指窃听者可以对所有传输的量子比特进行攻击的攻击方式。为了检测出窃听者的攻击，本方案采用了诱骗态的方法[9-10]。比如在针对集体相移噪声的协议中，诱骗态被随机选取并被随机插入到待传输的量子序列中。由于诱骗态选取及插入的随机性，窃听者无法区分诱骗态以及用于生成密钥的量子态，因此窃听者并不能将两者区别对待。于是可以做出如下假设：测量后的诱骗态以及用于生成密钥的量子态将会指数级地确定拥有相同量级的错误数[11]。这样，便可以通过测量后诱骗态结果的正确与否，来判断窃听者是否存在。

窃听者每攻击一个诱骗态，其被发现(即测量后诱骗态结果不正确)的概率为 1/4。因此在窃听者攻击 m 个诱骗态后，其被发现的概率为 $1-(3/4)^m$，易知 m 越大，发现窃听者的概率越大。而一旦发现了窃听者，便终止本次协议并重新开始。当协议继续(即没有发现窃听者)的情况下，窃听者所获取的关于原始密钥的互信息量小于 2^{-l}(即指数级减小)，其中 l 为 Alice 和 Bob 共同选取的安全系数，且 $l>0$。

令传输前用于生成密钥的量子态 $|\Psi_{A'}\rangle=|q_5^{i'}q_2^iq_3^{i'}q_4^{i'}\rangle$，该量子态在集体噪声信道下传输时，虽然可以免受集体相移噪声的影响，但仍可能受到窃听者的攻击，因此 Bob 最终所得的状态可能是不纯的，可以用密度矩阵 $\boldsymbol{\rho}$ 表示。由上面所做出的假设可知：当没有发现窃听者的情况下，即所有测量后诱骗态结果均正确的情况下，可以指数级地确定用于生成密钥的量子态没有产生错误，也就是说传输后所得的状态 $\boldsymbol{\rho}$ 相对于传输前状态 $|\Psi_{A'}\rangle^{\otimes n}$ 的保真度指数级接近 1，即可令 $F(\boldsymbol{\rho}, |\Psi_{A'}\rangle^{\otimes n})^2>1-2^{-s}$，其中 s 可以取任意大的正数。当 $F(\boldsymbol{\rho}, |\Psi_{A'}\rangle^{\otimes n})^2>1-2^{-s}$ 时，$S(\boldsymbol{\rho})<2^{-c}+2^{O(-2s)}$，其中 $c=s-\log_2(2n+s+1/\ln 2)$。

另外由 Holevo 界[11]可知，$S(\boldsymbol{\rho})$ 为窃听者所能获取的关于密钥的互信息量的上界。因此在本文中，当协议继续(即没有发现窃听者)的情况下，窃听者所能获取的关于原始密钥的互信息量一定为指数级的小，这样保证了协议在分配原始密钥过程中的无条件安全性[12]。

但由于在协议继续的情况下，所得原始密钥可能有不匹配的情况，也就是说窃听者可能只攻击了其中几个量子态而没被发现(即窃听者所攻击状态的数量 m 较小，因此有 $(3/4)^m$ 的概率不被发现)，因此仍需要继续进行密钥协商和保密放大的工作。

根据原始密钥只有极少误码数的特点，可以采用 Cascade 方法[13]来进行密钥协商。具体叙述如下：由于

$1-(3/4)^{20}=0.997$，即当窃听者总共攻击了 20 个诱骗态时，窃听者几乎一定会被发现，因此可以认为原始密钥中最多只有 20 位的误码数。首先进行第 1 轮操作：Alice 和 Bob 对各自的原始密钥 $k_1k_2\cdots k_n$ 进行分组，分组大小为 $g=\max\{n/(4\times 20),10\}$。分组是随机进行的，即将比特 k_i 通过随机映射函数 $f(i)=j,1\leqslant i\leqslant n,0\leqslant j\leqslant n/g$ 分到第 j 组。在分组结束后，可以认为每个分组内的误码数有较大概率不多于 1。接着计算每个分组的奇偶校验和并通过公开信道进行比对，如发现某个分组的奇偶校验和不同，则进行二分法查找，找到错误比特后进行纠正。直至所有分组的奇偶校验和被纠正至相同后，第 1 轮操作结束。接着进行第 2 轮操作，Alice 和 Bob 对各自的密钥重新进行分组，具体过程与第 1 轮操作相同。在完成上述 2 轮操作后，其实 Alice 和 Bob 仍不能完全确定他们之间拥有的密钥是否完全相同。因此还需要进行错误校验过程，错误校验可以通过比较两者密钥的哈希函数值来实现。若他们的哈希函数值相同，则两者之间拥有的密钥一定相同；若他们的哈希函数值不同，则两者之间的密钥肯定不同，此时可以选择抛弃此次分配的密钥并重新开始整个协议(需要注意的是，在经过上述 2 轮操作后，密钥仍不相同的概率是极小的)。

由于在上述的密钥协商过程中，Alice 和 Bob 通过公开信道交流了一定量的信息，因此还需进行保密放大的工作，以提取出具有更高安全性的密钥。保密放大可使用文献[14–15]中所述的普适类哈希函数来实现，在此不再赘述。综上所述，本协议对于集体攻击是绝对安全的。

3.2 个体攻击

由文献[16]可知，对于一阶段的量子密钥分配协议，考虑协议的无条件安全性时，若协议对于集体攻击是绝对安全的，则对于个体攻击也是绝对安全的。因此，本协议对于个体攻击是绝对安全的。

3.3 特洛伊木马攻击

由于本协议是一阶段的量子密钥分配协议，所有量子比特序列均只传输了 1 次，因此特洛伊木马攻击者没有机会提取出他所插入的间谍光子，即本协议无需使用任何特殊的检测设备便可以抵御特洛伊木马攻击[17-18]。

4　与其他方案的比较

为了证明本协议方案的优势，在这里将与其他最近提出的同样针对集体噪声的方案进行比较，详见表 3，以集体相移噪声的比较为例。

表 3 各方案的比较(以集体相移噪声的比较为例)

Table3 Comparison of different schemes (taking schemes against the collective-dephasing noise for example)

	YANG and HWANG's scheme[4]	CHANG and YANG's scheme[5]	proposed scheme
quantum source	four-particle GHZ state	three-particle GHZ state	Bell state
quantum communication	two-step	two-step	one-step
devices for Trojan horse attack	No	No	No
qubit efficiency	20%	22.22%	28.57%
whether or not considering the information reconciliation	No	No	Yes

下面将针对集体相移噪声的情况进行更加详细的说明，集体旋转噪声的情况与其类似，在此不再赘述。

4.1 量子源

在 CHANG 和 YANG 的方案中，要求对量子态执行 GHZ 基测量，这一测量方式实际所使用的测量设备较为复杂。本方案仅要求对量子态执行 Bell 基以及 X 基的测量，这 2 种测量方式实际所使用的测量设备较为简单[11]。

4.2 量子通信方式

在 YANG 和 HWANG 的方案以及 CHANG 和 YANG 的方案中，所采用的量子通信方式均为两阶段。本方案对此进行了改进，将量子通信方式改为一阶段。由此产生的优点：首先协议的平均执行时间变短；另外，对于 YANG 和 HWANG 的方案以及 CHANG 和 YANG 的方案，要求通信双方 Alice 和 Bob 都具有将量子比特暂时存储起来的能力；本方案中，只要求 Bob 具有将量子比特暂时存储起来的能力即可，因此本方案可能的应用情况为 Alice 作为客户端，而 Bob 作为服务器端，服务器端往往拥有更强大的性能；最后，光脉冲在光纤中的双向传输会产生严重的瑞利后散射，从而导致对于光子数错误的计数[19]，将量子通信方式改为一阶段后，便可以解决这一问题。

4.3 量子比特效率

量子比特效率(Qubit Efficiency，QE)定义如下[4]：$QE = q_c / q_t$，其中 q_c 表示原始密钥的传统比特总数，q_t 表示方案中生成的光子总数。在本方案中，为了得到 $2n$ 个传统密钥比特，Alice 准备了 n 个五粒子态和 n 个两粒子诱骗态。因此本方案的量子比特效率 $QE = \dfrac{2n}{5n+2n} = 28.57\%$，同理可得 YANG 和 HWANG 的方案以及 CHANG 和 YANG 的方案中的量子比特效率分别为 20%及 22.22%，可以发现本方案的量子比特效率是所有针对集体噪声容错的量子密钥分配方案[4-5,17-18]中最好的。

4.4 密钥协商过程

由于可能存在窃听者只攻击了几个量子态而没被发现的情况(如 3.1 中所述)，即分配给通信双方 Alice 和 Bob 的原始密钥不匹配的情况，因此需要对提出的量子密钥分配协议考虑密钥协商和保密放大的过程。YANG 和 HWANG 以及 CHANG 和 YANG 都忽略了这一点，本方案中给出了一种可行的密钥协商和保密放大的方案(如 3.1 中所述)，虽然这一方案不是最优的，但至少是可行的。

5 结论

本文使用 Bell 态对集体噪声信道下容错的量子密钥分配方案进行了改进，提高了量子比特效率，而且本方案的量子比特效率 28.57%是所有针对集体噪声容错的量子密钥分配方案中最好的。此外本文所提出的量子密钥分配方案是一阶段的，这样更容易被实现。最后，本文针对协议执行过程中可能存在的原始密钥不匹配的情况，提出了一种可行的密钥协商和保密放大的方案。

值得一提的是，本方案较理想的应用场景为保偏光纤，这是由于保偏光纤中的主要噪声为双折射效应所引起的集体噪声[20]。不过仍有许多问题有待解决，最重要的在于：以上讨论仅针对了集体噪声信道下的情况，但本协议也可运用在普通的量子信道(即普通的单模光纤)中，因此为进一步增加实用性，本协议在普通量子信道中的表现以及具体的实施细节还有待考量。另外，本文所提出的密钥协商和保密放大的方案不是最优的，更优的方案可进一步考虑。

参考文献：

[1] BENNETT C H,BRASSARD G. Quantum cryptography:public key distribution and coin tossing[J]. Theoretical Computer Science, 2014,560(1):7-11.

[2] BENNETT C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992,68(21):3121-3124.

[3] WANG X B. Fault tolerant quantum key distribution protocol with collective random unitary noise[J]. Physical Review A, 2004,72(5):762-776.

[4] YANG C W,HWANG T. Trojan horse attack free fault-tolerant quantum key distribution protocols[J]. Quantum Information Processing, 2014,13(3):781-794.

[5] CHANG C H,YANG C W,HWANG T. Trojan horse attack free fault-tolerant quantum key distribution protocols using GHZ states[J]. International Journal of Theoretical Physics, 2016,55(9):1-12.

[6] KWIAT P G,BERGLUND A J,ALTEPETER J B,et al. Experimental verification of decoherence-free subspaces[J]. Science, 2000,290(5491):498-501.

[7] GU B,MU L,DING L,et al. Fault tolerant three-party quantum secret sharing against collective noise[J]. Optics Communications, 2010,283(15):3099-3103.

[8] YANG C W,TSAI C W,HWANG T. Fault tolerant two-step quantum secure direct communication protocol against collective noises[J]. Science China Physics,Mechanics and Astronomy, 2011,54(3):496-501.

[9] LO H K,MA X,CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005,94(23):230504.

[10] GOTTESMAN D,LO H K,LUTKENHAUS N,et al. Security of quantum key distribution with imperfect devices[J]. Quantum Information and Computation, 2004,4(5):325-360.

[11] NIELSON M A,CHUANG I L. Quantum Computation and Quantum Information[M]. [S.l.]:Cambridge University Press, 2010.
[12] SHOR P W,PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000,85(2):441–444.
[13] BRASSARD G,SALVAIL L. Secret-key reconciliation by public discussion[J]. Proceeding EUROCRYPT '93 workshop on the theory and application of cryptographic techniques on advances in cryptology. Lofthus,Norway:ACM, 1993:410–423.
[14] BENNETT C H,BRASSARD G,ROBERT J M. Privacy amplification by public discussion[J]. SIAM Journal on Computing, 1988,17(2):210–229.
[15] BENNETT C H,BRASSARD G,CRÉPEAU C,et al. Generalized privacy amplification[J]. IEEE Transactions on Information Theory, 1995,41(6):1915–1923.
[16] RENNER R,GISIN N,KRAUS B. Information-theoretic security proof for quantum-key-distribution protocols[J]. Physical Review A, 2005,72(1):012332.
[17] LI X H,ZHAO B K,SHENG Y B,et al. Fault tolerant quantum key distribution based on quantum dense coding with collective noise[J]. International Journal of Quantum Information, 2009,7(8):1479–1489.
[18] LI C Y,LI Y S. Fault-tolerate quantum key distribution over a collective-noise channel[J]. International Journal of Quantum Information, 2010,8(7):1101–1109.
[19] GISIN N,RIBORDY G,TITTEL W,et al. Quantum cryptography[J]. Physics, 2002,74(1):145–195.
[20] YAMAMOTO T,SHIMAMURA J,OZDEMIR S K,et al. Faithful qubit distribution assisted by one additional qubit against collective noise[J]. Physical Review Letters, 2005,95(4):040503-1–040503-4.

作者简介:

高　昊(1994–),男,上海市人,在读硕士研究生,主要研究方向为量子通信.email: 16210720124@fudan.edu.cn.

陈晓光(1964–),男,安徽省五河县人,博士,副教授,主要研究方向为无线通信与量子通信.

钱松荣(1960–),男,上海市人,教授,主要研究方向为网络与数据通信.