基于循环码和信息压缩融合的量子保密通信算法

马鸿洋[1,2]，张鑫[3]，徐鹏翱[3]，刘芬[2,3]，范兴奎[1,2]

（1. 青岛理工大学理学院，山东 青岛 266520；2. 青岛理工大学量子光学与量子通信研究中心，山东 青岛 266520；
3. 青岛理工大学信息与控制工程学院，山东 青岛 266520）

摘 要：针对经典保密通信中信息安全传输的问题，提出了一种基于循环码和信息压缩的量子保密通信算法。首先，发送端对传输的信息进行预处理，将其分割为长度不等的 2 组数据，分别用于循环编码和压缩编码。然后，发送端添加一串量子态传输至接收端，采用误码数作为信道安全检测的依据，若信道安全，则对预处理后的数据量子态处理，利用量子稳定子码编码分段并传输，依据稳定字码的特性克服环境引起的误码。最后，接收端接收到量子信息后进行解码，并解循环和解压缩从而获得数据。安全性分析表明，所提量子保密通信算法能较好地抵抗篡改和截断信息的攻击。仿真结果表明，对于数据压缩部分按 5 分段能获得较好的效果。

关键词：循环码；信息压缩；量子稳定子码；通信效率；量子保密通信

中图分类号：TN911

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020059

Quantum secure communication algorithm based on cyclic code and information compression

MA Hongyang[1,2], ZHANG Xin[3], XU Peng'ao[3], LIU Fen[2,3], FAN Xingkui[1,2]

1. School of Science, Qingdao University of Technology, Qingdao 266520, China
2. The Research Center for Quantum Optics and Quantum Communication, Qingdao University of Technology, Qingdao 266520, China
3. School of Information and Control Engineering, Qingdao University of Technology, Qingdao 266520, China

Abstract: For the problem that the classical secure communication was challenging to transmit information, a quantum secure communication algorithm based on cyclic code and information compression was proposed. First, the data was encoded into two sets of data with different lengths by the sender, one set of data was used for cycling coding and the other one was used to compress coding. Second, single-photon sequence was transmitted to the receiver on the quantum channel by the sender. The error number was used as the basis of channel security detection. If the channel was secure, quantum states were encoded for the data, and segment transmitted by quantum stabilizer codes. The error caused by the environment can be overcome according to characteristic of the stable code. Finally, the information was decoded after receiving the quantum information, then recirculated and decompressed to obtain data. The security analysis shows that the quantum secure communication algorithm can resist the attack of jamming and spoofing attacked. The simulation results show that good results can be obtained to 5 segments for data compression.

Key words: cyclic code, information compression, quantum stabilizer code, communication efficiency, quantum secure communication

收稿日期：2019−09−10；**修回日期**：2020−01−10

基金项目：国家自然科学基金资助项目（No.11975132, No.61772295）；山东省自然科学基金资助项目（No.ZR2019YQ01）；山东省高等学校科技计划基金资助项目（No.J18KZ012）

Foundation Items: The National Natural Science Foundation of China (No.11975132, No.61772295), The Natural Science Foundation of Shandong Province (No.ZR2019YQ01), Shandong Province Higher Educational Science and Technology Program (No.J18KZ012)

1　引言

信息安全[1]是政府企业和个人隐私等领域发展的必要保障，而量子保密通信[2-10]是解决信息安全的有效手段之一，是一种与经典保密通信相互补充的通信方式。量子保密通信在理论上具有经典通信所不具备的绝对安全性，在政府机构、企业金融、个人信息等领域有重大的应用价值和发展前景。

1984 年，Bennett 等[11]提出了第一个量子密码分发协议，即 BB84 编码协议；1991 年，Ekert[12]提出了 EPR 编码协议；1992 年，Bennett[13]提出了 E92 编码协议；2002 年，Long 等[14]提出了基于纠缠光子对的量子保密通信方案；2004 年，Deng 等[15]借鉴经典密码的一次一密的思想提出基于单光子的一次一密量子安全直接通信方案，简称 DL04 方案；2007 年，Wen 等[16]提出了基于 EPR 对的量子签名协议的方案，并证明采用该方案即使通信被窃听也不会泄露机密信息；同年，Li 等[17]提出了基于纠缠态的秘密信息共享方案；2008 年，杨宇光等[18]参考经典 Shamir 秘密共享方案提出没有纠缠的门限量子保密通信协议，对相应的幺正算符操作从而获取秘密信息。2009 年，秦素娟等[19]提出集体幅值阻尼信道上的量子保密通信，且能克服量子信道中集体噪声；2014 年，郭大波[20]对高斯量子密钥分发数据提出性能优化方案；2014 年，吴贵铜等[21]提出双向的带身份认证的无信息泄露的量子保密通信协议，能够解决信道噪声问题；2015 年，常利伟等[22]提出利用最大纠缠信道和部分纠缠信道，构造了 2 个多方控制量子通信协议。随着量子通信的发展[23-26]，2019 年，王华等[27]提出了基于量子密钥分发的城域光通信网络架构方案；同年，Qian 等[28]提出一种有效抵御量子密钥分发系统探测器控制攻击的方案；2020 年，Guo 等[29]提出基于量子信道的因果序的相干叠加的量子通信方案，并通过实验验证了该方案能够超越标准量子香农理论的限制。

本文提出了一种循环码和信息压缩混合使用的量子保密通信算法。首先发送端对传输的信息进行预处理，分割为长度不等的 2 组数据，其中一组数据用于循环编码，另一组数据用于压缩编码，提高通信效率；其次，发送端添加一串量子态传输给接收端，根据接收端宣布的误码数作为信道安全检测的依据，若信道安全，则对预处理好的数据量子态处理，利用量子稳定子码编码分段并传输，依据稳定字码的特性克服环境引起的误码，提高准确率；最后，接收端依据校验矩阵获得正确传输的量子信息，并解循环和解压缩，从而获得数据。该算法在考虑环境噪声的前提下，利用量子稳定字码对传输的量子态进行编码优化，保证了传输量子态的准确性。

2　基础知识

2.1　信息压缩与循环

信息压缩是指按照一定的算法对数据重新进行组织排列，减少冗余数据。设数据表示为 G，依次按照 m bit 划分，记为：m 比特 | m bit | … | m bit。如果临近的比特串按位相同，例如 $0111100101\cdots|0111100101\cdots$，则被压缩为 $0111100101\cdots|0$；如果临近的比特串按位相反，如 $0111100101\cdots|1000011010\cdots$，则被压缩为 $0111100101\cdots|1$。

循环码是线性分组码中的一个重要子类，由于其具有循环特性，因此其编码和伴随式较容易实现。假设 $g(x)$ 需要生成 $[n,k]$ 循环码，$u(x)$ 为要编码的信息，$\frac{g(x)}{u(x)x^{n-k}}$ 的余式为 $b(x)$，则 $v(x)=b(x)+u(x)x^{n-k}$，可推算出相应的码字，其中最右边的 k bit 为信息位，最左边的 $(n-k)$ bit 为校验位，用其相对应的校验函数进行校验。

2.2　稳定子码

量子稳定子码 $[n,k,d]$ 称为量子加性量子码，是一类结构丰富的量子纠错码，记为 $C(W)$，其中，n 是编码后的比特数，k 是原始的比特数。其特点是 Abel 子群 W 隶属 n 量子位 Pauli 算子群，该子群内元素本征值为 +1，所构造的本征值空间为 H_s，则当 $|\varphi\rangle_i \subset H_s$ 时，对于任意的 $\boldsymbol{M}(\boldsymbol{M}\in W)$，存在 $\boldsymbol{M}|\varphi\rangle_i=|\varphi\rangle_i$。$H_s$ 所对应的量子码为稳定子码，$\boldsymbol{M}$ 为 W 的生成元，子群 W 为稳定子码 $C(W)$ 的稳定子，表示为

$$C(W)=|\varphi\rangle:\boldsymbol{M}|\varphi\rangle_i=|\varphi\rangle_i,\forall\boldsymbol{M}\in W$$

$$W=\prod_{j=1}^{n-k}\boldsymbol{M}_j^{b_j},b_j\in\{0,1\},j=1,2,\cdots,n-k$$

3　算法描述

3.1　数据分割操作

将比特串 $P=\{P_1,P_2,\cdots,P_K\}$ 分割为长度不等的

比特串，分别表示为 $a=\{P_1,P_2,\cdots,P_C\}$ 和 $b=\{P_{C+1},P_{C+2},\cdots,P_K\}$，且 $a>>b$，$K=a+b$。对比特串 a 进行压缩操作，对比特串 b 进行循环操作。数据分段以及数据循环和数据压缩如图 1 所示。

3.2 压缩操作和循环操作

对 $a=\{P_1,P_2,\cdots,P_C\}$ 进行压缩操作，对 $b=\{P_{C+1},P_{C+2},\cdots,P_K\}$ 按照 $g(x)=1+x+x^3$ 和 $u(x)=1+x^3$ 进行循环操作，压缩后的比特串为 $c=\{P_1,P_2,\cdots,\ P_{C-X}\}$，$X$ 是可压缩的长度。循环后的比特串为 $d=\{P_{C+1},\cdots,P_K,\cdots,P_Y\}$，选择的循环码为 (7,4)，因此 $d=1.75b$。

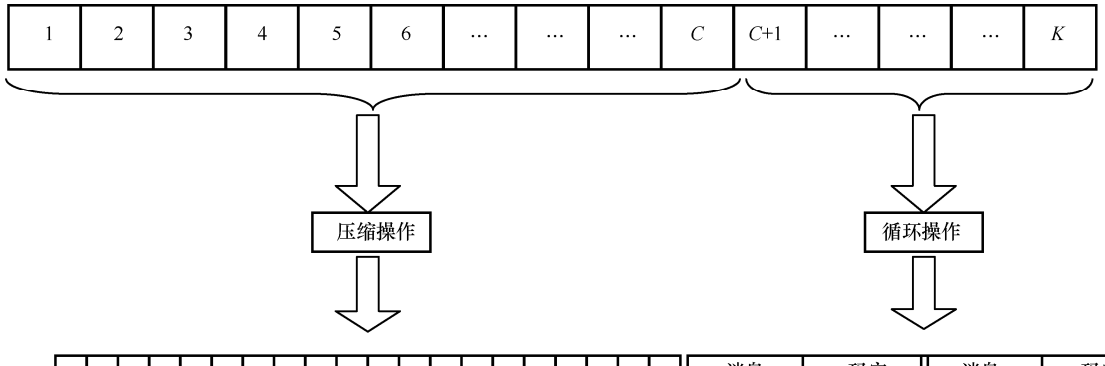
循环部分采用(7,4)循环码，将比特数据按 4 分段，然后将 4 位数据循环成 7 位的数据，可以纠正单个比特错误，并且能够检测任意 2 个比特错误的组合。利用(7,4)循环码能将易出错区域的准确率从 0.062 5 提升到 0.312 5。为了尽可能降低复杂度，本文选用(7,4)循环码对易出错字段进行有效纠正。

将 2 个比特串 c 和 d 重新组合为 $Q=c+b$，$c=\{P_1,P_2,\cdots,P_{C-X}\}$中发生压缩的位置记录标记为 Sign-$A$，通过经典信道传给接收端，Sign-$A$ 信息作为解压缩操作的起始比特位；循环操作对应的校验矩阵也通过经典信道传给接收端，用来进行解循环操作。

3.3 信道安全检测

对于信道安全检测信息，为了保证不丢失有效数据 Q。本文没有采用 Q 中的信息作为信道检测，而是添加一组长度为 n bit 的量子态来检测信道安全。

选取 n bit 信息，发送端制备一系列的单光子态 $|\Psi_0\rangle=\otimes_{i=1}^{n}\left(a_i|0\rangle+b_i|1\rangle\right)$，其中 $|\alpha_i|^2+|\beta_i|^2=1$。$n$ 个量子态随机分发，一般采用 4 个量子态，分别为 $|0\rangle$、$|1\rangle$、$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$、$\frac{|0\rangle-|1\rangle}{\sqrt{2}}$；将序列标记 $\lambda=\{\lambda_1,\lambda_2,\cdots,\lambda_n\}$ 发送给接收端；接收端收到发送的单光子态后，记录测量结果 $\rho=\{\rho_1,\rho_2,\cdots,\rho_n\}$，并在公共信道上告知发送端。发送端对公布的数据进行比对，设出错的信息数（用相应光子数表示信息出错数）为 D，误码率阈值 $t=\left[\frac{d-1}{2}\right]$，其中，$d$ 为汉明距离（设量子纠错码能纠正的最大位数不超过 t），若 $D\leqslant t$，则说明量子信道是安全的，接收端向发送端反馈一个信道安全确认帧；否则，说明量子信道存在窃听者，或者环境噪声超过纠错码的最大纠错能力，则终止此次通信过程。此处，通信过程除了信道安全检测外，不需要其他附加信息的交换。需要说明的是，在 3.5 节解压缩和解循环的过程中，需要 Sign-A 的标记信息（此标记信息用 BB84 协议通信，



消息	码字	消息	码字
0000	0000000	0001	1010001
1000	1101000	1001	0111001
0100	0110100	0101	1100101
1100	1011100	1101	0001101
0010	1110010	0011	0100011
1010	0011010	1011	1001011
0110	1000110	0111	0010111
1110	0101110	1111	1111111

图 1 数据分段及数据压缩和数据循环

但其为位置信息，数据量非常小，对通信所造成的时延可以忽略），但该标记信息与量子通信无关。

3.4　编码纠错的过程

把比特串 Q 按块传输，每块为 k bit，共 m 块，即 $Q=mk$，其量子串表示为

$$\left|\Psi^1\right\rangle=\otimes_{j=1}^{Q=mk}\left(a_i\left|0\right\rangle+b_i\left|1\right\rangle\right)=\otimes_{j=0}^{m-1}\left(a_{mj+1}\left|0\right\rangle+b_{mj+1}\left|1\right\rangle\right)\cdot$$
$$\left(a_{mj+2}\left|0\right\rangle+b_{mj+2}\left|1\right\rangle\right)\cdots\left(a_{mj+k}\left|0\right\rangle+b_{mj+k}\left|1\right\rangle\right)\quad(1)$$

其中，第 j 块量子比特串表示为

$$\left|\Psi_j^1\right\rangle=\left(a_{mj+1}\left|0\right\rangle+b_{mj+1}\left|1\right\rangle\right)\cdot$$
$$\left(a_{mj+2}\left|0\right\rangle+b_{mj+2}\left|1\right\rangle\right)\cdots\left(a_{mj+m}\left|0\right\rangle+b_{mj+m}\left|1\right\rangle\right)\quad(2)$$

根据式(2)，在第 j 块比特串中任取第 i 量子态 $a_i\left|0\right\rangle_c+b_i\left|1\right\rangle_c$，稳定子码编码形式为

$$\alpha_i\left|0\right\rangle_c+\beta_i\left|1\right\rangle_c=\alpha_i\left[\prod_{i=1}^{n-k}(I+\boldsymbol{M}_i)\right]\left|0\cdots0\right\rangle+$$
$$\beta_i\overline{X}\left[\prod_{i=1}^{n-k}(I+\boldsymbol{M}_i)\right]\left|0\cdots0\right\rangle=$$
$$\alpha_i[(I+\boldsymbol{M}_1)(I+\boldsymbol{M}_2)\cdots(I+\boldsymbol{M}_{n-k})]\left|0\cdots0\right\rangle+\beta_i(X\cdots X)\cdot$$
$$[(I+\boldsymbol{M}_1)(I+\boldsymbol{M}_2)\cdots(I+\boldsymbol{M}_{n-k})]\left|0\cdots0\right\rangle\quad(3)$$

生成元 $\boldsymbol{M}_i$ 作用于 $\left|\varphi\right\rangle_i$，其正常本征值应为+1；如果本征值变为 –1，则说明比特传输中出现错误，该错误用算子 $\boldsymbol{E}_i$ 表示。因为，$\boldsymbol{M}_i$ 与 $\boldsymbol{E}_i$ 之间存在相互对易和相互反对易这 2 种关系，分别记为 $[\boldsymbol{E}_i,\boldsymbol{M}_i]=\boldsymbol{E}_i\boldsymbol{M}_i-\boldsymbol{M}_i\boldsymbol{E}_i=0$，$[\boldsymbol{E}_i,\boldsymbol{M}_i]=\boldsymbol{E}_i\boldsymbol{M}_i+\boldsymbol{M}_i\boldsymbol{E}_i=0$。利用稳定子 W 的 $(n-k)$ 个生成元测量，可得到本征值 $\{(-1)^{W_1},\cdots,(-1)^{W_i},\cdots,(-1)^{W_{n-k}}\}$，其中 $W_i\in\{0,1\}$。

携带有效信息的第 j 块包含 k bit 的比特串，经过稳定子纠错编码后以此扩展。对于每个量子比特，编码前确定稳定子纠错编码的子群 W 总个数为 $\sum_{\boldsymbol{M}_i\in W}\boldsymbol{M}_i=\prod_{i=1}^{n-k}(I+\boldsymbol{M}_i)$。对于任意的 $\boldsymbol{M}_i(\boldsymbol{M}_i\in W)$，存在 $\boldsymbol{M}_i\left|\varphi\right\rangle_i=\left|\varphi\right\rangle_i$。$\boldsymbol{M}_i$ 为稳定子 W 群内 $n-k$ 个生成元中的任意一个，由以下 4 个酉正算子组合而成。

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad\sigma_y=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\quad\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

其生成元的编码信息为

$$\left|x_1\cdots x_k\right\rangle=\left[\prod_{i=1}^{n-k}(I+\boldsymbol{M}_i)\right]\overline{X_1^{x_1}}\cdots\overline{X_k^{x_k}}\left|0\cdots0\right\rangle=$$
$$\overline{X_1^{x_1}}\cdots\overline{X_k^{x_k}}\left(\sum_{\boldsymbol{M}_i\in W}\boldsymbol{M}_i\left|0\cdots0\right\rangle\right)\quad(4)$$

其中，$\overline{X_i}$ 为比特翻转酉转换，$x_i\in\{0,1\}$。

依次对所有的 $E_i(\varphi_{ic})$ 进行测量，判断这个 k 数据块中出现的所有错误信息以及纠错位。生成元 $\boldsymbol{M}$ 用矢量偶表示，$\boldsymbol{M}_1,\cdots,\boldsymbol{M}_{n-k}$ 为 $(n-k)\times2n$ 阶的校验矩阵。

$$\begin{pmatrix}\boldsymbol{M}_1\\\vdots\\\boldsymbol{M}_{n-k}\end{pmatrix}\Leftrightarrow\boldsymbol{H}=\left(I\mid\boldsymbol{H}_X\right)=\begin{pmatrix}h_1\\\vdots\\h_{n-k}\end{pmatrix}$$

其中，$\boldsymbol{H}_X$ 是生成元 $\boldsymbol{M}_1,\cdots,\boldsymbol{M}_{n-k}$ 的比特翻转 X 组成的矩阵。本文协议中量子比特只存在比特翻转，不存在相位翻转错误。$\boldsymbol{H}$ 作用于接收到的量子态，得到所有 $\boldsymbol{M}_i$ 的本征值矩阵 $\boldsymbol{H}'$，根据 $\boldsymbol{H}'$ 判断出现比特翻转错误的所有量子位。

接收端根据测量结果和量子伴随式比对，可判断 X 翻转的出错量子位。X 翻转错误对应酉正算子 σ_x。针对出错量子位进行对应的酉正门操作，将纠正后的码字反向编码，获得的正确量子信息。因为单光子作为信息的载体，容易受到环境噪声的影响，所以利用量子稳定子码能较好地克服环境噪声的影响。

3.5　接收到信息的解循环和解压缩过程

发送端可以将相应校验函数等信息通过经典信道传输给接收端，字符串分割点位置 Sign-*A* 用 BB84 协议通信。

接收端通过校验函数和 Sign-*A* 解循环，解压缩 0111100101…|0|0111100101…|1 → 10111100101…|0111100101…0111100101…1000011010… 的相关内容进行相应的还原操作。

4　安全性分析

本文协议可能会受到来自协议本身和第三方的攻击，下面对这 2 种情况的安全性进行分析。

4.1　量子态发生窃听情况的安全性分析

假设在通信过程中发生窃听时，对量子态的攻击实行操作 $\boldsymbol{E}$。

$$\boldsymbol{E}\left|\Psi\right\rangle=\left|\Phi\right\rangle$$

其中，$\left|\Phi\right\rangle=m\left|x\right\rangle+n\left|y\right\rangle,\left|m\right|^2+\left|n\right|^2=1$。$\left|x\right\rangle$和$\left|y\right\rangle$为 4 个量子态$\left|0\right\rangle$、$\left|1\right\rangle$、$\frac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}$、$\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}$中的 2 个。经过窃听后，单光子态 $\left|\Psi_0\right\rangle=\otimes_{i=1}^{n}\left(a_i\left|0\right\rangle+b_i\left|1\right\rangle\right)$（$\left|\alpha_i\right|^2+\left|\beta_i\right|^2=1$）变为

$$\boldsymbol{E}|\Psi_0\rangle=|\Phi_0\rangle=\otimes_{i=1}^{n}(m_i|x\rangle+n_i|y\rangle)$$

设 $m^2=a$，$n^2=b$，得到 $a+b=1$。因为窃听后基态变化的随机性，4 个基态是出现的最大量，可能被选择其中的 2 个，即出现的组合是 $\mathrm{C}_4^2=6$ 种，且出现的概率相同。所以得到窃听概率为

$$\rho=\frac{-\sum_{i=1}^{6}\frac{1}{6}\mathrm{lb}\frac{1}{6}}{6}=\frac{2.585}{6}\approx 0.43$$

对于每个基态所包含的最大信息量为

$$I(|x\rangle_i)=-a\mathrm{lb}a-(1-a)\mathrm{lb}(1-a)=H(a)$$

因为 4 个基态出现的概率相同，都是 $\frac{1}{4}$，所以 $I=\sum_{i=1}^{4}I_{|x\rangle_i}=\frac{1}{4}\times 4H(a)=H(a)$，即可以接受窃听的最大总信息量为 $H(a)$（$0\leqslant H(a)\leqslant 1$）。当 $H(a)=0$ 时，窃听的信息为 0，窃听概率是 0；当 $H(a)=1$ 时，窃听到一位量子位上所携带的全部信息，此时概率 $\rho=0.43$。本文中，$Q=mk$，$\lim\limits_{Q\to\infty}\rho^Q=\lim\limits_{Q\to\infty}0.43^Q\approx 0$。因为 Q 数值较大，窃听到多位量子态的概率趋近于零，安全性较高。

4.2 第三方窃听信道安全检测光子携带的信息

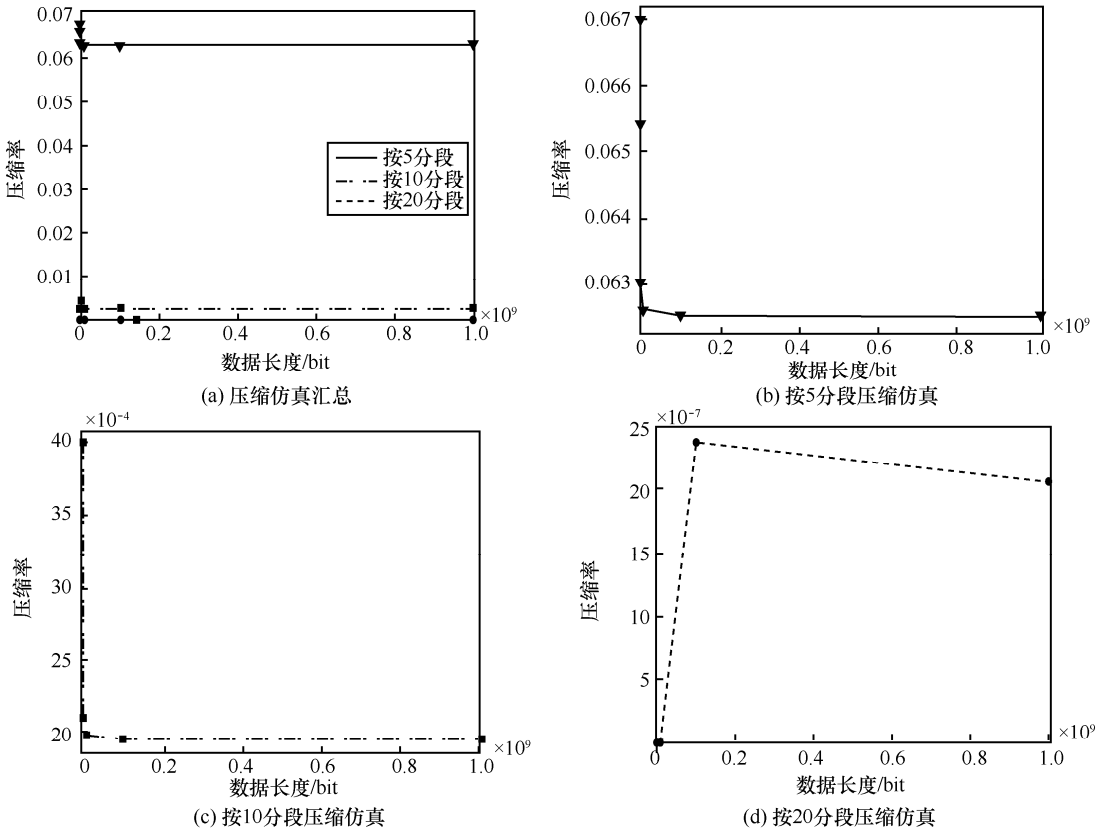
第三方窃听到 3.3 节所述检测光子携带的信息时，不会导致信息泄露，因为检测光子携带的信息只是用于检测误码，而不是要传输的有效信息。此时，只需再次传输检测信息即可。

4.3 第三方窃听编码后的信息

第三方窃听到 3.1 节所述循环操作和压缩操作后的信息，即 $c=\{P_1,P_2,\cdots,P_{C-X}\}$，$d=\{P_{C+1},\cdots,P_K,\cdots,P_Y\}$，由于 Sign-*A* 的标记信息由 BB84 协议保障，第三方不知道 Sign-*A* 的标记信息，对窃取的信息无法解压缩和解循环，因此不会导致泄露信息，仍可保障安全性。

5 仿真实验

本文利用 Python 语言生成 3.1 节所述数据，对其压缩部分进行仿真实验，利用 Mathematica 计算最终的压缩率。在数据压缩中，本文主要考虑数据分段情况和数据长度情况，分别按 5、10、20 分段。所有仿真均是对 $10^5\sim10^9$ bit 数据进行模拟，仿真结果如图 2 所示，其中，图 2(a)是按 5、10、20 分段压缩的仿真汇总，图 2(b)～图 2(d)分别为按 5、



(a) 压缩仿真汇总　(b) 按5分段压缩仿真

(c) 按10分段压缩仿真　(d) 按20分段压缩仿真

图 2　压缩仿真结果

10、20 分段压缩的仿真。

从图 2 可以看出，当分段情况确定时，数据串长度的变化对压缩比率的影响很小；对应位相同或相反的概率均为 0.5，假设按 P 长度进行分段，压缩成功的可能性为 0.5^P，在长度一定的情况下，分段数越小，压缩率越高；按 20 分段的压缩率非常小，几乎可以忽略。由仿真结果可知，按 5 分段压缩率最高。

6　结束语

本文提出了一种循环码和信息压缩混合使用的量子保密通信算法，对经典信息进行操作，利用循环码提升传输准确率，利用信息压缩提升传输效率；利用稳定子码对量子信息进行操作，对出现的比特翻转进行纠错；此外，对协议的安全性进行了分析。仿真结果表明，所提算法在保障安全性的前提下，有效地克服了环境噪声，并且传输效率和传输准确率都达到了较好的效果。

参考文献：

[1] 杨义先, 孙伟, 钮心忻. 现代密码新理论[M]. 北京: 科学出版社, 2002: 134-135.
YANG Y X, SUN W, NIU X X. The new theory of modern cryptography[M]. Beijing: Science Press, 2002: 134-135.

[2] WANG H, ZHAO Y, YU X, et al. Resilient quantum key distribution (QKD)-integrated optical networks with secret-key recovery strategy[J]. IEEE Access, 2019(5): 60079-60090.

[3] GILLES B, FELIX B, NICOLAS G, et al. Multiuser quantum key distribution using wavelength division multiplexing[J]. Applications of Photonic Technology, 2003(5260): 149-153.

[4] ZHU W, CROZIER K B. Quantum mechanical limit to plasmonic enhancement as observed by surface-enhanced Raman scattering[J]. Nature Communications, 2014(5): 1-8.

[5] 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.

[6] CAO Y, ZHAO Y L, COLMAN-MEIXNER C, et al. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)[J]. Optics Express, 2017,25(22): 26453-26467.

[7] 梁建武, 程资, 石金晶, 等. 基于量子图态的量子秘密共享[J]. 物理学报, 2016,65(16): 35-41.
LIANG J W, CHENG Z, SHI J J, et al. Quantum secret sharing based on quantum graph States[J]. Acta Physica Sinica, 2016,65(16): 35-41.

[8] 佟鑫, 温巧燕, 朱甫臣. 基于 GHZ 态纠缠交换的量子秘密共享[J]. 北京邮电大学学报. 2007,30(1): 44-48.
TONG X, WEN Q Y, ZHU F C. Quantum secret sharing based on GHZ state entanglement swapping[J]. Journal of Beijing University of Posts and Telecommunications, 2007,30(1): 44-48.

[9] MARKHAM D, SANDERS B C. Graph states for quantum secret sharing[J]. Physical Review A, 2008,78(4):042309.

[10] ZHANG W, DONG S, SHENG Y B, et al. Quantum secure direct communication with quantum memory[J]. Physical review letters,2017,118(22):220501.

[11] BENNETT C H, BRASSARD G. Quantum cryptography：public key distribution and coin tossing[C]//Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. Piscataway: IEEE Press, 1984: 175-179.

[12] EKERT A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991,67(6):661-663.

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

[14] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. Physical Review A, 2002, 65(3): 032302.

[15] DENG F G, LONG G L. Secure direct communication with a quantum one-time pad[J]. Physical review A,2004,69(5):052319.

[16] WEN X J, LIU Y, ZHANG P Y. Information signature protocols using Einstein-Podolsky-Rosen pairs[J]. Journal of Dalian University of Technology, 2007, 47(3): 424-428.

[17] LI X H, LI C Y, DENG F G, et al. Quantum secure direct communication with quantum encryption based on pure entangled states[J]. Chinese Physics, 2007, 16(8):2149-2153.

[18] 杨宇光, 张兴. 没有纠缠的门限量子安全直接通信[J]. 中国科学(G 辑:物理学 力学 天文学),2008(5):523-530.
YANG Y G, ZHANG X. Quantum secure direct communication without entanglement threshold [J]. Science of China (series G: physics, mechanics and astronomy), 2008(5): 523-530.

[19] 秦素娟, 温巧燕, 孟洛明, 等. 集体幅值阻尼信道上的量子安全直接通信[J]. 中国科学(G 辑:物理学 力学 天文学), 2009(5): 693-697.
QIN S J, WEN Q Y, MENG L M, et al. Quantum secure direct communication on collective amplitude damped channels [J]. Science of China (series G: physics, mechanics and astronomy),2009(5):693-697.

[20] 郭大波, 张彦煌, 王云艳. 高斯量子密钥分发数据协调的性能优化[J]. 光学学报, 2014,34(1): 233-239.
GUO D B, ZHANG Y H, WANG Y Y. Performance optimization for the reconciliation of Gaussian quantum key distribution[J]. Acta Optica Sinica, 2014,34(1): 225-231.

[21] 吴贵铜, 周南润, 龚黎华, 等. 集体噪声信道上带身份认证的无信息泄露的量子对话协议[J]. 物理学报, 2014, 63(6): 50-57.
WU G T, ZHOU N R, GONG L H, et al. Quantum dialogue protocol with identity authentication on collective noise channel without information leakage [J]. Acta Physica Sinica, 2014, 63(6): 50-57.

[22] 常利伟, 郑世慧, 谷利泽, 等. 多方控制量子通信协议[J]. 通信学报, 2015, 36(6): 139-148.
CHANG L W, ZHENG S H, GU L Z, et al. Multi-party controlled quantum communication protocol[J]. Journal on Communications, 2015, 36(6): 139-148.

[23] SHI P, LI N C, WANG S M, et al. Quantum multi-user broadcast

protocol for the “platform as a service” model[J].Sensors, 2019,19(23), 5257.

[24] QIN L G, WANG Z Y, MA H Y, et al. Optomechanical entanglement switch in the hybrid opto-electromechanical device[J]. Journal of the Optical Society of America B, 2019, 36(6): 1544-1550.

[25] MA H Y, TENG J K, HU T, et al. Co-communication protocol of underwater sensor networks with quantum and acoustic communication capabilities[J]. Wireless Personal Communications, 2020: doi.org/10.1007/s11277-020-07192-7.

[26] MA H Y, XU P A, SHAO C H, et al. Quantum private query based on stable error correcting code in the case of noise[J]. International Journal of Theoretical Physics, 2019, 58(12):4241-4248.

[27] 王华, 赵永利. 量子密钥分发城域光组网技术前瞻[J]. 通信学报, 2019, 40(9): 168-174.
WANG H, ZHAO Y L. Overview of quantum key distribution metropolitan optical networking technology[J]. Journal on Communications, 2019, 40(9): 168-174.

[28] QIAN Y J, HE D Y, HOU Z B, et al. Robust countermeasure against detector control attack in a practical quantum key distribution system[J].Optica,2019,6(9):1178.

[29] GUO Y, HU X M, HOU Z B, et al. Experimental transmission of quantum information using a superposition of causal orders[J]. Physical Review Letters, 2020, 124 (3): 30502.

[作者简介]

马鸿洋（1976– ），男，山东青岛人，博士，青岛理工大学教授，主要研究方向为网络空间安全、量子信息、量子保密通信等。

张鑫（1996– ），男，山东寿光人，青岛理工大学硕士生，主要研究方向为量子通信、量子计算、信息安全等。

徐鹏翱（1995– ），男，山东菏泽人，青岛理工大学硕士生，主要研究方向为量子图像、量子通信、量子计算等。

刘芬（1996– ），女，山东临朐人，青岛理工大学硕士生，主要研究方向为量子机器 、量子信息、信息安全等。

范兴奎（1970– ），男，山东嘉祥人，博士，青岛理工大学教授，主要研究方向为代数学、量子信息计算、量子群表示论等。