量子 LDPC 码在 BB84 协议中的应用研究

李苗苗,王超一,李 飞,赵生妹
LI Miao-miao,WANG Chao-yi,LI Fei,ZHAO Sheng-mei

南京邮电大学 通信与信息工程学院,南京 210003
College of Telecommunications & Information Engineering,Nanjing University of Posts and Telecommunications,Nanjing 210003,China
E-mail:y050820@njupt.edu.cn

LI Miao-miao,WANG Chao-yi,LI Fei,et al.Research on application of quantum LDPC code for BB84 quantum key distribution.Computer Engineering and Applications,2008,44(8):128-130.

Abstract: Considering noise in the quantum channel of BB84 quantum key distribution protocol,an improved model of BB84 protocol with quantum error correction code,such as Quantum Low Density Parity Check code(QLDPC) is proposed in this paper.By numerical simulation,the effect of quantum error correction code on BB84 protocol is analyzed in the case of the efficiency of transmission rate.The results show that quantum LDPC codes have good ability to overcome the noise,raise the efficiency of transmission rate and verify the availability of the improved model.

Key words: BB84 protocol;quantum Low Density Parity Check code;efficiency of transmission rate

摘 要:针对 BB84 量子密钥分配协议中量子信道存在噪声,设计一种带有量子纠错码的改进的 BB84 协议模型,在模型中用量子低密度奇偶校验码(量子 LDPC)作为纠错码对发送量子态进行编码。通过数值仿真,从密钥传输效率的角度分析量子纠错编码对 BB84 协议的影响。结果表明量子 LDPC 码能克服噪声,提高了密钥传输效率,验证了在含噪量子信道中改进的 BB84 协议模型的有效性。

关键词:BB84 协议;量子 LDPC 码;密钥传输效率
文章编号:1002-8331(2008)08-0128-03 **文献标识码:**A **中图分类号:**TP393

1 引言

1984 年,Bennett 和 Brassard 提出第一个量子密钥分配协议(QKD)[1],它在仅满足量子物理学定律的条件下提供了绝对的安全性。为了分析简便,BB84 协议中的量子信道假设不含噪声。然而,实际量子密钥分配过程中,由于环境噪声,使得量子态的演化过程与环境间存在着不可避免的相互作用,这种相互作用将引起量子态与环境态纠缠, 导致原始密钥的误码率增大。以至于可能出现这样的情况,即使通信过程中没有窃听,最终估计的误码率却超过安全标准(Security Criteria),因此降低了密钥共享的效率。借鉴经典信道中通过纠错编码提高含噪信道传输的可靠性,将量子纠错编码应用到 BB84 协议中提高密钥传输的效率是值得研究的问题。

构造量子纠错码常用的方法是基于 Calderbank-Shor-Steane 码(也称 CSS 码)[2,3]和稳定子码[4],较为简捷方法是基于 CSS 码直接从经典线性纠错码中获得对应的量子版本。低密度奇偶校验矩阵码(Low Density Parity Check code),即 LDPC[5],是一种性能优越的线性分组码。在经典 LDPC 的基础上通过 CSS 构造原理实现量子纠错码是一种可行的方法。M.S.Postol 在有限几何 LDPC 码的基础上提出构造量子 LDPC 码的思路[6];D.J.C.Mackey 等人在 CSS 码基础上,利用特殊稀疏序列提出了几种构造校验矩阵的方法, 并在此基础上构造量子 LDPC码[7]。

针对含噪的 BB84 协议,文献[8]介绍一种基于 CSS 码的一对非规则量子 LDPC 码应用于协议中经典信道上的纠错和秘密放大,通过分析量子 LDPC 码的译码性能得出该码具有克服噪声能力的结论。本文提出一个含噪量子信道中带量子 LDPC 码的 BB84 协议改进模型,使用文献[8]中量子 LDPC 码的构造方法, 通过数值仿真分析量子 LDPC 码克服量子噪声的能力、以及对提高密钥传输效率的影响。

2 带量子 LDPC 码的 BB84 协议改进模型

在无噪 BB84 量子密钥分配协议模型基础之上,假设发送

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60672133);江苏省自然科学基金(the Natural Science Foundation of Jiangsu Province of China under Grant No.BK2006236);南京邮电大学校基金(the Foundation of NJUPT under Grant No.NY206020)。

作者简介:李苗苗(1984-),女,硕士研究生,主要研究领域是量子信息处理;王超一(1982-),男,硕士研究生,主要研究领域是量子信息处理;李飞(1964-),教授,研究方向为现代通信中的智能信号处理、量子信息技术;赵生妹(1968-),教授,研究方向为无线通信与信号处理技术、量子信息技术。

收稿日期:2007-09-17 **修回日期:**2007-11-27

方 Alice 和接收方 Bob 间的量子信道存在噪声,导致在量子信道上传输的极化态发生错误。现在考虑利用量子纠错编码技术克服量子信道噪声的影响，提出量子 LDPC 码在 BB84 协议中的应用模型,如图 1 所示。

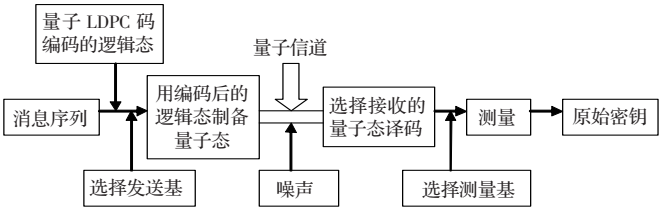

图 1　含噪量子信道中带量子纠错编码(量子 LDPC 码)的 BB84 协议改进模型

按照时间顺序,模型过程步骤如下:

(1)Alice 准备要发送的二进制消息序列、一组与消息序列长度一致的发送基(等概地选择⊕或者⊗),根据 BB84 协议规则和所选的基把消息序列制备成一系列量子态,也即极化态。

(2)Alice 采用量子 LDPC 码编码方式,对已经制备好的每个极化态进行编码,然后发送编码后的极化态到量子信道上。

(3)极化态在量子信道上传输,受量子噪声干扰,极化态发生相位或者比特翻转或者相位和比特都发生翻转。考虑到利用 CSS 码解码原理进行解码时，纠相位错的过程等同于在 C2 空间中纠比特错误,所有本文主要考虑信道存在比特翻转错误情况。

(4)在接收端,Bob 随机地选择一组测量基(等概地选择⊕或者⊗)待用。根据经典信道上与 Alice 的信息交换,仅保留与 Alice 选择的测量基一致的对应位置上的极化态。

(5)对保留的极化态译码,纠正在传输过程中受噪声干扰引起的错误。对译码后仍未能纠正的错误极化态做丢弃处理;而对那些传输过程中未发生错误或者发生错误但经过译码过程得以纠正的极化态,用第四步中选择的相应基测量,得到原始密钥。

(6)统计密钥传输效率(Efficiency of Transmission Rate)。密钥传输效率是指在某一个位置,Bob 选择的测量基与 Alice 的对应位置上的发送基一致,并且在同一位置接收到的极化态是正确的或者经过译码后是正确的,那么他在该位置测量之后得到的就是有效的原始密钥。统计所有位置上 Bob 得到的有效原始密钥个数与 Alice 发送的消息序列长度的比率就是密钥传输效率。

同 BB84 协议模型一样，改进模型中得到原始密钥之后，Alice 和 Bob 随机地从原始密钥中选择一个共同的子集进行误码率估计,通过估计值与安全标准的比较,判断是否存在窃听。

3　数值仿真及结果分析

为了验证 BB84 协议改进模型的有效性,本章做一个具体的数值仿真,通过数值仿真结果分析量子 LDPC 码对密钥传输效率的影响。

3.1　构造量子 LDPC 码

根据 BB84 协议改进模型，关键的步骤是用量子 LDPC 编码量子态。在经典 LDPC 码基础上,给合 CSS 码的构造原理,介绍量子 LDPC 码的一种构造方法[8]。假设 LDPC 码 C_1 的校验矩阵是 $\boldsymbol{H}_1$,维数为 $M\times N$;从 $\boldsymbol{H}_1$ 中选出 $N-M$ 列,按列重从小到大的顺序重新排列,构成 $M\times(N-M)$维矩阵 $\boldsymbol{H}_1'$。若把 $\boldsymbol{H}_1'$的每一行作为一个 $N-M$ 长的消息序列编码到 C_1 码空间中,则产生 M 个 N 长的码字;再把生成的这 M 个码字作为行,构成一个 $M\times N$ 维的矩阵,记做 $\boldsymbol{H}_2'$;将 $\boldsymbol{H}_2$ 作为生成矩阵,定义 C_2;则 $C_2\subset C_1$,获得量子 LDPC 码。如下是量子 LDPC 码(25,5)的具体构造过程:

(1)选择一个构成非规则 LDPC 码的校验矩阵 $\boldsymbol{H}_1$,其维数为 10×25,该 LDPC 码记作 $C_1(25,15)$。

$$\boldsymbol{H}_1=\begin{bmatrix}
1&1&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&1&1&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0\\
0&0&1&1&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0\\
0&0&0&1&1&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0
\end{bmatrix}$$

(2)从 $\boldsymbol{H}_1$ 中选出 15 列,构成(10×15)维矩阵 $\boldsymbol{H}_1'$,并把这 15 列按列重从小到大的顺序重新排好;然后,把 $\boldsymbol{H}_1'$的每一行作为一个长度为 15 的信息序列编码到 C_1 的码空间中,则产生 10 个长度是 25 的码字;最后把生成的这 10 个码字作为行,构成一个(10×25)维的矩阵,记作 $\boldsymbol{H}_2'$。

(3)将 $\boldsymbol{H}_2'$作为生成矩阵,定义 $C_2(25,10)$,C_2 校验矩阵记作 $\boldsymbol{H}_2$。

显然,经过上述过程产生的 C_1 和 C_2 满足 $C_2\subset C_1$,符合 CSS 码的必备条件。为了验证该方法获得的量子 LDCPC 码的纠错性能,以 C_1 和 C_2 构造的量子 LDPC(25,15-10)码,编码长为 10 000 的消息序列，在仅考虑比特错误的 BSC 信道中，采用 BP 译码算法获得译码后块错误概率与比特翻转概率关系曲线如图 2 所示,其中 BP 译码最大循环次数为 100。从图 2 可知,用该方法构造的量子 LDPC 码具有克服噪声的能力。

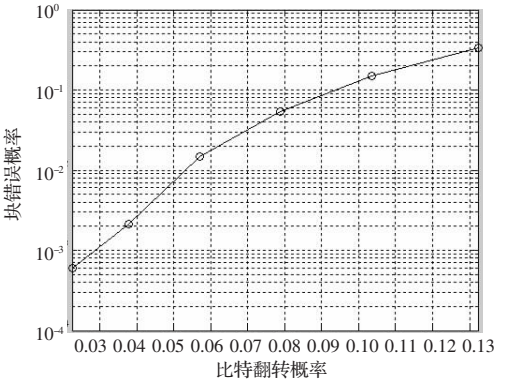

图 2　块错误概率与比特翻转概率关系曲线

3.2　量子 LDPC 码在 BB84 协议中的应用仿真

按照图 1 模型,仿真实现含噪量子信道上带量子 LDPC 的 BB84 协议改进模型。本节仿真中的编码参数为:量子 LPDC 码码长 25,码率 0.2,其中 C_1 码长 25,码率 0.6。首先 Alice 随机地

选择长度为 2 000 的二进制消息序列，按照第 2 章中过程第(1)步制备成一系列量子态；然后依第(2)步编码，结合 BB84 协议[9]，编码后发送到量子信道上的极化态与消息序列的对应关系可以写成式(1)：

$$0\rightarrow\begin{cases}\oplus\rightarrow|0\rangle_L\\ \otimes\rightarrow\dfrac{1}{\sqrt{2}}(|0\rangle_L+|1\rangle_L)\end{cases},1\rightarrow\begin{cases}\oplus\rightarrow|1\rangle_L\\ \otimes\rightarrow\dfrac{1}{\sqrt{2}}(|0\rangle_L-|1\rangle_L)\end{cases}\quad(1)$$

其中$|0\rangle_L$,$|1\rangle_L$是逻辑态，即编码后的极化态。这些极化态在量子信道上传输过程中，受噪声干扰，在一些未知的位上发生比特翻转(因为本文只考虑比特翻转)。到达接收端后，Bob 根据事先准备好的测量基是否与 Alice 的发送基一致，有选择地对接收到的极化态译码。因为通信双方等概地选择基⊕或者⊗，所以他们选择相同基的可能性为 50%左右，也即，Bob 选择译码的极化态个数为 1 000 左右。借鉴经典纠错码的方法，Bob 判断译码是否正确，丢弃那些译码后仍然错误的极化态，而那些译码正确的极化态经过测量之后，便可保留为原始密钥。

另一方面，假设含噪信道上的 BB84 协议不带量子纠错码，Bob 保留的原始密钥是它的测量基与 Alice 的发送基一致的相应位置上的测量结果，因为量子信道上存在比特翻转概率(在此仅考虑比特翻转)，那么它保留的原始密钥很可能是错误的量子态的测量结果，因而增大估计误码率。

含噪量子信道带量子 LDPC 编码的 BB84 协议通信中，发送消息序列长度是 2 000，量子纠错码用基于 CSS 码构造的量子 LDPC 码，码长 25，码率 0.2。因为主要考虑比特翻转错误，信道模型用 BSC 信道。译码算法是 BP 算法，其中最大循环次数是 100。含噪量子信道带量子 LDPC 编码和不带纠错编码的 BB84 协议中，密钥传输效率与比特翻转概率关系曲线如图 3 所示。

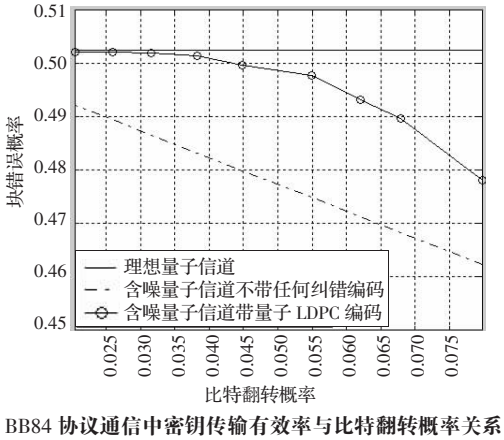

图 3 BB84 协议通信中密钥传输有效率与比特翻转概率关系曲线

值得说明的是模型中测量过程理想化，表现为一旦 Bob 选择的测量基正确，译码成功后的极化态经过测量，一定与消息序列中的比特相对应。

图 3 所示的三条曲线分别表示理想量子信道、含噪量子信道不带纠错编码和含噪量子信道带量子 LDPC 编码时，一次 BB84 协议通信的密钥传输效率与比特翻转概率的关系。事实上，信道理想时的密钥传输效率和比特翻转概率之间不存在关系曲线，为了给后两种情况做参考，才把理想信道的效率用直线表示在图 3 中。本次通信理想信道效率为 50.25%(即信道理想曲线纵坐标的值)。从图 3 可以看出，当信道受噪声干扰时，带量子 LDPC 码的 BB84 协议通信的密钥传输效率明显高于不带纠错编码的 BB84 协议通信。密钥传输效率的提高，意味着量子 LDPC 编码降低了量子噪声对获得的原始密钥进行误码率估计的影响，因此本文设计的 BB84 改进模型是有效的。

4 结论

本文提出含噪量子信道的 BB84 协议改进模型，通过数值仿真验证了模型的有效性。从密钥传输效率的角度分析 BB84 协议改进模型的系统性能，数值计算结果表明量子 LPDC 在含噪量子信道中具有克服噪声干扰的能力，提高了密钥传输的效率。BB84 协议从物理上保证了密钥传输的安全性，量子纠错编码与 BB84 协议相结合保证了含噪量子信道量子密钥传输的可行性。

参考文献：

[1] Bennett C H,Brassard G.Quantum cryptography:public key distribution and coin tossing[C]//Proceeding of the IEEE International Conference on Computer,Systems and Signal Processing,1984:175-179.

[2] Calderbank A R,Shor P W.Good quantum error correcting codes exist[J].Phys Rev A,1996,54:1098-1105.

[3] Steane A M.Multiple particle interference and error correction[C]//Proceeding of the Royal Society of London Series A,1996,452:2551-2577.

[4] Nielsen M,Chuang I.量子计算和量子信息(二)[M].郑大钟，赵千川，译.北京：清华大学出版社，2005:100-121.

[5] Gallager R.Low-density parity-check codes[J].IEEE Transactions on Information Theory,1962:21-28.

[6] Postol M S.A proposed quantum low density parity check code.arXiv:quant-ph/0108131,2001,29.

[7] Mackay D,Mitchison G,Mcfadden P.Sparse graph codes for quantum error-correction[J].IEEE Transactions Information Theory,2004,50:2315-2330.

[8] Ohata M,Matsuura K.A method of constructing CSS codes with LDPC codes for the BB84 quantum key distribution protocol.arXiv:quant-ph/0702184v1,2007.

[9] 赵生妹，李飞，郑宝玉.基于经典计算机的量子加密算法仿真[J].量子电子学报，2004,21:331-336.