一种基于量子纠错编码的量子密钥分配协议

赵生妹 李苗苗 郑宝玉
(南京邮电大学信号处理与传输研究院 南京 210003)

摘 要：量子加密从物理机制上保证了密钥分配的绝对安全，然而由于量子密钥分配过程中量子信道存在噪声，使得传输效率不高的量子密钥分配效率进一步降低。量子低密度奇偶校验(量子 LDPC)码由于在码长和码率的选择方面具有巨大的灵活性，且信赖于稀疏图，已成为目前量子纠错编码的研究热点。该文借鉴经典纠错编码能够提高传输可靠性的特性，针对 BB84 协议，设计一种基于量子 LDPC 码的 BB84 协议。通过数值仿真，分析量子 LDPC 码对 BB84 协议的密钥传输效率的影响。结果表明基于量子纠错码的 BB84 协议的密钥传输效率得到提高，验证了在含噪量子信道中基于量子 LDPC 码的量子密钥分配协议的有效性。

关键词：信息安全；量子密钥分配协议；量子 LDPC 码；密钥传输效率
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2009)04-0954-04

A Novel Quantum Key Distribution Protocol Based on Quantum Error Correction Code

Zhao Sheng-mei Li Miao-miao Zheng Bao-yu
(*Institute of Signal Processing and Transmission*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210003, *China*)

Abstract: Quantum cryptograph ensures the absolute security of key distribution on physics. However, not too high key transmission efficiency will be further reduced because of the noise in the quantum channel of key distribution. Having great flexibility with respect to block-length and rate, quantum Low Density Parity Check (LDPC) code based on sparse-graph becomes a hot topic in quantum error correction. Borrowing from the idea that the transmission reliability can be improved with error correction code in classical communications, a novel BB84 key distribution protocol is designed based on quantum LDPC in this paper. By numerical simulation, the effect of quantum error correction code on BB84 protocol is analyzed in the case of the transmission efficiency. The results show that quantum LDPC codes have good ability to overcome the noise, raise the transmission efficiency, and verify the availability of the proposed model.

Key words: Information security; Quantum key distribution protocol; Quantum Low Density Parity Check (LDPC) code; Key transmission efficiency

1 引言

加密算法的安全性是信息机密性、完整性和可用性的基础。经典信息论已证明了使用与消息等同长度的密钥，进行一次一钥加密，具有绝对的安全性。由于量子巨大的并行计算能力，理论上已证明一旦量子计算机出现，现有的加密算法不再安全[1,2]。量子密钥分配协议给出了一种全新的思路来解决密钥分配问题。与经典密钥分配过程不同，量子密钥分配依赖于物理定律保证了密钥分配的安全性，同时在密钥分配过程中依据物理特性提供外界窃听的检测机制[3]。最著名的密钥分配协议是1984年Bennett和Brassard提出BB84量子密钥分配协议(Quantum Key Distribution, QKD)，通常为了分析简便，协议中量子信道是假设不含噪声的。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态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(QBER)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)，而误判为窃听者存在，放弃这次密钥的获取。这样将进一步降低通过每次量子密钥分配获取共享密钥的概率。借鉴经典信道中通过纠错编码能够提高含噪信道传输的可靠性特性，本文考虑将量子纠错编码应用到量子密钥分配的协议中，提高密钥传输效率。

构造量子纠错码常用的方法之一是基于Calderbank-Shor-Steane码(也称CSS码)[4,5]，CSS码是直接从经典线性纠错码获得量子纠错码的一种方法。低密度奇偶校验(Low-

2007-12-03 收到，2008-11-24 改回
国家自然科学基金(60672133)，江苏省自然科学基金(BK2006236)，江苏省“青蓝工程”(No.TJ207006)和教育部博士点专项科研基金(20060293003)资助课题

Density Party-Check，LDPC)码是一种性能接近香农极限(Shannon-limit)的好码[6]，最大特点是它的校验矩阵是稀疏的，即校验矩阵中只有很少部分“1”元素，其它均为“0”元素。由于它是一种线性分组码，可直接在此基础上通过CSS方法构造相应量子码。Postol曾在有限几何LDPC码的基础上提出构造量子LDPC码的构造思路[7]；Mackey等人在CSS码基础上，利用特殊稀疏序列提出了几种构造量子LDPC码校验矩阵的方法，获得相应的量子LDPC码的校验矩阵[8]。我们在基于稀疏循环序列经典LDPC码构造方法的基础上，结合CSS编码原理，给出一种量子LDPC码的构造方法[9]。

量子 LDPC 码与其它量子纠错码相比，具有以下特性：(1)它的经典对应码是目前最好的纠错码，依赖于稀疏图特性；(2)稀疏图码使得与量子纠错过程相互作用的量子位数保持最少，每个量子比特只与有限量子位作用，对于正则量子 LDPC 码，作用位数与码长无关；(3)码长和码率选择具有巨大的灵活性。与量子 CSS 码应用于量子公钥密码和消息认证[10]、量子直接安全通信[11]不同。本文将在已获得的量子 LDPC 码的基础上，借鉴经典纠错码的使用方法，结合 BB84 协议，提出一个基于量子 LDPC 码的 BB84 协议，以克服量子噪声对密钥传输效率的影响，并通过数值仿真分析这种协议对提高密钥传输效率的作用。

2　BB84 协议及量子纠错编码基本理论

2.1 BB84 协议模型

密钥的产生和分配常常涉及三方，一般假设 Alice 和 Bob 为合法通信者，Eve 为窃听者。考虑 BB84 协议模型[1,12]。设有两对相互正交的粒子极化基：水平/垂直极化基(以⊕表示)和对角线斜极化基(以⊗表示)，对它们进行相应的编码：在水平垂直基空间中$|0>$为 0，$|1>$为 1；在对角线斜极化基空间中$|+\rangle$为 0，$|-\rangle$为 1，且$|+\rangle=(1/\sqrt{2})(|0\rangle+|1\rangle)$，$|-\rangle=(1/\sqrt{2})(|0\rangle-|1\rangle)$。Alice 随机选择两个不同基对密钥消息序列(0 和 1 的比例接近 1/2)编码并发送相应的极化光子序列。Bob 也随机地选择一组极化基对 Alice 发送来的极化光子进行测量，并相互通过公共信道比较所选极化基，将相同极化基所对应的测量结果保留为原始密钥，丢弃不相同极化基所对应的信息。为了检测 Eve 是否窃听，还必须对原始密钥进行一系列的操作，如数据筛选、数据纠错和保密加强等，然后计算误码率，判断该误码率是否小于 BB84 的安全标准。如果不符合安全标准，则需放弃这次密钥分配，最后才能获得在不可克隆原理保证下具有足够安全的密钥。

2.2 量子纠错编码理论

量子纠错码依赖于量子比特。单量子比特是一量子态，可以处于$|0>$，$|1>$两个特征态的任意叠加态，表示为$|\psi\geq a|0>+b|1>$，其中 a,b 是可连续取值的复数，满足$|a|^2+|b|^2=1$。n 个量子比特串可表示 $N=2^n$ 维 Hilbert 空间中的态矢量，记着$|\psi\rangle=\sum_{i=0}^{N-1}\psi_i|i\rangle$，其中$\sum_x|\psi_i|^2=1$。量子纠错码的重要作用是克服量子态与环境作用引起的消相干错误，需要注意的是这种错误为连续错误。常用的解决方法是将量子错误看作是一种线性算子，它的作用使正确的量子态变化为错误态。对于一个量子比特来说，量子错误算子可表示为 2×2 的复酉矩阵，它们分别是发生比特翻转的错误算子($\boldsymbol{X}$)，发生相位翻转的错误算子($\boldsymbol{Z}$)和同时发生比特翻转和相位翻转的错误算子($\boldsymbol{Y}$)。加上没有发生错误的算子($\boldsymbol{I}$)，统称为 Pauli 矩阵，具体形式为

$$\boldsymbol{X}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\quad \boldsymbol{Y}=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix},\quad \boldsymbol{Z}=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix},\quad \boldsymbol{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \tag{1}$$

因为作用在单量子比特上的任何酉算子都可表示为 Pauli 矩阵的线性组合，所以如果一种量子码能纠正 $\boldsymbol{X},\boldsymbol{Y}$ 和 $\boldsymbol{Z}$ 这 3 种类型的错误，则它将能纠正任何错误。

重要的一类量子纠错编码称为 CSS 码，它是由 Calderbank, Shor 和 Steane 共同提出的[4,5]。一个 CSS 码是由一组线性码所构造。对于一组线性码 $C_1(n,k_1)$ 与 $C_2(n,k_2)$，其中 $C_2\subset C_1$，即 $k_2<k_1$。长为 k_1-k_2 的 CSS 码是由所有量子态 $|x+C_2>$ 张成的空间，其中 $x\in C_1$，而量子态 $|x+C_2>$ 定义为

$$\left|x+C_2\right\rangle=\frac{1}{\sqrt{2^{k_2}}}\sum_{y\in C_2}|x+y\rangle \tag{2}$$

这里“+”表示的是模 2 加。CSS 码实际上是在 C_1 内所有 2^{k_1} 个码字中逐列表示为 $2^{k_1-k_2}$ 个以 C_2 为基础的陪集，因此它的维数为$|C_1|/|C_2|=2^{k_1-k_2}$，即有 $2^{k_1-k_2}$ 逻辑态，于是通过式(2)可获得 $2^{k_1-k_2}$ 个逻辑态。由于错误算子 $\boldsymbol{Y}$ 可以表示同时发生比特翻转和相位翻转，所以我们能够利用 C_1 和 $C_2^{\perp}$ 的经典纠错性质来检测和纠正这一量子错误。其中利用 C_1 的纠错性能，对 CSS(C_1,C_2) 上最多 t 个比特翻转错误进行纠正，利用 $C_2^{\perp}$ 的经典纠错性质，对 CSS(C_1,C_2) 上最多 t 个比特的相位翻转错误进行纠正。

3　基于量子 LDPC 码的 BB84 协议模型

3.1 量子 LDPC 码的构造

首先，我们按照一种简单的量子 LDPC 码的构造方法[13]构造量子 LDPC 码。假设 LDPC 码 C_1 的校验矩阵是 $\boldsymbol{H}_1$，维数为 $M\times N(M<N)$；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。则由此构造过程可知 $C_2\subset C_1$，根据 CSS 码的定义式，可获得基于 CSS 的量子 LDPC 码。现以量子 LDPC 码(25,5)为例具体描述该方法的构造过程：

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

(2)从 $\boldsymbol{H}_1$ 中选出 15 列，构成(10×15)维矩阵 $\boldsymbol{H}_1'$，并把

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

图 1 LDPC 码 $C_1(25,15)$的校验矩阵 $\boldsymbol{H}_1$

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

很显然，经过上述过程所产生的 C_1 和 C_2 不仅码长相同，而且满足 $C_2 \subset C_1$，具备了构造量子 CSS 码的条件。按照 CSS 码的构造方法，能够获得相应的量子 LDPC 码。为了验证该方法获得的量子 LDPC 码的纠错性能，现以量子 LDPC 码(n=25，k_1-k_2=15 − 10)为例，用它编码长为 20000 的消息序列，同时在仅考虑比特错误的信道中传输。接收端采用 BP 译码算法获得块错误概率与信道比特翻转概率关系，结果如图 2 所示，其中 BP 译码算法最大循环次数设为 100。图 2 结果表明随着信道比特翻转概率的增加，量子 LDPC 码的纠错能力逐渐下降。在仅考虑 20000 个消息序列的情况下，该方法构造的量子 LDPC 码具有较好的克服噪声的能力。

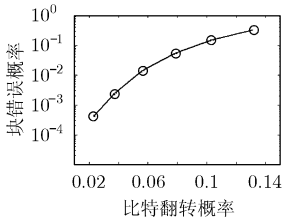

图 2 仅考虑比特翻转错误时量子 LDPC 码块错误概率与信道比特翻转概率间关系

3.2 基于量子 LDPC 码的 BB84 协议模型

在获得量子 LDPC 码的构造方法后，本文给出一种应用于含噪量子信道的 BB84 量子密钥分配协议的修改模型。在无噪 BB84 量子密钥分配协议模型基础之上，假设发送方 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。利用量子纠错编码技术，现设计一种基于量子 LDPC 码的 BB84 协议模型，与 BB84 协议模型描述类似，新的协议模型的具体步骤如下：

(1)Alice 准备要发送的二进制消息序列和一组与消息序列长度一致的发送基(等概地选择 $\oplus$ 或者 $\otimes$)，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，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纠错编码。然后将编码后的极化态发送到量子信道上，这时发送基也相应地变换为由逻辑态构建的 $\oplus$ 和 $\otimes$ 基；

(3)极化态在量子信道上传输，受量子噪声干扰，极化态可能发生相位翻转或者比特翻转或者相位和比特同时发生翻转等 3 种错误模式。考虑到 CSS 码特点，即相位和比特同时翻转错误等价于“比特翻转错误 + 相位翻转错误”；相位翻转错误可等价于“非门 + 比特翻转错误 + 非门”，现仅考虑量子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(等概率地选择由逻辑态构造的 $\oplus$ 或者 $\otimes$)待用。根据经典信道上与 Alice 交换的信息，只保留与 Alice 选择的测量基相一致的对应位置上的极化态；

(5)对保留的极化态将采用量子 LDPC 的 BP 译码算法译码，纠正在传输过程中受噪声干扰引起的比特错误。对译码后仍未能纠正的错误极化态作丢弃处理；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(4)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。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。

同常见的 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，通过估计值与预先设定的门限值比较，判断是否存在窃听，能否获取安全的密钥。

4 数值计算和分析

为了进一步说明上述改进模型，现通过数值计算方法，分析在含噪量子信道上基于量子 LDPC 的 BB84 协议的抗量子噪声性能。首先 Alice 随机地选择一个长的二进制消息序列，按协议步骤第(1)步制备成一系列量子态。然后依据第(2)步对每个量子态进行编码，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为

$$0\rightarrow\begin{cases}\oplus\rightarrow|0\rangle_L\\ \otimes\rightarrow\dfrac{1}{\sqrt{2}}(|0\rangle_L+|1\rangle_L)\end{cases},\ 1\rightarrow\begin{cases}\oplus\rightarrow|1\rangle_L\\ \otimes\rightarrow\dfrac{1}{\sqrt{2}}(|0\rangle_L-|1\rangle_L)\end{cases}\tag{3}$$

其中 $|0>_L$, $|1>_L$ 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(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，即 Bob 选择译码的极化态个数为传送总个数的一半左右。通过量子码的译码，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，为了方便比较，本文同时计算了含噪信道上的不带量子纠错码的 BB84 协议。此时，Bob 保留的原始密钥是他的测量基与 Alice 的发送基相一致的相应位置上的测量结果。由于量子信道存在噪声，如比特翻转错误，那么他保留的原始密钥也可能将是一个错误的测量结果。

为了直观显示量子 LDPC 对 BB84 协议克服量子噪声的作用，现给出基于量子纠错编码的 BB84 协议的密钥传输效率性能的数值计算。假设发送消息序列长度是 50000，量子 LDPC 码(25,5)的码长 25，码率为 0.2，量子 LDPC 码的译码方法仍采用 BP 算法，迭代的最大循环次数设置为 100。图 3 显示了含噪量子信道中基于量子编码 BB84 协议，不带量子纠错编码的 BB84 协议和理想量子信道下 BB84 协议中密钥传输效率与信道比特翻转概率的关系。值得说明的是模型中的测量都假设为理想情况，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 Alice 发送消息序列中的相对应比特相同。

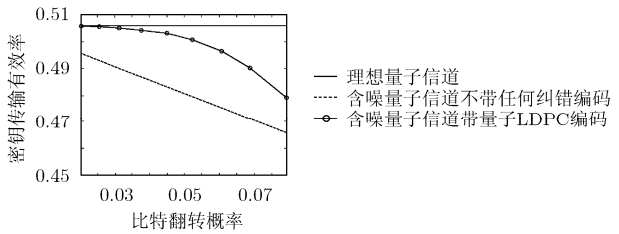

图 3 BB84 协议通信中密钥传输有效率与比特翻转概率关系曲线

由图 3 可知，理想量子信道(即不含噪声)下 BB84 协议的密钥传输效率为 50.6%(即对应于理想信道曲线的纵坐标值)。事实上，理想信道的密钥传输效率与比特翻转概率之间不存在关系曲线，为了给后两种情况作参考，才把理想信道的效率用直线表现出来。而且在理想情况下，由于 Bob 有一半的概率能获得密钥，所以密钥传输效率应在 50%左右，实验中得到的 50.6%结果与实际相符。从图还可以看出，当信道受噪声干扰时，基于量子 LDPC 码的 BB84 协议的密钥传输效率要明显高于不带纠错编码的 BB84 协议。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，验证了基于量子纠错编码的 BB84 模型的有效性。

5　结束语

基于量子力学特性的量子密钥分配协议具有可证明的安全性，并提供对窃听者行为的可检测机制，这是现有的所有的密钥分配过程无法比拟的。但是由于量子密钥分配协议的特点，使得密钥传输效率不高，而且量子噪声将进一步降低密钥传输效率。本文借鉴经典纠错编码有效提高传输可靠性的特性，针对 BB84 协议，设计一种基于量子纠错编码的 BB84 协议。通过数值计算验证了该协议的有效性。量子密钥分配中较低的密钥传输效率是量子加密实现中的一大困难，基于量子纠错编码的量子密钥分配协议的提出为有效解决困难给出一个新的方向。

参 考 文 献

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

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

[3] Masato Koashi. Unconditional security of quantum key distribution and the uncertainty principle. *J. Phys.*: *Conf. Series*, 2006, 36: 98–102.

[4] Calderbank A R and Shor P W. Good quantum error correcting codes exist. *Phys. Rev. A*, 1996, 54: 1098–1105.

[5] Steane A M. Multiple particle interference and error correction. *Proc. Royal Society of London Series A*, 1996, 452: 2551–2577.

[6] MacKay D and Neal R M. Near Shannon limit performance of low density parity check codes. *Electronic Letters*, 1996, 32(18): 1645–1646.

[7] Postol M S. A proposed quantum low density parity check code. http://xxx.lanl.gov/abs/quant-ph/0108131, 2001.

[8] MacKay D J C, Mitchison G, and McFadden P L. Sparse graph codes for quantum error correction. *IEEE Trans. on Information Theory*, 2004, 50(10): 2315–2330.

[9] 蔡镇, 赵生妹. 一种基于稀疏循环序列的量子低密度校验码的构造. 南京邮电大学学报(自然科学报), 2007, 27(4): 54–59.

[10] 李峥, 马智, 吕欣等. 基于量子 CSS 纠错码的量子公钥密码和消息认证. 电子与信息学报, 2006, 28(3): 537–541.

[11] 冯国登. 基于量子 Calderbank-Shor-Steane 纠错码的量子安全直接通信. 软件学报, 2006, 17(3): 509–515.

[12] 赵生妹, 李飞, 郑宝玉. 量子密钥分配协议在概率克隆/重发攻击下的安全性. 电子与信息学报, 2005, 27(10): 1639–1642.

[13] Ohata M, Matsuura K. A method of constructing CSS codes with LDPC codes for the BB84 quantum key distribution protocol. http://xxx.lanl.gov/abs/quant-ph/0702184, 2007.

赵生妹：　女，1968 年生，教授，博士，研究方向为量子信息处理、无线网络信号处理.

李苗苗：　女，1984 年生，硕士生，研究领域为量子信息处理.

郑宝玉：　男，1945 年生，教授，博士生导师，研究方向为智能信号处理.