基于 Polar 码的纠错延后量子协商协议

肖红*, 施鹏, 赵生妹

南京邮电大学信号处理与传输研究院, 南京 210009

* E-mail: 15951906299@163.com

收稿日期: 2014-10-30; 接受日期: 2015-01-21

国家自然科学基金(批准号: 61271238, 61475075)、教育部高等学校博士学科点专项科研基金(编号: 20123223110003)、江苏省高校自然科学基金研究项目(编号: 11KJA510002)和江苏高校优势学科建设工程项目资助

摘要 提出了一种基于纠错(EC)延后的量子密钥分发协商协议. 该协议不直接对密钥进行 EC, 而是将 EC 延后到信息交换后进行. 这种量子密钥分发协商协议具有两个优点: 1) EC 延后可使量子密钥分发网络中不直接相连的两个节点通过共同的可信节点共享密钥串; 2) EC 延后可简化整个协商过程, 只通过简单的信道编码就能完成 EC, 还能同时纠正通信过程中产生的误码和信息本身存在的误码. 本文理论上分析了所提协议的密钥利用率; 并以误比特率为标准, 结合 Polar 信道编码, 通过数值仿真说明所提协议的可靠性与安全性, 并与等同条件下应用低密度奇偶校验码(LDPC 码)的量子密钥分发协商协议进行比较, 结果表明基于 Polar 码的协商协议可获得更加完善的性能.

关键词

量子密钥分发协商
纠错延后
Polar 码

1 引言

量子密钥分发协议(QKD)中, Alice 将信息编码于量子态中, 并将量子态通过一个物理通道(如光纤或自由空间)传送给 Bob; Bob 接收量子态后对其测量以获得原始信息. 经过对基、窃听测试、纠错(error correction, EC)及秘密放大(private amplifier, PA)后, Alice 与 Bob 间获得一致的安全密钥. QKD 的绝对安全性由量子力学的海森堡测不准原理和量子不可克隆定理保证, 在 QKD 整个协商传输过程中, 即使窃听者 Eve 拥有无限的计算能力也无法获得密钥串信息^[1].

协议中 Alice 和 Bob 合法用户双方通过测量与对基, 共享一组长度为 n 的比特串 X 和 Y (Alice 获得含有共享比特串的随机序列 X , Bob 获得含有共享比特

串的随机序列 Y), 而传输过程中窃听者 Eve 也可能获取一组与 X 和 Y 相关的随机序列 Z . 但是由于实际量子信道中环境噪声的干扰, 以及可能存在着设备缺陷, X 与 Y 中有些位置的比特值会存在一定的误差, 同时窃听方随机序列 Z 可能窃取到部分密钥信息, 因此完整的 QKD 协商协议还需在测量和对基以后进行两个重要的后处理过程, EC^[2]和 PA^[3]. 前者也称为协商协议(reconciliation), 它是指纠正比特串 X 和 Y 中的误差, 而后者通过函数映射保证了 Eve 不能从 Z 中获取密钥信息^[4].

1984 年, Bennett 和 Brassard 提出第一个 QKD, 即 BB84 协议^[5], 这是迄今为止最成熟、应用最广的 QKD, 其安全性已从理论上得到严格的证明. 在 BB84 协议中, 存在 2 对互无偏极化基: 水平垂直极化基(以 $\oplus$ 为表示)和斜极化基(以 $\otimes$ 表示), 其中在水

引用格式: 肖红, 施鹏, 赵生妹. 基于 Polar 码的纠错延后量子协商协议. 中国科学: 技术科学, 2015, 45: 843–848

Xiao H, Shi P, Zhao S M. A reconciliation protocol with delayed error correction for quantum key distribution (in Chinese). Sci Sin Tech, 2015, 45: 843–848, doi: 10.1360/N092014-00228

平垂直基中 $|0\rangle$ 编码为 0, $|1\rangle$ 为 1; 斜极化基中 $|+\rangle$ 为 0, $|-\rangle$ 为 1. Alice 随机选择一组基对消息序列编码并发送相应的极化光子序列. Bob 也随机地选择极化基对 Alice 发送来的极化光子进行测量, 并通过公共信道相互对比极化基, 将相同极化基所对应的测量结果保留为原始密钥. 若窃听测试的量子误码率小于安全阈值, 通过量子协商和 PA 等技术, 可得到安全密钥. 协商协议迄今也已经有一些发展, 其中 Cascade 协商协议是 Brassard 和 Salvail^[6]于 1994 年首先提出的协商协议, 其采用奇偶校验码, 但是该协议需要 Alice 和 Bob 双方进行一定步数的交互通信后才能完成 EC, 步数多少由错误概率估值计算获得. 随后为了减少通信双方的交互性, 有学者对分块长度的优化进行了很多研究, 如 Sugimoto 和 Yamazaki^[7]在保证误比特率处于非常低的范围内的同时研究出了最佳分块长度的确定方法; 后来又有学者对 Cascade 协商协议进行了优化改进, 比如 Buttler 等人^[8]在提出的 Winnow 协议中采用了汉明码, 以及 Liu 等人^[9]提出的用来优化协调中每比特所需信息的 Liu 协调协议. 随着现代编码理论的发展, 相关信源压缩编码的思想也被应用到 QKD 协商协议中, 如 Nguyen 等人^[10]提出将 Turbo 码应用到 QKD 协商协议中; Duligall 等人^[11]和 Elkouss 等人^[12]提出将低密度奇偶校验码 (LDPC 码) 应用到 QKD 协商协议中, 2013 年南京邮电大学 Zhao 等人^[13]和 Gong 等人^[14]又将轨道角动量 (OAM) 应用到 QKD 协商协议中.

信道编码的选择对协商协议的效率起到关键作用, 因此选择能达到信道容量的编码至关重要. Polar 码是 Arikan 在 2007 年提出的一种编码方式, 并且 Arikan 证明了对于二进制对称信道(BSC)Polar 码可以达到信道容量, 后来, Korada, Urbanke 和 Sasoglu 等人证明了对于任意的二进制输入离散信道(DMC), Polar 码同样可以达到信道容量; 另一方面, Polar 码的编译码复杂度都较低^[15], 所以一经提出就引起了海内外广大学者的关注. 利用 Polar 码的优势, Jouguet 和 Kunz-Jacques^[16]将 Polar 码应用到 QKD 协商协议中, 但是采用了相关信源编码与联合译码.

QKD 网络中存在着两个节点不直接相连, 但有与这两个节点都相连的共同可信节点的特殊情形, 此时常用的协商协议将不适用. 鉴于文献[4]在这种情形下提出了一种 PA 延后思想, 通过 PA 延后以实

现密钥共享. 本文提出了一种基于 EC 延后的协商协议, 以解决 QKD 网络中这种特殊问题: 不在信息交换前完成密钥的协商过程, 而在完成信息交换后再对信息进行 EC. 这样不需要进行相关信源编码, 整个协商过程只需要直接通过简单的信道编码就能完成 EC 过程, 简化了整个协商协议; 同时通过 EC 延后, EC 过程可以同时考虑加密信息传输过程中产生的误码, 还可以一并纠正. 考虑到 Polar 码的优越性, 本文以 Polar 码为例验证 QKD 协商协议的性能.

论文章节安排主要如下: 第二节主要介绍基于 EC 延后的协商协议; 第三节主要从密钥生成率的角度对基于 EC 延后的协商协议进行理论分析; 第四节主要对基于 Polar 码的协商协议的可靠性和安全性进行仿真验证.

2 基于 EC 延后的协商协议

量子密钥分发协商协议通常在量子态传输之后需要两个后处理步骤: EC, 以确保 Alice 和 Bob 的密钥一致; PA, 以确保 Eve 没有获取到关于密钥的有用信息. 产生的最终密钥可以被用在随后的加密程序中, 如一次一密(OTP).

针对上一节提到的 QKD 网络中的特殊情形, 本文考虑不对密钥直接执行 EC 和 PA 的量子密钥分发协商协议. 假设先执行 OTP 操作, 将 EC 和 PA 延后到 OTP 之后执行, 这样执行的 OTP 的安全性较弱. 但是本文提出的 EC 延后是可执行的, 因为原来密钥中的错误只是简单地加入到 OTP 加密消息中, 比特位错误不会影响信息的安全性. 另外延后的 PA 操作可以保证密钥的安全性, 文献[4]中已经论证了 PA 延后对 QKD 协商协议的安全性和密钥生成率都不会产生影响.

下面给合图 1, 具体描述所提出的 EC 延后协议.

假设 Alice 拥有 n 比特长度的初始密钥 $\vec{a}$, 对于 Eve 可能窃取的关于这个比特串的那一部分信息, 可以通过 PA 延后来加强其安全性^[4]. Bob 也同样拥有 n 比特长度的初始密钥 $\vec{b}$, 但 $\vec{a}$ 和 $\vec{b}$ 之间由于信道噪声的存在会存在差异. 具体的 EC 延后协商协议如下.

Alice 和 Bob 合法用户双方通过测量与对基, 共享一组长度为 n 的不完全一致的比特串密钥 $\vec{a}$ 和 $\vec{b}$, 随后不直接对密钥执行 EC 和 PA, 而直接使用不完

图 1 EC 延后协商协议

全一致的密钥对信息执行 OTP 加密. Bob 使用不一致不安全的密钥加密信息, 并将加密信息传送给 Alice, Alice 接收到加密信息后也使用不一致不安全的密钥进行解密. 在这之后再执行 EC 操作和 PA 操作. 整个 EC 延后协议可用图 1 表示.

1) Alice 和 Bob 通过 BB84 协议对基测量得到存在差错的两个长度为 n 比特串 $\vec{a}$ 和 $\vec{b}$;

2) Bob 将要传送的长度为 k 的信息 $\vec{m}_1$ 通过信道编码映射到长度为 n 的比特串 $\vec{m}_2$, 之后将序列 $\vec{b}$ 与 $\vec{m}_2$ 进行模二加, 通过经典信道将结果 $\vec{b} \oplus \vec{m}_2$ 发送给 Alice (为了简化描述, 这里我们认为经典信道是无噪信道);

3) Alice 在接收到 Bob 传过来的 $\vec{b} \oplus \vec{m}_2$ 的结果后, 与 Alice 自己的初始密钥串进行异或, 得到 $\vec{a} \oplus \vec{b} \oplus \vec{m}_2$. 若用 $\vec{e}$ 表示序列 $\vec{a}$ 和 $\vec{b}$ 之间的差错图案, Alice 异或得到的结果可以表示为 $\vec{e} \oplus \vec{m}_2$;

4) 针对步骤 2) 中的信道编码方法, 对 $\vec{e} \oplus \vec{m}_2$ 进行译码, 并 EC, 即可恢复出信息序列 $\vec{m}_1$.

若考虑到 Eve 窃听到的信息, 则会有部分信息被窃听到, 不过可以根据 [4] 中提出的 PA 延后的方法将这部分被窃听的信息去掉.

对于特殊情形, QKD 网络中可能有两个节点不直接相连, 但是有与之相连的共同可信节点, 对于这样的情况协商协议可以通过 EC, PA 延后实现共享密钥串. 假设 Bob 和 Charlie 之间需要建立密钥, 但是他们之间并没有量子信道直接相连. 而双方与 Alice 都有量子信道相连, 并且 Alice 和 Charlie 之间已经共享了一个密钥池, 其中每组密钥都是绝对安全的. 我们可以通过 BB84 在 Bob 和 Alice 之间共享一对存在差错的密钥 $\vec{b}$ 和 $\vec{a}$, Alice 从密钥池中随机选出一组

密钥 $\vec{m}$, 之后 Alice 将 $\vec{a} \oplus \vec{m}$ 传给 Bob. Bob 在接收到此初步加密的序列后再用自己掌握的密钥与加密比特串进行异或操作, 则可以得到与 $\vec{m}$ 存在一定差异的比特串 $\vec{m}'$. 之后可以通过 Bob 和 Charlie 之间的经典信道执行 EC 和 PA 操作, 使得到的密钥达到绝对安全.

仔细分析基于 EC 延后的协商协议, 发现它有两个优势: 1) 当 QKD 网络中的节点不直接彼此相连, 但分别连接到一个共同的可信中继节点时, 延后 EC 对各节点间的密钥共享有很大作用. QKD 只需要在每个节点和中间信任中继器之间进行协商, 而无需在整个节点网络中都执行后处理操作. 后处理如 EC 和 PA 可以延后到某两个节点决定共享一个密钥之后, 在这种情况下, 这些后处理步骤仅在它们之间执行. 2) 该协商协议可简化整个协商过程, 只通过简单的信道编码就能完成 EC, 另外实际通信中加密信息传输过程中也会有噪声干扰, 基于 EC 延后的协商协议还能一并纠正通信过程中产生的误码和信息本身存在的误码.

3 密钥生成率性能分析

Alice 和 Bob 交换量子信息后, 双方共享一组比特串 $\mathbf{X}$ 和 $\mathbf{Y}$, 而窃听者 Eve 获有与 $\mathbf{X}$ 和 $\mathbf{Y}$ 相关的一组随机序列 $\mathbf{Z}$. 因此那些对密钥直接 EC 的协商协议理论上的密钥生成率 K_{th} 可以描述为

$$K_{th} = H(\mathbf{X} | \mathbf{Z}) - H(\mathbf{X} | \mathbf{Y}). \quad (1)$$

式中 $H(\mathbf{X} | \mathbf{Z})$ 的大小取决于 Eve 所采用的攻击方式, 而 $H(\mathbf{X} | \mathbf{Y})$ 表示在已知 $\mathbf{Y}$ 的条件下 $\mathbf{X}$ 的信息熵. $H(\mathbf{X} | \mathbf{Y})$ 也可以描述成 Bob 要纠正 $\mathbf{Y}$ 中所有错误时, 需要 Alice 传给 Bob 的最小经典信息量. 而只有当协商协议理想的情况下, $H(\mathbf{X} | \mathbf{Y})$ 才能达到最小值. 实际应用中, 由于密钥长度的限制以及编码方法的非理想性, $H(\mathbf{X} | \mathbf{Y})$ 无法达到上述理论值, 故 (1) 得到的是理论密钥生成率. 因此实际的密钥生成率 K_{real} 可以写成

$$K_{real} = H(\mathbf{X} | \mathbf{Z}) - fH(\mathbf{X} | \mathbf{Y}), \quad (2)$$

其中 f 是一个大于 1 的参数, 用来描述协商效率.

在 EC 延后的整个过程中, 使用 n 比特长的初始密钥进行加密传输 k 比特的信息, 而传输速率最大为其等价信道容量 C , 从而得到单比特密钥的利用率为

$$\eta = \frac{k}{n} = C = 1 - H(\mathbf{X} | \mathbf{Y}). \quad (3)$$

另一方面, 窃听者 Eve 根据其使用的不同的攻击方式, 获得的随机序列 Z 与初始序列 X 重合部分不同, 所以可以得到本文提出方法理论上的密钥利用率为

$$K'_{th} = H(X|Z) - H(X|Y). \quad (4)$$

上述公式(4)与(1)完全一样, 可见本文提出的将 EC 延后的协商方法理论上并没有影响密钥利用率.

在实际应用中使用的码字长度 n 有限长, 信道编码的性能往往达不到信道容量, 所以实际的密钥利用率可表示为

$$K'_{real} = H(X|Z) - gH(X|Y), \quad (5)$$

其中 g 是大于 1 的有理数. 随着 LDPC 码与 Turbo 码编译码理论的发展, 这两种码字性能已经十分接近香农限, 故在 EC 延后协商协议中使用这两种码字可以使得 g 的取值接近 1.

4 数值仿真

Alice 和 Bob 合法用户双方通过测量与对基, 共享一组长度为 n 的比特串 X 和 Y , 窃听者 Eve 也可能获取一组与 X 和 Y 相关的随机序列 Z . 离散量子密钥分发 (DVQKD) 协议和连续量子密钥分发 (CVQKD) 协议的量子信道不同, 对于 DVQKD, X 和 Y 可等效于一个 BSC 的输入和输出, 参数为量子错误概率 QBER; 对于 CVQKD, X 和 Y 可等效于是一个高斯信道 (AWGN) 的输入和输出^[14].

现通过数值仿真验证该协商协议的可靠性和安全性. 仿真中以 Polar 码为 EC 编码, 从误比特率角度

分析该方案的性能, 同时也将其性能与基于 LDPC 码 EC 延后协商方案的性能进行比较. 数值仿真中基本参数设置如下: 最大帧数设为 10^6 , 最大迭代次数为 60, 纠错码码率为 0.375, 码长为 2^9 , 可计算出纠错码中信息位长度为 192.

4.1 可靠性验证

方案的可靠性由 Alice 接收到信息的误比特率来衡量. 根据协议可知, Alice 接收到的信息与 Bob 发送信息的误差等同于 Alice 和 Bob 的密钥误差. 对于 DVQKD, Bob 的密钥可以看作是由 Alice 的密钥输入一个差错概率为 ϵ 的等价 BSC 信道的输出. 根据 BB84 协议, 差错产生概率一般控制在 10% 以内, 所以设置等价 BSC 信道的错误概率 ϵ 取值在 [0.01 0.02 0.03...0.1]. 对于 CVQKD, 设定高斯信道 AWGN 的信噪比为 5 dB. 分别对 DVQKD 和 CVQKD 进行数值仿真, 结果如图 2 所示.

由图 2 可知, 对于 Polar 码, 随着 BSC 信道错误概率的增大, 接收端接收的信息的误比特率随之变大. 但即使错误概率取最大值 10% 时, Alice 端接收信息的误比特率也在可接受范围内, 即仍几乎可以实现无差错通信. 与基于 LDPC 码的量子密钥分发协调性能相比较, 结果表明基于 Polar 码的误比特率始终比基于 LDPC 码的小. 换言之, 使用 Polar 码时的可靠性更好.

总而言之, 结合以上 Polar 码的可靠性仿真数据结果分析, Polar 码可以可靠地运用于 DVQKD 和

图 2 Alice 端接收信息的误比特率与错误概率曲线图

(a) Polar 码和 LDPC 码在 DVQKD 系统中的误比特率性能比较; (b) Polar 码和 LDPC 码在 CVQKD 系统中的误比特率性能比较

图3 窃听者 Eve 接收信息的误比特率与错误概率曲线图

(a) Polar 码和 LDPC 码在 DVQKD 系统中的误比特率比较; (b) Polar 码和 LDPC 码在 CVQKD 系统中的误比特率比较

CVQKD, 保证数据可靠准确地传送到接收端.

4.2 安全性的验证

方案的安全性可以由窃听端 Eve 接收信息的误比特率来衡量. 根据协议可知 Eve 窃取的信息与 Bob 发送的正确信息的误差等同于 Alice 和 Eve 窃取的密钥误差. 对于 DVQKD, Eve 窃取的密钥可以看作是由 Alice 的密钥通过一个概率误差为 0.5 的 BSC 信道得到的. 对于 CVQKD, 设定高斯信道的信噪比为 5 dB. 分别对 DVQKD 和 CVQKD 进行数值仿真, 结果如图 3.

由图中曲线可知, 窃听者窃听到的结果译码后误比特率较大, 趋近于 1, 即窃听者窃听到的信息量趋于零. 而且与基于 LDPC 码的性能进行比较, 其窃听到的信息的误比特率比 LDPC 码大很多. 换言之, 基于 Polar 码的协商协议的安全性比基于 LDPC 码的安全性更好.

总而言之, 结合以上 Polar 码的安全性仿真数据结果分析, Polar 码可以保证安全地运用于 DVQKD 和

CVQKD.

5 结束语

本文对传统的量子密钥分发协商协议进行了 EC 延后的改进. 这种基于 EC 延后的量子密钥分发协商协议能够为 QKD 网络中不直接相连但有共同可信节点的两个节点之间建立密钥; 同时该方案还有两个优点: 1) EC 延后可以直接通过简单的信道编码来完成 EC 过程, 而不是相关信源编码; 2) 通过 EC 延后, EC 过程可以同时考虑加密信息传输过程中产生的误码, 还可以一并纠正. 论文证明了基于 EC 延后的量子密钥分发协商协议没有影响密钥利用率. 最后本文将 Polar 码应用到该量子密钥协商协议中, 并与基于 LDPC 码的协商性能比较, 结果表明基于 Polar 码的 EC 延后量子密钥分发协商协议的误比特率在允许误差范围中, 且性能好于基于 LDPC 码的 EC 延后量子密钥协商协议.

参考文献

- 1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. New York, 1984. 175–179
- 2 Shannon C E. A mathematical theory of communication. Bell Syst Tech J, 1948, 27: 379–423
- 3 Bennett C H, Brassard G, Robert J M. Privacy amplification by public discussion. SIAM J Comput, 1988, 17: 210–229
- 4 Fung C H F, Ma X, Chau H F, et al. Quantum key distribution with delayed privacy amplification and its application to the security proof of a two-way deterministic protocol. Phys Rev A, 2012, 85: 2308–2317
- 5 Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
- 6 Brassard G, Salvail L. Secret key reconciliation by public discussion. Lecture Note in Computer Science. 1994, 765: 410–423
- 7 Sugimoto T, Yamazaki K. A study on secret key reconciliation protocol “Cascade”. IEICE Trans Fundamentals, 2000, E83-A: 1987–1991

- 8 Buttler W T, Lamoreaux S K, Torgerson J R, et al. Fast, efficient error reconciliation for quantum cryptography. *Phys Rev A*. 2003, 67: 2303–2310
- 9 Liu S, Tilbrog H C A V, Dijk M V. A practical protocol for advantage distillation and information reconciliation. *Des Codes Cryptography*, 2003, 30: 39–62
- 10 Nguyen K C, Assche G, Cerf N J. Side-information coding with turbo code and its application to quantum key distribution. *International Symposium on Information Theory and its Applications*. Parma, 2004
- 11 Duligall J L, Godfrey M S, Harrison K A, et al. Low cost and compact quantum cryptography. *New J Phys*, 2006, 8: 249–265
- 12 Elkouss D, Leverrier A, Alléaume R, et al. Efficient reconciliation protocol for discrete-variable quantum key distribution. *IEEE Int Symp Information Theory Seoul*, 2009, doi: 10.1109/ISIT.2009.5205475
- 13 Zhao S M, Gong L Y, Li Y Q, et al. A large-alphabet quantum key distribution protocol using orbital angular momentum entanglement. *Chin Phys Lett*, 2013, 30: 060305
- 14 Gong L Y, Pan J X, Liu B B, et al. A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords, *J Comput Sys Sci*, 2013, 79:122–130
- 15 Arkan E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans Inform Theory*, 2009, 55: 3051–3073
- 16 Jouguet P, Kunz-Jacques S. High performance error correction for quantum key distribution using polar codes. *arXiv*: 1204.5882

A reconciliation protocol with delayed error correction for quantum key distribution

XIAO Hong, SHI Peng & ZHAO ShengMei

Institute of Signal Processing & Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210009, China

A delayed error-correction (EC) reconciliation protocol for quantum key distribution (QKD) is proposed in the paper, where the error correction operation is operated after the messages have been transmitted. There are two advantages of the proposed protocol. First, it is possible for the two nodes without a direct quantum link to share secret keys, when the two nodes are separately connected to a common trusted relay in the QKD network. Besides, the reconciliation protocol with the delayed EC also simplifies the whole reconciliation process. It corrects both errors caused by communications during QKD process and that inherent in message bits. The key generation rate of the delayed EC protocol is presented. Finally, the bit error rate of the proposed protocol is analyzed when using polar codes as the error correction codes. The results show that the performance of the delayed EC reconciliation protocol with polar codes were better than those using low-density parity check code.

quantum key distribution reconciliation, delayed error correction, polar codes

doi: 10.1360/N092014-00228