一种基于 BB84 协议的量子密钥分配改进方案

栾　欣，郭义喜，苏锦海，赵洪涛
（解放军信息工程大学，郑州 450004）

摘　要：针对 BB84 协议对存在窃听的有噪信道中进行量子密钥分配效率不高的问题，提出一种改进方案。新方案在发送方与接收方都加入类似签名的过程，能够很好地判断窃听的存在，并且窃听者只能获取少量的密钥信息，在保障传输过程安全的同时，提高了量子密钥分配的效率。

关键词：量子密钥分配(QKD)；BB84 协议；错误率；信道噪声
中图分类号：TP393.04　　**文献标志码**：A　　**文章编号**：1001-3695(2013)09-2807-03
doi:10.3969/j.issn.1001-3695.2013.09.063

Improved scheme of quantum key distribution based on BB84 protocol

LUAN Xin, GUO Yi-xi, SU Jin-hai, ZHAO Hong-tao
(*PLA University of Information Engineering*, *Zhengzhou* 450004, *China*)

Abstract: In order to solve the low transmission efficiency problem of the BB84 protocol in the noisy channel with wiretap inside, this paper proposed an improved scheme. The new scheme added a process, similar to signature, to the sender and the receiver, was able to judge the existence of eavesdropping, and the eavesdropper could only get a small amount of key information. So, the new scheme ensures the safety of the transmission process, at the same time, improves the efficiency of the quantum key distribution.

Key words: quantum key distribution(QKD); BB84 protocol; error rate; channel nois

现代社会人们对于通信的安全性要求越来越高。目前大规模使用的加密算法都是传统的加密方式，依赖于数学算法的复杂性，在安全上没有严格的证明。尤其在信息产业迅猛发展的今天，计算机技术日新月异，原先许多看似安全的加密算法在更加强大、高效的计算机面前败下阵来。因此，寻求一个在理论上绝对安全的通信协议迫在眉睫，量子密码学和量子密钥分配(QKD)应运而生。经典信息论已经证明使用与消息等长度的密钥，对信息进行一次一密加密，在理论上具有绝对的安全性。QKD 正是基于一次一密的安全理论，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，QKD 依赖于更为本质的物理规律，即量子力学中的海森堡测不准原理和量子态不可克隆定理；同时在密钥分配过程中提供针对外界窃听的检测机制，也就是说，如果窃听者尝试拦截和处理量子传输信息，将不可避免地留下痕迹，最终只能被发现。

从 1984 年第一个 QKD 协议到现在，国内外提出了大量基于 BB84 协议的改进协议或者全新的 QKD 协议。但是很少能非常简单地解决这类问题：在有噪信道中，如何判断传输信息的错误率是由信道噪声产生，还是存在窃听引起的，这就导致接收方有时无法准确判断错误产生的原因，也就无法判定是否存在窃听，只能盲目地丢弃信息，极大地影响了密钥分配效率。本文在介绍 BB84 协议的基础上对其进行改进，提出一种新的 QKD 协议，对于一个给定的信息量，该协议可以有效地减少窃听者能够从中获取的信息，并且无论何时，一旦窃听出现，信息的错误率将明显增长。

1　BB84 协议

QKD 只用来产生和分配密钥，而不传输任何的通信信息。这些密钥是用来辅助选用的加密算法对信息进行加解密，加密之后的信息才能在信道上传输。在 BB84 协议中，量子通信实际上是由两个阶段完成的：a)通过量子信道进行密钥的通信；b)通过经典信道进行密钥的协商，探测窃听者是否存在，然后确定最后的密钥。其通信系统如图 1 所示。

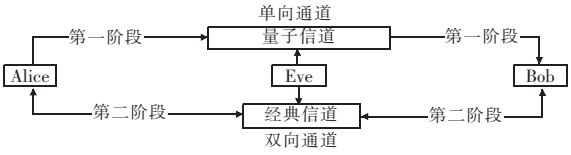

图 1　BB84 协议中的量子通信系统

BB84 协议使用了两套不同的正交基：a)线性偏振状态 $|0°\rangle$ 和 $|90°\rangle$（代表水平线性偏振状态和垂直线性偏振状态），用直线基“+”表示；b)旋转偏振状态 $|45°\rangle$ 和 $|135°\rangle$（代表右旋和左旋），用斜线基“×”表示。因此，根据表 1 中量子信息比特与量子状态基的具体对应关系可知，从 Alice 发送到 Bob 的量子有四种状态：$|0\rangle$，$|1\rangle$，$|+\rangle$，$|-\rangle$，其中，$|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$，$|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$。

收稿日期：2012-11-28；**修回日期**：2013-01-11

作者简介：栾欣(1988-)，男，江苏南京人，硕士研究生，主要研究方向为量子密码学、量子密钥服务与管理(luanxinfanrong@sina.com)；郭义喜(1971-)，男，山东烟台人，副教授，主要研究方向为量子密码学、质量检测与认证、网络安全；苏锦海(1968-)，男，河北张家口人，教授，主要研究方向为军事通信学、信息安全、密钥服务与管理；赵洪涛(1982-)，男，河南郑州人，硕士研究生，主要研究方向为军事通信学.

表 1 量子信息比特与量子状态基的对应关系表

量子比特	+	×
0	$\|0°\rangle$,$\|0\rangle$	$45°\rangle$,$\|+\rangle$
1	$\|90°\rangle$,$\|1\rangle$	$135°\rangle$,$\|-\rangle$

BB84 协议的执行过程可以通过以下步骤来完成:

1)量子信道

a)Alice 准备 m 个比特为 0 和 1 的量子,两类量子数量相当,每个比特为 0 的量子随机地取$|0\rangle$和$|+\rangle$两种状态之一,每个比特为 1 的量子随机地取$|1\rangle$和$|-\rangle$两种状态之一,然后通过量子信道发送给 Bob。

b)Bob 随机地选取两组测量基“+”和“×”中的一种,对接收到的量子进行测量,得到自己的量子比特。

2)经典信道

c)Bob 与 Alice 通过经典信道公布自己的测量基,Alice 告诉 Bob 哪些测量基是与自己相同的,也就是正确的。

d)Bob 丢弃那些测量基不同情况下得到的比特,得到初步的共享密钥。

e)Bob 随机选取一些密钥发送给 Alice,Alice 确认是否一致,这个过程通常要执行几次,确认没有错误产生。

f)最后通过一些错误修正和保密放大得到最终的密钥。

表 2 给出了一个从发送者到接收者的 BB84 协议实现的具体例子。需要说明的是,对于一个处于旋转偏振状态的量子,如果 Bob 选用了直线基对其测量,则该量子态要么塌缩至水平态,要么成垂直态。

表 2 一个 BB84 协议具体实现过程的例子

量子	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice 的比特	1	0	0	1	1	1	0	1	0	0	0	1	1	0	1
Alice 的测量基	×	+	×	×	+	+	×	×	×	+	+	×	×	×	+
Alice 的量子态	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$
Bob 的测量基	×	+	+	×	×	+	×	+	×	+	×	×	×	+	+
Bob 的比特	1	0	1	1	1	1	0	0	0	0	0	1	1	1	1
测量基是否相同	Y	Y		Y		Y	Y		Y	Y		Y	Y	Y	
初步密钥	1	0		1		1	0		0	0		1	1		1
随机检测密钥				1						0					
Alice 进行核实				OK						OK					
剩下的密钥	1	0				1	0		0			1	1		1

从表 2 可以看出,在理想环境下,Alice 和 Bob 能产生和共享相同的随机密钥。实际应用环境中,需要考虑仪器误差和信道噪声,如果 Eve 对所有量子实行 Intercept/Resend(I/R)攻击,他能得到 50% 的信息,与此同时,Alice 和 Bob 最后共享的密钥中大约有 25% 的错误,所以他们能很容易地检测到 Eve 的存在。如果 Eve 只对 40% 的信息实行 I/R 攻击,他能得到 20% 的信息,而这时错误率将只有 10%。这种情况下,Eve 导致的错误率和信道噪声引起的错误率将无法区分(实验表明,由信道噪声和仪器误差引起的错误率大约在 10%)。为了通信安全,Alice 和 Bob 只能假定所有的错误是由 Eve 引起的,从而把原本可以接受的密钥丢弃,进行重复的传输操作,造成极大的浪费。

2 改进后的 QKD 协议

针对 BB84 协议在有噪环境中和存在窃听情况下的不足,本文对其进行改进,对于每个从 Alice 发出的量子,随机次数地执行一种类似签名的操作 $R(\phi)$;Bob 收到后,也随机次数地执行这种操作;最后,在经典信道中相互告知对方执行的次数,通过简单的计算就可以判断此次信息传输中是否存在窃听的情况。

此方案具有两个明显的优势:a)对于任意多的信息量(假设为 n),窃听者只能从中得到 $2/n$ 的信息;b)错误率对于窃听的出现非常敏感,一旦窃听出现,错误率将明显提升。所以,相比 BB84 协议,该方案更适合在有噪环境下和存在窃听的情况下使用。下面就是改进后方案的实现过程:

a)Alice 随机地准备 m 个量子,每个量子处于$|0\rangle$和$|1\rangle$两种状态之一。

b)对于每个量子态,Alice 执行 i 次独立操作 $R(\phi)$,其中:

$$R(\phi)=\begin{bmatrix}\cos\phi & -\sin\phi\\ \sin\phi & \cos\phi\end{bmatrix},i\in\{0,1,\cdots,n-1\}\text{ and }\phi=\pi/n$$

因此,经过处理之后发出的量子状态是 $R(\phi)^i|0\rangle$或者是 $R(\phi)^i|1\rangle$。

c)Bob 接收到量子后,对每个量子态执 j 次的独立操作 $R(\phi)$,$j\in\{0,1,\cdots,n-1\}$,然后再用标准基对每个处理后的量子态进行测量。

d)Alice 通过经典信道告诉 Bob 他对每个量子态进行 $R(\phi)$操作的次数。

e)Bob 接收到 Alice 发来的次数 i 的序列串后,经过简单的计算,对于每一对相应的 i 和 j,如果 $(i+j)\bmod n\neq 0$ 或者 $(i+j)\bmod n\neq n/2$,则告诉 Alice 丢弃对应的量子。

f)Alice 和 Bob 测试密钥的安全性,随机选取一些保留下来的密钥,经过对比,如果发现错误,表示传输过程不安全,这些密钥将被丢弃,重新前面的过程,直到没有错误出现。

g)经过最后的错误修正和保密放大操作后,得到最终的安全密钥。

表 3 给出了一个从 Alice 到 Bob 的改进后的方案。

表 3 一个改进后的方案具体实现过程的例子

量子	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice 的比特	1	0	0	1	1	1	0	1	0	0	0	1	1	0	1
$i\in\{0,1,\cdots,n-1\}$	3	9	8	2	5	0	1	7	4	5	9	8	6	0	4
$j\in\{0,1,\cdots,n-1\}$	4	6	5	8	1	3	9	8	5	2	0	7	4	7	2
Bob 的结果	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0
$(i+j)\bmod 10=0$ 或者 $(i+j)\bmod 10=15$		Y		Y			Y						Y	Y	
共享的密钥		0		1			0						1	1	

在改进后的方案中,Eve 只能获得 $2/n$ 的信息,同时,Alice 和 Bob 在他们筛选过的密钥中有 $(n-2)/n$ 的错误。假设 $n=10$,Eve 可以获得 20% 的信息,这就意味着 Eve 获得的信息减少了大约 30%(与 BB84 协议对比)。更为重要的是,Alice 和 Bob 筛选后的密钥中大约有 80% 的错误,这就意味着错误率大约提升了 70%(与 BB84 协议对比)。由此可以看出,通过对 BB84 协议改进得到的新方案可以非常灵敏地检测到是否有窃听的存在,并且可以有效地用于 QKD 的分析与实现。

3 正确性证明

对比 BB84 协议,改进后的方案对发出和接收到的每个量子进行了随机次数的独立操作 $R(\phi)$,下面通过数学公式的推导,证明改进后方案步骤 e)的正确性,从而得出整个方案在实际操作中是可行的。证明过程如下:

$$R(\phi)=\begin{bmatrix}\cos\phi & -\sin\phi\\ \sin\phi & \cos\phi\end{bmatrix}^{\chi}=\begin{bmatrix}\cos\chi\phi & -\sin\chi\phi\\ \sin\chi\phi & \cos\chi\phi\end{bmatrix}$$

当 $\phi=\pi/n$ 时:

$$R(\pi/n)^{i+j}=\begin{bmatrix}\cos\pi/n & -\sin\pi/n\\ \sin\pi/n & \cos\pi/n\end{bmatrix}^{i+j}=$$

$$\begin{bmatrix}\cos(i+j)\pi/n & -\sin(i+j)\pi/n\\ \sin(i+j)\pi/n & \cos(i+j)\pi/n\end{bmatrix}$$

若$(i+j)\bmod n=0$,此时$(i+j)=kn$,就有

$$R(\pi/n)^{i+j}=\begin{bmatrix}\cos k\pi & -\sin k\pi\\ \sin k\pi & \cos k\pi\end{bmatrix}=\begin{bmatrix}\pm1 & 0\\ 0 & \pm1\end{bmatrix}$$

其中:±取决于 k 的值,当 k 是奇数时,$\cos k\pi$ 取 -1,当 k 是偶数时,$\cos k\pi$ 取 $+1$。这种情况下,若初始状态是$|0\rangle$,Bob 最后得到的状态是$|0\rangle$,说明 Bob 的测量结果与 Alice 的比特一致。

若$(i+j)\bmod n=n/2$,n 是一个偶数,此时$(i+j)=kn+n/2$,有

$$R(\pi/n)^{i+j}=\begin{bmatrix}\cos(k\pi+\pi/2) & -\sin(k\pi+\pi/2)\\ \sin(k\pi+\pi/2) & \cos(k\pi+\pi/2)\end{bmatrix}=\begin{bmatrix}0 & \pm1\\ \pm1 & 0\end{bmatrix}$$

其中:±取决于 k 的值,当 k 是奇数时,$\sin(k\pi+\pi/2)$取 -1,当 k 是偶数时,$\sin(k\pi+\pi/2)$取 $+1$。这种情况下,若初始状态是$|0\rangle$,Bob 得到的是$|1\rangle$,同理,若初始状态是$|1\rangle$,Bob 得到的是$|0\rangle$。这就说明 Bob 的测量结果始终与 Alice 的原始状态相反,因此,Bob 可以猜到 Alice 的原始状态。

若$(i+j)\bmod n\neq0$ 或$(i+j)\bmod n\neq n/2$,Bob 就无法知道原始状态是$|0\rangle$或者是$|1\rangle$。

从上述证明可以看出,此方案在理论上是正确的,有完整、严密的数学推导来保证。在实际应用中,也是可以实现的,可以非常好地检测到传输过程中是否存在窃听。因为如果存在窃听,窃听者必然会破坏这种经过随机次数的独立操作处理过的量子态信息,当被破坏的量子态再传到 Bob 时,Bob 通过随机次数的独立操作,再与 Alice 在经典信道中比对,可以立马发现窃听者的存在。

4　结束语

本文改进后的方案使得窃听者只能得到少量的信息,并且更容易被发现。这就意味着,在产生错误比较多的有噪环境下或者存在窃听风险的信道中,此方案能很好地保护共享密钥的安全。当然此方案也有缺点,Alice 和 Bob 需要对量子态执行多次独立的 $R(\phi)$操作,这消耗了资源,影响了通信速率。下一步工作就是要设计出快速高效的软硬件结构来执行多次的 $R(\phi)$操作,真正使得量子密钥分配快速、高效、安全。

参考文献:

[1] 李承祖. 量子通信和量子计算[M]. 长沙:国防科技大学出版社,2008.

[2] 龙桂鲁,邓富国,曾谨言. 量子力学新进展[M]. 北京:清华大学出版社,2011.

[3] 吴张斌,陈光,杨伯君. 基于 BBM92 协议的量子密钥分发系统改进方案[J]. 量子电子学报 2009,26(5):1023-1028.

[4] BENSON O,SANTORI C,PELTON M. Regulated and entangled photons from a single quantum dot [J]. Phys Rev A,2004,84(11):2513-2516.

[5] LJUNGGREN D,BOURENNANE M,KARLSSON A. Authority based user authentication in quantum key distribution [J]. Phys Rev A,2000,62(2):022305.

[6] 赵生妹,李苗苗,郑宝玉. 一种基于量子纠错编码的量子密钥分配协议[J]. 电子与信息学报,2009,31(4):6708-6712.

[7] 王建秋,嵇英华,余信理. 量子通信网络安全性研究[J]. 电子技术,2009,46(1):8988-8993.

[8] WANG X. Quantum key distribution with 4 intensities of coherent light [J]. Phys Rev A,2005,72(1):012322.

[9] 权东晓,裴昌幸,朱畅华,等. 一种新的预报单光子源诱骗态量子密钥分发方案[J]. 物理学报,2008,57(9):5600-5604.

[10] 林育群,王发强,米景隆. 基于随机相伴编码的确定性量子密钥分配[J]. 物理学报,2007,56(10): 3806-3810.

[11] DENG Fu-guo, LONG Gui-lu. Secure direct communication protocol with a quantum one-time pad [J]. Phys Rev A, 2004, 69 (5): 052319.

(上接第 2806 页)

从表 2 中可以看出,WSC 码具有较好的嵌入效率且均大于 2.5,比 WPC 最少高出 0.5。因此 WSC 码比湿纸码具有更好的隐写安全性。同时可以看出,在分组长度一定时 WSC 码在线性完备码模式下取得最大嵌入效率。当湿纸率为 0 时,WSC 退化为基于纠错码的隐写码。但与其他编码方式[4]相比,WSC 码的嵌入效率还是比较低的。

综合 WSC 的三个性能分析,与 WPC 相比,WSC 具有更高的嵌入效率,提高了隐写算法的安全性,且在 $k\leqslant16$ 时,(n,k)模式下的计算复杂度较低,适合用于信息隐藏。

4　结束语

本文利用循环码中校正子与陪集的映射关系提出了一种基于循环码的湿纸隐写码。WSC 不仅保持了湿纸码的“不依靠载体元素本身传递信息”的特性,同时也提高了嵌入效率。与 WPC 相比,在 $k\leqslant16$ 时 WSC 码具有较低的计算复杂度。下一步的主要工作集中在研究湿纸率、编码模式与嵌入效率、编码成功率的内在联系。

参考文献:

[1] CRANDALL R. Some notes on steganography[EB/OL]. (2007-12). http://os. inf. u2dresden. de/ ~ westfeld/crandall. pdf.

[2] WESTFELD A. High capacity despite better steganalysis[C]//Proc of the 4th Information Hiding International Workshop. Berlin: Springer-Verlag,2001:289-302.

[3] ZHANG Wei-ming, WANG Shuo-zhong, ZHANG Xin-peng. Improving embedding efficiency of covering codes for applications in steganography[J]. IEEE Communications Letters,2007,11(8):680-682.

[4] FILLER T, JUDAS J, FRIDRICH J. Minimizing embedding impact in steganography using Trellis-coded quantization[C]//Proc of SPIE, Electronic Imaging, Media Forensics and Security Ⅶ. 2010.

[5] FILLER T, FRIDRICH J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Trans on Information Forensics and Security,2010,6(3):920-935.

[6] BIERBRAUER J, FRIDRICH J. Construction good covering codes for applications in steganography[EB/OL]. [2010-05-10]. http://citeseerx. ist. psu. edu/riewdoc/download? doi = 10. 1. 1. 83. 3356&rep = repl&type = pdf.

[7] FRIDRICH J, GOLJAN M, LISONEK P, *et al*. Writing on wet paper [J]. IEEE Trans on Signal Processing, 2005, 53 (10): 3923-3935.

[8] FRIDRICH J, GOLJAN M, SOUKAL D. Efficient wet paper codes [C]//Proc of Information Hiding Workshop. 2005.

[9] LIN Shu, COSTELLO D J. Error control coding[M]. 2nd ed. [S. l.]: Prentice Hall,2004.