量子密钥分配协议在概率克隆/重发攻击下的安全性

赵生妹 李 飞 郑宝玉
(南京邮电学院信号与信息研究所 南京 210003)

摘 要：该文基于概率克隆理论提出了一种量子密钥分配协议的攻击策略，密钥攻击者通过概率克隆机将发送端发送的量子态进行概率克隆，并根据自己的结果重新产生一个新的量子态发送给接收端。理论计算证明了量子密钥分配协议在这种攻击策略下仍具有足够的安全性。在经典计算机上设计并仿真量子密钥分配过程，仿真结果与理论分析相吻合。

关键词：攻击策略，量子密钥分配协议，不可克隆理论，概率克隆机
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2005)10-1639-04

The Security of Quantum Key Distribution under Probabilistic Clone/ Resend Attack

Zhao Sheng-mei Li Fei Zheng Bao-yu
(*Institute of Signal and Information Processing , Nanjing University of P. & T., Nanjing* 210003, *China*)

Abstract In this paper, an attack scheme based on probabilistic cloning machine is proposed, where the eavesdropper measures the quantum state from sender with a probabilitstic cloning machine, and resends the receiver a new result. It is shown that there is still an asymptotic perfect security of quantum key distribution under this attack strategy. The simulation results on classical computer are consistent with the theoretic ones.

Key words Attack strategy, Quantum key distribution, No-clone theorem, Probabilistic cloning machine

1 引言

自从 1984 年以来，量子密钥分配协议(Quantum Key Distribution protocol)得到了广泛的关注。量子密钥分配协议具有可证明的安全性，并且能够检测密钥分配过程中是否存在窃听者(或攻击者)，因而成为目前加密技术研究领域的新热点[1,3]。为了证明量子密钥分配协议的安全性，各种攻击方法相继提出[4,5]，包括集体攻击和个体攻击策略。在个体攻击中，最为简单的攻击是截取/重发攻击策略。当采用这种策略攻击时，窃听者Eve截取发送者Alice发送的量子态，测量获得一个结果；然后根据自己的结果，产生一个新的量子态，并发送给接收者Bob。Gisin等人已证明量子密钥分配协议在这种简单的攻击策略下具有绝对的安全性[4]。

从非正交量子态的不可克隆原理(No-Cloning Theorem)，可以证明窃听者(Eve)不能从量子密钥分配过程上获取任意有用信息。因为发送者(Alice)和接收者(Bob)可以根据密钥分配过程中估算的误码率(error bit rate)，要么放弃这次密钥分配结果，要么从筛选密钥(sifted keys)中提取安全的密钥。然而，对于两个非正交量子态，段-郭已证明可通过概率克隆机(a probabilistic cloning machine)进行概率克隆[6,7]，这与保证量子密钥分配协议安全性的不可克隆原理存在不一致性。因此，量子密钥分配协议的安全性值得进一步深入研究。本文提出一种利用概率克隆机进行攻击的策略，针对BB84 协议和 6 态协议，从理论上分析量子密钥分配协议在这种攻击策略下的安全性。

2 概率克隆/重发攻击策略

密钥分配及其攻击过程常常涉及三方，一般假设Alice和Bob为合法通信者，Eve为窃听者。在BB84 协议中[2]，存在两对相互正交的光子极化基：水平/垂直极化基(以 $\oplus$ 表示)和对角线斜极化基(以 $\otimes$ 表示)。在水平垂直基空间中，态 $|0\rangle$ 编码 0，$|1\rangle$ 编码 1；在对角线斜极化基空间中，$|\bar{0}\rangle$ 编码 0，$|\bar{1}\rangle$ 编码 1，且 $|\bar{0}\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$，$|\bar{1}\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$。6 态协议是BB84 协议的直接推广[3]，除了以上的 4 种量子态

2004-05-10 收到,2004-09-03 改回
国家自然科学基金（60272066）和江苏省高校自然科学基金（03KJB510091）资助课题

外，Alice 还将发送 $\left|\bar{\bar{0}}\right\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+i|1\rangle\right)$ 和 $\left|\bar{\bar{1}}\right\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-i|1\rangle\right)$ 两种量子态(对应于圆极化基⊙)，并将 $\left|\bar{\bar{0}}\right\rangle$ 编码 0，$\left|\bar{\bar{1}}\right\rangle$ 编码 1。

从集 $S=\{|\psi_o\rangle,|\psi_1\rangle\}$ 中选取的两个非正交量子态已被证明可通过幺正变换再加上一定的测量进行概率克隆[6,7]。具体表示为

$$\begin{aligned}U\left(|\psi_0\rangle|\Sigma\rangle|m_P\rangle\right)&=\sqrt{\eta_0}|\psi_0\rangle|\psi_0\rangle|m_0\rangle+\sqrt{1-\eta_0}\left|\phi^0_{\mathrm{ABP}}\right\rangle\\U\left(|\psi_1\rangle|\Sigma\rangle|m_P\rangle\right)&=\sqrt{\eta_1}|\psi_1\rangle|\psi_1\rangle|m_1\rangle+\sqrt{1-\eta_1}\left|\phi^1_{\mathrm{ABP}}\right\rangle\end{aligned}\tag{1}$$

其中 $|\psi_0\rangle,|\psi_1\rangle$ 是 A 系统所产生的两个非正交量子态；它们是概率克隆机的输入态；$|\Sigma\rangle$ 是概率克隆机的初始状态；$|m_P\rangle,|m_0\rangle$ 和 $|m_1\rangle$ 分别是克隆机中探测器(Probe)在不同时刻的状态；$\left|\phi^0_{\mathrm{ABP}}\right\rangle,\left|\phi^1_{\mathrm{ABP}}\right\rangle$ 是由系统 A、克隆机和探测器组成的复合系统(ABP)的两个状态；η_0 和 η_1 则分别对应量子态 $|\psi_0\rangle$ 和 $|\psi_1\rangle$ 的克隆效率。如果满足 $<m_0|\phi^0_{\mathrm{ABP}}>=<m_1|\phi^0_{\mathrm{ABP}}>=0$ 和 $<m_0|\phi^1_{\mathrm{ABP}}>=<m_1|\phi^1_{\mathrm{ABP}}>=0$，将可得到:

$$\frac{\eta_0+\eta_1}{2}\le\frac{1-\langle\psi_0/\psi_1\rangle}{1-\langle\psi_0|\psi_1\rangle^2\langle m_0|m_1\rangle}\le\frac{1}{1+\langle\psi_0|\psi_1\rangle}\tag{2}$$

这表明对两个非正交量子态同时克隆时，克隆效率间存在着一定的关联。如果进一步假设克隆效率独立于输入量子态时，即 $\eta_0=\eta_1=\eta$，则对非正交量子态 $|\psi_0\rangle$ 和 $|\psi_1\rangle$，克隆的平均效率为

$$\eta\le\frac{1}{1+\langle\psi_0|\psi_1\rangle}\tag{3}$$

借鉴截取/重发攻击方案，本文提出概率克隆/重发攻击策略，其中 Eve 使用概率克隆机进行窃听，然后将她自己获取的量子比特发送给 Bob。由于式(3)是针对两个非正交量子态同时克隆时的平均克隆效率，在 BB84 协议中 Alice 能够选择发送的量子态仅为 $|0\rangle,|1\rangle,\left|\bar{0}\right\rangle,\left|\bar{1}\right\rangle$ 4 种极化量子态，因而输入到概率克隆机的两个量子态将是这 4 种量子态的组合。我们把每种组合称为一个输入量子态集。根据 Alice 选择每种量子态的概率，能够计算出每个输入量子态集出现的概率，从而得到 Eve 通过这种攻击策略可获取的信息量，并因此判断 BB84 协议是否具有足够的安全性。通过相似计算过程，也可以判断 6 态协议在这种攻击策略下的安全性。

3 密钥分配协议安全性证明

由式(3)可知，概率克隆机的平均克隆效率 η 取决于两个输入量子态的内积。根据两个量子态间的“覆盖”程度，可将有关计算分 3 类情况，即正交的、非正交的和完全相同的。

如果两个输入量子态相互正交，那么克隆效率将趋近于 1，计算过程如下：

$$\left.\begin{aligned}\eta&\le\frac{1}{1+\langle\psi_0|\psi_1\rangle}=\frac{1}{1+\langle0|1\rangle}=1\\\eta&\le\frac{1}{1+\left\langle\bar{0}\middle|\bar{1}\right\rangle}=\frac{1}{1+\left\langle\bar{\bar{0}}\middle|\bar{\bar{1}}\right\rangle}=1\end{aligned}\right\}\tag{4}$$

如果两个输入量子态是非正交的，则

$$\left.\begin{aligned}\eta&\le\frac{1}{1+\left\langle0\middle|\bar{0}\right\rangle}=\frac{1}{1+\left\langle0\middle|\bar{1}\right\rangle}=2-\sqrt{2}=0.5858\\\eta&\le\frac{1}{1+\left\langle1\middle|\bar{0}\right\rangle}=\frac{1}{1+\left\langle1\middle|\bar{1}\right\rangle}=2-\sqrt{2}=0.5858\end{aligned}\right\}\tag{5}$$

如果两个输入量子态完全相同，平均克隆效率将接近 0.5。因为

$$\left.\begin{aligned}\eta&\le\frac{1}{1+\langle0|0\rangle}=\frac{1}{1+\langle1|1\rangle}=0.5\\\eta&\le\frac{1}{1+\left\langle\bar{0}\middle|\bar{0}\right\rangle}=\frac{1}{1+\left\langle\bar{1}\middle|\bar{1}\right\rangle}=0.5\end{aligned}\right\}\tag{6}$$

针对 BB84 协议，表 1 列出各种可能的两个输入量子态集及其最大平均克隆效率。如果 Alice 等概率地发送 4 种量子态，通过计算得到每个输入量子态集出现的概率如表 1 的第 2 列所示。因此，经过克隆机克隆后的最大克隆效率为

$$\begin{aligned}\bar{\eta}_{\mathrm{BB84}}&=2\times\frac{1}{8}\times1+4\times\frac{1}{8}\times0.5858\\&\quad+4\times\frac{1}{16}\times0.5=0.6679\end{aligned}\tag{7}$$

表 1 BB84 协议中输入量子态集及其最大概率克隆效率

输入量子态集	量子态集概率	最大概率克隆效率
$\{|0\rangle,|1\rangle\},\{|\bar{0}\rangle,|\bar{1}\rangle\}$	1/8	1.0
$\{|0\rangle,|\bar{0}\rangle\},\{|0\rangle,|\bar{1}\rangle\},\{|1\rangle,|\bar{0}\rangle\},\{|1\rangle,|\bar{1}\rangle\}$	1/8	0.5858
$\{|0\rangle,|0\rangle\},\{|1\rangle,|1\rangle\},\{|\bar{0}\rangle,|\bar{0}\rangle\},\{|\bar{1}\rangle,|\bar{1}\rangle\}$	1/16	0.5

这表明，在 BB84 协议中 Eve 通过概率克隆机最多能克隆 66.79%的输入量子态。也就是说，她使用概率克隆/重发攻击策略攻击时，能够发送 66.79%的正确量子态给 Bob，而不会引起 Alice 和 Bob 的任何注意。但是，对于剩余的 33.21%的量子态，Eve 的操作必将引起它们的变化，而且 Eve 获得的量子态与 Alice 发送的不存在相关性。当 Eve 重发给 Bob 时，Bob 只有一半的概率得到与 Alice 相同的码字(0 或 1)。由此，可以计算出在 Eve 进行概率克隆/重发攻击策略下，

Alice 和 Bob 之间密钥分配的误码率为 16.6%，Eve 可获得的信息量最大为

$$I_{\mathrm{BB84}} = 0.6679 + \frac{1}{2} \times (1 - 0.6679) = 0.834 \tag{8}$$

与简单的截取/重发攻击策略相比，Eve获取了较多的信息(在截取/重发下为 75%[4])，且密钥分配过程的误码率得到降低(在截取/重发下为 25%)。但是Alice和Bob仍可根据个体攻击下BB84 协议的安全标准(11%)[8]检测出Eve的存在，从而放弃这次密钥分配过程产生的密钥。

如果Eve在窃听过程中只克隆部分量子态，以便降低由于她的干扰所引起的误码率，使之达到BB84 个体攻击的安全标准范围之内。然而，这时Bob从Alice获取的信息量必将大于Eve从Alice获得的信息量，Alice和Bob可通过保密增强技术(privacy amplification)[9]从筛选密钥中提取安全的密钥。因而在这样的攻击策略下，BB84 协议仍具有足够的安全性。

表 2 列出 6 态协议在概率克隆/重发攻击策略下各种可能的输入量子态集及各自的最大克隆效率。计算得出：Eve 利用概率克隆机平均克隆概率为 64.05%，获取的最大信息量为 81.9%，而Alice与Bob间的误码率为 17.9%， 比简单的截取/重发攻击策略下的估算值(33.3%)有明显降低，但仍高于个体攻击下的安全标准(12.7%) [10]。与BB84 一样，6 态协议在概率克隆/重发下同样具有足够的安全性。

表 2　6 态协议中输入量子态集及其最大概率克隆效率

输入量子态集	量子态集概率	最大概率克隆效率
$\{\|0\rangle,\|1\rangle\},\{\|\bar{0}\rangle,\|\bar{1}\rangle\},\{\|\tilde{0}\rangle,\|\tilde{1}\rangle\}$	1/18	1.0
$\{\|0\rangle,\|\bar{0}\rangle\},\{\|0\rangle,\|\bar{1}\rangle\},\{\|1\rangle,\|\bar{0}\rangle\},\{\|1\rangle,\|\bar{1}\rangle\}$ $\{\|0\rangle,\|\tilde{0}\rangle\},\{\|0\rangle,\|\tilde{1}\rangle\},\{\|1\rangle,\|\tilde{0}\rangle\},\{\|1\rangle,\|\tilde{1}\rangle\}$ $\{\|\bar{0}\rangle,\|\tilde{0}\rangle\},\{\|\bar{0}\rangle,\|\tilde{1}\rangle\},\{\|\bar{1}\rangle,\|\tilde{0}\rangle\},\{\|\bar{1}\rangle,\|\tilde{1}\rangle\}$	1/18	0.5858
$\{\|0\rangle,\|0\rangle\},\{\|1\rangle,\|1\rangle\},\{\|\bar{0}\rangle,\|\bar{0}\rangle\},\{\|\bar{1}\rangle,\|\bar{1}\rangle\},$ $\{\|\tilde{0}\rangle,\|\tilde{0}\rangle\},\{\|\tilde{1}\rangle,\|\tilde{1}\rangle\}$	1/36	0.5

4　仿真结果

我们用经典计算机仿真了量子密钥分配过程，用以观察在不同的攻击策略下Eve获取的信息量与它对密钥分配过程干扰程度之间的关系。与较复杂的量子信息处理过程不同，量子密钥分配过程仅包括量子态的制备及测量这两种操作，在经典计算机上仿真该过程是可能的[11,12]。从分配协议中极化量子态的产生过程看，一个极化量子态取决于极化基的选取和比特值的设置。仿真过程中可以采用两个变量来描述，其中一个表示极化基(⊕ 或⊗ 或⊙)，另一个表示比特值(0 或 1)。量子密钥分配协议规定Alice随机地选择极化基和比特值[2,3]，这两个变量的具体取值可以通过伪随机数产生器来产生。仿真的另一问题是量子态的测量。由于BB84 协议和 6 态协议中使用的是投影测量，仿真中采用以下计算方法：(1)在没有Eve干扰的情况下，如果Alice和Bob使用相同的极化基，那他们得到的结果是相关的，对应的极化基和比特值将完全相同，可将Alice 的极化基和比特值拷贝给Bob；如果两者使用不同的极化基，Bob测量的比特值应当是随机的，可使用伪随机数产生一个随机值赋值Bob。(2)如果存在Eve的干扰，Bob从密钥分配过程获取的任何比特值都将取决于Eve重发的量子态，仿真时只需将Eve替代Alice即可。至于Eve如何从Alice处获取相关的量子态，取决于Eve所采用的窃听方案。

值得说明的是，在仿真计算模型中假设 Alice 与 Bob 是通过理想量子信道发送和接收量子态的，他们间的误码率由 Eve 的干扰所引起。得到筛选密钥(sifted keys)后，Alice 和 Bob 随机地从筛选密钥中选择一些比特值作为测试位，估算所得的筛选密钥的误码率。如果这个误码率大于相应密钥分配的安全标准，他们将放弃这次密钥的分配；反之，他们将这剩余的筛选密钥通过纠错算法(error correction)获取一个共享的比特串。

针对BB84 和 6 态协议，图 1 描述了截取/重发理论、截取/重发仿真和概率克隆/重发仿真等情况下，Eve获取的信息量与Eve干扰间的关系。其中L_1表示截取/重发的理论计算结果，L_2表示截取/重发的仿真结果，L_3表示概率克隆/重发的仿真结果，I_{AB} 为Alice与Bob间互信息与Eve干扰理论结。对比L_1和L_2曲线，两曲线趋势基本相似，表明仿真与理论果分析相吻合； L_3与L_2相比，在相同的误码率下Eve可获取更多的信息量，表明概率克隆/重发攻击策略比截取/重发策略更具有攻击力，与理论分析的结果相一致。

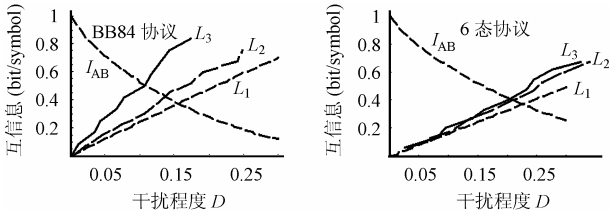

图 1　Eve 从密钥分配中获取的信息与它对密钥分配干扰间关系曲线

5　结束语

本文依据概率克隆理论，设计概率克隆/重发攻击策略，并针对 BB84 和 6 态协议进行了理论分析。结果表明，在 BB84 中 Eve 可获取 83.4%信息量，且 Alice 和 Bob 间的密钥分配误码率下降到 16.6%；至于 6 态协议，Eve 可获取的信息量有所降低，降为 81.9%，密钥分配的误码率有所上升，升为 17.9%。6 态协议与 BB84 协议相比，在概率克隆/重发攻击策略下具有一定的优势。尽管如此，Alice 和 Bob 可依据量

子密钥分配协议个体攻击的安全标准，要么检测到 Eve 的存在而放弃这次密钥的分配结果，要么使用保密增强技术从筛选密钥中提取安全的密钥。因此，量子密钥分配协议在概率克隆/重发攻击下仍具有足够的安全性。根据量子密钥分配过程的特点，本文还设计并实现了量子密钥分配协议的仿真程序，其仿真结果与理论分析相吻合。

参 考 文 献

[1] Gottesman D, Lo Hoi-Kwong. Proof of security of quantum key distribution with two-way classical communications [J]. *IEEE Trans. on Info. Theory*, 2003, 49(2): 457－475.

[2] Bennett C H, Brassard G. Quantum cryptography: public-key distribution and coin tossing [A], Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing[C]. Bangalore, India. 1984: 175－179.

[3] BruB D. Optimal eavesdropping in quantum cryptography with six states [J]. *Phy. Rev. Lett*., 1998, 32(14): 3018－3021.

[4] Gisin N, *et al*.. Quantum cryptography[J]. *Rev. Mod. Phys*, 2002, 74(1) : 145－195.

[5] Bihan E, *et al*.. Security of quantum key distribution against all collective attacks[EB/OL], available at http://xxx.lanl.gov/quant p h/ 9801022, 1998.

[6] Duan Lu-Ming, Guo Guang-Can. A probabilistic cloning machine for replicating two non-orthogonal states [J], *Phys. Lett*., 1998, A 243: 26－264.

[7] Duan Lu-Ming, Guo Guang-Can. Probabilistic cloning and identification of linearly independent quantum states [J]. *Phy. Rev. Lett.*, 1998, 80(22): 4999－5002.

[8] Volovich I V, Volovich Ya I. On classical and quantum cryptography [EB/OL], available at http://xxx.lanl.gov/quant-ph/ 0108133, 2001.

[9] Bennett C H, *et al*.. Generalized privacy amplification [J]. *IEEE Trans. on Info. Theory*, 1995, 41(6): 1915－1923.

[10] Lo Hoi-Kwong. Proof of unconditional security of six-state quantum key distribution scheme [EB/OL], available at http://xx x.anl.gov/quant-ph/0102138, 2001.

[11] Williams C P, Clearwater S H. Explorations in Quantum Computing[M], New York, Berlin, Heidelberg: Springer-Verlag, 1998: 163－178.

[12] Zhao Sheng-mei, Li Fei Zheng Bao-yu. On simulation of quantum cryptography [J]. *The Journal of China Universities of Posts and Telecommunications*, 2002, 9(4): 13－18.

赵生妹：女，1968 年生，副教授，在职博士生，研究方向为量子信息处理.

李 飞：女， 1966 年生，副教授，在职博士生，研究方向为量子信息处理.

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.