三量子态量子密钥分发协议安全性分析

王者，姚治海，苟立丹，王晓茜

长春理工大学理学院，吉林 长春 130022

摘要 研究了具有优秀安全性的 PBC00 协议。为了便于制备偏振态与实现协议，将 PBC00 协议的偏振态改为 $|1\rangle$、$|0\rangle$和$|+\rangle$。为了分析协议的安全性，假设窃听者使用截获重发的方式对量子密钥分发(QKD)过程进行窃听，分析了窃听者可能使用的测量基矢，计算得出由窃听者引起的密钥错误率。介绍了以 BKM07 协议为基础的改动后的三量子态 QKD 方案，分析了其安全性。研究结果表明，改动后的 PBC00 协议具有更好的发现窃听者的能力，且易于实现，具有实际应用的潜力。

关键词 量子光学；量子通信；BB84 协议；三量子态量子密钥分发协议；安全性分析

中图分类号 O413.1 **文献标识码** A

doi：10.3788/LOP54.122702

Security Analysis of Three-State Quantum Key Distribution Protocol

Wang Zhe, Yao Zhihai, Gou Lidan, Wang Xiaoqian

College of Science, Changchun University of Science and Technology, Changchun, Jilin 130022, *China*

Abstract The PBC00 protocol with excellent security features is studied. For the purpose of preparing polarization states and realizing protocol, the polarization states of the PBC00 protocol are changed to the $|1\rangle$, $|0\rangle$ and $|+\rangle$. For the purpose of analyzing the secutity of protocol, it is assumed that the eavesdropper uses the intercept-resend strategy to eavesdrop during the quantum key distribution (QKD) process. The measurement basic vectors that the eavesdropper may use are analyzed and the key error rates caused by the eavesdropper are calculated. The modified three-state QKD protocol based on the BKM07 protocol is introduced and its security is analyzed. The study results show that the modified PBC00 protocol has a stronger ability to detect eavesdroppers, is easy to implement, and has a practical application potential.

Key words quantum optics; quantum communications; BB84 protocol; three-state quantum key distribution protocol; security analysis

OCIS codes 270.5565; 270.5568; 270.5585

1 引 言

近年来，网络技术和信息技术发展迅速，量子通信为信息的安全传输提供了一种新的方法，受到了学者们的广泛关注。1984 年，世界上第一个量子密钥分发(QKD)协议被提出，简称为 BB84 协议[1]。1989 年，美国 IBM 公司第一次在实验上实现了 QKD[2]，使 BB84 协议由理论走向了实践。BB84 协议的安全性基于量子力学的几个基本性质[3-4]，完全不同于经典密码体系中基于计算复杂性的基本原理，可以在理论上达到绝对安全通信[5-6]。BB84 协议的提出及学者们对其进一步的深入研究[7]，使绝对安全的信息传输成为可能，多种在安全性、效率、实用性等方面各具特色的 QKD 协议相继出现。如，基于连续变量体系的量子通信，其平均光子数很高，受到了学者们的广泛关注[8-10]。但其实验装置都是非理想的[11]，影响 QKD 协议的安全性。

收稿日期：2017-07-06；**收到修改稿日期**：2017-07-20

基金项目：国家自然科学基金(11305020，11547242，11647054)、吉林省教育厅“十三五”科学技术研究规划项目(吉教科合字 2016 第 354 号)

作者简介：王者(1994—)，男，硕士研究生，主要从事量子通信方面的研究。E-mail：1054803144@qq.com

导师简介：王晓茜(1982—)，女，博士，副教授，主要从事量子信息物理和量子光学方面的研究。E-mail：xqwang21@163.com(通信联系人)

针对探测装置自身的不完美，Lo 等[12]提出了一个测量设备无关 QKD(MDI-QKD)协议，避免了针对探测装置的窃听，有效提高了安全通信距离。各国学者以此协议原型为基础，提出了各种不同的实验方案[13-15]。

2000 年，Phoenix 等[16]提出了一个相较于 BB84 协议更容易实现的 QKD 协议，简称为 PBC00 协议。PBC00 协议增加了第三个非正交的偏振态，相对于 B92 协议[17]其安全性更高，可以更有效地抵抗窃听者的攻击。2004 年，Renes 等[18]改进了 PBC00 协议，改进后的协议简称为 R04 协议。该协议中应用了球形编码方式，增强了抵抗窃听者的能力，并提高了密钥的利用率。2008 年，Boileau 等[19]证明了 R04 协议和 PBC00 协议的无条件安全性。2016 年，Schiavon 等[20]通过实验证明了 R04 协议的可行性，发现虽然其部分效率指标低于 BB84 协议的，但其更易于实现，完全可以成为除 BB84 协议之外的又一个备选 QKD 协议。R04 协议与 PBC00 协议有很大程度的相似性，Schiavon 等[20]的分析也可以理解为对 PBC00 协议的肯定。2007 年，Boyer 等[21]提出了四态半 QKD 协议，简称为 BKM07 协议，并证明了其稳健性。2009 年，Zou 等[22]简化了 BKM07 协议，减少了协议使用的量子态数量，并证明了协议的稳健性。

为了使 PBC00 协议的可应用范围更广泛，本文将协议所需的偏振态改为一对正交态和一个非正交态，分析了在窃听者存在的情况下此方案的安全性。并分析了 Zou 等[22]改动后的使用三个量子态的半 QKD 协议，此协议同样利用一对正交态与一个非正交态完成密钥分发。分别计算得出了两个协议中窃听者引起的密钥错误率，得出了发现窃听者所需要的最少测量次数。

2 改动后 PBC00 协议的安全性分析

2.1 协议简介

最初的 PBC00 协议，使用了三个非正交互为对称的偏振态。在接下来要介绍的协议中，基于 PBC00 协议的思路，利用一对正交偏振态$|1\rangle$、$|0\rangle$和一个非正交偏振态$|+\rangle$完成密钥分发并进行研究，协议过程如下。

1) 首先，Alice 随机地生成一组二进制数据串，根据这组数据串从三个偏振态$|A\rangle$、$|B\rangle$或$|C\rangle$(分别对应$|1\rangle$、$|0\rangle$和$|+\rangle$)中选择待发送的量子态并进行制备，提前确定没有被发送的量子态。将制备完成的量子态通过量子信道发送给接收方 Bob。

2) 收到 Alice 发送过来的量子态后，Bob 选择这三个偏振态中的任意一个垂直投影算符 $\hat{\boldsymbol{P}}_{j\perp}$($j$ 为 1，0 或+)作为测量基矢，以相等的先验概率从三个测量算符中选择一个，测量接收到的量子比特。

3) Bob 测量后如果得不到测量结果，则告知 Alice 将收到的量子态丢弃。

4) Bob 测量后如果出现结果，则 Alice 通过经典信道告知 Bob 哪一个量子态没有被发送。Bob 借助 Alice 提供的信息，根据自身使用的测量基矢排除一个量子态(假使 Bob 选择测量基矢 $\hat{\boldsymbol{P}}_{1\perp}$ 测量量子态后出现测量结果，即可排除与此测量基矢正交的$|1\rangle$)。如果可以确定 Alice 发送的量子态则完成一次密钥共享，不能确定则将此量子态丢弃。

5) Bob 利用图 1 所示的循环图，将确定后的量子态与 Alice 告知的没有被发送的量子态组合成对应的二进制数据串(顺时针为比特 0，逆时针则为比特 1)，确定最终密钥。

6) 双方随机抽取一部分密钥，来估计误码率以及是否有窃听者 Eve 的存在，若误码率在一定的阈值范围内，则利用纠错技术进行纠错，并对纠错后的密钥进行隐私放大，从而避免通信过程和纠错过程中的信息泄露，最后提取到无条件安全的密钥。

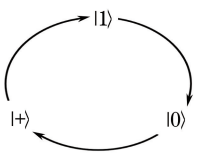

图 1 三态循环图

Fig. 1 Cyclic map of three-state

2.2 存在窃听者时的安全性分析

假设 Alice 发送的量子态为$|j\rangle$(取$|1\rangle$、$|0\rangle$或$|+\rangle$)，Eve 截获量子态并测量出正确结果的概率为 $P(j$，

j),Alice 选择发送每个量子态的先验概率为 x_j。则 Alice 发送的三种量子态被 Eve 截获后,可以分辨出量子态为$|1\rangle$、$|0\rangle$或$|+\rangle$的概率为

$$P_{\mathrm{D}}=\sum_j x_j P(j,j)。\tag{1}$$

在此三量子态密钥分发协议中,因为使用投影算符测得有结果与无结果的概率不同,可以假设结果为1(得到测量结果)或为0(无测量结果)两种情况,分别考虑它们的分辨概率,得出 Eve 可以得出正确测量结果的最大概率,所有可能出现的情况见表1。

表1 三种测量基矢下得到正确测量结果的概率

Table 1 Probabilities for obtaining correct measurement results under three measurement basic vectors

Measurement basic vector	$\|1\rangle$		$\|0\rangle$		$\|+\rangle$	
	0	1	0	1	0	1
$\hat{\boldsymbol{P}}_{1_\perp}$	1	0	0	1	$\frac{1}{2}$	$\frac{1}{2}$
$\hat{\boldsymbol{P}}_{0_\perp}$	0	1	1	0	$\frac{1}{2}$	$\frac{1}{2}$
$\hat{\boldsymbol{P}}_{+_\perp}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	0

从表1可以看出,存在一对正交态的三量子态密钥分发协议,使用三种投影算符测量得到正确结果的概率是相等的。如果发送方选择了正交归一的测量基矢$\{|1\rangle,|0\rangle\}$,那么 Alice 发送的所有$|1\rangle$、$|0\rangle$都将被 Eve 测得。这时,可能得到的正确分辨量子态的概率为

$$P_{\mathrm{D}}=\frac{2}{3}。\tag{2}$$

此结果表明,Eve 截获量子态并测量后,在不改变测得结果的情况下,直接将量子态发送给 Bob,至少有2/3的可能性不会被发现。但这个结果没有包含所有可能的情况,Bob 收到 Eve 重发的量子态后,选择不同的测量基矢会出现多种不同的结果。

在 Alice 和 Bob 接下来传输和测量量子比特的过程中,窃听者的行为会在公共信道被揭露。如果发现窃听者截取了部分信息,在这个过程中可以将选择作为最终密钥的部分信息丢弃,以保证整个通信过程的绝对安全。信息的发送方和接收方仅仅不知道窃听者 Eve 所使用的测量方式和测量结果。Eve 会使用所选择的测量方式对每一个量子态进行测量,并根据测量得出的结果传输一个新的量子态给 Bob,凭借这种方式伪装自己。考虑如下情况。Eve 使用了2.1节提到的完备归一的测量基$\{|1\rangle,|0\rangle\}$进行测量。在这种情况下,Eve 如果截获量子态后测得的结果为$|1\rangle$,则发送$|1\rangle$给 Bob。如果 Alice 发送$|+\rangle$被 Eve 截获并测量重发后,量子态各有1/2的几率改变为$|1\rangle$或$|0\rangle$然后被 Bob 接收。Bob 作为接收方,其量子态可以表示为如下密度矩阵

$$\rho=\frac{1}{2}|1\rangle\langle 1|+\frac{1}{2}|0\rangle\langle 0|。\tag{3}$$

(3)式表明,Bob 接收任意量子态后,可以使用 ρ 计算出在窃听者存在的环境下,仍可以得到正确匹配结果的概率。Bob 得到一个正确的结果需要具备如下条件:

1) Alice 选择发送量子态$|1\rangle$或$|0\rangle$;

2) Bob 测量接收到的量子态后得到测量结果;

3) Eve 的截获重发操作没有影响到 Bob 接收到正确的量子态;

4) Alice 公布的未发送的量子态可以帮助 Bob 确定最终密钥。

Bob 测量接收到的量子态后,可以得到匹配结果的概率为

$$P_{C_1}=\frac{2}{3}\times\frac{1}{2}\mathrm{Tr}(\hat{\boldsymbol{P}}_{1_\perp}\rho+\hat{\boldsymbol{P}}_{0_\perp}\rho+\hat{\boldsymbol{P}}_{+_\perp}\rho)=\frac{1}{8},\tag{4}$$

式中 Tr 代表求迹,系数2/3为 Alice 发送的量子态为$|1\rangle$或$|0\rangle$的概率,系数1/2为 Alice 公布的可以帮助 Bob 确定最终密钥的量子态的概率。

还有另一种 Eve 改变了 Alice 发送的量子态,但 Bob 仍可以得到正确结果的情况,具体如下:

1) Alice 选择发送量子态$|+\rangle$;

2) Bob 使用$\hat{\boldsymbol{P}}_{1_\perp}$或$\hat{\boldsymbol{P}}_{0_\perp}$作为测量基矢并得到测量结果;

3) Alice 公布的未发送的量子态可以帮助 Bob 确定最终密钥。

在上述条件下,Bob 测量接收到的量子态后,可以得到匹配结果的概率为

$$P_{C_2}=\frac{1}{3}\times\frac{1}{2}\mathrm{Tr}(\hat{\boldsymbol{P}}_{1_\perp}\rho+\hat{\boldsymbol{P}}_{0_\perp}\rho)=\frac{1}{24}。\tag{5}$$

共享的密钥串中有一部分是由 Eve 的干扰而产生的错误密钥,错误密钥的产生满足如下三个条件:

1) Alice 选择发送量子态$|+\rangle$;

2) Bob 使用测量基矢$\hat{\boldsymbol{P}}_{+_\perp}$测量接收到的量子态后得到测量结果;

3) Alice 公布的未发送的量子态可以帮助 Bob 确定最终密钥。

Eve 引起错误密钥的概率为

$$P_{M}=\frac{1}{3}\times\frac{1}{2}\mathrm{Tr}(\hat{\boldsymbol{P}}_{+_\perp}\rho)=\frac{1}{48}。\tag{6}$$

由(6)式可以得出,Eve 引起的错误率为(1/48)/(1/8+1/24)=1/8,则 Eve 不被发现的概率为 7/8。

进一步分析了在此 QKD 协议中,Bob 得到正确密钥与 Eve 引起错误密钥的条件与概率,窃听者不被发现的概率曲线如图 2 所示。在实际应用中,由信道引起的错误率较低,一旦密钥错误率达到了 1/8 左右,则可判定协议中有窃听者存在。根据此探测概率可知,当测量次数达到 45 以上时,有很大概率发现窃听者的存在。

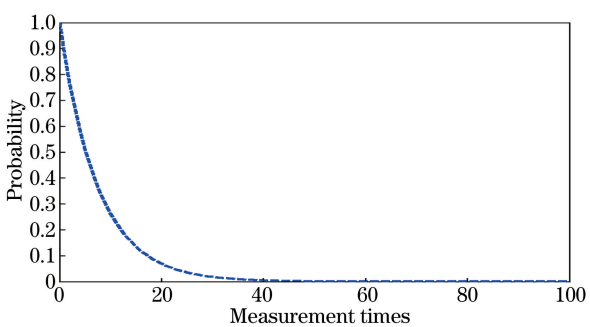

图 2 改动后 PBC00 协议中窃听者不被发现的概率曲线

Fig. 2 Probability curve for eavesdropper not being detected in modified PBC00 protocol

3 半量子 QKD 协议的安全性分析

在常规的 QKD 协议中,如果选用量子的偏振特性编码信息,为了保证通信的绝对安全性,在信息的发送方与接收方之间传输的密钥通常存在一对非正交偏振的量子态,以防止窃听者悄无声息地截获密钥。而在这个被称为半量子三量子态 QKD 协议中,密钥接收方接收到的密钥信息类似于经典信息理论中二值系统的取值。

3.1 协议简介

1) Alice 随机生成并发送 $N=6n(1+x)$个量子态($|1\rangle$、$|0\rangle$和$|+\rangle$)给 Bob,其中 n 为最终密钥需求数量,x 为一个固定系数,以保证通信结束后可以得到足够的密钥数量。

2) Bob 接收到量子态后有两种选择:其一,使用$\{|1\rangle,|0\rangle\}$基矢测量并将得到的结果重新发送给 Alice,简称为 SIFT 操作;其二,直接选择将量子态重返回给 Alice,简称为 CTAL 操作(Alice 每次都是接收到 Bob 发送的上一个量子态之后,再发送下一个量子态给 Bob)。

3) Alice 使用发送量子态时选用的基矢测量 Bob 返回的量子态。

4) Alice 公布发送的量子态中哪一个为$|+\rangle$,Bob 公布测量了哪些量子态。接下来 Alice 与 Bob 共享一串 Bob 使用$\{|1\rangle,|0\rangle\}$基矢测得正确结果的量子态,简称为 Z-SIFT 比特,并将这部分量子态作为最终的比特密钥。

5) Alice 检查 CTAL 操作中被返回量子态的错误率是否超过阈值，并从上述最终得出的 Z-SIFT 比特序列中选取部分作为测试比特，与 Bob 比对测量值及检查错误率，判断整个通信过程是否安全。

6) 双方随机抽取一部分密钥，估算出误码率来判断是否有窃听者的存在。若误码率在一定的阈值范围内，则利用纠错技术进行纠错，并对纠错后的密钥进行隐私放大，提取到无条件安全的密钥。

3.2 存在窃听者时的安全性分析

Alice 以先验概率 x_j 选择发送量子态。Eve 同样使用完备归一的测量基{|1⟩,|0⟩}测量截获的信息。只要 Alice 发送的量子态为|1⟩或|0⟩，Eve 必定可以获得正确的测量结果。但是由于 Bob 的 CTAL 操作，有 1/2 的量子态将被丢弃。Eve 正确分辨出截获量子态的概率为

$$P_{\mathrm{D}}=\frac{1}{3}。\tag{7}$$

在这个半经典的 QKD 协议中，因为接收方 Bob 只使用一种测量基矢测量信息，可能出现的结果相对简单。假设 Eve 为了获取更多的信息，同样选择使用测量基{|1⟩,|0⟩}测量截获的信息。首先，Alice 发送一串量子态给 Bob，Eve 在这个过程中截获并重发量子态，Eve 有 1/3 的可能改变了量子态的状态。Bob 收到 Eve 重发的量子态后，有 1/2 的可能不对其进行测量直接返还给 Alice，Alice 收到信息后选用与发送时同样的基矢测量，有 1/2 的可能发现量子态被改变，从而检测出窃听者的存在。

如果 Eve 选择在 Bob 将信息返回给 Alice 的过程中截获量子态，仍可以发现 Eve 的存在。原因是 Eve 无法得知 Bob 返回给 Alice 的量子态是执行了 SIFT 操作还是 CTAL 操作。Eve 有 1/2 的可能截获未经测量的量子态，这部分量子态中存在|+⟩，会引起的错误率为 1/12。即密钥分发结束后，从最终密钥中抽取 n 个密钥作为测试密钥，Eve 不被发现的概率为$(11/12)^n$，如图 3 所示。可知当测量次数达 65 以上时，有很大概率发现窃听者的存在。

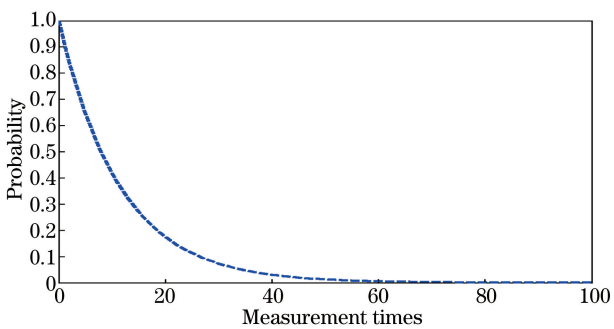

图 3 半 QKD 协议下窃听者不被发现的概率曲线

Fig. 3 Probability curve for eavesdropper not being detected in semi-QKD protocol

4 结 论

半量子 QKD 协议的整个实现过程与结果的测量都相对简单，但在窃听者的检测方面，与改动后的 PBC00 协议存在差距。通信双方可以根据需求选择合适的方案完成密钥分发。值得一提的是，如果窃听者使用{|1⟩,|0⟩}基矢测量截获信息，两个协议中密钥的利用效率与发现窃听者的概率都取决于 Alice 发送的密钥中|+⟩所占的比率，发送方可以根据需要选择最佳的取值，以达到理想的通信效果。

参 考 文 献

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

[2] Bennett C H, Bessette F, Brassard G, *et al*. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3-28.

[3] Wootters W K, Zurek W H. A single quantum cannot be cloned[J]. Nature, 1982, 299(5886): 802-803.

[4] Heisenberg W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik (in German)[J].

Zeitschrift für Physik, 1927, 43(3/4): 172-198.

[5] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441.

[6] Mayers D. Unconditional security in quantum cryptography[J]. Journal of the ACM, 2001, 48(3): 351-406.

[7] Liu Lingling, Jing Mingyong, Yu Bo, *et al*. Polarization control in single photons phase coding quantum key distribution system[J]. Laser & Optoelectronics Progress, 2015, 52(7): 072701.
刘令令, 景明勇, 于波, 等. 单光子相位编码量子密钥分发系统中的偏振控制[J]. 激光与光电子学进展, 2015, 52(7): 072701.

[8] Liu Youming, Wang Chao, Huang Duan, *et al*. Study of synchronous technology in high-speed continuous variable quantum key distribution system[J]. Acta Optica Sinica, 2015, 35(1): 0106006.
刘友明, 汪超, 黄端, 等. 高速连续变量量子密钥分发系统同步技术研究[J]. 光学学报, 2015, 35(1): 0106006.

[9] Chen Yan, Shen Yong, Zou Hongxin. An all-fiber continuous variable quantum key distribution based on multi-bits coding of single pulse[J]. Acta Optica Sinica, 2015, 35(7): 0727001.
陈岩, 沈咏, 邹宏新. 基于单脉冲多位编码的全光纤连续变量量子密钥分发[J]. 光学学报, 2015, 35(7): 0727001.

[10] Wang Yunyan, Guo Dabo, Zhang Yanhuang, *et al*. Algorithm of multidimensional reconciliation for continuous-variable quantum key distribution[J]. Acta Optica Sinica, 2014, 34(8): 0827002.
王云艳, 郭大波, 张彦煌, 等. 连续变量量子密钥分发多维数据协调算法[J]. 光学学报, 2014, 34(8): 0827002.

[11] Guo Xueshi, Gao Kang, Liu Nannan, *et al*. Differential detection system for measuring the quantum noise of pulsed light[J]. Acta Optica Sinica, 2013, 33(9): 0927002.
郭学石, 高亢, 刘楠楠, 等. 适用于测量脉冲光量子噪声的差分探测系统[J]. 光学学报, 2013, 33(9): 0927002.

[12] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[13] Ma X, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(6): 3818-3821.

[14] Liu Y, Chen T Y, Wang L J, *et al*. Experimental measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2013, 111(13): 130502.

[15] Zhu Feng, Wang Qin. Quantum key distribution protocol based on heralded single photon source[J]. Acta Optica Sinica, 2014, 34(6): 0627002.
朱峰, 王琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014, 34(6): 0627002.

[16] Phoenix S J D, Barnett S M, Chefles A. Three-state quantum cryptography[J]. Journal of Modern Optics, 2000, 47(2/3): 507-516.

[17] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121.

[18] Renes J M. Spherical code key distribution protocols for qubits[J]. Physical Review A, 2004, 70(5): 052314.

[19] Boileau J C, Tamaki K, Batuwantudawe J, *et al*. Unconditional security of a three state quantum key distribution protocol[J]. Physical Review Letters, 2005, 94(4): 040503.

[20] Schiavon M, Vallone G, Villoresi P. Experimental realization of equiangular three-state quantum key distribution[J]. Scientific Reports, 2016, 6: 30089.

[21] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob[J]. Physical Review Letters, 2007, 99(14): 140501.

[22] Zou X, Qiu D, Li L, *et al*. Semiquantum-key distribution using less than four quantum states[J]. Physical Review A, 2009, 79(5): 052312.