doi:10.3788/gzxb20124109.1113

可控量子秘密共享协议窃听检测虚警概率分析

叶天语,蒋丽珍

(浙江工商大学 信息与电子工程学院,杭州 310018)

摘 要:对孙莹等提出的利用 Greenberger-Horne-Zeilinger 态实现的可控量子秘密共享协议 Alice-Bob 信道和 Alice-Charlie 信道窃听检测的虚警概率进行分析,指出该协议窃听检测虚警概率不为 0 的原因在于窃听检测测量基选择的随机性.然后,提出一种改进的利用 Greenberger-Horne-Zeilinger 态实现的可控量子秘密共享协议,以确定性的方式选择窃听检测的测量基.理论分析表明,改进的利用 Greenberger-Horne-Zeilinger 态实现的可控量子秘密共享协议不仅能够以原协议 2 倍的概率发现任何一个内部不可信方,从而具有更高的安全性,而且窃听检测虚警概率达到 0.

关键词:量子密码;可控量子秘密共享;窃听检测;虚警概率

中图分类号:TN918 **文献标识码**:A **文章编号**:1004-4213(2012)09-1113-5

0 引言

量子密码利用量子力学性质实现无条件安全,是量子力学最重要的应用之一.量子密码主要包括量子密钥分配(Quantum Key Distribution,QKD)[1-2]、量子秘密共享(Quantum Secret Sharing,QSS)[3-9]、量子安全直接通信(Quantum Secure Direct Communication,QSDC)[10-13]等方面.QKD 的目标是远距离的合法通信双方利用量子信号的传输在双方之间确立无条件安全的共享密钥.Bennett 和 Brassard[1]于 1984 年利用单粒子载体提出第一个 QKD 协议——BB84 协议.龙桂鲁等[2]于 2002 年提出一个高效的两步 QKD 协议.QSS 是经典秘密共享在量子领域的推广,只有所有秘密共享者合作才能得到通过量子信号传输的秘密.Hillery 等[3]于 1999 年利用 Greenberger-Horne-Zeilinger(GHZ)三重态提出第一个 QSS 方案.孙莹等[4]吸取文献[2]的块传输和分步传输思想,结合文献[5]提出的利用 Grover 搜索算法实现的酉操作,提出的一种利用 GHZ 态实现的可控 QSS 协议.郝亮等[6]认为文献[5]的基于 8 态 Grover 算法的 QSS 协议存在安全漏洞,从而提出相应改进方法.郝亮等[7]进一步提出基于 4 态 Grover 算法的 QSS 协议,并在实验上进行了验证.QSDC 的目标是在远距离的合法通信双方之间利用量子信号直接传送秘密.Beige 等[10]于 2002 年提出第一个 OSDC 协议.邓富国等[11]吸取文献[2]的分步传输思想,利用密集编码提出一个高效 QSDC 协议.

各类量子密码协议都通过窃听检测过程检测是否存在窃听,如果合法通信者发现窃听检测检测到的错误率大于所设定的门限值就认为存在窃听,反之则认为没有发生窃听.量子密码协议的安全性高度依赖于窃听检测过程的有效性.已提出的量子密码协议[1-13]往往只关注并分析窃听检测的漏警概率,却忽略了窃听检测的虚警概率.本文认为一个有效的量子密码协议的窃听检测过程应该具备以下特点:1)当不存在窃听时,该协议的虚警概率应为 0;2)当存在窃听时,该协议能以较高的概率检测到窃听.不幸地是,一些已提出的量子密码协议并未同时具备以上两点,如孙莹等[4]在 2008 年提出的一种利用 GHZ 态实现的可控 QSS 协议.本文以文献[4]的可控 QSS 协议为例分析量子信道的窃听检测虚警概率,指出该协议窃听检测虚警概率不为 0 的原因在于窃听检测测量基选择的随机性.然后,提出一种改进的利用 GHZ 态实现的可控 QSS 协议,以确定性的方式选择窃听检测的测量基.理论分析表明,改进的利用 GHZ 态实现的可控 QSS 协议不仅能够以原协议 2 倍的概率发现任何一个内部不可信方,从而具有更高的安全性,而且窃听检测虚警概率达到 0.

基金项目:国家自然科学基金(No. 60972071)和浙江省自然科学基金(No. LQ12F02012,No. Y6100421)资助

第一作者:叶天语(1982-),男,讲师,工学博士,主要研究方向为量子密码学、信息隐藏与数字水印. Email: flystu008@yahoo.com.cn

收稿日期:2012-02-23;**修回日期**:2012-04-17

1 利用GHZ态实现的可控QSS协议描述及窃听检测虚警概率分析

1.1 协议描述

文献[4]的可控QSS协议存在窃听检测虚警概率不等于0的缺陷.该协议基本内容如下:

Step1:Alice制备N个GHZ态$|\Psi_1\rangle_{ABC}=\frac{1}{\sqrt{2}}(|000\rangle_{ABC}+|111\rangle_{ABC})$,形成2个序列$P(A)=\{P_1(A),P_2(A),\cdots,P_N(A)\}$和$P(BC)=\{P_1(BC),P_2(BC),\cdots,P_N(BC)\}$,分别简记为$P(A)$和$P(BC)$.

Step2:Alice生成一个长$3N$bit的二进制随机序列,并且从事先约定的编码方案中随机选择1种,按码字与$U_i(i=1,2,\cdots,8)$操作的对应,将该二进序列每3 bit一组编码成酉操作,作用在$P(BC)$的每对粒子上,该酉操作记为U_A.然后随机选取$\{I\otimes I,I\otimes H,H\otimes I\}$之一作用在编码后的$P(BC)$的每对粒子上.最后Alice制备一系列随机处于$\{|\varphi^{\pm}\rangle,|\psi^{\pm}\rangle,|\Phi^{\pm}\rangle,|\Psi^{\pm}\rangle\}$8态之一的粒子对穿插在$P(BC)$中,用于检测窃听,称这些粒子对为样本粒子对.样本粒子对的数目足够进行统计分析即可.将新序列记为$P'(BC)$,发送给Bob.

Step3:Bob收到$P'(BC)$后,通知Alice.然后Alice与Bob开始进行窃听检测,步骤如下:

1)Alice告诉Bob随机穿插在$P'(BC)$序列中的样本粒子对的位置.

2)Bob随机选择基$\{|\varphi^{\pm}\rangle,|\psi^{\pm}\rangle\}$和$\{|\Phi^{\pm}\rangle,|\Psi^{\pm}\rangle\}$之一测量$P'(BC)$中的样本粒子对,然后公布所选的测量基和最后的测量结果.

3)Alice根据自己制备样本粒子对的初态信息和Bob公布的测量结果进行比较确定错误率.若错误率大于某固定的阈值,则认为存在窃听,于是放弃该次协议,重新开始;否则继续下一步.

Step4:Alice制备一些随机处于$\{|+z\rangle,|-z\rangle,|+x\rangle,|-x\rangle\}$4态之一的粒子穿插在序列$P(A)$中,这些粒子称为样本粒子,用于检测窃听.样本粒子的数目足够进行统计分析即可.将新序列记为$P'(A)$,发送给Charlie.

Step5:Charlie收到序列$P'(A)$后通知Alice,然后Alice和Charlie开始进行窃听检测,步骤如下:

1)Alice告诉Charlie随机穿插在$P'(A)$序列中的样本粒子的位置.

2)Charlie从$\{\sigma_z,\sigma_x\}$中随机选取测量基测量这些粒子.测量完成后,Charlie公布他所选择的测量基和最后的测量结果.

3)Alice将自己制备样本粒子的初态信息和Charlie公布的测量结果进行比较,确定错误率.若错误率大于某一固定阈值,则认为存在窃听,于是放弃该次协议,重新开始;反之,继续进行下一步.

Step6:Alice从N个GHZ态中随机选出1个,公开它的位置和编码,然后把第2步生成的随机序列中剩下的$3(N-1)$bit作为自己加密所用的密钥.当Alice想让Bob和Charlie重建自己的秘密时,就公布自己对$P(BC)$中哪些粒子作了H操作,从而实现Alice能控制何时重建秘密.

Step7:由于Bob拥有序列$P(BC)$,Charlie拥有序列$P(A)$,所以只有当Bob和Charlie在一起,才能利用8个GHZ态构成的三量子系统完备正交基对Alice编码后的GHZ态的3个粒子进行测量,从而得出U_A.根据Alice公开的在某位置上GHZ态的编码,Bob和Charlie可以推出Alice使用的是哪种编码方案,最终获得Alice加密消息使用的密钥.测量之前,先根据Alice公布的在$P(BC)$哪些粒子上作了H操作,对这些粒子再作1次H操作,然后再分别测量每个GHZ态.这样就保证了只有Bob和Charlie合作才能对Alice的秘密进行解密.

1.2 窃听检测虚警概率分析

文献[4]的可控QSS协议共进行了两次窃听检测,分别为Step3的对Alice-Bob信道进行的窃听检测和Step5的对Alice-Charlie信道进行的窃听检测.这里分别对这两次窃听检测的虚警概率进行分析.

1)不同基下的量子态测量结果

根据量子态投影测量理论,可以得到$|\pm z\rangle$和$|\pm x\rangle$四个量子态在基$\{\sigma_z,\sigma_x\}$下的测量结果如表1所示,括号中的数字表示概率.例如,利用σ_z基对$|+x\rangle$进行测量将分别以1/2的概率得到$|+z\rangle$和$|-z\rangle$.

表1 $|\pm z\rangle$和$|\pm x\rangle$在$\{\sigma_z,\sigma_x\}$基下的测量结果

Table 1 The measurement results of $|\pm z\rangle$ and $|\pm x\rangle$ in the basis of $\{\sigma_z,\sigma_x\}$

	$\|+z\rangle$	$\|-z\rangle$	$\|+x\rangle$	$\|-x\rangle$
σ_z	(1)$\|+z\rangle$	(1)$\|-z\rangle$	$\left(\frac{1}{2}\right)\|+z\rangle$ $\left(\frac{1}{2}\right)\|-z\rangle$	$\left(\frac{1}{2}\right)\|+z\rangle$ $\left(\frac{1}{2}\right)\|-z\rangle$
σ_x	$\left(\frac{1}{2}\right)\|+x\rangle$ $\left(\frac{1}{2}\right)\|-x\rangle$	$\left(\frac{1}{2}\right)\|+x\rangle$ $\left(\frac{1}{2}\right)\|-x\rangle$	(1)$\|+x\rangle$	(1)$\|-x\rangle$

同样地,根据量子态投影测量理论,可以得到4个Bell态和$|\Phi^{\pm}\rangle$与$|\Psi^{\pm}\rangle$8个量子态在基$\{|\varphi^{\pm}\rangle,|\psi^{\pm}\rangle\}$和$\{|\Phi^{\pm}\rangle,|\Psi^{\pm}\rangle\}$下的测量结果如表2所示,括号中的数字表示概率.

表 2　4 个 Bell 态和 $|\Phi^{\pm}\rangle$ 与 $|\Psi^{\pm}\rangle$ 在基 $\{|\varphi^{\pm}\rangle,|\psi^{\pm}\rangle\}$ 和 $\{|\Phi^{\pm}\rangle,|\Psi^{\pm}\rangle\}$ 下的测量结果

Table 2　The measurement results of four Bell states, $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ in the basis of $\{|\varphi^{\pm}\rangle,|\psi^{\pm}\rangle\}$ and $\{|\Phi^{\pm}\rangle,|\Psi^{\pm}\rangle\}$

	$\|\varphi^+\rangle$	$\|\varphi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
$\{\|\varphi^{\pm}\rangle,\|\psi^{\pm}\rangle\}$	(1) $\|\varphi^+\rangle$	(1) $\|\varphi^-\rangle$	(1) $\|\psi^+\rangle$	(1) $\|\psi^-\rangle$	$\left(\frac{1}{2}\right)\|\varphi^+\rangle$	$\left(\frac{1}{2}\right)\|\varphi^-\rangle$	$\left(\frac{1}{2}\right)\|\varphi^-\rangle$	$\left(\frac{1}{2}\right)\|\varphi^+\rangle$
					$\left(\frac{1}{2}\right)\|\psi^-\rangle$	$\left(\frac{1}{2}\right)\|\psi^+\rangle$	$\left(\frac{1}{2}\right)\|\psi^+\rangle$	$\left(\frac{1}{2}\right)\|\psi^-\rangle$
$\{\|\Phi^{\pm}\rangle,\|\Psi^{\pm}\rangle\}$	$\left(\frac{1}{2}\right)\|\Phi^+\rangle$	$\left(\frac{1}{2}\right)\|\Phi^-\rangle$	$\left(\frac{1}{2}\right)\|\Phi^-\rangle$	$\left(\frac{1}{2}\right)\|\Phi^+\rangle$	(1) $\|\Phi^+\rangle$	(1) $\|\Phi^-\rangle$	(1) $\|\Psi^+\rangle$	(1) $\|\Psi^-\rangle$
	$\left(\frac{1}{2}\right)\|\Psi^-\rangle$	$\left(\frac{1}{2}\right)\|\Psi^+\rangle$	$\left(\frac{1}{2}\right)\|\Psi^+\rangle$	$\left(\frac{1}{2}\right)\|\Psi^-\rangle$				

2）Alice-Bob 信道窃听检测虚警概率分析

不失一般性，假设 Alice 在 Step2 制备的穿插在 $P'(BC)$ 中用于检测窃听的某个样本粒子对为 $|\varphi^+\rangle$. Alice 告诉 Bob 该样本粒子对的位置.

①Bob 以 1/2 的概率选择基 $\{|\varphi^{\pm}\rangle,|\psi^{\pm}\rangle\}$ 对该样本粒子对进行测量，那么他的测量结果为 $|\varphi^+\rangle$. Bob 公布所选的测量基和最后的测量结果. Alice 根据该样子粒子对的初态信息和 Bob 公布的测量结果进行比较后认为没有发生窃听行为.

②Bob 以 1/2 的概率选择基 $\{|\Phi^{\pm}\rangle,|\Psi^{\pm}\rangle\}$ 对该样本粒子对进行测量，那么他的测量结果为 $|\Phi^+\rangle$（1/2 的概率）和 $|\Psi^-\rangle$（1/2 的概率）. Bob 公布所选的测量基和最后的测量结果. Alice 根据该样子粒子对的初态信息和 Bob 公布的测量结果进行比较，那么无论 Bob 的测量结果是 $|\Phi^+\rangle$ 还是 $|\Psi^-\rangle$，即使此时没有发生任何窃听，Alice 都将认为此时发生了窃听.

综合①和②，Alice-Bob 信道窃听检测的虚警概率为 $1/2\times(1/2+1/2)=1/2$. 造成 Alice-Bob 信道窃听检测虚警概率不为 0 的原因是 Bob 随机选择基 $\{|\varphi^{\pm}\rangle,|\psi^{\pm}\rangle\}$ 和 $\{|\Phi^{\pm}\rangle,|\Psi^{\pm}\rangle\}$ 之一测量随机穿插在 $P'(BC)$ 中的样本粒子对.

3）Alice-Charlie 信道窃听检测虚警概率分析

不失一般性，假设 Alice 在 Step4 制备的穿插在 $P'(A)$ 中用于检测窃听的某个样本粒子为 $|+z\rangle$. Alice 告诉 Charlie 该样本粒子的位置.

①Charlie 以 1/2 的概率选择基 $\{\sigma_z\}$ 对该样本粒子进行测量，那么他的测量结果为 $|+z\rangle$. Charlie 公布所选的测量基和最后的测量结果. Alice 根据该样子粒子的初态信息和 Charlie 公布的测量结果进行比较后认为没有发生窃听行为.

②Charlie 以 1/2 的概率选择基 $\{\sigma_x\}$ 对该样本粒子进行测量，那么他的测量结果为 $|+x\rangle$（1/2 的概率）和 $|-x\rangle$（1/2 的概率）. Charlie 公布所选的测量基和最后的测量结果. Alice 根据该样子粒子的初态信息和 Charlie 公布的测量结果进行比较，那么无论 Charlie 的测量结果是 $|+x\rangle$ 还是 $|-x\rangle$，即使此时没有发生任何窃听，Alice 都将认为此时发生了窃听.

综合①和②，Alice-Charlie 信道窃听检测的虚警概率为 $1/2\times(1/2+1/2)=1/2$. 造成 Alice-Charlie 信道窃听检测的虚警概率不为 0 的原因是 Charlie 从 $\{\sigma_z,\sigma_x\}$ 中随机选取测量基测量随机穿插在 $P'(A)$ 序列中的样本粒子.

综合 2）和 3），利用 GHZ 态实现的可控 QSS 协议的窃听检测虚警概率为 $1/2\times1/2+1/2\times1/2+1/2\times1/2=3/4$. 显然，该协议的窃听检测虚警概率过高，即使没有发生任何窃听行为，Alice 也会以 3/4 的概率放弃该次协议. 我们认为一个有效的 QSS 协议窃听检测过程应该具备以下特点：1）当不存在窃听时，该协议的虚警概率应为 0；2）当存在窃听时，该协议能以较高的概率检测到窃听. 由上述分析可知，利用 GHZ 态实现的可控 QSS 协议不具备第一个特点，不具有有效性.

2　改进的利用 GHZ 态实现的可控 QSS 协议及其分析

2.1　改进协议描述

文献[4]的可控 QSS 协议存在窃听检测虚警概率不为 0 的缺陷，原因在于 Bob 和 Charlie 窃听检测时测量基选择的随机性. 为了克服这一缺陷，将该协议的 Step3 和 Step5 分别改造为（其他步骤保持不变）：

Step3：Bob 收到 $P'(BC)$ 后，通知 Alice. 然后 Alice 与 Bob 开始进行窃听检测，步骤如下：

1）Alice 告诉 Bob 随机穿插在 $P'(BC)$ 序列中的样本粒子对的位置和对应的测量基.

2）Bob 根据 Alice 告知的测量基测量 $P'(BC)$ 中的样本粒子对，然后公布自己的测量结果.

3）Alice 根据自己制备样本粒子对的初态信息和 Bob 公布的测量结果进行比较确定错误率. 若错误率大于某固定的阈值，则认为存在窃听，于是放弃该次协议，重新开始；否则继续下一步.

Step5：Charlie 收到序列 $P'(A)$ 后通知 Alice，

然后 Alice 和 Charlie 开始进行窃听检测，步骤如下：

1）Alice 告诉 Charlie 随机穿插在 $P'(A)$ 序列中的样本粒子的位置和对应的测量基.

2）Charlie 根据 Alice 告知的测量基测量这些粒子. 测量完成后，Charlie 公布他的测量结果.

3）Alice 将自己制备样本粒子的初态信息和 Charlie 公布的测量结果进行比较，确定错误率. 若错误率大于某一固定阈值，则认为存在窃听，于是放弃该次协议，重新开始；反之，继续进行下一步.

2.2 窃听检测虚警概率分析

对改进的利用 GHZ 态实现的可控 QSS 协议的 Alice-Bob 信道和 Alice-Charlie 信道窃听检测虚警概率进行分析.

1）Alice-Bob 信道窃听检测虚警概率分析

不失一般性，假设 Alice 在 Step2 制备的穿插在 $P'(BC)$ 中用于检测窃听的某个样本粒子对为 $|\varphi^+\rangle$. Alice 告诉 Bob 该样本粒子对的位置和对应的测量基. Bob 选择基$\{|\varphi^\pm\rangle,|\psi^\pm\rangle\}$对该样本粒子对进行测量，那么他的测量结果为 $|\varphi^+\rangle$. Bob 公布自己的测量结果. Alice 根据该样子粒子对的初态信息和 Bob 公布的测量结果进行比较后认为没有发生窃听行为. 因此此时 Alice-Bob 信道窃听检测的虚警概率为 0.

2）Alice-Charlie 信道窃听检测的虚警概率分析

不失一般性，假设 Alice 在 Step4 制备的穿插在 $P'(A)$ 中用于检测窃听的某个样本粒子为 $|+z\rangle$. Alice 告诉 Charlie 该样本粒子的位置和对应的测量基. Charlie 选择基$\{\sigma_z\}$对该样本粒子进行测量，那么他的测量结果为 $|+z\rangle$. Charlie 公布自己的测量结果. Alice 根据该样子粒子的初态信息和 Charlie 公布的测量结果进行比较后认为没有发生窃听行为. 因此，此时 Alice-Charlie 信道窃听检测的虚警概率为 0.

综合 1）和 2），改进的利用 GHZ 态实现的可控 QSS 协议的窃听检测虚警概率为 0.

2.3 安全性分析

对于 QSS 协议，如果可以通过检测窃听发现参与方的窃听，那么任何窃听者（无论内部还是外部）的窃听行为都会被检测到[8]. 于是，QSS 协议的安全目标就是能阻止内部不可信方的欺骗[9].

1）Charlie 是不可信方

假设 Charlie 是不可信方，他在 Step2 截获了 Alice 发给 Bob 的粒子对序列 $P'(BC)$，并将自己生成的假信号序列 $P'(B^*\ C^*)$ 发送给 Bob. 因为 Charlie 不知道 Alice 对 $P(BC)$ 哪些粒子做了 H 操作，所以他此时测量得不到任何信息，也不知道 Alice 随机插入的样本粒子对处于哪个态，伪造序列时只能随机选取$\{|\varphi^\pm\rangle,|\psi^\pm\rangle\}$或$\{|\Phi^\pm\rangle,|\Psi^\pm\rangle\}$基. 不失一般性，假设 Alice 在 Step2 制备的穿插在 $P'(BC)$ 中用于检测窃听的某个样本粒子对为 $|\varphi^+\rangle$. 在窃听检测时，由于 Alice 告诉 Bob 该样本粒子对的位置和对应的测量基，Bob 能够选择正确的测量基$\{|\varphi^\pm\rangle,|\psi^\pm\rangle\}$对该样本粒子对进行测量，那么 Charlie 有两种不会暴露：一是 Charlie 以 1/8 的概率伪造了正确的量子态 $|\varphi^+\rangle$，Bob 测量后能以 1 的概率得到 $|\varphi^+\rangle$；二是 Charlie 以 1/8 的概率伪造了 $|\Phi^+\rangle$或$|\Psi^-\rangle$，Bob 测量后都能以 1/2 的概率得到 $|\varphi^+\rangle$. 因此，Charlie 的窃听行为以 $1-[1/8+(1/8+1/8)\times1/2]=3/4$ 的概率被发现.

2）Bob 是不可信方

假设 Bob 是不可信方，他设法在协议的 Step4 截获 Alice 发给 Charlie 的 $P'(A)$，并将自己生成的假信号序列 $P'(A^*)$ 发送给 Charlie. 不失一般性，假设 Alice 在 Step2 制备的穿插在 $P'(A)$ 中用于检测窃听的某个样本粒子为 $|+z\rangle$. 在窃听检测时，由于 Alice 告诉 Charlie 该样本粒子的位置和对应的测量基，Charlie 能够选择正确的测量基$\{\sigma_z\}$对该样本粒子进行测量，那么 Bob 有两种情况不会暴露：一是 Bob 以 1/4 的概率伪造了正确的量子态 $|+z\rangle$，Charlie 测量后能以 1 的概率得到 $|+z\rangle$；二是 Bob 以 1/4 的概率伪造了 $|+x\rangle$或$|-x\rangle$，Charlie 测量后都能以 1/2 的概率得到 $|+z\rangle$. 因此，Bob 的窃听行为以 $1-[1/4+(1/4+1/4)\times1/2]=1/2$ 的概率被发现.

综合 1）和 2），当 Charlie 是不可信方时，改进的利用 GHZ 态实现的可控 QSS 协议以 3/4 的概率发现 Charlie 的窃听行为；当 Bob 是不可信方时，改进的利用 GHZ 态实现的可控 QSS 协议以 1/2 的概率发现 Bob 的窃听行为. 然而，原协议只能分别以 3/8 和 1/4 的概率发现内部不诚实的 Charlie 和 Bob 的窃听行为. 因此，相比于原协议，改进的利用 GHZ 态实现的可控 QSS 协议能够以 2 倍的概率发现任何一个内部不可信方，从而具有更高的安全性.

3 结论

针对孙莹等利用 GHZ 态实现的可控 QSS 协议，本文分别分析了 Alice-Bob 信道和 Alice-Charlie 信道窃听检测的虚警概率，指出该协议窃听检测虚警概率不为 0 的原因在于窃听检测测量基选择的随机性. 然后，本文提出一种改进的利用 GHZ 态实现的可控 QSS 协议，以确定性的方式选择窃听检测的

测量基. 理论分析表明，改进的利用 GHZ 态实现的可控 QSS 协议不仅能够以原协议 2 倍的概率发现任何一个内部不可信方，从而具有更高的安全性，而且窃听检测虚警概率达到 0. 虽然本文只分析了 QSS 协议的窃听检测虚警概率，由于所有的量子密码协议都有窃听检测的环节，本文的窃听检测虚警概率分析方法可以推广到各类量子密码协议.

参考文献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public-key distribution and coin tossing[C]. Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 1984, **11**: 175-179.

[2] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. *Physical Review A*, 2002, **65**: 032302.

[3] HILLERY M, BUZEK V, BERTHIAUME A. Quantum secret sharing[J]. *Physical Review A*, 1999, **59**(3): 1829-1834.

[4] SUN Ying, QIN Su-juan, WEN Qiao-yan, *et al*. Controllable quantum secret sharing using GHZ states[J]. *The Journal of Beijing University of Posts and Telecommunications*, 2008, **31**(1): 9-13.
孙莹，秦素娟，温巧燕等. 利用 GHZ 态实现可控的量子秘密共享[J]. 北京邮电大学学报, 2008, **31**(1): 9-13.

[5] HSU L Y. Quantum secret-sharing protocol based on Grover's algorithm[J]. *Physical Review A*, 2003, **68**: 022306.

[6] HAO L, LI J L, LONG G L. Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution [J]. *Science China: Physics, Mechanics & Astronomy*, 2010, **53**(3): 491-495.

[7] HAO L, WANG C, LONG G L. Quantum secret sharing protocol with four state Grover algorithm and its proof-of-principle experimental demonstration [J]. *Optics Communications*, 2011, **284**(14): 3639-3642.

[8] KARLSSON A, KOASHI M, IMOTO N. Quantum entanglement for secret sharing and secret splitting [J]. *Physical Review A*, 1999, **59**: 162.

[9] DENG F G, LI X H, ZHOU H Y, *et al*. Improving the security of multiparty quantum secret sharing against Trojan horse attack[J]. *Physical Review A*, 2005, **72**: 044302.

[10] BEIGE A, ENGLERT B G, KURTSIEFER C, *et al*. Secure communication with a publicly known key[J]. *Acta Physica Polonica A*, 2002, **101**: 357.

[11] DENG F G, LONG G L, LIU X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. *Physical Review A*, 2003, **68**: 042317.

[12] ZHAN You-bang, ZHANG Ling-ling, ZHANG Qun-yong. Quantum secure direct communication by entangled qutrits and entanglement swapping [J]. *Optics Communications*, 2009, **282**(23): 4633-4636.

[13] QIN Su-juan, GAO Fei, WEN Qiao-yan, *et al*. Improving the quantum secure direct communication by entangled qutrits and entanglement swapping against intercept-and-resend attack[J]. *Optics Communications*, 2010, **283**(7): 1566-1568.

False Alarm Probability of Eavesdropping Checks for Controllable Quantum Secret Sharing

YE Tian-yu, JIANG Li-zhen

(*College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou* 310018, *China*)

Abstract: The false alarm probability of eavesdropping checks on both Alice-Bob quantum channel and Alice-Charlie quantum channel in the controllable quantum secret sharing protocol using Greenberger-Horne-Zeilinger states proposed by Y. Sun et al. is analyzed. The reason why the total false alarm probability of eavesdropping checks in the controllable quantum secret sharing protocol using Greenberger-Horne-Zeilinger states is not equal to 0 lies in the randomness of measurement basis selection for eavesdropping checks. Afterward, an improved controllable quantum secret sharing protocol using Greenberger-Horne-Zeilinger states is proposed, based on using deterministic measurement basis for eavesdropping checks. Theoretical analysis shows that compared with the original one, the improved scheme can discover the eavesdropping from any internal dishonest participant with twice probability, and possesses much higher security. Moreover, the total false alarm probability of eavesdropping checks in the improved scheme is equal to 0.

Key words: Quantum cryptography; Controllable quantum secret sharing; Eavesdropping check; False alarm probability