Computer Science and Application 计算机科学与应用, 2017, 7(7), 688-695
Published Online July 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.77080

Hans汉斯

A Quantum Key Distribution Protocol Based on the Single Polarization Photon

Tao Fu[1], Haibin Wang[2]

[1]Jiangsu Bosh Company of Software & Technology, Nanjing Jiangsu
[2]School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing Jiangsu
Email: dsfu@vip.sina.com

Received: Jul. 12th, 2017; accepted: Jul. 23rd, 2017; published: Jul. 26th, 2017

Abstract

A simple and efficient quantum key distribution protocol (called SEQDKD) is proposed. Based on the single polarization photon system, the protocol can efficiently realize the quantum key distribution. Meantime, it is more scientific that we use different efficiency calculation methods to measure the efficiency of different protocols. Compared with other common quantum key distribution protocols, our protocol is more efficient and easier to implement. More importantly, this protocol is theoretically proved to be secure against the intercept-resend attack.

Keywords

Key Distribution Efficiency, Quantum Key Distribution, Single Polarized Photon

一种基于单偏振光子的量子密钥分配协议

傅　涛[1]，王海彬[2]

[1]江苏博智软件科技股份有限公司，江苏　南京
[2]南京信息工程大学计算机与软件学院，江苏　南京
Email: dsfu@vip.sina.com

收稿日期：2017年7月12日；录用日期：2017年7月23日；发布日期：2017年7月26日

摘　要

提出一种简单而有效的量子密钥分配协议(简称为SEQDKD)。协议基于单偏振光子系统，实现了高效率的量子密钥分配任务。并针对不同的协议情况而采用不同的效率计算方法，更加科学。相较于常见的量子密钥分配协议而言，本协议达到了高的密钥分配效率并且易于实现。更重要的是，理论论证表明，该

文章引用: 傅涛, 王海彬. 一种基于单偏振光子的量子密钥分配协议[J]. 计算机科学与应用, 2017, 7(7): 688-695.
https://doi.org/10.12677/csa.2017.77080

协议对于截获重发攻击是安全的。

关键词

密钥分配效率，量子密钥分配，单偏振光子

1. 引言

随着量子信息技术的发展，人们实现了很多非常有意义的应用，如量子密钥分配(Quantum Key Distribution, QKD) [1] [2]、量子直接通信(Quantum Direct Communication, QDC) [3] [4]以及量子隐形传态(Quantum Teleportation, QT) [5] [6] [7]等。

总体而言，QKD 协议可以分为两类：一类基于单光子比如 BB84 [1]和 B92 [2]，而另一类基于纠缠系统[8] [9] [10]。就我们所知，单光子系统的优势在于易于实现，但效率较低。相对而言，纠缠系统的效率较高但实现复杂。

在 Degiovanni 等人[11]提出的量子超密密钥分配协议(QDKD)中，通过使用纠缠对的操作来实现密钥信息的嵌入。为了能够实现简单并同时提高效率，我们通过将此 QDKD 协议和传统非对称 BB84 协议结合起来，设计了一种简单且有效的量子超密密钥分配协议(简称为 SEQDKD)。其中，使用两个密钥分配的效率参数：理论效率(ε_1)和实际效率(ε_2)。SEQDKD 协议具有和非对称 BB84 协议相同的实际效率，同时相比 BB84 协议和 Degiovanni 等提出的 QDKD 协议，拥有更高的实际效率。除此之外，本协议和 Degiovanni 等提出的 QDKD 协议一样，具有同样的理论效率，且比 BB84 和非对称 BB84 协议的理论效率要高。

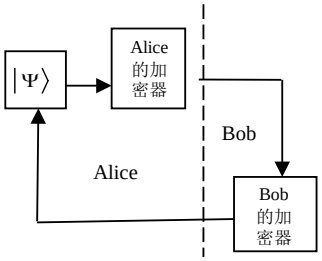
2. SEQDKD 协议内容

首先定义作用于单光子的四个偏振操作：

$$\begin{cases} u_{00}:\theta_p = 0^\circ \\ u_{01}:\theta_p = 45^\circ \\ u_{11}:\theta_p = 90^\circ \\ u_{10}:\theta_p = 135^\circ \end{cases} \tag{2}$$

其中，θ_p 表示光子的偏振角度。图 1 描述了 SEQDKD 协议的基本原理。

Alice 随机制备一个光子态$|\Psi\rangle$并使其以相同概率处于态$|0\rangle$和$|1\rangle$之一，随机使用四个操作之一来使光子偏振，然后将光子发送给 Bob。Bob 不测量他接收到的光子而是同样随机使用四个操作之一并发送回来。Alice 接着以概率$(1-p)$使用 R 基或者以概率 p 使用 D 基测量这个光子从而恢复态$|\Psi\rangle$。测量之后，她宣布“00”表示$|\Psi'\rangle - |\Psi\rangle = |0\rangle$，“01”表示$|\Psi'\rangle - |\Psi\rangle = |-\rangle$，“10”表示$|\Psi'\rangle - |\Psi\rangle = |1\rangle$以及“11”表示$|\Psi'\rangle - |\Psi\rangle = |+\rangle$。接着，Alice 和 Bob 从公共通道共享这些基信息并且将错误的测量基丢弃。Bob 宣称偏振光子处于0°或者90°表示比特“0”，处于45°或者135°表示比特“1”。Alice 可以比较她的光子和 Bob 的宣布信息来判断她用的是正确的基还是错误的基，接着以“Y”和“N”的形式给出响应。Alice



Alice \ Bob	u_{00}	u_{01}	u_{11}	u_{10}
u_{00}	00	01	10	**11**
u_{01}	01	10	11	**00**
u_{11}	10	11	00	**01**
u_{10}	**11**	**00**	**01**	**10**

Figure 1. SEQDKD protocol using single-polarization photonic
图 1. 使用单偏振光子的 SEQDKD 协议

和 Bob 知道他们自己的操作和公开信息“00”、“01”、“10”、“11”，所以他们知道对方使用的操作。最后他们可以共享每个光子的四个 bit 信息。

以一个 12 个比特的序列信息为例，详细的操作如表 1 所示。表中，对于第一个 bit，在 Alice 执行操作之后她得到处于$|0\rangle$态的光子。从公开的比特信息“0”(如不改变使用的基)和 Alice 使用 R 基这两个条件，Alice 可以知道她选择了正确的基。而且，Alice 检查她的测量结果$|1\rangle$和$|\Psi'\rangle-|\Psi\rangle=|1\rangle-|0\rangle=|1\rangle$，并且之后她公布信息“10”。因为 Alice 和 Bob 都知道他们自己的操作，所以 Alice 知道 Bob 使用了操作u_{11}，同时 Bob 知道 Alice 使用了操作u_{00}。最后，他们分享四个信息比特“0011”，其中“00”由 Alice 的操作产生而“11”由 Bob 的操作产生。就是说，每次前两个比特由 Alice 产生而后两个比特由 Bob 产生。

因为 Alice 和 Bob 的部分信息是对外公开的，如 Bob 的公开信息“0”或者“1”和 Alice 的公开信息“00”、“01”、“10”、“11”，所以窃听者 Eve 可以在公共通道通过对他们的公开信息进行相关操作来截获一些信息。比如，表 1 中 Alice 和 Bob 对于第一个比特的公开信息是“10”和“0”。Eve 不会直接获得密钥 B(Bob 拥有的后两个比特)的相关信息，但是她可以知道密钥 B 的可能值为“00”或者“11”。并且根据 Alice 的公开信息“10”，Eve 可以得到密钥 A (Alice 拥有的前两个比特)和密钥 B 的相关性，比如她当密钥 B 是“00”时可推出密钥 A 是“11”。不可否认的是这会产生安全问题，事实上这个问题和 Degiovanni 等的 QDKD 协议的问题是一样的。为了确保安全，我们可以和 QDKD 协议中同样的方式使用密钥 A 和密钥 B。

如图 2 所示，正确接收的全部概率可由情况 1、情况 4、情况 6 和情况 7 相加而得，这样我们就可以得到概率为$\left((1-p)^3+3p^2(1-p)\right)$。本协议中经典比特和量子比特的数量是$b_s=4, b_t=3$且$q_t=q_{(\mathrm{A}\to\mathrm{B})}=q_{(\mathrm{A}\leftarrow\mathrm{B})}=1$，其中当$b_t=3$时步骤 4 中是两个比特且步骤 5 中是一个比特(如表 1 所示)，效率ε_1和ε_2分别是

$$\begin{aligned}\varepsilon_1&=\left(b_s/\left(q_t+b_t\right)\right)\\&=\left(4\times\left((1-p)^3+3p^2(1-p)\right)\right)/(1+3),\\&=\left((1-p)^3+3p^2(1-p)\right)\end{aligned}\tag{3}$$

$$\begin{aligned}\varepsilon_2&=\left(0.5\times b_s/\left(q_{(\mathrm{A}\to\mathrm{B})}+q_{(\mathrm{A}\to\mathrm{B})}\right)\right)\\&=\left(0.5\times4\times\left((1-p)^3+3p^2(1-p)\right)\right)/(1+1).\\&=\left((1-p)^3+3p^2(1-p)\right)\end{aligned}\tag{4}$$

当p趋向于 0 时，$\varepsilon_1=\varepsilon_2$的值趋近于 100%。因为效率$\varepsilon_1=100\%$和 Degiovanni 等的 QDKD 协议一样，本协议也是超密的。

Table 1. Example of Alice sharing 12 bits of information with Bob in SEQDKD protocol
表 1. SEQDKD 协议中 Alice 和 Bob 分享 12 比特信息的例子

	信息序列	1	2	3	4	5	6	7	8	9	10	11	12
(1)	Alice 初始态	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
(2)	Alice 操作	u_{00}	u_{11}	u_{11}	u_{01}	u_{10}	u_{11}	u_{01}	u_{10}	u_{00}	u_{11}	u_{01}	u_{01}
	操作之后粒子态	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
(3)	Bob 操作	u_{11}	u_{11}	u_{10}	u_{11}	u_{10}	u_{10}	u_{00}	u_{00}	u_{00}	u_{00}	u_{01}	u_{10}
	操作之后粒子态	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
(4)	Alice 的基	*R*	*R*	*D*	*D*	*R*	*R*	*D*	*D*	*R*	*D*	*R*	*R*
	公开信息	10	00	01	11	10	01	01	11	00	10	10	00
(5)	Bob 公开信息	0	0	1	0	1	1	0	0	0	0	1	1
(6)	Alice 的反馈	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y
(7)	共享信息	0011	1111	1110	0111	1010	–	0100	1000	0000	–	0101	0110

(1) Alice 随机制备一个光子态 $|\Psi\rangle$ 并使其以相同概率处于态 $|0\rangle$ 和 $|1\rangle$ 之一；(2) Alice 随机使用四个操作之一来使光子偏振；(3) Bob 随机使用四个操作之一来使光子偏振；(4) Alice 使用 R 基或者使用 D 基测量这个光子并宣布结果；(5) Bob 宣称偏振光子处于 0° 或者 90° 表示比特“0”，处于 45° 或者 135° 表示比特“1”；(6) Alice 发回 “Y” 和“N”来表示正确的和错误的基；(7) Alice 和 Bob 共享每个光子的四个 bit 信息。

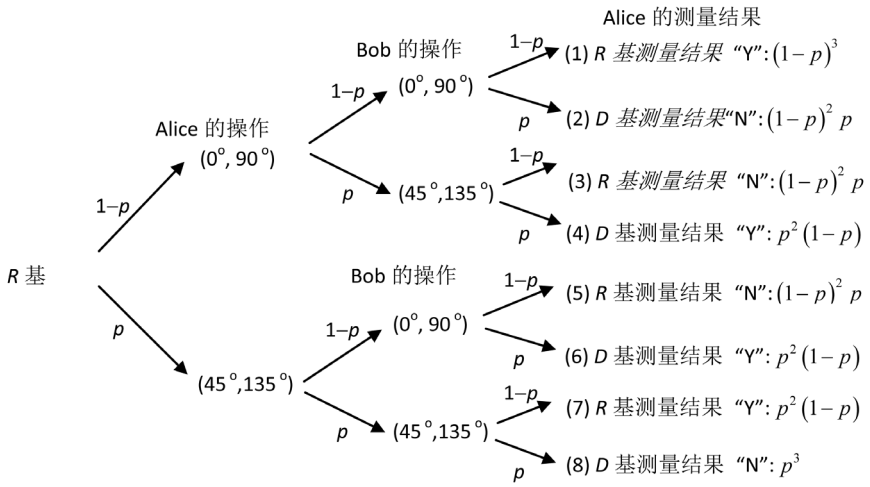


Figure 2. Receive probability of 8 situations
图 2. 所有八种情况的接收概率

3. 安全性分析

3.1. 安全性分析

我们的协议将带有偏振概率的操作作用于单偏振光子来传输秘密信息，因此对于截获重发攻击是脆弱的。和偏振 BB84 协议类似，我们应该对我们的协议进行错误分析。假设窃听者 Eve 使用 R 基以概率 p_R，或者使用 D 基以概率 p_D 截获通道中的光子，并且什么都不做的概率是 $(1-p_R-p_D)$。通过使用截获重发攻击，Eve 有两种方法去破解我们的协议。一种方法是只在一个阶段(Alice→Bob 或者 Bob→Alice 阶段)进行截获重发攻击；另一种方法是在两个阶段(Alice→Bob 和 Bob→Alice 阶段)都进行截获重发攻击。这两种情况的错误概率计算如下：

1) 单阶段截获重发攻击：

在 Alice→Bob (或者 Bob→Alice)阶段通过重发光子，如果选择了错误的基去截获光子就会造成错误。首先，我们讨论在 Alice→Bob 阶段的截获情况，所有的错误情况总结在表 2 中。

假设 Alice 准备了一个处于$|0\rangle$态光子且她的操作是u_{00}或者u_{11}，那么此光子将偏振为$|0\rangle$态光子或者$|1\rangle$态光子，且均由 R 基测量得到。当 Eve 使用 D 基去截获光子，她得到错误测量结果并重新发送错误的光子态($|+\rangle$或者$|-\rangle$)。在 Bob 公布结果之后，Alice 知道基并没有改变，并且她将使用 R 基接收错误的态。但是，因为 Eve 重发的错误的光子而共享错误光子的概率是 50%。最终，这种情况的概率是

$$(1-p)\times(p_D)\times(1-p)\times(1-p)\times 1/2=(1-p)^3(p_D/2) \tag{5}$$

根据错误分析，在 Alice 使用 R 基和 D 基的情况下，Eve 窃听错误概率$E_R^{(\mathrm{A}\to\mathrm{B})}$和$E_D^{(\mathrm{A}\to\mathrm{B})}$分别由下面二式得到：

$$\begin{aligned} E_R^{(\mathrm{A}\to\mathrm{B})} &= \left(\frac{\text{the error probability with eavesdropping using } R\text{-basis}}{\text{the correct received probability without eavesdropping using } R\text{-basis}}\right) \\ &= \left(\frac{\text{Case }(1)+\text{Case }(4)\text{ in Table 2}}{\text{Case }(1)+\text{Case }(7)\text{ in Figure 1}}\right) \\ &= \left((1-p)^3(p_D/2)+(1-p)p^2(p_R/2)\right)\Big/\left((1-p)^3+(1-p)p^2\right) \\ &= \left((1-p)^2p_D+p^2p_R\right)\Big/\left(2\left((1-p)^2+p^2\right)\right) \end{aligned} \tag{6}$$

$$\begin{aligned} E_D^{(\mathrm{A}\to\mathrm{B})} &= \left(\frac{\text{the error probability with eavesdropping using } D\text{-basis}}{\text{the correct received probability without eavesdropping using } D\text{-basis}}\right) \\ &= \left(\frac{\text{Case }(2)+\text{Case }(3)\text{ in Table 2}}{\text{Case }(4)+\text{Case }(6)\text{ in Figure 1}}\right) \\ &= \left((1-p)p^2(p_D/2)+(1-p)p^2(p_R/2)\right)\Big/\left(2(1-p)p^2\right) \\ &= \left((p_D+p_R)/4\right) \end{aligned} \tag{7}$$

因此，对于单阶段(Alice→Bob)中截获重发攻击的平均错误概率$\bar{E}^{(\mathrm{A}\to\mathrm{B})}$为

$$\begin{aligned} \bar{E}^{(\mathrm{A}\to\mathrm{B})} &= \left(\frac{\text{the error probability with eavesdropping}}{\text{the correct received probability without eavesdropping}}\right) \\ &= \left(\frac{\text{Case }(1)+\text{Case }(2)+\text{Case }(3)+\text{Case }(4)\text{ in Table 2}}{\text{Case }(1)+\text{Case }(4)+\text{Case }(6)+\text{Case }(7)\text{ in Figure 1}}\right) \\ &= \left((1-p)^2(p_D/2)+p^2(p_R+p_D/2)\right)\Big/\left(\left((1-p)^2+3p^2\right)\right) \end{aligned} \tag{8}$$

Table 2. The error probability of Eve(E) uses the wrong genes to bug in Alice(A)→Bob(B) stage
表 2. Eve(E)在 Alice(A)→Bob(B)阶段中使用错误的基窃听错误概率

	A 的操作	E 的基	B 的操作	A 的基	错误概率
(1)	$(0^\circ,90^\circ)$ $(1-p)$	D (p_D)	$(0^\circ,90^\circ)$ $(1-p)$	R $(1-p)$	$(1-p)^3(p_D/2)$
(2)	$(0^\circ,90^\circ)$ $(1-p)$	D (p_D)	$(45^\circ,135^\circ)$ (p)	D (p)	$(1-p)p^2(p_D/2)$
(3)	$(45^\circ,135^\circ)$ (p)	R (p_R)	$(0^\circ,90^\circ)$ $(1-p)$	D (p)	$(1-p)p^2(p_R/2)$
(4)	$(45^\circ,135^\circ)$ (p)	R (p_R)	$(45^\circ,135^\circ)$ (p)	R $(1-p)$	$(1-p)p^2(p_R/2)$

假设 Alice 总是窃听到 R 基(比如 $p_R=1$ 和 $p_D=0$)，那么

$$\bar{E}^{(\mathrm{A}\to\mathrm{B})}=\left(p^2\Big/2\left((1-p)^2+3p^2\right)\right) \tag{9}$$

因为 Alice 使用趋近于 1 的概率操作 u_{00} 和 u_{11}，则以概率 $p_R=1$ 和 $p_D=0$ 窃听量子通道是有可能的。当 p 趋近于 0 时平均错误概率 $\bar{E}^{(\mathrm{A}\to\mathrm{B})}\to 0$，故而 Alice 和 Bob 不能检测到 Eve 的窃听存在。错误分析可以使得我们的协议能够抵抗单阶段(Alice→Bob)中的截获重发攻击。很明显，从公式(8)中可以看出，错误概率 $\bar{E}_D^{(\mathrm{A}\to\mathrm{B})}$ 的值为 1/4。

其次，考虑 Bob→Alice 阶段中的拦截。表 3 展示了由于 Bob→Alice 阶段中出现的窃听而导致的错误情况。假设 Alice 准备了一个处于 $|0\rangle$ 态光子，在 Alice 和 Bob 的操作之后，那么此光子将偏振为 $|0\rangle$ 态光子或者 $|1\rangle$ 态光子，且均由 R 基测量得到。当 Eve 使用 D 基去截获光子，她得到错误测量结果并重新发送错误的光子态($|+\rangle$ 或者 $|-\rangle$)。在 Bob 公布结果之后，Alice 知道基并没有改变，并且她将使用 R 基接收错误的态。但是，因为 Eve 重发的错误的光子而共享错误光子的概率是 50%。

在这种情况下，当 Alice 使用 R 基和 D 基的错误概率 $E_R^{(\mathrm{B}\to\mathrm{A})}$，$E_D^{(\mathrm{B}\to\mathrm{A})}$ 以及平均错误概率 $\bar{E}^{(\mathrm{B}\to\mathrm{A})}$ 可以分别一下列公式得到

$$\begin{aligned}E_R^{(\mathrm{B}\to\mathrm{A})}&=\left(\frac{\text{Case }(1)+\text{Case }(4)\text{ in Table 3}}{\text{Case }(1)+\text{Case }(7)\text{ in Figure 1}}\right)\\&=\left((1-p)^3(p_D/2)+(1-p)p^2(p_D/2)\right)\Big/\left((1-p)^3+(1-p)p^2\right)\\&=\left((1-p)^2p_D+p^2p_D\right)\Big/\left(2\left((1-p)^2+p^2\right)\right).\end{aligned} \tag{10}$$

$$\begin{aligned}E_D^{(\mathrm{B}\to\mathrm{A})}&=\left(\frac{\text{Case }(2)+\text{Case }(3)\text{ in Table 3}}{\text{Case }(4)+\text{Case }(6)\text{ in Figure 1}}\right)\\&=\left((1-p)p^2(p_R/2)+(1-p)p^2(p_R/2)\right)\Big/\left(2(1-p)p^2\right)\\&=p_R/2.\end{aligned} \tag{11}$$

$$\begin{aligned}\bar{E}^{(\mathrm{B}\to\mathrm{A})}&=\left(\frac{\text{Case }(1)+\text{Case }(2)+\text{Case }(3)+\text{Case }(4)\text{ in Table 3}}{\text{Case }(1)+\text{Case }(4)+\text{Case }(6)+\text{Case }(7)\text{ in Figure 1}}\right)\\&=\left((1-p)^2(p_D/2)+p^2(p_R+p_D/2)\right)\Big/\left(\left((1-p)^2+3p^2\right)\right)\\&=\left(p^2\Big/\left((1-p)^2+3p^2\right)\right)\text{ for }p_R=1\text{ and }p_D=0.\end{aligned} \tag{12}$$

从以上公式可以明显看出，当 p 趋近于 0 时 $\bar{E}^{(\mathrm{B}\to\mathrm{A})}\to 0$。但是，通过错误分析平均错误概率 $\bar{E}_D^{(\mathrm{B}\to\mathrm{A})}$ 是 1/2。

2) 双阶段截获重发攻击

事实上，Eve 能够在两个阶段(Alice→Bob 和 Bob→Alice)同时进行窃听。考虑这个情况，Eve 在两个阶段中至少会用错一个基。错误基将光子偏振到另一个基并且结果会处于表 3 中可能的错误情况。

在两个阶段(Alice→Bob 和 Bob→Alice)中，当使用 R 基和 D 基由于 Eve 的窃听而分别导致错误的概率，以及平均错误概率可以有下面公式计算得到

$$\begin{aligned}E_R^{(\mathrm{A}\to\mathrm{B})}&=\left(\frac{\text{Case }(1)+\text{Case }(4)+\text{Case }(5)+\text{Case }(8)\text{ in Table 4}}{\text{Case }(1)+\text{Case }(4)+\text{Case }(6)+\text{Case }(7)\text{ in Figure 1}}\right)\\&=\left(\left((1-p)^2\left(2p_D^2+3p_Dp_R\right)+p^2\left(p_R^2+2p_Dp_R+2p_D^2\right)\right)\Big/4\left((1-p)^2+p^2\right)\right)\end{aligned} \tag{13}$$

Table 3. The situation which Eve(E) at least uses one wrong gene in one of the two stages
表 3. 双阶段之一 Eve(E)至少使用一个错误的基的情况

	A 的操作	E 的基	B 的操作	E 的基	A 的基	错误概率
(1)	$(0^\circ,90^\circ)$ $(1-p)$	D (p_D)	$(0^\circ,90^\circ)$ $(1-p)$	–	R $(1-p)$	$(1-p)^3(p_D^2/2)+(1-p)^3(p_Dp_R/4)$
(2)	$(0^\circ,90^\circ)$ $(1-p)$	D (p_D)	$(45^\circ,135^\circ)$ (p)	–	D (p)	$(1-p)p^2(p_Dp_R/2)+(1-p)p^2(p_D^2/4)$
(3)	$(45^\circ,135^\circ)$ (p)	R (p_R)	$(0^\circ,90^\circ)$ $(1-p)$	–	D (p)	$(1-p)p^2(p_R^2/2)+(1-p)p^2(p_Dp_R/4)$
(4)	$(45^\circ,135^\circ)$ (p)	R (p_R)	$(45^\circ,135^\circ)$ (p)	–	R $(1-p)$	$(1-p)p^2(p_R^2/4)+(1-p)p^2(p_Dp_R/2)$
(5)	$(0^\circ,90^\circ)$ $(1-p)$	R (p_R)	$(0^\circ,90^\circ)$ $(1-p)$	D (p_D)	R $(1-p)$	$(1-p)^3(p_Dp_R/2)$
(6)	$(0^\circ,90^\circ)$ $(1-p)$	R (p_R)	$(45^\circ,135^\circ)$ (p)	R (p_R)	D (p)	$(1-p)p^2(p_R^2/2)$
(7)	$(45^\circ,135^\circ)$ (p)	D (p_D)	$(0^\circ,90^\circ)$ $(1-p)$	R (p_R)	D (p)	$(1-p)p^2(p_Dp_R/2)$
(8)	$(45^\circ,135^\circ)$ (p)	D (p_D)	$(45^\circ,135^\circ)$ (p)	D (p_D)	R $(1-p)$	$(1-p)p^2(p_D^2/2)$

$$\begin{aligned} E_D^{\mathrm{A}\to\mathrm{B}} &= \left(\frac{\text{Case }(2)+\text{Case }(3)+\text{Case }(6)+\text{Case }(7)\text{ in Table 4}}{\text{Case }(1)+\text{Case }(4)+\text{Case }(6)+\text{Case }(7)\text{ in Figure 1}}\right) \\ &= \left((1-p)p^2\left(p_D^2/4+p_R^2/2+p_Dp_R/4+p_R^2/2+p_Dp_R\right)\right)\Big/\left(2(1-p)p^2\right) \\ &= \left(\left(5p_Rp_D+p_D^2+4p_R^2\right)/8\right). \end{aligned} \tag{14}$$

$$\begin{aligned} \bar{E}^{\mathrm{A}\to\mathrm{B}} &= \left(\frac{\text{All cases in Table 4}}{\text{Case }(1)+\text{Case }(4)+\text{Case }(6)+\text{Case }(7)\text{ in Figure 1}}\right) \\ &= \left((1-p)^2\left(p_D^2/2+3p_Dp_R/4\right)+p^2\frac{\left(5p_R^2/4+3p_D^2/4+7p_Dp_R/4\right)}{\left((1-p)^2+3p^2\right)}\right) \\ &= \left(\left(5p^2/4\right)\Big/\left((1-p)^2+3p^2\right)\right)\text{ for }p_R=1\text{ and }p_D=0 \end{aligned} \tag{15}$$

当p趋近于0时 $\bar{E}^{(\mathrm{B}\to\mathrm{A})}\to 0$。通过错误分析，错误概率 $\bar{E}_D^{(\mathrm{B}\to\mathrm{A})}$ 的值为1/2。因为 $\bar{E}_D^{(\mathrm{A}\to\mathrm{B})}=1/4$，$\bar{E}_D^{(\mathrm{B}\to\mathrm{A})}=1/2$ 和 $\bar{E}_D^{(\mathrm{B}\to\mathrm{A})}=1/2$，这显然超过了原始BB84协议中的错误概率1/4，Alice和Bob可以成功的检测到Eve的窃听。

3.2. 比较

在 BB84 协议、非对称 BB84 协议、Degiovanni 等 QDKD 协议以及我们提出的协议的比较情况见表 4。当然，效率是 QKD 协议中一个重要的比较因素。效率 ε_1 和 ε_2 都要他们自己的特点，并且我们可以合适的情况使用合适的效率。本文提出的 SEQDKD 协议相对于非对称 BB84 协议和 Degiovanni 等 QDKD 协议而言，效率 ε_1 为 100%(BB84 协议的 $\varepsilon_1=25\%$，且偏振 BB84 协议的 $\varepsilon_1=50\%$)；同时使用单偏振光子实现而不是用纠缠光子对实现，更重要的是，效率 ε_2 的值是 100% (BB84 协议和 QDKD 协议的 $\varepsilon_2=50\%$)。从表 4 可知，在这四个 QKD 协议中，很明显我们提出的协议无论从理论还是从实际出发都是最好的选择。

4. 结论

本节我们提出一个新的协议，协议基于非对称的单偏振光子，实现了高效率的量子密钥分配任务。并针对不同的协议情况(如一阶段协议和二阶段协议)而采用不同的效率计算方法，更加科学。该协议达到

Table 4. The comparison of QKD protocol
表 4. QKD 协议的比较

QKD协议		BB84	偏振BB84	SEQDKD	Degiovanni等协议
经典比特和量子比特数量	b_s	0.5	1	4	2
	b_t	1	1	3	1
	q_t	1	1	1	1
	$q_{(A\to B)}$	1	1	1	1
	$q_{(A\leftarrow B)}$	0	0	1	1
效率	ε_1	25%	50%	100%	100%
	ε_2	50%	100%	100%	50%
其它要求		无	错误分析	单光子操作和错误分析	纠缠对操作和反相关检查
传输阶段		单阶段(Alice→Bob)		双阶段 (Alice→Bob; Bob→ Alice)	
攻击		抗截获重发攻击			不能抗个人攻击
光子类型		单偏振光子			纠缠对

了高的密钥分配效率($\varepsilon_1 = \varepsilon_2 = 100\%$)并且易于实现(单光子)。更重要的是，理论证明表明本协议可以成功抵抗截获重发攻击，是可靠的。

基金项目

江苏省 2016 年度科技发展基金，项目编号：宁科(2016) 138 号。

参考文献 (References)

[1] Bennet, C.H. and Brassard, G. (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, New York, **175**, 8.

[2] Bennet, C.H. (1992) Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, **68**, 3121-3124. https://doi.org/10.1103/PhysRevLett.68.3121

[3] Deng, F.G., Long, G.L. and Liu, X.S. (2003) Two-Step Quantum Direct Communication Protocol Using the Einstein-Podolsky-Rosen Pair Block. *Physical Review A*, **68**, 042317. https://doi.org/10.1103/PhysRevA.68.042317

[4] Liu, Y.M., Wang, D., Liu, X.S., *et al*. (2009) Revisiting Naseri's Secure Quantum Sealed-Bid Auction. *International Journal of Quantum Information*, **7**, 1295-1301. https://doi.org/10.1142/S0219749909005808

[5] Bennett, C.H., Brassard, G., Crépeau, C., *et al.* (1993) Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Physical Review Letters*, **70**, 1895-1899. https://doi.org/10.1103/PhysRevLett.70.1895

[6] Long, L.R., Li, H.W., Zhou, P., *et al.* (2011) Multiparty-Controlled Teleportation of an Arbitrary GHZ-Class State by Using a d-Dimensional (N+2)-Particle Nonmaximally Entangled State as the Quantum Channel. *Science China-Physics Mechanics & Astronomy*, **54**, 484-490. https://doi.org/10.1007/s11433-011-4246-8

[7] Bechmann-Pasquinucci, H. and Tittel, W. (2000) Quantum Cryptography Using Larger Alphabets. *Physical Review A*, **61**, 062308. https://doi.org/10.1103/PhysRevA.61.062308

[8] Ekert, A. (1991) Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, **67**, 661 https://doi.org/10.1103/PhysRevLett.67.661

[9] Bennett, C.H. and Wiesner, S.J. (1992) Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States. *Physical Review Letters*, **69**, 2881-2884. https://doi.org/10.1103/PhysRevLett.69.2881

[10] Lo, H.K. and Chau, H.F. (1999) Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, **283**, 2050-2056. https://doi.org/10.1126/science.283.5410.2050

[11] Degiovanni, I.P., Ruo Berchera, I., Castelletto, S., *et al.* (2004) Quantum Dense Key Distribution. *Physical Review A—Atomic, Molecular, and Optical Physics*, **69**, 032310. https://doi.org/10.1103/PhysRevA.69.032310