引用本文：孔奉波，赖红，熊海灵：基于算术编码的确定性安全量子通信[J]. 光通信技术，2019，43(7)：31–36.

基于算术编码的确定性安全量子通信

孔奉波[1]，赖 红[1]，熊海灵[1,2*]

（1.西南大学 计算机与信息科学学院，重庆 400715；2.西南大学 商贸学院，重庆 402460）

摘要：为了提高量子直接通信的光子利用率和通信效率，基于算术编码提出了一个确定性安全量子通信方案。首先利用喷泉码预先共享少量经典信息，完成测量基信息和解码信息的共享。然后通过简化的算术编码来编码机密信息并制备对应的单光子序列进行机密信息的传输，算数编码的使用提高了协议通信效率和光子利用率。使用与 BB84 协议同样的物理设备可实现该方案。通过安全性分析可知：该方案具有较高的安全性，可抵抗现有的截取－测量－重放攻击、假信号攻击、纠缠附加粒子攻击和光子数分离等攻击手段。

关键词：量子直接通信；确定性安全量子通信；单光子；算术编码

中图分类号：TN918　**文献标识码**：A　**文章编号**：1002-5561(2019)07-0031-06

DOI：10.13921/j.cnki.issn1002–5561.2019.07.008　**开放科学(资源服务)标识码(OSID)**：

Deterministic secure quantum communication based on arithmetic coding

KONG Fengbo[1], LAI Hong[1], XIONG Hailing[1,2*]

(1. College of Computer and Information Science, Southwest University, Chongqing 400715, China;
2. Business College, Southwest University, Chongqing 402460, China)

Abstract: In order to improve the photon utilization and communication efficiency of quantum direct communication, a deterministic secure quantum communication scheme based on arithmetic coding is proposed. Firstly, the fountain code is used to pre-share a small amount of classical information to complete the sharing of measurement base information and decoding information. Then, the secret information is encoded by simplified arithmetic coding, and the corresponding photons sequence are prepared to transmit the secret information. The using of arithmetic coding improves protocol communication efficiency and photon utilization. What's more, the scheme can be implemented using the same physical device as the BB84 protocol. According to the security analysis, the scheme has high security. It can resist the existing intercept-measure-resend attack, false-signal attack, entanglement-measure attack, photon-number-splitting attack, and so on.

Key words: quantum direct communication; deterministic secure quantum communication; single photon; arithmetic coding

0 引言

量子直接通信分为量子安全直接通信（QSDC）和确定性安全量子通信（DSQC）[1]。QSDC 与 DSQC 最大的区别在于除窃听检测外是否需要交换其它经典信息。QSDC 无需交换其它经典信息便可直接得到发送方发送的机密信息，而 DSQC 则需要交换其它经典信息才可以得到发送方发送的机密信息。通过分析现有的多个协议可知，现有的大部分 DSQC 协议要么利用纠缠交换，要么利用酉操作来进行机密信息的加载和传输。然而，这两类协议均具有以下至少一个缺陷：①存在安全性漏洞[2-6]；②需量子存储器的辅助[7,8-10]；③高维纠缠态光子的测量具备一定的难度且成本较高[11-13,9-10,14-15]；④窃听检测和加载机密信息分两步进行，降低了通信效率[4,7,16]；⑤大量光子需来回传输进行窃听检测或消息传递，使其存在木马攻击的风险[4,7,16]；⑥每个粒子至少需要 1 比特的经典信息辅助；⑦需丢

收稿日期：2019–03–24。

基金项目：国家自然科学基金(批准号：41271292，61702427)资助。

作者简介：孔奉波(1993–)，女，硕士，现就读于西南大学计算机与信息科学学院计算机应用技术专业。曾参加由赖红老师主持的国家自然科学基金青年项目“基于斐波那契螺线的轨道角动量纠缠态的量子保密通信研究”(编号 61702427)。主要从事量子通信、量子保密通信方面的研究。

*** 通信作者**：熊海灵(E–mail：xionghl@swu.edu.cn)。

弃用于检测窃听的光子，降低了光子利用率。以上问题的存在使现有的大部分 DSQC 协议在实现上具有一定的技术难度，同时也增加了 DSQC 的成本。因此，针对上述问题，本文利用单光子作为信号源提出一种基于算术编码的 DSQC 方案。

1 背景知识

算术编码是无损信源编码中的一种，属于非分组码，该编码从全序列出发，考虑信源信号之间的依赖关系[18]。本文通过一个具体例子来说明算术编码的具体编码过程。假设信源信号只包含 4 个字符{A，B，C，D}，且各字符出现的概率分别为{0.1，0.4，0.2，0.3}。根据字符概率将初始间隔[0，1)分成 4 个子间隔，即 A[0，0.1)、B[0.1，0.5)、C[0.5，0.7)和 D[0.7，1)。现要编码信息 CADACDB，编码具体计算步骤如表 1 所示，具体过程如下所述：

①首先读入字符 C，因 C 在初始间隔中属于[0.5，0.7)区间，因此在读入信号 C 后编码区间由[0，1)变为[0.5，0.7)；

②接着读入字符 A，因 A 在初始区间[0，1)内占该区间前 10%，因此将其对应到区间[0.5，0.7)的前 10%，得到编码区间[0.5，0.52)；

③重复上述步骤，直到所有字符都被读入，最后得到的编码区间为字符串 CADACDB 的编码区间，任取该区间内任一数作为字符串 CADACDB 的编码值进行输出，如输出 0.5143876。

算术编码的解码过程与编码过程刚好相反，本文不再进行细致阐述。

2 方案描述

本文将算数编码简化，利用简化的算术编码和喷泉码的思想设计了一种安全便捷实用的 QSDC 方案，将一般的 QSDC 中两步(检测和发送机密信息)合并为一步，无需多次来回传送光子序列，也无需丢弃检测窃听的光子，提高了光子利用率。在实际有噪声的信道上可减少光子在量子信道上的损耗，而且无需量子存储器，使得通信安全直接且更简便，方案的大致流程如图 1 所示。方案基于如下 3 个基本假设：

①量子信道属于无噪声信道，攻击者 Eve 可拦截和操纵量子信道上的量子数据；

②经典信道上的信息可被 Eve 窃听，但不能做任何修改；

③发送方 Alice 和接收方 Bob 是合法的通信者。

表 1 字符串 CADACDB 的算术编码过程

步骤	输入符号	编码间隔	间隔
1	C	[0.5，0.7)	0.2
2	A	[0.5，0.52)	0.2×0.1
3	D	[0.514，0.52)	0.2×0.1×0.3
4	A	[0.514，0.5146)	0.2×0.1×0.3×0.1
5	C	[0.5143，0.51442)	0.2×0.1×0.3×0.1×0.2
6	D	[0.514384，0.51442)	0.2×0.1×0.3×0.1×0.2×0.3
7	B	[0.5143876，0.514402)	0.2×0.1×0.3×0.1×0.2×0.3×0.4

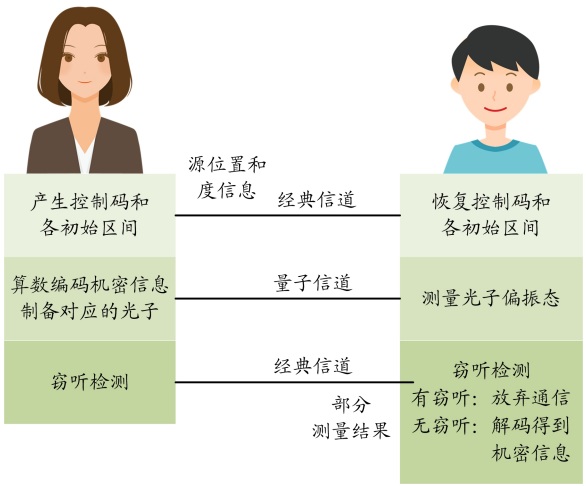

图 1 基于算术编码的确定性安全量子通信过程

2.1 准备和预计算

Alice 将要传送的机密信息的二进制比特串划分为等长的多个信息块 s_i，每块长度均为 4 比特，不足 4 比特的用 0 补齐低位，补位后的机密信息 S 可表示为：

$$S=\mathop{\Big\|}_{i=1}^{k} s_i \tag{1}$$

补位的信息可通过经典信道告知 Bob。在 Bob 解码得到机密信息 S 后将补位去掉即为机密信息的二进制比特串。

2.1.1 编码过程

本文中，$x_i^{[j]}$表示整数序列 x_i 的第 j 个整数，$s_i^{[j]}$表示信息块 s_i 的第 j 位比特值。对 S 中的每块信息 s_i 进行如下编码。

①初始(j=1)：取第 1 级(初始)区间为(a,b)，其中 a、b 满足条件：$b-a$=160。

②递归操作 ($1<j\leqslant 5$)：假设第 j–1 级区间为$(c,$

$d)$，在区间(c,d)内取区间中位数 $x_i^{[j-1]}$。若 $s_i^{[j-1]}=0$，则第 j 级区间取$(a,x_i^{[j-1]})$；若 $s_i^{[j-1]}=1$，则第 j 级区间取$(x_i^{[j-1]},b)$。

③选取第 5 级区间(e,f)内任意一个整数 P，将 P 转化为二进制值，且可在其高位填充适当个数的比特 0，形成比特串 y_i，y_i 即为信息块 s_i 的编码值。填充比特的目的是使攻击者无法根据信息块的比特长度推断其值大小。例如，若 p=1，其二进制值为 1，填充后 y_i=00001，攻击者无法通过二进制比特串的位数得知 P 值。

初始区间为(a,b)时，根据编码过程，秘密信息块 s_i 所对应的所有可能的区间划分如表 2 所示。假设初始区间为(0,160)，s_i=0110，其编码过程如图 2 所示。根据编码规则 s_i=0110 经过编码后的编码值为 y_i=0111111。同时，由表 2 可知，第五级区间(60,70)内的任一整数 P 均可作为 s_i=0110 的编码值，使得同样的信息块 s_i 当初始区间相同时可以用不同的编码值来进行编码，由此也进一步保证了方案的安全性。

表 2 机密信息及其所对应的所有区间划分情况

第一级区间	第二级区间	第三级区间	第四级区间	第五级区间	秘密信息
(a,b)	$(a+80,b)$	$(a+120,b)$	$(a+140,b)$	$(a+150,b)$	1111
				$(a+140,a+150)$	1110
			$(a+120,a+140)$	$(a+130,a+140)$	1101
				$(a+120,a+130)$	1100
		$(a+80,a+120)$	$(a+100,a+120)$	$(a+110,a+120)$	1011
				$(a+100,a+110)$	1010
			$(a+80,a+100)$	$(a+90,a+100)$	1001
				$(a+80,a+90)$	1000
	$(a,a+80)$	$(a+40,a+80)$	$(a+60,a+80)$	$(a+70,a+80)$	0111
				$(a+60,a+70)$	0110
			$(a+40,a+60)$	$(a+50,a+60)$	0101
				$(a+40,a+50)$	0100
		$(a,a+40)$	$(a+20,a+40)$	$(a+30,a+40)$	0011
				$(a+20,a+30)$	0010
			$(a,a+20)$	$(a+10,a+20)$	0001
				$(a,a+10)$	0000

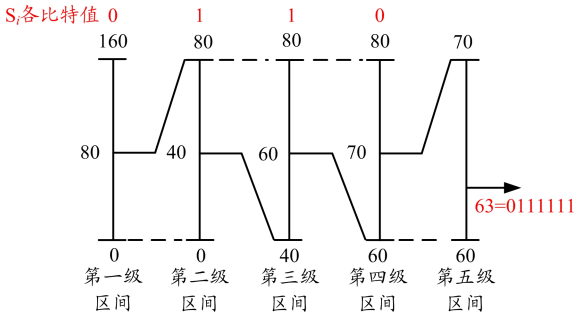

图 2 编码信息块 s_i=0110 的过程

2.1.2 解码过程

由编码信息 y_i 解码得到机密信息块 s_i 的过程如下。

①已知编码信息块 y_i 和第一级区间(a,b)。

②递归操作$(1\leqslant j\leqslant 5)$：将 y_i 与第 j 级区间(m,n)的中位数 $x_i^{[j]}$ 进行比较，当 $y_i>x_i^{[j]}$，则 $s_i^{[j]}=1$，第 j+1 级区间为$(x_i^{[j]},n)$；当 $y_i<x_i^{[j]}$，则 $s_i^{[j]}=0$，第 j+1 级区间为$(m,x_i^{[j]})$。

至此完成对编码信息块 y_i 的解码，恢复机密信息块 s_i。

2.1.3 控制码和初始区间的产生

本文运用喷泉码的编码思想[19]来产生控制码和初始区间。其中，用于编码的源数据通过 BB84 协议的方式产生，且源数据无需很长的比特串。控制码和初始区间保证了我们方案的安全性。其中，控制码决定了非正交态粒子的正确测量基：0 表示线偏振基⊕，1 表示对角偏振基⊗。Alice 和 Bob 协商产生控制码 B_1 的过程如下。

①Alice 与 Bob 通过 BB84 的方式产生一串只有双方知道的比特串作为喷泉码的源数据，其安全性由 BB84 协议安全性保证。

②Alice 通过喷泉码编码的方式产生 14 个编码比特，组成控制码 B_1。通过经典信道将 B_1 中各比特的度和组成该比特的源数据的位置发送给 Bob，Bob 根据收到的度和位置信息，利用源数据恢复出编码比特串 B_1。至此，Alice 和 Bob 完成控制码 B_1 的共享。Alice 与 Bob 协商初始区间的过程如下：

A)Alice 选取任意一个整数 a，得到初始区间(a,b)，其中 b=a+160。

B)整数 a 对应二进制值$(a)_2$，Alice 利用控制码的源码产生$(a)_2$，与喷泉码编码方式不同的是，其编码是通过选取合适的源码连接成$(a)_2$而非选取源码的异或值作为编码信息，将组成$(a)_2$源码的位置信息经过经典信道发送给 Bob。

③Bob 接收到源码的位置信息，通过己方的源码和位置信息，恢复出$(a)_2$的值，由$(a)_2$得到初始区间。

例如，当第一级区间取(23，183)时，假设 Alice 与 Bob 通过 BB84 协议产生的源码为 10110，Alice 与 Bob 产生$(a)_2$的过程如图 3 所示，其中$(23)_2$=10111。

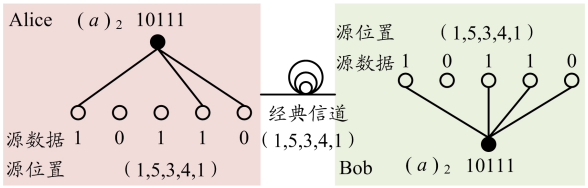

图 3 Alice 与 Bob 协商产生$(a)_2$的过程

我们定义产生的各初始区间的下界值 a 组成的集合为 A：

$$A=\{a_1,a_2,a_3,\cdots,a_k\} \tag{2}$$

由于源码是 Alice 与 Bob 基于 BB84 协议产生的，仅为 Alice 和 Bob 所知，其安全性等价于 BB84 协议的安全性，而 BB84 已被证明是无条件安全的量子密钥分配协议[20]。若不知道源码信息，攻击者 Eve 不能得到控制码和初始区间的相关信息。在实际中，通过 BB84 产生的源码不止图 3 中的 5 个，且 Alice 在选取源码产生$(a)_2$时也可在$(a)_2$的高位补 0 来隐藏$(a)_2$的真实长度。

2.2 DSQC 方案具体过程

我们通过一个例子来阐述方案的具体过程，假设 Alice 要传送给 Bob 的机密信息 S 为比特串 11000100 10100111001110110101010，其长度 l 刚好满足 l mod 4=0，若 l mod 4≠0，则在最后一个信息块的低位用比特 0 补齐，使其每个信息块均为 4 比特。秘密信息 S 划分后表示为 $S=s_1\|s_1\|\cdots\|s_8$。Alice 与 Bob 量子通信的具体过程如下。

①根据 2.1.3 节控制码和初始区间的产生过程，Alice 与 Bob 共同产生 8 个初始区间和 14 比特控制码 B_1。这里假设产生的 8 个初始区间为 d_1=(23，183)、d_2=(5，165)、d_3=(42，202)、d_4=(21，181)、d_5=(54，214)、d_6=(31，191)、d_7=(75，235)和 d_8=(3，163)；控制码为 B1=01101001010110。

②基于初始区间 d_1=(23，183)，Alice 根据本文的编码规则编码机密信息块 s_1=1100，得到第五级区间为(143，153)，取该区间内任一整数 P=150，得到 s_1 的编码值为 y_1=10010110。重复同样的操作来编码其它信息块$\{s_2,s_3,s_4,s_5,s_6,s_7,s_8\}$，得到的结果如表 3 所示。

③Alice 循环使用控制码 B_1 所表示的测量基来制备相应的偏振光子用于编码 y_i，$|H\rangle$和$|L\rangle$偏振光子编码比特 0，$|V\rangle$和$|R\rangle$编码比特 1。由表 3 可得机密信息 S 编码后的编码比特串 Y 长度为 62，需要循环使用 5 次控制码 B_1。

表 3 Alice 编码机密信息 S 的结果

信息块 s_i	初始区间	第 5 级区间	P	编码块 y_i
1100	(23，183)	(143，153)	150	10010110
0100	(5，165)	(45，55)	53	00110101
1010	(42，202)	(142，152)	143	10001111
0111	(21，181)	(91，101)	93	01011101
0011	(54，214)	(84，94)	90	01011010
1011	(31，191)	(141，151)	145	10010001
0110	(75，235)	(135，145)	143	10001111
1010	(3，163)	(103，113)	108	01101100

④Alice 将编码后的光子序列 Q 划分为多个光子序列块 q_i，每个光子序列块 q_i 对应编码信息块 y_i。

$$Q=\{q_1,q_2,q_3,\cdots,q_8\} \tag{3}$$

⑤通过量子信道 Alice 将各光子序列块 q_i 分别发送给 Bob。Bob 循环使用控制码 B_1 选取正确的测量基进行光子序列的测量。

⑥当完成光子序列 Q 的传输后，Bob 也完成了光子偏振态的测量。Alice 选取部分光子与 Bob 进行窃听检测，Bob 告知 Alice 所选取的光子的测量结果，Alice 进行错误比对。当错误率超过约定的阈值，则认为有窃听存在，Alice 与 Bob 重新选取合适的时间再次进行秘密通信，但 2 次通信所选取的初始区间集合 A 不能完全一样。若无窃听，则用于检测窃听的光子的测量结果也无需丢弃，进行纠错后，Bob 根据喷泉码产生的初始区间，利用本文的解码规则进行解码就可得到 S，通过经典信道 Alice 告知 Bob 低位填充的比特位，Bob 去掉填充的比特后得到 Alice 的机密信息。

上述方案适用于 Alice 与 Bob 的机密通信内容较短的情况。当 Alice 有大量机密信息与 Bob 共享时，我们只需将上述步骤中的第一步进行稍微修改即可，即在步骤①中 Alice 只需准备适当个数的初始区间，对各个信息块 s_i 顺序循环使用准备的几个初始区间进行编码，也能达到相同的安全性，同时无需 Alice 的告知 Bob 可自行判断是否需要循环使用初始区间。做这样的处理是因为当 Alice 与 Bob 通信内容较少时，其信息块较少，所需准备的初始区间个数较少，因此经典信息传输也较少。但当 Alice 与 Bob 通信内容

较多时，若对每个信息块均使用不同的初始区间进行编码，所需传送的经典信息较多。

另外，本文设计的方案还较为灵活，可根据实际情况对机密信息块长度的划分进行适当调整，当机密信息块划分长度为 k 比特时，经算术编码的编码值选择第 k+1 级区间内的任一整数即可。同时，本方案还可实现双向 QSDC，将其扩展为量子对话协议。

3 安全性分析

本方案与 BB84 协议相同，量子不可克隆定理保证了窃听者 Eve 无法确定由 Alice 制备和传输的光子的偏振状态。在 BB84 协议中，通信双方随机选择测量基以防止 Eve 通过窃听获取通信内容，而该协议通过提前协商测量基的选取顺序使得只有 Alice 和 Bob 知道测量基选取的正确顺序。而且，本方案用于检测窃听的光子，其测量结果无需丢弃，因为算术编码的特性使单个光子测量结果与其前后多个测量结果相关，因此仅知道不连续的部分测量结果，无法得知其它测量结果依然得不到任何关于 S 的信息。更进一步，即使 Eve 得知其它粒子的测量结果，由于其不知道初始区间，无法正确解码信息，所以也得不到 S 的任何信息。这也使得我们的方案与现有的大部分方案相比更有优势——窃听检测和机密信息传输可一次同时进行。此外，方案中设定初始区间间隔为 160，一方面能够使第五级区间内可用于编码同一个数据块的整数足够多；另一方面即使两信息块相同（s_i=s_j）且初始区间相同（d_i=d_j），也可得到不同的编码信息块（y_i≠y_j），增强了方案的安全性。在此，我们进行典型攻击模式下的安全性分析来证明我们方案的安全性。

3.1 截取–测量–重放攻击

假设 Eve 截取了 Alice 发送给 Bob 的光子并在测量后将其重新发送给 Bob。但是 Eve 并不能得到 Alice 的机密信息 S，反而只会给量子系统引入干扰从而被合法通信者发现。首先 Eve 通过窃听经典信道得知决定控制码 B_1 的各比特的度和决定该比特的源数据的位置信息，同时也可得到决定初始区间各个 a 值的源数据的位置信息。但由于 Eve 不知道源数据比特串，因此不能得到控制码 B_1 和初始区间的任何信息，也就无法得知测量基选取的正确顺序和编码的正确初始区间。其次，初始区间和控制码 B_1 以喷泉码的方式产生，其可以在线生成，具有灵活性和随机性的特点。在这种情况下，Eve 只能通过猜测选择自认为正确的测量基进行测量。控制码 B_1 虽然长度仅为 14 比特，但若无喷泉码的源码信息，Eve 仅能通过猜测选取测量基，其完全选对的概率仅为 $1/2^{14}$=0.0000610351562，该概率微乎其微；当 B_1 长度为更多比特时，Eve 猜测正确所有测量基的概率几乎接近于 0，也就是说 Eve 不可能猜对全部测量基。其对光子的测量只会给系统带来干扰，在 Alice 与 Bob 检测窃听时将会发现窃听的存在而放弃此次直接通信，Eve 也未能从测量的结果中得到任何有用的信息，其测量结果对 Eve 仅是一串随机的比特串。因此，面对此类攻击时，我们的方案是安全的。

3.2 假信号攻击

假设 Eve 截取了 Alice 发送给 Bob 的光子并将自己准备的光子代替合法光子发送给 Bob。同上分析，由于 Eve 发送给 Bob 的“假”光子会在 Alice 与 Bob 检测窃听时被发现，则 Alice 与 Bob 会放弃此次直接通信。由于不知道正确测量基信息，Eve 截取的合法光子也不能得到正确测量结果，其测量结果只能是一串随机的比特串，无任何意义。因此，面对此类攻击时，我们的方案是安全的。

3.3 纠缠附加粒子攻击

假设 Eve 截取发送给 Bob 的合法光子，并把自己准备的粒子与合法粒子纠缠起来，后将合法光子发送给 Bob，而自己保留附加的粒子，期待通过测量附加粒子获取信息。如 Eve 经过幺正操作 E 将其准备的粒子 $|e\rangle$ 与合法光子 $|m\rangle$ 产生纠缠，则有：$|e\rangle|m\rangle\rightarrow a|e_m\rangle|m\rangle+b|\overline{e_m}\rangle|m+1\rangle$，其中，$|a|^2+|b|^2=1$，$\langle e_i|\overline{e_i}\rangle=0$。即 Eve 在不影响单个合法光子的情况下得到该光子的正确测量结果的概率为 $|a|^2$。假设 $|a|^2=1/2$，Alice 传输的光子数为 200 个，可得 Eve 纠缠附加粒子后不引入错误的概率为 $1/2^{200}=6.22301528\times10^{-61}$，该概率几乎接近于 0，Eve 不可能在不引入错误的前提下得到合法光子的量子态。因此，此类攻击手段对于我们的方案无效。

3.4 木马攻击

木马攻击通常利用不可见光子进行信息的窃取。攻击者 Eve 最先考虑的一般都是此类攻击。不可见光子攻击大致过程如下：Eve 预先准备了一系列具有特殊波长的不可见光子，这种光子波长接近合法光子波长；然后 Eve 在 Alice 发送光子之前将不可见光子插入发送给合法参与者的光子中，期待通过合法参与者的反馈信息从而在插入的粒子中获取秘密信息。然而，由于在我们的方案中光子的传输是单向和一次性的，因此可主动避免特洛伊木马攻击。所以 Eve 不能通过

此种攻击手段获取任何有用的信息。我们的方案能有效防止最常见的特洛伊木马攻击。

3.5 光子数分离攻击

光子数分离攻击（Photon Splitting attack，PNS）主要针对现实环境下产生单光子设备的不理想性来进行攻击。因现实设备产生的单光子源不可避免地存在多光子的情况，从而使得攻击者能够截取多余的光子态进行分析而不被合法通信者发现。但此攻击手段对于我们的方案来说是无效的。首先，即使攻击者 Eve 能够分离多光子脉冲中的一个光子，但由于 Alice 与 Bob 并未在经典信道上交换测量基的信息，因此 Eve 不知道正确的测量基，其对光子的测量结果只能是随机比特值，无任何意义。其次，即使 Eve 能从 Alice 与 Bob 窃听检测时交互的经典信息中得到手中部分光子所表示的比特值，但由于其无法得到该光子所在光子序列块 q_i 中的全部光子所表示的编码值，因此 Eve 得不到任何有效的信息。更进一步，即使 Eve 得到光子序列块 q_i 中光子的全部比特值，但由于不知其对应的初始区间不能对其进行正确解码，Eve 同样得不到有用信息。由此可知，面对此类攻击时，我们的方案是安全的。

4 结束语

本文分析了现有方案存在的诸多问题，针对存在的问题，基于算术编码的思想提出一种 DSQC 方案。本方案无需纠缠光子，无需酉操作，也无需量子存储器的协助，通过使用与 BB84 协议同样的物理设备便可实现。结合喷泉码预先共享少量经典信息，完成了机密信息的直接传输和测量解码。结合算术编码，提高光子利用率的同时还增强了方案的安全性，而且算数编码的使用还实现了窃听检测和机密信息加载操作的合并，提高了方案通信效率。安全性分析表明：本方案具有较高的安全性，能抵抗现有的针对量子直接通信的多种攻击手段。除此之外，本方案还可实现双向量子直接通信，因此可将其扩展为量子对话协议。

参考文献：

[1] 龙桂鲁，王川. 量子直接通信[J]. 科学杂志，2009，61(6)：17–22.
[2] SHIMIZU K, IMOTO N. Communication channels secured from eavesdropping via transmission of photonic Bell states [J]. Physical Review A, 1999, 60(1): 157–166.
[3] BEIGE A, ENGLERT B G, KURTSIEFER C, et al. Secure communication with a publicly known key[J]. Acta Phys Pol A, 2002, 101: 357–368.
[4] BOSTRÖM K, FELBINGER T. Deterministic secure direct communication using entanglement [J]. Physical Review Letters, 2002, 89 (18): 187902-1–187902-5.
[5] WÓJCIK A. Eavesdropping on the "ping-pong" quantum communication protocol [J]. Physical Review Letters, 2003, 90 (15): 157901-1–157901-12.
[6] ZHANG Z, LI Y, MAN Z. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss [J]. Physics Letters A, 2005, 341(5–6): 385–389.
[7] ZHU A D, XIA Y, FAN Q B, et al. Secure direct communication based on secret transmitting order of particles [J]. Physical Review A, 2006, 73 (2): 457–460.
[8] LI X H, DENG F G, LI C Y, et al. Quantum secure direct communication without maximally entangled states [J]. Journal of the Korean Physical Society, 2006, 49(4): 1354–1359.
[9] YUAN H, SONG J, ZHOU J, et al. High-capacity deterministic secure four-qubit W state protocol for quantum communication based on order rearrangement of particle pairs [J]. International Journal of Theoretical Physics, 2011, 50(8): 2403–2409.
[10] TSAI C W, HSIEH C R, HWANG T. Dense coding using cluster states and its application on deterministic secure quantum communication [J]. The European Physical Journal D, 2011, 61(3): 779–783.
[11] YAN F L, ZHANG X Q. A scheme for secure direct communication using EPR pairs and teleportation [J]. The European Physical Journal B-Condensed Matter and Complex Systems, 2004, 41(1): 75–78.
[12] MAN Z X, ZHANG Z J, LI Y. Deterministic Secure Direct Communication by Using Swapping Quantum Entanglement and Local Unitary Operations [J]. Chinese Physics Letters, 2005, 22(1): 18–21.
[13] YUAN H, SONG J, ZHOU J, et al. High-capacity deterministic secure four-qubit W state protocol for quantum communication based on order rearrangement of particle pairs [J]. International Journal of Theoretical Physics, 2011, 50(8): 2403–2409.
[14] LIU Z H, CHEN H W, LIU W J, et al. Deterministic secure quantum communication without unitary operation based on high-dimensional entanglement swapping [J]. Science China Information Sciences, 2012, 55(2): 360–367.
[15] JOY D, SURENDRAN S P, SABIR M. Efficient deterministic secure quantum communication protocols using multipartite entangled states [J]. Quantum Information Processing, 2017, 16(6): 157–167.
[16] LUCAMARINI M, MANCINI S. Secure Deterministic Communication without Entanglement [J]. Physical Review Letters, 2005, 94 (14): 140501-1–140501-5.
[17] 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, December 9–12, 1984, Bangalore, India. New York: IEEE Press, 1984.
[18] 傅祖芸，赵建中. 信息论与编码[M]. 第 2 版. 北京：电子工业出版社，2014.
[19] LUBY M. LT Codes[C]// The 43rd Annual IEEE Symposium on Foundations of Computer Science, November 16–19, 2002, Vancouver, BC, Canada. Washington: IEEE Computer Society Press, 2002: 271.
[20] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Physical Review Letters, 2000, 85 (2): 441–444.