Quantum Key Distribution with High Order Fibonacci-like Orbital Angular Momentum States

Z. Pan, J. Cai, C. Wang

Abstract—The coding space in quantum communication could be expanded to high-dimensional space by using orbital angular momentum (OAM) states of photons, as both the capacity of the channel and security are enhanced. Here we present a novel approach to realize high-capacity quantum key distribution (QKD) by exploiting OAM states. The innovation of the proposed approach relies on a unique type of entangled-photon source which produces entangled photons with OAM randomly distributed among high order Fibonacci-like numbers and a new physical mechanism for efficiently sharing keys. This combination of entanglement with mathematical properties of high order Fibonacci sequences provides the QKD protocol which is immune to photon-number-splitting attacks and allows secure generation of long keys from few photons. Unlike other protocols, reference frame alignment and active modulation of production and detection bases are unnecessary.

Index Terms—Orbital angular momentum; quantum key distribution; high order Fibonacci-like sequence .

I. INTRODUCTION

SECURE keys generation between distant users could be realized by using quantum key distribution (QKD) [1], [2], [3], [4]. QKD is to encode and decode the classical keys on the quantum state of single photons, traditionally on the polarization degrees of freedom or the phase degrees of freedom. The non-cloning principle guarantees the security of the QKD process, and that any eavesdropping behavior could be discovered by the communication parties.

However, the high channel loss and low channel capacity are two main disadvantages of quantum communications. During the past decades, various approaches are exploited to reduce the channel loss and extend the communication distance [5], [6]. On the other hand, increasing the dimension of quantum systems would increase the channel capacity which brings several advantages for quantum communication [7], [8], [9]. For example, the coding capacity and the security are increased along with the increment of the Hilbert space, and with the increment of the mutually unbiased bases [10], [11], [12], [13]. Here the larger Hilbert space could be realized by using multi-level atoms [14], [15], hyperentangled photons [16], [17], or the orbital angular momentum (OAM) state of single photons [18], [19], [20].

Z. Pan is with State Key Laboratory of Information Photonics and Optical Communications, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

J. Cai is with State Key Laboratory of Information Photonics and Optical Communications, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

C. Wang is with State Key Laboratory of Information Photonics and Optical Communications, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

Especially, by using OAM state of photons [21], several novel applications in quantum information have been proposed [22], [23], [24], for instance, golden angle (GA) spiral arrays can be applied to generate multiple OAM values encoding well-defined numerical sequences on their farfield radiation patterns [25]. It may also be possible to combine GA spirals with spontaneous parametric down conversion (SPDC) in a nonlinear crystal to engineer a new type of entangled light source, which produces photon pairs whose summation of OAM values is a Fibonacci number. This novel setup allows efficient production of states with large OAM values in quantum communications [26].

Here in this study, we propose a high-capacity coding method and an efficient QKD scheme by employing high order Fibonacci sequence recursion onto OAM states to create a different optical spiral. The third order Fibonacci recursion provides several properties for us to to improve the security from eavesdropping through generating encryption keys with large numbers of digits by using much smaller numbers of photons.

II. QUANTUM KEY DISTRIBUTION USING OAM STATES ENCODED BY THIRD-ORDER FIBONACCI SEQUENCE

Recently, Simon et al. presented a high-capacity QKD scheme by randomly encoding the Fibonacci sequence onto entangled OAM states [27]. Here by introducing the higher order Fibonacci recursion relation, we start with the third-order recursion relation as $F_n = F_{n-1} + F_{n-2} + F_{n-3}$, here we assign the initial values as $F_1 = 1, F_2 = 2$ and $F_3 = 3$. The optical vortices which have been employed for communication can be generated in several different ways: spiral phase plate can generate optical vortices with OAM equals to $l\hbar$; the transformation from Hermite-Gaussian (HG) mode to Laguerre-Gaussian (LG) mode can also be useful to generate the optical vortices we need. Diffractive optical elements can provide another way to generate the optical vortices, for example, by using inhomogeneous anisotropic media [28].

A. Basic setup

Here the source light is prepared in a superposition state with OAM values equal to third-order Fibonacci numbers as (1, 2, 3, 6, 11, 20, 37, 68, ...). And we choose N as the consecutive values, $F = \{F_{n_0}, F_{n_0+1}, ..., F_{n_0+N-1}\}$, and assign a block of binary digits to each so that equal numbers of 0's and 1's occur. Each photon should be able to generate $log_2 N$ bits of information if OAM values in this set are used.
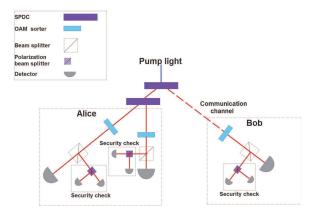
Fig. 1. Setup for the implementation of QKD with Fibonacci-valued OAM states. The pump light is used to pump the nonlinear crystal, producing signal-idler pairs each with three photons through SPDC process. Alice chooses randomly one photon of each pair to send to Bob and keeps the remaining two photons. The OAM sorters are arranged to only allow photons to reach single-photon detectors if they are third-order Fibonacci-valued, with OAM l_{a_1}, l_{a_2} and l_b. These OAM values fulfill the relation: $F_n = l_{a_1} + l_{a_2} + l_b$. Only pairs of values l_{a_1}, l_{a_2} and l_b which sum to F_n values are kept.

For simplicity, we set $N = 8$ to illustrate the principle for qubits coding. The third-order Fibonacci numbers from 1 to 68 can be assigned to three-digit blocks as follows: $1 = 000$, $2 = 001$, $3 = 010$, $6 = 011$, $11 = 100$, $20 = 101$, $37 = 110$, $68 = 111$. Three key digits could be encoded on the OAM of a single photon. The SPDC spiral bandwidth is able to span the largest gap in F. It is obvious that both information capacity and security could be improved with larger sets F. To simplify the case, we assume that OAM sorters only allow positive OAM values to reach the detectors.

As shown in Fig.1, two SPDC processes are exploited for the generation of entangled OAM states in third order Fibonacci sequence. After the first SPDC process, one of each pair (l_b) is sent straight to Bob while the OAM sorters are arranged to allow only photons with OAM in F ($l_b = F_{n_i}$) to register. The other photon(l_a), however, needs another SPDC process to be turned into pairs (l_{a_1}, l_{a_2}) before sending to Alice. The photons reserved by Alice should also be sent through the same OAM sorters as Bob's to make sure that only photons with OAM equal to third-order Fibonacci numbers are eventually retained. As the collinear SPDC (type I or type II) OAM conservations implies the relations $l_{a_1} + l_{a_2} + l_b = l$. In this case, the third-order Fibonacci recursion forces l_{a_1}, l_{a_2} and l_b to be the three adjacent third-order Fibonacci numbers immediately preceding $l = F_n$. For example, by taking $l = F_n = F_6 = 20$, l_{a_1}, l_{a_2} and l_b should be in the set $\{F_{n-1} = F_5 = 11, F_{n-2} = F_4 = 6, F_{n-2} = F_3 = 3\}$.

Moreover, we develop a set of regulations which allows Alice and Bob to generate the three bits' communication through classical channel. And the quantum keys could be generated by the classical calculation on the shared bits. As is illustrated in TABLE I, we allocate one binary bit to each OAM value under the rules as: if $(n \bmod 8) \in \{1, 2, 3, 4\}$, then $B_n = 0$, otherwise $B_n = 1$. Here in TABLE I, we can see that there are only two kinds of bits: $B_1, B_4, B_5, B_8, B_9, ...$ are on the "edge" of each set while $B_2, B_3, B_6, B_7, B_{10}, ...$ are in the "center" of each set.

Based on Alice's possible reception of photons, we can divide all possible situations into 5 categories, as illustrated in TABLE II. For example, if Alice measures two adjacent OAM values in the third-order Fibonacci sequence, like $|F_6\rangle \otimes |F_7\rangle$ with $(B_{a_1}, B_{a_2}) = (1, 1)$ in the third row of TABLE II, then Bob could have the photon with $l_b = F_5$ ($B_b = B_5 = 1$) or F_8 ($B_b = B_8 = 1$). In comparison, the classification from Bob's angle is much simple who has only one photon thus he can only anticipate three possible evaluations for original OAM value l.

B. The regulations of the QKD protocol

Here we present a set of regulation for both Alice and Bob to send binary bits to each other in order to realize practical communication.

As is illustrated in TABLE III, on Alice's side, her first rule is that if she obtains two photons with OAM values equal to F_{n_1} and F_{n_2} where n_1 and n_2 satisfies: $n_2 = n_1 + 2$ and $B_{n-1} = B_{n-2} = p$, then Alice sends $!p$ to Bob first. After that Alice will send another $!p$ to Bob after receiving the responding bit from Bob. Otherwise as her second rule, Alice sends either B_{n_1} or B_{n_2} to Bob first and sends B_{n_2} or B_{n_1} to Bob after receiving the responding bit from Bob.

On Bob's side, here we also define two rules for coding, as is illustrated in TABLE IV.

First, if Bob obtains the photon with OAM value equal to F_{n_3} where $(n_3 \bmod 4) \in \{2, 3\}$ (Bob's bit is a "central" bit). Then if Bob can dope out at least one of Alice's values after she sends her first bit, he would send "1"; otherwise he would send "0" to illustrate his inability to dope out any of Alice's values. This is called the recognition flag for it allows Bob to tell Alice if he is able to dope out at least one OAM value of hers from only the first bit she sends. To be more clear in this situation, if Alice sends Bob $B_{a_1} \neq B_b = B_{n_3}$, then Bob sends "1". Or he sends "0" on condition that he receives Alice's result as $B_{a_1} = B_b = B_{n_3}$.

Second, if Bob has the photon with OAM value equal to F_{n_3} where $(n_3 \bmod 4) \in \{0, 1\}$ (Bob's bit is an "edge" bit). If Alice sends him $B_{a_1} \neq B_b$, then Bob sends the recognition flag as is stated in 1, which is "1" in this particular case. Otherwise if Alice sends Bob $B_{a_1} = B_b$, then Bob sends $!(n_3 \bmod 4)$ to Alice. This would illustrate if Bob's bit is on the "right" edge or the "left" edge of its set.

The whole regulation is showed in TABLE V.

C. The procedures of QKD

Now we analyse the procedures of QKD in detail. First we assume $x = (-1)^{3-(n_3 \bmod 4)}$ to simplify the discussion below and express the exchange process from Bob's perspective.

Bob has the photon with OAM value equal to F_{n_3} where $(n_3 \bmod 4) \in \{2, 3\}$(Bob's bit is a central bit).

1) If Alice sends Bob $B_{a_1} \neq B_b = B_{n_3}$, then it will be easy for Bob to know exactly which OAM value Alice has.

   a) Alice sends her bit according to her second rule. This means that Alice has $|F_{n_3+x}\rangle \otimes |F_{n_3+2*x}\rangle$, so she would surmise that Bob's photon $|F_b\rangle =$

n	1	2	3	4	5	6	7	8	9	10
F_n	1	2	3	6	11	20	37	68	125	230
Sending bits (B_n)	0	0	0	0	1	1	1	1	0	0
Center(c) or edge(e)	e	c	c	e	e	c	c	e	e	c

TABLE I
THE BIT ALLOCATED FOR EACH OAM VALUE.

Alice				Bob		
type		(l_{a_1}, l_{a_2})	(B_{a_1}, B_{a_2})	type	l_b	B_b
adjacent	(c,c)	(F_6, F_7)	(1,1)	e	F_5/F_8	1/1
	(c,e)	(F_7, F_8)	(1,1)	c/e	F_6/F_9	1/0
	(e,e)	(F_8, F_9)	(1,0)	c	F_7/F_{10}	1/0
discontinuous	(c,e)	(F_6, F_8)	(1,1)	c	F_7	1
		(F_7, F_9)	(1,0)	e	F_8	1

TABLE II
THIS TABLE STATES ALL FIVE POSSIBLE SITUATIONS REGARDING ALICE'S RECEPTION OF PHOTONS. BOB'S POSSIBLE RECEPTION IN EVERY SITUATION IS ALSO GIVEN. THE OAM VALUES GIVEN HERE (l_{a_1}, l_{a_2}, l_b) ARE ONLY EXAMPLES TO ELABORATE.

Alice ($F_{a_1} = F_{n_1}$, $F_{a_2} = F_{n_2}$)	The first bit Alice sends to Bob	The second bit Alice sends to Bob
$n_2 = n_1 + 2, B_{n-1} = B_{n-2} = p$	$!p$	$!p$
$n_2 = n_1 + 2, B_{n-1} \neq B_{n-2}$	$B_{n_1}(B_{n_2})$	$B_{n_2}(B_{n_1})$
$n_2 = n_1 + 1$		

TABLE III
ALICE'S REGULATIONS.

Bob's bit B_b (c/e) ($F_b = F_{n_3}$)	The first bit Bob receives from Alice(B_{a_1})	The bit Bob sends to Alice
c	$B_{a_1} \neq B_b$	1
	$B_{a_1} = B_b$	0
e	$B_{a_1} \neq B_b$	1
	$B_{a_1} = B_b$	$!(n_3 \bmod 4)$

TABLE IV
BOB'S REGULATIONS.

Alice(n_1, n_2)	Bob(n_3)	Alice sends to Bob	Bob sends to Alice	Alice sends to Bob
$n_2 = n_1 + 2, B_{n-1} = B_{n-2} = p$	c	$!p \neq B_b$	1	$!p$
		$!p = B_b$	0	$!p$
	e	$!p \neq B_b$	1	$!p$
		$!p = B_b$	$!(n_3 \bmod 4)$	$!p$
$n_2 = n_1 + 2, B_{n-1} \neq B_{n-2}$ or $n_2 = n_1 + 1$	c	$B_{n_1}(B_{n_2}) \neq B_b$	1	$B_{n_2}(B_{n_1})$
		$B_{n_1}(B_{n_2}) = B_b$	0	$B_{n_2}(B_{n_1})$
	e	$B_{n_1}(B_{n_2}) \neq B_b$	1	$B_{n_2}(B_{n_1})$
		$B_{n_1}(B_{n_2}) = B_b$	$!(n_3 \bmod 4)$	$B_{n_2}(B_{n_1})$

TABLE V
THE WHOLE REGULATIONS.

$|F_{n_3}\rangle$ or $|F_b\rangle = |F_{n_3+3*x}\rangle$. If Bob has $|F_{n_3+3*x}\rangle$, he will only be able to dope out one of Alice's value through her first bit if she sends B_{n_3+x}. If he has $|F_{n_3}\rangle$, he will only be able to know any one of Alice's value through her first bit if she sends B_{n_3+2*x}. So Bob sending the recognition flag would be sufficient for Alice to deduce what OAM value Bob has.

Because Bob's bit is a central bit, its minimum distance to the nearest opposite bit should be 2 (The distance between F_n and F_m is defined as $|n - m|$), and the nearest opposite bit is B_{n_3+2*x}. So Bob surmises that Alice should own $|F_{n_3+2*x}\rangle$. Also because all three OAM values Alice and Bob share should be three adjacent third-order Fiboncci numbers, and because Bob already has $|F_{n_3}\rangle$, he can deduce that Alice should also own $|F_{n_3+x}\rangle$ which is between $|F_{n_3+2*x}\rangle$ and $|F_{n_3}\rangle$.

So after receiving Bob's response bit, Alice would send B_{n_3+2*x} which is equal to B_{n_3}.

b) Alice sends her bit according to her first rule.
So she has $|F_{n_3+x}\rangle \otimes |F_{n_3-x}\rangle$ and she sends $!B_{n_3+x}$ and $!B_{n_3-x}$ respectively to Bob regardless of the order while $!B_{n_3+x} = !B_{n_3-x} \neq B_b = B_{n_3}$. In this situation, she already knows that Bob's value is F_{n_3}. So what bit Bob would send doesn't actually matter here for it won't affect Alice's correct guess of Bob's OAM value.

It is worth mentioning that the second rule would not be confused with the first rule as there is only one opposite bit within the maximum distance to B_{n_3} to maintain that all three OAM values are adjacent: B_{n_3+2*x}. So when two opposite bits are sent to Bob, this contradiction would eliminate the possibility of the second rule. During the communication under Alice's second rule, Bob would receive "01" while under her second rule he would receive "00", which would be sufficient for him to distinguish the two cases.

In both cases above Alice should have $|F_{n_3+x}\rangle$. So Bob should send Alice "1" to illustrate that he is able to identify one of Alice's value.

2) If Alice sends Bob $B_{a_1} = B_b = B_{n_3}$, then she can only be sending it according to her first rule.
So Alice could have sent any one in $\{B_{n_3+x}, B_{n_3-x}, B_{n_3-2*x}\}$ and she could have $|F_{n_3+2*x}\rangle \otimes |F_{n_3+x}\rangle$ or $|F_{n_3-x}\rangle \otimes |F_{n_3-2*x}\rangle$. As the two possibilities share no common value of Alice, Bob should send "0" to illustrate his inability to acknowledge any of Alice's bits.

a) If Alice has $|F_{n_3+2*x}\rangle \otimes |F_{n_3+x}\rangle$, she would surmise that Bob has $|F_{n_3+3*x}\rangle$ or $|F_{n_3}\rangle$, each requires a different bit from Alice in order to identify one of Alice's values. This is the same as 1.(a) and Bob would be able to acknowledge all of Alice's values after receiving all two bits from her.

b) If Alice has $|F_{n_3-x}\rangle \otimes |F_{n_3-2*x}\rangle$, she would surmise that Bob has $|F_{n_3-3*x}\rangle$ or $|F_{n_3}\rangle$. If Bob has $|F_{n_3-3*x}\rangle$, he would be able to identify one of Alice's bit through the first bit from her. He wouldn't if he has $|F_{n_3}\rangle$.

So sending the recognition flag here can still help Alice know Bob's value. After that, Alice would send the other bit she has to Bob, which should be able to make Bob fully aware of Alice's values.

Bob has the photon with OAM value $F_b = F_{n_3}$ while $(n_3 \bmod 4) \in \{0, 1\}$. (Bob's bit is an "edge" bit.)

1) If Alice sends Bob $B_a = B_b = B_{n_3}$, then Bob will know that $B_a \in \{B_{n_3+x}, B_{n_3+2*x}\}$. Alice should possess $|F_{n_3+x}\rangle \otimes |F_{n_3+2*x}\rangle$ or $|F_{n_3+x}\rangle \otimes |F_{n_3-x}\rangle$, with a common value $|F_{n_3+x}\rangle$. So Bob sends "1".

a) If Alice has $|F_{n_3+x}\rangle \otimes |F_{n_3-x}\rangle$, then she knows that Bob's value is F_{n_3}. So what bit Bob would send doesn't actually matter here for it won't affect Alice's correct guess of Bob's OAM value.
After Bob sends his bit to Alice, Alice would send another bit of hers to Bob, which is opposite to the first bit she sent to Bob. And because Bob's bit is surrounded closely by two different bits, this would be enough for Bob to know the exact bits Alice has.

b) If Alice has $|F_{n_3+x}\rangle \otimes |F_{n_3+2*x}\rangle$, she would only surmise that Bob has $|F_{n_3}\rangle$ or $|F_{n_3+3*x}\rangle$. Because those two bits are of the same category (they are both "edge" bits), their only difference is whether they are on the "left" or the "right" side of their set. We stipulate that if Bob's bit (B_b) is on the "left" edge of its set, or in another way, $B_{b-1} \neq B_b$ and $B_{b+1} = B_b$, then Bob would send "1" to Alice, otherwise if $B_{b-1} = B_b$ and $B_{b+1} \neq B_b$, then Bob would send "0" to Alice, which forms Bob's second rule to send $!(n_3 \bmod 4)$. This would be sufficient for Alice to acknowledge Bob's value. After this, Alice would send another bit of hers to Bob, leading to their full understanding of each other's values.

2) If Alice sends Bob $B_a \neq B_b = B_{n_3}$, she should possess $|F_{n_3+x}\rangle \otimes |F_{n_3-x}\rangle$ or $|F_{n_3-2*x}\rangle \otimes |F_{n_3-x}\rangle$.

a) If Alice has $|F_{n_3+x}\rangle \otimes |F_{n_3-x}\rangle$, Alice would know Bob's value needless of his bit. And she would be able to inform him of his value later with another bit like in 1.(a).

b) If Alice has $|F_{n_3-2*x}\rangle \otimes |F_{n_3-x}\rangle$, she should surmise that Bob has $|F_{n_3-3*x}\rangle$ or $|F_{n_3}\rangle$. Because if Bob has $|F_{n_3-3*x}\rangle$, he can't determine what value Alice has (let's assume that $B_0 = 1$ to accord the third-order Fibonacci recursion) while he can if he has $|F_{n_3}\rangle$. So Bob could send the recognition flag to Alice as is stated in Bob's rule.
After that Alice would send another bit of hers to pass on all the information Bob needs to know Alice's values.

After these process, Alice and Bob can add up their values

to get the pump value, which serves as one segment of the key.

III. THE SECURITY PERFORMANCE OF THE QKD PROTOCOL

Traditionally, the security checking of the protocol is based on the polarization degrees of freedom. In the proposed QKD protocol, by randomly choosing the photons in the checking mode, the two communication parties could discover the eavesdropping behavior [29]. Moreover, the security checking process could be realized by using the OAM degrees of freedom. During the detection of eveasdropping, if Alice measures $\{l_{a_1}, l_{a_2}\} = \{6, 20\}$, the state reaches Bob should be $|11\rangle$; if Alice measures $\{l_{a_1}, l_{a_2}\} = \{3, 6\}$ or $\{l_{a_1}, l_{a_2}\} = \{20, 37\}$, the state reaches Bob should be $\frac{1}{\sqrt{2}}\{|2\rangle + |11\rangle\}$ or $\frac{1}{\sqrt{2}}\{|11\rangle + |68\rangle\}$. Suppose there is an eavesdropper in the channel, called Eve, who perform the intercept-resend attack on the protocol. For example, she intercepts Bob's photon and reads out the value $l_b = 11$. However, she could not able to know what photon to resend to Bob: $|11\rangle$, $\frac{1}{\sqrt{2}}\{|2\rangle + |11\rangle\}$ or $\frac{1}{\sqrt{2}}\{|11\rangle + |68\rangle\}$. The wrong photons would change the right distribution of each value in Bob's measurement, which would expose her eveasdropping. And it's worth mentioning that as shown in TABLE VI, the classical information exchanged between Alice and Bob is insufficient for an eavesdropper to determine the value.

Assuming an intercept-resend attack is performed by Eve, the average probability of a correct guess is 37.92%. The probability would drop according to the increment of the number of Fibonacci values used. Also the protocol is intrinsically immune to photon-number splitting attack. If a multi-photon pulse is sent into the spiral source, there is no reason for the photons that come out to be in the same state: they are distributed among the different third-order Fibonacci numbers in the same manner as they would if they had been sent one by one. Siphoning off one photon from a pulse will reveal nothing about the state of the other photons in that pulse to the eavesdropper, thus making the attack invalid for Eve.

Moreover, the security checking could be improved by simply changing some unnecessary bits of Alice into the random bits. From the procedure analysis of the protocol, we know that under certain circumstances, Bob would be able to acknowledge at least one value of Alice's through only the first bit of hers. If we change this bit into a random bit or to indicate the method of calculating secret keys, to add up or to multiply for example, the ambiguity will be increased, making it harder for Eve to guess the right value from the classical information exchange. Meanwhile we can make simple rules to determine how to process the values when Bob knows all of them to get the secret keys.

Here we simply change that bit into the random bit. For every case in which Bob would be able to know all Alice's values, we stipulate they choose the smallest two values to add up to get the secret key. The result is shown in TABLE VII. For every case in which Bob would be able to know all Alice's values, we assume that they choose the smallest two
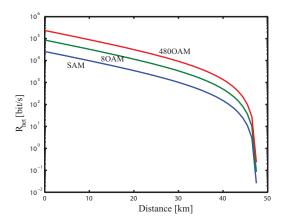

Fig. 2. Bit rate, after error correction and privacy amplification, vs fiber length for QKD protocols with respective coding space of SAM, 8 OAM states and 480 OAM states.

values to add up to get the secret key. The result is shown in TABLE VII.

This table has shown the first step in improving the protocol, and Eve's average correct guessing rate will be decreased to 27.32%.

Some values, like "3", "355", are actually calculated in several different cases(000, 001). This is because in every case in which Bob can acknowledge all Alice's values, we stipulate that the smallest two values be added to get the secret key. By choosing the values with common rules to avoid as many overlap as possible, further improvement can be achieved. Here if we stipulate that they choose digits and the calculating method (add or multiply) differently according to $(n_3 \bmod 4)$ $(l_b = l_{n_3})$, the average correct guess rate can be decreased to 22.01%, as shown in TABLE VIII.

Notice that the distribution of possibilities regarding every classical information exchange case is not balanced. So we can only retain the cases with a relatively better performance (with more possible secret key values) to further improve the protocol. As an extreme case, we only retain the results of the classical information exchange "010" (the case with the most possible key values) and discarded all the others, we may achieve a minimum Eve's correct guessing rate as 10%.

For a coding space of N Fibonacci values, this rate can be decreased to $\frac{9}{10*(N+1)}$, with information entropy density increased to $\log_2 \frac{10*(N+1)}{9}$ per photion. Here we numerically simulated the performance of the protocol in Fig.2 and Fig.3.

First in Fig.2, the relation between the keys rate and the communication distance is presented. Here the frequency f_{rep} is set as 10MHz, the intensity of pulse is 0.1 photon per pulse and the channel loss of the fiber is 0.2dB/km. The efficiency of the detector is set as 0.1, and the dark count of the detector is 10^{-4} per second. The imperfect interference or polarization contrast induced quantum bit error rate is neglected. We found that the keys generation rate increases with the increment of coding space of the OAM states. In Fig.3, we present the relation of the coding bits and security performance with different coding space. In Fig.3(a), the bits values of each
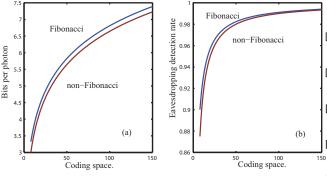
Fig. 3. Figure (a), (b) shows that information entropy carried by every photon and eavesdropping detection rate increase with the enlargement of coding space. Both figures give the performance of both Fibonacci and non-Fibonacci OAM protocols.

photon is enlarged by using our protocol compared with traditional method without Fibonacci. And in Fig.3(b), the security of the protocol is improved as the eavesdropping behavior will easily be discovered.

IV. SUMMARY

In summary, exploiting the OAM states based on third-order Fibonacci recursion, we proposed a high-capacity encoding scheme for quantum key distribution. The secure key distribution is realized by using three particles entangled state and third-order Fibonacci sequence which could be generalized to high-order sequence and multi-parties quantum network. Compared with the traditional method, the probability for detecting the eavesdropper could be increased to 90% with only $N = 8$ OAM values, which can be further improved with the increment of the number of OAM values used. Also the protocol is intrinsically immune to photon splitting attack and the security can be further enhanced implementing a new type of decoy state.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. New York, 1984, pp. 175–179.

[2] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, p. 238, 2003.

[3] F.-G. Deng and G. L. Long, "Controlled order rearrangement encryption for quantum key distribution," *Physical Review A*, vol. 68, no. 4, p. 042315, 2003.

[4] S. Wang, W. Chen, J. F. Guo, Z. Q. Yin, H. W. Li, Z. Zhou, and Z. F. Han, "2 ghz clock quantum key distribution over 260 km of standard telecom fiber," *Optics Letters*, vol. 37, no. 6, p. 1008, 2012.

[5] H.-J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[6] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, "Hybrid quantum repeater using bright coherent light," *Physical Review Letters*, vol. 96, no. 24, p. 240501, 2006.

[7] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Physical Review A*, vol. 61, no. 6, p. 062308, 2000.

[8] R. Heilmann, M. Grafe, S. Nolte, and A. Szameit, "A novel integrated quantum circuit for high-order w-state generation and its highly precise characterization," *Science Bulletin*, vol. 60, no. 1, pp. 96–100, 2015.

[9] M. Huber and M. Pawłowski, "Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement," *Phys. Rev. A*, vol. 88, p. 032309, 2013.

[10] J. Schwinger, "Unitary operator bases," *Proceedings of the National Academy of Sciences of the United States Of America*, vol. 46, no. 4, p. 570, 1960.

[11] I. Ivonović, "Geometrical description of quantal state determination," *Journal of Physics A: Mathematical and General*, vol. 14, no. 12, p. 3241, 1981.

[12] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Annals of Physics*, vol. 191, no. 2, pp. 363–381, 1989.

[13] J. Lawrence, Č. Brukner, and A. Zeilinger, "Mutually unbiased binary observable sets on n qubits," *Physical Review A*, vol. 65, no. 3, p. 032320, 2002.

[14] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. OBrien, A. Gilchrist, and A. G. White, "Simplifying quantum logic using higher-dimensional hilbert spaces," *Nature Physics*, vol. 5, no. 2, pp. 134–141, 2008.

[15] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Physical Review Letters*, vol. 88, no. 12, p. 127902, 2002.

[16] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Physical Review A*, vol. 71, no. 4, p. 044305, 2005.

[17] H. Bechmann-Pasquinucci and A. Peres, "Quantum cryptography with 3-state systems," *Physical Review Letters*, vol. 85, no. 15, p. 3313, 2000.

[18] S. Oemrawsingh, X. Ma, D. Voigt, A. Aiello, E. Eliel, J. Woerdman *et al.*, "Experimental demonstration of fractional orbital angular momentum entanglement of two photons," *Physical Review Letters*, vol. 95, no. 24, p. 240501, 2005.

[19] E. Nagali, D. Giovannini, L. Marrucci, S. Slussarenko, E. Santamato, and F. Sciarrino, "Experimental optimal cloning of four-dimensional quantum states of photons," *Physical Review Letters*, vol. 105, no. 7, p. 073602, 2010.

[20] J. Leach, B. Jack, J. Romero, A. K. Jha, A. M. Yao, S. Franke-Arnold, D. G. Ireland, R. W. Boyd, S. M. Barnett, and M. J. Padgett, "Quantum correlations in optical angle–orbital angular momentum variables," *Science*, vol. 329, no. 5992, pp. 662–665, 2010.

[21] L. Allen, M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, "Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes," *Physical Review A*, vol. 45, no. 11, p. 8185, 1992.

[22] S. Franke-Arnold, L. Allen, and M. Padgett, "Advances in optical angular momentum," *Laser & Photonics Reviews*, vol. 2, no. 4, pp. 299–313, 2008.

[23] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, "Entanglement of the orbital angular momentum states of photons," *Nature*, vol. 412, no. 6844, pp. 313–316, 2001.

[24] L. Chen, J. Lei, and J. Romero, "Quantum digital spiral imaging," *Light: Science & Applications*, vol. 3, p. e153, 2014.

[25] S. F. Liew, H. Noh, J. Trevino, L. Dal Negro, and C. H., "Localized photonic band edge modes and orbital angular momenta of light in a golden-angle spiral," *Opt. Express*, vol. 19, p. 23631, 2011.

[26] M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, "Efficient separation of the orbital angular momentum eigenstates of light," *Nature Communications*, vol. 4, p. 2781, 2013.

[27] D. S. Simon, N. Lawrence, J. Trevino, L. Dal Negro, and A. V. Sergienko, "High-capacity quantum fibonacci coding for key distribution," *Physical Review A*, vol. 87, no. 3, p. 032312, 2013.

[28] L. Marrucci, C. Manzo, and D. Paparo, "Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media," *Physical Review Letters*, vol. 96, no. 16, p. 163905, 2006.

[29] G. L. Long, F.-G. Deng, C. Wang, X.-H. Li, K. Wen, and W.-Y. Wang, "Quantum secure direct communication and deterministic secure quantum communication," *Frontiers of Physics in China*, vol. 2, no. 3, pp. 251–272, 2007.

Eve sees	000	001	010	011	100	101	110	111
Secret key	6,11	20,423	11,20,68, 125,423	20,37,230	37,230	68,125	20,37,230, 423	6,11,37, 125,230

TABLE VI

IN THE TOP ROW, THE FIRST AND THE THIRD DIGIT IN EACH PAIR ARE THE CLASSICAL BITS SENT BY ALICE SEPARATELY, THE SECOND DIGIT IS THE BIT SENT BY BOB. THE SECOND ROW SHOWS ALL CORRESPONDING POSSIBLE SECRET KEYS.

Eve sees	000	001	010	011	100	101	110	111
Secret key	3,5,355	3,9,355	9,17,26, 162,193	9,17,26, 162,193	31,105	31,105,57	2,14,17, 31,105, 193,298	2,14,17, 31,105, 193,298

TABLE VII

IN THE TOP ROW, THE FIRST AND THE THIRD DIGIT IN EACH PAIR ARE THE CLASSICAL BITS SENT BY ALICE SEPARATELY, THE SECOND DIGIT IS THE BIT SENT BY BOB. THE SECOND ROW SHOWS ALL CORRESPONDING POSSIBLE SECRET KEYS.

Eve sees	000	001	010	011	100	101	110	111
Secret key	3,6,11	2,20, 423, 28750	2,14,51,17, 31,105,193, 298,13125, 44390	0,33,30, 66,2516, 15640, 8500	9,17,26, 162,193 1147, 3876	18,66,99, 120,340, 4625, 7141, 8500	37,31, 230	220,68, 125

TABLE VIII

IN THE TOP ROW, THE FIRST AND THE THIRD DIGIT IN EACH PAIR ARE THE CLASSICAL BITS SENT BY ALICE SEPARATELY, THE SECOND DIGIT IS THE BIT SENT BY BOB. THE SECOND ROW SHOWS ALL CORRESPONDING POSSIBLE SECRET KEYS.