www.nature.com/scientificreports

SCIENTIFIC REPORTS

OPEN

Received: 04 April 2016
Accepted: 18 July 2016
Published: 12 August 2016

Hybrid threshold adaptable quantum secret sharing scheme with reverse Huffman-Fibonacci-tree coding

Hong Lai[1], Jun Zhang[2], Ming-Xing Luo[3], Lei Pan[2], Josef Pieprzyk[4,5], Fuyuan Xiao[1] & Mehmet A. Orgun[6,7]

With prevalent attacks in communication, sharing a secret between communicating parties is an ongoing challenge. Moreover, it is important to integrate quantum solutions with classical secret sharing schemes with low computational cost for the real world use. This paper proposes a novel hybrid threshold adaptable quantum secret sharing scheme, using an *m*-bonacci orbital angular momentum (OAM) pump, Lagrange interpolation polynomials, and reverse Huffman-Fibonacci-tree coding. To be exact, we employ entangled states prepared by *m*-bonacci sequences to detect eavesdropping. Meanwhile, we encode *m*-bonacci sequences in Lagrange interpolation polynomials to generate the shares of a secret with reverse Huffman-Fibonacci-tree coding. The advantages of the proposed scheme is that it can detect eavesdropping without joint quantum operations, and permits secret sharing for an arbitrary but no less than threshold-value number of classical participants with much lower bandwidth. Also, in comparison with existing quantum secret sharing schemes, it still works when there are dynamic changes, such as the unavailability of some quantum channel, the arrival of new participants and the departure of participants. Finally, we provide security analysis of the new hybrid quantum secret sharing scheme and discuss its useful features for modern applications.

Secret sharing is an important and powerful tool for protecting confidentiality and integrity of sensitive information, such as missile launch codes, bank account information, medical information and encryption keys. Secret sharing can be categorized into two broad classes: classical and quantum. Secret sharing was invented in its classical form simultaneously by Shamir[1] and Blakley[2]. The Shamir secret sharing splits a secret into multiple shares in such a way that a large enough collection of shares can be used to reconstruct the secret. The minimum number of shares that enables the reconstruction is called the threshold or in general the access structure. However, if the number of shares is smaller than the threshold, then they provide no information about the secret. In other words, when a fewer than the threshold number of shares are compromised, the secret cannot be revealed. Later many other secret sharing schemes[3–7] have been proposed to improve the traditional ones. The obvious weakness of classical secret sharing is that an adversary can duplicate shares without being detected. As a result, eavesdropping attacks could happen in the reconstruction phase when the participants send their shares to a combiner who computes the secret.

To address the eavesdropping problem, Hillery *et al.*[8] extended classical secret sharing (CSS) to a (m, n)-threshold quantum secret sharing (QSS), which is the generation of quantum key distribution (QKD)[9–11]. In their scheme, GHZ states are used to transmit the shares securely in the presence of eavesdroppers, like the method used in ref. 12. The security of their scheme is guaranteed by the quantum no-cloning theorem[13]. Following Hillery *et al.*'s work, many quantum secret sharing schemes[14–27] have been proposed with rigorous security proofs as well

[1]School of Computer and Information Science, Southwest University, Chongqing 400715, China. [2]School of Information Technology, Deakin University, Geelong, VIC, 3220, Australia. [3]School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China. [4]School of EE&CS, Queensland University of Technology, Brisbane, Australia. [5]Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland. [6]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia. [7]Faculty of Information Technology, Macau University of Science and Technology, Avenida Wai Long, Taipa, 999078, Macau. Correspondence and requests for materials should be addressed to H.L. (email: hlai@swu.edu.cn) or M.A.O. (email: mehmet.orgun@mq.edu.au)

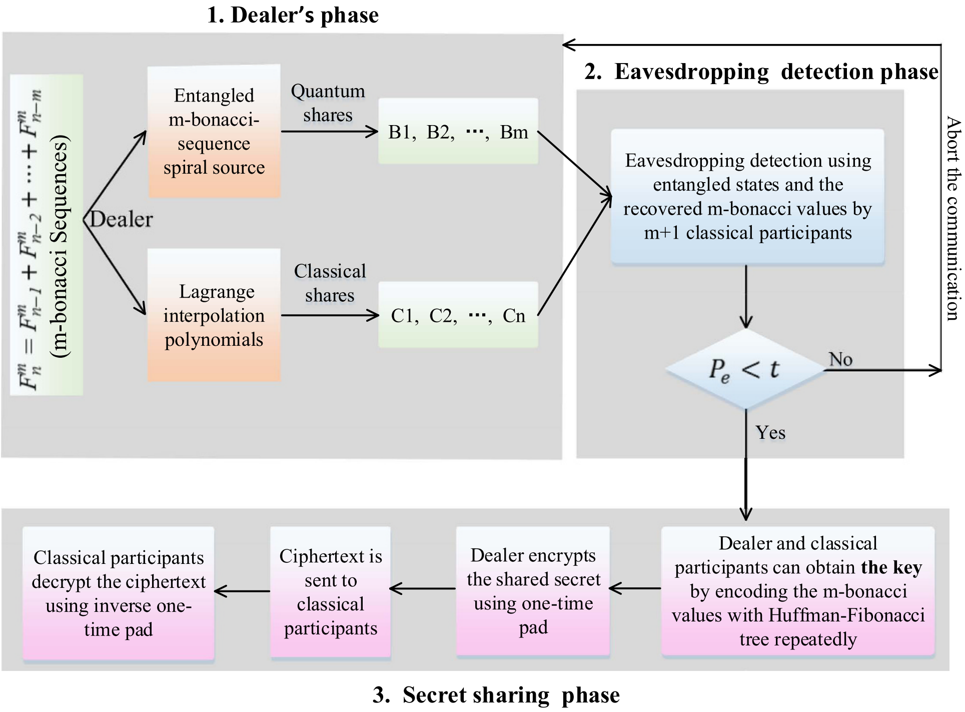
1. Dealer's phase
$F_n^m = F_{n-1}^m + F_{n-2}^m + \cdots + F_{n-m}^m$ (m-bonacci Sequences)
Dealer
Entangled m-bonacci-sequence spiral source
Quantum shares
B1, B2, ···, Bm
Lagrange interpolation polynomials
Classical shares
C1, C2, ···, Cn
2. Eavesdropping detection phase
Eavesdropping detection using entangled states and the recovered m-bonacci values by m+1 classical participants
$P_e < t$
No
Yes
Abort the communication
Dealer and classical participants can obtain the key by encoding the m-bonacci values with Huffman-Fibonacci tree repeatedly
Dealer encrypts the shared secret using one-time pad
Ciphertext is sent to classical participants
Classical participants decrypt the ciphertext using inverse one-time pad
3. Secret sharing phase

Figure 1. The sketch for the hybrid threshold adaptable QSS scheme which consists of three parts. $F_n^m = F_{n-1}^m + F_{n-2}^m + \cdots + F_{n-m}^m$ represents *m*-bonacci sequences, $B_1, B_2, \cdots, B_m$ denote *m* quantum shares, and $C_1, C_2, \cdots, C_n$ denote *n* classical shares, P_e denotes the error rate and *t* the preset threshold value for P_e.

as properties that make them suitable for many applications. Though quantum secret sharing can detect eavesdropping, Źukowski *et al.*[23] argue that QSS is different from CSS. The main difference is that in QSS, the choice of parameters *m* and *n* is restricted while in CSS, the parameters can be arbitrarily selected as long as $n \geq m$. In particular, in a (*m*, *n*)-threshold QSS, the parameters *m*, *n* must satisfy the condition, $2m - 1 > n$, which is imposed by the quantum no-cloning theorem[13]. However, in practice, security policies and the adversary structure demand the parameters *m* and *n* to be flexible and scalable. Therefore, it is very challenging to develop a new (*m*, *n*)-threshold QSS scheme, whose parameters *m* and *n* are not restricted.

In this paper, we propose a hybrid quantum secret sharing scheme to address this challenge. The new scheme is free from any restrictions on the parameters *m* and *n* and therefore it is suitable for many real-world applications. We employ entangled states prepared by *m*-bonacci sequences to detect eavesdropping, which can be done by any subset of participants that contains at least $\left\lceil \frac{m}{2} \right\rceil$ (ceiling $(x) = \lceil x \rceil$ is the smallest integer greater than or equal to *x*) members. That is to say, not all participants are required to reach a consensus in order to reveal eavesdropping. We use *m*-bonacci sequences encoded in Lagrange interpolation polynomials to generate the secret, with no restrictions imposed on the parameters *m*, *n*. Given that *m*-bonacci numbers can be represented by Fibonacci numbers, we use the structure of the Huffman-Fibonacci tree with the greedy algorithm to encode *m*-bonacci sequences, i.e., the higher the frequency at which a Fibonacci number appears in *m*-bonacci sequences, the longer the block of binary codes. Therefore, our scheme can greatly improve the coding capacity, thus reducing the use of entangled photons, which are expensive and difficult to prepare. In real-world applications, some changes may occur when a new participant joins or alternatively, an existing participant leaves or there is a sudden disruption of some quantum channels. The new scheme has the capability to deal with such changes since the *m*-bonacci-number coding can be easily modified to reflect changes in secret sharing.

Results

In this section, we first describe a new hybrid quantum secret sharing based on *m*-bonacci sequences, as shown in Fig. 1. The scheme consists of two components: quantum and classical. The classical component allows to establish an infinite random sequence in a way of quantum encoding, which is shared by classical participants. The classical shares of the random sequence allow any $m+1$ participants to recover the sequence. The one-time-pad encryption is done by a collection of $m+1$ classical participants. The decryption can be done by any other collection of $m+1$ classical participants. There are three phases in the proposed scheme:

- share generation and distribution – the dealer phase
- eavesdropping detection phase
- secret reconstruction phase

Then its security is analyzed and compared with other related QKD protocols.

F_n^m	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$	$n=9$	$n=10$
$m=2$	1	2	3	5	8	13	21	34	55	89
$m=3$	1	2	4	7	13	24	44	81	149	274
$m=4$	1	2	4	8	15	29	56	108	208	401
$m=5$	1	2	4	8	16	31	61	120	236	464
$m=6$	1	2	4	8	16	32	63	125	248	492

Table 1. Fibonacci numbers of order $m = 2, 3, 4, 5, 6$.

New hybrid threshold quantum secret sharing scheme. First, we introduce the generalized Fibonacci sequence[28], that is so-called m-bonacci sequence which is used in our later scheme. The m-bonacci sequence of order $m \geq 2$ denoted by F_n^m ($n \in \mathbb{N}_+$) is defined by the following recurrence[28,29]:

$$F_n^m = F_{n-1}^m + F_{n-2}^m + \cdots + F_{n-m}^m; \tag{1}$$

with the first $m - 2$ initial terms set to 0 and the $(m - 1)$th initial term set to 1. In particular, the 2-bonacci sequence is the usual Fibonacci sequence[30]; 3-bonacci sequence is usually called the Tribonacci sequence[28]. In Table 1, we list the first ten m-bonacci numbers when $m = 2, 3, 4, 5, 6$.

Then, we present the entities used in our secret sharing, which are as follows:

- a dealer,
- m (which is the same as m in m-bonacci numbers) participants who hold quantum shares (quantum participants),
- ℓ participants who hold classical shares (classical participants) and
- Adversaries.

Dealer is a party who is trusted by all quantum and classical participants. It is responsible for the initialization of the secret sharing. It generates shares and distributes them to all the participants. It is assumed that after finishing its tasks, the dealer "forgets" all the parameters of the scheme together with the secret.

Quantum participants hold their quantum shares. Each quantum participant owns one quantum share. Their task is to detect eavesdropping. This guarantees unconditional security of the scheme.

Classical participants hold their classical shares. There are ℓ classical participants. They are responsible for secret reconstruction. Each classical participant receives their share from the dealer via a classical secure channel. Unlike in CSS, in our hybrid QSS, any q ($q \geq m + 1$) classical participants can recover the key (secret) using their classical shares (after eavesdropping detection).

Adversaries includes the outsider and at most m insiders. The former has no valid share, while the latter is actually a legal participant with a valid share.

Finally, the proposed hybrid $((t', \quad m), (m + 1, \quad \ell))$ threshold QSS is defined as follows:

Definition 1 (Hybrid $((t', \ m), (m + 1, \quad \ell))$ threshold QSS). There are m (where $\ell > m > t'$) quantum participants and ℓ classical participants. The secret can be recovered by $m + 1$ classical participants and t' quantum participants. t' quantum shares from t' quantum participants can be used for eavesdropping detection while $m + 1$ classical shares owned by $m + 1$ classical participants can be used to recover the secret.

The steps of our scheme are described in details as follows:

Dealer phase. (1) Dealer first prepares entangled states using the m-bonacci number source as shown in Fig. 2. To be exact, the entangled states are prepared by the recurrence relation $F_n^m = \sum_{i=1}^{m} F_{n-i}^m$ on the Vogel spiral (refer to Simon *et al.*'s work[31,32]). After entering the spontaneous parametric down conversion (SPDC), the entangled states are broken into m entangled photons with smaller m-bonacci values. Each red circle dot represents an orbital angular momentum (OAM) shifter that takes the OAM in that branch to zero. Each place where lines split or cross is implied to have a beam splitter. The portion shown has OAM values from F_{n-1}^m to F_{n-m}^m coming out of the OAM sorter.

An OAM-entangled outgoing state depends on m, which is as follows:

$$\sum_m (|F_{n-1}^m F_{n-2}^m \cdots F_{n-m}^m\rangle + |F_{n-2}^m F_{n-3}^m \cdots F_{n-1}^m\rangle + \cdots + |F_{n-m}^m F_{n-1}^m \cdots F_{n-m+1}^m\rangle)_{B_1 B_2 \cdots B_m} \tag{2}$$

where the index m runs through the allowed m-bonacci numbers in the pump beam: $\sum |F_n^m\rangle$. Each of the m quantum participants receives one entangled photon from the entangled states. In the lab of each quantum participant, there are two types of detection sorters (i.e., the E_i sorter and the F_i sorter, $i \in \{1, 2, \cdots, m\}$), directing the entangled photon to one of them at random. The E_i sorter is made up of an OAM sorter[33] followed by a set of single-photon detectors. The OAM sorter transmits OAM eigenstates of various pump values into various outgoing directions, allowing them to be registered and determined in different detectors. The F_i sorter is used to distinguish different superpositions of the form. The states obtained in the E_i- and F_i- type measurements are nonorthogonal to each other. Therefore, the security of our proposed scheme is based on the fact that nonorthogonal states are indistinguishable[34], and this principle is similar to the one used in the BB84[9] and Ekert[10] protocols. However, the equation (2) has an unusual feature, that is, the states detected in the E_i-type measurement form a mutually orthogonal set among themselves, while those in the F_i-type measurements are not all orthogonal to each other but form a

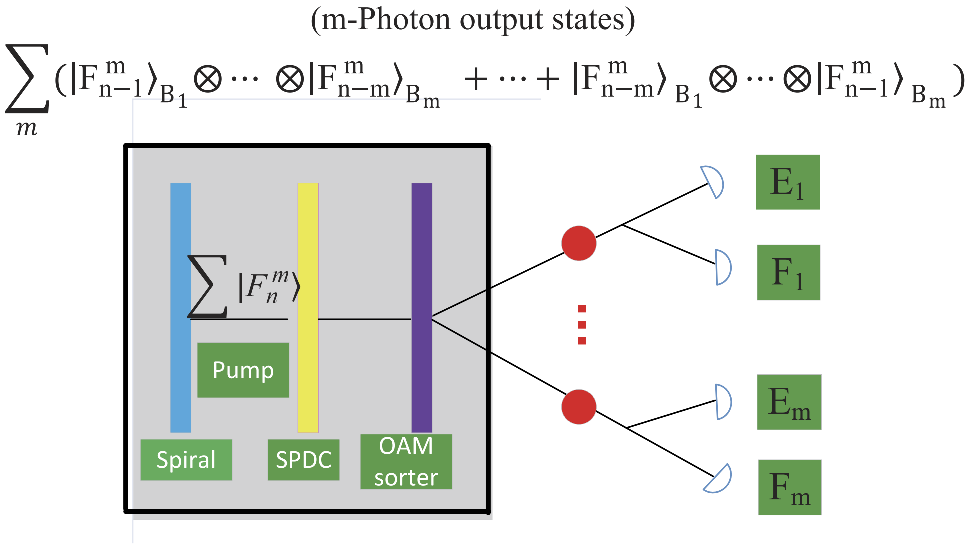
(m-Photon output states)
$\sum_m (|F^m_{n-1}\rangle_{B_1} \otimes \cdots \otimes |F^m_{n-m}\rangle_{B_m} + \cdots + |F^m_{n-m}\rangle_{B_1} \otimes \cdots \otimes |F^m_{n-1}\rangle_{B_m})$
$\sum |F^m_n\rangle$
Pump
Spiral
SPDC
OAM sorter
E1
F1
Em
Fm

Figure 2. Setup for entangled states with *m*-bonacci-valued OAM on the Vogel spiral adapted from that of Simon *et al*.[31,32]. After entering SPDC, the entangled states are broken into m entangled photons. Each red circle dot represents an OAM shifter that takes the OAM in that branch to zero. Each place where lines split or cross is implied to have a BS. The portion shown has OAM values from F^m_{n-1} to F^m_{n-m} coming out of the OAM sorter. A pair of detectors E_i and F_i ($i \in \{1, 2, \cdots, m\}$) are used at the output ports of the final nonpolarizing BSs. The E_i sorter is used for allowing photons to arrive at the arrays of single-photon detectors when they are m-bonacci values, and the F_i sorter is used for allowing "diagonal" superposition and filtering out any non-m-bonacci values.

chain, where each state is nonorthogonal to the two adjacent states in the chain. Moreover, for orbital angular momentum, it is not necessary for quantum states that are orthogonal in Hilbert space to associate to orthogonal vectors in the physical space. Likewise, it is not necessary for quantum states that are nonorthogonal in Hilbert space to associate to nonorthogonal vectors in the physical space. That is the second fact for our scheme's security.

(2) The beam splitter in the quantum participant's laboratory, sends the entangled photon to either the sorter E_i or the sorter F_i at random, where $i \in \{1, 2, \cdots, m\}$. Quantum participants $B_1, B_2, \cdots, B_m$ record the sorter to which the photon goes and the detected OAM value.

(3) Dealer allocates $F^m_n = \sum_{i=1}^m F^m_{n-i}$ to classical participants $C_1,\ C_2,\ \cdots,\ C_\ell$ in the following way. Note that if there is something wrong with quantum channel transmission or the composition of classical participants changes (i.e., a new participant wants to join or an existing participant wishes to leave), then the dealer chooses adaptable m-bonacci numbers to produce new secret shares in terms of the mentioned flow of participants. This is a novel feature of our threshold adaptable secret sharing scheme.

Next the dealer uses the following algorithm to encode the secret:

Algorithm

(1) Choose a prime p, $p > \max(F^m_{n-1}, \ell)$.
(2) Randomly and uniformly generate a number $a_0 \in \mathbb{Z}_p$ and create a polynomial: $f(x) = F^m_{n-1}x^m + F^m_{n-2}x^{m-1} + \cdots + F^m_{n-m}x + a_0 \mod p$, where $a_i \in F^m_n,\ \ a_0 \in \mathbb{Z}_p$.
(3) Sample $f(x)$ at ℓ points such that $A_1 = f(1), A_2 = f(2), \ldots, A_\ell = f(\ell)$. The final ℓ shares are $(i', A_{i'})$, for $1 \le i' \le \ell$.

Finally, the dealer communicates ℓ shares $(i', A_{i'})$ to appropriate classical participants, where $1 \le i' \le \ell$.

Eavesdropping detection phase. During the process of secret share distribution, when there is a mismatch in the entangled state photons, and if the error rate P_e is larger than the preset threshold t between Dealer and participants, they abort this communication and return to the Dealer's phase. Otherwise, the communication continues to obtain a secure key for encrypting the shared secret, until the dealer sends an error notification or stops sending secret shares. The details are given below.

(1) Any $m + 1$ classical participants use their shares $\cup\{(i', A_i')\}$ to reconstruct the polynomial $f(x) = F^m_{n-1}x^m + F^m_{n-2}x^{m-1} + \cdots + F^m_{n-m}x + a_0 \mod p$. Then they can obtain the coefficients of the polynomial, i.e., $F^m_{n-m}, \cdots, F^m_{n-1}$. F^m_n can be computed as $F^m_n = \sum_{i=1}^m F^m_{n-i}$.
(2) Any $\left\lceil \frac{m}{2} \right\rceil$ (when $m > 2$) of $B_1, B_2, \cdots, B_m$ quantum participants can detect eavesdropping, by comparing the detected values with the values recovered by the $m + 1$ classical participants. We take $m = 2$ for example to

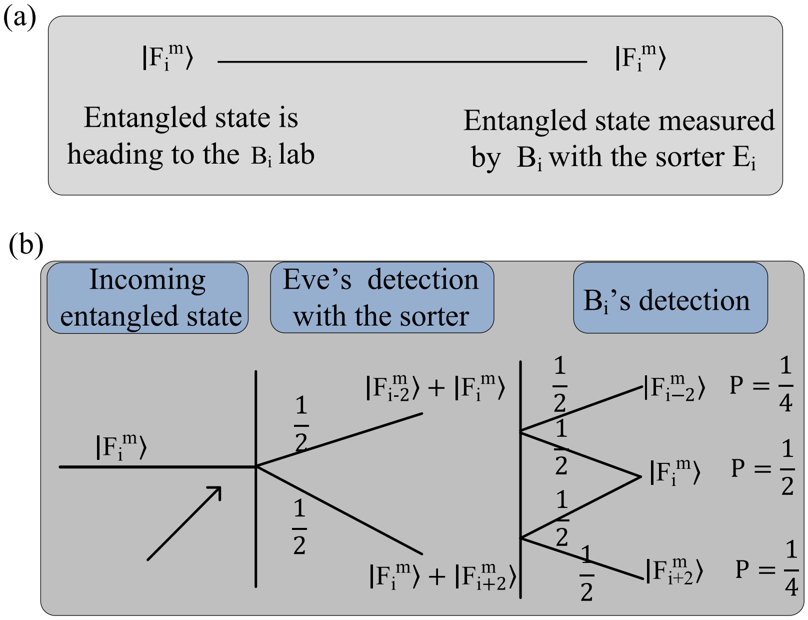

Figure 3. When $m = 2$, the outcome probabilities for eigenstates, where P denotes the probability. (**a**) When the entangled photons goes to the E_i sorter in B_i's laboratory, and Eve also happens to choose the E_i sorter, an incoming eigenstate should be unchanged. (**b**) When Eve chooses the F_i sorter, each eigenstates can turn in two different superposition detections. If one of these superpositions is transmitted to B_i, the net outcomes are now three eigenstates that he could detect.

illustrate how eavesdropping is detected. Suppose that an adversary Eve is eavesdropping on the quantum channel between B_1, B_2. Clearly, she does not know which type of a detection measurement (the sorter E_i or the sorter F_i) took place in B_i's laboratory ($1 \le i \le m$). So, Eve has to guess. If the entangled photon goes to the E_i sorter in Eve's laboratory when going to the F_i sorter in B_i's laboratory, or the entangled photon goes to the F_i sorter in Eve's laboratory when going to the E_i sorter in B_i's laboratory, then the B_i measurement is going to be erroneous with the probability of $\frac{1}{2}$. Eve's activity is going to be detected by B_1, B_2, ⋯, B_m when they compare their scheme transcripts. More precisely, we have the following two cases to consider:

(1) Eve makes an E_i-type measurement on a photon, which is actually in the eigenstate $|F_i^m\rangle$. Then she will detect one of the two $|F_{i-2}^m\rangle + |F_i^m\rangle$ or $|F_i^m\rangle + |F_{i+2}^m\rangle$, with the probability of $\frac{1}{2}$, respectively. She can send a copy of it to B_i. If B_i receives one of these superpositions and makes an F_i-type measurement, she will read out one of the values F_{i-2}^m, F_i^m, or F_{i+2}^m, with the respective probabilities of $\frac{1}{4}$, $\frac{1}{2}$, $\frac{1}{4}$ (see (a) and (b) in Fig. 3). However, she should obtain $|F_i^m\rangle$ with the probability of 1 if there is no eavesdropper.

(2) Eve makes an F_i-type measurement on a photon, which is actually in the superposition state $|F_{i-2}^m\rangle + |F_i^m\rangle$. She will detect one of the two eigenstates F_{i-2}^m, F_i^m, with the probability of $\frac{1}{2}$, respectively. Eve may send a copy of it to B_i. If B_i receives one of these eigenstates and makes an E_i-type measurement, she will obtain one of the superpositions $|F_{i-2}^m\rangle + |F_i^m\rangle$ or $|F_i^m\rangle + |F_{i+2}^m\rangle$ or $|F_{i+2}^m\rangle + |F_{i+4}^m\rangle$, with the respective probabilities of $\frac{1}{4}$, $\frac{1}{2}$, $\frac{1}{4}$ (see (a) and (b) in Fig. 4). However, she should only obtain $|F_{i-2}^m\rangle + |F_i^m\rangle$ with the guaranteed probability of 1 if there is no eavesdropper.

In both cases, if Eve eavesdrops with a fraction η (fraction of times Eve interferes) of the trials, the fraction of times Eve guesses wrong basis is $\frac{1}{2}$, and the fraction of times wrong basis leads to error is $\frac{1}{2}$. So, when quantum participant B_1 compares her results with B_2's, they will find that their outcomes are inconsistent a fraction f of the time, which is

$$\begin{aligned} f &= \eta \times \frac{1}{2} \times \frac{1}{2} \\ &= \frac{\eta}{4} \end{aligned}$$

Note that in our scheme, each entangled photon binds the classical share together. Moreover, not all quantum participants are needed to detect eavesdropping when $m > 2$. This is because we can apply the recovered m-bonacci numbers with classical shares, to verify its consistency with the m-bonacci numbers carried by entangled states. Furthermore, with the detected values from the entangled photons, we can assess the security of the quantum channel (whether it is free from the adversarial activity or not).

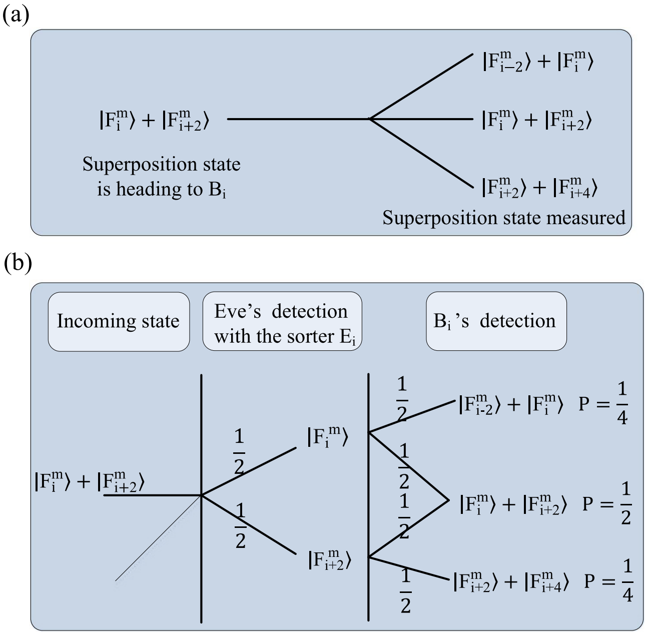
(a)
|F$^m_{i-2}$⟩ + |F^m_i⟩
|F^m_i⟩ + |F$^m_{i+2}$⟩
|F^m_i⟩ + |F$^m_{i+2}$⟩
Superposition state is heading to B$_i$
|F$^m_{i+2}$⟩ + |F$^m_{i+4}$⟩
Superposition state measured
(b)
Incoming state
Eve's detection with the sorter E$_i$
B$_i$'s detection
|F^m_i⟩ + |F$^m_{i+2}$⟩
1/2
1/2
|F$_i^m$⟩
|F$^m_{i+2}$⟩
1/2
|F$^m_{i-2}$⟩ + |F^m_i⟩ P = 1/4
1/2
1/2
|F^m_i⟩ + |F$^m_{i+2}$⟩ P = 1/2
1/2
|F$^m_{i+2}$⟩ + |F$^m_{i+4}$⟩ P = 1/4

Figure 4. When $m = 2$, the outcome probabilities for superposition states where P denotes the probability. (**a**) When the entangled photons goes to the F_i sorter in B_i's laboratory without being eavesdropped, B_i can measure the superposition state correctly, or either of the other two superpositions states. (**b**) When Eve chooses the E_i sorter, she can detect two possible eigenstates with the probability of $\frac{1}{2}$ respectively, which can result in two different superpositions with the probability of $\frac{1}{4}$ besides the original superposition state.

Secret reconstruction phase. If the participants detect eavesdropping and the error rate is higher than the preset threshold value t, they abort the communication and postpone the secret reconstruction phase. Otherwise, any $m + 1$ classical participants can use their classical shares to recover values F^m_{n-m}, ..., F^m_{n-1}, Furthermore, F^m_n can be obtained for encoding each sub-key, which constitutes the key for encrypting the secret. With the key, the $m + 1$ classical participants can recover and further share the secret.

In this scheme, we use quantum coding to generate the key for encrypting messages. Moreover, various m-bonacci sequences can be used to encode the final key. That is, m is changeable for the key, which can address the problems of restricted quantum sources in certain settings and the membership change of participants, such as the joining of a new participant or departure of existing participants. Therefore, our scheme is more practical compared the other quantum secret sharing schemes.

Security Analysis

First, using the technique of Simon *et al.*[31,32,35], we show that our scheme is secure against insider and outsider attacks (Theorems 1 and 2). Later, we analyze the security of the proposed scheme and show that it is immune against a number of attacks including cloning, impersonation, replay and man-in-the-middle attacks.

Theorem 1 (Insiders attacks). Given the hybrid $((t',\ m), (m + 1, \ell))$ threshold QSS, and the set of classical shares available for any $k < m + 1$ insiders (classical participants) is $s_{K_d} = \{s_{k_{i_1}} = f(i_1) | k_{i_1} \in K_d\}$, $(K_d \subseteq \{1, 2, \ldots, n\}, |K_d| = d < m + 1)$, then scheme is asymptotically perfect with respect to the set of probability distributions $P(\cdot)$ on the secret space S. That is, for any $\epsilon > 0$, there exists an integer p_0 such that for any $p > p_0$ with $S = \mathbb{Z}_p$, we have

$$\Delta(s;\ s_{K_d}) = H(s) - H(s|s_{K_d}) \leq \varepsilon \tag{3}$$

where $H(s)$ is the entropy of s, the conditional entropy $H(s|s_{K_d})$ denotes the entropy of s conditioned on s_{K_d}, and $\Delta(s;\ \ s_{K_d})$ denotes the entropy loss of s generated by the knowledge of s_{K_d}.

Proof. It is worth noting that our proposed hybrid $((t',\ m), (m + 1, \ell))$ threshold QSS uses the polynomial $f(x) = F^m_{n-1}x^m + F^m_{n-2}x^{m-1} + \cdots + F^m_{n-m}x + a_0 \mod p$, where $a_i \in F^m_n$, *for* $i = n - m, \ldots, n - 1, a_0 \in F_p$. The sub-secret $s^{i_1} = F^m_{n-1} + F^m_{n-2} + \cdots + F^m_{n-m}$. Assume that there are d $(d = |K_d| < m + 1)$ insiders. $A_{K_d} = \{A_{k_{i_1}} | A_{k_{i_1}} \in \{f(1), f(2), \ldots, f(\ell)\}, k_i \in K_d\}$ with d classical shares $s_{K_d} = \{s_{k_{i_1}} = f(i_1) | k_{i_1} \in K_d\}$, where i_1 is the public information of $A_{k_{i_1}}$, A_{K_d} can conspire to compute

$$f(x) = \sum_{k_{i_1} \in K_d} A_{k_{i_1}} \prod_{k_j \in K_d, k_j \neq k_{i_1}} \frac{x - x_{k_j}}{x_{k_{i_1}} - x_{k_j}} \tag{4}$$

Next, we only need to consider the case of $d = m$, i.e., the upper bound of $P(s|s_{K_d})$, the probability of the secret with the knowledge of s_{K_d}. If the $s^{i'}$ obtained by the recovered Lagrange polynomial is less than p, then we can have $s^{i'_1} \neq s^{i_1}$, so, $P(s|s_{K_d}) = \frac{1}{p-1}$ because the recovered value $s^{i'_1}$ can be removed from the secret space $S = \mathbb{Z}_p$. Note that a_0 is chosen at random in F_p and thus $P(s) = \frac{1}{p}$. So, we have

$$\begin{aligned} \Delta(s;\ s_{K_d}) &= H(s) - H(s|s_{K_d}) \\ &\leq \log p - \log(p-1) \\ &= \log \frac{p}{p-1} \quad p \to +\infty \\ &< \epsilon \end{aligned} \tag{5}$$

That is to say, when $p \to +\infty$, $\Delta(s;\ s_{K_d}) \to 0$. Hence, for any $k < m+1$ classical participants, our proposed hybrid $((t',\ m),\ (m+1, \ell))$ threshold QSS is asymptotically perfect with respect to the set of probability distributions $P(\cdot)$ on the secret space S. □

Theorem 2 (Outsider attacks). Given the hybrid $((t',\ m),\ (m+1, \ell))$ threshold QSS, and the set of the quantum participants' shares is Q with $|Q| = m$, and an outsider has already known any subset $\{Q_k^i,\ k < m\}$ of Q_m^i, then scheme is asymptotically perfect with respect to the set of probability distributions $P(\cdot)$ on the secret space S. That is, for any $\epsilon > 0$, there exists an integer p_0 such that for any $p > p_0$ with $S = \mathbb{Z}_p$, we have

$$\Delta(s;\ Q_k) = H(s) - H(s|Q_k) \leq \epsilon \tag{6}$$

where $H(s)$ is the entropy of s, the conditional entropy $H(s|Q_k)$ denotes the entropy of s conditioned on Q_k, and $\Delta(s; Q_k)$ denotes the entropy loss of s generated by the knowledge of Q_k.

Proof. First, there are $m+1$ $(m > t')$ classical participants $\{C_1, C_2, \cdots, C_{m+1}\}$ and t' quantum participants $\{B_1, B_2, \cdots, B_{t'}\}$. Suppose that an outsider has already known Q_k^i quantum shares and recovered the value $s^{i'_1} = F_{n-1}^{m'} + F_{n-2}^{m'} + \cdots + F_{n-m}^{m'}$. Let us examine the probability of $s^{i'_1} = s^{i_1}$, and $p(s^{i_1}|Q_k^i)$ is the probability of the sub-secret s^{i_1} with the knowledge of $Q_k^{i_1}$. $s^{i'_1} = s^{i_1}$ means $F_{n-1}^{m'} + F_{n-2}^{m'} + \cdots + F_{n-m}^{m'} = F_{n-1}^{m} + F_{n-2}^{m} + \cdots + F_{n-m}^{m}$.

On the one hand, for the party who detects a particular m-bonacci number, there is still an m-fold uncertainty about the m-bonacci number other parties detect in ref. 32. For example, when $F_i^m = F_{i-1}^m + F_{i-2}^m$, if the outsider detects the value F_{i-1}^m, the other party's value can be F_i^m or F_{i-2}^m. Moreover, due to the quantum no-cloning theorem[13], outsiders will be detected when eavesdropping over the quantum channels (see Figs 3 and 4). Therefore, $\{m|(\sum_{i=1}^{m} c_i F_i^m - \sum_{i=1}^{m'} c_i F_i^{m'}),\ m \geq 2\}$ are uniformly distributed. To some degree, this suggests the sub-secret $s^{i'_1}$ and s^{i_1}, even s' and s are actually independent of each other.

On the other hand, the quantum participants' shares are independent of the classical participants' shares. Moreover, the quantum participants' shares are used for eavesdropping detection rather than key generation. Consequently, outsiders cannot use their quantum shares directly as they do in Cleve *et al.*'s QSS[14] to obtain the secret. Therefore, outsiders cannot have a better way to get the secret except to assume $s' = s$.

Second, as we know, the classical shares are allocated in Shamir's SS[1], which are uniformly distributed over $\mathbb{Z}_p$. Given that $s^{i_1} = F_{n-1}^m + F_{n-2}^m + \cdots + F_{n-m}^m$, and $p(s) = \frac{1}{p}$. The probability for outsiders to successfully obtain the values without being detected is $\left(\left\lfloor \frac{p}{F_n^m} \right\rfloor + 1\right) p^{-1}$, where $\left\lfloor \frac{p}{F_n^m} \right\rfloor$ means that the largest integer is less than or equal to $\frac{p}{F_n^m}$. Hence, the entropy loss of the secret satisfies

$$\begin{aligned} \Delta(s;\ Q_k) &= H(s) - H(s|Q_k) \\ &\leq \log F_n^m - \log \frac{p}{\left\lfloor \frac{p}{F_n^m} \right\rfloor + 1} \\ &= \log \frac{F_n^m \times \left(\left\lfloor \frac{p}{F_n^m} \right\rfloor + 1\right)}{p} \\ &< \log \frac{p + F_n^m}{p} \\ &= \log \frac{1 + \frac{F_n^m}{p}}{\frac{F_n^m}{p}} \quad p \to +\infty \\ &< \epsilon \end{aligned} \tag{7}$$

That is to say, when $p \to +\infty$, $\Delta(s; Q_k) \to 0$. Hence, our proposed hybrid $((t',\ m),\ (m+1, \ell))$ threshold QSS is asymptotically perfect with respect to the secret space S. Here, $\log\ F_n^m$ is the abbreviation of $\log_2 F_n^m$. □

Resistance against cloning and impersonation attacks. Our scheme is based on the fact that the nonorthogonal states are indistinguishable, so it is immune against cloning and impersonation attacks. Even if Eve successfully detects the value of an m-bonacci-value-entangled photon, according to the quantum no-cloning theorem, she is unable to clone any other undetected m-bonacci-value-entangled photon.

Let us consider impersonation attacks. A possible strategy Eve can use is to capture the original m-bonacci-value-entangled photon and send a fake m-bonacci-value-entangled photon, say $|F_{n-1}^m\rangle$, to other quantum participants. To be exact, after Dealer sends the state, Eve simply captures the original state and stores it. She then sends one m-bonacci-value-entangled photon from the fake state $|F_{n-1}^m \cdots F_{n-m}^m\rangle$ to other quantum participant B_i. However, due to the particular encoding used in our scheme, the m-bonacci-value-entangled photon varies and the impersonation attack is easy to be detected. For example, if she detects that the value of entangled photon is 2 from $|F_{n-1}^5\rangle$, she sends one 3-bonacci-value-entangled photon as the fake state. Obviously, the impersonation attack does not succeed.

Resistance against replay attacks. Our scheme is immune against replay attacks. A replay attack is such an attack that a valid data transmission is maliciously or fraudulently repeated or delayed. Because we use adaptable m-bonacci sequences for preparing m-bonacci-sequence entangled states, the quantum and classical shares change accordingly. Moreover, due to the use of varying m-bonacci numbers to prepare entangled states, Eve cannot know which m-bonacci sequence is really used every time. For example, suppose that for the fourth subkey, 3-bonacci sequences are used, however, 6-bonacci sequences are used for the fifth subkey. As a result, it is impossible to launch an impersonation attack by inserting the used m-bonacci sequences for the subkey. Therefore, our scheme is immune to replay attacks.

Resistance against man-in-the-middle attacks. A man-in-the-middle attack is an attack, in which Eve intercepts the transmitted entangled photons and replays other entangled photons. We now show that our scheme provides resistance against the man-in-the-middle attacks. First, quantum channels are authenticated; second, for the party who detects a particular m-bonacci number, there is still a m-fold uncertainty about the m-bonacci number other parties detect. Suppose that the eavesdropper Eve, is in possession of an entangled state analyzer for the m-bonacci-value entangled states. If so, she will be able to distinguish $|F_{n-1}^m\rangle, |F_{n-2}^m\rangle, \cdots$, or $|F_{n-m}^m\rangle$ when Dealer sends one of them. However, in the detected sorter, she has a random outcome. Suppose the eavesdropping strategy is to resend the m-bonacci-value entangled state according to the result of her m-bonacci-value entangled state analysis. In order to detect the eavesdropper, we should consider what happens if, for instance, the state $|F_{n-1}^m\rangle$ is sent by Dealer. In one $\frac{1}{2^{m-1}}$th of the cases Eve chooses the right sorter, and resends the m-bonacci-value entangled state perfectly. In the remaining $1 - \frac{1}{2^{m-1}}$ of the cases Eve chooses the wrong sorter and sends the superposition state $|F_{n-2}^m\rangle + |F_{n-3}^m\rangle + \cdots + |F_n^m\rangle$. These states will be correctly detected by $B_1, B_2, \cdots B_m$ together with any $m+1$ classical participants. By adding all the probability of causing an error becomes $\frac{1}{2^{m-1}}\left(\frac{1}{2^{m-1}} \times \frac{1}{m} + \frac{2^{m-1}-1}{2^{m-1}} \times \frac{1}{m}\right) = \frac{1}{m \times 2^{m-1}}$, which is the same as two-state cryptography. In a manner similar to the two-state cryptography, it is also possible to launch a more complex eavesdropping attack using an ancilla, or measuring in an intermediate basis compared to the {0, 1} bases. However, the eavesdropper is still detectable, and the fundamental security remains. Hence, our scheme provides resistance against the man-in-the-middle attacks.

Discussion

Simon *et al.*[31] used positive and negative OAM pumps to improve information capacity which can only be doubled, and their scheme needs a joint quantum operation. Moreover, with 2-bonacci values used alone, to multiple the information capacity, larger 2-bonacci values should be used, and the available bandwidth becomes more of a challenge. Also, they argued that though lower error rates can be achieved by the use of higher-2-bonacci values (Fibonacci numbers), the transmission distances are shorter. While the longer distances can be achieved by the use of lower-2-bonacci values, the error rates are higher. When only 2-bonacci values are used, it is hard to satisfy the requirements of lower error rates and longer transmission distances. Based on these mentioned problems, we incorporate m-bonacci sequences into both quantum and classical coding, with reverse Huffman-Fibonacci-tree coding, to achieve higher-capacity and lower-bandwidth hybrid threshold adaptable QSS scheme.

The information capacity. Given the above conclusion, proper m-bonacci values can be chosen to achieve the lower error rates and longer distances. Hence, we propose to use Huffman coding tree to encode m-bonacci numbers with the greedy algorithm, which can greatly improve the coding capacity, thus reducing the use of entangled photons. To be exact, for fixed m-bonacci number sets, we use binary representations of m-bonacci numbers based on Fibonacci numbers of order $m \geq 2$ (see Equation (11)). Hence, this paper extends Simon *et al.*'s quantum key distribution protocol presenting a novel feature, where Fibonacci numbers 1, 2, 3, 5, 8, 13, 31, 34 are used. According to the method of reverse Huffman-Fibonacci-tree coding in Eqs (11) and (12) of the following section, each m-bonacci number can then represent a binary string as follows:

$$\begin{aligned} c = c_1 \cdot 0 || c_2 \cdot (10) || c_3 \cdot (110) || c_4 \cdot (1110) || c_5 \cdot (11110) \\ || c_6 \cdot (111110) || c_7 \cdot (1111110) || c_8 \cdot (1111111) \end{aligned} \tag{8}$$

Schemes	Ref. 1	Ref. 14	Ref. 24	Ref. 26	Our scheme
Adaptable threshold	No	No	No	No	Yes
Flexible threshold	Yes	No	No	No	Yes
Robustness	High	Low	Low	Low	High
Detect eavesdropping	No	Yes	Yes	Yes	Yes
The information capacity		1bit	1bit	1bit	$(\sum_{i=1}^{7} ic_i + 7c_8)$ bits
Classical communication overhead	$\ell\|P\|$ bits	0bit	$(2m - \ell - 1)\frac{\|P\|}{\ell}$ bits	0bit	$\frac{\ell\|p\|\|P\|}{10\ell}$ bits
Quantum communication overhead	0	$\ell\|P\|$ qubits	$(2\ell - 2m + 1)\frac{\|P\|}{\ell}$ qubits	$\ell\|P\|$ qubits	$\frac{m\,\|\,P\|}{10\ell}$ qubits
Hybrid quantum secret sharing	No	No	Yes	Yes	Yes

Table 2. Performance comparison of HQSS with previous QSSs. m is the threshold value, and ℓ denotes ℓ classical or quantum participants, P and p ($P \gg p$) are primes which are used in ref. 1 and our scheme, and $|P|$ and $|p|$ denote the bit number of P and p.

where $c_{i^*} \in \{0, 1\}$, $i^* \in \{1, 2, \ldots, 8\}$, and $c_{i^*} \cdot (\underbrace{11\cdots1}_{i^*-1}0)$ denotes when $i^* = 1$, the corresponding codes are $\underbrace{11\cdots1}_{i^*-1}0$; when $i^* = 0$, there are no corresponding codes.

Therefore, the information capacity of each m-bonacci number is

$$I_c = \sum_{i=1}^{7} ic_i + 7c_8 \tag{9}$$

Take $4=3+1, 7=5+2, 15=13+2, 16=13+3, 24=21+3, 29=21+8, 31=21+8+2, 32=21+8+3$ for example (as shown in Table 1, according to Equations (11) and (12), their binary Fibonacci representations would be as follows:

$$\begin{aligned} &4 = 3 + 1{:}1111101111111, && 7 = 5 + 2{:}111101111110,\\ &15 = 13 + 2{:}1101111110, && 16 = 13 + 3{:}110111110,\\ &24 = 21 + 3{:}10111110, && 29 = 21 + 8{:}101110,\\ &31 = 21 + 8 + 2{:}1011101111110, && 32 = 21 + 8 + 3{:}101110111110. \end{aligned} \tag{10}$$

It can be seen from Equation (10), compared with the high-capacity coding in terms with Simon *et al.*'s protocol, in which they double the information capacity per photon, we multiply the information capacity. In the above example, the average bits per photon is 10.375. If the size of the key is 360,000, we need to prepare about 36,000 rather than 90,000 entangled states, making our scheme more practical. This is because it is difficult and costly to prepare entangled states.

Besides the information capacity, Table 2 compares the features of our proposed scheme with those of the secret sharing schemes in refs 1, 14, 24 and 26. The comparison suggests that our secret sharing scheme is more suitable for real-world applications. Distinct from the well-known Shamir's classical secret sharing scheme[1] against secret leakage, our proposed scheme can both detect eavesdropping and protect the secret from leaking. Meanwhile, compared with QSS schemes[14,24,26], our scheme can achieve the adaptability and flexibility based on the following two facts: 1) the various m-bonacci values are used to adapt to participant mobility; 2) the m-bonacci values are encoded in Lagrange polynominal, and as a result, any t' quantum participants and any $m+1$ classical participants can recover the secret. Due to the no-cloning theorem and its impact on parameters, for QSS schemes[14,24,26,31], the parameters ℓ and t' must satisfy the requirement of $\ell < 2t' - 1$, and once t' quantum participants are fixed, other quantum participants are unable to participate in the recovery of the secret. However, in our scheme, the parameters ℓ and t' can be arbitrary, and our scheme is robust when a new participant joins or an existing participant leaves.

Unlike eavesdropping detection in QSS schemes[14,24,26], due to entangled states prepared by m-bonacci sequences, the detection is possible by any subset that contains at least $\left\lceil \frac{m}{2} \right\rceil$ participants. That is to say, none of the number of threshold value quantum participants are required to reach a consensus in order to reveal eavesdropping. Because the method of the Huffman-Fibonacci coding is employed in our scheme, the classical bits denoted by every m-bonacci number are significantly improved, from four bits at most to more than ten bits using a similar experimental setup. Consequently, our scheme can greatly improve the coding capacity, thus reducing the use of entangled photons which are expensive and difficult to prepare. Moreover, to generate the secret, the m-bonacci sequences encoded in Lagrange interpolation polynomials and the Huffman-Fibonacci coding are applied. So, compared with the CSS in ref. 1 where the size of secret shares is the same as that of the secret itself, our scheme allows the former to be of much smaller than the secret itself. To be exact, the smaller m-bonacci sequences such as $m = 2, 3, 4, 5, 6$ can be used in our proposed scheme, the pump values in Fig. 1 is smaller and the size of classical shares is much smaller since the size of the prime is much smaller than that used in ref. 1. In addition, we generate secret shares for blocks generation, thus significantly reducing the bandwidth compared with ref. 1.

For the communication overhead, there are m quantum and ℓ classical participants. Let P and p ($P \gg p$) be primes, then the communication overhead in ref. 1 is $n|P|$ bits, where $|P|$ and $|p|$ denote the bit number of P and p. It can be known that the size of the key is $|P|$, so, $|P|$ photons are prepared. In ref. 14, only quantum channel is used, so, the communication overhead is $n|P|$ qubits. The ref. 24 proposes a hybrid quantum secret sharing, in

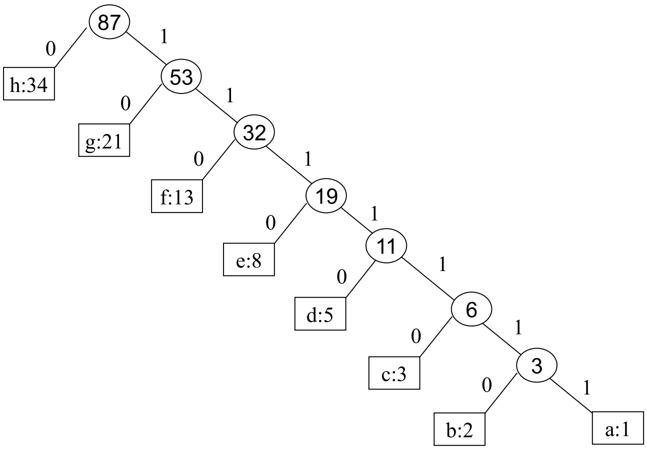

Figure 5. The Huffman-Fibonacci coding tree for the eight Fibonacci numbers (as symbol frequencies) from 1 to 34.

which both quantum and classical channel are used. There are $(2\ell - 2m + 1)$ quantum participants and $(2m - \ell - 1)$ classical participants. Therefore, the quantum communication overhead for the scheme in ref. 26 is $\frac{(2\ell - 2m + 1)|P|}{n}$ qubits, and the classical communication overhead is $\frac{(2m - \ell - 1)|P|}{\ell}$ bits. In our scheme, the quantum communication overhead is at most $\frac{m\,|\,P|}{10\ell}$ qubits, and the classical communication overhead is $\frac{\ell\,|\,p\,||\,P|}{10\ell}$ bits.

In conclusion, we combine the Huffman-Fibonacci quantum coding with Lagrange polynomials to achieve threshold adaptable QSS. The key point of our scheme is that it does not suffer from the restriction derived from the quantum no-cloning theorem, because it permits secret sharing for arbitrary values of parameters ℓ and $m+1$ provided that $\ell \geq m + 1$. We use the Huffman coding tree to encode the obtained m-bonacci numbers, aiming at improving the coding capacity greatly, and thus incurring a low communication overhead. When compared to the existing QSS schemes, there is an improvement in sharing the secret without joint quantum operations. Meanwhile, our scheme still works when there are dynamic changes in comparison with existing quantum secret sharing, such as the unavailability of some quantum channel, the arrival of new participants and the departure of participants.

Methods

Huffman-Fibonacci coding. Fraenkel and Klein[29] showed that any integer including an m-bonacci number can be represented by a binary string of length r, c_r, c_{r-1}, …, c_2, c_1 such that

$$F_n^m = \sum_{i=1}^{r} c_i F_{r-i}^2. \tag{11}$$

When one uses the following procedure to produce it, the Equation (11) will be unique. Given the integer F_n^m, find the largest Fibonacci number F_r^2 smaller or equal to F_n^m; then continue recursively with $F_n^m \sim F_r^2$. Therefore, for coding, we explore the properties of Fibonacci representations for variable-length encoding, especially the trade-off between their robustness and their scalability efficiency. To be exact, we use the Huffman coding in ref. 36 and the greedy algorithm in ref. 37 to improve the coding capacity of the detected m-bonacci values.

$m+1$ classical participants encode the reconstructed m-bonacci value based on the fact that the higher the frequency at which Fibonacci numbers appear in m-bonacci values, the longer the set of binary codes, which is opposite to the idea of Huffman coding. Let the binary codes of $F_r^2,\ F_{r-1}^2,\ \cdots,\ F_1^2$ be $C_r^2,\ C_{r-1}^2,\ \cdots,\ C_1^2$ respectively. So, the binary codes of F_n^m are represented by the concatenation of $C_r^2||C_{r-1}^2||\cdots||C_1^2$. For example, if the frequencies from 1 to 34 which appear in m-bonacci values decrease, the coding is as follows (see Fig. 5);

$$\begin{aligned} &F_1^2 = 1{:}1111111, F_2^2 = 2{:}1111110, F_3^2 = 3{:}111110, F_4^2 = 5{:}11110,\\ &F_5^2 = 8{:}1110, F_6^2 = 13{:}110, F_7^2 = 21{:}10, F_8^2 = 34{:}0. \end{aligned} \tag{12}$$

So, the available reconstructed F_{n-m}^m is used in terms of Eqs (9) and (12), and a sub-key can be obtained. The key can be obtained by concatenating all the sub-keys generated in the same way.

$$\begin{aligned} &F_{n-8}^m = \sum_{i^*=1}^{r} c_{i^*}^1 F_{r-i^*}^2,\ F_{n-7}^m = \sum_{i^*=1}^{r} c_{i^*}^2 F_{r-i^*}^2,\ F_{n-6}^m = \sum_{i^*=1}^{r} c_{i^*}^3 F_{r-i^*}^2,\ F_{n-5}^m = \sum_{i^*=1}^{r} c_{i^*}^4 F_{r-i^*}^2,\\ &F_{n-4}^m = \sum_{i^*=1}^{r} c_{i^*}^5 F_{r-i^*}^2,\ F_{n-3}^m = \sum_{i^*=1}^{r} c_{i^*}^6 F_{r-i^*}^2,\ F_{n-2}^m = \sum_{i^*=1}^{r} c_{i^*}^7 F_{r-i^*}^2,\ \ F_{n-1}^m = \sum_{i^*=1}^{r} c_{i^*}^8 F_{r-i^*}^2, \end{aligned} \tag{13}$$

where $c_{i^*}^1,\ c_{i^*}^2,\ \ldots,\ c_{i^*}^7,\ c_{i^*}^8 \in \{0,\ 1\}$.

For example, if the final detected values of available entangled states are $F_7^3 = 44 = 34 + 8 + 2$, $F_6^4 = 29 = 21 + 8, \cdots$, their corresponding coding is 011101111110, 101110, ··· in terms of Eq. (12). The key can be established with $\underbrace{011101111110\|101110\|\cdots}$ concatenated for secret sharing. In other words, any $m+1$ classical participants can share the secret encrypted by the key using the one-time-pad encryption.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **22,** 612–613 (1979).
2. Blakeley, G. R. Safeguarding cryptographic keys. In: *Proc. AFIPS*, 313–317 (Arlington VA, USA, 1979).
3. Chor, B., Goldwasser, S., Micali, S. & Awerbuch, B. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Proc. 26th Annu. IEEE Symp. Found. Comput. Sci.* 383–395 (Portland, USA, 1985).
4. Feldman, P. A practical scheme for non-interactive verifiable secret sharing. In *Proc. 28th Annu. Symp. Found. Comput. Sci.* 427–438 (1987).
5. Pedersen, T. P. Non-interactive and information-theoretic secure verifiable secret sharing. In: *CRYPTO'92*, **576,** 129–140 (1992).
6. Iftene, S. Secret sharing schemes with applications in security protocols. *Technical report, University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science* (2007).
7. Miao, F. Y., Xiong, Y., Wang, X. F. & Moaman, B. Randomized component and its application to (t, m. n)-group oriented secret sharing. *IEEE Trans. Inf. Forensics Security* **10,** 889–898 (2015).
8. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59,** 1829–1834 (1999).
9. Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing*, 175–179 (Bangalore, 1984).
10. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
11. Li, Q., Chan, W.-H. & Zhang, S.-Y. Semiquantum key distribution with secure delegated quantum computation. *Sci. Rep.* **6,** 19898 (2016).
12. Sheng, Y.-B. & Zhou, L. Deterministic entanglement distillation for secure double-server blind quantum computation. *Sci. Rep.* **5,** 7815 (2015).
13. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299,** 802–803 (1982).
14. Cleve, R., Gottesman, D. & Lo, H.-K. How to share a quantunm secret. *Phys. Rev. Lett.* **83,** 648–652 (1999).
15. Karlsson, A., Koashi, M. & Imoto, N. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **59,** 162–168 (1999).
16. Tittel, W., Zbinden, H. & Gisin, N. Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **63,** 042301–042306 (2001).
17. Gottesman, D. Theory of quantum secret sharing. *Phys. Rev. A* **61,** 042311 (2000).
18. Xiao, L., Long, G.-L., Deng, F.-G. & Pan, J.-W. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **69,** 052307 (2004).
19. Karimipour, V. & Asoudeh, M. Quantum secret sharing and random hopping: Using single states instead of entanglement. *Phys. Rev. A* **92,** 030301 (2015).
20. Wei, K.-J., Ma, H.-Q. & Yang, J.-H. Experimental circular quantum secret sharing over telecom fiber network. *Opt. Express* **21,** 16664–16669 (2013).
21. Deng, F.-G., Zhou, H.-Y. & Long, G.-L. Circular quantum secret sharing. *J. Phys. A: Math Gen.* **39,** 14089–14099 (2006).
22. Yang, Y.-H. *et al.* Quantum secret sharing via local operations and classical communication. *Sci. Rep.* **5,** 16967 (2015).
23. Żukowski, M., Zeilinger, A., Horne, M. A. & Weinfurter, H. Quest for GHZ states. *Acta Phys. Pol. A* **93,** 187 (1998).
24. Fortescue, B. & Gour, G. Reducing the quantum communication cost of quantum secret sharing. *IEEE Trans. Inf. Theory* **58,** 6659–6666 (2012).
25. Tompa, M. & Woll, H. How to share a secret with cheaters. *J. Cryptol.* **1,** 133–138 (1988).
26. Rahaman, R. & Parker, M. G. Quantum scheme for secret sharing based on local distinguishability. *Phys. Rev. A* **91,** 022330 (2015).
27. Lau, H.-K. & Weedbrook, C. Quantum secret sharing with continuous-variable cluster states. *Phys. Rev. A* **88,** 04231 (2013).
28. Kilic, E. & Tasci, D. On the Generalized Order-*k* Fibonacci and Lucas Numbers. *Rocky Mountain J. Math.* **36,** 1915–1926 (2006).
29. Fraenkel, A. S. & Klein, S. T. Robust universal complete codes for transmission and compression. *Discrete. Appl. Math.* **64,** 31–55 (1996).
30. Hilton, P. & Pedersen, J. Fibonacci and Lucas Numbers in Teaching and Research. *J. Math. Informatique* **3,** 36–57 (1991–1992).
31. Simon, D. S. *et al.* High-capacity quantum Fibonacci coding for key distribution. *Phys. Rev. A* **87,** 032312 (2013).
32. Simon, D. S., Fitzpatrick, C. A. & Sergienko, A. V. Discrimination and synthesis of recursive quantum states in high-dimensional Hilbert spaces. *Phys. Rev. A* **91,** 043806 (2015).
33. Lavery, M. P. J., Robertson, D. J., Berkhout, G. C. G., Love, G. D., Padgett, M. J. & Courtial, J. Refractive elements for the measurement of the orbital angular momentum of a single photon. *Opt. Express* **20,** 2110–2115 (2012).
34. Horodecki, M., Sen, A., Sen, U. & Horodecki, K. Local indistinguishability: More nonlocality with less entanglement. *Phys. Rev. Lett.* **4,** 047902 (2003).
35. Simon, D. S., Fitzpatrick, C. A. & Sergienko, A. V. Security in the multi-dimensional Fibonacci protocol. *arXiv*:1503.04448. (2015).
36. Huffman, D. A method for the construction of minimum redundancy codes. *Proc. IRE* **40,** 1098–1101 (1952).
37. Edmonds, J. Matroids and the greedy algorithm. *Math. Programming* **1,** 126–136 (1971).

Acknowledgements

Hong Lai has been supported by the Fundamental Research Funds for the Central Universities (No. XDJK2016C043) and the Doctoral Program of Higher Education (No. SWU115091). Jun Zhang is supported by the National Natural Science Foundation of China (No. 61401371). Mingxing Luo is supported by the National Natural Science Foundation of China (No. 61303039). Josef Pieprzyk has been supported by National Science Centre, Poland, project registration number UMO-2014/15/B/ST6/05130. Fuyuan Xiao is supported by the Fundamental Research Funds for the Central Universities (No. XDJK2015C107) and the Doctoral Program of Higher Education (No. SWU115008). The paper is also supported by the financial support by the 1000-Plan of Chongqing by Southwest University (No. SWU116007).

Author Contributions

H.L. proposed the theoretical method. H.L., J.Z., L.P., J.P. and M.-X.L. wrote the manuscript text. M.A.O. and F.X. reviewed the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Lai, H. *et al.* Hybrid threshold adaptable quantum secret sharing scheme with reverse Huffman-Fibonacci tree coding. *Sci. Rep.* **6**, 31350; doi: 10.1038/srep31350 (2016).