SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2017, Vol. 60 082501:1–082501:14
doi: 10.1007/s11432-016-9061-4

An efficient quantum blind digital signature scheme

Hong LAI[1*], Mingxing LUO[2], Josef PIEPRZYK[3,4], Zhiguo QU[5], Shudong LI[6,7] & Mehmet A. ORGUN[8,9*]

[1]*College of Computer and Information Science, Southwest University, Chongqing* 400715*, China;*
[2]*Information Security and National Computing Grid Laboratory, School of Information Science and Technology, Southwest Jiaotong University, Chengdu* 610031*, China;*
[3]*School of Electrical Engineering and Computer Science, Queensland University of Technology, Brisbane* QLD 4000*, Australia;*
[4]*Institute of Computer Science, Polish Academy of Sciences, Warsaw* 01-248*, Poland;*
[5]*School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing* 210044*, China;*
[6]*College of Mathematics and Information Science, Shandong Technology and Business University, Yantai* 264005*, China;*
[7]*School of Computer Science, National University of Defense Technology, Changsha* 410073*, China;*
[8]*Department of Computing, Macquarie University, Sydney* NSW 2109*, Australia;*
[9]*Faculty of Information Technology, Macau University of Science and Technology, Avenida Wai Long, Macau* 519020*, China*

Received January 18, 2017; accepted March 9, 2017; published online July 10, 2017

Abstract Recently, many quantum digital signature (QDS) schemes have been proposed to authenticate the integration of a message. However, these quantum signature schemes just consider the situation for bit messages, and the signing-verifying of one-bit modality. So, their signature efficiency is very low. In this paper, we propose a scheme based on an application of Fibonacci-, Lucas- and Fibonacci-Lucas matrix coding to quantum digital signatures based on a recently proposed quantum key distribution (QKD) system. Our scheme can sign a large number of digital messages every time. Moreover, these special matrices provide a method to verify the integration of information received by the participants, to authenticate the identity of the participants, and to improve the efficiency for signing-verifying. Therefore, our signature scheme is more practical than the existing schemes.

Keywords blind quantum digital signature, Fibonacci-, Lucas- and Fibonacci-Lucas matrix coding, digital messages, signing-verifying modality

Citation Lai H, Luo M X, Pieprzyk J, et al. An efficient quantum blind digital signature scheme. Sci China Inf Sci, 2017, 60(8): 082501, doi: 10.1007/s11432-016-9061-4

1 Introduction

Digital signatures have been invented to play the same role as hand-written signatures [1]. The main difference between the two is the environment in which they function. For hand-written signatures, a piece of paper binds the text of a document and a signature. In the computer environment, a digital

* Corresponding author (email: hlai@swu.edu.cn, mehmet.orgun@mq.edu.au)

signature needs to bind both the text of a document and the identity of a signer in such a way that forging the signature is "impossible". The identity of a signer is a secret key, which is used in the signing algorithm. A matching public key is used to verify digital signatures. To avoid trivial attacks, public verification keys need to be certified by a public-key infrastructure (PKI). Digital signatures are designed using (believed) intractable mathematical problems such as integer factorisation (used in RSA signatures [2, 3]) or discrete logarithm (applied in ElGamal signatures [4]). Unfortunately, both integer factorisation and discrete logarithm problems are "easy" on quantum computers [5]. Consequently, both RSA and ElGamal signatures can be forged at will by quantum algorithms. A growing importance of digital signatures and their wide-spread applications are the main drivers towards the development of quantum signatures, which are efficient and whose security is guaranteed by the laws of physics rather than computational assumptions. In recent years, a few quantum digital signature (QDS) solutions have been proposed [6–17].

The first QDS algorithm has been proposed by Gottesman and Chuang [7]. They used a quantum one-way function to build their signature. A weakness of their signature is that it needs a long-term quantum memory. In the followup research, many authors [10, 12–14] have improved the Gottesman and Chuang (GC) QDS algorithm. However, their solutions have been developed under an (unrealistic) assumption that the communication channels are authenticated (in other words, they assume that quantum channels cannot be eavesdropped). Amiri et al. [18] have designed a QDS algorithm with no specific trust assumptions on quantum channels. Yin et al. [19] have proposed to use a single-photon qubit state and phase-randomized weak coherent states to remove the assumptions about secure quantum channels. Recently, Donaldson et al. [20] have implemented a quantum digital signature that allows to communicate signatures up to a kilometre range using a standard quantum key distribution link.

A digital signature scheme is said to be secure if it is unforgeable, nonrepudiable and non-transferable [6]. Unforgeability indicates the fact that an adversary cannot create a valid signature for any message. Nonrepudiation means that the signer of a message cannot deny the action of signing the message after the fact. Transferability requires any receiver of a valid signature to be able to verify its validity using public information only and without any interaction with the signer. There are two main differences between classical and quantum signatures: (1) quantum signatures can be verified once only, while classical signatures can be verified an arbitrary number of times, and (2) the verification of quantum signatures requires a one-time verification public key. Note that classical signatures are verified by a single public key that can be fetched as an appropriate certificate from a PKI.

The signatures schemes developed so far allow to sign a single-bit message and the signer has to know the message. In many applications (such as electronic elections and notary systems), messages have to be signed blindly (or without knowing the content of messages). In this paper, we propose an efficient algorithm for quantum digital signatures without the need for quantum memory. The building blocks we use are the Simon et al. quantum key distribution (QKD) protocol and the Fibonacci coding [21, 22]. The Fibonacci coding is applied to convert the QKD protocol into our QDS protocol. As a research result of an independent interest, we generalise the Fibonacci binary coding to Fibonacci (or Fibonacci-Lucas/Lucas) matrix coding. The generalisation enables our QDS to detect and correct transmission errors, which may occur with a high rate.

The remainder of this paper is organised as follows. In Section 2, three kinds of coding matrices (Fibonacci, Lucas and Fibonacci-Lucas) are defined and their properties are studied. Next we introduce Simon's et al. QKD protocol and an improved version of it in Section 3. Section 4 is the main part of the work and presents our QDS protocol. Security and efficiency analysis are given in Section 5. Section 6 concludes the work with a brief summary of our contributions.

2 Quantum coding matrices

In this section, we define three classes of coding matrices, i.e., Fibonacci Q_p^n-matrix, Lucas R_p^n-matrix, and Fibonacci-Lucas T_p^n-matrix and investigate their properties.

2.1 Fibonacci matrices

Fibonacci numbers F_n [23] are an infinite sequence of integers defined by the following recursion:

$$F_n = F_{n-1} + F_{n-2}, n \geqslant 2, \tag{1}$$

where the first two elements of the sequence are $F_0 = 0$ and $F_1 = 1$. Taking the first three integers F_0, F_1, F_2 of the Fibonacci sequence, we can construct a 2×2 Fibonacci matrix:

$$Q_1 = \begin{pmatrix} F_0 & F_1 \\ F_1 & F_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \tag{2}$$

where $\det(Q_1) = F_0F_2 - F_1^2 = -1$. Using recursion (1), we can compute the nth power of the Fibonacci matrix Q_1 as follows:

$$Q_1^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}. \tag{3}$$

Since $\det(A^n) = (\det(A))^n$, we have $\det(Q_1^n) = (\det(Q_1))^n = (-1)^n$. This means that Fibonacci matrices Q_1^n are invertible and their inverse matrices are given as

$$Q_1^{-2k} = \begin{pmatrix} F_{2k+1} & -F_{2k} \\ -F_{2k} & F_{2k-1} \end{pmatrix}, \quad \text{for } n = 2k, \tag{4}$$

$$Q_1^{-(2k+1)} = \begin{pmatrix} -F_{2k+2} & F_{2k+1} \\ F_{2k+1} & -F_{2k} \end{pmatrix}, \quad \text{for } n = 2k+1. \tag{5}$$

Construction of Q_p. We define a new class of Fibonacci matrices Q_p, where $p = 2, 3, \ldots$ and Q_1 is given by (2). The class satisfies the following relation:

$$Q_p = \begin{pmatrix} Q_1 & Q_1 & \cdots & Q_1 & Q_1 \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{I} & \ddots & \mathbf{O} \\ \vdots & \vdots & \ddots & \ddots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I} \end{pmatrix},$$

where the 2×2 matrix $\mathbf{O}$ contains zero entries only and the 2×2 matrix $\mathbf{I}$ is an identity matrix. It is easy to prove that matrices Q_p^n satisfy the following properties in terms of (3):

$$\det(Q_p^n) = (\det(Q_p))^n = (-1)^{pn}. \tag{6}$$

Note that according to (6), Q_p^n (where $p = 1, 2, 3, \ldots$) is invertible and its inverse can be calculated using (4) and (5), which are as follows:

$$Q_p^{-n} = \begin{pmatrix} Q_1^{-n} & -I & \cdots & -I & -I \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{I} & \ddots & \mathbf{O} \\ \vdots & \vdots & \ddots & \ddots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I} \end{pmatrix}.$$

2.2 Lucas matrices

Lucas numbers L_n [24] are an infinite sequence of integers, defined by the following recursion holds

$$L_n = L_{n-1} + L_{n-2}, n \geqslant 2, \tag{7}$$

where the integers $L_0 = 2$ and $L_1 = 1$ start the sequences and $n = 1, 2, \ldots$. Lucas and Fibonacci numbers share the following conjugate relation [24]:

$$L_n = F_{n+1} + F_{n-1}. \tag{8}$$

Let us define a 2×2 matrix R_1 as

$$R_1 = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}. \tag{9}$$

According to (1) and (3), we can define the nth power of R_1 as

$$R_1^n = \begin{pmatrix} L_{n-1} & L_n \\ L_n & L_{n+1} \end{pmatrix} = Q_1^n \times \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}, \tag{10}$$

$$\det(R_1^n) = \det\left(Q_1^n \times \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}\right) = 5 \times (-1)^{n+1}. \tag{11}$$

The above relations imply that R_1^n is invertible and its inverse matrix R_1^{-n} can also be derived using the properties of Lucas sequences. They are

$$R_1^{-2k} = \begin{pmatrix} \dfrac{L_{2k+1}}{5} & -\dfrac{L_{2k}}{5} \\ -\dfrac{L_{2k}}{5} & \dfrac{L_{2k-1}}{5} \end{pmatrix}, \quad \text{for } n = 2k, \tag{12}$$

$$R_1^{-(2k+1)} = \begin{pmatrix} -\dfrac{L_{2k+2}}{5} & \dfrac{L_{2k+1}}{5} \\ \dfrac{L_{2k+1}}{5} & -\dfrac{L_{2k}}{5} \end{pmatrix}, \quad \text{for } n = 2k+1. \tag{13}$$

Construction of R_p. We use matrix R_1 to build a new class of Lucas matrices R_p that satisfy the following relation:

$$R_p = \begin{pmatrix} R_1 & R_1 & \cdots & R_1 & R_1 \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{I} & \ddots & \mathbf{O} \\ \vdots & \vdots & \ddots & \ddots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I} \end{pmatrix},$$

where the 2×2 matrix $\mathbf{O}$ contains zero entries only and the 2×2 matrix $\mathbf{I}$ is an identity matrix. It is easy to prove that matrices R_p^n satisfy the following properties:

$$\det(R_p^n) = (\det R_p)^n = (-1)^{p(n+1)} 5^p. \tag{14}$$

Note that according to (14) R_p^n are invertible and their inverses can be calculated using (12) and (13), where $p = 1, 2, 3, \ldots$. Their inverses are as follows:

Table 1 Terms of Fibonacci and Lucas sequences

n	1	2	3	4	5	6	7	8	9	10
F_n	1	1	2	3	5	8	13	21	34	55
L_n	1	3	4	7	11	18	29	47	76	123

$$R_p^{-n} = \begin{pmatrix} R_1^{-n} & -I & \cdots & -I & -I \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{I} & \ddots & \mathbf{O} \\ \vdots & \vdots & \ddots & \ddots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I} \end{pmatrix}.$$

2.3 Fibonacci-Lucas matrices

Fibonacci and Lucas sequences can be used jointly (see [25]) to create a new class of matrices, which we call them Fibonacci-Lucas matrices. They are consecutive powers of T_1 and are defined according to the following recursion:

$$T_1^n = \begin{pmatrix} F_{n-1} & F_n \\ L_{n-2} & L_{n-1} \end{pmatrix}, \tag{15}$$

where the first Fibonacci-Lucas matrix T_1 is

$$T_1 = \begin{pmatrix} F_1 & F_2 \\ L_0 & L_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}. \tag{16}$$

As shown in Table 1, Lucas and Fibonacci numbers satisfy the relation $L_{n-1} = F_n + F_{n-2}$, thus T_1^n can be written as

$$T_1^n = \begin{pmatrix} F_{n-1} & F_n \\ F_{n-1} + F_{n-3} & F_n + F_{n-2} \end{pmatrix}. \tag{17}$$

We can now calculate the determinant of Fibonacci-Lucas matrices. The following transformations are self-explanatory:

$$\begin{aligned} \det(T_1^n) &= \det \begin{pmatrix} F_{n-1} & F_n \\ F_{n-1} + F_{n-3} & F_n + F_{n-2} \end{pmatrix} = \det \begin{pmatrix} F_{n-1} & F_n \\ F_{n-1} & F_n \end{pmatrix} + \det \begin{pmatrix} F_{n-1} & F_n \\ F_{n-3} & F_{n-2} \end{pmatrix} \\ &= \det \begin{pmatrix} F_{n-1} & F_n \\ F_{n-3} & F_{n-2} \end{pmatrix} = (-1) \det \begin{pmatrix} F_{n-3} & F_{n-2} \\ F_{n-1} & F_n \end{pmatrix}. \end{aligned} \tag{18}$$

We use the properties of Fibonacci matrices from Subsection 2.1 and arrive at the following result:

$$\det(T_1^n) = (-1)^{n-3}, \quad n = 4, 5, \ldots. \tag{19}$$

The inverse matrix T_1^{-n} is

$$T_1^{-2k} = \begin{pmatrix} L_{2k+1} & -F_{2k} \\ -L_{2k} & F_{2k} \end{pmatrix} \text{ for } n \text{ even}, \tag{20}$$

$$T_1^{-(2k+1)} = \begin{pmatrix} -L_{2k+1} & F_{2k} \\ L_{2k} & -F_{2k} \end{pmatrix} \text{ for } n \text{ odd}. \tag{21}$$

The matrix T_1^n can be used to produce matrices of higher dimensions $T_2^n, T_3^n, \ldots, T_p^n$.

Construction of T_p. We use matrix T_1 to build a new class of Fibonacci-Lucas matrices T_p that satisfy the following relation:

$$T_p = \begin{pmatrix} T_1 & T_1 & \cdots & T_1 & T_1 \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{I} & \ddots & \mathbf{O} \\ \vdots & \vdots & \ddots & \ddots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I} \end{pmatrix},$$

where the 2×2 matrix $\mathbf{O}$ contains zero entries only and the 2×2 matrix $\mathbf{I}$ is an identity matrix. It is easy to prove that matrices R_p^n satisfy the following properties:

$$\det(T_p^n) = (\det(T)_p)^n = (-1)^{pn}. \tag{22}$$

Note that according to (22) R_p^n are invertible and their inverses can be calculated using (20) and (21), where $p = 1, 2, 3, \ldots$. Their inverses are as follows:

$$T_p^{-n} = \begin{pmatrix} T_1^{-n} & -I & \cdots & -I & -I \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{I} & \ddots & \mathbf{O} \\ \vdots & \vdots & \ddots & \ddots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I} \end{pmatrix}.$$

2.4 Matrix encryption

Consider a message that is a sequence of integers $\{m_i\}_{i=1,2,\ldots}$. Integers of the message can be packed into a square $\ell \times p$ matrix M. The arrangements of messages in M can be to some extent arbitrary as integers can be determined by selecting odd or even number of digits. For instance, assume we have a message 489165723489625471635, then we can create a 3×4 matrix

$$M = \begin{pmatrix} 48 & 91 & 65 & 723 \\ 4 & 89 & 6 & 25 \\ 47 & 16 & 3 & 5 \end{pmatrix}.$$

Given a matrix K matrix encryption can be defined as follows (see [26]):

$$E = M \times K. \tag{23}$$

The decryption can be done using the inverse matrix K^{-1}

$$M = E \times K^{-1}, \tag{24}$$

where K can be either Q_p^n or R_p^n or T_p^n. For instance, consider again the message 489165723489625471635 and the key matrix

$$K = Q_2^7 = \begin{pmatrix} 8 & 13 & 8 & 13 \\ 13 & 21 & 13 & 21 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then the matrix encryption is

$$E = M \times K = \begin{pmatrix} 48 & 91 & 65 & 723 \\ 4 & 89 & 6 & 25 \\ 47 & 16 & 3 & 5 \end{pmatrix} \times \begin{pmatrix} 8 & 13 & 8 & 13 \\ 13 & 21 & 13 & 21 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Decryption is

$$M = E \times K^{-1} = \begin{pmatrix} 48 & 91 & 65 & 723 \\ 4 & 89 & 6 & 25 \\ 47 & 16 & 3 & 5 \end{pmatrix} \times \begin{pmatrix} 8 & 13 & 8 & 13 \\ 13 & 21 & 13 & 21 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} -21 & 13 & -1 & 0 \\ 13 & -8 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 48 & 91 & 65 & 723 \\ 4 & 89 & 6 & 25 \\ 47 & 16 & 3 & 5 \end{pmatrix}.$$

The encryption described above is symmetric encryption. Symmetric cryptography needs a secure channel to distribute secret keys between two communicating parties. Moreover, the above-mentioned matrix encryption is linear, and can be breakable in a chosen plaintext attack [27].

However, on the one hand, Bennett and Brassard [28] and Ekert [29] showed that key distribution can be done via an insecure channel using a quantum protocol. Note that if the key matrix K is either Q_p^n or R_p^n or T_p^n, then the matrix K can be determined after two elements of the matrix are known. This is due to the recursive nature of the matrix. The crucial point here is that we use the matrix K to encode quantum states. On the other hand, we follow Simon et al. [21, 22] who recently proposed a quantum key distribution (QKD) protocol with Fibonacci coding. The authors use Fibonacci sequences (or Lucas sequences) to prepare entangled states. Two communicating parties can detect the Fibonacci values for the entangled states with the designated sorters. More importantly, Q_p^n or R_p^n or T_p^n can be used just one time, and their order is determined by quantum random generators in Alice's, Bob's and Charlie's laboratories. Considering these, the quantum matrix encryption is secure. We present a brief description of Simon et al.'s QKD protocol in the next subsection.

3 QKD protocols

We first introduce Simon et al.'s original QKD protocol. Then we show how the protocol can be improved in coding efficiency of entangled states when we use the Fibonacci, Lucas or Fibonacci-Lucas matrices defined in Section 2.

3.1 Simon et al.'s QKD protocol

The main idea behind Simon et al.'s QKD protocol [21] is the use of a Vogel spiral [30]. This allows either Alice or Bob (or even a third party) to prepare a source of entangled Fibonacci-valued orbital angular momentum (OAM) states. Fibonacci-valued entangled pairs then leave the spiral and enter the down-conversion crystal. The down-conversion breaks each Fibonacci value into two lower OAM values. In both Alice's and Bob's laboratories, there is a beam splitter directing some regular proportion of the beam to two different types of OAM sorters L and D. The beam splitters randomly transmit the entangled photons to either the L or D sorter. The L sorter allows Fibonacci-valued entangled photons to arrive at the arrays of single-photon detectors only. The D sorter allows "diagonal" superposition in the form $\frac{1}{\sqrt{2}}(|F_n\rangle + |F_{n+2}\rangle)$ and filters out any non-Fibonacci entangled photon.

There are four possible cases for the sorters. Namely, the entangled photon is sent to

(1) L by the beam splitters in both Alice's and Bob's laboratories,

(2) L and D by the beam splitters in Alice's and Bob's laboratories respectively,

(3) D and L by the beam splitters in Alice's and Bob's laboratories respectively,

(4) D by the beam splitters in both Alice's and Bob's laboratories.

Note that the cases (1)–(3) are only available for the key establishment.

3.2 Improved QKD protocol

We show how to use the three classes of Fibonacci, Lucas and Fibonacci-Lucas matrix coding, to improve Simon et al.'s QKD protocol. According to Simon et al.'s QKD protocol, Alice randomly prepares m two-photon entangled states $\{|\varphi\rangle_1,\ |\varphi\rangle_2,\ \ldots, |\varphi\rangle_m\}$, which are in the following states:

$$\sum_n (|F_{n-1}\rangle_{\rm s}|F_{n-2}\rangle_{\rm i} + |F_{n-2}\rangle_{\rm s}|F_{n-1}\rangle_{\rm i}); \tag{25}$$

$$\sum_n (|F_{n+1}\rangle_{\rm s}|F_{n-1}\rangle_{\rm i} + |F_{n-1}\rangle_{\rm s}|F_{n+1}\rangle_{\rm i}), \tag{26}$$

where the subscripts "s" and "i" represent the signal photon and the idler photon, respectively. For State (25), one entangled photon goes to Alice and the other goes to Charlie through the unauthenticated quantum channel. For State (26), one half entangled photon goes to Alice and Bob, respectively via the insecure quantum channel. For Bob and Charlie, the received entangled photons can be both in states either (25) or (26).

Each entangled photon goes to one of the three sorters $\{L, D_1, D_2\}$ (note that D_1, D_2 are both included in D, where D_1, D_2 are used to filter and block any photons whose states are not Fibonacci or Lucas values respectively) in the party laboratories randomly and independently. The parties record the obtained outcomes. L allows photons to arrive at the arrays of single-photon detectors when their states represent Fibonacci values. The parties: Alice, Bob and Charlie announce their results. There are three possible results: (1) both the entangled photons go to D_1; (2) both the entangled photons go to D_2; and (3) one entangled photon goes to D_1 and the other goes to D_2. The parties discard all the data and keep the entangled photons left. For the photons, Alice (Bob) announces the set of states she (he) chooses via authenticated classical channels. The parties now compare their measurements with the two entangled states. They exchange the information among themselves using authenticated classical channels. They also detect Fibonacci or Lucas values used in the relevant matrices.

For example, if the detected Fibonacci value is 8, the key matrix can be constructed as follows:

$$\begin{pmatrix} \mathbf{8} & 13 \\ 13 & 21 \end{pmatrix} = Q_1^7, \quad \begin{pmatrix} 8 & 13 & 8 & 13 \\ 13 & 21 & 13 & 21 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = Q_2^7, \ldots.$$

If the detected Lucas value is 11, the key matrix can be constructed as follows:

$$\begin{pmatrix} 4 & 7 \\ \mathbf{11} & 18 \end{pmatrix} = P_1^3, \quad \begin{pmatrix} 4 & 7 & 4 & 7 \\ \mathbf{11} & 18 & \mathbf{11} & 18 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = P_2^3, \ldots.$$

If the detected Fibonacci and Lucas values are $F_n = 8 = 0 \pmod 2$ and $L_n = 11 = 1 \pmod 2$, the Fibonacci-Lucas matrix should be

$$\begin{pmatrix} 5 & 8 \\ \mathbf{11} & 18 \end{pmatrix} = T_1^4, \quad \begin{pmatrix} 5 & 8 & 5 & 8 \\ \mathbf{11} & 18 & \mathbf{11} & 18 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = T_2^4, \ldots.$$

4 Proposed QDS

Our QDS scheme has the following five stages: setup, key distribution, message blinding, signing and verification. We assume that there are authenticated classical channels and insecure quantum channels

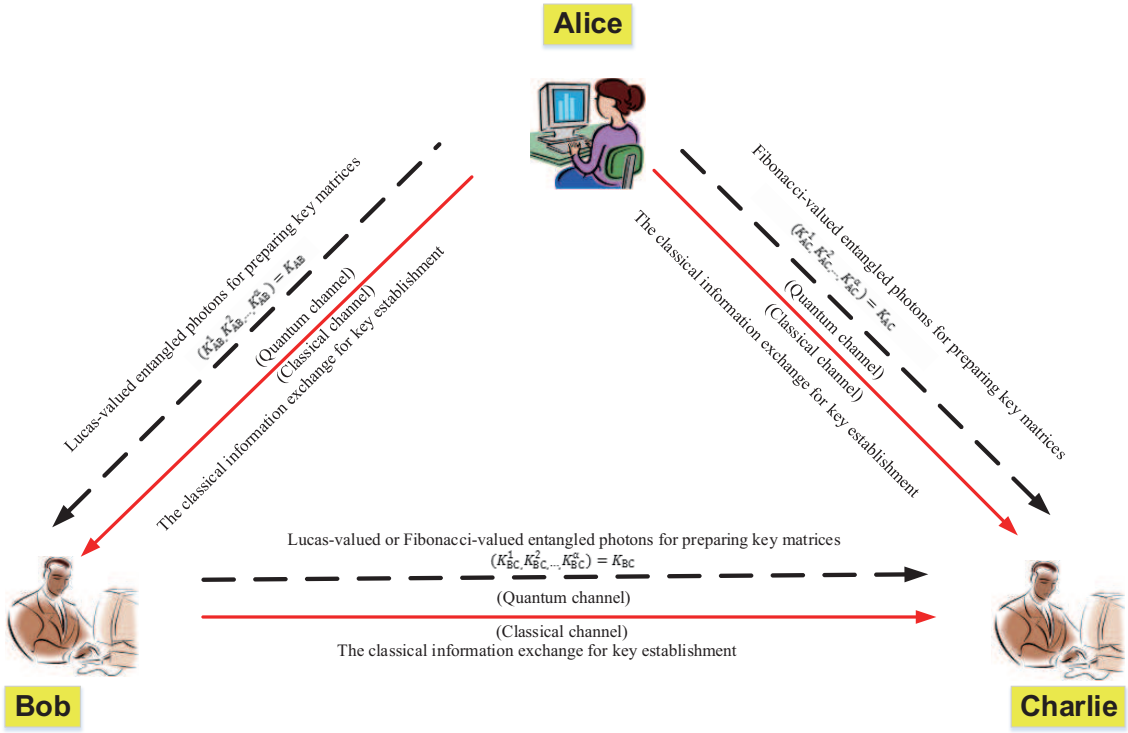

Figure 1 (Color online) The sketch for quantum key distribution of our QDS scheme, where $K_{\rm AB}$, $K^i_{\rm AB}$, $K_{\rm AC}$, $K^i_{\rm AC}$, $K_{\rm BC}$, and $K^i_{\rm BC}$ $(i = 1, 2, \ldots, \alpha)$ are key matrices.

among Alice, Bob and Charlie. Every pair of parties share different quantum key matrices $K_{\rm AB}$, $K_{\rm AC}$ and $K_{\rm BC}$ respectively. We use Simon et al.'s QKD algorithm to produce the key matrices $K_{\rm AB}$, $K_{\rm AC}$ and $K_{\rm BC}$, which are of the form Q^n_p or R^n_p or T^n_p.

4.1 Setup

In our signature, we have three participants: (1) the holder (owner) of a message, Alice who transforms the message into an n-square matrix $(n = 2, 3, \ldots)$ and blinds the matrix, (2) the signer Bob who signs blind messages, (3) the verifier Charlie who checks if a signature matches a message.

4.2 Key distribution

Alice and Bob, Alice and Charlie, Bob and Charlie establish the pairwise quantum key matrices $K_{\rm AB}$, $K_{\rm AC}$ and $K_{\rm BC}$ (see Figure 1), respectively.

The parties use the QKD protocol described in Subsection 3.2 and establish their pairwise key matrices (see Table 2): $\{K^1_{\rm AB}, K^2_{\rm AB}, \ldots, K^\alpha_{\rm AB}\} = K_{\rm AB}$ between Alice and Bob; $\{K^1_{\rm AC}, K^2_{\rm AC}, \ldots, K^\alpha_{\rm AC}\} = K_{\rm AC}$ between Alice and Charlie; and $\{K^1_{\rm BC}, K^2_{\rm BC}, \ldots, K^\alpha_{\rm BC}\} = K_{\rm BC}$ between Bob and Charlie. Note that the order of these key matrices is determined by Alice's, Bob's and Charlie's quantum random generators.

4.3 Message blinding

Alice takes her message and transforms it into matrices $(M_1, M_2, \ldots, M_\alpha) = M$, where $M_k = (m_{tj})_{n\times n}$, $k \in \{1, 2, \ldots, \alpha\}$, $t, j \in \{1, 2, \ldots, n\}$. Next she blinds the message matrix M using the key $K_{\rm AC}$ (see Table 2) and obtains the blind message

$$M'_k = M_k \times K^k_{\rm AC}, \quad k \in \{1, 2, \ldots, \alpha\}. \tag{27}$$

Then Alice encrypts the blind message M' with the key $K_{\rm AB}$ as follows:

$$M''_k = M'_k \times K^k_{\rm AB}, \quad k \in \{1, 2, \ldots, \alpha\}, \tag{28}$$

Table 2 An example for key distribution and digital signature

$V_{\rm s}$ a)	S_1 b)	S_2 c)	$V_{\rm r}$ d)	$R_{\rm K}$ e)	$M_{\rm K}$ f)	M_k g)	$M_{\rm K}\times M_k$
8	L	L	8	2	$\begin{pmatrix}\mathbf{8} & 13\\ 13 & 21\end{pmatrix}$	$\begin{pmatrix}2 & 1\\ 0 & 7\end{pmatrix}$	$\begin{pmatrix}16 & 99\\ 26 & 160\end{pmatrix}$
11	L	D_1	11	2	$\begin{pmatrix}4 & 7\\ \mathbf{11} & 21\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 3 & 6\end{pmatrix}$	$\begin{pmatrix}25 & 42\\ 74 & 126\end{pmatrix}$
8, 11	D_2	L	8, 11	4	$\begin{pmatrix}\mathbf{8} & 13 & \mathbf{8} & 13\\ \mathbf{11} & 18 & \mathbf{11} & 18\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 2 & 0 & 7\\ 0 & 3 & 6 & 0\\ 0 & 4 & 1 & 1\end{pmatrix}$	$\begin{pmatrix}30 & 49 & 30 & 56\\ 33 & 54 & 39 & 54\\ 44 & 72 & 45 & 73\end{pmatrix}$
8	D_2	D_2	–	2	–	–	–

a) $V_{\rm s}$: the value for the entangled state.
b) S_1: one participant's sorter.
c) S_2: the other participant's sorter.
d) $V_{\rm r}$: the value for the recovered entangled state.
e) $R_{\rm K}$: the rank of key matrix.
f) $M_{\rm K}$: the key matrix.
g) M_k: the kth message matrix.

and M_k, $M_{k'}$ and M'_k. Finally, Alice sends $(M''_k, \det(M'_k))$ to Bob, and $\det(M_k)$ to Charlie.

4.4 Signing

Bob signs message M blindly by creating a signature for the message M'. This means that Bob does not know the contents of M. He executes the following steps:

(1) He checks the authenticity of $(M''_k, \det(M'_k))$. First he decrypts the M''_k with the key $K^k_{\rm AB}$ and obtains

$$M'_k = M''_k \times (K^k_{\rm AB})^{-1}, \tag{29}$$

where $(K^k_{\rm AB})^{-1}$ denotes the inverse matrix of $K^k_{\rm AB}$. If the determinant of M'_k recovered by Bob is not equal to the value of the determinant obtained from Alice, Bob aborts this communication. Otherwise, he performs the next step.

(2) He signs the blind message M'_k using $K^k_{\rm BC}$. The signature is

$$S^k = M'_k \times K^k_{\rm BC}. \tag{30}$$

(3) He sends the signature $S = \{S^1, S^2, \ldots, S^\alpha\}$ to Charlie (see Figure 2).

4.5 Verification

Charlie verifies the signature obtained from Bob. He uses the key $K_{\rm AC}$ and the determinant $\det(M)$. He executes the following steps.

(1) Having received the signature S, Charlie decrypts it using $K_{\rm BC}$ and obtains the blind message M'. Next he un-blinds the message M' with $K_{\rm AC}$ and obtains M.

(2) Charlie checks if the determinant of M recovered from the signature is the same as $\det(M)$ obtained from Alice. If the check holds, he verifies the following equations:

$$\begin{aligned}\det(S^k) &= \det(M'_k K^k_{\rm BC}) = \det(M'_k) \times \det(T^n_p)\\ &= (-1)^n \det(M'_k) = (-1)^{2n} \det(M_k).\end{aligned} \tag{31}$$

If the verification holds as well, Charlie accepts S^k. Otherwise, he aborts this communication (see Figure 2).

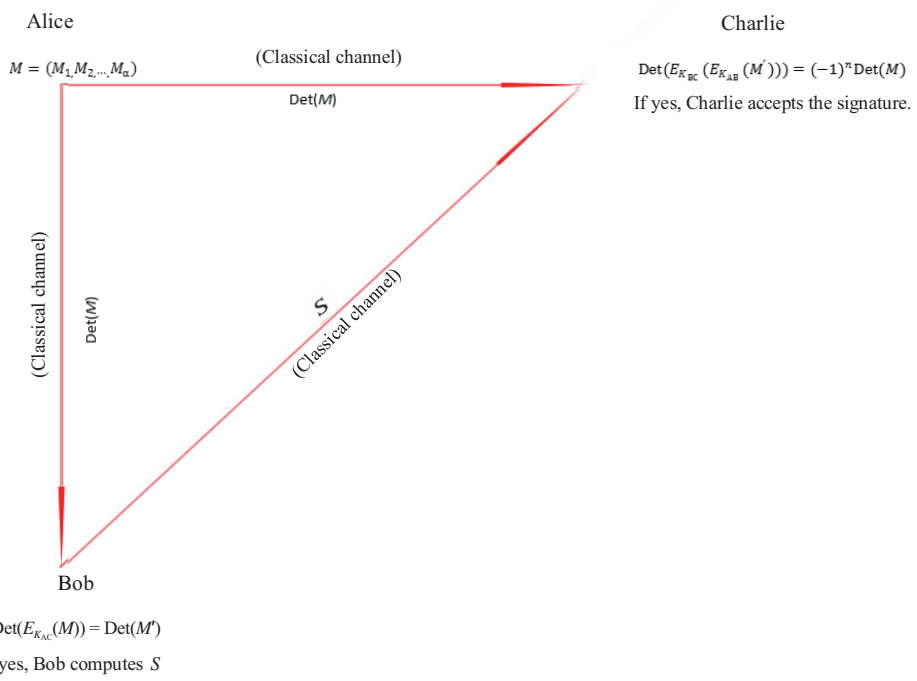

Figure 2 (Color online) The sketch for the process of signature and verification of our QDS scheme, where $K_{\mathrm{AB}} = \{K_{\mathrm{AB}}^1, K_{\mathrm{AB}}^2, \ldots, K_{\mathrm{AB}}^\alpha\}$, $K_{\mathrm{AC}} = \{K_{\mathrm{AC}}^1, K_{\mathrm{AC}}^2, \ldots, K_{\mathrm{AC}}^\alpha\}$, $K_{\mathrm{BC}} = \{K_{\mathrm{BC}}^1, K_{\mathrm{BC}}^2, \ldots, K_{\mathrm{BC}}^\alpha\}$ are all in the form of matrices; $M' = E_{K_{\mathrm{AB}}}\{M\} = M \times K_{\mathrm{AB}}$, $M'' = E_{K_{\mathrm{AC}}}\{M'\} = M' \times K_{\mathrm{AC}}$, $S = E_{K_{\mathrm{BC}}}\{M'\} = M' \times K_{\mathrm{BC}}$, $\det(M')$ is the determinant of M'.

5 Security analysis

In principle, at most one participant can be dishonest in the three-party QDS scheme. This is because the majority vote is usually used to cope with disputes [14, 15, 22]. Our blind QDS protocol is suitable for implementation with current technologies for QKD protocols based on Simon et al's work [21, 22]. In this section, in the context of the relevant work on quantum blind signatures [19, 20, 31–34], we show that our signature resists both the forgery and repudiation attacks. Alice can be traced, though the message is blind. Moreover, we discuss the efficiency, the error detection and correction capability of our protocol.

5.1 Signature forgery

A forgery by either Alice or Charlie is much easier to create than by an external participant. Thus we concentrate on forgery by an internal participant (either Alice or Charlie). We further assume that only one of them can be dishonest (so, we exclude collusion of Alice and Charlie). Suppose that Alice wishes to forge Bob's signatures. This is impossible without the knowledge of the key matrix K_{BC}. Furthermore, the value for every entangled photon is a Fibonacci number. On the other hand, the value for the corresponding entangled state can be either a Fibonacci or a Lucas number. For each pair of entangled states, one goes to Bob's laboratory directly. This means that Alice has to make a guess at $\{K_{\mathrm{BC}}^1, K_{\mathrm{BC}}^2, \ldots, K_{\mathrm{BC}}^\alpha\} = K_{\mathrm{BC}}$. The probability of guessing the correct Fibonacci or Lucas value is $\frac{1}{4}$. Assume that 50 pairs of entangled states are used, then Alice guesses successfully all these entangled states with the probability of 8×10^{-31} (almost 0). In addition, the corresponding determinant values of $\det(M_k), k = \{1, 2, \ldots, \alpha\}$ are sent to guarantee that the Bob signature is authentic.

Suppose Alice wants to entangle her quantum states with the entangled states for preparing K_{BC} in order to obtain some information about Bob's signature. The quantum channel for the transmitted message is one way. Therefore, she cannot obtain any information from the signature because she does not know the key K_{BC}. Most importantly, Charlie may identify Alice at the verification stage because she is not able to provide a correct K_{BC}. Consequently, Alice fails to forge the Bob signatures.

5.2 Repudiation attacks

Note that Charlie can verify the authenticity of signatures using (22). If a signature passes it, Charlie is sure that Bob has created the signature. If Bob disavows his signature, Charlie immediately can discover that this is not true. In the verification stage, Charlie obtains S and translates it using K_{BC} to get M'. Furthermore he uses K_{AC} to obtain the clear message M. The message is authenticated by checking if $\det(M_k)$ is equal to the determinant obtained from Alice. If the check holds, Charlie informs Alice and Bob that the blind signature is authentic. Otherwise, the signature is considered to be invalid and the signature protocol is aborted immediately. This means that neither Alice nor Bob can deny the signature.

5.3 Efficiency of QDS

Unlike the existing QDS protocols [5–15], our protocol can sign long messages and is not restricted to binary ones. Signatures are generated using cryptographic matrices that correspond to entangled states encoded by Fibonacci and Lucas sequences. The number of the elements in a matrix can be chosen at random. Due to the recursive property of Fibonacci and Lucas matrices, the number of the entangled states that are used to prepare Fibonacci and Lucas matrices can be greatly reduced. Besides, a message can be packed into a matrix using different encodings. Matrix multiplication can be implemented very efficiently. Our signature protocol deals with messages of an arbitrary length. An improvement in efficiency is largely due to the fact that both Bob and Charlie send to Alice different entangled states. This is in a stark contrast with previous protocols, where Alice sends to Bob and Charlie the same signature states.

5.4 Error detection and correction of our QDS

Due to the introduction of Fibonacci, Lucas and Fibonacci-Lucas matrices, an additional feature of our signature protocol is its ability to detect errors. This is done by the verification of blind messages and their signatures.

Stakhov [26] has shown that Fibonacci and Lucas matrix signatures have an ability of error correction. To be exact, if the dimension of a matrix is 2, the correction ability of Fibonacci Q_1^n and Q_2^n matrix coding is 93.33% and 99.80%, respectively, and when p is larger, the correction ability is higher than 99.80%. This exceeds an ability of all other well-known error correcting codes.

5.5 Traceability

In case of a disagreement between Alice and Bob, Charlie can trace the owner of a message (Alice) using (6), (19) and (22) and adjudicate whether or not the signature is valid.

5.6 Blindness

Our protocol allows Bob to sign a message blindly, i.e., Bob does not know the contents of the message. However, Bob can confirm the authenticity of the blind message M', i.e., he knows that it comes from Alice. Table 3 illustrates the main features of our QDS protocol and compares it with other relevant protocols [10, 11, 16, 18, 19].

6 Conclusion

In this paper, we have presented a new protocol for secure information transmission over insecure quantum channels and authenticated classical channels with symmetric key algorithms based on Simon et al's protocol [21, 22] and Fibonacci, Lucas, and Fibonacci-Lucas matrices. The proposed protocol will not only enhance the efficiency of quantum digital signature but also save computation time and reduce power requirements. Moreover, our protocol has an ability to detect and correct errors. The security of our protocol is guaranteed by the quantum one-time pad and quantum key distribution [21]. Hence, it is

Table 3 The feature comparisons

Protocol	[10]	[11]	[16]	[18]	[19]	Our QDS
Carrier for transmitting information	SP[h)]	ES[i)]	ES	SP	SP	ES
The state of message being signed	BM[j)]	BM	BM	BM	BM	DM[k)]
The state of signed message	CM[l)]	CM	CM	CM	CM	CM
Quantum key	Yes	Yes	Yes	Yes	Yes	Yes
The ability to recover the encrypted message	Yes	Yes	Yes	Yes	Yes	Yes
XOR operations	Yes	Yes	Yes	Yes	Yes	No
Matrix multiplication	No	No	No	No	No	Yes
Efficiency for signature	$\leqslant 1$	$\leqslant \frac{3}{2}$	$\leqslant 1$	$\leqslant 1$	$\leqslant 1$	$\leqslant \ell_M$
Detection ability	No	No	No	No	No	Yes
Blind	No	Yes	Yes	No	No	Yes

h) SP: single photons.
i) ES: entangled states.
j) BM: bit message.
k) DM: digital message.
l) CM: classical message.

unconditionally secure. Also, our scheme adopts the technology of OAM entangled states distribution and nonorthogonal states are indistinguishable. Thus, our protocol is practical and can be set up using the current technology.

Acknowledgements Hong LAI was supported by Fundamental Research Funds for the Central Universities (Grant No. XDJK2016C043), 1000-Plan of Chongqing by Southwest University (Grant No. SWU116007), and Doctoral Program of Higher Education (Grant No. SWU115091). Mingxing LUO was supported by Sichuan Youth Science & Technique Foundation (Grant No.2017JQ0048). Josef PIEPRZYK was supported by National Science Centre, Poland (Grant No. UMO-2014/15/B/ST6/05130). Shudong Li was supported by National Natural Science Foundation of China (Grant Nos. 61672020, 61662069, 61472433), Project Funded by China Postdoctoral Science Foundation (Grant Nos. 2013M542560, 2015T81129) and A Project of Shandong Province Higher Educational Science and Technology Program (Grant Nos. J16LN61, 2016ZH054). The paper was also supported by A Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) and Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology (CICAEET).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 William S. Cryptography and Network Security: Principles and Practice. 2nd ed. New Jersey: Prentice Hall, 2003. 67–68
2 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM, 1978, 21: 120–126
3 Cramer R, Shoup V. Signature schemes based on the strong RSA assumption. ACM Trans Inf Syst Secur, 2000, 3: 161–185
4 ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: Proceedings of Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1984. 10–18
5 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev, 1999, 41: 303–332
6 Amiri R, Andersson E. Unconditionally secure quantum signatures. Entropy, 2015, 17: 5635–5659
7 Gottesman D, Chuang I. Quantum digital signatures. arXiv:quant-ph/0105032, 2001
8 Chaum D, Heyst E V. Group signatures. In: Advances in cryptography-EUROCRYPT'91. Berlin: Springer, 1991. 257–265
9 Zeng G H, Keitel C H. Arbitrated quantum-signature scheme. Phys Rev A, 2002, 65: 1–6
10 Wallden P, Dunjko V, Kent A, et al. Quantum digital signatures with quantum-key-distribution components. Phys Rev A, 2015, 91: 042304
11 Shi J J, Shi R H, Guo Y, et al. Batch proxy quantum blind signature scheme. Sci China Inf Sci, 2013, 56: 052115
12 Dunjko V, Wallden P, Andersson E. Quantum digital signatures without quantum memory. Phys Rev Lett, 2014, 112: 040502

13 Collins R J, Donaldson R J, Dunjko V, et al. Realization of quantum digital signatures without the requirement of quantum memory. Phys Rev Lett, 2014, 113: 040502
14 Arrazola J M, Wallden P, Andersson E. Multiparty quantum signature schemes. Quantum Inf Comput, 2016, 6: 0435
15 Wang T Y, Cai X Q, Ren Y L, et al. Security of quantum digital signatures for classical messages. Sci Rep, 2014, 5: 9231
16 Wen X J, Niu X M, Ji L P, et al. A weak blind signature scheme based on quantum cryptography. Optics Commun, 2009, 282: 666–669
17 Li F G, Shirase M, Takagi T. Cryptanalysis of efficient proxy signature schemes for mobile communication. Sci China Inf Sci, 2010, 53: 2016–2021
18 Amiri R, Wallden P, Kent A, et al. Secure quantum signatures using insecure quantum channels. Phys Rev A, 2016, 93: 032325
19 Yin H L, Fu Y, Chen Z B. Practical quantum digital signature. Phys Rev A, 2016, 93: 032316
20 Donaldson R J, Collins R J, Kleczkowska K, et al. Experimental demonstration of kilometer-range quantum digital signatures. Phys Rev A, 2016, 93: 012329
21 Simon D S, Lawrence N, Trevino J, et al. High-capacity quantum Fibonacci coding for key distribution. Phys Rev A, 2013, 87: 032312
22 Simon D S, Fitzpatrick C A, Sergienko A V. Discrimination and synthesis of recursive quantum states in high-dimensional Hilbert spaces. Phys Rev A, 2015, 91: 043806
23 Esmaeili M, Moosavi M, Gulliver T A. A new class of Fibonacci sequence based error correcting codes. Cryptogr Commun, 2017, 9: 379–396
24 Vajda S. Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications. New York: Ellis Horwood Ltd.-Halsted Press, 1989
25 Mishra M, Mishra P, Adhikary M C, et al. Image encryption using Fibonacci-Lucas transformation. Int J Cryptogr Inf Secur, 2012, 2: 131–141
26 Stakhov A P. Fibonacci matrices, a generalization of the cassini formula and a new coding theory. Chaos Soliton Fract, 2006, 30: 56–66
27 Rey A, Sanchez G. On the security of the golden cryptography. Int J Netw Secur, 2008, 7: 448450
28 Bennett C H, Brassard G. Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984. 175–179
29 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663
30 Vogel H. A better way to construct the sunflower head. Math Biosci, 1979, 44: 179–189
31 Wang T Y, Cai X Q, Zhang R L. Security of a sessional blind signature based on quantum cryptograph. Quant Inf Process, 2014, 13: 1677–1685
32 Wang T Y, Wen Q Y. Fair quantum blind signatures. Chin Phys B, 2010, 19: 060307
33 Wen X J, Chen Y Z, Fang J B. An inter-bank E-payment protocol based on quantum proxy blind signature. Quant Inf Process, 2013, 12: 549–558
34 Cai X Q, Zheng Y H, Zhang R L. Cryptanalysis of a batch proxy quantum blind signature scheme. Int J Theor Phys, 2014, 53: 3109–3115