Arbitrated quantum-signature scheme

Guihua Zeng* and Christoph H. Keitel†
Theoretische Quantendynamik, Fakultät für Physik, Universität Freiburg, Hermann-Herder-Strasse 3, D-79104 Freiburg, Germany
(Received 11 May 2001; revised manuscript received 6 August 2001; published 1 April 2002)

The general principle for a quantum-signature scheme is proposed and investigated based on ideas from classical signature schemes and quantum cryptography. The suggested algorithm is implemented by a symmetrical quantum key cryptosystem and Greenberger-Horne-Zeilinger (GHZ) triplet states and relies on the availability of an arbitrator. We can guarantee the unconditional security of the algorithm, mostly due to the correlation of the GHZ triplet states and the use of quantum one-time pads.

DOI: 10.1103/PhysRevA.65.042312 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

Quantum cryptography combines quantum theory with classical cryptography. The main goal of this field is to take advantage of purely quantum effects to provide unconditionally secure information exchange [1], in contrast, in general, to classical methods. Those are mostly very secure due to the complexity of the system employed; however, they become increasingly vulnerable with more powerful computers and, thus, improved means of handling complexity. Many advances have been put forward in quantum cryptography in recent years, including enhanced insights into the basic theory [2], quantum key management [3,4], quantum secret sharing [5], quantum authentication [6], and quantum-bit commitment [7]. In particular, quantum key distributions attracted special interest due to technological advances that allow their implementations in laboratory, and theoretical investigations, which proved them to be unconditionally secure [4].

An important issue in cryptography is the reliable assignment of a message to its originator. A certification that a particular person has noted or agreed to a message composed by someone else appears to be often equally useful. Signature schemes are developed classically so far for this purpose as an addition to a message such that the message can neither be disavowed by the signatory nor can it be forged by the receiver or a possible attacker [8]. Up to now, conventional (handwritten) and digital approaches have been employed in practical applications. While conventional signatures cannot be transmitted in the electronic network and are vulnerable to forgery, digital signatures have been used widely and with considerable success in *e*-commerce. However, classical cryptography and thus also classical signature schemes are, in general, not unconditionally secure and are in addition difficult to assign to messages in qubit format.

In this paper, we put forward a quantum-signature scheme as a method of assigning messages by quantum methods to its originator or other users. The algorithm takes advantage of the correlation of Green-Horne-Zeilinger (GHZ) states [9], various qubit operations, and a symmetrical quantum key cryptosystem. It is shown to be unconditionally secure, i.e., may not be forged or modified in any way by the receiver or attacker. In addition it may neither be disavowed by the signatory nor may it be deniable by the receiver.

The paper is arranged as follows. In Sec. II, we investigate at first the general principles we demand for a quantum-signature scheme which is then proposed and described in detail in Sec. III. The proposed scheme includes an initial phase, a signing phase and a verifying phase. In Sec. IV, the unconditional security of the proposed algorithm is derived and the quantum signature is shown neither to be disavowable by the signatory nor to be deniable for the receiver. Conclusions are drawn in Sec. V.

II. GENERAL REQUIREMENTS

Before presenting the proposed algorithm, we put forward several aspects to be expected to be fulfilled for a quantum-signature scheme and which have led us to design the quantum signature algorithm to follow. Similar to classical digital signatures [8] we demand the following signature rules, where only the last is characteristic for quantum-signature schemes.

(1) *No modifications and no forgery.* Neither the receiver nor a possible attacker are able to change the signature or the attached message after completion. The signature may not be reproduced as well.

(2) *No disavowals.* The signatory may not successfully disavow the signature and the signed message. It may be possible for the receiver to identify the signatory. The receiver may not successfully deny the receipt of the message and signature.

(3) *Firm assignments.* Each message is assigned anew to a signature and may not be separated from it afterwards.

(4) *Quantum nature.* The signature involves purely quantum-mechanical features without a classical analog and is therefore by nature nonreproducible and may not be disavowed or forged.

In analogy to conventional and digital signature schemes, a quantum signature algorithm should consist also of both a signature and a verification algorithm. These algorithms will also have to be prepared by an initial phase, which initializes or prepares the system parameters and creates the keys. As usual the signatory, receiver, and possible attacker are referred to as Alice, Bob, and Oscar, respectively, where appropriate. We assume a message to be signed to be carried by

*Email address: guihuazeng@hotmail.com
†Email address: keitel@physik.uni-freiburg.de

a string of qubits $|P\rangle$. The signing algorithm is denoted QS_K with key K to be used in the signature phase. In the verification phase, the resulting signature $|S\rangle$ with $|S\rangle = QS_K(|P\rangle)$ can subsequently be verified using a verification algorithm $QV_{K'}$ with key K'. Note the keys K and K' may be the same (symmetrical key cryptosystem) as assumed here or may be different (public key cryptosystem) [8]. Given a pair $(|P\rangle,|S\rangle)$, the verification algorithm when applied is required to result ''true'' or ''false'' depending on whether the signature is authentic or forged.

A quantum-signature scheme may thus be defined as a five-tuple $(\mathcal{P},\mathcal{S},\mathcal{K},\mathcal{Q}_s,\mathcal{Q}_v)$ with the following abbreviations.

(a) $\mathcal{P}$ is a set of possible quantum messages (qubits).

(b) $\mathcal{S}$ is a set of possible signatures. It may consist of qubits or classical bits.

(c) $\mathcal{K}$ is a set of possible keys. It may be a quantum key or a classical key.

(d) $\mathcal{Q}_s$ is a set of possible quantum signature algorithms.

(e) $\mathcal{Q}_v$ is a set of possible quantum verification algorithms.

For each key $|K\rangle \in \mathcal{K}$, there need be a signature algorithm $QS_K \in \mathcal{Q}_s$ and a corresponding verification algorithm $QV_{K'} \in \mathcal{Q}_v$. $QS_K:\mathcal{P}\rightarrow\mathcal{S}$ and $QV_{K'}:\mathcal{P}\times\mathcal{S}\rightarrow\{T,F\}$ (where T means ''true'' and F means ''false'') are functions such that the following equation is satisfied for every message $|P\rangle \in \mathcal{P}$ and for every signature $|S\rangle \in \mathcal{S}$:

$$QV_{K'}(|P\rangle,|S\rangle)=\begin{cases} True & \text{if } |S\rangle = QS_K(|P\rangle) \\ False & \text{if } |S\rangle \neq QS_K(|P\rangle). \end{cases} \quad (1)$$

We emphasize that the signature $|S\rangle$ and the keys may be composed of quantum or classic bits, but we require the signature and verification algorithms QS_K and $QV_{K'}$ to be of quantum nature.

We recall that signature schemes are generally divided into two categories, the so called *true* and the *arbitrated* signature schemes. The true signatures can be produced and verified independently by the sender and the receiver, respectively. In this category, the signature algorithm is secret but the verification algorithm is public. A judge may be called only to settle possible disagreements or disputes. In an arbitrated signature scheme, however, all communications involve a so-called arbitrator, who authenticates and validates the signed messages. In this category, both signature algorithm and verification algorithm are secret. In the arbitrated signature scheme, the arbitrator is required to be trustworthy, because the arbitrator has access to the contents of the messages and the signatures. While a true signature scheme is in general favorable, arbitrated digital signature schemes were shown to be applicable and useful, especially with reduced requirements on the trustworthiness of the arbitrator [10]. In the following, we develop an arbitrated quantum signature scheme based on the requirements and definitions in this section.

III. DESCRIPTION OF THE PROPOSED ALGORITHM

The proposed algorithm includes three phases: the initial phase, the signature phase, and the verification phase. The scheme involves three partners, signatory Alice, receiver Bob, and the arbitrator. In the initial phase, the three communicators entangle themselves via GHZ states and distribute their secret keys. In the signature phase, Alice prepares and signs her message and obtains an entangled quantum set of the message and signature. In the verification phase, Bob verifies Alice's signature with the arbitrator's help.

A. Initial phase

This phase generates the keys, sets up the system, and distributes the GHZ particles required for our signature scheme.

Step 1: Generation and distribution of keys. Alice and Bob begin by obtaining their secret keys K_a, K_b, where K_a, K_b are employed in the communications between Alice and the arbitrator and between Bob and the arbitrator, respectively. These keys may be obtained by using standard technologies of quantum and classic cryptography. Our keys here are assumed to be generated via quantum cryptographic methods (see, e.g., BB84 or EPR protocols in [3]) because of their unconditional security.

Step 2: Generation and distribution of GHZ triplet states. Our algorithm relies crucially on the entanglement of the three involved communicators Alice, Bob, and the arbitrator. This shall be established here prior to each communication by a distribution of one particle of GHZ triplet states to each of the three. For convenience, we assume the arbitrator to create and distribute the GHZ particles in our consideration. When the arbitrator receives Alice's or Bob's application for an arbitrated communication, he is required to create a string of GHZ triplet states and then to distribute two particles of each GHZ triplet state to Alice and Bob (one each) and to keep the remaining one for himself for each GHZ state. As a consequence, the arbitrator, Alice, and Bob are entangled because they hold one particle of each GHZ triplet state. The GHZ states for a three-particle system involve eight orthonormal triplet states, while in this paper, for convenience, we restrict ourselves to the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \quad (2)$$

We emphasize for above procedures, that step 1 is finished once the system has been set up, and that it is not necessary to repeat it in later communications. Step 2 is necessary to be redone for every single communication, the necessity of which becomes clear in the description of the algorithm.

As a practical consideration we add at this stage that GHZ triplet states have been widely studied in quantum-information science [5,11] and, in particular, have been successfully implemented experimentally [12,13]. With respect to our demands on the GHZ states in step 2, a practical realization may follow the procedure presented in [14]. Along those lines the arbitrator may generate a short weak-light pulse and then employ an interferometer to split this pulse into two pulses of smaller, equal amplitude, following each other with a fixed phase relation. The light is then fo-

cused into a nonlinear crystal where some of the pump photons are down-converted into correlated photon pairs. While the first part of the setup is located with the arbitrator, the two down-converted weak photon beams are separated and sent one each to Alice and Bob. This approach has been successful for the experimental verification of quantum key sharing [15], such that it should be feasible, in principle, also for our proposed algorithm.

B. Signing phase

This phase corresponds to the actual signature algorithm QS_K, i.e., to sign the message $|P\rangle$ with a suitable signature $|S\rangle$. The following steps are required.

Step 1. Alice creates a string of qubits $|P\rangle$ (information qubits) that carry the message to be signed. We assume n qubits in the string, such that $|P\rangle$ reads

$$|P\rangle=\{|p_1\rangle,|p_2\rangle,\ldots,|p_n\rangle\}, \tag{3}$$

where the symbol $\{\cdots\}$ denotes a set in this paper and $|p_i\rangle$ a single qubit in the string $|P\rangle$. Any qubit $|p_i\rangle(i=1,2,\ldots,n)$ in $|P\rangle$ can be expressed as a superposition of the two eigenstates $|0\rangle,|1\rangle$, i.e.,

$$|p_i\rangle=\alpha_i|0\rangle+\beta_i|1\rangle, \tag{4}$$

where α_i,β_i are complex numbers with $|\alpha_i|^2+|\beta_i|^2=1$. Using the above Eq. (4), Alice's information string of qubits can be represented as

$$|P\rangle=\{\alpha_1|0\rangle+\beta_1|1\rangle,\alpha_2|0\rangle+\beta_2|1\rangle,\ldots,\alpha_n|0\rangle+\beta_n|1\rangle\}. \tag{5}$$

Step 2. The aim for Alice in this step is to create a secret string of qubits $|R\rangle$, which involves not only random features, but also depends clearly on the information string $|P\rangle$. As a first step Alice relates the key $K_a=\{|K_a^1\rangle,|K_a^2\rangle,\ldots,|K_a^n\rangle\}$ to a sequence of measurement operators $\mathcal{M}_{K_a}$, often referred to as a measurement basis, which we denote as

$$\mathcal{M}_{K_a}=\{\mathcal{M}^{\,1}_{K_a^1},\mathcal{M}^{\,2}_{K_a^2},\ldots,\mathcal{M}^{\,n}_{K_a^n}\}. \tag{6}$$

The operators $M^i_{K_a^i}$ are defined to arise from the key $|K_a^i\rangle$ for $i\in\{1,2,\ldots,n\}$ via $M^i_{K_a^i}|K_a^i\rangle=\lambda_i|K_a^i\rangle$. There is thus a degree of arbitrariness in the definition of these operators with λ_i being the corresponding eigenvalues. As a simple example, this may, e.g., be carried out for a key K_a consisting of nonorthogonal states $|a\rangle$ and $|b\rangle$ (see, e.g., the Bennett 1992 (B92) protocol in [4]) by choosing two appropriate operators O_a and O_b, where $O_a|a\rangle=\lambda_1|a\rangle$ and $O_b|b\rangle=\lambda_2|b\rangle$. This way, Alice may obtain a string of measurement bases $\mathcal{M}_{K_a}$ consisting of O_a and O_b by transferring $|K_a^i\rangle=|a\rangle$ to $M^i_{K_a^i}=O_a$ and $|K_a^j\rangle=|b\rangle$ to $M^i_{K_a^i}=O_b$ for $\{i,j\}\in\{1,2,\ldots,n\}$. Alternatively Alice may use the measurement basis of polarized photons, e.g., as in the BB84 protocol and let the bit "1" (or qubit $|\pi/4\rangle$ and $|3\pi/2\rangle$) correspond to the diagonal measurement basis and "0" (or qubit $|0\rangle$ and $|\pi/2\rangle$) correspond to the rectilinear measurement basis, or vice versa [6].

After the transformation, Alice is required to measure the information string of qubits $|P\rangle$ using $\mathcal{M}_{K_a}$ and obtains

$$|R\rangle=\mathcal{M}_{K_a}|P\rangle=\{|r_1\rangle,|r_2\rangle,\ldots,|r_n\rangle\}, \tag{7}$$

where $|r_i\rangle=\mathcal{M}^{\,i}_{K_a^i}|p_i\rangle$ and denotes the ith qubit in the string of $|R\rangle$. Note the string $|R\rangle$ is secret, associated with Alice's message, and involves both quantum mechanics and Alice's actions. It will form an essential part of the full signature scheme.

Step 3. Alice entangles each qubit of the information string $|P\rangle$ with one particle each of her equally long GHZ particle string to form a particle pair. This may be implemented by applying a joint measurement on both particles, such as in a quantum logic gate operation [15]. Each combination generates a four-particle entangled state, involving the three GHZ particles and the information qubit. Using Eqs. (2) and (4) the four-particle entangled state can be described as follows:

$$\begin{aligned}|\phi\rangle_i&=|p_i\rangle\otimes|\psi\rangle\\&=\frac{1}{2}\{|\Psi^+_{12}\rangle_a(\alpha_i|00\rangle_{Ab}+\beta_i|11\rangle_{Ab})\\&\quad+|\Psi^-_{12}\rangle_a(\alpha_i|00\rangle_{Ab}-\beta_i|11\rangle_{Ab})\\&\quad+|\Phi^+_{12}\rangle_a(\beta_i|00\rangle_{Ab}+\alpha_i|11\rangle_{Ab})\\&\quad+|\Phi^-_{12}\rangle_a(\beta_i|00\rangle_{Ab}-\alpha_i|11\rangle_{Ab})\},\end{aligned} \tag{8}$$

where the subscripts a,A,b correspond, respectively, to Alice, the arbitrator and Bob. $|\Psi^+_{12}\rangle,|\Psi^-_{12}\rangle,|\Phi^+_{12}\rangle,|\Phi^-_{12}\rangle$ denote the four Bell states [16].

Step 4. Alice carries out n Bell measurements, i.e., for each $i\in\{1,\ldots,n\}$ the state $|\phi\rangle_i$ in Eq. (8) is projected to one of its four summands written on top of each other. The effect of this measurement is to disentangle Alice's two particles (information qubit and GHZ particle) to be in one of the four Bell states and to retain the arbitrator's and Bob's corresponding GHZ particles to be in a two-particle entanglement state as visible in Eq. (8). Thus, Alice obtains the following set $\mathcal{M}_a$ of quantum states:

$$\mathcal{M}_a=\{\mathcal{M}^{\,1}_a,\mathcal{M}^{\,2}_a,\ldots,\mathcal{M}^{\,n}_a\}, \tag{9}$$

where $\mathcal{M}^{\,i}_a$ may be any of the four Bell states in $\{|\Psi^+_{12}\rangle,|\Psi^-_{12}\rangle,|\Phi^+_{12}\rangle,|\Phi^-_{12}\rangle\}$, which, in particular, is the result arising from her Bell measurement on state $|\phi\rangle_i$ in Eq. (8).

Step 5. Alice obtains the quantum signature $|S\rangle$ for the information qubit string $|P\rangle$ by encrypting $\mathcal{M}_a$ and the secret qubit string $|R\rangle$ by the secret key K_a, i.e.,

$$|S\rangle=K_a(\mathcal{M}_a,|R\rangle). \tag{10}$$

$\mathcal{M}_a$, even though consisting of quantum-mechanical Bell states, may be presented by classical bits, and thus be encrypted by a classical one-time pad. $|R\rangle$ could be encrypted

by the approach known as ''quantum-state operation.'' Another way would be to transfer $\mathcal{M}_a$ into a string of qubits $|\mathcal{M}_a\rangle$ and then make measurements on both $|\mathcal{M}_a\rangle$ and $|R\rangle$ via $\mathcal{M}_{K_a}$.

Step 6. Alice sends the string of information qubits $|P\rangle$ followed by the signature $|S\rangle$ to Bob.

We emphasize again that the signature is associated with $|P\rangle$ because $|R\rangle$ was generated via the string of information qubits. We note also that, at this state already, Alice's secret key was crucial in preparing the signature such that it appears difficult at least for Alice to disavow it in the face of the arbitrator or for Bob and the attacker to forge it. In addition we realize that the separation of the message and signature by Oscar would not benefit him or anybody else because the message is valid only with the correct signature and new messages will be assigned new signatures. The arbitrator has been hardly involved up to this stage but this will change in the verification phase to be discussed in the following.

C. Verification phase

A verification algorithm QV_K is developed here such that Bob is able to verify Alice's signature $|S\rangle$ and consequently judge the authenticity of the information qubits $|P\rangle$. The verification process in this scheme requires the help of the arbitrator because Bob does not possess Alice's key, which is necessary for the verification of the signature. The verification phase is executed by the following procedure.

Step 1. Bob measures his string of GHZ particles, which, at this stage, are only entangled to the particles of the arbitrator. The measurement is performed such that the two possible outcomes are either $|+x\rangle$ or $|-x\rangle$ with $|+x\rangle = 1/\sqrt{2}(|0\rangle+|1\rangle)$ and $|-x\rangle = 1/\sqrt{2}(|0\rangle-|1\rangle)$ (referred to as measurements in the x direction). The sequence of the results of the measurement $\mathcal{M}_b$ can thus be expressed as

$$\mathcal{M}_b=\{\mathcal{M}_b^1,\mathcal{M}_b^2,\ldots,\mathcal{M}_b^n\}, \tag{11}$$

where $\mathcal{M}_b^i$ is any of two states in $\{|+x\rangle,|-x\rangle\}$. Encrypting $\mathcal{M}_b,|S\rangle$ and $|P\rangle$ with the aid of Bob's key K_b, he obtains

$$y_b=K_b(\mathcal{M}_b,|S\rangle,|P\rangle). \tag{12}$$

Then, Bob sends y_b to the arbitrator.

Step 2. The arbitrator becomes active now and generates a verification parameter γ based on the communication from Bob, which also contains information from Alice. After receiving y_b, the arbitrator decrypts it using K_b, and obtains $|S\rangle,|P\rangle,\mathcal{M}_b$. Then the arbitrator decrypts $|S\rangle$ using the key K_a, which he has since step 1 of the initial phase. This gives rise to $|R'\rangle$ via the correlation of the GHZ triplet states [5] and $|R'\rangle$ needs to be compared with $|R\rangle$. With $|R'\rangle$, $|P\rangle$ and $\mathcal{M}_{K_a}$, the arbitrator then creates a parameter γ via

$$\gamma=\begin{cases}1 & \text{if } |R'\rangle=|R\rangle=\mathcal{M}_{K_a}|P\rangle,\\ 0 & \text{if } |R'\rangle\neq|R\rangle=\mathcal{M}_{K_a}|P\rangle.\end{cases} \tag{13}$$

Step 3. The arbitrator measures or evaluates the states of the particles in his string of GHZ particles. In previous steps, the arbitrator has already obtained the measurement results $\mathcal{M}_a,\mathcal{M}_b$ of Alice and Bob, so that he can easily determine his states using Eq. (8). Equally the arbitrator may choose an appropriate sequence of measurement operators to measure his string of GHZ particles, and obtains either way $\mathcal{M}_t=\{\mathcal{M}_t^1,\mathcal{M}_t^2,\ldots,\mathcal{M}_t^n\}$. Note that $\mathcal{M}_t^i$ may be $|+x\rangle$ or $|-x\rangle$ with the same definitions as in Sec. I for Bob. Encrypting $\mathcal{M}_a,\mathcal{M}_b,\mathcal{M}_t,|S\rangle$, and γ via the key K_b, the arbitrator obtains

$$y_{tb}=K_b(\mathcal{M}_a,\mathcal{M}_b,\mathcal{M}_t,\gamma,|S\rangle). \tag{14}$$

Following completion of this procedure, the arbitrator sends y_{tb} to Bob.

Step 4. Bob decrypts y_{tb} and obtains $\mathcal{M}_a,\mathcal{M}_b,\mathcal{M}_t,|S\rangle$, and γ. These parameters will turn out essential for Bob for the verification of Alice's signature. This will occur in the two steps to follow, where the first is to eliminate obvious forgeries quickly while the second is more demanding but allows for full security.

Step 5. Bob undertakes the first verification for Alice's signature $|S\rangle$ via the parameter γ. If $\gamma=0$, the signature has obviously been forged and Bob may reject the message $|P\rangle$ immediately. If $\gamma=1$, Bob goes on for further verification to the next step.

Step 6. The relation $\gamma=1$ merely shows that the secret string of qubits $|R\rangle$ is correct. However, this does not fully confirm that the signature $|S\rangle$ is correct because the attacker may have forged the signature by other means [see Eq. (10)]. Thus Bob needs a further verification. This will have to be obtained via the initial correlation of the GHZ triplet states. Taking advantage of $\mathcal{M}_a$ and $\mathcal{M}_t$ and a further transformation to be detailed later in Eq. (17), Bob evaluates the information string of qubits $|P'\rangle$. This information string Bob has to compare with the original information string of qubits $|P\rangle$. If $|P'\rangle=|P\rangle$, the signature is completely correct and Bob accepts $|P\rangle$, otherwise, he rejects it. We emphasize that the result $|P'\rangle$ is obtained from a calculation and not a direct physical measurement, because Bob's particle has already been measured in step 1 of the verification phase. However, since $\mathcal{M}_t$ depends on $\mathcal{M}_b$, the result of the calculation $|P'\rangle$ is equally influenced by Bob's measurement. This is useful regarding high security because it prevents eavesdropping via intercepting Bob's GHZ particle as analyzed in [5].

We note that $\mathcal{M}_a$ and $\mathcal{M}_t$ are essential for Bob to obtain $|P'\rangle$ as is obvious from Eq. (8). If, e.g., Alice's result is $|\Psi_{12}^+\rangle$ or $|\Psi_{12}^-\rangle$, Bob's density matrix of the GHZ particle reads

$$\rho_b=|\alpha_i|^2|0\rangle_{bb}\langle 0|+|\beta_i|^2|1\rangle_{bb}\langle 1|, \tag{15}$$

while in the remaining two cases $|\Phi_{12}^+\rangle$ and $|\Phi_{12}^-\rangle$, Bob's density matrix of the GHZ particle is

$$\tilde{\rho}_b=|\beta_i|^2|0\rangle_{bb}\langle 0|+|\alpha_i|^2|1\rangle_{bb}\langle 1|. \tag{16}$$

Thus even with Alice's results $\{\mathcal{M}_a^i\}$, Bob can only obtain part, of the information of the qubit $|p_i\rangle$ without the knowledge of $\mathcal{M}_t$. In order to obtain $|p_i\rangle$, Bob needs thus $\mathcal{M}_a,\mathcal{M}_t$ and in addition simultaneously the following transformations [5]:

$$|\Psi_{12}^{+}\rangle_a|+x\rangle_A \rightarrow I, \quad |\Phi_{12}^{+}\rangle_a|+x\rangle_A \rightarrow \sigma_x,$$

$$|\Psi_{12}^{+}\rangle_a|-x\rangle_A \rightarrow \sigma_z, \quad |\Phi_{12}^{+}\rangle_a|-x\rangle_A \rightarrow \sigma_x\sigma_z,$$

$$|\Psi_{12}^{-}\rangle_a|+x\rangle_A \rightarrow \sigma_z, \quad |\Phi_{12}^{-}\rangle_a|+x\rangle_A \rightarrow \sigma_x\sigma_z,$$

$$|\Psi_{12}^{-}\rangle_a|-x\rangle_A \rightarrow I, \quad |\Phi_{12}^{-}\rangle_a|-x\rangle_A \rightarrow \sigma_x, \tag{17}$$

where $\sigma_i, i=x,y,z$ are the Pauli matrices and I is the identity matrix. How this above transformation should be employed will be explained below with the help of an example.

We assume, for example, that Alice's result is $|\Psi_{12}^{+}\rangle$, so that following Eq. (8) the arbitrator's and Bob's entanglement state must be

$$|\varphi\rangle_{Ab} = \alpha_i|00\rangle + \beta_i|11\rangle. \tag{18}$$

It can be rewritten as

$$|\varphi\rangle_{Ab} = \frac{\sqrt{2}}{2}|+x\rangle_A(\alpha_i|0\rangle_b + \beta_i|1\rangle_b) + \frac{\sqrt{2}}{2}|-x\rangle_A(\alpha_i|0\rangle_b - \beta_i|1\rangle_b). \tag{19}$$

Obviously, when the arbitrator's result is $|+x\rangle$, the above equation shows that Bob's calculated result is $\alpha_i|0\rangle+\beta_i|1\rangle$, which just equals $|p_i\rangle$. This means that under the transformation I Bob can calculate the result $|p_i\rangle$. When, however, the arbitrator's result is $|-x\rangle$, Bob's calculated result is $\alpha_i|0\rangle-\beta_i|1\rangle$. In this case we do not get the original information qubit in spite of the absence of forgery. Thus a transformation is necessary, which is the reason of Eq. (17). According to Eq. (17) for the arbitrator's result $|-x\rangle$, Bob makes the transformation σ_z on the state $\alpha_i|0\rangle-\beta_i|1\rangle$. Finally Bob obtains the state of $|p_i\rangle$, which is the same as the corresponding state in the original string $|P\rangle$. This is the proof that the signature was authentic, while if Bob's results after the transformation Eq. (17) had been different to the corresponding state in the original string $|P\rangle$, there must have been some sort of fraud. This procedure via Eq. (17) has to be carried out for each state in the information string $|P\rangle$. Alice's signature is only successfully verified if all n elements are rederived by Bob in the procedure described above in step 6.

We summarize this section and emphasize that the verification phase needs the assistance of an arbitrator. This becomes clear from steps 2 and 3, however, the verification itself is completed mainly by Bob. This reduces the dependence on the arbitrator somewhat. It also saves the resources of the network system because the complete execution of the verification by the arbitrator is likely to become a considerable burden on the network system. The parameter γ should be useful for a reasonably large efficiency of the verification procedure. When $\gamma=0$, the received string $|R'\rangle$ differs from the original secret string of qubits $|R\rangle$, so that the signature is obviously to be rejected instantaneously. In this case Bob does not need to make further verifications, so that further efforts are avoided. When $\gamma=1$, the authenticity, however, is not confirmed yet because the attacker may have forged the signature $|S\rangle$ by other means. In the practical situation, for example, in which the K_a has been discovered without Alice's awareness, the parameter γ will not be of any help to discover this happening. In this case Oscar may forge $|R\rangle$ but without $\mathcal{M}_a$ may not find $|S\rangle$. In step 6, with the help of the correlation of the GHZ triplet states, Bob would then discover any fraud.

IV. SECURITY ANALYSIS AND DISCUSSION

The security analysis of the quantum-signature scheme is different from what we are used to for quantum key distributions. In the signature scheme, complete security requires that the signatory cannot disavow the signature, and that the receiver and the attackers have no possibility to obtain the signature or the signature keys so that they may forge the signature. In the following, we will demonstrate that our proposed algorithm is unconditionally secure.

A. Impossibility of forgery

A dishonest Bob or an attacker may seek to forge Alice's signature to his own benefit. In the following we show that neither Bob nor any attacker may forge the signature or the message.

We begin by assuming that Bob is dishonest and tries to forge Alice's signature. If successful, this is beneficial for him because he can change Alice's signature and design a new signature to a message favorable to him. This is impossible, however, because the signature key K_a is secretly kept by Alice and the arbitrator. As a consequence, Bob cannot obtain the correct state $|R\rangle$, which is necessary for the generation of the signature [please see Eq. (10)]. Subsequently the parameter γ is not correct, so that this forgery can be noted when the arbitrator is called to settle a dispute between Alice and Bob.

The attacker is bound to be unsuccessful in our algorithm, because the only public parameters are $|P\rangle, |S\rangle, y_b, y_{tb}$ and they do not offer any information on the secret keys K_a and K_b. Especially, when the communicators encrypt the messages by a one-time pad algorithm, which is relatively easy to be implemented in quantum cryptography, the security is very high. Even if the attacker does somehow get hold of Alice's and Bob's keys, a forgery still remains impossible. This is because the attacker has no access to Alice's measurement results $\mathcal{M}_a$, which are secret and are involved in generating the quantum signature $|S\rangle$ [see again Eq. (10)]. The verification condition $|P'\rangle=|P\rangle$ cannot be satisfied without the correct $\mathcal{M}_a$. Thus, the correlation of the GHZ triplet state prevents forgery by an attacker.

B. Impossibility of disavowal by the signatory

If Alice disavows her signature, it is very easy to discover it, due to Alice's key being contained in the signature $|S\rangle$. Thus, if Alice and Bob are engaged in a dispute because of Alice's disavowal, they just need to send the signature $|S\rangle$ to the arbitrator. If the signature $|S\rangle$ contains Alice's key K_a, this signature has been carried out by Alice, otherwise, the

signature has been forged by Bob or the attacker. Therefore, the arbitrator is in the position to judge whether Alice has disavowed her signature.

C. Impossibility of denial by the receiver

A conventional and a digital signature scheme is termed undeniable if Bob cannot deny his receiving of Alice's files. This feature is not generally demanded of a signature but it may be useful for many practical applications. Our algorithm contains this property, i.e., Bob cannot disavow his receiving of the signature $|S\rangle$ and the information qubit string $|P\rangle$. This is essentially impossible because he needs the assistance of the arbitrator in the verification process. In addition we can reduce the dependence on the arbitrator by small modifications without losing this property of having an undeniable signature scheme. In the verification procedure, Bob obtains y_b in step 1 and sends it to Alice rather than to the arbitrator as in the original version. Then Alice obtains the new signature $|\tilde{S}\rangle = K_a(\mathcal{M}_a, |R\rangle, y_b)$ and sends it to the arbitrator. We emphasize here that Alice cannot obtain Bob's key by knowing Y_b. The arbitrator then modifies y_{ta} in step 3 of the verification phase to be

$$\tilde{y}_{tb} = K_b(\mathcal{M}_a, \mathcal{M}_b, \mathcal{M}_t, \gamma, |\tilde{S}\rangle). \tag{20}$$

After this change Alice's and Bob's keys are included in the signature $|\tilde{S}\rangle$. Then Bob cannot disavow the fact that the received files have come from Alice, i.e., Bob's receipt of the files is undeniable.

V. CONCLUSIONS

The general principle and all detailed procedures of a quantum-signature scheme have been described and explained. The similarities to the digital signature scheme were pointed out but emphasis was laid on the description of the quantum methods in the algorithms, such as the use of GHZ states. Our quantum signature scheme includes three phases: the initial phase, the signature phase, and the verification phase. In the initial phase, all keys are prepared and distributed and, in particular, an entanglement is established among the communicators including the arbitrator. In the signature phase, a quantum signature is generated in association with the message and as a function of various quantum operations, keys, GHZ states and Bell measurements. The receiver verifies the authenticity of the quantum signature in the verification phase. Similar to classical arbitrated signature schemes, the verification of the quantum-arbitrated signature scheme also needs the help of the arbitrator. The proposed algorithm should be practicable in small networks (e.g., local rather than wide-spread network systems). The security analysis showed that the proposed scheme is unconditionally secure and may neither be disavowed by the signatory nor deniable by the receiver.

ACKNOWLEDGMENTS

This work was supported by the Alexander von Humboldt-Stiftung under Grant No. IV CHN 1069575 STP and by Deutsche Forschungsgemeinschaft (Nachwuchsgruppe within SFB 276).

[1] S. Wiesner SIGACT News **15**, 78 (1983); C.H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Advances in Cryptology*, Proceedings of Crypto'82 (Plenum Press, New York, 1982) p. 267.

[2] B. Schumacher, Phys. Rev. Lett. **80**, 5695 (1998).

[3] C. H. Bennett, and G. Brassard, *Advances in Cryptology*, Proceedings of Crypto'84 (Springer-Verlag, Berlin, 1984) p. 475; A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C.H. Bennett, *ibid.* **68**, 3121 (1992).

[4] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992); W.T. Buttler *et al.*, Phys. Rev. A **57**, 2379 (1998); P.W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[5] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[6] G. Zeng and W. Zhang, Phys. Rev. A **61**, 032303 (2000).

[7] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999).

[8] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (Wiley, New York, 1994).

[9] D. Greenberger, M.A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of Universe*, edited by M. Kaftos (Kluwer Academic, Dordrecht,1989); D. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[10] H. Meijer and S. Akl, *Advance in Cryptography*, Proceedings of Crypto'81 (Springer-Verlag, Berlin, 1981), p. 65.

[11] S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A **57**, 822 (1998).

[12] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[13] D. Bouwmeester, J. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).

[14] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

[15] A. Barenco, D. Deutsch, and A. Ekert, Phys. Rev. Lett. **74**, 4083 (1995).

[16] P.G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **75**, 4337 (1995).