Counterfactual quantum certificate authorization

Akshata Shenoy H.,† R. Srikanth,∗ and T. Srinivas†
†ECE Dept., Indian Institute of Science, Bangalore, India
∗PPISR, Bangalore, India

In counterfactual quantum cryptography, secure information is transmitted between two spatially separated parties even when there is no physical travel of particles transferring the information between them. We propose here a tripartite counterfactual quantum protocol for the task of certificate authorization. Here a trusted third party, Alice, authenticates an entity Bob (e.g., a bank) that a client Charlie wishes to securely transact with. The protocol is counterfactual with respect to either Bob or Charlie. We prove its security against a general incoherent attack, where Eve attacks single particles. We believe that this is the first instance of a multipartite protocol in the counterfactual paradigm.

I. INTRODUCTION

Suppose a client (Charlie) wishes to undertake a business transaction with a bank Bob. Charlie looks up Bob’s website via an internet search but is unsure of the website’s authenticity. His transaction requires him to securely transmit confidential information to Bob. A solution to this frequently encountered problem in e-commerce is certificate authorization (CA) where Alice, a well-known trusted third party (TTP) validates Bob’s website on request from Charlie. Classically, this task is accomplished via digital signatures and public-private keys [1, 2].

Alice, as a certificate authority, has a mutual agreement with a financial firm, whereby the latter provides her with the current information about Bob’s claimed online identity. Upon verifying that the website indeed belongs to Bob, Alice issues certificates in the form of digital signatures and public-private keys, thereby validating Bob’s website. Charlie can now transact with Bob using the latter’s certified public key. Alice keeps herself updated regarding the renewal/expiry of certificates and current information of the certificate holders. For example, if Bob changes the name of his website, the certificate issued to the website becomes invalid. To resume transactions, he needs to submit an application for a new certificate including legal documents supporting the change.

Here we wish to introduce a quantum method to accomplish the above described task in the counterfactual paradigm which we call counterfactual quantum certificate authorization (CQCA). Counterfactual quantum cryptography is based on the idea of interaction-free measurements, that involves communicating information even without the physical transmission of a particle, a point that is of foundational interest. Information is transferred by blocking rather than transmitting a particle. While this is also possible classically, but in the classical case, the blockade results in a particle detection near the blockade, whereas in the quantum case by virtue of single particle nonlocality, the particle may detected away from the blockade, which is the counterfactual element here. Counterfactual protocols use orthogonal states for encoding bits and experimental realization by others, including a fully counterfactual version of N09 protocol using a Mach-Zehnder interferometer set-up. The present authors proposed a semi-counterfactual quantum key distribution (QKD) protocol to clarify the origin of security in the counterfactual paradigm.

In the proposed CQCA protocol, Alice, in certifying Bob to Charlie, enables the latter two to share a secure random key. In this respect, the quantum version differs from classical CA, where Alice plays no role in the secure communication between Bob and Charlie. Thus the security must be considered with respect to both a malicious eavesdropper Eve as well Alice, who could overstep her CA role and try to eavesdrop on their transaction.

The article is structured as follows: In Section (II), a protocol for CQCA is presented. In Section (III), we prove its security in the case of a general incoherent attack by Eve, and a semi-honest Alice. In the section (IV), we provide a summary and conclusions.

II. A PROTOCOL FOR CA

Alice, Bob and Charlie are assumed to be online on both a conventional classical as well as a quantum network. He sends a classical request to certificate authority Alice, whose station is equipped with a single-photon source (SPS) and a beam splitter (BS) (Figure 1). After classically intimating Charlie and Bob, Alice initiates the protocol by transmitting to them a packet that consists of a single photon, which is split at BS into channels that lead to Bob and Charlie. We label these particles B and C. Note that each transmission packet will contain a header, body, and possible footer. The header contains instructions about the type of data the packet is carrying,
including packet length, packet number, the origin and destination of the packet. The footer consists of a couple of bits that indicate to the receiving device the termination of the packet. Thus, the header and the footer hold control information for negotiating the network, while the body will house the quantum data.

A single-photon of arbitrary polarization emitted from SPS is represented after BS by

\[ |\Psi\rangle_{BC} = \frac{1}{\sqrt{2}}(|0\rangle_B|\psi\rangle_C + i|\psi\rangle_B|0\rangle_C) \]  

where the first (second) ket refers to the transmitted (reflected) or Charlie (Bob) arm.

Bob and Charlie each possess a photon-number resolving detector \( D_B \) and \( D_C \), respectively, that absorbs the photon by process 3, and a Faraday mirror that applies operation \( F \), which is to reflect the photon without introducing additional phase. The operation \( A \) is assumed to be equipped with spectral filtering to time-resolve multiple photon arrivals. Each of the participants randomly applies the operation \( F \) (reflect) or \( A \) (absorb). The following possibilities arise: (1) Bob and Charlie both apply \( F \), which results in detection at the detector \( D_2 \) with probability \( 1/2 \); (2) Bob (Charlie) applies \( F \) (A) or vice versa. With probability \( 1/2 \) the particle is detected at \( D_1 \) or at \( D_2 \), and with probability \( 1/2 \), it is absorbed at Bob’s or Charlie’s end; (3) If Bob and Charlie both apply \( A \), there is necessarily a detection at one of their ends.

The corresponding probabilities are summarized in Table I. Bob and Charlie adopt the convention whereby Alice’s \( D_1 \) detection when they apply \( A\bar{F} \) \((\bar{F}A)\) corresponds to a 0 (1) secret bit. The efficiency of the protocol can be calculated as:

\[
P(D_1) = P(D_1|(F, A))P((F, A)) + P(D_2|(F, A))P((F, A)) = (1/4)(1/4) + (1/4)(1/4) = 1/8.\]

| (Bob/Charlie) F A | D_2, 1 | (D_1, 1/2), (D_2, 1/2), (NULL, 1/2) | (D_1, 1/2), (D_2, 1/2), (NULL, 1/2) |
|---------------|---------|--------------------------|--------------------------|
| F             |         | (D_1, 1/2), (D_2, 1/2),  | (NULL, 1/2)              |
| A             |         | (D_1, 1/2), (D_2, 1/2),  | (NULL, 1/2)              |

TABLE I: Probabilities for outcomes corresponding to Bob’s and Charlie’s actions.

We present the basic protocol: (1) Upon receiving Bob’s classical, authenticated request and Charlie’s consent, Alice injects \( n \) single photons sequentially into the input port of BS; (2) Bob and Charlie randomly apply operations \( F \) or \( A \) in the arm \( B \) and \( C \), respectively; (3) On the \( n \) outcome data collected, a fraction \( nf \) (where \( f < 1 \)) is randomly selected by Bob and Charlie (by discussion over an authenticated classical channel), for which they ask Alice to announce her detection data (which can be NULL, \( D_1 \) or \( D_2 \)). Bob and Charlie announce their settings \( (A \text{ or } F) \) and outcome (in case of \( A \), as to whether a photon was registered or not in their respective detector \( D_B \) or \( D_C \)) information. Bob and Charlie determine whether the obtained experimental data is sufficiently close to the probabilities in Table I. If yes, then the anti-correlated settings corresponding to the \( D_1 \) detections form a secure key shared between them. The protocol is fully counterfactual in the sense that when a secret bit is generated due to \( D_1 \) detections, the photon would not have physically travelled along one of the arms, i.e., it did not physically travel via the Bob arm or Charlie arm, even though both their choices contribute to the bit generation.

The closeness of the experimental data to the pattern in the table is estimated using the figures of merit given below:

**Coincidence check.** They verify that the fraction of coincidence detections when both Bob and Charlie apply \( A \)

\[
\kappa = P(D_B D_C|AA) \]  

is sufficiently close to 0.

**Visibility check.** The visibility of the interference fringes

\[
\mathcal{V} = \frac{P(D_2|FF) - P(D_1|FF)}{P(D_1|FF) + P(D_2|FF)} \]  

must be sufficiently close to 1.

**Bias check.** The bias in Alice’s outcomes when their settings are anti-correlated

\[
B = \max\{|P(D_1|AF) - P(D_2|AF)|, |P(D_1|FA) - P(D_2|FA)|\} \]  

must be sufficiently close to 0.

**Determining error rate.** The secret bits shared between Bob and Charlie are generated precisely when a honest Alice announces a \( D_1 \) detection, for ideally in this case their inputs are anti-correlated. Deviation from this pattern allows them estimate the error rate on the raw key:

\[
e = P(FF|D_1) + P(AA|D_1), \]  

which must be sufficiently close to 0.

**Estimating multi-photon pulses and channel losses.** Two other figures of merit are estimates on \( r \), the rate of multiple count, which may be due to dark counts or certain photon-number non-preserving attacks [22], and \( \lambda \), transmission loss rate over the channel.

(5) In the above, if any of \( \kappa, \mathcal{V}, B, e \) and the other figures of merit are not sufficiently close to their expected value, then Bob and Charlie abort the protocol run. Otherwise, the remaining approximately \((1 - f)n/8\) bits corresponding to Alice’s \( D_1 \) detection are used for further classical post-processing to extract a smaller secure key via key reconciliation and privacy amplification.
If she receives it back, then Bob applied launch such an attack, by sending a particle to Bob alone. Initial secret bit is 0. Suppose, irrationally, that she does arm, since although she gains full information on either arm, since she gains nothing by sending photons along a single arm. Thus, in principle, we may assume that she is random, but and Charlie's choices deterministically according to whether the respective particle returns to her or not. This is foiled by the coincidence check, where Bob and Charlie would find coincidence counts when they apply AA.

Alice gains nothing by sending photons along a single arm, since although she gains full information on either Bob or Charlie's choice, she would know nothing about the other's choice, so that her information on the potential secret bit is 0. Suppose, irrationally, that she does launch such an attack, by sending a particle to Bob alone. If she receives it back, then Bob applied F, and if not, he applied A. In the latter case, in step (3) of the protocol, the only outcome consistent with the experiment is that Alice should announce NULL, given that Bob has a detection. Hence no secret bit is generated.

Now, in the former case, Charlie may have applied F or A with equal probability. Further, in the second case, Charlie couldn't have detected a particle. If we now consider the cases FA and FF such that Charlie did not detect a photon on DC, then Alice should obtain outcome D1 with probability $P(C\rightarrow A)P(D1|FA') + P(C\rightarrow F)P(D1|FF) = \frac{1}{4}P(D1|FA') + \frac{3}{4}P(D1|FF) = \frac{1}{4} + 0 = \frac{1}{4}$, and outcome D2 with probability $P(C\rightarrow A)P(D2|FA') + P(C\rightarrow F)P(D2|FF) = \frac{1}{4}P(D2|FA') + \frac{3}{4}P(D2|FF) = \frac{1}{4} + \frac{3}{4} = \frac{3}{4}$, where $A'$ denotes that Charlie applied A and did not detect a photon. Now Alice needs to fake the statistics to be compatible with the honest protocol. Suppose Alice randomly generates numbers 0 and 1 with probability $\frac{1}{2}$ and $\frac{3}{4}$, and announces D1 (D2) when she obtains 0 (1). Her announcement of D1 will deterministically lead to an error if Charlie had applied F (since $P(D1|FF) = 0$). In this fake attack, Alice does not know what Charlie's operation was irrespective of whether she outputs D1 or D2, and so $P(C \rightarrow F|D1) = \frac{1}{2}$. An analogous argument applies if Alice sends a particle to Charlie alone. Thus if Alice transmits such single-path particles to Bob or Charlie with probability $p$, then from Eq. (5), Table I, we see that Bob and Charlie will detect an error with probability $e = P(A \rightarrow D1) = p \frac{1}{2} = \frac{p}{2}$. To counter this, Alice may choose to announce only $D2$, in which case $e = 0$, but bias $B = 2 \times \frac{p}{4} = \frac{p}{2}$.

III. SECURITY

Unlike in classical CA, where Alice only certifies the digital signature and is by definition trustworthy, in the present quantum case, Alice participates in the key generation. Thus, in principle, we may assume that she is not to be trusted. More precisely, her action may be characterized as semi-honest in that she fulfills her CA role per the honest protocol, but may collude with Eve (Section IIIA) to extract key information. Our study of the proof of security therefore first examines protection against a semi-honest Alice, while Section IIIB considers the case of dishonest Eve.

### A. Security against Alice-Eve

To eavesdrop, suppose Alice transmits single photons along both arms B and C, and infer Bob’s and Charlie’s choices deterministically according to whether the respective particle returns to her or not. This is foiled by the coincidence check, where Bob and Charlie would find coincidence counts when they apply AA.

Alice gains nothing by sending photons along a single arm, since although she gains full information on either Bob’s or Charlie’s choice, she would know nothing about the other’s choice, so that her information on the potential secret bit is 0. Suppose, irrationally, that she does launch such an attack, by sending a particle to Bob alone. If she receives it back, then Bob applied F, and if not, he applied A. In the latter case, in step (3) of the protocol, the only outcome consistent with the experiment is that Alice should announce NULL, given that Bob has a detection. Hence no secret bit is generated.

Now, in the former case, Charlie may have applied F or A with equal probability. Further, in the second case, Charlie couldn’t have detected a particle. If we now consider the cases FA and FF such that Charlie did not detect a photon on DC, then Alice should obtain outcome D1 with probability $P(C\rightarrow A)P(D1|FA') + P(C\rightarrow F)P(D1|FF) = \frac{1}{4}P(D1|FA') + \frac{3}{4}P(D1|FF) = \frac{1}{4} + 0 = \frac{1}{4}$, and outcome D2 with probability $P(C\rightarrow A)P(D2|FA') + P(C\rightarrow F)P(D2|FF) = \frac{1}{4}P(D2|FA') + \frac{3}{4}P(D2|FF) = \frac{1}{4} + \frac{3}{4} = \frac{3}{4}$, where $A'$ denotes that Charlie applied A and did not detect a photon. Now Alice needs to fake the statistics to be compatible with the honest protocol. Suppose Alice randomly generates numbers 0 and 1 with probability $\frac{1}{2}$ and $\frac{3}{4}$, and announces D1 (D2) when she obtains 0 (1). Her announcement of D1 will deterministically lead to an error if Charlie had applied F (since $P(D1|FF) = 0$). In this fake attack, Alice does not know what Charlie’s operation was irrespective of whether she outputs D1 or D2, and so $P(C \rightarrow F|D1) = \frac{1}{2}$. An analogous argument applies if Alice sends a particle to Charlie alone. Thus if Alice transmits such single-path particles to Bob or Charlie with probability $p$, then from Eq. (5), Table I, we see that Bob and Charlie will detect an error with probability $e = P(A \rightarrow D1) = p \frac{1}{2} = \frac{p}{2}$. To counter this, Alice may choose to announce only $D2$, in which case $e = 0$, but bias $B = 2 \times \frac{p}{4} = \frac{p}{2}$.

### B. Security against Eve

The above checks rule out Alice from deviating from the honest protocol, though she may still collude with Eve (i.e., Alice is constrained to be semi-honest). We assume that Eve operates under the assumption that all pulses are single-photon pulses. This is because multi-photon pulses potentially lead to deviation from perfect anti-correlation between Bob and Charlie, and hence are not useful even for the legitimate parties. The last check mentioned above is intended for this purpose.

We discuss the attack scenario where Eve attacks each run individually, by entangling the light along both the arms with a separate probe positioned near either arm. These probes $E_1$ and $E_2$ are prepared in the initial ready state $|R\rangle_{E_1}|R\rangle_{E_2}$. During the transmission from Alice to Bob-Charlie, Eve applies the (number-preserving) interaction [22] on the joint $BE_1$ and $CE_2$ systems:

$$K = \ket{0}_j \langle 0 \otimes K_0 + \ket{1}_j \langle 1 \otimes K_1, \tag{6}$$

such that $\langle 0|K_1^+K_0|0\rangle \equiv \langle y|m \rangle = \cos(\theta_j)$, where $j \in \{B,C\}$. For simplicity, we assume $\theta_B = \theta_C = \theta$. This
interaction produces the state:

\[
|\Psi\rangle_{BCE} = \mathcal{K}|\Psi\rangle_{BC}|RR\rangle_E = \frac{1}{\sqrt{2}}(|\psi\rangle_B|0\rangle_C|y,n\rangle_E
+ |0\rangle_B|\psi\rangle_C|n,y\rangle_E),
\]

where we use the notation \( E \equiv E_1E_2 \). The Bob-Charlie action \((F,F)\) leaves the \(|\Psi\rangle_{BCE}\) unchanged. In the case of Bob and Charlie applying \((F,A)\), the resulting states are \(\frac{1}{\sqrt{2}}|0\rangle_B|0\rangle_C|y,n\rangle_E \) or \(\frac{1}{\sqrt{2}}|\psi\rangle_B|0\rangle_C|y,n\rangle_E\), of which the former implies detection by Bob and the latter leads potentially to a \(D_1\) detection for secret bit 1. In the case of \((A,F)\), the resulting states are \(\frac{1}{\sqrt{2}}|0\rangle_B|0\rangle_C|y,n\rangle_E \) or \(\frac{1}{\sqrt{2}}|\psi\rangle_B|0\rangle_C|n,y\rangle_E\), of which the former implies detection by Charlie and the latter leads potentially to a \(D_1\) detection for secret bit 0. The attack does not affect the probability for secret bit generation, which remains, as in Table I

\[
P(D_1|AF) = P(D_1|FA) = \frac{1}{4} \quad \text{(8)}
\]

That Eve does not gain on attacking the return leg applies here too as in semi-counterfactual QKD [22].

Thus, the most general incoherent number preserving attack (which entails channel’s losslessness) that Eve can launch would be to use the above onward leg attack, and then measure her probe \(E_1E_2\) after Alice’s announcement. The timings of pulses transmitted by Alice must be random, for if Eve knew the transmission schedule, she would use a Alice-like set-up to probe Bob’s or Charlie’s setting by inserting a photon into the stream \(B\) or \(C\) in synchrony with Alice, and checks if it returns or not. In principle, this trojan horse attack can be detected using spectral filtering [13]. An alternative is to exploit the fact that coding here is not polarization-based, and to use a Bennett-Brassard-1984-like [23] check [22]. However, the security here is undermined if Alice colludes with Eve by supplying her with the polarization information.

In our analysis, we assume the worst-case scenario where Eve has complete knowledge of the transmission schedule between Alice and Bob. Thus she times her attack to happen just when the particle is about to enter Bob’s station, and completes it after Alice’s announcement of \(D_1\) detection events.

Eve jointly measures her probes \(E_1\) and \(E_2\), the information she extracts being dependent on her ability to distinguish between states \(|y,n\rangle_E\) and \(|n,y\rangle_E\). From Eq. (7) an upper bound on her information is the Holevo quantity

\[
\chi(\theta) = S\left(\frac{\Pi_{|y,n\rangle} + \Pi_{|x,n\rangle}}{2}\right) = \frac{1}{2} \left[S\left(\Pi_{|y,n\rangle}\right) + S\left(\Pi_{|y,n\rangle}\right)\right],
\]

where \(S(\cdot)\) denotes von Neumann entropy and \(\Pi_{|x\rangle}\) the projector to state \(|x\rangle\). The square-bracketed quantity in Eq. (9) vanishes because of the purity of the considered states. The reduced density matrix of \(E_1E_2\) in Eq. (7) is:

\[
\rho_E = \frac{1}{2} \begin{pmatrix}
2\cos^2(\theta) & \cos(\theta)\sin(\theta) & \cos(\theta)\sin(\theta) \\
\cos(\theta)\sin(\theta) & \sin^2(\theta) & 0 \\
\cos(\theta)\sin(\theta) & 0 & \sin^2(\theta)
\end{pmatrix},
\]

in the basis \(\{|y,y\rangle,\{|y,y\rangle,\{|y,y\rangle,\{|y,y\rangle\}\}, leaving out \(|y^+,y\rangle\), which lies outside the support of \(\rho_E\). The above matrix is of rank 2, whose non-vanishing eigenvalues are \(e_1 = \frac{1}{2}(1-\cos(2\theta))\) and \(e_2 = \frac{1}{4}(3 + \cos(2\theta))\), so that Eve’s information \(I_E \equiv I_{BE} = I_{CE}\), using Eq. (9), is

\[
I_E \leq \chi(\theta) = H(e_1) = H\left(\frac{1 - \cos(2\theta)}{4}\right),
\]

where \(H(x) \equiv -x \log_2(x) - (1 - x) \log_2(1 - x)\) denotes the Shannon binary entropy.

Let us consider the disturbance caused by Eve. In the given direction of polarization of the photon, Alice’s beam splitter may be represented as:

\[
d_1^i = \frac{1}{\sqrt{2}}(b^i + ic^i), \quad d_2^i = \frac{1}{\sqrt{2}}(b^i - ic^i),
\]

where \(a^i, b^i\) are the creation operators for the modes \(A,B\), respectively, and \(d_1^i\) and \(d_2^i\) are creation operators corresponding to detections at \(D_1\) and \(D_2\), respectively. Hence, the state \(|\phi\rangle_{AB}\) evolves to

\[
|\Psi\rangle \rightarrow \frac{1}{\sqrt{2}} \left(|\langle D_1| + |D_2\rangle|_{BC} |y,n\rangle_E
+ \frac{|\langle D_1| - |D_2\rangle|_{BC} |n,y\rangle_E}{\sqrt{2}}\right),
\]

from which, it follows that

\[
\text{Prob}(D_2|FF) = \frac{1}{4}||\langle y,n\rangle_E - |n,y\rangle_E||^2
= \frac{1}{2} \sin^2(\theta).
\]

We thus find that the visibility \(\mathcal{V}\), conditioned on both applying \(F\), falls from 1 to

\[
\mathcal{V} = \frac{1 + \cos(2\theta)}{2},
\]

where, by the assumption of channel losslessness, \(P(D_1|FF) + P(D_2|FF) = 1\). The error rate \(e\) in Eq. (3) becomes, by Bayesian rule,

\[
e = \frac{P(FF|D_1)}{P(D_1)} = \frac{P(D_1|FF)P(FF)}{P(D_1)}
= \frac{\sin^2(\theta)}{1 + \sin^2(\theta)},
\]

so that the mutual information between Bob and Charlie is

\[
I_{BC} = 1 - H(e).
\]
FIG. 2: The falling curve represents $I_B = I_C$ (in this symmetric model, where Eve attacks both arms with the same strength, parametrized by $\theta$), while the rising curve represents $I_E$.

The condition for positive key rate in the protocol is

$$K = I_{BC} - \min\{I_{BE}, I_{CE}\} > 0, \quad (18)$$

where $K$ is the secret bits that can be distilled after Bob and Charlie perform key reconciliation and privacy amplification. The security condition (18) becomes, from Eqs. (11), (16) and (17),

$$H\left(\frac{1 - \cos(2\theta)}{4}\right) + H\left(\frac{\sin^2(\theta)}{1 + \sin^2(\theta)}\right) < 1, \quad (19)$$

or $\theta \lesssim 0.42$ rad, which, in view of Eq. [16], implies $e \lesssim 14.25\%$ (see Figure 2).

IV. DISCUSSION AND CONCLUSIONS

Here we have have extended the concept of counterfactual cryptography to the multipartite scenario, by introducing the task which is the quantum version of CA. We have analyzed its security against general incoherent attacks. A practical implementation of the present protocol is feasible, given the existing experimental realization of counterfactual QKD [17, 21]. CQCA can also be derived from the N09 protocol, just as the present protocol is derived from the semi-counterfactual QKD protocol of Ref. [22]. The latter offers a practical advantage over the former in that it does not use polarization encoding, unlike the former. We remark that a non-counterfactual quantum CA (QCA) scheme can be obtained using two-particle entanglement and the idea of a cryptographic switch [25]. It will be interesting to study the security of such a protocol, as compared with the present CQCA scheme.

[1] R. L. Rivest, Lecture notes in computer science 1465, 178 (1998).
[2] L. M. Kohnfelder, Ph.D. thesis, Massachusetts institute of technology (1978).
[3] G.-C. Guo and B.-S. Shi, Phys. Lett. A 256, 109 (1999).
[4] T.-G. Noh, Phys. Rev. Lett. 103, 230501 (2009).
[5] H. Salih, Z.-H. Li, M. Al-Amri, and M. S. Zubairy, Phys. Rev. Lett. 110, 170502 (2013).
[6] A. C. Elitzur and L. Vaidman, Found. of Phys. 23, 987 (1993).
[7] P. G. Kwiat, A. G. White, J. R. Mitchell, O. Nairz, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. 83, 4725 (1999).
[8] A. S. H. and R. Srikanth (2013), arXiv:1311.7127.
[9] L. Goldberg and L. Vaidman, Phys. Rev. Lett. 75, 1239 (1995).
[10] A. Avella, G. Brida, I. P. Degiovanni, M. Genovese, M. Gramegna, and P. Traina, Phys. Rev. A 82, 062309 (2010).
[11] M. Koashi and N. Imoto, Phys. Rev. Lett. 79, 2383 (1997).
[12] Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han, and G.-C. Guo, Phys. Rev. A 82, 042335 (2010).
[13] S. Zhang, J. Wang, and C. J. Tang, Europhys. Lett. 98, 30012 (2012).
[14] S. Zhang, J. Wang, C. jing Tang, and Q. Zhang, Chin. Phys. B 21, 060303 (2012).
[15] Z.-Q. Yin, H.-W. Li, Y. Yao, C.-M. Zhang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A 86, 022313 (2012).
[16] Y. Sun and Q.-Y. Wen, Phys. Rev. A 82, 052318 (2010).
[17] M. Ren, G. Wu, E. Wu, and H. Zheng, Laser Phys. 21, 755 (2011).
[18] G. B. Xavier and J. P. V. der Weid, Opt. Lett. 36, 1764 (2011).
[19] G. B. Xavier, T. R. da Silva, G. T. T. ao, and J. P. V. der Weid, Elec. Lett. 47, 608 (2011).
[20] M. Jiang, S. Sun, and L. Liang, Journal of Quantum Info. Sc. 1, 116 (2011).
[21] G. Brida, A. Cavanna, I. P. Degiovanni, M. Genovese, and P. Traina, Laser Phys. Lett. 9, 247 (2012).
[22] A. S. H., R. Srikanth, and T. Srinivas, Euro Phys. Lett. 103, 60008 (2013).
[23] C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore (1984), p. 175.
[24] I. Csizár and J. Körner, IEEE Trans. Inf. Theory 24, 339 (1978).
[25] N. Srinatha, S. Omkar, R. Srikanth, S. Banerjee, and A. Pathak (2012), qu. Info. Proc.: DOI 10.1007/s11128-012-0487-3.