Entanglement-based quantum communication prevents tracking the message sender

Michael Siomau

Physics Department, Jazan University, P.O. Box 114, 45142 Jazan, Kingdom of Saudi Arabia

(Dated: August 21, 2014)

PACS numbers: 03.67.Hk, 03.65.Ud

The possibility to attain the current position of the message sender without person’s consent seriously compromises the secrecy of correspondence. Classical communication systems cannot guarantee the security of communication against unwanted tracking, because the sender must broadcast a signal to send a message. The source of the signal could be always located, at least in principle. Quantum communication, as we show here, enables sending the message by local manipulations with pre-distributed entangled quantum systems and without transmitting any physical signal and, therefore, secure the sender’s location.

Application of quantum systems for communication surpasses classical ways of exchanging information in its security [1]. The fundamental no-cloning principle [2, 3] on a par with probabilistic nature of quantum measurements guarantee unconditional security of quantum communication [4]. However, it has been never analyzed how quantum communication changes the problem of positioning the message sender. Clearly, if the communication parties use single quantum systems, for example photons, to communicate, the sender must broadcast a signal to send a message and, therefore, could be located by standard methods, such as triangulation. We show that the use of quantum nonlocality [5], i.e. entangled states, for communication dramatically change our ability to reveal sender’s location without her/his permission. We present a family of simple protocols for transmitting classical and quantum information, where the message is sent by means of local manipulations and measurements on pre-distributed entangled systems and series of on-off detection events. In contrast to standard methods of communication with entangled states [1], suggested protocols never require the sender to broadcast a physical signal during the message transmission preventing any possibility of unpermitted positioning.

In general, the exchange of information requires pre-distribution of some communication resource between partners, such as addresses, devises or physical systems. Although during this exchange the location of the partners is of no secret, the distribution of the physical resource does not contain any information about future communication.

Suppose, the sender and the receiver, traditionally named Alice and Bob, share a sequence of entangled qubit pairs [4], so that each qubit pair is independent from the others and is initially prepared in a Bell state

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0_a0_b\rangle + |1_a1_b\rangle), \tag{1}$$

where basis states $|0_i\rangle$ and $|1_i\rangle$ of the qubits $i = a, b$ could be associated with polarization states of photon.

Alice wants to send a message to Bob, but is unwilling to reveal her location. Immediately after the distribution of the entangled pairs Alice’s location is known for Bob. In order to postpone the communication until Alice’s location changes, the partners may store their qubits in a quantum memory [6]. Alternatively, Alice may request assistance from the third party – Charlie. She may share entangled states with Charlie and ask him to distribute independent entangled states with Bob and to perform operation known as entanglement swapping [7]. In this case, Alice and Bob share entangled states, while they never directly communicated. Although Charlie may have some information about Alice’s location, it is secret for Bob.

Having distributed the entangled qubit pairs, Alice may start the communication at her convenience. Let us assume first that Alice wants to send classical information, i.e. a bit string. She measures first qubit from her qubit sequence in $\{|0\rangle, |1\rangle\}$ basis obtaining binary value 0 or 1 with equal probability. Alice’s action leads to the collapse of the two-qubit wave function (1) and the detection of the other qubit from the pair by Bob. If they use the same basis (and we assume so), the results of their measurements are identical and random. Let say they obtained 0. The first measurement indicates the beginning of data transmission to Bob. He broadcasts publicly ‘OK’ (confirming receiving the bit) and repeats cyclically with some time interval $t$ the names of two operations: leave the result as it is (L) or invert it (I). Depending on the value of the first bit in Alice’s message, she chooses suitable moment of time to measure the second qubit in her sequence giving Bob the answer what to do with the first bit and sending the second random bit at the same time (see Figure [1]). Bob acknowledges receiving the second bit by broadcasting ‘OK’. This indicates to Alice that the transmission was successful. Any detection event that does not fit timing of the intervals is recognized as a mistake, which could appear, for example, due to detectors noise or imperfections of the entangled pairs. The time interval is to be chosen to ensure that Alice receives Bob’s broadcast. Currently, it is possible to distribute entangled systems in free space for distances over 144 km [8]. Therefore, the time interval should be at least $t = 144/c \approx 5 \times 10^{-4}$ s, where $c$ is the speed of light. There is no need to take into account the speed of the wave function collapse, because theory predicts it to
The above protocol for classical information transmission could be modified to avoid Bob’s public broadcast at all. During the stage of the entangled pairs distribution, Alice and Bob agree on the time interval \( t \) and the order of operations they will count. After that, they organize their qubit sequences in blocks, so that each block contains two entangled pairs. While Alice sends the first bit of her message initiating the data transmission, Bob responds by measuring the second qubit from the first block. By doing this, Alice and Bob synchronize their local watches and start counting. Subsequently, the first qubit pair from each block is used by Alice to send the message, while the second is used by Bob to confirm receiving the message (see Figure 1b). In this protocol neither Alice nor Bob broadcast any signal during the data transmission, i.e. they both preserve their locations in secret.

The second protocol has lower transmission capacity comparing to the first one: while one qubit pair per bit is needed to communicate within the first protocol, two qubit pairs per bit are used in the second. However, if the second protocol is in use, there are very little demands on the quality of the qubit pairs exploited by Bob, because the communication parties do not utilize the results of measurements on these qubits to send the message. In case the distributed entangled pairs are corrupted by decoherence, Alice and Bob may apply the entanglement distillation \([10]\) to increase the amount of entanglement in the first entangled pair from the block by reducing the entanglement of the second pair from the same block.

General quantum information processing emerges the necessity to transmit arbitrary quantum states instead of classical bits. The first communication protocol should be thus modified to allow Alice to send qubits. Alice and Bob arrange their qubit sequences in blocks so that each block contains two entangled pairs. Alice measures the first qubit from the first block initiating the data transmission and prepares this qubit in the state she wants to transmit. After that she teleports the state to Bob using the second entangled pair from the first block.

To teleport an arbitrary qubit state \( |\chi\rangle \) to Bob, Alice performs Bell measurement on the two-qubit system consisting of this qubit \( |\chi\rangle \) and one qubit from the entangled pair \([11]\). Due to Alice’s action, Bob’s qubit (i.e. the other qubit from the entangled pair) is instantaneously projected into one of four states \( |\chi\rangle, X|\chi\rangle, Z|\chi\rangle \) or \( XZ|\chi\rangle \), where \( X \) and \( Z \) are the Pauli operators \([4]\). Alice must inform Bob, which of the four unitary transformations \( U_1 = I, U_2 = X, U_3 = Z, U_4 = ZX \), where \( I \) – the identity operator, he needs to perform on his state to obtain the original qubit state \( |\chi\rangle \).

Detecting the first qubit from his qubit sequence, Bob knows that the first quantum state is to be teleported. He broadcasts the labels of four operations that could be performed on the teleported state to obtain the submitted state. Operating with the second block at suitable time, Alice tells Bob what to do with the first teleported qubit (see Figure 2).

Interestingly, the method of signalling by disentangling qubit pairs is widely used in quantum interferometry \([12]\). For example in the classical experiment for quantum teleportation, Bouwmeester et al. used so-called trigger photon to indicate that a quantum state is under way \([13]\). However, the measurement of one of the qubits from an entangled pair has never been used to send classical information about operations that need to be performed of the results of the measurements.

The protocol for quantum information transmission could be further improved to avoid Bob’s broadcast, in the same way as the second protocol for classical information transmission improves the first one. Alice and Bob arrange their qubit sequences in blocks of three entangled pairs: the first pair is used by Alice to signal Bob, the second is spent for teleportation, while the third is exploited by Bob to communicate back to Alice.

Although the suggested protocols ensure security of the message sender’s location, the security of the transmitted message is conditioned. Because it is generally assumed that the third party, the eavesdropper typically named Eve, can not directly access the results of Alice’s and Bob’s measurements, the security of the transmitted data fully relies on the security of the entangled pair distribution. To ensure the security of the latter, Alice and
Bob could perform standard methods for quantum error correction and security amplification on the entangled states during the stage of their distribution [4]. If, nevertheless, Eve succeeds to access \( n \) random qubit pairs, for example, by entangling her probe with the entangled states shared by Alice and Bob, she could get at most \( n/4 \) (qu-)bits of the message, in case of the communication by the first protocol for classical data transmission and the protocol for quantum information transmission; and up to \( n/8 \) bits, if Alice and Bob use the second protocol for classical data transmission. Eve gets such a small portion of information, because only the event of the next (qu-)bit transmission makes the previous result meaningful. Eve gains maximal information about the message, if she access \( n \) qubit pairs in a row. This type of intrusion, however, causes serious disturbance of the continuous sequence of the intercepted entangled pairs, which could be easily detected by the authorized partners during the distribution of the entangled pairs.

In spite of their conceptual simplicity, practical implementation of the suggested protocols may be challenging with current technologies. Although pre-distribution of the perfect entangled pairs, which are pre-requisite for the protocols, could be accomplished by entanglement purification and entanglement distillation protocols [10], it is difficult to preserve the entangled pairs till the communication, because of absence of high efficiency quantum memory. Nevertheless, rapid development of quantum technologies suggest that such a quantum memory may be available in the nearest future [6].

The secrecy of correspondence is very intimate issue in the modern world. To date, the presented protocols are the only communication protocols that physically guarantee the security of the message sender’s location and may offer, at the same time, the secure data transmission. The combination of both mentioned factors manifests a new goal of quantum communication – the complete secrecy of correspondence.

Acknowledgments

I’m grateful to Ali Al-Kamli for his support and encouragement during this project. This work is supported by KACST under research grant 34-37.

\[ \text{FIG. 2: The protocol for quantum information transmission. Alice uses two qubit pairs to send a quantum state: one qubit pair – for signalling Bob, the other for teleportation. Each detection event tells Bob what to do with previously received state.} \]

[1] N. Gisin and R. Thew, Nat. Photon. 1, 165 (2007).
[2] W.K. Wootters and W.H. Zurek, Nature 299, 802 (1982).
[3] D. Dieks, Phys. Lett. A 92, 271 (1982).
[4] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information (Cambridge Univ. Press, Cambridge, 2000).
[5] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. 47, 777 (1935).
[6] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S.J. Dewhurst, N. Gisin, C.Y. Hu, F. Jelezko, S. Kröll, J.H. Müller, J. Nunn, E. Polzik, J. Rarity, H. de Riedmatten, W. Rosenfeld, A.J. Shields, N. Skold, R.M. Stevenson, R. Thew, I. Walmsley, M. Weber, H. Weinfurter, J. Wrachtrup and R.J. Young, Eur. Phys. J. D 58, 1 (2010).
[7] M. Żukowski, A. Zeilinger, M.A. Horne and A.K. Ekert, Phys. Rev. Lett. 71, 4287 (1993).
[8] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodniks, C. Barbieri, H. Weinfurter and A. Zeilinger, Nat. Phys. 3, 481 (2007).
[9] J. Yin, Y. Cao, H.-L. Yong, J.-G. Ren, H. Liang, S.-K. Liao, F. Zhou, C. Liu, Y.-P. Wu, G.-S. Pan, Q. Zhang, C.-Z. Peng and J.-W. Pan, Phys. Rev. Lett. 110, 260407 (2013).
[10] C.H. Bennett, G. Brassard, B. Schumacher, J.A. Smolin, W.K. Wootters, Phys. Rev. Lett. 76, 722 (1996).
[11] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K. Wootters, Phys. Rev. Lett. 70, 1895 (1993).
[12] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger and M. Żukowski, Rev. Mod. Phys. 84, 777 (2012).
[13] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Nature 390, 575 (1997).