Quantum Inf Process (2013) 12:149–155
DOI 10.1007/s11128-012-0363-1

# Improving security of the ping-pong protocol

**Piotr Zawadzki**

Received: 19 October 2011 / Accepted: 17 January 2012 / Published online: 2 February 2012


**Abstract** A security layer for the asymptotically secure ping-pong protocol is proposed and analyzed in the paper. The operation of the improvement exploits inevitable errors introduced by the eavesdropping in the control and message modes. Its role is similar to the privacy amplification algorithms known from the quantum key distribution schemes. Messages are processed in blocks which guarantees that an eavesdropper is faced with a computationally infeasible problem as long as the system parameters are within reasonable limits. The introduced additional information preprocessing does not require quantum memory registers and confidential communication is possible without prior key agreement or some shared secret.

**Keywords** Quantum cryptography · Quantum secure direct communication · Privacy amplification · Ping-pong protocol

## 1 Introduction

A paradigm of quantum secure direct communication (QSDC) has been studied for the last decade [1]. QSDC protocols are designed for transmission of classic information over quantum channels but contrary to quantum key distribution (QKD) schemes, they do not require prior key agreement for confidentiality provision. The so called ping-pong protocol [2] has attracted a lot of attention, as it is provably asymptotically secure in lossless channels [3]. It has been also shown that protocol variants based on higher dimensional systems and exploiting superdense information coding also share this feature [4,11,12,15]. The problem with the ping-pong protocol security lies in

P. Zawadzki (✉)
Institute of Electronics, Silesian University of Technology, Akademicka 16, 44-100 Gliwice, Poland
e-mail: Piotr.Zawadzki@polsl.pl

the fact that the offered eavesdropping detection probability per signal particle is too low [11,15]. In effect, an eavesdropper is detected with a reasonably probability only for sufficiently long sequences. In practice, such protocols cannot be used because an eavesdropper can intercept some part of the message before he is detected. To cope with this problem a two-step and/or batch processing of qubits has been proposed [5,9,12,13]. As an alternative, some additional quantum processing analogous to privacy amplification in QKD protocols has been proposed [7]. However, those solutions are not implementable with the current technology because of the requirement of the large photonic quantum memory registers [6].

The estimated security of the ping-pong protocols is even worse in noisy environments when legitimate users tolerate some level of transmission errors and/or losses. If that level is too high compared to the quality of the channel, then an eavesdropper can peek some fraction of signal particles hiding himself behind accepted quantum bit error rate (QBER) threshold [14,16]. But the possibility to intercept some part of the message without being detected renders the protocol insecurity. However, the ping-pong protocol is still an interesting object of further investigations, despite its problems with the level of the offered security level, as its remains one of not too many QSDC protocols that have laboratory implementations [10].

The method to overcome the difficulties summarized above is presented in the paper. The proposed supplementing of the ping-pong protocol with a properly designed message pre- and post-processing steps can assure the security on the level required by a given application. Although in the considered improvement the message is processed by blocks, the main advantage of the proposed approach is the elimination of quantum registers. Thus the improved protocol can be, in principle, realized in practice. Moreover, in the resulting protocol, contrary to many others QSDC protocols, the noise in quantum channel works in advantage to the legitimate users improving the security of communication. It is shown that Eve is faced with a computationally infeasible problem as long as the quality of the quantum communication falls within a prescribed margin. This renders that Eve intercepts no useful information and the improved protocol is secure.

## 2 The ping-pong protocol in short

Let us consider the seminal version of the ping-pong protocol [2] in which the message and control mode are executed only in computational basis. The communication process is started by Bob, the recipient of information, who prepares two maximally entangled qubits. Without loss of generality it may be assumed that they are in the state

$$|\psi^+\rangle = \left(|0\rangle_t|1\rangle_h + |1\rangle_t|0\rangle_h\right)/\sqrt{2} \tag{1}$$

One of the qubits, denoted as “home”, is kept confidential, while the second one, named the “travel”, is sent to Alice via publicly accessible quantum channel. Alice randomly selects message mode or control mode. In message mode she applies to the travel qubit a transformation $Z^{\mu}$

$$Z^{\mu}|k\rangle_t = (-1)^{k\mu}|k\rangle_t \tag{2}$$

where $k = 0, 1$ and $\mu$ denotes the value of the encoded classic bit. The entanglement of qubits causes that Alice's local operations have non local effects. The system composed from the home and travel qubits is left unchanged or transformed into another maximally entangled state

$$|\psi^{-}\rangle = \left(|0\rangle_t|1\rangle_h - |1\rangle_t|0\rangle_h\right)/\sqrt{2} \tag{3}$$

Next, the travel qubit is sent back to Bob, who performs collective measurement on both qubits.

Malicious Eve may try to intercept some information encoded by Alice. Her actions are perceived by legitimate users as noise and/or losses, so a special control mode is used for the eavesdropping detection. Alice switches to the control mode in some randomly selected protocol cycles. In this mode she measures the received travel qubit and the fact of switching is announced via public classic channel. It is assumed that although public information is accessible to Eve, she can't control its content. It follows that Alice and Bob have to be able to check authenticity of the classic data what in turn implies that legitimate parties share some key or the classic channel is authenticated by some other means. Bob subsequently measures the home qubit and asks Alice to reveal the value of her measurement. Because of the fragile entanglement of the two-qubit system the result of Bob's measurement is fully determined by the value obtained by Alice. Any deviation from that correlation indicates the presence of Eve. It has been shown [2,3] that Eve by measuring the travel qubit and the ancilla can intercept at most $I(d) = -d\log_2 d - (1-d)\log_2(1-d)$ bits, where $d$ denotes eavesdropping detection probability. Thus, to intercept non-zero information she has to risk detection in the control mode. As a result the protocol is asymptotically secure—Eve's activity is detected with probability approaching to one when the number of eavesdropping operations goes to infinity. Similar relations can be derived for variants employing superdense coding and higher dimensional signal particles [11,15].

Instead of mounting an incoherent attack introducing noise Eve can steal some particles as it has been proposed in [14,16]. Those attacks preserve correlations required by the control mode at the price of introduction of 25% losses. As long as legitimate users tolerate non ideal transmission efficiency, and the number of lost particles is sufficiently low, the attacks of this type are undetectable in the seminal protocol. However, they also introduce errors in the message mode also at rate 25%, and that feature can be exploited to considerably limit their usefulness.

## 3 Security improvement

The information to be encoded is divided onto blocks $[m]_n$ with length $L$ each. Let $M = \{m_\mu\}$ be the message padded [8] to length $NL$. Alice and Bob use an error correcting code $ECC(\cdot)$ which is able to recover from the errors below QBER threshold and cryptographic function $Hash(\cdot)$ that returns $L$-bit hash of its input.

1. Preprocessing
   (a) Alice generates a random preprocessing key $K = \{k_\mu\}$ composed of $L$ bits.
   (b) For each message block Alice calculates

$$[s]_n = [m]_n \oplus Hash\,(K, n) \tag{4}$$

   where $n$ denotes the number of the block. The blocks $[s]_n$ form an encoded sequence $S$.
   (c) Alice calculates a protected key

$$KP = K \oplus [s]_0 \oplus [s]_1 \cdots \oplus [s]_{N-1} \tag{5}$$

   (d) and its hash

$$HP = Hash\,(KP, x) \tag{6}$$

   where $x$ is some random number.
2. Communication
   (a) Alice quantumly sends $ECC\,(KP)$, $ECC\,(HP)$ and classically $x$.
   (b) Bob finds

$$KP' = ECC^{-1}\,(E\,(ECC\,(KP))) \tag{7a}$$
$$HP' = ECC^{-1}\,(E\,(ECC\,(HP))) \tag{7b}$$

   where $E\,(\cdot)$ denotes modifications introduced by an attack operation and/or channel imperfections, and checks equality

$$HP' \stackrel{?}{=} Hash\left(KP', x\right) \tag{8}$$

   If it does not hold it means that errors induced by noise and/or eavesdropping have not been corrected and communication is broken down.
   (c) Otherwise communication is continued. Alice quantumly sends blocks $ECC\,([s]_n)$ and Bob decodes them as $\left[s'\right]_n = ECC^{-1}\,(E\,(ECC\,([s]_n)))$.
3. Postprocessing
   (a) The preprocessing key is recovered as

$$K' = KP' \oplus \left[s'\right]_0 \oplus \left[s'\right]_1 \ldots \oplus \left[s'\right]_{N-1} \tag{9}$$

   (b) When the preprocessing key is known the $n$-th message block is decoded as

$$\left[m'\right]_n = \left[s'\right]_n \oplus Hash\left(K', n\right) \tag{10}$$

   If error level in the quantum channel exceeds correction capabilities of the $ECC$, then $\left[s'\right]_n \neq [s]_n$ and based on (9) $K' \neq K$. The properties of the hash function guarantee that $\left[m'\right]_n$ is completely different from $\left[m'\right]_n$. Such

event can be easily detect by the integrity check implemented in the higher layer what is usually the case in communication systems.

## 4 Analysis

The hash function properties guarantee that correct decoding (10) of a single message bit requires the knowledge of the correct value of the corresponding bit from the encoded sequence $S$ and the whole preprocessing key $K$ which in turn, based on (9), depends on protected key $KP$ and whole encoded sequence $S$. It follows that it is sufficient to protect only a transmission of $KP$ to provide message confidentiality on a reasonable level. In further analysis it will be assumed that protocol cycles in control mode are executed only during $KP$ transmission. If the quantum channel is perfect and communicating parties did not employ any error correction then the attack on the protected key block is detected with probability $1-(1-d)^C$ where $C$ is the number of control modes. But for $d < 1/2$ Eve has incomplete information $I(d)$ about message encoded by Alice, thus she has to guess a part of the key and she is faced with problem of complexity $2^{(1-I(d))L}$. If she mounts an attack giving her complete information then she will be detected with probability close to one before any message related data is sent. On the other hand her information gain is small for the weakly detected ($\lim_{d\to 0} I(d) = 0$) attacks and she is faced with a computationally infeasible problem as long as $L$ is selected sufficiently large. Moreover, incoherent attacks also introduce some bit error ratio $b$ in a message mode. Thus additionally any attack in a lossless channel will be detected by the key integrity check with probability $(1-(1-b)^n)(1-2^{-L})$, where $n$ denotes the number of intercepted particles.

If the quantum channel is still perfect but legitimate users tolerate errors and/or losses on levels QBER and QLOSS, respectively then Eve is in a better position. This is the limiting case of the situation when Eve replaces the original imperfect quantum channel with a better one, or Alice and Bob underestimate the quality of the channel they have already been using. The non zero accepted QBER changes detectability of the incoherent attack. The interception of the entire protected key is then detected with probability

$$p_{control} = 1-(1-d)^{C(1-\mathrm{QBER})} \tag{11}$$

where $C$ is the number of conclusive control modes. At the same time $(\mathrm{QBER}/b)L$ particles can be intercepted in message mode without exceeding correction capabilities of the protection code. Thus an attack on the entire protected key is detected with probability given by

$$p_{mic} = \left(1-(1-b)^{L(1-\mathrm{QBER}/b)}\right)\left(1-2^{-L}\right) \tag{12}$$

and valid for $0 \le \mathrm{QBER}/b \le 1$. Which of those expressions is more decisive depends on mutual relation between $C$, $L$ and $b$. As the connection between induced bit error rate $b$ in the message mode and properties of incoherent attacks is not well investigated, the first of those expressions should serve as tool for parameter $C$ selection providing

desired security level. Moreover Eve is still faced with problem of key guessing of complexity $2^{(1-I(d))L}$. Contrary to the lossless case, she may stay invisible as long as she intercepts less than QBER portion of particles. But in this case she has to solve a problem of complexity $2^{(L-\mathrm{QBER})}2^{(1-I(d))\mathrm{QBER}}$.

Another kind of an attack can be mounted with techniques summarized in [14,16]. Those attacks are by design undetectable in the control mode as long as the number of lost particles is within tolerance accepted by legitimate parties. In the improved version [16] induced losses are on the 25% level and may be detected by monitoring transmission quality. Unfortunately such test are not reliable and cannot be used in a quantum channel with losses exceeding that limit. However, at the same time bit error rate in message mode is also equal to $b = 0.25$ and expression (12) can be used

$$p_{mic} = \left(1 - \left(\frac{3}{4}\right)^{L(1-4\,\mathrm{QBER})}\right)\left(1 - 2^{-L}\right) \tag{13}$$

The non detection probability $1 - p_{mic} \approx (3/4)^{L(1-4\,\mathrm{QBER})}$ is very close to zero for $L = 256$ and QBER of order of a few percent—a value easily satisfied by contemporary quantum channels. At the same time Eve's knowledge about the protected key is limited by mutual information $I_{AE} = \frac{3}{4}\log_2\frac{4}{3}$ per intercepted particle [14,16]. Thus Eve is still faced with a problem of computational complexity equal to $2^{(1-I_{AE})L}$.

The application of the proposed security layer has also consequences related to the efficiency of the protocol. The protected key hash (6) and protected message sequence (4) carry data which is insensitive to eavesdropping, thus there is no point to execute control modes during their transfer. This greatly improves protocol efficiency and the portion of the saved control modes can be executed during the protected key transfer improving that way the protocol properties.

## 5 Conclusion

The proposed security layer exploits inevitable errors induced by the eavesdropping in the control and message modes—a property not used so far. It is shown that properly combined primitives, which are well known in the classic cryptography, provide a layer which gives the reasonable security for the quantum deterministic communication. The function of that layer is similar to the privacy amplification known from the quantum key distribution schemes, except that proposed improvement does not introduce randomization of the information content and deterministic character of communication is preserved. The processing of the message in blocks guarantees that an eavesdropper for incoherent attacks is faced with a computationally infeasible problem as long as system parameters, such as a block length and an accepted error rate, are within reasonable limits. It is also worth noting that although primitives known from the classic cryptography have been used to build an additional layer, no key agreement or shared secrets are required for confidential communication.

The main conceptual advantage of QSDC communication over QKD protocols resides in its versatility. QSDC can be used for deterministic transmission of small

portions of sensitive data without key agreement as well as for regular QKD. The proposed protocol may be attractive alternative also in this second application as the main sources of quantum resources wastage, that is, the key sifting and privacy amplification just do not appear.



## References

1. Beige, A., Englert, B.G., Kurtsiefer, C., Weinfurter, H.: Secure communication with a publicly known key. Act. Phys. Pol. **101**(3), 357–368 (2002)
2. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
3. Boström, K., Felbinger, T.: On the security of the ping-pong protocol. Phys. Lett. A **372**(22), 3953–3956 (2008)
4. Cai, Q.Y., Li, B.W.: Improving the capacity of the Boström-Felbinger protocol. Phys. Rev. A **69**(5), 054301 (2004)
5. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
6. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin. Phys. Lett. **21**(11), 2097–2100 (2004)
7. Fu-Guo, D., Gui-Lu, L.: Quantum privacy amplification for a sequence of single qubits. Commun. Theor. Phys. **46**(3), 443 (2006)
8. ISO/IEC 9797-1: Information technology—Security techniques—Message Authentication Codes (MACs)-Part 1: Mechanisms using a block cipher (1999)
9. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**(3), 032302 (2002)
10. Ostermeyer, M., Walenta, N.: On the implementation of a deterministic secure coding protocol using polarization entangled photons. Opt. Commun. **281**(17), 4540–4544 (2008)
11. Vasiliu, E.V.: Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits. Quantum Inf. Process. **10**, 189–202 (2011)
12. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**(4), 044305 (2005)
13. Wang, C., DengF.G. Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt. Commun. **253**(1), 15–20 (2005)
14. Wójcik, A.: Eavesdropping on the ping-pong quantum communication protocol. Phys. Rev. Lett. **90**(15), 157901 (2003)
15. Zawadzki, P.: Security of ping-pong protocol based on pairs of completely entangled qudits. Quantum Inf. Process. pp. 1–12 (2011). doi:10.1007/s11128-011-0307-1. http://dx.doi.org/10.1007/s11128-011-0307-1
16. Zhang, Z., Man, Z., Li, Y.: Improving Wójciks eavesdropping attack on the ping-pong protocol. Phys. Lett. A **333**, 46–50 (2004)