# Confidential Deterministic Quantum Communication Using Three Quantum States

Piotr ZAWADZKI
Institute of Electronics
Silesian University of Technology, POLAND

***Abstract*—A secure quantum deterministic communication protocol is described. The protocol is based on transmission of quantum states from unbiased bases and exploits no entanglement. It is composed form two main components: a quantum quasi secure quantum communication supported by a suitable classical message preprocessing layer. Contrary to many others propositions, it does not require large quantum registers. A security level comparable to classic block ciphers is achieved by a specially designed, purely classic, message pre- and post-processing. However, unlike to the classic communication, no key agreement is required. The protocol is also designed in such a way, that noise in the quantum channel works in advantage to legitimate users improving the security level of the communication.**

***Keywords- quantum cryptography; quantum secure direct communication; privacy amplification.***

## I. INTRODUCTION

The interest in quantum communication is motivated by the promise of provable security based on the laws of physics. The most mature protocols use quantum channels for secure quantum key distribution (QKD) which is further used by legitimate parties to protect communication over classic channels [1]. The content of the key resulting from QKD execution is not determined by either of users but is random and settled by the protocol completion itself. An alternative paradigm of a quantum secure direct communication (QSDC) has been investigated in the last decade [2,3]. QSDC protocols offer confidential transmission of deterministic classic information over a quantum channel without a prior key agreement. Most QSDC protocols are completely robust [4-7]. It means, that an eavesdropper cannot intercept any information without introducing errors in the transmission. Unfortunately, the absence of privacy amplification step in QSDC protocols causes that complete robustness guarantees only quasi security in perfect quantum channels – there exists finite, nonzero probability that some information is intercepted without detection. Situation is even worse in noisy environments when legitimate users tolerate some level of transmission errors. If that level is to high compared to the quality of the channel then an eavesdropper can peek some fraction of signal particles hiding himself behind acceptable QBER threshold. The possibility to intercept some part of the message without being detected renders protocol insecurity. This difficulty has been resolved by processing qubits in blocks [8-12] and/or using quantum privacy amplification [13,14]. However, such an approach requires large quantum registers which are not realizable at present with photonic techniques.

In this paper QSDC security is improved by message classic processing. The quantum protocol based on single photon transmission and not exploiting quantum entanglement is supplemented by pre- and post-processing procedures. The quantum part requires only one qubit register and such photonic quantum memory operating in high temperature has been already realized experimentally [15]. The preprocessing part is an adaptation of the transform proposed in [16] to the specific requirements of quantum communication. In the resulting protocol, contrary to many others QSDC protocols, the noise in quantum channel works in advantage for the legitimate users improving the security of communication.

## II. PROTOCOL DESCRIPTION

Alice, the sender of information, is able to generate three quantum states $|0>$, $|1>$ and $|+>=(|0>+|1>)/\sqrt{2}$. Bob, the recipient of the message, is equipped with one qubit quantum register and is able to perform quantum measurements in Z and X bases. Users are connected with quantum and classic communication channels. Information in classic channel is not confidential and may be freely eavesdropped. However, it is assumed that this information cannot be modified by distrusted parties. On the contrary, the quantum channel may be tampered with no limitations – any data manipulation allowed by the laws of physics is permitted. Let $\mu=1,\dots,N$ and $M=\{m_\mu\}$ be the data block of bits which Alice is going to send.

### A. Preprocessing

1. Alice generates a random sequence of bits $K=\{k_\mu\}$. This sequence is further called a preprocessing key.
2. Alice encrypts some publicly known text T with the classic cipher of a well established reputation that produces a ciphertext $\{c_\mu\}=C=E_K(T)$ of size $N$ using a preprocessing key $K$ ($E_K$ denotes encryption operation),
3. The preprocessed sequence $S=(s_\mu,s_{N+\mu})$ which will be sent is composed of two parts. The first part is formed by bitwise xoring the ciphertext from the previous step with the message bits:

$$s_\mu = m_\mu \; xor \; c_\mu, \tag{1}$$

and the second part of sequence S is calculated as

$$s_{N+\mu} = k_\mu \; xor \; s_\mu. \qquad (2)$$

The encoding operation is invertible only when all bits of the sequence S are received without errors, thus some error correction code is used to protect against noise $B = ECC(S)$. Sequence B is sent to Bob via the quantum channel.

### B. Communication

Qubits are processed in one-by-one manner. Alice randomly switches between control and message mode and uses classic channel to notify Bob, that the last qubit of the given data block was sent so he should proceed with the post-processing step. The sequence $\{s_{N+\mu}\}$ is sent first.

#### 1) Control mode

1. Alice randomly prepares one of the states$|0>$, $|1>$ or $|+>$ which is sent to Bob.
2. Bob stores the received state in quantum register and notifies Alice.
3. Alice informs Bob that this qubit should be processed in control mode and informs Bob about the state preparation basis (Z or X).
4. Bob measures a quantum register in the basis specified by Alice.
5. If the selected basis was X, Bob knows that the measured state should be $|+>$. The appearance of $|->$ denotes a transmission error. Alice is notified about a failure.
6. If the selected basis was Z, Bob informs Alice about a measurement result and Alice compares that result with the value used in the state encoding. Bob is informed about comparison correctness.

If an error rate averaged over sufficiently large number of control qubits exceeds the correction capabilities of the ECC code then transmission is aborted before entire message is sent.

#### 2) Message mode

1. Alice encodes bit sequence $B = \{b_\mu\}$ as states $|0>$ and $|1>$ and sends them to Bob.
2. Bob stores the received state in quantum register and notifies Alice.
3. Alice informs Bob that this qubit should be processed in message mode.
4. Bob measures quantum register in Z basis, stores the measurement result as $b'_\mu$ in classic memory and notifies Alice that he is ready for the reception of the next qubit.

### C. Postprocessing

ECC data is used to correct errors on the received sequence $S' = ECC^{-1}(B')$,

1. The preprocessing key is recovered as $k'_\mu = s'_\mu \; xor \; s'_{N+\mu}$.
2. The ciphertext sequence is again calculated as $C' = E_{K'}(T)$ and the message decoded as $m'_\mu = s'_\mu \; xor \; c'_\mu$.

If any of the bits in the sequence $S'$ is incorrect then the key $K'$ is also incorrect and the sequence $C'$ is completely different from $C$ (this behavior is guaranteed by the properties of the classic cipher). It follows that Eve can recover a message only when she correctly intercepts entire sequence $S$. Incorrect detection on only one position results in (almost) random decoded message.

## III. Analysis

An important step in studying protocol security is an investigation of its robustness. Robustness of the protocol informs how large disturbance is introduced by an eavesdropper intercepting some information. QKD protocols can be secure when they are partly or completely robust [4]. However, security requirements for QSDC protocols are much more stringent because of the absence of privacy amplification step. As a result partly robust QSDC protocols are considered insecure and complete robustness guarantees only quasi security, i.e. there is a finite, non-zero probability that eavesdropper intercepts some part of the message without being detected. Although similar property also holds for classic cipher, the problem with QSDC security lies in fact, that offered eavesdropping detection probability is relatively low and Eve is detected with reasonable probability only after sufficiently large number of protocol cycles. The pre- and post-processing steps introduced herein provide all or nothing logic in the message interception possibility. Thus proposed protocol is insecure only when its quantum part is not robust. Contrary, if the quantum part is partly robust or completely robust then introduced classic pre- and post-processing steps provide protocol computational security. In the following it will be proven that quantum part is robust in lossless quantum channels and partly robust in a lossy case. This renders that Eve intercepts no useful information and protocol is secure. The provided security margin is related to the quantum transmission quality and QBER introduced by the eavesdropping.

Let us consider robustness of the protocol in the noiseless quantum channel case. As it follows from the Stinespring's dilation theorem, the most general quantum operation, which may be performed on the signal qubit by an eavesdropping Eve is described by an unitary operation that entangles the signal qubit with the ancilla system of dimension $2^2$. Such a transformation is described by four complex numbers $\alpha_k, \beta_k$

$$\mathrm{U}|0>|\varphi> = \alpha_0 |0>|\varphi_{00}> + \beta_0 |1>|\varphi_{01}>, \qquad (3)$$

$$\mathrm{U}|1>|\varphi> = \alpha_1 |0>|\varphi_{10}> + \beta_1 |1>|\varphi_{11}>. \qquad (4)$$

where $|\varphi_{kl}>$ denotes Eve's probe states and $|\varphi>$ is the initial state of the ancilla which is not entangled with the signal qubit. The normalization ensures that $|\alpha_k|^2 + |\beta_k|^2 = 1$. The same entangling operation has to be applied to the message and control qubits because Eve acquires information what mode has been used after the qubit has been stored in Bob's register. Eve is detected with probability $|\beta_0|^2$ and $|\alpha_1|^2$ when legitimate users test in Z basis. It follows from (3) and (4) that

$$\begin{gathered} U|+>|\varphi>=|+>(\alpha_0\,|0>|\varphi_{00}>+\beta_0\,|1>|\varphi_{01}>)+ \\ +|+>(\alpha_1\,|0>|\varphi_{10}>+\beta_1\,|1>|\varphi_{11}>)+ \\ +|->(\alpha_0\,|0>|\varphi_{00}>-\beta_0\,|1>|\varphi_{01}>)+ \\ +|->(\alpha_1\,|0>|\varphi_{10}>-\beta_1\,|1>|\varphi_{11}>)\,, \qquad (5) \end{gathered}$$

where $|->=(|0>-|1>)/\sqrt{2}$. Thus she is detected in X basis with probability

$$(|\alpha_0|^2+|\beta_0|^2+|\alpha_1|^2+|\beta_1|^2)/4=1/2 \qquad (6)$$

because $U$ is unitary. Thus overall Eve's detectability is minimized when $|\beta_0|^2=|\alpha_1|^2=0$. But in that case Eve's probe space is limited to two states and an entangling operation may be reduced to simple CNOT in which signal qubit is used as the control one. At the same time such operation provides maximal information about the state of the signal qubit when Eve performs measurements in Z basis. The quantum part of the protocol is completely robust because Eve can't intercept any information without risking to be detected. However, robustness of the quantum transmission implies only quasi security of the QSDC protocol.

Let us further consider how introduced preprocessing improves the security characteristic of the protocol and assume that legitimate users use ECC code able to recover from a given QBER although they operate in noiseless channel. Such assumption is favorable to the eavesdropper, as she can now intercept some signal particles and her actions will be undistinguishable from the noise. Because Eve is detected in X with probability $1/2$, it means that she can peek $2N \times QBER$ of signal qubits per block without inducing an alarm. This is the best case scenario for the eavesdropper. If the channel has been noisy Eve would have to attack a less percentage of particles to hide herself behind the total limit of errors. Thus it may be assumed that she knows $2 \times QBER$ fraction of $s_\mu$ and $s_{N+\mu}$ sequences and the rest part of these sequences remains random to her.

The preprocessing key is recovered as $k'_\mu = s'_\mu\ xor\ s'_{N+\mu}$. But correctly recovered are only these fragments for which bits on corresponding positions of sequences $s'_\mu$ and $s'_{N+\mu}$ are correct and that happens with probability $(2\,QBER)^2$. Thus to recover the message $m_\mu = s_\mu\ xor\ \mathrm{E_K(T)}$ malicious Eve has to attack a key space $[1-(2\,QBER)^2]\times N$ of a well established cipher and guess $[1-(2\,QBER)]\times N$ bits of the sequence $s'_\mu$. It follows that number of bits that have to be tested in brute force attack exceeds $N$ for $QBER \leq (\sqrt{5}-1)/4 \cong 0.31$. Available presently quantum channels may provide a better performance. Thus computational complexity of an attack on the protocol exceeds complexity of brute force guessing of the message contents. Protocols with such property are regarded in classic cryptography as secure. It is worth noting that although computational complexity of the brute force attack has been considered above, the proposed protocol does not require establishment of the shared secret for secure operation. Moreover, the block cipher used in the protocol works only in encryption mode, thus may be replaced by another cryptographic primitive providing randomization of the input data, for instance, a stream cipher generator or keyed hash function.

The performance of the described protocol is determined by the overhead related to the transmission of test qubits and a check block $s_{N+\mu}$. The number of test qubits must provide reliable estimation of the channel quality within one data block because decision about channel reliability should be taken before the sequence $s_\mu$ with encoded message is sent. As a matter of fact the control protocol cycles may be disabled during encoded message transmission as at this point of protocol execution is too late for the eavesdropping detection. The overhead related to transmission of the check sequence may be diminished for messages longer than $N$ bits. In such case message is padded and divided onto blocks $m_\mu^{(0)}$, $m_\mu^{(1)}$, …, $m_\mu^{(M)}$ and each block is processed and sent independently $s_\mu^{(k)} = m_\mu^{(k)}\ xor\ c_\mu$. The block with encoded preprocessing key $k_\mu\ xor\ s_\mu^{(0)}\ xor \ldots xor\ s_\mu^{(M)}$ is sent as the first one.

## IV. Conclusion

A single photon based protocol for quantum secure direct communication has been proposed. Although its quantum part is only quasi secure, the classic pre- and post-processing of the message improves protocol security to the desired level. The introduced protocol has very small demands on quantum resources and can be, in principle, practically implemented in the near future. Although the protocol is not unconditionally secure, the provided security margin is high in noisy quantum channels. It also offers some advantages compared to quantum key agreement schemes proposed so far. The unconditional security of QKD protocols has been proved in the limit of the infinite length of the block being processed and the length of the secret key is less than 50% of qubits sent. However, efficiency of QKD scales very badly with the decrementation of the sequence size and for moderate blocks of size $10^6$ the efficiency does not exceed 2% [17]. The proposed approach offers improved efficiency at the price of the computational security. It is also more versatile as it may be used for confidential exchange of short sensitive messages without key agreement and for regular QKD as well. Protocol also offers also some advantages compared to presented so far QSDC schemes [2,5] – the quasi security limitation has been conquered without requirement of large quantum memory registers which are out of the reach of the present state of the art technology.

## References

[1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, “Quantum cryptography”, Rev. Mod. Phys., vol. 74, pp. 145-195, 2002

[2] K. Boström and T. Felbinger, “Deterministic secure direct communication using entanglement”, Phys. Rev. Lett., vol. 89, pp. 187902, 2002

[3] A. Beige, B. G. Englert, C. Kurtsiefer and H. Weinfurter, “Secure communication with a publicly known key”, Act. Phys. Pol., vol. 101, pp. 357-368, 2002

[4] M. Boyer, R. Gelles, D. Kenigsberg and T. Mor, “Semiquantum key distribution”, Phys. Rev. A, vol. 79, pp. 032341, 2009

[5] M. Lucamarini and S. Mancini, “Secure deterministic communication without entanglement, Phys. Rev. Lett., vol. 94, pp. 140501, 2005

[6] K. Boström and T. Felbinger, “On the security of the ping-pong protocol”, Phys. Lett. A, vol. 372, pp. 3953-3956, 2008

[7] G. L. Long, F. G. Deng, C. Wang, X. H. Li, K. Wen and W. Y. Wang, “Quantum secure direct communication and deterministic secure quantum communication”, Front. Phys. China, vol. 2, pp. 251-272, 2007

[8] F. G. Deng, G. L. Long and X. S. Liu, “Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block”, Phys. Rev. A, vol. 68, pp. 042317, 2003

[9] S. Lin, Q. Y. Wen, F. Gao and F. C. Zhu, “Quantum secure direct communication with □-type entangled states”, Phys. Rev. A, vol. 78, pp. 064304, 2008

[10] J. Wang, Q. Zhang and C. Tang, “Quantum secure direct communication without a pre-established secure quantum channel”, Int. J. Quant. Inf., vol. 4, pp. 925–934, 2006

[11] G. Gao, “Two quantum dialogue protocols without information leakage”, Opt. Commun., vol. 283, pp. 2288-2293, 2010

[12] G. F. Shi, X. Q. Xi, M. L. Hu and R. H. Yue, “Quantum secure dialogue by using single photons”, Opt. Commun., vol. 283, pp. 1984-1986, 2010

[13] F. G. Deng and G. L. Long, “Reply to ‘Comment on “Secure direct communication with a quantum one-time-pad”’”, Phys. Rev. A, vol. 72, pp. 016302, 2005

[14] D. Fu-Guo and L. Gui-Lu, „Quantum privacy amplification for a sequence of single qubits”, Commun. Theor. Phys., vol. 46, pp. 443, 2006

[15] K. F. Reim, P. Michelberger, K. C. Lee, J. Nunn, N. K. Langford and I. A. Walmsley, “Single-photon-level quantum memory at room temperature”, Phys. Rev. Lett., vol. 107, pp. 053603, 2011

[16] R. L. Rivest, “All-or-nothing encryption and the package transform”, LNCS, vol. 1297, pp. 210-218, 1997

[17] V. Scarani, H. Bechmann-Pascanucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, “The security of practical quantum key distribution”, Phys. Rev. Lett., vol. 107, pp. 053603, 2011

## AUTHORS PROFILE

P. Zawadzki received M.S. degree in theoretical physics from Silesian University, Katowice, Poland, in 1989 and Ph.D. degree in electromagnetic engineering from Silesian University of Technology, Gliwice, Poland, in 1998. His research interests include numerical simulation of interactions between telecommunication infrastructure with the lightning electromagnetic pulse, data protection in telecommunication networks and quantum information processing in the context of quantum cryptography.