Państwowa Medyczna Wyższa Szkoła Zawodowa w Opolu

ISSN 2080-2021 • e-ISSN 2449-9021

Prace poglądowe | Reviews

DOI: 10.5604/2081-2021.1191752

QUANTUM DIGITAL SIGNATURES FOR UNCONDITIONAL SAFE AUTHENTICITY PROTECTION OF MEDICAL DOCUMENTATION

Podpisy kwantowe zapewniające bezwarunkową autentyczność dokumentacji medycznej

ARKADIUSZ LIBER[A–G]
RAFAŁ RUSEK[A–G]

Katedra Informatyki,
Politechnika Wrocławska

A – przygotowanie projektu badania | study design, **B –** zbieranie danych | data collection, **C –** analiza statystyczna | statistical analysis, **D –** interpretacja danych | data interpretation, **E –** przygotowanie maszynopisu | manuscript preparation, **F –** opracowanie piśmiennictwa | literature search, **G –** pozyskanie funduszy | funds collection

SUMMARY

Modern medical documentation appears most often in an online form which requires some digital methods to ensure its confidentiality, integrity and authenticity. The document authenticity may be secured with the use of a signature. A classical handwritten signature is directly related to its owner by his/her psychomotor character traits. Such a signature is also connected with the material it is written on, and a writing tool. Because of these properties, a handwritten signature reflects certain close material bonds between the owner and the document. In case of modern digital signatures, the document authentication has a mathematical nature. The verification of the authenticity becomes the verification of a key instead of a human. Since 1994 it has been known that classical digital signature algorithms may not be safe because of the Shor's factorization algorithm. To implement the modern authenticity protection of medical data, some new types of algorithms should be used. One of the groups of such algorithms is based on the quantum computations. In this paper, the analysis of the current knowledge status of Quantum Digital Signature protocols, with its basic principles, phases and common elements such as transmission, comparison and encryption, was outlined. Some of the most promising protocols for signing digital medical documentation, that fulfill the requirements for QDS, were also briefly described. We showed that, a QDS protocol with QKD components requires the equipment similar to the equipment used for a QKD, for its implementation, which is already commercially available. If it is properly implemented, it provides the shortest lifetime of qubits in comparison to other protocols. It can be used not only to sign classical messages but probably it could be well adopted to implement unconditionally safe protection of medical documentation in the nearest future, as well.

Keywords: quantum computing, quantum signature, quantum cryptography, medical documentation, medical documentation authentication

STRESZCZENIE

Współczesna dokumentacja medyczna ma coraz częściej postać cyfrową, a co za tym idzie – wymaga stosowania cyfrowych metod zapewniających zachowanie jej poufności, integralności i autentyczności. Jedną z metod zapewnienia autentyczności dokumentów jest ich podpisywanie. Stosowany w przypadku dokumentacji papierowej podpis odręczny bezpośrednio związany jest z wykonawcą ze względu na jego psychomotoryczną naturę. Związany jest również z podłożem oraz zastosowanym środkiem pisarskim. Dzięki tym cechom istnieje ścisły materialny związek pomiędzy wykonawcą a dokumentem. W przypadku współczesnych podpisów cyfrowych autentyfikacja dokumentów ma charakter matematyczny. Weryfikacja podpisującego staje się w zasadzie weryfikacją wprowadzonego klucza, a nie osoby, która go wprowadza. Od 1994 roku wiadomo, iż klasyczne algorytmy podpisu cyfrowego mogą być stosunkowo szybko przełamywane dzięki zastosowaniu propozycji Shora. Rozwiązaniem problemu może być zastosowanie algorytmów podpisu kwantowego. Przedmiotem pracy jest analiza najnowszych algorytmów podpisów kwantowych, możliwych do zastosowania w autentyfikacji dokumentacji medycznej. W ramach pracy przeprowadzono analizę współczesnych algorytmów podpisów kwantowych. W szczególności zaś przedstawiono te obiecujące, mogące mieć zastosowanie w zapewnieniu bezwarunkowej ochrony autentyczności dokumentacji medycznej, oparte na protokole QDS z elementami QKD. Praca stanowi materiał wyjściowy do dalszych badań związanych z praktyczną realizacją tego typu zabezpieczeń w istniejących systemach gromadzenia i przetwarzania dokumentacji medycznej.

Słowa kluczowe: obliczenia kwantowe, podpis kwantowy, kryptografia kwantowa, dokumentacja medyczna, autentyfikacja dokumentacji medycznej (*PU-HSP* 2015; 9, 4: 34–39)

Introduction

Nowadays, modern medical documentation appears most often in an online form and, therefore, requires some digital methods to ensure its confidentiality, integrity and authenticity. A digital document authenticity may be secured with the use of a digital signature based on the mathematical superposition of the encryption scheme and one-way hashing function mappings. The most practical implementations of the encryption function, used in digital signing algorithms, are founded on some difficult problems defined in the number theory, especially, on the factorization problem.

In 1994, a mathematician, Peter Shor, formulated the Shor`s algorithm [1] based on some special properties of quantum computing. This algorithm is able to find the prime factors of a given integer number. By doing so, it compromises the security of RSA and other cryptosystems based on the difficult problem of the integer numbers' factorization. The encryption based on this cryptosystem is used in some of the classical Digital Signatures protocols.

The first Quantum Digital Signature protocol was proposed in 2001 by Gottesman and Chuang [2]. This protocol was designed for classical messages only. The initial enthusiasm lasted until the publication of Barnum et al. [3], in which it was proved that if the protocol allows the receiver to read a message before the end of the verification phase it also allows him to modify it without the risk of being detected.

Fortunately, in 2002, Zeng and Keitel [4] presented the first Arbitrated Quantum Signature (AQS) protocol. The assumption was that the arbitrator is trustworthy to both the signatory and the receiver. The arbitrator will never try to forge or disavow and will always complete the protocol on his side. This protocol makes signing quantum messages possible and it uses GHZ states (three qubit entanglement) to deliver the signature to the receiver for the verification. Next, Li et al. [5] showed that Bell states (two qubit entangled states) can be used instead of GHZ states. This protocol was later improved by Zou et al. [6] who proposed an AQS protocol without using the entangled states.

In the real commercial world, it is impossible to find the arbitrator that will be trustworthy to both a signatory and a receiver. Therefore, a new AQS protocol with an untrusted arbitrator was proposed by Yu-Guang Yang et al. [7] and later improved by Xiangfu Zou et al. [8]. This protocol enables signing only a classical message.

Another type of Quantum Digital Signature was proposed by Dunjko, Wallden and Andersson [9] in 2014. This is the protocol of Quantum Digital Signature with Quantum Key Distribution components. This protocol was later improved [10] and experimentally implemented [11] soon afterwards. This is a protocol without an arbiter and it enables signing a classical message. Its main advantage is that it can be implemented by using the equipment for quantum key distribution that is already available commercially.

To simplify, we can assume that medical documentation has a form of a vector which may be interpreted as a message.

The principles of classical and quantum signatures

The main principles of a classical Digital Signature are also valid for a Quantum Digital Signature [4,5]:

- No modifications and no forgery: Neither a message nor a signature can be changed in a forbidden way during the protocol by any of the participants. The signature cannot also be reproduced.
- No disavowals: A signatory is identified unambiguously as the author of the signature by the receiver. The receiver cannot pretend that he didn't receive the message or the signature.
- No repudiation: if the verification is done by more than one participant (for example a receiver and an arbitrator), then all of them must obtain the same verification result.

No modifications and no forgery principle is provided by both the fact that the measurement of qubits changes its state and the no-cloning theorem [12]. It states that, in general, unknown quantum states may not be copied. The choice of the encryption is also very important because it has been proved that some types of encryption functions allow the modification

of the message and/or the signature without discrediting the positive verification.

No disavowals principle must be provided by the protocol itself and no repudiation principle must be provided by the verification phase of the protocol.

Phases of quantum signing

The basic structure of the protocol is:

1. Initialization phase.
2. Signing phase.
3. Verification phase.

The initialization phase is a basic setup in which, for example, secret keys or entangled qubits, that will be used later for teleporting data, are shared between the participants.

The signing phase is a phase in which a signatory creates a signature. This phase ends when the signatory sends a message and the signature to a receiver or an arbitrator.

During the verification phase a receiver checks if the signature matches the message and the signatory. The failure of the verification means that either some of the participants are not honest or a malevolent third party has intervened. It can also be the effect of a poor correction error.

Common elements

Common elements of Quantum Digital Signature protocols are:

- Comparing.
- Transmitting.
- Encrypting.

The most significant element of the verification phase is the ability to compare two sets of bits or qubits. For classical bits it is an easy task. There is no problem to distinguish between bit 0 and bit 1. The measurement of the qubits causes the loss of the information about the state that the qubit had before the measurement. Fortunately, there is a way to compare two unknown quantum states without measuring them – it is done by the Swap Test [13].

To compare the states of qubits q_1 and q_2, an additional qubit q_0 must be used. The initial state of q_0 is set to |0>. In the first step, the Hadamard gate operator is used on qubit q_0. In the next step, the Fredkin gate operator swaps the states of qubits q_1 and q_2 with qubit q_0 as a control qubit. Another steps take advantage of the Hadamard gate operator again on q_0 and then measure it. If q_1 and q_2 are equal, then q_0 will always be measured as 0. If q_1 and q_2 are different than measured, the result of q_0 will be either |0> or |1> – with 50% probability for each if q_1 and q_2 are in orthogonal states and 25% probability if they are in different orthogonal basis, for example, if q_1 belongs to the set {|0>;|1>} and q_2 to {|+>;|->}.

The classical channels can also be used for transmitting bits securely. The bits can be easily copied and processed using the standard PC equipment. Transmitting of qubits requires a quantum channel established between a sender and a receiver. One of the most promising systems that can be applied here is the Linear Optical Quantum Computing (LOQC) [14]. It uses photons as qubits. The equipment for processing the photonic qubits consists of the photon detectors, beam splitters, mirrors and phase shifters. A great advantage of LOQC is that the photons can be easily transmitted via fiber optic cables. The best results of quantum processing will be for the devices that can work on single photons.

Another practical technology to be used in QDS protocols is the Quantum Repeaters [15] – mainly a set of engineering principles and protocols that manage errors and losses in the communication networks based on the qubits transmission.

The Quantum Memory [16] may also prove useful. It allows to store the photonic qubit states for later processing in doped crystals as atomic excitations.

An exceptional example of the transmition is a key distribution for which Quantum Key Distribution protocols [17] can be used. These protocols have been proved to be unconditionally secure and, what is more important, have been already successfully implemented in several experimental facilities around the world such as DARPA Quantum Network in Massachusetts, Tokyo QKD network or Secure Communication based on Quantum Cryptography (SECOQC) in Vienna.

Usually, for communication between participants, a public board (classical public communications chan-

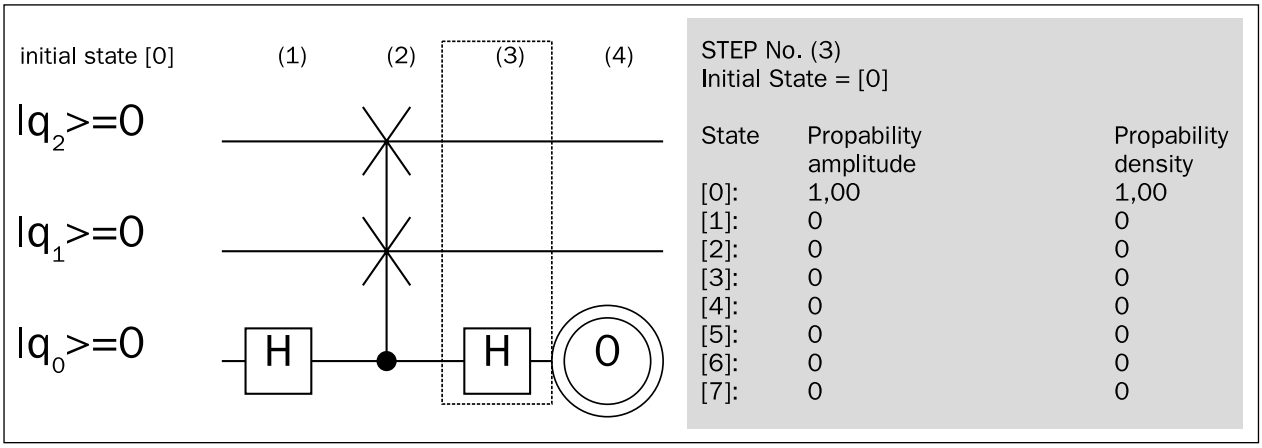

Figure 1. Illustration of Swap Test simulation with the use of software implemented by the authors

nel) is also used. The assumptions of the public board are that it can be susceptible to eavesdropping but not to the injection or alteration of messages and it cannot be blocked [6]. Additionally, the communication via the public board should be done with the identification of a writer and a time stamp.

In a typical digital signature scheme, one-way function is used instead of a plain message. It should be easy to calculate using a key and a message as the arguments and, very hard or impossible, to do the reverse calculation without knowing the key.

There are 2 quantum encryption protocol families that are used in QDS protocols:

– Quantum One-Time Pad (QOTP),
– Quantum Hashing.

Quantum One-Time Pads known also as Quantum Vernam Cipher [18,19] is a technique that requires generating a key randomly, each time it is needed for encrypting and decrypting data (thus it is a symmetric encryption). The input data for the encryption is a chain of qubits and the output data is also a chain of qubits, so it can be considered as a "quantum-quantum" type encryption. First schemes of QOTP used Pauli operators. To encrypt a message, generating a 2n qubit key is sufficient, which was proved by Boykin and Roychowdhury, [19]. This is a shared key. Initially, the encryption was done by Pauli operators: σz and σx. Later, it was shown [20] that, because of the commutativity of Pauli operators, a message and a signature with this encryption can be easily forged. Non-commutative operators were proposed to replace Pauli operators [21,22].

A different type of QOTP was proposed by Liu et al. [23]. It is called Decoy Quantum One Time Pad. Instead of modifying the quantum state of qubits, it adds some additional qubits to the sequence of messages/signature. The insertion place in a sequence is determined by a shared key. Additionally, revealing the standard bases on the public board and, then, measuring the added qubits, can be used to detect eavesdroppers and to check for errors in transmission.

Quantum Hashing uses a chain of classical bits at input and output, thus, giving a "classical-quantum" type encryption. This function was proposed by Ablayev and Vasiliev [24] and is based on the Quantum Fingerprinting function proposed by Buhrman et al [13]. This function uses the composition of n classical bits. The hashing procedure requires d+1 qubits, where d<n for large n (on the example calculations shown in [24] for n=32 authors have obtained d=15 and for n=32768, d=257). The initial state of each qubit is |0>. The next step is executing the Hadamard gate operators on each of d qubits. After that a set of controlled rotation gate operators is done. The rotation is done always on the additional qubit called a target qubit. The rotation operations are controlled by the qubits and bits of the message. The rotations are done by a specific angle which is determined for each operation by a key. These rotations are done around Y axis on the Bloch sphere. At the end of the hashing procedure, the quantum state of a target qubit is our hashed signature of the message.

The verification of a signature is done by performing the same set of controlled rotations but with negative angles. The measurement of all d+1 qubits should give the result equal to the initial state, that is |0> for each qubit. Otherwise, the verification is not passed.

The protocols

Three AQS protocols [4-6] were created on the way of the process of simplification. They use the QOTP encryption and they are intended for a quantum message. They require, at the beginning, three copies of a quantum message. A signatory encrypts them using QOTP with a private key. The first message is finally decrypted by a receiver at the end of the protocol if the verification phase is successful (it needs to be decrypted earlier also by an arbitrator). The second message is verified by the arbitrator who, using the Swap Test, compares it with the first message. If the verification is successful, the second message becomes a signature and is sent to the receiver. The third message is teleported to the receiver in AQS protocols with GHZ states [4] and with Bell states [5] or is delivered directly to the receiver with QOTP encryption that has been done using the key shared between the receiver and the signatory [6]. The third message is then verified by the receiver who, using the Swap Test, compares it with the first message (which is now decrypted by the arbitrator). If both verifications (by the arbitrator and the receiver) are successful, the receiver asks the signatory on the public board (thus accepting the signature) to publish a key for the final decryption of the first message.

The AQS protocol with an untrusted arbitrator [7,8] is intended for a classical message. This protocol uses a classical hashing function for the encryption of a classical message. It also uses a simple encryption algorithm for transcribing classical bits to qubits. The qubits are used here mainly to provide the unconditional security while delivering a signature to the receiver.

At the beginning of the protocol, a signatory adds some additional data to the message such as his and the receiver's ID, a time stamp and a unique random number (to protect against forgery by replacing an original message/signature with the one created before). Then, he encrypts everything using a classical hashing function. The signatory adds the same unique random number to the result of hashing and encodes all the bits to qubits using two keys where one of them is shared with the arbitrator and the second one is shared with the receiver. After receiving the qubits, the arbitrator decrypts them using his shared key and sends the qubits to the receiver. The receiver also decrypts the qubits with his shared key and transcribes the qubits to bits, thus, getting a hashed bit sequence and a unique random number. Without the knowledge of the message and the time stamp, the receiver is not able to decrypt the whole hashed message. He asks the signatory to publish other elements of the hashed message on the public board and, finally, he is able to create a new classical hashed message and compare it with the obtained one from the arbitrator. In this protocol the arbitrator acts as a middleman between the signatory and the receiver. The arbitrator also records all the data from the public board in his memory bank, so he can resolve possible disputes between the signatory and the receiver in the future.

The Quantum Digital Signature with Quantum Key Distribution components protocol [9-11] is executed by a signatory and two receivers, where the first receiver forwards a message and a signature to the second one. Qubits are not used directly to sign the message but rather to agree on a shared key between the participants. After the shared key is agreed, no qubits are present in the protocol and the message can be sent at any time later, thus, the other name for this protocol is: Quantum Digital Signature without the requirement of Quantum Memory.

A signatory sends two - qubit sequences (one corresponding to a message bit 0 and another to a message bit 1) to both receivers. Each qubit in a sequence is in one of four states: {|0>;|1>;|+>;|->}. Both receivers choose to keep or to send the qubit to the other receiver for each qubit in the sequence. Then, they measure each qubit and note the opposite result (this method is called quantum state elimination measurement). For example, if they measured |0> they note |1> and, if they measured |-> they note |+>.

The signatory signs each message bit separately by sending the bit of the message (0 or 1) and the signature as a classical bit sequence that describes the qubit states of a corresponding qubit sequence.

To verify the signature, a receiver compares, for each position in a sequence, the opposite states recorded with the states in the signature. The verification is positive for the states which are different. Because of possible errors and the method used in the protocol of quantum state elimination, the verification might be accepted even if some non-compliance occurs. To handle this situation, thresholds for accepting the comparison are used in the protocol.

The great advantage of this protocol is that it can be done using already available equipment for Quantum Key Distribution and that qubits are measured earlier than in the AQS protocols, so this protocol doesn't require the long time quantum memory.

Other types of Quantum Signatures

For more specific applications, two different types of protocols are being developed: Quantum Blind Signatures and Quantum Proxy Signatures.

In Quantum Blind Signatures, the author of the message sends the encrypted message to a signatory and receives a signed message from him. Then, he can send his message and the signature to a receiver who can authenticate the signature of this message. This type of protocol can be used for voting systems (a voting manager signs the votes but is not the author of the vote) and banking transactions (a bank signs a money transaction but is not the author of it). Some protocols for Quantum Blind Signature were proposed, for example, by Xiaojun Wen et al. [25] and by Tian-Yin Wang and Qiao-Yan Wen [26].

In Quantum Proxy Signatures, the author of the message, for some reasons, can't sign the message himself (for example because of his illness). He authorizes another person, called a proxy signer or a group of proxy signers, to sign the message on his behalf. Some protocols for Quantum Proxy Signatures were proposed, for example, by Yu-Guang Yang and QiaoYan Wen [27] and by Tian-Yin Wang and Zong-Li Wei [28].

Conclusions

In the paper, the current knowledge status of Quantum Digital Signature protocols, with its basic principles, phases and common elements such as transmission, comparison and encryption, was outlined. Some of the most promising protocols for signing digital medical documentation, that fulfill the requirements for QDS, were also briefly presented. The implementation of three AQS protocols require the measurement in a standard and diagonal bases with the use of QOTP encryption. It then allows the quantum message to be signed. The implementation of the AQS protocol with an untrusted arbitrator requires a quantum computer capable of executing only the Hadamard gate operation and the measurement in a standard and diagonal base However, it enables signing only classical messages. The QDS protocol with QKD components requires the equipment similar to the equipment used for QKD for its implementation, which is already commercially available. If properly implemented, it provides the shortest lifetime of qubits in comparison to the other protocols. It also enables signing only classical messages, but probably it could be well adopted to implement unconditionally safe protection of medical documentation in the nearest future.

The sources of funding

The research was funded by the authors.

The conflict of interests

The authors do not report any conflicts of interests.

References

1. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J Comput* 1997; 26(5): 1484–1509.
2. Gottesman D, Chuang I. Quantum digital signatures. arXiv preprint quant-ph/0105032. 2001. [online] 2001 [cited 18.06.2015]. Available from URL: http://arxiv.org/abs/quant-ph/0105032.
3. Barnum H, Crépeau C, Gottesman D, Smith A, Tapp A. *Authentication of quantum messages*. In: *Proceedings of the 43th Annual IEEE Symposium on Foundations of Computer Science; Vancouver, BC, Canada 16-19 November 2002*; Los Alamitos: IEEE Computers Society; 2002: 449–458.
4. Zeng G, Keitel Ch. Arbitrated quantum-signature scheme. *Phys Rev A* 2002; 65.4: 042312.
5. Li Q, Chan WH, Long D-Y. Arbitrated quantum signature scheme using Bell states. *Phys Rev A* 2009; 79.5: 054307.
6. Xiangfu Z, Daowen Q. Security analysis and improvements of arbitrated quantum signature schemes. *Phys Rev A* 2010; 82.4: 042325.
7. Yang Y-G, Zhou Z, Teng Y-W, Wen Q-Y. Arbitrated quantum signature with an untrusted arbitrator. *Eur Phys J D* 2011; 61 (3): 773–778.
8. Xiangfu Z, Daowen Q, Mateus P. Security analyses and improvement of arbitrated quantum signature with an untrusted arbitrator. *Internat J Theor Phys* 2013; 52(9): 3295–3305.

9. Dunjko V, Wallden P, Andersson E. Quantum Digital Signatures without quantum memory. *Phys Rev Lett* 2014; 112.4: 040502.
10. Dunjko V, Wallden P, Andersson E. Quantum digital signatures with quantum key distribution components. arXiv preprint 1403.5551 [online] 2014 Available from URL: http://arxiv.org/pdf/1403.5551.pdf.
11. Collins R, Donaldson RJ, Dunjko V, Wallden P, Clarke PJ, Andersson E. Realization of quantum digital signatures without the requirement of quantum memory. *Phys Rev Lett* 2014; 11.4: 040502.
12. Wootters W, Żurek W. A single quantum cannot be cloned. *Nature* 1982; 299: 802–803.
13. Buhrman H, Cleve R, Watrous J, de Wolf R. Quantum fingerprinting. *Phys Rev Lett* 2001; 87.16: 167902.
14. Kok P, Munro WJ, Nemoto K, Ralph TC, Dowling JP, Milburn GJ. Linear optical quantum computing with photonic qubits. *Rev Modern Physics* 2007; 79 (1): 135.
15. Van Meter R, Touch J. Designing quantum repeater networks. *IEEE Commun Mag* 2013; 51(8): 64–71.
16. Bussières F, Sangouarda N, Afzeliusa M, de Riedmattenbc H, Simond Ch, Titteld W. Prospective applications of optical quantum memories. *J Modern Optics* 2013; 60.18: 1519–1537.
17. Chardin G, Fackler O, Van Thanh Tran J, editors. *Progress in atomic physics neutrinos and gravitation*. Proceedings of the XXVIIth Rencontre de Moriond Series: Moriond Workshops, January 25-February 1, 1992; Les Arcs, Savoie: Frontieres; 1992.
18. Leung D. Quantum Vernam cipher, arXiv preprint quant-ph/0012077. 2000 [online] 2012 [cited 12.06.2014]. Available from URL: http://arxiv.org/abs/quant-ph/0012077.
19. Boykin PO, Roychowdhury V. Optimal encryption of quantum bits. *Phys Rev A* 2003; 67.4: 042317.
20. Gao F, Qin S-J, Guo F-Z, Wen Q-Y. Cryptanalysis of the arbitrated quantum signature protocols. *Phys Rev A* 2011; 84.2: 022344.
21. Zhang J. Arbitrated quantum signature protocol using EPR Pairs. *Journal of Networks* 2012; 7(11): 1803–1810.
22. Kejia Z, Dan L, Qi S. Security of the arbitrated quantum signature protocols revisited. *Phys Scr* 2014; 89.1: 015102.
23. Liu F, Qin S-J, Qi S. An arbitrated quantum signature scheme with fast signing and verifying. *Quantum Inf Process* 2014; 13(2: 491–502.
24. Ablayev F, Vasiliev A. Quantum hashing. arXiv preprint 1310.4922.2013 [online] 2013 [cited 4.03.2015]. Available from URL: http://arxiv.org/abs/1310.4922.
25. Wen X, Niua X, Jia L, Tiana Y. A weak blind signature scheme based on quantum cryptography. *Opt Commun* 2009; 282(4): 666–669.
26. Wang T-Y, Wen Q-Y. Fair quantum blind signatures. *Chin Phys B* 2010; 19(6).
27. Yang Y-G, Wen Q-Y. Threshold proxy quantum signature scheme with threshold shared verification. *Sci China Ser G* 2008; 51(8): 1079–1088.
28. Wang T-Y, Wei Z-L. One-time proxy signature based on quantum cryptography. *Quantum Inf Process* 2012; 11(2): 455–463.

Correspondence address:
dr inż. Arkadiusz Liber
Katedra Informatyki, Wydział Informatyki i Zarządzania
Politechnika Wrocławska
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
Tel. (+48) 713 203 207
E-mail: arkadiusz.liber@pwr.wroc.pl

mgr inż. Rafał Rusek
Katedra Informatyki, Wydział Informatyki i Zarządzania
Politechnika Wrocławska
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
E-mail: rafal.rusek@gmail.com

Received: 27.10.2015
Reviewed: 04.11.2015
Accepted: 05.11.2015