Quantum-secured blockchain

E.O. Kiktenko,[1,2] N.O. Pozhar,[1] M.N. Anufriev,[1] A.S. Trushechkin,[1,2]
R.R. Yunusov,[1] Y.V. Kurochkin,[1,3] and A.K. Fedorov[1,4]

[1]*Russian Quantum Center, Skolkovo, Moscow 143025, Russia*
[2]*Steklov Mathematical Institute of Russian Academy of Sciences, Moscow 119991, Russia*
[3]*Institute for Quantum Science and Technology, University of Calgary, Calgary AB T2N 1N4, Canada*
[4]*LPTMS, CNRS, Univ. Paris-Sud, Université Paris-Saclay, Orsay 91405, France*

(Dated: May 29, 2017)

Blockchain is a distributed database which is cryptographically protected against malicious modifications. While promising for a wide range of applications, current blockchain platforms rely on digital signatures, which are vulnerable to attacks by means of quantum computers. The same, albeit to a lesser extent, applies to cryptographic hash functions that are used in preparing new blocks, so parties with access to quantum computation would have unfair advantage in procuring mining rewards. Here we propose a possible solution to the quantum-era blockchain challenge and report an experimental realization of a quantum-safe blockchain platform that utilizes quantum key distribution across an urban fiber network for information-theoretically secure authentication. These results address important questions about realizability and scalability of quantum-safe blockchains for commercial and governmental applications.

INTRODUCTION

The blockchain is a distributed ledger platform with high Byzantine fault tolerance, which enables achieving consensus in a large decentralized network of parties who do not trust each other. A paramount feature of blockchains is the accountability and transparency of transactions, which makes it attractive for a variety of applications ranging from smart contracts and finance to manufacturing and healthcare [1]. One of the most prominent applications of blockchains is cryptocurrencies, such as Bitcoin [2]. It is predicted that ten percent of global GDP will be stored on blockchains or blockchain-related technology by 2025 [3].

In a modern blockchain network, any member can introduce a record (*transaction*) to the ledger. Every transaction must be signed by its initiator's digital signature; this rule enables, for example, exchange of digital assets between parties. The transactions are stored on each member's computer (*node*) as a sequence of groups known as *blocks*. All transactions that have been introduced over a period of time are compiled in a block that is linked to the previous one [4]. This linking is implemented by cryptographic hash functions: each block contains a hash value of its content, and the content also includes the hash of the previous block (Fig. 1). Any modification of a block inside the chain yields a change of its hash, which would in turn require modification of all subsequent blocks. This structure protects the data inside a blockchain from tampering and revision [5].

While each node is allowed, in principle, to introduce a block to the network, each blockchain network has a set of rules that organize and moderate the block formation process. In Bitcoin, for example, a member introducing a new block must solve an NP-hard problem: introduce a set of numbers to the block's header such that the hash of that header must not exceed a certain value (this paradigm is known as *proof-of-work*). In this way,
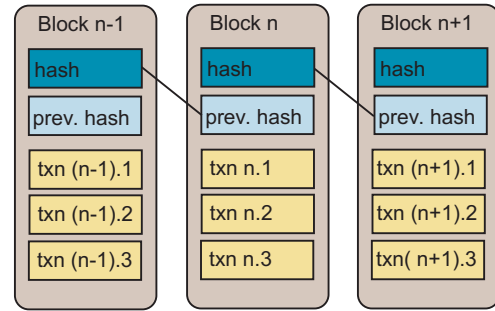

Figure 1. Organization of data in blockchains ("txn" stands for "transaction").

the blocks are guaranteed not to emerge too frequently, so every node has an opportunity to verify the validity of the block and the transactions therein before a new block arrives. This ensures the identity of the database stored by all network nodes. Whenever a new block is accepted by the community, its "miner" is rewarded in bitcoins for the computational power they spend.

A more detailed summary of the blockchain concept is presented in Appendix.

We see that blockchain relies on two one-way computational technologies: hash functions and digital signatures. Most blockchain platforms rely on the elliptic curve public-key cryptography (ECDSA) or the large integer factorization problem (RSA) to generate a digital signature [5]. The security of these algorithms is based on the assumption of computational complexity of certain mathematical problems [6].

A universal quantum computer would enable efficient solving of these problems, thereby making digital signatures, including those used in blockchains, insecure. In particular, Shor's quantum algorithm solves factorisation of large integers and discrete logarithms in polynomial time [7] Another security issue is associated with Grover's

search algorithm [8], which allows quadratic speedup in calculating the inverse hash function. In particular, this will enable a so-called 51-percent attack, in which a syndicate of malicious parties controlling a majority of the network's computing power would monopolize the mining of new blocks. Such an attack would allow the perpetrators to sabotage other parties' transactions or prevent their own spending transactions from being recorded in the blockchain.

The security of blockchains can be enhanced by using post-quantum digital signature schemes [9, 10] for signing transactions. Such schemes are considered to be robust against attacks with quantum computers [11]. However, this robustness relies on unproven assumptions. Furthermore, post-quantum digital signatures are computationally intensive and are not helpful against attacks that utilize the quantum computer to dominate the network's mining hashrate.

Another way to guarantee authentication in the quantum era is to use quantum key distribution (QKD), which guarantees information-theoretic security based on the laws of quantum physics [12–14]. QKD is able to generate a secret key between two parties connected by a quantum channel (for transmitting quantum states) and a public classical channel (for post processing). The technology enabling QKD networks have been demonstrated in many experiments [15–25] and is now publicly available through multiple commercial suppliers.

In the present work, we describe a blockchain platform that is based on QKD and implement an experiment demonstrating its capability in a three-node urban QKD network. We believe this scheme to be robust against not only the presently known capabilities of the quantum computer, but also those that may potentially be discovered in the future to make post-quantum cryptography schemes vulnerable.

The utility of QKD for blockchains may appear counterintuitive, as QKD networks rely on trust among nodes, whereas the earmark of many blockchains is the absence of such trust. However, employing QKD for communication between two parties via a direct quantum channel permits these parties to authenticate each other. That is, nobody can pretend to be somebody else when introducing a transaction. In this way, QKD, in combination with classical consensus algorithms, can be used in lieu of classical digital signatures.

RESULTS

Here we consider a blockchain protocol within a two-layer network with n nodes. The first layer is a QKD network with pairwise communication channels that permit establishing information-theoretically secure private key for each pair of nodes. The second (classical) layer is used for transmitting messages with authentication tags based on Toeplitz hashing (see Appendix) that are created using the private keys procured in the first layer.

For concreteness, we consider a blockchain maintaining a digital currency.

The operation of the blockchain is based on two procedures: (i) creation of transactions and (ii) construction of blocks that aggregate new transactions. New transactions are created by those nodes who wish to transfer their funds to another node. Each individual new transaction record is constructed akin to those in Bitcoin, i.e. contains the information about the sender, receiver, time of creation, amount to be transferred, and a list of reference transactions that justifies that the sender has enough funds for the operation (see Appendix). This record is then sent via authenticated channels to all other $n-1$ nodes, thereby entering the pool of unconfirmed transactions. Each node checks these entries with respect to their local copy of the database and each other, in order to verify that each transaction has sufficient funds, and forms an opinion regarding the transaction's admissibility. At this stage, the community does not attempt to exclude double-spending events (a dishonest party sending different versions of a particular transaction to different nodes of the network).

Subsequently, the unconfirmed transactions are aggregated into a block. We abolish the classical blockchain practice of having the blocks proposed by individual "miners", because it is vulnerable to quantum computer attacks in at least two ways. First, transactions are not rigged with digital signatures. This means that a miner has complete freedom to fabricate arbitrary, apparently valid, transactions and include them in the block. Second, a node equipped with a quantum computer is able to mine new blocks dramatically faster than any non-quantum node. This opens a possibility for attacks such as the 51-percent attack described above.

Instead, we propose to create blocks in a decentralized fashion. To this end, we employ the "broadcast" protocol proposed in the classic paper by Shostak, Lamport and Pease [26] (see Appendix). This protocol allows achieving a Byzantine agreement in any network with pairwise authenticated communication provided that the number of dishonest parties is less than $n/3$ (which we assume to be the case). At a certain moment in time (e.g. every ten minutes), the network applies the protocol to each unconfirmed transaction, arriving at a consensus regarding the correct version of that transaction (thereby eliminating double-spending) and whether the transaction is admissible. Each node then forms a block out of all admissible transactions, sorted according to their time stamps. The block is added to the database.

Because the broadcast protocol is relatively forgiving to the presence of dishonest or faulty nodes, our blockchain setup has significant tolerance to some of the nodes or communication channels not operating properly during its implementation. We also emphasize that, while the broadcast protocol is relatively data intensive, the data need not be transmitted through quantum channels. Quantum channels are only required to generate private keys.

While the proposed protocol seems to be efficient against quantum attacks on the distribution of transactions and formation of blocks, the database is still somewhat vulnerable while it is stored. A possible attack scenario is as follows: a malicious party equipped with a quantum computer works off-line to forge the database. It changes one of the past transaction records to its benefit and performs a Grover search for a variant of other transactions within the same block such that its hash remains the same, to make the forged version appear legitimate. Once the search is successful, it hacks into all or some of the network nodes and substitutes the legitimate database by its forged version. However, the potential of this attack to cause significant damage appears low, because the attacker would need to simultaneously hack at least one-third of the nodes to alter the consensus. Furthermore, because the Grover algorithm offers only a quadratic speed-up with respect to classical search algorithms, this scenario can be prevented by increasing the convention on the length of the block hash to about a square of its safe non-quantum value.

We experimentally study the proposed blockchain protocol on the basis of a four-node, six-link network [Fig. 2(a)] with information-theoretically secure authentication. We use an urban fiber QKD network recently developed by our team (see Appendix) to procure authentication keys for two of the links connecting three nodes; the key generation in the remaining four links is classical.

We test the operation of the blockchain and implement the construction of a simple transaction block under the following settings [Fig. 2(a)]. Nodes A, B and C perform legitimate transactions, whereas node D tries to process three different transactions, i.e. realize a double-spending attack. The pool of unconfirmed transactions at each node thus consist of three legitimate and one inconsistent transactions. The broadcast protocol is then launched on the basis of these transaction pools. This protocol eliminates node D's double-spending transaction after the second communication round and permits the formation of a block containing legitimate transactions only [Fig. 2(c)].

OUTLOOK

In summary, we have developed a blockchain protocol with information-theoretically secure authentication based on a network in which each pair of nodes is connected by a QKD link. We have experimentally tested our protocol by means of a three-party urban fibre network QKD in Moscow.

A crucial advantage of our blockchain protocol is its ability to maintain transparency of transactions and security against attacks with quantum algorithms. Our results therefore open up possibilities for realizing scalable quantum-safe blockchain platforms. If realized, such a blockchain platform can limit economic and social risks from imminent breakthroughs in quantum computation technology.
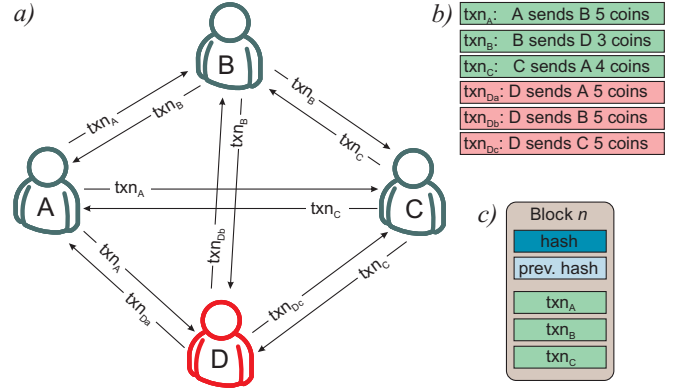

Figure 2. Creation of a block in a quantum-secure blockchain. a) Each node who wishes to implement a transaction sends identical copies of that transaction to all other nodes. Nodes A, B and C, whose transactions are denoted as txn_A, txn_B and txn_C, respectively, follow the protocol. Node D is cheating, attempting to send non-identical versions txn_{Da}, txn_{Db} and txn_{Dc} of the same transaction to different parties. b) Transaction contents. c) The nodes implement the broadcast protocol to reconcile the unconfirmed transactions and form the block. They discover that the transaction initiated by node D is illegitimate and exclude it.

Typical key generation rates of currently available QKD technologies are sufficient for operating a large-scale blockchain platforms based on our protocol. Moreover, remarkable progress in theory and practice of quantum communications, including recent experiments on ground-to-satellite QKD and quantum repeaters, could open the door to developing a public worldwide QKD network ("the quantum Internet" [27]) and extending quantum-safe blockchain platforms to the global scale.

The development of the "quantum Internet" will allow our protocol to preserve anonymity of each network member. A member will be able to access the global QKD network from any station, authenticate themselves to other parties using their private seed keys (see Appendix) and enact a desired transaction.

Our protocol is likely not the only possible quantum-safe blockchain platform. In this context, important horizons are opened by technologies that permit direct transmission of quantum states over multipartite networks combined with light quantum information processing. This includes, for example, protocols for quantum multiparty consensus [28, 29] and quantum digital signatures [30], which have been successfully studied in experiments, including metropolitan networks [31]. An additional important research avenue is more efficient, quantum-technology based consensus algorithms [32]. Most importantly, we hope that our work will raise awareness and interest of the quantum information community to the problem of security of distributed ledgers in the era of quantum technology.

APPENDIX

Blockchain workflow

Here we sum up the main definitions and concepts of conventional blockchains.

1. The *blockchain* is a distributed database in which the records are organized in a form of consecutive blocks. The term "distributed" means that copies of the database are stored by all the nodes that are interested in maintaining it, and that there is no single control center in charge of the network.

2. *Distributed consensus* is a set of rules governing the blockchain construction and operation accepted by the nodes maintaining this blockchain.

3. A *transaction* is an elementary record in a blockchain. In order to create a transaction, one (i) forms a corresponding record, (ii) signs it using a digital signature, and (iii) sends the record to all the nodes maintaining the blockchain. For example, if we use a blockchain for maintaining a cryptocurrency, then the transaction corresponds to a transfer of some amount of money from one party to another.

4. A *block* contains a number of transactions created over a certain period of time. Newly created transactions enter a so-called pool of unconfirmed transactions. Because such transactions are created at a faster rate than the typical network latency time, it is difficult for the community to agree on their time sequence and validity. This motivates the solution to aggregate new transactions into large blocks that are introduced at regular time intervals that are much longer than the network latency.

   In order to create a block with new transactions, a node needs to (i) check the validity of new transactions and discard invalid ones, (ii) combine the new transactions and the hash value of the last block in the existing blockchain, (iii) fulfill the additional moderation requirements imposed on new proposed block by the network rules (an example is the proof of work rule in Bitcoin), and (iv) send the new block to all other nodes. Each node then verifies the block's validity and adds it to the local copy of the blockchain.

5. The *cryptographic hash function* $H(\cdot)$ is a one-way map from arbitrary length strings to fixed-length strings (let say, 256 or 512 bit). The term "cryptographic" means that it act is pseudo-random way, *i.e.* any modification of the argument string x (even in a single bit) yields a major and unpredictable change of $H(x)$. Moreover, it is commonly believed that there is no classical algorithm, except brute-force, to invert the hash function, i.e. solve an equation such as $H(x) = h$. Quantum algorithms, in particular, Grover's algorithm [8], allow quadratic speed up in solving such problems.

6. The *digital signature* is an algorithm which allows one to verify that a certain message has been created by a particular author. The basic idea is that the author has a pair of keys: private key k_{priv} and public key $k_{\mathrm{publ}}(k_{\mathrm{priv}})$, and there is a one-way function $\mathrm{sgn}(m, k)$, such that the triplet

$$\{m, \mathrm{sgn}(m, k_{\mathrm{priv}}), k_{\mathrm{publ}}\} \qquad (1)$$

verifies the fact the author posseses k_{priv}, but does not allow one to determine k_{priv}.

Information-theoretically secure authentication

Two parties, Alice and Bob, can authenticate messages sent to each other if they share a secret private key K_{aut} that is not known to anyone else. The private key of necessary length can be generated via QKD provided that the parties have a small amount of "seed" key to authenticate themselves to each other in the beginning of the session. Once the private key is established, the authentication procedure is as follows: Alice sends to Bob a message with a hash tag generated using that key. After receiving the message, Bob also computes its hash tag. If the hash tags coincide, Bob can be certain that the message has arrived from Alice.

In our protocol, we use Toeplitz hashing due to its computational simplicity [33, 34]. Let the lengths of all messages and their hash tags be the same: l_M and l_h respectively. The hash tag of the ith message M_i is calculated according to

$$h(M_i) = T_S M_i \oplus r_i, \qquad (2)$$

where T_S is a $l_h \times l_M$ Toeplitz matrix generated by a string S of length $l_h + l_M - 1$, r_i is a bit string of length l_h, and $\oplus$ is the bitwise xor. Both S and r_i are private and taken from the common private key K_{aut}. Then the probability that an eavesdropper will correctly guess the hash tag of a modified message is not more than 2^{-l_h}.

If a series of messages is transmitted, the string S can be reused without compromising security, while the string r_i must be generated anew every time. In this way, the private key is consumed at a rate of l_h bits per message. In our experiment, $l_h = 40$ and $l_M = 2048$.

QKD network

The basis for our experimental work is our recently developed modular QKD device [25, 35–38] driven by a National Instruments NI PCIe-7811R card. This setup uses a semiconductor laser LDI-DFB2.5G controlled by an FPGA board Spartan-6 to generate optical pulses at the standard telecommunication wavelength 1.55 m and a 10 MHz repetition rate. We have used ID230 single-photon detectors from ID Quantique.

The QKD network contains two links with different physical implementations, realized in an urban environment in Moscow. The parameters of both links are listed in the table below.

	First link	Second link
Encoding	polarization	phase
Length (km)	30	15
Loss (dB)	13	7
Key rate (bit/s)	20	100

Broadcast protocol and block construction

Here we briefly summarize the protocol for reaching Byzantine agreement in the presence of faulty nodes [26, 39]. Consider n nodes connected by pairwise authenticated channels. Let each ith node possess a certain private value V_i.

The goal of the protocol is to make all nodes aware of all V_i's with a complication that there are m "dishonest" (or faulty) nodes. This can be rephrased as obtaining an n-dimensional consensus vector $\vec{V}^{\mathrm{cons}}$ with the following properties: (i) all the honest nodes obtain the same vector $\vec{V}^{\mathrm{cons}}$, and (ii) the ith component of $\vec{V}^{\mathrm{cons}}$ equals V_i for all honest nodes.

The consensus vector is determined through a series of communication rounds that proceed as follows.

- In the first round, the nodes transmit their values of V_i to each other.

- In subsequent rounds, the nodes communicate all the information they received in the previous round from other nodes (messages are of the form such as "node i_2 told node i_1 that node i_3 told node i_2 ... that node i_r told node i_{r-1} that its private value is U").

In Ref. [26], Lamport, Shostak and Pease proved that the consensus vector can be obtained with no more than $m + 1$ rounds for $m < n/3$ dishonest nodes.

In our setup, the private value V_i is the pool of transactions received by the ith node (together with its own transactions), as well as the set of bits indicating the node's opinion of each transaction's admissibility. After obtaining the consensus vector $\vec{V}^{\mathrm{cons}}$, the honest nodes are able to create a block containing the complete set of admissible transactions from the pool.

A shortcoming of the protocol of Ref. [26] in its original form is that it becomes exponentially data-intensive if a large number of cheating or unoperational nodes are present. Therefore further research on developing an efficient consensus protocol is required. We are optimistic that this issue can be resolved. Indeed, classical blockchain networks do routinely face the same challenge and have learned to deal with it efficiently.

[1] Franco, P. *Understanding Bitcoin: Cryptography, Engineering and Economics* (John Wiley & Sons, 2014).

[2] Extance, A. The future of cryptocurrencies: Bitcoin and beyond. *Nature* **526**, 21–23 (2015)

[3] Marr, B. *How Blockchain Technology Could Change The World*. Forbes, May 27, 2016.

[4] Swan, M. *Blockchain* (O'Reilly Media, Inc., 2015).

[5] Witte, J.H. The blockchain: A gentle four page introduction. *arXiv:1612.06244*.

[6] Schneier, B. *Applied cryptography* (John Wiley & Sons, Inc., New York, 1996).

[7] Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).

[8] Grover, L.K. A fast quantum mechanical algorithm for database search. Proceedings of 28th Annual ACM Symposium on the Theory of Computing (New York, USA, 1996), pp. 212–219.

[9] Lamport, L. Constructing digital signatures from a one-way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.

[10] Merkle, R. Secrecy, authentication and public key systems / A certified digital signature. Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University, 1979.

[11] Bernstein, D.J. *Introduction to post-quantum cryptography* (Springer-Verlag Berlin Heidelberg, 2009).

[12] Gisin, N., Ribordy, G., Tittel, W., & Zbinden H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).

[13] Scarani, V., *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).

[14] Diamanti, E., Lo, H.-K., & Yuan, Z. Practical challenges in quantum key distribution. *npj Quant. Inf.* **2**, 16025 (2016).

[15] Salvail, L., *et al.* Security of trusted repeater quantum key distribution networks. *J. Comput. Sec.* **18**, 61–87 (2010).

[16] Elliott, C., *et al.* Current status of the DARPA quantum network. *Proc. SPIE* **5815**, 138 (2005).

[17] Peev, M. *et al.* The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009).

[18] Stucki, D. *et al.* Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **13**, 123001 (2011).

[19] Chen, T.-Y. *et al.* Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt. Express* **17**, 6540–6549 (2009).

[20] Chen, T.-Y. *et al.* Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **18**, 27217–27225 (2010).

[21] Wang, S. *et al.* Field test of wavelength-saving quantum key distribution network. *Opt. Lett.* **35**, 2454 (2010).

[22] Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387 (2011).

[23] Fröhlich, D. *et al.* A quantum access network. *Nature* **501**, 69–72 (2013).

[24] Zhang, Q. *et al.* Chinas 2,000-km quantum link is almost complete. *IEEE Spectr.*, Oct. 2016.

[25] Kiktenko, E.O. *et al.* Demonstration of a quantum key distribution network across urban fiber channels. arXiv:1705.07154.

[26] Pease, M., Shostak, R., & Lamport, L. Reaching agreement in presence of faults. *J. ACM* **27**, 228 (1980).

[27] Kimble, H.J. The quantum internet. *Nature* 453, 1023–1030 (2008).

[28] Fitzi, M., Gisin, N., & Maurer, U. Quantum solution to the Byzantine agreement problem. *Phys. Rev. Lett.* **87**, 217901 (2001).

[29] Smania, M., Elhassan, A.M., Tavakoli, A. & Bourennane, M. Experimental quantum multiparty communication protocols. *npj Quant. Inform.* **2**, 16010 (2016).

[30] Gottesman, D. & Chuang, I. Quantum digital signatures. *arXiv:quant-ph/0105032.*

[31] Yin, H.-L. *et al.* Experimental measurement-device-independent quantum digital signatures over a metropolitan network. *Phys. Rev. A* **95**, 042338 (2017).

[32] Fitzi, M., *et al.* Detectable Byzantine agreement secure against faulty majorities, Proceedings of the 21st ACM Symposium on Principles of Distributed Computing, 118–126 (2002).

[33] Krawczyk, H. LFSR-based hashing and authentication. *Lect. Notes Comp. Sci.* **839**, 129–139 (1994).

[34] Krawczyk, H. New hash functions for message authentication. *Lect. Notes Comp. Sci.* **921**, 301–310 (1995).

[35] Sokolov, A.S. *et al.* Modular quantum key distribution setup for research and development applications. *arXiv:1612.04168.*

[36] Kiktenko, E.O., Trushechkin, A.S., Kurochkin, Y.V., & Fedorov, A.K. Post-processing procedure for industrial quantum key distribution systems. *J. Phys. Conf. Ser.* **741**, 012081 (2016).

[37] Kiktenko, E.O. *et al.* Symmetric blind information reconciliation for quantum key distribution. *arXiv:1612.03673.*

[38] Kiktenko, E.O. *et al.* Post-processing procedure for quantum key distribution systems. Zenodo. Available at: https://dx.doi.org/10.5281/zenodo.200365.

[39] Lamport, L., Shostak, R., & Pease, M. The Byzantine generals problem. *ACM T. Progr. Lang. Sys.* **4**, 382 (1982).