Post-quantum digital signature scheme with BB84 protocol[1]

Giorgi Labadze[a], Maksim Iavich[b], Giorgi Iashvili[b], Avtandil Gagnidze[c], Sergiy Gnatyuk [d]

[a] *Georgian Technical University,77 Kostava Street, Tbilisi, 0108, Georgia*
[b] *Caucasus University, 1 Paata Saakadze street, Tbilisi, 0102, Georgia*
[c] *Scientific Cyber Security Association, 26 Otar Lortkipanidze, Tbilisi, 0108, Georgia*
[d] *National Aviation University, Liubomyra Huzara Ave, 1, Kyiv 03058, Ukraine*

Abstract

Data encryption is the classical way of ensuring the various types of the sensitive data. The global release of quantum computers is expected in the near future. Quantum computers have the ability to break the existing classical digital signatures. Because, the classical digital signature schemes are vulnerable to the attacks of quantum computers. This fact involves the different research efforts that look for digital signatures that are secure against quantum computer-based attacks. In the paper, we analyze some digital signature schemes, which are secure against attack of quantum computers. The described schemes have various efficiency problems. Merkle signature scheme is analyzed, it's great problem is the very big size of the key pair. The paper analyzes the quantum key distribution protocols. BB84 key distribution protocol is described and analyzed. In the paper, we offer the novel scheme with reduced size of the key. The security of the scheme is analyzed. The key of the novel scheme is much less, than in the case of Merkle digital signature scheme.

Keywords
Post-quantum, digital signature, BB84 protocol;

1. Introduction

Scientists are actively working on the creation of quantum computers. Google Corporation, Universities Space Research Association and federal agency NASA together with D-WAVE began to work on design of quantum processors. D-WAVE is the manufacturer of quantum processors. D-Wave 2X is a quantum processor and it contains physical qubits. Google is working on releasing the new CPUs. On February 18, D-Wave Systems, which is the leader in creation of computing systems based on quantum calculations, software, and different services, published a novel study in the collaboration with Google employers. This study demonstrates a big computational advantage of the performance, which increases the size of simulation and problem complexity, to over three million times in comparison with the classical methods used in the real world. The mentioned performance advantage, exhibited in a hard quantum simulation of the materials, and it is a serious step in the journey toward computations advantage in the area of quantum computing. The result of the scientists at D-Wave and Google also shows that quantum calculations can be harnessed in order to offer a big computational advantage in D-Wave CPUs, at the problem scale, which need the thousands of qubits. The last experiments performed on different D-Wave CPUs represent by the most global quantum simulations implemented by the existing quantum computers today.

Quantum computers can break existing digital signature schemes. Different of RSA alternatives are offered. Mostly these schemes have different security and efficiency problems. Hash-based digital signature schemes are the post-quantum secure alternatives.

2. Hash-based digital signature schemes

2.1 The Lamport–Diffie one-time signature scheme

The Lamport–Diffie one-time signature scheme is a hash-based digital signature scheme [1]. Its signature key *X* contains *2n* random lines of the length *n*. Its verification key *Y* is of the same size.

$$X= (x_{n-1}[0], x_{n-1}[1], x_{n-2}[0], x_{n-2}[1],\ldots, x_0[0], x_0[1]) \in \{0,1\}^{n,2n} \quad (1)$$

$$Y= (y_{n-1}[0], y_{n-1}[1], y_{n-2}[0], y_{n-2}[1], \ldots, y_0[0], y_0[1]) \in \{0,1\}^{n,2n} \quad (2)$$

The verification key is obtained by means of one-way function:

$y_i[j] = f_o(x_i[j])$, $0<=i<=n-1$, $j=0,1$, f_o is the mentioned one-way function f_o: $\{0,1\}^n \rightarrow \{0,1\}^n$

To sign the message *m* we need to transform it to size n, my means of the hash function: h(m)=hashed = ($hashed_{n-1}$, $hashed_{n-2}$, … , $hashed_0$), where *h* is the cryptographic hash function. The signature of the message is done as follows: signature= ($x_{n-1}[hashed_{n-1}]$, $x_{n-2}[hashed_{n-2}]$, …, $x_0[hashed_0]$) $\in \{0,1\}^{n,n}$. The length of the signature is n^2.

2.2 The Winternitz one-time signature scheme

The Winternitz gives us the possibility to decrease the size of the signature [2]. In the scheme several bits of the hashed message are signed simultaneously by means of one line of the key. The Winternitz parameter is w> = 2, and it is equal to the number of bits, which must be signed simultaneously. $v_1=n/w$ and $v_2=(\log_2 v_1 +1+w)/w$, with $v= v_1+ v_2$ must be calculated. Its signature key *X* contains *2n* random lines of the length *v*. Its verification key *Y* is of the same size.

$$X= (x_{v-1}[0], x_{v-1}[1], x_{v-2}[0], x_{v-2}[1],\ldots, x_0[0], x_0[1]) \in \{0,1\}^{v,2n} \quad (3)$$

$$Y= (y_{v-1}[0], y_{v-1}[1], y_{v-2}[0], y_{v-2}[1], \ldots, y_0[0], y_0[1]) \in \{0,1\}^{v,2n}, \text{ where } y_i=f_o^{2^{w-1}}(x_i), \text{ and } 0<=i<=v-1 \quad (4)$$

The checksum is calculated as follows: $c=\sum_{i=v-v1}^{v-1}(2^w-p_i)$. Considering that $c<= v_1 2^w$, the length of the binary representation is $\log_2 v_1 2^w+1$.

We hash the message, hash=$p_{v-1},\ldots, p_{v-p1}$.The minimum number of zeros are prepended to the binary representation in order to obtain the length of the representation, dividable by *w*. Consequently, it is divided into v_2 parts of length *w*. The message is signed as follows: signature=($f_o^{p_{v-1}}(x_{v-1})$, …, $f_o^{p_0}(x_0)$). The signature size is *vn*. To verify the signature the following equation must be verified: $(f_o^{(2^w-1-p_{v-1})})(signature_{n-1})$, …, $(f_o^{(2^w-1-p_0)})(signature_0) = y_{n-1}, \ldots y_0$.

2.3 Merkle signature scheme

The one-time signature cannot be used in practice, as the uniques key pair of the keys is needed for every message. In 1979, Ralph Merkle offered the Merkle signature scheme. It uses a binary tree of hashes, the root of the tree is the public key. The size of the tree is H>=2. 2^H documents can be signed securely by

one public key. 2^H pairs of signatures and verification keys are generated. X_i, Y_i, 0<=i<=2H. The leaves of the tree are by means of the hashing of the keys. $h:\{0,1\}^* \rightarrow \{0,1\}^n$

The parent node is received by means of the concatenation and hashing of the previous pair of nodes. Each message is transformed to the size *n* by means of the the secure hash function. The signature is a concatenation of the one-time signature, the one-time verification key, the index of the chosen key and of the fraternal nodes according to the selectedkey. The size of the signature size is much bigger in the comparison to one-time signature schemes [3-6].

3. Quantum key distribution

Quantum key transmission is a method that allows two parties, conditionally Alice and Bob, to use a common secret key for cryptographic purposes. To ensure privacy of the notice, Alice and Bob agree on a piece of shared confidential information that we call the key [7,8]. Encryption occurs as a result of merging the notice and the key so that the result is incomprehensible to an interested party for whom the key is unknown. A recipient of the notice uses a copy of the key to decrypt it.

Firstly, it should be noted, that purpose of transmitting a quantum key is not to encrypt information, but rather to guarantee the secret transmission of the key. In turn, lawful parties can use this key to encrypt information. Confidentiality of the transmitted information is ensured by two aspects: Quantum key transmission and encryption algorithm. If either of these two aspects is violated, a whole system will collapse; accordingly we must point out the strengths of both aspects.

4. BB84 protocol

4.1 Encoding random bits with the help of qubits

In classical information theory, all notices can be converted to zeros and ones at some point. That is why a unit of information is called a bit or $\{0,1\}$. The quantum protocol BB84 cannot be described in classical terms, so we have to adapt our language to this new parameter [9,10]. There is a compliance between the quantum state of some physical system and the information that it carries.

The quantum state is mainly written with Dirac notations, between a vertical line and an angular parenthesis, as $|\psi\rangle, |1\rangle$ either $|x\rangle$; Particles of quantum information are displayed with the same notation.

In quantum theory, the smallest piece of information is a qubit, the quantum equivalent of a bit. In a physical system, qubit matching is the electron rotation or photon polarization. Mathematically a qubit is described by a set of two complex numbers.

$$\{\alpha|0\rangle + \beta|1\rangle : \ |\alpha|^2 + |\beta|^2 = 1 \ \alpha, \beta \in C\} \tag{5}$$

Two basic qubits, which match to two orthogonal states in a quantum system. Qubits $|0\rangle$ $(\alpha = 1, \beta = 0)$and $|1\rangle$ $(\alpha = 0, \beta = 1)$can be viewed as the quantum equivalent of bits of 0 and 1, respectively. α and β in another meaning we say that qubit is in superposition $|0\rangle$and $|1\rangle$. For example, qubits $2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$and $\sin\pi/6\,|0\rangle + \cos\pi/|1\rangle$; $|0\rangle$and $|1\rangle$both are in superposition, even though they are different. BB84 Alice uses encoding random (classic) bits called key elements using four different qubits. Bits 0 can be encoded $|0\rangle$or $|+\rangle = 2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$. Bits 0 can be encoded $|1\rangle$or $|-\rangle = 2^{-1/2}|0\rangle + 2^{-1/2}|1\rangle$. Take into account the difference in symbols. In both cases, Alice chooses any coding rule on a random basis, according to probability. She then sends the photon with the selected qubit to Bob. When photon goes to Bob's stop, he wants to decrypt what Alice has sent. For this, he must conduct measurements. However, the laws of quantum mechanics do not allow Bob to fully decipher the qubit. It is often impossible to accurately understand the obtained qubit $\alpha|0\rangle + \beta|1\rangle$ α and β coefficient. Instead, Bob should choose a pair of orthogonal qubits and make measurements that distinguish only them. We say that two qubits $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$and $|\psi\rangle = \alpha'|0\rangle + \beta'|1\rangle$are orthogonal if $\alpha\alpha' * + \beta\beta' * = 0$.

Take orthogonal qubits $|0\rangle$and$|1\rangle$. Bob can take measurements to find out what Alice has sent $|0\rangle$or$|1\rangle$. But what happened if she sends $|+\rangle$ either $|-\rangle$? In fact, Bob gets the result by accident! In general, if Bobby gets $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, he measures $|0\rangle$with probability $|\alpha|^2$and $|1\rangle$ with probability $|\beta|^2$. Remember $|\alpha|^2 + |\beta|^2 = 1$. In practice, $|+\rangle$ and $|-\rangle$Bob gets $|0\rangle$and $|1\rangle$ with each probability ½. Hence, Bob cannot distinguish $|+\rangle$ and $|-\rangle$. In this case he takes the value of uncorrelated bits. What is special about qubits $|0\rangle$ and $|1\rangle$? It is possible to record equivalently $|0\rangle = 2^{-1/2}|+\rangle + 2^{-1/2}|-\rangle$ and $|0\rangle = 2^{-1/2}|+\rangle - 2^{-1/2}|-\rangle$.

Accordingly in this case, Bob can decode Alice's notice when she sends $|+\rangle$ and $|-\rangle$, but he will not be able to analyze $|0\rangle$ and $|1\rangle$. An example of transmission detection is given in Figure1.2.

In BB84 protocol, Bob randomly selects the measurements, in about half of the cases he chooses $|0\rangle$ and $|1\rangle$, and in other cases he distinguishes $|+\rangle$and $|-\rangle$. At this stage Alice does not reveal which coding rule she has used. Consequently, Bob correctly measures only half of the bits that Alice has sent him and does not know which of them is correct. After sending a long stream of key elements, Alice informs Bob about the coding rule.

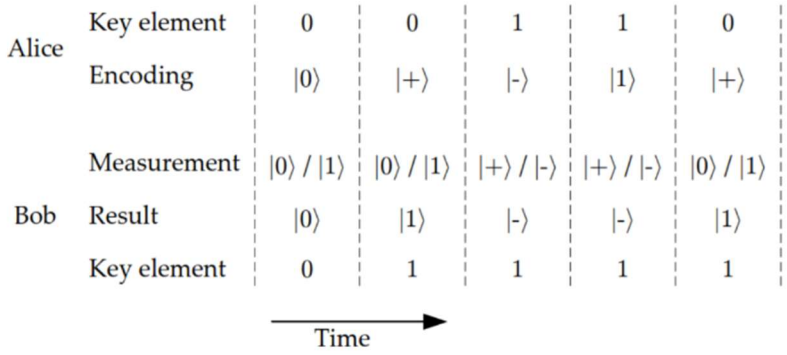

Figure 1.2: Transmission example using BB84.

The first two strings are those what Alice is sending. The third string shows the measurement method chosen by Bob and the possible result obtained as a result of the measurement.

Alice has chosen all the basic elements, now Bob can throw away all the wrong measurements; This part of the protocol is called Shift (so called Shifting) which is shown in Figure 1.3.

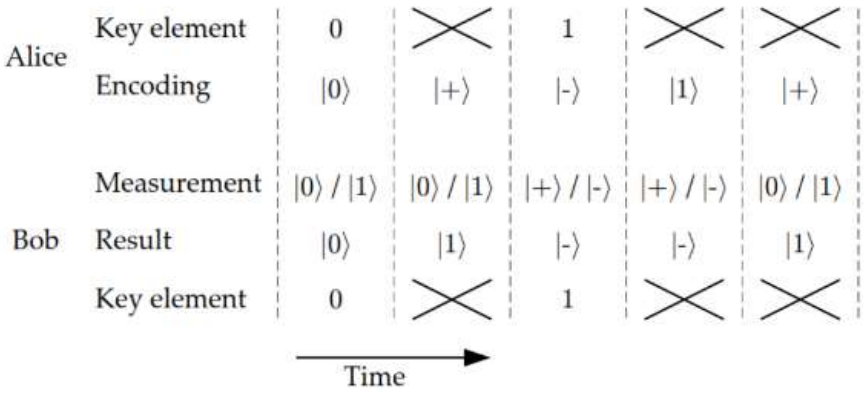

Figure 1.3: Transmission shifting

To summarize so far, Alice sends Bob random bits. Alice selects four different qubits for bit encoding (two supposed qubits per bit). Bob chooses one of two measurement methods for decoding. Bob may not always be able to determine what Alice has sent, but after shifting, Alice and Bob retain most of the bits for which the transmission was done successfully. This scheme of transmission allows Alice and Bob to notice the hearing.

4.2 Eavesdropping recognition.

A key feature of hearing recognition is the fact that information is encoded in non-orthogonal qubits. Eva can certainly catch the quantum train and try to measure it. But like Bob, she does not know in advance which pair of train Alice has chosen, for all the basic elements. As Bob and Eva can successfully chooses $|0\rangle$ and $|1\rangle$, when Alice uses $|+\rangle$ and $|-\rangle$ or vice versa.

In quantum mechanics, measurements are destructive. After measuring the particle, we get the result as a condition. More precisely, suppose that observer measures the qubit $|\phi\rangle$ to distinguish $|0\rangle$ and $|1\rangle$. After the measurement the qubit will become $|\phi\rangle \rightarrow |\phi'\rangle = |0\rangle$ or $|\phi\rangle \rightarrow |\phi'\rangle = |1\rangle$, depending on the measurement result, it does not matter what it was, unless the qubit is one of them that the observer wants to distinguish (for example $|0\rangle$ or $|1\rangle$)

In all cases, when Eva catches a photon, she measures it and sends it to Bob, she has a probability ¼,error probability between Alice and Bob's bits.

Let us demolish this opportunity. Eva has a probability ½ to measure the correct pair. When Eva does this she does not touch the condition and remains unnoticed. But she is not always lucky. However, when she measures the wrong set, she sends Bob the wrong position (e.g. $|+\rangle$ or$|-\rangle$, $|0\rangle$ or$|1\rangle$instead). This situation is described in Figure 1.4. In the wrong position, Bob basically measures a random bit that has a probability of ½ coinciding with Alice bit and a probability of ½ an error.

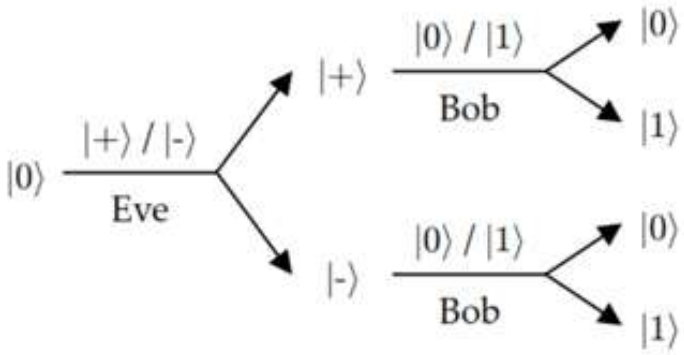

Figure 1.4: Possible results when Eva uses incorrect measurements for hearing

Therefore, when Eva tries to listen, she gets an irrelevant result in about ½ cases. She may decide not to write to Bob the conditions for which she obtained an irrelevant result. But it is impossible for her to make a similar distinction because she does not know what method of coding is used.

Rejecting the basic elements is nonsense for Eva, as this pattern will not be used to make Alice and Bobby the key. However, if she relays the situation (even though she is wrong in ½ of case), Alice and Bob will discover her existence due to an unusually large number of errors in their basic elements.

Bob and Eva have the same difficulty with the information sent by Alice, because they do not know which coding rule is used. But the situation is not symmetrical for Bob and Eva: All communications are necessary for shifting, in the classic authenticated channel. This allows Alice to find out that she is talking to Bob and not Eva. Consequently, the legal parties guarantee that Eva will not be able to influence on the shifting process. Thus, Alice and Bob can only compare key elements that have been measured correctly. To determine the existence of a listener, Alice and Bob must be able to detect transmission errors. To do

this, there is a way to open part of the shifted key. A given protocol can show $l + n$ the key element after transmission (e.g., l + n = 100,000) indexed from 0 to l + n -1, Alice randomly selects the n index (e.g. n = 1000) then communicates with Bob. Then Alice and Bob open the corresponding n key elements to count the number of errors, any error means there was some hearing. The absence of errors gives us some statistical confidence that there has been no hearing. But it is possible that Eva was lucky, or guessed the coding rule, or made mistakes on other key elements. Of course then the remaining basic elements will be used to create the secret key.

4.3 Getting a secret key

If errors are detected, Alice and Bob can discontinue the protocol as errors can be caused by listening. In the extreme case this prevents the creation of a key that may be known to the opponent. This side of the decision can be a little tough. In practice, physical realization is not ideal because errors can be caused by many reasons other than hearing, such as noise or loss in a quantum channel, incomplete generation of a quantum state, or incomplete deduction. Also, Eve may have heard a small part of the encrypted key, creating the remaining elements of the key to create the secret key. Accordingly, a way must be found to establish a quantum key protocol for more sustainable noise.

Alice and Bob count the number of errors in the detected key elements and divide this number by n to get an estimate of the expected fraction e. The error of the whole set of basic elements, the estimate e, is called the bit error norm. After that, they can conclude how much information Eve possesses about the key elements. For example, they can statistically estimate that Eve knows no more than I_E bit of l in the key elements. This is part of the protocol evaluation. The formula that gives us I_E quantity is not explained here; This is the result of an analysis of what hearing can do based on the laws of quantum mechanics. Also I_E does not exactly tell to Alice and Bob what Eva knows about the key elements. Eve may know the exact meaning I_E of the elements or just the result of several derivative functions l. Which gives I_E information in the sense of Shannon. At this point, Alice and Bob know that open key elements have an e error rate, and a potential listener has I_E information about them. With a classic shared authenticated channel, Alice and Bob can even try to create a completely secret key; this part is called the secret key distillation.

The secret key distillation, involves a stage called an agreement, which aims to correct transmission errors. A step called privacy enhancement that removes Eva's information at the expense of shortening the key length. We briefly describe these two processes.

In the case of BB84, the agreement usually takes an interactive look. Errors will be corrected by the protocol. Alice and Bob alternately reveal equal subsets of their basic elements. When they find the ratio difference, it means that the corresponding subsets contain an indeterminate number of errors. In extreme cases at least one. Using a dichotomy, they can point the location of the error and correct it. They repeat this process in sufficient quantities and as a result Alice and Bob change equal bits.

During the secret key distillation, all communications take place through a common authenticated classic channel. Remember that Eva can not intervene in this process, but she can listen to exchanged notices, which in this case contains exchanged equal bits. Thus, Eve's knowledge includes $I_E + |M|$ bits, equal bits of meaning $|M|$, that were discovered during the correction. To keep the key secret, the idea of enhancing privacy is to use what Eve does not know. Alice and Bob can compute the function f of the key elements, so as to spread partial Eve ignorance throughout the result. Such a function (for example, as a hash function in classical cryptography) is chosen so that each output bit depends on most or not most of the input bits. For example, such a function consists of calculating bits of equal random subsets. Suppose that Eve knows a bit x_1 but does not know about the meaning of a bit x_2. If the function f $x_1 + x_2 \, mod \, 2$, Eva can not open the output value until two possibilities

$x_1 + x_2 = 0(mod)\, 2$ and $x_1 + x_2 = 1(mod)2$ are equal no matter what the value x_1 has. The price that we have to pay for privacy is that the length of the output secret key should be less than the length of the partial secret key. The size of the abbreviation is approximately equal to the number of bits that Eve knows and the result of the key size $l - I_E - |M|$ in bits. Getting the maximum size of a key is possible when Eve

does not know about the constituent bits of the key and (for example, $l - I_E - |M| = 0$) is important that reducing explain as little information as possible which will be enough for Alice and Bob to be able to correct all the mistakes. Note that, we have to correct errors twice during quantum transmission from the number of bits produced by the secret key. We must first attribute the errors to the listening and I_E count. Also, errors must be corrected quickly, for which part of the bits must be opened and considered as $|M|$. Finally, the secret key, obtained after enhancing the confidentiality, can be used by Alice and Bob for cryptographic purposes. In particular, they can use the key to encrypt the message or create a secret channel.

5. The novel scheme

The idea is to use one time signature scheme instead of Merkle scheme. It will involve reducing the signature length. In order to transfer the key, BB84 protocol is used. As one time signature, we use Winternitz scheme.

To sign the message the signature and verifications keys are generated. For this, the Winternitz parameter is w> = 2, and it is equal to the number of bits, which must be signed simultaneously. v_1=n/w and v_2=($\log_2 v_1$ +1+w)/w, with v= v_1+ v_2 must be calculated. The signature key *X* contains *2n* random lines of the length *v*. Its verification key *Y* is of the same size.

X= ($x_{v-1}[0]$, $x_{v-1}[1]$, $x_{v-2}[0]$, $x_{v-2}[1]$,…, $x_0[0]$, $x_0[1]$) ∈ $\{0,1\}^{v,2n}$.

Y= ($y_{v-1}[0]$, $y_{v-1}[1]$, $y_{v-2}[0]$, $y_{v-2}[1]$, …, $y_0[0]$, $y_0[1]$) ∈ $\{0,1\}^{v,2n}$, where $y_i=f_o^{2^{w-1}}(x_i)$, and 0<=i<=v-1.

Now the verification keys must be transferred, it is performed using BB84 protocol. For this are preformed: encoding random bits with the help of qubits, eavesdropping recognition, getting a secret key. To sign the message it hashed: hash=k_{p-1},…, k_{p-p1}.The checksum is calculated as follows: $c=\sum_{i=v-v1}^{v-1}(2^w-p_i)$. Considering that c<= $v_1 2^w$, the length of the binary representation is $\log_2 v_1 2^w$+1. The minimum number of zeros are prepended to the binary representation in order to obtain the length of the representation, dividable by *w*. Consequently, it is divided into v_2 parts of length *w*. The message is signed as follows: signature=(f_o^p_{v-1}(x_{v-1}), …, f_o^p_0(x_0)).

To verify the signature the following equation must be verified: (f_o^(2^w-1-v_{v-1})) ($signature_{n-1}$), …, (f_o^(2^w-1-v_0))($signature_0$) = y_{n-1}, … y_0.

6. Security and results.

As the result we have received, the hash based digital signature scheme, which is secure, because it use the classical version of Winternitz one-time scheme and BB84 protocol. To break the system we need either to break Winternitz one-time or BB84 protocol. Both of this is impossible, because of the initial assumptions. The signature size is vn, which is much less than in the case of Merkle.

7. Acknowledgments

The work was conducted as a part of PHDF-19-519 financed by Shota Rustaveli National Science Foundation of Georgia.

8. References

[1] Buchmann J., Dahmen E., Ereth S., Hülsing A., Rückert M. (2011) On the Security of the Winternitz One-Time Signature Scheme In: Nitaj A., Pointcheval D. (eds) Progress in Cryptology – AFRICACRYPT 2011. Lecture Notes in Computer Science, vol 6737. Springer, Berlin, Heidelberg

[2] R. Merkle. (1979) Secrecy, authentication and public key systems / A certified digital signature Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University.
[3] Gagnidze A., Iavich M., Iashvili G., (2017) Analysis of post-quantum cryptography use in practice. Bulletin of the Georgian National Academy of Sciences, 2, 12: 29-36
[4] Gagnidze A., Iavich M., Iashvili G., (2017) Analysis of post-quantum cryptography use in practice. Bulletin of the Georgian National Academy of Sciences, 2, 12: 29-36
[5] Gagnidze, A., Iavich, M., Iashvili, G., Novel version of Merkle cryptosystem, Bulletin of the Georgian National Academy of Sciences, 2017
[6] Iavich, M., Gagnidze, A., Iashvili, G., Hash based digital signature scheme with integrated TRNG, CEUR Workshop Proceedings, 2018
[7] D. Gottesman, H. -. Lo, N. Lutkenhaus and J. Preskill, "Security of quantum key distribution with imperfect devices," *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, Chicago, IL, USA, 2004, pp. 136-, doi: 10.1109/ISIT.2004.1365172.
[8] Diamanti, E., Lo, HK., Qi, B. *et al.* Practical challenges in quantum key distribution. *npj Quantum Inf* **2,** 16025 (2016). https://doi.org/10.1038/npjqi.2016.25
[9] Li, HW., Yin, ZQ., Wang, S. *et al.* Randomness determines practical security of BB84 quantum key distribution. *Sci Rep* **5,** 16200 (2015). https://doi.org/10.1038/srep16200
[10] Kalra M., Poonia R.C. (2019) Design a New Protocol and Compare with BB84 Protocol for Quantum Key Distribution. In: Bansal J., Das K., Nagar A., Deep K., Ojha A. (eds) Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing, vol 817. Springer, Singapore. https://doi.org/10.1007/978-981-13-1595-4_76