Information & Security

Published since 1998

Niemiec, Dziech, Stypiński & Derkacz,
vol. 43, no. 1 (2019): 62-72
https://doi.org/10.11610/isij.4306

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Quantum-based Solutions for the Next-generation Internet

Marcin Niemiec* (✉), *Andrzej Dziech*, *Miłosz Stypiński, Jan Derkacz

AGH University of Science and Technology, Mickiewicza 30, 30-059 Krakow, Poland
http://agh.edu.pl

ABSTRACT:

Quantum physics influences modern computer science and communications. We observe new quantum-based solutions which are being implemented in practical networks. This article introduces these techniques and explains how they can change the next-generation Internet and communication. The basics of quantum mechanics and such effects as birefringence and entanglement are briefly introduced. Next, the most popular quantum-based solutions which are good candidates for modern services in the next-generation Internet are described. The quantum key distribution process, as well as the idea and validation of a quantitative approach to security in quantum cryptography, are presented. In addition to security methods, quantum-based solutions for data processing and transmission are explained: superdense coding, the medium access control protocol with quantum entanglement and the idea of quantum computing. The final section concludes the article and indicates current initiatives and future directions.

ARTICLE INFO:

RECEIVED: 19 SEP 2019
REVISED: 28 AUG 2019
ONLINE: 17 SEP 2019

KEYWORDS:

quantum techniques, next-generation Internet, communications, security

✉ Corresponding Author: Tel.: +48 126173937; E-mail: niemiec@kt.agh.edu.pl

Introduction

Interest in quantum-based mechanisms for communications is growing rapidly. Solutions such as quantum cryptography or quantum random number generators are not just theories, but are being used in practice. However, these mechanisms are not very widespread as yet; they will probably form part of the next-generation Internet.

The main advantages of these methods are security and performance. Quantum-based cryptography and true random number generators increase security to a level unachieved by any previous solutions. Superdense coding and other techniques based on quantum entanglement can improve the bit-rate of communication systems. It seems that even technological problems such as effective quantum repeaters will be solved in the near future. Then, quantum-based solutions will be widely implemented in practical networks.

This article presents a few quantum-based solutions which are developing rapidly. Some of them are already being used in practice. Others are still theoretical models and have not been implemented yet. Nevertheless, all of them aspire to be components of the next generation of communications.

Quantum Basics

Quantum mechanics is a special branch of physics. It describes the behaviour of matter and energy at the atomic and subatomic levels. Nowadays, some features of quantum mechanics are being used to design new methods of improving the security and performance of modern communication networks. At the beginning of this article, some of the principles and models which have a direct connection with quantum-based solutions for communications will be presented.

Qubit

A *bit* is a basic term of communications and computer science. It is a unit of computer information which can have only two possible values: 0 or 1. A unit of quantum information is called a *qubit* (quantum bit). A qubit can have two possible values (normally 0 or 1). However, it can also be a superposition of both. This superposition can be presented as a vector in the Bloch sphere (Figure 1) – an abstract sphere with antipodal opposite points representing two specific states. Two extreme opposite points in the sphere are conventionally written as $|0\rangle$ and $|1\rangle$. Any quantum state is called *ket* and presented as $|\psi\rangle$.

We can assume that each state in quantum mechanics is represented as a vector in Hilbert space. Then, two basic states, $|0\rangle$ and $|1\rangle$ are orthonormal and we can define a given qubit as a superposition of two orthonormal quantum states:

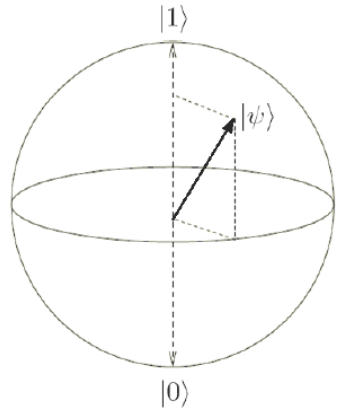

Figure 1: A qubit in the Bloch sphere.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

where:

$$|\alpha|^2 + |\beta|^2 = 1$$

This means that when we perform a measurement on a qubit, we obtain the state $|0\rangle$ with the probability $|\alpha|^2$ or the state $|1\rangle$ with the probability $|\beta|^2$. Therefore, the sum of these probabilities equals 1. This physical interpretation means that the quantum state before the measurement could be in superposition, but the measurement may damage this state. The object's state will be determined by the measurement and will be equal to $|0\rangle$ or $|1\rangle$. This observation leads directly to the Heisenberg Uncertainty Principle.

Heisenberg Uncertainty Principle

In 1927, Werner Heisenberg published one of the fundamental principles of quantum physics.[1] He proved that it is not possible to measure accurately both the position and momentum of a physical system. These quantities can only be determined with some characteristic uncertainty. The mathematical notation of this principle is presented as follows:

$$\Delta x \cdot \Delta p \geq \frac{h}{4\pi}$$

where Δx and Δp are measurement uncertainties of a particle's position and momentum respectively, and h is Planck's constant $(h \approx 6.626 \cdot 10^{-34}\, J \cdot s)$. This well-known equation shows that measuring the position of a particle with high precision makes it impossible to measure momentum precisely. In general, the Uncertainty Principle states that it is impossible to measure some physical quantities with the same, high precision. Position and momentum are only one example of these pairs. Another example is the polarization of photons.

Birefringence

Birefringence is the decomposition of light into two rays when it passes through certain materials – for example, calcite crystals. The decomposition depends on the polarization of the photons. We can assume that:

- horizontally-polarized photons appear in the upper ray,
- vertically polarized photons appear in the lower ray.

Diagonally polarized light (45°) is decomposed into two rays: some photons appear in the upper ray and the rest will be observed in the lower ray of the calcite crystal. However, if we pass a single photon with the polarization 45°, it cannot be simultaneously vertical and horizontal at the output. It 'chooses' only one of the polarizations, with a probability of ½. An experiment with polarized photons and a birefringent calcite crystal is presented in Figure 2. Using the considered calcite crystal, we are able to measure perfectly the photons with vertical and horizontal polarizations (0° and 90°). However, we lose information about diagonally-polarized photons.

Entanglement

Usually, the quantum state of single particles is independent of others. However, we can produce pairs of particles which interact in a very interesting way: if we measure the state of one particle, then the state of the second particle can be fully determined. This means that we need only measure one particle to know the states of both. Additionally, the states of the particles are completely random before measurement occurs. The entangled state of two different particles (indices 1 and 2) can be presented as:

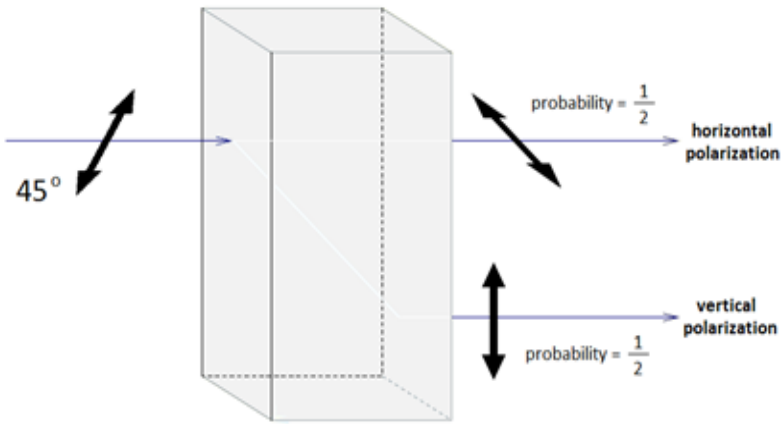

Figure 2: Polarized photon (45°) entering a birefringent calcite crystal.

$$\frac{1}{\sqrt{2}}(|\updownarrow\rangle_1 |\leftrightarrow\rangle_2 + |\leftrightarrow\rangle_1 |\updownarrow\rangle_2)$$

This means that if the first particle has vertical polarization, the second has horizontal polarization, and if the first particle has horizontal polarization, the second has a vertical polarization. Both possibilities can appear with a probability ½. It should be noted that the entanglement phenomenon still retains this feature, even if the particles are separated by great distances.

Quantum-based Solutions

Interest in quantum effects for computer science and communications continues to grow. In this section, the most popular quantum-based solutions are presented. They are good candidates for modern services in the next generation of the Internet and communications.

Quantum key distribution

Secure distribution or agreement of encryption keys are crucial to data confidentiality. Currently, when we use modern ciphers with popular key distribution methods, we are not sure if an intruder is eavesdropping on the communication. In this way, a hidden intruder can scan the network and obtain sensitive data. Quantum key distribution ensures a very high level of security, because it is not possible to eavesdrop on the communication in a passive way.[2] If an eavesdropper reads the distributed key, this will change the quantum states of the photons and will thus be revealed. This is possible because measurement influences the quantum state, and it is not possible to clone an unknown quantum state.

Popular quantum key distribution protocols, such as BB84,[3] are based on the polarization of single photons, which carry information coded in quantum states (i.e. different polarizations: vertical, horizontal, diagonal). In this way, the recipient and potential eavesdropper do not know which detector should be used to measure the polarization precisely. It is not a problem for the intended recipient – when they announce the configuration of a detector which was used during the measurement of a received photon, the sender confirms that the obtained result is correct or asks for this bit to be deleted from the final key because the obtained result is not certain.

What about eavesdropping on a quantum distributed key? If the eavesdropper chooses an inappropriate detector to perfectly measure the polarization, the polarization of the photon is changed. Sender and recipient uncover the eavesdropper if they compare part of the obtained key. In this way, passive eavesdropping is not possible. If someone wants to eavesdrop photons and read confidential information, they will change the quantum states of the photons.

Quantum cryptography

Quantum key distribution ensures a very high level of security. However, it is only part of the complete key establishment process. For example, the sender and recipient must estimate errors in the distributed key by computing the Quantum Bit Error Rate (QBER). The QBER is defined as the ratio of the number of wrong bits to the total number of bits. It is worth emphasizing that not only Eve is responsible for errors – they may occur because of disturbance in the quantum channel, optical misalignment, noise in detectors, and so on.
After the bit error estimation, Alice and Bob use key distillation protocols. These protocols usually involve two steps:

- key reconciliation – in this step sender and recipient must find and correct or delete occurred errors,
- privacy amplification – sender and recipient should strengthen their privacy and construct the final key by deleting some of the distributed bits.

However, effective management of security and efficiency in quantum cryptography is needed. To solve this problem, Niemiec and Pach considered security in a quantitative way.[4, 5] This approach is crucial when we want to map different end-user requirements to a quantum cryptography system. Using this strategy, end-users can choose an appropriate security level. In reference to the measure of information introduced by Hartley,[6] the measure of security *J(k)* in quantum key distribution was proposed. This function was defined as:

$$J(k) = \log \frac{k}{n}$$

where *log* represents the natural logarithm, *k* is the number of uncovered bits, and *n* is the length of the key. Additionally, the entropy of security and function of entropy of security *S(k)* in quantum cryptography were defined. This function is analogous to the entropy defined by Shannon [7] and was defined as:

$$S(k) = -\frac{k}{n} \log \frac{k}{n}$$

If we divide the function *S(k)* by the number of bits *n*, we obtain a general relationship which we can use to control the security and efficiency of a system with quantum cryptography. Additionally, this function has one maximum in the value 0.1 (it corresponds to the situation when we uncover and compare approx. 37 % bits of the distributed key). Therefore, we are able to define two different levels of security: basic and advanced. This idea makes it possible to personalize end-users' security.

The approach was verified by numerous simulations [8] performed with a QKD Simulator tool.[9] The simulator calculated the difference between real values of QBER (called *true_QBER*) and QBER calculated using the proposed

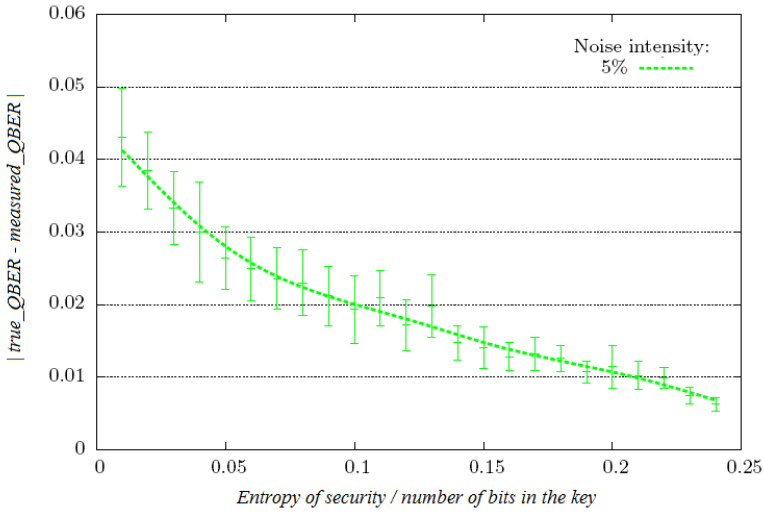

Figure 2: Validation of a quantitative approach to security in quantum cryptography (simulations of QBER).[8]

method (called *measured_QBER*). During the simulations, the length of all distributed keys was 1000 bits; however, the eavesdropped bits were different, ranging between one and 1000 bits. Figure 3 presents the results of simulations with noise intensity of 5% – typical noise in real quantum channels. The function in the graph is decreasing, with the most significant changes (exponential curve) observed at the basic security level (for values smaller than 0.1). Smaller changes (linear curve) are observed at the advanced security level (for values greater than 0.1). This means that at the basic security level, security increases faster than at the advanced level.

Quantum random number generator

The generation of random numbers plays a crucial role in many modern applications, mainly used by the security services. The security of encrypted data is based on the strength of its keys. Therefore, the keys must be generated randomly. Otherwise, an intruder can predict the key and read confidential data. Random numbers are also needed in other applications – during numerical simulations of complex systems, in the gaming industry, etc. Nowadays, software generators are commonly used. Unfortunately, computers are deterministic systems, and they produce pseudo-random numbers. Therefore, it is impossible for a software program to generate a sequence of truly random numbers.

Because of the principles of physics, quantum-based generators are an excellent source of randomness. One example is a photon with polarization 45° entering a birefringent calcite crystal (Figure 2). We have already mentioned that a photon with the polarization 45° 'chooses' only one of two possible polarizations (0° or 90°) with a probability of ½. We can put detectors at the outputs of

the crystal and detect the resultant photons. Horizontally-polarized photons appearing in the upper ray can generate bit 0, and vertically polarized photons appearing in the lower ray can generate bit 1. This can be an excellent random number generator.

Another example is transmission upon a semi-transparent mirror; this solution is implemented in practice.[10] A single photon can be reflected or transmitted. It is intrinsically random, and any external parameters do not influence this process. Using this technique, sequences of truly random numbers can be produced.

Quantum communications

Quantum effects support not only data security, but also the efficiency of communication networks. An example of such a solution is superdense coding. Using superdense coding it is possible to send two bits of classical information using just one qubit.[11] To achieve this improvement, both the sender and recipient must share an entangled pair of photons. If the sender wants to send a two-bit message (four different possibilities: 00, 01, 10 or 11), they perform a single qubit operation on their qubit. This operation transforms the qubit into one of four orthonormal states – according to the message which the sender wants to send. Now, the transformed qubit is sent to the recipient, who can perform a measurement on the joined pair and obtain the two-bit message.

Another example proposes applying quantum effects to ALOHA, a well-known medium access control (MAC) protocol. There, entangled pairs of photons can improve the capacity utilization of shared media. In systems using slotted ALOHA, the time dimension is divided into time slots.[12] At the beginning of each slot, users decide whether to send a packet or not. For two users, the packet will be successfully delivered if only one user transmits in a single time slot. If neither user sends a packet, or both users attempt to send their packets in the same time slot, the transmission is lost. Therefore, only half the time slots will be utilized on average. How can this be improved? Sandor Imre presents a system using the ALOHA protocol and shared entangled pairs of photons.[13] In the proposed system, even the packet collision and the unused channel carry information. Therefore, sending one classical bit and using quantum entanglement, it is possible to transmit as many as 2.5 classical bits on average. This significantly improves the efficiency of communication.

Quantum computer

The evolution of quantum mechanics emerged into another direction of quantum-based solutions which is quantum computing. The operation of a quantum computer is essentially different from a standard one. Instead of operating on bits, a quantum computer uses qubits as a basic mean of data in its registers. Hence, the state of the register can be presented as a superposition of all possible values of an n-length vector from $\{0,1\}^n$ space,[14] which can be defined as:

$$|\psi\rangle = \sum_{x=0}^{n} \alpha_x |x\rangle$$

where:

$$\sum_{x=0}^{n} | \alpha_x |^2 = 1$$

Not fully deterministic nature of quantum computer creates new opportunities as well as new threats to computing and communications. Regarding a few types of computing problems, the quantum computer enables the usage of quantum algorithms which solve the task in a more efficient manner. Example problems which are possible to solve on the quantum computer are searching the unstructured database using Grover's algorithm [15] and integer factorization and finding a discrete algorithm using Shor's algorithm.[16]

The latter algorithm is a potential threat to global cybersecurity. Using Shor's algorithm implementation on a powerful quantum computer could break the fundamental security of commonly used asymmetric cryptography. However, the post-quantum cryptography is a trend that aims to develop quantum-proof security algorithms.

Further development

The transition towards quantum communication and the Internet can be divided into few milestones. Each of them is an important improvement in the quality and security of quantum-based solutions.[17]

Currently, the technology allows us to create a trusted repeaters network in order to perform QKD. This solution is based on a trusted node between the sender and receiver, which extends the maximum distance between the communicating parties and removes the need for a full mesh network. The next steps to achieve end-to-end quantum communication are to prepare and measure networks. These networks enable the transmission of prepared one-qubit state to any node in the network. Security-wise this step is a significant improvement due to the fact that the intermediary node is superseded. This means QKD is available between any nodes in the network since any eavesdropping disturbs the quantum state of transmitted qubits.

Further development of quantum technology could result in the ability to share entangled qubits between any two nodes in the network. Here, the nodes are assumed to have a capability of deterministically measuring the state of the qubit. More advanced technology would enable nodes to store the state of the qubit for some time using quantum memory. This would allow performing blind quantum computing, secret sharing, and time-limited clock synchronization. The last step is the transition from each node being capable of performing small few-qubit fault-tolerant operations to full quantum computing.

Conclusions

Security is one of the most important challenge of modern telecommunications.[18] Entirely new ways of solving problems of security and performance are

currently being developed. Laws of physics ensure that every eavesdropper can be uncovered, bit rates can be increased, truly random numbers can be generated, etc. Some of these solutions are already being implemented; however, they are not very popular because such communication systems need to work under special conditions (i.e. direct quantum channel between the sender and the recipient). Other techniques are still at the theoretical model stage and have not been applied yet. Nevertheless, quantum-based solutions allow users to improve the security and performance of communication networks. Therefore, quantum-based services should become popular solutions in the next-generation Internet.

Acknowledgement

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

References

[1] Werner Heisenberg, "Uber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," *Zeitschrift fur Physik*, 43 (1927): 172–198.

[2] Gilles Van Assche, *Quantum Cryptography and Secret-Key Distillation* (Cambridge: Cambridge University Press, 2006).

[3] Charles H. Bennett and Gilles Brassard, "Public Key Distribution and Coin Tossing," *IEEE International Conference on Computers, Systems, and Signal Processing* (1984), 175–179.

[4] Marcin Niemiec and Andrzej R. Pach, "The Measure of Security in Quantum Cryptography," *IEEE Global Telecommunications Conference - GLOBECOM* (2012).

[5] Marcin Niemiec and Andrzej R. Pach, "Management of security in quantum cryptography," *IEEE Communications Magazine* 51, no. 8 (2013): 36–41.

[6] Ralph V. Hartley, "Transmission of information," *Bell System Technical Journal* 7 (1928): 535–563.

[7] Claude E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal* 27 (1948): 379–423, 623–653.

[8] Marcin Niemiec, "Design, Construction and Verification of a High-Level Security Protocol Allowing to Apply the Quantum Cryptography in Communication Networks," Ph.D. Thesis, AGH University of Science and Technology, 2011.

[9] Marcin Niemiec, Łukasz Romański and Marcin Święty, "Quantum cryptography protocol simulator," Multimedia communications, services and security, volume 149 of Communications in Computer and Information Science, Springer Berlin Heidelberg (2011): 286–292.

[10] ID Quantique White paper, "Random number generation using quantum physics," April 2010.

[11] Charles H. Bennett and J. Wiesner, "Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states," *Phys. Rev. Lett.* 69, (1992): 2881-2884.

[12] Lawrence G. Roberts, "ALOHA Packet System With and Without Slots and Capture," *Computer Communications Review* 5, no 2 (1975): 28–42.

[13] Sandor Imre, "Quantum Hyperdense Coding for Distributed Communications," *Quantum Physics*, *arXiv:1210.2856* (2012).

[14] Artur Ekert, Patrick Hayden, and Hitoshi Inamori, "Basic concepts in quantum computation," *Quantum Physics, arXiv:quant-ph/0011013* (2010).

[15] Lov K. Grover, "A fast quantum mechanical algorithm for database search," *Quantum Physics, arXiv:quant-ph/9605043* (1996).

[16] Peter W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA (1994): 124-134.

[17] Stephanie Wehner, David Elkouss, Ronald Hanson, "Quantum Internet: A Vision for the Road Ahead," *Science* 362, no 6412 (2018).

[18] Paweł Korus and Andrzej Dziech, "Efficient Method for Content Reconstruction with Self-Embedding," *IEEE Transaction on Image Processing*, vol. 22, no 3 (2013): 1134 - 1147.

About the Authors

Marcin **Niemiec** was awarded his PhD and PhD Hab. in telecommunications in 2011 and 2019 respectively. Currently he works as assistant professor at the Department of Telecommunications, AGH University of Science and Technology, Poland. His research interests focus on cybersecurity. He has been involved in numerous European projects (FP6, FP7 and H2020). He is the co-author of over 80 publications. E-mail: niemiec@kt.agh.edu.pl.

Andrzej **Dziech** received his PhD.Hab. in telecommunications. He is full professor since 1986. His fields of interest are related to digital communication, image and data processing, information and coding theory, intelligent monitoring, data protection. He is the author of 240 publications, including 5 books and he was supervisor of 19 Ph.D. students. He was coordinator of many national and international projects, including the FP7 project INDECT.

Miłosz **Stypiński** received his B.SC in ICT from AGH University of Science and Technology, Krakow, Poland in 2018. Now, he is a M.Sc. student of ICT at AGH University of Science and Technology. His current research interests focus on cybersecurity and data analysis.

Jan **Derkacz** is a staff member of the Department of Telecommunications at AGH University of Science and Technology. He actively participated in several national and international research projects in the area of Information and Communications Technologies and Security.