XX IMEKO World Congress
Metrology for Green Growth
September 9–14, 2012, Busan, Republic of Korea

POSITION-BASED QUANTUM CRYPTOGRAPHY IN THE DISTRIBUTED MEASUREMENT SYSTEM

Piotr Bilski[1,2], *Wiesław Winiecki*[1]

1) Institute of Radioelectronics, Warsaw University of Technology, Warsaw, Poland, pbilski@ire.pw.edu.pl, W.Winiecki@ire.pw.edu.pl
2) Faculty of Applied Informatics and Mathematics, Warsaw University of Life Sciences, Warsaw, Poland, piotr_bilski@sggw.pl

Abstract: The paper presents the analysis of a secure transmission channel between nodes in the distributed measurement system. Its security is discussed, using the position-based scheme, where each node is authenticated based on its geographical position. To decrease the threat of the adversary disguising as the authorized node and eavesdropping the transmission, the quantum cryptography scheme is used. The paper presents the modifications and practical implementation issues of such a communication scheme in the distributed measurement system. Time measurement accuracy and clock synchronization are considered, as well as technical difficulties in delivering the secure quantum channel in the open space.

Keywords: quantum cryptography, distributed measurement systems, authentication schemes

1. INTRODUCTION

Distributed measurement systems (DMS) became the standard in the automation and control applications. Introduction of the fast computer equipment facilitated creating more universal and flexible approaches. The same microcontrollers or programmable logical controllers (PLC) can be used for multiple purposes, depending on their selected configuration of the software controlling the measurement task. Abilities of the specialized computers allow for increasing the number of measurements taken at each location and processing them on-site. Also, with the rising accessibility to communication media, even the simplest devices contain network interfaces. This increases the range and expands applications of DMS, but also introduces security threats, which may compromise the measurement and control operation [1].

The secure transmission of measurement data is an important topic in the age of terrorism and ubiquitous access to the computer networks. Multiple structures delivering services to the society (power plants, water supply stations, traffic control centers) are now partially or fully automated, which is possible thanks to the reliable and efficient hardware. The rising amount of micro- electromechanical systems (MEMS) will be used to gather multiple measurements and send them to servers through the central cloud-based storage. Unfortunately, this facilitates intruder attacks, aiming at taking control over the system or damaging it beyond repair. Therefore sophisticated cryptographic protocols must be used to prevent compromising the system by the potentially the attacker.

The paper presents the application of the position-based cryptography to ensure safety and integrity of measurement data, transmitted within the DMS. This new idea was already considered for application in distributed systems, including sensory networks [2]. To increase security of the system, the quantum cryptography protocol was added to the scheme [3]. The following paper considers applying this methodology to the specific applications of DMS, including measurement and processing nodes. Apart from theoretical aspects, practical problems are also considered here. The architecture and simplified model of the contemporary DMS is in section 2. Fundamentals of the cryptography for the needs of the DMS are in section 3. The position-based quantum cryptography key exchange protocol is in section 4, while section 5 contains practical issues related to the possible implementation of the protocol. Section 6 contains conclusions and future prospects of the proposed scheme.

2. SECURITY OF DMS

The contemporary DMS is a versatile heterogenic system, containing various nodes, depending on their purpose and hardware capabilities [4]. There are two categories of nodes: measurement and processing (Fig. 1). The former are responsible for obtaining measurement data from the outside world and, optionally, processing then immediately. The second group consists of devices responsible for storing and processing data obtained from remote measurement nodes. They can also work as the control nodes, sending commands to the measurement nodes. Two problems cause the security threats there. Firstly, the computational power of the measurement nodes is limited and additional effort imposed by the cryptographic algorithms may be unacceptably high. This is the case for small microcontrollers or intelligent sensors, powered by batteries. The solution may be the additional module responsible only for encryption of the measured data, which would be safely transmitted to the processing node immediately after acquisition. The problem is the limitation of the power consumed by the remote node. Therefore

cryptographic methods must be simple [5]. This problem usually does not exist on the processing node, which is the personal or industrial computer with relatively high computational resources. Contemporary trends of stressing ecological aspects in technology (such as energy scavenging) prefer power-saving methods and algorithms. Therefore efficient cryptographic methods on both sides of communication are preferred.

The second problem is the character of the transmission medium. In industrial applications, critical for the society, specialized networks are used, next to the Ethernet standard computer network. To ensure the safety from the outside-world intruders, such a system is usually separated from any widely accessible medium (such as the Internet). To discuss the security of the modern DMS we make the following assumptions:

- the attack comes from within the system, which must be physically penetrated.
- The intruder is unable to take control over the nodes directly, but only by sending remote commands.
- The weakest point in the DMS infrastructure is the transmission medium.
- The size of the DMS is limited to no more than 1-2 km.

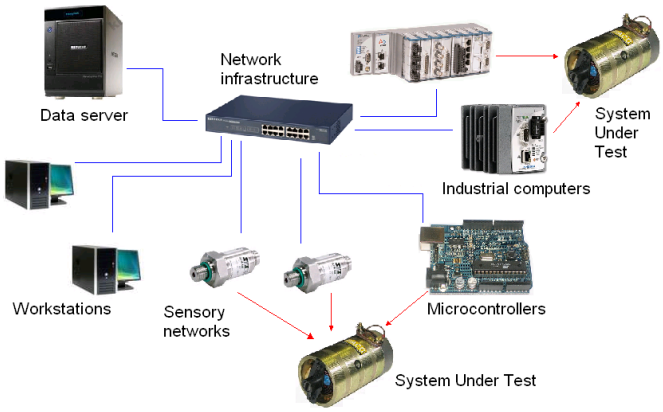

Fig. 1. Architecture of the DMS

The attacker must use the communication network utilized by the DMS. It is possible by positioning him within the range of the wireless network or by connecting to the cable in the case of the wired network. Although computer transmission protocols are well established and used in industrial applications, some systems require individual methods and protocols, fostering the development of alternative cryptographic approaches [6].

3. POSITION-BASED CRYPTOGRAPHY IN DMS

This is the novel type of cryptography, facilitating authentication and safe data transmission [6], suitable for the wireless communication, especially between sensors within the smart dust [7]. It simplifies the cryptographic key management (generation and distribution), which is the most difficult task. The main idea here is that the node proves that is the valid participant of the communication system by providing its geographical position. It is entitled to send measurement data and receive commands from the control nodes only if the position is correct with the value previously agreed between participants of the DMS. Such a node is called a prover (P). Its position is determined by measuring the time of sending and receiving the control messages to and from other nodes, which verify if P is the part of the legitimate communication scheme. These nodes are called verifiers V_i ($i=1,\ldots,n$). Only if the response from the prover returns to the verifiers "in time", it is considered as the authentic node of the DMS. In the scheme illustrating the position-based communication (Fig. 2), $d(P,V_i)$ is the Euclidean distance between the prover and one of verifiers.

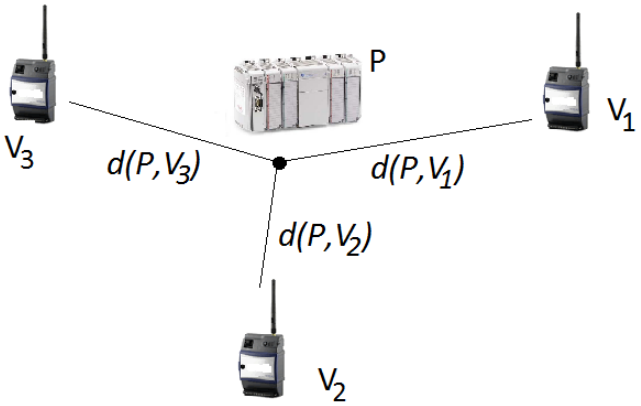

Fig. 2. Scheme of the position-based cryptography.

To successfully implement this type of cryptography, the number of verifiers in DMS must be at least greater by one than the number of the considered dimensions [3]. In practical applications the maximum number of three dimensions is needed, but increasing number of verifiers increases the accuracy of the algorithm (Fig. 3). All verifiers generate and send their control messages m_i to P in a way that all reach it in the same time (operations gen_mes and send_mes). The prover must process these messages (proc_mes) and resend responses r_i (operation send_resp) in a way that all V_i get them in the same moment (operation recv_resp). Finally, all verifiers agree that P is the authorized node of the DMS. If the time measurement was available with the infinite precision, the only node able to send r_i in time would be P. This ensures that the attackers A_j ($j=1,\ldots,m$) located inside the DMS would never be mistaken with the legitimate node, although they can acquire all m_i and send r_i. Because the time instants of the transmission m_i are fixed to the position of P, any other node is not able to obtain all of them at the same time and respond accordingly.

pos_auth(P, $V_1,\ldots,V_n$)
  $\boldsymbol{m}$=gen_mes($V_1,\ldots,V_n$)
    send_mes($V_1,\ldots,V_n$, $\boldsymbol{m}$)
  $\boldsymbol{r}$=proc_mes(P, $\boldsymbol{m}$)
    send_resp(P, $\boldsymbol{r}$)
    recv_resp($V_1,\ldots,V_n$,$\boldsymbol{r}$)

Fig. 3. Position-based authentication scheme [3].

In practice, the transmission time is known with limited accuracy. Therefore attackers located close to P may try to intercept messages m_i and immediately respond, pretending to be the authorized nodes. Depending on the accuracy of

timers in V_i, the probability of such a case is ε. In [3], the position of P was assumed known to all V_i and A_i. The latter might be able to calculate the moments of resending the data to V_i, therefore the initial scheme of the authentication is not secure. The problem is even more serious, when the number of attackers is equal to number of verifiers and every attacker is responsible for covering only the closest verifier to its position. Synchronized attackers knowing position of each other and P, will jam the latter and take over its role.

4. QUANTUM POSITION-BASED AUTHENTICATION SCHEME

Introducing the quantum cryptography to the position-based scheme increases security of the DMS. The most common key-exchange protocols (QKD) are four-state BB84 [8] and two-state B92 [9]. The first one is used in transmissions of the highest security (for example, some bank transfers [10]). The main application of QKD is the key exchange. In DMS such methods can be used to minimize the chance of the successful attack on P. A complex method for generating r_i in response to m_i must be proposed. The quantum (n-qubit) state is shared between P and all V_i, besides some classical information: p and v_i. The 2-qubit state - EPR pair (1) is the simplest one applicable:

$$\left|\Psi\right\rangle_{AB} = \frac{\left(\left|0\right\rangle\left|0\right\rangle + \left|1\right\rangle\left|1\right\rangle\right)}{\sqrt{2}} \qquad (1)$$

The quantum state is a set of such EPR pairs [11] (one for each (P, V_i)), therefore usage of the quantum teleportation to exchange information about values of qubits is possible. The transmission is executed in the same time between all pairs to generate the full quantum and classical information. The former is transmitted using the quantum channel, i.e. by the agreed pair of qubits, manifesting the quantum entanglement property [12]. This way both nodes read the same value of the qubit (although no traditional communication between them is executed). To obtain bits from the quantum states, Bell measurements must be performed in the particular basis (which is a randomly selected bit). The classical information is sent through the traditional medium (air). The aim of this procedure is to calculate the new quantum state (1)

$$\left|\Phi\right\rangle_{\bar{A}\bar{B}} = U_{p,v_i}\left|\Psi\right\rangle_{AB} \qquad (2)$$

where $U_{p,vi}$ is the set of fixed unitary operators (known to all parties) transforming the state $\left|\Psi\right\rangle$ into $\left|\Phi\right\rangle$. This way, using the quantum bits teleportation each node concatenates the new classical information (obtained from measuring qubits) to the previously possessed. Finally all parties exchange their fragments of the classical information to obtain the new quantum state (1).

The security of QKD is based on the no-cloning property of the quantum state. If the intruder intercepts the state and reads its value, it can't be passed to the prover without compromising the eavesdropper. However, such a scheme can be attacked by n intruders, who locate themselves on the path between P and subsequent V_i (each verifier is "covered" by one A_i). When A_i obtain their m_i, they use the teleportation to calculate the operator U, and subsequently generate r_i, immediately sent to verifiers (Fig. 4).

In [3], the position-based authentication protocol, resilient to such an attack, was proposed. It requires the private communication between verifiers. If intruders do not have any information about entangled states (used for teleportation between V_i and P), the BB84 scheme can be applied (Fig. 5). First, verifiers select a set of random bits $\boldsymbol{X}$ and exchange them (operation gen_qubit_base). In the simplest case they are classical bits x, θ and the qubit $H^{\theta}\left|x\right\rangle$. To calculate x, the node P requires both the bit θ and the qubit, which must be obtained at the same time (operation send_mes). The P calculates x by measuring the qubit in the basis of θ (operation proc_mes) and returns x to verifiers (operation send_resp). The node P is considered authentic only if the value of x is correct and it is revealed on time (operation recv_resp).

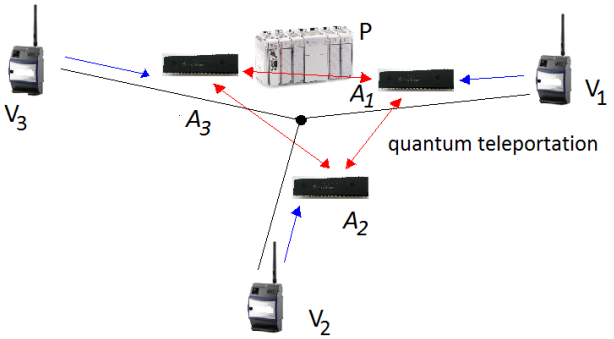

Fig. 4. Illustration of the attack of intruders on the position based scheme.

quant_pos_auth(P, V_1,…,V_n)
  $\boldsymbol{X}$=gen_qubit_base(V_1,…,V_n)
    send_mes(V_1,…,V_n, $\boldsymbol{X}$)
  x=proc_mes(P, $\boldsymbol{X}$)
    send_resp(P, x)
    recv_resp(V_1,…,V_n,x)

Fig. 5. Position-based quantum authentication scheme [3].

Such a scheme is efficient as long as the probability ε of guessing the transmitted bit value is acceptably low. To decrease ε, one must repeat the scheme from Fig. 5 multiple times. Their number depends on the desired level of security. This approach is used not only to authenticate the position of each node, but also during the transmission. Currently such a method is considered safe and recommended for the measurement nodes with limited computational power.

5. IMPLEMENTATION ISSUES IN DMS

The presented scheme is theoretically correct and ensures security of the DMS with the high probability (increasing with each round of the quantum state calculation). Its practical implementation considers the method of implementing the quantum states, time

measurement and security assurance. The following section discusses these problems.

5.1. Quantum states realization

The quantum states exchanged between nodes are implemented by the pairs of entangled quantum states (usually represented by particles of light). Two methods are applicable here: faint laser pulses, emitting single photons, or entangled photon pairs. Transmission using both approaches is in Fig. 6, where photons are detected by Avalanche Photo Diodes (APD). They are currently the most accurate receiving devices.

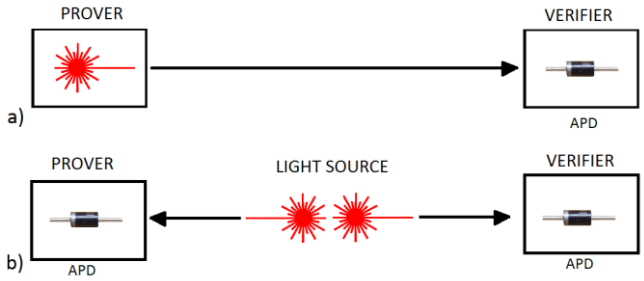

Fig. 6. Methods of transmitting the quantum state: using faint laser pulses (a) and through entangled photon pairs (b)

The first method requires the precise source of photons (faint laser pulses) [13]. The main problem is the stochastic nature of the light source, making generation of a single photon difficult, expressed by the Poison statistics (3):

$$p(n) = \frac{\mu^n}{n!} e^{-n} \tag{3}$$

where $p(n)$ is the probability of generating n photons and μ is the mean photon number generated by the source. If the laser generates multiple photons (identical copies), they can be used by the intruder to intercept the QKD.

The quantum-entangled photon pairs can be generated by some crystals. Currently practical methods of transmission systems are proposed [14]. The Ekert protocols use advantages of this method [15]. Currently there are no applicable devices for the DMS, although this solution is more attractive, ensuring greater accuracy. The probability to generate multiple photons is comparable to faint laser pulses, but this method of generating the light is immune to beam-splitting attack. Unfortunately, it is also more difficult technically and expensive solution (because of the larger spectral width).

The other party of the transmission must be equipped with the detector sensitive enough to detect a single photon. This technology is considered safe, although in [16] was proven that if implemented improperly, the system can be compromised using off-the-shelf equipment to intercept the keys and leaving no trace of the attack. Its limitation is the speed of light. The main issue is the hardware realization of the system in the open space, where laser light is diffused in the air (which is described by the noise ratio). Currently applied avalanche photodiodes [17] are able to detect subsequent pulses with over 1 to 2.5 Gb/s efficiency [18]. This is sufficient throughput for most operations of the typical DMS, where scalar or vector numbers are transmitted from the measurement nodes. In the opposite direction the commands are sent from the control node.

Another problem is the size and power sources for the DAQ nodes. Current solutions in QKD assume relatively equipment including traditional hardware, such as FPGA in the transmitter and receiver [18]. Two applications of free space quantum cryptography were considered: computer network communication (Ethernet) and data exchange between satellites (or between the satellite and the ground station). The available power is in such cases is greater than in the measurement node (unless powered from the AC line) This limits contemporary solutions to large equipment.

The distance of the communication between the measurement nodes is also important. The assumed range of the considered system is up to a few kilometers, although recent experiments proved that the correct transmission over 140 km is possible [19]. The main problem is the interference with the environment, which depends on the applied wavelength and weather conditions. As transmission errors come from eavesdropping or failures of the link, it is necessary to ensure the lowest quantum bit error rate (QBER) possible (4).

$$QBER = \frac{n_e}{n_s} \leq E_{tr} \tag{4}$$

where n_s is the number of transmitted bits, n_e is the number of incorrect bits (because of eavesdropping or deficiencies of the transmission channel) and E_{tr} is the maximum acceptable value. Current research are aimed at lowering QBER below 1% (although even values at about 15 percent are sometimes acceptable) [20]. If the QBER is greater than the assumed value (determined considering the interference with environment), the eavesdropping is suspected. To obtain it, the combination of spectral, spatial and temporal filtering is used [21]. Currently acceptable values of the attenuation are about -70 dB, which delivers enough accuracy for the DMS at the range of 1 to 4 kilometers (considering the required line of sight between the laser and the detector). This is related to the quantum error correction, as cryptographic system works flawlessly only if the quantum channel is perfectly separated from the external environment. As it is hardly obtainable in practice, multiple methods are proposed to compensate for the loss of the quantum state. These approaches are still developed [22].

Another problem is the size and power requirements of the communication devices. DMS usually requires small, portable equipment, making the contemporary laser systems impractical. Both sources and receivers are from 25 to 50 cm. Although for the satellite system the node lens' aperture is relatively large (about 100 cm), the DMS of the local range (within 2 km) will require smaller lens. Currently there are no suitable low-power systems that could be installed in the small and remote measurement nodes.

The wavelength generated by the laser is important to avoid problems with increasing QBER. Therefore values above 650 nm are usually selected. This allows for sending the photons over long distances without the influence of the

background noise. Generally longer waves are easier detectable by APD, therefore the DMS would require light with length of about 800 nm.

The transmission speed for the designed DMS is relatively small, as single numbers and characters are sent in both directions. Contemporary QKD systems ensure the maximum speed of 10Mb/s in the open space (equal to the old Ethernet standard) This capacity is enough if the measurement nodes send only scalar values and receive short commands. Therefore for most cases (except, for instance, video transmissions), this speed would be acceptable for DMS applications.

5.2. Precision of time measurement

Precision of the time measurement affects the accuracy of the position verification. Existing methods are based on the time measurement. Precise timers are used for that purpose. Their top accuracy is about single picoseconds. It is suitable for measuring time in every distributed system. The main disadvantage of such a device is its price and physical dimensions [23], but in most cases cheaper and less accurate timers are sufficient. The time measurement for the distance calculation is as follows. After the verifier sends its message m_i, it starts the timer, which runs until the response from P is obtained. The time is calculated as in (5):

$$t_{pos} = \frac{t_m + t_r}{2} \approx t_m \tag{5}$$

where t_{pos} is the time required by the message to reach the prover and return to the verifier, t_m is the time of the message reaching the P and t_r is the time required by the response r to reach V_i. It is assumed that times of travelling both directions is the same, which might not be true. Also, t_{pos} is obtained after multiple repeats of the test measurements, where the mean value and the standard deviation is obtained. Similar methods are used in computer networks [24], but their efficiency depends on the range of the system. As the accurate time prediction in the Internet is impossible, the range of the secure DMS would also be limited to the area where transmission conditions are predictable, and standard deviation of repeated time measurements would be minimal. Still, the attacker located close to P can exploit the inaccuracies to send the message with the delay that will not be detected by verifiers. This problem will not be solved even by implementing the timers with the highest available accuracy. The quantum key distribution makes the attack more difficult, especially when intruders have no information about entangled states exchanged between the legitimate nodes. The latter, however, require additional secure channel to communicate.

Another consideration is the DMS with moving nodes. The scheme from [3] is designed for stationary parties. Implementation of the security protocol for mobile measurement nodes would require fast update on the times (3) related to the changing position of the node. This problem is presented in [25].

The time accuracy in the quantum part of the scheme depends on the synchronization between the devices. Theoretically they can be coupled with the infinite precision. In practice, the most important parameter is the jitter of the APD, determining what will be delay of receiving the photon. This can be exploited during the eavesdropping. To maintain the synchronization atomic clocks are used. Attempts to decrease the initial jitter of the APD are also made [18]. In the DMS, with the distance between nodes up to a few kilometers, the required clock precision must be as high as possible.

5.3. Security of the quantum key distribution

The security of QKD depends on the theoretical properties of the algorithms and their practical implementations. Most protocols (BB84, B92) ensure the security by creating long keys with multiple bits, from which some might be intercepted by the intruder. To obtain the extremely low probability of eavesdropping, both sides of communication must generate keys of the particular length. The practical aspect of ensuring the security depends on the used equipment. According to Fig. 6, there are two methods of transmitting quantum states. If the faint laser pulses are used, there is the problem of more than one photon generation, which makes the beam-splitting attacks possible [26]. They exploit the non-ideal nature of the light sources. As bases required for the quantum measurement to obtain the bit value are announced publicly, the attacker can intercept the non-ideal pack of many photons, store one of them in the quantum memory and send the rest to the original destination (without being detected). When the bases used for the measurement are announced, A_i measures the stored photon and obtains the required information. Although counter-measures were developed (decoy state protocol) [27], they require the minimal quality of the channel, otherwise the transmission will be impossible. To increase the precision of the light source, the Vertical Cavity Surface Emitting Laser (VCSEL) was proposed [28], which is more flexible than edge-emitting lasers. However, the probability of generating multiple photons is still non-zero, threatening the security of the system.

The security of the system based on entangled photon pair is currently verified. Recently the complex approach, based on blinding the APD was proposed [29]. Although it assumes usage of the fiber optics for the quantum information transmission, with small changes it can also be used to intercept qubits in the open air. The scheme assumes the position and number of attackers as in Fig. 4. This experiment shows that the security of the discussed system significantly limits the distance between the nodes [29].

6. CONCLUSIONS

The paper presented the analysis of the application of quantum position-based cryptography to the secure DMS. Details of the position-based verification were presented. Quantum key exchange scheme and its support for the introduced scheme was explained. Finally, advantages and weaknesses of the presented solution were discussed, especially considering practical implementation using the contemporary technology.

The practical implementation of the scheme requires the following features of the equipment used for the task:

- Small factor of QKD devices, coupled with measurement nodes
- Limited requirement for the power (possibly using energy scavenging)
- Laser light sources ensuring small QBER in the free space. This requires greater wavelengths (above 800 nm)

The security requirements of the protocols to be used in the DMS can be met by using keys long enough to minimize the eavesdropping probability. The main problem poses the equipment to execute the task. Currently it is in the preliminary stage of tests, therefore impossible to use in the practical applications. Also, the time is required to verify security of BB84, B92 and Ekert protocols implemented in the free space (as new methods of attack are still developed). It is believed that introduction of quantum computers would revolutionize cryptography and theory of computations. Currently the cost of the hardware is too large, making it implementable in banking and military. This makes applications in DMS not yet possible.

7. REFERENCES

[1] Winiecki W., Adamski T., Bobiński P., Łukaszewski R.: "Bezpieczeństwo rozproszonych systemów pomiarowo-sterujących (RSPS)" (Security of Distributed Measurement and Control Systems), Przegląd Elektrotechniczny (Electrical Review), vol. LXXXIV, no. 5 (2008), pp. 220-227.

[2] Y. Zhang, W. Liu, Y. Fang, D. Wu, "Secure localization and authenticationin ultra-wideband sensor networks," IEEE Journal on Selected Areas in Communications, no. 24, pp. 829-835, 2006.

[3] H. Buhrman, N. Chandrany, S. Fehrz, R. Gellesy, V. Goyalx, R. Ostrovsky, C. Schanerk, "Position-Based Quantum Cryptography: Impossibility and Constructions, " online: eprint.iacr.org/2010/275.pdf, 2010.

[4] P. Bilski, W. Winiecki, „Multi-core implementation of the symmetric cryptography algorithms in the measurement system," Measurement, No. 43, pp. 1049-1060, 2010.

[5] J. Olszyna, W. Winiecki, "Low-power implementation of Montgomery modular multiplication algorithm for distributed measurement and control systems," Electrical Review, no. 9a, pp. 69-71, 2011.

[6] N. Chandran, V. Goyal, R. Moriarty, R. Ostrovsky, "Position Based Cryptography," IACR Cryptology ePrint Archive, p. 364, 2009.

[7] M. D. Scott, B. E. Boser, K.S. J. Pister, "An Ultralow-Energy ADC for Smart Dust," IEEE Journal of Solid-State Circuits, vol. 38, no. 7, pp. 1123-1129, July 2003.

[8] C.H. Bennett, G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, 1984.

[9] C. H. Bennett. "Quantum cryptography using any two orthogonal states". Phys. Rev. Lett., Vol. 68, No. 21, 1992, pp. 3121-3124.

[10] "World Premiere: Bank Transfer via Quantum Cryptography Based on Entangled Photon," online: http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf, 21 April 2004.

[11] H.-Y. Tseng, J. Lin, T. Hwang, "New quantum private comparison protocol using EPR pairs," Quantum Information Processing, http://dx.doi.org/10.1007/s11128-011-0251-0, 2011.

[12] H. Buhrman, R. Cleve, W. van Dam, "Quantum Entanglement and Communication Complexity," SIAM J. Comput, vol. 30, no. 6, pp. 1829–1841, 2001.

[13] S. Felix, N. Gisin, A. Stefanov, and H. Zbinden, "Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses," Journal of Modern Optics, Vol. 48, Issue 13, 2001, pp. 2009-2021.

[14] A. Sharma, V. Ojha, "Quantum cryptography with photon pairs," International Journal of Engineering Science and Technology, Vol. 2(7), 2010, pp. 3320-3325.

[15] A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, "Practical quantum cryptography based on two-photon interferometry", Phys. Rev. Lett. 69, 1992, 1293-1296.

[16] M. J. Schwartz, "Quantum Cryptography Breached With Lasers," InformationWeek, online: http://www.informationweek.com/news/security/vulnerabilities/227300318 2010.

[17] M. Ghioni, S. Cova, A. Lacaita, and G. Ripamonti, "New silicon epitaxial avalanche diode for single-photon timing at room temperature", Electron. Lett., No. 24, 1988, pp. 1476-1477.

[18] D. J. Rogers, J. C. Bienfang, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, L. Ma, D. H. Su, Carl J. Williams, and Charles W. Clark, "Free-Space Quantum Cryptography in the H-alpha Fraunhofer Window," Proc. of SPIE Vol. 6304, 630417, 2006.

[19] R. Ursin, "Free-Space quantum cryptography over 144 km and a mission proposal for going into space", 2012, online: http://quantum.nasa.gov/materials/2012-01-21-A5-Ursin.pdf

[20] I. Ordavo, "Free-Space Quantum Cryptography," 2006, on-line: http://xqp.physik.uni-muenchen.de/publications/files/theses_diplom/diplom_ordavo.pdf

[21] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," New J. Phys. 11, 2009.

[22] M. D. Reed, L. DiCarlo, S. E. Nigg, L. Sun, L. runzio, S. M. Girvin, R. J. Schoelkopf, "Realization of three-qubit quantum error correction with superconducting circuits," Nature, doi:10.1038/nature10786, 2012.

[23] T. P. Celano, S. R. Stein, G. A. Gifford, B. A. Mesander, B. J. Ramsey, "Sub-Picosecond Active Timing Control over Fiber Optic Cable," 2002 IEEE Int. Freq. Control Symposium and PDA Exhibition, pp. 510-516.

[24] J. C. Eidson, "Measurement, Control and Communication Using IEEE 1588," Springer, April 2006.

[25] S. Capkun, M. Cagalj, M. Srivastava, "Secure localization with hidden and mobile base stations," IEEE INFOCOM, 2006.

[26] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, "Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol," Physical Review Letters, Vol. 84, No. 20, 2000, pp. 4733-4736.

[27] S. Ali, S. Saharudin, M. R. B. Wahiddin, "Implementation of Decoy State Protocol," European Journal of Scientific Research, Vol.33 No.1, 2009, pp.183-186.

[28] J. M. Ostermann, P. Debernardi, C. Jalics, A. Kroner, M. Feneberg, M. C. Riedl, and R. Michalzik, "Monolithic polarization control of multimode VCSELs by a dielectric surface grating," Proceedings of SPIE Vol. 5364, 2004, pp. 201-212.

[29] Q. Liu, I. Gerhardt, V. Makarov, J. Skaar, A. Lamas-Linares, V. Scarani, C. Kurtsiefer, "Full Eavesdropping on a practical QKD system," JTuC2 – CLEO:QUELS , 2. May 2011, Baltimore, on-line: http://qolah.org/papers/cleo2011.pdf.