Quantum Cryptography and Simulation: Tools and Techniques

Shuangbao Wang
Morgan State University
1700 E Cold Spring Road
Baltimore, Maryland 21251
+1 443-885-4503
shuangbao.wang@morgan.edu

Matthew Rohde
Columbus State University
4225 University Avenue
Columbus, Georgia 31907
+1 706-507-8183
matthew.rohde@csu.edu

Amjad Ali
Thomas Edison University
111 W. State St.
Trenton, NJ 08608
+1 609-984-1130
aali@tesu.edu

ABSTRACT
The advancement of quantum mechanics has accelerated the quantum computer architecture and hardware. However, algorithms and implementations to take the full advantage of entanglements provided by quantum devices are still far behind. Quantum cryptography offers the possibility of theoretically perfect security based on the principles of quantum mechanics, ensuring that the presence of an eavesdropper will be detected before any sensitive information is transmitted. However, the relevant technology is still under development – hardware, though commercially available, is still in an immature state, and the protocols used to implement secure communications using that hardware may still be improved. The use of simulations is an important tool for studying quantum cryptography, as they can enable researchers to make valuable insights at a relatively low cost. The data garnered from working with simulations can provide direction for further research both in the development of new communications protocols and in the improvement of actual hardware systems.

CCS Concepts
• Security and Privacy → Cryptography → Cryptanalysis and other attacks

Keywords
Quantum cryptography; Quantum key distribution; Security; Simulation.

1. INTRODUCTION
The threat on public key cryptography is growing. For the next decade or so, quantum computers will be able to instantly break the encryption of sensitive data protected by today's strongest encryption. The need for secure methods of electronic communication has increased by orders of magnitude in recent decades, as the use of the Internet for critical and sensitive communications in areas such as government, military, and financial transactions has expanded continuously. Traditional means of securing messages sent through public or otherwise unsecured channels have generally involved the application of cryptographic algorithms to encode the content of messages in a such a way that only the intended recipients should be able to decode and read them. In modern computer systems, this typically involves the use of one or more encryption keys that are used to encode and decode the data being transmitted. Aside from the possibility of an encoded message being compromised by sophisticated mathematical analysis (or even by brute force attacks, should a sufficiently powerful computer be available), one of the most important weaknesses of this kind of security is the possibility that the key needed to decode the message could itself be intercepted and copied. The most secure methods of encryption require that the key not be reused, and as such it quickly becomes difficult to continually establish new keys between parties without their becoming compromised by an eavesdropper [1].

Although many experiments are carried out using real, physical hardware, due to the difficulty and cost of obtaining equipment necessary to test theories and protocols relating to quantum mechanics-based communications, simulation software is often used instead of performing physical experiments [2]. This allows the most promising protocols and technologies to be identified before a significant investment in hardware needs to be made. This paper will begin by exploring the principles behind quantum cryptography, some of the more popular protocols that are in use, and the state of currently available technology, before focusing on the methods used to perform quantum cryptography simulations.

ICCSP 2020, January 10–12, 2020, Nanjing, China.
ACM ISBN 978-1-4503-7744-7/20/01…$15.00.
DOI: https://doi.org/10.1145/3377644.3377671

2. QUANTUM CRYPTOGRAPHY
Currently, quantum cryptography has the methods of fully use of the quantum entanglements or hybrid of quantum and existing public key cryptography, and in the form of through satellite media or fiber optic networks.

2.1 Background
When using classical forms of communication, it is possible for an eavesdropper to intercept a message, copy or read it, and then send the message on to the intended recipient without leaving a trace of their presence. Indeed, doing so is trivial – an attacker only needs to copy any data packets of interest that pass through a node they control, and then simply forward those packets onward. For this reason, encryption is needed to establish private lines of communication through a network, unless that network is, for example, an internal network definitely guaranteed to be secure from undesired interference. Even with encryption, however, an eavesdropper may be able to obtain the key needed to decrypt data, if the sender and receiver are trying to establish initial communications over the network.

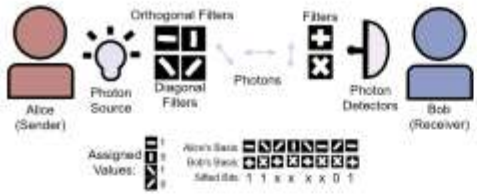

Figure 1. Quantum Key Distribution – establishing a shared string of bits.

Quantum cryptography can solve this problem by providing secure channels of communication through the exploitation of the principles of quantum mechanics. The Heisenberg uncertainty principle states that it is impossible to measure the quantum state of a particle without altering it [3]. In addition, the no cloning theorem states that the quantum state of a particle cannot be copied [4]. These principles together form the basis of quantum cryptography. If an eavesdropper tries to record information encoded in the quantum states of particles, they will disturb those particles, creating noise in the channel that will reveal their presence. Since copying quantum states is impossible, they will also be unable to record the transmission for later analysis.

One of the most common "prepare and measure" quantum key distribution protocols is the BB84 method, so called because it was originally proposed by Bennett and Brassard in 1984 [5]. In this protocol, Alice sends photons to Bob in order to establish the quantum channel. Each photon is encoded with one of two orthogonal polarization bases, and each polarization may represent one of two states (e.g. a linearly polarized photon may be either vertically or horizontally polarized). Bob measures the state of each photon along a randomly chosen basis (as he cannot predict which basis was used for each photon). In the next step, Alice and Bob use classical communication to compare the bases used for each photon, and discard those that do not match. The result is a collection of bits that may be used as a key (Fig. 1). The final step is to sacrifice some matching segments of the key to determine the error rate by comparing them over the classical channel. If the error rate exceeds the error rate that is expected to be caused by the transmission medium, then the presence of an eavesdropper is assumed and the process begins again [6] (Fig. 2). Once a key has been generated without the presence of an eavesdropper, it can be used to send encrypted data over the classical channel.

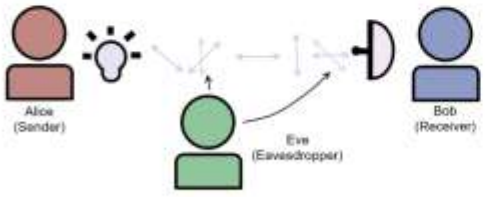

Figure 2. Quantum Key Distribution – establishing a shared string of b Error rate increased due to the presence of an eavesdropper altering photons' quantum states.

In entanglement protocols, such as the Ekert91 protocol described by Artur Ekert in 1991 [7], a photon source generates streams of entangled photons, sending one of each pair to Alice and the other to Bob. Alice and Bob are then able to use these photons to generate a key. In the Ekert91 protocol, Alice and Bob measure the photons according to randomly chosen bases and use a classical communication channel compare the bases they chose, discarding those that do not match, similarly to Bob's step in the BB84 protocol. As in the BB84 protocol, they then sacrifice some portion of the key to determine the error rate in order to detect any eavesdropping.

2.2 Current Status

The number of experiments in quantum cryptography has increased in recent years, and some technologies making practical use of quantum key distribution are available on the market. Although current technology still has limitations in terms of both range and speed, it is already being used for a variety of government and military applications, as well as by finance firms to protect high stakes transactions.

The United States-based firm MagiQ Technologies offers an assortment of communications technologies to customers such as the United States military and NASA. Their research arm provides several cutting edge quantum mechanics-based technologies. These include the QPN 8505 quantum key distribution system, which is designed to be integrated into classical networking systems to provide an additional layer of security to critical military and financial systems [8, 9]. Their laboratories also are focused on the development of several other technologies, including a photon entanglement system intended to produce entangled photons that are compatible with existing fiber-optic cables [10].

The Swiss company IDQ, meanwhile, offers three main branches of quantum mechanics-based technologies. They are able to provide quantum key distribution and quantum key generation hardware that implements the BB84 and SARG protocols to enable secure network communication [11]. They also provide systems for detecting single photons [12], and random number generators that exploit quantum mechanical phenomena to generate numbers [13]. Starting in 2007, IDQ's encryption technology was put in place to secure transmissions of election results from local vote-counting centers to a central data warehouse in Switzerland [14]. IDQ's equipment was similarly used at the 2010 World Cup in South Africa to provide secure communications between an off-site operations center and the Moses Mabhida Stadium in Durban [15].

These are not the only organizations offering or researching quantum encryption technology. The Australian company QuintessenceLabs offers services similar to those of IDQ, including quantum random number generators and quantum key distribution equipment that is compatible with off the shelf optical cables and networking components [16]. They also offer a software development kit meant to make it easy to integrate their encryption technology with other applications [17]. Meanwhile, the British defense firm QinetiQ has also worked to develop quantum networking technologies. Their work, alongside research performed by the United States National Institute of Standards and Technology, Harvard, Boston University, and BBN Technologies led to the creation of the DARPA Quantum Network, the first quantum cryptography network ever implemented [18].

Recent research has also been conducted on using satellites to create a network for quantum communication [19]. As an alternative to standard methods of quantum key distribution, very recent work by a group of Chinese researchers into quantum teleportation, which was widely reported in the news media due to

a sensational interpretation of the term "teleportation," has suggested that satellite communications based on the use of entangled photons to transmit data could provide a secure method of communication over great distances [20].

In a world that is increasingly reliant on electronic transactions to manage virtually every aspect of life, ensuring that critical communications are safe from spying and unauthorized access is of paramount concern. The use of quantum cryptography in securing critical communications channels is likely to continue to proliferate as the relevant technology matures.

3. SIMULATION

Due to the cost, noises, and time constraints, most people use simulators to conduct quantum cryptography study and experiments.

3.1 Background

Significant time and resources have been invested in recent years into improving the practical quantum encryption technology on the market, as well as into developing new methods of quantum encryption, in the hopes of reducing the cost of equipment and making such systems more robust and reliable. As previously mentioned, many experiments are carried out using real optical equipment in laboratories or in limited or carefully controlled real-world settings. For example, the DARPA Quantum Network was developed both to facilitate sending encrypted messages, and to test the encrypted network itself [18].

Some physical experiments are relatively modest in nature. For example, an experiment conducted in Padua in 2011 involved a transmission over a distance of fifty meters in an interior hall which was kept running for several hours [21]. Even this experiment, however, required customized optical equipment and access to a large controlled space where the experiment could be conducted without being disturbed. Many systems require much more elaborate and costly equipment in order to be tested. Certainly, the satellite experiments recently conducted in China must have been very expensive, as the cost of a satellite launch runs in the tens of millions of dollars – to say nothing of the cost of the satellites themselves.

There is also a great deal of research into quantum cryptography that focuses strictly on mathematical analysis of the system being examined, but simulations may be superior to his method in many cases as they allow for stochastic elements to be taken into consideration. Since optical communications systems involve many such elements, such as noise in the communications channel or interactions with the transmission medium, this is an important consideration.

3.2 Quantum Simulation Tools

When performing simulations of quantum cryptography protocols, naturally the first decision that must be made is to decide on the method to be used actually to create the simulation. One option is to model the protocol directly, simulating the behavior of photons and other elements of the system simply by assigning probabilities to various behaviors. Another option is to model the optical system itself, simulating each element of the system and then using those elements to build the complete simulated communications network. As the use of fiber optics for networking applications has become commonplace, there are several off-the-shelf software packages available commercially for the simulation of optical systems.

Some researchers, of course, choose to create custom software for the purposes of simulation. For example, in "An Empirical Analysis of the Cascade Error Reconciliation Protocol for Quantum Key Distribution" [22-26].

Some researchers make their simulation software available to others to facilitate simulation research in general. For example, in "Object-Oriented Quantum Cryptography Simulation Model", X. Zhang et al. propose an object-oriented model for simulating quantum cryptography, which also includes classical cryptography algorithms. Their model uses a layered structure. The lowest layer implements simulations of necessary quantum logic gates, such as the Hadamard gate, as well as classical logic gates, matrix support, and so on. Higher layers incorporate common algorithms including cryptography algorithms, configuration settings, and a GUI. They suggest that this system will be useful for preparing simulations of quantum communications protocols since it provides a set of tools that simulate common features of quantum systems that can be accessed using typical software development paradigms.

3.3 Current Status

Simulations are now regularly used to explore quantum cryptographic systems, both to test communications protocols and before constructing any physical apparatus based on their results. One of the main drawbacks of any model that is tested in simulation is the uncertainty that the model accurately reflects the real system, but enough research has now been conducted in quantum cryptography (and in quantum mechanical systems in general) to provide evidence that the simulations being performed are accurate.

The simulation allowed a new error correction scheme to be tested against the more common Cascade scheme. This study makes a particularly good example of the value of simulation, since it is certainly likely that simulating the satellite network was less expensive than building it would have been.

It is clear that the use of simulation is extremely valuable in studying quantum cryptography. A great deal of work can be accomplished through simulation, including research into technologies and protocols that cannot yet actually be built in the laboratory. Therefore, not only can simulation inform which experiments are likely to be worth performing with physical hardware today, it can help to pinpoint which theoretical paths are most likely to yield useful results.

4. A CLOSER LOOK AT TWO SIMULATIONS OF THE BB84 PROTOCOL

To understand how simulations are used to enable research of quantum cryptography, it is worthwhile to take a detailed look at two such simulations. The simulations performed by B. Archana and S. Krithika using OptSim™ [23] and by Abudhahir Buhari, Zuriati Ahmad Zukarnain, et al. using OptiSystem™ [25] both seek to implement the BB84 quantum key distribution protocol using optical network simulation software. As such, comparing the methods employed by both groups and the difficulties they encountered will help both to illustrate how such tools can be used to good effect to study quantum encryption, as well as to suggest future improvements or additions to such software that would be helpful for this purpose.

They discovered, however, that existing libraries for OptSim™ already provide additional tools for analyzing the polarization of individual photons, as well as power meters that could be used alongside these components to simulate photon detectors [23].

Fortunately, OptSim™ also provides a robust selection of light sources and transmission mediums that can be used for quantum simulation without significant modifications.

As previously mentioned, Abudhahir Buhari, Zuriati Ahmad Zukarnain, Shamla K. Subramaniam, Hishamuddin Zainuddin and Suhairi Saharudin similarly created a simulation of the BB84 protocol using OptiSystem™ [25]. They noted that there are a number of methods of simulating quantum cryptographic protocols, and list several specific software packages and custom examples created by other researchers for this purpose. However, they suggest that simulating the hardware of an optical communications system directly in a specialized optical simulation suite such as OptiSystem™ may be helpful to discover and investigate issues that could arise from the hardware itself, and which might not be apparent from work done using simulation software designed specifically for quantum cryptographic simulations, since such software may make incorrect assumptions about the way in which the hardware would behave [25].

As has been previously mentioned, the use of simulations such as these for studying quantum cryptography is quite valuable, as constructing or obtaining hardware to test quantum communication protocols can be prohibitively expensive, and the hardware necessary for examining some of the newest concepts in the field may not even yet be possible to build. As both of these examples indicate, simulating the hardware itself is possible and can be a practical method of studying quantum encryption. Using software suites such as OptSim™ and OptiSystem™s. Since both teams of researchers discovered that significant customization was necessary to enable these software suites to accommodate quantum encryption, however, it would be useful if a library, or even perhaps an entire specialized optical simulation suite, were to be developed with a focus on the simulation of quantum cryptography.

5. SIMULATION RESULTS LEADING TO SUGGESTIONS FOR FURTHER DEVELOPMENT

To prove the value of simulations in researching quantum cryptographic protocols, it is worthwhile to examine some actual simulation experiments and their results. Aside from the conclusions drawn by these researchers from their work, these studies provide clear evidence that simulations can be used to produce important insights to aid the development of quantum cryptography. Work on both protocols and hardware systems can be improved through the use of simulations, and their results can help to provide direction and theoretical background for further research.

5.1 Simulation of Quantum Key Distribution

As discussed previously, one of the principle areas of quantum cryptography that can be studied with the aid of simulations is quantum key distribution. A study by Minal Lopes and Dr. Nisha Sarwade focuses on the creation and validation of a model of quantum key distribution by implementing the model in MATLAB and comparing the results of simulations using the model to the results of experiments performed using physical equipment to determine the model's accuracy. Specifically, their study focuses on the efficiency of establishing a secure key between two parties, based on the particular characteristics of the equipment being used. Their model seeks to take into account as many of these characteristics as possible to ensure its accuracy.

This research proves the value of simulations based on robust models for studying quantum key distribution protocols by establishing the validity of such models. Ultimately, Lopes and Sarwade assert that the results of their simulations prove that their model accurately models a quantum key distribution setup that uses laser pulses and fiber optic cables to send transmissions. They note that their model also clearly indicates that future developments that make single photon sources more viable and that reduce dark counts and other detection errors will have a major impact on the rate at which a key can be established, making quantum key distribution much more practical. This not only provides further impetus for research into such technology, but also provides a clear reason why simulations such as these are worthwhile – they not only permit the study of systems that already exist, but also allow preliminary research to be performed regarding systems that cannot yet be built.

5.2 Simulation of the Cascade Error Correction Protocol

In addition to enabling researchers to study the implementation of quantum cryptographic protocols and the hardware used for that implementation, simulations can be useful for studying the communications protocols themselves. As an example, in research performed at the U.S. Air Force's Center for Cyberspace Research, Timothy Calver, Michael Grimaila, and Jeffrey Humphries performed an analysis of the Cascade error reconciliation protocol using a custom simulator created using C++ [26]. The Cascade protocol is used to correct errors in the transmitted key during the classical communication phase of quantum key distribution, and is also important for identifying the possible presence of an eavesdropper [26]. The authors note that ensuring the validity of this protocol is of vital importance, since it is already being used in real applications of quantum encryption.

This research proves the value of simulations for the study of quantum encryption protocols. The authors note that it is common for 50% of the bits shared over the quantum channel to be consumed in the error estimation phase [26, 27]. The results of their simulations suggest that this may be reduced to 25% without a significant loss to the accuracy of the calculation. This would increase the number of bits remaining to be used for the key by 50%, resulting in a substantial increase in the efficiency of the key distribution protocol. These results clearly show the value of using simulations to investigate protocols used for quantum encryption, and suggest that further research into protocols currently in use may yield potential improvements that have been overlooked.

6. CONCLUSIONS

Quantum cryptography offers the possibility of a significant increase to the security of communications, at a time when electronic communications are already of vital importance and only becoming more and more critical to a wide variety of industries and government functions. Experimental hardware is constantly under development, but the cost of custom cutting edge optical equipment, satellites, and other equipment makes performing tests prohibitively expensive in many cases. While physical experiments will always be necessary, simulations based on robust models can provide the opportunity to study many different communications protocols and hardware configurations, leading to new methods of implementing quantum cryptography and suggesting the most promising paths to pursue in the development of new hardware. The ability to change the parameters of a simulation to quickly test a wide variety possibilities can save funds and offer a significant increase to the

efficiency of research. As the studies referenced as examples in this paper show, the continued development and use of quantum cryptographic simulations is essential to the development of quantum cryptography and likely will lead to many new improvements in both protocols and new hardware.

7. REFERENCES

[1] Mobin Javed and Khurram Aziz. 2009. A Survey of Quantum Key Distribution Protocols. In Proceedings of the 7th International Conference on Frontiers of Information Technology (FIT '09), Article 39, 5 pages. DOI=https://dx.doi.org/10.1145/1838002.1838046

[2] Abudhahir Buhari, Zuriati Ahmad Zukarnain, Shamla K.Subramaniam, et al. 2012. An Efficient Modeling and Simulation of Quantum Key Distribution Protocols using OptiSystem™. In 2012 IEEE Symposium on Industrial Electronics and Applications. Pages 84-89. DOI: https://dx.doi.org/10.1109/isiea.2012.6496677

[3] Jan Hilgevoord. 2016. The Uncertainty Principle. Retrieved September 10, 2017 from https://plato.stanford.edu/entries/qt-uncertainty/

[4] Jeffrey Bub. 2015. Quantum Entanglement and Information. Retrieved September 10, 2017 from https://plato.stanford.edu/entries/qt-entangle/

[5] C. H. Bennett and G. Brassard. 1984. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Volume 175. Pages 175-179. Retrieved August 21, 2017 from http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

[6] Dagmar Bruss, Gábor Erdélyi, Tim Meyer, et al. 2007. Quantum Cryptography: A Survey. In ACM Comput. Surv. 39, 2, Article 6 (July 2007). 27 pages. DOI=https://dx.doi.org/10.1145/1242471.1242474

[7] Artur K. Ekert. 1991. Quantum Cryptography Based on Bell's Theorem. In Physical Review Letters, Vol. 67, No. 6. Pages 661-663. DOI: https://doi.org/10.1103/PhysRevLett.67.661

[8] Yoshito Kanamori, Seong-Moo Yoo, and Mohammad Al-Shurman. 2005. A Quantum No-Key Protocol for Secure Data Communication. In Proceedings of the 43rd annual Southeast regional conference - Volume 2 (ACM-SE 43), Vol. 2. Pages 92-93. DOI: https://dx.doi.org/10.1145/1167253.1167274

[9] Alla Altalib, Yomna Al-Ibrahim, Zahra Almahfoudh, et al. 2015. Security Measures in a Keyless Quantum Communication Protocol. In 2015 Fifth International Conference on e-Learning (econf). Pages 53-57. DOI: https://dx.doi.org/10.1109/ECONF.2015.33

[10] MagiQ Technologies. 2017. MagiQ Research Labs. Retrieved September 9, 2017 from http://www.magiqtech.com/research-labs/

[11] IDQ. 2017. Quantum-Safe Crypto. Retrieved September 9, 2017 from http://www.idquantique.com/quantum-safe-crypto/

[12] IDQ. 2017. Single-Photon Systems. Retrieved September 9, 2017 from http://www.idquantique.com/photon-counting/

[13] IDQ. 2017. Random Number Generation. Retrieved September 9, 2017 from http://www.idquantique.com/random-number-generation/

[14] Paul Marks. 2007. Quantum Cryptography to Protect Swiss Election. Retrieved September 12, 2017 from https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/

[15] Swiss Quantum. 2010. Quantum Encryption to Secure World Cup Link. Retrieved September 12, 2017 from http://swissquantum.idquantique.com/?Quantum-encryption-to-secure-World

[16] QuintessenceLabs. 2017. Quantum Cybersecurity. Retrieved September 12, 2017 from https://www.quintessencelabs.com/quantum-cybersecurity/

[17] QuintessenceLabs. 2017. Quantum Cybersecurity - Ultimate Data Protection. Retrieved September 12, 2017 from https://www.quintessencelabs.com/products/#clientSDK

[18] Chip Elliott, Alexander Colvin, David Pearson, et al. 2005. Current Status of the DARPA Quantum Network. In Proceedings Volume 5815, Quantum Information and Computation 30, 12 pages. DOI: https://dx.doi.org/10.1117/12.606489

[19] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, et al. 2017. Satellite-to-Ground Quantum Key Distribution. In Nature 549, 43–47 (07 September 2017), 18 pages. DOI: https://dx.doi.org/10.1038/nature23655

[20] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, et al. 2017. Ground-to-Satellite Quantum Teleportation. In Nature 549, 70–73 (07 September 2017), 16 pages. DOI: https://dx.doi.org/10.1038/nature23675

[21] M. Canale, D. Bacco, et al. 2011. A Prototype of a Free-Space QKD Scheme Based on the B92 Protocol. In Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL '11). 5 pages. DOI: https://doi.org/10.1145/2093698.2093884

[22] OptSim Product Overview. 2017. Synopsys, Inc. Retrieved September 20, 2017 from https://www.synopsys.com/optical-solutions/rsoft/system-network-optsim.html

[23] B. Archana and S. Krithika. 2015. Implementation of BB84 Quantum Key Distribution using OptSim. In 2015 2nd International Conference on Electronics and Communication Systems. Pages 457-460. DOI: https://dx.doi.org/10.1109/ECS.2015.7124946

[24] OptiSystem. 2017. Optiwave Systems Inc. Retrieved September 20, 2017 from https://optiwave.com/category/products/system-and-amplifier-design/optisystem/

[25] Abudhahir Buhari, Zuriati Ahmad Zukarnain, et al. 2012. An Efficient Modeling and Simulation of Quantum Key Distribution Protocols using OptiSystem™. In 2012 IEEE Symposium on Industrial Electronics and Applications. Pages 84-89. DOI: https://dx.doi.org/10.1109/isiea.2012.6496677

[26] Timothy Calver, Michael Grimaila, et al. 2011. An Empirical Analysis of the Cascade Error Reconciliation Protocol for Quantum Key Distribution. In Proceedings of the Seventh Annual Workshop on Cyber Security and Information

Intelligence Research (CSIIRW '11). 4 pages. DOI: https://dx.doi.org/10.1145/2179298.2179363

[27] Wajdi Al-Khateeb, Khalid Al-Khateeb, Nur Elyana Ahmad, Siti Norussaadah Mohd Salleh. 2013. Practical Considerations on Quantum Key Distribution (QKD). In 2013 International Conference on Advanced Computer Science Applications and Technologies. Pages 278-283. DOI: https://dx.doi.org/10.1109/ACSAT.2013.62