PAPER • **OPEN ACCESS**

Efficient Hardware Implementation for Quantum key Distribution Protocol using FPGA

To cite this article: Yasir Amer Abbas and Alharith A. Abdullah 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1076** 012043

Efficient Hardware Implementation for Quantum key Distribution Protocol using FPGA

Yasir Amer Abbas[1] and Alharith A. Abdullah[2]

[1] College of Engineering, University of Diyala, Diyala, Iraq
[2] College of Information Technology, University of Babylon, Babil, Iraq

Email: dr.yasiral-zubaidi@uodiyala.edu.iq

Abstract. This paper presents a new hardware implementation of the quantum key distributed cryptography protocol using Field Programmable Gate Array (FPGA). In many security applications, the software implementations of key distribution algorithms are slow and inefficient. In order to solve this problems, new hardware architecture was proposed to speed up the performance and flexibility of key distribution algorithms. The concurrent computing designs quantum key distribution protocol with reducing the hardware area, producing a high throughput and low latency. It also showed high speed processing and consumed low power. An efficient hardware architectural model for quantum key distribution protocol was developed using very high-speed integrated circuit hardware description language (VHDL). This hardware designed to be used with any quantum key distribution protocol to distribution the secret key securely. The hardware implemented and test with Spartan-3 FPGA board and the results show a throughput of 8 Mbps and efficiency of 1.6 Mbps/slice.

1. Introduction

The quantum cryptography is the most useful solution for information security systems nowadays, which describes the ultimate method for key distribution, and it is different from various of the classical cryptosystems used today, where these security systems regularly have draws due to computational power and the complexity of implementations of the mathematical problems, in contrast, the quantum cryptography security is based on physics laws. [1]

Quantum cryptography and especially Quantum Key Distribution (QKD) which is named (BB84) after its inventor's Bennett and Brassard, used as the most research direction in the past twenty years and now proceeds to a majority field of the quantum field [2]. The (BB84) protocol allows the secret key establishment mechanism within two users' connection, using a combination of classical and quantum channels. The essential benefit of (BB84) deals with the “quantumness” of the signals transferred within the quantum channel, which leads to detect any eavesdropping threats affected on the communication line, This characteristic of (BB84) guides to a particular property, which it doesn't achieve by classical cryptography techniques, So it provides Key Establishment beside the high-security standard as unconditional or information-theoretic security. In this paper, the hardware design within the Xilinx environment to apply the (BB84) Protocol. The used (FPGA) boards, namely, Spartan-4 examines the suggested hardware model. Due to the important applications of (BB84) there are many studies deals with this protocol and the enhancement it; we review some important contributions in this field.

The researchers [3] proposed a new method for modifying the (BB84) protocol based on two-way classical and parallel entanglement protocol purification. The proposed protocol was optimized to reduce (QBER) and the results reached a maximum error rate of 20%. On the other hand, the general declaration of the rules was dispensed with in this model. The researchers in [4] used the (BB84) with traditional cryptography to obtain more secure authentication mechanisms and also reduce authentication cost. Whereas researchers in [5] presented a solution to the problem of insecurity in the classical key distribution methods, and the solution to this problem comes by using quantum key distribution, where (BB84) reduces risks in key distribution and thus provides high security in addition to error detection. While the authors in [6] proposed another way to enhance the quantum key distribution protocol (BB84), that came from using the basis of the original (BB84) protocol. The proposal is based on enabling the two parties to negotiate a shared secret key without using the classic channel. Their results indicated that the proposed protocol utilized approximately 60%–80% of the bits generated therefore provide better results compared to the standard (BB84) protocol. The researchers at [7] relied on the Legendre symbol to encoding a stream of bits into polarized photons. In their proposal, a public channel was not used to negotiate the bases. Rather, both the sender and the receiver negotiate to use the Legendre code function and then only use a quantum channel, thus reducing the time and increasing the length of the final key. In [8] the researchers proposed a hybrid protocol based on (BB84) protocol and public key cryptography in order to obtain a strong key based on the quantum physical properties and mathematical intricacies of the public key algorithm.
The paper is totally presented as follows: Section II, we explain the used (BB84) protocol and the main protocol components. In section III, the hardware design by using the Very High-Speed Integrated Circuit Hardware Description Language (VHDL) implementation of BB84 protocol. Section V deals with simulation and results. Finally, the of this paper are conclude in section VI.

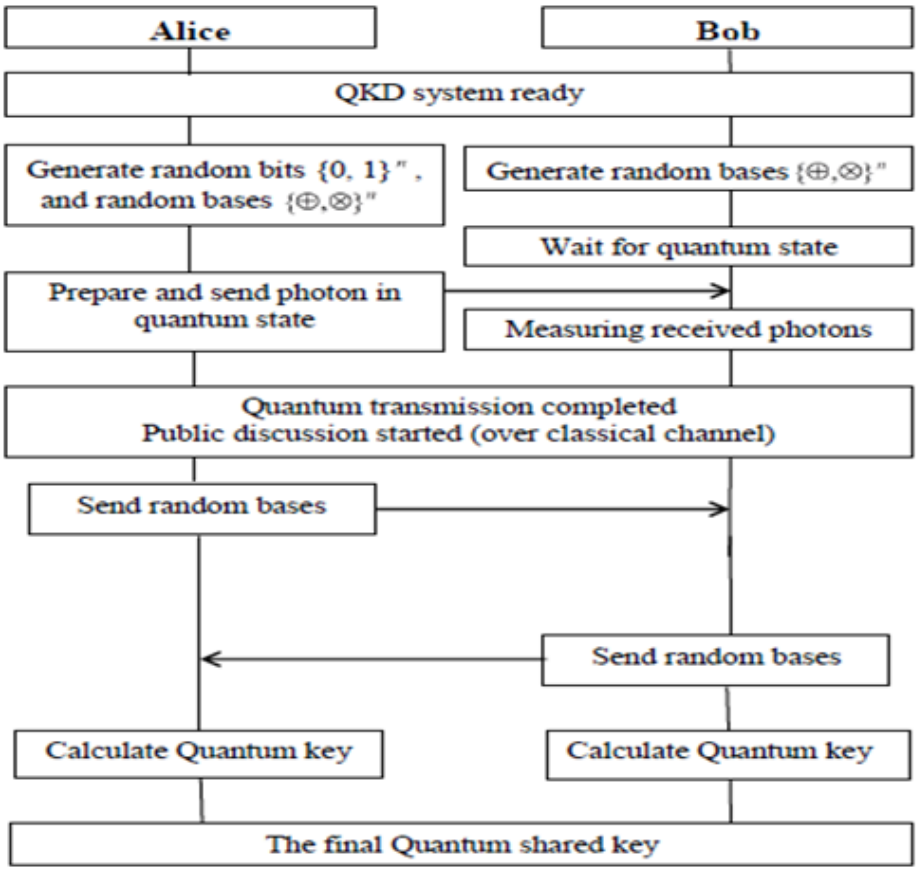

Figure 1. The chart of quantum key distribution protocol (BB84) steps.

2. Quantum Key Distribution Protocol (BB84)

In brief, within the (BB84) the partners (Alice and Bob) want to agree on a secret key concept regarding no eavesdropper (Eve) to gain important information, and the operations summarized as Alice sends any bit of the secret key in one of a collection of conjugate bases in another side, It does not recognize by Eve, and the key used remains protected through the impossibility of holding simultaneously the state of a quantum system bases. [9]. And, the Figure 1 describes the main operation steps within the (BB84) protocol.

3. Hardware Implementation of BB84 Protocol

New hardware designed with low power is implementing using VHDL.The proposal hardware is implemented using FPGAs because of the adaptability given by the FPGA technology. BB84 are designed in hardware using VHDL and tested it by using simulation and test vector.

The top-down methodology will explain the proposal hardware designed for BB84, Figure 2 shown the register transfer language (RTL) for transfer the quantum key signal to binary. The hardware architecture for proposal design are dependent on send and received of based and stage. The hardware architecture is dependent on numbers of simple logic operation to transfer quantum key operation to binary, first the sender based is checked. The send operation is start with enter send stage, then the based dependent of based and stage the angle will be generated, the second operation done at receiver side, the hardware logic circuit designed working to check three things (received and send stage and based send) the binary key will be generated. The proposal hardware designed with simple architecture that can transfer and quantum key to binary with on clock cycle.

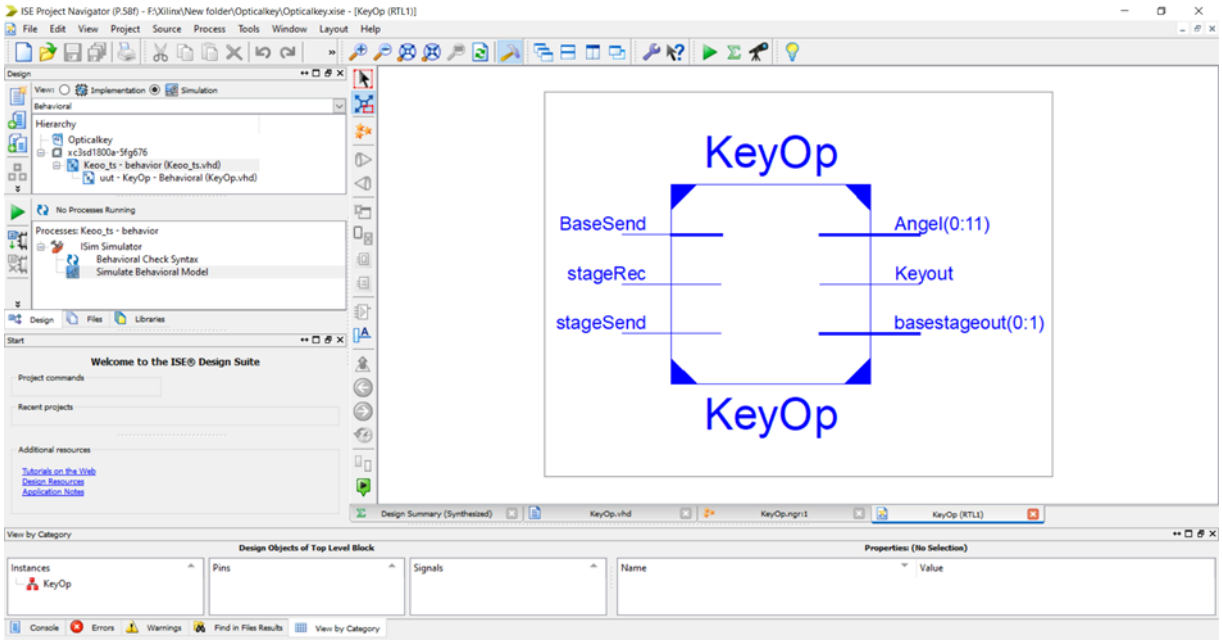

Figure 2. Transfer quantum key signal to binary by RTL.

4. Simulation and Result

The used system implemented with the Xilinx ISE V14.5 WebPACK and (ModelSimXE P.58f) for design synthesis and simulation tool based on the Very High-Speed hardware description language (VHDL) for Spartan-3.

The main objective of the used design is to provide low latency and low-cost hardware implementation and improving the security by adding BB84 protocol. Through, the used model design, the lowest potential gate is examined to produce a low latency hardware component.

Figure 3 shows the Simulation of test vector of BB64 protocol using tool (ModelSimXE P.58f) from Xilinx, it shows all possibilities of base and angle that enter randomly to the hardware proposal design. For example, when the based is bit (1), send base bit (0) and the base stage to output is bits (10), then the based stage is bit (0) that mean the key is bit (1) with angle (zero). The hardware design is test with all four angles with random data, based and stages.

Figure 3. Simulation of BB64 proposal designed.

The synthesis report for hardware deigned display a frequency 8 Mbps, total number of slices is 5 and power consumption 0.027W. The hardware design with concurrent architecture that allow executed all operation in one clock cycle, this architecture increasing the throughput and efficiency that shown in Table 1.

Table 1. FPGA implementations synthesis results for bb84.

Algorithm	Block Size	Device	Clock Cycle	Max Freq (MHz)	Throughput (Mbps)	Total Equiv Slices	Efficiency (Mbps/Slice)	Power (Watt)	Delay (ns)
BB84	1 bit	Spartan-3 XC3S50	1	8	8	5	1.61	0.027	8.064

5. Conclusion

This paper presented a hardware design of FPGA for implementing quantum cryptography protocol (BB84). The hardware architecture was designed to transfer any optical data to binary with within one clock cycle while having a high throughput, low power and high efficiency with high security depend on the concepts of quantum. This low cost design is important to give a better picture of implementation cost should it aims at implementing the algorithm in a smart card or any other portable devices. The results for both FPGA boards showed a higher throughput and efficiency while consuming low power as compared with the previous studies. The results show a throughput of 8 Mbps and efficiency of 1.6 Mbps/slice and with power consumption 0.027W with Spartan-3.

References

[1] S. K. Lenka, V. Ojha, A. Sharma, 2010 *Security of Entanglement Based Version of BB84 protocol for Quantum Cryptography* IEEE.

[2] C. H. Bennett and G. Brassard, 2014 *Quantum cryptography: Public key distribution and coin tossing* Theor. Comput. Sci., vol. 560, no. P1, pp. 7–11.

[3] K. Wen and G. L. Long, 2005 *Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communications* Phys. Rev. A, vol. 72, no. 2, p. 22336.

[4] S. T. F. Al-janabi and O. K. Jasim, 2015 *Reducing the Authentication Cost in Quantum Cryptography* no. 6.
[5] R. D. Sharma and A. De, 2011 *A new secure model for quantum key distribution protocol* 6th International Conference on Industrial and Information Systems, pp. 462–466.
[6] A. A. Abdullah and Y. H. Jassem, 2019 *Enhancement of Quantum Key Distribution Protocol BB84* J. Comput. Theor. Nanosci., vol. 16, no. 3, pp. 1138–1154.
[7] A. A. Abdullah, R. Z. Khalaf, and H. B. Habib, 2019 *Modified BB84 Quantum Key Distribution Protocol Using Legendre Symbol* 2nd Scientific Conference of Computer Sciences (SCCS), pp. 154–157.
[8] A. A. Abdullah and S. S. Mahdi, 2019 *Hybrid Quantum-Classical Key Distribution* International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-8 Issue-12, 4786-4791.
[9] S. Rana, S. Hossain, H. Imam Shoun, Mohammod Abul Kashem, 2018 *An Effective Lightweight Cryptographic Algorithm to Secure Resource-Constrained Devices* (IJACSA) International Journal of Advanced Computer Science and Applications.