Robotics & Automation Engineering Journal
ISSN: 2577-2899

Juniper Publishers
key to the Researchers

Review Article
Volume 5 Issue 3 - February 2023
DOI: 10.19080/RAEJ.2023.05.555665

Robot Autom Eng J

FPGA Based Architecture for Quantum Communication System

Noorulden Basil*

Department of Information Technology, Al-esraa University College, Baghdad, Iraq

Submission: January 01, 2023; **Published:** February 07, 2023

***Corresponding author:** Noorulden Basil, Department of Information Technology, Al-esraa University College, Baghdad, Iraq

Abstract

This paper presents the equipment and programming design that can be utilized in these frameworks which carries out pragmatic quantum key conveyance (QKD) and quantum arbitrary number age (QRNG). Plans This engineering makes the most of the capacities of the framework on a chip (SoC) that executes Programmable door cluster (FPGA) and double center CPU. Relegating time-bound errands For FPGA and CPU the executives, we have made an adaptable framework with ideal asset designation. A business off- the-rack (COTS) assessment board that incorporates the SoC. Likewise with a change for information stream, the general framework design can be utilized as QKD transmitter, QKD collector. What's more, the control and acknowledgment unit QRNG. At last, we utilized double center execution and saw the synchronization QKD carries out equipment streams to execute stream dispatchers where the bit is continually getting new information. One runs at a decent rate from an outside QRNG source and different sudden spikes in demand for a FPGA Communicating a qubit to a QKD collector. The framework was effectively tried during a long exhibit Its strength and security. This confirmation prepares for a safer execution of QKD. Since QKD states are produced by a totally evident stochastic interaction with genuine outright security Not with explicit augmentation components. Finally, it permits us to see a singular amount. The transmitter incorporates arbitrary numbers and qubit age.

Keywords: Cots; Qkd; Fpga; Cpu; Qc

Introduction

One of the promising applications is quantum correspondence (QC). Quantum innovation and as of late procured Suitable inspiration for business programs. Quantum Key and quantum irregular number age (QRNG) are two principal quality control advances Their mix gives a feeling of complete security Moral, resistant to outer assault. Awareness Such a framework requires the undertaking and improvement of a few Parts: from optical change in accordance with electronic control, From page on advanced administration to authoritative programming. Notwithstanding a particular quantum execution that can This is significant for various security conventions The thing of all settings of an observing board to guarantee a specific way of behaving, high goal, Furthermore, high-speed computations. With this structure, modified field projects can be FPGA is practically obligatory Decision for such projects [1,2]. FPGA gives more Advantage as far as energy utilization [3].

which can This be a vital element for basic applications like CubeSat Assignments for satellite quality control [4]. In any case, writing The FPGA program for quality control mostly centers around equipment speed increase after QKD handling [5-8] and needs subtleties. Show of the board framework structures likewise, utilizing both FPGA and CPU capacities This was just proposed in [9] yet has been examined Encryption and organization capabilities in our article Give a typical FPGA-based design for control also, perusing elements of value control frameworks. It abuses the stone monument an equal CPU, framing a framework on a chip (SoC), Further develop adaptability and delivery supported execution QKD project, with practically no expansion, by outside QRNG. The engineering can without much of a stretch be utilized independently QKD (DV- QKD) and Discrete Variable QRNG (DVQRNG) Execution of utilizations, control capabilities of those frameworks Also, there is an unmistakable potential Additionally utilized in persistent variable QKD (CVQKD). What's more, consistent variable QRNG (CV-QRNG) are introduced Helper advanced to-simple converter (DAC) and A simple to-advanced converter (ADC) should be added. This the engineering was executed and tried at the rudimentary level Assessment board: Zed Board Avnet that mounts Zynq-7020 SoC. As well as giving an ideal trade Among cost and execution, FPGA chip (Artix-7) It showed great outcomes

in radio conditions [10] and its A decent decision for both the view and There were additionally satellite QC applications, Zed Board It was effectively utilized in a new quantum processing project [11], It shows superb dependability. Activity of both The SoC levels (FPGA and CPU1) lead to a more significant level Adaptability permits you to scale the program's elements A particular piece of the chip for a particular program, The framework can be designed through and through (information stream from PC/client or underneath (information stream from the design of the quantum framework to the PC/client).

This framework has the adaptability to be utilized with numerous conventions structure and effectively worked with different tests [12-21] as of late. As of late this It was likewise tried on a model QKD transmitter The satellite is reasonable for the CubeSat mission [22]. KY, the principal part of KY. Because of the presence of two atomic We likewise planned, created, and effectively tried the CPU A double center program prepared to do for all time putting away information Move from outer source to CPU and afterward to FPGA. This component is critical to executing strong security the QKD framework, since it joins the QRNG yield stream with a QKD stream without irregular number extension (which has an extremely high exchange rate with cost This subverted security [23-24] and made ready for exchange QKD gadgets with full unqualified security. The remainder of this article is organized as follows. that in the subsequent part contains an outline of the design. Parts III and IV have the FPGA and CPU levels Portrayed in Section V, a double center engineering for a QKD. The transmitter is provided with framework test results.

Fpga Architecture Overview

Current FPGA-based QKD frameworks don't utilize potential SoC design and single-layer execution FPGA design on a chip to play out any tasks, indeed, even those that can be handled by a solitary processor Furthermore, it doesn't require a lot of investment [25,26]. This approach is conceivable. Execution of the entire prompts a more effective framework Plan adaptability in FPGAs can be diminished as a matter of course Changes require appropriate review of the gear The plan work process is mind boggling. This is our framework Because of its design, it comprises of two unique layers For SoC capacities. low level FPGA, it has generally vigorous elements and high goal it will be finished. The more elevated level is one of the CPUs that Answerable for information the board choices and capabilities as well as correspondence with the rest of the world. Notwithstanding the division of capabilities, there is another division A central issue for support and recharging Engineering, as the two levels require different programming Dialects (VHDL/Verilog versus C/C++) and others Project bunches Two additional layers i.e., end client/outer. (Figure 1) the quantum source and the design correspond to the main mix.

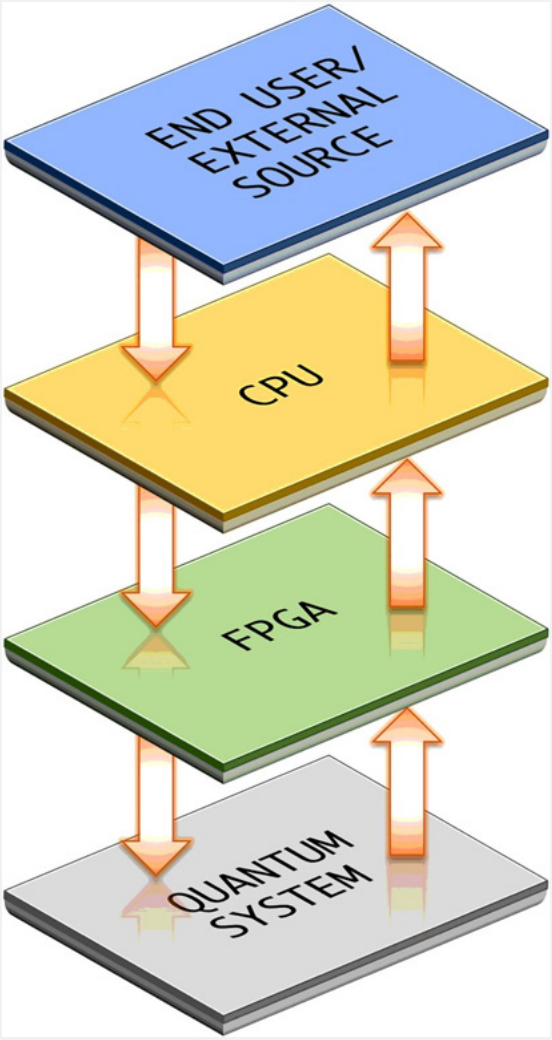

Figure 1: The four-layer structure Overview system.

A transmittable engineering framework has been created Controlling a specific quantum instrument can be simple Change between hierarchical and base around work processes, this shows the contrast between QKD transmitter what's more, QKD/QRNG collector programs. For QKD applications, the ongoing adaptation of the design isn't carried out between post-handling and time synchronization Shipper and beneficiary. As a matter of fact, A Just FPGA-based post-handling is valuable if it chips away at both Alice and Bob, it speeds up Handling on a single side won't bring functional advantages because of potential aggravations at the opposite end. be that as it may, DV-QKD demands an investment to- computerized converter (TDC). to recognize the appearance season of a solitary approaching photon. Thus, a proficient FPGA execution of DV-QKD The beneficiary should incorporate TDC and post-handling action This approach will be perceptible FPGA projection endeavors without making significant advantages Standard business PC

How to cite this article: Noorulden Basil. FPGA Based Architecture for Quantum Communication System. Robot Autom Eng J. 2023; 5(3): 555665. DOI: 10.19080/RAEJ.2023.05.555665

(PC) can be adequate as our execution, keep the back speed.

Additionally in research and natural turn of events, Later This permit an exceptionally basic getting it and promoting Programming and thusly straightforward similarity with a given QKD The reason for controlling various conventions and it shows. That is the reason we decided to carry out PC Post- handling can be handily adjusted for various tests. Be that as it may, when the business is more designated arrangement where elite execution should be wanted Notwithstanding adaptability, there can be FPGA-based post-handling Area of future reconciliation and audit. on a similar PC We additionally execute Qubit4Sync, which is the latest post-handling Synchronization technique for time arrangement Two gatherings [27] comprise any pointless selective space.

In this engineering, the information stream begins from the external A gadget, for example, a QRNG or PC then goes through the CPU FPGA lastly to the information yield (I/O) pins on the chip. This plan is appropriate for QKD transmitter. The encryption key is produced by QRNG progressively or currently put away in the PC and took care of through the CPU A FPGA that controls committed quantum equipment Therefore, the state generator. As made sense of underneath, The initial step of correspondence from an outside gadget A CPU that sudden spikes in demand for Gigabit Ethernet.

This test gives high transmission proficiency (more than 600). Mbps) and the incredible adaptability of Ethernet is wide Norm Because there is no encryption of the information stream, it is Protection of the correspondence channel is vital from snooping, this should be possible by setting up A confidential neighborhood (LAN), truly detached from different organizations, between the SoC and an outside gadget. The second layer in the stack is the CPU FPGA. Two arrangements were carried out for this activity. Setup boundaries, for example, qubit or all out recurrence the length of the transmission with the most reduced revive rate Direct correspondence through cutting edge Extensible Interface (AXI) convention. Yet, for the source Key exchange can arrive at a standard information pace of 400 Mbps we utilized inner DDR RAM, open from the CPU and RAM (BRAM), It is coordinated in the FPGA yet accessible from the CPU AXI convention. Entryway, with the most extreme length Mbits - tail is separated into two sections, yes When FPGA peruses from one section, the processor can Update information put away in other substance The show was at that point procured by Ethernet. These permits Continue the information and synchronization of the appearance FPGA-A gadget is so I/OS it. It is communicated in it the quantum framework determined, leave signals are sent External volume interface (standard LVCMOS33) or FPGA Masonite Porters (LVCMOS18) Reactive sheets and afterward increase by passing just external Scene.

In this setup the data set - blate beginnings with input/os Controlled FPGA and afterward sent FPGA to the processor and toward the finish of the processor to space the gadget can be utilized for QKD receptor or on the other hand for qrng where the electrical sign is caused Outside gadgets, some place individual visual finders, test FPGA I/OS. Test and sign put away later supplanted, by processor, unfamiliar PC, to complete After the QKD convention, That is, the evaluation of boundaries, a revision of blunders and a duplication protection. Correspondence points of interaction of lower levels Hierarchical arrangement. should be for this situation, the connection between The CPU and the outer PC should go about as a channel In a protected neighborhood organization, the information stream isn't encoded in this mode. A LAN is utilized to guarantee an elevated degree of safety The PC-CPU association should be devoted, in this way Truly isolated from the item utilized for correspondence among sending and getting PCs.

Proposed Fpga Layer

The FPGA execution permits exact timing Optical control arrangement of the genuine limit Planning every activity as indicated by the framework clock A critical part of carrying out the QKD/QRNG framework. When utilized in a QKD, FPGA transmitter design is answerable for the right creation of power beats that control the electro-optical parts of the framework. FPGA takes care when QRNG/QKD is utilized as collector Outside electrical sign understanding capabilities from single-photon indicators Due flawlessly, may likewise think about the program Structure CV-QKD [28] and CV-QRNG [29,30]. The thing that matters is that the FPGA connection point is required Right outside DAP (on CV-KKD transmitter) and Outside ADC (for CV-QKD and CV-QRNG receptor).

Summed up and worked on construction of FPGA plan This is displayed in Figure 2. The program shows variety This design can be utilized in an assortment of value control applications Without transforming anything aside from the first point of interaction module quality States regulator in QKD dispatcher arrangement; SPD Reader and QRNG conventions in QRNG/QKD recipient one and the heading of information stream. Utilization of plan Blocks with AXI support for correspondence and information move to (from) a CPU with devoted BRAM and VHDL FPGA information the board unit, Memory Manager unit, furthermore, outer sign age (perusing), Q States regulator, furthermore, SPD Reader blocks. Incorporates QRNG application extraordinary modules that permit you to produce irregular information Conventions [31,32]. Permits you to design AXI-GPIO boundaries Perusing hinder signals from and to the CPU Extra VHDL modules. Empowers AXI-CDMA usefulness Information move from the RAM board to the BRAM(s) [33]. The memory director is liable for information the board Trade among BRAM(s) and other extraordinary modules. BRAM is partitioned into two memory the board areas It will sound each time it arrives at the end two sections (while perusing or composing) and then again, the sign is perused by AXI- GPIO and

How to cite this article: Noorulden Basil. FPGA Based Architecture for Quantum Communication System. Robot Autom Eng J. 2023; 5(3): 555665. DOI: 10.19080/RAEJ.2023.05.555665

deciphered as a hinder Composes (peruses) new information to (from) the CPU. The feline framework clock is set in the 100 territory, what's more, 200 MHz relying upon the application. future Upgrades will think about expanding this recurrence further Speed up. But, as a matter of fact More tight timing requirements show a higher clock recurrence High information throughput to/from outside gadget It can surpass gigabit data transfer capacity limits [34,35].

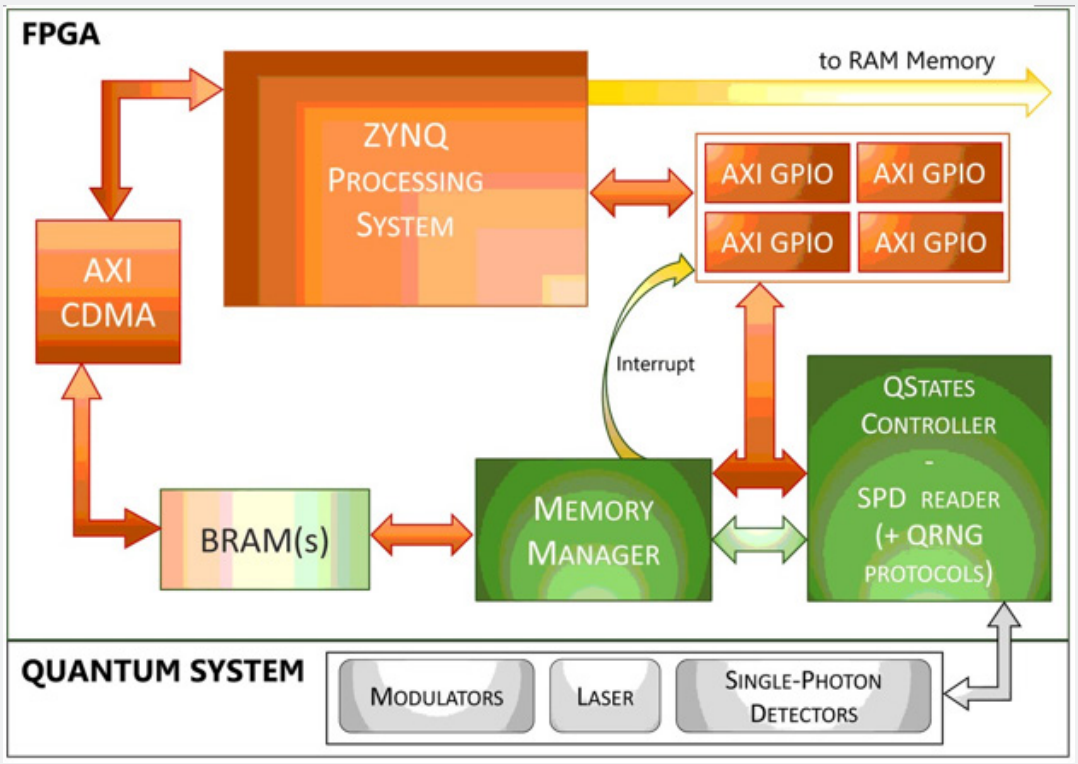

Figure 2: FPGA Schematic view for the proposed system.

The overall engineering portrayed before is as yet the objective Being convention blind and can be utilized to arrange the QKD transmitter regulator no matter what the specific QKD convention and qubit. encryption of the module only for spirit It requires an extraordinary plan to encode the crude key information in the result power beats. This is a QStates regulator module in view of What is normally finished in the writing (see, for instance, La Quantum level determination module [8]), driving the qubit Unlock by scrambling the crude key information in the power yield Pulses that control lasers and electro- optical modulators. We have created many kinds of this module [28-31] got from [28-31] for the chose QKD convention The notable BB84 [32] and executions [16,18,20,22].

Here is an exceptionally short clarification. The most recent variants are introduced in [22]. The PC clock is set Up to 200 MHz, a 5 ns beat result can be given. Encoding each qubit ostensibly requires something like that 15 second time frame polarization coding descriptor Three distinct extremity levels and one result are required heartbeat in three different time positions (0-5 ns, 5-10 ns, and 10-15 ns). The lure is handled similarly technique, depiction of three distinct degrees of power [33,34], But it just requests the result beat in the two change states (0-5 ns and 5-10 ns) alongside the laser potential Let everything go First, the beat is applied to the laser driver aside from some rot in each opening (0-5 ns). Sickness. For offset and synchronization of result flags The length of the optical way can likewise make some discrete memories change Used for any sign. comparative brief guides, it has a place with specific QKD and qubit encryption conventions, Our benefit is notable in the writing [35]. Just two voltage levels are expected for this given by FPGA (and formal speed increase). level) Avoid utilizing DACs or staggered gadgets. Two unique GATEs are introduced: one Polarization scrambles information and others for trickery one Because each qubit requires 2 pieces to separate in three post positions and in the other 2 pieces Discrimination in three ways of double dealing, BRAM a similar size is set and a similar hinder is empowered standard It can be improved for lucidity Common qubit encoding involving three pieces for + extremity Bait encryption However, we chose to utilize it two + two encryption is predominantly for two reasons.

The primary explanation Three-cycle encryption requires greater intricacy, and it is normal to recognize ineptitude with a particular goal in mind Each byte contains multiple pieces however under three pieces Qubits encode information put away in one byte. The subsequent explanation is that 2 + 2-cycle encryption permits division of ways, memory and transmission. Extremity Control Protocol (TCP) attachments. furthermore,

How to cite this article: Noorulden Basil. FPGA Based Architecture for Quantum Communication System. Robot Autom Eng J. 2023; 5(3): 555665. DOI: 10.19080/RAEJ.2023.05.555665

breaks down information and further develops dependability and adaptability The general framework is essentially equivalent to the FPGA plan for the QKD recipient for DV-QRNG. In the two cases the I/Os Along with the result signals from single-photon locators, And FPGA carries out the most common way of making models for creation A little string containing the computerized portrayal of time Single-photon occasions are first switched over completely to an information sign to the FPGA synchronization district utilizing formal nonconcurrent synchronization The SPD peruse incorporates an equipment module.

Afterward, in for the situation of QRNG, the example pieces are transitory It is gathered and afterward handled with the proper blocks Use arbitrary age conventions for little informational indexes depicted in [14]. The irregular cycle is then put away and controlled. It is supplanted by 32-bit utilizing memory the board Live and hinder call at the ith BRAM address Whenever it arrives at half or end. Additionally, this engineering It was likewise conceivable to empower synchronization QRNG, which must be executed [21]. This specific program is expected to produce an irregular number. It is made solely after a specific trigger occasion. Thus, The QRNG should be synchronized with the test device, an adjustment of design was expected To permit recuperation of all irregular information comprehensive SPD tests, quickly at a given time. There was a redesign outer electrical sign from Test arrangement. An irregular piece is then utilized for age A helper yield port that controls a particular optical part Improved security of testing Numerical number, the construction was likewise copied and it created two irregular pieces that were churnalized.

Also, for additional subtleties, see [21]. Fundamentally, deleting an age Moral blocks become social designs QKD ought to be utilized as collector. In any case, there is a disadvantage to this the execution of the permit is restricted in time framework clock, even in a top of the line FPGA bundle situation, something like 1 GHz. For elite execution QKD, sub nanosecond goal in the recipient Subsequently this strategy can be an answer Only for minimal expense QKD frameworks. Nonetheless, the plan and TDC- FPGA module reconciliation (i.e., [36-38]). or on the other hand the utilization of outside coordinated circuits (for instance, [39]) permits partition the second time Therefore, the application in elite execution QKD frameworks. Future work will investigate such arrangements, as a matter of fact.

Cup Layer

Computer chip programming is executed independently/parametrically. A product doesn't need a working framework. This is This is a major benefit of having extremely light and quick programming with a higher plan cost Software created in C Furthermore, C + + dialects assume a part in the FPGA layer interface with an outside source and an end client, it fundamentally makes it conceivable interfere with strategy to move (read) information from (to). Oversee memory for (with) BRAM whenever RAM It arrives at the center of the finish of BRAM. This likewise actuates it TCP association attachments for getting orders and information from an outer source or client to speak with the rest of the world, the TCP convention chosen Thanks to the force of this convention The chance of losing information parcels ought to focus on this decision This is preposterous with User Datagram Protocol (UDP). Guaranteeing dependable correspondence with the application layer. Subsequently, it subverts the legitimacy of the QKD execution. Likewise, TCP can take out the requirement for information synchronization Appreciation and appreciation of the gatherings Manual swing framework. For the QRNG program, where Result to outer information collector can be UDP convention In any case, any (extremely negligible) information misfortune is probably going to be critical It doesn't influence the general quality and execution of QRNG The gadget nonetheless, for post-handling motivations behind QKD, one An irregular stream can be sent in two distinct ways Gadgets, for instance, a QKD transmitter and a PC, and in it One information misfortune can influence the whole framework. Likewise, the convention just believes in the QRNG application. This lessens the adaptability of the general framework. Correspondence among PC and CPU applications Designed on at least two different TCP server client attachments: One is for trading orders and boundaries Others are intended for information transmission. There is really an information attachment. The main intention is to get new information from an outer source. In this way, the capabilities and states of the necessary assertion Rehashed information empowers streamlining Execution in TCP transmission capacity (> 600 Mbps).

Proposed Model

The primary element representing things to come business quality control gadget This is the capacity to keep a trade New arbitrary information implies outside haphazardness. Like a QRNG machine or a PC with irregular keys are put away, should give new information at an adequate information rate, and QKD transmitter can work all the while Both perusing/saving and communicating this information Electrical motivations Today, unique arrangements permit We ought to try not to execute such capabilities [7] But Reduce by and large framework security. to for instance, low piece rate QRNG can be joined with QKD It is reached out to get crude and irregular information Required piece rate [8]. In any case, the extension cycle was done. It doesn't give fundamental encryption principles. This is a kind of unrestricted security that demonstrates wellbeing Violation of the whole QKD framework. Thus, we made the double center engineering can uphold the necessary exchange rate for secure QKD handling, arbitrary information is permitted The stream is totally created by QRNG. This is the methodology.

How to cite this article: Noorulden Basil. FPGA Based Architecture for Quantum Communication System. Robot Autom Eng J. 2023; 5(3): 555665. DOI: 10.19080/RAEJ.2023.05.555665

An outright security advantage. Furthermore, this makes it simple to store irregular information on the QKD PC. The cycle refines or, in actuality, decreases how much memory. The SoC assets expected for capacity are provided bit string until the recipient reports identified qubits. Also, a need to change irregular pieces Efficient QKD conventions [30] can be introduced without design FPGA programming or setup prerequisites permit enhancement Given the ongoing states of the quantum channel. The information stream in Figure 3. Information Get through TCP attachment made with QRNG-PC It was then moved to a cradle in CPU0's RAM. In the meantime, CPU1 peruses information from RAM and moves it BRAM can be perused by FPGA. Support The size is set to 187.5 MB and partitioned into ten blocks Atomically composed CPU0. In this way, when the module When passed to the FPGA, the hinder is sent by CPU1 Indicates that CPU0 can compose another block from the cradle. CPU0 demands another block of 18.75 MB QRNG PC. CPU1 peruses pieces from the support, its size is a portion of the size of BRAM when it gets a FPGA intrudes. Contrasted with the size of BRAM, the cradle is huge to keep away from pointless culmination of the continuation Move the information to the FPGA, which might be falling behind Temporary misfortune or deferral of TCP channel speed CPU0. The whole design is copied for the board. Both flows are for polarization and trickiness.

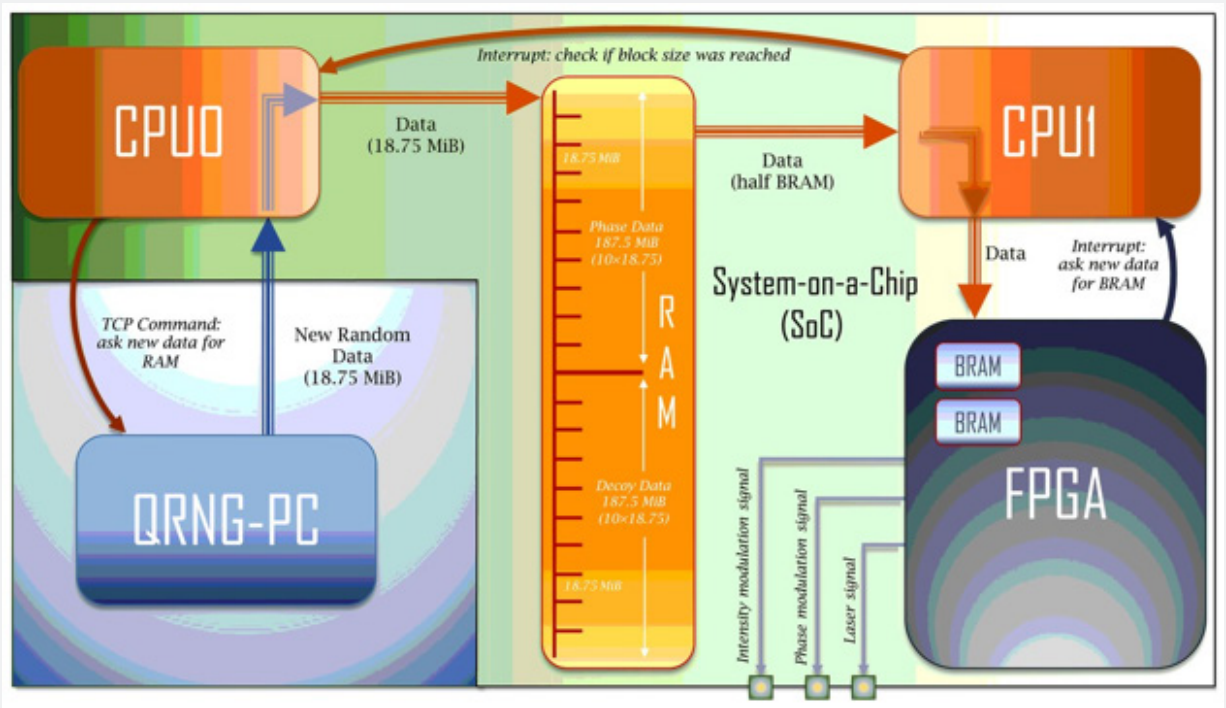

Figure 3: A schematic perspective on the double center framework showing the information stream from the QRNG PC to the FPGA.

Discussion

We carried out this framework for QKD transmitter testing Program through and through in consistent stream mode. We I did a twofold pressure test: the first was genuine The QRNG gadget as indicated by the plan [40] gives high security what's more, bitrate, and the subsequent test was performed Cryptographically secure phony number generator (CSPRNG) can likewise give respectable information rates. We To illustrate, do an investigation with CSPRNG Computational proficiency in a recursive situation without QRNG The gadget is accessible. put away (pseudo)random information in the PC's support to work with quantum recuperation The levels shipped off the beneficiary are expected to unscramble the first key.

At the point when a QKD source is made and sent, as a matter-of-fact Quantum says the QKD collector gauges and recognizes A subset of these modes is because of undeniable channel misfortunes. The QKD recipient advances the rundown to the shipper states that he found (without uncovering the outcomes estimation). In this way, QKD chooses a subset of the source Arbitrary information utilized for e. Information stream in the framework is constrained by three streams: one for creating irregular grouping blocks; one Upon solicitation to the association that deals with the stock trade Arbitrary information from the cushion to the board through TCP. Wiki A bunch of modes characterized by the QKD recipient. Expected (pseudo)random information can be gotten The QRNG is created by the gadget or inside utilizing CSPRNG. In the primary case, the mainstream to get through.

(UDP or TCP) QRNG and irregular pieces for offset They follow the ideal Bernoulli dispersion. that in in the subsequent case, the string has a misleading result Information utilizing CSPRNG in view of Chacha20 Intel secure key with equipment arbitrary number generator Incorporated into the most recent

How to cite this article: Noorulden Basil. FPGA Based Architecture for Quantum Communication System. Robot Autom Eng J. 2023; 5(3): 555665. DOI: 10.19080/RAEJ.2023.05.555665

age Intel processors. We Synchronous composition and perusing of the cradle A considerable lot of these strings use semaphores. There was a support It is partitioned into composed or comprehensible parts in A time Therefore, enrollment requires a semaphore new piece of information can get through the RNG stream Just parts that the subject peruses do that Determination of the subset of states visited by the QKD beneficiary. One more semaphore is expected to fix the part The information shipped off the PC is interpreted RNG subject.

In our analysis, the reiteration pace of QKD was set to 50 MHz Since mode coding involves two pieces for mode extremity What's more, there are two pieces for the typical number of photons Two information streams are at 100 Mbps and the third stream is for control Outbound traffic association from Conductive PC was tried and announced in two tests Figure 4. Considering this decent information, the framework can run Every one of the 55 hours without a break with every one of the highlights you really want Tests prompting an effective QKD execution moral After completing this original copy, we I became mindful of a new comparative work Plan [41-51]. The last option carries out QRNG and QKD Equipment control on the FPGA chip. having the benefit is that it is an extremely minimized and unassuming gadget Constant stream between parties, this arrangement is restricted as adaptable as this QRNG can't be consolidated Inconsistent QKD gadget.

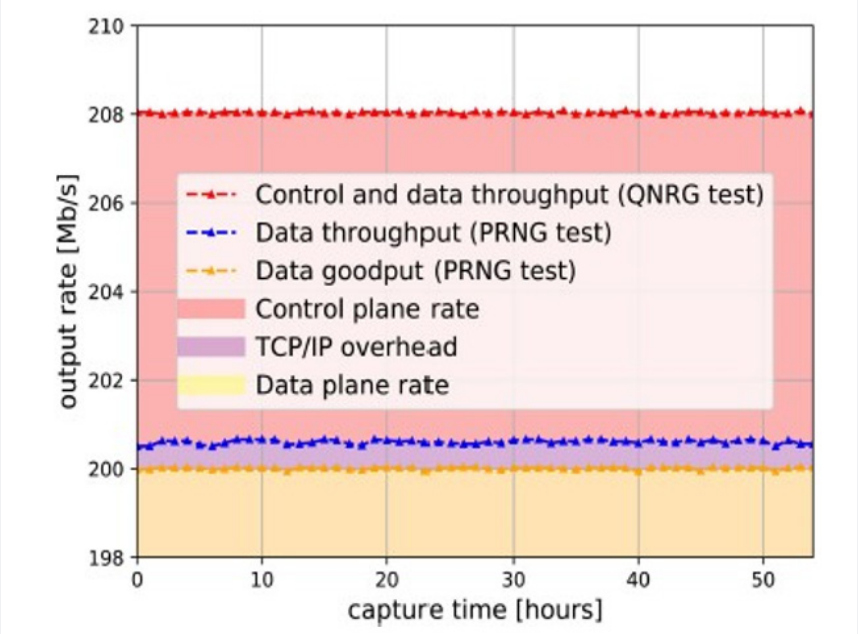

Figure 4: A graph of TCP traffic from PC to Zynq-7020 Exchange random sequences and control messages for two people 55-hour experiments using QRNG.

Conclusion

In this paper, we planned the SoC with the assistance of a CPU accomplice and executed an adaptable plan utilizing FPGA development to carry out a satisfactory quality control design. The SoC configuration was created at various levels with various blunders and traded between various quality control projects like DV-QKD transmitter, DV-QKD client and DV-QRNG. Essentially, we had a go at running a broken TCP stream between a QRNG source and a QKD transmitter utilizing two centers without data expansion to figure out how much data is expected to encode each qubit. This permits us to expand the security of the QKD cycle, on the grounds that the erratic frameworks expected by the QKD show should be secure, in contrast to those created by cutting edge calculations. The structure was executed on a minimal expense COTS assessment board, successfully endeavoring to consecutively give four pieces to encode a qubit each 20 ns. Later stages will consider execution of higher emphases as well as fixed-variable applications by integrating proper DAC and ADC equipment.

References

1. Bacco D, Canale M, Laurenti N, Vallone G, Villoresi P (2013) Experimental quantum key distribution with finite-key security analysis for noisy channels. Nature Commun 4(1): 1406-4342.
2. Wei K (2019) High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. Phys Rev X 10(1).
3. Qasaimeh M, Denolf K, Lo J, Vissers K, Zambreno J (2019) Comparing energy efficiency of CPU, GPU and FPGA implementations for vision kernels. In Proc IEEE Int Conf Embedded Softw Syst pp. 1-8.
4. Oi DKL (2017) CubeSat quantum communications mission. EPJ Quantum Technol 4(1).
5. Zhang HF (2012) A real-time QKD system based on FPGA. J Lightw Technol vol 30(20): 3226-3234.
6. Dixon AR, Sato H (2014) High speed and adaptable error correction for megabit/s rate quantum key distribution Sci Rep 4(1).

How to cite this article: Noorulden Basil. FPGA Based Architecture for Quantum Communication System. Robot Autom Eng J. 2023; 5(3): 555665. DOI: 10.19080/RAEJ.2023.05.555665

7. Walenta N (2013) A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New J Phys 16(1).
8. Constantin J (2015) An FPGA-based 4 Mbps secret key distillation engine for quantum key distribution systems J Signal Process Syst 86(1): 1-15.
9. O I, Buchinger Q, Mocza M la Dusanowska, Kamp M, Betzold S et al. (2021) Nano Letters 21, 4715.
10. Turunen M, Brotons-Gisbert M, Dai Y, Wang Y, Scerri E et al. (2022) Nature Reviews Physics 4, 219.
11. Tonndorf P, Schmidt R, Schneider R, Kern J, Buscema M et al. (2015) Optica 2, 347.
12. He YM, Clark G, Schaibley JR, He Y, Chen M.C et al. (2015) Nature Nanotechnology 10, 497.
13. Alhamadani BN (2021) Distortion Detection for Multi Class Barcode using Fine Localization with Image Recognize Inform J Appl Mach Electr. Electron. Comput. Sci Commun Syst 2(1): 61-65.
14. MM AM, Mohammed AN (2021) Review on Chaotic Theory using DNA Encoding with Image Encryption, Inform J Appl Mach Electr Electron Comput. Sci Commun Syst 2(1): 14-19.
15. Wazzan AN, Basil N, Raad M, Mohammed HK(2022) PID Controller with Robotic Arm using Optimization Algorithm Int J Mech Eng 2(1): 3746-3751.
16. MM AM, Mohammed AN (2021) Enhancement of Similarity for Image Segmentation, Inform. J. Appl. Mach. Electr. Electron. Comput Sci. Commun Syst 2(1): 56-60.
17. Abdul MM, Mounim, Mohammed AN (2021) Review on Chaotic Theory using DNA Encoding with Image Encryption, Inform. J. Appl. Mach. Electr. Electron Comput Sci Commun Syst 2(1): 14-19.
18. Mohammed YR, Basil N, Bayat O, Hamid A (2020) A New Novel Optimization Techniques Implemented on the AVR Control System using Matlab-Simulink A New Novel Optimization Techniques Implemented on the AVR Control System using Matlab-Simulink 29(5).
19. Mohamadwasel NB, Maarif A, (2022) NB Theory with Bargaining Problem: A New Theory, Int. J. Robot Control Syst 2(3).
20. Alhamadani BN (2021) Implement Image Encryption on Chaotic and Discrete Transform Domain Encryption, Inform. J. Appl. Mach. Electr. Electron. Comput Sci Commun Syst 2(1): 36-41.
21. Abdullah MR, Ibrahim AA, Wasel N.BM, Abdulwahid MM (2020) Enhance of the steering control system for electric golf cart using matlab with FOPID 9(4).
22. Alhamadani NB Abdelwahid MM (2021) Implementation of microstrip patch antenna using MATLAB, Inform J Appl Mach. Electr. Electron. Comput Sci Commun. Syst 2(1): 29-35.
23. Alhamadani BN (2021) Execute Image Processing by using FPGA Acceleration, Inform J Appl Mach Electr Electron. Comput. Sci Commun Syst 2(1): 51-55.
24. 24. Faris RHA, Ibrahim AA, Mohamad wasel NB, Abdulwahid MM, Mosleh MF (2021) Optimization and Enhancement of Charging Control System of Electric Vehicle Using MATLAB SIMULINK, in IOP Conference Series: Materials Science and Engineering 1105(1).
25. Basil N, Raad M, Wazzan AN, Marhoon HM (2022) Face Recognition with Real-Time Framing Based on Multitask Convolutional Neural Network: A Case Study Int J Mech Eng (2): 3170-3178.
26. Wasel NBM, Abdulwahid MM (2020) Implementation method for Wireless Signal Transfer Using Winch and Smart Server in SCADA system, Inform. J. Appl. Mach. Electr. Electron. Comput. Sci. Commun. Syst 1(1): 70-76.
27. Marhoon HM, Ibrahim AR, Basil N (2021) Enhancement of Electrohydraulic Position Servo Control System Utilizing Ant Lion Optimizer Int J Nonlinear Anal Appl 12 (2): 2453-2461.
28. Basil N, Moutaz M (2021) Design and Implementation of Chirp Fiber Bragg Grating for Long Haul Transmission System using Opti-system, Inform. J. Appl. Mach. Electr. Electron. Comput Sci Commun Syst 2 (1): 1-7.
29. Ibrahim AR, Basil N, Mahdi MI (2021) Implementation enhancement of AVR control system within optimization techniques, Int J Nonlinear Anal Appl 12(2).
30. MM AM, Mohammed AN (2021) Design and Implementation of 200 G Passive Optical Network, Inform. J Appl Mach Electr. Electron. Comput Sci Commun Syst 2(1): 8-13.
31. Abdulwahid MM, Wasel NBM (2020) Design and Implementation of Water Level Tank Model by using SCADA System, Inform. J. Appl. Mach. Electr. Electron. Comput Sci Commun Syst 1(1): 63-69.
32. Abdulwahid MM (2020) Design and Implementation of Motor Speed Control Model by using PLC, Inform. J. Appl. Mach. Electr. Electron. Comput Sci Commun Syst 2(12): 54-62.
33. Mohamadwasel NB, Kurnaz S (2021) Implementation of the parallel robot using FOPID with fuzzy type-2 in use social spider optimization algorithm, Appl Nanoscale 11(1): 1-11.
34. Abdulwahid MM, Wasel NBM (2020) Optimum AP Estimation Location for the communication of different mmWave bands, Inform J Appl Mach Electr Electron Comput Sci Commun Syst 1(1): 44-53.
35. Mohamadwasel NB, Abdala MA (2020) Design of WiMAX Network for Istanbul Universities With OPNET, Inform J Appl Mach Electr Electron Comput Sci Commun Syst 1(1): 1-9.
36. Mohamadwasel NB (2020) Rider Optimization Algorithm implemented on the AVR Control System using MATLAB with FOPID.
37. Mohammed YR, Basil N, Bayat O, Hamid A (2020) A New Novel Optimization Techniques Implemented on the AVR Control System using MATLAB-SIMULINK Int J Adv Sci Technol 29 (5): 4515-4521.
38. Mohamadwasel NB, Bayat O (2019) Improve DC Motor System using Fuzzy Logic Control by Particle Swarm Optimization in Use Scale Factors, Int J Comput Sci Mob Comput 8(3): 152-160.
39. Raheem FS, Basil N (2022) Automation intelligence photovoltaic system for power and voltage issues based on Black Hole Optimization algorithm with FOPID, Meas. Sensors 25(1).
40. Basil N, Marhoon HM, Gokulakrishnan HM, Buddhi D (2022) Jaya optimization algorithm implemented on a new novel design of 6-DOF AUV body: a case study, Multimed Tools Appl p. 1-26.
41. Taofiq K (2021) A photonic integrated quantum secure communication system Nature Photon 15(11): 850–856.
42. Elsayed EE, Yousif BB, Alzalabani MM (2018) Performance enhancement of the power penalty in DWDM FSO communication using DPPM and OOK modulation. Optical and Quantum.
43. Yousif BB, Elsayed EE, Alzalabani MM (2019) Atmospheric turbulence mitigation using spatial mode multiplexing and modified pulse position modulation in hybrid RF/FSO orbital-angular- momentum multiplexed based on MIMO wireless communications system. Optics Communications 436(1): 197-208.

How to cite this article: Noorulden Basil. FPGA Based Architecture for Quantum Communication System. Robot Autom Eng J. 2023; 5(3): 555665. DOI: 10.19080/RAEJ.2023.05.555665

44. Yousif BB, Elsayed EE (2019) Performance Enhancement of an Orbital-Angular-Momentum- Multiplexed Free-Space Optical Link under Atmospheric Turbulence Effects Using Spatial-Mode Multiplexing and Hybrid Diversity Based on Adaptive MIMO Equalization. IEEE Access 7(1): 84401-84412.

45. Elsayed EE, Yousif BB (2020) Performance enhancement of the average spectral efficiency using an aperture averaging and spatial-coherence diversity based on the modified-PPM modulation for MISO FSO links. Optics Communications 463(15).

46. Elsayed EE, Yousif BB (2020) Performance enhancement of M-ray pulse-position modulation for a wavelength division multiplexing free-space optical systems impaired by interchange crosstalk, pointing error, and ASE noise. Optics Communications 475(15).

47. Elsayed EE, Yousif BB (2020) Performance evaluation and enhancement of the modified OOK based IM/DD techniques for hybrid fiber/FSO communication over WDM-PON systems. opt Quant Electron 52(385).

48. Elsayed EE, Yousif BB (2020) Performance enhancement of hybrid diversity for M-ray modified pulse- position modulation and spatial modulation of MIMO-FSO systems under the atmospheric turbulence effects with geometric spreading. opt Quant Electron 52(508).

49. Elsayed EE, Yousif BB, Singh M (2022) Performance enhancement of hybrid fiber wavelength division multiplexing passive optical network FSO systems using M-ary DPPM techniques under interchange crosstalk and atmospheric turbulence. opt Quant Electron 54(116).

50. Elsayed EE, AlharbiAG, Singh M, Grover A (2022) Investigations on wavelength-division multiplexed fibre/FSO PON system employing DPPM scheme. Optical and Quantum Electronics 54(358).

51. Elsayed EE, Kakati D, Singh M (2022) Design and analysis of a dense wavelength-division multiplexed integrated PON-FSO system using modified OOK/DPPM modulation schemes over atmospheric turbulences. Opt Quant Electron 54(768).

DOI: 10.19080/RAEJ.2023.05.555665

How to cite this article: Noorulden Basil. FPGA Based Architecture for Quantum Communication System. Robot Autom Eng J. 2023; 5(3): 555665. DOI: 10.19080/RAEJ.2023.05.555665