ISBN 978-93-84468-20-0
Proceedings of 2015 International Conference on Future Computational Technologies (ICFCT'2015)
Singapore, March 29-30, 2015, pp. 1-7

FPGA Implementation of New Genearation Cryptographic Algorithm

N. Bharathiraja[$], P. Karthigaikumar[*], and Sreejitha Sasikumar[+]
[*] Department of Electronics and Telecommunication Engineering,
[$] Research Scholoar, Anna University, Chennai
[+] Department of Electronics and Communication Engineering,
Karpagam College of Engineering, Coimbatore, Tamilnadu, India
p.karthigaikumar@gmail.com

Abstract**:** *In data and telecommunications, cryptography is necessary when communicating over any untrusted medium particularly the internet. Technology advancement is evolving daily which demands for a new cryptographic algorithm. Recent advancements in cryptography have led to a new technique called Quantum Cryptography. It is an effort which allows two users of a common communication channel to create a body of shared and secret information, which generally takes the form of a random string of bits and can be used as a conventional secret key for confidential information. In this paper, FPGA implementation of quantum key based AES algorithm is presented. The hardware implementation provides better and faster results compared to other environment. This method offers high security compared to the ancient cryptographic systems. To the best of our knowledge, this is the first research paper in realizing the AES with quantum key in FPGA.*

Key word**:** Quantum key, FPGA, Security, throughput

1. Introduction

One of the major problems that are faced in today's world of communication is lack of security. The problem of confidentiality, authenticity and anonymity have been studied extensively in cryptography, and the notion of provable security is the foundation for most of the modern cryptographic research. Recently NIST announced that AES is best option [1] for securing the data than any other security algorithms. The strength of cryptographic algorithm depends on its key. Although it is assumed that no one has cracked the strongest encryption keys used in commerce and government; there is no guarantee that these keys, based on factoring large numbers, will be secure forever. Due to current advancement in cryptography, there are most efficient techniques available nowadays. One such technique is Quantum cryptography. The main advantage of Quantum cryptography over other traditional methods is that the exchange of information can kept be secure in a very strong sense. Even when assuming speculative eavesdroppers with unlimited computing power, the laws of physics guarantee that the secret key exchange will be secure.

Several architectures have been proposed to implement the AES algorithm by different authors given in [2]. A new and different foundation for cryptography through the uncertainty of quantum physics was found in [3]. Quantum coding has been used in association with Public key cryptographic techniques to get several schemes for unforgettable subway tokens. Instead of an ordinary channel, a quantum channel is set up which does not permit any eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely.

Simulation of quantum cryptography over JAVA platform and a DNA based algorithm for secure communication is designed [4]. Their system can guard against man in the middle attack, eavesdropping,

spoofing, and packet sniffing and replay attack. This is because the fundamentals of QC are based on the laws of physics; thus the eavesdropper would be unable to generate the exact replica of the photons exchanged between the communicating parties as well as record the stream of photons exchanged between them. However their system needs research on overcoming distance limitations and protection against denial of service attack and to devise cost effective methods for generation, polarization, transmission of photons and retaining their polarizations over long distance.

Research in quantum cryptography is carried out and the quantum key distribution protocols are discussed in high length [5]. Her work focuses on quantum cryptography which uses quantum key distribution which uses basic quantum properties to detect eavesdroppers in one of the two ways: either by relying on the Heisenberg Uncertainty Principle or by the violation of Bell's Inequalities in entanglement based schemes.

Cryptography and its various methods are being elaborately discussed in [6]. This book gives an overview of cryptography and network security.

Quantum key distribution is the most matured application of quantum communication [7]. Here they introduce a TDC (time to digital converters) based on FPGA. High precision TDC can effectively reduce the system timing jitter, resulting in lower quantum bit error rate (QBER) and higher key rate.

Implementation of a high-speed and low power encryption algorithm with high throughput for encrypting the image is been carried out in [8]. Here they have selected a highly secured symmetric key encryption algorithm in order to increase throughput and speed using pipelining of four stages and also for reducing power consumption using resource sharing, pipelining and signal gating.

The overview of existing methods is given in table 1.

TABLE I: Overview of existing works in Quantum cryptography

AUTHOR	CONCEPT
[9]	FPGA technologies are discussed in detail including its properties and also the advantages of FPGA in cryptographic applications.
[4]	Quantum key distribution is discussed in high length. And DNA based algorithm is used for secure communication
[5]	Discusses about Quantum Key distribution protocols.
[7]	Discusses quantum key distribution as the most matured application of quantum communication. Here they introduce a TDC (time to digital converters) based on FPGA.

2. Implementation Of Proposed Quantum Key Based Aes Algorithm

Quantum key distribution is a key establishment protocol which creates symmetric key material by using quantum properties of light which is capable of transferring information from sender to receiver in a manner through which the indisputable results of quantum mechanics will highlight any eavesdropping by an opponent. This can be used to derive a key which can be used to encrypt plaintext using a one-time pad encryption.

By keeping these security reasons in mind, quantum phenomena supporting quantum key distribution protocol is explored widely and thus security is based on the "laws of physics" becomes a reality.

Quantum communication involves encoding information in quantum states or qubits as opposed to classical communication's use of bits. Usually photons are used for these quantum states.

2.1 BB84 Protocol

BB84 protocol [10-13] is named after its inventors Charles H. Bennett and Gilles Brassard, and was originally explained using photon polarization states to transmit information. Any two pairs of conjugate states can be used for this protocol. The sender and receiver are connected through quantum communication channels which transmit quantum states. In case of photons, this channel is simply an optical fiber or free space.

The first step in BB84 is quantum transmission. A creates a random bit (0 or 1) and then selects one of the two bases (rectilinear or diagonal in this case) to transmit it in. It then prepares a photon polarization state depending both the bit value and basis, as shown in the table 2. So for example '0' is encoded in the rectilinear

basis (+) as a vertical polarization state and '1' is encoded in the diagonal basis (x) as a 135° state. It then transmits a single photon in the state specified to B, using the quantum channel. This process is then repeated from the random bit stage by recording the state, basis and time of each photon sent.

According to quantum mechanics, none of the possible measurement distinguishes between the 4 different polarization states shown in table 2, as they are not all orthogonal. The only possible measurement is between any two orthogonal states. So, for example, measuring in the rectilinear basis gives a result of horizontal or vertical. If the photon was created as horizontal or vertical then this measures the correct state, but if it was created as 45° or 135°, then the rectilinear measurement instead returns either horizontal or vertical at random. Furthermore, after this measurement the photon is polarized in the state it was measured in (horizontal or vertical), with all information about its initial polarization lost.

TABLE II: Shows the four different polarization states

Basis	0	1
+	↑	→
X	↗	↘

Now receiver B does not know the basis of the photons that were encoded in, all he can do is to select a basis at random to measure in, either rectilinear or diagonal. He does this for each photon he receives, recording the time, measurement basis used and measurement result. After B has measured all the photons, he communicates with sender A over the public classical channel. A, then broadcasts the basis each photon was sent in, and B, the basis each was measured in. They both discard photon measurements (bits) where B used a different basis, which is half on average, leaving half the bits as a shared key. Table 3 shows that how the exchange of key is happening in QC.

TABLE III: Exchange of Key in QC

A's random bit	0	1	1	0	1	0	0	1
A's random sending basis	+	+	×	+	×	×	×	+
Photon polarization A sends	↑	→	↘	↑	↘	↗	↗	→
B's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization B measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

If a third party (usually referred to as 'eavesdropper') has gained any information about the photons' polarization, this introduces errors in B's measurements.

The key generated will be in the form of zeroes and ones, random bit depending upon the direction of flow of the photons.

2.2 Authentication

This protocol [14] uses the classical as well as quantum cryptographic protocols. The different steps for mutual authentication between A and B are,

Step 1: If A wants to communicate with B, initially A and B send their unique identity to authentication server through public channel.

Step 2: Once it verifies their identities, the authentication server (AS) produce a random stream of basis and sends it to A and B.

Step 3: The AS then simulates a random stream of photons and pass it to A and its complement to B.

Step 4: "A" then sends a portion of received photons to B, and B checks for its complement bits.

Step 5: Once the verification completed, B repeats the same procedure but sends a separate stream of photons.

The key that is generated as per BB84 protocol is then passed as the cipher key into the AES encryption and decryption block. The flow is shown in figure 1 for encryption and decryption respectively.

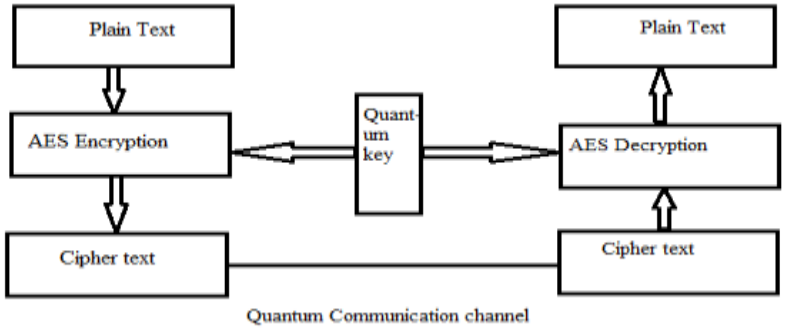

Fig. 1: Quantum key based AES Enc/Dec flow diagram

The message is encrypted using AES encryption algorithm. The bit length of AES can be of 128,192, & 256. Here AES of 128 bit length is used. Since the algorithm is of 128 bit, the key generated will be also of 128 bit. Each character of a message produces 24 bits; a total of 120 bits is used for message, the rest 8bits go on for padding. The padding is either divided into 4 bits in forward primer or 4bits of reverse primer, defined by user. The message is then carefully transmitted through a channel and then received by the receiver. The receiver decodes the message and the original data for the coded text is obtained.

3. Results And Discussions

The throughput, area consumption and efficiency are the most important parameters in evaluating the performance of the implementation. The proposed architecture is prototyped in Xilinx Virtex 7vx330tffg1157-2 device. The proposed concept was coded using VHDL and simulated using ISE Simulator. The synthesis reports were taken using Xilinx 14.4.

3.1 Simulation Results

*A. **Simulation of basic AES***

Initially the basic AES encryption and decryption was simulated and tested with NIST test inputs to validate the encrypted and decrypted data. The basic 128-bit AES code was written using VHDL and simulated.

The basic AES encryption and decryption outputs were shown in figure 2. The key size considered here is 128 bits. The input plaintext given for AES encryption is 00112233445566778899aabbccddeeff. The ciphertext obtained is 69c4e0d86a7b0430d8cdb78070b4c55a.

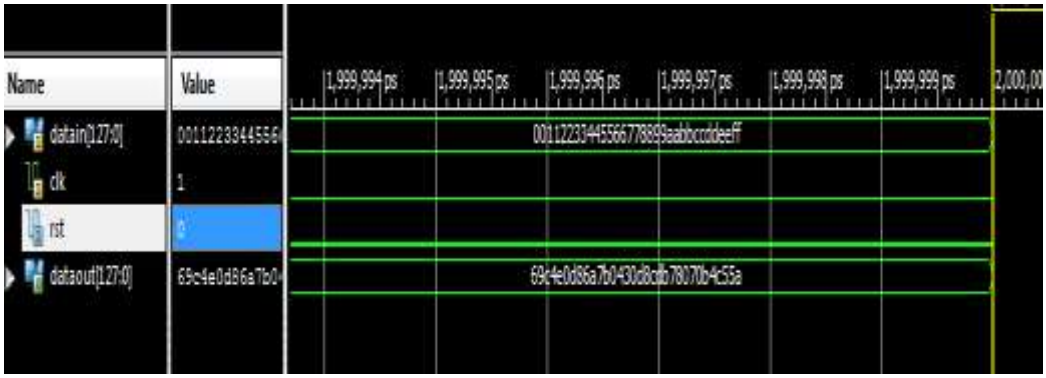

Fig. 2: Basic AES encryption.

Decryption being the inverse process of encryption, the input text here is output obtained from the encryption block, which is: 69c4e0d86a7b0430d8cdb78070b4c55a. After the decryption, the original plaintext was obtained which is shown in figure 3.

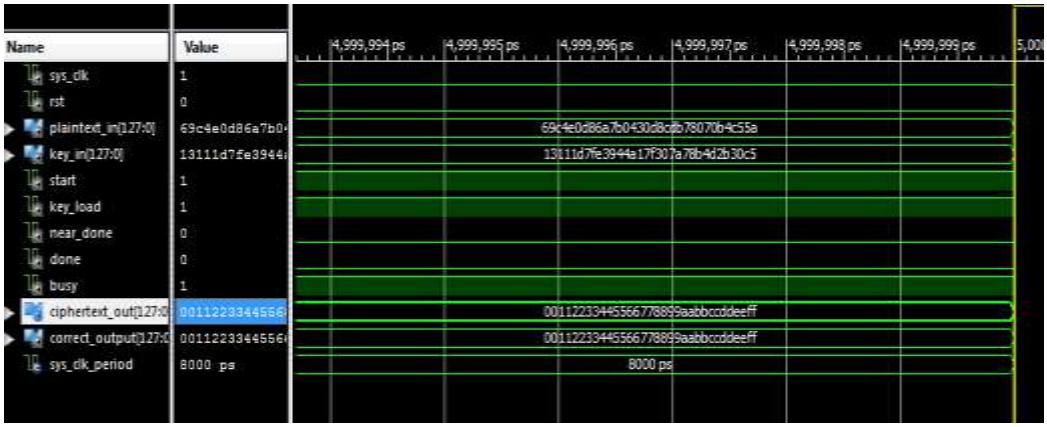

Fig. 3: Basic AES decryption

B. ***Simulation of AES algorithm using quantum key***

Here the key given to AEs algorithm is obtained from quantum concept. The first step is the generation of quantum key. As discussed in chapter 2, BB84 protocol plays an important role in generating the quantum key. The key consists of randomly generated bits of zeroes and ones based on quantum transmission. In figure 4, it shows that at the clock event the corresponding key in single bit is generated. Here 'a' is assigned as '1' and b is assigned as '0'.

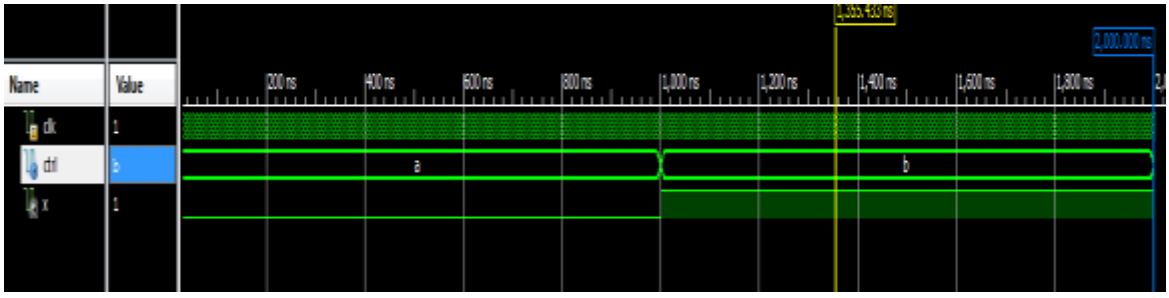

Fig. 4: quantum key generation

The quantum key thus generated is passed to the AES encryption stage. The key is of size 128 bits. If the key size is of 128 bits, the algorithm performs 10 rounds of encryption and decryption. The plaintext passed here is: 00112233445566778899aabbccddeeff. The quantum key is assigned as 'q_key'. The ciphertext obtained is given in figure 5.

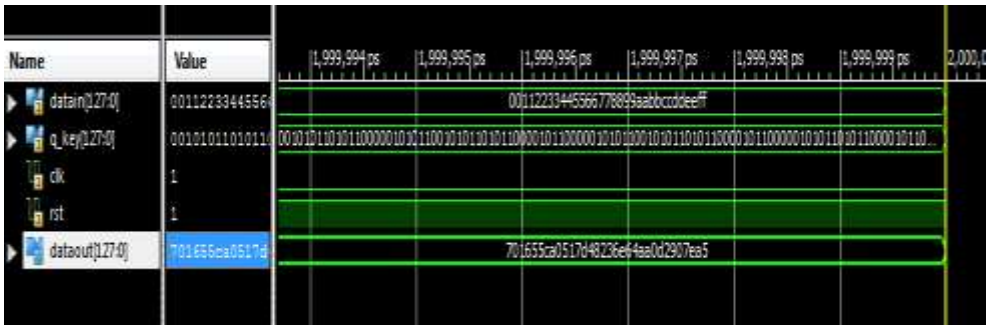

Fig. 5: AES encryption using quantum key

The figure 6 demonstrates the AES decryption process. The output obtained in the encryption stage is passed as the input here along with the quantum key generated. The initial plaintext is obtained after the decryption process.

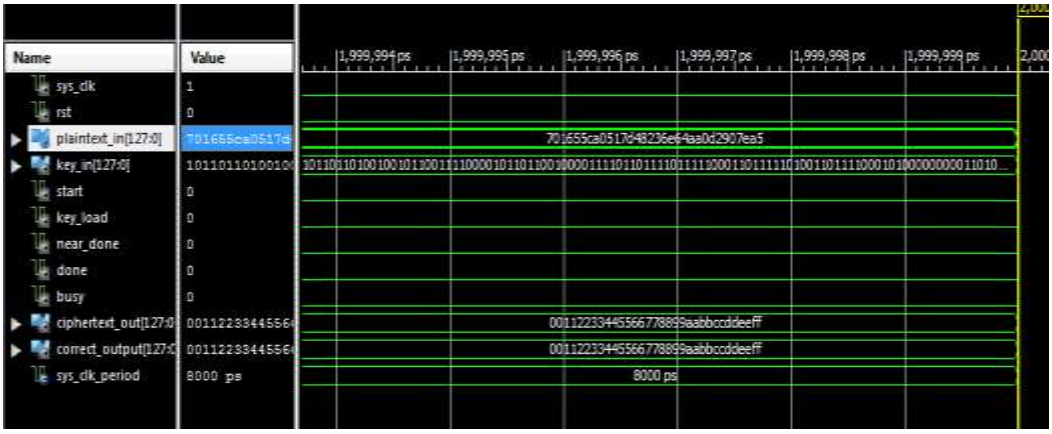

Fig. 6: AES decryption using quantum key

3.2 Synthesis And Power Reports

A. Synthesis results and performance analysis

The synthesis results after the place and route of the implemented architecture on the Xilinx Virtex- VII FPGA was detailed in Table 4. Herein, the maximum frequency and the hardware resource's consumption in terms of slices were specified. The results demonstrate that the proposed architecture can be easy and efficiently implemented on FPGA technologies. Indeed, our implementation on a Xilinx Virtex-VII device uses only 6803 CLB-Slices under the maximum frequency of 50.15 MHz.

To evaluate the performance of the proposed hardware implementation, the throughput rate and efficiency metrics are used. In our case, the throughput rate (defined as the number of bits per unit of time) and the efficiency is defined as number throughput per area. Therefore the throughput and efficiency of our proposed architecture are 6.4 Gbps and 0.94 Mbps for basic AES. The throughput can be increased using pipelining and parallel processing concept.

TABLE IV: Performance comparison of proposed system with conventional system

PARAMETER	**AES with Traditional Key**	**AES with Quantum Key**
	ENCRYPTION	**ENCRYPTION**
Number of Slices	6610	6803
Number of IOB	257	257
Number of GCLK's	1	1
Freq (MHz)	32.52	50.15
Throughput (Gpbs)	4.2	6.4
Efficiency (Mbps)	0.64	0.94

From the table, it is observed that AES with Quantum key consumes more slices than traditional AES algorithm. This is due to the complexity involved to generate the key using quantum concept. Since the basics of Quantum Cryptography is based on law of physics, the intruder could not able to get the exact photons transmitted between two people and hence the of AES with quantum key is higher than traditional AES algorithm.

The power obtained for the proposed architecture using Xilinx XPower Analyzer is 143 mW.

4. Conclusion

In this research work, a quantum key of 128 bit is generated and it is passed on as key to the AES encryption and decryption. From the analysis it has been proved that AES with quantum key has higher throughput and

security than traditional AES. Hence conclusion can be wrapped up stating that quantum key is better not only in terms of security but also uses less power and gives high speed execution.

5. References

[1] National Inst. of Standards and Technology (NIST), "Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES)", 2001.

[2] K. Rahimunnisa, P. Karthigaikumar, N. Anitha Christy, S. Suresh Kumar, J. Jayakumar, **"**PSP: Parallel sub-pipelined architecture for high throughput AES on FPGA and ASIC**"** Central Europ. J. Computer Science, 3(4), 173-186, 2013. http://dx.doi.org/10.2478/s13537-013-0112-2

[3] Charles H. Bennett, Gilles Brassard, "Quantum cryptography: public key distribution and coin tossing", International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 10-12, 1984. http://dx.doi.org/10.1016/j.tcs.2014.05.025

[4] SharvariGogte, et al., "Simulation of Quantum Cryptography and use of DNA based algorithm for Secure Communication." IOSR Journal of Computer Engineering 11(2), 64-71, 2013.

[5] Sheila Cobourne, " Quantum Key Distribution Protocols and Applications", Royal Holloway, University of London, Egham, Surrey TW20 0EX, England, 2011.

[6] William Stallings, "Cryptography and Network Security", Third Edition, Prentice Hall International, 2003

[7] Qi Shen, et al, "An FPGA-Based TDC for Free Space Quantum Key Distribution" IEEE transaction on Nuclear Science, 60 (5), 3570 – 3577, 2013. http://dx.doi.org/10.1109/TNS.2013.2280169

[8] G. H. Karimian, et al, "A High Speed and Low Power Image Encryption with 128 Bit AES Algorithm", IJCEE, 4(3), 367-372, 2012. http://dx.doi.org/10.7763/IJCEE.2012.V4.514

[9] Wollinger T. and Paar C., "How secure are FPGAs in cryptographic applications?", in Proceedings of the 13th International Conference on Field-Programmable Logic and Applications, FPL2003, Lisbon, Portugal, Sep. 1-3, Lecture Notes in Computer Science,Vol. 2778, Springer, 91-100, 2003.

[10] Mehrdad S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System, 2009 Sixth International Conference on Information Technology: New Generations, 1644-1648, Las Vegas, 2009

[11] Marcin Sobota, Adrian Kapczy_ski, Arkadiusz Banasik, "Application of Quantum Cryptography protocols in Authentication process", The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic , 15-17 September 2011.

[12] Yoshito Kanamori, Seong-Moo Yoo, Don A. Gregory, Frederick T. Sheldon, "On Quantum Authentication Protocols", proceedings of IEEE GLOBECOM, 2005.

[13] http://swissquantum.idquantique.com/?Key-Sifting

[14] D. Richard Kuhn, "A quantum cryptographic protocol with detection of compromised server", Quantum Information and Computation, Vol. 5, No.7, 551-560, 2005.