Patent Search

Invention Title	INNOVATION OF ML AND QUANTUM CRYPTOGRAPHY FOR SOC APPLICATIONS
Publication Number	35/2023
Publication Date	01/09/2023
Publication Type	INA
Application Number	202341047886
Application Filing Date	16/07/2023
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMMUNICATION
Classification (IPC)	H04L0009080000, H04L0009060000, H04L0009320000, G06N0010000000, H04L0009000000

Inventor

Name	Address	Country
Prashant	Research Scholar (Roll no: 5VY16PEJ83), Department Of ECE, Visvesvaraya Technological University (VTU) Regional Resource Center Belagavi-560091, Karnataka, India . Email: prashantece403@gmail.com	India
Prof (Dr.) Baswaraj Gadgay	Regional Director, Visvesvaraya Technological University (VTU)Regional Campus, Kalaburagi-585105, Karnataka, India. Email : bvgadgay@gmail.com	India
Prashant Bachanna	Assistant Professor Department Of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Hydeerabad-500043, Telangana, India Email: b.prashant@iare.ac.in	India

Applicant

Name	Address	Country
Prashant	Research Scholar (Roll no: 5VY16PEJ83), Department Of ECE, Visvesvaraya Technological University (VTU) Regional Resource Center Belagavi-560091, Karnataka, India . Email: prashantece403@gmail.com	India

Abstract:

[1] In recent decades, quantum computing-based cryptography has become the latest and more secure for the transmission of data through different protocols that wired or wireless in communications. In order to optimize power dynamic and static utilization in digital circuits, Machine Learning (ML) and Quantum computing are major role in designing and implementing cryptography systems. ML is a widely used trained method in any high-level synthesis (HLS) for better and faster performa the estimation of power and hardware resources utilization before implementing on downstream application on FPGA. High-quality and large-volume datasets are ne training ML models in order to make accurate predictions. To train ML models connected to HLS, practitioners must create their own dataset because the present dat in this field are either private or have restricted use.The combination of these two techniques will increase the security level and be used for key authentications and Quantum Key Distribution (QKD) along with ML enables the communicating parties to detect the side channel effects and protection of keys from noisy channels. The generates random keys which can use as private and public keys for data exchange between two parties to ensure these two parties have proper access to meaningf the key. The SHA-256 generates 256-bit hash values that are used for authenticating the signatures and data on the fly so that encryption and decryption can process operation without waiting for hash values as private and public keys. The proposed design has been validated using benchmarking the overhead and measured perfo degradation and shown their suitability for SoC and FPGA systems. The complete design is synthesized using Vivado Design Suite 2018.1 and interfaced with Software Development Kit (SDK) for validation of data transfer between the user application and FPGA.

Complete Specification

Description:DESCRIPTION OF THE INVENTION

[11] The master and slave want to share important information other than random numbers like secrete photos, important passwords, and any other useful inform to provide security to them, required a lot of memory, and area and also consumes more power so in order to optimize the hybrid techniques such as ML and QKD incorporated in the design. The QKD-based encryption uses module 2 addition between information and key, the key is generated by quantum computing, and the encryption expression is given by

$Q_e=M \oplus_2 Q_k$--------(1)

Where Q_eis quantum encryption, M is secreted information to be transmitted and Q_k is the key generated by quantum, and M is given by

$M=Q_e \oplus_2 Q_k$--------(2)

[12] The BB84 protocol is a basic quantum cryptography protocol and it is used to share secrete keys without pre-sharing of the secret key. The information exchan between master and slave procedure is as follows.

Master selects a random bit that is generated by the QKD generator.

Master selects a random basis which is denoted by B_z or B_x using a random bit generator. This random bit is encoded and then transmits the “qubit” to the slave the quantum channel as shown in Fig.1.Slave selects a random basis (B_z or B_x) using a random generator and it measured the received qubit and decodes the or bits. Once both are shared same basis then it is nothing but both are having same secret bits. If both don’t have the same bits then they share the same bit with a

View Application Status