RESEARCH ARTICLE OPEN ACCESS

Quantum Cryptography and VIASAT Devices: FPGA Implementation and Protocol Offloading

Dmitry Mikhaylov[1,*], Muhammad Saeed[1], Yasser F. Al Wahedi[1], Lebedev Philipp [2], Klimov Oleg [2] and Artemii Akopov [2]

[1] *Abu Dhabi Maritime Academy, Abu Dhabi, P.O. Box 54477, United Arab Emirates 1;*
[2] *QUROS PTE. LTD, Singapore 2;*
* *Correspondence: dmitry.mikhaylov@adports.ae*

ABSTRACT:
This article explores the feasibility of implementing quantum-resistant cryptographic algorithms on VIASAT devices, focusing on the implementation of FPGA (Field-Programmable Gate Array). The research addresses the resource-intensive nature of post-quantum cryptography and discusses mechanisms to offload traffic efficiently. It investigates the challenges of adapting small electronic devices in sea communications and proposes solutions to enhance their capabilities..

KEYWORDS: quantum computation; quantum information ; computation statistics

---

Date of Submission: 09-04-2024 Date of acceptance: 21-04-2024

I.

II. Introduction

Modern technological advances in the field of quantum computing shed light on new prospects in the field of information technology. The hallmark of quantum computing is using quantum bits (qubits) to represent information, allowing parallel computing and problems beyond the scope of classical computing power.

A. Background

1. Rise of quantum computing and its threat to classical cryptography

The ascendance of quantum computing marks a tectonic shift. Diverging from the binary world of classical computers, where bits oscillate between 0 and 1, quantum counterparts employ quantum bits or qubits. Due to the enigmatic phenomena of superposition and entanglement, these enigmatic qubits can exist in a myriad of states concurrently. This unique attribute empowers quantum computers to undertake intricate computations at velocities that elude their classical counterparts.

Numerous pivotal factors contribute to the escalating fascination and fervor encircling quantum computing:

- **Proliferation of Parallelism**: Quantum computers simultaneously navigate multiple realms of possibilities, courtesy of superposition. This intrinsic parallelism equips them to unravel specific problems at an exponential pace, dwarfing the capabilities of classical computers (Mavroeidis et al., 2018).
- **Speed:** Quantum computers harbor the potential to rapidly decipher specific enigmas, outpacing classical computation's speed (Mavroeidis et al., 2018). Tasks such as deciphering colossal numbers, optimizing intricate systems, and emulating quantum systems metamorphose into streamlined operations with the advent of quantum computing.
- **Cryptographic Conundrums:** Quantum computing casts a formidable shadow over the realm of cryptography. While it posits the jeopardy of dismantling prevailing cryptographic methodologies, it concurrently presents an avenue to concoct novel, impregnable encryption algorithms grounded in quantum tenets (Lindsay, 2018).
- **Optimization:** Quantum computers emerge as ideals of excellence in tackling optimization quandaries, spanning logistical intricacies in supply chain orchestration to refining financial portfolios. Industries tethered to labyrinthine optimization stand to reap substantial dividends from the quantum computational arsenal (Yang et al., 2023).

Despite the optimistic promises, quantum computing finds itself in the embryonic phase, grappling with formidable hurdles such as preserving the fragile quantum states (coherence) and mitigating errors. Across the global spectrum, researchers and corporate entities are ardently pursuing materializing pragmatic quantum computers and delineating the expansive horizons of their practical applications.

Leading entities in the technology sector, including IBM, Google, Microsoft, and pioneering startups like Rigetti and IonQ, are investing substantially in quantum computing research (Yang et al., 2023). Acknowledging the strategic significance of quantum technology, governments actively contribute to the international race for quantum supremacy — the point at which a quantum computer surpasses the capabilities of the most advanced classical computers in specific tasks.

As quantum computing progresses, it holds the potential to revolutionize various disciplines, reshape industries, and confront computational challenges once deemed impossible. However, the practical, widespread integration of quantum computing remains on the horizon, necessitating the resolution of both scientific and engineering challenges, endeavors that researchers are diligently undertaking (Mavroeidis et al., 2018). The ensuing years are poised to witness remarkable strides in developing and applying quantum computing technologies.

In the realm of computational advancements, the specter of quantum computing looms as a formidable challenge to the stalwart bastion of classical cryptography, particularly the widely embraced public-key encryption algorithms. The bedrock of the cryptographic defenses rests upon the labyrinthine nature of specific mathematical difficulties, such as the intricate factoring of colossal numbers or navigating the realm of discrete logarithms (Mavroeidis et al., 2018). Traditional computing architectures find themselves shackled by an insurmountable temporal burden in resolving these enigmatic challenges, erecting a resilient encryption barricade.

Conversely, the quantum juggernaut, armed with the arsenal of quantum parallelism and the formidable Shor's Algorithm, can catapult the factorization of substantial numbers and the computation of discrete logarithms into an exponential sprint. This prowess, unfortunately, threatens the sanctity of well-established cryptographic bastions like RSA and ECC (Elliptic Curve Cryptography).

In the labyrinth of cryptographic landscapes, quantum cryptography emerges as a sentinel, offering fortified security for communication networks, including the intricate web of maritime connectivity epitomized by VIASAT connections. Operating on the esoteric principles of quantum mechanics, quantum cryptography ostensibly cloaks communication channels with an armor impervious to specific breeds of attacks, especially those orchestrated by the formidable quantum computers.

A distinguishing hallmark of quantum cryptography lies in its omniscient gaze, capable of discerning any nefarious endeavor to eavesdrop on the ethereal symphony of communication. This feat is accomplished through the intricate choreography of quantum entanglement and the no-cloning theorem, asserting that the pristine quantum essence of a particle remains impervious to exact replication.

In the tapestry of quantum cryptographic configurations, any interloping audacity to seize quantum information triggers a metamorphic cascade in the quantum states of involved particles. This metamorphosis, akin to a cosmic whisper, resonates with the vigilant custodians of the communication conduit. The intrinsic ability to unveil such clandestine endeavors positions quantum cryptography as an indomitable citadel safeguarding the sanctity of communication channels.

1. VIASAT in sea communications

In global communications, VIASAT emerges as a ubiquitous supplier of satellite communication solutions, mainly specializing in maritime communication. Their array of products and services is meticulously crafted to cater to the intricate demands of nautical applications, ensuring a seamless and intricate web of connectivity while navigating the vast seas (De Gaudenzi et al., 2018). Let's delve into the salient facets of VIASAT's foray into maritime communications:

VSAT Systems: VIASAT, with finesse, presents the Very Small Aperture Terminal (VSAT) systems tailored expressly for maritime deployment. The VSAT technology, an intricate symphony of high-speed, bidirectional satellite communication, seamlessly intertwines ships and maritime vessels with the tapestry of the internet, corporate networks, and assorted communication platforms (De Gaudenzi et al., 2018). These systems prove pivotal in applications ranging from ship management and crew welfare to optimizing operational efficiency with an intricately woven web of connectivity.

Maritime Broadband Services: VIASAT, with a penchant for sophistication, delivers maritime broadband services harnessing the prowess of satellite technology. This transcendent connectivity provides vessels navigating the seas with a high-speed conduit to the internet realm (De Gaudenzi et al., 2018). These services, a testament to technological sophistication, bolster various maritime applications encompassing email correspondence, internet exploration, and expeditious data transference.

Hardware and Terminals. In their arsenal, VIASAT adorns itself with an assortment of maritime satellite communication hardware featuring satellite terminals and antennas. These rugged marvels are meticulously crafted to endure the rigors of the maritime expanse, steadfastly providing unwavering connectivity even in the face of adverse weather conditions (De Gaudenzi et al., 2018). The resolute design of these devices is a testament to VIASAT's commitment to providing reliable communication infrastructure.

Managed Network Services: with a wise approach, VIASAT extends its purview to encompass managed network services tailored explicitly for maritime applications. This suite of services encapsulates vigilant network monitoring, optimization protocols, and adept troubleshooting mechanisms (VIASAT, 2023). Their implementation serves as the linchpin in ensuring the optimal functionality of maritime communication systems, minimizing downtime and disruptions.

Global Coverage: A distinguishing feature of VIASAT's satellite communication services lies in their expansive global coverage (VIASAT, 2023). This, in effect, empowers seafaring vessels to maintain connectivity even in the remotest and offshore locales where conventional communication infrastructure might languish in limitation. The global expanse of VIASAT's services is the backbone that fortifies the connectivity of ships navigating the vast, uncharted waters of the world.

B. Research objectives and significance

Objective 1

Pioneering the development and integration of cryptographic algorithms impervious to quantum threats.

Significance: As the specter of quantum computing advances looms large, the imperative to fortify sensitive information intensifies. This research endeavors to fortify cryptographic resilience against quantum assaults, thus contributing substantively to establishing robust and future-proof security measures.

Objective 2

Architecting solutions based on FPGA, customized to cater to VIASAT devices.

Significance: VIASAT devices assume a pivotal role within communication systems. This exploration seeks to refine their operational prowess by harnessing the capabilities of FPGA technology. The import lies in augmenting the efficiency and adaptability of VIASAT devices, ultimately fostering improvements in communication reliability and speed.

Objective 3

Scrutinizing strategies for efficient protocol offloading to optimize resource utilization.

Significance: The optimization of resources stands as a linchpin for the efficacy of network protocols. This study pivots on identifying and implementing protocol offloading techniques aimed at curtailing resource consumption. The import lies in the amelioration of overall network performance, the reduction of latency, and the ensuring of optimal resource utilization within communication systems.

III. Quantum-Resistant Cryptography

A. Overview of quantum computing threats

Quantum computing, while holding tremendous promise for solving complex problems at unimaginable speeds with classical computers, also brings about several potential threats and challenges. Here's an overview of some critical quantum computing threats:

Shor's Algorithm and Cryptographic Vulnerabilities

Shor's Algorithm emerges as a groundbreaking innovation, particularly for its potential to undermine the foundational security of widely adopted cryptographic systems. Classical encryption algorithms such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) currently hinge on the intricate process of factoring large numbers into their prime components (Ugwuishiwu et al., 2020). When harnessed by a sufficiently potent quantum computer, Shor's Algorithm exhibits the efficiency to conduct this factorization with remarkable speed.

Within classical computing, factorizing large numbers is exceedingly time-intensive, forming the bedrock of security for many encryption protocols. For instance, RSA relies on the intricacy of factoring the product of two sizable prime numbers to safeguard communications (Ugwuishiwu et al., 2020). At the same time, ECC depends on the complexity of solving the elliptic curve discrete logarithm problem. These methods presently furnish a robust protective layer for sensitive data during transmission.

Nevertheless, the advent of quantum computing, spearheaded by Shor's Algorithm, ushers in a paradigmatic shift. Quantum computers, employing the principles of superposition and entanglement, can process copious amounts of information concurrently, rendering the conventional challenges of factorization obsolete. Shor's Algorithm can adeptly factorize large numbers in polynomial time on a quantum computer, presenting a formidable threat to the security underpinnings of RSA and ECC (Seo, 2018).

The consequences of a quantum computer successfully implementing Shor's Algorithm are profound, particularly within communication systems. Given that a significant portion of the world's digital communication relies on the security of RSA and ECC, the advent of quantum-powered decryption capabilities jeopardizes the confidentiality of sensitive information (Seo, 2018). This peril extends across various sectors, encompassing finance, healthcare, government communications, and any other domain where secure data transmission is paramount.

To counter this vulnerability, there is an imperative for developing and implementing quantum-resistant cryptographic algorithms. Post-quantum cryptography is an active area of research dedicated to formulating encryption methods that remain secure even in the face of quantum attacks (Seo, 2018). As quantum computing technology advances, the urgency to transition to these quantum-safe cryptographic solutions becomes increasingly critical to preserving the integrity and confidentiality of digital communication systems.

Data Security

The realm of data security undergoes a profound metamorphosis with the introduction of quantum computing, presenting unparalleled prospects and formidable hurdles. A pivotal apprehension revolves around the potential of quantum computers to unravel data shielded by conventional encryption algorithms. Unlike their classical counterparts operating on bits, quantum computers employ qubits, allowing them to execute intricate computations exponentially faster in specific scenarios, notably in the decryption of classically encrypted data.

The fundamental peril emanates from Shor's Algorithm, a quantum algorithm proficient in efficiently factoring large numbers and resolving specific mathematical quandaries at an exponential pace compared to the most adept classical algorithms. This groundbreaking advance imperils the integrity of classical encryption methods extensively utilized to secure confidential information.

In practical terms, envision a situation where data encrypted with traditional approaches, such as the prevalent Advanced Encryption Standard (AES) or other classical symmetric and asymmetric encryption algorithms, becomes susceptible to decryption by an adequately sophisticated quantum computer (Abdullah, 2017). This vulnerability extends across diverse domains of data security, encompassing personal correspondence, financial dealings, medical archives, and governmental clandestine information.

The imperative to counter this vulnerability becomes increasingly conspicuous as quantum computers advance. The Necessity for formulating and deploying quantum-resistant cryptographic algorithms arises as a pivotal retort to this imminent menace (Cichocki, 2023). Post-quantum cryptography emerged as the discipline committed to devising encryption methodologies capable of withstanding the computational prowess of quantum computers.

Quantum-resistant algorithms are crafted to furnish security against both classical and quantum assaults, ensuring the confidentiality of sensitive information endures even in the face of quantum progress. These algorithms frequently hinge on mathematical challenges posited to be formidable for both classical and quantum computers to unravel, thereby upholding robust data security (Cichocki, 2023).

The transition to quantum-resistant cryptographic algorithms is a technical requisite and a strategic imperative. The evolution and embrace of such algorithms demand synergy among researchers, industry mavens, and policymakers to institute standardized practices universally applicable across diverse systems and platforms. As quantum computers approach practical integration, the proactive assimilation of quantum-resistant cryptographic measures becomes a cornerstone in the perpetual endeavor to fortify the secrecy and privacy of digital information in the quantum epoch.

Quantum Key Distribution (QKD) Vulnerabilities

QKD's distinctive strength lies in its ability to identify any unauthorized attempts at interception or eavesdropping during communication, presenting a security level deemed theoretically impervious within the quantum mechanics framework.

However, notwithstanding its theoretical solidity, the pragmatic deployment of QKD systems introduces an array of hurdles and potential susceptibilities (Huang et al., 2018). One notable concern revolves around the hardware employed in QKD implementations. The intricate quantum states crucial to QKD are exceedingly susceptible to external factors, including temperature fluctuations and electromagnetic interference. These external variables can introduce discrepancies or inadvertent disclosures in the quantum information exchanged, jeopardizing the security assurances embedded in QKD (Huang et al., 2018).

Moreover, QKD systems are prone to side-channel attacks, a category of assaults exploiting inadvertently disclosed information during the physical enactment of cryptographic systems (Huang et al., 2018). These attacks may involve leveraging vulnerabilities in detectors, measuring instruments, or other components of the QKD system. For example, subtle fluctuations in detector efficiency or the timing of photon emissions might be exploited by adversaries to access the quantum key illicitly.

In response to these practical vulnerabilities, ongoing research is committed to augmenting the resilience of QKD systems, spanning various facets:

- **Advancements in Quantum Hardware:** Researchers are diligently crafting more robust and fault-tolerant quantum hardware to alleviate the impact of external elements on quantum states (Xu et al., 2020). This encompasses progress in quantum key generators, detectors, and other pivotal components.
- **Error Rectification Approaches:** Investigations into techniques for error correction in quantum communication protocols are underway (Xu et al., 2020). These methods aim to rectify errors introduced during the transmission of quantum information, ensuring the dependability of exchanged keys.
- **Quantum Repeaters:** A critical area of exploration is the development of quantum repeaters, which extend the range of quantum communication by adeptly managing and rectifying errors in quantum states across longer distances (Liu et al., 2022).
- **Post-Processing Security:** Research endeavors are channeled towards enhancing the security of classical post-processing steps involved in QKD, recognizing vulnerabilities that may emerge during the classical processing of quantum information (Curly & Lo, 2019).

As the domain of quantum communication matures, sustained collaboration between researchers, engineers, and industry partners proves indispensable in fortifying the pragmatic implementation of QKD. The objective is to substantiate that the theoretical security assurances of QKD seamlessly transition into real-world scenarios, cultivating a novel era of secure communication resilient against classical and quantum threats.

Breaking Hash Functions

The emergence of quantum computation not only presents hurdles to conventional encryption methods but also instigates apprehensions about the soundness of widely employed hash functions. Hash functions are indispensable cryptographic instruments that transform input data into fixed-size strings of characters, commonly known as hash values. They play a pivotal role in upholding the integrity and genuineness of data, furnishing a distinctive identifier or "digest" for any specified set of information (Chiesa et al., 2022). Nevertheless, the computational prowess of quantum computers, particularly their capacity to execute certain computations exponentially faster than classical computers, jeopardizes the security of these hash functions.

In classical computation, hash functions are constructed as one-way functions, implying that reversing the process and deducing the original input data from the hash value should be computationally unfeasible (Chiesa et al., 2022). This attribute forms the bedrock for the security of digital signatures, certificates, and other cryptographic protocols reliant on the imperviousness and integrity of hash functions.

Quantum computers, equipped with algorithms like Grover's Algorithm, can potentially compromise the one-way nature of these hash functions. Grover's Algorithm facilitates a quadratic acceleration in search of an unsorted database, altering the security parameters conventionally regarded as sufficient in the classical computing realm.

Postquantum cryptography has emerged as a pivotal research area to counter this vulnerability. Post-quantum cryptography endeavors to devise cryptographic algorithms capable of withstanding the computational might of quantum computers (Yang et al., 2019). Researchers concentrate on fabricating quantum-resistant hash functions and digital signature schemes within this overarching endeavor.

Quantum-resistant hash functions are crafted to uphold their security attributes even when confronted with quantum attacks. These functions must endure the plausible threat posed by quantum algorithms attempting to discover collisions (two distinct inputs yielding the same hash value) or reverse the hashing process.

Digital signatures, reliant on hash functions to assure the integrity of the signed data, are also focal points of research (Yang et al., 2019). Post-quantum digital signatures aspire to offer cryptographic mechanisms that remain secure even when confronted with the capabilities of quantum computers.

The evolution of quantum-resistant hash functions and digital signatures is a technical challenge and a strategic imperative. It involves a multidisciplinary approach, amalgamating expertise in mathematics, computer science, and cryptography to devise algorithms capable of safeguarding digital communication in a quantum-driven future.

As quantum computers progress, the ongoing initiatives in post-quantum cryptography are indispensable for laying the groundwork for a new cryptographic edifice that can furnish long-term security for digital systems, shielding against prevailing and prospective quantum threats.

Global Communication Security

The looming specter of quantum computers casts a formidable shadow over the global communication infrastructure, especially concerning the compromise of widely employed encryption protocols. Existing communication systems heavily lean on cryptographic algorithms to fortify the conveyance of sensitive data. Conventional encryption methodologies, exemplified by RSA and ECC, the stalwarts of secure communication, face the peril of vulnerability due to the robust computational prowess inherent in quantum computers (Seo, 2018).

The eminent peril emanates from Shor's Algorithm, a quantum marvel proficient in swiftly factorizing large numbers and resolving specific mathematical quandaries at speeds exponentially surpassing classical algorithms (Djordjevic, 2020). Consequently, the underpinnings of security for widely embraced encryption protocols might be subverted, ushering in a substantial hazard to the confidentiality and integrity of information coursing through global networks.

To confront this impending menace, an imperative arises for the inception and execution of quantum-safe communication protocols. These protocols, often denoted as post-quantum or quantum-resistant cryptographic algorithms, are meticulously crafted to withstand the computational might wielded by quantum computers. Their mission is to erect a secure bastion for communication in a future where the cryptographic terrain may undergo fundamental transformation owing to the emergence of quantum computing.

Crucial facets in the evolution of quantum-safe communication protocols encompass:

- **Lattice-Based Cryptography:** A promising avenue for post-quantum security relies on the intricacies of specific lattice problems to furnish a bedrock for secure communication (Mohsen, Bahaa-Eldin, & Sobh, 2017).
- **Code-Based Cryptography:** Harnessing the complexity of decoding linear codes to fortify information, showcasing resilience against quantum assaults, and being explored as potential contenders for post-quantum encryption (Balamurugan et al., 2021).
- **Hash-Based Signatures:** Contemplated quantum-resistant alternatives for ensuring the integrity and authenticity of digital signatures anchored in the security of hash functions (Srivastava, Baksi, & Debnath, 2023).
- **Multivariate:** Polynomial Cryptography. Delving into the deployment of systems involving multivariate polynomial equations for encryption, undergoing scrutiny for its resilience against quantum onslaughts (Kuang & Perepechaenko, 2023).
- **Symmetric-Key:** Cryptography. Quantum-safe symmetric-key cryptographic algorithms, rooted in the security of block ciphers, are being investigated as substitutes for conventional symmetric encryption methods (Mitra et al., 2017).

The transition to quantum-safe communication protocols demands a concerted collaboration involving researchers, industry mavens, and policymakers. Standardization initiatives are pivotal to assure interoperability and widespread integration of these protocols across diverse communication systems and platforms (Kannwischer et al., 2022).

Tackling these perils mandates a synergistic endeavor from researchers, policymakers, and industry stakeholders to devise and institute robust quantum-safe solutions and strategies. Persistent research and establishing global standards will play an indispensable role in assuaging the risks accompanying the advent of quantum computing.

B. Necessity for post-quantum cryptographic algorithms

The imperative for post-quantum cryptographic algorithms emerges in response to the looming specter of quantum computing. Traditional cryptographic methodologies, reliant on the intricate computational nature of specific mathematical predicaments, face the peril of swift subversion by the commanding computational prowess inherent in quantum computers.

Shor's Algorithm, a pivotal quantum algorithm, has demonstrated the capacity to adeptly unravel mathematical difficulties such as the factorization of expansive numbers and discrete logarithm challenges. This immediately threatens commonly employed encryption techniques, potentially jeopardizing the impregnability and secrecy of classified information.

The Necessity for post-quantum cryptographic algorithms finds its roots in the Necessity to rectify these vulnerabilities and guarantee the enduring security of digital dialogues. As quantum computational capabilities progress, the authenticity of conventional cryptographic protocols undergoes critical scrutiny, prompting the imperative for formulating and embracing cryptographic approaches resilient against quantum perils.

The gravity of post-quantum cryptographic algorithms extends beyond immediate security, encompassing the fortification of long-term security, preservation of data confidentiality, and assurance of the dependability of digital endorsements. Industries and entities navigating within regulatory frameworks also confront the prospect of evolving compliance standards mandating the assimilation of these cutting-edge cryptographic methodologies.

In essence, the shift towards post-quantum cryptographic algorithms epitomizes a forward-looking response to the transformative potential of quantum computing. It stands as a pivotal stride in reinforcing the bedrock of data security, conserving the privacy inherent in digital interactions, and upholding confidence in the global communication infrastructure amid the burgeoning challenges posed by the advent of quantum technologies.

C. Selection and evaluation of quantum-resistant algorithms

In navigating the quantum computing landscape, strategic selection and evaluation of algorithms resistant to quantum advancements are pivotal measures against potential security threats. The intricate realm of quantum-resistant algorithms demands a discerning exploration, embracing a rich tapestry of cryptographic methodologies to fortify against quantum incursions.

Diversify your consideration across various quantum-resistant algorithms, encompassing lattice-based cryptography, code-based cryptography, hash-based signatures, multivariate polynomial cryptography, and symmetric-key cryptography. Each approach boasts distinctive merits and vulnerabilities, presenting a mosaic of options to fortify against potential risks.

Delve into the security assumptions inherent in each Algorithm, unraveling the mathematical quandaries upon which they hinge. Scrutinize the viability of quantum assaults targeting these mathematical problems. A profound grasp of the foundational security principles is imperative to craft judicious choices.

Scrutinize the cryptographic robustness of chosen algorithms, factoring in elements like key size, computational intricacy, and resilience against diverse attacks. The aim is to secure algorithms that meet and exceed prevailing cryptographic benchmarks, establishing a robust defense.

Probe into the pragmatic performance metrics of quantum-resistant algorithms, examining computational efficiency, essential generation speed, and suitability for specific applications. Achieving an equilibrium between security and practicality becomes paramount for universal adoption.

Champion algorithms were harmonizing with ongoing standardization endeavors. Collaborate with initiatives and bodies ardently working towards erecting quantum-resistant cryptography standards, propelling such algorithms' widespread embrace.

Give precedence to algorithms weathered through meticulous peer-reviewed exploration and academic validation. Algorithms resilient under the scrutiny of the broader cryptographic community instill confidence in their security assertions.

Survey the feasibility of deploying selected algorithms across diverse systems and platforms. Gauge compatibility with existing infrastructure, assess integration ease and anticipate potential deployment challenges.

Evaluate the practicability of transitioning to quantum-resistant algorithms, encompassing strategies for migrating cryptographic systems (Ott & Peikert, 2019). Ensure a seamless transition, upholding security amidst the coexistence of classical and quantum-resistant algorithms.

Immerse in dialogue within the post-quantum cryptographic community, remaining abreast of the latest advancements, vulnerabilities, and recommendations. Active involvement in discussions and collaborations with domain experts becomes pivotal for informed decision-making.

The intricate task of electing and assessing quantum-resistant algorithms necessitates a holistic and sophisticated approach. Balancing theoretical security assurances with real-world applicability defines the trajectory of these algorithms amid the evolving quantum threat landscape.

IV. VIASAT Devices and FPGA Implementation

A. Introduction to VIASAT devices in sea communications

VIASAT emerges as a prominent force in satellite communication, offering groundbreaking solutions across various domains, notably in maritime communications. The company specializes in tailoring devices and systems to address the distinctive challenges inherent in the maritime communication landscape. Let's delve into VIASAT's notable contributions to sea communication.

VIASAT's Very Small Aperture Terminal (VSAT) systems are meticulously designed for maritime utilization, delivering steadfast broadband connectivity amidst the vastness of the open sea (Zhang et al., 2023). Employing diminutive yet stabilized antennas, these systems forge and sustain communication links with satellites, ensuring a continuous stream of high-quality data and voice connectivity.

To facilitate efficient data transmission across satellite networks, VIASAT provides maritime modems and terminals. These devices, equipped with sophisticated modulation and coding schemes, optimize bandwidth usage, guaranteeing steadfast communication in challenging maritime environments (VIASAT, 2023).

The maritime antennas crafted by VIASAT boast durability and stability, pivotal for maintaining consistent satellite communication aboard moving vessels. These stabilized antennas adeptly counteract the effects of vessel motion, assuring an unwavering and robust connection even in the turbulence of rough seas.

VIASAT's commitment to global coverage via its expansive satellite network empowers ships to stay seamlessly connected, irrespective of geographical location (VIASAT, 2023). This global outreach proves indispensable for maritime operations, facilitating effective communication both in the openness of the high seas and in coastal regions alike.

Security and reliability are paramount in VIASAT's communication solutions tailored for maritime applications. Robust encryption measures and other security features shield sensitive data transmitted over the satellite network (VIASAT, 2023).

B. FPGA technology and its suitability for small electronic devices

In the realm of miniaturized electronic gadgets, the Field-Programmable Gate Array (FPGA) technology emerges as a beacon of promise, boasting distinctive merits in terms of malleability, efficacy, and versatility. Unlike the conventional Application-Specific Integrated Circuits (ASICs), FPGAs represent programmable entities capable of post-manufacturing configuration and reconfiguration, rendering them exceptionally well-suited for various applications within miniature electronic devices (Dang et al., 2023).

The aptness of FPGA technology for petite electronic devices is rooted in its intrinsic pliancy. FPGAs afford the luxury of real-time reprogramming, empowering developers to institute alterations and enhancements sans the Necessity for hardware adjustments (Uran, 2021). This adaptability proves invaluable in the swiftly evolving landscape of compact electronic devices, wherein design prerequisites and functionalities may undergo metamorphosis over time.

Furthermore, FPGAs shine in circumstances where personalization and optimization bear paramount importance. In the realm of pint-sized electronic devices, where spatial constraints often demand a delicate equilibrium between performance and dimensions, FPGAs proffer the advantage of tailoring the hardware to the specific difficulties of applications (Dang et al., 2023). This capability to craft configurations tailored to particular applications augments overall efficacy and performance—an indispensable consideration for devices constrained by finite physical proportions.

FPGA technology's energy efficiency constitutes another pivotal element contributing to its appropriateness for petite electronic devices. FPGAs can undergo optimization for minimal power consumption, positioning them as idyllic candidates for battery-powered devices or those deployed in energy-conscious environments (Dang et al., 2023). This efficiency is realized through the capacity to selectively activate and deactivate specific components contingent upon the prevailing operational demands, thereby minimizing power usage without compromising functionality.

Moreover, FPGAs expedite the development cycle for miniature electronic devices. The programmable essence of these devices facilitates swift prototyping and testing, thereby expediting the design trajectory. This agility is advantageous in industries where the time-to-market factor assumes critical significance.

C. FPGA implementation for quantum-resistant algorithms

Here, one must consider several aspects: hardware architecture considerations and algorithm integration.

When looking into Hardware Architecture Considerations, there is a dire need to focus on quantum-resistant hardware design, the capability to parallel processing, efficient resource allocation optimization, and scalability (Policarpo, Nery, & Albuquerque, 2022). These requirements will help to develop a quantum-resistant FPGA unit capable of establishing an optimally secure connection.

Utilizing FPGA to implement the algorithm integration requires using numerous mathematical equations and calculations and translating them into hardware description languages. This would incur further customization of the FPGA with an additional benefit from parallelism. Parallel processing of the FPGA would substantially boost the further development of quantum cryptography and its application in maritime use.

Further optimization of the Algorithm would utilize a more efficient memory use (Policarpo, Nery, & Albuquerque, 2022). FPGA architecture has several memory types, namely the on-chip RAM and external interfaces. Memory management is a substantial part of the algorithm implementation process, as it will minimize access latency and increase the data throughput. The latter is of immense importance in the maritime industry.

Successful FPGA implementation for quantum-resistant algorithms requires carefully balancing hardware architecture considerations and algorithm integration/optimization. By addressing these aspects thoughtfully, one can develop efficient and secure solutions for small electronic devices resistant to quantum threats.

V. Protocol Offloading Strategies

A. Understanding the resource-intensive nature of post-quantum cryptography

In safeguarding data against the looming quantum threats, the domain of post-quantum cryptography grapples with intricacies owing to its resource-intensive character. Alleviating these intricacies demands a keen focus on protocol offloading strategies:

- **Cryptographically Tailored Hardware Augmentation:** Acknowledging the computational exigencies inherent in post-quantum algorithms, one stratagem involves channeling cryptographic functions to bespoke hardware accelerators. Specialized contrivances, such as cryptographic co-processors, wield the potential to substantially amplify the processing celerity and efficiency of algorithms resilient to quantum incursions.
- **Optimization via Parallel Processing Prowess:** Operations in post-quantum cryptography invariably entangle themselves in labyrinthine mathematical computations. Harnessing the parallel processing prowess embedded in contemporary processors or specialized hardware entities like GPUs facilitates the dispersion of computational burdens across manifold cores, elevating overall operational efficacy.
- **Discerning Offloading Tied to Threat Magnitudes:** The imperative for post-quantum safeguarding is not uniformly applicable to all data categories. Instituting a stratagem that discriminately transfers cryptographic processes contingent on data sensitivity optimizes the judicious use of resources. Data of lesser import might embrace more lightweight cryptographic algorithms, preserving the weightier post-quantum counterparts for information of a profoundly sensitive nature.
- **Adaptable Resource Apportionment Dynamics:** Responding to fluctuating computational requisites, dynamic resource apportionment strategies can intelligently allocate processing resources following real-time demand. This assures the optimal distribution of resources to cryptographic processes as the need arises, precluding undue stress on the system.

B. Challenges in Implementing Quantum-Resistant Algorithms on VIASAT Devices:

In the realm of satellite communication, VIASAT devices, despite their advanced capabilities, encounter specific quandaries when assimilating algorithms resilient to quantum intrusion:

- **Constrained Computational Potency:** VIASAT devices, often crafted with limitations in power and size, may exhibit restricted computational prowess. Executing resource-intensive post-quantum algorithms on such devices mandates meticulous consideration to guarantee efficient functionality sans compromising efficacy.
- **Imperatives for Real-Time Discourse:** VIASAT devices are pivotal in instantaneous communication, especially in nautical environments. Quantum-resistant algorithms, characterized by computational intricacy, may introduce latency. Striking a balance between the imperative for quantum resistance and the difficulties of real-time communication poses a problem, demanding meticulous algorithmic selection and optimization.
- **Limitations in Bandwidth:** Quantum-resistant algorithms might necessitate augmented key sizes and amplified data transmission, impacting bandwidth consumption. VIASAT devices, navigating within constricted bandwidth domains, must negotiate the delicate equilibrium between quantum resilience and the sustenance of effective communication links.
- **Upgradability and Harmonization**: VIASAT devices often boast prolonged operational life spans. Guaranteeing the harmonization and upgradability of quantum-resistant algorithms proves indispensable for acclimating to evolving cryptographic benchmarks. Approaches to implementation should encompass the seamless amalgamation of new algorithms sans necessitating extensive alterations to hardware.

Effectively addressing the resource-intensive aspects of post-quantum cryptography entails strategic offloading techniques, encompassing specialized hardware acceleration, optimization through parallel processing, selective offloading, and the reasonable allocation of dynamic resources. Simultaneously, instating quantum-resistant algorithms on VIASAT devices involves traversing hurdles linked to restricted computational potency, real-time communication prerequisites, bandwidth restrictions, and the imperative for enduring upgradability. Successful strategies revolve around the nuanced equilibrium between cryptographic robustness and pragmatic operational considerations.

VI. Adaptation Challenges and Solutions

A. Challenges

While exhibiting remarkable capabilities, VIASAT devices encounter occasional resource constraints, such as limited FPGA space and computational capacity. When integrating quantum-resistant cryptography onto FPGAs, meticulous optimization becomes imperative. The objective is to ensure the selected algorithms operate efficiently within these limitations without compromising overall performance.

The incorporation of quantum-resistant cryptographic algorithms into FPGAs introduces formidable challenges. These algorithms may impose significant computational demands, necessitating the surmounting of obstacles to translate intricate mathematical operations into efficient hardware designs. Striking a harmonious equilibrium between algorithmic intricacy and FPGA design restrictions becomes pivotal in attaining security and performance objectives.

Prioritizing power consumption is crucial for VIASAT devices designed with energy efficiency. Integrating quantum-resistant cryptography may introduce additional power requirements, demanding judicious management to prevent excessive energy consumption that could adversely affect device operation and battery life.

VIASAT devices play a pivotal role in real-time communication, particularly in dynamic environments such as maritime settings. Quantum-resistant cryptography, with its potential computational overhead, may introduce latency. Effectively addressing this challenge involves ensuring FPGA implementations of these algorithms meet the stringent requirements of real-time communication.

Maintaining security and adhering to certification standards are imperative when incorporating quantum-resistant cryptography (Deng, 2020). The trustworthiness of VIASAT devices hinges on FPGA implementations aligning with these standards, and navigating the intricate regulatory landscape may be requisite for certification.

VIASAT devices often boast extended operational lifetimes. The integration of FPGA-based quantum-resistant cryptography raises the challenge of ensuring cryptographic solutions' long-term viability and upgradability (Deng, 2020). Devices must be meticulously designed to accommodate future algorithmic enhancements without necessitating substantial hardware modifications.

The fusion of FPGA and quantum-resistant cryptography introduces challenges in testing and validation. Establishing rigorous testing protocols becomes necessary to verify the integrated solution's correct functionality, security, and resilience. This encompasses considerations for potential side-channel attacks and vulnerabilities specific to FPGA implementations (Deng, 2020).

Quantum-resistant algorithms may impact bandwidth usage due to larger key sizes and increased data transmission (Deng, 2020). VIASAT devices operate within constrained bandwidth environments, requiring astute management of the trade-off between quantum resistance and maintaining efficient communication links.

Designing and implementing FPGA solutions for quantum-resistant cryptography pose educational and skill challenges. Ensuring the development team possesses the requisite expertise. It remains up-to-date with evolving cryptographic standards, and FPGA technologies can be an enduring challenge.

B. Potential Solutions

In terms of potential solutions, there are three viable vectors of development. These are the modifications to hardware and software, adopting a cost-effective approach, and improving the overall performance.

1. Hardware and software modifications

In our relentless pursuit of eminence, we are dedicated to amplifying the hardware benchmarks of VIASAT devices. An indispensable facet involves assimilating avant-garde processing units meticulously crafted to elevate computational acumen. This encompasses the integration of CPUs endowed with superior efficacy and specialized processors such as FPGA units, custom-tailored for cryptographic paradigms resilient against quantum threats.

A pivotal stride forward encompasses amplifying memory capacity, spanning both RAM and storage realms. By broadening the memory horizons of our devices, we endow them with the prowess to adeptly handle extensive datasets and execute intricate applications with seamless fluidity. This proves imperative in meeting the computational exigencies imposed by sophisticated cryptographic algorithms, ensuring the sustainability of applications enriched with advanced functionalities.

Our allegiance to adaptability manifests in adopting a modular hardware architecture. This strategic approach facilitates effortless upgrades and modifications, offering a facile assimilation pathway for novel components or technologies. This strategic design minimizes the Necessity for extensive overhauls, guaranteeing the sustained adaptability of VIASAT devices to evolving imperatives.

Furthermore, we accord paramount importance to the perpetual refinement of our devices through periodic firmware and software updates. These updates transcend mere security patches, encompassing enhancements to algorithms, protocols, and the holistic performance of the system. By steadfastly committing to innovation and

ISSN: 2248-9622, Vol. 14, Issue 4, April, 2024, pp: 151-164

augmentation, our overarching goal is to furnish VIASAT users with an experience that is dependable and at the vanguard of technological sophistication.

2. Cost-effective approaches
In the meticulous construction of VIASAT solutions, the company prioritizes judicious decision-making from inception. In the preliminary conceptualization phase, the attention gravitates toward selecting constituents that achieve an exquisite equilibrium between efficacy and economic viability. This scrupulous assessment spans processors, memory units, and communication modules, ensuring that each constituent augments the gadget's capabilities without compromising fiscal sagacity.
Adopting an open-minded stance towards software development, open-source resolutions ought to be integrated to augment the functionalities of our contrivances. We incorporate enhancements without incurring substantial developmental expenditures by harnessing well-supported and community-forged software. This cost-efficient strategy optimizes resources and cultivates a collaborative and inventive milieu.
Cognizant of the ecological ramifications and attuned to operational expenditures, optimal energy governance in VIASAT devices ought to be enforced. This involves utilizing energy-conserving components and meticulously calibrating power management strategies, particularly critical for devices functioning in secluded or off-grid locales. Here, every determination associated with power consumption directly impacts the economic sustainability of operations.
In the dedication to enduring viability, VIASAT devices should focus on scalability as a paramount consideration. This forward-thinking methodology allows incremental refinements and diminishing initial outlays while ensuring adaptability to progressing technology or emergent requisites.

3. Performance improvements
In the unwavering commitment to achieving excellence, a premium on the constant refinement of VIASAT solutions through myriad strategic approaches is placed. A pivotal facet of this dedication involves the perpetual fine-tuning of software algorithms, explicitly focusing on cryptographic algorithms and communication protocols. This ongoing optimization is geared towards augmenting code efficiency, curtailing processing overhead, and integrating algorithmic enhancements to propel continuous performance improvements.
To elevate the overall efficacy of our systems, we leverage the parallel processing capabilities inherent in modern processors and dedicated accelerators. This judicious use of parallelization proves especially advantageous for tasks demanding substantial computational resources, such as cryptographic operations, significantly contributing to the efficiency and speed of our devices.
The optimization of real-time communication is of paramount importance, particularly in applications like maritime communication. We guarantee expeditious and reliable data transmission through the meticulous refinement of real-time communication protocols. This is indispensable for the operational triumph of VIASAT devices, where minimal latency emerges as a pivotal determinant.
In our unwavering pledge to deliver devices of exemplary performance, we institute a comprehensive system for continuous monitoring. This proactive methodology enables us to identify and address performance bottlenecks promptly. The regular optimization of both hardware and software constituents, informed by insights gleaned from ongoing monitoring, assures sustained enhancements in the capabilities of VIASAT devices.

VII. Implications

In examining the repercussions of this inquiry, substantial implications unfold for users of VIASAT devices, particularly those reliant on satellite communication spanning diverse sectors. Crucial considerations encompass the proficient execution and validation of quantum-resistant algorithms on FPGA-equipped VIASAT devices, furnishing users with an elevated level of security affirmation. This proves pivotal in scenarios where data confidentiality and integrity reign supreme, such as in military communications, maritime operations, and other applications marked by heightened sensitivity.

The beneficiaries of VIASAT devices stand to harvest rewards from the inherent adaptability of quantum-resistant algorithms, fortifying communication channels against potential quantum threats. The revelations instill confidence in the robustness of VIASAT devices, ensuring sustained operational efficacy in the face of advancements in quantum computing.

The insights gleaned from this research significantly contribute to the enduring viability of VIASAT devices, confronting the challenge of integrating quantum-resistant cryptography. Users can envisage a trajectory for forthcoming enhancements, guaranteeing the resilience and adaptability of their devices to evolving cryptographic standards, thereby safeguarding their investments.

Grasping the performance implications of integrating quantum-resistant algorithms on VIASAT devices aids users in making prudent decisions concerning the equilibrium between security and operational efficiency. This knowledge holds particular relevance for optimizing communication in resource-constrained environments, such as satellite networks.

The study unveils prospects for future exploration and development, charting a course for progress in secure satellite communication. Potential avenues for further investigation encompass building upon this research to contribute to the establishment of industry benchmarks for quantum-resistant algorithms in satellite communication. Collaborative endeavors among stakeholders could lead to the formulation universally accepted cryptographic protocols tailored for VIASAT devices.

Delving into the amalgamation of quantum-resistant algorithms with emerging technologies, such as artificial intelligence (AI) and edge computing, presents a stimulating avenue for research. Understanding the synergies between these technologies can pave the way for more intelligent and adaptive VIASAT communication systems.

Subsequent research could focus on the real-world implementation of VIASAT devices with quantum-resistant cryptography. Case studies spanning diverse operational landscapes would yield valuable insights into the practical implications, challenges, and advantages of incorporating these advanced security measures.

As quantum-resistant cryptography gains prevalence, future research could explore practical strategies for user enlightenment and training. Ensuring that end-users, operators, and decision-makers possess the knowledge to optimize the security benefits of VIASAT devices contributes to the system's overall resilience.

Ongoing research initiatives can zero in on refining the performance of quantum-resistant algorithms on FPGA-equipped VIASAT devices. This encompasses the continuous optimization of cryptographic protocols, exploration of innovative hardware architectures, and adaptation to advancements in FPGA technology.

The ramifications of this study transcend immediate advantages for VIASAT device users, exerting influence on the broader panorama of secure satellite communication. The future research directions delineated here aim to build upon the groundwork laid by a future study, nurturing innovation, standardization, and continual enhancement in the field.

VIII. Conclusion

Amidst the exploration of quantum-resistant algorithms on FPGA-equipped VIASAT devices, this study delves into the intricacies of integration and testing. The primary objective is to elevate satellite communication's security and performance benchmarks. A concise overview of the pivotal discoveries is outlined below:

The study underscored the practicality of incorporating quantum-resistant algorithms onto FPGA-equipped VIASAT devices. This showcased the devices' adaptability to sophisticated cryptographic solutions.

Upon integrating quantum-resistant cryptography, discernible effects on VIASAT device performance metrics were observed. Despite introducing computational overhead, the research identified strategies to alleviate this impact and sustain operational efficiency.

The potential of quantum-resistant algorithms to fortify the security posture of VIASAT devices was evident. The study accentuated the need to stay ahead of quantum threats, shedding light on the efficacy of these cryptographic measures.

Critical considerations underscore the imperative nature of quantum-resistant cryptography for VIASAT devices:

Given the imminent strides in quantum computing, integrating quantum-resistant cryptography becomes paramount for future-proofing VIASAT devices. This guards against potential vulnerabilities posed by quantum adversaries.

Quantum-resistant algorithms are pivotal in preserving the confidentiality and integrity of sensitive data transmitted via VIASAT devices. Adopting quantum-resistant cryptography is imperative as these devices form the bedrock of secure communication across sectors.

The study illuminated that embracing quantum-resistant cryptography contributes to VIASAT devices' long-term viability and upgradability. This adaptability ensures these devices evolve alongside emerging cryptographic standards without requiring extensive hardware alterations.

In essence, this research furnishes invaluable insights into secure satellite communication. Integrating quantum-resistant algorithms onto FPGA-equipped VIASAT devices is a viable solution to the dynamic landscape of cryptographic threats. The key takeaways encapsulate the essence of the study:

The study accentuated the delicate equilibrium between security and performance in implementing quantum-resistant cryptography on VIASAT devices. Attaining optimal results mandates meticulous consideration of algorithmic efficiency and hardware capabilities.

The study underscored the perpetual need for adaptation to quantum advances. VIASAT devices, integral components of satellite communication, must proactively incorporate cryptographic measures resilient against evolving quantum threats.

The findings underscore the Necessity for collaborative industry endeavors to standardize and advocate the adoption of quantum-resistant cryptography. Establishing industry-wide best practices ensures a unified approach to securing satellite communication systems.

User awareness and education stand as vital components of successful implementation. As quantum-resistant cryptography integrates into VIASAT devices, educating end-users and operators about the significance of these measures becomes crucial for maximizing efficacy.

In summary, the infusion of quantum-resistant cryptography into VIASAT devices signifies a proactive stride toward ensuring satellite communication's enduring security and viability. This study contributes foundational knowledge in this evolving field, paving the way for further advancements and collaborative efforts to fortify the resilience of VIASAT devices against quantum challenges.

References

[1]. Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network Security, 16(1), 11.

[2]. Balamurugan, C., Singh, K., Ganesan, G., & Rajarajan, M. (2021). Post-quantum and code-based cryptography—some prospective research directions. Cryptography, 5(4), 38.

[3]. Chiesa, A., Ma, F., Spooner, N., & Zhandry, M. (2022, February). Post-quantum succinct arguments: breaking the quantum rewinding barrier. In 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS) (pp. 49-58). IEEE.

[4]. Cichocki, R. (2023). State-Sponsored and Organized Crime Threats to Maritime Transportation Systems in the Context of the Attack on Ukraine. TransNav: International Journal on Marine Navigation & Safety of Sea Transportation, 17(3).

[5]. Curty, M., & Lo, H. K. (2019). Foiling covert channels and malicious classical post-processing units in quantum key distribution. npj Quantum Information, 5(1), 14.

[6]. Dang, H., Yang, H., Kong, D., & Zan, L. (2023, August). Review of FPGA-Based Digital-to-Time Converters. In 2023 IEEE 16th International Conference on Electronic Measurement & Instruments (ICEMI) (pp. 243-252). IEEE.

[7]. De Gaudenzi, R., Del Rio Herrero, O., Gallinaro, G., Cioni, S., & Arapoglou, P. D. (2018). Random access schemes for satellite networks, from VSAT to M2M: A survey. International Journal of Satellite Communications and Networking, 36(1), 66-107.

[8]. Deng, T. (2020, February). Mutual Connection in 5G Based Space Information Networks: Opportunities and Challenges. In Space Information Networks: 4th International Conference, SINC 2019, Wuzhen, China, September 19–20, 2019, Revised Selected Papers (Vol. 1169, p. 175). Springer Nature.

[9]. Djordjevic, I. B. (2020, July). Secure, global quantum communications networks. In 2020 22nd International Conference on Transparent Optical Networks (ICTON) (pp. 1-5). IEEE.

[10]. Huang, A., Barz, S., Andersson, E., & Makarov, V. (2018). Implementation vulnerabilities in general quantum cryptography. New Journal of Physics, 20(10), 103016.

[11]. Kannwischer, M. J., Schwabe, P., Stebila, D., & Wiggers, T. (2022, June). Improving software quality in cryptography standardization projects. In 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 19-30). IEEE.

[12]. Kuang, R., & Perepechaenko, M. (2023). Optimization of the multivariate polynomial public key for quantum safe digital signature. Scientific Reports, 13(1), 6363.

[13]. Lindsay, J. (2018). Why quantum computing will not destabilize international security: The political logic of cryptology. Available at SSRN 3205507.

[14]. Liu, R., Rozenman, G. G., Kundu, N. K., Chandra, D., & De, D. (2022). Towards the industrialisation of quantum key distribution in communication networks: A short survey. IET Quantum Communication, 3(3), 151-163.

[15]. Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.

[16]. Mitra, S., Jana, B., Bhattacharya, S., Pal, P., & Poray, J. (2017, November). Quantum cryptography: Overview, security issues and

future challenges. In 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix) (pp. 1-7). IEEE.
[17]. Mohsen, A. W., Bahaa-Eldin, A. M., & Sobh, M. A. (2017, December). Lattice-based cryptography. In 2017 12th International Conference on Computer Engineering and Systems (ICCES) (pp. 462-467). IEEE.
[18]. Ott, D., & Peikert, C. (2019). Identifying research challenges in post quantum cryptography migration and cryptographic agility. arXiv preprint arXiv:1909.07353.
[19]. Policarpo, R. C., Nery, A. S., & Albuquerque, R. D. O. (2022, November). Quantum-resistant Cryptography in FPGA. In 2022 Workshop on Communication Networks and Power Systems (WCNPS) (pp. 1-5). IEEE.
[20]. Seo, W. Y. (2018). Comparing RSA ECC and post quantum cryptography. J. Math. Anal. Appl, 10, 19-33.
[21]. Srivastava, V., Baksi, A., & Debnath, S. K. (2023). An Overview of Hash Based Signatures. Cryptology ePrint Archive.
[22]. Ugwuishiwu, C. H., Orji, U. E., Ugwu, C. I., & Asogwa, C. N. (2020). An overview of quantum cryptography and shor's algorithm. Int. J. Adv. Trends Comput. Sci. Eng, 9(5).
[23]. Uran, P. (2021). Design of an FPGA-based Data Acquisition System for a Shore-based Maritime Radar Network (Master's thesis, NTNU).
[24]. VIASAT. (2023). Maritime terminals – optimizing SATCOM connectivity at sea. VIASAT official website. https://www.viasat.com/products/terminals-and-radios/maritime-terminals/
[25]. Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), 025002.
[26]. Yang, Y. G., Bi, J. L., Li, D., Zhou, Y. H., & Shi, W. M. (2019). Hash function based on quantum walks. International Journal of Theoretical Physics, 58, 1861-1873.
[27]. Yang, Y., Jang, K., Baksi, A., & Seo, H. (2023). Optimized implementation and analysis of cham in quantum computing. Applied Sciences, 13(8), 5156.
[28]. Zhang, N., Feng, J., Zhang, P., & Gong, F. (2023). Parallel Doubly Fed Symbol Timing Recovery Algorithm and FPGA Implementation for Burst Broadband Satellite Access. IEEE Transactions on Very Large Scale Integration (VLSI) Systems.