IEEE SA
STANDARDS ASSOCIATION

INDUSTRY CONNECTIONS
WHITE PAPER

HYBRID QUANTUM-INSPIRED INTERNET PROTOCOL INDUSTRY CONNECTIONS GROUP

STABILIZING QUBITS WITH DYNAMIC FREQUENCIES, THE IMPLICATIONS ON POST-QUANTUM ENCRYPTION PROTOCOLS, AND A HYBRID QUANTUM INTERNET

Authored by

Ean Mikale
Chair, IEEE HQI IC Group

Sharon Waters
Member IEEE HQI IC Group

LaResha Swiney
Secretary, IEEE HQI IC Group

IEEE

ACKNOWLEDGMENTS

Special thanks are given to the following reviewers of this paper:

Shana Pepin

Purva Rajkotia

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

PDF: STDVA27313 979-8-8557-1224-7

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association ("IEEE SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require the use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patent claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the ICCom members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

STABILIZING QUBITS WITH DYNAMIC FREQUENCIES, THE IMPLICATIONS ON POST-QUANTUM ENCRYPTION PROTOCOLS, AND A HYBRID QUANTUM INTERNET

ABSTRACT

The reliability and stability of qubits are critical for the advancement of quantum computing and the development of secure quantum communication networks. This white paper explores the challenges associated with qubit stabilization and introduces dynamic frequency modulation as a novel solution to these challenges. The paper presents experimental findings that demonstrate how dynamic frequencies can enhance qubit coherence by mitigating decoherence and noise, providing a more robust mechanism than static frequency approaches.

Dynamic frequency modulation effectively stabilizes various qubit types, including superconducting and trapped ions, by continuously adjusting operational parameters to counteract environmental fluctuations. These advancements not only improve qubit performance but also have significant implications for post-quantum encryption protocols, which are designed to secure information against quantum attacks.

The paper discusses how stabilized qubits can impact encryption methods, such as quantum key distribution (QKD) and Quantum Elliptical Curve Cryptography (QECC), by enhancing computational integrity and error rates. However, the ability to stabilize qubits also introduces potential risks, as it may lead to vulnerabilities in quantum cryptographic systems if not adequately addressed.

Future research directions include optimizing frequency modulation algorithms and integrating machine learning for predictive adjustments, aiming to improve quantum system performance and security. The findings underscore the need for continued development in both quantum and classical cryptographic methods to safeguard against emerging threats.

Overall, this research highlights the transformative potential of dynamic frequency stabilization in quantum technology, emphasizing the need for proactive measures in cybersecurity and the integration of quantum technologies across various sectors.

1. INTRODUCTION AND BACKGROUND

1.1. INTRODUCTION

The purpose of a hybrid quantum-inspired Internet, or even a full quantum Internet, heavily relies on its prospect for security (ScienceDaily [1]).[1] As a result of this scientific assumption, world governments have begun to recommend and implement post-quantum encryption and algorithms based on quantum mechanics. Qubits, the fundamental units of quantum information, are highly sensitive to environmental disturbances, leading to decoherence and loss of quantum information. It is believed that the qubit is too fragile and will always collapse, ensuring the security of the information. However, our research, with wide implications across sectors and industries, shows that with dynamic frequencies, qubits can be stabilized and explored using reverse engineering and cyber-forensics techniques.

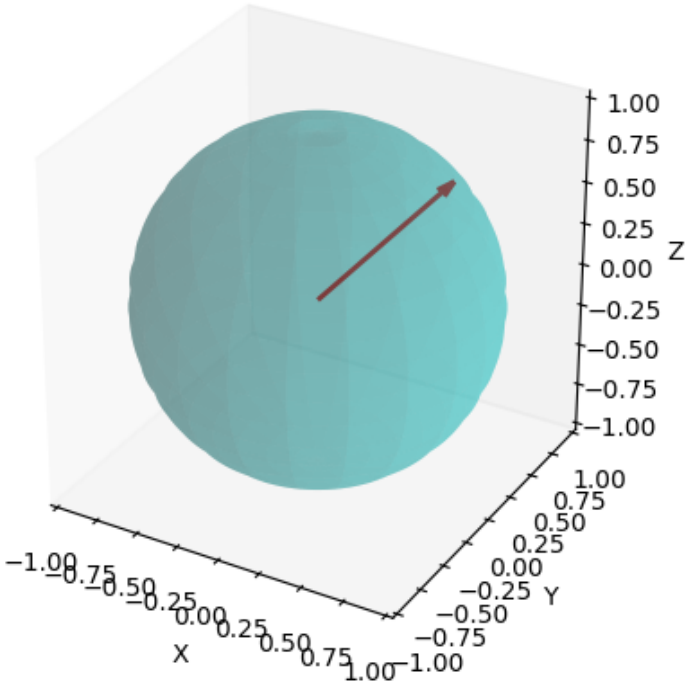
1.2. BACKGROUND

A qubit is the quantum equivalent of a classical computational bit. While a bit can exist in two states, 0 and 1, a qubit can exist in multiple states simultaneously, a property known as superposition. Similar to how bits are used for computation as an on/off switch, qubits, with their infinite possible simultaneous states, vastly increase the complexities and possibilities of quantum computation compared to classical computing. (See FIGURE 1.) Additionally, qubits can be entangled, providing powerful computational capabilities. However, these advantages are undermined by qubit instability. Decoherence, induced by interactions with the surrounding environment, disrupts the quantum state, leading to errors in computation. While a challenge for telecommunications, this instability can be a positive attribute for cybersecurity.

Several techniques have been developed to stabilize qubits, such as error correction codes, cryogenic cooling, and the use of specialized materials. Despite these advances, achieving long-term qubit stability remains a significant hurdle. This also poses a significant hurdle for bad actors seeking to bypass current encryption methods and techniques for cyber-ransoms. During the first phase of full quantum-internet adoption, mitigation must occur (Delft University [2]).

[1]Numbers in brackets correspond to the references in Section 4.

FIGURE 1 **A BLOCH PLOT OF A QUBIT SHOWING THE NEAR-INFINITE POSSIBILITIES USING A SPHERE FOR COMPUTATION, AS OPPOSED TO A 0 OR A 1**



2. DYNAMIC FREQUENCIES FOR QUBIT STABILIZATION

2.1. EXPERIMENTAL RESULTS

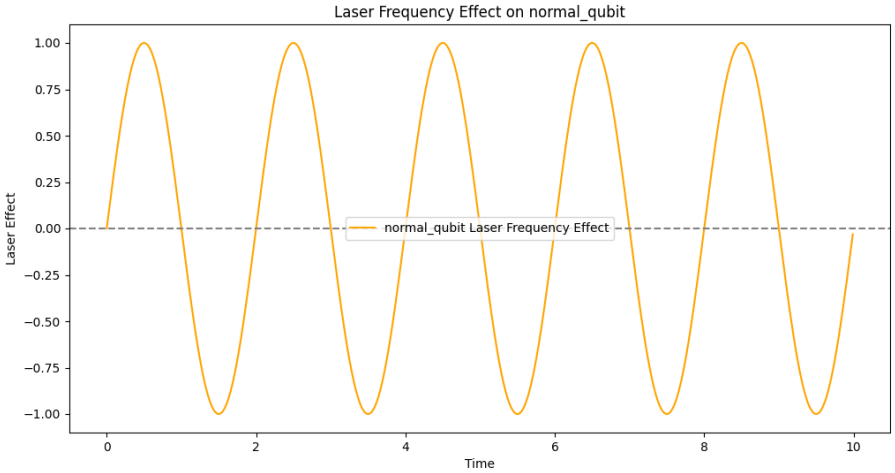
Our recent experiments have demonstrated that dynamic frequency modulation can effectively stabilize qubits without collapsing with wave function (DatacenterDynamcis [3]). By varying the frequency of qubit operations dynamically, researchers have been able to counteract the effects of environmental noise and decoherence. This approach was successfully simulated on eight different qubit types, showing significant improvements in qubit coherence times compared to static frequency operations. It has been proposed that quantum become fully integrated into 6G (Cisco [4]).

However, it is believed that quantum technologies may not be ready for deployment by the end of the decade, when 6G is expected to be deployed. Our work, conducted on classical systems, utilizes the real-world power of quantum-classical networks, leveraging the best of both quantum and classical systems to create a superior hybrid system. Such networks, capable of deployment on classical systems, show that commercial quantum

business cases and adversarial capabilities are closer to market entry and viability than previously imagined. Such technology can also enable and enhance the accuracy and security of next-generation 6G cellular/wireless communications, using the new math of quantum mechanics for encryption over classical computational encryption methods (Inside Quantum Technology [5]).

The experimental setup involved subjecting qubits to a series of controlled frequency variations while monitoring their quantum states. The results indicated that qubits maintained coherence for longer periods with reduced error rates. This dynamic approach provided a more robust stabilization mechanism that was adaptable to various types of qubits and operational conditions. (See FIGURE 2.)

FIGURE 2 SIMULATION RESULTS OF QUBIT STABILIZATION USING FREQUENCY MODULATION



2.2. MECHANISMS OF DYNAMIC FREQUENCIES

Dynamic frequencies work by continuously adjusting the operational parameters of qubits, thereby compensating for environmental fluctuations in real-time. This method leverages advanced frequency modulation techniques, such as phase-locked loops and adaptive resonance tuning, to maintain optimal states. Modulation is common in wireless (Neitzke [6]).

For instance, dynamic frequency adjustments in superconducting qubits help mitigate the impact of thermal noise and electromagnetic interference. This same technique has been shown to work both on superconducting qubits as well as with simulated qubits. Research shows promise for utilizing such methodologies on any qubit type. The adaptability of dynamic frequencies allows for real-time corrections, ensuring sustained qubit stability.

3. IMPLICATIONS ON POST-QUANTUM ENCRYPTION PROTOCOLS

3.1. IMPACT ON ENCRYPTION PROTOCOLS

Post-quantum encryption protocols are designed to be secure against quantum attacks, which leverage the computational power of quantum computers to break classical encryption schemes. Stabilized qubits pose a threat to these protocols by stabilizing the qubit so that it may be inspected for data, making all such cryptographic protocols that rely on quantum information collapse and become insecure. The more the systems scale in qubit-count, the larger the attack surface becomes.

Dynamic frequency stabilization improves the stabilization of quantum operations, resulting in lower error rates and increased computational integrity. However, this can also be used both ways to extract information from the initialized qubit or qubits in transit. This reliability of information security is crucial for protocols such as quantum key distribution (QKD), quantum random number generation (QRNG), Quantum Elliptical Curve Cryptography (QECC), and other cryptographic applications, and require government, industry, academia, and civil society to put resources towards the creation of hardened and dynamic post-quantum cryptographic protocols (IEEE [7]).

3.2. INDUSTRIES MOST IMPACTED

While many industries are touched by the implications of our research, specific industries that are more vulnerable than others also exist. Currently, medical institutions, banking institutions, and infrastructure industries are most at risk, with the capability to extract data dynamically from qubits. The industry needs to expend resources to address this large potential gap in the cyber-security defense enterprise.

3.3. FUTURE DIRECTIONS

The adoption of dynamic frequency stabilization in quantum computing opens new avenues for research and development. Future advancements may focus on optimizing frequency modulation algorithms, integrating machine learning for predictive adjustments, and scaling these techniques for larger quantum systems. Additional research must be done concerning the implications of dynamic frequency modulation, as well as classical encryption and computational methods. Questions still remain as to whether full-quantum encryption

is unsafe compared to classical methods due to frequency modulation (Anwar [8]).

Before organizations can incorporate quantum technology across all aspects of human society and industry, it needs to be safe. There must be a workforce of cybersecurity and quantum computing professionals and engineers who understand the true strengths and weaknesses of quantum and quantum-inspired technologies to provide proactive mitigation strategies.

Long-term, the implications for cybersecurity are profound. Stable qubits can lead to m more secure communication channels, enhanced data protection, and resilient encryption standards (Daimmeier [9].)

4. REFERENCES

The following sources have either been referenced within this paper or may be useful for additional reading:

[1] ScienceDaily. (2024). New advancements in quantum computing stabilize qubits. Retrieved from https://www.sciencedaily.com/releases/2024/05/240515122712.htm

[2] Delft University of Technology. (Retrieved 2024). The six stages of quantum networks. Retrieved from https://tu-delft.foleon.com/tu-delft/quantum-internet/the-six-stages-of-quantum-networks/

[3] DatacenterDynamics. (2022). Why do we need a quantum internet? Retrieved from https://www.datacenterdynamics.com/en/analysis/why-do-we-need-a-quantum-internet/

[4] Cisco. (2022). Making a quantum-ready internet. Retrieved from https://outshift.cisco.com/blog/making-a-quantum-ready-internet

[5] Inside Quantum Technology. (2024). Quantum technology as key enabler for 6G wireless communication? Retrieved from https://www.insidequantumtechnology.com/news-archive/quantum-particulars-guest-column-quantum-technology-as-key-enabler-for-6g-wireless-communication/

[6] Neitzke, A. (2023). Quantum computing and post-quantum cryptography. arXiv. https://arxiv.org/abs/2301.02609

[7] IEEE. (2016). Quantum Internet: A vision for the road ahead. https://ieeexplore.ieee.org/document/7849014

[8] Anwar, H. (2022). Quantum cryptography: A path to secure communication. arXiv. https://arxiv.org/abs/2205.09476

[9] Daimmeier, L. (2022). Dynamic frequency modulation for quantum communication. arXiv. https://arxiv.org/abs/2208.05020

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571