Quantegrity

A Quantum-Enhanced E-Voting System as a Premier Quantum Internet Application

Viduranga Shenal Landers
Dinithi Sulakshani Kaushani Karunadasa
[1] University of Colombo School of Computing, Colombo, Sri Lanka
vidurangalanders@gmail.com
dinithichandani2002@gmail.com

Abstract
As electronic voting systems become integral to modern democratic processes, their security and integrity are of paramount importance. The Quantegrity system represents a groundbreaking advancement in e-voting technology by leveraging quantum internet capabilities to provide unprecedented security and verifiability. This report examines how Quantegrity establishes itself as a premier quantum internet application through its innovative integration of quantum cryptographic principles with practical voting requirements.

1 Introduction

As electronic voting systems become integral to modern democratic processes, their security and integrity face unprecedented challenges in the quantum era. Traditional e-voting systems, relying on classical cryptographic techniques, are becoming increasingly vulnerable to advancing computational capabilities and cyber threats. The Quantegrity system addresses these challenges by creating a quantum-based e-voting system that leverages quantum internet capabilities. The system represents a groundbreaking advancement in quantum internet applications by demonstrating how quantum principles can enhance critical infrastructure while maintaining practical usability. By implementing quantum key distribution (QKD) and quantum oracles in a real-world voting system, Quantegrity establishes itself as a premier example of quantum internet technology application. This report examines how Quantegrity innovatively integrates quantum cryptographic principles with practical voting requirements to create a system that is resilient to both classical and quantum threats while remaining accessible to voters.

2 Key Technologies in Quantegrity System

2.1 Quantum Key Distribution (QKD)

At the heart of Quantegrity lies the implementation of Quantum Key Distribution, an unconditionally secure method for distributing encryption keys. The system employs the BB84 protocol, which operates by transmitting quantum states between parties. The process begins with the sender (Alice) transmitting quantum states to the receiver (Bob) using randomly chosen bases. The security is guaranteed by fundamental quantum mechanical principles, particularly the no-cloning theorem and the uncertainty principle.

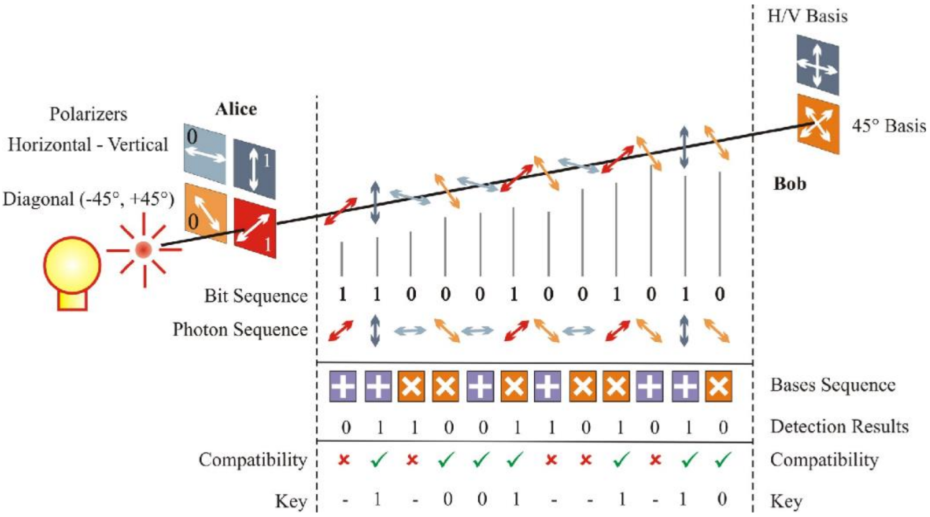


Fig. 1. BB84 protocol (adapted from (Legré, 2009))

The BB84 protocol implementation in Quantegrity works through several precise steps:

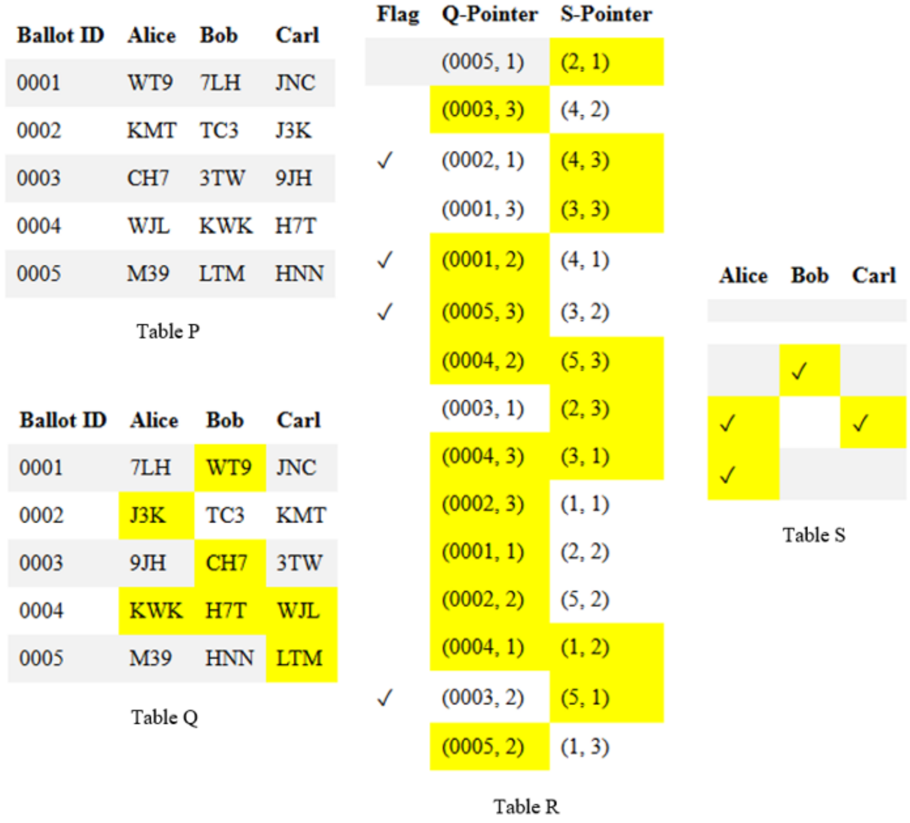
1. The sender prepares quantum states using random bases (rectilinear or diagonal)
2. The receiver measures these states using independently chosen random bases
3. Both parties publicly compare their basis choices
4. They retain only the results where they used matching bases
5. The remaining bits form the secure key after error correction and privacy amplification

2.2 Quantum Oracles

A quantum oracle is a black box operation that performs specific computational tasks on quantum states. In Quantegrity's implementation, these oracles serve as fundamental components for quantum cryptographic operations. The system leverages quantum oracles particularly for secure multi-party computation protocols. In blind quantum computation, a voter can delegate computations to a server without revealing input data or computation results. This is achieved by preparing an encrypted quantum state using QKD, sending it to the server for computation using a quantum oracle, and then decrypting the result using the QKD key. Additionally, quantum oracles enable the implementation of quantum digital signatures and fingerprinting protocols, providing secure authentication and verification of quantum states - essential features for a secure voting system.

2.3 Scantegrity Voting System

The Scantegrity voting system serves as the foundational framework that Quantegrity enhances with quantum capabilities. The system employs optical scan paper ballots with invisible ink confirmation codes, which are crucial for verification. The confirmation codes are generated randomly and independently for each candidate on each ballot, with a unique ballot ID number for tracking. The mixnet process, which is essential for vote privacy and verification, operates through four interconnected tables (P, Q, R, and S). Table P contains the initial confirmation codes, while Table Q is derived through pseudorandom shuffling. Table R manages the voting process with three columns: a flag indicating vote status, a Q-pointer linking to table Q, and an S-pointer connecting to table S. The final table, S, contains only flags and serves as the mechanism for vote tallying.



Ballot ID	Alice	Bob	Carl
0001	WT9	7LH	JNC
0002	KMT	TC3	J3K
0003	CH7	3TW	9JH
0004	WJL	KWK	H7T
0005	M39	LTM	HNN

Table P

Ballot ID	Alice	Bob	Carl
0001	7LH	WT9	JNC
0002	J3K	TC3	KMT
0003	9JH	CH7	3TW
0004	KWK	H7T	WJL
0005	M39	HNN	LTM

Table Q

Flag	Q-Pointer	S-Pointer
	(0005, 1)	(2, 1)
	(0003, 3)	(4, 2)
✓	(0002, 1)	(4, 3)
	(0001, 3)	(3, 3)
✓	(0001, 2)	(4, 1)
✓	(0005, 3)	(3, 2)
	(0004, 2)	(5, 3)
	(0003, 1)	(2, 3)
	(0004, 3)	(3, 1)
	(0002, 3)	(1, 1)
	(0001, 1)	(2, 2)
	(0002, 2)	(5, 2)
	(0004, 1)	(1, 2)
✓	(0003, 2)	(5, 1)
	(0005, 2)	(1, 3)

Table R

Alice	Bob	Carl
	✓	
✓		✓
✓		

Table S

Fig. 2. Table P, Q, R, and S with revealed votes highlighted

2.4 Symmetrically Entangled Deutsch-Jozsa Quantum Oracle (SEDJO)

The Symmetrically Entangled Deutsch-Jozsa Quantum Oracle (SEDJO) protocol represents a significant advancement in quantum key distribution. The protocol begins with entanglement distribution, where a Bell pair is created using Hadamard and CNOT gates. These entangled qubits are distributed between the voter and election authority. In the key encoding phase, both parties choose random n-bit key strings (sA and sB) and encode them into their qubits using quantum oracles, applying phase shifts based on key bits. The measurement phase involves both parties measuring their qubits in the computational basis, obtaining classical bit strings mA and mB. Finally, in the key derivation phase, one party communicates their initial key via a classical channel, allowing computation of a shared secret key through XOR operations (K = sA ⨁ sB ⨁ mB = mA).

The protocol can be implemented using a quantum circuit, as shown in Figure 4, where 4 entangled qubit pairs are shared between Alice and Bob. In this example implementation, Alice has chosen sA to be "1001" and Bob has chosen sB to be "1100".

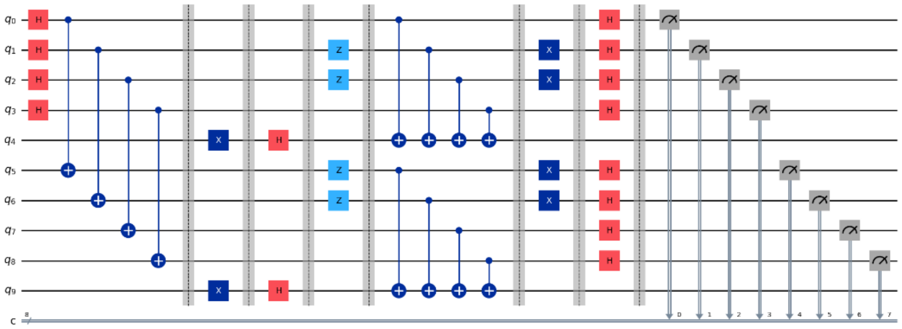


Fig. 3. Example SEDJO with ($s_A = 1001$ and $s_B = 1100$)

This circuit implementation results in the measurement shown in Figure 5. The experiment, conducted on the qasm_simulator provided by the Qiskit library, demonstrates the distribution of possible outcomes for both key pairs concatenated as (sA + sB). While current quantum computer limitations result in some noise and uneven distribution, this does not affect the protocol's security as key generation in QKD does not require perfect distribution.

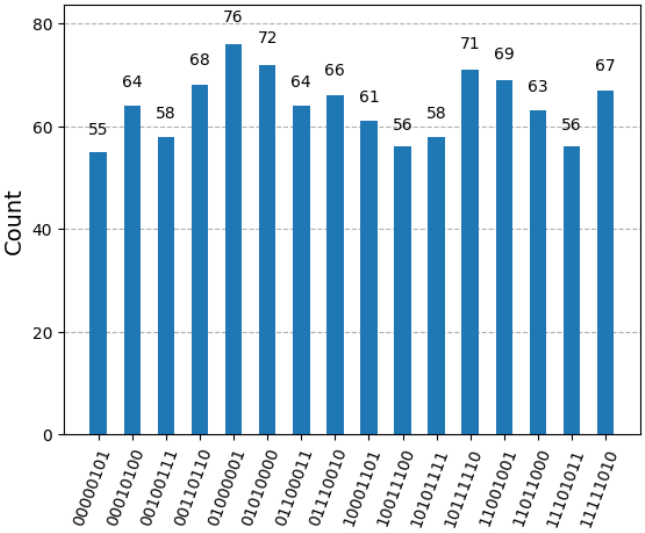


Fig. 4. Measurement histogram of sample SEDJO with 1024 shots

This implementation provides unique advantages in key validation and security through quantum entanglement properties. For an initial key of length n, the protocol provides 2n unique key combinations, allowing for built-in validation mechanisms that enhance the system's security and reliability.

3 Quantegrity E-Voting System

The Quantegrity e-voting system is a hybrid quantum-classical system that combines the Scantegrity voting system with the SEDJO protocol for quantum key distribution. The main components of the Quantegrity system are derived from the Scantegrity system, with the addition of quantum components for enhanced security and verifiability.

The proposed quantum-enhanced e-voting system consists of four main components. A voter system that handles the voter login, verification and voting process. An Election Authority system that oversees the voting process and voter registration. A voting server that runs the Scantegrity voting system A QKD service that is responsible for generating and distributing secure cryptographic keys between the voter and the EA server.

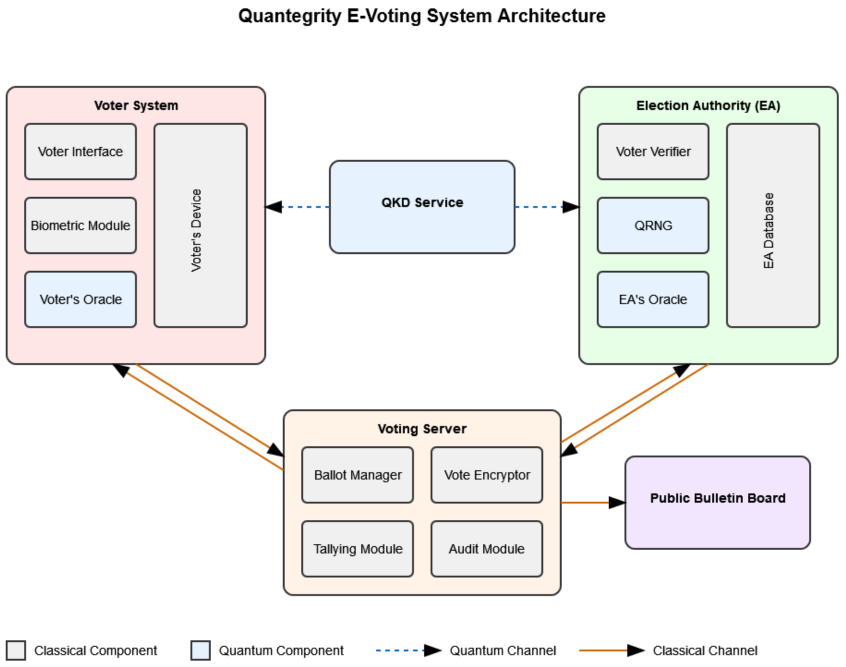


Fig. 5. Quantegrity E-voting system

3.1 Key components and their interactions

3.1.1. Quantum Key Distribution (QKD) module

The QKD module or the SEDJO protocol is responsible for generating and distributing secure cryptographic keys between the voter and the Election Authority (EA) server. Furthermore, the same SEDJO protocol is use to transfer some information that are crucial to verify the voter identity or to safely transmit the ballots. As most of today's QKD systems are specific to a single protocol, it is assumed that the idea of initiating the QKD process includes the distribution of entangled qubit pairs, initial setup of input and output qubits, as well as final setup of output qubits after the secret key inputs. Measurement of new keys and derivation of the quantum keys are regarded as separate processes.

Here is a summary of the steps of distributing a key or transferring information:

- Alice (voter) and Bob (EA official) initiates a QKD process using the QKD service module and receives entangled qubit pairs that are initialized for oracle inputs.
- Alice and Bob both input their secret keys to their oracles respectively.
- Both measure their qubits in the oracle.

- One of Alice or Bob may use a classical communication channel to provide some crucial information for the other to derive the key or decrypt information.

3.1.2. Biometric authentication module

. The biometric authentication module is responsible for verifying the identity of the voters using their biometric data. During the registration phase, voters enroll their biometric data (e.g., fingerprints) at the designated registration centers or if secure enough, using an online platform. The biometric templates are used to encrypt a QKD-generated key which will be stored in the voter ID card and the central database.

During the voting phase, voters authenticate themselves by providing their biometric data using their mobile phones or personal computers. The biometric authentication module extracts biometric data from the voter and uses it to decrypt the quantum key in the voter ID card.

3.1.3. Quantum Random Number Generator (QRNG) module

The QRNG module generates true random numbers using the inherent randomness of quantum systems. QRNGs are used for various purposes in the e-voting system, such as generating unique voter IDs, generating confirmation codes in ballots, and shuffling the ballot order.

A QRNG can be simply obtained by executing a simple quantum circuit consisting of a qubit in equal superposition, which can be obtained by using a Hadamard gate. Continuous measurement of this circuit will generate a real random number of a required length (n). The same can be achieved by creating a quantum circuit of n qubits, applying Hadamard gates to all the qubits to create an equal superposition, and measuring all the qubits at once.

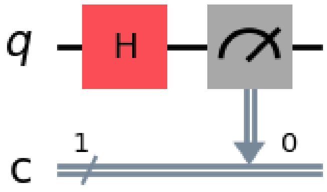


Fig. 6. QRNG Circuit

3.2 Voter registration and authentication process

The voting process begins with the voter registration and authentication phase. Alice (voter) goes to a registration center where she presents her National ID and biometric data (e.g., fingerprints) to Bob (EA official). Bob uses this information to verify Alice's identity. He then scans Alice's biometric signatures (BS_K) and generates two quantum random numbers (Q_K1 and Q_K2) using a QRNG. Bob encrypts Q_K1 using BS_K and stores it on her Voter ID card, along with a newly created Voter ID number (V_ID). Finally, Bob securely stores these values (BS_K, Q_K1, Q_K2, and V_ID) in an encrypted database on the EA server, and Alice receives her Voter ID card and device registration password (QK_2).

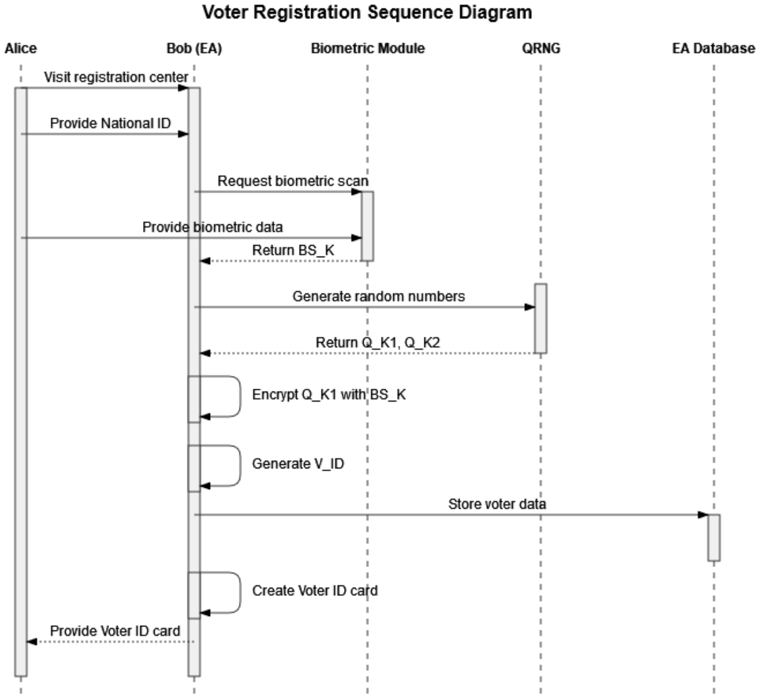


Fig. 7. Voter Registration

To complete the registration process, Alice goes home and logs in to the online voting platform using her Voter ID number (V_ID) and biometric signature (BS_K). She then initiates device verification, prompting Bob to send her a one-time-password (OTP) encrypted with her quantum random number (Q_K2) through a classical channel. Alice decrypts the OTP using Q_K2 and successfully validates her device on the platform.

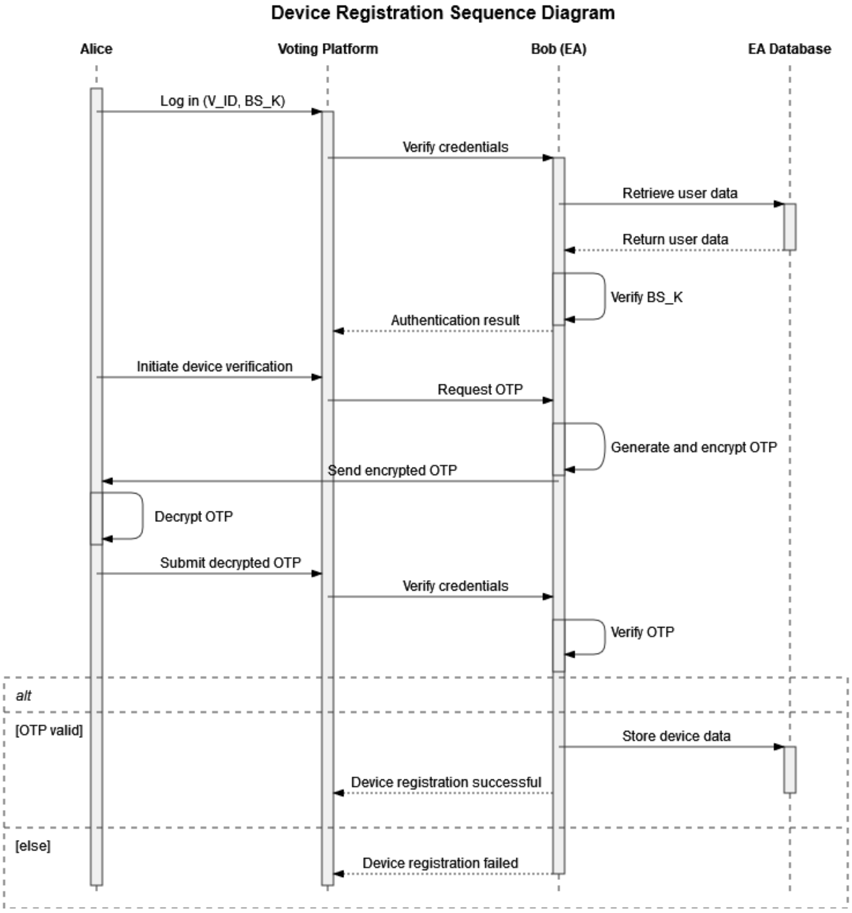


Fig. 8. Device Registration

On election day, Alice logs in to the online voting platform using her Voter ID number (V_ID) and biometric signature (BS_K). Bob verifies her eligibility to vote and initiates a QKD process, inputting Alice's stored quantum random number (Q_K1) into his oracle. Alice then uses her device's biometric module to read her biometric signature (BS_K) again and decrypt the encrypted Q_K1 stored on her Voter ID card. She inputs this decrypted key into her own oracle, and both Alice and Bob measure their newly generated keys. If Alice successfully decrypted the key, they will both possess the same new key (AQ_K1). Bob then sends Alice a one-time password (OTP) encrypted with AQ_K1, which she decrypts using AQ_K1 to validate her identity on the platform and proceed to vote.

This process ensures that the voter has used her biometric signature and her voter ID card on a registered device, which is highly unlikely to be possessed at once by any malicious actor. Since elections are more vulnerable to mass attacks to manipulate the end results, it is even more unlikely for an attacker to gain access to so many biosignatures, voter ID cards and access to their registered devices.

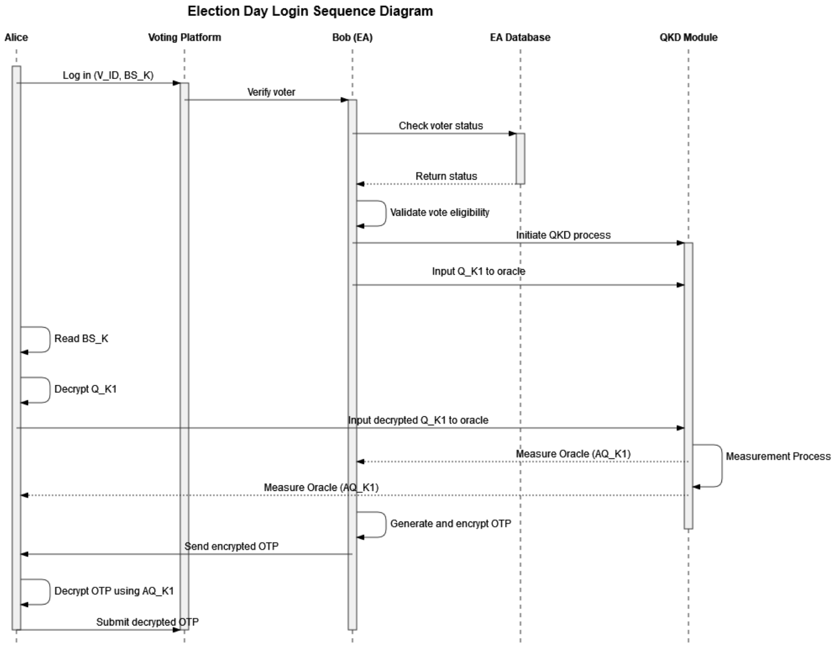


Fig. 9. Election Day Login

3.3 Secure vote casting and transmission

Once a voter has been authenticated using their biometric data, voter ID, and OTP, they proceed to cast their vote on the online platform. Before an election begins, Bob creates all the necessary ballots, confirmation codes, and mixnet tables to conduct the election. This can be regarded as a pre-election process.

Ballot creation and tabulation will be done as the same as in the Scantegrity system. In the Remotegrity system, a voter is given two Ballots with an Authorization ID which contains multiple authorization codes for voting and identity authorization. However, in the Quantegrity system, due to the ability to securely communicate information, it was regarded as unnecessary to add such verifications and random Ballot assignments.

In the Quantegrity system, one can decide to spoil a ballot as the same as in the paper based Scantegrity system and the pre-election procedures do not create a few ballots specific to a voter. Ballots are allocated to voter based on demand and are taken from a pool pre-configured ballot.

With her identity verified, Alice is ready to cast her vote. Bob initiates another Quantum Key Distribution (QKD) process, inputting the previously established key (AQ_K1) into his oracle. Alice does the same, and they both measure a new key

(VQ_K1). For enhanced security, Bob doesn't store this key or link it to Alice, potentially redirecting her to a separate, secure voting server.

He then encrypts a Ballot ID (B_ID) using VQ_K1 and sends it to Alice. After decrypting the B_ID, Alice chooses to either vote or spoil her ballot. If she chooses to spoil it, she receives all the confirmation codes associated with that ballot. If she chooses to vote, she is presented with the election questions and selects her answers. Alice encrypts her chosen answer with VQ_K1 and sends it to Bob, who then sends back a confirmation code (C_C) encrypted with VQ_K1. Alice decrypts this code (C_C) and stores it for future verification.

Rest of the election will be similar to the Scantegrity system. The purpose of this explanation is to highlight how the Scantegrity system could be enhanced with QKD to make it a viable solution for internet voting.

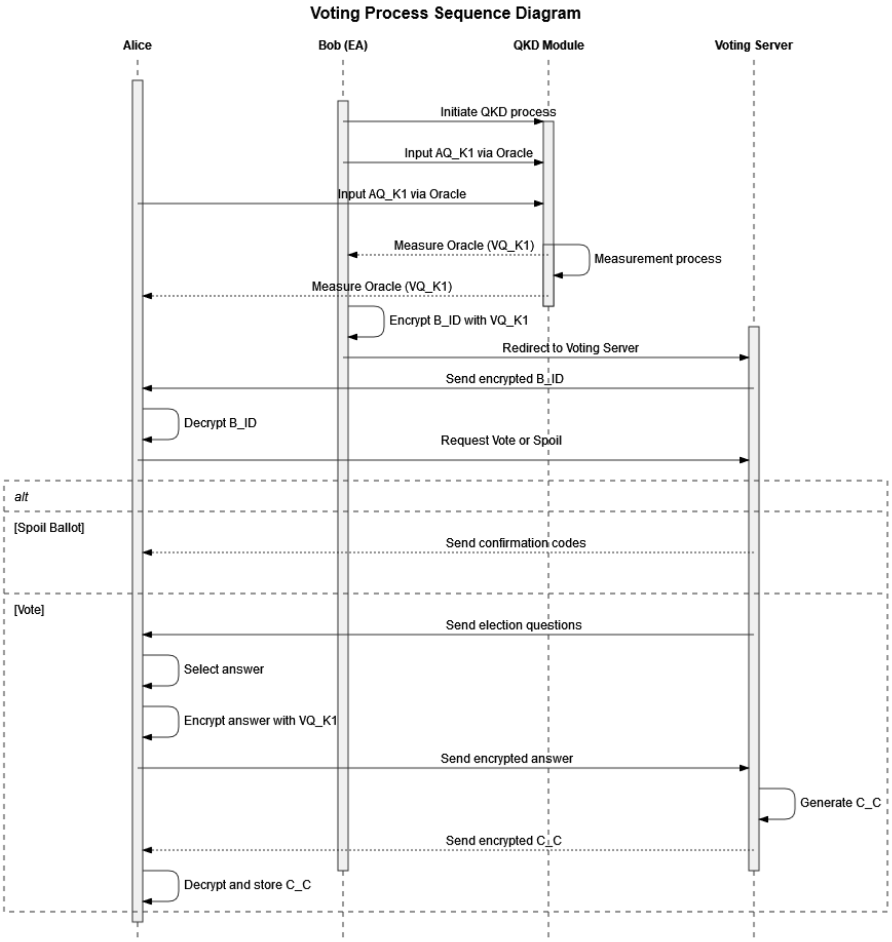


Fig. 10. Voting Process

3.3.1. Transmission over quantum or QKD-secured classical channels

The encrypted votes can be transmitted from personal computer to the central tabulation server using either a quantum channel or a classical channel secured by QKD.

If a quantum channel is available, the encrypted votes can be directly transmitted using quantum states, leveraging the inherent security of quantum communication.

Alternatively, if a quantum channel is not feasible, the encrypted votes can be transmitted over a classical channel that has been secured using QKD. In this case, the QKD-generated keys are used to encrypt the votes before transmission, and the classical channel is used for the actual data transfer.

3.3.2. Use of QRNGs for randomization and unpredictability

. Quantum Random Number Generators (QRNGs) are used throughout the voting process to ensure the randomness and unpredictability of various critical operations. QRNGs generate true random numbers by exploiting the inherent randomness of quantum systems

In the proposed e-voting system, QRNGs are used for generating unique voter IDs for each voter, generating ballot confirmation codes, generating seeds for randomized shuffling of ballot order, and generating random keys and OTPs. The use of QRNGs adds an additional layer of security and trust to the e-voting system by ensuring that critical operations are truly random and unpredictable.

3.4 Summary

In summary, the Quantegrity system leverages the key ideas and components of the Scantegrity system, including ballots with hidden confirmation codes, a public bulletin board for verifiability, and a mixnet-based tallying process. However, the Quantegrity system also incorporates quantum cryptographic primitives, such as the SEDJO protocol for quantum key distribution and quantum authentication, to provide enhanced security and verifiability guarantees.

The use of the SEDJO protocol in particular allows the Quantegrity system to generate and distribute encryption keys in a secure and verifiable manner, without relying on classical cryptographic assumptions. The protocol also enables secure communication between the various components of the system, preventing any attempt by an adversary to tamper with the election data.

Overall, the Quantegrity system represents a promising approach to integrating quantum cryptography into the design of e-voting systems, providing a strong foundation for secure, verifiable, and trustworthy elections in the post-quantum era.

4 Security Analysis and Proofs

The security analysis of Quantegrity demonstrates its effectiveness as a practical quantum internet application, showing how quantum principles can enhance real-world systems.

4.1 Threat model and attack scenarios

Quantegrity's security model addresses both external and internal threats through its quantum-enhanced architecture.

4.1.1. External attacks Prevention

The system's quantum features provide comprehensive protection against external threats through multiple security mechanisms. Through QKD protocols, the system can immediately detect any attempts to intercept communications, effectively preventing eavesdropping. The implementation of quantum states ensures vote integrity during transmission, making any tampering attempts evident. System availability is maintained through the hybrid classical-quantum channels, which provide resilience against denial-of-service attacks. The quantum authentication system prevents impersonation attempts by making man-in-the-middle attacks infeasible within the quantum framework.

4.1.2. Internal threat mitigation

The quantum components of Quantegrity create robust protections against internal threats through several innovative mechanisms. The quantum key generation system prevents unauthorized key sharing, effectively blocking potential collusion attempts. Through the implementation of quantum states, any vote modification becomes immediately detectable, ensuring the integrity of the voting process. The system's quantum authentication mechanisms ensure that only authorized personnel can access critical components, providing strong access control.

4.2 Security advantages of quantum integration

The security benefits of Quantegrity arise from the integration of three key quantum technologies. At its foundation, the SEDJO Protocol Implementation provides unconditionally secure key distribution. This is complemented by Quantum Oracle Operations, which enable secure multi-party computation essential for vote processing. The system's security is further enhanced by Quantum Random Number Generation, which ensures true randomness for critical operations. Together, these quantum features make Quantegrity particularly well-suited as a quantum internet application by comprehensively addressing the fundamental security challenges in e-voting.

5 Implementation and Practical Considerations

5.1 Technology integration

Quantegrity showcases practical quantum internet application development through its comprehensive integration approach. The system successfully combines quantum and classical components in a hybrid architecture that maximizes the benefits of both technologies. This design supports the gradual deployment of quantum features, allowing for scalable implementation as quantum technology develops. The interface design maintains user-friendliness while incorporating advanced quantum systems, ensuring accessibility for all users.

5.2 Integration with existing infrastructure

The system achieves seamless integration with current voting systems through careful architectural design. Building on the established Scantegrity system, Quantegrity enhances existing functionality while maintaining compatibility. The quantum security layer integrates smoothly with traditional voting processes, providing enhanced protection without disrupting existing operations. This flexibility allows the system to adapt to various voting environments and requirements.

5.3 User experience and accessibility

In the realm of user experience, Quantegrity successfully balances advanced security with practical usability. The interface remains intuitive despite the sophisticated quantum backend, ensuring that voters can easily navigate the voting process. The system's universal access design accommodates various voting devices and locations, making it accessible to all voters. The verification system provides straightforward quantum-secured verification methods that allow voters to confirm their votes while maintaining the highest security standards.

6 Quantegrity as a premier quantum internet application

6.1 Fundamental Advantages

Quantegrity's exceptional suitability as a quantum internet application is demonstrated through its comprehensive integration of quantum features. The direct quantum integration leverages fundamental quantum properties through the SEDJO protocol to provide unconditional security that's impossible in classical systems. The system utilizes quantum randomness generators to ensure completely unbiased election processes, eliminating any possibility of predictability or manipulation. Vote transmission security is guaranteed through quantum states that make tampering immediately detectable, ensuring complete vote integrity throughout the process.

The practical implementation aspects further strengthen Quantegrity's position as a premier application. The hybrid architecture successfully combines quantum security features with classical efficiency, optimizing system performance while maintaining security. The design fully supports real-world election requirements through scalable architecture that can handle varying election sizes and requirements. Through its modular structure, the system enables incremental enhancement of quantum features, allowing organizations to gradually upgrade their security capabilities as quantum technology advances.

6.2 Technical Innovation and Impact

6.2.1. Quantum Protocol Advancement

The system advances quantum internet capabilities through significant protocol innovations. The enhanced QKD implementation improves key distribution efficiency while maintaining security through the SEDJO protocol. Integration of quantum oracles with the system enables secure multi-party computation that protects vote privacy while allowing necessary processing. The biometric-quantum authentication system provides unforgeable voter verification by combining quantum states with biological identifiers.

The network optimization achieves efficient quantum resource utilization through careful management of quantum states and channels. The system maintains balanced usage of quantum and classical channels, ensuring optimal performance while preserving security. The quantum state distribution architecture scales effectively across different network sizes and configurations, supporting widespread deployment.

6.2.2. Real-World Applications

In critical infrastructure, Quantegrity demonstrates practical quantum advantages through multiple security enhancements. The system provides information-theoretic security for vote transmission, ensuring that intercepted data remains protected even against future quantum computer attacks. The quantum-secured voter authentication system prevents identity fraud while maintaining voter privacy. The implementation creates tamper-evident election records that can be verified without compromising vote secrecy.

The usability aspects of the system maintain accessibility while leveraging quantum features. Security features remain transparent to users while providing full protection, and the verification mechanisms allow voters to confirm their votes' integrity through straightforward processes.

6.3 Model for future applications

Quantegrity serves as a comprehensive template for future quantum internet applications through its architectural innovations. The system demonstrates effective quantum-classical integration that optimizes both technologies' strengths while minimizing their limitations. The quantum protocol implementation scales efficiently across different deployment sizes, and the distributed processing architecture maintains security across multiple voting locations.

The implementation strategy provides valuable insights for future quantum applications. The resource management system efficiently allocates quantum resources while maintaining system performance. User interaction remains straightforward despite the sophisticated quantum backend, and the security protocols deploy robustly across various environmental conditions. This comprehensive approach establishes Quantegrity as a model for developing practical quantum internet applications that balance advanced security features with real-world usability requirements.

7 Conclusion and Future Impact

7.1 Significance as a Quantum Internet Application

Quantegrity has established itself as a premier quantum internet application through its innovative integration of quantum cryptographic principles with practical voting requirements. The system demonstrates significant security innovations by implementing quantum cryptography in a real-world context, providing unconditional security for critical operations while maintaining verifiable processes. This achievement is particularly noteworthy as it bridges the gap between theoretical quantum advantages and practical implementation requirements.

The system's implementation excellence is evident in its successful integration of quantum and classical components, proving that quantum protocols can be effectively scaled while maintaining user accessibility. By achieving this balance, Quantegrity demonstrates that quantum technologies can enhance critical infrastructure without compromising usability or introducing operational complexity. The system's architecture serves as a model for future quantum applications, showing how quantum resources can be optimally utilized within existing infrastructure.

In terms of technology advancement, Quantegrity makes significant contributions to quantum protocol development and resource optimization. The SEDJO protocol and quantum oracle implementations represent important innovations in quantum key distribution and secure computation. These developments extend beyond e-voting applications, offering valuable insights for the broader field of quantum internet applications.

7.2 Broader Impact

The development of Quantegrity has profound implications for quantum internet advancement through its novel protocol innovations. The enhanced quantum key distribution methods and improved quantum oracle implementations provide a foundation for future quantum applications. The system's approach to quantum state management offers practical solutions to common challenges in quantum communication and computation.

In the realm of applied security, Quantegrity demonstrates the feasibility of deploying quantum cryptography in critical systems. The successful implementation of quantum authentication and verifiable security measures provides valuable insights for other security-critical applications. This practical demonstration of quantum security advantages helps bridge the gap between theoretical quantum cryptography and real-world security requirements.

7.3 Future Directions

The success of Quantegrity opens several promising avenues for future development. System enhancement efforts will focus on optimizing protocols, improving scalability, and refining user interfaces based on deployment experience. These improvements will contribute to the system's effectiveness while providing valuable insights for quantum application development.

The potential for technology transfer represents another important direction for future work. The principles and approaches demonstrated in Quantegrity can be adapted to other critical systems requiring high security and verifiability. The system's security model and implementation patterns provide a valuable template for developing quantum-enhanced applications across various domains.

7.4 Final Summary

Quantegrity represents a significant milestone in the development of quantum internet applications, demonstrating how quantum technologies can enhance critical infrastructure while maintaining practical usability. The system successfully combines quantum security advantages with real-world operational requirements, providing a model for future quantum internet applications. By proving that quantum internet capabilities can deliver concrete benefits in critical applications, Quantegrity advances both the theoretical and practical aspects of quantum computing.

The system's comprehensive approach to quantum-classical integration, coupled with its practical implementation strategies, establishes a robust foundation for future quantum internet applications. Through its success in securing and enhancing election infrastructure, Quantegrity demonstrates the tangible value of quantum technology in critical systems. This achievement not only validates the potential of quantum internet applications but also provides a clear pathway for their continued development and deployment across various domains.

*This report is based on a project implementation of the Quantegrity e-voting system. The complete project implementation and documentation can be found on:

http://dx.doi.org/10.13140/RG.2.2.33924.03200

References

1. Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R., . . . Sherman, A. (2008). Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. *USENIX Workshop on Accurate Electronic Voting Technology*. USENIX.
2. Galois. (2015). *The Future of Voting End-toend Verifiable Internet Voting.* USA: U.S. Vote Foundation.
3. IBM Quantum. (2024, Sep 27). *Qiskit*. Retrieved from https://www.ibm.com/quantum/qiskit
4. Landers, V. (2023). Symmetrically Entangled Quantum Oracles for Quantum Key Distribution. *Preprint*.
5. Landers, V. (2024, Sep 27). *Quantegrity*. Retrieved from Github: https://github.com/VidurangaLanders/Quantegrity
6. Legré, M. (2009, Dec 3). *Quantum Quantum Cryptography Cryptography – A Reality A Reality Today*. Retrieved from id Quantique: https://indico.cern.ch/event/71768/attachments/1035636/1475548/idQCERN_-_Quantum_Cryptography.pdf
7. Liao, S., Cai, W., Liu, W., & al, e. (2017). Satellite-to-ground quantum key distribution. *Nature, 549*, 43-47. doi:https://doi.org/10.1038/nature23655
8. Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016). Quantum random number generation. *npj quantum information*.
9. Nielsen, M. A., & Chuang, I. L. (2011). *Quantum Computation and Quantum Information* (10 ed.). Cambridge University Press.
10. Shor, P. W., & Preskill, J. (2000). Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 441-444.
11. Simon, D. R. (1997). On the power of quantum computation. *SIAM journal on computing*, 1474-1483.
12. Stanley, M., Gui, Y., Unnikrishnan, D., Hall, S., & Fatadin, I. (2022). Standards, Recent Progress in Quantum Key Distribution Network Deployments and. *Journal Of Physics: Conference Series*.
13. Toshiba. (2024, Sep 13). *Quantum Key Distribution*. Retrieved from https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html
14. Wolf, R. (2021). *Quantum Key Distribution* (1 ed.). Springer Cham. doi:https://doi.org/10.1007/978-3-030-73991-1
15. Zagórski, F., Carback, R., Chaum, D., Clark, J., Essex, A., & Vora, P. (2013). Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System. *Applied Cryptography and Network Security. ACNS 2013. Lecture Notes in Computer Science.* Berlin, Heidelberg: Springer.