Enhancing Position Verification in Multi-Node Quantum Networks

Ziyan Zhang*
MNS Group
University of Amsterdam
Amsterdam, the Netherlands
z.zhang12@uva.nl

Florian Speelman
TCS Group
University of Amsterdam
Amsterdam, the Netherlands
f.speelman@uva.nl

Paola Grosso
MNS Group
University of Amsterdam
Amsterdam, the Netherlands
p.grosso@uva.nl

***Abstract*—Quantum position verification (QPV) is emerging as a promising application for quantum networks, leveraging spatial and quantum information to verify locations. However, current discussions on QPV protocols are largely confined to perfect experimental setups and one-dimensional scenarios. To address this gap, we extend the QPV$^{f}_{BB84}$ protocol to two dimensions. First, we define the requirements for the 2D QPV task and assess its performance under real-world constraints, which potentially expose the system to external attacks. To strengthen the protocol against these vulnerabilities, we study the 'danger zones', defining a region in spacetime within which attackers can manipulate these real-world constraints to convince verifiers. We then develop two algorithms to implement this theory: the *Verifiable Vertices Selection* algorithm, which identifies nodes that can validate their locations with designated verifiers, and the *Malicious Prover Location Identification* algorithm, which determines the 'danger zone' around the prover. Finally, we present a case study to demonstrate the conceptual implementation of the protocol. Our findings advance the development of secure and practical QPV protocols while highlighting the potential of quantum networks in the noisy intermediate-scale quantum (NISQ) era.**

***Index Terms*—quantum network, quantum cryptography, quantum communication**

I. Introduction

In an era where digital communication forms the backbone of our global interactions, quantum networks are emerging as the next frontier. At their core, quantum networks provide a significant advancement by introducing quantum communication, where qubits serve as information carriers [1]. With increasingly efficient quantum communication hardware [2], the demand for real-world applications is growing. One such application is Quantum Position Verification (QPV) [3], which stands out as a promising use case for quantum networks.

Position Verification (PV) involves using one's location as a token of identity, without requiring a pre-shared cryptographic key [4]. Identity authentication processes occur in everyday life, and PV can significantly enhance the security and reliability of these operations. For example, banks can prevent unauthorized access by verifying that transactions are initiated only from legitimate, pre-approved positions, such as a customer's home or a specific branch, as shown in Fig. 1. Participants in PV are either *provers*, i.e. nodes that want their exact position to be confirmed, or *verifiers*, i.e. nodes that attest the location of the prover.

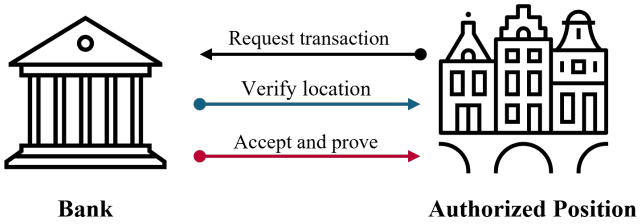


Figure 1: A simplified illustration of the PV protocol for banking authentication.

One of the core concepts enabling PV protocols is the principle of relativity, which states that information cannot travel faster than the speed of light. The most basic classical PV protocol is *distance bounding*, which upper bounds the distance between a prover and a verifier by timing the message exchanges between them, under the assumption that communication occurs at the speed of light in a classical channel. However, such a protocol doesn't suffice to precisely specify a location, only bounding distance [5].

To go from distance bounding to position verification, we could attempt to introduce additional verifiers. A more complex protocol involves two verifiers aiming to verify a prover's location precisely. Both verifiers send messages to the prover simultaneously and require a pre-agreed response, ensuring mutual certification. Nevertheless, this protocol has been proved insecure to adversaries positioned along the direct line between the verifiers [6]. Here the integration of quantum communication helps to reduce the chance of simple eavesdropping, resulting in Quantum Position Verification (QPV) [7].

Unlike classical PV, which relies on sending two classical bit streams, QPV leverages a quantum communication channel to ensure security. The no-cloning theorem makes it impossible for adversaries to copy an unknown qubit, thereby blocking attacks that simply intercept and copy information. This QPV protocol (QPV$^{f}_{BB84}$ protocol) has been proven secure against attackers who do not pre-share entangled quantum states [8]. A more detailed illustration of this protocol will be provided in Section II.

However, most discussions about QPV protocols are limited

to perfect experimental setups and 1D cases, which are not relevant to real-world applications [9]. The main objective of our work is to assess and improve the feasibility of QPV tasks in real-life network topologies. To achieve this, in Sec. III we analyze the requirements for the 2D QPV task and give a detailed definition of 2D-QPV$^f_{BB84}$ protocol. We then quantify the protocol's performance under real-world conditions. We subject our protocol to various practical constraints using a quantum network simulator (see Sec. III). Our simulation results indicate that quantum operation errors and photon loss are the primary contributors to the protocol's error rate.

To further enhance the feasibility of the protocol, we examine the 2D-QPV$^f_{BB84}$ protocol within spacetime models (see Sec. IV). Initially, we analyze a standard network topology where verifiers are symmetrically distributed around the prover. In such a configuration, the security of our protocol cannot be guaranteed due to geometric constraints. These limitations suggest that a malicious prover cannot deceive the verifiers beyond a certain area [10]. To better align with real-world constraints, we further refine this area by incorporating the prover's processing time. We specified this refined area as the 'danger zone'.

Moreover, we develop two algorithms (see Sec. V) that can be applied to any network topology: the *Verifiable Vertices Selection* algorithm identifies which nodes in the network can prove their location given a set of known verifiers; the *Malicious Prover Location Identification* algorithm determines the 'danger zone' from which dishonest prover can attack the protocol.

Furthermore, in Section VI, we conduct a case study to illustrate and evaluate the QPV task under practical conditions, incorporating complex network topologies and real-world constraints. We specify the process of implementing the protocol in real-life scenarios and demonstrate that our proposed algorithms enhance both the feasibility and security of the position verification task.

II. Background

In this section, we introduce the prerequisites, notations, and assumptions used for QPV tasks.

A. Entanglement

Entanglement is a unique quantum mechanics phenomenon where two or more particles become strongly interconnected. A particular example of an entangled pair is the Einstein-Podolsky-Rosen (EPR) pair. An EPR pair represents two maximally entangled particles. EPR pairs can be described using two types of orthonormal basis vectors: the computational basis and the Hadamard basis. The computational basis consists of the standard binary states $|0\rangle$ and $|1\rangle$, while the Hadamard basis is composed of the superposition states $|+\rangle$ and $|-\rangle$.

A fundamental feature of entanglement is the non-locality of entangled pairs. This means that the state of one particle instantly determines the state of the other, regardless of the distance between them. For example, consider an EPR pair in the computational basis: $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, If we measure the first qubit and find it in the state $|1\rangle$, the second qubit must be in the state $|0\rangle$, and vice versa. This property is remarkably useful in QPV$^f_{BB84}$ protocol, where it allows the verifier to effectively examine the measurement results claimed by the prover.

B. QPV$^f_{BB84}$ protocol

Here we define one round of the 1D-QPV$^f_{BB84}$ protocol (Definition. II.1) [11] [12]. The spacetime sequence of this protocol is shown in Fig. 2. At unit time $t = 1$, all information arrives at the prover P. Verifiers V_0 and V_1 receive results from P at unit time $t = 2$. The green shaded regions represent the spacetime region before time unit 1. These regions are formed by light travel distances from V_0 and V_1 to the prover P, denoted as region L and R respectively.

Definition II.1 (1D-QPV$^f_{BB84}$ protocol)**.** *For $n \in \mathbf{N}$, f is a boolean function $f := \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ programs measurement basis $\mathbf{B}$. Basis 0 and 1 denote respectively the computational basis and Hadamard basis.*

1) Verifier V_0 and V_1 pre-agree on two random strings x, y and V_0 prepares the EPR pair $|\Psi\rangle$.
2) V_0 sends one qubit Q of $|\Psi\rangle$ and x to the prover P, and V_1 sends y to P. These three pieces of information should arrive at P simultaneously.
3) P measures the qubit Q with the programmed basis $\mathbf{B}$ immediately upon receipt, then broadcasts the measurement outcome to verifiers V_0 and V_1. If the qubit is lost, the prover sends "$\varnothing$" (photon loss).
4) V_0 measures the local qubit and records the outcome as m. Let a and b be the answers received by verifiers V_0 and V_1, respectively. V_0 and V_1 share (a, b, m) in one round of communication, if both a and b arrive on time and match m, the verifiers record this round as "c" (correct); if the answers do not match m, they record it as "w" (wrong). Otherwise, the result is recorded as "\" (abort).

To fully convince the verifier, this protocol is repeated n times. We also consider constraints such as photon loss and quantum noise. These constraints lead to an error rate p_{err} even when there is only an honest prover. Let η be the successful qubit transmission efficiency over n attempts. By executing this protocol n times, an honest prover will broadcast $2n$ outcomes such that the verifiers would record "c", "w", "$\varnothing$", and "\" with probability:

- $\mathbb{P}(c) = \eta(1 - p_{err})$
- $\mathbb{P}(w) = \eta p_{err}$
- $\mathbb{P}(\varnothing) = 1 - \eta$
- $\mathbb{P}(\backslash) = 0$

If the overall result matches the expected probability distribution, we accept the prover's location. However, if a malicious prover $P^\star$ employs an attack strategy resulting in $\mathbb{P}(c^\star) \approx \mathbb{P}(c)$ as well as an acceptable $\mathbb{P}(\backslash)$, we consider the attack successful.

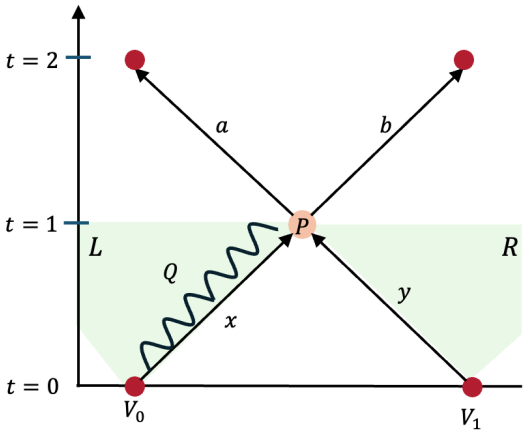


Figure 2: The spacetime sequence of the 1D-QPV$^f_{BB84}$ protocol.

To ensure the security of the protocol, the measurement basis $\mathbf{B}$ should remain unknown until all keys are well received by the prover P. This condition is easily met in 1D-QPV$^f_{BB84}$ protocol. In this setup, two regions L and R formed by the light cone of the events sending messages from two verifiers, are disjoint (see Fig. 2). This disjoint geometry also guarantees the correct measurement outcome cannot simultaneously be obtained from two independent quantum registers [13].

III. 2D Quantum Position Verification

While the 1D-QPV$^f_{BB84}$ protocol offers fundamental insights, its application is limited. In experiments, verifiers and the prover are rarely aligned in a straight line, which raises concerns about the protocol's security and effectiveness in higher-dimensional settings [10].

In this section, we explore the requirements for 2D-QPV$^f_{BB84}$ protocol. Building on these requirements, we define 2D-QPV$^f_{BB84}$ protocol leverage entangled pairs. Additionally, we identify three major real-world constraints that affect the protocol's practical implementation: quantum operation errors, photon loss, and clock synchronization. We then assess how these constraints influence the performance of 2D-QPV$^f_{BB84}$ protocol.

A. Requirements

To thoroughly investigate the requirements for the QPV task, we first examine a scenario where the 1D-QPV$^f_{BB84}$ protocol is extended to a 2D plane. In this setup, two verifiers are aligned on a straight line, while the prover is positioned off this line. An attacker could exploit this by finding a symmetric point on the plane that is closer to the verifiers, yet still maintains the geometric symmetry.

To prevent this exploitation, the protocol must ensure the prover is located within the intersection area defined by the distances between the prover and the verifiers. This reasoning extends to QPV$^f_{BB84}$ protocol in any n-dimensional space, as demonstrated by Theorem. III.1.

Theorem III.1 (General Requirement)**.** In an n-dimensional QPV$^f_{BB84}$ protocol, $n+1$ verifiers are required to uniquely determine the position of a prover in general.

Proof: The prover's position can only be verified within the convex hull $\mathcal{C}$ of the geometry formed by the verifiers. For n verifiers, there exists at most $n-1$ dimensional convex hull. Thus, in a general case, to verify a prover's location in n dimensional space, we need at least $n+1$ verifiers.

A special case is that in an n-dimensional QPV$^f_{BB84}$ protocol, if the prover's location $\mathbf{p}$ lies within the convex hull of the positions of n verifiers $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$, i.e.,

$$\mathbf{p} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i, \tag{1}$$

where $\sum_{i=1}^{n} \lambda_i = 1$ and $\lambda_i \geq 0$ for all i, then these n verifiers are sufficient to verify the prover's location. ■

Based on our derivation for the general requirements, we introduce three verifiers into the 2D-QPV$^f_{BB84}$ protocol to ensure the geometry satisfies Theorem. III.1. Additionally, each verifier is assigned a key to program the measurement basis. All other settings remain consistent with Definition. II.1. We define one round of our 2D-QPV$^f_{BB84}$ protocol as follows:

Definition III.1 (2D-QPV$^f_{BB84}$ protocol)**.** *For $n \in \mathbf{N}$, f is a boolean function $f := \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ programs measurement basis $\mathbf{B}$. Basis 0 and 1 denote respectively the computational basis and Hadamard basis.*

1) Verifier V_0, V_1, and V_2 pre-agree on three random strings x, y, z and V_0 prepares the EPR pair $|\Psi\rangle$.
2) V_0 sends one qubit Q of $|\Psi\rangle$ and x to the prover P, V_1 and V_2 sends y and z to P, respectively. These four pieces of information should arrive at P simultaneously.
3) P measures the qubit Q with the programmed basis $\mathbf{B}$ immediately upon receipt, then broadcasts the measurement outcome to verifiers V_0, V_1, and V_2. If the qubit is lost, the prover sends "$\varnothing$" (photon loss).
4) V_0 measures the local qubit and records the outcome as m. Let α, β, γ be the answers received by verifiers V_0, V_1, and V_2, respectively. If both α, β, and γ arrive on time and match m, the verifiers record this round as "c" (correct); if the answers do not match m, they record it as "w" (wrong). Otherwise, the result is recorded as "\" (abort).

In this 2D-QPV$^f_{BB84}$ protocol, no additional results are introduced compared to the 1D case. The additional keys only increase the computation complexity of the challenge. Therefore, the outcome probability distribution remains the same as in Definition. II.1.

B. Real-world constraints

The security of quantum position verification has been theoretically proven under ideal conditions [14]. However, the practical implementation of this task faces significant challenges due to real-world constraints. In experimental settings, fulfilling these essential requirements—such as transmitting

quantum information at the speed of light (c) and conducting error-free quantum operations—proves to be difficult.

We identify three primary drawbacks when applying the QPV task experimentally. Firstly, qubits are highly sensitive to distortions caused by environmental noise, hardware imperfections, and operational inaccuracies, leading to unpredictable quantum evolution. Secondly, during transmission, qubits (usually photons) may be lost due to absorption, scattering, or deviation onto unintended paths, thereby reducing the protocol's efficiency. Lastly, quantum information travels slower than classical information, which can be transmitted at the speed of light (c) using microwaves. In contrast, quantum information typically travels at about $\frac{2}{3}c$ in an optical fiber. This speed differential complicates message synchronization and allows potential attackers to exploit timing variations.

1) Quantum operation errors: In the context of the QPV task, quantum errors typically include State Preparation and Measurement (SPAM) errors. These errors consist of two main components: state preparation errors, which occur when there are deviations from the intended or ideal quantum state during preparation, and measurement errors, which arise when inaccuracies occur in determining the quantum state of a qubit or quantum system during measurements. The SPAM error probability can be expressed as

$$P_{\text{SPAM}} = P_{\text{sp}} + P_{\text{m}} - P_{\text{sp}}P_{\text{m}} \tag{2}$$

where P_{sp} is the probability of state preparation error, and P_{m} is the probability of measurement error. The item $-P_{\text{sp}}P_{\text{m}}$ accounts for the possibility of both types of errors occurring simultaneously, which wouldn't affect the correctness of the system.

It is difficult to quantify state preparation and measurement errors separately without an ancillary system [15]. These two errors usually happen together [16], triggered by various parameters. However, since they all belong to bit-flip errors, we can easily represent their impact via simulation.

To assess these errors in the QPV task, we use the NetSquid [17], an event-driven quantum network simulator to evaluate the 2D-QPV$^{f}_{BB84}$ protocol's performance. In Fig. 3 we compare the protocol's error rate p_{err} against various quantum error probability p_Q, subject to three types of quantum errors: SPAM error, Measurement error, and State Preparation error. For clarity, we set the average p_Q to 20%, which is significantly larger than the SPAM error rate in experiments (4×10^{-3}) [18]. In general, the protocol's error rate p_{err} increases as p_Q rises. Among the error types, SPAM error (red line) consistently remains the highest across the entire range of p_Q.

Measurement error (black line) shows an exponential increase and typically lies between the SPAM and State Preparation errors throughout most of the range. In contrast, State Preparation error (blue line) remains the lowest among the three error types. This lower impact is because the verifier only needs to assess the non-locality of the EPR pair, regardless of their exact states. Therefore, even if the initial state deviates to an undesired state, it does not affect the correctness of the

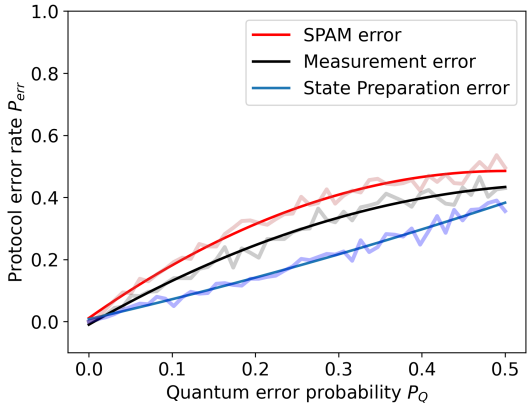


Figure 3: Protocol error rate p_{err} v.s. Quantum error probability p_{Q}

QPV$^{f}_{BB84}$ protocol as long as the verifier can successfully prepare the EPR pair.

Through simulation, we can effectively distinguish the contributions of measurement and state preparation errors. Notably, measurement error significantly impacts the quantum error in the 2D-QPV$^{f}_{BB84}$ protocol.

2) Photon loss: Photon is naturally the most suitable carrier for establishing quantum links between end nodes [9]. Currently, there are two types of photonic quantum channels: free-space channels via satellites [19] and fiber-based channels [20]. Each type of channel has its advantages, but both suffer from photon loss, which inevitably affects the communication rate across the network. The loss rate can be 0.2dB/km for photons in standard telecom bands. In general, let α be the photon loss coefficient (dB/km), the probability of photon loss P_{loss}over distance d is:

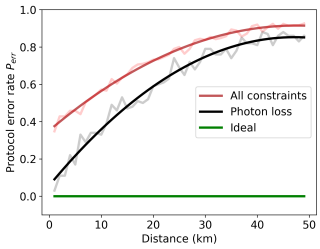
$$P_{\text{loss}} = 1 - 10^{-\frac{\alpha d}{10}} \tag{3}$$

This information loss can significantly jeopardize the protocol. In Fig. 4a, we compare the protocol's error rate against distance under three conditions: ideal, photon loss, and all constraints. Our results show that photon loss significantly increases the protocol's error rate, with an obvious effect over longer distances.

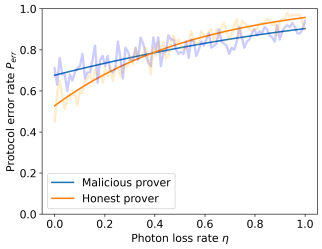
Moreover, attackers can manipulate photon loss to compromise the protocol. We introduce the random guess strategy [8], as shown in Definition. III.2. This attack strategy is easy to implement since it does not require complex quantum operations.

Definition III.2 (Random Guess Strategy)**.** *Let Alice, Bob, and Charlie eavesdrop on the intermediate point between the verifier and the prover. We assume they can intercept both classical and quantum information.*

1) Alice intercepts the qubit $|\Psi\rangle$, measures with a random basis $\tilde{x}$ instead of programmed basis **B**
2) When Bob and Charlie receive the key, they immediately send it to Alice to see if programmed basis **B** match $\tilde{x}$



(a) Protocol error rate p_{err} vs. distance for ideal conditions, photon loss, and all constraints.



(b) Protocol error rate p_{err} vs. photon loss rate η for malicious and honest provers.

Figure 4: Impact of photon loss on protocol error rates: (a) shows how different constraints affect the error rate over distance, (b) shows how photon loss rate affects the error rate under different prover scenarios.

3) If yes, then they broadcast this result, if not, they send "$\varnothing$" (photon loss) instead to mislead the verifier.

As shown in Fig. 4b, we apply this attack to our protocol, comparing the protocol's error rate P_{err} between a malicious prover and an honest prover under increasing photon loss rates η. This strategy becomes more effective as the photon loss rate increases. Specifically, when the photon loss rate η exceeds 0.4, the honest prover's error rate surpasses the malicious prover's, making the malicious prover more convincing to the verifiers.

3) clock-synchronization: Ensuring the security of messages in the quantum position verification task necessitates that all information arrives at the prover simultaneously. This requirement demands precise control over the timing and delay of information transmission. However, achieving such synchronization accuracy in practice is challenging and raises several open questions. One potential solution is to use an ancillary system, such as a qubit, to facilitate synchronization [21]. An alternative approach involves integrating classical network techniques. Recent research suggests that leveraging a programmable quantum data plane presents a promising solution to these challenges [22].

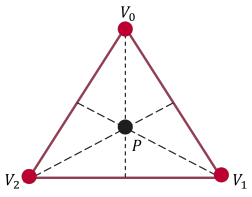
IV. 2D QPV Models

In this section, we investigate two models based on our 2D-QPV$^{f}_{BB84}$ protocol to assess its security across different network topologies.

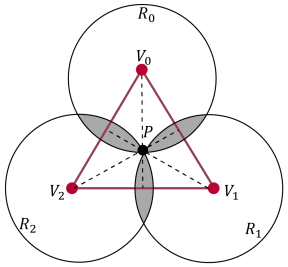
A. Standard network topology

To give a comprehensive analysis of the 2D-QPV$^{f}_{BB84}$ protocol, we consider the following scenario: Three verifiers V_0, V_1, and V_2 are positioned at the vertices of an equilateral triangle, with the honest prover P located at the center. The light cone from the prover P to each verifier V_i (where $i = 0, 1, 2$) form three circular regions R_0, R_1, R_2, as illustrated in Fig. 5.

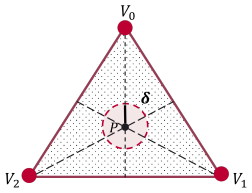
To examine the security of our 2D-QPV$^{f}_{BB84}$ protocol within this model, it is intuitive to extend the disjoint reasoning



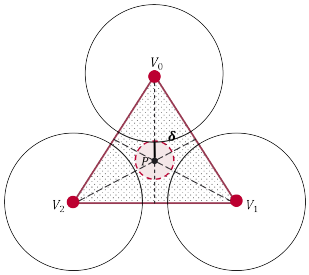
(a) The standard network topology model.



(b) $\delta = 0$



(c) 'Danger zone' with diameter δ around the prover P.



(d) $\delta = 0.23$

Figure 5: Illustration of the standard 2D-QPV$^{f}_{BB84}$ protocol model and its security considerations: (a) The standard model where verifiers V_0, V_1, and V_2 are equidistant from the prover P; (b) The initial setup without the 'danger zone' ($\delta = 0$)showing three overlapping regions formed by the light cone from the prover P to the verifiers; (c) The 'danger zone' (in pink) with a diameter δ around the prover P, where malicious prover outside this zone cannot break the protocol by intercepting keys; (d) When $\delta = 0.23$, the three regions are disjoint, reducing the risk of information interception by attackers.

used in the 1D-QPV$^{f}_{BB84}$ protocol (Fig. 2) to the 2D case. However, as shown in Fig. 5b, the three regions R_0, R_1, R_2 in our 2D-QPV$^{f}_{BB84}$ protocol overlap instead of being disjoint. This overlap allows attackers to program the correct measurement basis before the information reaches the prover P. Therefore, outside this area, a malicious prover cannot make the verifiers accept [10].

The time at which the measurement basis $\mathbf{B}$ is programmed marks the earliest time when a point at a distance δ from the prover P gains access to all keys x_0, x_1, x_2. In the standard model, this occurs when $\delta \approx 0.23 \cdot l$ [10], where l is the distance between the prover and a verifier. Consequently, this area forms a circle with a diameter of 2δ, which corresponds to approximately 46% of l. We refer to this region as the 'danger zone', as beyond this area, a malicious prover is unable to compromise the protocol. However, this 'danger zone' is insufficient as it overlooks the complexities of overlapping areas within the zone and real-world constraints.

B. Arbitrary network topology

In real-world network topologies, nodes involved in the protocol are often not uniformly distributed, which introduces

significant complexities and challenges to protocol security. Moreover, the time required for the prover to respond opens a window for attackers to exploit the protocol. These constraints highlight a critical limitation: the 'danger zone' in the standard model, which is intended to identify where a malicious prover cannot successfully deceive the verifier, does not adequately represent the threats or vulnerabilities inherent in actual network setups. More importantly, it fails to specify areas that directly threaten protocol integrity. Hence, refining the definition and scope of the 'danger zone' in the standard model is essential to accommodate real-world networks' diverse configurations and vulnerabilities more effectively.

To enhance our understanding of the 'danger zone' in more complex network setups, we consider a basic configuration of four nodes, including three verifiers and one prover. We configure a logical arbitrary triangle, where the three verifiers V_0, V_1, and V_2 are located at each vertex of the triangle, separated with different distances d_{01}, d_{02}, and d_{12}; the prover P is located inside the triangle, and the distance from each verifier to prover P is denoted as d_0, d_1 and d_2, as illustrated in Fig. 6a. We also incorporate the prover's processing time ϵ, which is necessary for programming functions and conducting qubit measurements, into our revised model (see Fig. 6b).

To further refine our security analysis, we utilize spacetime geometry, which is a set of all locations in both space and time. An event $C(x,t)$ occurs at space x and time t. Throughout our analysis, we assume a flat spacetime, characterized by $(t, x_1, x_2, ..., x_n)$ with $t, x_1, x_2, ..., x_n \in \mathcal{R}$. Following the definitions in [10], we define the *causal future* $C^+(x)$ of an event x as the set of all events reachable from x, similarly, we define *causal past* as $C^-(x)$ as all events in the past that can influence x. We designate V_i^+ as the spacetime position where V_i sends the information and V_i^- as the point where V_i expects a response from the prover P. These adjustments enable us to develop a more robust security framework, leading to Theorem. IV.1:

Theorem IV.1. Let Ω denote the overlap region in a flat spacetime for our 2D-QPV$^f_{BB84}$ protocol, defined as $\Omega := \bigcap_{i=0}^{2} C^+(V_i^+) \cap C^-(V_0^-) \cap C^-(V_1^-) \cap C^-(V_2^-)$. If the spacetime trajectory of the prover P is represented by $\mathbf{P}(x, t+\epsilon)$, then the protocol remains secure if $\Omega \backslash \mathbf{P}(x, t+\epsilon) = \varnothing$.

Proof: Assume for contradiction that there exists a set E within the same spacetime such that $E \subset \Omega$ and $E \cap \mathbf{P}(x, t+\epsilon) = \varnothing$. This would imply that there is a feasible position and time within E for a malicious prover not located on $\mathbf{P}(x, t+\epsilon)$ to receive the signals x_1, x_2, x_3, compute the outcomes honestly, and transmit them back to the verifiers within the allowed time constraints, thereby potentially compromising the security of the protocol.

This scenario contradicts the condition in the theorem. According to the theorem, for the protocol to remain secure, no such E should exist; thus, the prover's spacetime trajectory $\mathbf{P}(x, t+\epsilon)$ must intersect with Ω, ensuring all necessary interactions occur within the secure region defined by Ω. Therefore, any existence of E such that $E \backslash \mathbf{P}(x, t+\epsilon) = \varnothing$ leads to a contradiction, implying the necessity of our condition for protocol security. ∎

Theorem. IV.1 establishes a more comprehensive and effective security framework than the disjoint reasoning approach. It is applicable across various network topologies and accounts for extra processing time for the prover. Moreover, this theorem enables us to identify the actual 'danger zone' Γ, where attackers could potentially manipulate the prover's processing time to execute attacks. We define this zone in Corollary. IV.1.1.

Corollary IV.1.1. *In flat spacetime, given points x, y and a real number d, let $\mathcal{E}(x, y, d)$ denote an ellipse with foci x and y.*

Assume verifier V_i sends information at time t_i^+ and position x_i^+, and expects the response at time t_j^- and position x_j^-. Then the region Ω is equivalent to $\Pi = \bigcap_{\substack{i=0 \\ j=0}}^{2} \mathcal{E}(x_i^+, x_j^-, t_j^- - t_i^+ - \epsilon)$.

Proof: For any $z \in \Omega$,

$$\text{iff } \exists t : (z,t) \in P = \bigcap_i C^+((x_i^+, t_i^+ + \epsilon)) \cap \bigcap_j C^-((x_j^-, t_j^-))$$

$$\text{iff } \exists t : (\forall i : \|x_i^+ - z\| \leq t - t_i^+ - \epsilon) \wedge (\forall j : \|x_j^- - z\| \leq t_j^- - t)$$

$$\text{iff } \exists t : (\max_i \|x_i^+ - z\| + t_i^+ + \epsilon \leq t) \wedge (\max_j \|x_j^- - z\| - t_j^- \leq -t)$$

$$\text{iff } \max_{i,j} \|x_i^+ - z\| + t_i^+ + \epsilon + \|x_j^- - z\| - t_j^- \leq 0$$

$$\text{iff } \forall i, j : \|x_i^+ - z\| + \|x_j^- - z\| \leq t_j^- - t_i^+ - \epsilon$$

$$\text{iff } z \in \bigcap_{i,j} E(x_i^+, x_j^-, t_j^- - t_i^+ - \epsilon)$$

∎

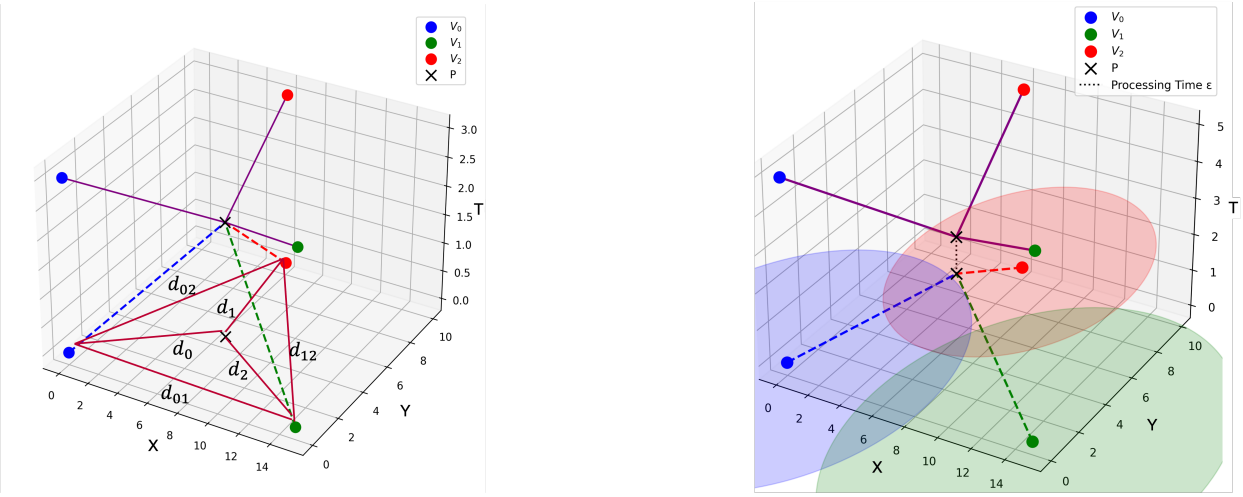
This strategy allows us to define the 'danger zone' $\Gamma = \Pi \backslash \mathbf{P}$ in any network configuration. By identifying this region, we can better understand the potential vulnerabilities where attackers might manipulate the processing times of the honest prover.

V. Algorithms

To effectively apply the 2D-QPV$^f_{BB84}$ protocol in practical scenarios, we outlined several requirements in previous sections, including the geometry of verifiers and the prover (Sec. III-A) and real-world constraints (Sec. III-B). Additionally, the vulnerability to physical attacks on network nodes poses a significant threat, potentially allowing adversaries to compromise the protocol's security.

To address these challenges and enhance both the feasibility and security of the protocol, we propose two algorithms. The *Verifiable Vertices Selection* (VVS) algorithm selectively identifies and assesses nodes that can prove their location within a network topology by a designated set of verifiers.

Furthermore, the *Malicious Prover Location Identification* (MPLI) algorithm enhances security by leveraging insights



(a) General model in spacetime.

(b) Model adaptation with prover's processing time ϵ.

Figure 6: Illustrations of the general model in spacetime with different settings.

from our 'danger zone' theorem. This algorithm predicts potential nodes within a network topology that could exploit vulnerabilities in the protocol, thereby enabling preemptive strategies against malicious attacks.

Together, these algorithms contribute to enhancing the practical applicability and robustness of our 2D-QPV$^{f}_{BB84}$ protocol in real-world environments. Further, in Sec. VI, we provide a case study using our proposed algorithms based on real-world network topology.

A. *VVS: Verifiable Vertices Selection*

Current quantum nodes are expensive and consume substantial energy [23]. Such resource scarcity drives the need to optimize the utility of quantum networks for specific tasks such as position verification. To leverage quantum networks effectively for position verification tasks, it is essential to first determine the coverage provided by certain quantum nodes within the network.

it is essential to ensure that the prover remains within the convex hull defined by the verifiers' geometric arrangement, as stated in Theorem III.1. Our *VVS* algorithm, presented in Algorithm. 1, addresses this requirement for a given QPV task by ensuring the verifiability of nodes within the specified geometric constraints. Additionally, our previous security analysis in Sec. IV demonstrates that placing the prover closer to the centroid of the verifiers' geometry enhances the protocol's security. The *VVS* algorithm also evaluates the nodes based on their security aspects.

Specifically, *VVS* takes four input parameters: the network topology in a graph format G, and three verifiers' locations V_0, V_1, and V_2. The *VVS* starts by initializing an empty set S to store the verifiable vertices (Line 1). It then computes the centroid C of the triangle formed by V_0, V_1, and V_2 (Line 2). For each vertex x in the set G (Line 3), it initializes an 'accumulator' to 0 (Line 4). The algorithm then loops through each pair of verifiers (i, j) where $i, j \in \{0, 1, 2\}$ and $i \neq j$ (Line 5). For each pair, it checks if the sum of distances from vertex x to verifiers V_i and V_j is less than the distance between verifiers V_i and V_j (Line 6). If this condition is true, the 'accumulator' is incremented by 1 (Line 7). After checking all pairs, if the 'accumulator' equals 3 (Line 8), vertex x is added to S (Line 9). Finally, the list S is sorted by the distance of each vertex x to the centroid C in ascending order (Line 10). After all vertices have been processed, the algorithm returns the sorted set S (Line 11).

Algorithm 1: *VVS*: Verifiable Vertices Selection

Input: A set of vertices G, three verifiers' locations denoted as V_0, V_1, V_2

Output: A set S of vertices can be proved location by V_0, V_1, V_2, sorted by their effectiveness

1 Initialize $S \leftarrow \emptyset$;
2 Compute the centroid C of V_0, V_1, V_2:

$$C = \left(\frac{x_{V_0} + x_{V_1} + x_{V_2}}{3}, \frac{y_{V_0} + y_{V_1} + y_{V_2}}{3} \right)$$

3 **for** *each vertex* x *in* G **do**
4 accumulator $\leftarrow 0$;
5 **for** *each pair* (i, j) *where* $i, j \in \{0, 1, 2\}$, $i \neq j$ **do**
6 **if** $d(x, V_i) + d(x, V_j) < d(V_i, V_j)$ **then**
7 accumulator $\leftarrow$ accumulator $+ 1$;
8 **if** *accumulator* $= 3$ **then**
9 Add x to S;
10 Sort S by $d(C, d(x, C))$;
11 **return** S;

B. *MPLI: Malicious Prover Location Identification*

Malicious Prover Location Identification (*MPLI*) is crucial in enhancing the security of position verification tasks. By

predicting potential locations where malicious provers could take over the network, MPLI allows for preemptive measures to be taken to secure the verification process. This proactive approach helps in the early detection of threats.

MPLI leverages the 'danger zone' theorem we proposed. Given a network topology and the QPV task's setup, the algorithm predicts which nodes within the network could potentially be exploited as malicious provers. The algorithm is detailed as Algorithm. 2.

The *MPLI* algorithm takes six input parameters: a set of vertices G, the locations of three verifiers V_0, V_1, V_2, the location of the prover P, and the prover's response time ϵ. The algorithm begins by initializing an empty set Π to store the 'danger zone' (Line 1). It then iterates through each pair of verifiers (Line 2) to determine the size of the 'danger zone' using Corollary IV.1.1 (Lines 3 to 7). Next, the algorithm initializes an empty set M to store potential malicious provers (Line 8) and iterates through each node N in G (Line 9). For each node, it checks if N is neither a verifier nor the prover (Line 10) and if N belongs to the 'danger zone' set Π (Line 11). If both conditions are met, N is added to the set M (Line 12). Finally, the algorithm returns the set M of potential malicious provers (Line 13).

Algorithm 2: *MPLI*: Malicious Prover Location Identification

Input: A set of vertices G, three verifiers' locations V_0, V_1, V_2, the prover's location P, and response time ϵ

Output: A set of vertices $M \in G$ that could be potential malicious prover

1 Initialize $\Pi \leftarrow \emptyset$;
2 **for** *each pair of verifier indices* (i, j) *from* 0 *to* 2 **do**
3 $t_j^+ = t_i^+ = \frac{d_i}{c}$
4 Calculate the ellipse $\mathcal{E}(v_i^+, v_j^-, t_j^- - t_i^+ - \epsilon)$
5 **if** Π *is empty* **then**
6 $\Pi \leftarrow \mathcal{E}(v_i^+, v_j^-, t_j^- - t_i^+ - \epsilon)$;
  else
7 $\Pi \leftarrow \Pi \cap \mathcal{E}(v_i^+, v_j^-, t_j^- - t_i^+ - \epsilon)$;
8 Initialize $M \leftarrow \emptyset$;
9 **for** *each node* N *in* G **do**
10 **if** $N \neq V_i$ *where* $i \in \{0, 1, 2\}$ ***and*** $N \neq P$ **then**
11 **if** $N \in \Pi$ **then**
12 Add N to M;
13 **return** M;

The *MPLI* algorithm identifies the 'danger zone' within the network where attackers may effectively compromise the protocol by manipulating the response time window.

VI. Case Study

In this section, we present an illustrative case study to demonstrate the conceptual implementation of the QPV$^f_{BB84}$ protocol under real-world scenarios. We begin by detailing the network topology and the parameters for our 2D-QPV$^f_{BB84}$ protocol. We then describe the conceptual framework of our proposed protocol within a representative network topology.

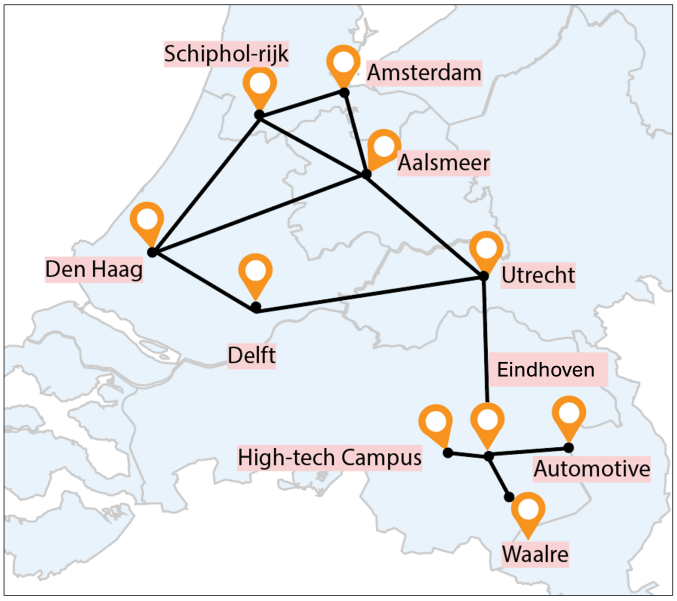


Figure 7: Quantum Internet Deployment Plan in the Netherlands (QDNL project). Nodes (in orange) within this network should perform quantum communication.

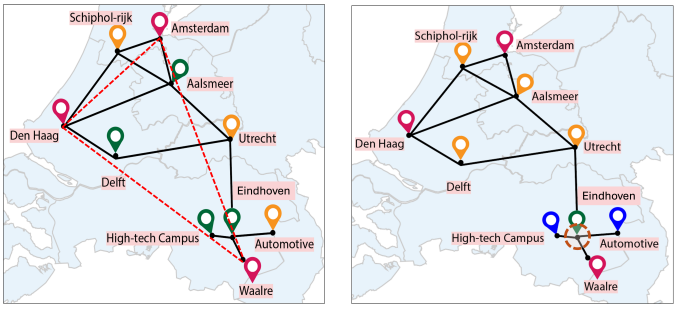
A. Experiment set-up

To illustrate the utility of our proposed algorithms, we use the quantum internet deployment plan in the Netherlands (QDNL) [24], shown in Fig. 7. The QDNL project envisions a nationwide quantum internet encompassing three primary regions: Amsterdam, Delft, and Eindhoven. These regions are interconnected, with each node capable of quantum communication both within and between the areas.

To ensure our analysis reflects realistic conditions, we incorporated relevant constraints from Sec. III. We introduced quantum operation errors and photon loss into the quantum channels, setting the quantum error probability at 0.4% and the photon loss rate at 0.2 dB/km. Additionally, we set the quantum operation time to 200 nanoseconds, sufficient for a complete single-qubit measurement [25]. To address synchronization issues, we manually created a control plane to delay information transmission times, ensuring the simultaneous arrival of data. This effectively 'stretched' the QDNL network topology into straight-line connections, transforming the physical topology into an abstract logical topology. For the rest, we keep the settings in Sec. III.

B. Case study

We begin the position verification task with the *Verifier Selection Problem*. For general 2D QPV tasks, selecting three verifiers is essential. The challenge in this selection lies in balancing coverage and efficiency.



(a) The *VVS* algorithm. (b) The *MPLI* algorithm.

Figure 8: Implementing two algorithms on the QDNL network topology: (a) The *VVS* algorithm selects three nodes as verifiers (in claret) based on the QPV protocol's geometry requirements, identifying four nodes that can prove their location (in green); (b) The *MPLI* algorithm identifies Eindhoven as the prover (in green) and determines the 'danger zone' (in brown).

A verifier set with broader coverage involves positioning verifiers at relatively large distances from each other. As noted in Theorem. III.1, greater distances between verifiers result in a larger convex hull, which allows the protocol's geometry to encompass more nodes and effectively test their locations. However, this arrangement sacrifices efficiency, requiring more precise synchronization and longer running times, which may increase vulnerability to attacks. In contrast, a verifier set optimized for efficiency covers fewer nodes but benefits from higher synchronization accuracy and shorter running times, thereby enhancing both performance and security.

To better illustrate our proposed algorithms, we prioritize a set with higher coverage. In this scenario, we select Amsterdam, Den Haag, and Waalre as our verifiers (see Fig. 8a). Using our *Verifiable Vertices Selection (VVS)* algorithm, we determine that this verifier set covers Aalsmeer, Delft, High-tech Campus, and Eindhoven, which are the locations we can verify. This selection scheme covers around 57% of the nodes inside this network, excluding the three verifiers.

Before initiating the protocol, we undertake preemptive actions to identify potential threats. For example, with Eindhoven as the prover, we evaluate whether nearby nodes might act as malicious provers. Our *Malicious Prover Location Identification (MPLI)* algorithm, takes the network topology and the protocol configuration (with Amsterdam, Den Haag, and Waalre as verifiers and Eindhoven as the prover) as inputs, pinpoints nodes within the 'danger zone' around the prover. In this case, no nodes within this network fall inside this zone (see Fig. 8b). Given this configuration, our 2D-QPV$^{f}_{BB84}$ protocol is theoretically secure within this network setup.

To complete the QPV task, the protocol is repeated at least a hundred times to generate an outcome distribution. If this distribution matches our expectations and exhibits a low abort rate, we then authenticate the prover's location and proceed with forwarding for further applications.

VII. Conclusion

In this paper, we extended the quantum position verification task to a more broadly applicable two-dimensional case. To achieve this, we thoroughly investigated the requirements and assessed the protocol under real-world constraints. We also developed two models to identify the 'danger zone' around the prover, thereby enhancing the protocol's security. Initially, we introduced the standard model along with its security claims based on geometry properties. However, this model proved insufficient for handling complex network topologies and real-world conditions. Consequently, we refined our 'danger zone' theory to accommodate complex network configurations. To ensure the effective execution of our 2D-QPV$^{f}_{BB84}$ protocol, we designed two algorithms: the *Verifiable Vertices Selection (VVS)* algorithm, which determines the coverage of verifiable nodes based on the network topology and verifier sets; and the *Malicious Prover Location Identification (MPLI)* algorithm, which leverages our 'danger zone' model to identify potential malicious provers within the network. These approaches collectively enhance the security and efficiency of the protocol. To illustrate the entire process, we conducted a case study using the QDNL network topology, demonstrating that four key processes are essential to complete the position verification task: verifier selection, malicious node identification, repeated protocol execution, and results matching.

Despite these advancements, our work is limited to evaluating the protocol against the random guess attack model, leaving other potential attack models unexplored. Future research should focus on more complex attack scenarios, such as those leveraging pre-entangled adversaries, to better understand the protocol's resilience under diverse conditions. Additionally, future studies should analyze a broader range of QPV protocols in real-world scenarios, including those utilizing squeezed states or Bosonic modes. Another limitation of our study is the lack of a detailed solution for the clock synchronization constraint. To address this, we are working on integrating a programmable network control plane to mitigate these challenges. Furthermore, integrating programmable control planes enables a more flexible control of quantum networks and their applications.

As quantum network technologies continue to evolve, our findings offer valuable insights into the development of practical and secure QPV protocols. We are actively incorporating computer network techniques, such as programmable control planes and data planes, to bridge the gap between theoretical designs and real-world implementation, bringing QPV closer to practical deployment.

The authors have provided public access to their code and/or data at: https://doi.org/10.5281/zenodo.14629988.

VIII. Acknowledgment

This work was supported by the Dutch National Growth Fund (NGF), as part of the Quantum Delta NL program.

References

[1] Z. Zhang, C. Papagianni, F. Speelman, and P. Grosso, "Towards complete quantum network stacks, a survey," *IEEE Network*, 2024.

[2] J.-L. Liu, X.-Y. Luo, Y. Yu, C.-Y. Wang, B. Wang, Y. Hu, J. Li, M.-Y. Zheng, B. Yao, Z. Yan *et al.*, "Creation of memory–memory entanglement in a metropolitan quantum network," *Nature*, vol. 629, no. 8012, pp. 579–585, 2024.

[3] A. Kent, W. J. Munro, and T. P. Spiller, "Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 84, no. 1, p. 012326, 2011.

[4] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position based cryptography," in *Annual International Cryptology Conference*. Springer, 2009, pp. 391–407.

[5] S. Halevi, *Advances in Cryptology-CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009, Proceedings*. Springer, 2009, vol. 5677.

[6] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky, "Position-based quantum cryptography," *arXiv preprint arXiv:1005.1750*, 2010.

[7] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions," *SIAM Journal on Computing*, vol. 43, no. 1, pp. 150–178, 2014.

[8] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography," *New Journal of Physics*, vol. 15, no. 10, p. 103002, 2013.

[9] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, p. eaam9288, 2018.

[10] D. Unruh, "Quantum position verification in the random oracle model," in *Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II 34*. Springer, 2014, pp. 1–18.

[11] L. Escolà-Farràs and F. Speelman, "Lossy-and-constrained extended non-local games with applications to cryptography: Bc, qkd and qpv," 2024. [Online]. Available: https://arxiv.org/abs/2405.13717

[12] A. Bluhm, M. Christandl, and F. Speelman, "A single-qubit position verification protocol that is secure against multi-qubit attacks," *Nature Physics*, vol. 18, no. 6, pp. 623–626, 2022.

[13] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of modern physics*, vol. 86, no. 2, pp. 419–478, 2014.

[14] J. Liu, Q. Liu, and L. Qian, "Beating Classical Impossibility of Position Verification," in *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), M. Braverman, Ed., vol. 215. Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, pp. 100:1–100:11. [Online]. Available: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2022.100

[15] H. Yu and T.-C. Wei, "Efficient separate quantification of state preparation errors and measurement errors on quantum computers and their mitigation," *arXiv preprint arXiv:2310.18881*, 2023.

[16] J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Y. Chen *et al.*, "State preservation by repetitive error detection in a superconducting quantum circuit," *Nature*, vol. 519, no. 7541, pp. 66–69, 2015.

[17] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpedek, M. Skrzypczyk *et al.*, "Netsquid, a network simulator for quantum information using discrete events," *Communications Physics*, vol. 4, no. 1, p. 164, 2021.

[18] C. Ryan-Anderson, J. G. Bohnet, K. Lee, D. Gresh, A. Hankin, J. P. Gaebler, D. Francois, A. Chernoguzov, D. Lucchetti, N. C. Brown, T. M. Gatterman, S. K. Halit, K. Gilmore, J. A. Gerber, B. Neyenhuis, D. Hayes, and R. P. Stutz, "Realization of real-time fault-tolerant quantum error correction," *Phys. Rev. X*, vol. 11, p. 041058, Dec 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.11.041058

[19] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[20] S. Bose, "Quantum communication through an unmodulated spin chain," *Physical review letters*, vol. 91, no. 20, p. 207901, 2003.

[21] L. Zhang, Z. Wang, Y. Wang, J. Zhang, Z. Wu, J. Jie, and Y. Lu, "Quantum synchronization of a single trapped-ion qubit," *Physical Review Research*, vol. 5, no. 3, p. 033209, 2023.

[22] W. Kozlowski, F. Kuipers, R. Smets, and B. Turkovic, "Quip: A p4 quantum internet protocol prototyping framework," *IEEE Journal on Selected Areas in Communications*, 2024.

[23] Z. Han, C. Lyu, Y. Zhou, J. Yuan, J. Chu, W. Nuerbolati, H. Jia, L. Nie, W. Wei, Z. Yang, L. Zhang, Z. Zhang, C.-K. Hu, L. Hu, J. Li, D. Tan, A. Bayat, S. Liu, F. Yan, and D. Yu, "Multilevel variational spectroscopy using a programmable quantum simulator," *Phys. Rev. Res.*, vol. 6, p. 013015, Jan 2024. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevResearch.6.013015

[24] W. Kozlowski, F. A. Kuipers, R. Smets, and B. Turkovic, "Quip: A p4 quantum internet protocol prototyping framework," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 7, pp. 1936–1949, 2024.

[25] L. Chen, H.-X. Li, Y. Lu, C. W. Warren, C. J. Križan, S. Kosen, M. Rommel, S. Ahmed, A. Osman, J. Biznárová *et al.*, "Transmon qubit readout fidelity at the threshold for quantum error correction without a quantum-limited amplifier," *npj Quantum Information*, vol. 9, no. 1, p. 26, 2023.