An Improved Quantum Anonymous Notification Protocol for Quantum-Augmented Networks

Nitin Jha[1,*], **Abhishek Parakh**[1,+], **and Mahadevan Subramaniam**[2,+]

[1]Kennesaw State University, GA, USA
[2]University of Nebraska Omaha, NE, USA
[*]Corresponding author: njha1@students.kennesaw.edu
[+]This work is partly sponsored by NSF award #2324924 and #2324925.

ABSTRACT

The scalability of current quantum networks is limited due to noisy quantum components and high implementation costs, thereby limiting the security advantages that quantum networks provide over their classical counterparts. Quantum Augmented Networks (QuANets) address this by integrating quantum components in classical network infrastructure to improve robustness and end-to-end security. To enable such integration, Quantum Anonymous Notification (QAN) is a method to anonymously inform a receiver of an incoming quantum communication. Therefore, several quantum primitives will serve as core tools, namely, quantum voting, quantum anonymous protocols, quantum secret sharing, etc. However, all current quantum protocols can be compromised in the presence of several common channel noises. In this work, we propose an improved quantum anonymous notification (QAN) protocol that utilizes rotation operations on shared GHZ states to produce an anonymous notification in an n-user quantum-augmented network. We study the behavior of this modified QAN protocol under the dephasing noise model and observe stronger resilience to false notifications than earlier QAN approaches. The QAN framework is also proposed to be integrated with a machine-learning classifier, enhanced quantum-augmented network. Finally, we discuss how this notification layer integrates with QuANets so that receivers can allow switch-bypass handling of quantum payloads, reducing header-based information leakage and vulnerability to targeted interference at compromised switches.

Please note: Abbreviations should be introduced at the first mention in the main text – no abbreviations lists. Suggested structure of main text (not enforced) is provided below.

1 Introduction

Quantum Communication is one of the key aspects of the quantum internet, similar to how communication is an integral part of the current age internet. Current age quantum internet research faces several scalability issues similar to early models of the internet. Other than scalability issues, the practical realization of quantum protocols has always faced several hardware issues. All the initial work regarding quantum key distribution (QKD) protocols, such as BB84[1], B92[2], etc., is based on ideal single-photon sources. However, in practice, ideal single-photon sources are not practical. This has been worked out by using other imperfect single-photon sources, such as heralded spontaneous parametric down-conversion (SPDC), to simulate single-photon sources.[3] Several works pointed out the usefulness of the multiphoton approach as a possible solution to several challenges associated with single photon sources.[4,5] Multi-photon QKD protocols have been studied as a possible solution to several noises, such as decoherence, bit-flip, phase-flip, etc.[6] However, there is a problem associated with the multiphoton approach, namely higher risk of siphoning attacks, lesser key-rates due to increased occupancy of bandwidth (same number of bits have more corresponding qubits), etc. Therefore, we need to study other possible solutions to noise in quantum devices that can address both the security and scalability issues.

Quantum Augmented Networks (QuANets) is a recent development leading to scalable and practical idea of a global quantum internet. As the quantum components remain ridden by several noises such as *decoherence*, *attenuation*, etc., the scalability of purely quantum networks is severely limited. These noises reduce the fidelity of the quantum states over large distances. The preliminary model of QuANet used in this paper was proposed by the authors in[7]. Figure. (1) describes the working of this model. It consists of three stages as explained in[8]: (1) ML classifier assigns a privacy label to each message, determining if there's any private content, (2) the message is selectively encrypted using quantum encryption if it has any private content, (3) transmitting the message packet, and then reaching their destinations. The outgoing packet in this method consists of the following parts: (1) Headers: considers information regarding classical or quantum encryption, addresses, etc., and (2) Payloads: quantum-encrypted or classical-encrypted payload. There are certain core vulnerabilities of this approach, especially in the case of networks having compromised switches.

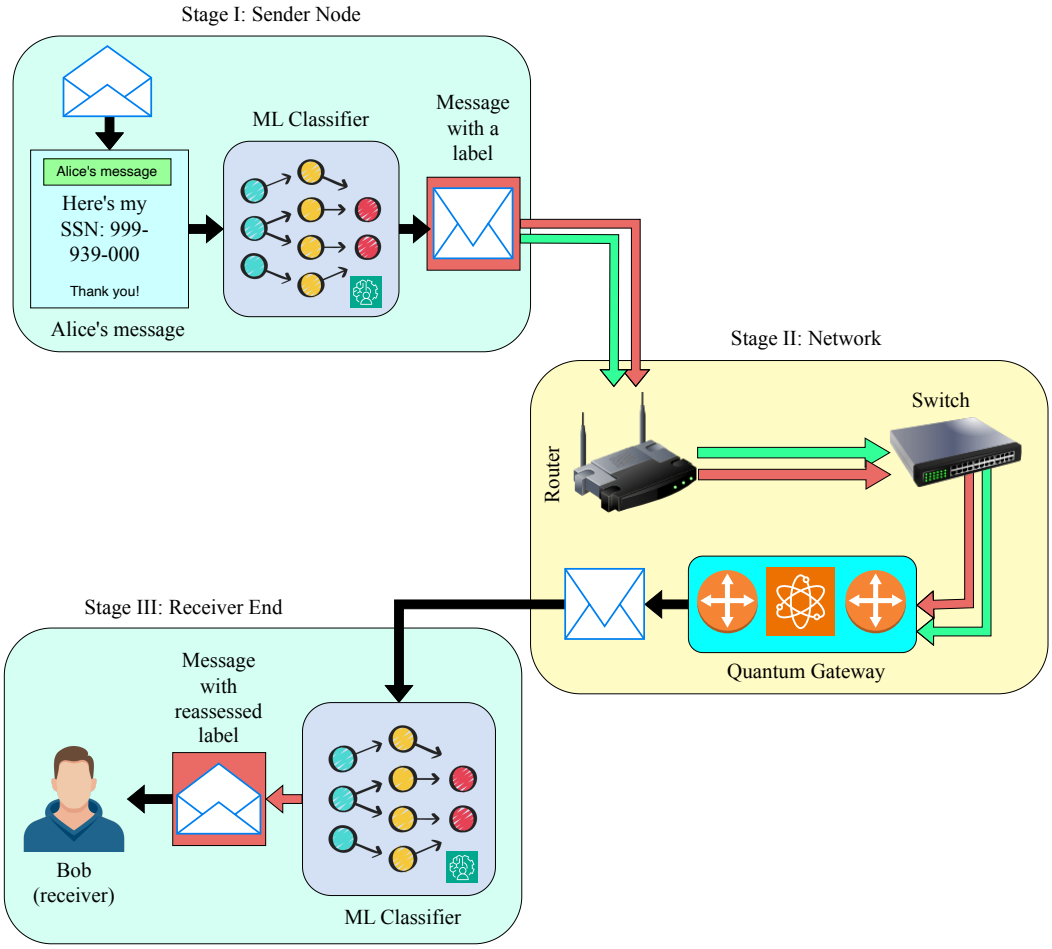

Figure 1. One vision of quantum augmented network, as presented in[7]. The work presents the idea of using machine learning algorithms to selectively classify communication messages in "private" and "non-private" classes. This allows us to only use quantum encryption for private classes and save resources for non-private messages. In the diagram, the **red** arrow indicates the flow of private/quantum-encryption information, and the **green** arrow indicates the flow of non-private/classical encrypted information.

A critical vulnerability in this QuANet arises from the possibility of compromised switches. In a practical network, we have to assume the presence of several compromised switches and limited trusted ones. Considering the above model of QuANet, we consider the class of attacks performed by compromised switches. For example, if we include information about a packet header containing quantum payload, then an attacker can use this information to flag packets having sensitive information, leading to traffic inference attacks. An adversary can selectively attack packets that have a quantum payload by either delaying or dropping them. There can also be several attacks based on network monitoring rather than active attacks. Therefore, the practical realization of QuANets depends not only on the robust quantum encryption techniques but also on mitigating several network-level attacks as mentioned above.

1.1 Related Works

Based on above mentioned issues, we introduce the use of the quantum anonymous notification (QAN) protocol as an extra layer in the quantum augmented network framework. A general QAN protocol allows a user in the network to anonymously notify any other user in the network using pairs of pre-shared GHZ states[9]. Several earlier works explores the quantum anonymous notification (QAN) protocols from both theoretical and experimental perspective[9–11].

The work by Khan et al., proposed one of the popular formalizations of QAN, relying on GHZ correlations to establish sender anonymity while ensuring message delivery[9]. However, these early approaches were primarily theoretical and did not account for realistic imperfections in the physical layer, such as photon loss, depolarizing noise, or detector inefficiencies. Several subsequent work aim to address these issues to enhance scalability and practicality. For instance, de Jong et al., and

Ruckle et al., demonstrated anonymous conference key agreement schemes using linear cluster states, paving the way for multi-party anonymous communication channels[11,12]. Similarly, Yang et al., introduced anonymous quantum transmission mechanisms that rely on EPR-based entanglement distribution, enabling message transfer without revealing sender or receiver identities[13].

Furthermore, Zheng et al., investigated collision detection in multi-user networks by leveraging higher-partite entangled states, highlighting how quantum resources can enable contention-free medium access in anonymous communication settings[14]. Large-scale feasibility has also been demonstrated in city-scale experiments involving up to eight users, showing the potential of GHZ and cluster-state-based architectures for practical anonymous communication by Huang et al[15]. Some other works such as by Unnikrishnan et al. proposed one of the first realistic implementations of anonymous quantum communication under noise, showing how anonymity can be preserved even with imperfect entanglement[16]. Gong et al. presented a W-state-based anonymous communication framework that incorporates both notification and collision detection sub-protocols, directly aligning with the goals of QAN systems[17].

Despite these advances, existing QAN protocols often overlook the impact of environmental noise and decoherence, which can significantly degrade entanglement fidelity and, consequently, the reliability of anonymity verification. In this work, we propose an improved QAN protocol that uses rotation operations to introduce a phase change that results in a parity flip after measurement by the receiver. This modified QAN protocol shows a lower probability of false notifications in the case of channel noise. The following are the main contributions of this work:

1. The QAN protocol has been studied under two types of dephasing noise models, while providing anonymity to both the user and the receiver.
2. The integration mechanism with QuANet is presented.
3. This integration addresses a key vulnerability: context-bearing headers that reveal the presence of quantum payloads and enable targeted interference. This integration makes “switch independence" possible, where the receiver can allow for a switch-bypass in case of an anonymous notification. This reduces contextual leakage at compromised switches, limits possible adversarial traffic selection, and preserves end-point anonymity.

This paper is structured as follows. Sec 2 defines the quantum anonymous protocol and provides a test case showing the working of this protocol. In this section, we also present simulation results for the working of the QAN protocol, a comparison of the accuracy of our improved QAN protocol with older approaches under noise models, and analyze two possible attacks on this system. Sec 4.1 integrates the idea of quantum augmented networks with the use of quantum anonymous protocol, providing a foundation for future work on integrating these ideas into a full communication stack.

2 Methods

2.1 The Quantum Anonymous Notification Protocol

There are several approaches to quantum networks which are based on quantum voting[18–20], quantum secret sharing[21–23], quantum conference agreement[24,25], etc. Early works regarding the quantum internet[26] were based on the ideas mentioned above. One key aspect of any communication network is preserving the privacy of the involved users. Therefore, even in the case of quantum internet, we need to utilize different privacy-preserving techniques to guarantee private communications. A Quantum Anonymous Notification protocol allows a sender to notify the intended receiver of an incoming communication while preserving the identity of the involved parties. Earlier works on QAN focus mainly on preserving the identity of either the receiver or the sender; however, we propose a modified QAN protocol that preserves the identity of both users.

In an earlier work[9], the authors propose an anonymous quantum private comparison protocol in an n-node quantum network using quantum anonymous notification protocol (QAN). In this work, we modify the QAN protocol such that instead of using two unitary operations, we share parts of an angle (α) using secret sharing, and then use this to execute the QAN. The details of this modification is as follows,

Step 1: Distributing GHZ states.

We assume the network constitutes of n users $(1,2\cdots,n)$, and each party distributes one $n-$partite GHZ state among the n parties as follows,

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right). \tag{1}$$

They then send exactly one qubit to each of the other $(n-1)$ parties, along with the local index. Concretely, when party j sends a qubit to party i, they tagged as $\Phi_j^{-1}(i)$ of GHZ_j.”

Thus recipient i learns both

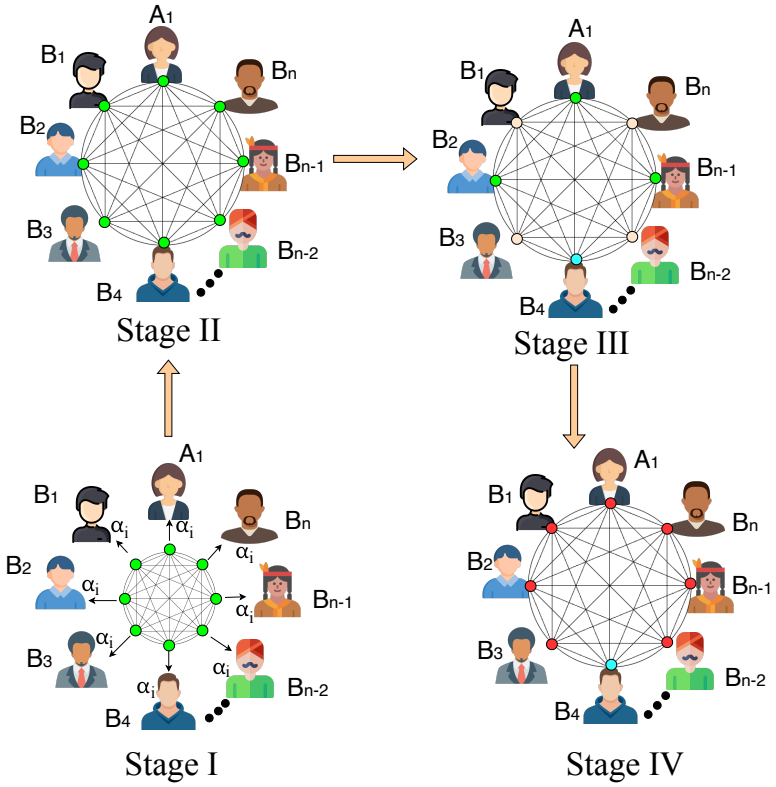

Figure 2. A schematic diagram representing different stages of the outlined QAN protocol. The diagram shows a network having n-users, A represents Alice, and all other nodes are marked $B_i \in [1,n]$, as each of them is equally likely to be the receiver of the notification by Alice. *Stage I* is distributing the secret share of the angle α, and the GHZ state. *Stage II* represents each node holding a state, and waiting to perform the relevant rotation operation. *Stage III* represents the execution of the QAN. Green nodes show the application of $R_z(\alpha')$, and yellow nodes show no rotation application. *Stage IV* is the final stage of the QAN protocol, where Bob's (receiver, marked by B_4) node is highlighted in blue, and every other node is marked by red. This signifies that Bob identifies a notification upon doing the post-measurement parity calculation.

a. which GHZ state it came from (j), and

b. which position in that state they hold ($\Phi_j^{-1}(i)$),

without ever learning the full bijection Φ_j. We denote that qubit by q_j^i—the i^{th} user's share of $|\text{GHZ}_j\rangle$.

Step 2: Setting up distributed angle (α).

This is one of the most important steps towards the final execution of the QAN. For each GHZ state j, a global angle α_j is selected and split into secret shares using quantum secret sharing. Each party i receives a sub-share α_j^i such that,

$$\sum_{i=1}^{n} \alpha_j^i \equiv \alpha_j \mod 2\pi. \tag{2}$$

This ensures that no single party learns the complete value of any α_j.

Step 3: Applying rotation operator to the qubit.

Each party i applies a local rotation $R_z(\alpha_j^i)$ to their qubit q_j^i in every GHZ state $j \in \{1,2,\ldots,n\}$.

$$R_z(\alpha_j^i) = e^{-i\alpha_j^i Z/2}. \tag{3}$$

However, if a party is the *notifier* (e.g., Alice) and wishes to notify an anonymous receiver associated with GHZ state index r, then for $j = r$ she modifies her rotation,

$$R_z(\alpha_r^i + \delta), \quad \text{with probability } P_z, \tag{4}$$

This phase shift, δ, allows for a change in the parity for the receiver (r) to detect a notification, while still preserving the anonymity of the notifier.

Step 4: Applying Hadamard gate and performing measurement. After applying the Hadamard H to each qubit q_j^i and measuring in the computational basis to obtain bits

$$\{m_j^i \mid j = 1, \ldots, n\} \tag{5}$$

user i takes all n bits (including m_i^i) and applies a private random permutation π_i before broadcasting. In other words, they broadcast

$$\{m^i_{\pi_i(1)},\, m^i_{\pi_i(2)},\, \ldots,\, m^i_{\pi_i(n)}\} \tag{6}$$

so that no one—neither other users nor eavesdroppers—can tell which bit was the self-measurement bit for any particular user.

Step 5: Calculating post-measurement parity. Once every user has broadcast n permuted bits, each node collects the full multi-set of n^2 bits for GHZ_j. They then compute the global parity

$$m_j = \bigoplus_{i=1}^{n} m_j^i, \tag{7}$$

summing over all i (including the self-measurement bit). This ensures that the parity truly reflects all n measurement outcomes, so a flip in round j signals a notification for user j.

Step 6: Repetition of the method.

Each party checks the parity value m_j for each GHZ state. The intended receiver (Bob) would check his GHZ index and calculate m_r. If $m_r = 1$ in any round, Bob would conclude that he got a notification.

Figure. (2) presents a schematic representation of the working of the modified QAN protocol. The QAN protocol can broadly be divided into four stages as represented in the Figure. (2). In the previous approach of the QAN protocol (as in[9]), all the users in the network know the qubit index assigned to each user. However, distributing n, n-partite GHZ states with known qubit assignments compromises overall anonymity. To address this, we modify the approach such that each user distributes their own set of n n-partite GHZ states for which the user assignments are only known to the distributor. We show that this preserves the anonymity of both the sender and the receiver, even if we consider the network consisting of semi-honest parties.

1. Each user in the network shares one n-partite GHZ state, and for the GHZ state shared by user U_j, they know the indexing for each qubit and user in the network (as explained in next section).
2. The secret share of angle is only done once; this shall be used throughout all the GHZ states.
3. Now, if Alice wants to notify Bob in the network, she would use the n $n-$partite GHZ state shared by her, such that she knows which qubit corresponds to Bob. Every other user would operate on all the n $n-$partite GHZ states they own, except the one that they shared.
4. Everyone would measure all of these GHZ states, and finalize the QAN protocol.
5. Upon measurement and final XOR calculation, Bob would find a notification from the state Alice shared, and nothing from the other states.

2.2 Example Case: 3-User Network

We consider a basic network consisting of 3 users: Alice, Bob, and Charlie. The exact steps would be,

1. Each of them prepares and distributes a $3-$partite GHZ state,

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{8}$$

   - Alice distributes GHZ_A, Charlie gets one qubit, Bob gets one, and she keeps one herself.

- Bob distributes GHZ_B, sending qubits to Alice and Charlie.
- Charlie distributes GHZ_C, similarly sharing qubits.

Each of these users knows the qubit mapping for the GHZ state they shared. So, for GHZ_A *only Alice* knows the mapping,

$$\text{index } 0 \rightarrow \text{Alice}, \quad \text{index } 1 \rightarrow \text{Bob}, \quad \text{index } 2 \rightarrow \text{Charlie} \tag{9}$$

2. If *Alice* wants to inform *Bob*: she uses GHZ_A, i.e., the GHZ state she prepared, and applies the modified rotation $R_z(\alpha_j + \delta)$ with probability P_z for the index corresponding to Bob. For the other two GHZ states, GHZ_B and GHZ_C, Alice applies just the normal rotation ($R_z(\alpha_j)$).
3. Bob and Charlie perform similar rotation ($R_z(\alpha_j)$) except the one they created, i.e., Bob does not do anything with GHZ_B and Charlie does not do anything with GHZ_C.
4. Hadamard operation and measurement. Each party does the following,
   - Applies Hadamard H to all GHZ qubits they own.
   - Measures them on a computational basis.
   - Publicly shares measurement outcomes.
5. For each GHZ state, the parity is computed:

$$m_j = m_j^A \oplus m_j^B \oplus m_j^C \tag{10}$$

   where m_j^X is the measurement bit from user X on GHZ_j.
6. Bob gets the notification. Bob measures the parity from all the GHZ states he received, i.e., from Alice and Charlie. He should see a notification from one of the GHZ states that he received.

This example can be extended to n-user network, and the generalized protocol as presented in *Algorithm 1*.

3 Results

In this section, we present the simulation results based on Algorithm 1, with specific parameters presented in the Table. 1 along with the noise models used, and some possible attacks on the modified QAN system. Before presenting the simulation outcomes, we briefly discuss the theoretical basis underlying the expected results. The notification detection process in the QAN protocol depends on the interference of shared GHZ states, where local phase rotations determine whether the receiver observes a parity flip. Channel noise, modeled through dephasing and depolarizing effects, reduces the coherence of these GHZ states and thereby lowers the contrast between notification and no-notification cases. The performance of GHZ-based communication schemes is strongly influenced by the fidelity and coherence of the entangled states used, as discussed in earlier works on noisy multipartite entanglement and quantum communication[27] As coherence decreases, the overall probability of successful notification detection is expected to drop, while false-positive events become more likely. The following section presents simulation results that illustrate these effects and highlight the improved robustness of the modified QAN protocol compared to a prior approach.

3.1 Simulation Results

For simulation, we focus on the GHZ state shared by the notifier, Alice, in an $n = 4$ network. Through these simulations, we present the performance of our proposed QAN protocol, and the comparison of the modified QAN protocol to the protocol presented in[9]. Through the simulations, we present the performance of the modified QAN protocol (in Figure. (3)), and the performance comparison of the modified QAN protocol with respect to the original QAN protocol under depolarizing noise models (in Figure. (5)). The other simulation parameters are as follows,

Figure. (3) shows the curves for 3 different values of P_z for increasing number of K. In this figure, we have plotted the probability of a notification detected by the intended receiver when the sender applied the rotation for receiver index qubit with a probability of P_Z, plotted against the number of repetitions of QAN rounds, K.

Algorithm 1 Modified n-user Distributed QAN

procedure QAN_PROTOCOL(n, u, r, $\{|\mathrm{GHZ}_j\rangle\}_{j=1}^{n}$, $\{\alpha_j^{(i)}\}_{i=1}^{n}$, P_z) ▷ u is the notifier's user index, r is the GHZ index to notify.
  for each user $i = 1,\ldots,n$ **do** ▷ Rotation phase
    for each GHZ index $j = 1,\ldots,n$ **do**
      if $i = j$ **then**
        continue ▷ Skip your own GHZ
      else if $i = u$ and $j = r$ **then** ▷ Notifier injecting notification
        With probability P_z: apply $R_z\left(\alpha_j^{(i)} + \pi\right)$
        With probability $1 - P_z$: apply $R_z\left(\alpha_j^{(i)}\right)$
      else ▷ All other cases
        Apply $R_z\left(\alpha_j^{(i)}\right)$
      end if
    end for
  end for

  ▷ Hadamard, measurement, and broadcast
  for each user $i = 1,\ldots,n$ **do**
    Apply Hadamard H to each qubit q_j^i
    Measure to get bits $\{m_j^{(i)}\}_{j=1}^{n}$
    Broadcast all $m_j^{(i)}$ for which $j \neq i$
  end for

  ▷ Parity computation and local notification check
  for each GHZ index $j = 1,\ldots,n$ **do**
    Compute $m_j = \bigoplus_{i=1}^{n} m_j^{(i)}$
    Let $v = \Phi_j(r)$ be the receiver slot for GHZ_j
    if $m_j = 1$ and current user $i = v$ **then**
      User v concludes "Notification received."
    end if
  end for
end procedure

Table 1. Simulation parameters

Parameter	Value(s)	Notes
Secret angle shares (α_i)	$0\ \forall\ i$	No net pre-rotation on the initial state; sets baseline phase to zero.
Number of users (n)	4	Network of four parties.
Notification phase kick (δ)	π	Additional probabilistic rotation applied at the receiver index ($j = r$).
Rounds per experiment (K)	$[1,9]$	Used to observe how detection probability accumulates with repetitions.
Notifier actuation probability (P_z)	$[0.1,\ 0.3,\ 0.45]$	Probability that the notifier applies $\alpha' = \alpha + \delta$ on the receiver's index in a round.

From the Figure. (3), We notice that for the increased value of the probability of rotation application, the detection of notification by the receiving party improves significantly. We notice that we can find a middle-ground between increasing N values and P_z values to optimize the overall notification detection probability. Figure (4) illustrates that the QAN protocol preserves user anonymity. The $x-$axis shows the flipper index, i.e., the qubit index for possible notifier or receiver. The $y-$axis shows the outcome index, which shows the combined bit-string obtained by measuring the GHZ state, and the $z-$axis presents the probability of different outcome strings when measured by different flipper indices (i.e., users). The protocol achieves a high notification detection rate across various P_Z and K values while maintaining notifier anonymity, as shown in the figures mentioned above.

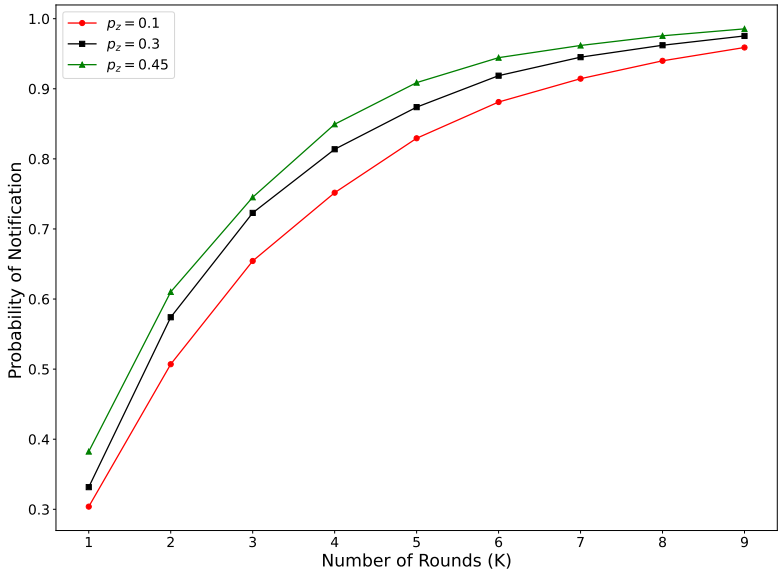

Figure 3. Simulation results for QAN protocol outlined in Sec[2] for detection probability of notification received for increasing number of runs for different values of P_z, i.e., probability of application of the rotation operator by the notifier for the receiver index.

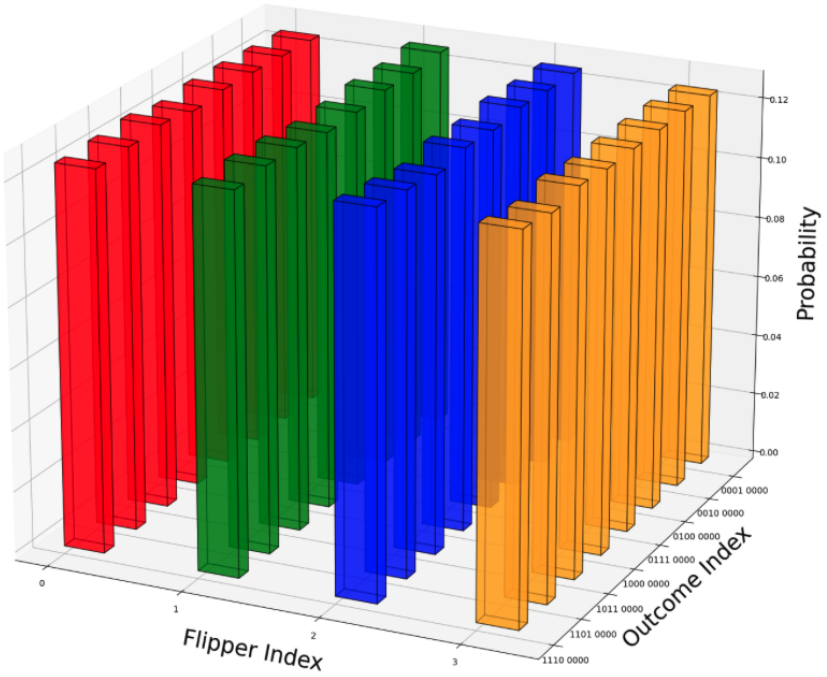

Figure 4. The probability distribution of different states in the QAN protocol shows a uniform distribution. It, thus, preserves the anonymity of the notifier. Here, we plotted the probability distribution of various strings averaged over 1000 simulation runs.

3.2 Noise Integration

To study the extent of the effectiveness of the protocol, we introduce depolarizing noise models and present the comparison of the false-positive notification detection in our modified QAN approach (using rotation operators) vs the QAN protocol

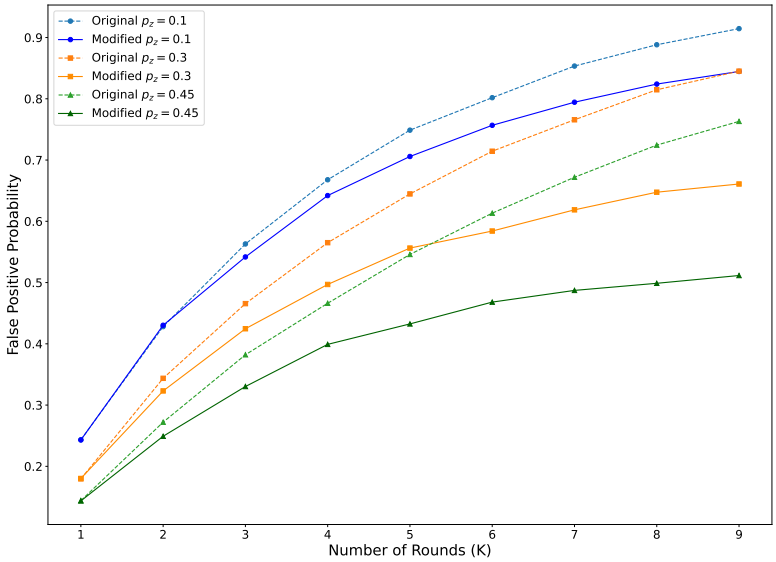

Figure 5. This figure shows the false positive rate of notification detection in the presence of noise models mentioned above for the modified QAN protocol proposed in this work, compared to the QAN presented by Khan et al.[9]. The false positive rate is calculated as any notification detected by an unintended party, as a result of different noise models present in the network.

presented in[9]. Dephasing noise model is explored because it sets the detection gap and therefore how many rounds are needed for reliable detection on real links. For this simulation, we used the following noise model,

1. *Single qubit Depolarizing noise*:

   For a single qubit gate, $G \in \{H, U, Z\}$, (U is a possible unitary matrix operator, such as a rotation operator) is applied as,

   $$\mathscr{E}_{\text{single}}(\rho) = (1-p)\rho + \frac{p}{3}\left(X\rho X^\dagger + Y\rho Y^\dagger + Z\rho Z^\dagger\right), \tag{11}$$

   where,

   - ρ is the density matrix of the quantum state
   - p is the probability of depolarizing noise channel being applied (for simulation we used $p = 0.01$)
   - X, Y, Z are Pauli's matrices

2. *Two-qubit Depolarizing noise*:

   For the controlled-X (CX) gate, a two-qubit depolarizing channel is applied as,

   $$\mathscr{E}_{\text{two}}(\rho) = (1-p)\rho + \frac{p}{15}\sum_{i=1}^{15} P_i \rho P_i^\dagger, \tag{12}$$

   where,

   - ρ is the density matrix of the quantum state
   - p is the probability of depolarizing noise channel being applied (for simulation we used $p = 0.02$)
   - P_i are the 15 non-identity two-qubit Pauli operators ($X \otimes Y$, $Z \otimes X$, $X \otimes I$, etc.)

3.3 Attacks

The anonymity of the users participating in the QAN protocol mentioned in the above section can be analyzed for some attacks where we consider semi-honest participants and compromised users. Here, we show that even if we consider all the users in the network to be semi-honest, the anonymity of any sender and receiver is preserved.

3.3.1 Assuming Semi-Honest Parties

We assume the set of users to be $u = \{1, 2, 3, \ldots, n\}$. For each user j, we consider a $n-$partite GHZ state represented as follows,

$$|\text{GHZ}_j\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right), \tag{13}$$

which is prepared and distributed by user j. The user j has an associated secret mapping Φ_j which lets them know which qubit belongs to which user in the system. This can be written as,

$$\Phi_j : \{1, 2, \ldots, n\} \rightarrow u. \tag{14}$$

This shows the mapping (bijective mapping) of each qubit in $|GHZ_j\rangle$ belongs to one user. This mapping, as mentioned, is only known to the distributor, j.

Now, we consider a general notifier, u, and a general receiver, v. The user u will use $|GHZ_u\rangle$, i.e., the state they distributed. For the secret mapping, Φ_u, there exists a unique index, r, such that,

$$\Phi_u(r) = v. \tag{15}$$

During the QAN stage, every party modifies its qubit by applying a rotation operator ($R_z(\alpha_j)$), where α_j is the secret share of angle distributed to each user in the network. However, the notifier u modifies the rotation on her qubit in position r by applying a rotation of ($R_z(\alpha_j + \delta)$) with probability of P_z. All other parties, upon receiving their qubits from $|GHZ_u\rangle$ apply the standard $R_z(\alpha_j)$.

After the Hadamard gate application, and measurement is done (in computational basis), all parties declare the result for i^{th} qubit, i.e., every other qubit except their index. Let m^i be the measurement outcome for i^{th} qubit, so the global parity is defined as,

$$m = \oplus_{i=1}^{n} m^i. \tag{16}$$

In an ideal no-noise scenario, for the no-notification case $m = 0$, with a high probability. However, for a case when notifier u wants to notify v, the m changes to 1 with some probability. Crucial thing to note here is that only the receiver v can identify the parity change for the j^{th} qubit associated with them. Even if we consider semi-honest users, i.e., they try to gain information from publicly shared data, they are not able to identify any local parity change– which only v can calculate.

3.3.2 Compromised User

If we consider a network with m compromised users, such that $m \leq n/2$. We consider one of the compromised users to be $\mathscr{C}$. A similar argument can be used to show that the anonymity of the sender and receiver is preserved, unless the compromised party is the sender. However, even in this case, where $\mathscr{C}$ is the sender, the only information she can gain by publication announcement is the index of the receiver. However, since for each user there exists a different secret mapping defined by them, no further information can be gained by outsiders, even if half of the users in the system are compromised.

However, if we consider a system with a large number of compromised users, it can cause some issues with the overall working of the system. Since, QAN step comes before transmission of an actual quantum-encrypted message, a compromised node can apply random rotations to random indices to disrupt the overall parity of the system. Thus, this particular disruption needs to be taken care of in the long run for practical deployments.

In practical hardware implementations, the fidelity of shared GHZ states may not remain ideal due to gate errors, loss, and decoherence. A small drop in the initial fidelity would slightly lower the contrast between the notification and no-notification cases. This means the detection probability decreases marginally, while the false-positive rate shows a small increase. Although a detailed quantitative analysis is beyond the current scope, this trend follows the expected behavior of multipartite GHZ states under noise-heavy conditions and emphasizes the importance of maintaining high state-preparation fidelity for reliable network performance.

4 Discussions

The modified QAN protocol has been presented in this work, and the performance has been validated through several experiments, and security under several plausible attacks has also been studied. Now, we will discuss how this QAN protocol can be integrated with the QuANet framework, such that we can achieve some protection from compromised switches in a network by achieving switch-independence.

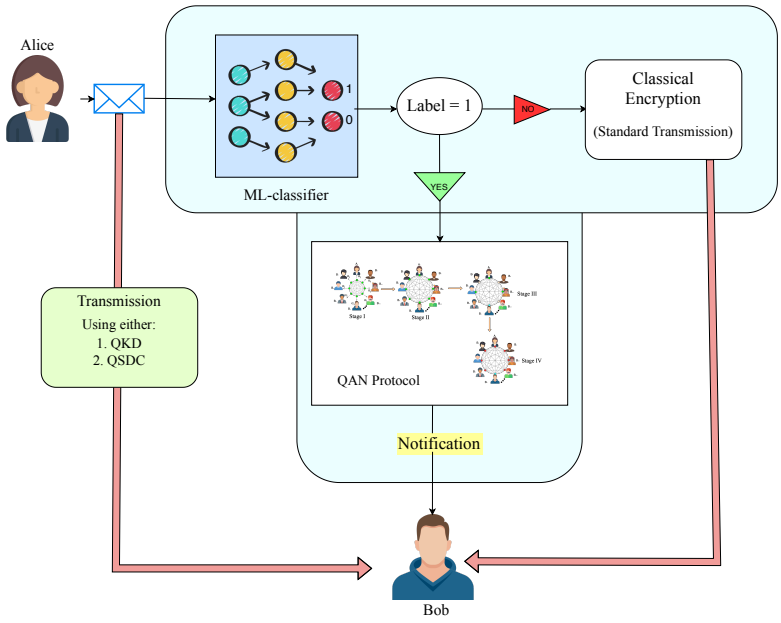

Figure 6. A schematic diagram of the combined protocol that integrates the QAN protocol into the idea of quantum augmented network presented in[7]. The diagram is divided into two parts: (1) the part outlined in *blue box* outlines the protocol that's executed before actual transmission, (2) the red arrows mark the transmission and encryption method. In the first half of the protocol, Alice gets a privacy label for her message, and based on that, she either initiates the QAN protocol or she uses classical encryption techniques (for example, AES, etc.) to transmit her message to Bob. Once QAN is performed (for private messages), we move on to the transmission phase. In this phase, if QAN was used, Alice and Bob either start a QKD run or Alice sends a packet with a quantum payload to Bob right after the notification.

4.1 Integrating QAN with the QuANet Framework

The integration of the QAN protocol with the quantum-augmented network (QuANet) protocol helps us address some of the key security weaknesses of the QuANet structure. The QuANet framework presented in[8] uses machine-learning classifiers to assign a privacy label to each outgoing communication. If a communication contains some private content, then quantum encryption is used to transmit it securely over the network. This quantum-encrypted payload is sent in a packet with quantum and classical headers as outlined in[7]. However, having such packets flagged as "quantum encrypted" can have security concerns if switches are compromised. A high-level schematic diagram for the protocol is also presented as a Figure. (6) The three main steps of this integration are as follows:

1. ML-Based Privacy classifier: determines if a message contains any private content. The definition of "privacy" is user dependent, for example, personal identifiers, medical and financial identifiers, etc.

2. Quantum Anonymous Notification Protocol: If any message is classified to have private content, this should be triggered by the sender (referred to as Alice across this work). The receiver (Bob) should receive a notification.

3. The receiver (Bob) informs the switch to bypass incoming packets directly to the quantum gateway, where the quantum payload can be processed. This avoids the switch to interact with the packet, such as interacting with the packet header.

The integration of the QAN protocol with the QuANet framework is formally presented in *Algorithm 2*. The protocol begins with an ML-based decision procedure that evaluates the privacy level of a composed message M. If the message is classified as non-private (L=0), classical encryption is applied before transmission. Otherwise, if the message is deemed private (L=1), the Quantum Anonymous Notification (QAN) protocol is invoked.

By using this integrated approach to a quantum augmented network, the protocol achieves *switch independence*, which is particularly beneficial in the case where there are compromised switches in the system. This also allows us to remove any information from the packet headers that identifies any packets with private contents, i.e., quantum-encrypted payload. This would help us reduce any directed attacks that can be performed by the adversaries as a result of these compromised switches in the network.

Algorithm 2 Integrated Protocol

procedure ML-BASED DECISION
  Compose message M.
  $L \leftarrow \mathrm{ML}(M)$ ▷ $L = 0$: non-private; $L = 1$: private.
  if $L = 0$ **then**
    Apply classical encryption to M.
    Transmit M.
    return .
  else
    Proceed to QAN protocol.
  end if
end procedure
procedure QUANTUM ANONYMOUS NOTIFICATION
  Assumption: GHZ states are pre-distributed.
  Alice triggers QAN to notify Bob.
  QAN is executed by the network.
end procedure
procedure SWITCH BYPASS ACTIVATION
  Route subsequent packets directly to the quantum gateway.
end procedure
procedure PACKET ARRIVAL
  Packet with quantum payload arrives at the quantum gateway
  Decryption and Measurement Done
end procedure

4.2 Conclusion

In this work, we presented an improved Quantum Anonymous Notification (QAN) protocol that can be easily integrated with a Quantum-Augmented Network (QuANet) framework. The proposed QAN protocol uses quantum secret sharing to establish a secret share of the angle that every user in the system holds, which is then modified by any sender to anonymously notify the receiver using pre-shared GHZ states. The integration of QAN with the QuANet framework allows us to modify the pre-proposed structure of message packets, such as headers, payload, etc. The header information from these packets can be exploited by compromised switches to gain some contextual information, as this framework uses selective quantum encryption for messages containing private information. The adversaries can thus use such information to either delay or drop these packets at these compromised switches. Use of QAN before actual transmission would allow the receivers to bypass incoming messages from the switches, and also help in reducing the information that is provided in the headers. This is what we like to refer to as *switch independence*.

The simulation results as shown in the Figure. (3) and Figure. (4) shows that the QAN protocol achieves decent notification-detection probability even for smaller rounds (K). We also present a comparison of the working of our QAN protocol to one of the earlier defined approaches under a couple of noise models. From the Figure. (5), we can see that the false-positive rate for notification detection is significantly different (about 10% for any $K \geq 3$) for our approach vs the older one. We also present an analysis for two possible attack scenarios for our QAN protocol, and show that the anonymity of the sender-receiver pair is maintained even in the case of all users being semi-honest, or users in the system being compromised. Future works can focus on active attacks, such as rotation poisoning or targeted $Z-$gate attacks. For example, we consider the case of the last-speaker steering attack. Here, an adversary holds on till they can see others' broadcasts and then chooses their bit to cause the final parity changes. These attacks can be further avoided by providing each party with certifications and signatures to avoid this class of attacks. If we consider the case of a rotation poisoning attack by a single compromised node that slightly perturbs its local rotation each round, we notice that the shared GHZ coherence degrades, false notify events become more likely, true notifications are harder to confirm, and convergence slows as the network size grows. A simple mitigation is to randomize local bases across rounds, watch for sudden drops in measured coherence, and aggregate a few rounds by majority vote so one misbehaving node cannot drive the outcome.

These modification to the QuANet architecture not only increases the overall security of the system, but also provide us with a scalable and more robust framework than the stand-alone QuANet framework. The future work can look at network simulation for this work to gain more insights about possible bottlenecks and shortcomings in a fully-fledged network scenario. There are, however, some limitations of this work that needs to be further studied in upcoming studies such as the analysis of fidelity

of sharing GHZ states under noise-heavy hardware, a more thorough analysis of the performance of switch-independence in different network configurations, and thus, development of any further protocols which can streamline the integration of our QAN protocols with other quantum secure direct communication (QSDC) protocols necessary for quantum secure communication[28,29]. In addition to this, the modified QAN can be used in the development of quantum augmented microgrid structures, where we integrate the use of quantum components such as quantum key distribution, quantum anonymous notification, and quantum random number generation to develop a secure quantum-augmented microgrid.

Authors Contributions

N.J. is the primary author of the manuscript and received intellectual inputs from A.P. and M.S. to guide the research. All authors edited the manuscript.

Data availability statement

All data generated or analysed during this study are included in this published article [and its supplementary information files].

Additional Information (Competing Interests)

None

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (1984).
2. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. review letters* **68**, 3121 (1992).
3. Yuan, X., Zhang, Z., Lütkenhaus, N. & Ma, X. Simulating single photons with realistic photon sources. *Phys. Rev. A* **94**, 062305 (2016).
4. Burr, J., Parakh, A. & Subramaniam, M. Evaluating different topologies for multi-photon quantum key distribution. In *Quantum Information Science, Sensing, and Computation XIV*, vol. 12093, 60–75 (SPIE, 2022).
5. Pont, M. *Multi-photon quantum interference and entanglement*. Ph.D. thesis, Université Paris-Saclay (2023).
6. Jha, N., Parakh, A. & Subramaniam, M. Effect of noise and topologies on multi-photon quantum protocols. In *Quantum computing, communication, and simulation IV*, vol. 12911, 148–161 (SPIE, 2024).
7. Jha, N., Parakh, A. & Subramanian, M. A ml based approach to quantum augmented http protocol. In *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, vol. 2, 591–592 (IEEE, 2024).
8. Jha, N., Parakh, A. & Subramaniam, M. Towards a quantum-classical augmented network. In *Quantum Computing, Communication, and Simulation V*, vol. 13391, 72–86 (SPIE, 2025).
9. Khan, A., Shin, H. *et al.* Quantum anonymity for quantum networks. *arXiv preprint arXiv:2007.11176* (2020).
10. Zheng, W. & Gong, B. Anonymous notification in practical quantum networks. In *2024 43rd Chinese Control Conference (CCC)*, 9017–9021 (IEEE, 2024).
11. de Jong, J., Hahn, F., Eisert, J., Walk, N. & Pappa, A. Anonymous conference key agreement in linear quantum networks. *Quantum* **7**, 1117 (2023).
12. Rückle, L. *et al.* Experimental anonymous conference key agreement using linear cluster states. *Phys. Rev. Res.* **5**, 033222 (2023).
13. Yang, Y.-G. *et al.* Towards practical anonymous quantum communication: A measurement-device-independent approach. *Phys. Rev. A* **104**, 052415 (2021).
14. Zheng, W. & Gong, B. Anonymous collision detection for practical quantum networks. *Phys. Lett. A* **525**, 129854 (2024).
15. Huang, Z. *et al.* Experimental implementation of secure anonymous protocols on an eight-user quantum key distribution network. *npj quantum information* **8**, 25 (2022).
16. Unnikrishnan, A. *et al.* Anonymity for practical quantum networks. *Phys. review letters* **122**, 240501 (2019).
17. Gong, B., Gao, F. & Cui, W. Anonymous communication protocol over quantum networks. *Quantum Inf. Process.* **21**, 99 (2022).

18. Vaccaro, J. A., Spring, J. & Chefles, A. Quantum protocols for anonymous voting and surveying. *Phys. Rev. A- At. Mol. Opt. Phys.* **75**, 012333 (2007).

19. Li, Y.-R., Jiang, D.-H., Zhang, Y.-H. & Liang, X.-Q. A quantum voting protocol using single-particle states. *Quantum information processing* **20**, 1–17 (2021).

20. Arapinis, M., Lamprou, N., Kashefi, E. & Pappa, A. Definitions and security of quantum electronic voting. *ACM Transactions on Quantum Comput.* **2**, 1–33 (2021).

21. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).

22. Gottesman, D. Theory of quantum secret sharing. *Phys. Rev. A* **61**, 042311 (2000).

23. Senthoor, K. & Sarvepalli, P. K. Theory of communication efficient quantum secret sharing. *IEEE Transactions on Inf. Theory* **68**, 3164–3186 (2022).

24. Murta, G., Grasselli, F., Kampermann, H. & Bruß, D. Quantum conference key agreement: A review. *Adv. Quantum Technol.* **3**, 2000025 (2020).

25. Pickston, A. *et al.* Conference key agreement in a quantum network. *npj Quantum Inf.* **9**, 82 (2023).

26. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).

27. Guo, Y. & Yang, S. Noise effects on purity and quantum entanglement in terms of physical implementability. *npj Quantum Inf.* **9**, 11 (2023).

28. Sun, Z.-Z. *et al.* Quantum communication network routing with circuit and packet switching strategies. *IEEE J. on Sel. Areas Commun.* (2025).

29. Zou, X. & Qiu, D. Three-step semiquantum secure direct communication protocol. *Sci. China Physics, Mech. & Astron.* **57**, 1696–1702 (2014).

30. Azuma, K. *et al.* Quantum repeaters: From quantum networks to the quantum internet. *Rev. Mod. Phys.* **95**, 045006 (2023).

31. Elliott, C. The darpa quantum network. In *Quantum Communications and cryptography*, 91–110 (CRC Press, 2018).

32. Sasaki, M. *et al.* Field test of quantum key distribution in the tokyo qkd network. *Opt. express* **19**, 10387–10409 (2011).

33. Peev, M. *et al.* The secoqc quantum key distribution network in vienna. *New journal physics* **11**, 075001 (2009).

34. Ribezzo, D. *et al.* Deploying an inter-european quantum network. *Adv. Quantum Technol.* **6**, 2200061 (2023).

35. Kak, S. A three-stage quantum cryptography protocol. *Foundations Phys. Lett.* **19**, 293–296 (2006).

36. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. review letters* **85**, 441 (2000).

37. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without bell's theorem. *Phys. review letters* **68**, 557 (1992).