Implementation of a Quantum Authentication Protocol Using Single Photons in Deployed Fiber

Changho Hong *, Youn-Chang Jeong, Se-Wan Ji

Posted Date: 27 February 2026

doi: 10.20944/preprints202602.1334.v1

Keywords: quantum communication; quantum network; quantum authentication

 doi:10.20944/preprints202602.1334.v1

Article

Implementation of a Quantum Authentication Protocol Using Single Photons in Deployed Fiber

Changho Hong *, Youn-Chang Jeong and Se-Wan Ji

The affiliated institute of ETRI, Yuseong-daero 1559, Yuseong-gu, Daejeon, 34044, South Korea

* Correspondence: hchc11@nsr.re.kr; Tel.: +82-42-870-4967

Abstract

With the increasing importance of securing quantum communication networks, practical and robust entity authentication is a critical requirement. Accordingly, we propose and experimentally validate a quantum entity authentication protocol specifically designed for integration with BB84-type QKD workflows and existing terminal architectures. We analyze the protocol's security against intercept–resend man-in-the-middle impersonation, showing that an unauthenticated adversary induces a characteristic 25% correlation error and that the rejection probability approaches unity as the number of detected authentication events increases. For practical realization, the protocol is deployed using weak coherent pulses with decoy-state estimation to bound single-photon contributions and mitigate photon-number-splitting–enabled leakage. The system is demonstrated over a field-deployed fiber link of approximately 20 km with ~8 dB optical loss using signal/decoy intensities of ~0.5/~0.15 and sending probabilities 0.88/0.10/0.02 (signal/decoy/vacuum). Across both verification directions, stable operation is observed with QBER typically fluctuating between 1% and 4% while the sifted key rate remains constant over time. These results provide an experimental basis for integrating physical-layer entity authentication into deployed quantum communication networks.

Keywords: quantum communication; quantum network; quantum authentication

1. Introduction

The proliferation of quantum information infrastructures has catalyzed the development of a global quantum internet, promising a paradigm shift in secure communication through the principles of quantum mechanics [1,2]. While Quantum Key Distribution (QKD) has reached a certain level of maturity, the overarching security of any quantum-cryptographic framework is fundamentally predicated on the robustness of entity authentication [3,4]. Without a rigorous mechanism to verify the legitimacy of communicating parties, even channels with information-theoretic security remain susceptible to man-in-the-middle (MitM) and impersonation attacks [5,6]. As the advent of fault-tolerant quantum computers threatens the computational hardness underlying classical public-key infrastructures (PKI), there is increasing interest in authentication protocols whose security is derived from the laws of physics [7,8].

In 2020, the U.S. National Security Agency (NSA) explicitly stated that QKD itself provides no mechanism to authenticate the source of a QKD transmission and that entity authentication therefore requires either asymmetric cryptography or preplaced keys [9]. This position clarifies that the practical vulnerabilities of QKD deployments may hinge on whether peer identity is assured, and it further implies that the overall security level of QKD-based communication systems is determined by the assumptions underpinning the authentication layer. Traditionally, QKD systems have relied on information-theoretic message authentication codes (MACs) based on universal hashing—most notably the Wegman–Carter family—seeded with a short pre-shared symmetric key [10]. The Wegman–Carter paradigm offers an "unconditional" authentication notion that statistically bounds forgery even against an adversary with unbounded computational power. Moreover, researchers have systematically examined the conditions and limitations for economizing and recycling

 doi:10.20944/preprints202602.1334.v1

authentication keys, supporting feasibility analyses in the QKD setting [11]. From the perspective of large-scale networking and scalability, however, pre-shared-key authentication entails bootstrap requirements as well as key distribution and management overhead. As a practical alternative, several studies have proposed and experimentally explored integrating PKI and post-quantum cryptography (PQC) into the authentication layer of QKD deployments [12]. PQC standardization has been pursued on the basis of mathematical problems believed to remain hard in the presence of quantum computing (e.g., structured lattices and hash-based constructions) [13]. This hybrid approach, which couples "computational authentication" with QKD, is often motivated as a means to ease near-term deployment while leveraging QKD-derived secrecy over longer horizons [12,14]. Yet, unlike QKD's physics-based or information-theoretic security narrative, this hybrid approach anchors the assurance of "who established the key with whom" in computational assumptions, potentially yielding a heterogeneous assurance profile across the system. Furthermore, given that the quantum threat to conventional public-key cryptography was catalyzed by polynomial-time quantum algorithms for factoring and discrete logarithms, designs that place the entire trust chain—including authentication—on computational premises may remain in tension with long-term security goals, particularly those requiring enduring confidentiality and sustained trustworthiness [7].

Against this backdrop, there is strong motivation to align the entity authentication required for QKD operation with its underlying security objectives, including strong adversarial models and physics-based guarantees. When the authentication layer relies on assumptions that diverge from those underlying QKD's security claim, the resulting end-to-end security argument can become fragmented [9,15,16]. In this sense, the proposed quantum entity authentication protocol strengthens end-to-end security in QKD-based communications by addressing, from a physics-based standpoint, the foundational question of "with whom the secret key is securely shared."

The theoretical landscape of quantum-based authentication was pioneered by Barnum et al., who established the foundational criteria for the non-malleability of quantum states [17]. While early research focused extensively on quantum message authentication (QMA), the conceptual framework has evolved toward quantum entity authentication (QEA) and identification [18,19]. In these schemes, the no-cloning theorem provides a physical guarantee that an adversary cannot replicate the "quantum credentials" or "unclonable tokens" assigned to a legitimate user [20,21]. Various identification protocols using entangled states or single-photon measurements have been proposed to ensure that identity verification does not leak information that could be exploited in subsequent sessions [22,23]. Recently, these frameworks have been further expanded to complex network environments, such as protocols for simultaneous multiparty authentication involving classical third parties [24].

Despite these theoretical advancements, a gap remains between idealized protocols and their physical realization in practical communication channels. A significant portion of existing experimental literature relies on Weak Coherent Pulses (WCP) as a surrogate for single photons [25,26]. However, the Poissonian photon-number distribution of WCPs introduces a critical vulnerability: the photon number splitting (PNS) attack, where an eavesdropper can intercept redundant photons to gain partial information about the user's identity without being detected [27,28]. Furthermore, environmental decoherence and channel attenuation in optical fibers or free-space links degrade the signal-to-noise ratio (SNR), often leading to an increase in false rejection rates (FRR) in real-world deployments [29,30].

This paper contributes to advancing the practical realization of quantum networks by implementing and experimentally validating a quantum authentication protocol in a deployed communication setting. Our protocol adopts a challenge–response architecture in which the user's identity is encoded in polarization degrees of freedom and is designed to be executable within the operational framework of BB84-type QKD without requiring changes to the overall system architecture. We provide an analysis of the authentication success rate and associated security bounds under realistic channel noise and detector inefficiencies. These results support the feasibility of integrating physical-layer authentication into next-generation quantum networks, so that user

 doi:10.20944/preprints202602.1334.v1

legitimacy can be verified under the same physics-based threat considerations that motivate quantum-secure communication [4,30].

From both security and engineering standpoints, the proposed protocol offers several practical advantages. First, it is designed as a lightweight, PSK-seeded challenge–response procedure that can be executed periodically or on an event-driven basis within a BB84-type QKD operation, enabling mutual entity authentication without requiring changes to the existing optical hardware or disrupting the QKD workflow. Second, because the measurement basis is implicitly determined by the shared PSK, a MitM adversary lacking the PSK is forced into basis guessing. This induces a characteristic correlation error and allows the verifier to drive the rejection probability arbitrarily close to unity by increasing the number of detected authentication events while tolerating the intrinsic channel QBER. Third, the protocol is deployment-oriented: although defined in a single-photon model, it remains compatible with practical WCP transmitters by adopting decoy-state estimation to bound single-photon contributions and suppress PNS-enabled information leakage, thereby retaining security guarantees comparable to idealized single-photon settings in realistic channels [25–28,31–34]. Finally, while our realization focuses on polarization encoding, the same protocol logic can be mapped to phase-based encodings commonly used in standard QKD terminals, supporting seamless integration as a physical-layer authentication function in future quantum communication infrastructures [35].

The remainder of this paper is organized as follows. Section 2 presents the protocol description and operational steps of the proposed quantum entity authentication method. Section 3 provides a security evaluation of the proposed protocol, including the analysis framework needed for practical implementations (e.g., bounds in the WCP/decoy-state setting). Section 4 reports on the experimental realization and observed performance metrics over a deployed fiber link. Finally, Section 5 concludes the paper and discusses implications for integrating physical-layer authentication into future quantum communication infrastructures.

2. Protocol Description

Entity authentication requires several preconditions. The proposed quantum entity authentication protocol is described under the following assumptions.

Pre-shared authentication key

Alice and Bob share a pre-distributed entity-authentication key, denoted by A_k, which is used as a pre-shared key (PSK).

State–bit mapping

Each symbol of the PSK is a two-bit string. For the i-th symbol $(A_k)^i \in \{00, 01, 10, 11\}$, the corresponding single-photon quantum state is chosen according to the BB84 state set

$$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\} \tag{1}$$

The mapping is defined as

$$\begin{aligned} |0\rangle &\rightleftarrows 00, \\ |1\rangle &\rightleftarrows 01, \\ |+\rangle &\rightleftarrows 10, \\ |-\rangle &\rightleftarrows 11. \end{aligned} \tag{2}$$

Each entity is assigned a unique authentication key, typically issued by a trusted authority. The entity identifier (ID) itself does not represent the PSK; rather, the PSK is a shared secret credential bound to that ID. The protocol is designed to execute either periodically or aperiodically, running concurrently with a BB84-type QKD protocol. We assume that a pre-agreed time or event triggers the authentication procedure; accordingly, this work focuses on the protocol's operational steps.

 doi:10.20944/preprints202602.1334.v1

Let $(A_k)^i = (b_i, v_i)$ denote the two bits of the i-th PSK symbol, where $b_i \in \{0,1\}$ is the first bit and $v_i \in \{0,1\}$ is the second bit.

Step 1. State preparation from PSK

Alice generates a single photon and prepares its quantum state according to the shared PSK:

$$|\psi_i\rangle = S((A_k)^i) \quad (3)$$

where $S(\cdot)$ is the mapping defined equation (2). For example, if $(A_k)^i = 10$, then $|\psi_i\rangle = |+\rangle$.

Step 2. Random nonce operation

Alice samples a random nonce bit $n_i \in \{0,1\}$ and applies

$$|\phi_i\rangle = N_i|\psi_i\rangle, \; N_i \in \{I, i\sigma_y\} \quad (4)$$

We interpret $n_i = 0$ as selecting $N_i = I$ and $n_i = 1$ as selecting $N_i = i\sigma_y$.

Step 3. Quantum transmission

Alice transmits the resulting single-photon state $|\phi_i\rangle$ to Bob over the quantum channel.

Step 4. Basis choice and measurement

Bob chooses a measurement basis (MB) according to the first bit b_i of $(A_k)^i$:

- If $b_i = 0$, Bob measures in the z-basis $\{|0\rangle, |1\rangle\}$.
- If $b_i = 1$, Bob measures in the x-basis $\{|+\rangle, |-\rangle\}$.

Bob stores his measurement outcome for each successfully detected photon.

If the channel were lossless and the nonce operation were not applied, Bob could directly confirm that the PSK A_k are deterministically recovered from his measurement outcomes. In practice, channel loss and the deliberate random nonce operation invalidate these simplifying assumptions.

The remaining steps depend on which party plays the verifier and which plays the prover.

Case a: Alice is the verifier and Bob is the prover

Step 5a. Bob reconstructs nonce bits

Using the stored measurement outcomes and A_k, Bob reconstructs the nonce bit values and announces them to Alice over the public (classical) channel.

A convenient way to express this reconstruction is as follows. Let $m_i \in \{0,1\}$ denote Bob's measurement result encoded as

- $m_i = 0$ for outcomes $|0\rangle$ (in z-basis) or $|+\rangle$ (in x-basis).
- $m_i = 1$ for outcomes $|1\rangle$ (in z-basis) or $|-\rangle$ (in x-basis).

From the action of N_i, in the ideal setting we have

$$m_i = v_i \oplus n_i \quad (5)$$

and Bob can compute

$$\hat{n}_i = m_i \oplus v_i \quad (6)$$

Step 6a. Alice verifies Bob

Alice compares Bob's announced nonce-bit sequence $\{\hat{n}_i\}$ with her locally chosen nonce bits $\{n_i\}$. If the correlation agrees within the intrinsic quantum bit error rate (QBER) of the Alice–Bob quantum channel, Alice accepts Bob as authenticated; otherwise, she rejects.

Case b: Bob is the verifier and Alice is the prover

Step 5b. Bob requests nonce disclosure

Bob requests Alice to disclose the nonce bit values corresponding to the nonce operator $\{N_i\}$ applied in Step 2.

Step 6b. Alice discloses nonce bits

Alice discloses the nonce-bit values over the public (classical) channel.

Step 7b. Bob verifies Alice

Bob checks the correlation between the disclosed nonce bits $\{n_i\}$ and his measurement outcomes $\{m_i\}$. If the correlation agrees within the intrinsic QBER of the Alice–Bob quantum channel, Bob accepts Alice as authenticated; otherwise, he rejects.

Section 3.3.1 offers a more in-depth analysis of the acceptance rule.

 doi:10.20944/preprints202602.1334.v1

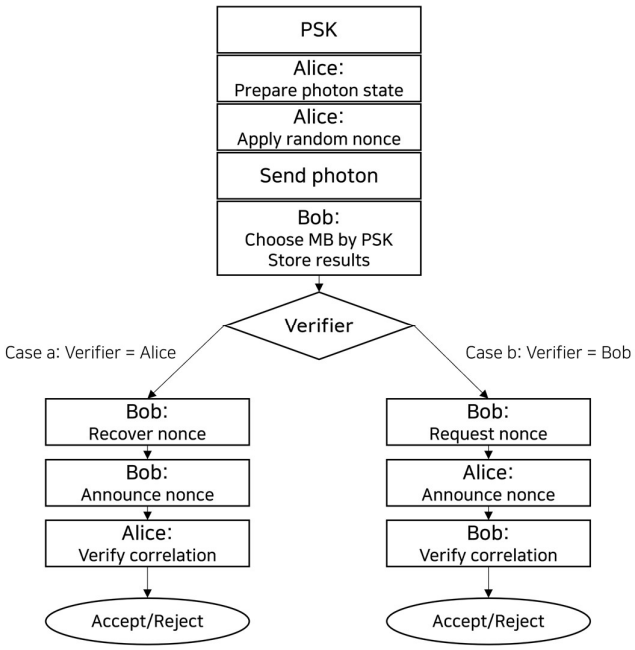


Figure 1. Flowchart of the proposed quantum entity authentication protocol. Since this protocol provides mutual authentication, its execution branches depending on the verifier.

For implementation validation on a deployed fiber, the proposed protocol adopts WCPs and the decoy-state technique commonly used in QKD. Further details are discussed in a subsequent section 3.2.

3. Security Evaluation of the Proposed Protocol

3.1. Security Analysis of Man-in-the-Middle Attacks

The security of the proposed protocol relies fundamentally on the secrecy of the PSK, denoted as A_k, which is distributed beforehand between Alice and Bob. In this analysis, we assume the public classical channel is authenticated but not encrypted, meaning an adversary can observe but not modify classical messages without detection. Consequently, the primary attack surface available to an external adversary (Eve) is the quantum channel.

Eve's primary objective is to impersonate either Alice or Bob (impersonation attack) or to extract information regarding A_k. To achieve this, Eve typically employs a MitM strategy, specifically the intercept-resend attack, where she intercepts the quantum signals transmitted over the channel, measures them, and resends new states to the recipient. Since the proposed protocol provides mutual authentication, we evaluate the security from two perspectives: (1) Alice as the verifier authenticating Bob, and (2) Bob as the verifier authenticating Alice.

Consider the scenario where Alice acts as the verifier and Bob as the prover. Eve intercepts the quantum signal transmitted by Alice and performs a measurement to forge a valid response. However, since Eve does not possess the PSK (A_k), she has no knowledge of the correct Measurement Basis (MB) for each signal. Consequently, she must choose a basis at random. When Eve measures in the wrong basis (which happens with a probability of 1/2) and resends the resulting state, Bob—who measures in the correct basis determined by A_k—will obtain a random result. This process introduces an error rate of 25% in the reconstructed nonce bits compared to the original bits sent by Alice. In Step 6a, Alice compares the nonce sequence reconstructed by the prover with her local values. The probability that Eve successfully passes this verification without triggering an error is $\left(\frac{3}{4}\right)^D$, where D is the number of successfully detected quantum states used for authentication. Therefore, the probability that the protocol rejects an unauthenticated adversary is given by:

 doi:10.20944/preprints202602.1334.v1

$$(P_f)^{Bob} = 1 - \left(1 - \frac{1}{4}\right)^D \quad (7)$$

As D increases, the rejection probability $(P_f)^{Bob}$ converges to 1, ensuring unconditional security against the intercept-resend attack.

In the reverse scenario where Bob verifies Alice, the security logic remains symmetric. If Eve attempts to impersonate Alice by sending forged quantum states, she must again guess the basis defined by A_k. Bob, measuring these states according to the correct PSK, will observe a 25% error rate in the correlation between his measurement outcomes and the nonce values subsequently disclosed by Eve (or forged by Eve). Accordingly, the probability of Bob rejecting an illegitimate prover in Step 7b is:

$$(P_f)^{Alice} = 1 - \left(1 - \frac{1}{4}\right)^D \quad (8)$$

In an ideal lossless environment, the number of authentication bits D would equal half the length of the used PSK string (i.e., $D \sim |A_k|/2$). However, in practical implementations, channel loss and detector inefficiency significantly reduce the number of valid detection events. The parameter D is analogous to the concepts of yield and overall gain used in QKD performance analysis. The yield is defined as the conditional probability that a signal sent by Alice results in a detection by Bob. The overall gain (Q_μ) represents the ratio of the total number of detected signals to the total number of transmitted pulses. Consequently, the effective length D corresponds to the number of final detected events at Bob's side. In typical QKD systems operating over standard optical fiber distances, the overall gain Q_μ is often observed in the order of 10^{-3} or lower depending on the transmission distance [31–33]. Therefore, to achieve a sufficiently high security parameter D (and thus a rejection probability close to 1), the protocol must transmit a sufficient number of pulses to compensate for the system's overall attenuation.

3.2. Security Analysis Within a QKD Realization Framework

Although the protocol is defined in the single-photon setting, its communication-channel implementation adopts WCPs and the decoy-state method. We follow the standard decoy-state modeling adopted by Park et al. [34] to lower-bound the single-photon contribution, since multi-photon events can enable PNS–type leakage and are therefore treated as not contributing to secure authentication strength.

3.2.1. Channel/Detector Model and Overall Gain

Let t_{AB} be the channel transmittance, η_{Bob} represent Bob-side component transmission, η_D be detector efficiency. Define the overall transmission efficiency

$$r = t_{AB}\,\eta_{Bob}\,\eta_D \quad (9)$$

When fiber loss is α dB/km over distance l km and Bob-side component loss is β dB,

$$t_{AB} = 10^{-\alpha l/10},\ \eta_{Bob} = 10^{-\beta/10}. \quad (10)$$

Let Y_0 be the background (vacuum) yield (dark counts + background clicks). For an i-th photon state, we use the yield model

$$Y_i = 1 - (1 - Y_0)(1 - r)^i. \quad (11)$$

For a WCP with mean photon number x (e.g., signal $x = \mu$, decoy $x = \nu$), the photon-number distribution is Poisson:

$$P_x(i) = e^{-x}\frac{x^i}{i!}. \quad (12)$$

The overall gain (click probability) is

$$Q_x = \sum_{i=0}^{\infty} P_x(i)\,Y_i = \sum_{i=0}^{\infty} e^{-x}\frac{x^i}{i!}[1 - (1 - Y_0)(1 - r)^i]. \quad (13)$$

For simplification of Q_x, we split the sum:

$$Q_x = \sum_{i=0}^{\infty} e^{-x}\frac{x^i}{i!} - (1 - Y_0)\sum_{i=0}^{\infty} e^{-x}\frac{x^i}{i!}(1 - r)^i$$

$$= 1 - (1 - Y_0)e^{-x}\sum_{i=0}^{\infty}\frac{(x(1-r))^i}{i!}. \quad (14)$$

 doi:10.20944/preprints202602.1334.v1

Use $\sum_{i=0}^{\infty}\frac{\alpha^i}{i!} = e^a$:

$$e^{-x}\sum_{i=0}^{\infty}\frac{(x(1-r))^i}{i!} = e^{-x}e^{x(1-r)} = e^{-xr}. \quad (15)$$

Hence,

$$Q_x = 1-(1-Y_0)e^{-xr}. \quad (16)$$

3.2.2. QBER Model

Let $e_0 = 1/2$ be the error probability of background clicks (random outcomes), and let e_d be the intrinsic misalignment/detection error probability for true signal clicks. Then

$$E_xQ_x = e_oY_o + e_d(Q_x - Y_o). \quad (17)$$

Substituting (16) gives

$$E_xQ_x = e_oY_o + e_d\,(1-(1-Y_0)e^{-xr} - Y_0)$$
$$= e_oY_o + e_d\,(1-Y_0)(1-e^{-xr}). \quad (18)$$

3.2.3. Decoy-State Bounds for Single-Photon Terms

Use three intensities: signal μ, weak decoy ν, and vacuum 0 ($0 < \nu < \mu$). Let the observed gains and QBERs be Q_μ, Q_ν, Q_0, E_μ and E_ν. From vacuum decoy, $Y_0 = Q_0$. Multiply by e^x to obtain the standard decoy expansion:

$$Q_xe^x = \sum_{i=0}^{\infty}Y_i\frac{x^i}{i!}. \quad (19)$$

In particular,

$$Q_\mu e^\mu = Y_o + Y_1\mu + Y_2\frac{\mu^2}{2!} + Y_3\frac{\mu^3}{3!} + \cdots,$$
$$Q_\nu e^\nu = Y_o + Y_1\nu + Y_2\frac{\nu^2}{2!} + Y_3\frac{\nu^3}{3!} + \cdots. \quad (20)$$

A conservative lower bound on the single-photon yield Y_1 (vacuum + weak decoy) is

$$Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu-\nu^2}\left(Q_\nu e^\nu - \frac{\nu^2}{\mu^2}Q_\mu e^\mu - \frac{\mu^2-\nu^2}{\mu^2}Y_0\right). \quad (21)$$

Then the single-photon gain satisfies

$$Q_1 = Y_1\mu e^{-\mu} \Rightarrow Q_1 \geq Q_1^L = Y_1^L\mu e^{-\mu}, \quad (22)$$

Similarly, using the error gain expansion

$$E_xQ_xe^x = \sum_{i=0}^{\infty}e_iY_i\frac{x^i}{i!}, \quad (23)$$

an upper bound on the single-photon error rate is

$$e_1 \leq e_1^U = \frac{E_\nu Q_\nu e^\nu - e_0Y_0}{Y_1^L\nu}. \quad (24)$$

3.2.4. Lower Bound on Usable Authentication Trials

Let N be the number of WCP pulsed used for one execution of the authentication procedure (i.e., the number of indices i for which Alice prepares $|\phi_i\rangle$ and Bob attempts detection/measurement). Define the random variable X as the number of detected single-photon authentication events among these N pulses. Under independent trials, $X \sim Binomial(N, Q_1)$. Since $Q_1 \geq Q_1^L$, a conservative approximation uses Q_1^L. For sufficiently large N, apply a normal approximation:

$$X \approx \mathcal{N}\left(NQ_1^L, NQ_1^L(1-Q_1^L)\right). \quad (25)$$

Let z_a be the standard normal quantile for a one-sided confidence level $1-\alpha$ ($0 < \alpha < 1$). Then a finite-size lower bound on usable trials is

$$D = NQ_1^L - z_a\sqrt{NQ_1^L(1-Q_1^L)}. \quad (26)$$

It means that with confidence at least $1-\alpha$ at least D detected single-photon events are available for the authentication decision rule in Section 3.3.

3.3. Security Analysis for the Authentication Protocol Under QKD Framework

3.3.1. Acceptance Rule (QBER-Threshold)

 doi:10.20944/preprints202602.1334.v1

Let $\mathcal{I}$ be the set of indices used for verification, with $|\mathcal{I}| = D$ as lower-bounded in (26). Define the mismatch indicator

$$\triangle_i = \begin{cases} 1, \hat{n_i} \neq n_i \ (Case\ a: Alice\ virifies\ Bob), \\ 1, m_i \neq v_i \oplus n_i \ (Case\ a: Alice\ virifies\ Bob), \end{cases} \quad (27)$$

and the total mismatch count

$$W = \sum_{i \subset \mathcal{I}} \triangle_i. \quad (28)$$

The verifier accepts iff the mismatch rate is below a threshold $\tau \in \left(0, \frac{1}{2}\right)$:

$$\frac{W}{D} \leq \tau, W \leq \tau D. \quad (29)$$

3.3.2. Completeness: False Rejection Probability

Assume an honest prover and verifier. Let the per-trial mismatch probability on the verified set be e_{auth}, dominated by the single-photon error rate. Conservatively,

$$e_{auth} \leq e_1^U, \quad (30)$$

where e_1^U is estimated in (24). Under independent trials,

$$W \sim \text{Binomial}(D, e_{auth}). \quad (31)$$

The FRR is therefore

$$P_{FRR} = Pr[W > \tau D] \leq \sum_{k=\lfloor \tau D \rfloor + 1}^{D} \binom{D}{k} (e_{auth})^k (1 - e_{auth})^{D-k}. \quad (32)$$

For $\tau > e_{auth}$, a Chernoff bound yields

$$\Pr[W > \tau D] \leq \exp\left(-D \cdot \mathrm{KL}(\tau \parallel e_{auth})\right), \quad (33)$$

where the binary relative entropy is

$$\mathrm{KL}(\tau || e) = \tau \ln\left(\frac{\tau}{e}\right) + (1 - \tau) \ln\left(\frac{1-\tau}{1-e}\right). \quad (34)$$

For large D,

$$W \approx \mathcal{N}(De_{auth}, De_{auth}(1 - e_{auth})), \quad (35)$$

so

$$P_{FRR} \approx 1 - \Phi\left(\frac{\tau D - De_{auth}}{\sqrt{De_{auth}(1-e_{auth})}}\right) = 1 - \Phi\left(\frac{\tau - e_{auth}}{\sqrt{e_{auth}(1-e_{auth})/D}}\right), \quad (36)$$

where $\Phi(\cdot)$ is the standard normal cumulative distribution function (CDF).

3.3.3. Soundness: Impersonation Success Probability

We analyze impersonation under the standard assumption that the PSK bits $\{(b_i, v_i)\}_{i \subset \mathcal{I}}$ are unknown to the adversary and are computationally indistinguishable from uniform (or information-theoretically uniform if provisioned as such). In particular, the value-bit is unbiased:

$$\Pr[v_i = 0] = \Pr[v_i = 1] = \frac{1}{2}. \quad (37)$$

In the ideal relation $m_i = v_i \oplus n_i$, for any fixed $m_i \in \{0,1\}$ we have

$$\Pr[n_i = 0 \mid m_i] = \Pr[v_i = m_i \mid m_i] = \frac{1}{2},$$
$$\Pr[n_i = 1 \mid m_i] = \Pr[v_i \neq m_i \mid m_i] = \frac{1}{2}. \quad (38)$$

Hence, without knowledge of v_i, the adversary's optimal single-bit guessing probability for the correct nonce value is bounded by

$$p_{guess}(n_i) \leq \frac{1}{2}. \quad (39)$$

Therefore, regardless of whether the adversary impersonates the prover in Case a (must output $\hat{n_i}$ or Case b (must disclose n_i), each verified position succeeds with probability at most 1/2, and mismatches occur with probability at least 1/2.

Let W_E denote the mismatch count under impersonation. Then

$$W_E \sim \text{Binomial}\left(D, \frac{1}{2}\right). \quad (40)$$

The false acceptance rate (FAR), i.e., the impersonation success probability under the threshold rule (29), is

$$P_{FAR} \leq \Pr[W_E \leq \tau D] - \sum_{k=0}^{\lfloor \tau D \rfloor} \binom{D}{k} \left(\frac{1}{2}\right)^D. \quad (41)$$

For $0 < \tau < 1/2$, use

 doi:10.20944/preprints202602.1334.v1

$$\sum_{k=0}^{\lfloor \tau D \rfloor} \binom{D}{k} \le 2^{D h_2(\tau)}, \quad (42)$$

where the binary entropy is

$$h_2(\tau) = -\tau \log_2 \tau - (1-\tau)\log_2(1-\tau). \quad (43)$$

Substitute (42) into (41):

$$P_{FAR} \le 2^{D h_2(\tau)} \cdot 2^{-D} = 2^{-D(1-h_2(\tau))}. \quad (44)$$

If the adversary guesses the entire tested PSK segment correctly, impersonation succeeds trivially. Since each tested index uses two PSK bits (b_i, v_i), the tested segment has length $2D$ bits; thus

$$P_{guess-PSK} = 2^{-2} \ . \quad (45)$$

A conservative total bound is

$$P_{imp} \le \max\{2^{-2D}, 2^{-D(1-h_2(\tau))}\}. \quad (46)$$

Equivalently, define the security strength (in bits) as

$$\kappa = -\log_2 P_{imp} \implies \kappa \ge \min\{2D, D(1-h_2(\tau))\}. \quad (47)$$

To simultaneously achieve $P_{FRR} \le \epsilon_{FRR}$ and $P_{imp} \le 2^{-\kappa}$, one may:

① estimate e_{auth} (or use e_1^U)
② choose $\tau > e_{auth}$ to ensure small P_{FRR} via (32)~(36)
③ choose D so that $D(1-h_2(\tau)) \ge \kappa$ via (47)
④ ensure that the channel/decoy setting yields this D via (26).

3.3.4. PSK Management

The present protocol uses the PSK A_k directly to determine the prepared states and Bob's measurement bases in Section 2, while the nonce bits are revealed (Case b) or effectively exposed through prover messages (Case a). Therefore, long-term security requires explicit management of PSK reuse, particularly in practical implementations using WCP, where multi-photon emissions may allow additional information leakage over repeated sessions.

For one authentication execution that verifies $|\mathcal{J}| = D$ positions, the amount of PSK material consumed is

$$\left|A_k^{(\mathcal{J})}\right| = 2D, \quad (48)$$

because each verified position uses two PSK bits (b_i, v_i). If mutual authentication is achieved by running both directions, the total PSK consumption becomes

$$\left|A_{k,mutual}^{(\mathcal{J})}\right| = 4D. \quad (49)$$

In the WCP setting, with mean photon number xxx, the probability of emitting at least two photons is

$$P_{\ge 2}(x) = 1 - \Pr[0] - \Pr[1] = 1 - e^{-x}(1+x). \quad (50)$$

A conservative operational stance is that any authentication indices associated with multi-photon emissions can become progressively less secure under repeated use (e.g., an adversary may keep an extra photon and correlate later public information related to nonce disclosure/announcement). This motivates a strict or bounded PSK reuse policy.

A robust information-theoretic refresh policy is available when the authentication procedure is executed during BB84-type QKD operation. Let $K_{QKD}^{(s)}$ denote the secret key distilled from the QKD session sss. Define the PSK segment for the next authentication session $(s+1)$ by extracting fresh bits from the previous QKD key:

$$A_k^{(s+1)} \leftarrow \text{first } 2D^{(s+1)} \text{ bits of } K_{QKD}^{(s)}, \quad (51)$$

(or $4D^{(s+1)}$ bits if mutual authentication is performed). This requires the key-budget condition

$$\left|K_{QKD}^{(s)}\right| \ge 2D^{(s+1)} \quad (\text{or } \left|K_{QKD}^{(s)}\right| \ge 4D^{(s+1)} \text{ for mutual authentication}). \quad (52)$$

Under standard QKD security, this yields fresh PSK segments independent of prior public transcripts, enabling "one-time consumption" of PSK symbols across sessions. If long PSK storage is operationally undesirable, a computationally motivated alternative is to maintain a master secret K_{master} of λ bits and derive a per-session PSK using a keyed derivation function. Specifically, let KDF(·) denote a key derivation function (or equivalently a pseudorandom function (PRF) instantiated

 doi:10.20944/preprints202602.1334.v1

KDF) that, for a fixed secret key, maps a public "context" string to an output bit string that is computationally indistinguishable from uniform to any efficient adversary without the key. In our setting, the context binds the derived PSK to the session and the authentication direction to ensure domain separation. The per-session PSK is then derived as

$$A_k^{(s)} = \mathrm{KDF}(K_{master}, \mathrm{sid} = s \parallel \mathrm{role}), \quad (53)$$

where 'role' distinguishes protocol directions (e.g., Alice →Bob vs. Bob→Alice) to avoid cross-protocol/key reuse. Here, 'sid = s 'denotes a public session identifier (e.g., a monotonically increasing counter or a timestamp) that is unique per authentication execution, and 'role' is a public label that specifies the authentication direction (e.g., "A→B" or "B→A") for domain separation. The derived string $A_k^{(s)}$ is then parsed into D two-bit symbols to define the per-trial basis/value bits used in the protocol:

$$\left(A_k^{(s)}\right)_i = \left(b_i^{(s)}, v_i^{(s)}\right),\ i = 1, \dots, D\ , \quad (54)$$

with $\left(b_i^{(s)}, v_i^{(s)}\right)$ assigned from consecutive bit pairs of $A_k^{(s)}$ (hence $\left|A_k^{(s)}\right| = 2D$ bits for one-way authentication, or $4D$ bits for mutual authentication).

The master secret is then refreshed using newly generated QKD keys:

$$K_{master} \leftarrow \mathrm{KDF}\left(K_{master}, K_{QKD}^{(s)}\right). \quad (55)$$

This approach preserves per-session freshness while reducing stored authentication material, and can be combined with a hard limit on the number of authentication executions per master-secret epoch.

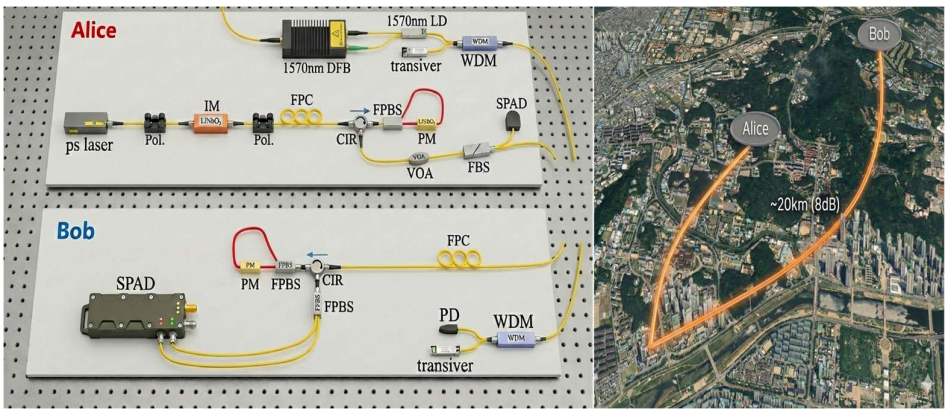
In summary, because the protocol directly binds A_k to state preparation and basis choice, and because WCP implementations inevitably introduce multi-photon probability $P_{\geq 2}(x)$, long-term soundness is best supported by (i) treating PSK symbols as consumable resources of size $2D$ (or $4D$ for mutual authentication) and (ii) enforcing explicit refresh rules, preferably with QKD-generated keys when available.

4. Realization Results on Communication Channels

In this section, we describe the experimental implementation of the proposed quantum entity authentication protocol over a deployed optical network. Although the protocol is theoretically defined based on single-photon sources, the implementation utilizes WCPs and the decoy-state method to ensure security against photon-number-splitting attacks, as discussed in the security analysis. The quantum states employed in this experiment are four polarization states of photons.

4.1. Experimental Configuration

In this implementation, Alice and Bob utilized photon polarization states ($|D\rangle$, $|A\rangle$, $|R\rangle$, $|L\rangle$). These polarization states correspond to the protocol's quantum states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, respectively. We assumed that the PSK was securely distributed between Alice and Bob beforehand. Figure 2 illustrates the experimental setup for the quantum authentication system, which consists of Alice, Bob, a quantum channel, and a classical channel.



 doi:10.20944/preprints202602.1334.v1

Figure 2. Experimental setup for proposed quantum entity authentication implementation. At Alice (transmitter), picosecond optical pulses are generated and shaped using an intensity modulator, prepared with well-defined polarization, and encoded using an all-fiber module incorporating a fiber polarizing beam splitter (FPBS) and a phase modulator. A classical synchronization channel from a 15xx-nm laser diode (LD; clock) is wavelength-multiplexed using wavelength-division multiplexing (WDM). A fiber beam splitter (FBS) provides an optional monitoring tap directed to single-photon avalanche diodes (SPAD). The signals are transmitted through a field-deployed fiber span of approximately 20 km with an overall loss of about 8 dB. At Bob (receiver), WDM separates the classical channels; the clock channel is detected with a photodiode (PD) and interfaced through a classical transceiver for synchronization. Separately, the quantum channel is polarization-aligned using a fiber polarization controller (FPC), analyzed in an FPBS-based polarization decoding system, and detected with SPADs.

4.1.1. Transmitter (Alice)

Alice encodes the quantum states according to the PSK and transmits them to Bob. The decoy states are randomly selected by Alice. Alice's setup comprises a light source, a quantum state encoding device, a mean photon number monitor, clock synchronization, and classical communication modules.

- **Light Source:** We used a picosecond pulsed laser (ps laser) operating at a wavelength of 1550 nm with a spectral bandwidth of < 1 nm and a temporal pulse width of approximately 500 ps. The laser generates pulses for signal and decoy states, while no pulse is generated for the vacuum state.
- **Intensity Modulation:** An intensity modulator (IM) determines the signal and decoy intensities. The IM is stabilized at the minimum transmission point using a bias controller and a 1570 nm pilot laser. When generating signal states, the IM is inactive (allowing the pulse to pass); for decoy states, voltage is applied to attenuate the pulse intensity. An optical attenuator is then used to reduce the pulses to the single-photon level before they enter the quantum channel.
- **State Encoding:** The quantum state encoding device consists of a Sagnac interferometer and a phase modulator (PM) [35]. The incident photon polarization is $|D\rangle$, which is converted into one of the four states ($|D\rangle$, $|A\rangle$, $|R\rangle$, $|L\rangle$) depending on the voltage applied to the PM. During encoding, Alice applies the random bit-flip operation required by the authentication protocol.
- **Monitoring:** A mean photon number monitor, consisting of a 50:50 beam splitter and a single-photon detector (SPD), measures the presence of photons in the pulses sent to Bob. Assuming a Poissonian photon number distribution, this setup estimates the mean photon number for signal and decoy states.

4.1.2. Receiver (Bob)

Bob is responsible for decoding and measuring the incoming quantum states. His setup includes a fiber polarization controller (FPC), a polarization state decoding device, a polarization measurement unit, a trigger detector, and a clock synchronization module.

- **Polarization Control:** The FPC compensates for polarization drifts caused by the quantum channel, converting the arbitrary unitary transformation induced by the fiber into an identity operation.
- **Decoding and Measurement:** Bob's decoding device is structurally identical to Alice's encoder. Based on the basis information derived from the locally stored PSK, Bob applies a voltage to his PM to switch between the z-basis ($|D\rangle$, $|A\rangle$) and the x-basis ($|R\rangle$, $|L\rangle$). The photons are then measured using a polarization beam splitter (PBS) and single-photon avalanche diodes (SPADs) with a detection efficiency of approximately 20%.
- **Synchronization:** Both entities are synchronized to a 10 MHz clock. Alice transmits a trigger signal alongside the quantum signal. Bob detects this trigger using a photodiode (PD) and a pre-amplifier to maintain synchronization.

 doi:10.20944/preprints202602.1334.v1

4.1.3. Communication Channels

The system utilizes both quantum and classical channels, similar to a QKD architecture.

- **Classical Channel:** Assumed to be an authenticated public channel where an eavesdropper can read but not modify messages. It is used for clock signals, trigger signals (via ns pulse laser and PD), and classical information exchange (via TCP/IP).
- **Quantum Channel:** The experiment utilized the deployed optical network connecting Alice and Bob via a detour route. The physical distance is approximately 20 km. While the theoretical loss for this distance is around 4 dB, the measured optical loss was approximately 8 dB.

4.2. Experimental Conditions

Prior to the execution of the protocol, Alice and Bob are assumed to share a PSK of size 1,048,576 bits (524,288 bits×2). One "train" sent by Alice consists of 524,288 qubits. The mean photon numbers for signal and decoy states were set to approximately 0.5 and 0.15, respectively. The probabilities for sending signal, decoy, and vacuum states were configured to approximately 0.88, 0.10, and 0.02. Table 1 summarizes the experimental parameters.

Table 1. Experimental conditions for the implementation of the quantum authentication protocol.

Parameter		Value
Average photon number	Signal	~0.5
	Decoy	~0.15
Intensity probabilities	Signal	0.88
	Decoy	0.10
	Vacuum	0.02
PSK size		1,048,576 bits
One train length		524,288 qubits
Alice's bit flip probability		50%
Quantum channel length		~ 20 km
Quantum channel loss		~ 8 dB

4.3. Experimental Results and Analysis

The proposed quantum authentication protocol was implemented on a physically deployed network.

4.3.1. Key Rate and QBER Performance

In a practical authentication scenario, reusing the same PSK is insecure. However, for the purpose of validating the implementation on a deployed fiber, we transmitted one train (524,288 qubits) every 5 seconds using the pre-distributed keys. Figure 3 illustrates the sifted key rate over a duration of approximately 1500 seconds. Since Alice and Bob share the PSK, they always measure in the same basis. Consequently, the volume of the sifted key is identical to that of the raw key. The results show a stable key rate over time. The difference in key generation rates between signal and decoy states is due to their different mean photon numbers.

 doi:10.20944/preprints202602.1334.v1

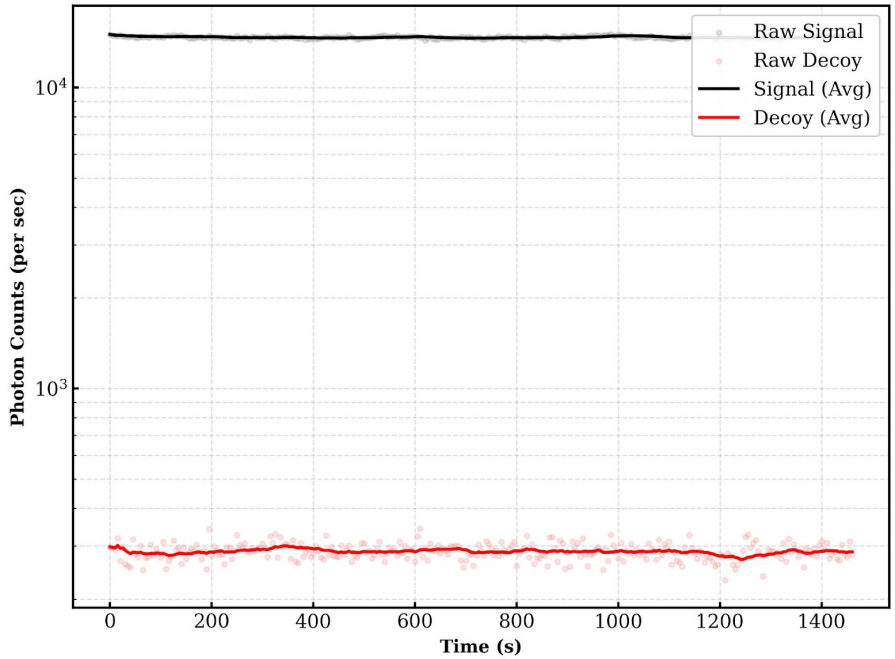


Figure 3. Shifted key rate over time.

Figure 4 presents the Quantum Bit Error Rate (QBER) for signal and decoy states. The QBER was calculated using the PSK and Alice's bit-flip information. Due to the lower mean photon number and probability of decoy states, the sifted key volume for decoys is smaller, resulting in larger statistical fluctuations in the QBER compared to the signal states.

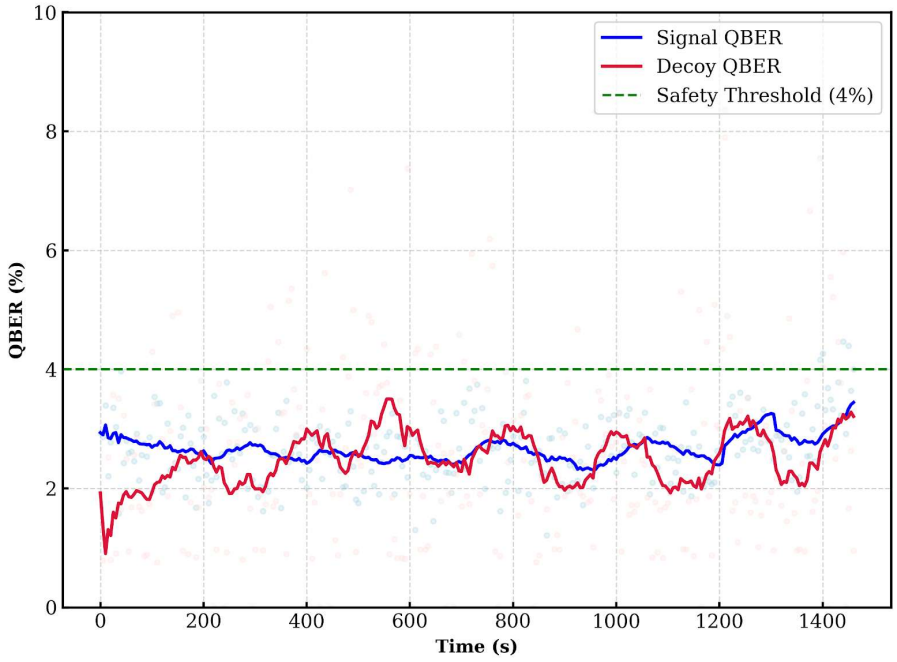


Figure 4. QBER when all bit-flip information is disclosed. The green dashed line indicates the operational safety threshold ($\delta \approx 4\%$). This value is based on the acceptance rule defined in Section 3.3.1, which requires the QBER to remain below a specific limit to minimize the FAR. As validated in the experimental results, the system

 doi:10.20944/preprints202602.1334.v1

maintains a QBER between 1% and 4% under normal conditions, confirming that a 4% threshold provides a robust margin to distinguish legitimate signals from potential attacks.

4.3.2. Case A: Alice as Verifier, Bob as Prover

We first evaluated the scenario where Alice acts as the verifier and Bob as the prover. Alice measured the key rate and QBER using her local PSK, her bit-flip records, and the measurement results announced by Bob.

Figure 5 shows the key rate for this configuration. Since Alice performs the bit-flip operation with a 50% probability, the key generation rates for the "no bit flip" and "bit flip" cases are similar and remain stable over time.

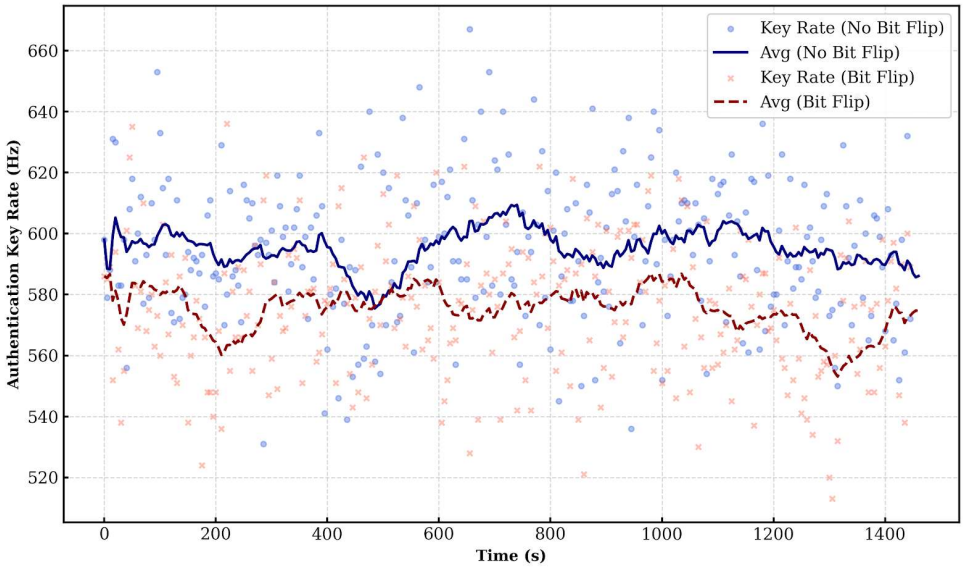


Figure 5. Key rate (Verifier: Alice, Prover: Bob).

Figure 6 displays the QBER measured by Alice. The QBER mostly remains within the range of 1% to 4%. Instances where the QBER deviates from this range tend to occur simultaneously for both "no bit flip" and "bit flip" cases. Alice accepts Bob as authenticated if the observed QBER falls within the pre-defined security threshold.

 doi:10.20944/preprints202602.1334.v1

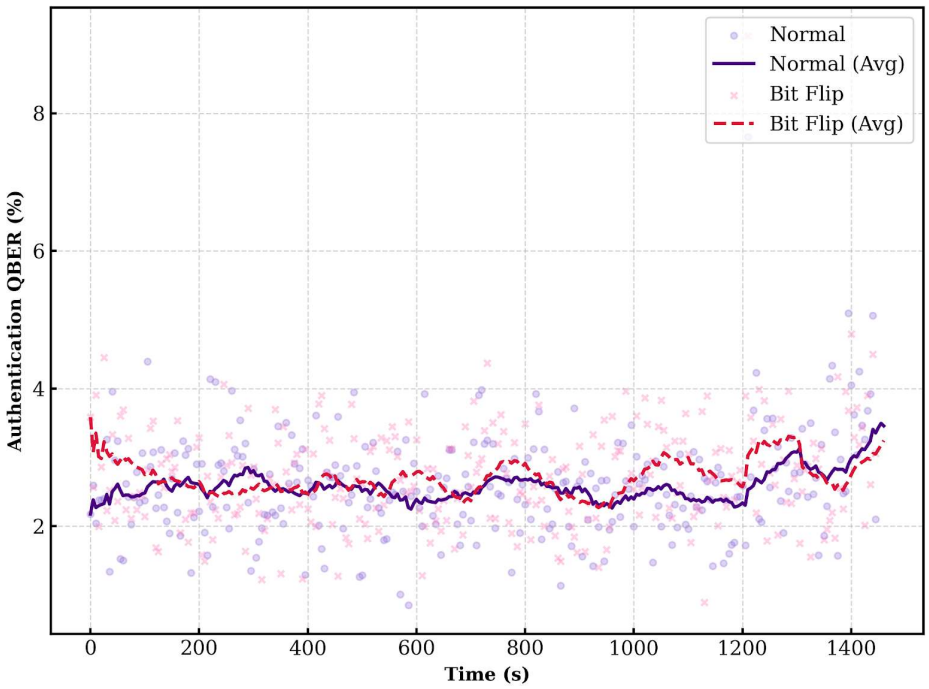


Figure 6. QBER (Verifier: Alice, Prover: Bob).

4.3.3. Case B: Bob as Verifier, Alice as Prover

Next, we evaluated the reverse scenario where Bob acts as the verifier and Alice as the prover. In this case, Alice discloses her bit-flip information to Bob. Bob then calculates the key rate and QBER based on Alice's disclosed information, his measurement outcomes, and the PSK. Figure 7 shows the key rate results measured by Bob. Similar to the previous case, the key rates for "no bit flip" and "bit flip" are comparable due to the 50% flip probability.

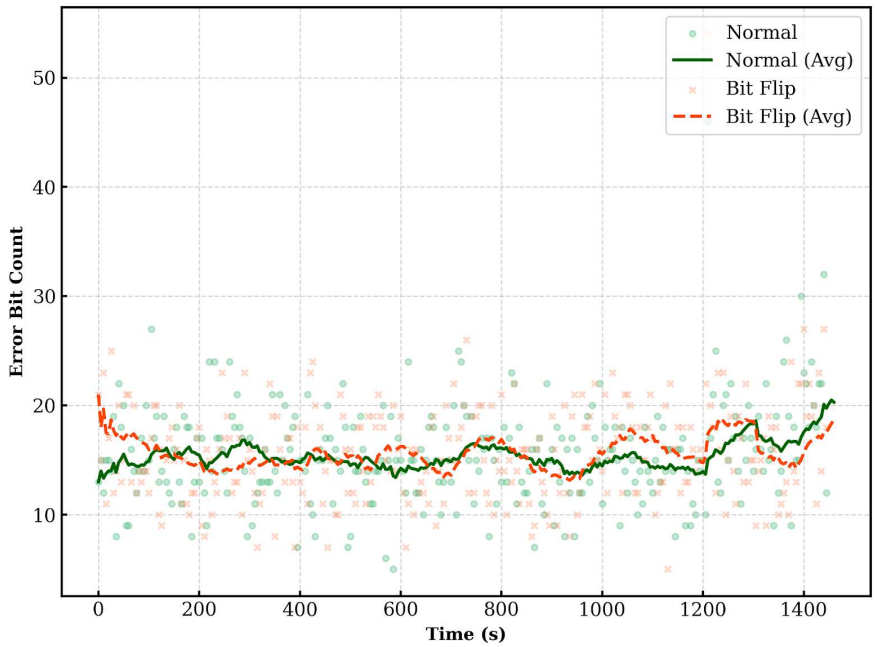


Figure 7. Key rate (Verifier: Bob, Prover: Alice).

 doi:10.20944/preprints202602.1334.v1

Figure 8 presents the QBER measured by Bob using the bit-flip information provided by Alice. Consistent with the Alice-verifier scenario, the QBER is generally observed between 1% and 4%. Bob authenticates Alice based on this QBER value.

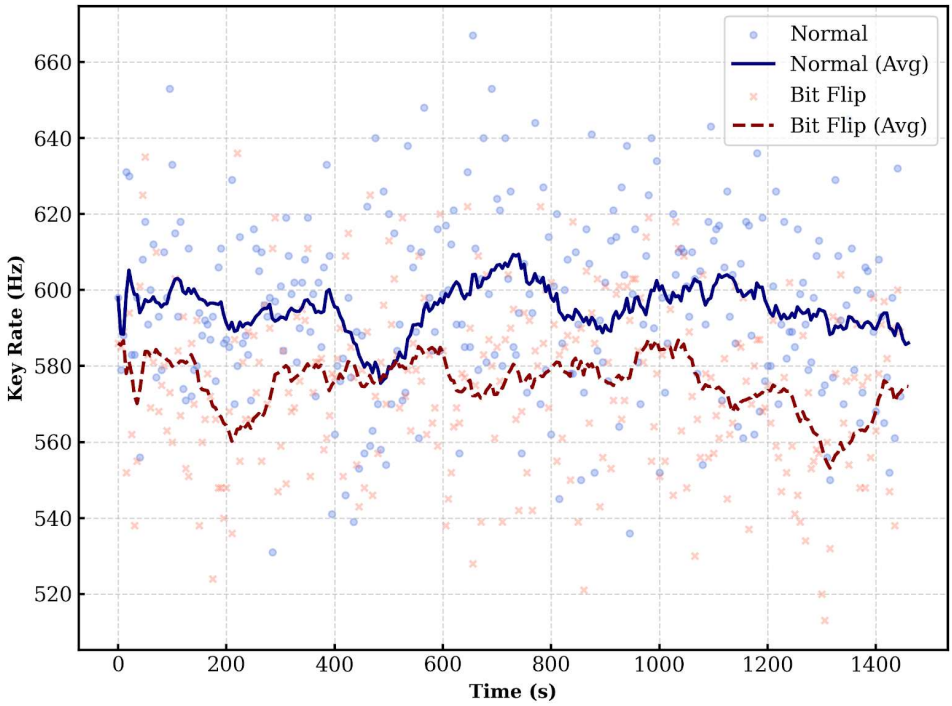


Figure 8. QBER (Verifier: Bob, Prover: Alice).

The experimental results confirm that the proposed quantum authentication protocol can be stably implemented over a real-world optical network. While the key rate remained constant, the QBER showed fluctuations between 1% and 4%.

5. Conclusion

The overarching security of any quantum-cryptographic framework is fundamentally predicated on the robustness of entity authentication. Without a rigorous mechanism to verify the legitimacy of communicating parties, even channels with information-theoretic security remain susceptible to MitM and impersonation attacks. To address this critical vulnerability, this research has successfully implemented and experimentally validated a quantum authentication protocol over a real-world communication network. By securing the authentication process using the laws of physics rather than computational hardness, the proposed scheme aligns the security level of identity verification with that of the QKD process itself.

A significant advantage of the proposed protocol is its practical feasibility within existing quantum network infrastructures. We demonstrated that the protocol can be deployed on standard QKD systems without requiring any modifications to the optical hardware. By utilizing polarization states for encoding and employing the decoy-state method to counter PNS attacks, the system effectively utilizes WCP while maintaining security guarantees comparable to those of single-photon sources. Although this study exclusively demonstrates and analyzes polarization encoding, the protocol is equally applicable to phase-based encoding—analogous to standard QKD implementations—with comparable performance expectations. This compatibility ensures that physical-layer authentication can be seamlessly integrated as an intrinsic feature of future quantum communication terminals.

 doi:10.20944/preprints202602.1334.v1

The theoretical analysis and experimental results confirm the protocol's capability to provide robust mutual authentication. Our security analysis established that an adversary performing an intercept-resend attack introduces a detectable error rate due to the lack of the PSK, thereby allowing the verifier to reject illegitimate entities with a probability that converges to unity. Furthermore, we validated the protocol over a deployed optical fiber network spanning approximately 20 km. The experimental results showed stable key rates and QBER within the required security thresholds, proving the protocol's resilience against environmental decoherence and channel attenuation. These findings underscore the feasibility of integrating quantum entity authentication into next-generation networks, thereby ensuring a holistic security architecture for the global quantum internet.

Author Contributions: Conceptualization, C.H.; Methodology, C.H. and S.-W.J.; Validation, C.H., Y.-C.J. and S.-W.J.; Experimental implementation Y.-C.J.; Formal analysis, C.H. and S.-W.J.; Investigation, C.H. and Y.-C.J.; Writing—original draft, C.H.; Writing—review and editing, C.H., Y.-C.J. and S.-W.J.; Visualization, C.H. and Y.-C.J.; Supervision, C.H.; Project administration, C.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Research Council of Science & Technology (NST) grant by the Korea government (MSIT) (No. CAP22053-200).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kimble, H.J. The quantum internet. *Nature* **2008**, 453, 1023–1030.
2. Wehner, S.; Elkouss, D.; Hanson, R. Quantum internet: A vision for the road ahead. *Science* **2018**, 362, eaam9288.
3. Lütkenhaus, N. Security against individual attacks in quantum key distribution. *Phys. Rev. A* **2000**, 61, 052304.
4. Curty, M.; Lütkenhaus, N. Quantum authentication of classical messages. *Phys. Rev. A* **2001**, 64, 042313.
5. Muller, A.; Zbinden, H.; Gisin, N. Quantum cryptography over 23 km in optical fiber. *EPL* **1993**, 23, 383.
6. Lo, H.-K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, 283, 2050–2056.
7. Shor, P.W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 20–22 November **1994**; *IEEE Computer Society*: Washington, DC, USA, **1994**; pp. 124–134.
8. Bernstein, D.J. Introduction to post-quantum cryptography. In *Post-Quantum Cryptography*; Bernstein, D.J., Buchmann, J., Dahmen, E., Eds.; Springer: Berlin/Heidelberg, Germany, **2009;** pp. 1–14.
9. National Security Agency (NSA). NSA Cybersecurity Perspectives on Quantum Key Distribution and Quantum Cryptography. *News & Highlights*, 26 October **2020**.
10. Carter, J.L.; Wegman, M.N. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **1981**, 22, 265–279.
11. Portmann, C. Key recycling in authentication. *arXiv* **2012**, arXiv:1202.1229.
12. Wang, L.-J.; Zhang, K.-Y.; Wang, J.-Y.; Cheng, J.; Yang, Y.-H.; Tang, S.-B.; Yan, D.; Tang, Y.-L.; Liu, Z.; Yu, Y.; Zhang, Q.; Pan, J.-W. Experimental authentication of quantum key distribution with post-quantum cryptography. *npj Quantum Inf.* **2021**, 7, 67.
13. National Institute of Standards and Technology (NIST). What Is Post-Quantum Cryptography? Available online: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography (accessed on 29 January 2026).
14. Atutxa, A.; Sanz, A.; Salegi, E.; Huarte, M.; Astorga, J.; Jacob, E. Authentication of the QKD classical channel through Post-Quantum Cryptography in a multi-site 5G/6G quantum-safe communication network. In

 doi:10.20944/preprints202602.1334.v1

Proceedings of the 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Mangosuthu, South Africa, 31 March **2025**; pp. 648–654.

15. Chen, A.C.H. Man-in-the-Middle Attacks Targeting Quantum Cryptography. *arXiv* **2025**, arXiv:2503.13457.
16. Amellal, H.; El Hajjami, S.; Kaushik, K.; Chhabra, G.; Yadav, S.A. Quantum Man-in-the-Middle Attacks on QKD Protocols: Proposal of a Novel Attack Strategy. In *Proceedings of the 2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, Gautam Buddha Nagar, India, 14–16 September **2023**; pp. 513–519.
17. Barnum, H.; Crépeau, C.; Gottesman, D.; Smith, A.; Tapp, A. Authentication of quantum messages. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, Vancouver, BC, Canada, 16–19 November **2002**; pp. 449–458.
18. Zeng, G.; Keitel, C.H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **2002**, 65, 042312.
19. Damgård, I.B.; Fehr, S.; Salvail, L.; Schaffner, C. A quantum protocol for confident identification. In *Advances in Cryptology* – CRYPTO 2007; Menezes, A., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, **2007**; Volume 4622, pp. 360–378.
20. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, 299, 802–803.
21. Pastawski, F.; Yao, N.Y.; Jiang, L.; Lukin, M.D.; Cirac, J.I. Unforgeable noise-tolerant quantum tokens. *Proc. Natl. Acad. Sci. USA* **2012**, 109, 16079–16082.
22. Aharon, N.; Vaidman, L. Quantum identification of a person. *Phys. Rev. A* **2013**, 88, 062315.
23. Dusek, M.; Lütkenhaus, N.; Hendrych, M. Quantum cryptography. *Prog. Opt.* **2006**, 49, 381–454.
24. Li, X.; Zhang, K.; Zhang, L.; Zhao, X. A New Quantum Multiparty Simultaneous Identity Authentication Protocol with the Classical Third-Party. *Entropy* **2022**, 24, 483.
25. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, 74, 145–195.
26. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, 81, 1301.
27. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, 85, 1330.
28. Lütkenhaus, N.; Jahma, M. Quantum key distribution with realistic states: photons splitting attacks and quantum tagging. *New J. Phys.* **2002**, 4, 44.
29. Liao, S.-K.; Cai, W.-Q.; Liu, W.-Y.; Zhang, L.; Li, Y.; Ren, J.-G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.-P.; Li, F.-Z.; Chen, X.-W.; Sun, L.-H.; Jia, J.-J.; Wu, J.-C.; Jiang, X.-J.; Wang, J.-F.; Huang, Y.-M.; Wang, Q.; Zhou, Y.-L.; Deng, L.; Xi, T.; Ma, L.; Hu, T.; Zhang, Q.; Chen, Y.-A.; Liu, N.-L.; Wang, X.-B.; Zhu, Z.-C.; Lu, C.-Y.; Shu, R.; Peng, C.-Z.; Wang, J.-Y.; Pan, J.-W. Satellite-to-ground quantum key distribution. *Nature* **2017**, 549, 43–47.
30. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; Pereira, J.L.; Razavi, M.; Shaari, J.S.; Tomamichel, M.; Usenko, V.C.; Vallone, G.; Villoresi, P.; Wallden, P. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, 12, 1012–1236.
31. Rosenberg, D.; Harrington, J.W.; Rice, P.R.; Hiskett, P.A.; Peterson, C.G.; Hughes, R.J.; Lita, A.E.; Nam, S.W.; Nordholt, J.E. Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber. *Phys. Rev. Lett.* **2007**, 98, 010503.
32. Zhao, Y.; Qi, B.; Ma, X.; Lo, H.-K.; Qian, L. Experimental Decoy State Quantum Key Distribution Over 15 km. *Phys. Rev. Lett.* **2006**, 96, 070502.
33. Dixon, A.R.; Yuan, Z.L.; Dynes, J.F.; Sharpe, A.W.; Shields, A.J. Gigahertz decoy-state quantum key distribution with 1.5 Mbps secure key rate. *Opt. Express* **2008**, 16, 18790–18797.
34. Park, H.; Park, B.K.; Woo, M.K.; Kang, M.-S.; Choi, J.-W.; Kang, J.-S.; Yeom, Y.; Han, S.-W. Mutual entity authentication of quantum key distribution network system using authentication qubits. *EPJ Quantum Technol.* **2023**, 10, 48.
35. Agnesi, C.; Avesani, M.; Stanco, A.; Villoresi, P.; Vallone, G. All-fiber self-compensating polarization encoder for quantum key distribution. *Opt. Lett.* **2019**, 44, 2398–2401.

 doi:10.20944/preprints202602.1334.v1

disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.