IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 March 2025, accepted 30 March 2025, date of publication 8 April 2025, date of current version 22 April 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3558944

RESEARCH ARTICLE

Experimental Implementation of Enhanced Security Coherent One-Way Quantum Key Distribution

AMIRHOSEIN DADAHHANI[1], SOHEIL HAJIBABA[1], HAMID ASGARI[1], MAJID KHODABANDEH[1], FATEMEH REZAZADEH[1], AZAM MANI[2], AND SEYED AHMAD MADANI[1]

[1]Quantum Communication Group, Iranian Center for Quantum Technologies (ICQTs), Tehran 1983969411, Iran
[2]Department of Engineering Science, College of Engineering, University of Tehran, Tehran 1439957131, Iran

Corresponding author: Seyed Ahmad Madani (seyed.ahmad.madani@gmail.com)

ABSTRACT Coherent One-Way (COW) is a simple and widely utilized quantum key distribution (QKD) protocol, favored in both experimental and commercial applications. In this paper, we compare the information that an eavesdropper, Eve, can acquire in both the 2-decoy and 1-decoy COW protocols. Our findings demonstrate that the 2-decoy protocol offers enhanced security compared to the original 1-decoy COW, all while preserving the simplicity of implementation. Furthermore, we have experimentally implemented the improved security COW-QKD (2-decoy protocol), achieving a secure key rate exceeding 0.5 kbps over a distance of 110 km (22 dB loss) in optical fiber, with an interference visibility greater than 80%. We also emphasize that monitoring the click rates of the data line detector for each state individually serves as a powerful method for detecting zero-error attacks.

INDEX TERMS Quantum key distribution, experimental quantum cryptography, coherent one-way.

I. INTRODUCTION

Recent advancements in quantum computing have raised significant concerns regarding the security of existing communication and cryptography methods [1], [2]. Consequently, researchers are actively seeking alternative secure communication methods [3], [4]. Fortunately, the principles of quantum mechanics provide a robust solution for establishing secure communication channels. Quantum Key Distribution (QKD) is a technique that provides an unconditionally secure means of communication between two parties [5]. Following the introduction of the first QKD protocol by Bennett and Brassard [6] in 1984 and subsequent experimental demonstrations [7] in 1992, several QKD protocols have been proposed and implemented. These protocols are generally categorized based on their implementation methods into Free-Space QKD [8]—which facilitates satellite-based QKD [9]—and fiber-optic QKD. While satellite QKD represents a promising way for global communication [10], fiber-based QKD has attracted much more attention due to the widespread availability of optical fiber infrastructure. This focus has led to the development of high-key-rate QKD systems capable of operating over distances of hundreds of kilometers [11], [12], [13], as well as the establishment of Quantum Networks [14], [15].

Among the various QKD protocols, the Coherent One-Way (COW) protocol [16], [17], [18] stands out for its popularity and commercialization [19], owing to its economical setup and relatively straightforward implementation. Since its initial implementation in 2009 [20], the COW protocol has undergone continuous development and enhancement [13], [21], [22], [23], [24], [25], [26], [27], [28], [29]. These modifications —which are mainly experimental— have resulted in improved key rates, longer achievable distances, and greater system integration [30]. Despite these advantages, there are still some ambiguities regarding the security of this protocol over long distances [31], [32]. In response, several strategies have been proposed to enhance its security through simple modifications to the original protocol [33], [34], [35].

One such strategy involves introducing two consecutive vacuum states $|00\rangle$, as a second decoy state, into the original

The associate editor coordinating the review of this manuscript and approving it for publication was Alessio Giorgetti.

COW protocol. In [35], by adding the second decoy state $|00\rangle$, the authors provide an estimation of the phase error rate (instead of visibility), and propose a security proof based on that. Additionally, [33] demonstrated that, compared to the original 1-decoy cow protocol, the 2-decoy version is more robust against certain zero-error attacks. In this paper, we compare the 2-decoy and 1-decoy protocols within a more general framework. We calculate the mutual information between Alice and Bob in both protocols and show that introducing the second decoy state $|00\rangle$, enhances the security by reducing the upper bound of information accessible to an eavesdropper, Eve. Notably, while the addition of the vacuum decoy state does not introduce extra experimental challenges, it significantly enhances the protocol's security and decreases the maximum information available to Eve by an order of magnitude. We then proceed to experimentally implement the enhanced security protocol and discuss its security aspects.

This paper is structured as follows: In Section II, we describe the 2-decoy protocol and highlight its advantages over the 1-decoy version. Section III outlines the experimental methods, followed by the presentation of results in Section IV. Finally, in Section V, we investigate zero-error attacks against COW and demonstrate that monitoring the gain of the data line detector for each input state individually, is an effective approach for detecting zero-error attacks.

II. 2-DECOY COW-QKD PROTOCOL

In this section, we describe the enhanced security COW protocol and show how the addition of a second decoy state, $|00\rangle$, reduces Eve's information on the shared key.

A. PROTOCOL DESCRIPTION

Similar to the original protocol, Alice prepares the logical states:

$$|0_L\rangle_k = |\alpha\rangle_{2k-1}|0\rangle_{2k}, \tag{1}$$
$$|1_L\rangle_k = |0\rangle_{2k-1}|\alpha\rangle_{2k}, \tag{2}$$

and the decoy states:

$$|D_0\rangle_k = |0\rangle_{2k-1}|0\rangle_{2k}, \tag{3}$$
$$|D_1\rangle_k = |\alpha\rangle_{2k-1}|\alpha\rangle_{2k}, \tag{4}$$

where $|0\rangle$ is the vacuum state, and $|\alpha\rangle$ is a coherent state with mean photon number $\mu = |\alpha|^2$. Alice transmits these states with the probabilities $P_{|0_L\rangle} = P_{|1_L\rangle} = (1-f)/2$ and $P_{|D_0\rangle} = P_{|D_1\rangle} = f/2$ through a quantum channel characterized by its transmission rate η_{ch}. It is evident that f represents the decoy ratio.

On the receiving side, Bob employs an asymmetric beamsplitter with a transmission coefficient t_B to split the incoming pulses into the data line and the monitoring line. In the data line, the raw key is obtained by measuring the arrival time of each pair of pulses with detector D_T (See Figure 1). In the monitoring line, an interferometer with two detectors, D_{M1} and D_{M2}, is used to check the coherence between adjacent non-vacuum pulses. The presence of an eavesdropper would disrupt this coherence, thus affecting the visibility defined as:

$$V = \frac{P(D_{M1}) - P(D_{M2})}{P(D_{M1}) + P(D_{M2})}, \tag{5}$$

where $P(D_{Mi})$ is the click probability of detector D_{Mi}.

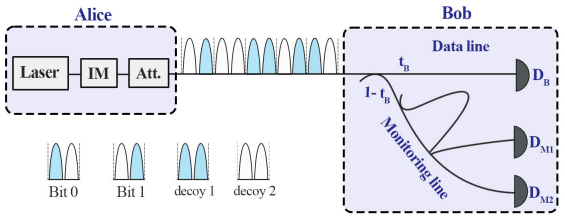

FIGURE 1. A schematic representation of the 2-decoy COW-QKD protocol.

B. SECURITY ADVANTAGE OF THE 2-DECOY PROTOCOL

The Csiszar-Korner bound [36] provides a lower limit for the secret key rate shared between Alice and Bob in the case of individual attacks:

$$r_{sk} \geq I(A:B) - \min\{I(A:E), I(B:E)\}, \tag{6}$$

where r_{sk} is the secret key rate, and $I(X:Y)$ denotes the mutual information between X and Y.

A smaller value of $\min\{I(A:E), I(B:E)\}$ indicates that Eve has obtained less information, thereby contributing to a more secure protocol. The values of $I(A:E)$ and $I(B:E)$ depend on the specific attack that Eve performs on the channel.

Here, we focus on the most effective Intercept-Resend attack applicable to the COW protocol to show that the 2-decoy protocol offers enhanced security. In this attack, Eve performs time-of-arrival measurements on the bits sent by Alice and subsequently prepares a state to send to Bob based on her measurement outcomes. We note that, Eve replaces the coherent state $|\alpha\rangle$ with a coherent state $|\beta\rangle$, where $|\beta|^2 \gg |\alpha|^2$. By selecting a sufficiently large $|\beta|^2$, Eve ensures that every non-empty state results in a detection click on Bob's side with almost complete probability. Therefore, if Bob's detectors exhibit no dark counts, he would accurately recover the same states that Eve holds. We also assume that Eve has replaced the channel between Alice and Bob with a lossless channel, maximizing her information gain about Alice's transmitted states. Furthermore, we assume Eve's detector operates ideally (i.e., it has full efficiency and no dark counts), and thus the only difference between Eve's and Alice's states arises from the non-orthogonality of the states $|00\rangle$, $|\alpha\alpha\rangle$, $|0\alpha\rangle$, $|\alpha 0\rangle$.

Next, we compute and compare the upper bounds of the information obtained by Eve during this attack for the 2-decoy and 1-decoy protocols.

1) 2-DECOY PROTOCOL

In this protocol, Alice transmits four different states $|00\rangle$, $|\alpha\alpha\rangle$, $|0\alpha\rangle$, and $|\alpha 0\rangle$ with probabilities $\frac{f}{2}$, $\frac{f}{2}$, $\frac{1-f}{2}$, and $\frac{1-f}{2}$,

TABLE 1. Eve's measurement outcomes corresponding to each state transmitted by Alice.

Alice's Transmitted State		Eve's Measured State	
Probability	State	State	Probability
$\frac{f}{2}$	$\|00\rangle$	$\|00\rangle$	1
$\frac{f}{2}$	$\|\alpha\alpha\rangle$	$\|00\rangle$ $\|0\alpha\rangle$ $\|\alpha0\rangle$ $\|\alpha\alpha\rangle$	$(e^{-\mu})^2$ $e^{-\mu}(1-e^{-\mu})$ $e^{-\mu}(1-e^{-\mu})$ $(1-e^{-\mu})^2$
$\frac{1-f}{2}$	$\|0\alpha\rangle$	$\|00\rangle$ $\|0\alpha\rangle$	$e^{-\mu}$ $(1-e^{-\mu})$
$\frac{1-f}{2}$	$\|\alpha0\rangle$	$\|00\rangle$ $\|\alpha0\rangle$	$e^{-\mu}$ $(1-e^{-\mu})$

respectively. Eve intercepts (steals) the transmitted states and performs time-of-arrival measurements on the signals. Considering the non-orthogonality of the sent states, Eve's measurement outcomes will correspond to the sent states with certain probabilities. Table1 summarizes the probabilities associated with different outcomes of Eve, conditioned to states transmitted by Alice. For instance, if Alice sends the state $|\alpha0\rangle$, Eve regards it as either $|00\rangle$ with probability $|\langle\alpha|0\rangle|^2$ or as $|\alpha0\rangle$ with probability $1-|\langle\alpha|0\rangle|^2$. The difference between the probability distributions of Alice's and Eve's states is clearly evident in Table1.

To calculate the mutual information between Alice and Eve, we need to determine ρ_{AE}, ρ_A, and ρ_E. To derive ρ_{AE}, we need the probability distribution $P(|\Phi_A\rangle, |\Psi_E\rangle)$, which corresponds to the probability that Alice transmits the state $|\Phi_A\rangle$ and Eve detects the state $|\Psi_E\rangle$. We calculate this joint probability distribution by using the conditional probability relation $P(|\Phi_A\rangle, |\Psi_E\rangle) = P(|\Psi_E\rangle||\Phi_A\rangle)P(|\Phi_A\rangle)$. After some straightforward calculations and using the values presented in Table1, we derive the probability distribution shown in Table2. From these probabilities, we construct the density matrix ρ_{AE} and compute $S(\rho_{AE})$. The density matrix of Alice can also be written as:

$$\rho_A = \frac{f}{2}|00\rangle\langle 00| + \frac{f}{2}|\alpha\alpha\rangle\langle\alpha\alpha| + \frac{1-f}{2}|0\alpha\rangle\langle 0\alpha| + \frac{1-f}{2}|\alpha0\rangle\langle\alpha0|, \tag{7}$$

and the density matrix of Eve is expressed as:

$$\begin{aligned}\rho_E = &\left(\frac{f}{2}(1+e^{-2\mu}) + (1-f)e^{-\mu}\right)|00\rangle\langle 00| \\ &+ \frac{f}{2}(1-e^{-\mu})^2|\alpha\alpha\rangle\langle\alpha\alpha| \\ &+ \left(\frac{f}{2}e^{-\mu}(1-e^{-\mu}) + \frac{(1-f)}{2}(1-e^{-\mu})\right)|0\alpha\rangle\langle 0\alpha| \\ &+ \left(\frac{f}{2}e^{-\mu}(1-e^{-\mu}) + \frac{(1-f)}{2}(1-e^{-\mu})\right)|\alpha0\rangle\langle\alpha0|,\end{aligned} \tag{8}$$

from which, we can calculate the entropies $S(\rho_A)$ and $S(\rho_E)$.

Using the method explained above, all the quantities $S(\rho_A)$, $S(\rho_E)$, and $S(\rho_{AE})$ will be obtained as functions of μ and f, and one can calculate the mutual information $I(A:E)$ for typical values of μ and f in a COW experiment. With our experimental values of $\mu = 0.11$ and $f = 0.25$ (discussed in the next section), we arrive at $I(A:E) \approx 0.00213$.

TABLE 2. The joint probability distribution of the states of Alice and Eve, for the intercept-resend attack to the 2-decoy protocol.

$\|\Psi_E\rangle \otimes \|\Phi_A\rangle$	Probability	$\|\Psi_E\rangle \otimes \|\Phi_A\rangle$	Probability
$\|00\rangle \otimes \|00\rangle$	$\frac{f}{2}$	$\|00\rangle \otimes \|0\alpha\rangle$	$\frac{1-f}{2}e^{-\mu}$
$\|0\alpha\rangle \otimes \|00\rangle$	0	$\|0\alpha\rangle \otimes \|0\alpha\rangle$	$\frac{1-f}{2}(1-e^{-\mu})$
$\|\alpha0\rangle \otimes \|00\rangle$	0	$\|\alpha0\rangle \otimes \|0\alpha\rangle$	0
$\|\alpha\alpha\rangle \otimes \|00\rangle$	0	$\|\alpha\alpha\rangle \otimes \|0\alpha\rangle$	0
$\|00\rangle \otimes \|\alpha\alpha\rangle$	$\frac{f}{2}e^{-2\mu}$	$\|00\rangle \otimes \|\alpha0\rangle$	$\frac{1-f}{2}e^{-\mu}$
$\|0\alpha\rangle \otimes \|\alpha\alpha\rangle$	$\frac{f}{2}e^{-\mu}(1-e^{-\mu})$	$\|0\alpha\rangle \otimes \|\alpha0\rangle$	0
$\|\alpha0\rangle \otimes \|\alpha\alpha\rangle$	$\frac{f}{2}e^{-\mu}(1-e^{-\mu})$	$\|\alpha0\rangle \otimes \|\alpha0\rangle$	$\frac{1-f}{2}(1-e^{-\mu})$
$\|\alpha\alpha\rangle \otimes \|\alpha\alpha\rangle$	$\frac{f}{2}(1-e^{-\mu})^2$	$\|\alpha\alpha\rangle \otimes \|\alpha0\rangle$	0

To find a lower bound for the secret key rate, according to Equation 6, we must also calculate $I(B:E)$ to ascertain which of $I(A:E)$ or $I(B:E)$ is smaller. The computation of $I(B:E)$ follows a similar procedure to that of $I(A:E)$. However, it is vital to note that the primary reason for the differences between the probability distributions of Eve's states and those of Bob's states stems from the dark counts of Bob's detector. This is due to the fact that Eve prepares coherent pulses with a high photon number, rendering states $|\beta\rangle$ and $|0\rangle$ nearly orthogonal. Consider the case that Eve has transmitted the state $|\beta0\rangle$ to Bob. Bob would recognize the state $|\alpha0\rangle$ with probability $1-p_d$ (assuming no dark count occurs) or the state $|\alpha\alpha\rangle$ with probability p_d (if dark counts are present in Bob's detector). Similarly, the probability distributions for the other states $|00\rangle$, $|\beta\beta\rangle$, and $|0\beta\rangle$ sent by Eve can be calculated. Ultimately, we find $I(B:E) \approx 0.00226$. As illustrated, $I(B:E)$ is larger than $I(A:E)$, which aligns with expectations given the high number of photons per pulse sent by Eve. Consequently, the second term in the Csiszar-Korner limit (Equation 6) for the 2-decoy protocol is 0.00213, indicating the information obtained by Eve per bit.

2) 1-DECOY PROTOCOL

To find the upper bound of the information obtained by Eve in the 1-decoy protocol, we follow the same steps as the previous case. In the 1-decoy protocol, Alice transmits the states $|\alpha\alpha\rangle$, $|0\alpha\rangle$, and $|\alpha0\rangle$ with the probabilities f, $\frac{1-f}{2}$, and $\frac{1-f}{2}$, respectively. The subsequent calculations follow straightforwardly, with detailed computations available in the appendix. Ultimately, we find $I(A:E) \approx 0.0680$ and $I(B:E) \approx 0.0751$.

As seen, the information available to Eve during the Intercept-Resend attack in the 2-decoy protocol is on the order of 0.002, while in the 1-decoy protocol, it is significantly higher, on the order of 0.07. Thus, the introduction of the second decoy state dramatically reduces the information available to Eve, thereby enhancing the security of the protocol. The calculated numbers, 0.07 and 0.002 for the 1-decoy and 2-decoy protocols, are based on our experimental

values for μ, f, and p_d. However, the superiority of the 2-decoy protocol over the 1-decoy protocol for standard values of μ, f, and p_d in COW experiments can easily be verified.

In the COW protocol, Alice prepares coherent pulses with a very low mean photon number μ such that the overlap $\langle\alpha|0\rangle$ remains significant. By incorporating the state $|00\rangle$, we introduce a state that is not orthogonal to the other states, thus increasing the overlap. This augmented overlap complicates state discrimination for Eve, resulting in a reduced information gain. This is indeed the key point of the enhanced security of the 2-decoy protocol and serves as the foundation of the security of all QKD protocols. For instance, the use of two non-orthogonal bases in the BB84 protocol underpins its security, as each prepared state in one basis is represented as a superposition in the other basis.

With this proof established, we proceeded to implement a COW-QKD experiment utilizing two decoy states.

III. EXPERIMENTAL METHODS

In this experiment, we have used a 1550 nm continuous wave (CW) DFB laser as the coherent source. A lithium-niobate intensity modulator (IM) prepares the COW states using the random input signal from a quantum random number generator (QRNG) [37]. The corresponding on/off signals coming from a high-speed field programmable gate array (FPGA) are shaped and amplified before being directed into the modulator. The prepared decoy ratio f is set at 0.25. The operational frequency of the driving intensity modulator, the pulse emission rate from Alice, and the gating frequency of the single-photon avalanche detectors (SPADs) are all synchronized at 100 MHz. At this working frequency, with a pulse width of 4.6 ns, we achieved an extinction ratio (ER) exceeding 15 dB.

To continuously monitor the output power—and consequently the mean photon number per pulse—and to provide feedback for the variable optical attenuator, we incorporated a 50:50 beam splitter following the modulator. One output from the beam splitter is directed to a monitor detector for power measurement, while the other goes to the quantum channel. By employing a variable optical attenuator alongside a fixed optical attenuator, we reduced the power to enter the single-photon regime, achieving a mean photon number $\mu = 0.11$.

On the Bob side, an optical isolator is implemented to prevent information leakage resulting from detection backfiring or back-reflections during potential Trojan horse attacks [23], [38]. A 90:10 beam splitter divides the input signal into the data and the monitoring lines. In the data line, a single-photon detector D_T measures the arrival times of incoming photons. The monitoring line, includes two single-photon detectors, D_{M1} and D_{M2}, that measure the output of an unbalanced Michelson interferometer. To ensure that the interferometry is polarization-independent, we employed two Faraday mirrors. The lengths of the interferometer arms are arranged such that the path difference matches the distance between two consecutive pulses. To guarantee stability and tunability of the interferometer, we incorporated thermal insulation and active temperature stabilization, along with a piezoelectric cell to maintain the destructive interference at D_{M2}.

To achieve synchronization, we employed a pulsed 1550 nm laser directly controlled by an FPGA. The pulses had a repetition rate of 50 MHz, which is half of the operational frequency. After traversing a separate classical line, the pulses were detected using a classical photodetector on the receiver side. The detected signal was then fed to the FPGA to gate the single-photon detectors and the time controller unit, serving as the start signal for time stamping. At room temperature, the dark count rate of the single-photon detectors is approximately 40 to 60 counts per second, with a dark count probability of around 5×10^{-7} per gate at 10% efficiency. A schematic representation of the setup is illustrated in Figure 2.

Once the raw key has been exchanged, we calculate the quantum bit error rate (QBER), visibility, and detection rates for the four states in the data line detector (see Section V). If the detection rates fall within the expected thresholds, we proceed to the post-processing stage. In the post processing, we initially perform the sifting process on the raw key, to derive the sifted key. To eliminate the quantum bit errors, we apply a syndrome decoding scheme utilizing Low-Density Parity-Check (LDPC) matrices [39], [40], [41]. While the corrected key can already be employed in cryptography applications, a classical privacy amplification step is essential. The final key is obtained by applying a universal hash function on the corrected key.

IV. EXPERIMENTAL RESULTS

In Section II-B, we demonstrated that the upper bound of information available to Eve through an Intercept-Receive attack in the 2-decoy protocol is approximately 0.002 per bit. Hence, we expect that the values obtained from our experimental data will be below this threshold. The information that Eve can obtain through an intercept-resend attack is given by [17]

$$I_{Eve} = (1 - V)\frac{1 + e^{-\mu\eta_{ch}}}{2e^{-\mu\eta_{ch}}}, \tag{9}$$

where η_{ch} represents the channel transmission rate. Therefore, Eve's information can be calculated by utilizing the visibility values that were determined in the laboratory and are illustrated in Figure 4.

Figure 3, shows the upper bound (red rectangles) and also the experimental values (blue triangles) of the information obtained by Eve. It is evident that Eve's information never reaches the upper bound calculated in Section II-B. It is important to note that the bound of 0.002 for Eve's information is derived under the assumption that she has replaced the communication channel between Alice and Bob with a lossless one, and it is why we see that this upper bound of the Eve's information is independent of distance (or channel loss). Conversely, if we relax this assumption, the bound of Eve's information would decrease as the distance

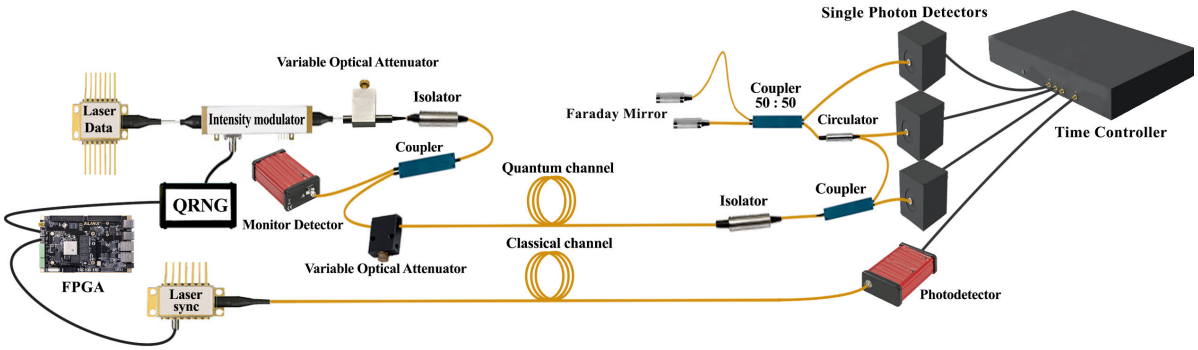

FIGURE 2. A schematic representation of the experimental setup for the implementation of the 2-decoy protocol.

increases. The purple circles in the same figure, correspond to the upper bound of Eve's information when we consider a lossy channel between Alice and Bob. The calculations for this scenario are analogous to those of section II, except that the value of μ should be replaced with $\mu\eta_{ch}$. Depending on the level of channel loss (ranging from 1 dB to 22 dB), η_{ch} varies between 79% and 0.6%. As anticipated, the experimental values for Eve's information consistently fall below this lossy upper bound.

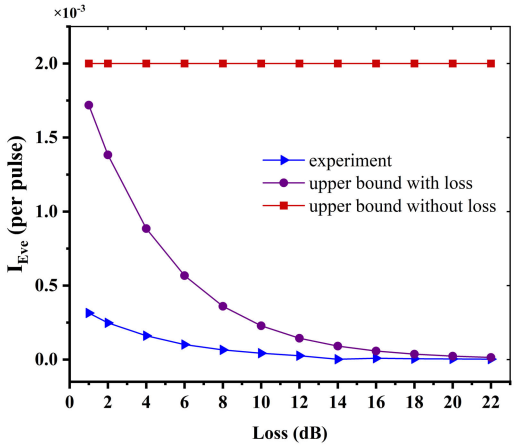

FIGURE 3. Eve's information as a function of channel loss.

The QBER, visibility, and key generation rates are presented in Figure 4, as functions of channel loss. As depicted in the figure, the QBER exhibits a clear upward trend with increasing distance. This increase of QBER can be attributed to the corresponding decrease of the signal-to-noise ratio (SNR), which causes dark counts to become more significant. Despite this upward trend, it is noteworthy that the QBER remains below 10% across the whole range of the distances considered. This threshold is critical because, in QKD protocols, a QBER below 10% is generally regarded as acceptable for secure key generation.

As it is evident in Figure 4, visibility also decreases as the distance increases. This behavior is a natural outcome of the same factors responsible for the rise in QBER—namely, the decline in SNR. However, despite its decrease, visibility remains relatively high, consistently above 80%.

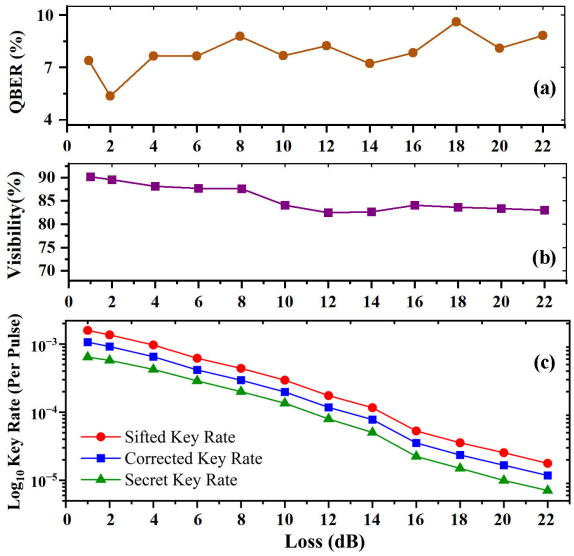

FIGURE 4. Experimental values of (a)QBER, (b)visibility, and (c)key generation rates as functions of channel loss.

Figure 4 also illustrates the sifted key rate, corrected key rate and secret key rate. The secret key rate is calculated from the final key rate, by subtracting the portions related to Eve's information. The Eve's information has been calculated in the presence of beam splitter and IR attack, the information that can be obtained by Eve per bit is given by [17]

$$I_{Eve} = \mu(1-\eta_{ch}) + (1-V)\frac{1+e^{-\mu\eta_{ch}}}{2e^{-\mu\eta_{ch}}}, \qquad (10)$$

where the first term is due to the beam splitter attack and the second term is regarded to the IR attack. Our findings indicate that even at a loss of 22 dB, corresponding to a distance of approximately 110 km when using low-loss optical fibers, a secret key rate on the order of 10^{-5} can still be achieved.

V. ZERO-ERROR ATTACK AGAINST COW PROTOCOL

The unconditional security of the COW protocol has not yet been conclusively established due to its structural characteristics. However, significant efforts have been made in the literature to address this issue [42], [43]. Consequently, the security of this protocol against various types of attacks remains an active area of research [34], [35], [44], [45], [46], [47], [48], [49], [50], [51], [52].

Within the context of the security of QKD protocols, there exists a group of attacks known as ''zero-error attacks.'' As the name suggests, these attacks cannot be detected by the parameters examined by Alice and Bob. In the COW protocol zero-error attacks are the attacks that cannot be identified through visibility and QBER.

In this section, we will examine two specific zero-error attacks and we propose a specific method for their detection in the COW protocol. It is essential to note that the security analysis presented here is entirely theoretical, and thus far, no laboratory implementations have been performed to execute these attacks. Based on the calculations conducted in this section, we investigate the additional parameters (detector gains) in conjunction with visibility and QBER during the post-processing phase To ensure that a zero-error attack has not occurred.

In addition to certain zero-error attacks applicable to all QKD protocols (like Beam-Splitter attack), there exist particular zero-error attacks specifically tailored for the COW protocol. In these scenarios, Eve exploits the structural properties of the COW protocol to execute attacks that are undetectable by either Alice or Bob [31], [32], [33], [53]. In fact, the COW protocol features two structural characteristics that facilitate the design of such attacks. The first is the presence of vacuum states, which lead to a lack of coherence between the vacuum pulses and their adjacent pulses. The second is the linear independence of the transmitted states, which allows for Unambiguous State Discrimination (USD) [54], [55] by Eve. We call these attacks as structural attacks.

Below, we will investigate two particular structural attacks explained in [33], and we will show that these attacks pose a security threat to the COW protocol if one solely relies on visibility to detect eavesdropping. In fact, these attacks can be easily detected if, in addition to monitoring visibility, appropriate statistical criteria for the detector clicks are also examined. ([33] introduced these attacks and investigate the effects of them on the statistical parameters like detection rates. In our work we investigate the detection rates for each input state individually. This approach allows us to establish a bound on the acceptable detection rates that can be verified during the post-processing stage).

A. THE USD3 ATTACK

In the USD3 attack, Eve performs Unambiguous State Discrimination on three-pulse sequences transmitted by Alice [33]. This measurement allows her to distinguish the sequence $0\alpha0$ from other possible three-pulse sequences (e.g., $\alpha0\alpha$, $0\alpha\alpha$, etc.). Eve selects the state $0\alpha0$ for her discrimination because she seeks a sequence with vacuum pulses at both ends, to avoid breaking the coherence. If the unambiguous measurement is successful, Eve prepares a similar state and sends it to Bob. Otherwise, she sends nothing.

This attack does not affect visibility or QBER; therefore, it generally qualifies as a QKD zero-error attack. However, we will show that in the COW protocol, Alice and Bob can easily detect Eve if they utilize a portion of their data to compute some extra quantities (rates) $G_{\alpha0}$, $G_{0\alpha}$, $G_{\alpha\alpha}$, and G_{00}, where G_{ψ} is the probability that Alice transmits the state ψ and Bob also receives the same state ψ.

Let us examine the variations in the receiving rate of the state $|\alpha0\rangle$, following the implementation of a USD3 attack. As defined above, let $G_{\alpha0}$ represent the probability that Alice transmits the state $\alpha0$ and Bob also receives the same state when no eavesdropping has occurred, and let $G'_{\alpha0}$ denote the same probability when Eve has intervented with a USD3 attack. Following, we investigate the relation between $G_{\alpha0}$ and $G'_{\alpha0}$

In the USD3 attack, Eve separates three-pulse sequences from Alice's transmitted states. If Alice sends $|\alpha0\rangle$, it has a probability of 1/2 for being positioned on the right side of the three-pulse sequence and a probability of 1/2 for being on the left side. If $|\alpha0\rangle$ is on the left, Eve blocks the sequence as she is searching for a three-pulse sequence of the form $0\alpha0$. If $|\alpha0\rangle$ is on the right side, Eve's action depends on the pulse that is located on the left end of the sequence.

Figure 5 illustrates different situations that may occur, together with their corresponding probabilities. As an instance, the transmitted state next to the right $|\alpha0\rangle$ is $|0\alpha\rangle$ with the probability of $\frac{1-f}{2}$, and Eve will never achieve a successful USD3 measurement in this situation, and will therefore block the state. Another possible situation occurs when $|\alpha0\rangle$ follows another $|\alpha0\rangle$, which also happens with a probability of $\frac{1-f}{2}$. In this case, Eve may either succeed in her measurement with probability P_c and send a sequence $0\alpha0$ to Bob, or fail with probability $1-P_c$ and thus block the sequence. Other situations and their probabilities, together with corresponding actions of Eve are illustrated in Figure 5.

Ultimately, by executing a USD3 attack, Eve reduces the receiving rate of $|\alpha0\rangle$. The probability of receiving the state $|\alpha0\rangle$ (by Bob), after the USD3 attack is related to the initial probability by

$$G'_{\alpha0} = \frac{1}{2} \times \left(\frac{1-f}{2} \times P_c + \frac{f}{2} \times P_c \right) G_{\alpha0} = \frac{P_c}{4} G_{\alpha0}. \quad (11)$$

Therefore, after a USD3 attack, the receiving rate of $|\alpha0\rangle$ will decrease by more than a factor of $\frac{1}{4}$.

Similar calculations show the same result for the receiving rate of $|0\alpha\rangle$, i.e. $G'_{0\alpha} = P_c G_{0\alpha}/4$. The receiving rates of both $|\alpha0\rangle$ and $|0\alpha\rangle$ decrease significantly after a USD3 attack. However, the situation is even worse for the two decoy states $|00\rangle$ and $|\alpha\alpha\rangle$. If Eve executes a USD3 attack on these pulses,

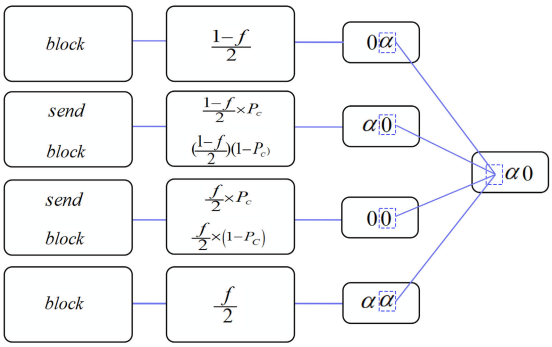

FIGURE 5. Eve implements a USD3 attack. The graph shows various situations of three-pulse sequences (and their corresponding probabilities) when Alice sends $|\alpha 0\rangle$.

G'_{00} and $G'_{\alpha\alpha}$ will both vanish, resulting in Bob receiving no decoy states. This occurs because Eve is searching for the sequence $0\alpha 0$ among all possible three-pulse sequences, and the two decoy states $|00\rangle$ and $|\alpha\alpha\rangle$ can never be a part of such sequence.

B. THE USD4 ATTACK

This attack is similar to USD3, except that Eve performs her measurements on four-pulse sequences and tries to unambiguously discriminate the state $0\alpha\alpha 0$ from all other possible four-pulse sequences [33]. Employing a similar analysis as in USD3, it is straightforward to show that, in the USD4 attack, the decoy states will be completely blocked, and the receiving rates of $|\alpha 0\rangle$ and $|0\alpha\rangle$ will decrease by more than a factor of $1/4$. Table 3 summarizes the results obtained for the receiving rates in the presence of USD3 and USD4 attacks.

TABLE 3. Bob's detection rates after USD3 and USD4 attacks.

	USD3	USD4
$G'_{\alpha 0}$	$\frac{P_c^{0\alpha 0}}{4}\times G_{\alpha 0}$	$\frac{1-f}{4}\times P_c^{0\alpha\alpha 0}\times G_{\alpha 0}$
$G'_{0\alpha}$	$\frac{P_c^{0\alpha 0}}{4}\times G_{0\alpha}$	$\frac{1-f}{4}\times P_c^{0\alpha\alpha 0}\times G_{0\alpha}$
G'_{00}	0	0
$G'_{\alpha\alpha}$	0	0

The amount of reduction in receiving rates is significant and detectable by Alice and Bob. Therefore, if Eve performs such attacks, Alice and Bob can easily identify her presence and halt the key exchange process. Briefly stated, the USD3 and USD4 attacks cannot be regarded as security threats, if in addition to visibility and QBER, Alice and Bob check the expected thresholds of the receiving rates for each state separately. This consideration has been incorporated into our post-processing operations, such that an alarm will trigger if any of the receiving rates fall below the expected threshold.

We have discussed two specific zero-error attacks in detail; still, additional zero-error attacks warrant further investigation. For instance, Ref. [32] introduces one of the most potent zero-error attacks, claiming that the secure length of the COW protocol is less than 50 km. However, we note that the mentioned attack can also become detectable by examining the receiving rates of each state, rather than the overall rate. The authors have also briefly hinted to this point in the discussion section.

VI. CONCLUSION

In conclusion, we demonstrated that although there is no unconditional security proof for the Coherent One-Way (COW) quantum key distribution protocol, its security can be improved through minor modifications, such as the inclusion of a second decoy state $|00\rangle$. We initially conducted a theoretical investigation of the enhanced security protocol, establishing the advantages of the 2-decoy protocol compared to the original version. Subsequently, we experimentally implemented this enhanced security protocol and compared the experimental results with the theoretical predictions. Furthermore we illustrated that, for the COW protocol, some zero-error attacks can be identified by monitoring the gains of different states. These findings indicate a significant enhancement and pave the way for future modifications.

APPENDIX

2-DECOY PROTOCOL

$I(B:E)$ can be computed in a manner analogous to $I(A:E)$. The density matrices of Alice and Eve are represented by Equations 7 and 8, respectively. As explained in the main text, it is evident that the probability distribution of Eve's states differs from that of Alice's initial states. Table 4 presents the probabilities of Eve's detected states.

TABLE 4. Eve's states and their probabilities when she performs the intercept-resend attack to the 2-decoy protocol.

Eve's detected states	
State	Probability
$\|00\rangle$	$\frac{f}{2}(1+e^{-2\mu})+(1-f)e^{-\mu}=P_1$
$\|\alpha\alpha\rangle$	$\frac{f}{2}(1-e^{-\mu})^2=P_2$
$\|0\alpha\rangle$	$\frac{f}{2}e^{-\mu}(1-e^{-\mu})+\frac{1-f}{2}(1-e^{-\mu})=P_3$
$\|\alpha 0\rangle$	$\frac{f}{2}e^{-\mu}(1-e^{-\mu})+\frac{1-f}{2}(1-e^{-\mu})=P_4$

TABLE 5. Bob's measurement outcomes conditioned to each of Eve's transmitted states when Eve performs the intercept-resend attack to the 2-decoy protocol.

Eve's transmitted state		Bob's measured state	
Probability	State	State	Probability
P_1	$\|00\rangle$	$\|00\rangle$ $\|0\alpha\rangle$ $\|\alpha 0\rangle$ $\|\alpha\alpha\rangle$	$(1-P_d)^2$ $P_d(1-P_d)$ $P_d(1-P_d)$ P_d^2
P_2	$\|\beta\beta\rangle$	$\|\alpha\alpha\rangle$	1
P_3	$\|0\beta\rangle$	$\|0\alpha\rangle$ $\|\alpha\alpha\rangle$	$1-P_d$ P_d
P_4	$\|\beta 0\rangle$	$\|\alpha 0\rangle$ $\|\alpha\alpha\rangle$	$1-P_d$ P_d

According to the results summarized in Table 4, Eve transmits the states $|00\rangle$, $|\beta\beta\rangle$, $|0\beta\rangle$, and $|\beta 0\rangle$ to Bob with probabilities P_1, P_2, P_3, and P_4, respectively. Due to the high intensity of the pulses transmitted by Eve, the dark count of

Bob's detector is the only reason of the difference between the states transmitted by Eve and the results inferred by Bob. For instance, if Eve sends $|0\beta\rangle$, Bob will detect either $|0\alpha\rangle$ with a probability of $1 - P_d$ or $|\alpha\alpha\rangle$ with a probability of P_d. The probabilities of Bob's detected states, conditioned on Eve's transmitted states, are presented in Table 5. Using the conditional probabilities of Table 5, one can easily find the probability distribution of Bob's states, shown in Table 6.

TABLE 6. Bob's states and their probabilities when Eve performs the intercept-resend attack to the 2-decoy protocol.

Bob's measured states	
State	Probability
$\|00\rangle$	$P_1(1-P_d)^2$
$\|0\alpha\rangle$	$P_1P_d(1-P_d)+P_3(1-P_d)$
$\|\alpha 0\rangle$	$P_1P_d(1-P_d)+P_4(1-P_d)$
$\|\alpha\alpha\rangle$	$P_1P_d^2+P_2+P_3P_d+P_4P_d$

Considering the probabilities of Tables 4, 5, and 6, we can find the density matrices ρ_{EB}, ρ_B, and ρ_E and calculate their Von-Neumann entropies. With $S(\rho_B)$, $S(\rho_E)$, and $S(\rho_{BE})$ determined, we can easily compute $I(B:E)$. The comparison between $I(B:E)$ and $I(A:E)$ is discussed in the main text.

1-DECOY PROTOCOL

In this protocol, Alice sends three states $|\alpha\alpha\rangle$, $|0\alpha\rangle$, and $|\alpha 0\rangle$ with probabilities f, $\frac{1-f}{2}$, and $\frac{1-f}{2}$, respectively. While Alice does not transmit $|00\rangle$, considering the non-orthogonality of $|0\rangle$ and $|\alpha\rangle$, the detectors of Eve or Bob may some times not register a click. This is equivalent to the occurrence of the state $|00\rangle$. For example, if Alice sends $|\alpha\alpha\rangle$, Eve's measurement outcomes will be $|\alpha\alpha\rangle$, $|0\alpha\rangle$, $|\alpha 0\rangle$, and $|00\rangle$, occurring with probabilities of $(1-e^{-\mu})^2$, $e^{-\mu}(1-e^{-\mu})$, $e^{-\mu}(1-e^{-\mu})$, and $e^{-2\mu}$, respectively. The remaining calculations follow a similar approach to those of the 2-decoy protocol, and hence, we omit the details and step-by-step calculations. The final values are presented in the main text.

ACKNOWLEDGMENT

The authors thank Reza Asadi, CEO of Iranian Center for Quantum Technologies (ICQTs) and all colleagues, who helped them in this work, especially Mehdi Bozorgi, Reza Omidi, Majid Jaberi, and Seyed Mahdi Ameli.

DISCLOSURES

The authors declare no conflicts of interest.

DATA AVAILABILITY

Data underlying the results presented in this article are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999.

[2] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," 2018, *arXiv:1804.00200*.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.*, vol. 74, no. 1, p. 145, 2002.

[4] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-quantum Cryptography*. Cham, Switzerland: Springer, 2009, pp. 1–14.

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, p. 1301, 2009.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

[8] S.-K. Liao et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Aug. 2017.

[9] Y. Xue, "Satellite-relayed intercontinental quantum network," *J. Phys., Conf. Ser.*, vol. 2229, no. 1, Mar. 2022, Art. no. 012028.

[10] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, no. 1, pp. 1–12, Nov. 2016.

[11] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," *Appl. Phys. Lett.*, vol. 96, no. 16, Apr. 2010.

[12] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, no. 1, p. 163, 2017.

[13] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photon.*, vol. 9, no. 3, pp. 163–168, Mar. 2015.

[14] D. Stucki et al., "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, Dec. 2011, Art. no. 123001.

[15] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, p. 10387, May 2011.

[16] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography," 2004, *arXiv: quant-ph/0411022*.

[17] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, no. 19, Nov. 2005.

[18] D. Stucki, S. Fasel, N. Gisin, Y. Thoma, and H. Zbinden, "Coherent one-way quantum key distribution," *Proc. SPIE*, vol. 6583, pp. 194–197, May 2007.

[19] . [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/cerberis-xg-qkd-system/

[20] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, "Continuous high speed coherent one-way quantum key distribution," *Opt. Exp.*, vol. 17, no. 16, p. 13326, 2009.

[21] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New J. Phys.*, vol. 12, no. 6, Jun. 2010, Art. no. 063027.

[22] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys.*, vol. 11, no. 7, Jul. 2009, Art. no. 075003.

[23] N. Walenta et al., "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New J. Phys.*, vol. 16, no. 1, Jan. 2014, Art. no. 013047.

[24] J. Constantin, R. Houlmann, N. Preyss, N. Walenta, H. Zbinden, P. Junod, and A. Burg, "An FPGA-based 4 mbps secret key distillation engine for quantum key distribution systems," *J. Signal Process. Syst.*, vol. 86, no. 1, pp. 1–15, Jan. 2017.

[25] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, "Modulator-free coherent-one-way quantum key distribution," *Laser Photon. Rev.*, vol. 11, no. 4, Jul. 2017, Art. no. 1700067.

[26] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, Nov. 2018, Art. no. 190502.

[27] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," *Appl. Phys. Lett.*, vol. 112, no. 17, Apr. 2018.
[28] P. Malpani, S. Kumar, and A. Pathak, "Implementation of coherent one way protocol for quantum key distribution up to an effective distance of 145 km," *Opt. Quantum Electron.*, vol. 56, no. 8, p. 1369, Jul. 2024.
[29] G. K. Shaw, S. Sridharan, and A. Prabhakar, "Optimal temporal filtering for COW-QKD," in *Proc. IEEE Int. Conf. Signal Process. Commun. (SPCOM)*, Jul. 2022, pp. 1–4.
[30] R. Sax, A. Boaron, G. Boso, S. Atzeni, A. Crespi, F. Grünenfelder, D. Rusca, A. Al-Saadi, D. Bronzi, S. Kupijai, H. Rhee, R. Osellame, and H. Zbinden, "High-speed integrated QKD system," *Photon. Res.*, vol. 11, no. 6, p. 1007, 2023.
[31] J. González-Payo, R. Trényi, W. Wang, and M. Curty, "Upper security bounds for coherent-one-way quantum key distribution," *Phys. Rev. Lett.*, vol. 125, no. 26, Dec. 2020, Art. no. 260510.
[32] R. Trényi and M. Curty, "Zero-error attack against coherent-one-way quantum key distribution," *New J. Phys.*, vol. 23, no. 9, Sep. 2021, Art. no. 093005.
[33] C. Branciard, N. Gisin, N. Lutkenhaus, and V. Scarani, "Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography," *Quantum Inf. Comput.*, vol. 7, no. 7, pp. 639–664, Sep. 2007.
[34] E. Lavie and C. C.-W. Lim, "Improved coherent one-way quantum key distribution for high-loss channels," *Phys. Rev. Appl.*, vol. 18, no. 6, Dec. 2022, Art. no. 064053.
[35] R.-Q. Gao, Y.-M. Xie, J. Gu, W.-B. Liu, C.-X. Weng, B.-H. Li, H.-L. Yin, and Z.-B. Chen, "Simple security proof of coherent-one-way quantum key distribution," *Opt. Exp.*, vol. 30, no. 13, p. 23783, 2022.
[36] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[37] S. Hajibaba, A. Dadahkhani, and S. A. Madani, "Fabrication and evaluation of high-quality and low-cost quantum random number generators," *Opt. Continuum*, vol. 1, no. 7, p. 1572, 2022.
[38] A. Vakhitov, V. Makarov, and D. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *J. Modern Opt.*, vol. 48, no. 13, pp. 2023–2038, Nov. 2001.
[39] E. Kiktenko, A. Trushechkin, Y. Kurochkin, and A. Fedorov, "Post-processing procedure for industrial quantum key distribution systems," *J. Phys., Conf. Ser.*, vol. 741, Aug. 2016, Art. no. 012081.
[40] E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov, "Symmetric blind information reconciliation for quantum key distribution," *Phys. Rev. Appl.*, vol. 8, no. 4, Oct. 2017, Art. no. 044017.
[41] E. O. Kiktenko, A. O. Malyshev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, and A. K. Fedorov, "Error estimation at the information reconciliation stage of quantum key distribution," *J. Russian Laser Res.*, vol. 39, no. 6, pp. 558–567, Nov. 2018.
[42] M. Mafu, A. Marais, and F. Petruccione, "A necessary condition for the security of coherent-one-way quantum key distribution protocol," *Appl. Math. Inf. Sci.*, vol. 8, no. 6, pp. 2769–2773, Nov. 2014.
[43] M. Koashi, "Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse," *Phys. Rev. Lett.*, vol. 93, no. 12, Sep. 2004, Art. no. 120501.
[44] C. Branciard, N. Gisin, and V. Scarani, "Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography," *New J. Phys.*, vol. 10, no. 1, Jan. 2008, Art. no. 013031.
[45] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, "Characterising the correlations of prepare-and-measure quantum networks," *npj Quantum Inf.*, vol. 5, no. 1, p. 17, Feb. 2019.
[46] L. Lydersen, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocols," *J. Modern Opt.*, vol. 58, no. 8, pp. 680–685, May 2011.
[47] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, "Security of distributed-phase-reference quantum key distribution," *Phys. Rev. Lett.*, vol. 109, no. 26, Dec. 2012, Art. no. 260501.
[48] S. N. Molotkov and T. A. Potapova, "Security of quantum key distribution with a laser reference coherent state, resistant to loss in the communication channel," *Laser Phys. Lett.*, vol. 12, no. 6, Jun. 2015, Art. no. 065201.
[49] D. A. Kronberg, A. S. Nikolaeva, Y. V. Kurochkin, and A. K. Fedorov, "Quantum soft filtering for the improved security analysis of the coherent one-way quantum-key-distribution protocol," *Phys. Rev. A, Gen. Phys.*, vol. 101, no. 3, Mar. 2020, Art. no. 032334.
[50] D. A. Kronberg, E. O. Kiktenko, A. K. Fedorov, and Y. V. Kurochkin, "Analysis of coherent quantum cryptography protocol vulnerability to an active beam-splitting attack," *Quantum Electron.*, vol. 47, no. 2, pp. 163–168, Feb. 2017.
[51] M. Stoilov, "A classical attack on the coherent one way protocol for quantum key distribution," *arXiv:2003.07198*, 2020.
[52] M.-Y. Li, X.-Y. Cao, Y.-M. Xie, H.-L. Yin, and Z.-B. Chen, "Finite-key analysis for coherent one-way quantum key distribution," *Phys. Rev. Res.*, vol. 6, no. 1, Jan. 2024, Art. no. 013022.
[53] M. Curty, "Foiling zero-error attacks against coherent-one-way quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 104, no. 6, Dec. 2021, Art. no. 062417.
[54] A. Chefles, "Unambiguous discrimination between linearly independent quantum states," *Phys. Lett. A*, vol. 239, no. 6, pp. 339–347, Mar. 1998.
[55] A. Chefles and S. M. Barnett, "Optimum unambiguous discrimination between linearly independent symmetric states," *Phys. Lett. A*, vol. 250, nos. 4–6, pp. 223–229, Dec. 1998.

AMIRHOSEIN DADAHKHANI received the M.S. degree in photonics from the Laser and Plasma Research Institute (LAPRI), Shahid Beheshti University, Tehran, Iran, in 2018. Then, he joined Iranian Center for Quantum Technologies (ICQTs), as an Experimental Researcher and works on quantum communication project. His research interests include quantum physics, quantum communication, quantum key distribution, quantum networks, and fiber optics.

SOHEIL HAJIBABA received the Master of Science degree in solid-state physics from the University of Tehran, in 2020. He is an Experimental Physicist. He joined Iranian Center for Quantum Technologies (ICQTs), as a Researcher. His research interest includes quantum physics and technologies.

HAMID ASGARI received the master's degree in photonics from Kharazmi University, in 2018. He is currently an Experimental Expert with Iranian Center for Quantum Technologies (ICTQs). His main research interests include nonlinear optics and quantum sciences.

MAJID KHODABANDEH received the M.Sc. degree in atomic molecular physics from Tarbiat Modares University, Tehran, Iran, where he is currently pursuing the Ph.D. degree in optics and laser focusing on advanced topics in quantum communication and photonics. His current research interests include quantum communication, quantum information, quantum metrology, nonlinear optics, quantum optics, and interferometry.

FATEMEH REZAZADEH received the M.Sc. and Ph.D. degrees in quantum information and computation from the Sharif University of Technology, Tehran, Iran, in 2014 and 2020, respectively. She was Postdoctoral Researcher with the Sharif University of Technology, in 2021. She is currently a Researcher with Iranian Center for Quantum Technologies (ICQTs), Tehran. Her current research interest includes the security of quantum key distribution.

AZAM MANI received the B.Sc. degree in physics from the Sharif University of Technology, Tehran, Iran, in 2007, the M.Sc. degree from the Quantum Information Group, Physics Department, Sharif University of Technology, and the Ph.D. degree from the Quantum Information Group, Physics Department, Sharif University of Technology, in 2014. Following her doctoral studies, she was a Postdoctoral Researcher with the Quantum Information Group, for two years. Currently, she holds the position of an Assistant Professor with the College of Engineering, University of Tehran, Iran. Her current research interests include quantum key distribution (QKD) and the fundamental principles of quantum information, such as quantum coherence.

SEYED AHMAD MADANI received the B.Sc. degree in electrical electronic engineering from the University of Tabriz, in 2011, the M.Sc. degree in electronic/photonic engineering from the Amirkabir University of Technology, Tehran, in 2014, and the Ph.D. degree in electronic/photonic engineering from the University of Tabriz, in 2021. Since 2018, he has been the Director of the Quantum Communication Project, Iranian Quantum Technologies Center. His research interests include quantum communication, quantum key distribution, and quantum optics.