Trusted Reconfigurable Intelligent Surface for Multi-User Quantum Key Distribution

Steven Kisseleff, *Senior Member, IEEE,* and Symeon Chatzinotas, *Fellow, IEEE*

***Abstract*—We consider a multi-user quantum key distribution (QKD) system based on free-space optics (FSO) in terrestrial environment. Due to obstacles in the signal path, FSO-QKD is heavily affected by decoherence and other harmful effects. In order to avoid the performance degradation, trusted nodes (TNs) are introduced in the QKD network. However, in absence of alternative signal routes, the classical data and the quantum key are relayed by the same TN, which makes it a promising target for an eavesdropping attack. In order to address this issue, we explore the use of a trusted reconfigurable intelligent surface (RIS) that passively reflects the classical signals and manipulates them to make the encryption consistent with the distributed keys. The concept is supported by numerical simulations with multiple FSO-QKD users and an eavesdropper. We demonstrate that the level of data protection is very high with the proposed concept even in case of a successful attack on the trusted RIS and a complete key acquisition by the eavesdropper.**

***Index Terms*—Quantum key distribution, free-space optics, trusted node, reconfigurable intelligent surface, precoding**

I. Introduction

A. Quantum key distribution with trusted nodes

Quantum key distribution (QKD) is one of the approaches to withstand the potential threat of quantum computers, which are expected to provide sufficient computational power to break the existing data encryption using Shor's fast factorization algorithm [1] and parallel computation [2]. Hence, QKD has been proposed as a paradigm shift that relies on the laws of quantum physics rather than on the computational complexity [3]. In particular, the so-called no-cloning theorem suggests that the eavesdropping on quantum channels can be detected by the receiver [4]. Accordingly, QKD protocols have been proposed to ensure that only the key is retained, which is identified as not eavesdropped. Through this, QKD is capable of guaranteeing an unconditional security and represents a very active research field [5].

The implementation of QKD systems has become increasingly mature in the recent years. Nevertheless, the use of QKD based on free-space optics (FSO) in terrestrial domain is rather limited due to the rich scattering environment, especially in urban areas, which often lead to the decoherence of the quantum states. Through this, the reliability of the key distillation and the eavesdropping detection become challenging. A similar problem occurs for the transmissions over large distances using optical fibers. To combat these issues, intermediate trusted nodes (TNs) are suggested to extend the transmission distance or avoid signal blockage by means of simply relaying the key in a hop-by-hop manner [6]–[8]. Accordingly, trusted nodes are likely to be part of the future quantum networks.

Typically, TNs perform the following actions[1]: QKD with the source and the destination over optical channels as well as relaying of the classical data and the key over optical or RF channels[2]. Since this node has access to the data and the key, i.e., the data can be readily decrypted, such nodes represent the potential targets of active eavesdropping attacks [10].

To address this issue, we propose to employ the recently introduced reconfigurable intelligent surface (RIS).

B. Reconfigurable intelligent surfaces for QKD

RIS consists of multiple reconfigurable reflective elements that have the capability to manipulate the signal features. Through this, the radio environment can be manipulated to benefit the system performance [11]. In this context, the main advantages of RIS are related to increased spatial diversity, reduced power consumption and low latency. The advantages of RIS-aided transmission have been analyzed for various systems and scenarios so far, such as 6G [12], satellite communications [13], challenging environments [14], etc. In addition, the use of RIS to enhance the physical layer security has been extensively studied (e.g. [15], [16]) typically aiming at the maximization of the secrecy rate. Moreover, RIS have been utilized for the generation of secret keys based on the reciprocity of wireless channels [17], [18].

Unlike other publications on RIS-aided secure networking, in this paper, we propose to employ RIS as part of a TN for a multi-user QKD system. Unlike traditional TNs, RIS-based TN does not retransmit the classical data and the key after the QKD process. Instead, the data transmitted by the BS is not received, but merely reflected towards the UE. Hence, it is not possible for the eavesdropper to obtain the secret information even in case of a successful attack on the TN's memory. Furthermore, the proposed non-linear beamforming contributes to data protection by destroying the correlation between the signals received by the intended user and the eavesdropper. Correspondingly, the security level of RIS-based TNs is much higher than that of the traditional TNs.

This work was supported by Luxembourg National Research Fund (FNR) under the CORE project RISOTTI C20/IS/14773976.

The authors are with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg. Email: steven.kisseleff@uni.lu, symeon.chatzinotas@uni.lu.

[1]Note that the measurement-device-independent (MDI) protocol can be employed to avoid exposing the key to the node. However, according to [9], it is impossible to build QKD networks solely using the MDI nodes, which makes the use of trusted nodes inevitable [10].

[2]In this work, we assume that the classical signals are transmitted over RF channels. Through this, the transmission of classical and quantum information is perfectly decoupled and can be executed simultaneously.

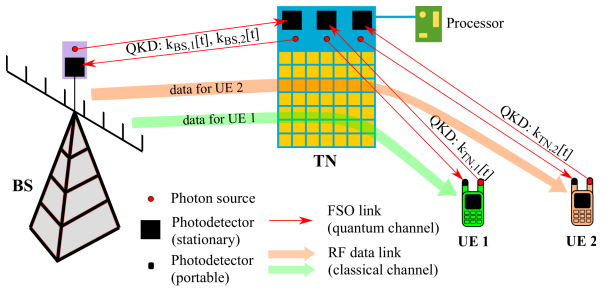

Fig. 1. Considered scenario incl. BS, trusted RIS and two UEs.

C. Contributions

The contributions of the paper are summarized as follows:

- the concept of RIS-based TN for multi-user QKD is proposed and its operation is described;
- the optimization problem for RIS-based over-the-air data encryption is identified, mathematically formulated and solved via iterative linearization.
- thorough simulations of the proposed concept are provided for a realistic street scenario.

The remainder of the paper is organized as follows. Section II describes the employed system model and identifies the design problem. In Section III, the concept of RIS-based TN and the corresponding optimization approach are proposed. Then, the numerical results are shown in Section IV. Subsequently, the paper is concluded in Section V.

Notation

For vectors and matrices we use bold font. $(\cdot)^T$, $(\cdot)^H$ and $(\cdot)^{-1}$ denote transpose, hermitian transpose and inverse matrix operation, respectively. $\mathrm{diag}(\cdot)$ operator maps the diagonal elements of a matrix onto a vector. $\mathrm{sign}(x)$ returns 1 for $x \geq 0$ and -1 otherwise. $\mathcal{E}_t\{\cdot\}$ is an expectation operator. j is the imaginary unit. In addition, $\mathcal{R}\{\cdot\}$ and $|\cdot|$ denote the real part and the absolute value of a complex number, respectively.

II. System Model

A. Assumptions

We consider a non-line-of-sight (NLoS) multi-user downlink scenario, where the base station (BS) equipped with N antennas provides simultaneous secure communication to M single-antenna users (UEs) on the street while the direct signal paths between the BS and the UEs are blocked by obstacles. Accordingly, a TN is deployed in a position, where LoS propagation is possible between BS and TN as well as between TN and UEs. To enable the FSO-QKD, all nodes, i.e. BS, TN and UEs, are equipped with optical transceivers (photon sources and photodetectors) in addition to the classical RF antennas, see Fig. 1. In addition, the TN is equipped with RIS and a processor for the reconfiguration and QKD purposes.

The transmission of quantum information is decoupled from the classical data transmission. Due to the assumed LoS propagation and relatively short transmission distances in urban scenarios, the QKD process is straightforward. For instance, we assume the original BB84 protocol [3] with the UE authentication via [19]. The QKD executed between the BS and the TN produces a set of keys $k_{\mathrm{BS},m}[t]$, $\forall m, t$, which is used to encrypt the transmitted data packets. Also, TN performs QKD with the UEs and obtains another set of keys, i.e. $k_{\mathrm{TN},m}[t]$, $\forall m, t$. Here, we assume that the length of the data packet K is selected according to the shortest key of the two links. This packet lengths is thus related to the effective key exchange rate (KER) for the entire route BS↔RIS↔UE. The classical data transmission can be initiated by TN after both QKD processes are finished by sending a short packet to the BS, which would indicate the length of the key K.

According to [3], the unconditional security with QKD can be only guaranteed, if the key is used only once (so-called one-time pad). Accordingly, the classical data rate should match the KER, which is typically very low, i.e. a few kqbit/s. Hence, high data rates for the transmission of classical data are not required and we focus on a low-order modulation scheme, i.e. binary phase-shift keying (BPSK). For simplicity, we consider the encryption of data symbols using qbits from the quantum keys via sign flipping. Specifically, the sign of a symbol is flipped in case of qbit '1' and remains unchanged in case of qbit '0'. Further, the encryption is applied after the forward error correction (FEC) encoding of the data packets.

The RIS is implemented as part of the TN and consists of L elements[3]. Typically, the optimization of the RIS reflection coefficients is performed at the BS and then sent to the RIS via separate control signaling. We restrict ourselves to a low-resolution reflection modulation, i.e. each phase shift can be selected only from a 1-bit resolution set $\{-1, 1\}$. Through this, the total amount of control signaling between the BS and the TN is significantly reduced compared to high resolution of phase shifts especially for a RIS with many reflective elements.

We assume that the RIS can be fully reconfigured on a symbol-by-symbol basis. This assumption is realistic thanks to the low data rate (equal to the KER) and the recent progress in fast reconfigurable metasurfaces and Schottky diodes with switching time in the order of nanoseconds [20], [21].

B. Signal propagation

For all links of the system, we assume quasi-static block-fading channels, which are perfectly known to the BS from a thorough channel estimation due to the static deployment of BS and TN as well as the portable FSO equipment of UEs. Although some channel estimation errors may still occur in practice, the impact of imperfect channel state information is beyond the scope of this work. The received classical data symbol at the mth UE in the tth symbol interval is given by

$$y_m[t] = \mathbf{h}_{2,m}^T \mathbf{Z}[t] \mathbf{H}_1 \mathbf{x}[t] + w_m[t], \ \forall m, t, \tag{1}$$

where $\mathbf{x}[t] \in \mathbb{C}^{N\times 1}$ denotes the transmit vector at the BS, $\mathbf{H}_1 \in \mathbb{C}^{L\times N}$ is the channel matrix of the link between the BS and the RIS, and $\mathbf{h}_{2,m} \in \mathbb{C}^{L\times 1}$ stands for the channel vector between the RIS and the mth UE. $\mathbf{Z}[t] \in \mathbb{C}^{L\times L}$ is the phase shift matrix of the RIS that contains the phase shifts $[\mathrm{e}^{j\theta_1[t]}, \mathrm{e}^{j\theta_2[t]}, \ldots, \mathrm{e}^{j\theta_L[t]}]$ with $\theta_l[t] \in \{0, \pi\}$, $1 \leq l \leq L$ on its main diagonal (indicating the 1-bit resolution) while the

[3]Note that RIS as part of the TN can be utilized in additional applications, e.g. sensing. Then, depending on the implementation, only a fraction of all available phase shifts may be used to support QKD.

off-diagonal elements are zero. In addition, $w_m[t] \in \mathbb{C}$ denotes the additive white Gaussian noise (AWGN) from $\mathcal{CN}(0, \sigma_w^2)$.

The transmit vector $\mathbf{x}[t]$ is modeled as

$$\mathbf{x}[t] = \sum_{m=1}^{M} \mathbf{a}_m s_m[t] k_{\mathrm{BS},m}[t], \ \forall m, t, \tag{2}$$

where $\mathbf{a}_m \in \mathbb{C}^{N\times 1}$ is the beamforming vector for the mth UE, $s_m[t] \in \{-1, 1\}$ denotes the tth transmit symbol from the BPSK alphabet and $k_{\mathrm{BS},m}[t] \in \{-1, 1\}$ denotes the tth key symbol that has been used by the BS to secure the transmission. For simplicity, both $s_m[t], \forall m, t$ and $k_{\mathrm{BS},m}[t], \forall m, t$ are assumed to be i.i.d. random sequences of BPSK symbols. In particular, this means that $\mathcal{E}_t\{k_{\mathrm{BS},m}[t]\} = 0$ and $\mathcal{E}_t\{k^{-1}_{\mathrm{BS},m}[t] k_{\mathrm{BS},m}[t]\} = 1, \forall m$.

We focus on a zero-forcing (ZF) precoder at the BS:

$$[\mathbf{a}_1, \ldots, \mathbf{a}_M] = \mathbf{H}_{\mathrm{tot}}^H \left(\mathbf{H}_{\mathrm{tot}} \mathbf{H}_{\mathrm{tot}}^H\right)^{-1} \tag{3}$$

with $\mathbf{H}_{\mathrm{tot}} = [\mathbf{h}_{2,1}, \ldots, \mathbf{h}_{2,M}]^T \mathbf{H}_1$. Note that for the calculation of the precoder we implicitly assumed the phase shift matrix $\mathbf{Z}[t]$ to be an identity matrix. While ZF precoding produces fully orthogonal, i.e. non-interfering, data streams, any manipulation of $\mathbf{Z}[t]$ would destroy this orthogonality leading to co-channel interference. In this context, a joint optimization of the RIS phase shift matrix and the precoding vectors might be possible, e.g., using the techniques from [22], in addition to the method proposed here. However, in this work we focus on the novel functionality of RIS, such that more sophisticated designs of the precoder are beyond the scope of this work.

After the transmission of the classical signals, the UE decodes the received data packet either using a hard decision-based decoding strategy, i.e.,

$$\tilde{s}_m[t] = \mathrm{sign}\left(\mathcal{R}\{y_m[t]\} k^{-1}_{\mathrm{TN},m}[t]\right), \ \forall m, t, \tag{4}$$

or using a soft decision-based FEC decoding. In the latter case, the reliability of detected symbols can be indicated using the log-likelihood ratios (LLRs). Similar to the traditional LLR calculation for BPSK-modulated transmissions in presence of AWGN, we obtain[4]

$$\begin{aligned} \mathrm{LLR}_m[t] &= \log\left(\frac{\Pr(s_m[t] = +1 | \mathcal{R}\{\tilde{y}_m[\cdot]\})}{\Pr(s_m[t] = -1 | \mathcal{R}\{\tilde{y}_m[\cdot]\})}\right) \\ &= \frac{2\mathcal{R}\{y_m[t]\} k^{-1}_{\mathrm{TN},m}[t]}{\sigma_w^2}, \ \forall m, t, \end{aligned} \tag{5}$$

where $\tilde{y}_m[\cdot]$ stands for the total received and decrypted data packet. These LLRs can be then fed into a FEC decoder.

However, the two sets of keys $k_{\mathrm{BS},m}[t], \ \forall m, t$ and $k_{\mathrm{TN},m}[t], \ \forall m, t$ are statistically independent since they originate from two different QKD processes. Moreover, $k_{\mathrm{BS},m}[t]$ is only known to the BS and the TN, but it is unknown to the intended UE.[5] Through this, the original sequence $s_m[t]$ is uncorrelated both with $\hat{s}_m[t]$ and with $\mathrm{LLR}_m[t]$. Hence, both hard and soft decoding attempts would fail.

[4]Note that the calculation of the LLRs does not involve any interference terms from the adjacent non-orthogonal beamforming vectors as these may not be known to the respective UE.

[5]Similarly, $k_{\mathrm{TN},m}[t], \ \forall m, t$ is unknown to the BS, such that it is impossible, e.g., to pre-compensate $k_{\mathrm{TN},m}[t], \ \forall m, t$.

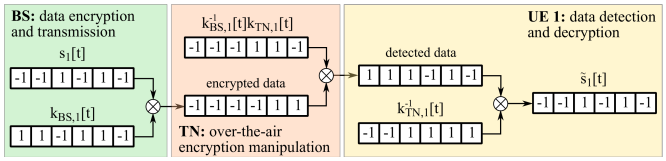

Fig. 2. Example of data packet propagation from BS to UE 1.

There are only two options available to make sure that the UE can correctly decrypt the data: (i) the UE has to be notified about $k_{\mathrm{BS},m}[t]$ and (ii) the encryption has to be manipulated by the TN. The first option corresponds to the state-of-art TN implementation [10], which is detrimental for the system security as in case of corrupted QKD of the UE link both keys are revealed to the eavesdropper. Hence, in the next section, we will propose a method to address the second option.

III. RIS-based Encryption Manipulation

A. Concept

We start by considering the sequence $k_{\mathrm{tot},m}[t] = k^{-1}_{\mathrm{TN},m}[t] k_{\mathrm{BS},m}[t]$. This sequence represents the remaining encryption after the decryption attempt by the mth UE. To ensure a correct decryption by the UE, the TN needs to manipulate the signal in such a way that this sequence is compensated. Specifically, TN needs to perform over-the-air encryption of symbols with the complementary sequence $k^{-1}_{\mathrm{tot},m}[t]$. The over-the-air encryption can be achieved by manipulating the phase shifts of RIS on a symbol-by-symbol basis, such that the sign of the BPSK symbol pertaining to the mth UE is flipped, if $k_{\mathrm{tot},m}[t] = -1$. An example of the data packet propagation from BS to UE is depicted in Fig. 2.

The corresponding design of RIS requires a substantial amount of spatial diversity, which can only be enabled using a large number of RIS elements. Hence, with a small- or moderate-sized RIS, i.e. insufficient spatial diversity, it may not be possible for the received signal to match exactly the original BPSK constellation. Instead, due to the similarity of this problem with the symbol-level precoding problem [23], we suggest to exploit extended regions of the constellation:

$$\mathcal{R}\{y_m[t]\} \left\{ \begin{array}{ll} \geq \sigma_w \sqrt{\Gamma_m} + I_m[t], & \text{if } k_{\mathrm{tot},m}[t] = 1, \\ \leq -\sigma_w \sqrt{\Gamma_m} - I_m[t], & \text{otherwise,} \end{array} \right\} \forall m, t, \tag{6}$$

where Γ_m is the hypothetical distance-preserving signal-to-noise ratio (SNR) of the mth UE and $I_m[t]$ denotes the magnitude of the co-channel interference. This interference comes from the precoding vectors of the ZF precoder which are no longer orthogonal, if $k_{\mathrm{tot},m}[t] \neq 1$ holds for at least one UE due to the changes of $\mathbf{Z}[t]$. While Γ_m can be imposed as a fixed value in principle, the maximization of Γ_m seems more promising. Thus, in Section III-B, we propose an optimization problem, which aims at determining the phase shifts of RIS for the maximized signal quality.

Interestingly, the non-linear dependency of the received signal on the combination of keys and transmitted symbols contributes to the data protection as the received signal is more and more non-linearly distorted with increasing distance between the UE and an eavesdropper. Accordingly, for a successful attack, the eavesdropper needs to be in close proximity

of the target UE and the TN (in order to connect to its memory and read the key) at the same time, which is challenging.

B. Problem formulation and solution

The phase shift optimization problem in the tth symbol interval can be formulated as follows:

$$\begin{aligned} &\underset{\mathbf{Z}[t],\lambda_m[t],I_m[t]}{\text{maximize}} \ \min_m\{\lambda_m[t]\}, \qquad (7)\\ \text{s.t.: } &\text{(C1) } \mathcal{R}\{\mathbf{h}_{2,m}^T\mathbf{Z}[t]\mathbf{H}_1\mathbf{a}_m\}k_{\text{tot},m}[t] \geq \lambda_m[t] + I_m[t],\ \forall m,\\ &\text{(C2) } \sum_{u\neq m}\left|\mathcal{R}\{\mathbf{h}_{2,m}^T\mathbf{Z}[t]\mathbf{H}_1\mathbf{a}_u\}\right| \leq I_m[t],\ \forall m,\\ &\text{(C3) } \text{diag}(\mathbf{Z}[t]) \in \{-1,1\}^{L\times 1}. \end{aligned}$$

In this problem, we maximize the minimum distance $\lambda_m[t]$ between two constellation points across all UEs by taking into account the interference between the adjacent data streams. The constraint (C1) represents a slight reformulation of (6) and describes the sign flipping of the received signal, if the two keys ($k_{\text{BS},m}[t]$ and $k_{\text{TN},m}[t]$) do not match, i.e. $k_{\text{tot},m}[t] = -1$. Note that $\sigma_w\sqrt{\Gamma_m}$ in (6) has been replaced by $\lambda_m[t]$ in order to maximize the signal quality. The maximum magnitude of the interference is upper bounded by an auxiliary variable $I_m[t]$, see constraint (C2). The constraint (C3) indicates the 1-bit resolution of the reflection coefficients.

This is a mixed-integer problem that can be solved, e.g., via full search over all integer variables. The corresponding complexity is then $\mathcal{O}(2^L)$, which may be too high for a RIS with many reflective elements. We provide an alternative solution based on the approximation of the integer variables as continuous-valued in the range $[-1,1]$. For this, we notice that any real- and continuous-valued variable β in the range $[-1,1]$ can be forced to attain an integer value from $\{-1,1\}$ by maximizing β^2. However, such a maximization is non-convex. Hence, we introduce an iterative linearization of β^2 via Taylor series, i.e., $\beta_{n+1}^2 \approx \beta_n^2 + 2\beta_n(\beta-\beta_n)$, where β_n denotes the value of β obtained in the nth iteration. This approach has been used in various works in the past and is therefore not part of our contribution.

We apply the linearization to all reflective coefficients in matrix $\mathbf{Z}[t]$. For the clarity of exposition, we denote $\mathbf{g} = \text{diag}(\mathbf{Z}[t])$. Then, we incorporate the maximization of $\mathbf{g}^T\mathbf{g}$ using above linearization in the objective function and obtain:

$$\min_m\{\lambda_m[t]\} + \mu\cdot(\mathbf{g}_n^T\mathbf{g}_n + 2\mathbf{g}_n^T(\mathbf{g}-\mathbf{g}_n)), \qquad (8)$$

where μ is a properly selected scaling factor. The resulting optimization problem is linear and can be easily solved using interior-point methods. The overall iterative algorithm is described using a pseudocode notation in Alg. 1. The loop is executed Q times[6]. The complexity is $\mathcal{O}(QL^3)$, cf. [24].

In practice, the number of symbols per packet K is larger than the number of key combinations 2^M. Accordingly, some of the key combinations are likely to repeat. Thus, in order to avoid delays and waste of resources, we suggest to pre-compute the phase shift matrices for all 2^M key combinations $k_{\text{tot},m}[t], \forall m$ at the BS and store them at the TN. The resulting codebook has a size of only $2^M L$ bits since L bits are required to store all phase shifts for a single key combination. In this case, the TN would simply pick the corresponding set of phase shifts pertaining to the keys used in the tth symbol interval.

[6]We observed that $Q = 5$ is sufficient for the convergence.

Algorithm 1 Iterative calculation of reflective coefficients

Input: $\mathbf{H}_1$, $\mathbf{h}_{2,m}$, $\mathbf{a}_m$, $k_{\text{tot},m}[t]$, $\forall m$;
Output: $\mathbf{Z}[t]$

1: Initialize $\mathbf{Z}_0[t] = \mathbf{I}$;
2: **for** $q = 1$ **to** Q **do**
3: Solve (7) by replacing its objective with (8) and (C3) with $\text{diag}(\mathbf{Z}[t]) \in [-1,1]^{L\times 1}$;
4: Set $\mathbf{Z}_q[t] \leftarrow \mathbf{Z}[t]$;
5: **end for**
6: $\mathbf{Z}[t] \leftarrow \text{sign}(\mathbf{Z}_Q[t])$.

IV. Numerical results

In this section, we evaluate the performance of the proposed method in terms average bit error rate (ABER). For this, we assume that $M = N$ UEs are scattered on the street in front of the BS while the TN is placed at the building facade 30 m away from the BS in the direction of the UEs and 5 m aside of the street. The closest position of the UEs to the BS is assumed to be 20 m and the most distant position is 40 m. Note that we assume the direct signals from the BS to be blocked by obstacles. Further, the minimum distance between any two UEs is 5 m. For the BS and TN, the height of the antenna position is set to 3 m while it is 1.5 m for the UEs. For the channels between the BS, TN and the UEs we impose Rician fading with the LoS factor of 3 dB. For the total transmit power at the BS we assume 43 dBm. The noise variance is set to -80 dBm. Regarding the FEC coding, we focus on a low-density parity check (LDPC) code with the code rate of 1/2. Furthermore, the length of each encoded packet K is 100 bits. We obtain the simulation results from 2000 channel realizations with 200 packet transmissions per UE and per realization. Thus, we transmit 4×10^7 bits per UE per simulation point in total. In addition, we introduce a distributed eavesdropper with access to the TN's memory, i.e. all keys are revealed, and in close proximity (1 m distance) to each of the target UEs. The observations are optimally combined for the signal decorrelation. Clearly, this is the worst case scenario as the eavesdropper is in possession of all information except for the classical data. In this case, if TN were implemented using a traditional relay, the eavesdropper would be able to perfectly decrypt the information. We display the results obtained using the proposed method and a benchmark, which represents the traditional RIS-aided precoded transmissions with phase shifts optimized to minimize the maximum BER among all UEs. For this benchmark, we assume that the key of the first link has been forwarded by the TN to the respective UE via optical signaling using the quantum key encryption of the second link. Note that this benchmark scheme is thus already less secure than the proposed method, as explained earlier.

Fig. 3 depicts the results for different numbers of UEs and RIS elements. We observe that with increasing number of RIS elements the performance of the target users improves since the spatial diversity is much higher with a large number

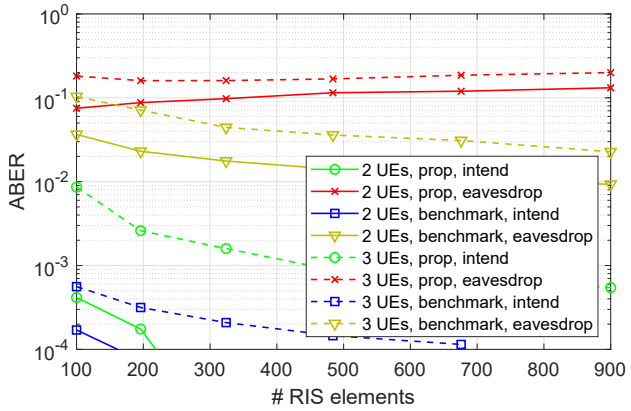

Fig. 3. ABER vs. number of RIS elements and numbers of UEs.

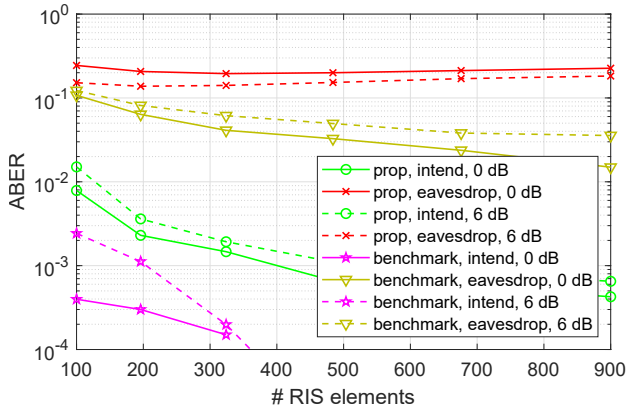

Fig. 4. ABER vs. number of RIS elements and Rician factors.

of signal paths. With the proposed method and two UEs, it is already enough to utilize a RIS with 256 elements to reach ABER below 10^{-4}. With three UEs, we observe a slower decrease in ABER with increasing number of RIS elements. Interestingly, with any number of UEs, we obtained a very poor performance for the eavesdropper, i.e. ABER between 8% and 22%. With the benchmark, we obtain a very good performance for the intended UE, but also a satisfactory performance for the eavesdropper. Specifically, the eavesdropper demonstrates an ABER decrease by up to an order of magnitude compared to the proposed solution with a large number of RIS elements.

In Fig. 4, we show ABER for three UEs obtained with Rician factors of 0 dB and 6 dB. We observe that for the intended UEs and for the eavesdropper with the benchmark scheme ABER increases with increasing Rician factor, which is due to the reduced spatial diversity pertaining to the line-of-sight (LoS) component of the Rician fading. In contrast, for the eavesdropper with the proposed solution, we observe an improvement of the ABER due to improved correlation between the channels of the eavesdropper and the UE. However, the difference in ABER is not large, such that the performance of the eavesdropper is very poor with ABER of at least 20% with 6 dB Rician factor.

V. Conclusion

In this paper, a novel concept of trusted RIS-aided multi-user QKD has been proposed. The problem of encryption manipulation that accounts for the different keys in the sub-links has been tackled by optimizing the phase shift matrix of RIS in each symbol interval. Simulation results demonstrate a good average performance for the intended UEs. In contrast, the performance of an eavesdropper is very poor even in case of a successful attack on the TN, i.e., revealing all secret keys. Accordingly, the proposed concept represents the next step in securing future terrestrial QKD networks.

References

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. of Symp. Found. Comp. Sc.*, 1994, pp. 124–134.

[2] K. A. Fisher *et al.*, "Quantum computing on encrypted data," *Nat. commun.*, vol. 5, no. 1, pp. 1–7, 2014.

[3] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of IEEE Int. Conf. on Comp. Sys. and Sign. Pr.*, 1984.

[4] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[5] Y. Cao *et al.*, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surv. & Tut.*, vol. 24, no. 2, pp. 839–894, 2022.

[6] C. Elliott, "Building the quantum network," *New Journ. Phys.*, vol. 4, no. 1, p. 46, 2002.

[7] W. Stacey *et al.*, "Security of quantum key distribution using a simplified trusted relay," *Physical Review A*, vol. 91, no. 1, p. 012338, 2015.

[8] M. Mehic *et al.*, "A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks," *IEEE/ACM Transactions on Networking*, vol. 28, no. 1, pp. 168–181, 2019.

[9] H.-K. Lo *et al.*, "Measurement-device-independent quantum key distribution," *Phys. rev. lett.*, vol. 108, no. 13, p. 130503, 2012.

[10] Y. Cao *et al.*, "Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks," *IEEE Journ. Sel. Areas in Commun.*, vol. 39, no. 9, pp. 2701–2718, 2021.

[11] C. Liaskos *et al.*, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, 2018.

[12] E. Basar, "Reconfigurable intelligent surface-based index modulation: A new beyond MIMO paradigm for 6G," *IEEE Trans. on Commun.*, vol. 68, no. 5, pp. 3187–3196, 2020.

[13] K. Tekbiyik *et al.*, "Reconfigurable intelligent surfaces empowered THz communication in LEO satellite networks," *IEEE Access*, vol. 10, pp. 121 957–121 969, 2022.

[14] S. Kisseleff *et al.*, "Reconfigurable intelligent surfaces in challenging environments: Underwater, underground, industrial and disaster," *IEEE Access*, vol. 9, pp. 150 214–150 233, 2021.

[15] L. Yang *et al.*, "Secrecy performance analysis of ris-aided wireless communication systems," *IEEE Trans. on Veh. Techn.*, vol. 69, no. 10, pp. 12 296–12 300, 2020.

[16] L. Kong *et al.*, "On the impacts of phase shifting design and eavesdropping uncertainty on secrecy metrics of RIS-aided systems," in *Proc. of Europ. Conf. on Netw. and Commun. 6G Summit*, 2022, pp. 494–499.

[17] X. Lu *et al.*, "Intelligent reflecting surface assisted secret key generation," *IEEE Sign. Process. Lett.*, vol. 28, pp. 1036–1040, 2021.

[18] G. Li *et al.*, "On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems," *IEEE Trans. Inform. For. Sec.*, vol. 17, pp. 211–225, 2021.

[19] D. Ljunggren *et al.*, "Authority-based user authentication in quantum key distribution," *Phys. Rev. A*, vol. 62, p. 022305, Jul 2000.

[20] M. A. Sedaghat *et al.*, "Load modulated arrays: a low-complexity antenna," *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 46–52, 2016.

[21] O. A. Abdelraouf *et al.*, "Recent advances in tunable metasurfaces: Materials, design, and applications," *ACS nano*, vol. 16, no. 9, pp. 13 339–13 369, 2022.

[22] J. Ye *et al.*, "Joint reflecting and precoding designs for SER minimization in reconfigurable intelligent surfaces assisted MIMO systems," *IEEE Trans. on Wir. Commun.*, vol. 19, no. 8, pp. 5561–5574, 2020.

[23] A. Li *et al.*, "A tutorial on interference exploitation via symbol-level precoding: overview, state-of-the-art and future directions," *IEEE Commun. Surv. & Tut.*, vol. 22, no. 2, pp. 796–839, 2020.

[24] F. A. Potra and S. J. Wright, "Interior-point methods," *Journ. of Comp. Appl. Math.*, vol. 124, no. 1, pp. 281–302, 2000.