DOI:
10.1109/ICCW.2019.8756986

Document Version
Peer reviewed version

On Fair Secure Rate Maximization for NOMA Downlinks Using Quantum Key Distribution

Zhaohui Yang *, Jiancao Hou *, Wei Xu † and Mohammad Shikh-Bahaei *
*Centre for Telecommunications Research, Department of Informatics, Kings College London, London WC2B 4BG, U.K.
†National Mobile Communications Research Laboratory, Southeast University, Nanjing 211111, China
E-mail:yang.zhaohuikcl.ac.uk,jiancao.hou@kcl.ac.uk, wxu@seu.edu.cn, m.sbahaei@kcl.ac.uk

***Abstract*—Quantum key distribution (QKD) ensures two individuals to establish a secret key by exchanging photon quantum states, which ensures the security and can be promising to assist future wireless communications. In this paper, we investigate a quantum-assisted wireless communication system, where QKD is first performed to generate secure key, and wireless communication is conducted for data transmission via non-orthogonal multiple access (NOMA). To guarantee user fairness, the aim is to maximize the minimal secure rate among all users. To solve this nonconvex problem, an iterative algorithm with low complexity is proposed, where the closed-form solution is obtained in each iteration. Simulation results are illustrated to show the superiority of the proposed algorithm.**

***Index Terms*—Secure communication, NOMA, QKD distribution, resource allocation.**

I. Introduction

Security has become an essential requirement in modern communication systems [1], [2]. Due to the broadcasting feature of wireless links, wireless communication systems are inherently vulnerable to eavesdropping and security can not be absolutely guaranteed [3]. However, in quantum communication, the security can be theoretically guaranteed based on the quantum no-cloning theorem [4] and the fundamental postulate of quantum physics that every measurement perturbs a system [5]. Due to this advantage, quantum communication gains its popularity in applications of secure key distribution [6]–[11].

Quantum key distribution (QKD) [6] is a method to generate a secret key between two individuals (usually named as Alice and Bob) by transmitting non-orthogonal quantum states. After the transmission, Alice and Bob generate a secure key according to measurement of these quantum states. To prevent attack, Alice and Bob need to authenticate the key message in classical channels.

Theoretically, an experimental demonstration of QKD was conducted over a short distance of 32 cm on an optical cable [7]. Since then, there has been continuous progress on both theoretical and technological sides of QKD in fiber-based systems. For free space, QKD has been successfully implemented in [10], [11]. The maximum distance has recently been pushed up to 400 km [8]. The authors in [9] have demonstrated the feasibility of QKD through satellite communications. Despite the absolute security of quantum communication so far as we know, there lacks contribution in applying QKD to conventional wireless communications.

With superposition coding and successive interference cancelation (SIC), NOMA achieves higher spectral efficiency than conventional time division multiple access (TDMA) [12]–[15]. Since the QKD guarantees high security with high complexity in implementation an the conventional NOMA can ensure high data rate with low complexity and low security, this motivates us to combine the QKD and NOMA together, where the QKD is used for key generation to ensure the security and conventional NOMA is employed for transmitting data with high rate.

In this paper, we consider a quantum-assisted wireless communication system with one base station (BS) serving multiple legitimate users. The security against an eavesdropper is investigated in this paper. The main contributions of this paper are summarized as follows:

1) We formulate the minimal secure rate maximization problem for NOMA downlinks with QKD, where the QKD transmission is first performed to generate secure key between the BS and users and NOMA is then conducted.
2) To solve the nonconvex minimal secure rate maximization problem, a low-complexity algorithm is proposed, where the closed-form solution is obtained in each step.

The rest of the paper is organized as follows. In Section II, we introduce the system model and formulate the problem. Section III provides an iterative algorithm. Some simulation results are shown in Section IV and conclusions are finally drawn in Section V.

II. System Model and Problem Formulation

We consider a downlink single-cell network with one BS, K legitimate users and an eavesdropper, as shown in Fig. 1. The set of all K users are denoted by $\mathcal{K} = \{1, \cdots, K\}$. To perform QKD, the BS is configured with a photon emitter and, correspondingly, the user is equipped with a photon detector. For ensuring the security, the two-stage secure transmission protocol is adopted in Fig. 2. In the first stage of time transmission, QKD transmission is performed through quantum channel, where multiple users are allocated with secure key via time division and the time period of QKD transmission for user k is t_k. Using the secure key obtained in the first stage, data transmission is conducted in the second stage through conventional wireless broadcast channel during the time period, t_{K+1}.

A. QKD Transmission

To obtain the secure key for user k, we exploit the efficient QKD scheme with non-maximally entangled states [5]. As

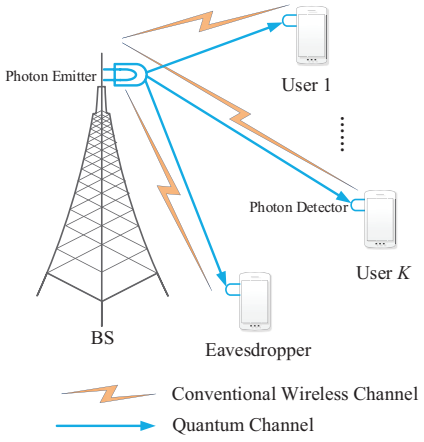

Fig. 1. A quantum-assisted wireless communication system.

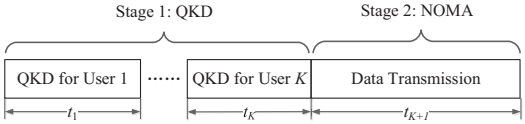

Fig. 2. Two-stage secure transmission protocol.

depicted in Fig. 3, the QKD scheme consists of three phases: photon transmission, measurement, and announcement and comparison.

In the first phase, the BS prepares pairs of photons with non-maximally entangled state

$$|AB\rangle = \alpha\,|H\rangle_A\,|H\rangle_B + \beta\,|V\rangle_A\,|V\rangle_B\,, \tag{1}$$

where $|\alpha|^2 + |\beta|^2 = 1$, A and B stand for two entangled photons, and $|H\rangle$ and $|V\rangle$ respectively represent the horizonal and vertical linear polarization. Then with probability $\frac{1}{2}$, the state $|AB\rangle$ is randomly transformed into its equivalent sate

$$|AB\rangle' = \beta\,|H\rangle_A\,|H\rangle_B + \alpha\,|V\rangle_A\,|V\rangle_B\,. \tag{2}$$

Next, a sequence of photons B of each pair are transmitted to user k, while photons A are correspondingly left at the BS.

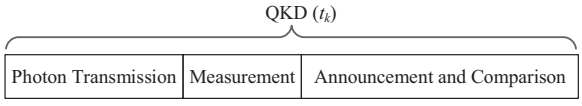

Fig. 3. Three-phase QKD scheme.

In the second phase, the BS and user k independently measure the photons A and photons B, respectively. Specifically, the BS performs the measurement in one of the two bases, obtained by rotating the rectilinear bases by angles 0 and $\pi/4$ with probabilities $1-\epsilon_k$ and ϵ_k, respectively. User k takes the measurements in one of the three bases, obtained by rotating the rectilinear bases by angles 0, $\theta \triangleq \tan^{-1}(\beta/\alpha)$, and $-\theta$, with probabilities $1-\epsilon_k$, $\epsilon_k/2$, and $\epsilon_k/2$, respectively. The probability ϵ_k is publicly known to both the BS and user k. After performing the measurements, both the BS and user k record the measurement results with their bases.

After having exchanged enough photons, user k announces in the third phase on the public channel the sequence of used bases. The BS compares this sequence with the bases that the BS measured. For example, as shown in Table I (0, $\pi/4$, θ and $-\theta$ means rotating the rectilinear bases by angles 0, $\pi/4$, θ and $-\theta$, respectively), if user k uses base 0, the BS utilizes base 0, the obtained bits at the BS and user k are the same, i.e., user k utilizes the correct base. For the case, when user k uses base θ, the BS chooses base 0, the obtained bits at the BS and user k are not absolutely the same, i.e., user k uses the incorrect base in this situation. Then, the BS tells user k on the public channel on which occasions its measurements were done in the correct bases. When the BS and user k utilize the compatible basis, they should get perfectly correlated bits. However, due to imperfections in the setup, there will be some errors to a potential eavesdropper. To ensure security of the key, the BS and user k randomly pick a fixed number, m_k, of photons and publicly compare their results.

The BS and user k divide up their obtained data into 12 cases according to the actual used states, bases and bit values yielded, as shown in Table I.

For each photon, the eavesdropper does not know which non-maximally entangled state it is chosen from. A biased eavesdropping attack is performed at the eavesdropper, i.e., the eavesdropper takes the measurements in one of the three bases, obtained by rotating the rectilinear bases by angles 0, θ, and $-\theta$, with probabilities p_1, p_2, and p_3, respectively. For a biased eavesdropping attack, the average error rate [1] is [5]

$$e_k = \frac{2|\alpha|^2|\beta|^2[2(1-\epsilon_k)^2(p_2+p_3)+\epsilon_k^2 p_1+2\epsilon_k^2(|\alpha|^2-|\beta|^2)(p_2+p_3)]}{(1-\epsilon_k)^2+\epsilon_k^2/2}. \tag{3}$$

Since the eavesdropper has no prior knowledge of the used base of user k, it is assumed that the eavesdropper always eavesdrops only along the rectilinear base (i.e., $p_1 = 1$, $p_2 = p_3 = 0$) for simplicity. Further applying $p_1 = 1$ and $p_2 = p_3 = 0$, equation (3) is simplified as

$$e_k = \frac{4|\alpha|^2|\beta|^2\epsilon_k^2}{2(1-\epsilon_k)^2+\epsilon_k^2}. \tag{4}$$

To calculate the value of error rate e_k, there should be enough photons for an accurate estimation. Denote N_k as the number of entangled pairs chosen by the BS for user k, i.e., N_k photons are transmitted from the BS to user k. For each state of $|AB\rangle$ and $|AB\rangle'$, the probability that the BS uses base $\pi/4$ and user k chooses a base θ or $-\theta$ is

$$q_k = \epsilon \times \frac{\epsilon_k}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{\epsilon_k^2}{8}, \tag{5}$$

where ϵ_k is the probability that the BS uses base $\pi/4$, $\frac{\epsilon_k}{2}$ is the probability that user k chooses the base θ or $-\theta$, the first $\frac{1}{2}$ is the probability that the BS measures 0 or 1 under each base, and the last $\frac{1}{2}$ is the probability for state $|AB\rangle$ or $|AB\rangle'$. As a result, there are

$$N_k q_k = \frac{N_k \epsilon_k^2}{8} \tag{6}$$

[1]Error rate means that the secure key of the user is obtained by the eavesdropper.

TABLE I
MEASUREMENT COMPARISON [5].

The BS base	0	0	0	0	0	0	$\pi/4$	$\pi/4$	$\pi/4$	$\pi/4$	$\pi/4$	$\pi/4$
The BS bit value	0	0	0	1	1	1	0	0	0	1	1	1
User k base	0	θ	-θ	0	θ	-θ	0	θ	-θ	0	θ	-θ
User k bit value	0	0/1	0/1	1	0/1	0/1	0/1	0	0/1	0/1	0/1	1
Correct base?	yes	no	no	yes	no	no	no	yes	no	no	no	yes
Key	0			1				0				1
Probability	$\frac{1}{2}(1-\epsilon_k)^2$			$\frac{1}{2}(1-\epsilon_k)^2$				$\frac{1}{4}\epsilon_k^2$				$\frac{1}{4}\epsilon_k^2$

photons for the case the BS uses the base $\pi/4$ and user k chooses a base, i.e., θ or $-\theta$ under a state, i.e., $|AB\rangle$ or $|AB\rangle'$, which should be larger than a fixed number m_k to ensure the refined error analysis for user k [5]. It yields

$$\frac{N_k \epsilon_k^2}{8} \geq m_k. \tag{7}$$

Since the quantum channel resource is always precious, we only need to set the minimal value N_k satisfying (7), i.e., $N_k = \lceil 8m_k/\epsilon_k^2 \rceil$, where operator $\lceil \cdot \rceil$ means round up.

It is assumed that only one photon is transmitted in the quantum channel in each time. Since there are N_k photons to be transmitted for user k, the required period QKD can be evaluated as[2]

$$t_k = \frac{N_k d_k}{c} = \frac{d_k}{c} \left\lceil \frac{8m_k}{\epsilon_k^2} \right\rceil, \tag{8}$$

where d_k is the distance between the BS and user k, and c is the constant speed of the light.

B. NOMA Transmission

After the QKD transmission for generating secure key, NOMA scheme is used for data transmission in the second stage. The channel gain between the BS and user k is denoted by h_k. Without loss of generality, the channels are sorted as $h_1 \leq \cdots \leq h_K$. According to [12], the achievable rate of user k can be given by

$$r_k = B \log_2 \left(1 + \frac{h_k p_k}{h_k \sum_{l=k+1}^{K} p_l + \sigma^2} \right), \tag{9}$$

where B is the system bandwidth, p_k is the transmit power of the BS for user k, and σ^2 is the noise power. According to (9), user m can decode the message of weaker user i ($i < m$) and remove it from the received signal such that the interference of user m is only from user l ($l > m$) [16]–[18].

Given the data transmission time is t_{K+1} and average error of QKD transmission is e_k for user k, the average secure rate for user k is

$$\begin{aligned} R_k(t_{K+1}, \epsilon_k, \boldsymbol{p}_k) &= \frac{t_{K+1}}{T}(1-e_k) r_k \\ &= \frac{t_{K+1}}{T}(1-e_k) B \log_2 \left(1 + \frac{h_k p_k}{h_k \sum_{l=k+1}^{K} p_l + \sigma^2} \right), \end{aligned} \tag{10}$$

where T is the total transmission time including both QKD and data transmissions, $\boldsymbol{p}_k = [p_k, p_{k+1}, \cdots, p_K]$, and e_k is the average QKD error rate defined in (3).

[2]For measurement and announcement and comparision time, it can be modelled as a linear function of the photons similar to (8).

C. Problem Formulation

To guarantee user fairness and improve the secure rate, we formulate the problem to maximize the minimal average secure rate among all K users (i.e, max-min rate optimization problem). Now, it is ready to formulate the problem of minimal secure rate maximization problem as

$$\max_{\boldsymbol{p},\boldsymbol{\epsilon},\boldsymbol{t}} \min_{k \in \mathcal{K}} \quad R_k(t_{K+1}, \epsilon_k, \boldsymbol{p}_k) \tag{11a}$$

$$\text{s.t.} \quad t_k = \frac{d_k}{c} \left\lceil \frac{8m_k}{\epsilon_k^2} \right\rceil, \quad \forall k \in \mathcal{K} \tag{11b}$$

$$\sum_{k=1}^{K+1} t_k \leq T \tag{11c}$$

$$\sum_{k=1}^{K} p_k \leq P_{\max} \tag{11d}$$

$$0 \leq \epsilon_k \leq 1, t_k \geq 0, \quad \forall k \in \mathcal{K} \tag{11e}$$

$$p_k \geq 0, \quad \forall k \in \mathcal{K} \tag{11f}$$

where $\boldsymbol{p} = [p_1, p_2, \cdots, p_M]$, $\boldsymbol{\epsilon} = [\epsilon_1, \epsilon_2, \cdots, \epsilon_M]$, $\boldsymbol{t} = [t_1, t_2, \cdots, t_{M+1}]$, $R_k(t_{K+1}, \epsilon_k, \boldsymbol{p}_k)$ is the average secure rate of user k defined in (10), and $P_{\max}$ is the maximal transmission power of the BS. Constraints (11b) show the QKD transmission time. The maximal transmission time constraint is given in (11c) and the maximal power constraint in presented in (11d).

III. PROPOSED ALGORITHM

Since problem (11) is nonconvex due to nonconvex objective function (11a), it is general hard to obtain the globally optimal solution. In the following, we propose a low-complexity algorithm via iteratively optimizing power control $\boldsymbol{p}$ with fixed probability $\boldsymbol{\epsilon}$ and time $\boldsymbol{t}$, and updating probability $\boldsymbol{\epsilon}$ and time $\boldsymbol{t}$ with optimized power control $\boldsymbol{p}$.

A. Optimal Power Control

Denote R_0 as the minimal average secure rate among the K users. Introduce a new variable R_0, problem (11) with given $\boldsymbol{\epsilon}$ and $\boldsymbol{t}$ can be rewritten as

$$\max_{\boldsymbol{p}, R_0} \quad R_0 \tag{12a}$$

$$\text{s.t.} \quad R_k(t_{K+1}, \epsilon_k, \boldsymbol{p}_k) \geq R_0, \quad \forall k \in \mathcal{K} \tag{12b}$$

$$(11d), (11f). \tag{12c}$$

Before solving problem (12), we present the following two lemmas of the optimal conditions.

Lemma 1: For the optimal solution $(\boldsymbol{p}^*, R_0^*)$ of problem (12), constraints (12b) always hold with equality, i.e.,

$R_1(t_{K+1}, \epsilon_1, \boldsymbol{p}_1^*) = \cdots = R_K(t_{K+1}, \epsilon_K, \boldsymbol{p}_K^*) = R_0^*$, where $\boldsymbol{p}_k^* = [p_k^*, p_{k+1}^*, \cdots, p_K^*]$.

Proof: Please refer to Appendix A. □

Lemma 2: For the optimal solution $(\boldsymbol{p}^*, R_0^*)$ of problem (12), maximal power constraint (11d) holds with equality, i.e., $\sum_{k=1}^K p_k^* = P_{\max}$.

Proof: Please refer to Appendix B. □

Lemma 1 shows that even with different average QKD error rates, it is always max-min rate optimal for all users to transmit with the same secure rate [19]–[21]. According to Lemma 2, it is always rate improving to increase transmission power.

Theorem 1: The optimal solution of problem (12) is

$$p_k^* = \frac{P_{\max}(2^{b_k R_0^*} - 1)}{2^{\sum_{l=1}^{k-1} b_l R_0^*}} + \frac{(2^{b_k R_0^*} - 1)\sigma^2}{2^{b_k R_0^*} h_k} - \sum_{l=1}^{k-1} \frac{(2^{b_l R_0^*} - 1)(2^{b_k R_0^*} - 1)\sigma^2}{2^{\sum_{j=l}^{k-1} b_j R_0^*} h_l}, \quad \forall k \in \mathcal{K}, \quad (13)$$

and R_0^* is the solution of

$$\frac{P_{\max}}{2^{\sum_{l=1}^{K} b_l R_0}} - \sum_{l=1}^{K} \frac{(2^{b_l R_0} - 1)\sigma^2}{2^{\sum_{j=l}^{K} b_j R_0} h_l} = 0, \quad (14)$$

where $b_k = \frac{T}{t_{K+1}(1-e_k)B}$ for all $k \in \mathcal{K}$.

Proof: Please refer to Appendix C. □

Since the right hand of (14) is strictly decreasing with R_0, the unique solution R_0^* can be effectively obtained by using the bisection method.

B. Optimal Probability and Time Allocation

Using new variable R_0, problem (11) with given power control $\boldsymbol{p}$ becomes

$$\max_{\boldsymbol{\epsilon}, \boldsymbol{t}, R_0} \quad R_0 \quad (15a)$$

$$\text{s.t.} \quad (11b), (11c), (11e), (12b). \quad (15b)$$

For problem (15), we have the following lemma about the optimal solution.

Lemma 3: For the optimal solution $(\boldsymbol{\epsilon}^*, \boldsymbol{t}^*, R_0^*)$ of problem (15), we always have $R_k(t_{K+1}^*, \epsilon_k^*, \boldsymbol{p}_k) = R_0^*$ if $0 < \epsilon_k^* < 1$; otherwise $\epsilon_k^* \in \{0, 1\}$.

Proof: Please refer to Appendix D. □

Lemma 3 presents the structure of the optimal probability ϵ_k, which helps us obtain the optimal solution of problem (15) with fixed t_{K+1} in closed form.

Theorem 2: Given NOMA transmission time t_{K+1}, the optimal probability and time allocation of problem (15) is

$$\epsilon_k^* = 1 - \sqrt{\frac{4|\alpha|^2|\beta|^2 t_{K+1} r_k}{2(t_{K+1} r_k - R_0^* T)} - \frac{1}{2}}\Bigg|_0^1, \quad \forall k \in \mathcal{K}, \quad (16)$$

$$t_k^* = \frac{d_k}{c}\left\lceil \frac{8m_k}{\left(1 - \sqrt{\frac{4|\alpha|^2|\beta|^2 t_{K+1} r_k}{2(t_{K+1} r_k - R_0^* T)} - \frac{1}{2}}\Big|_0^1\right)^2} \right\rceil, \quad \forall k \in \mathcal{K}, \quad (17)$$

and R_0^* is the unique solution of

$$\sum_{k=1}^{K} \frac{d_k}{c}\left\lceil \frac{8m_k}{\left(1 - \sqrt{\frac{4|\alpha|^2|\beta|^2 t_{K+1} r_k}{2(t_{K+1} r_k - R_0^* T)} - \frac{1}{2}}\Big|_0^1\right)^2} \right\rceil = T - t_{K+1}. \quad (18)$$

where $a|_b^c = \min\{\max\{a, b\}, c\}$.

Proof: Please refer to Appendix E. □

Theorem 2 shows the optimal solution of problem (15) with fixed time t_{K+1}. To obtain the optimal solution of problem (15), we can use the one-dimensional search method to find the optimal t_{K+1}^*.

C. Iterative Algorithm

The iterative power control, probability and time allocation algorithm is given in Algorithm 1, where ξ is the stepsize of the one-dimensional search method. Since the optimal solution is obtained in each step, the objective value of the proposed Algorithm 1 is non-decreasing, i.e., Algorithm 1 always converges.

Algorithm 1 Iterative Power Control, Probability and Time Allocation

1: Set the initial solution $(\boldsymbol{p}^{(0)}, \boldsymbol{\epsilon}^{(0)}, \boldsymbol{t}^{(0)})$ of problem (11) and the iteration number $n = 0$.
2: Obtain the optimal $\boldsymbol{p}^{(n+1)}$ of problem (11) with given $(\boldsymbol{\epsilon}^{(n)}, \boldsymbol{t}^{(n)})$ according to Theorem 1.
3: **repeat**
4: **for** $t_{K+1} = 0 : \xi : T$ **do**
5: Obtain the optimal $(\boldsymbol{\epsilon}^*, t_1*, \cdots, t_K^*)$ of problem (11) with given $\boldsymbol{p}^{(n+1)}$ and t_{K+1} according to Theorem 2.
6: **end for**
7: Denote the optimal solution of problem (11) with given $\boldsymbol{p}^{(n+1)}$ by $(\boldsymbol{\epsilon}^{(n+1)}, \boldsymbol{t}^{(n+1)})$.
8: Set $n = n + 1$.
9: **until** the objective value (11a) converges

The complexity of Algorithm 1 in each iteration lies in solving problem (11) with given power control $\boldsymbol{p}$. According to (16)-(18), the complexity of solving problem (11) with given $\boldsymbol{p}$ and t_{K+1} is $\mathcal{O}(K + \log_2(1/\kappa))$, where $\mathcal{O}(\log_2(1/\kappa))$ is the complexity of solving equation (18) by using the bisection method with accuracy κ. Thus, the complexity of solving problem (11) with given $\boldsymbol{p}$ is $\mathcal{O}(L_1 K + L_1 \log_2(1/\kappa))$, where $L_1 = T/\xi$ is the number of times by the one-dimensional search method to obtain the optimal t_{K+1} As a result, the total complexity of solving problem (11) s $\mathcal{O}(L_1 L_2 K + L_1 L_2 \log_2(1/\kappa))$, where L_2 denotes the number of outer times for Algorithm 1.

IV. Simulation Results

There are $K = 2$ users uniformly distributed in a square area of size 1 km × 1 km. The system bandwidth is $B = 1$ MHz and the noise power spectrum density is $\sigma^2 = -104$

dBm. The total transmission time $T = 1$ s, and the constant speed of the light is $c = 3 \times 10^8$ m/s. The large-scale path loss is $L(d) = 17 + 30\log(d)$, and the small scale fading follows exponential distribution with one. We set $m_1 = \cdots = m_K = m$. Unless otherwise specified, $m = 10$, $|\alpha||\beta| = \frac{1}{2}$ and $P_{\max} = 30$ dBm.

We compared the proposed algorithm with the exhaustive search method to obtain a near globally optimal solution of problem (11) (labelled as 'EXH'), which refers to running the proposed algorithm 1 with 100 initial starting points, and the TDMA, which refers to the data transmission is performed via TDMA instead of NOMA in stage 2

Fig. 4 illustrates the secure rate versus maximal transmission power of the BS. It is shown that the proposed algorithm yields better secure rate than TDMA. This is due to the fact that users can simultaneously transmit data in NOMA, which result in longer data transmission time for each user in NOMA than that in TDMA. Moreover, the EXH algorithm yields the best performance at the sacrifice of high computational capacity. The gap between the proposed algorithm and EXH is small especially for low maximal transmission power, which indicates that the proposed algorithm can approach the near globally optimal solution.

The secure rate versus photon numbers m (the minimum photon number to ensure the refined error analysis for all users) is presented in Fig. 5. It is seen from this figure that the secure rate decreases with the photon numbers. This is due to the fact that large photon numbers requires long QKD transmission time, which can reduce the secure rate according to (11a). It is also found that the secure rate decreases with $|\alpha||\beta|$.

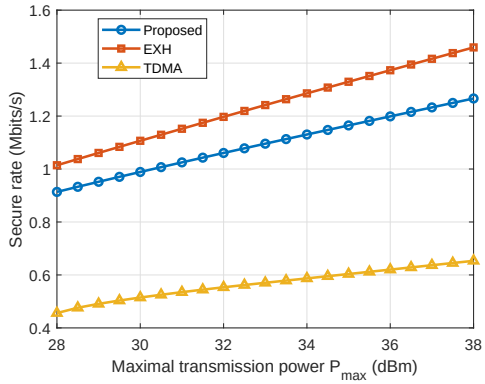

Fig. 4. Secure rate versus maximal transmission power $P_{\max}$.

V. Conclusion

The minimal secure rate maximization problem was studied for a quantum-assisted wireless communication system. It was shown that there is a trade-off between the QKD transmission and conventional wireless transmission via power control, probability and time allocation. To maximize the minimal secure rate, it is recommended to choose small state probability $|\alpha||\beta|$ in QKD scheme.

Appendix A
Proof of Lemma 1

Assume that constraints (12b) do not always hold with equality for all $k \in \mathcal{K}$ in the optimal solution $(\boldsymbol{p}^*, R_0^*)$ of problem (12). Without loss of generality, we can further assume that $R_1(t_{K+1}, \epsilon_k 1, \boldsymbol{p}_1^*) \neq R_2(t_{K+1}, \epsilon_2, \boldsymbol{p}_2^*)$ and $R_0^* = \min\{R_1(t_{K+1}, \epsilon_k 1, \boldsymbol{p}_1^*), R_2(t_{K+1}, \epsilon_2, \boldsymbol{p}_2^*)\}$.

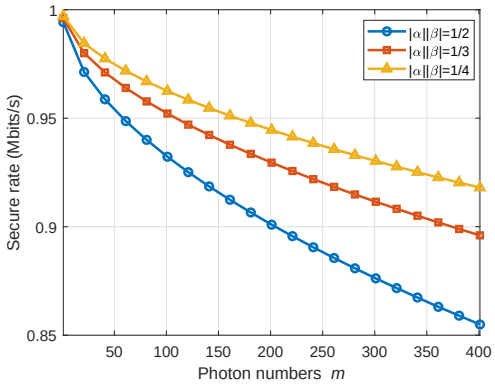

Fig. 5. Secure rate versus photon numbers m.

If $R_1(t_{K+1}, \epsilon_k 1, \boldsymbol{p}_1^*) > R_2(t_{K+1}, \epsilon_2, \boldsymbol{p}_2^*) = R_0^*$, we can slightly decrease power p_1^* to $p_1' = p_1^* - \delta$ and increase power p_2^* to $p_2' = p_2^* + \delta$, where $\delta > 0$ is a small positive constant such that

$$\begin{aligned} R_1(t_{K+1}, \epsilon_k 1, \boldsymbol{p}_1^*) &> R_1(t_{K+1}, \epsilon_1, [p_1', p_2', p_3^*, \cdots, p_K^*]) \\ &\geq R_2(t_{K+1}, \epsilon_2, [p_2', p_3^*, \cdots, p_K^*]) \\ &> R_2(t_{K+1}, \epsilon_2, \boldsymbol{p}_2^*) = R_0^*. \end{aligned} \quad \text{(A.1)}$$

The first and last inequalities in (A.1) follow from the fact that secure rate $R_k(t_{K+1}, \epsilon_k, \boldsymbol{p})$ in (10) monotonically increases with p_k. Based on (A.1), we can construct a new solution $(p_1', p_2', p_3^*, \cdots, p_K^*, R_0' = R_2(t_{K+1}, \epsilon_2, [p_2', p_3^*, \cdots, p_K^*]))$, which meets all the constraints of problem (12) and yields better objective value than solution $(\boldsymbol{p}^*, R_0^*)$. This contradicts the fact that $(\boldsymbol{p}^*, R_0^*)$ is the optimal solution of problem (12).

If $R_2(t_{K+1}, \epsilon_2, \boldsymbol{p}_2^*) > R_1(t_{K+1}, \epsilon_k 1, \boldsymbol{p}_1^*) = R_0^*$, we can slightly increase p_1^* and decrease p_2^* to construct a new feasible solution with higher objective value than $(\boldsymbol{p}^*, R_0^*)$.

As a result, Lemma 1 is proved by contradiction.

Appendix B
Proof of Lemma 2

Assume that the optimal solution $(\boldsymbol{p}^*, R_0^*)$ of problem (12) satisfies $\sum_{k=1}^K p_k^* < P_{\max}$. We can construct a new solution $(\bar{\boldsymbol{p}} = [\bar{p}_1, \bar{p}_2, \cdots, \bar{p}_K], \bar{R}_0)$

$$\bar{p}_k = \frac{P_{\max}}{\sum_{k=1}^K p_k^*} p_k^*, \quad \bar{R}_0 = \min_{k \in \mathcal{K}} R_k(t_{K+1}, \epsilon_k, \bar{\boldsymbol{p}}_k). \quad \text{(B.1)}$$

Since $\frac{P_{\max}}{\sum_{k=1}^K p_k^*} > 1$, we can show that $R_k(_{K+1}, \epsilon_k, \bar{\boldsymbol{p}}_k) > R_k(_{K+1}, \epsilon_k, \boldsymbol{p}_k^*)$ from (10) and consequently

$$\bar{R}_0 > \min_{k \in \mathcal{K}} R_k(_{K+1}, \epsilon_k, \boldsymbol{p}_k^*) = R_0^*. \quad \text{(B.2)}$$

Thus, $(\bar{\boldsymbol{p}}, \bar{R}_0)$ is a feasible solution with higher objective value of problem (12) than $(\boldsymbol{p}^*, R_0^*)$, which contradicts that $(\boldsymbol{p}^*, R_0^*)$ is the optimal solution, i.e, Lemma 2 is proved.

Appendix C
Proof of Theorem 1

Denote

$$a_k = \sum_{l=k}^K p_l, b_k = \frac{T}{t_{K+1}(1-e_k)B}, a_{K+1} = 0, \quad \forall k \in \mathcal{K}. \quad \text{(C.1)}$$

Setting $R_k(t_{K+1}, \epsilon_k, \boldsymbol{p}) = R_0$ from Lemma 1, equation (10) becomes

$$b_k R_0 = \log_2 \left(\frac{h_k a_k + \sigma^2}{h_k a_{k+1} + \sigma^2} \right). \tag{C.2}$$

According to (C.2), we can obtain

$$a_{k+1} = \frac{a_k}{2^{b_k R_0}} - \frac{(2^{b_k R_0} - 1)\sigma^2}{2^{b_k R_0} h_k}. \tag{C.3}$$

Using the recursive formulation (C.3) and $a_1 = \sum_{k=1}^{K} p_k = P_{\max}$ from Lemma 2, we have

$$a_k = \frac{P_{\max}}{2^{\sum_{l=1}^{k-1} b_l R_0}} - \sum_{l=1}^{k-1} \frac{(2^{b_l R_0} - 1)\sigma^2}{2^{\sum_{j=l}^{k-1} b_j R_0} h_l}. \tag{C.4}$$

Setting $a_{K+1} = 0$ from (C.1) to (C.4) results in (14). Based on (C.1), we have

$$p_k = a_k - a_{k+1}. \tag{C.5}$$

Further applying (C.4) and (C.5) yields (13).

Appendix D
Proof of Lemma 3

We first show that e_k increases with ϵ_k. According to (4), average QKD error rate can be rewritten as

$$e_k = \frac{4|\alpha|^2|\beta|^2}{\frac{2}{\epsilon_k^2} - \frac{4}{\epsilon_k} + 3}. \tag{D.1}$$

Since

$$\left(\frac{2}{\epsilon_k^2} - \frac{4}{\epsilon_k} \right)' = \frac{4\epsilon_k - 4}{\epsilon_k^3} \leq 0, \quad \forall 0 \leq \epsilon_k \leq 1, \tag{D.2}$$

the denominator of e_k is decreasing. Thus, e_k is increasing with ϵ_k and $R_k(t_{K+1}, \epsilon_k, \boldsymbol{p}_k)$ decreases with ϵ_k from (10).

Then, assume that $R_k(t_{K+1}^*, \epsilon_k^*, \boldsymbol{p}_k) > R_0^*$ if $0 < \epsilon_k^* < 1$. Since $R_k(t_{K+1}, \epsilon_k, \boldsymbol{p}_k)$ decreases with ϵ_k, we can increase ϵ_k^* to ϵ_k' such that $R_k(t_{K+1}^*, \epsilon_k^*, \boldsymbol{p}_k) > R_k(t_{K+1}^*, \epsilon_k', \boldsymbol{p}_k) = R_0^*$ if $R_k(t_{K+1}^*, 1, \boldsymbol{p}_k) < R_0^*$; otherwise, we increase ϵ_k^* to $\epsilon_k' = 1$. According to (11b)-(11c), it is found that ϵ_k' is also feasible. Since the objective value is not decreased with new feasible solution ϵ_k', Lemma 3 is proved.

Appendix E
Proof of Theorem 2

According to (4) and $R_k(t_{K+1}, \epsilon_k, \boldsymbol{p}) = R_0$ from Lemma 3, equation (10) becomes

$$R_0 = \frac{t_{K+1} r_k}{T} \left(1 - \frac{4|\alpha|^2|\beta|^2\epsilon_k^2}{2(1-\epsilon_k)^2 + \epsilon_k^2} \right). \tag{E.1}$$

Solving (E.1) and considering constraints (11e) can result in (16). Further substituting (16) into (11b) yields (17). Based on (17) and the maximal time constraint (11c), we have

$$\sum_{k=1}^{K} \frac{d_k}{c} \left\lceil \frac{8m_k}{\left(1 - \sqrt{\frac{4|\alpha|^2|\beta|^2 t_{K+1} r_k}{2(t_{K+1} r_k - R_0 T)} - \frac{1}{2}} \Big|_0^1 \right)^2} \right\rceil \leq T - t_{K+1}. \tag{E.2}$$

Since the left term of (E.2) increases with objective value R_0, the maximal R_0 is achieved when (E.2) holds with equality.

Acknowledgment

This work was supported by EPSRC grant EP/P003486/1.

References

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *arXiv preprint arXiv:1902.10265*, 2019.

[2] M. Chen, W. Saad, and C. Yin, "Virtual reality over wireless networks: Quality-of-service model and learning-based resource management," *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5621–5635, Nov. 2018.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

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

[5] P. Xue, C.-F. Li, and G.-C. Guo, "Efficient quantum-key-distribution scheme with nonmaximally entangled states," *Phys. Rev. A*, vol. 64, p. 032305, Aug. 2001.

[6] C. H. Bennett, "Quantum crytography," in *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore, India, 1984*, 1984, pp. 175–179.

[7] C. Bennett, "Ch bennett, f. bessette, g. brassard, l. salvail, and j. smolin, j. cryptology 5, 3 (1992)." *J. Cryptology*, vol. 5, p. 3, 1992.

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

[9] 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, p. 190502, Nov 2018.

[10] W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, no. 15, p. 3283, 1998.

[11] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," *Phys. Rev. Lett.*, vol. 113, p. 060503, Aug 2014.

[12] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Jul. 2014.

[13] Z. Yang, W. Xu, C. Pan, Y. Pan, and M. Chen, "On the optimality of power allocation for NOMA downlinks with individual QoS constraints," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1649–1652, July 2017.

[14] W. Shin, M. Vaezi, B. Lee, D. J. Love, J. Lee, and H. V. Poor, "Non-orthogonal multiple access in multi-cell networks: Theory, performance, and practical challenges," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 176–183, Oct. 2017.

[15] Z. Yang, C. Pan, W. Xu, Y. Pan, M. Chen, and M. Elkashlan, "Power control for multi-cell networks with non-orthogonal multiple access," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 927–942, Feb. 2018.

[16] K. Wang, Y. Liu, Z. Ding, and A. Nallanathan, "User association in non-orthogonal multiple access networks," in *Proc. IEEE Int. Conf. Commun.*, Kansas City, MO, USA, May 2018, pp. 1–6.

[17] Z. Yang, W. Xu, Y. Pan, C. Pan, and M. Chen, "Energy efficient resource allocation in machine-to-machine communications with multiple access and energy harvesting for IoT," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 229–245, Feb. 2018.

[18] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5G and beyond," *IEEE Proceedings*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017.

[19] Z. Yang, W. Xu, Y. Pan, C. Pan, and M. Chen, "Optimal fairness-aware time and power allocation in wireless powered communication networks," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3122–3135, July 2018.

[20] Z. Yang, C. Pan, M. Shikh-Bahaei, W. Xu, M. Chen, M. Elkashlan, and A. Nallanathan, "Joint altitude, beamwidth, location and bandwidth optimization for UAV-enabled communications," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1716–1719, Aug 2018.

[21] Z. Yang, C. Pan, Y. Pan, Y. Wu, W. Xu, M. Shikh-Bahaei, and M. Chen, "Cache placement in two-tier hetnets with limited storage capacity: Cache or buffer?" *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5415–5429, Nov 2018.