Effective Secrecy Rate for a Downlink NOMA Network

Wenjuan Yu, *Member, IEEE*, Arsenia Chorti, *Member, IEEE*, Leila Musavian, *Member, IEEE*, H. Vincent Poor, *Fellow, IEEE*, and Qiang Ni, *Senior Member, IEEE*

***Abstract*— In this paper, a novel approach is introduced to study the achievable delay-guaranteed secrecy rate, by introducing the concept of the effective secrecy rate (ESR). This study focuses on the downlink of a non-orthogonal multiple access (NOMA) network with one base station, multiple single-antenna NOMA users and an eavesdropper. Two possible eavesdropping scenarios are considered: 1) an internal, unknown, eavesdropper in a purely antagonistic network; and 2) an external eavesdropper in a network with trustworthy peers. For a purely antagonistic network with an internal eavesdropper, the only receiver with a guaranteed positive ESR is the one with the highest channel gain. A closed-form expression is obtained for the ESR at high signal-to-noise ratio (SNR) values, showing that the strongest user's ESR in the high SNR regime approaches a constant value irrespective of the power coefficients. Furthermore, it is shown the strongest user can achieve higher ESR if it has a distinctive advantage in terms of channel gain with respect to the second strongest user. For a trustworthy NOMA network with an external eavesdropper, a lower bound and an upper bound on the ESR are proposed and investigated for an arbitrary legitimate user. For the lower bound, a closed-form expression is derived in the high SNR regime. For the upper bound, the analysis shows that if the external eavesdropper cannot attain any channel state information (CSI), the legitimate NOMA user at high SNRs can always achieve positive ESR, and the value of it depends on the power coefficients. Simulation results numerically validate the accuracy of the derived closed-form expressions and verify the analytical results given in the theorems and lemmas.**

***Index Terms*— Effective capacity, secrecy rate, NOMA, delay-outage probability.**

Manuscript received June 13, 2018; revised March 29, 2019; accepted August 14, 2019. Date of publication September 6, 2019; date of current version December 10, 2019. This work was supported in part by the U.K. Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/N032268/1 and Grant EP/K011693/1, in part by the EU Seventh Framework Programme (FP7) under Grant PIRSES-GA-2013-610524, in part by the Royal Society Project under Grant IEC170324, and in part by the U.S. National Science Foundation under Grant ECCS-1647198 and Grant CNS-1702808. The associate editor coordinating the review of this article and approving it for publication was Prof. S. Yang. *(Corresponding author: Wenjuan Yu.)*

W. Yu is with the 5G Innovation Centre, Institute for Communication Systems, University of Surrey, Guildford GU2 7XH, U.K. (e-mail: w.yu@surrey.ac.uk).

A. Chorti is with ETIS, UMR 8051, Université Paris Seine, Université Cergy-Pontoise, ENSEA, CNRS, 95000 Cergy, France (e-mail: arsenia.chorti@ensea.fr).

L. Musavian is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, U.K. (e-mail: leila.musavian@essex.ac.uk).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Q. Ni is with the InfoLab21, School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K. (e-mail: q.ni@lancaster.ac.uk).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2019.2938515

I. Introduction

NON-ORTHOGONAL multiple access (NOMA) is considered to be a promising multiple access (MA) technique for fifth generation (5G) and beyond (B5G) networks, because of its advantages over conventional orthogonal multiple access (OMA) schemes, in terms of spectral efficiency [1], cell-edge throughput [2], and energy efficiency [3]. Power-domain NOMA[1] allows multiple users to transmit with different transmission power levels, but using the same radio resources, such as subcarrier channels, codes and time slots [4], [5]. Specifically, superposition coding is applied at the transmitter to enable user-multiplexing, while multiuser separation techniques such as successive interference cancellation (SIC) are applied at the receiver to eliminate the co-channel interference and decode the superimposed messages [6], [7]. The users with higher channel gains can obtain the prior information of weaker users in accordance with the NOMA principle. On one hand, the obtained prior information can be utilized to help the weaker users to decode their messages [2], but as mentioned in [8], this can also cause security issues.

Providing secure communication has always been an important issue in wireless networks. Traditionally, security is carried out at upper layers of the protocol stack, relying on encryption algorithms which are agnostic to the wireless channels' physical properties [9], [10]. However, in 5G and Internet of things (IoT) networks, with the explosive growth in the number of low-complexity, power and computationally constrained devices, the concept of physical layer security (PLS) is attracting considerable attention. PLS exploits the randomness of wireless channels to ensure that the transmitted information cannot be decoded by a malicious eavesdropper [10], [11]. Based on the concept of perfect secrecy proposed by Shannon [12], Wyner introduced the wiretap channel model, in which two legitimate users can communicate reliably through a main channel while keeping the exchanged messages confidential from an eavesdropper. Considering Gaussian wiretap channels, the secrecy capacity, i.e., the maximum achievable rate which guarantees reliable communication while the eavesdropper cannot decode any confidential message, is equal to the difference between the main channel's Shannon capacity and the adversary channel's Shannon capacity [9], [13]. Consequently, confidential transmission in Gaussian wiretap

[1] In the following sections, the power-domain NOMA is simply referred to as NOMA.

channels requires that the legitimate user's channel has a higher signal-to-noise ratio (SNR) than the wiretap channel [11]. On the other hand, the ergodic secrecy capacity for wireless fading channels can be positive even when the adversary has a higher average SNR than the legitimate user's channel, which indicates that fading can be beneficial for secrecy [11]. This is because whenever the legitimate user experiences a higher channel gain than the eavesdropper, this fading realization can be exploited for secure transmission [9].

Focusing on large-scale networks utilizing the NOMA protocol, PLS was investigated in [14] and [15] by invoking stochastic geometry. By adopting a user pairing technique which allows two mobile users to share one orthogonal radio resource, the exact analytical expressions for the secrecy outage probability were derived and analyzed for single-antenna and multiple-antenna scenarios [15]. In [16], the feasible transmit power region was first identified to maximize the sum of secrecy rates for a single-input single-output NOMA system, which satisfies all users' required quality-of-service (QoS) values. Then, a closed-form expression was derived for the proposed optimal power allocation strategy. In [17], a network in which the source and an untrusted relay simultaneously transmit signals through non-orthogonal channels was considered. It was concluded that the proposed non-orthogonal relaying scheme provides an improved ergodic secrecy rate, compared to the conventional orthogonal relaying schemes.

Although investigating the secrecy capacity in different wireless networks with the NOMA protocol applied, the aforementioned literature adopts the physical layer channel model, i.e., Shannon theory, without placing emphasis on the legitimate users' delay requirements. On the other hand, for the emerging delay-sensitive wireless communication networks and applications [18], such as vehicular communications, e-health communication and Tactile Internet, delay QoS guarantees will play a critical role in 5G and beyond 5G networks. Furthermore, in future wireless networks, users are expected to necessitate flexible delay guarantees for achieving different service requirements. Henceforth, in order to satisfy diverse delay requirements, a simple and flexible delay QoS model is imperative to be applied and investigated. In this respect, the effective capacity (EC) theory was proposed in [19], with EC denoting the maximum constant arrival rate which can be served by a given service process, while guaranteeing the required statistical delay provisioning. By considering the secrecy rate as the given service rate, we propose in turn the novel concept of the effective secrecy rate (ESR); ESR represents the maximum constant arrival rate that can be securely served, on the condition that the required delay constraint can be statistically satisfied.

In this paper, focusing on a downlink NOMA network with one base station (BS), multiple single-antenna mobile users and an eavesdropper, we aim to propose and thoroughly analyze the ESR for delay-sensitive NOMA users. Different from the user paring design in [14] and [15], we assume that all legitimate NOMA users can transmit using the same resource slot. To provide a comprehensive study, two different eavesdropping scenarios are considered in this paper. Firstly, a purely antagonistic network is studied, in which every NOMA user can act as a passive eavesdropper intercepting confidential messages intended for other users. A practical scenario for this case would be ad-hoc networks with confidential information broadcasted with existing untrusted peers [10]. Secondly, when all NOMA users are trustworthy, there may exist an external eavesdropper that has an interest in compromising the network's security. Hence, with an external eavesdropper intending to decode the NOMA users' messages, the ESR of an arbitrary legitimate user is proposed and investigated, while satisfying their corresponding statistical delay requirement.

Considering the above eavesdropping scenarios, this paper has the following main contributions:

- After proposing the concept of ESR, we theoretically analyze the impact of delay exponent θ on ESR and provide Theorem 1. It is proved that the ESR monotonically decreases with θ. Specifically, we prove that when $\theta \to 0$, the ESR converges to the traditional ergodic secrecy rate, while when $\theta \to \infty$, it represents the delay-limited case and simulation results show that the value of ESR reduces to zero, for Rayleigh fading channels.
- In the presence of an unknown internal eavesdropper, the only legitimate receiver which can achieve a non-zero secrecy rate is the user with the highest channel gains.[2] For the strongest user, we derive the closed-form expressions for the ESR and the traditional ergodic secrecy rate, at high SNRs. Furthermore, we show that the strongest user can achieve higher ESR if it has a distinctive advantage in terms of channel gain with respect to the second strongest user. Also, it is proved that the ESR in the high SNR regime approaches a constant value irrespective of the power coefficients.
- In the presence of a malicious external eavesdropper, a lower bound and an upper bound are respectively analyzed for the ESR and the traditional ergodic secrecy rate.[3] For the lower bound, the closed-form expressions are derived for the high SNR regime. For the upper bound, the analysis shows that if the external eavesdropper cannot attain any channel state information (CSI), the legitimate NOMA user in the high SNR regime can always achieve positive delay-guaranteed secrecy rate, and the value of it depends on the power coefficients.
- Simulation results verify the accuracy of the derived closed-form expressions and confirm the tightness of the proposed bounds. The impact of the delay requirements, the size of the NOMA set and the power coefficient settings is also investigated. Specifically, it is shown that when there is an external eavesdropper, a legitimate NOMA user with stronger channel gains will be more impacted in terms of its achievable ESR, in order to guarantee a required statistical delay QoS. Further, numerical results also reveal that a larger user set leads to smaller ESR values for the legitimate users in both eavesdropping scenarios.

[2]Hereafter, the user with the highest channel gain is referred to as the strongest user.

[3]We note that in this case, these results are not limited to the strongest user.

The rest of the paper is organised as following: the system model is discussed in Section II. The theory of EC is briefly reviewed in Section III, followed by analytical expressions of the ESR for the scenarios of an internal and an external eavesdropper, respectively. Section IV includes simulation results and discussions, followed by conclusions summarized in Section V.

II. System Model

A classical cellular downlink transmission is considered, where one BS transmits public and confidential messages to M single-antenna NOMA users in the presence of a malicious eavesdropper. The wireless channels from the BS to legitimate NOMA users and the eavesdropper are all assumed to be block fading, i.e., the channel gains remain constant within each fading-block, but independently change from one block to the next. Each fading-block duration $T_{\rm f}$ is equal to the frame size, which is an integer multiple of the symbol period.

The channel gains from the BS to the $m^{\rm th}$ user and the eavesdropper are assumed to be Rayleigh distributed and denoted by $h_m, m \in \{1\ldots,,M\}$[4] and h_e,[5] respectively. Without loss of generality, all NOMA users and the malicious adversary's channel gains are assumed to be ordered as $0 < |h_1|^2 \leq |h_2|^2 \ldots \leq |h_{M_E}|^2 \leq |h_e|^2 \leq |h_{M_{E+1}}|^2 \ldots \leq |h_M|^2$, in which M_E indicates the number of NOMA users that have smaller or equal channel gains with respect to the eavesdropper. The BS transmits the signal $\sum_{i=1}^{M}\sqrt{\gamma_i}Ps_i$ to all legitimate users in accordance with NOMA principle. Here, γ_i is the $i^{\rm th}$ user's power coefficient, P is the total transmission power, and s_i is the message for the $i^{\rm th}$ user with $\mathbb{E}\left[|s_i|^2\right]=1$. By following the NOMA protocol [20], the power coefficients[6] are ordered as $\gamma_1 \geq \cdots \geq \gamma_M$, and $\sum_{i=1}^{M}\gamma_i = 1$.

The received signals y_m at the $m^{\rm th}$ legitimate user, $1 \leq m \leq M$, and y_e at the eavesdropper are respectively given as [21]:

$$y_m = h_m \sum_{i=1}^{M}\sqrt{\gamma_i}Ps_i + n_m, \tag{1}$$

$$y_e = h_e \sum_{i=1}^{M}\sqrt{\gamma_i}Ps_i + n_e, \tag{2}$$

where n_m, n_e denote zero-mean additive white Gaussian noise (AWGN) at the $m^{\rm th}$ user and at the eavesdropper, respectively, i.e., $n_m, n_e \sim \mathcal{N}(0,\sigma^2)$.[7]

Based on the NOMA principle, the $m^{\rm th}$ user applies the SIC technique to detect its own messages, by successively decoding the weaker users' messages, i.e., the $i^{\rm th}$ user with $|h_i|^2 < |h_m|^2$, and then eliminating the message from the SNR received signals [22]. On the other hand, the messages for the user with stronger channel gains, i.e., the $i^{\rm th}$ user with $|h_i|^2 > |h_m|^2$, will be considered as noise at the $m^{\rm th}$ user. To ensure that SIC is successfully applied at the $m^{\rm th}$ user, it is assumed that $R_{i\to m} \geq \tilde{R}_i$ [23], where $R_{i\to m}$ denotes the $m^{\rm th}$ user's data rate to decode the $i^{\rm th}$ user's message and $\tilde{R}_i$ is the target data rate for the $i^{\rm th}$ user. Therefore, when it decodes its own message, the $m^{\rm th}$ legitimate NOMA user's achievable rate, in b/s/Hz, is given by [14]

$$R_m = \log_2\left(1+\frac{\rho|h_m|^2\gamma_m}{\rho|h_m|^2\sum_{i=m+1}^{M}\gamma_i+1}\right), \quad 1 \leq m \leq M, \tag{3}$$

where ρ is the transmit SNR, i.e., $\rho = \dfrac{P}{\sigma^2}$.

Regarding the eavesdropper, it employs SIC to detect the $m^{\rm th}$ legitimate user's messages with an achievable decoding rate denoted by $R_e^{(m)}$. Considering that the eavesdropper can be within the set of NOMA users or distinct from them, the corresponding mathematical expressions of $R_e^{(m)}$ can be different and we will study them respectively in the following Section. The $m^{\rm th}$ NOMA user's secrecy rate is achievable when an encoding scheme exists that simultaneously ensures reliable communication and perfect secrecy with respect to the eavesdropper. In the following, the m-th user's achievable secrecy rate is denoted by R_s^m and expressed as [9]

$$R_s^m = \left[R_m - R_e^{(m)}\right]^+, \quad 1 \leq m \leq M, \tag{4}$$

where R_m is given in (3) and $[x]^+ = \max\{0,x\}$.

III. Effective Secrecy Rate

In order to support the emerging delay-sensitive wireless communication services and applications, in the following, we first introduce the theory of EC. Then, we introduce the concept of the ESR as an achievable arrival rate that can be securely served, while statistically satisfying the required delay QoS constraints. Let us take the $m^{\rm th}$ user as an example. Assume a first-in-first-out (FIFO) buffer for the $m^{\rm th}$ user at the BS.[8] Define $D_m(t)$ as the delay experienced by a packet arriving at time t. From [19], the probability of the delay $D_m(t)$ exceeding a maximum delay limit $D_{\max}^m$ can be estimated as

$$P_{\rm delay}^{\rm out} = \Pr\{D_m(t) > D_{\max}^m\} \approx \Pr\{\mathcal{Q}(t)>0\}{\rm e}^{-\theta_m\mu D_{\max}^m}, \tag{5}$$

where $P_{\rm delay}^{\rm out}$ denotes the delay violation probability limit for the $m^{\rm th}$ user, $\Pr\{\mathcal{Q}(t)>0\}$ is the probability of a non-empty buffer at time t, $D_{\max}^m$ is the given delay bound in the unit of symbol duration, and θ_m ($\theta_m > 0$) represents the exponential decay rate. The authors in [19] proved that the constant arrival rate needs to be limited to the value of μ, which equals to EC, so that a target delay violation probability limit can be met. Let $\{R_s^m(t), t = 1,2,\ldots\}$ be a series of non-negative random variables, representing the service process of the $m^{\rm th}$ user. Assume that the service process satisfies Gärtner-Ellis theorem [24]. Then, the EC for the $m^{\rm th}$ user on a block-fading channel is defined as

$$E_{\rm s}^m = -\frac{1}{\theta_m T_{\rm f} B}\ln\left(\mathbb{E}\left[e^{-\theta_m T_{\rm f} B R_s^m}\right]\right), \quad \text{(b/s/Hz)}, \tag{6}$$

[4]The time index t is omitted hereafter.

[5]The instantaneous channel gain h_e is unknown, if the eavesdropper is an external adversary.

[6]Adaptive power allocation can influence the exact values of ESR, but this is beyond the scope of this paper and optimal power allocation to maximize the network's sum ESR is considered to be a future research topic.

[7]For simplicity, the noise variances at all users and the eavesdropper are assumed to be identical and equal to σ^2.

[8]It is assumed that for every served user, there is one virtual buffer at the BS.

where $\mathbb{E}[\cdot]$ is the expectation over its channel gains. When the focus is on the rate that can be securely transmitted, we can obtain the ESR for the m^{th} user, by inserting the achievable secrecy rate R_s^m, given in (4), into (6).

From (5), it can be noted that θ_m denotes the exponential decay rate of delay violation probability, for the m^{th} user. A smaller value of θ_m indicates that the user has a relatively loose delay QoS requirement, while a larger value of θ_m means that a more stringent delay QoS is required. In particular, when $\theta_m \to 0$, the probability of the experienced delay exceeding a given bound approaches one. When $\theta_m \to \infty$, it indicates that the user cannot tolerate any delay outage. To clarify, we summarize in the following theorem.

Theorem 1: The ESR for the m^{th} user, i.e., E_{s}^m in (6), is a monotonically decreasing function in θ_m. When $\theta_m \to 0$, E_{s}^m converges to the ergodic secrecy rate, i.e., $\mathbb{E}[R_s^m]$. When $\theta_m \to \infty$, this represents the delay-limited scenario and the value of E_{s}^m reduces to zero.

Proof: See Appendix A. ∎

Theorem 1 shows that the proposed ESR, describing the delay-guaranteed secrecy rate,[9] contains a delay exponent θ_m indicating the stringency of delay requirement. Specifically, this theorem reveals that the ESR is a more general performance metric, which includes the traditional ergodic secrecy rate at an extreme case. For delay-limited scenarios, i.e., when $\theta_m \to \infty$, the value of E_{s}^m reduces to zero for Rayliegh fading channels, which will be shown in Section IV.

A. Effective Secrecy Rate With an Internal Eavesdropper

In this section, we first consider a purely antagonistic network in which every user can be a potential eavesdropper intercepting the confidential messages of the other users. Assume that the knowledge of CSI for all legitimate users is perfectly known at the BS, which implies that the internal eavesdropper's CSI is available. Note that by applying SIC, the user with the strongest channel gains can successfully decode the information of other NOMA users which have weaker channel gains. Hence, when there is an untrusted internal adversary, the only legitimate receiver which can achieve a non-zero secrecy rate is the M^{th} user which has the strongest channel gains. Specifically, the worst case scenario is that the $(M-1)^{\text{th}}$ user acts as the eavesdropper and intends to detect the M^{th} user's messages. Then, the secrecy rate for all legitimate users can be expressed as

$$R_s^m = \begin{cases} \log_2\left(1+\rho|h_M|^2\gamma_M\right) \\ -\log_2\left(1+\rho|h_{M-1}|^2\gamma_M\right), & m=M, \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

For ease and compactness, in the following we introduce the notation: $q_m = \rho\gamma_m$, $Q_m = \rho\sum_{i=m}^{M}\gamma_i$, and $\beta_m = -\frac{\theta_m T_f B}{\ln 2}$, where $m \in \{1, 2\ldots, M\}$.

[9]Here, we are talking about the amount of arrival rate that can be securely served and delay statistically guaranteed.

Then, the M^{th} user's ESR can be provided by inserting (7) into (6), which yields

$$E_{\text{s}}^M = \frac{1}{\beta_M}\log_2\left(\mathbb{E}\left[\left(\frac{1+q_M|h_M|^2}{1+q_M|h_{M-1}|^2}\right)^{\beta_M}\right]\right). \tag{8}$$

By setting $y = |h_M|^2$, and $x = |h_{M-1}|^2$, (8) can be expanded as

$$E_{\text{s}}^M = \frac{1}{\beta_M}\log_2\Bigg(\iint\limits_{\substack{0<x<\infty \\ y\geq x}}\left(\frac{1+q_M y}{1+q_M x}\right)^{\beta_M} \times f_{(M-1,M)}(x,y)\,\mathrm{d}x\,\mathrm{d}y\Bigg), \tag{9}$$

where $f_{(M-1,M)}(x,y)$ denotes the joint probability density function (PDF) of the ordered channel gains $|h_{M-1}|^2$ and $|h_M|^2$, with $|h_{M-1}|^2 \leq |h_M|^2$. For M unordered independent channel gains which are Rayleigh distributed with a unit-variance, we define the PDFs of the unordered $|h_{M-1}|^2$ and $|h_M|^2$ as $f(x)$ and $f(y)$, respectively. Then, the cumulative distribution functions (CDF) of the unordered channel gains are given as $F(x)$ and $F(y)$. When all users' channel gains are ordered, the statistical features follow the theory of order statistics [25]. Hence, the joint PDF of the ordered $|h_{M-1}|^2$ and $|h_M|^2$, with $|h_{M-1}|^2 \leq |h_M|^2$, is given by [25]

$$f_{(M-1,M)}(x,y) = M(M-1)f(x)\left(F(x)\right)^{M-2}f(y). \tag{10}$$

Finally, by inserting the joint PDF $f_{(M-1,M)}(x,y)$ into (9), we provide the following theorem.

Theorem 2: Suppose that there is an internal eavesdropper among all NOMA users. Considering the worst case scenario, the M^{th} user's achievable ESR can be written as

$$E_{sc}^M = B_M + \frac{1}{\beta_M}\log_2\Bigg(\sum_{\nu=0}^{M-2}\binom{M-2}{\nu}(-1)^\nu e^{\frac{\nu}{q_M}} \times \sum_{k=0}^{\infty}\frac{(-1)^k}{k!}\frac{(\nu+1)^k}{k-\beta_M+1}\left[\Gamma\left(k+2,\frac{1}{q_M}\right) - \left(\frac{1}{q_M}\right)^{k-\beta_M+1}\times\ \Gamma\left(1+\beta_M,\frac{1}{q_M}\right)\right]\Bigg), \tag{11}$$

where $B_M = \frac{\ln(M(M-1))+2q_M^{-1}}{\beta_M \ln 2}$ and $\Gamma(\cdot,\cdot)$ is the incomplete Γ function.

Proof: See Appendix B. ∎

Note that it is difficult to directly analyze (11) and to obtain intuition of the impact of the various parameters on the ESR. To obtain a tractable expression, in the following, we derive the closed-form expression for E_{s}^M at high SNRs. Firstly, at high SNRs, i.e., $\rho \gg 1$, R_s^M can be simplified to

$$\lim_{\rho\to\infty} R_s^M = \log_2\left(\frac{|h_M|^2}{|h_{M-1}|^2}\right). \tag{12}$$

The ergodic secrecy rate at high SNRs, i.e., $\lim_{\rho\to\infty}\mathbb{E}[R_s^M]$, equals to $\mathbb{E}\left[\log_2\left(\frac{|h_M|^2}{|h_{M-1}|^2}\right)\right]$. This shows that at high SNRs, the M^{th} user's ergodic secrecy rate depends only on the (ratio of) channel gains between the M^{th} user and the internal eavesdropper.

Then, the ESR at high SNRs for the M^{th} user, denoted as $\lim_{\rho\to\infty} E_{\text{s}}^{M}$, can be expressed as

$$\lim_{\rho\to\infty} E_{\text{s}}^{M} = \frac{1}{\beta_M}\log_2\left(\mathbb{E}\left[\left(\frac{|h_M|^2}{|h_{M-1}|^2}\right)^{\beta_M}\right]\right). \quad (13a)$$

Comparing to the case of the ergodic capacity, we can clearly see the impact of the exponential delay decay exponent captuted in β_M. From (13a), we can note that for a fixed value of delay factor β_M, the ESR value at high SNRs increases with the ratio of channel gains. This demonstrates that the M^{th} user can achieve higher delay-guaranteed secrecy rate if it has a distinctive advantage in terms of channel gain with respect to second in rank user. By setting $y = |h_M|^2$, and $x = |h_{M-1}|^2$, (13a) can be expanded as

$$\lim_{\rho\to\infty} E_{\text{s}}^{M} = \frac{1}{\beta_M}\log_2\left(\iint\limits_{\substack{0<x<\infty\\ y\geq x}} \left(\frac{y}{x}\right)^{\beta_M} f_{(M-1,M)}(x,y)\,\mathrm{d}x\,\mathrm{d}y\right). \quad (14)$$

After applying the joint PDF $f_{(M-1,M)}(x,y)$, we derive the closed-form expressions for $\lim_{\rho\to\infty} E_{\text{s}}^{M}$ and $\lim_{\rho\to\infty}\mathbb{E}\left[R_s^M\right]$ in the following theorem.

Theorem 3: Suppose that there is an unknown internal eavesdropper among all NOMA users. Considering the worst case scenario, the closed-form expression for the M^{th} user's ESR at high SNRs, i.e., $\lim_{\rho\to\infty} E_{\text{s}}^{M}$, is given by

$$\lim_{\rho\to\infty} E_{\text{s}}^{M} = \frac{1}{\beta_M}\log_2\Bigg(M(M-1)\Gamma(1-\beta_M) \times \sum_{s=0}^{M-2}\binom{M-2}{s}(-1)^s {}_2\mathbf{F}_1\left[\begin{matrix}1-\beta_M,\ 2\\ 2-\beta_M\end{matrix}; -1-s\right]\Bigg), \quad (15)$$

where $\Gamma(\cdot)$ is gamma function and ${}_2\mathbf{F}_1\left[\begin{smallmatrix}a,\ b\\ c\end{smallmatrix}; z\right]$ is the generalized hypergeometric function [26]. Furthermore, for comparison purposes, the ergodic secrecy rate for the M^{th} user at high SNRs, i.e., $\lim_{\rho\to\infty}\mathbb{E}\left[R_s^M\right]$, can be expressed in closed-form, given in (16).

$$\lim_{\rho\to\infty}\mathbb{E}[R_s^M] = M(M-1)\sum_{s=0}^{M-2}\binom{M-2}{s} \times(-1)^s\frac{1}{s+1}\log_2(s+2). \quad (16)$$

Proof: See Appendix C. ∎

From (15), we can notice that when the transmit SNR asymptotically approaches infinity, the M^{th} user's ESR approaches a constant value, irrespective of the transmit SNR and the power coefficients. Furthermore, from (15) and (16), one can note that when the M^{th} user's delay requirement changes (when β_M varies), $\lim_{\rho\to\infty}\mathbb{E}\left[R_s^M\right]$ will not change but the value of ESR, i.e., $\lim_{\rho\to\infty} E_{\text{s}}^{M}$, will be influenced. This is due to the fact that the delay violation probability is not taken into account in traditional secrecy rate, but is considered in the proposed ESR. This demonstrates the gains in considering the delay-guaranteed ESR in low-latency communications.

The validity of the above derived closed-form expressions, given in (15) and (16), will be verified in Section IV, by comparing with Monte Carlo results. Moreover, simulation results will also show that $\lim_{\rho\to\infty} E_{\text{s}}^{M}$ converges to $\lim_{\rho\to\infty}\mathbb{E}\left[R_s^M\right]$, when $\theta_M \to 0$ (or $\beta_M \to 0$). In other words, we can get that $\lim_{\substack{\rho\to\infty\\ \theta_M\to 0}} E_{\text{s}}^{M} = \lim_{\rho\to\infty}\mathbb{E}\left[R_s^M\right]$. This verifies Theorem 1 and confirms that the proposed ESR is a more flexible metric, with the traditional ergodic secrecy rate emerging as a special case.

B. Effective Secrecy Rate With an External Eavesdropper

Here, we assume that all NOMA users are trustworthy and there exists an external eavesdropper which is distinct from the set of legitimate users and intends to decode as many NOMA users' confidential messages as possible. Then, by employing SIC, the adversary's achievable rate for detecting the m^{th} user's message, namely $R_e^{(m)}$, can be given in (17) [21], shown at the top of the next page.

By inserting (3) and (17) into (4) and applying the defined notations $q_m = \rho\gamma_m$, $Q_m = \rho\sum_{i=m}^{M}\gamma_i$, where $m = \{1, 2, \ldots, M\}$, the secrecy rate for the m^{th} user can be then given in (18), shown at the top of the next page. Firstly, when $1 \leq m \leq M_E$, i.e., $|h_m|^2 \leq |h_e|^2$, we have that $\log_2\left(1+\frac{q_m|h_m|^2}{Q_{m+1}|h_m|^2+1}\right)$ is smaller than or equal to $\log_2\left(1+\frac{q_m|h_e|^2}{Q_{m+1}|h_e|^2+1}\right)$, which means that $R_s^m = 0$. On the other hand, when $M_E+1 \leq m \leq M$, we have $\frac{1}{|h_m|^2} \leq \frac{1}{|h_e|^2}$ and $Q_{m+1} \leq Q_{M_E+1} - q_m$. This means that $R_s^m \geq 0$, when $M_E+1 \leq m \leq M$. Hence, the secrecy rate R_s^m can be simplified to (19), shown at the top of the next page.

Assume that the relative order of all NOMA users and the eavesdropper's channel gains is known, i.e., $0 < |h_1|^2 \leq |h_2|^2 \ldots \leq |h_{M_E}|^2 \leq |h_e|^2 \leq |h_{M_E+1}|^2 \ldots \leq |h_M|^2$. Then, by inserting (19) into (6), we have the conditional ESR, namely E_{cs}^{m}, given below.

Case 1: for the m^{th} user with $1 \leq m \leq M_E$

In this case, it is known that the m^{th} user has weaker channel gains compared to the eavesdropper, i.e., $|h_m|^2 \leq |h_e|^2$. Under this condition, by inserting (19) into (6), we have that $E_{\text{cs}}^{m} = 0$.

Case 2: for the m^{th} user with $M_E+1 \leq m \leq M$

In this case, it is known that the m^{th} user has stronger channel gains compared to the eavesdropper, i.e., $|h_m|^2 \geq |h_e|^2$. Under this condition, we can get that

$$E_{\text{cs}}^{m} = \frac{1}{\beta_m}\log_2\left(\mathbb{E}\left[\left(\frac{Q_m|h_m|^2+1}{Q_{m+1}|h_m|^2+1} \times\frac{(Q_{M_E+1}-q_m)\,|h_e|^2+1}{Q_{M_E+1}|h_e|^2+1}\right)^{\beta_m}\right]\right). \quad (20)$$

At this point, a short note on the circumstances under which the ESR can be evaluated is in place. The design of secrecy encoders utilizes so the called (double) binning techniques and relies on full CSI knowledge, i.e., both the legitimate

$$R_e^{(m)} = \begin{cases} \log_2\left(1+\dfrac{\rho|h_e|^2\gamma_m}{\rho|h_e|^2\sum_{i=m+1}^{M}\gamma_i+1}\right), & 1\le m\le M_e, \\ \log_2\left(1+\dfrac{\rho|h_e|^2\gamma_m}{\rho|h_e|^2\sum_{i=M_E+1,i\neq m}^{M}\gamma_i+1}\right), & M_E+1\le m\le M, \end{cases} \tag{17}$$

$$R_s^m = \begin{cases} \left[\log_2\left(1+\dfrac{q_m|h_m|^2}{Q_{m+1}|h_m|^2+1}\right)-\log_2\left(1+\dfrac{q_m|h_e|^2}{Q_{m+1}|h_e|^2+1}\right)\right]^+, & 1\le m\le M_E, \\ \left[\log_2\left(1+\dfrac{q_m|h_m|^2}{Q_{m+1}|h_m|^2+1}\right)-\log_2\left(1+\dfrac{q_m|h_e|^2}{(Q_{M_E+1}-q_m)|h_e|^2+1}\right)\right]^+, & M_E+1\le m\le M, \end{cases} \tag{18}$$

$$R_s^m = \begin{cases} 0, & 1\le m\le M_E, \\ \log_2\left(1+\dfrac{q_m|h_m|^2}{Q_{m+1}|h_m|^2+1}\right)-\log_2\left(1+\dfrac{q_m|h_e|^2}{(Q_{M_E+1}-q_m)|h_e|^2+1}\right), & M_E+1\le m\le M, \end{cases} \tag{19}$$

and the eavesdropper's CSI need to be readily available. This assumption is reasonable in the internal eavesdropper scenario, as the in the NOMA network the source (BS) needs the full CSI to perform the power allocation among the users; indeed, the scenario of a NOMA network with internal eavesdroppers provides an excellent example of how an eavesdropper's CSI can be known to the legitimate transmitter.

On the other hand, in the external eavesdropper case, this assumption is no longer viable; an external passive attacker would indeed have every incentive to conceal themselves and not leak information regarding their actual CSI. However, there is a fundamental difference between a network's secrecy rate and effective secrecy rate. Inspecting the expression in (19) for the ESR, it is clear that it involves an expectation over the distribution of the attacker's channel gains when the legitimate receiver is stronger than the attacker. What is notably different with respect to the evaluation of the secrecy rate, is the fact that in essence only the order – in terms of received SNR – of the eavesdropper among the set of M NOMA users comes into play, as opposed to the case of the secrecy rate in which the exact eavesdropper's SNR needs to be known for the evaluation.

This in turn, is consistent with the way the CSI is fedback to the BS in the uplink of actual systems, such as LTE and NB-IoT, in which instead of the exact CSI and SNR values, an SNR range is determined in the form of a "channel quality indicator" (CQI) [27]. In a realistic setting, it is therefore conceivable that with the aid of artificial noise techniques [28] it is possible to control the range of SNRs that are attainable by the attacker and provide the legitimate users the opportunity to feedback to the BS relevant information regarding the CQI of a potential eavesdropper, therefore removing ambiguities in the evaluation of the ESR.

In terms of the actual design of the secrecy encoders, although it is beyond the scope of the present work, it can be argued that in dense NOMA networks with multiple CQI levels, this information can be taken into account in the design, accounting for the worst case scenario in which the SNR of the eavesdropper is assumed to be in the upper limit of the respective CQI range. Such an approach would of course need to be taken into account in the evaluation of the ESR, but at this point is left as future work.

To calculate E_{cs}^m, we define $z_1 = |h_m|^2$, $z_2 = |h_e|^2$, and note that the joint PDF $f(z_1, z_2) = f_{(m)}(z_1)f(z_2)$.[10] Here, $f_{(m)}(z_1)$ is the PDF of the ordered m^{th} user's channel gains following order statistics and $f(z_2)$ is the PDF of the external adversary's channel gains, which is Rayleigh distributed with unit variance. From the theory of order statistics, we have that

$$f_{(m)}(z_1) = \psi_m f(z_1)\left(1-F(z_1)\right)^{M-m} F(z_1)^{m-1}. \tag{21}$$

Here, $\psi_m = \frac{1}{B(m,M-m+1)}$ and $B(\mu, w)$ is the beta function, i.e., $B(\mu,w) = \Gamma(\mu)\Gamma(w)\big(\Gamma(\mu+w)\big)^{-1}$, where $\Gamma(\mu) = \mu!$, when μ is a positive integer. By inserting the joint PDF $f(z_1, z_2)$ into (20), we provide the following theorem.

Theorem 4: Suppose that there is an external eavesdropper. Assume that the order of the eavesdropper's channel gains among the set of NOMA users is known. For the m^{th} user with $m \geq M_E + 1$, its conditional ESR, i.e., E_{cs}^m, can be simplified to (22), while assuming $\gamma_m \leq \sum_{i=m+1}^{M}\gamma_i$, where $m \neq \{M-1, M\}$, and $a = M - m + 1 + s$. At high SNRs, its conditional ESR, i.e., $\lim_{\rho\to\infty} E_{\text{cs}}^m$, equals to $\log_2\left(\frac{Q_m}{Q_{m+1}}\frac{Q_{M_E+1}-q_m}{Q_{M_E+1}}\right)$.

$$\begin{aligned} E_{\text{cs}}^m \approx \frac{1}{\beta_m}\log_2\Bigg(\psi_m\left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m}\Bigg(\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s\frac{1}{a} \\ +\frac{\beta_m q_m}{Q_{m+1}Q_m}\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s e^{\frac{a}{Q_m}}E_i\left(-\frac{a}{Q_m}\right)\Bigg) \\ \times\left(\frac{Q_{M_E+1}-q_m}{Q_{M_E+1}}\right)^{\beta_m}\Bigg(1-\frac{\beta_m q_m e^{\frac{1}{Q_{M_E+1}}}}{(Q_{M_E+1}-q_m)Q_{M_E+1}} \\ \times E_i\left(-\frac{1}{Q_{M_E+1}}\right)\Bigg)\Bigg). \end{aligned} \tag{22}$$

Proof: See Appendix D. ∎

[10]The legitimate NOMA users and the external adversary are independent, so the joint PDF is the product of two marginal PDFs.

$$\breve{R}_s^m = \begin{cases} \log_2\left(1+\dfrac{q_m|h_m|^2}{Q_{m+1}|h_m|^2+1}\right) - \log_2\left(1+\dfrac{q_m|h_e|^2}{Q_{m+1}|h_e|^2+1}\right), & |h_m|^2 \geq |h_e|^2, \\ 0, & \text{otherwise.} \end{cases} \tag{25}$$

Note that when there exists an external eavesdropper, obtaining the conditional ESR, i.e., E_{cs}^m, requires the relative order of the eavesdropper, in terms of the received SNR, among the set of M NOMA users. If this information is not available, the exact value of E_{cs}^m cannot be obtained. Hence, in the following sections, we study and analyze a lower bound and an upper bound for the ESR, which do not require any prior information of the adversary's relative order.

1) Lower Bound on the ESR With an External Eavesdropper: From [21, ch. 15], it is noted that before the adversary detects the m^{th} user's message, if we assume that the first $m-1$ NOMA users' information has already been successfully decoded, then, we overestimate the malicious adversary's decoding capability. This can happen if the external eavesdropper attains the prior information of the first $m-1$ users' CSI. Therefore, an upper bound on $R_e^{(m)}$ can be given by

$$\hat{R}_e^{(m)} = \log_2\left(1+\frac{q_m|h_e|^2}{Q_{m+1}|h_e|^2+1}\right),\ 1 \leq m \leq M. \tag{23}$$

The lower bound on the m^{th} user's achievable secrecy rate can then be expressed as

$$\breve{R}_s^m = \left[R_m - \hat{R}_e^{(m)}\right]^+, \tag{24}$$

which can be extended to (25), shown at the top of this page.

In practice, the external eavesdropper is independent from NOMA users, which means its channel gains can be higher or lower than the m^{th} user. Hence, we aim to provide a lower bound on the ESR for the m^{th} user, which represents an average delay-guaranteed rate that can be at least obtained, no matter whether the eavesdropper has a better channel condition or not. By inserting $\breve{R}_s^m$ into (6), the lower bound on the ESR for the m^{th} user, i.e., $\breve{E}_{\text{s}}^m$, in the presence of an external eavesdropper, can be expressed as

$$\breve{E}_{\text{s}}^m = -\frac{1}{\theta_m T_{\text{f}} B}\ln\left(\iint\limits_{D_1}\left(\frac{Q_m z_1+1}{Q_{m+1}z_1+1}\frac{Q_{m+1}z_2+1}{Q_m z_2+1}\right)^{\beta_m} \times f(z_1,z_2)\,\mathrm{d}z_1\,\mathrm{d}z_2 + \iint\limits_{D_2} f(z_1,z_2)\,\mathrm{d}z_1\,\mathrm{d}z_2\right), \tag{26}$$

where $D_1 = \{(z_1,z_2), z_1 \geq z_2\}$, and $D_2 = \{(z_1,z_2), z_1 < z_2\}$. Then, after applying the joint PDF $f(z_1,z_2)$, $\breve{E}_{\text{s}}^m$ in (26) can be expanded as

$$\breve{E}_{\text{s}}^m = -\frac{1}{\theta_m T_{\text{f}} B}\ln\left(\psi_m \iint\limits_{D_1}\left(\frac{Q_m z_1+1}{Q_{m+1}z_1+1}\frac{Q_{m+1}z_2+1}{Q_m z_2+1}\right)^{\beta_m} \times \frac{e^{-(M-m+1)z_1-z_2}}{\left(1-e^{-z_1}\right)^{1-m}}\,\mathrm{d}z_1\,\mathrm{d}z_2 + \psi_m \iint\limits_{D_2} e^{-(M-m+1)z_1} \times \left(1-e^{-z_1}\right)^{m-1} e^{-z_2}\,\mathrm{d}z_1\,\mathrm{d}z_2\right). \tag{27}$$

To bring more insights, we approximate $\breve{E}_{\text{s}}^m$ at high SNRs and provide the following theorem.

Theorem 5: Suppose that there is an external eavesdropper. The lower bound on the ESR for the m^{th} user, i.e., $\breve{E}_{\text{s}}^m$, can be approximated at high SNRs and given in (28), based on the condition that $\gamma_m \leq \sum_{i=m+1}^{M}\gamma_i$, where $m \neq \{M-1, M\}$.

$$\breve{E}_{\text{s}}^m \approx \frac{1}{\beta_m}\log_2\left(\psi_m\left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m}\left(A_1+\frac{\beta_m q_m}{Q_m Q_{m+1}}A_2\right) + \psi_m\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s\frac{1}{a+1}\right), \tag{28}$$

where A_1 and A_2 are given by

$$A_1 \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m}\sum_{s=0}^{m-1}\binom{m-1}{s}\frac{(-1)^s}{a}\left(\frac{1}{a+1} - \frac{\beta_m q_m}{Q_m Q_{m+1}}e^{\frac{a+1}{Q_m}}E_i\left(-\frac{a+1}{Q_m}\right)\right), \tag{29}$$

$$A_2 \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m}\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s e^{\frac{a}{Q_m}}\Bigg(e^{\frac{1}{Q_m}} \times\left(E_1\left(\frac{a+1}{Q_m}\right) - e^{-\frac{1}{Q_m}}E_1\left(\frac{a}{Q_m}\right)\right) - \frac{\beta_m q_m}{Q_m Q_{m+1}}e^{\frac{1}{Q_m}} \times\left(\left(r-\ln\left(Q_m\right)+E_1\left(\frac{1}{Q_m}\right)\right)E_1\left(\frac{a}{Q_m}\right) + \frac{1}{2}\left(\zeta(2)+\left(r+\ln\left(\frac{a}{Q_m}\right)\right)^2\right) + e^{-\frac{a}{Q_m}}\sum_{\delta=0}^{\Delta}\frac{e_\delta\left(\frac{a}{Q_m}\right)}{(\delta+1)^2} \times\left(-\frac{1}{a}\right)^{\delta+1} - \frac{a}{Q_m}{}_3\mathbf{F}_3\begin{bmatrix}1,\ 1,\ 1\\ 2,\ 2,\ 2\end{bmatrix}; -\frac{a}{Q_m}\Bigg)\Bigg)\Bigg). \tag{30}$$

and $a = M-m+s+1$. Furthermore, $\zeta(\cdot)$ is the Riemann zeta function, r is the Euler's constant, $e_m(x) = \sum_{s=0}^{m}\frac{x^s}{s!}$, $\Delta \geq 50$,[11] and $E_1(\cdot)$ is the exponential integral function [26]. For comparison purposes, the closed-form expression for the lower bound on ergodic secrecy rate, i.e., $\mathbb{E}[\breve{R}_s^m]$, is given in (31).

$$\mathbb{E}[\breve{R}_s^m] = \frac{\psi_m}{\ln 2}\Bigg(\sum_{s=0}^{m}\binom{m}{s}(-1)^s\frac{1}{a}\left(-e^{\frac{a}{Q_m}}E_i\left(-\frac{a}{Q_m}\right) + e^{\frac{a}{Q_{m+1}}}E_i\left(-\frac{a}{Q_{m+1}}\right)\right) + \sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s\frac{1}{a(a+1)} \times\left(-e^{\frac{a+1}{Q_{m+1}}}E_i\left(-\frac{a+1}{Q_{m+1}}\right) + e^{\frac{a+1}{Q_m}}E_i\left(-\frac{a+1}{Q_m}\right)\right)\Bigg). \tag{31}$$

Proof: See Appendix E. ∎

[11] Here, Δ is used in a finite sum, which approximates an infinite sum. The complete information is given in Appendix E.

We will demonstrate the validity of the derived analytical closed-forms in Section IV. Furthermore, in the following lemma, we explore the impact of ρ on the proposed lower bounds on the ergodic secrecy rate and the ESR, i.e., $\mathbb{E}[\breve{R}_s^m]$ and $\breve{E}_{\rm s}^m$, given in (24) and (28).

Lemma 1: When $\rho \to 0$, $\lim_{\rho\to 0} \mathbb{E}[\breve{R}_s^m] = 0$, $\lim_{\rho\to 0} \breve{E}_{\rm s}^m = 0$. When $\rho \to \infty$, $\lim_{\rho\to \infty} \mathbb{E}[\breve{R}_s^m] = 0$, and $\lim_{\rho\to \infty} \breve{E}_{\rm s}^m = 0$.

Proof: See Appendix F. ∎

Lemma 1 reveals that if the external eavesdropper has the prior information of the first $m-1$ users' CSI, the $m^{\rm th}$ user's achievable secrecy rate at high SNRs, no matter delay-guaranteed or delay-unguaranteed, becomes zero. Note that the above analysis is for a constant delay exponent. In simulation results, we will show more results for various delay requirements.

2) Upper Bound on the ESR With an External Eavesdropper: If none of the first $m-1$ users' information can be decoded when the eavesdropper intends to decode the $m^{\rm th}$ user's message, then we underestimate the decoding ability of the malicious adversary with SIC employed. This may happen if the eavesdropper cannot attain any prior information of the first $m-1$ users' CSI. Therefore, a lower bound on $R_e^{(m)}$ is given by

$$\breve{R}_e^{(m)} = \log_2\left(1 + \frac{q_m|h_e|^2}{Q_1|h_e|^2+1}\right), \quad 1 \le m \le M. \tag{32}$$

Hence, an upper bound on the secrecy rate, i.e., $\hat{R}_s^m$, can be written as

$$\begin{aligned}
&\hat{R}_s^m \\
&= \left[R_m - \breve{R}_e^{(m)}\right]^+ \\
&= \left[\log_2\left(1 + \frac{q_m|h_m|^2}{Q_{m+1}|h_m|^2+1}\right) - \log_2\left(1+\frac{q_m|h_e|^2}{Q_1|h_e|^2+1}\right)\right]^+ \\
&= \left[\log_2\left(1+\frac{q_m}{Q_{m+1}+\frac{1}{|h_m|^2}}\right) - \log_2\left(1+\frac{q_m}{Q_1+\frac{1}{|h_e|^2}}\right)\right]^+.
\end{aligned} \tag{33}$$

From (33), we can note that $\log_2\left(1+\frac{q_m}{Q_{m+1}+\frac{1}{|h_m|^2}}\right) \ge \log_2\left(1+\frac{q_m}{Q_1+\frac{1}{|h_e|^2}}\right)$, when $|h_e|^2 \le |h_m|^2$. However, when $|h_e|^2 \ge |h_m|^2$, the sign cannot be distinguished. Hence, the upper bound on the ESR for the $m^{\rm th}$ user with an external eavesdropper, i.e., $\hat{E}_{\rm s}^m$, can only be obtained numerically, by inserting $\hat{R}_s^m$ into (6).

Although the exact analytical closed-form for the proposed upper bound on the ESR is not available, the following lemma is provided to explore the impact of ρ on the upper bounds on the ergodic secrecy rate and the ESR, i.e., $\mathbb{E}[\hat{R}_s^m]$ and $\hat{E}_{\rm s}^m$.

Lemma 2: When $\rho \to 0$, $\lim_{\rho\to 0} \mathbb{E}[\hat{R}_s^m] = 0$, $\lim_{\rho\to 0} \hat{E}_{\rm s}^m = 0$. When $\rho \to \infty$, $\lim_{\rho\to \infty} \mathbb{E}[\hat{R}_s^m] = \lim_{\rho\to \infty} \hat{E}_{\rm s}^m = \log_2\left(\frac{Q_m}{Q_{m+1}}\frac{Q_1}{Q_1+q_m}\right)$.

Proof: See Appendix G. ∎

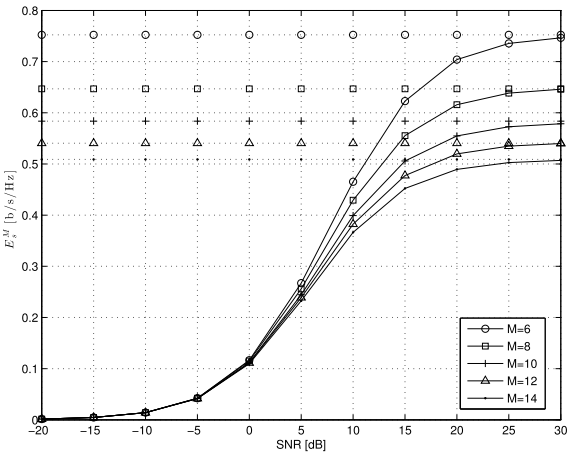


Fig. 1. $E_{\rm s}^M$, vs. the transmit SNR ρ, with an internal eavesdropper.

Lemma 2 reveals that if the malicious adversary cannot decode any of the first $m-1$ users' information, the $m^{\rm th}$ user can always achieve constant positive secrecy rates at high SNRs, for both delay-guaranteed and delay-unguaranteed, and the values depend on power coefficients. This result is in agreement with previous analyses in [10] which demonstrated that the secrecy rate in wireless multiuser networks reduces to finite asymptotic value at high SNRs.

IV. Numerical Results

The accuracy of the derived analytical closed-forms and the theoretical analysis given in Section III will be numerically validated in this section. Further, the impact of the delay requirements, the size of the NOMA set and the transmit SNR on the secrecy rate and the ESR will be examined as well, by assuming that a passive internal eavesdropper or an external eavesdropper exists. It is assumed that the bandwidth $B = 100$ kHz, the fading-block length $T_{\rm f} = 0.01$ ms, the power coefficients are given as $\gamma_i = \frac{M-i+1}{\mu}$ and μ is to ensure $\sum_{i=1}^M \gamma_i = 1$ [23], unless otherwise indicated. Note that a fixed power coefficient setting is adopted in this paper. This is because the main aim of this paper is to provide analytical results and reveal some insights about the delay-guaranteed secrecy rate. In future work, we will consider applying optimal power allocation to improve the system performance through optimally allocating available resources.

Suppose that there is an internal eavesdropper among all NOMA users. To validate the correctness of the analytical closed-form for $\lim_{\rho\to\infty} E_{\rm s}^M$, given in (15), we depict in Fig. 1 $E_{\rm s}^M$ versus the transmit SNR ρ, for different values of M. To plot this figure, it is assumed that the power coefficient is set to $\gamma_M = 0.1$ and the delay QoS exponent to $\theta_M = 0.01$. Specifically, the solid lines in Fig. 1 are obtained using Monte Carlo simulations, and the dashed lines are plotted using the closed-form expression, given in (15). From this figure, one can first notice that the proposed closed-form expression is accurate, because the Monte Carlo results at high SNRs converge to the analytical closed-form. Furthermore, at high SNRs, the value of $E_{\rm s}^M$ achieved with a larger M is smaller

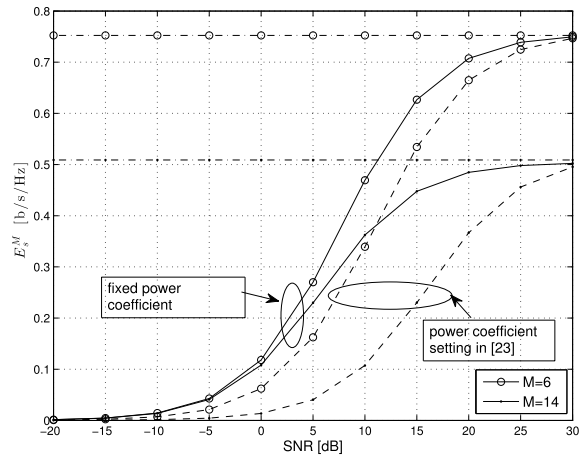


Fig. 2. E_{s}^{M} vs. the transmit SNR ρ, for two different power coefficient settings, with an internal eavesdropper.

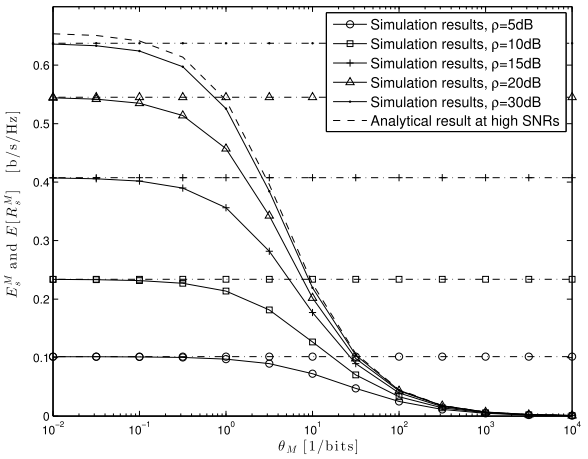


Fig. 3. E_{s}^{M} and $\mathbb{E}[R_{\mathrm{s}}^{M}]$ vs. θ_M, for different values of ρ, with an internal eavesdropper.

than those obtained with smaller values of M. This indicates that for a larger set of NOMA users, the delay-guaranteed maximum arrival rate that can be served by the strongest user decreases, in the presence of an internal eavesdropper. The reason is that in this case, the second best NOMA user, i.e., the internal eavesdropper, has a high probability of having similar channel conditions with the M^{th} user. Since our analysis in Section III-A show that the M^{th} user's ESR at high SNRs depends on the ratio of channel gains between the M^{th} user and the internal eavesdropper. Hence, we can expect that when the number of NOMA users increases, the M^{th} user will achieve smaller E_{s}^{M} values in the high SNR regime.

Note that Fig. 1 is plotted by setting a fixed power coefficient for the strongest user, i.e., $\gamma_M = 0.1$. What if the power coefficient γ_M is a value which depends on M? To explore the influence of power coefficients, Fig. 2 is depicted which include the curves of E_{s}^{M} versus the transmit SNR, with two different power coefficient settings considered. The solid lines show the curves by applying a fixed power coefficient setting, while the dashed lines are plotted for the varied power coefficient setting given in [23]. This figure first indicates that for fixed values of ρ and M, the E_{s}^{M} obtained with $\gamma_M = 0.1$ is larger than the one obtained with a varied power setting. Further, for a larger value of M, the gap between the solid line and the dashed line is larger. This is due to the fact that by adopting the varied power coefficient setting in [23], γ_M reduces with M, which results in a smaller E_{s}^{M}. Fig. 2 also indicates that for a fixed M, both of the two E_{s}^{M} curves, obtained with different power coefficient settings, converge to the same maximum limit at high SNRs. This numerically validates Theorem 3 in Section III-A, which proves that $\lim_{\rho\to\infty} E_{\mathrm{s}}^{M}$ approaches a constant value, irrespective of the power coefficients.

Recall that for the adopted link-layer channel model, i.e., the theory of EC, the delay exponent θ_M represents the exponential decay rate of the M^{th} user's delay violation probability. With a smaller θ_M, it indicates a slower decay rate, which allows a looser delay guarantee. Meanwhile, a more stringent delay provisioning can be represented by a larger θ_M [6]. Hence, we depict Fig. 3 which plots E_{s}^{M} and $\mathbb{E}[R_{s}^{M}]$ versus θ_M, for different values of ρ, so that the impact of θ_M can be investigated. The solid lines are plotted for E_{s}^{M}, while the dash-dotted lines are plotted for $\mathbb{E}[R_{s}^{M}]$. All solid lines and the dash-dotted lines are simulated using Monte Carlo method. Furthermore, the dashed line in this figure is plotted using the analytical closed-form for $\lim_{\rho\to\infty} E_{\mathrm{s}}^{M}$, given in (15). Firstly, Fig. 3 shows that for a fixed ρ, the value of E_{s}^{M} decreases with θ_M, and approaches 0 when the value of θ_M becomes very large. This confirms the monotonicity proof given in Theorem 1, which indicates that, a user with a stringent delay requirement will have to settle for a smaller delay-guaranteed secrecy rate, compared to one with a loose delay constraint. To the best of our knowledge, it is the first time that a delay-constrained secrecy rate analysis has been performed and the trade-off between them is discussed for a NOMA network. Furthermore, Fig. 3 also shows that when $\theta_M \to 0$, the E_{s}^{M} value matches with the ergodic secrecy rate $\mathbb{E}[R_{s}^{M}]$. This validates the theoretical conclusion proposed in Theorem 1, which proves that the ESR converges to the ergodic secrecy rate, when there is no delay constraint. Finally, from Fig. 3, we can also notice that when the transmit SNR ρ becomes larger, E_{s}^{M} gradually increases and approaches the analytical limit, i.e., the dashed line.

Suppose that there is an external eavesdropper distinct from the set of NOMA users. Fig. 4 plots the ESR for the m^{th} user, i.e., E_{s}^{m}, versus ρ, for different values of M. This figure aims to investigate the influence of the size of the NOMA user set on the m^{th} user's ESR. To plot this figure, we assume that the eavesdropper intends to decode the 4^{th} user's messages, i.e., $m = 4$. From Fig. 4, it is noted that when ρ increases, the value of E_{s}^{m} first increases, then becomes stable at high SNRs. Further, when M becomes larger, E_{s}^{m} reduces, which shows the same trend with Fig. 1. This indicates that when the size of the NOMA user set increases, the delay-guaranteed maximum arrival rate that can be securely served decreases, when there exists an external eavesdropper. Contrary to previous work [10] with multiple users in which only the best user can be served by the BS, in a NOMA network with power settings

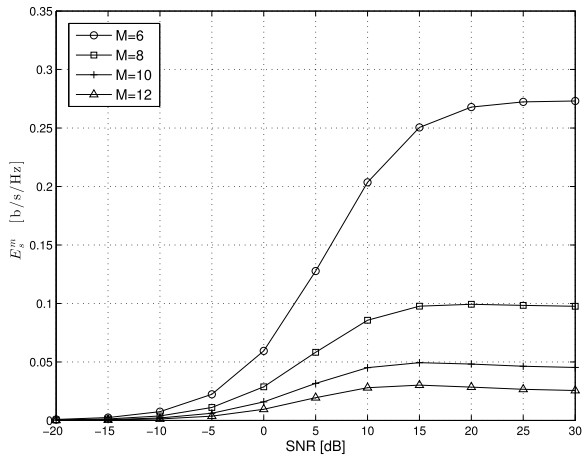


Fig. 4. $E_{\rm s}^m$ vs. the transmit SNR ρ, in the presence of an external eavesdropper.

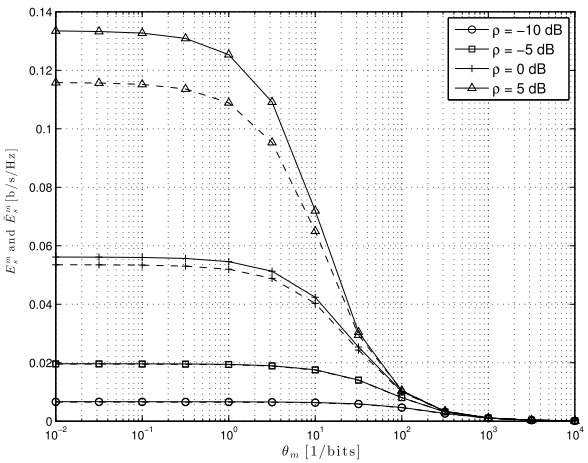


Fig. 6. $E_{\rm s}^m$ and $\breve{E}_{\rm s}^m$ vs. the delay exponent θ_m, for different values of ρ, with an external eavesdropper.

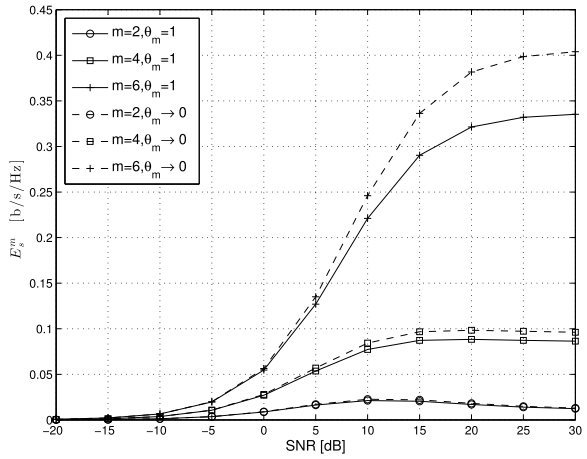


Fig. 5. $E_{\rm s}^m$ vs. the transmit SNR ρ, for different values of m and θ_m, with an external eavesdropper.

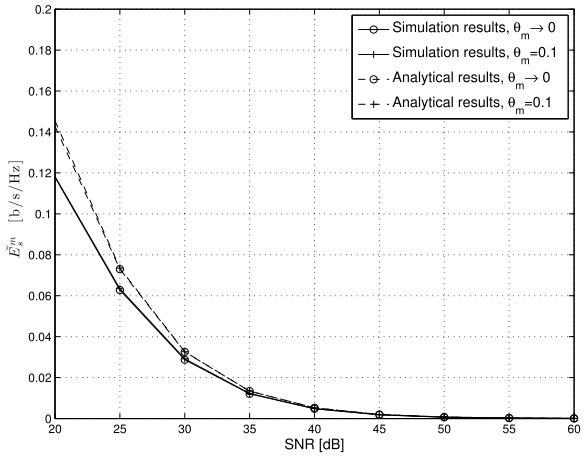


Fig. 7. $\breve{E}_{\rm s}^m$ vs. the transmit SNR ρ, for different θ_m values, with an external eavesdropper.

given in [23], increasing M will reduce the power available to each NOMA user, thus causing a decrease on the secrecy rate and the ESR.

To investigate the ESR for different users with various delay requirements, Fig. 5 plots the curves of $E_{\rm s}^m$ versus the transmit SNR, for various settings of m and θ_m. This figure first shows that for a larger value of m, the $E_{\rm s}^m$ value is larger. This indicates that when there is an external eavesdropper, the user with stronger channel conditions can achieve a higher delay-guaranteed rate. Furthermore, Fig. 5 also shows that for a specific user, the $E_{\rm s}^m$ obtained with $\theta_m \to 0$ is larger than the one achieved with $\theta_m = 1$. This is because the scenario of $\theta_m \to 0$ represents a no-delay-guaranteed situation, in which the delay violation probability approaches 1. Fig. 5 further shows that the gap of the $E_{\rm s}^m$ values between $\theta_m = 1$ and $\theta_m \to 0$ is larger for a larger value of m. This implies that a user with higher channel gains will have to make more sacrifices on its ESR value, so that the required statistical delay constraint can be satisfied.

In Section III-B.1, we proposed and analyzed a lower bound on the ESR for the $m^{\rm th}$ user, denoted as $\breve{E}_{\rm s}^m$, by overestimating the decoding capability of the external eavesdropper. Here, we include Fig. 6 which plots the curves of $E_{\rm s}^m$ (in solid lines) and the lower bound $\breve{E}_{\rm s}^m$ (in dashed lines) versus θ_m, for different values of ρ. To plot this figure, it is assumed that there are 8 NOMA users in total, i.e., $M = 8$, and the external eavesdropper intends to decode the $6^{\rm th}$ user's messages, i.e., $m = 6$. All curves shown in this figure are obtained using Monte Carlo simulation results. From Fig. 6, we first notice that both $E_{\rm s}^m$ and $\breve{E}_{\rm s}^m$ decrease with θ_m, which indicates that with an external eavesdropper existing, the achievable delay-guaranteed secrecy rate becomes smaller, when the user's delay requirement becomes more stringent. This numerically confirms the theoretical analysis given in Theorem 1. Furthermore, Fig. 6 shows that the proposed lower bound $\breve{E}_{\rm s}^m$ serves as a good lower bound for small SNR regime, and with the decrease of ρ, the gap between $E_{\rm s}^m$ and $\breve{E}_{\rm s}^m$ reduces.

To validate the accuracy of the closed-form expression for $\breve{E}_{\rm s}^m$, we include Fig. 7 which shows $\breve{E}_{\rm s}^m$ versus ρ, for various values of θ_m. The solid lines are plotted using the Monte Carlo results, while the dashed lines are shown using the

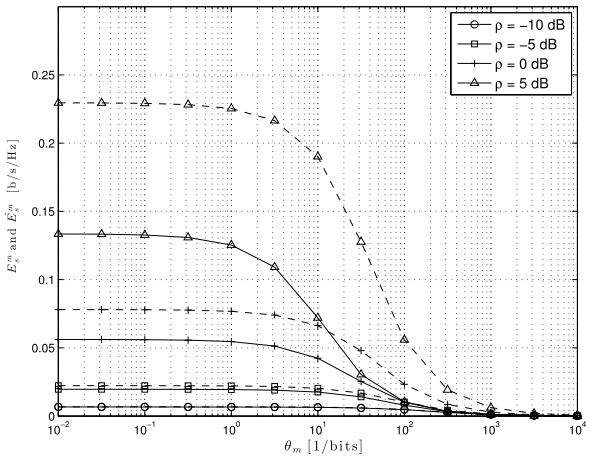


Fig. 8. $E_{\rm s}^m$ and $\hat{E_{\rm s}^m}$ vs. the delay exponent θ_m, for different values of ρ, with an external eavesdropper.

analytical results given in Theorem 5. Note that the given closed-form expression is valid only when $\gamma_m \leq \sum_{i=m+1}^{M} \gamma_i$, with $m \neq \{M-1, M\}$. Hence, to plot Fig. 7, we apply the power coefficient settings given in [23], i.e., $\gamma_i = \frac{M-i+1}{\mu}$, where μ is to ensure $\sum_{i=1}^{M} \gamma_i = 1$. By setting $M = 8$, $m = 6$, we can calculate the power coefficient values and find that $\gamma_m \leq \sum_{i=m+1}^{M} \gamma_i$ is satisfied. Fig. 7 first shows that when the transmit SNR gradually increases, the analytical closed-form results match with the Monte Carlo results, which confirms the validity of the derived closed-form at high SNRs. Furthermore, both the analytical and simulation results approach 0, at high SNRs. This confirms Lemma 1 in Section III-B.1.

In Section III-B.2, by underestimating the external eavesdropper's decoding capability, we proposed an upper bound on the ESR for the $m^{\rm th}$ user, denoted as $\hat{E_{\rm s}^m}$. To confirm the validity of the upper bound and to further investigate, Fig. 8 is plotted which includes the simulated $E_{\rm s}^m$ values (in solid lines) and the upper bound $\hat{E_{\rm s}^m}$ (in dashed lines) versus θ_m, for different values of ρ. Similar to Fig. 6, Fig. 8 also shows that both the $E_{\rm s}^m$ and the upper bound $\hat{E_{\rm s}^m}$ decrease with θ_m. This is due to the fact that with a larger θ_m indicating a more stringent statistical delay guarantee, the maximum achievable arrival rate which can be securely supported becomes smaller [6]. Furthermore, Fig. 8 also shows that the proposed $\hat{E_{\rm s}^m}$ can serve as a good upper bound, for relatively small transmit SNR values.

V. Conclusion

The delay-guaranteed secrecy rate, namely, ESR, has been introduced and investigated for a downlink NOMA network; ESR represents the maximum constant arrival rate which can be securely served by a legitimate user, while guaranteeing the required statistical delay constraints. Two eavesdropping scenarios have been considered: a purely antagonistic network with an unknown internal eavesdropper and a trustworthy NOMA network with an external eavesdropper. Assuming an internal eavesdropper exists, a closed-form expression for the ESR at high SNRs has been derived for the strongest user, which is the only user guaranteed to have a positive ESR in this case. Assuming that an external eavesdropper exists and has interest in jeopardizing the security of the network, a lower bound and an upper bound on the ESR have been proposed, respectively, and have been shown to be tight in the low SNR regime. Simulation results have shown that for both eavesdropping scenarios, a user with a stringent delay requirement serves a smaller amount of ESR, comparing to those with relatively loose delay constraints. Further, it has been shown that a legitimate NOMA user with higher channel gains will make greater sacrifices on its ESR value, so that a required statistical delay guarantee can be satisfied.

Appendix A
Proof for Theorem 1

Recall that the ESR for the $m^{\rm th}$ user, i.e., $E_{\rm s}^m$, is calculated by inserting the achievable secrecy rate R_s^m into (6), which is then given by

$$E_{\rm s}^m = -\frac{1}{\theta_m T_{\rm f} B} \ln\left(\mathbb{E}\left[e^{-\theta_m T_{\rm f} B R_s^m}\right]\right). \tag{34}$$

Note that $e^{-\theta_m T_{\rm f} B R_s^m}$ is a log-convex function in θ_m because $\ln\left(e^{-\theta_m T_{\rm f} B R_s^m}\right) = -\theta_m T_{\rm f} B R_s^m$ is a convex function in θ_m [29]. Since the log-convexity still holds under summations, therefore we could conclude that $\mathbb{E}\left[e^{-\theta_m T_{\rm f} B R_s^m}\right]$ is also a log-convex function in θ_m. Hence, it is clear that $\ln\left(\mathbb{E}\left[e^{-\theta_m T_{\rm f} B R_s^m}\right]\right)$ is convex, which means $-\ln\left(\mathbb{E}\left[e^{-\theta_m T_{\rm f} B R_s^m}\right]\right)$ is a concave function in θ_m.

We rewrite $E_{\rm s}^m$ as $\frac{f(\theta_m)}{g(\theta_m)}$, where $f(\theta_m) = -\ln\left(\mathbb{E}\left[e^{-\theta_m T_{\rm f} B R_s^m}\right]\right)$ and $g(\theta_m) = \theta_m T_{\rm f} B$. In order to prove that $E_{\rm s}^m$ is a monotonically decreasing function in θ_m, we take the first derivative of $E_{\rm s}^m$, which gives

$$\frac{\partial E_{\rm s}^m}{\partial \theta_m} = \left(\frac{f(\theta_m)}{g(\theta_m)}\right)' = \frac{f'(\theta_m)g(\theta_m) - g'(\theta_m)f(\theta_m)}{\left(g(\theta_m)\right)^2}. \tag{35}$$

Apparently, the denominator is a non-negative value. Let us consider the numerator only. We take the first derivative of the denominator and it gives

$$\begin{aligned}&\left(f'(\theta_m)g(\theta_m) - g'(\theta_m)f(\theta_m)\right)' \\ &\quad = f''(\theta_m)g(\theta_m) - g''(\theta_m)f(\theta_m),\end{aligned} \tag{36}$$

which can be simplified as $f''(\theta_m)g(\theta_m)$ because $g''(\theta_m) = 0$. Since we have proved that $f(\theta_m)$ is a concave function, i.e., $f''(\theta_m) \leq 0$, and also $g(\theta_m) \geq 0$, therefore it can be concluded that the numerator in (35) is a non-increasing function. Furthermore, it is easy to see that the numerator in (35) equals to 0 when $\theta_m = 0$, i.e., $f'(\theta_m)g(\theta_m) - g'(\theta_m)f(\theta_m)|_{\theta_m=0} = 0$. Finally, we can conclude that $\dfrac{\partial E_{\rm s}^m}{\partial \theta_m} \leq 0$, which implies that $E_{\rm s}^m$ monotonically decreases with θ_m.[12]

[12]The conclusion of monotonicity is obtained by excluding the possibility of $E_{\rm s}^m$ being a constant value, with respect to θ_m.

When $\theta_m \to 0$, we can obtain that

$$\lim_{\theta_m \to 0} E_{\mathrm{s}}^m = \lim_{\theta_m \to 0} -\frac{\left(\mathbb{E}\left[e^{-\theta_m T_{\mathrm{f}} B R_s^m}\right]\right)'}{T_{\mathrm{f}} B \mathbb{E}\left[e^{-\theta_m T_{\mathrm{f}} B R_s^m}\right]} \tag{37}$$

$$= \lim_{\theta_m \to 0} -\frac{\mathbb{E}\left[e^{-\theta_m T_{\mathrm{f}} B R_s^m}\left(-T_{\mathrm{f}} B R_s^m\right)\right]}{T_{\mathrm{f}} B \mathbb{E}\left[e^{-\theta_m T_{\mathrm{f}} B R_s^m}\right]} \tag{38}$$

$$= \mathbb{E}\left[R_s^m\right]. \tag{39}$$

Hence, this proves that when $\theta_m \to 0$, E_{s}^m converges to the ergodic secrecy rate $\mathbb{E}\left[R_s^m\right]$.

When $\theta_m \to \infty$, from (5), one can note that the probability of the delay exceeding a given delay bound approaches zero. It means that the user cannot tolerate any delay outage, which refers to the delay-limited scenario. According to [30], it shows that Rayleigh channel cannot support very stringent delay QoS requirement (when θ is extremely large), even using the optimal power policy. Our simulation results also confirm that the ESR becomes zero in this case.

APPENDIX B
PROOF FOR THEOREM 2

According to the theory of order statistics and by inserting (10) into (9), E_{s}^M can be written as

$$E_{\mathrm{s}}^M = \frac{1}{\beta_M}\log_2\left(M(M-1)\int_0^\infty\int_x^\infty\left(\frac{1+q_M y}{1+q_M x}\right)^{\beta_M} \times f(x)\left(F(x)\right)^{M-2} f(y)\,\mathrm{d}y\,\mathrm{d}x\right)$$

$$= \frac{1}{\beta_M}\log_2\left(M(M-1)\int_0^\infty\left(\frac{1}{1+q_M x}\right)^{\beta_M} e^{-x} \times\left(1-e^{-x}\right)^{M-2}\int_x^\infty (1+q_M y)^{\beta_M} e^{-y}\,\mathrm{d}y\,\mathrm{d}x\right). \tag{40}$$

Consider $E_{sc}^1 = \int_x^\infty (1+q_M y)^{\beta_M} e^{-y}\,\mathrm{d}y$ first. By setting $z_1 = \frac{1}{q_M} + y$, E_{sc}^1 can be transformed into $E_{sc}^1 = q_M^{\beta_M} e^{\frac{1}{q_M}}\int_{\frac{1}{q_M}+x}^\infty z_1^{\beta_M} e^{-z_1}\,\mathrm{d}z_1$. Then, from (3.381.6) in [31], we note that

$$\int_u^\infty \frac{e^{-x}}{x^v}\,\mathrm{d}x = u^{-\frac{v}{2}} e^{-\frac{u}{2}} W_{-\frac{v}{2},\frac{1-v}{2}}(u) \qquad [u>0], \tag{41}$$

where $W_{k,\mu}(z)$ is the Whittaker W function [26]. By applying (41), E_{sc}^1 can be given as

$$E_{sc}^1 = q_M^{\beta_M} e^{\frac{1}{q_M}}\left(\frac{1}{q_M}+x\right)^{\frac{\beta_M}{2}} e^{-\frac{1}{2q_M}-\frac{x}{2}} W_{\frac{\beta_M}{2},\frac{1+\beta_M}{2}}\left(\frac{1}{q_M}+x\right). \tag{42}$$

Finally, by inserting E_{sc}^1 into (40), E_{s}^M can be given as

$$E_{\mathrm{s}}^M = \frac{1}{\beta_M}\log_2\left(M(M-1)q_M^{\frac{\beta_M}{2}} e^{\frac{1}{2q_M}}\int_0^\infty (1+q_M x)^{-\frac{\beta_M}{2}} \times e^{-\frac{3}{2}x}\left(1-e^{-x}\right)^{M-2} W_{\frac{\beta_M}{2},\frac{1+\beta_M}{2}}\left(\frac{1}{q_M}+x\right)\mathrm{d}x\right)$$

$$= A_M + \frac{1}{\beta_M}\log_2\left(\int_0^\infty (1+q_M x)^{-\beta_M} e^{-x} \times\left(1-e^{-x}\right)^{M-2}\Gamma\left(1+\beta_M, \frac{1}{q_M}+x\right)dx\right), \tag{43}$$

where $A_M = \frac{1}{\beta_M}\log_2\left(M(M-1)q_M^{\beta_M} e^{\frac{1}{q_M}}\right)$, and $\Gamma(\cdot,\cdot)$ is the incomplete Γ function. Making use of the Binomial theorem we have that

$$(1-e^{-x})^{M-2} = \sum_{\nu=0}^{M-2}\binom{M-2}{\nu}(-1)^\nu e^{-\nu x}, \tag{44}$$

so that the following integral appears

$$\int_0^\infty (1+q_M x)^{-\beta_M} e^{-(\nu+1)x}\Gamma\left(1+\beta_M, \frac{1}{q_M}+x\right)\mathrm{d}x$$

$$= \int_{1/q_M}^\infty (q_M z)^{-\beta_M} e^{-(\nu+1)(z-\frac{1}{q_M})}\Gamma(1+\beta_M, z)\,\mathrm{d}z \tag{45a}$$

$$= q_M^{-\beta_M} e^{\frac{\nu+1}{q_M}}\int_{1/q_M}^\infty z^{-\beta_M} e^{-(\nu+1)z}\Gamma(1+\beta_M, z)\,\mathrm{d}z, \tag{45b}$$

by change of variable $z = x + \frac{1}{q_M}$. We set $I_\nu = \int_{1/q_M}^\infty z^{-\beta_M} e^{-(\nu+1)z}\Gamma(1+\beta_M, z)\,\mathrm{d}z$, so that

$$E_{sc}^M = B_M + \frac{1}{\beta_M}\log_2\left(\sum_{\nu=0}^{M-2}\binom{M-2}{\nu}(-1)^\nu e^{\frac{\nu}{q_M}} I_\nu\right), \tag{46}$$

where $B_M = \frac{\log_2(M(M-1))+2q_M^{-1}}{\beta_M}$. To evaluate I_ν we will use the following property

$$\int x^b\Gamma(s,x)\,\mathrm{d}x = \frac{1}{b+1}\left(x^{b+1}\Gamma(s,x) - \Gamma(s+b+1,x)\right), \tag{47}$$

and note that the limit of the right-hand side (RHS) for $x \to \infty$ is 0. To have only powers of z in I_ν, we resort in using the Taylor series expansion for the exponential function $e^{-(\nu+1)z} = \sum_{k=0}^\infty \frac{(-1)^k(\nu+1)^k z^k}{k!}$. Hence, I_ν becomes

$$I_\nu = \sum_{k=0}^\infty \frac{(-1)^k(\nu+1)^k}{k!}\int_{\frac{1}{q_M}}^\infty z^{k-\beta_M}\Gamma\left(1+\beta_M, z\right)\mathrm{d}x$$

$$= -\sum_{k=0}^\infty \frac{(-1)^k}{k!}\frac{(\nu+1)^k}{k-\beta_M+1}\left[\left(\frac{1}{q_M}\right)^{k-\beta_M+1} \times\Gamma\left(1+\beta_M, \frac{1}{q_M}\right) - \Gamma\left(1+\beta_M+k-\beta_M+1, \frac{1}{q_M}\right)\right]$$

$$= \sum_{k=0}^\infty \frac{(-1)^k}{k!}\frac{(\nu+1)^k}{k-\beta_M+1}\left[\Gamma\left(k+2, \frac{1}{q_M}\right) - \left(\frac{1}{q_M}\right)^{k-\beta_M+1}\Gamma\left(1+\beta_M, \frac{1}{q_M}\right)\right], \tag{48}$$

and finally

$$E_{sc}^M = B_M + \frac{1}{\beta_M}\log_2\left(\sum_{\nu=0}^{M-2}\binom{M-2}{\nu}(-1)^\nu e^{\frac{\nu}{q_M}}\right.$$

$$\times \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \frac{(\nu+1)^k}{k-\beta_M+1} \left[\Gamma\left(k+2, \frac{1}{q_M}\right) - \left(\frac{1}{q_M}\right)^{k-\beta_M+1} \Gamma\left(1+\beta_M, \frac{1}{q_M}\right) \right] \right). \quad (49)$$

APPENDIX C
PROOF FOR THEOREM 3

By applying the theory of order statistics and inserting (10) into (14), the M^{th} user's ESR at high SNRs can be given by

$$\lim_{\rho\to\infty} E_{\text{s}}^M = \frac{1}{\beta_M} \log_2 \left(M(M-1) \int_0^\infty \int_x^\infty \left(\frac{y}{x}\right)^{\beta_M} \times f(x) \left(F(x)\right)^{M-2} f(y)\, \mathrm{d}y\, \mathrm{d}x \right) \quad (50a)$$

$$= \frac{1}{\beta_M} \log_2 \left(M(M-1) \int_0^\infty \left(\frac{1}{x}\right)^{\beta_M} e^{-x} \left(1-e^{-x}\right)^{M-2} \times \int_x^\infty y^{\beta_M} e^{-y}\, \mathrm{d}y\, \mathrm{d}x \right). \quad (50b)$$

Then, by applying (41) to (50b), one can get that

$$\lim_{\rho\to\infty} E_{\text{s}}^M = \frac{1}{\beta_M} \log_2 \left(M(M-1) \int_0^\infty \left(\frac{1}{x}\right)^{\beta_M} e^{-x} \times \left(1-e^{-x}\right)^{M-2} x^{\frac{\beta_M}{2}} e^{-\frac{x}{2}} W_{\frac{\beta_M}{2}, \frac{1+\beta_M}{2}}(x)\, \mathrm{d}x \right). \quad (51)$$

Further, by using the binomial expansion and expanding $(1-e^{-x})^{M-2}$ as $\sum_{s=0}^{M-2} \binom{M-2}{s} (-1)^s e^{-xs}$, (51) can be transformed into

$$\lim_{\rho\to\infty} E_{\text{s}}^M = \frac{1}{\beta_M} \log_2 \left(M(M-1) \sum_{s=0}^{M-2} \binom{M-2}{s} (-1)^s \times \int_0^\infty x^{-\frac{\beta_M}{2}} e^{-\left(\frac{3}{2}+s\right)x} W_{\frac{\beta_M}{2}, \frac{1+\beta_M}{2}}(x)\, \mathrm{d}x \right). \quad (52)$$

From (13.23.4) in [26], we note that

$$\int_0^\infty e^{-zt} t^{w-1} W_{k,\mu}(t)\, \mathrm{d}t = \Gamma\left(\frac{1}{2}+\mu+w\right) \Gamma\left(\frac{1}{2}-\mu+w\right) \times {}_2\mathbf{F}_1 \left[\begin{matrix} \frac{1}{2}-\mu+w,\ \frac{1}{2}+\mu+w \\ w-k+1 \end{matrix} ; \frac{1}{2}-z \right] \times \left[\mathrm{Re}\left(w+\frac{1}{2}\right) > |\mathrm{Re}(\mu)|, \mathrm{Re}(z) > -\frac{1}{2} \right], \quad (53)$$

where ${}_2\mathbf{F}_1 \left[\begin{matrix} a,\ b \\ c \end{matrix} ; z \right]$ is the generalized hypergeometric function, and $\Gamma(\cdot)$ is the gamma function. By applying (53) to (52), the closed-form expression for $\lim_{\rho\to\infty} E_{\text{s}}^M$ can be finally expressed as

$$\lim_{\rho\to\infty} E_{\text{s}}^M = \frac{1}{\beta_M} \log_2 \left(M(M-1)\Gamma(1-\beta_M) \times \sum_{s=0}^{M-2} \binom{M-2}{s} (-1)^s {}_2\mathbf{F}_1 \left[\begin{matrix} 1-\beta_M,\ 2 \\ 2-\beta_M \end{matrix} ; -1-s \right] \right).$$

Then, for comparison purposes, here we derive the closed-form expression for the ergodic secrecy rate for the M^{th} user at high SNRs, i.e., $\lim_{\rho\to\infty} \mathbb{E}[R_s^M]$. Firstly, we note that $\lim_{\rho\to\infty} \mathbb{E}[R_s^M] = \mathbb{E}\left[\log_2\left(\frac{|h_M|^2}{|h_{M-1}|^2}\right)\right]$, which can be expanded as follows, after inserting the joint PDF (10).

$$\lim_{\rho\to\infty} \mathbb{E}[R_s^M] = M(M-1) \int_0^\infty \int_x^\infty \log_2\left(\frac{y}{x}\right) e^{-x} \times (1-e^{-x})^{M-2} e^{-y}\, \mathrm{d}y\, \mathrm{d}x. \quad (54)$$

By defining $z_0 = \frac{y}{x}$ and $1 \le z_0 \le \infty$, (54) can be rewritten as

$$\lim_{\rho\to\infty} \mathbb{E}[R_s^M] = M(M-1) \int_0^\infty x e^{-x} (1-e^{-x})^{M-2} \times \int_1^\infty \log_2(z_0) e^{-xz_0}\, \mathrm{d}z_0\, \mathrm{d}x \quad (55)$$

$$= \frac{M(M-1)}{\ln 2} \int_0^\infty x e^{-x} (1-e^{-x})^{M-2} \times \int_1^\infty \ln(z_0) e^{-xz_0}\, \mathrm{d}z_0\, \mathrm{d}x. \quad (56)$$

From (4.331.2) in [31], we have that

$$\int_1^\infty e^{-\mu x} \ln x\, \mathrm{d}x = -\frac{1}{\mu} E_i(-\mu), \quad \mathrm{Re}\ \mu > 0. \quad (57)$$

By applying (57), we get that

$$\lim_{\rho\to\infty} \mathbb{E}[R_s^M] = \frac{M(M-1)}{\ln 2} \sum_{s=0}^{M-2} \binom{M-2}{s} (-1)^s \times \int_0^\infty e^{-(s+1)x} E_1(x)\, \mathrm{d}x, \quad (58)$$

obtained after using $(1-e^{-x})^{M-2} = \sum_{s=0}^{M-2} \binom{M-2}{s} (-1)^s e^{-xs}$ and $E_i(-x) = -E_1(x)$, for $x > 0$. From (4.2.3) in [32], we have that

$$\int_0^\infty e^{-ax} E_1(bx)\, \mathrm{d}x = \frac{1}{a} \ln\left(1+\frac{a}{b}\right). \quad (59)$$

Hence, by applying (59), we finally obtain the close-form expression for the ergodic secrecy rate at high SNRs, given as

$$\lim_{\rho\to\infty} \mathbb{E}[R_s^M] = M(M-1) \times \sum_{s=0}^{M-2} \binom{M-2}{s} (-1)^s \frac{1}{s+1} \log_2(s+2). \quad (60)$$

APPENDIX D
PROOF FOR THEOREM 4

By inserting the joint PDF $f(z_1,z_2)$ into (20), E_{cs}^m is given by

$$E_{\text{cs}}^m = \frac{1}{\beta_m}\log_2\left(\int_0^\infty\int_0^\infty\left(\frac{Q_m z_1+1}{Q_{m+1}z_1+1}\times\frac{(Q_{M_E+1}-q_m)\,z_2+1}{Q_{M_E+1}z_2+1}\right)^{\beta_m} f(z_1,z_2)\,\mathrm{d}z_1\,\mathrm{d}z_2\right). \tag{61}$$

Here, $f(z_1,z_2) = f_{(m)}(z_1)f(z_2)$, where $f_{(m)}(z_1) = \psi_m f(z_1)F(z_1)^{m-1}\left(1-F(z_1)\right)^{M-m}$, $f(z_1) = e^{-z_1}$, $F(z_1) = 1-e^{-z_1}$, and $f(z_2) = e^{-z_2}$. Then, E_{cs}^m can be extended as

$$E_{\text{cs}}^m = \frac{1}{\beta_m}\log_2\left(\psi_m\int_0^\infty\left(\frac{(Q_{M_E+1}-q_m)\,z_2+1}{Q_{M_E+1}z_2+1}\right)^{\beta_m} e^{-z_2}\times\int_0^\infty\left(\frac{Q_m z_1+1}{Q_{m+1}z_1+1}\right)^{\beta_m} e^{-(M-m+1)z_1}\times\left(1-e^{-z_1}\right)^{m-1}\mathrm{d}z_1\,\mathrm{d}z_2\right). \tag{62}$$

By replacing $\left(1-e^{-z_1}\right)^{m-1}$ with binominal expansion $\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s e^{-z_1 s}$ and defining $a = M-m+s+1$, we can get that

$$E_{\text{cs}}^m = \frac{1}{\beta_m}\log_2\left(\psi_m\int_0^\infty\left(\frac{(Q_{M_E+1}-q_m)\,z_2+1}{Q_{M_E+1}z_2+1}\right)^{\beta_m} e^{-z_2}\times\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s\int_0^\infty\left(\frac{Q_m z_1+1}{Q_{m+1}z_1+1}\right)^{\beta_m}\times e^{-az_1}\,\mathrm{d}z_1\,\mathrm{d}z_2\right). \tag{63}$$

To simplify the above equation, we define A_{D_1} and A_{D_2} as follows and E_{cs}^m can be written as

$$E_{\text{cs}}^m = \frac{1}{\beta_m}\log_2\left(\psi_m A_{D_1}A_{D_2}\right), \tag{64a}$$

$$A_{D_1} = \sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s\int_0^\infty\left(\frac{Q_m z_1+1}{Q_{m+1}z_1+1}\right)^{\beta_m} e^{-az_1}\,\mathrm{d}z_1, \tag{64b}$$

$$A_{D_2} = \int_0^\infty\left(\frac{(Q_{M_E+1}-q_m)\,z_2+1}{Q_{M_E+1}z_2+1}\right)^{\beta_m} e^{-z_2}\,\mathrm{d}z_2. \tag{64c}$$

Let us focus on A_{D_1} first. It can be further expressed as

$$A_{D_1} = \left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m}\int_0^\infty\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s\times\left(1+\frac{\frac{q_m}{Q_{m+1}}}{Q_m z_1+1}\right)^{-\beta_m} e^{-az_1}\,\mathrm{d}z_1. \tag{65a}$$

By assuming that $q_m \le Q_{m+1}$, where $m \neq \{M-1, M\}$, $\left(1+\frac{\frac{q_m}{Q_{m+1}}}{Q_m z_1+1}\right)^{-\beta_m}$ can be approximated using the first two terms of generalized binomial expansion. Then, (65a) can be approximated as:

$$A_{D_1} \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m}\left(\int_0^\infty\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s e^{-az_1}\,\mathrm{d}z_1 - \frac{\beta_m q_m}{Q_{m+1}}\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s\int_0^\infty\frac{e^{-az_1}}{Q_m z_1+1}\,\mathrm{d}z_1\right). \tag{66}$$

From (3.352.4) in [31], we have that

$$\int_0^\infty\frac{e^{-\mu x}}{x+\beta}\,\mathrm{d}x = -e^{\beta\mu}E_i(-\mu\beta), |\arg\beta|<\pi, \quad \text{Re }\mu>0. \tag{67}$$

Then, by applying (67), A_{D_1} becomes

$$A_{D_1} \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m}\left(\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s\frac{1}{a} + \frac{\beta_m q_m}{Q_{m+1}Q_m}\times\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s e^{\frac{a}{Q_m}}E_i\left(-\frac{a}{Q_m}\right)\right). \tag{68}$$

Then, we can start to consider A_{D_2}, which can be expressed as

$$A_{D_2} = \left(\frac{Q_{M_E+1}-q_m}{Q_{M_E+1}}\right)^{\beta_m}\int_0^\infty\left(1+\frac{\frac{q_m}{Q_{M_E+1}-q_m}}{Q_{M_E+1}z_2+1}\right)^{\beta_m}\times e^{-z_2}\,\mathrm{d}z_2 \tag{69}$$

$$\approx \left(\frac{Q_{M_E+1}-q_m}{Q_{M_E+1}}\right)^{\beta_m}\left(\int_0^\infty e^{-z_2}\,\mathrm{d}z_2 + \frac{\beta_m q_m}{Q_{M_E+1}-q_m}\times\int_0^\infty\frac{e^{-z_2}}{Q_{M_E+1}z_2+1}\,\mathrm{d}z_2\right) \tag{70}$$

$$\approx \left(\frac{Q_{M_E+1}-q_m}{Q_{M_E+1}}\right)^{\beta_m}\left(1-\frac{\beta_m q_m}{(Q_{M_E+1}-q_m)\,Q_{M_E+1}}\times e^{\frac{1}{Q_{M_E+1}}}E_i\left(-\frac{1}{Q_{M_E+1}}\right)\right). \tag{71}$$

Finally, by inserting A_{D_1} and A_{D_2} into (64a), the E_{cs}^m for the m^{th} user is given by (22).

At high SNRs, for the m^{th} user with $m \ge M_E+1$, $\lim_{\rho\to\infty} E_{\text{cs}}^m$ is given by

$$\lim_{\rho\to\infty}E_{\text{cs}}^m = \frac{1}{\beta_m}\log_2\left(\mathbb{E}\left[\left(\frac{Q_m}{Q_{m+1}}\frac{Q_{M_E+1}-q_m}{Q_{M_E+1}}\right)^{\beta_m}\right]\right) = \log_2\left(\frac{Q_m}{Q_{m+1}}\frac{Q_{M_E+1}-q_m}{Q_{M_E+1}}\right). \tag{72}$$

APPENDIX E
PROOF FOR THEOREM 5

Recall that $\breve{E}_{\text{s}}^m$ can be expressed as

$$\breve{E}_{\text{s}}^m = \frac{1}{\beta_m}\log_2\left(B_{D_1}+B_{D_2}\right), \tag{73}$$

where

$$B_{D_1} = \psi_m \iint\limits_{D_1} \left(\frac{Q_m z_1 + 1}{Q_{m+1} z_1 + 1} \frac{Q_{m+1} z_2 + 1}{Q_m z_2 + 1}\right)^{\beta_m} \times \frac{e^{-(M-m+1)z_1 - z_2}}{\left(1 - e^{-z_1}\right)^{1-m}} \, \mathrm{d}z_1 \, \mathrm{d}z_2, \tag{74a}$$

$$B_{D_2} = \psi_m \iint\limits_{D_2} e^{-(M-m+1)z_1} \left(1 - e^{-z_1}\right)^{m-1} e^{-z_2} \, \mathrm{d}z_1 \, \mathrm{d}z_2. \tag{74b}$$

First, let us consider B_{D_2}. By replacing $(1 - e^{-z_1})^{m-1}$ with $\sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s e^{-z_1 s}$, we get that

$$B_{D_2} = \psi_m \int_0^\infty e^{-z_2} \int_0^{z_2} \sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s e^{-a z_1} \, \mathrm{d}z_1 \, \mathrm{d}z_2 \tag{75a}$$

$$= \psi_m \sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s \left(-\frac{1}{a}\right) \int_0^\infty e^{-z_2} \left(e^{-a z_2} - 1\right) \, \mathrm{d}z_2 \tag{75b}$$

$$= \psi_m \sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s \frac{1}{a+1}. \tag{75c}$$

Then, we can consider B_{D_1}. Let us define $BB_{D_1}(z_2)$ and rewrite B_{D1} as follows:

$$B_{D_1} = \psi_m \int_0^\infty \left(\frac{Q_{m+1} z_2 + 1}{Q_m z_2 + 1}\right)^{\beta_m} e^{-z_2} BB_{D_1}(z_2) \, \mathrm{d}z_2, \tag{76a}$$

$$BB_{D_1}(z_2) = \int_{z_2}^\infty \left(\frac{Q_m z_1 + 1}{Q_{m+1} z_1 + 1}\right)^{\beta_m} e^{-(M-m+1)z_1} \times \left(1 - e^{-z_1}\right)^{m-1} \, \mathrm{d}z_1, \tag{76b}$$

where $BB_{D_1}(z_2)$ can be written as

$$BB_{D_1}(z_2) = \left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m} \sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s \times \int_{z_2}^\infty \left(1 + \frac{\frac{q_m}{Q_{m+1}}}{Q_m z_1 + 1}\right)^{-\beta_m} e^{-a z_1} \, \mathrm{d}z_1. \tag{77}$$

By assuming that $q_m \leq Q_{m+1}$, where $m \neq \{M-1, M\}$, $\left(1 + \frac{\frac{q_m}{Q_{m+1}}}{Q_m z_1 + 1}\right)^{-\beta_m}$ can be approximated using the first two terms of generalized binomial expansion. Then, (77) can be approximated as

$$BB_{D_1}(z_2) \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m} \sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s \times \left(\int_{z_2}^\infty e^{-a z_1} \, \mathrm{d}z_1 - \frac{\beta_m q_m}{Q_{m+1}} \int_{z_2}^\infty \frac{e^{-a z_1}}{Q_m z_1 + 1} \, \mathrm{d}z_1\right). \tag{78}$$

From (3.352.2) in [31], we have that

$$\int_u^\infty \frac{e^{-\mu x}}{x + \beta} \, \mathrm{d}x = -e^{\beta\mu} E_i(-\mu u - \mu\beta), \quad u \geq 0, |\arg(u + \beta)| < \pi, \mathrm{Re}\ \mu > 0. \tag{79}$$

Then, $BB_{D_1}(z_2)$ can be finally approximated as

$$BB_{D_1}(z_2) \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m} \sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s \times \left(\frac{e^{-a z_2}}{a} + \frac{\beta_m q_m}{Q_m Q_{m+1}} e^{\frac{a}{Q_m}} E_i\left(-a z_2 - \frac{a}{Q_m}\right)\right). \tag{80}$$

By inserting $BB_{D_1}(z_2)$ back into B_{D_1}, we get (81), shown at the top of the next page. To simplify, (81) can be rewritten as

$$B_{D_1} = \psi_m \left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m} \left(A_1 + \frac{\beta_m q_m}{Q_m Q_{m+1}} A_2\right). \tag{82}$$

Let us consider A_1 first.

$$A_1 = \left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m} \sum_{s=0}^{m-1} \binom{m-1}{s} \frac{(-1)^s}{a} \times \int_0^\infty \left(1 + \frac{\frac{q_m}{Q_{m+1}}}{Q_m z_2 + 1}\right)^{\beta_m} e^{-(a+1)z_2} \, \mathrm{d}z_2, \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m} \sum_{s=0}^{m-1} \binom{m-1}{s} \frac{(-1)^s}{a} \times \left(\int_0^\infty e^{-(a+1)z_2} \, \mathrm{d}z_2 + \frac{\beta_m q_m}{Q_{m+1}} \int_0^\infty \frac{e^{-(a+1)z_2}}{Q_m z_2 + 1} \, \mathrm{d}z_2\right), \tag{83}$$

which is approximated by applying the first two terms of the generalized binomial expansion. By applying (3.352.4) in [31], given in (67), we can get that

$$A_1 \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m} \sum_{s=0}^{m-1} \binom{m-1}{s} \frac{(-1)^s}{a} \times \left(\frac{1}{a+1} - \frac{\beta_m q_m}{Q_m Q_{m+1}} e^{\frac{a+1}{Q_m}} E_i\left(-\frac{a+1}{Q_m}\right)\right). \tag{84}$$

Now we can start to work on A_2. Recall that

$$A_2 = \left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m} \sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s e^{\frac{a}{Q_m}} \times \int_0^\infty \left(1 + \frac{\frac{q_m}{Q_{m+1}}}{Q_m z_2 + 1}\right)^{\beta_m} e^{-z_2} E_i\left(-a z_2 - \frac{a}{Q_m}\right) \, \mathrm{d}z_2. \tag{85}$$

in which $\left(1 + \frac{\frac{q_m}{Q_{m+1}}}{Q_m z_2 + 1}\right)^{\beta_m}$ can be approximated using the first two terms of the generalized binomial expansion. Then, A_2 can be transformed into

$$A_2 \approx \left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m} \sum_{s=0}^{m-1} \binom{m-1}{s} (-1)^s e^{\frac{a}{Q_m}} \times \left(\int_0^\infty e^{-z_2} E_i\left(-a z_2 - \frac{a}{Q_m}\right) \, \mathrm{d}z_2 + \frac{\beta_m q_m}{Q_{m+1}} \int_0^\infty \frac{1}{Q_m z_2 + 1} e^{-z_2} E_i\left(-a z_2 - \frac{a}{Q_m}\right) \, \mathrm{d}z_2\right). \tag{86}$$

$$B_{D_1}=\psi_m\left(\frac{Q_{m+1}}{Q_m}\right)^{-\beta_m}\left(\underbrace{\sum_{s=0}^{m-1}\binom{m-1}{s}\frac{(-1)^s}{a}\int_0^{\infty}\left(\frac{Q_{m+1}z_2+1}{Q_mz_2+1}\right)^{\beta_m}e^{-(a+1)z_2}\,\mathrm{d}z_2}_{A_1}+\frac{\beta_m q_m}{Q_mQ_{m+1}}\right.$$
$$\left.\times\underbrace{\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s e^{\frac{a}{Q_m}}\int_0^{\infty}\left(\frac{Q_{m+1}z_2+1}{Q_mz_2+1}\right)^{\beta_m}e^{-z_2}E_i\left(-az_2-\frac{a}{Q_m}\right)\,\mathrm{d}z_2}_{A_2}\right), \tag{81}$$

By setting $y=az_2+\frac{a}{Q_m}$ and $\frac{a}{Q_m}\le y\le\infty$, A_2 can be rewritten as

$$A_2\approx\left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m}\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s e^{\frac{a}{Q_m}}\times\left(-\frac{1}{a}e^{\frac{1}{Q_m}}\int_{\frac{a}{Q_m}}^{\infty}e^{-\frac{1}{a}y}E_1(y)\,\mathrm{d}y-\frac{\beta_m q_m}{Q_mQ_{m+1}}e^{\frac{1}{Q_m}}\int_{\frac{a}{Q_m}}^{\infty}e^{-\frac{1}{a}y}E_1(y)\frac{1}{y}\,\mathrm{d}y\right). \tag{87}$$

From (4.2.1) in [32], we have that

$$\int e^{-ux}E_1(vx)\,\mathrm{d}x=\frac{1}{u}\big(E_1((u+v)x)-e^{-ux}E_1(vx)\big). \tag{88}$$

By applying (88), we get that

$$\int_{\frac{a}{Q_m}}^{\infty}e^{-\frac{1}{a}y}E_1(y)\,\mathrm{d}y=-a\left(E_1\left(\frac{a+1}{Q_m}\right)-e^{-\frac{1}{Q_m}}E_1\left(\frac{a}{Q_m}\right)\right). \tag{89}$$

Further, from (4.2.29) in [32], we have that

$$\int_c^{\infty}e^{-ux}E_1(vx)\frac{1}{x}\,\mathrm{d}x=(r+\ln(uc)+E_1(uc))\,E_1(vc)+\frac{1}{2}\big(\zeta(2)+(r+\ln(vc))^2\big)+e^{-vc}\sum_{\delta=0}^{\infty}\frac{e_\delta(vc)}{(\delta+1)^2}\left(-\frac{u}{v}\right)^{\delta+1}+\sum_{\delta=1}^{\infty}\frac{(-vc)^\delta}{\delta!\delta^2}. \tag{90}$$

By applying (90), we get that

$$\int_{\frac{a}{Q_m}}^{\infty}e^{-\frac{1}{a}y}E_1(y)\frac{1}{y}\,\mathrm{d}y=\left(r-\ln(Q_m)+E_1\left(\frac{1}{Q_m}\right)\right)\times E_1\left(\frac{a}{Q_m}\right)+\frac{1}{2}\left(\zeta(2)+\left(r+\ln\left(\frac{a}{Q_m}\right)\right)^2\right)+e^{-\frac{a}{Q_m}}\sum_{\delta=0}^{\infty}\frac{e_\delta\left(\frac{a}{Q_m}\right)}{(\delta+1)^2}\left(-\frac{1}{a}\right)^{\delta+1}+\sum_{\delta=1}^{\infty}\frac{\left(-\frac{a}{Q_m}\right)^\delta}{\delta!\delta^2}. \tag{91}$$

For simplicity, we define two notations, i.e., $\Psi_1=\sum_{\delta=0}^{\infty}\frac{e_\delta\left(\frac{a}{Q_m}\right)}{(\delta+1)^2}\left(-\frac{1}{a}\right)^{\delta+1}$ and $\Psi_2=\sum_{\delta=1}^{\infty}\frac{\left(-\frac{a}{Q_m}\right)^\delta}{\delta!\delta^2}$. In the following, we will show that both infinite summations, i.e., Ψ_1 and Ψ_2, can be calculated easily. Let us rewrite Ψ_1 as $\lim_{\Delta\to\infty}\sum_{\delta=0}^{\Delta}\frac{e_\delta\left(\frac{a}{Q_m}\right)}{(\delta+1)^2}\left(-\frac{1}{a}\right)^{\delta+1}$. One can easily show that Ψ_1 can be approximated using a finite summation, which converges for any values as long as $\Delta\ge 50$. Furthermore, by applying the definition of generalized hypergeometric function [26], we can replace Ψ_2 with $-\frac{a}{Q_m}{}_3\mathbf{F}_3\left[\begin{smallmatrix}1,\,1,\,1\\2,\,2,\,2\end{smallmatrix};-\frac{a}{Q_m}\right]$. Henceforth, A_2 can be finally expressed as

$$A_2\approx\left(\frac{Q_{m+1}}{Q_m}\right)^{\beta_m}\sum_{s=0}^{m-1}\binom{m-1}{s}(-1)^s e^{\frac{a}{Q_m}}\left(e^{\frac{1}{Q_m}}\times\left(E_1\left(\frac{a+1}{Q_m}\right)-e^{-\frac{1}{Q_m}}E_1\left(\frac{a}{Q_m}\right)\right)-\frac{\beta_m q_m}{Q_mQ_{m+1}}e^{\frac{1}{Q_m}}\times\left(\left(r-\ln(Q_m)+E_1\left(\frac{1}{Q_m}\right)\right)E_1\left(\frac{a}{Q_m}\right)+\frac{1}{2}\left(\zeta(2)+\left(r+\ln\left(\frac{a}{Q_m}\right)\right)^2\right)+e^{-\frac{a}{Q_m}}\sum_{\delta=0}^{\infty}\frac{e_\delta\left(\frac{a}{Q_m}\right)}{(\delta+1)^2}\times\left(-\frac{1}{a}\right)^{\delta+1}-\frac{a}{Q_m}{}_3\mathbf{F}_3\left[\begin{smallmatrix}1,\,1,\,1\\2,\,2,\,2\end{smallmatrix};-\frac{a}{Q_m}\right]\right)\right). \tag{92}$$

By inserting A_1, A_2, and B_{D_2} into (73), $\breve{E}_{\mathrm{s}}^m$ can be finally given in (28)-(30).

Then, we can start to derive the closed-form expression for $\mathbb{E}[\breve{R}_s^m]$, given in (93), shown at the top of the next page. Since B_1-B_4 have similar structures, here we only show the steps of deriving B_1 for simplicity.

$$B_1=\psi_m\int_0^{\infty}\log_2(Q_mz_1+1)\,e^{-(M-m+1)z_1}\left(1-e^{-z_1}\right)^{m-1}\times\int_0^{z_1}e^{-z_2}\,\mathrm{d}z_2\,\mathrm{d}z_1 \tag{94a}$$
$$=\psi_m\int_0^{\infty}\log_2(Q_mz_1+1)\,e^{-(M-m+1)z_1}\big(1-e^{-z_1}\big)^m\,\mathrm{d}z_1 \tag{94b}$$
$$=\psi_m\sum_{s=0}^{m}\binom{m}{s}(-1)^s\int_0^{\infty}\log_2(Q_mz_1+1)\,e^{-az_1}\,\mathrm{d}z_1. \tag{94c}$$

$$\begin{aligned}\mathbb{E}[\breve{R}_s^m] &= \iint\limits_{D_1}\left(\log_2\left(1+\frac{q_m z_1}{Q_{m+1}z_1+1}\right)-\log_2\left(1+\frac{q_m z_2}{Q_{m+1}z_2+1}\right)\right) f(z_1,z_2)\,\mathrm{d}z_1\,\mathrm{d}z_2\\ &= \underbrace{\iint\limits_{D_1}\log_2\left(Q_m z_1+1\right) f(z_1,z_2)\,\mathrm{d}z_1\,\mathrm{d}z_2}_{B_1} - \underbrace{\iint\limits_{D_1}\log_2(Q_{m+1}z_1+1) f(z_1,z_2)\,\mathrm{d}z_1\,\mathrm{d}z_2}_{B_2}\\ &\quad - \underbrace{\iint\limits_{D_1}\log_2(Q_m z_2+1) f(z_1,z_2)\,\mathrm{d}z_1\,\mathrm{d}z_2}_{B_3} + \underbrace{\iint\limits_{D_1}\log_2(Q_{m+1}z_2+1) f(z_1,z_2)\,\mathrm{d}z_1\,\mathrm{d}z_2}_{B_4}. \end{aligned} \tag{93}$$

By defining $Q_m z_1 = x$, B_1 can be transformed to

$$B_1 = \psi_m \frac{1}{Q_m}\sum_{s=0}^{m}\binom{m}{s}(-1)^s \int_0^\infty \log_2\left(x+1\right) e^{-\frac{a}{Q_m}x}\,\mathrm{d}x. \tag{95}$$

From (4.337.2) in [31], we have that

$$\int_0^\infty e^{-ux}\ln(1+vx)\,\mathrm{d}x = -\frac{1}{u}e^{\frac{u}{v}}E_i\left(-\frac{u}{v}\right), \quad |\arg\, v|<\pi, \mathrm{Re}\ u>0. \tag{96}$$

By applying (96), B_1 can be finally written as

$$B_1 = -\frac{\psi_m}{\ln 2}\sum_{s=0}^{m}\binom{m}{s}(-1)^s\frac{1}{a}e^{\frac{a}{Q_m}}E_i(-\frac{a}{Q_m}). \tag{97}$$

By following similar methods, B_2-B_4 can also be expressed in closed-form and finally, $\mathbb{E}[\breve{R}_s^m]$ is given in (31).

APPENDIX F
PROOF FOR LEMMA 1

Note that the lower bound on the ergodic secrecy rate, i.e., $\mathbb{E}[\breve{R}_s^m]$, is given by

$$\mathbb{E}[\breve{R}_s^m] = \mathbb{E}\left[\log_2\left(1+\frac{q_m|h_m|^2}{Q_{m+1}|h_m|^2+1}\right) - \log_2\left(1+\frac{q_m|h_e|^2}{Q_{m+1}|h_e|^2+1}\right)\right]. \tag{98}$$

By inserting $\rho\to 0$ (which means $q_m=0$ and $Q_{m+1}=0$) into (98), one can get that $\mathbb{E}[\breve{R}_s^m]=0$. Also, by inserting $\rho\to 0$ into (26), we can get that $\lim_{\rho\to 0}\breve{E}_s^m = 0$.

When $\rho\to\infty$, $\mathbb{E}[\breve{R}_s^m]$ can be approximated as

$$\mathbb{E}[\breve{R}_s^m] = \mathbb{E}\left[\log_2\left(1+\frac{q_m|h_m|^2}{Q_{m+1}|h_m|^2}\right) - \log_2\left(1+\frac{q_m|h_e|^2}{Q_{m+1}|h_e|^2}\right)\right], \tag{99}$$

which equals to 0. Also, by inserting $\rho\to\infty$ into (26), we can get that $\lim_{\rho\to\infty}\breve{E}_s^m = 0$.

APPENDIX G
PROOF FOR LEMMA 2

By inserting $\rho\to 0$ into $\hat{R}_s^m$, one can easily get that $\hat{R}_s^m = 0$ and $\mathbb{E}[\hat{R}_s^m]=0$. Then, by inserting $\lim_{\rho\to 0}\hat{R}_s^m = 0$ into (6), it is clear that $\lim_{\rho\to 0}\hat{E}_s^m = 0$.

On the other hand, when $\rho\to\infty$, $\lim_{\rho\to\infty}\hat{R}_s^m$ can be written as

$$\lim_{\rho\to\infty}\hat{R}_s^m = \left[\log_2\left(1+\frac{q_m}{Q_{m+1}}\right)-\log_2\left(1+\frac{q_m}{Q_1}\right)\right]^+, \tag{100}$$

which is a positive value. Then, we can get that $\lim_{\rho\to\infty}\mathbb{E}[\hat{R}_s^m] = \log_2\left(\frac{Q_m}{Q_{m+1}}\frac{Q_1}{Q_1+q_m}\right)$. By inserting (100) into (6), we can notice that $\lim_{\rho\to\infty}\hat{E}_s^m = \lim_{\rho\to\infty}\mathbb{E}[\hat{R}_s^m]$, which completes the proof.

REFERENCES

[1] Z. Ding *et al.*, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[2] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[3] F. Fang, H. Zhang, J. Cheng, and V. C. M. Leung, "Energy efficiency of resource scheduling for non-orthogonal multiple access (NOMA) wireless network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–5.

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

[5] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, 2nd Quart., 2017.

[6] W. Yu, L. Musavian, and Q. Ni, "Link-layer capacity of NOMA under statistical delay QoS guarantees," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4907–4922, Oct. 2018.

[7] Y. Liu, Z. Qin, M. Elkashlan, A. Nallanathan, and J. A. McCann, "Non-orthogonal multiple access in large-scale heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 12, pp. 2667–2680, Dec. 2017.

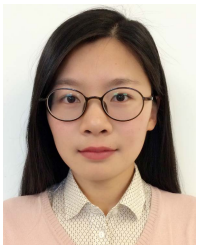
[8] S. M. R. Islam, M. Zeng, O. A. Dobre, and K.-S. Kwak, "Resource allocation for downlink NOMA systems: Key techniques and open issues," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 40–47, Apr. 2018.

[9] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[10] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1850–1863, Sep. 2013.

[11] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

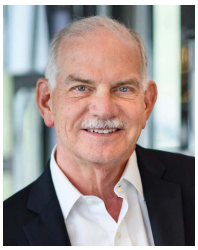
[12] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[13] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[14] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
[15] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
[16] Y. Zhang, H.-M. Wang, T.-X. Zheng, and Q. Yang, "Energy-efficient transmission design in non-orthogonal multiple access," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2852–2857, Mar. 2017.
[17] L. Lv, J. Chen, Q. Ni, and Z. Ding, "Design of cooperative non-orthogonal multicast cognitive multiple access for 5G systems: User scheduling and performance analysis," *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2641–2656, Jun. 2017.
[18] GSMA Intelligence. (Dec. 2014). *Understanding 5G: Perspectives on Future Technological Advancements in Mobile*. [Online]. Available: https://gsmaintelligence.com/research/2014/12/understanding-5g/451/
[19] D. Wu and R. Negi, "Effective capacity: A wireless link model for support of quality-of-service," *IEEE Trans. Wireless Commun.*, vol. 2, no. 4, pp. 630–643, Jul. 2003.
[20] Z. Ding *et al.*, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Aug. 2016.
[21] T. Q. Duong, X. Zhou, and H. V. Poor, *Trusted Communications with Physical Layer Security for 5G and Beyond*. Edison, NJ, USA: IET, Nov. 2017.
[22] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 938–953, Apr. 2016.
[23] 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, Dec. 2014.
[24] M. Ozmen and M. C. Gursoy, "Secure transmission of delay-sensitive data over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2036–2051, Sep. 2017.
[25] H. A. David and H. N. Nagaraja, *Order Statistics*, 3rd ed. New York, NY, USA: Wiley, 2003.
[26] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover, 1965.
[27] *Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Physical Layer; General Description, Release 8*, document TS 36.201, 3GPP, 2009.
[28] W. Wang, K. C. Teh, and K. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.
[29] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[30] J. Tang and X. Zhang, "Quality-of-service driven power and rate adaptation over wireless links," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 3058–3068, Aug. 2007.
[31] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. New York, NY, USA: Academic, 2000.
[32] M. Geller and E. W. Ng, "A table of integrals of the exponential integral," *J. Res. Nat. Bureau Standards*, vol. 73B, no. 3, pp. 191–210, Sep. 1969.



Wenjuan Yu received the Ph.D. degree in communication systems from the School of Computing and Communications, Lancaster University, Lancaster, U.K., in 2018. She is currently a Research Fellow with the 5G Innovation Centre, Institute for Communication Systems, University of Surrey, Guildford, U.K. Her research interests include radio resource management, uRLLC, 5G and beyond wireless networks. She is an Executive Editor of the *Transactions on Emerging Telecommunications Technologies*.

Arsenia Chorti (S'00–M'05) received the Ph.D. degree in electrical and electronic engineering from Imperial College London, U.K., in 2005. She undertook post-doctoral positions at the Universities of Southampton, U.K.; TCU, Greece; and UCL, U.K. She was a Marie Curie IOF with Princeton University, USA and ICS-FORTH, Greece. She has served as a Senior Lecturer of communications and networks with Middlesex University and as a Lecturer with the University of Essex, U.K. Since September 2017, she has been an Associate Professor with ETIS, UMR 8051, Université Paris Seine, Université Cergy-Pontoise, ENSEA, CNRS, France. Her research interests include physical layer security, resource allocation for B5G, and stochastic signal processing, wireless communications, and information theory in general. She has been a member of the IEEE Teaching Awards Committee since 2017.

Leila Musavian (S'05–M'07) received the Ph.D. degree in telecommunications from Kings College London, U.K. She was a Post-Doctoral Fellow with INRS-EMT, Canada, from 2006 to 2008, a Research Associate with McGill University, from 2011 to 2012, and a Lecturer with InfoLab21, Lancaster University, from 2012 to 2016. She is currently a Reader with the School of Computer Science and Electronic Engineering, University of Essex. Her research interests lie in 5G/B5G, uRLLC, radio resource management for next generation wireless networks, and energy harvesting communication systems. She is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and an Associate Editor of Wiley's *Internet Technology Letters*. She has served as an Executive Editor for the *Transactions on Emerging Telecommunications Technologies* from 2016 to 2019.



H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana–Champaign. Since 1990, he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor of Electrical Engineering. From 2006 to 2016, he served as the Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks, energy systems, and related fields. Among his publications in these areas is the recent book *Multiple Access Techniques for 5G Wireless Networks and Beyond* (Springer, 2019).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a Foreign Member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, the 2019 ASEE Benjamin Garver Lamme Award, a D.Sc. *honoris causa* from Syracuse University in 2017, and a D.Eng. *honoris causa* from the University of Waterloo in 2019.

Qiang Ni (M'04–SM'08) received the B.Sc., M.Sc., and Ph.D. degrees from the Huazhong University of Science and Technology, China, all in engineering. He is currently a Professor and the Head of the Communication Systems Group, School of Computing and Communications, Lancaster University, Lancaster, U.K. His research interests include the area of future generation communications and networking, including green communications and networking, millimeter-wave wireless communications, cognitive radio network systems, non-orthogonal multiple access (NOMA), heterogeneous networks, 5G and 6G, SDN, cloud networks, energy harvesting, wireless information and power transfer, the IoTs, cyber physical systems, machine learning, big data analytics, and vehicular networks. He has authored or coauthored more than 200 articles in these areas. He was an IEEE 802.11 Wireless Standard Working Group Voting Member and a contributor to the IEEE Wireless Standards.