Finite-Key Effects in Quantum Access Networks with Wireless Links

Sima Bahrani, Osama Elmabrok, Guillermo Currás Lorenzo, and Mohsen Razavi

School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, UK

***Abstract*—The finite-key effects in quantum access networks are studied. We consider a quantum-classical network where each user is equipped with a certain wavelength to exchange secure keys, using quantum key distribution techniques, and another one to exchange classical data. Users are connected to the central office via a passive optical network. The quantum users are connected to the fiber links via an indoor wireless channel. We investigate the regimes of operation within which a secure key can be exchanged in a reasonable amount of time. We find out that by properly designing the system, it is possible to run both quantum and classical systems at their full capacity.**

***Index Terms*—Quantum key distribution, optical wireless communications, passive optical networks, DWDM.**

I. Introduction

The ubiquitous adoption of online services in our daily lives would have not been possible without the development of mobile and wireless communications. Such systems have made the access to the network such convenient that any new technology needs to find a way to adapt itself to such platforms. The issue of data security is, nevertheless, an important matter especially when it comes to wireless communications. One of the enabling technologies that can provide us with future-proof security is that of quantum key distribution (QKD), where the security of the key exchange between legitimate users—a prerequisite for many cryptography applications—is guaranteed by the laws of quantum mechanics. QKD systems have been developed and tested across different media, but, in order to hit the large market of public customers, they have to take one more step and become available to mobile and wireless users. The initial steps toward this end have already been taken. Key exchange between a handheld device and an ATM has been demonstrated [1], [2] and chip-based prototypes are being developed [3]–[5]. Feasibility studies have also been done to show the possibility of providing QKD services in indoor environments under controlled light conditions [6], and then to connect such wireless users to the central office in a passive optical network (PON) [7]. The latter scenario has, however, been studied only in the asymptotic case when infinitely many key bits have been exchanged between the two users. In practice, we would like to exchange a secret key in a finite span of time, which requires us to study the feasibility of such systems under finite-size key conditions. This paper addresses such finite-key effects in a quantum-classical access network that relies on hybrid wireless-fiber links.

A wireless QKD system must overcome certain challenges before being implemented. The first of such issues is the background noise in the environment. QKD systems inherently operate in the low-photon-number regime, which implies that even a fraction of a background photon collected by the receiver can reduce the rate or possibly make the QKD system insecure. That may imply that, even for an indoor system, certain lighting conditions must hold for a QKD system to operate. Another challenge is with the use of wide beams, which makes a mobile device more accessible, but causes additional loss in the channel. The latter will be costly for our few-photon signals. Once we couple QKD signals to optical fibers and multiplex them with classical data channels, additional loss, due to the nature of PONs, and background noise, due to the Raman noise generated by data channels, must also be tolerated. These all contribute to a hostile environment for QKD operation. Luckily, it has been shown that by proper use of beam steering techniques, and under controlled light conditions, there would be regimes of operation in which secure exchange of keys would *asymptotically* be possible [7]. That corresponds to the limit when infinitely many key bits have been exchanged.

The number of bits exchanged in a QKD protocol is important because such systems rely on parameter estimation for the detection of eavesdroppers, error reconciliation, and privacy amplification. This is often done by measuring the rate of a certain event, e.g. an error in the key, by counting the number of bits in error and dividing it by the length of the key. Such a rate parameter would not, however, be identical to the underlying probability that we need to know in order to reliably do the above tasks. The rates would approach their corresponding probabilities only when we are in the asymptotic limit of exchanging infinitely many key bits. In a practical scenario that the block size of exchanged key bits is finite, we need rigorous techniques by which the underlying probabilities can be bounded within an interval around the observed/measured rate. If the chance of lying outside such an interval is less than a security parameter ε, then we can guarantee that the failure probability for our QKD system, because of this estimation process, is below ε, and that would quantify our confidence in the security of our QKD system. Initial techniques for bounding the failure probability was based on assuming Gaussian statistics for the parameters of interest [8]. Such techniques could not provide us with a rigorous proof of the system's security, but could have offered reasonable estimates for achievable key rates. It has recently been shown that by the use of Chernoff and Hoeffding

This research is partly funded by the UK EPSRC Grant EP/M013472/1 and EU H2020 Project 675662. All data generated in this paper can be reproduced by the provided methodology and equations.

inequalities one can come up with rigorous techniques for bounding the relevant parameters of interest [9]. In particular, by the use of the multiplicative form of Chernoff bounds, it can be shown that we can come very close to the tight bounds obtained from the Gaussian approximation [10].

In this paper, we look at a quantum-classical access network, where the quantum users are operating in an indoor wireless environment. The wireless QKD signals are coupled to an optical fiber, and then multiplexed, using dense wavelength division multiplexing (DWDM), with data channels for each user. A DWDM PON structure then connects the users to the central office. The question of interest for us is the time that it takes for a QKD user to exchange a key of a certain size with the central office, in the presence of Raman noise generated by the data channels and the background noise collected in the room. Looking at it from a different angle, we would like to examine if any, or how much, secret keys can be exchanged in this noisy environment within a reasonable time scale of a few seconds to a few minutes. Longer time scales perhaps void the whole purpose of using the wireless mode, and it might be more practical to use a cable-based solution. A finite time for key exchange requires us to revisit the security of our setup using finite-key techniques. In this work, we use and extend the results in [10] to achieve this objective.

The rest of the paper is organized as follows. In Sec. II, we describe the setup in detail. In Sec. III, we present the finite-key analysis for the setup, and in Sec. IV, we present some numerical results. Section V concludes the paper.

II. System Description

In this paper, we consider a quantum-classical DWDM-PON, as shown in Fig. 1. Such hybrid access networks enable multiple users to exchange secret key bits with the central office, in addition to transmitting their classical data. We assume that there are D users in the system. The kth user is allocated two wavelengths, λ_{d_k} and λ_{q_k}, corresponding to classical and quantum signals, respectively. Each classical channel uses the same wavelength for uplink and downlink to transmit data with a launch power I via the fiber link. The length of the fiber link between the central office and the splitting point of users is denoted by L_0, while the distance between the splitting point and the kth user is denoted by L_k, for $k = 1, ..., D$.

We assume that end users are working in an indoor environment. In principle, both the classical and quantum applications can use wireless optical links for their operation. Here we only focus on the quantum side of the game and assume that there is no interference between the classical signals and quantum ones in the wireless section of the link. To control the light conditions, we consider a windowless room, illuminated by a bulb at the center of the room. The wireless signals are collected at the ceiling by a telescope, and will be coupled to an optical fiber. This would result in an additional coupling loss, denoted by η_{coup}, but, instead, it enables the QKD user to exchange the key with the central office without necessarily trusting the optical equipment in the room. To reduce the deteriorating effect of such a coupling process, we assume that the QKD transmitter and the coupling node use beam steering techniques to provide full alignment [7]. We assume that the QKD transmitter is at the corner of the room, with a semi-angle at half power of $\Phi_{1/2}$.

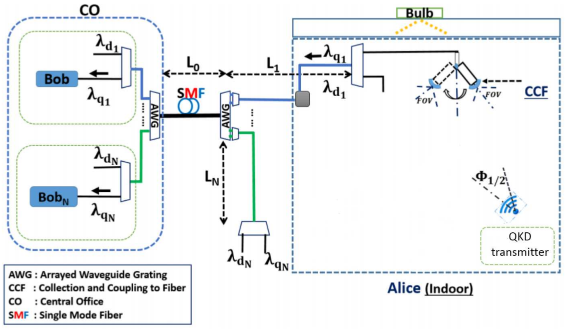

Fig. 1. A quantum-classical access network with embedded wireless indoor links.

For our DWDM system, we assume that the wavelengths available at the C-band, ranging from 1530 nm to 1565 nm, are used. With the channel spacing of 100 GHz, there would be 44 available channels. In order to allocate the channels to the available wavelengths appropriately, one should consider different sources of background noise generated by classical channels at the quantum ones, e.g., Raman noise and adjacent channel crosstalk. One possible setting is to assign the lowest wavelengths of the system to quantum channels and the largest ones to classical channels. While this method may not be the optimal solution [11], it would place quantum channels at the anti-stokes region of the Raman spectrum of all classical channels. Also, to reduce the level of such Raman noise at the quantum receivers, we assume the use of narrow bandpass filters at the quantum channels. On the other hand, adjacent channel crosstalk can be reduced by not allocating quantum and classical channels to adjacent wavelengths. In our setup, we assume that the two channels in the middle of the wavelength grid are not in use, which leaves us with 42 available channels corresponding to a maximum number of users of 21.

In our work, the decoy state BB84 protocol is used for the QKD setups [12]. We assume that two decoy states are used, where one of them has a mean photon number (intensity) of ν and the other one is the vacuum state. The intensity of the signal state, μ, is chosen to be larger than ν. The probabilities of choosing these intensity levels are denoted by q_s, q_w, and $1 - (q_s + q_w)$, for the signal state, weak decoy state, and vacuum state, respectively. As for the probabilities of Z and X bases in the BB84 protocol, we assume efficient QKD with asymmetrical probabilities P_z and $P_x = 1 - P_z$. With the transmission of N pulses in a QKD round by the QKD transmitter, we can obtain an upper bound for the final key rate. The free parameters μ, ν, q_s, q_w, and P_z, each has a range of possible values. To achieve the highest possible key rate, we optimize the key rate over these parameters.

III. Finite-Key Analysis

In this section, we present the finite-key analysis for the system described in Sec. II. According to the GLLP analysis, the final key length extracted from sifted bits in basis $\gamma \in \{z, x\}$ is lower bounded by [13]:

$$K^\gamma \geq M_1^{s\gamma}[1 - h(e_1^{ps\gamma})] - fM^{s\gamma}h(E^{s\gamma}), \tag{1}$$

where $f \geq 1$ denotes the error correction inefficiency and $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the Shannon binary entropy function. In (1), the superscript "s" represents the signal state; $M^{s\gamma}$, $E^{s\gamma}$, $M_1^{s\gamma}$, and $e_1^{ps\gamma}$, respectively, represent the number of successful detection events, the quantum bit error rate, the number of successful detection events from single-photon components, and the phase error rate of single-photon components in basis γ of the signal state. The first two parameters would specify how much error correction is needed. In practice, one can just measure how many parity bits are used in the error correction to exactly specify the cost of error correction in (1). The single-photon parameters should, however, be rigorously bounded to make sure that sufficient privacy amplification is in place. By using the decoy-state method, we can obtain a lower bound on $M_1^{s\gamma}$, denoted by $M_1^{s\gamma L}$, and an upper bound on $e_1^{ps\gamma}$, denoted by $e_1^{ps\gamma U}$, and use them in (1). The final key length, in bits, obtained from z and x bases would then be $K = K^z + K^x$.

The vacuum+weak decoy-state protocol uses three intensity levels corresponding to the signal state, weak decoy state, and vacuum decoy state, to generate pulses and encode key bits. In [10], it is shown that by using the set $A = \{M^{s\gamma}, E^{s\gamma}M^{s\gamma}, M^{w\gamma}, E^{w\gamma}M^{w\gamma}, M^{\upsilon\gamma}, E^{\upsilon\gamma}M^{\upsilon\gamma}\}$ of observed parameters, the single-photon parameters $M_1^{s\gamma L}$ and $e_1^{ps\gamma U}$ can be obtained. Here, the superscripts "w" and "υ" represent weak decoy state and vacuum decoy state, respectively. In the following, we summarize the key steps in [10] and apply it to our problem.

In [10], the Chernoff bound is used to calculate upper and lower bounds on averages of our observables in A, i.e., $\mathrm{E}^L[M^{s\gamma}], \mathrm{E}^U[M^{s\gamma}], ..., \mathrm{E}^L[E^{\upsilon\gamma}M^{\upsilon\gamma}], \mathrm{E}^U[E^{\upsilon\gamma}M^{\upsilon\gamma}]$, in such a way that $\Pr\{\mathrm{E}^L[\chi] < \mathrm{E}[\chi] < \mathrm{E}^U[\chi]\} \geq 1 - \varepsilon$, for any $\chi \in A$. ε will then be the *failure* probability in this case. For an observable value $\chi > 0$, it has been shown that

$$\mathrm{E}^L[\chi] = \frac{\chi}{1 + \delta^L} \tag{2}$$

and

$$\mathrm{E}^U[\chi] = \frac{\chi}{1 - \delta^U}, \tag{3}$$

where δ^L and δ^U is calculated by solving the following two equations:

$$\left(\frac{e^{\delta^L}}{(1 + \delta^L)^{(1+\delta^L)}}\right)^{\frac{\chi}{1+\delta^L}} = \frac{\varepsilon}{2} \tag{4}$$

$$\left(\frac{e^{-\delta^U}}{(1 - \delta^U)^{(1-\delta^U)}}\right)^{\frac{\chi}{1-\delta^U}} = \frac{\varepsilon}{2}. \tag{5}$$

For $\chi = 0$, the bounds are $\mathrm{E}^L[\chi] = 0$ and $\mathrm{E}^U[\chi] = -\ln(\varepsilon/2)$. The lower bound on M_1^γ and the upper bound on $e_1^{b\gamma}$, where $e_1^{b\gamma}$ is the bit error rate of single-photon components in basis γ, are given by:

$$M_1^{\gamma L} = Y_1^{\gamma L} N^\gamma (e^{-\mu}\mu q_s + e^{-\nu}\nu q_w), \tag{6}$$

$$e_1^{b\gamma U} = \frac{\frac{\mathrm{E}^U[E^{w\gamma}M^{w\gamma}]}{q_w N^\gamma}e^{\nu} - \frac{\mathrm{E}^L[E^{\upsilon\gamma}M^{\upsilon\gamma}]}{(1-q_s-q_w)N^\gamma}}{Y_1^{\gamma L}\nu}, \tag{7}$$

where

$$Y_1^{\gamma L} = \frac{\mu}{\mu\nu - \nu^2}\left((\frac{\mathrm{E}^L[M^{w\gamma}]}{q_w N^\gamma})e^{\nu} - (\frac{\mathrm{E}^U[M^{s\gamma}]}{q_s N^\gamma})e^{\mu}\frac{\nu^2}{\mu^2} - (\frac{\mathrm{E}^U[M^{\upsilon\gamma}]}{(1 - q_s - q_w)N^\gamma})\frac{\mu^2 - \nu^2}{\mu^2}\right). \tag{8}$$

In the above equations, $N^\gamma = P_\gamma^2 N$, where P_γ is the probability of choosing basis γ and N is the block size.

The next step is the calculation of $M_1^{s\gamma L}$. To this aim, we note that $\mathrm{E}[M_1^{s\gamma}] = p_1^{s\gamma}M_1^\gamma$, where $p_1^{s\gamma}$ is the conditional probability that a single-photon state corresponds to a coherent pulse with intensity μ (signal state). By applying the symmetric form of the Chernoff bound for the parameter $\bar{\chi} = p_1^{s\gamma}M_1^{\gamma L}$, a lower bound for $M_1^{s\gamma}$ can be obtained.

The final step is finding an upper bound on the phase error rate of single-photon components from the signal state in each basis, denoted by $e_1^{ps\gamma U}$. In [10], random sampling method has been used to calculate the upper bound e_1^{pszU} using e_1^{bxU}. The same approach can be used to calculate e_1^{psxU} using e_1^{bzU}. For more details on the finite key analysis of vacuum+weak decoy-state protocol, please refer to [10].

As mentioned in the previous section, the final key rate should be optimized over possible range of values for parameters μ, ν, q_s, q_w, and P_z. To solve this multivariate optimization problem, we can start by an appropriate initial set of values, and optimize the parameters one by one, assuming that other parameters are constant. This process should be iterated until we converge to a specific set of values for our parameters.

IV. Numerical Results

In this section, we evaluate the performance of the system described in Sec. II by providing some numerical results. We use a DWDM-PON system with 100 GHz channel spacing. We assume that users 1 to D are, respectively, allocated wavelengths $\lambda_{q_1} = 1530$ nm to $\lambda_{q_D} = 1530 + 0.8(D-1)$ nm on the wavelength grid for key exchange, and $\lambda_{d_1} = 1564.4 - 0.8(D-1)$ nm to $\lambda_{d_D} = 1564.4$ nm for data transmission. As for the relevant distances, we assume that $L_0 = 5$ km and $L_k = 500$ m, for $k = 1, ..., D$. In our indoor wireless environment, we assume that the QKD transmitter is located at the corner of the room and its beam is directed toward the QKD receiver, such that full alignment is maintained between the two nodes. The semi-angle at half power of the QKD source is assumed to be $\Phi_{1/2} = 1°$. Furthermore, the QKD receiver's field of view (FOV) is assumed to be $6°$. Other nominal values for the parameters of our system are listed in Table I, which are all attainable by today's established QKD technologies.

TABLE I
NOMINAL VALUES USED FOR SYSTEM PARAMETERS.

Parameter	Value
Quantum Efficiency	0.3
Receiver dark count rate	1E-6 ns^{-1}
Error correction inefficiency, f	1.22
Misalignment probability, e_d	0.033
Detector gate interval and pulse width	100 ps
Fiber attenuation coefficient	0.2 dB/km
AWG insertion loss	2 dB
Coupling loss, η_{coup}	10 dB
Repetition rate of QKD setup	1 GHz

In order to calculate the key rate, in this section, we assume that the measured values for the observable parameters χ in set A match that of the asymptotic limit scenario, when no eavesdropper is present. These asymptotic values have been calculated based on the analysis, and parameter values, in [7], in which the effect of various sources of noise including the Raman noise and bulb noise is considered. For any such value of χ, we then follow the prescription in (2)–(8) to find the relevant key parameters in the finite-key regime. We then use the obtained lower and upper bounds in (1) to find an upper bound on the key rate.

One of the key applications of wireless indoor QKD could be in topping up the key bank that users may keep on their portable devices. For such an application, a fair requirement is that the time that it takes for the user to top up should not be excruciatingly long. If the key exchange takes too long, the user may prefer to use an alternative method, e.g. a cable-based solution, for that matter. A limited time for key exchange, plus a finite pulse rate for photon transmission, implies that the block size we can use for key distribution is of finite size. In this section, we first attempt to answer two questions: (1) For a target secret key size, S, how much time is needed to establish the key? and (2) for a fixed given amount of time for key exchange, how many key bits can securely be exchanged? In both cases, we neglect the time that it takes for establishing the connection as well as that needed for post-processing.

In order to answer the above questions, we first study how the key rate depends on the employed block size as shown in Fig. 2(a). We consider a quantum-classical DWDM-PON with 20 users, where the launch power for data channels is on average -30 dBm. This is typically sufficient to guarantee an error rate below 10^{-9} for data channels. Because of the Raman noise generated by the data channels and its non-uniform distribution, different quantum channels experience different levels of background noise. In Fig. 2(a), and all other examples in this section, we have chosen the worst case scenario and present the key rate for the QKD user with the lowest secret key generation rate. As can be seen in Fig. 2(a), the secret key rate per pulse in this channel increases by increasing the block size, until it reaches its asymptotic limit of 4.3×10^{-4} b/pulse for very large block sizes. There are two observations to make in this figure. First, it can be seen that for a block size around 10^8 and less, the secure exchange of keys is not possible. That is, if the time that we have for key exchange is below a certain threshold, it would not be possible to exchange a secret key at all. The second observation is that if we need to work near the asymptotic limit, the time needed for key exchange could be unreasonably long. For instance, at a clock rate of 1 GHz for our QKD system, even a block size of 10^{12} pulses takes 1000 s to transmit, which implies that the user should allocate nearly 20 minutes to finish the key exchange.

Another way to look at the above problem is to work out for a target key size S, what block size, and correspondingly how much time is needed for key exchange. Figure 2(b) provides an answer to this question, in which the size of the final key, i.e., K is plotted versus N. It can be seen in this figure that for any fixed target key length, there would be an optimal block size. For example, for $S = 10^7$, our optimal choice for block size is about 6×10^{10} and the required time is about 1 minute. This length of key is large enough to refresh the seed in an AES-256 protocol nearly 40,000 times. It is possible to exchange shorter keys as well, but the longer the key the more time-efficient the key exchange will become.

Next, let us fix the key exchange duration and see how that would affect other system parameters. We have chosen this fixed time to be 100 s, which, at a clock rate of 1 GHz, corresponds to $N = 10^{11}$. One of the key parameters that needs to be set in such a hybrid network is the launch power for data channels. On the one hand, we do not want this parameter to be too low, or otherwise, our data channels will not be reliable. Choosing I to be too high, however, would result in a large amount of Raman noise, which dismantles the QKD operation, henceforth reducing the number of QKD users we can support. Figure 3 depicts the maximum possible number of users that can be supported for different values of launch power. It can be seen that for $I < -22$ dBm, it is possible to use the system at its full capacity. For launch powers larger than -22 dBm, the number of users drops sharply. For example, for $I = -20$ dBm, the maximum possible number of users reduces from 21 to 15. Within the parameters of our setup, the maximum toelrable launch power is 0.1 mW, which is one order of magnitude lower than the typical 1 mW power used in optical communications systems. This will indicate that the needs of quantum communications applications need to be accounted for in the design of future hybrid quantum-classical networks.

V. CONCLUSIONS

In this paper, we considered a quantum-classical access network with wireless indoor links. In this system, users were connected via wireless links to a DWDM PON structure. We investigated the possibility of exchanging secret key bits in a reasonable time of up to a few minutes by considering the finite-size key effects in our analysis. Our numerical results showed that by a careful specification of system parameters, such as launch power, block size and coupling loss, key exchange was feasible within practical times limits for a wireless user. In particular, we showed that the choice of launch power for data channels can significantly affect the number of QKD users that can be supported by the network. Proper initialization of the system is then required to allow expansion if needed.

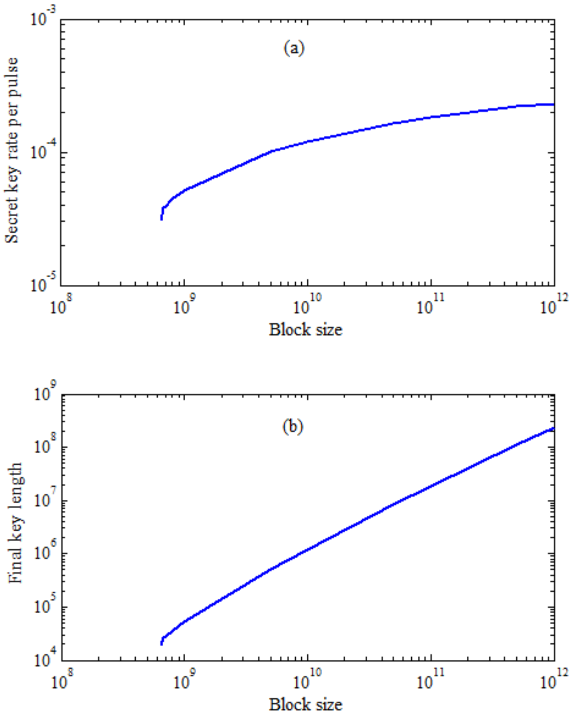

Fig. 2. (a) Secret key rate per pulse for different values of block size. (b) Final key length for different values of block size.

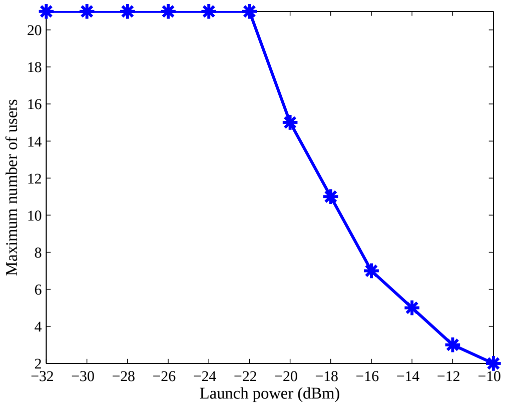

Fig. 3. Maximum number of QKD users that can be supported at different values of launch power.

References

[1] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, "Low cost and compact quantum key distribution," *New J. Phys.*, vol. 8, no. 10, p. 249, 2006.

[2] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O'Brien, and D. Bitauld, "Handheld free space quantum key distribution with dynamic motion compensation," *Opt. Exp.*, vol. 25, no. 6, pp. 6784–6795, 2017.

[3] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. OBrien, and M. G. Thompson, "Chip-based quantum key distribution," *Nature Commun.*, vol. 8, p. 13984, 2017.

[4] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," *Optica*, vol. 3, no. 11, pp. 1274–1278, Nov 2016.

[5] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, "Design and evaluation of a handheld quantum key distribution sender module," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 131–137, 2015.

[6] O. Elmabrok and M. Razavi, "Wireless quantum key distribution in indoor environments," *J. Opt. Soc. Am. B*, vol. 35, no. 2, pp. 197–207, Feb 2018.

[7] O. Elmabrok, M. Ghalaii, and M. Razavi, "Quantum-classical access networks with embedded optical wireless links," *J. Opt. Soc. Am. B*, vol. 35, no. 3, pp. 487–499, 2018.

[8] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, July 2005.

[9] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature Commun.*, vol. 5, p. 3732, 2014.

[10] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A*, vol. 95, no. 1, p. 012333, 2017.

[11] S. Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," *Sci. Rep.*, vol. 8, no. 1, p. 3456, 2018.

[12] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[13] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quant. Inf. Comput.*, vol. 4, p. 325, 2004.