IL NUOVO CIMENTO **47 C** (2024) 296
DOI 10.1393/ncc/i2024-24296-3

COMMUNICATIONS: SIF Congress 2023

Feasibility of quantum-secure communication in real-world networks

L. MARIANI

Department of Physics "E. R. Caianiello", University of Salerno - via Giovanni Paolo II 132, 84014, Fisciano (SA), Italy

received 7 February 2024

Summary. — In a world that heavily relies on the secrecy of digital data, the ongoing trend in the development of quantum computers is raising new concerns about the vulnerabilities of the ubiquitous public-key cryptography, which forms the foundation of common banking systems and blockchain technology. While these cryptographic schemes rely on the computational complexity of specific mathematical problems, Quantum Key Distribution (QKD) is claimed to provide unconditionally secure communication "by the laws of physics". On the other side, QKD's practical implementation is hindered by the severe decay of the information rates with the distance, which is intrinsic to the same quantum principles it relies on. The question driving this work is whether a real-world network, such as the one constituted by the Internet fiber infrastructure, might mitigate the rate-distance tradeoff enough to sustain a quantum-encrypted communication between trusted nodes.

1. – Quantum key distribution

In order to understand the current relevance of Quantum Key Distribution (QKD) in the field of information theory, it is useful to place it in context with the other cryptographic primitives, commonly classified into symmetric and asymmetric cryptography. The former relies on a shared secret for encryption: among all, the One-Time Pad (OTP) algorithm is proven to be *unconditionally secure*, meaning that no information can be intercepted by a malicious third party, regardless of the computational power at their disposal. OTP requires that a shared "disposable" key, as long as the message, is summed to the message and used only once. The necessity for a more effective cipher led to the development in the 70 s of asymmetric methods, which produce a private key known only to the owner and a public key shared with other users. Security is ensured by means of the computational complexity of an infeasible mathematical problem. However, despite overcoming the issue of the key exchange, this approach undermines the integrity of these algorithms for various reasons: a) the complexity of the problems needs to be continuously updated to stay ahead of any technological advance, b) there is no proof that an

alternative, faster route to brute-force attacks does not exist and finally c) Shor's algorithm, proposed in 1994, would allow a sufficiently powerful quantum machine to break the cipher [1].

The claim of QKD, first appeared in 1984 [2], is to enable key generation between two distant nodes —conventionally called Alice and Bob— which combined with the OTP cipher would allow for unconditionally secure communication based on quantum physics principles. Therefore QKD solves a), b) and c), even though it admittedly exhibits other drawbacks, mainly a strong decay of the achievable rate with the distance. In general, any QKD protocol requires Alice and Bob to agree a priori on a redundant set of ways to map classical information into quantum states; particularly, these consist in eigenstates of incompatible quantum observables —for example different photon polarization bases— that are then exchanged across a quantum channel. This redundance, that forces Bob to guess a basis to measure the state and causes the two parties to consequently discard part of the measurement outcomes, actually constitutes an advantage over a possible eavesdropper "Eve" trying to extract information while remaining unnoticed. Contrarily to the classical case, Eve cannot split nor copy the signal, therefore she needs to immediately send Bob a replacement for any state that she may intercept, and since —just like Bob— she does not know what the original state was, she has to guess, exposing herself to a non-negligible probability of being detected.

All the protocols that make use of observables with a discrete spectrum, such as polarization or spin, fall under the umbrella of Discrete-Variable QKD (DV-QKD). Since they often require producing, transmitting and detecting single quantum states, which demands quite a technological effort, a new class of protocols appeared around the year 2000 [3], based on observables with continuous spectra and thus taking the name of Continuos-Variable QKD (CV-QKD). Despite an even more severe decay of the rate with distance, this technology is more cost-effective and can be implemented in standard optical fibers. In CV-QKD, instead of choosing a direction along which they should perform the measurement of the quantum state, Alice and Bob choose to measure one of two quadratures, namely two conjugated variables: we can think of them as the phase and the amplitude of a laser beam. The best strategy that Eve can adopt in CV-QKD is an approach named *entangling cloner* [4]: she makes half of an entangled couple interfere with the state that Alice is sending to Bob, in such a way that it could be interpreted as due to a lossy quantum channel. A lower bound for the key rate is then given by $K = I(A : B) - I(B : E)$, where $I(X : Y)$ is the mutual information shared by X and Y. Since CV protocols are usually limited to the use of Gaussian states [5], K can be evaluated from the covariance matrix, which fully describes the system.

After the quantum phase is concluded, Alice and Bob use a public but authenticated classical channel, *e.g.*, an Internet connection, to select from their strings of measurements only the bits that correspond to a matching choice of bases —or quadratures. Finally, two post-processing steps are performed on the resulting key: *information reconciliation*, namely an error correction algorithm, and *privacy amplification*, a compression of the key that reduces to nearly zero the number of bits that may have been leaked.

2. – Complex networks

In the absence of quantum repeaters at the present day, the rate-distance tradeoff poses a severe limitation to long-range quantum cryptography. Therefore one of the proposed use cases for QKD is a Metropolitan Area Network (MAN), *i.e.*, a network of trusted nodes on the scale of the tens of kilometers, which would allow for indirect

quantum-secure communication through a route of key exchanges between neighbouring nodes. In order to realistically simulate this scenario, we opted for a generative model that can produce a network with all the complexity features that are usually found in real-world examples: the *small-world* property, consisting in a slow growth of the average distance in relation to the number of nodes in the graph [6]; the invariance under scale transformations, or *self-similarity* [7]; a *power-law* distribution of the degrees of the nodes, defined as the number of direct connections that each node has in the network [8]; and a strong *clustering*, namely the tendency of the nodes to form densely interconnected subgraphs [6].

The theoretical tool that we chose for the generation of such networks is the $\mathbb{S}_2$ model, belonging to the family of *geometric network models* [9]. It is characterized by two sets of coordinates: the *popularity* coordinates may be interpreted as the expected degrees of the nodes; the *similarity* coordinates are introduced as additional degrees of freedom of the model, distributed in a latent space provided with a metric (the $\mathbb{S}_2$ sphere in our case). The topology of the graph underlying the network is then given by the following connection probability [10]:

$$p_{ij} = \frac{1}{1 + (\frac{d_{ij}}{\mu k_i k_j})^{\beta}}, \tag{1}$$

where d_{ij} is the distance between nodes i and j in the latent space, k_i is the degree of node i, and μ, β are two parameters related to the average degree and to the clustering of the graph. Here values of $\mu = 0.0294$ and $\beta = 1.243$ have been inferred from the data of a real AS Internetsystem([1]) through the dedicated software Mercator [10]. In addition to that, every node is assigned a position in a real "geographical" space, needed to compute the length l of each of the quantum channels connecting it to its neighbours, and taken proportional to its position in latent space.

3. – Methods and preliminary results

In CV-QKD the behaviour of the key rate depends on the parameters that characterize the quantum channel, namely the transmittance T and the excess noise at Alice's site ε, both assumed to be due to the presence of an eavesdropper. Specifically $T = e^{-\frac{\alpha}{10} l}$ with α being the attenuation coefficient for the optical fiber at telecom wavelengths, and $\varepsilon = 2\varepsilon_0/\eta T$ [11], where η is the detector efficiency and ε_0 is the excess noise at Bob's site: fig. 1 (left) illustrates how ε_0 impacts the topology of the system. Considering state-of-the-art values for all the parameters involved ($\alpha = 0.2$ dB/km, $\eta = 0.95, \varepsilon_0 = 0.1$ in shot-noise units), it was then possible to estimate the critical distance d_c, defined as the largest distance at which safe communication at a positive rate can be achieved. Consequently, several randomized realizations of complex graphs were generated using the $\mathbb{S}_2$ model, and any edge that exceeded d_c, which would prove useless from a quantum security standpoint, was removed. For the sake of this work, we considered the resulting systems as realistic instances of a QKD network and we monitored two figures of merit: the *connectivity*, intended as the fraction of nodes in the giant component (*i.e.*, the largest cluster of the underlying graph), and the *key rate*, computed through a shortest-path algorithm (Dijkstra a.) and averaged over many pairs of nodes. Both quantities

([1]) `https://snap.stanford.edu/data/as-733.html`.

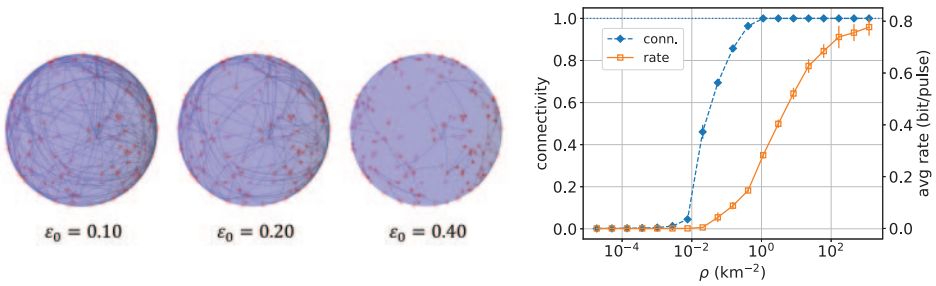

Fig. 1. – Effect of different values of ε_0 on the topology of the final network (left); connectivity (dashed line) and key rate (solid l.) as a function of node density (right).

have also been evaluated for different sizes of the system, to observe their behaviour in response of a change in the node density ρ. As we can see in fig. 1 (right), above a certain density the connectivity shows a steep increase, which suggests that the graph is going through percolation: a disconnected set of small clusters tends to merge into one giant component and the system recovers its ability to effectively provide a route between any couple of nodes. This can be ascribed to the fact that the smaller the average distance between neighboring nodes becomes, the more are the available edges and thus the available paths, which is also reflected on a growth in the average rate.

In conclusion, we have described the methods and the tools used to make a numerical analysis —through relatively simple and fundamental theoretical arguments— of the properties of a QKD network that could be implemented in a close future using currently available infrastructure. Further developments of this project may regard an integration of DV-QKD in the model, and investigate the possibility of using its longer range to bridge disconnected clusters of the network and improve the overall performance.

* * *

The author acknowledges that the present work is an overview of a paper in course of elaboration, co-authored with (in alphabetical order): A. Acín, F. Centrone, C. P. García, M. A. Serrano, J. van der Kolk, R. Yehia. The author would also like to thank C. Attanasio, R. Citro, S. Pagano for their mentoring as PhD supervisors.

REFERENCES

[1] Mosca M., *IEEE Secur. Priv.*, **16** (2018) 38.
[2] Bennett C. H. and Brassard G., *Theoretical Computer Science*, Vol. **560** (Elsevier) 2014, pp. 7–11.
[3] Ralph T. C., *Phys. Rev. A*, **61** (1999) 010302.
[4] Navascues M. and Acin A., *Phys. Rev. Lett.*, **94** (2005) 020505.
[5] Weedbrook C. *et al.*, *Rev. Mod. Phys.*, **84** (2012) 621.
[6] Watts D. J. and Strogatz S. H., *Nature*, **393** (1998) 440.
[7] Song C. *et al.*, *Nature*, **433** (2005) 392.
[8] Barabási A.-L. and Albert R., *Science*, **286** (1999) 509.
[9] Boguñá M. *et al.*, *Nat. Rev. Phys.*, **3** (2021) 114.
[10] García-Pérez G. *et al.*, *New J. Phys.*, **21** (2019) 123033.
[11] Roumestan F. *et al.*, *High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM*, in *2021 European Conference on Optical Communication (ECOC)* (IEEE) 2021, pp. 1–4.