Optical Identification for User Authentication in Quantum Key Distribution Systems

S. Civelli [1,2], P. Nadimi Goki[2,3], E. Parente[2], L. Potì[2,3,4], M. Secondini[2,3]

[1] CNR-IEIIT, stella.civelli@cnr.it
[2] Tecip Institute, Scuola Superiore Sant'Anna
[3] PNTLab, Consorzio nazionale interuniversitario per le telecomunicazioni (CNIT)
[4] Universitas Mercatorum

Abstract *We propose a novel technique for user authentication in fiber-based quantum key distribution systems. Practical implementation using coherent optical frequency-domain reflectometry is described and authentication security assessed. ©2023 The Author(s)*

Introduction

A generic quantum key distribution (QKD) system includes two users, Alice and Bob, who need to exchange a secret key used for message encryption/decryption. For this purpose, Alice and Bob, regardless of the type of protocol, use a classic service channel and a quantum channel. The former is often a segment of the public network without any strong constraints, while the latter is always a point-to-point fiber system whose length is limited by the secure key rate. Under these assumptions, an attacker has the power to manipulate the raw key created via the quantum states exchange and to listen to the conversation happening over the classical channel. Despite this, the post-processing of a QKD system allows to estimate a possible eavesdropper's intervention and the amount of information in her hands, and to eventually stop the protocol[1]. In this scenario, the authentication of the classical channel is essential to prevent a possible man-in-the-middle attack during post-processing, such that the two legitimate parties of the conversation can rely on other's true identity. In order to achieve this, a message authentication code (MAC) is generally employed and the most common examples of it are the Wegman-Carter authentication scheme and variations thereof[2]. Here, the security leans upon the mathematical complexity theory, in a way that polynomial-time adversaries are left with a neglectable probability of success in forgering[3].

Recently, the optical identification (OI) was proposed as a novel concept for identification, authentication, and monitoring. The OI takes advantage of the imperfections of physical elements—including devices, sub-systems, systems, and network elements—to define its own unique fingerprint, or signature[4]. In particular, it was shown that a single mode fiber (SMF) is a physical unclonable function, with its signature being the Rayleigh backscattering pattern (RPB) produced when stimulated by a propagating light, due to the random and unique density fluctuations in a SMF originated in the fabrication process[5]–[7]. This major characteristic was used for the implementation of OI, successfully identifying a fiber in a point-to-point scenario and for the path recognition in a passive optical network scenario[4],[8]. In this work, we propose and demonstrate to use OI for the authentication of the users in a QKD system, using the RBP caused by the user's pigtail as its signature.

Optical identification for user authentication

The quantum channel is a point-to-point communication system made of two transceivers and an optical fiber whose length is typically limited to few tens of kilometers by secure key rate. For mutual user identification process within a QKD system, we use the pigtail's RBP of each transceiver, as sketched in Fig. 1. In particular, Alice identifies Bob (equivalently, Bob identifies Alice) with the following protocol: (i) Alice scans the fiber link (i.e., the optical fiber including transceivers pigtails) through a tunable laser, (ii) Alice reads the RBP of the user to be identified performing C-OFDR, (iii) Alice retrieves the digital signature of the user, (iv) Alice compares the received signature with the public signature of Bob $\mathbf{b}$, (v) Alice identifies the user and start or abort QKD communication. In a network scenario, Alice compares the received signature with a set of public signatures $\{\mathbf{b}, \mathbf{c}, \mathbf{d}, \dots\}$ of the different users.

In this implementation, the signature of an user is the vector containing the bits obtained by reading the RBP with a single bit analog to digital converter (ADC) which acquires N samples. The sig-

nature can be equivalently seen as a QR code, as in Fig. 1.

The comparison of the received signature with $\mathbf{b}$ is done by evaluating the Hamming distance (HD), i.e., the number of bits that should be flipped to obtain the same vector. The HD of two binary vectors of i.i.d. bits is distributed as a binomial distribution with N trials and mean value Np, where p is the probability of having a *wrong* bit to be flipped. The decision rule for OI is: if HD is below the threshold t (the signatures are similar), the user is Bob and QKD communication starts, otherwise (the signatures are different in more than t bits) we abort communication. This concept is illustrated in Fig. 2, which reports the probability of the HD between the public signature of Bob $\mathbf{b}$ and the received signatures of (i) Bob $\tilde{\mathbf{b}}$, with mean $m_{\tilde{\mathbf{b}}}$, and (ii) another user $\tilde{\mathbf{e}}$—either Eve or another user of the network—with mean $m_{\tilde{\mathbf{e}}}$. Without loss of generality, the threshold is $t = (1-\gamma)m_{\tilde{\mathbf{e}}} + \gamma m_{\tilde{\mathbf{b}}}$, with $0 \leq \gamma \leq 1$.

The reliability of the decision metric is measured with the probability of false negative (FN) and false positive (FP). On the one hand, a FN—*Bob rejected by mistake*—occurs when Bob is the user, but the procedure fails and Alice does not recognize him. A FN happens when the HD between $\mathbf{b}$ and $\tilde{\mathbf{b}}$ is larger than t. On the other hand, a FP—*Eve accepted by mistake*—occurs when the user is not Bob, but the procedure fails and Alice identifies the user as Bob, i.e., the HD between $\mathbf{b}$ and $\tilde{\mathbf{e}}$ is smaller than t. In general, while it is desirable to minimize both the probability of FP and FN, one can tailor t to the system requirements: if t decreases, the security improves (the probability of FP decreases) at the expense of identification capabilities (the probability of FN increases). Overall, one can optimize t to minimize the weighted wrong identification (WWI) defined as

$$\text{WWI} = \underbrace{p(\text{FN})}_{\text{Bob rejected}} r + \underbrace{p(\text{FP})}_{\text{Eve accepted}} (1-r) \qquad (1)$$

where $0 \leq r \leq 1$ is a weight. The WWI measures the probability of FP and FN, taking into account the weight r, which should be chosen depending on the system requirements and application scenario.

Practical Implementation and Security Assessment

In a real system, each user includes an optical fiber (at least the transceiver pigtail) that can be used as unique identifier. Here we assume a

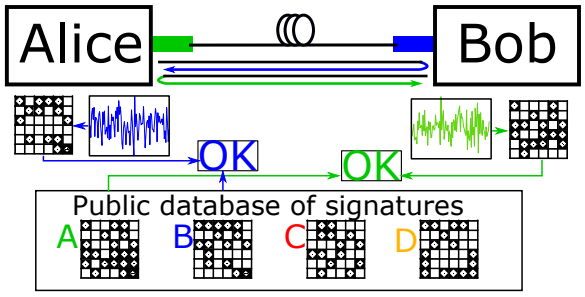

Fig. 1: Point-to-point authentication

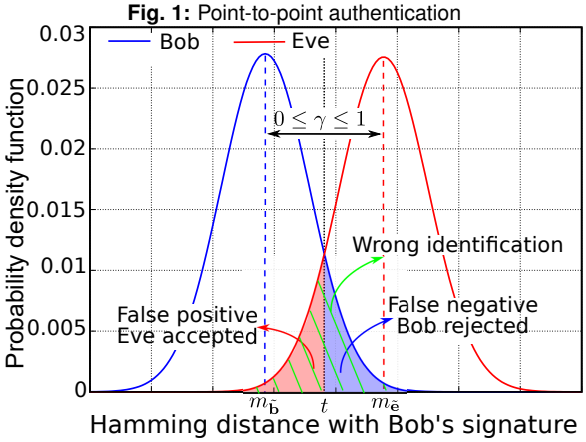

Fig. 2: Example of comparison of HD of $\mathbf{b}$ with $\tilde{\mathbf{b}}$ and $\tilde{\mathbf{e}}$.

pigtail of length $L = 0.3$m whose fingerprint is read through C-OFDR[9], having a single bit ADC, sweep rate $\gamma_{sw} = 7.5$THz/s, which acquires and stores N samples, with N at most equal to 5000. These characteristics are well below the capabilities of current ADC. For the sake of simplicity, in the following we denote as Eve any other user that is not Bob, including the other users of the network.

The results shown below are obtained through simulations, as follows. First, we generated the RBP for two users, Bob and Eve. Assuming a simple C-OFDR scheme as in Fig.3 and neglecting random phase noise, the received photocurrent $I(t)$ detected at the balanced photodetector is

$$I(t) = E_0 \sum_{k=1,\ldots,n} \sqrt{R_k} \cos(2\pi\gamma t \tau_k) \qquad (2)$$

where $k = 1, \ldots, n$ are n reflection points in the fiber, with reflectivity R_k and roundtrip time τ_k[4],[9]. The roundtrip time is defined as $\tau_k = 2s_k/v$, where v is the speed of light in the fiber and s_k is the position of the reflection point in the fiber. To properly simulate the Rayleigh backscattering, we place a random number n of reflection points in the fiber, while we select the reflectivity to ensure a Rayleigh

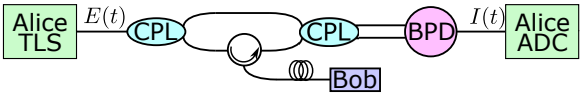

Fig. 3: C-OFDR scheme for RBP recognition. TLS: tunable laser source, CPL:coupler, BPD: balance photodetector.

scattering coefficient of 0.14dB/km. Next, AWGN noise is added to the two RBPs to emulate receiver thermal noise, and the RPBs are digitized with a single bit ADC to obtain the signature of Bob $\mathbf{b}$ (without noise, representing the public signature) and the received (with noise) signatures of Bob $\tilde{\mathbf{b}}$ and Eve $\tilde{\mathbf{e}}$. Finally, we compute the HD of $\mathbf{b}$ with $\tilde{\mathbf{b}}$ and $\tilde{\mathbf{e}}$. The procedure is repeated 10^3 times to obtain an accurate estimation of the mean values $m_{\tilde{\mathbf{b}}}$ and $m_{\tilde{\mathbf{e}}}$. The estimated mean value $m_{\tilde{\mathbf{b}}}$ (or $m_{\tilde{\mathbf{e}}}$) of the HD allows to directly estimate its probability density function, as a binomial distribution with N trials (the number of ADC samples) and probability of success $m_{\tilde{\mathbf{b}}}/N$ (or $m_{\tilde{\mathbf{e}}}/N$). Finally, we obtain the probability of false positive and false negative for a given threshold t.

Fig. 4(a) shows the probability of FP and FN as a function of the threshold position γ for different SNR and number of samples N. As expected, Fig. 4(a) shows that when γ approaches 1, the probability of FN, i.e., Bob rejected by mistake, becomes very small, but the probability of accepting Eve approaches 0.5, since in this case all users are likely to be accepted. On the contrary, when γ tends to zero, the probability of any user to be rejected is very high, and, therefore, the probability of FN becomes small, but the probability of FP approaches 0.5. As a consequence, an optimal system should be tailored to obtain a reasonable trade-off among these two effects. For example, if one want to have the same probability of FP and FN, the optimal value for γ ranges between 0.25 and 0.5, depending on the parameters involved.

Next, Fig. 4(b) shows the WWI (solid) and the probability of FN (dashed) and FP (dotted) as a function of the SNR, when γ is optimized to minimize R. When $r = 0.5$, the probability of FP and FN are approximately equal (and they are superimposed in the figure). Conversely, when r becomes smaller (e.g., $r = 10^{-12}$), the threshold γ gets closer to zero to minimize the probability of FP at the expense of an increased probability of FN. For example, if we assume that there are a lot of Eve attempts to break the system and we want to be sure that Eve does not succeed, it is reasonable to often reject the user. However, in this case, it is difficult to correctly identify Bob and the probability of FN is high. This underline that the decision metric γ and the weight r should be tailored to the system. For example, one could minimize the probability of FP, with the constraint that the probability of FN is smaller than $\leq 10^{-20}$.

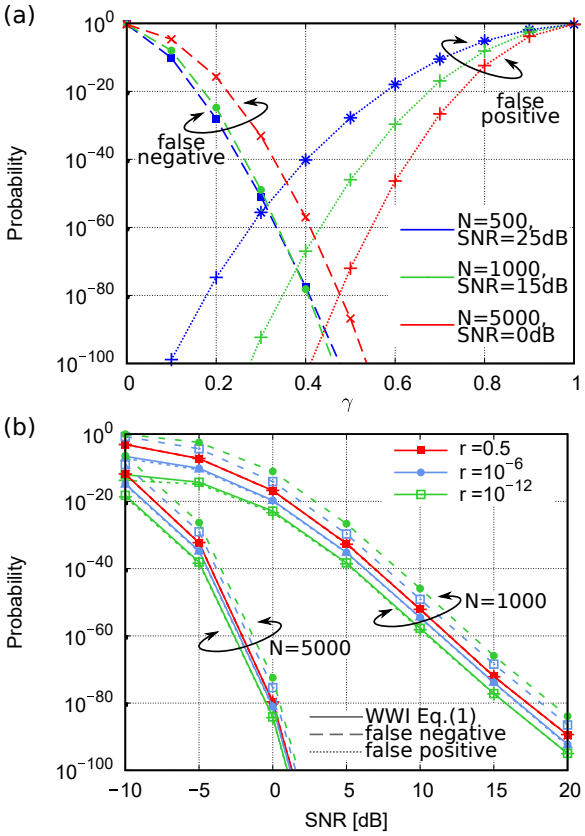

Fig. 4: (a) Probability of FP and FN versus threshold position γ, (b) probability of WWI, FP and FN, with optimized γ versus SNR, for different weights r.

Conclusion

A novel technique for the authentication of QKD communication users, based on optical identification, is proposed for the first time. In particular, the authentication of the users is achieved by the recognition of the Rayleigh backscattering pattern caused by the pigtail of the user. After describing the protocol, we test its security for different values of SNR, ADC samples, and decision rule. We show that the authentication protocol can be trusted, ensuring a probability of false positive (Eve accepted my mistake) and false negative (Bob rejected by mistake) well below 10^{-20} in most of the scenario of interest.

Acknowledgments

This work was partially supported by the following projects: FLEX-SCALE (101096909) under the HORIZON-JU-RIA program, ALLEGRO (101092766) under the HORIZON-RIA program, PNRR MUR project PE0000023-NQSTI, and National Operational Programme on Research and Innovation 2014-2020 - FSE REACT EU "Azione IV.5 Dottorati su tematiche Green".

References

[1] A. Ruiz Alba Gaya *et al.*, “Practical quantum key distribution based on the BB84 protocol,” in *Waves*, Instituto de

Telecomunicaciones y Aplicaciones Multimedia (iTEAM), vol. 1, 2011, pp. 4–14.

[2] M. Peev *et al.*, "A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography," *International Journal of Quantum Information*, vol. 3, no. 01, pp. 225–231, 2005.

[3] M. Rosulek, "Message authentication codes," *The Joy of Cryptography OE (1st)*, 2017.

[4] P. Nadimi Goki, S. Civelli, E. Parente, *et al.*, "Optical identification using physical unclonable functions," in *arXiv:2305.02141*, 2023.

[5] Y. Du, S. Jothibasu, Y. Zhuang, C. Zhu, and J. Huang, "Unclonable optical fiber identification based on rayleigh backscattering signatures," *Journal of Lightwave Technology*, vol. 35, no. 21, pp. 4634–4640, 2017.

[6] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for internet of things," *Computer Networks*, vol. 183, p. 107 593, 2020.

[7] F. Pavanello, I. O'Connor, U. Rührmair, A. C. Foster, and D. Syvridis, "Recent advances in photonic physical unclonable functions," in *2021 IEEE European Test Symposium (ETS)*, IEEE, 2021, pp. 1–10.

[8] L. Potí, P. Nadimi Goki, T. Teferi Mulugeta, N. Sambo, and R. Caldelli, "Optical fingeriprint: A possible direction to physical layer security, authentication, identification, and monitoring," in *61st FITCE International Congress "Future Telecommunications: Infrastructure and Sustainability*, 2022.

[9] F. Ito, X. Fan, and Y. Koshikiya, "Long-range coherent ofdr with light source phase noise compensation," *Journal of Lightwave Technology*, vol. 30, no. 8, pp. 1015–1024, 2012. DOI: 10.1109/JLT.2011.2167598.