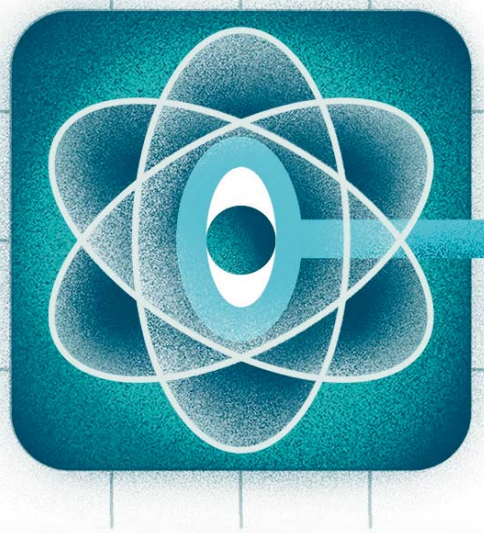

ENHANCING SECURITY THROUGH SMART PHOTONICS & QUANTUM INNOVATION

CNR-INO TECHNOLOGY TRANSFER GROUP*
Consiglio Nazionale delle Ricerche, Roma, Italy

Technological transfer at CNR-INO bridges cutting-edge research with real-world applications, particularly in optics and photonics. The action accelerates lab-to-market innovations, driving economic growth and societal resilience. Recently, CNR-INO researchers have pioneered technologies in security through quantum mechanics and smart photonics. These include quantum key distribution (QKD) for unparalleled data encryption and optical Physical Unclonable Functions (PUFs) for secure authentication. These advancements promise to revolutionize security, safeguarding critical infrastructure and sensitive data. Strategic collaborations with industries, technology licensing, and spin-offs aim to ensure early adoption, fostering robust digital resilience and trust.

a cura di S. Falciano e C. Spinella

1 Introduction

Technological transfer activities stand as a cornerstone of innovation, bridging the gap between cutting-edge research and real-world applications. With a rich legacy of pioneering advancements in Optics and Photonics, in the last decade the Istituto Nazionale di Ottica (National Institute of Optics – CNR-INO) has been seeking to accelerate the transition of innovations from the laboratory to the marketplace, fostering economic growth, technological leadership, and societal resilience in an increasingly digitized world. One important aspect, which we are here discussing, is the valorization of research activities within the realm of security. Harnessing the transformative potential of quantum mechanics and smart photonics, CNR-INO researchers have recently developed a suite of novel technologies poised to revolutionize security paradigms. From quantum communication and cryptography to authentication and certification protocols, these advancements hold the promise of fortifying critical infrastructure, protecting sensitive data, and mitigating emerging cyber threats and counterfeiting activities.

In the following sections, we illustrate how recent advances in quantum technologies and photonic smart materials are set to revolutionize security by highlighting two novel technologies developed by CNR-INO teams. Quantum innovations provide unparalleled data encryption and secure communication, effectively rendering traditional hacking methods ineffective. Concurrently, progress in photonics and smart materials is driving the creation of novel devices for data identification, significantly enhancing safety in our digital society.

2 Quantum-enabled unconditional security: safe communications using light quanta

As the amount of data exchanged worldwide increases yearly, the number of cyber-attacks and the average cost of lost or stolen information are dramatically growing [1]. Secure communications are hence becoming an impelling need to protect everyday life activities, such as e-commerce with credit cards, health data and internet banking, and more critical scenarios, like government and defence communications.

In this context, cryptography is a powerful method of protecting transmitted data from unauthorised access. Its security is based on shared keys between two communicating users, which, like passwords, are used for encryption and decryption of the shared information. A fundamental requirement to guarantee safe cryptography is to use random and secret keys previously distributed among the users. Therefore, distant parties must use a secure method to exchange cryptographic keys over common communication channels, facing the so-called key distribution problem. Today, the most widely used key distribution methods, like RSA, are based on one-way algorithms, i.e. on classical functions that are easy to compute but difficult to invert. The security of these methods is thus established on the limited ability of today's computers to invert specific functions but is threatened by the advent of new more powerful technology, such as quantum computers or new algorithms, which will compromise the reliability of current key distribution methods.

* CNR-INO Technology Transfer Group are Giuseppe Lombardo, Giulia Adembri, Maja Colautti, Annamaria Fedele and Chiara Mustarelli, integrated by Francesco Riboli, Alessandro Zavatta, Francesco S. Cataliotti for the specific application.

In 1984, Bennett and Brassard introduced the groundbreaking concept of quantum key distribution (QKD) [2]. This method, known as BB84 protocol, harnesses the laws of quantum physics and offers unparalleled security. This innovative method involves encoding each bit of a key in a qubit, represented by a quantum state of light, *e.g.* a single photon, travelling through a standard telecommunication optical fibre or a free-space optical channel. In particular, in the case of a single photon, the quantum state can identify any property and experimentally controllable degree of freedom of light, such as polarization, time of arrival, and frequency. Leveraging the non-orthogonality of quantum states, Heisenberg's uncertainty principle, and no-cloning theorem, QKD enables the communicating users to detect any unauthorised attempt to extract or copy the information carried by the photon, thereby evaluating the actual security of the received key. Consequently, the users can share the data, subsequently to the key exchange, only in correspondence to unconditional security. In particular, the unconditional security stems from the peculiarity of quantum systems to be irreversibly perturbed by any measurement performed on them. Since a measurement can be conceived as any kind of physical interaction with the system, any unauthorized external attempt of spying the key will be hence identified by checking the presence of modifications in the stream of single photons composing the key. This level of security can be mathematically derived directly from the quantum physical laws rather than based on uncertain assumptions of computational hardness. For this reason, QKD offers the unmatched benefit of being unaffected by the present and future advancements in classical and quantum computing [3].

Since its formulation, QKD has undergone considerable development over the last decades, making it the most advanced among emerging quantum technologies, both at the theoretical level and with practical implementations. Numerous QKD protocols have been successfully demonstrated over long transmission distances, often involving quantum networks. These networks are typically based on fibre optic infrastructures but also extend to satellite communications. In the present digital era, the unmatched security benefits offered by QKD have made its strategic applications of great interest, not only among the academic community but also private companies and government institutions, including standardisation institutes.

The CNR-INO research activity focuses on metropolitan-scale QKD links based on fibre optic and free space.

Figure 1a illustrates the in-field implementation of QKD by CNR-INO researchers over a single-mode fiber in the metropolitan area of Florence [4]. This setup not only demonstrates the feasibility of QKD in real-world conditions but also addresses the compatibility between current QKD technologies

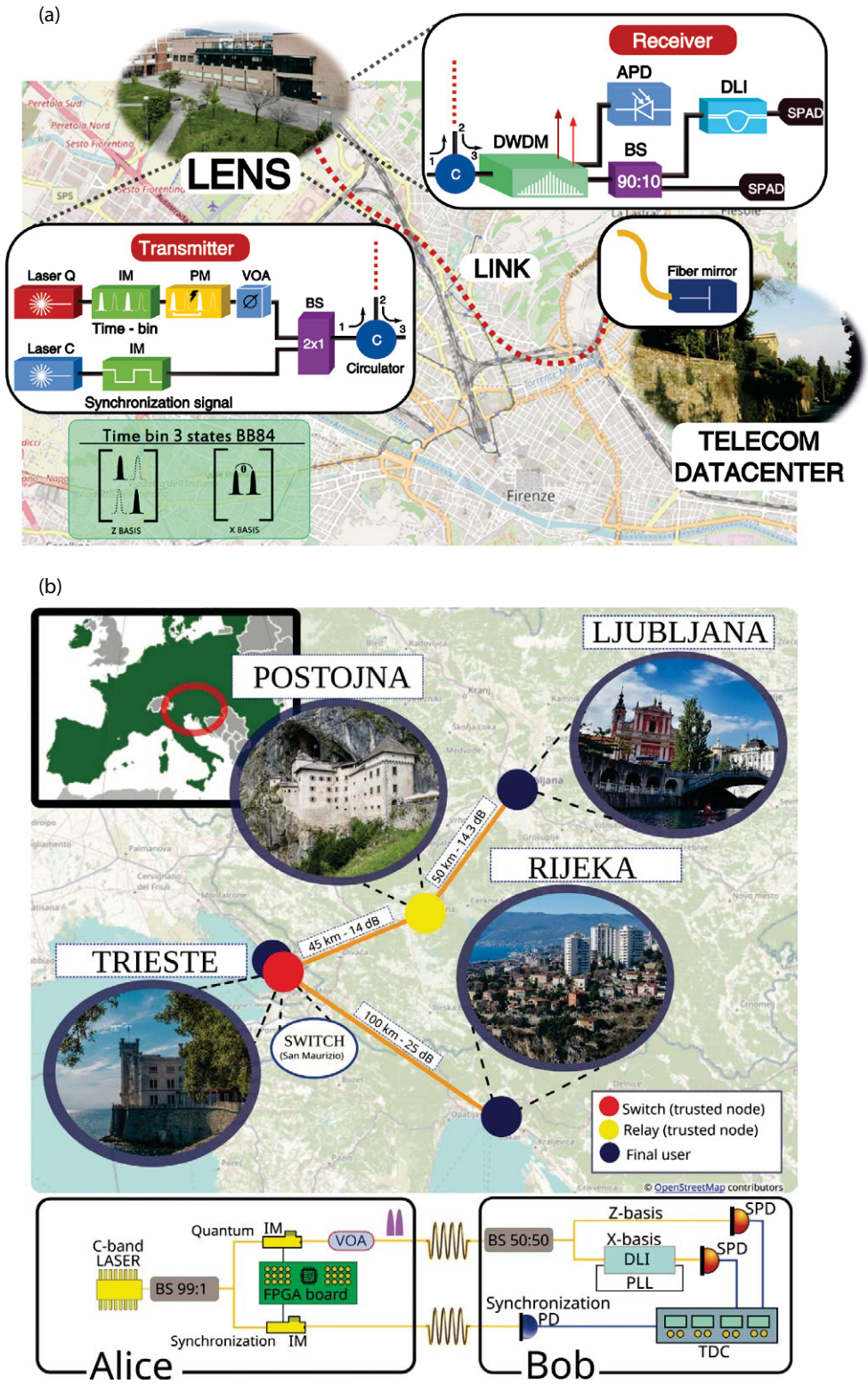

Fig. 1 (a) Experimental setup of the field trial QKD experiment in Florence. The transmission channel is a dark fiber link connecting the LENS laboratory, where Alice and Bob are located, to a TIM telecom datacenter, where a standard optical mirror is installed at the end of the fiber. (b) Network and setup schemes of the first Inter-European Quantum Network realised by CNR researchers during the G20 event in Trieste.

and classical optical communication systems [5].

This setup was then used for a public demonstration of QKD during the closing ceremony of the EuroScience Open Forum 2020 in the presence of the Italian Prime Minister. In collaboration with the DTU – Technical University of Denmark and the University of Trieste, this event was the first public demonstration of in-field QKD realized in Italy.

Meanwhile, researchers of the CNR-INO collaborated with the design and testing of novel protocols and setups to enable higher key generation rate and noise tolerance harnessing the so-called high-dimensional QKD, *i.e.* encrypting the key in a multi-dimensional quantum state or, otherwise said, harnessing and manipulating more than one photon degree of freedom simultaneously. The experimental validation of high-dimensional encoding was successfully carried out in the town of L'Aquila, where it was demonstrated exploiting path-encoding combined with a time-bin encoding in multi-core fibres deployed around the city centre of L'Aquila [6, 7].

Over these years, the CNR-INO team has enormously increased the readiness level of QKD technology, with the attention of several stakeholders, including governments and big industries. In 2020, researchers and entrepreneurs involved in the aforementioned activities founded a spin-off company of the CNR-INO called QTI – Quantum Telecommunications Italy (QTI, `qticompany.com`) to develop commercial QKD systems implementing the BB84 protocol in the time-bin domain. Its cutting-edge technology has already been tested in real environments on multiple occasions. In 2021, during the Digital Ministers' Meeting of the G20 in Trieste, QTI carried out the technical implementation of the first public demonstration of an intergovernmental quantum communication between three different European countries – Italy, Slovenia and Croatia [8]. This demonstration marked the first quantum transmission among three nodes (Trieste, Ljubljana, and Rijeka) in a real-world environment, achieving an attenuation of 25 dB on the longest link (fig. 1b).

Today, QTI operates within the TIM Group and commercializes turn-key QKD systems that are compatible with existing telecom infrastructure. QTI is also a QKD provider of the EuroQCI network, the European Union's initiative aiming to build a secure quantum communication infrastructure that will span the whole EU territory.

3 Unlocking physical complexity for reconfigurable unclonable authentication

Besides a secure communication and data sharing protocol, this digital era also calls for secure and reliable authentication methods to protect private information and to safeguard access to personal devices and services. To date, the most effective method for ensuring an authentication source involves the permanent storage of digital keys in electronic devices, for example in smartphones, car keys, bank cards or computers, and then relies on hardware cryptographic operations such as digital signatures or classical encryption algorythms. Unfortunately, besides the cost in terms of both design area and power consumption, this approach is often susceptible to invasive attacks, including malware and physical methods [9-11]. Protecting against such attacks necessitates active tamper detection and prevention circuitry, which must remain continuously powered, an inconvenient limitation especially for portable electronic devices. A promising new route to overcome this problem is the use of non-digital key generation processes, also called primitives, which can derive a secret key from relying on the unique complexity of physical system, thereby eliminating the need for continuously powered tamper-detection mechanisms. The key generation process can be modelled as a transformation process and mathematically described by a function, the so-called physical unclonable function (PUF) [12]. In practice, PUFs are randomly structured physical systems which exhibit a complex input-output behavior, in the PUF jargon called Challenges and Responses, that is unique to each PUF. Their uncontrollable individual disorder on small length scales makes them practically unclonable, even for their original manufacturer. Effectively, PUFs can disable various popular attack vectors compared to classical, permanently stored keys in digital memory, as their physical nature, randomness, and non-clonability prevents any remote purely digital data connection. In a typical authentication protocol that uses PUFs, the user holding the PUF identifies remotely via a digital communication channel to a central authority. The starting assumption for the protocol is that the central authority has stored in a secret library a sufficiently large database of input-output pairs or challenge-response pairs (CRPs) of the PUF, which has been measured in a previous step and represents a unique PUF identifier or fingerprint.

During the authentication phase, the central authority sends a series of randomly chosen challenges from its database to the user, which responds with specific answers generated by its PUF. Then the authority starts with the authentication procedures which mainly consists of comparing the received responses with the responses stored in the secret library for that specific PUF. If they match within the error threshold, which is previously carefully evaluated, then the identity of the PUF is confirmed. For the protocol to be effective, the database shall be large enough (*e.g.* 10^9 CRPs) since each CRP can be used only once in the above protocol, for the sake of security, consequently shrinking the library over time.

In this context, disordered photonic structures are the perfect choice for creating optical PUFs to be used for authentication or anticounterfeiting. These photonic systems are characterized by many degrees of freedom that under illumination with coherent light produce a complex intensity pattern in transmission and/or reflection. This pattern, known as speckle, is the result of the interference of numerous independent transmission channels and is extremely sensitive to microscopic changes in the physical structure of the materials [13–15], thereby serving as a unique fingerprint of the scattering volume.

Traditional optical-based PUFs are limited by their fixed or permanently modifiable configurations,

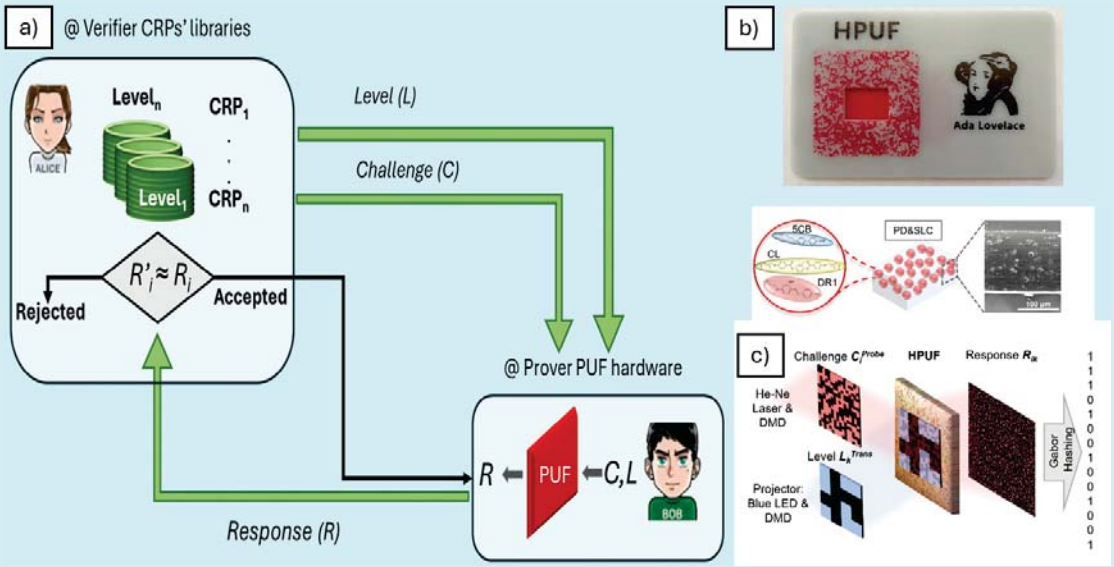

Fig. 2 (a) The authentication scheme of the Hyper PUF (HPUF) is mainly constituted by two processes: the first one consists in the token enrollment at the credential server provider (Alice), and secondly the authentication of a prover (Bob). During the enrollment of the token a subset of CRPs of the PUF are registered in a library. Then the PUF is assigned to the prover Bob. Every time Bob wants to be authenticated *e.g.* for a money transaction, Alice sends one of the challenges of the library to Bob, that interrogates the PUF (c) to generate the response *R* of the given challenge. Finally, the response is sent back to Alice that compares it with the one stored in the library.

allowing only a few numbers of CRPs exchange per device, and resulting in low information entropy for the generated keys. However, recent research at CNR-INO laboratories, in collaboration with INRIM, UniSi, UniFi, LENS and a German research group, has made significant strides in generating more complex photonic cryptographic keys. These advancements potentially enable cryptographic protocols that are resilient to future quantum computer attacks, marking a considerable step forward in the field of secure communications [16]. The novel technology proposed uses smart disordered photonic materials made of dye-doped Polymer-Dispersed and Polymer-Stabilized Liquid Crystals (PD&PS-LCs) (fig. 2). These materials can be reversibly reconfigured to achieve a spatial-temporal control of the scattering potential that can be made hysteresis-free by customizing their chemical composition. Furthermore, the optical PUFs made of PD&PS-LCs possess an extremely large internal degree of freedoms that translate in a net entropy increase of the generated key. This new technology enables the integration of multiple cryptographic functions in a single device, thus facilitating the creation of a multilevel optical PUF, referred to as Hyper-PUF (HPUF). Each level of the HPUF is defined by a distinct configuration of the scattering potential, significantly enhancing its cryptographic versatility and security.

This novel technology enables a wide range of practical applications. The spatial-temporal transformation of the scattering potential represents a promising solution not only as a primitive for multiuser or multiprocess authentication but also for quantum secure authentication [17–18] and nonlinear optical functions for cryptography and photonics [19]. Indeed, the strength of the multiple scattering of light, *i.e.* the opacity of the HPUF, can be varied from semi-transparent to strongly opaque by tuning the Liquid Crystal (LC) concentration and sample thickness and by doping with high-refractive-index particles. Conversely, a switchable scattering potential enables the experimental implementation of a random potential with a robust nonlinear optical response. Nonlinear cryptographic key generators, enabled by this technology, offer significantly higher resilience against machine-learning attacks and can be broadly applied as complex nonlinear optical functions in optical computing and machine learning [20].

4 Conclusion

Researchers at CNR-INO are transforming cutting-edge research into practical security solutions to tackle critical challenges of the digital era. By leveraging quantum mechanics and smart photonics, they have developed innovative technologies for quantum communication, cryptography, and authentication.

Quantum key distribution (QKD) provides unmatched security by utilizing quantum mechanics principles, offering resilience against current and future computational threats. CNR-INO's advancements in metropolitan-scale QKD links and high-dimensional QKD protocols demonstrate the potential for widespread adoption and integration into existing infrastructures.

Additionally, research on optical Physical Unclonable Functions (PUFs) has led to the development of optical cryptographic primitives. These enable all-optical multilevel operation through reversible switching of optical properties in flexible polymer-dispersed and polymer-stabilized LC films, generating highly complex authentication keys for multiuser authentication. This innovation overcomes the limitations of conventional digital security and standard PUF configurations, enabling cryptographic protocols resistant to future quantum computer attacks.

These innovations offer unparalleled data protection and robustness against cyber threats. Strategic collaborations with industrial partners, promotion of technology licensing, and spin-off creation should facilitate the early adoption of these smart and quantum-enabled security solutions, ensuring robust security and trust in our increasingly digital and interconnected world.

References

[1] Cisco annual internet report - white paper, https://www.cisco.com/c/en/us/solutions/collateral/executiveperspectives/annual-internet-report/white-paper-c11-741490.pdf (accessed: November 2022).

[2] C. H. Bennett, G. Brassard, "*Quantum cryptography: public-key distribution and coin tossing*," in: *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, 175 (1984).

[3] M. Mosca, "*Cybersecurity in an era with quantum computers: Will we be ready?*", *IEEE Security & Privacy*, 16 (2018) 38.

[4] D. Bacco, I. Vagniluca, B. Da Lio, N. Biagi, A. Della Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe *et al.*, "*Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area*," *EPJ Quantum Technol*., 6 (2019) 5.

[5] D. Bacco, I. Vagniluca, D. Cozzolino, S. M. Friis, L. Høgstedt, A. Giudice, D. Calonico, F. S. Cataliotti, K. Rottwitt, A. Zavatta, "*Toward fully- fledged quantum and classical communication over deployed fiber with up-conversion module*", *Adv. Quantum Technol*., 4 (2021) 2000156.

[6] D. Bacco, N. Biagi, I. Vagniluca, T. Hayashi, A. Mecozzi, C. Antonelli, L. K. Oxenløwe, A. Zavatta, "*Characterization and stability measurement of deployed multicore fibers for quantum applications*", *Photon. Res.*, 9 (2021) 1992.

[7] M. Zahidy, D. Ribezzo, C. De Lazzari, I. Vagniluca, N. Biagi, R. Müller, T. Occhipinti, L. K. Oxenløwe, M. Galili, T. Hayashi, D. Cassioli, A. Mecozzi, C. Antonelli, A. Zavatta, D. Bacco, "*Practical high-dimensional quantum key distribution protocol over deployed multicore fiber*", *Nat. Commun.*, 15 (2024) 1651.

[8] D. Ribezzo *et al.* "*Deploying an Inter-European Quantum Network*", *Adv. Quantum Technol.*, 6 (2022) 2200061.

[9] R. Anderson, in "*Security Engineering: A Guide To Building Dependable Distributed Systems"* (Wiley & Sons, Hoboken, NJ) 2020.

[10] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, Y. Yarom, in: *IEEE Symp. on Security and Privacy (SP)*, (IEEE, Piscataway, NJ) 2019, pp. 1–19.

[11] M. Lipp, M. Schwarz, D. Gruss Graz, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard Graz, P. Kocher, D. Genkin, Y. Yarom, M. Hamburg Rambus, in: *27th USENIX Security Symposium*.

[12] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, *Science,* 297 (2002) 2026.

[13] R. Berkovits, "*Sensitivity of the multiple-scattering speckle pattern to the motion of a single scatterer*", *Phys. Rev. B*, 43(1991) 8638.

[14] F. Riboli *et al.*, "*Tailoring correlations of the local density of states in disordered photonic materials*", *Phys. Rev. Lett.,* 119 (2017) 043902.

[15] G. E. Lio, S. Nocentini, L. Pattelli, E. Cara, D. S. Wiersma, U. Rührmair, F. Riboli, "*Quantifying the sensitivity and unclonability of optical physical unclonable functions*", *Ad. Photon. Res.*, 4 (2023) 2200225.

[16] S. Nocentini, U. Rührmair, M. Barni, D. S. Wiersma, F. Riboli, "*All-optical multilevel physical unclonable functions*", *Nat. Mater.*, 23 (2024) 369.

[17] B. Škorić, P. W. H. Pinkse, A. P. Mosk, "*Authenticated communication from quantum readout of PUFs", Quantum Inf. Process*, 16 (2017) 200.

[18] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škoric, P. W. H. Pinkse, "*Quantum-secure authentication of a physical unclonable key*", *Optica,* 1 (2014) 421.

[19] Y. Eliezer, U. Ruhrmair, N. Wisiol, S. Bittner, Cao, "*Tunable nonlinear optical mapping in a multiple-scattering cavity*", *PNAS,* 120 (2023) e2305027120.

[20] A. Vijayakumar, V. C. Patil, C. B. Prado, S. Kundu, "*Machine learning resistant strong PUF: possible or a pipe dream?*", in: *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 19–24* (IEEE) 2016.


Giuseppe Lombardo


Giulia Adembri


Maja Colautti


Annamaria Fedele


Chiara Mustarelli


Francesco Riboli


Alessandro Zavatta


Francesco S. Cataliotti

CNR-INO Technology Transfer Group is affiliated to the Istituto Nazionale di Ottica (National Institute of Optics – CNR-INO) of the Consiglio Nazionale delle Ricerche (Italian National Research Council - CNR), which is a leading research institute in the fields of Optics and Photonics, as well as in Quantum Technologies. The institute activities span from atomic, molecular and condensed matter physics to quantum optics, non-linear optics, and smart optical materials, with contributions to both fundamental research and applied technologies. In particular, the exploration of innovative technologies includes research in the fields of optical imaging, laser spectroscopy, optical communications, photonic devices and quantum technologies, fostering impact in the sectors of healthcare, cultural heritage, telecommunications, security, and environmental monitoring. CNR-INO has a longstanding tradition of solving yet-unmet needs of society and companies, since 1927 – year of its foundation, to foster expertise in optics and the creation of optical instrumentation which was a priority for the nation's security. Collaborating with industrial partners is often a key strategy to translate scientific expertise into practical applications, drive innovation, and contribute to economic growth. From this perspective CNR-INO promotes consulting services and collaboration activities with companies aimed at addressing specific technological challenges or developing innovative solutions by applying expertise in photonics.