Letter

optica

QUANTUM-SECURE AUTHENTICATION OF A PHYSICAL UNCLONABLE KEY

SEBASTIANUS A. GOORDEN,[1] MARCEL HORSTMANN,[1,2] ALLARD P. MOSK,[1] BORIS ŠKORIĆ,[3] AND PEPIJN W.H. PINKSE[1,*]

[1]*Complex Photonic Systems (COPS), MESA+ Institute for Nanotechnology, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands*
[2]*Laser Physics and Nonlinear Optics (LPNO), MESA+ Institute for Nanotechnology, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands*
[3]*Eindhoven University of Technology, PO Box 513, 5600 MB Eindhoven, The Netherlands*
**Corresponding author: p.w.h.pinkse@utwente.nl*

Received XX Month XXXX; revised XX Month, XXXX; accepted XX Month XXXX; posted XX Month XXXX (Doc. ID XXXXX); published XX Month XXXX

Authentication of persons and objects is a crucial aspect of security. We experimentally demonstrate Quantum-Secure Authentication (QSA) of a classical multiple-scattering key. The key is authenticated by illuminating it with a light pulse containing fewer photons than spatial degrees of freedom and verifying the spatial shape of the reflected light. Quantum-physical principles forbid an attacker to fully characterize the incident light pulse. Therefore, he cannot emulate the key by digitally constructing the expected optical response, even if all information about the key is publicly known. QSA offers a combination of highly desirable properties that is unmatched by any other authentication method. QSA uses a key that cannot be copied due to technological limitations and is quantum-secure against digital emulation. Moreover, QSA does not depend on secrecy of stored data, does not depend on unproven mathematical assumptions and is straightforward to implement with current technology.

OCIS codes: *(270.0270, 110.7348, 110.7050).*

http://dx.doi.org/10.1364/optica.99.099999

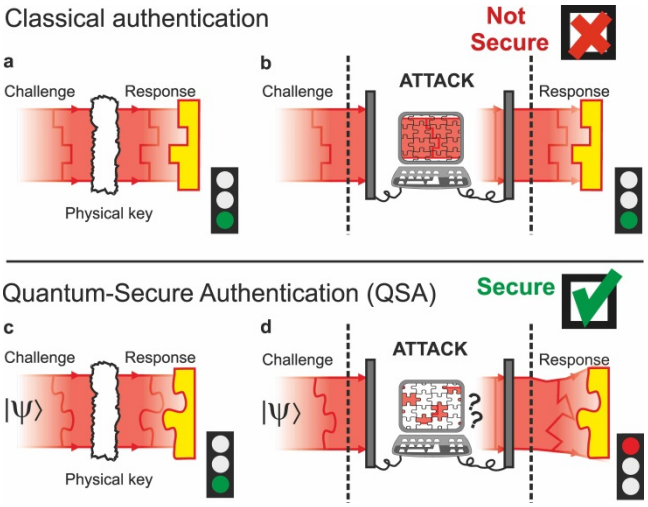

Fig. 1. The idea of Quantum-Secure Authentication (QSA): (a) In classical authentication of an optical unclonable physical key, a challenge wavefront of sufficient complexity is sent to the key. The response wavefront is compared with those stored in a database (yellow pieces) to make a pass (green light) or fail (red light) decision. However, this verification can be spoofed by an emulation attack (b) in which the challenge wavefront is completely determined and the expected response is constructed by the adversary who knows the challenge-response behavior of the key. In Quantum-Secure Authentication (c) the challenge is a quantum state for which an emulation attack (d) fails because the adversary cannot actually determine the quantum state and hence any attempt to generate the correct response wavefront fails.

Authentication of persons can be based on "something that you know", e.g. digital keys, or "something that you have", e.g. physical objects such as classical keys or official documents. A drawback of digital keys is that their theft can go unnoticed; a drawback of traditional physical keys is that they can be copied secretly. A Physical Unclonable Function (PUF) is a physical object that cannot feasibly be copied because its manufacture inherently contains a large number of uncontrollable degrees of freedom. Making a sufficiently accurate clone or concocting a device that mimics its physical behavior is infeasible, though not theoretically impossible, given the properties of PUFs

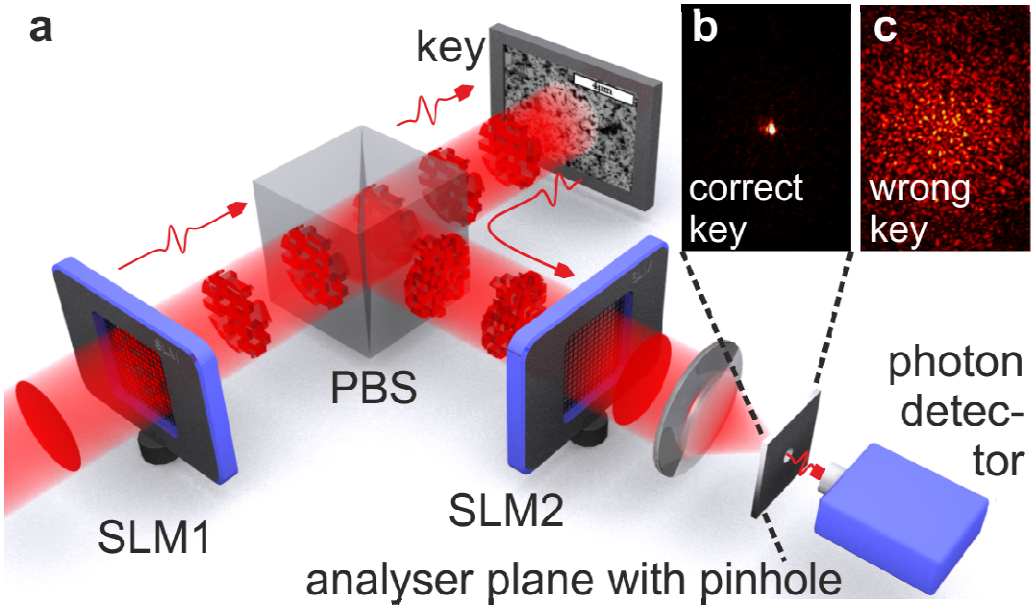

Fig. 2. Quantum-secure optical readout of a physical key. (a) Setup: A spatial light modulator (SLM1) creates the challenge by phase shaping a few-photon wavefront. In the experiment a 50x50 binary phase pattern is used with 0 and π phase delays. The challenge is sent to the ZnO key (scale bar is 4 µm) by a microscope objective (not shown). The response is coupled out by a polarizing beam splitter (PBS). The response is transformed back by SLM2 and then focused onto the analyzer plane. (b) Only if the key is the true unique key, the response has a bright spot in the center, holding ≈60% of the power in the image and allowing that fraction to pass a pinhole and land on a detector where photodetection clicks authenticate the key. (c) In case of a false key, the response in the analyzer plane is a random speckle pattern.

[1, 2]. See also the supplementary material. A PUF is a function in the sense that it reacts to a stimulus ("challenge") by giving a response. After manufacture there is a one-time characterization of the PUF in which its challenge-response behavior is stored in a database. The PUF (from this point referred to as the "key") can later be authenticated by comparing its response behavior to the database, see Fig. 1a.

When they are read out classically, PUFs are vulnerable to a class of attacks that we will refer to as digital emulation (Fig. 1b). Here the adversary has knowledge of the key's properties either from physical inspection of the key or by access to the challenge-response database. He intercepts challenges and is able to provide the correct responses by looking them up in his database. This is a highly relevant scenario as accessible databases are notoriously difficult to protect. So far the only defense against digital emulation is to deploy various sensors that try to detect if some form of spoofing is going on. This leads to an expensive arms race in which it is difficult to ascertain the level of security.

In this paper we present Quantum-Secure Authentication (QSA) of optical keys, a scheme with highly desirable properties: QSA
- uses a key that is infeasible to emulate physically.
- is unconditionally secure against digital emulation attacks.
- does not depend on secrecy of any stored data.
- does not depend on unproven mathematical assumptions.
- is straightforward to implement with current technology.

No comparable object authentication method currently exists. The use of quantum physics in QSA is inspired by quantum cryptography [3, 4, 5]. However, there are major differences. The aim of quantum cryptography is to generate a secret digital key known only to Alice and Bob, whereas QSA allows Alice to check if Bob possesses a unique physical object. Quantum cryptography requires the existence of an authenticated channel between Alice and Bob, typically based on a secret key that is shared beforehand [6]. In contrast, QSA needs only publicly available information; there are no secrets. See the supplementary material for an overview of cryptographic primitives and their properties.

Our implementation of QSA uses random scattering media as PUF [1, 7, 8]. The challenges are high-spatial-dimension states of light [9, 10, 11] with only a few photons. The response is speckle-like and depends strongly on the challenge and the positions of the scatterers. Due to the noncloning theorem [12] it is impossible for an adversary to fully determine the challenge and therefore to construct the expected response (Fig. 1c-d). The verifier can, however, easily verify the presence of the encoded information with an appropriate basis transformation, authenticating the key.

After its manufacture, the key is enrolled: the challenge-response pairs are measured with as much light as needed. Each of our challenges is described by a 50×50 binary matrix. Each element corresponds to a phase of either 0 or π. A spatial light modulator (SLM1) is used to transform the incoming plane wavefront into the desired challenge wavefront. The challenge is sent to the key and the reflected field is recorded in a phase-sensitive way. The challenge along with the corresponding response is stored in a challenge-response database. In our current implementation this requires 20 kB of computer memory per challenge-response pair which corresponds to 50 MB for a fully characterized key.

After enrolment, keys are authenticated using the setup illustrated in Fig. 2. Our light source is an attenuated laser beam chopped into 500 ns light pulses each containing n = 230±40 photons. Quantum readout of optical keys can be achieved with single or bi-photon states [13], squeezed states [14] or other fragile quantum states [15]. We use coherent states of light with low mean photon number [16], because in QSA they provide a similar security as other quantum states and are easier to implement in real-life applications. A challenge-response pair is constructed using

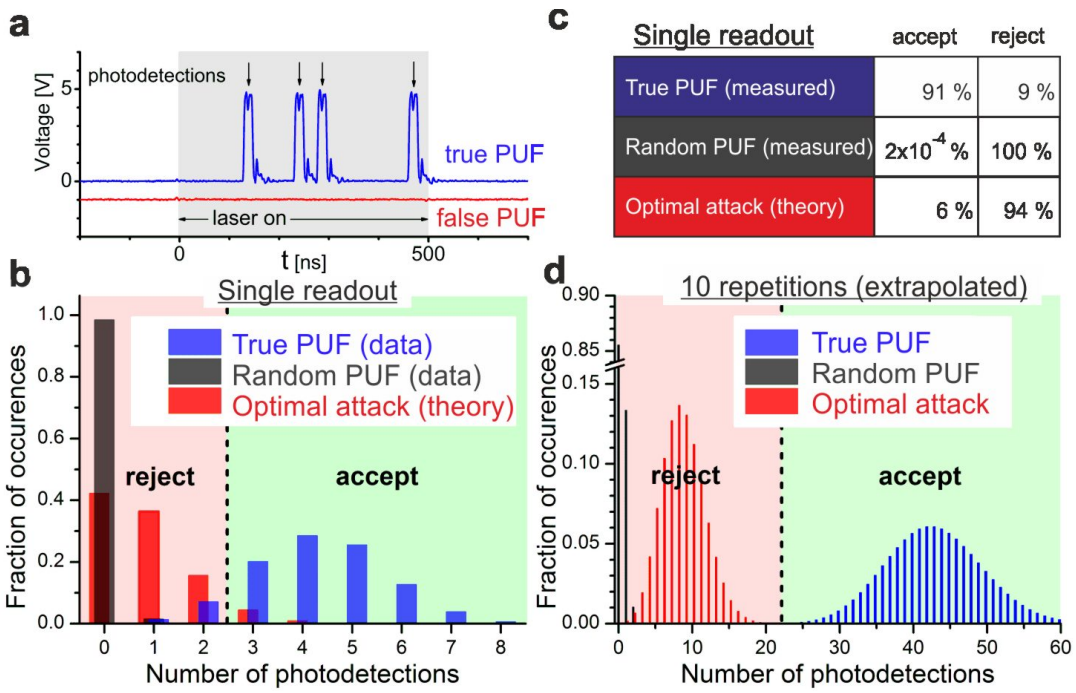

Fig. 3. Quantum-secure readout of an unclonable physical key (PUF), using challenge pulses with 230±40 photons distributed over 1100±200 modes. (a) Real-time examples for the true key (blue line) and a false key (red line, offset for clarity). (b) Measured number of photodetections in case of the true key, a random key (imitated by sending random challenges to the same key), and for an optimal attack given S=4. The threshold is chosen such that the false positive and negative probabilities are approximately equally small assuming an optimal attack. (c) Acceptance and rejection probabilities in case of the true key, a random key and in case of an optimal digital emulation attack. (d) Number of photodetections extrapolated to 10 repetitions: the false positive and false negative probabilities quickly decrease to order 0.01 %.

information from the database. SLM1 is used to shape the few-photon challenge wavefront, which is then sent to the key. The reflected wavefront is sent to SLM2, which adds to it the conjugate phase pattern of the expected response wavefront. Therefore, SLM2 transforms the reflected speckle field into a plane wave only when the response is correct. In case the response is wrong, SLM2 transforms the field into a completely different speckle field. When the response is correct, the lens positioned behind SLM2 focuses the plane wave to a point in the analyzer plane, as shown in Fig. 2b. A false key will result in a speckle on the analyzer plane as shown in Fig. 2c. Compared to the typical peak height in Fig. 2b of 1000 times the background, the loss of intensity in the center of Fig. 2c is dramatic. We spatially filter the field in the analyzer plane with a pinhole and image it onto a photon-counting detector. In Fig. 3a we show the typical photodetector signal for the correct response and for an incorrect response provided by the true and a false key, respectively. Only with the true key multiple photodetections are seen. After repeating the measurement 2000 times, Fig. 3b shows the histogram of the number of photodetections for the true key, resembling a Poissonian distribution with a mean of 4.3. Fig. 3b also shows the average histogram of photodetections when 5000 random challenges are sent to the key, with the key and SLM2 kept unchanged. This experiment gives an upper bound on the photodetections in case of an attack with a random key. This histogram resembles a Poissonian distribution with a mean of 0.016 photodetections. We can clearly discriminate between true and false keys.

In order to characterize the achievable security for one repetition of our readout, we introduce the quantum security parameter S,

$$S \equiv K/n, \qquad (1)$$

as the ratio of the number of controlled modes K and the average number of photons n in the challenge. The parameter K quantifies the dimensionality of the challenge space and is equal to the number of independent response wavefronts that are obtained by sending in different challenge wavefronts. It is well approximated by the number of speckles on the key illuminated by the challenge [17]. In our experiment we have K = 1100±200 and n = 230±40, yielding S = 5±1. Because a measurement of a photon can extract only a limited amount of information, a large S implies that the adversary can only obtain a small fraction of the information required to characterize the challenge. Therefore he cannot determine the correct response. An adversary who measures an optimal choice of field quadratures of the challenge cannot achieve a fidelity better than approximately [18]

$$F = F_{0K}/(S+1), \qquad (2)$$

where F is the fraction of photons detected by the verifier's hardware in case of an attack and F_{0K} is the fraction of photons detected when the response is correct. This result holds for $S > 1$ and $K >> 1$ and is in line with the intuition that a measurement of n photons can only provide information about n modes. Operating the readout in the regime $S > 1$ therefore gives the verifier an eminent security advantage which has its origin in the quantum character of light.

In the verification we aim to discriminate a correct key from an optimal attack. Given a conservative lower bound of S = 4, the number of photodetections on the single-photon detector in a single readout in case of an optimal (digital emulation) attack follows a Poissonian distribution with mean 0.86, as shown in Fig. 3b. Choosing a threshold of 3 or more photodetections for accepting the key, we find that the measured false reject ratio is 9%. In case of random challenges the false accept ratio is 1.7×10^{-4} % and the theoretical maximum false accept probability in case of

the digital emulation attack (Eq. 2) is 6% (Fig. 3c). The security improves exponentially by repeating the verification, every time choosing a different challenge and its corresponding SLM2 setting from the database. The individual photon counts are added, and a combined threshold is set. As illustrated in Fig. 3d, after 10 repetitions the false accept and false reject probabilities are of order 10^{-4}. As detailed in the supplementary information, after 20 repetitions they are both of order 10^{-9}. Thus, the false decision rates can be made negligible in a small number of repetitions.

In our implementation, the time for readout is limited to about 100 ms by the switching time of the SLM. Using faster micromirror-based SLMs [19, 20], the complete authentication protocol with 20 repetitions can be performed in less than a millisecond. The one-time enrolment of the key then takes on the order of a second. Quantum-secure authentication does not require any secret information and is therefore invulnerable to adversaries characterizing the properties of the key ("skimming"). Hence, QSA provides a practical way of realizing unprecedentedly secure authentication of IDs, credit cards, biometrics [21] and communication partners in quantum cryptography.

AUTHOR INFORMATION

All authors take full responsibility for the content of the paper. The authors declare competing financial interests: P.W.H.P., A.P.M. & B.S. have filed a patent application with the QSA concept. Correspondence should be addressed to P.W.H.P. (P.W.H.Pinkse@utwente.nl).

FUNDING INFORMATION

Stichting Fundamenteel Onderzoek der Materie (FOM)
Stichting STW
European Research Council (ERC) (279248)
Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) (VICI)

ACKNOWLEDGMENT

We thank J. Bertolotti, K.-J. Boller, G. Giedke, J. Herek, S.R. Huisman, T.J. Huisman, B. Jacobs, A. Lagendijk, G. Rempe, and W.L. Vos for support and discussions.

SUPPLEMENTAL DOCUMENTS

See Supplement 1 for supporting content.

REFERENCES

1. R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Physical one-way functions, Science **297**, 2026 (2002).
2. J. D. R. Buchanan, R. P. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, and M. T. Bryan, Forgery: 'fingerprinting' documents and packaging, Nature **436**, 475 (2005).
3. C. H. Bennett, G. Brassard, S. Breidbard, and S. Wiesner, Quantum cryptography, or unforgeable subway tokens, in Advances in Cryptology: Proceedings of CRYPTO '82, (Plenum, 1982), pp. 267–275.
4. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, IEEE International Conference on Computers, Systems and Signal Processing pp. 175–179 (1984).
5. B. Škoric, Quantum Readout of Physical Unclonable Functions, Int. J. Quant. Inf. **10**, 1250001-1–31 (2012).
6. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301–1350 (2009).
7. B. Škoric, P. Tuyls, and W. Ophey, Robust key extraction from physical uncloneable functions, in Applied Cryptography and Network Security (ACNS), vol. 3531 of *LNCS* (Springer, 2005), pp. 407 – 422.
8. P. Tuyls, B. Škoric, S. Stallinga, A. H. M. Akkermans, and W. Ophey, Information-theoretic security analysis of physical uncloneable functions, in 9th Conf. on Financial Cryptography and Data Security, A. S. Patrick and M. Yung, eds., vol. 3570 of *LNCS* (Springer, 2005), pp. 141–155.
9. S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, Quantum key distribution with higher-order alphabets using spatially encoded qudits, Phys. Rev. Lett. **96**, 090501 (2006).
10. V. D. Salakhutdinov, E. R. Eliel, and W. Löffler, Full-field quantum correlations of spatially entangled photons, Phys. Rev. Lett. **108**, 173604 (2012).
11. S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Quantum key distribution session with 16-dimensional photonic states, Sci. Rep. **3**, 2316 (2013).
12. W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature **299**, 802 – 803 (1982).
13. A. Peruzzo, M. Lobino, J. C. F. Matthews, N. Matsuda, A. Politi, K. Poulios, X.-Q. Zhou, Y. Lahini, N. Ismail, K. Wörhoff, Y. Bromberg, Y. Silberberg, M. G. Thompson, and J. L. O'Brien, Quantum walks of correlated photons, Science **329**, 1500–1503 (2010).
14. L.-A. Wu, H. J. Kimble, J. L. Hall, and H. Wu, Generation of squeezed states by parametric down conversion, Phys. Rev. Lett. **57**, 2520–2523 (1986).
15. D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information* (Springer, 2000).
16. P. W. H. Pinkse, T. Fischer, P. Maunz, and G. Rempe, Trapping an atom with single photons, Nature **404**, 365–368 (2000).
17. J. F. de Boer, M. C. W. van Rossum, M. P. van Albada, T. M. Nieuwenhuizen, and A. Lagendijk, Probability distribution of multiple scattered light measured in total transmission, Phys. Rev. Lett. **73**, 2567–2570 (1994).
18. B. Škoric, A. P. Mosk, and P. W. H. Pinkse, Security of quantum-readout PUFs against quadrature-based challenge-estimation attacks, Int. J. Quant. Inf. **11**, 1350041-1–15 (2013).
19. D. Akbulut, T. J. Huisman, E. G. van Putten, W. L. Vos, and A. P. Mosk, Focusing light through random photonic media by binary amplitude modulation, Opt. Express **19**, 4017–4029 (2011).
20. D. B. Conkey, A. M. Caravaca-Aguirre, and R. Piestun, High-speed scattering medium characterization with application to focusing light through turbid media, Opt. Express **20**, 1733–1740 (2012).
21. I. M. Vellekoop and A. P. Mosk, Focusing coherent light through opaque strongly scattering media, Opt. Lett. **32**, 2309 (2007).