Quantum-secure authentication of a physical unclonable key: supplementary material

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

¹Complex Photonic Systems (COPS), MESA+ Institute for Nanotechnology, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands

²Laser Physics and Nonlinear Optics (LPNO), MESA+ Institute for Nanotechnology, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands

³Eindhoven University of Technology, PO Box 513, 5600 MB Eindhoven, The Netherlands

*Corresponding author: p.w.h.pinkse@utwente.nl

Published 15 December 2014

This document provides supplementary information to “Quantum-secure authentication of a physical unclonable key,” <http://dx.doi.org/10.1364/optica.1.000421>. Detailed information on our experimental implementation is provided. We also place QSA into the cryptographic context, revealing its importance, and analyze the security of QSA against various types of attacks. Finally, we demonstrate exponential security gain by repeating the authentication procedure. © 2014 Optical Society of America

<http://dx.doi.org/10.1364/optica.1.000421.s001>

METHODS: SHAPING THE CHALLENGE AND RESPONSE WAVEFRONTS

Two halves (referred to as SLM1 and SLM2) of the same reflective Holoeye HEO 1080P phase-only spatial light modulator are used to shape challenge wavefronts and decode response wavefronts, respectively. We use 50x50 segments, each consisting of 16x16 pixels, to shape challenge wavefronts. Since the used beams are cylindrical, the corners of the 50x50 segments area are not illuminated, so that we effectively use $2500\pi/4 = 1963$ segments of SLM1. Each segment is set to a phase of either 0 or π , allowing a total of $2^{1963} = 10^{591}$ different challenges, of which 1963 are orthogonal. This number is slightly larger than the number of modes that is supported by the sample area that we illuminate, which is experimentally verified to be 1100 ± 200 . The challenge is focused onto the PUF using a 0.95 NA 63x Zeiss microscope objective. The response is collected using the same objective and measured in 130x130 segments using standard phase-shifting interferometry [1]. This data is used to find the phases of the response wavefront at the 130x130 corresponding segments with in total 800x800 pixels on SLM2. SLM2 is then set to flatten the phase of the response wavefront by adding the conjugate phase to the response wavefront.

THE KEY

Our PUF consists of zinc-oxide (ZnO) nanoparticles with an average grain size of 200 nm and air. The samples are created by

spray painting, using a method described in detail in [2]. The transport mean free path of such samples is $l_{tr} = 0.7 \pm 0.2 \mu\text{m}$. We use the key in reflection geometry because it is practical in real-life applications and collect the cross-polarized light to ensure multiple scattering in the bulk of the key. We illuminate a circular area with a diameter of approximately 15 μm on the surface of the key and collect light from an area with a diameter of approximately 25 μm .

CRYPTOGRAPHIC CONTEXT

In Table T1 an overview of important cryptographic methods is provided. Note that the overview is not limited to authentication methods. Unconditionally secure authentication methods have been proposed that use qubits as a key, e.g. quantum money and a number of methods based on quantum-entangled keys. These methods require quantum memory with long lifetimes that have not been achieved and are infeasible using current technology. Unconditionally secure classical authentication procedures, such as MACs (which are typically used in conjunction with QKD), are usually symmetric and require the distribution and secret storage of classical keys between every pair of parties that must be able to authenticate each other. Asymmetric classical protocols, such as RSA, are much more practical and are therefore widely used for establishing authentication, despite the fact that they are based on unproven mathematical assumptions and therefore not unconditionally secure. Besides that, also asymmetric protocols typically require secret storage of private keys. Classical

Method	Purpose	Technical Requirements	Security Assumptions		Status
			Physical	Mathematical	
BB84 [3]	Key exchange	Authenticated classical communication channel; single photons	none	none	Experimentally demonstrated, commercially available
SARG04 [4]	Key exchange	Authenticated classical communication channel; weak coherent pulses	none	none	Commercially available, more practical than BB84
Diffie-Hellman [5]	Key exchange	Authenticated classical communication channel	Quantum computers are infeasible to build	Discrete Logarithms are difficult to compute	Widely used
RSA [6]	Public-key crypto. Encryption; signatures		Quantum computers are infeasible to build	"RSA Assumption" ~Factoring a product of two large primes is difficult	Widely used
McEliece [7]	Public-key crypto. Encryption; signatures		none	Decoding an unknown linear code is difficult	Well studied; currently considered less practical than other asymmetric crypto
Message Authentication Codes (MACs) [8]	Message authentication	Short secret pre-shared key	none	none	Widely used
Mechanical key	Authentication; access control	Physical lock & key mechanism needed; key must be distributed first	Inferring key from lock is difficult	none	Ancient, still widely used
Quantum money [9, 10]	Anti-counterfeiting	Long-term storage and high fidelity initialization and readout of quantum memory	none	none	Proposed; Very difficult and expensive with current technology
Classical PUF authentication [11]	Object authentication, hands-on	Antispoofing detectors against emulation	PUF is physically unclonable	none	Experimentally demonstrated
QSA	Object authentication, hands-off	Fewer photons than modes	Lossless implementation of high-dimensional arbitrary unitaries is infeasible	none	New; Proven unconditionally secure against digital emulation [12]

Table S1. Overview of important cryptographic methods.

authentication which uses a Physical Unclonable Function (PUF) as a key has the advantages that it is practically impossible to copy the key and that it is not based on mathematical assumptions. However, every verifier must possess and be able to store secret information about the physical key. If the information about the key leaks, the key can be emulated using digital devices rendering the authentication protocol insecure. In QSA the key cannot be emulated, even if all information about the key is publicly known. QSA uses a key that cannot be copied or emulated, does not rely on stored secret information or unproven mathematical assumptions and is easy to implement with current technology. It is therefore the best object authentication method currently available.

SECURITY ANALYSIS

An adversary who does not have the PUF may attempt several attack strategies. We will address them here and show why they fail.

1) **Blinding attacks.** An additional detector which measures the total intensity outside the pinhole is sufficient to prevent false positive detections in case an adversary floods the system with light. In addition, flooding can be detected by including fake challenges, for which no photon detections are expected. The time needed for one repetition of the procedure is in practice limited only by the switching time of the SLM, on the order of 100 ms for the present SLM. Therefore there is ample room to randomly include fake challenges where (unknown to the adversary) no signal is expected. This also provides security against attacks that trigger the photodetector by non-optical means such as a beam of ionizing radiation. Note that the same requirements hold for QKD.

A QKD implementation has successfully been attacked by blinding the detectors [13].

2) A “**Digital Emulation Attack**”, in which the adversary attempts to measure the challenge and then estimates the response. As shown in [14] for single photon states and in [15] for quadrature measurements, this is doomed to fail. A newer result [12] shows that when a challenge consists of $n < K$ quanta in the same state, our scheme is secure against all challenge-estimation attacks. A quantitative example shows what the adversary can hope to achieve:

In our experiment the lower bound for the quantum security parameter S is 4. Assuming that the adversary has a perfect photon-counting or quadrature measuring camera, the expected squared inner product between the adversary’s best estimate and the correct challenge is equal to $1/(S+1) = 1/5$ [15]. He can therefore expect to obtain a number of photon clicks at the detector that is $1/5$ times the expected number of clicks with the correct challenge. The expected number of photons for the correct challenge is 4.3, so the attacker will obtain on average 0.8 photon clicks, well below the acceptance threshold of 3.

Experimentally we tested the scaling at the basis of this argument. We parameterize the challenge wavefronts by a K -dimensional complex vector C_0 . This C_0 is chosen by the verifier to yield the maximum light power in the focus behind SLM2 given the presence of the true PUF and the setting of SLM2. Now assume C_0 is replaced by another wavefront C_1 . We quantify the proximity of the challenge C_1 to the original challenge C_0 by the inner product $C_0 \cdot C_1 = \sum_{i=1..K} C_{0,i}^* \cdot C_{1,i}$, where the sum runs over the mode index. The fraction F of the light energy in the focus was experimentally found to scale as $F = 0.6 |C_0 \cdot C_1|^2$, confirming the scaling explained in [15].

3) Making an **exact physical copy** of the PUF. For our key this requires positioning millions of particles with the exact same high refractive index as zinc-oxide and with exactly the correct shapes at exactly the right positions on a nanometer scale. This is not possible with current technology and also not possible in the foreseeable future. To our knowledge no one even tried this.

4) Making a **passive optical device** that emulates the PUF’s physical challenge-response behavior. Since the PUF only realizes a complex linear transformation, one would be tempted to think that it is straightforward to make a passive optical device which does the same optical transformation as the PUF. It is not. The crucial point is that the adversary cannot know which challenge to expect, and therefore can only succeed if his passive optical device produces the correct response for a large fraction of the challenge space. In other words, he will have to emulate a large fraction of the optical properties of the PUF into his optical device. This comes close to making a copy of the PUF. A three-dimensional random scattering medium with front surface area A contains much more random information than can be encoded in a random scattering surface of the same area A . For our sample parameters, a single diffraction-limited spot focused on the surface of the PUF gives rise to a speckle pattern with a Gaussian envelope with a Full Width at Half Maximum (FWHM) of approximately $5\mu\text{m}$, containing about 10^2 speckles. When we illuminate the PUF with a random challenge, the illumination spot is much larger than a diffraction-

limited spot. The PUF is now seen to reflect a speckle pattern with a FWHM of about $15\mu\text{m}$, containing the equivalent of about 10^3 speckles. The reflection matrix describing the PUF is nonlocal (i.e., non-diagonal in any representation) as it connects surface points that are spatially separated by up to $5\mu\text{m}$. It is therefore impossible to emulate the PUF with a single scattering surface (e.g., that of an SLM), which would have a local reflection matrix.

An intriguing form of attack would be to make a PUF-emulating hologram into which a large portion of the PUF’s reflection matrix is written. Because of the low index of refraction contrast of photorefractive materials, on the order of 0.02 to 0.1 [16], such a hologram must be significantly larger than the true PUF to obtain sufficient reflectivity. Therefore, this form of attack can be easily foiled using a light source with a coherence length of the order of $30\mu\text{m}$, on the order of the average path length photons travel in the PUF. The average optical path in the hologram is much longer than the coherence length so that no speckle pattern will form.

Another intriguing form of attack would be by means of a PUF-emulating nanophotonic network. Since in principle every passive linear optical network can be emulated by a sufficiently complex network of, e.g., beam splitters [17], this is in theory possible. Work by, e.g., Miller et al. [18, 19] show the concepts needed to make such a network. However, an adversary who wants to emulate the PUF functionality needs to program a passive optical device with K modes and K^2 connecting elements while keeping all the involved path lengths equal to within the coherence length.

Despite the huge efforts already spent in making linear optical networks for linear optical quantum computing and quantum simulation, state of the art networks have at maximum on the order of 10 connected beam splitters [20] and losses of 0.2 dB per element for waveguide-based beam splitters [21]. Recently larger networks have been built [22], but they only work because of the high tolerance against phase errors possible in the functionality of the realized phased arrays, which does not apply for a PUF emulator. Alternative photonic-crystal-based networks could be smaller [23], but the corresponding losses are even higher. Hence, the extension to 106 connected nodes with overall losses of less than 10dB, extreme phase sensitivity and simultaneously keeping the differential path lengths to within 30 micrometer is still far out of reach of technology. If possible at all in future, it would require 10^6 optical elements each with a loss of less than 0.01 dB and a tremendous effort to emulate a single PUF.

A note about the scaling: For an K -mode PUF, the adversary needs to make a passive optical device with K^2 connecting elements. In our demonstration we have used on the order of 10^3 modes, but increasing this to 10^5 seems entirely feasible with present technology, given the availability of megapixel SLMs. With the state-of-the-art beam splitters [21], the required network of in the order of 10^{10} optical elements would have a loss of 20000dB and cover an area of the order of 1m^2 .

5) A **quantum-computer** can emulate our key only if it can perform arbitrary unitary operations on K -dimensional quantum states of light with low losses. The technologically most feasible way to do this seems to be through a tunable low-loss K -dimensional optical device. Such a device is at least as difficult to build as a passive low-loss K -dimensional optical device. This is infeasible for the same arguments presented in point 4) [24].

Fig. S1. Probability of a false positive (acceptance of a challenge estimation attack) and a false negative decision (rejection of a correct PUF) as a function of the security parameter S and the number of repetitions (rounds). The plot is made by varying n and choosing the optimal threshold, while keeping $K = 1062$.

6) **Hybrid strategies** that mix (complex) passive elements and measuring devices. In the proof of the security against challenge-estimation attacks [12] no assumptions are made about the basis in which the adversary measures the challenge. Even if the adversary can program an arbitrary linear transformation before the measurement, he cannot breach the QSA scheme by estimating the challenge. In fact it is always better for the adversary to use his linear transformation capabilities directly on the challenge state as in attack 4.

REPETITION FOR EXPONENTIAL SECURITY GAIN

Fig. S1 shows the calculated probability of false-positive and false-negative decisions as a function of S and the number of repetitions, with the number of modes K kept constant. For each point in Fig. S1 the threshold was chosen in the minimum between the photon detection distributions obtained with the true PUF and the one calculated for the optimal challenge estimation attack. This leads to false positive and false negative probabilities that are approximately equally small. At a moderate S the probability of an erroneous decision is already of order 10^{-4} after 10 repetitions. At high S it takes more repetitions to rule out incorrect decisions since high S (at fixed K) implies a low photon number n . Since the threshold can only be taken at an integer number of photons, one may notice some quantization steps. For larger numbers of repetitions the probability of an incorrect decision is reduced exponentially and can hence be made arbitrarily small.

REFERENCES

- [1] I. Yamaguchi and T. Zhang, Phase-shifting digital holography, *Opt. Lett.* **22**, 1268–1270 (1997).
- [2] E. G. van Putten, Disorder-enhanced imaging with spatially controlled light, Ph.D. thesis, University of Twente (2011).
- [3] 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).
- [4] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, *Phys. Rev. Lett.* **92**, 057901 (2004).
- [5] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Inf. Theory* **IT-22**, 644–654 (1976).
- [6] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21**, 120–126 (1978).
- [7] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, *Deep Space Network Progress Report* **44**, 114–116 (1978).
- [8] C. Paar and J. Pelzl, Message authentication codes (macs), in *Understanding Cryptography*, (Springer Berlin Heidelberg, 2010), pp. 319–330.
- [9] S. J. Wiesner, Conjugate coding, *ACM SIGACT News* **15**, 78–88 (1983).
- [10] F. Pastawskia, N. Y. Yaob, L. Jiang, M. D. Lukinb, and J. I. Cirac, Unforgeable noise-tolerant quantum tokens, *PNAS* **109**, 16079–16082 (2012).
- [11] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Physical one-way functions, *Science* **297**, 2026 (2002).
- [12] B. Škoric, Security analysis of quantum-readout PUFs in the case of challenge-estimation attacks, Submitted, <http://eprint.iacr.org/2013/479> (2013).
- [13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nature Photon.* **4**, 686–689 (2010).
- [14] B. Škoric, Quantum Readout of Physical Unclonable Functions, *Int. J. Quant. Inf.* **10**, 1250001–1 – 125001–31 (2012).
- [15] 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 – 1350041–15 (2013).
- [16] S. C. Barden, J. A. Arns, and W. S. Colburn, Volume-phase holographic gratings and their potential for astronomical applications, *Proc. SPIE* **3355**, 866 (1998).
- [17] M. Reck, A. Zeilinger, H. Bernstein, and P. Bertani, Experimental realization of any discrete unitary operator, *Phys. Rev. Lett.* **73**, 58–61 (1994).
- [18] D. A. B. Miller, All linear optical devices are mode converters, *Opt. Expr.* **20**, 23985 (2012).
- [19] D. A. B. Miller, Self-configuring universal linear optical component, *Phot. Research* **1**, 1–15 (2013).
- [20] P. J. Shadbolt, M. R. Verde, A. Peruzzo, A. Politi, A. Laing, M. Lobino, J. C. F. Matthews, M. G. Thompson, and J. L. O’Brien, Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit, *Nat. Phot.* **6**, 45–49 (2011).

- [21] D. D. John, M. J. R. Heck, J. F. Bauters, R. Moreira, J. S. Barton, J. E. Bowers, and D. J. Blumenthal, Multilayer platform for ultra-low-loss waveguide applications, *IEEE Photon. Technol. Lett.* **24**, 876–878 (2012).
- [22] J. Sun, E. Timurdogan, A. Yaacobi, E. S. Hosseini, and M. R. Watts, Large-scale nanophotonic phased array, *Nature* **493**, 195–199 (2013).
- [23] Y. Jiao, S. Fan, and D. A. B. Miller, Demonstration of systematic photonic crystal device design and optimization by low-rank adjustments: an extremely compact mode separator, *Opt. Lett.* **30**, 141–143 (2005).
- [24] D. P. DiVincenzo, Towards control of large-scale quantum computing, *Science* **334**, 50 (2011).