Effects of Kerr nonlinearity in physical unclonable functions

Georgios M. Nikolopoulos

1 Institute of Electronic Structure and Laser, Foundation for Research and Technology-Hellas, GR-70013 Heraklion, Greece

(Dated: November 22, 2022)

We address the question of whether the presence of Kerr nonlinearity in multiple-scattering optical media offers any advantage with respect to the design of physical unclonable functions. Our results suggest that under certain conditions, nonlinear physical unclonable functions can be more robust against the potential cloning of the medium, relative to their linear counterparts that have been exploited in the context of various cryptographic applications.

I. INTRODUCTION

Physical unclonable functions (PUFs) based on optical multiple scattering media have attracted considerable attention over the last decades, mainly because they are considered to pave the way for the development of novel more robust cryptographic protocols [1–16]. The optical multiple scattering medium essentially serves as a token, and the internal disorder renders its cloning a formidable technological challenge. At the same time, the response of the token to optical challenges is a complex pattern (speckle), which depends strongly on the internal disorder of the token as well as on the challenge. Different challenges pertain to different parameters of the incoming light, e.g., intensity, point and angle of incidence, wavelength or combinations thereof [1, 4, 8, 9, 12]. Formally speaking, the optical response of the token involves a large number of optical modes, and the speckle is essentially the result of interference of many paths that lead to a particular mode at the output [17]. In the framework of cryptographic applications, the speckle can be used raw as a fingerprint [4, 18], or it can be processed classically to yield a random numerical key [1, 9]. In any case, the sensitivity of the speckle to the potential cloning of the token, essentially determines the resistance of the cryptographic protocol under consideration against related attacks. A useful protocol should allow one to distinguish between a token and its clones, by comparing their responses to the same challenge (raw speckles or numerical keys).

All of the aforementioned studies rely on the use of a linear multiple scattering medium as token, which results in a linear relationship between the recorded intensity at a particular point at the output plane, and the electric field at the input plane. This linear relationship may render certain cryptographic protocols vulnerable to cloning attacks, provided the attacker has access to the raw speckle images that are produced by the setup for the particular token. It has been conjectured [1, 18] that such attacks can be thwarted by using nonlinear multiple scattering tokens, thereby breaking the linear dependence of the speckle on the electric field at the input. To the best of our knowledge, this conjecture remains an open question in the field up to date.

In this work, our aim is to address for the first time this open question, by investigating whether and under what conditions multiple scattering media with Kerr nonlinearity can offer some advantage over their linear counterparts, with respect to their robustness against cloning. To this end we focus on the speckle that is produced by a reference token, and we study its correlation to the speckles of different random clone tokens. Given the high sensitivity of the speckle to the internal disorder, we adopt a generic model for the (non)linear token, which allows us to reach definite general conclusions through the statistical analysis of the data. Our results suggest that, in general, speckles produced by tokens with focusing nonlinearity can be more robust to cloning, than speckles produced by linear tokens, or tokens with defocusing nonlinearity.

II. FORMALISM

In the diffusive limit [5–7, 17], the problem can be formulated in terms of $\mathcal{M}$ input and $\mathcal{M}$ output transverse spatial modes. For monochromatic laser light at wavelength $\lambda$, the electric field at the $m$th output mode is given by [19–22]

$$E_{m}^{(\text{out})}(\lambda) = \sum_{j=1}^{\mathcal{M}} \mathcal{T}_{m,j}^{(\lambda)} E_{j}^{(\text{in})}(\lambda),$$

(1)

where $\mathcal{T}_{m,j}^{(\lambda)}$ is the element of the multi-spectral transmission matrix linking the $m$th output mode, to the $j$th input mode, for light at wavelength $\lambda$. In the notation adopted throughout this work, the $i$th input and output transverse modes are associated with spatial coordinates $(x_i, y_i) := \rho_i$ at the input and output planes, which are located at $z = z_1$ and $z = z_2$, respectively. Hence, $E_{m}^{(\text{out})}(\lambda)$ and $E_{j}^{(\text{in})}(\lambda)$ are abbreviations to $E(\rho_m, z_2; \lambda)$ and $E(\rho_j, z_1; \lambda)$, respectively. For a given wavelength, the elements of the transmission matrix $\{\mathcal{T}_{m,j}^{(\lambda)}\}$ depend strongly on the realization of the disorder in the token, and can be treated as independent complex Gaussian random variables, with zero mean and variance given by $(1 − l/L)/\mathcal{M}$, where $L$ is the thickness of the token and $l \ll L$ is the mean free path. For a token with spectral correlation bandwidth $\delta \lambda_c$, the transmission matrices at two different wavelengths $\lambda_1$ and $\lambda_2$, with $|\lambda_1 − \lambda_2| > \delta \lambda_c$, can be treated as independent random matrices, thereby
The bandwidth (FWHM) of the pulse $\lambda$ pulse of bandwidth $\Delta \lambda$ degrees of freedom, corresponding to wavelengths electric field at frequency $c$.

For a token with spectral correlation bandwidth laser pulse from a multiple scattering nonlinear token. (a) under consideration, for the scattering of a Fourier-limited laser pulse from a linear multiple-scattering token, and the propagation is treated as a sequential process, pertaining to the scattering from a linear multiple-scattering token, and the propagation of the resulting fully-developed monochromatic speckle in a nonlinear homogeneous medium.

yielding uncorrelated monochromatic speckle patterns at the two wavelengths $[19–22]$. Equation (1) refers to the scattering of monochromatic light with wavelength $\lambda$ from a disordered linear token. To exploit the nonlinearity of a medium, one typically needs ultrashort laser pulses, so that to reach high intensities without damaging the medium. The spectrum of an ultrashort laser pulse involves many frequencies, and the power spectral density defines the power in each wavelength of the spectrum. Neglecting the spatial dependence of the field for a moment, for a Gaussian pulse of the form $E(t) = \sqrt{T_0} \exp[-t^2/2\tau^2] \exp(-12\pi v_0 t)$, the electric field at frequency $c = \lambda \nu$ is given by

$$E(\nu) = \sqrt{2\pi I_0 \tau} \exp \left[-2\pi^2 \tau^2 (\nu - \nu_0)^2 \right]. \quad (2)$$

The bandwidth (FWHM) of the pulse $|E(\nu)|^2 = \Delta \nu_p = \sqrt{\ln(2)} / \pi \tau$. $I_0$ and $T = 2\sqrt{\ln(2)} \tau$ denote the peak intensity (units of W/cm$^2$) and the FWHM of the pulse in time domain. The bandwidth can be expressed in terms of the wavelength using the relation $\Delta \lambda_p = \lambda_0^2 \Delta \nu_p / c$.

The spectral density is $S(\nu) = |E(\nu)|^2$, and $S(\nu) d\nu$ gives the fluence (energy per area) for frequencies between $\nu - d\nu/2$ and $\nu + d\nu/2$. Hence, the intensity carried by frequencies within the spectral correlation bandwidth $\delta \nu_c$ around $\nu$, can be approximated by

$$J(\nu) := \frac{S(\nu) \delta \nu_c}{\mathcal{N}} = \frac{I_0}{\mathcal{N}} \exp \left[-4\pi^2 \tau^2 (\nu - \nu_0)^2 \right], \quad (3)$$

where $\mathcal{N} \equiv \Delta \nu_p / \delta \nu_c$ represents the spectral degrees of freedom i.e., the number of spectral channels. When a pulse of bandwidth $\Delta \nu_p$ propagates through a multiple-scattering random token with spectral correlation bandwidth $\delta \nu_c$, the generated speckle is essentially a superposition of $\mathcal{N}$ uncorrelated monochromatic speckle patters [see Fig. 1(a)], with the exponent in Eq. (3) determining the weight of the different contributions $[19–22]$.

Let $E(\rho, z_2 ; \lambda_i)$ denote the two-dimensional speckle field at the output plane, for the $i$th component pertaining to wavefront shaping techniques in the presence of disorder and nonlinearity $[23]$. In the discretized model under consideration, the total speckle field at wavelength $\lambda_i$ is given by

$$E_m^{(\text{out})}(\lambda_i) \equiv E(\rho, z_2 ; \lambda_i) = \sqrt{J(\nu_i)} \Psi(\rho, z_2 ; \lambda_i), \quad (4a)$$

where

$$\Psi(\rho, z_2 ; \lambda_i) = \frac{1}{\sqrt{\mathcal{N}}} \sum_{j=1}^{\mathcal{M}} T_{m,j}^{(\lambda_i)} \quad (4b)$$

captures the effect of the internal random disorder of the token on the spatial profile of the electric field at the particular wavelength (see Ref. [5] and references therein). In the discretized model under consideration, the total speckle field at wavelength $\lambda_i$ is given by

$$E(\rho, z_2 ; \lambda_i) \equiv \{ E_m^{(\text{out})}(\lambda_i) : 1 \leq m \leq \mathcal{M} \}, \quad (4c)$$

where $E_m^{(\text{out})}(\lambda_i)$ is given by Eqs. (4a) and (4b).

What remains to be done, is the inclusion of nonlinearity in our model for the randomly disordered token. In general, the propagation of light in a nonlinear inhomogeneous medium is a rather challenging and time consuming task, because one has to know the details of scatterers (including position, size, and shape). Even if one models successfully a particular token with well-defined disorder, it is not clear at all what the results that will be obtained may imply for other tokens pertaining to different independent realizations of random disorder. Given that our task here is to investigate whether the nonlinearity can make speckle patterns more resilient to cloning, we will adopt a generic model for the token, consisting of a thin linear multiple-scattering medium, which is followed by a homogeneous layer with Kerr-type nonlinearity (see Fig. 1). A similar model has been used successfully in studies related to wavefront shaping techniques in the presence of disorder and nonlinearity $[23]$.

The speckle field $E(\rho, z_2 ; \lambda_i)$ for the $i$th spectral component at the output of the linear random medium is given by Eqs. (4). The propagation of this monochromatic speckle field in the nonlinear medium of thickness $L$, will be modeled by the following nonlinear wave equation $[24]$.\[ \text{FIG. 1. Schematic representation of the theoretical model under consideration, for the scattering of a Fourier-limited laser pulse from a multiple scattering nonlinear token. (a) For a token with spectral correlation bandwidth $\delta \lambda_c$ and a pulse of bandwidth $\Delta \lambda_p$, there are $\mathcal{N} \approx \Delta \lambda_p / \delta \lambda_c$ spectral degrees of freedom, corresponding to wavelengths $\lambda_0, \lambda_1, \ldots$. Different spectral components pertain to independent random monochromatic transmission matrices, and they give rise to uncorrelated monochromatic speckles. (b,c) The scattering of the $i$th spectral component from the nonlinear random token is treated as a sequential process, pertaining to the scattering from a linear multiple-scattering token, and the propagation of the resulting fully-developed monochromatic speckle in a nonlinear homogeneous medium.} \]
\[
\frac{1}{2k_i n_0} \nabla_2^2 \Psi(r; \lambda_1) + \frac{1}{2k_i n_0} \nabla_2^2 \Psi(r; \lambda_1) + k_i n_2 J(\nu_i) |\Psi(r; \lambda_1)|^2 \Psi(r; \lambda_1) = 0,
\]
(5)

FIG. 2. Speckle fields after propagation in a medium with (a,d) defocusing nonlinearity \(n_2 = -3 \times 10^{-16} \text{cm}^2/\text{W}\), (b,e) zero nonlinearity, and (c,f) focusing nonlinearity \(n_2 = 3 \times 10^{-16} \text{cm}^2/\text{W}\). Note the different color scales as one goes from negative to positive \(n_2\). Parameters: \(L = 100 \lambda_0\), \(\lambda_0 = 800\text{nm}\), \(I_0 = 2.6 \times 10^{13} \text{W/cm}^2\), \(T = 100\text{fs}\), \(n_0 = 1.47\), \(\mathcal{N} = 3\) (a-c) and \(\mathcal{N} = 5\) (d-f). In all of the cases, uniform illumination has been considered at the input.

where \(\nabla_2^2 \equiv \frac{\partial^2}{\partial z^2} + \frac{\partial^2}{\partial r^2}\), \(r \equiv (\rho, z)\), \(k_i = 2\pi/\lambda_i\), \(n_0\) is the linear refractive index, and the nonlinear refractive index (Kerr nonlinearity) is denoted by \(n_2\) and it is measured in \(\text{cm}^2/\text{W}\). This equation treats each spectral component independently, while propagation takes place on a discretized space, with the initial condition \(\Psi(\rho, z_0; \lambda_1) = \{\Psi(\rho_m, z_0; \lambda_1) : 1 \leq m \leq \mathcal{N}\}\), where \(\Psi(\rho_m, z_0; \lambda_1)\) is given by Eq. (4b). Note also that different spectral components experience different nonlinearities, and thus different dynamics, due to the intensity \(J(\nu_i)\). Throughout this work we are interested in short propagation lengths \(z_3 = L \lesssim 1\text{mm}\), so that the token is sufficiently thin for cryptographic applications (e.g., engineering of all-optical smart cards) [1, 8]. As a result, in Eq. (5) we neglect effects of dispersion, self-steepening and space-time coupling, assuming pulses with duration such that \(2\pi c T \gg \lambda_0\) [24]. For observation times long compared to the coherence time of the scattered light (\(\sim 1/\delta \nu_i\)), the intensity of the scattered light at the \(n\)th output mode after the nonlinear medium (plane at \(z = z_3\)) can be approximated by [17]

\[
I_m^{(\text{tot})} \simeq \sum_i J(\lambda_i) |\Psi(\rho_m, z_3; \lambda_i)|^2.
\]

(6)

We also neglect effects of free-space propagation, as they are expected to contribute equally in the speckles of the actual token and a clone. Without loss of generality, we consider odd values for \(\mathcal{N}\), with the index \(i \in \left[-(\mathcal{N} - 1)/2,(\mathcal{N} + 1)/2\right]\), and \(i = 0\) refers to the central wavelength \(\lambda_0 = c/\nu_0\).

Using the above sequential model for the nonlinear multiple-scattering token, we have performed a number of simulations, in order to gain insight into the role of the nonlinearity on the speckle that is produced by such a medium, as well as on the sensitivity of the speckle on the cloning of the token. Equation (5) was solved by means of the split-step Fourier method [25]. The reference token is described by a multi-spectral transmission matrix \(T_{\text{ref}} := \{T_{m,j}^{(\lambda_i)} : 1 \leq m, j \leq \mathcal{N}; -\mathcal{N}/2 \leq i \leq (\mathcal{N}+1)/2\}\). The matrix involves \([T_{\text{ref}}] = \mathcal{M} \times \mathcal{N} \times \mathcal{N}\) independent complex Gaussian random variables, with zero mean and variance \(\mathcal{M}^{-1}(1-1/L)\) (e.g., see [5, 17, 19–22] and references therein). The wavelength for the \(i\)th spectral degree of freedom is given by \(\lambda_i = \lambda_0 + i\delta \lambda_c\).

For a fixed multi-spectral transmission matrix, we generate random clones along the lines described in Refs. [5]. More precisely, the multi-spectral transmission matrix of a \(Q\)-close clone is obtained from \(T_{\text{ref}}\), by choosing new random values for \([Q[T_{\text{ref}}]]\) randomly chosen elements. The parameter \(Q\) is essentially associated with the quality of the cloning, with \(Q = 0\) and 1, corresponding to perfect and fully randomized clone, respectively.

III. RESULTS

Let us begin with the effect of Kerr nonlinearity on the speckle generated by a given token. The main findings are summarized in Fig. 2, which shows the speckles for a token with defocusing nonlinearity \((n_2 < 0)\), zero nonlinearity \((n_2 = 0)\), and focusing nonlinearity \((n_2 > 0)\). For defocusing nonlinearity the scattered light is distributed among a larger number of output modes, relative to the linear case. By contrast, for focusing nonlinearity the scattered light tends to concentrate within a small number of output modes, thereby leading to a small number of very bright spots in the pattern (note the different color scales in the density plots). These findings were present for all of the simulations we have performed, and the location as well as the intensities of these bright spots depend on the realization of the random disorder in the token. Moreover, we have found that the concentration of scattered light for focusing nonlinearity becomes weaker for increasing number of spectral degrees of freedom. This was to be expected, because according to Eqs. (3) and (5), effects of nonlinearity become weaker as we increase \(\mathcal{N}\). Analogous behavior is found as we decrease \(I_0\), for fixed \(\mathcal{N}\).

Typical PUF-based cryptographic protocols which use optical tokens exploit one way or another the strong dependence of the speckle image on the random internal disorder of the token as well as on the parameters of the input light [1, 4, 8, 9, 12]. In either case, the robustness of a protocol against the cloning of the token is mainly
A sample of our main findings is depicted in Fig. 3, where we show diagrams for a fixed reference token, as a function of the cloning factor \( Q \), for various combinations of parameters. As expected, the correlation decreases with increasing \( Q \), because the quality of the clones decreases. Moreover, we find a large overlap between the red and green boxes for all of the parameters, which suggests that the performance of the linear token (red boxes) is the same as (if not slightly better than) the performance of a token with defocusing nonlinearity (green boxes). By contrast, in the case of focusing nonlinearity (blue boxes), the recorded correlation coefficients tend to be smaller than the corresponding coefficients for a linear token (red boxes) with the same characteristics. In particular, it is worth noting that there is negligible overlap between the blue and red boxes in all of the cases shown in the figure, and it is only the maximum recorded values which have some overlap with the red boxes. Comparing Fig. 3(a) to 3(b) we find that the advantage of tokens with focusing nonlinearity is getting weaker for increasing values of \( N \), i.e., increasing number of spectral channels. However, this advantage tends to be restored partially if we increase the intensity of the input light [compare Fig. 3(b) to 3(d)]. Comparing Fig. 3(a) to 3(c) we also find that by increasing the thickness of the token, while keeping all other parameters constant, the advantage of the tokens with focusing nonlinearity is more pronounced, while at the same time we find a larger spread of the estimated correlation coefficients. Finally, as a result of Eq. (3), all of these findings do not seem to depend on the actual pulse duration \( T \), but rather on the number of spectral channels \( N \).

**IV. CONCLUDING REMARKS**

We have investigated how Kerr nonlinearity affects the sensitivity of a speckle to the cloning of the involved multiple-scattering optical token. Our results suggest that for focusing nonlinearity the correlation between the speckles of a reference token and its clones can be smaller than the ones for zero or defocusing nonlinearity. Hence, PUFs that rely on tokens with focusing nonlinearity are expected to be more robust against cloning, in the sense that they can distinguish easier between a reference token and its clones, with high probability.

This advantage is getting more pronounced for tokens with spectral correlation bandwidth equal or comparable to the bandwidth of the pulse, as well as for increasing thickness of the token, and/or increasing peak intensity of the pulse. The spectral correlation bandwidth of a token decreases quadratically with its thickness \( L \) [19–22], whereas for a given pulse duration the peak intensity should be below the damage threshold for the medium. For our purposes, we had to vary the Kerr nonlinearity \( n_2 \) in our simulations, while keeping all other parameters fixed, which would not have been possible if the present work had been restricted to a specific material. However,
for the focusing nonlinearity, where we have the most interesting findings, the main parameters pertain to fused silica [24, 27, 28]. This is a well-studied material in the literature, while it has been also discussed in the framework of PUFs [4]. The present findings are expected also to be present for other highly scattering media typically used in connection with PUFs, such as TiO$_2$ and ZnO [1, 2, 19–22].

The present work may serve as a benchmark for any future work on nonlinear PUFs. The identification of appropriate materials and systems for the validation of the present findings in the framework of experiments is an open question which deserves the attention of the community in the field.

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Science 297, 2026 (2002).
[2] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, Optica 1, 421 (2014).
[3] Uppu, R. et al. Asymmetric cryptography with physical unclonable keys. Quantum Sci. Technol. 4, 045011 (2019).
[4] H. Zhang, and S. Tzortzakis, Appl. Phys. Lett. 108, 211107 (2016). H. Zhang, D. Di Battista, G. Zacharakis, and S. Tzortzakis, Appl. Phys. Lett. 109, 039901 (2016).
[5] G. M. Nikolopoulos and E. Diamanti, Sci. Rep. 7, 46047 (2017).
[6] G. M. Nikolopoulos, Phys. Rev. A 97, 012324 (2018).
[7] L. Fladung, G.M. Nikolopoulos, G. Alber, M. Fischlin, Cryptography 3, 25 (2019).
[8] G. M. Nikolopoulos, Photonics 8, 289 (2021).
[9] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chainiotis, T. Nikas and D. Syvridis, Sci. Rep. 8, 9653 (2018).
[10] G. Gianfelici, H. Kampermann, and D. Bruss, Phys. Rev. A 101, 042337 (2020).
[11] P. Wang, F. Chen, D. Li, S. Sun, F. Huang, T. Zhang, Q. Li, K. Chen, Y. Wan, X. Leng, Y. Yao, Phys. Rev. App. 16, 054025 (2021).
[12] R. Horstmayer, B. Judkewitz, I. M. Vellekoop, S. Asawaworrarit, and C. Yan, Sci. Rep. 3, 3543 (2013).
[13] 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, Nature 436, 475 (2005).
[14] C. H. Yeh, P. Y. Sung, C. H. Kuo, and R. N. Yeh, Opt. Express 20, 24382-24393 (2012).
[15] G.M. Nikolopoulos, Opt. Express 27, 29367-29379 (2019).
[16] S. Chowdhury, A. Covic, R. Y. Acharya, S. Dupee, F. Ganji and D. Forte, J. Cryptogr. Eng. (2021). https://doi.org/10.1007/s13389-021-00255-w.
[17] J. C. Dainty, Laser Speckle and Related Phenomena (Springer Verlag, 1975).
[18] U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, and C. Jirauschek, https://eprint.iacr.org/2013/215.
[19] D. Andreoli, G. Volpe, S. Popoff, O. Katz, S. Grésillon, and S. Gigan, Sci. Rep. 5, 10347 (2015).
[20] M. Mounaix, D. Andreoli, H. Defienne, G. Volpe, O. Katz, S. Grésillon, and S. Gigan, Phys. Rev. Lett. 116, 253901 (2016).
[21] F. van Beijnum, E. G. van Putten, A. Lagendijk, and A. P. Mosk, Opt. Lett. 36, 373 (2011).
[22] E. Small, O. Katz, Y. Guan, and Y. Silberberg, Opt. Lett. 37, 3429 (2012).
[23] H. Frostig, E. Small, A. Daniel, P. OuLevey, S. Derevyanko, and Y. Silberberg, Optica 4, 1073 (2017).
[24] R. W. Boyd, Nonlinear Optics (Academic Press 2008).
[25] K. Okamoto, Fundamentals of Optical Waveguides (Academic Press 2006). Chap. 7.
[26] S. M. Ross, Introduction to Probability and Statistics for Engineers and Scientists (Academic Press 2014). Chap. 2.
[27] B. Chimier, U. Utéza, N. Sanner, M. Sentis, T. Itina, P. Lassonde, F. Légaré, F. Vidal, and J. C. Kieffer, Phys. Rev. B 84, 094104 (2011).
[28] T. Q. Jia, H. X. Chen, M. Huang, F. L. Zhao, X. X. Li, S. Z. Xu, H. Y. Sun, D. H. Feng, C. B. Li, X. F. Wang, R. X. Li, Z. Z. Xu, X. K. He, and H. Kuroda, Phys. Rev. B 73, 054105 (2006).