An optical authentication system based on imaging of excitation-selected lanthanide luminescence

Miguel R. Carro-Temboury,* Riikka Arppe,* Tom Vosch,† Thomas Just Sørensen†

Secure data encryption relies heavily on one-way functions, and copy protection relies on features that are difficult to reproduce. We present an optical authentication system based on lanthanide luminescence from physical one-way functions or physical unclonable functions (PUFs). They cannot be reproduced and thus enable unbreakable encryption. Further, PUFs will prevent counterfeiting if tags with unique PUFs are grafted onto products. We have developed an authentication system that comprises a hardware reader, image analysis, and authentication software and physical keys that we demonstrate as an anticounterfeiting system. The physical keys are PUFs made from random patterns of taggants in polymer films on glass that can be imaged following selected excitation of particular lanthanide(III) ions doped into the individual taggants. This form of excitation-selected imaging ensures that using at least two lanthanide(III) ion dopants, the random patterns cannot be copied, because the excitation selection will fail when using any other emitter. With the developed reader and software, the random patterns are read and digitized, which allows a digital pattern to be stored. This digital pattern or digital key can be used to authenticate the physical key in anticounterfeiting or to encrypt any message. The PUF key was produced with a staggering nominal encoding capacity of \(7^{3600}\). Although the encoding capacity of the realized authentication system reduces to \(6 \times 10^{104}\), it is more than sufficient to completely preclude counterfeiting of products.

INTRODUCTION

Secure communication and authentication of products pose major societal challenges. An optical authentication system based on physical unclonable functions (PUFs) may provide the solution. Using PUFs in an anticounterfeiting system will address the billion-dollar economic losses imposed by counterfeiting (1–3) and can potentially save lives if used to guarantee the authenticity of medicine (4–8). The randomness inherent in PUFs can be used for unbreakable public key encryption (9). The decryption key cannot be guessed, and because a PUF, by definition, cannot be copied, only the key holder may decipher the encrypted message. Here, we present a new optical authentication system based on PUF patterns of lanthanide-doped zeolite taggants in polymer films that are read using excitation-selected imaging of the lanthanide dopants. The system is demonstrated in the context of an anticounterfeiting system.

In anticounterfeiting, the established technologies all use tags that are the result of a deterministic process (10, 11). As a consequence, they all rely on restricted access to the ink or printing technology, which makes them susceptible to counterfeiting—even DNA tags are readily read and copied if a suitable incentive is present (10, 12). The highly secure encoding method presented here is different in nature because it uses statistically unique physical keys based on PUFs (13), which are based on nondeterministic, random features of the anticounterfeiting tag, making it impossible to duplicate even by the manufacturer, let alone the counterfeiters (13–21).

The presented authentication system is based on physical keys made from physical one-way functions better known as PUFs (14, 22–24). We make these unique random patterns in a stochastic process, where taggants supported in a polymer thin film create a random pattern on the substrate of choice (16). By imaging a selected area of the thin film, a unique physical key is created. Such a PUF key can be tagged onto every single blister pack of pills or designer hand bag, and each product will feature a unique key. All physical keys are read, and their digital keys are stored in a database, thereby allowing each product to be uniquely identified throughout the supply chain.

The physical key is read using three, energetically closely spaced, blue laser lines, each selectively exciting different lanthanide ions. The emission following the selective excitation is used to image the key. The control of excitation light rather than emission light resolves the different taggants used to form the unique pattern that is the PUF key. Upon each excitation wavelength, a different and unique random pattern emerges, and the digitized and combined pattern forms the unique digital key. This new method of reading the random pattern is different from known methods of optical multiplexing, which are read by analyzing the color composition of the emitted light (12, 25). When this new readout mode is combined with unique parameters for digitizing and comparing readouts, we have created a tamper-proof optical authentication system.

Here, we demonstrate the excitation-resolved optical authentication concept for anticounterfeiting using physical keys made from zeolites doped with europium(III), terbium(III), or dysprosium(III) ions immobilized in a polyvinyl alcohol (PVA) thin film (see Fig. 1). We exploit the narrow absorption lines of the lanthanides and lanthanide centered emission to resolve up to three binary responses, depending on the presence or absence of a given lanthanide in a given pixel (see Fig. 1). By using three lanthanide(III) ions, we achieve very high encoding capacities. The encoding capacity of our system (\(c^p\)) is defined by the number of possible responses exhibited by a random pattern (see Fig. 1). With three lanthanide(III) ions, we can achieve seven different responses, which we visualize using a standard color scheme (\(c = 7\); RGB-CMYK).

In the examples presented here, we image an area of 60 pixels × 60 pixels \((p = 3600)\), which gives a maximal encoding capacity of the proposed authentication system of \(7^{3600}\). Because the encoding capacity of the random pattern is infinite for all practical purposes, there will never be two identical keys, ensuring that the physical keys are impossible to copy.

Multiplexing with a matrix of graphical or optical codes is a known concept for anticounterfeiting, tracking, and authentication purposes...
An anticonteering or authentication system based on PUFs consists of several elements. First, there is the physical key—here, a physical random pattern or PUF key—that is read using a specific hardware. The readout—here, an image—is digitized using a specific set of parameters creating the digital key, which is stored in a database. For anticonteering, the process is performed at the point of origin of the product, and subsequent authentication then relies on rereading the physical key and converting the readout to a new digital key. This new digital key is then authenticated by comparing it to the stored digital key using dedicated software.

The physical key
We made the physical key by producing a random pattern formed from taggants made from zeolite 5A [Linde Type A (LTA)], where the counterions (Ca²⁺) have been exchanged by the relevant lanthanide(III) ions (see the Supplementary Materials for details) (38). The taggants are thus zeolites (microporous crystalline aluminosilicates) exchanged using an aqueous solutions of europium(III), terbium(III), and dysprosium(III) cations. The zeolites used are cubes with 2- to 4-µm edges (Fig. 1E). The three different taggants (Eu@LTA, Tb@LTA, and Dy@LTA) were mixed in water containing 3% (w/v) PVA [molecular weight (M_w) = 13,000 to 23,000], and the resulting suspension was spin-coated onto a microscope glass slide to form the random patterns with the properties represented in cartoon form in Fig. 1. The random patterns can be embossed in steel or leather, or the doped zeolites can be encased in glass. The stability of the random pattern and, thus, the physical key is determined by the substrate material used. Here, PVA on glass was used, where PVA is the limiting material. PVA is stable up to 200°C but is water-soluble. We did not observe any issues with stability of the physical keys over 18 months at ambient conditions but realize that a glass support may be too fragile and that water-soluble glue is not ideal for real-world applications. A selection of other tags on paper and glass are shown in the Supplementary Materials.

The readout
When the zeolites are doped with lanthanide ions, the narrow absorption and emission bands resulting from lanthanide centered emission can both be used to resolve the optical response (Fig. 2). Emission-resolved imaging allows the three taggants to be differentiated using their unique emission spectra (Fig. 2A), whereas the excitation-resolved imaging differentiates them on the basis of unique absorption bands (Fig. 2B). In the latter case, the emission can be recorded from the lanthanide-loaded zeolites following excitation using a wavelength that addresses an absorption band of the targeted lanthanide ion (Fig. 2B); each of the selected lanthanide ions—Eu³⁺, Tb³⁺, and Dy³⁺—may be addressed individually (Fig. 2B), which allows the emission of each lanthanide ion to be resolved despite overlapping emission spectra (Fig. 2A). The two methods have very different requirements when designing hardware for optical authentication of the random pattern: Emission-resolved method requires either a spectrometer or a filter-based detection, whereas for excitation-resolved method, only a single long-pass filter and a total intensity detector are enough to collect the emission, because only one lanthanide emits upon one selected excitation line. Further, if a filter-based hardware unit is used for emission-resolved readout, then it may be emulated using other emitters, whereas the excitation-resolved readout cannot because no other emitters have the narrow absorption bands exhibited by the lanthanide(III) ions. Thus, the excitation-selected readout adds an additional layer of security to the physical key.
Whereas emission-resolved imaging is well established, excitation-resolved imaging using close-lying absorption bands is not. To demonstrate that we are achieving excitation-resolved images, we used physical keys made using single taggants (Eu@LTA, Tb@LTA, or Dy@LTA). The taggants can be imaged following excitation at 450 nm for dysprosium, 465 nm for europium, and 488 nm for terbium. The images and spectra in Fig. 3 were recorded using a charge-coupled device (CCD)-based spectrometer (39, 40), and the emission spectra were recorded for each pixel. The narrow barcode-like emission lines leave no doubt as to the nature of the emitting species. The dysprosium emission is significantly weaker than that of europium or terbium but still detectable. The weaker signal of Dy³⁺ is predictable and due to nonradiative deactivation by high-energy O–H oscillators of water molecules trapped in the zeolite (33).

To further validate the excitation-selected imaging, we imaged the same physical key containing all three Ln taggants using spectrally resolved imaging (CCD-based spectrometer as detector) and excitation-resolved imaging [avalanche photodiode (APD) detector with a 532-nm long-pass filter]. The result is shown in Fig. 4, where the thin film was imaged using 465-, 488-, and 450-nm excitation wavelengths individually or all simultaneously. The emission spectra of each pixel were recorded and used to verify the origin of the recorded photons following excitation at the selected wavelength (see fig. S9). Cursory inspection of Fig. 4 shows that excitation-resolved imaging using lanthanide centered emission is as effective a tool as spectrally resolved imaging, demonstrating that either method outlined in Fig. 2 may be used to resolve the binary response of a random pattern formed by these taggants (see the Supplementary Materials for details). The images in Fig. 4 show that the dysprosium centered emission is very weak when compared to the terbium and europium centered emissions; too weak to perform well in fluorescence microscopy but sufficient to be used in excitation-selected multiplexing (see below).

More than one lanthanide has to be used in the PUF key because the method relies on the fact that the image cannot be emulated by other means. The narrow energy range used for excitation is deliberate, because all other emitters would be excited by all three excitation lines. Thus, an anticounterfeiting tag cannot be copied by bleaching of organic dyes or clever positioning of quantum dots, because these will emit in all channels. The lanthanide ions used here give very good contrast in excitation-selected imaging, particularly the combination using only dysprosium, 465 nm (Eu³⁺), G to 488 nm (Tb³⁺), and B to 450 nm (Dy³⁺). Thus, the three digitized images can be combined into one RGB digital key where the absence of a signal corresponds to black (R = 0, G = 0, and B = 0 [000]), whereas a signal in only one of the channels gives rise to the primary RGB colors (red [100], green [010], and blue [001]).

The encoding capacity of the resulting authentication systems (16). The multiple responses add complexity in the digital key because reading the physical key requires that three images are recorded using three different, energetically closely spaced, excitation wavelengths. Here, 465-, 488-, and 450-nm laser lines were used. The total intensity of each pixel is then recorded for each excitation channel and digitized in a binary form. The three images are then combined, where a color is designated for pixels where emission is detected following excitation using a specific laser line. We assigned letters/colors to pixels where emission is detected following excitation by a specific laser line: R to 465 nm (Eu³⁺), G to 488 nm (Tb³⁺), and B to 450 nm (Dy³⁺). Thus, the three digitized images can be combined into one RGB digital key where the absence of a signal corresponds to black (R = 0, G = 0, and B = 0 [000]), whereas a signal in only one of the channels gives rise to the primary RGB colors (red [100], green [010], and blue [001]).

The digital key
By increasing the number of possible responses in each pixel, excitation selection gives a higher spatial density encoding capacity than scattering-based methods, thus removing a possible limitation imposed by a low encoding capacity of the resulting authentication systems (16). The multiple responses add complexity in the digital key because reading the physical key requires that three images are recorded using three different, energetically closely spaced, excitation wavelengths. Here, 465-, 488-, and 450-nm laser lines were used. The total intensity of each pixel is then recorded for each excitation channel and digitized in a binary form. The three images are then combined, where a color is designated for pixels where emission is detected following excitation using a specific laser line. We assigned letters/colors to pixels where emission is detected following excitation by a specific laser line: R to 465 nm (Eu³⁺), G to 488 nm (Tb³⁺), and B to 450 nm (Dy³⁺). Thus, the three digitized images can be combined into one RGB digital key where the absence of a signal corresponds to black (R = 0, G = 0, and B = 0 [000]), whereas a signal in only one of the channels gives rise to the primary RGB colors (red [100], green [010], and blue [001]).

The encoding capacity of the resulting authentication systems (16). The multiple responses add complexity in the digital key because reading the physical key requires that three images are recorded using three different, energetically closely spaced, excitation wavelengths. Here, 465-, 488-, and 450-nm laser lines were used. The total intensity of each pixel is then recorded for each excitation channel and digitized in a binary form. The three images are then combined, where a color is designated for pixels where emission is detected following excitation using a specific laser line. We assigned letters/colors to pixels where emission is detected following excitation by a specific laser line: R to 465 nm (Eu³⁺), G to 488 nm (Tb³⁺), and B to 450 nm (Dy³⁺). Thus, the three digitized images can be combined into one RGB digital key where the absence of a signal corresponds to black (R = 0, G = 0, and B = 0 [000]), whereas a signal in only one of the channels gives rise to the primary RGB colors (red [100], green [010], and blue [001]).

The encoding capacity of the resulting authentication systems (16). The multiple responses add complexity in the digital key because reading the physical key requires that three images are recorded using three different, energetically closely spaced, excitation wavelengths. Here, 465-, 488-, and 450-nm laser lines were used. The total intensity of each pixel is then recorded for each excitation channel and digitized in a binary form. The three images are then combined, where a color is designated for pixels where emission is detected following excitation using a specific laser line. We assigned letters/colors to pixels where emission is detected following excitation by a specific laser line: R to 465 nm (Eu³⁺), G to 488 nm (Tb³⁺), and B to 450 nm (Dy³⁺). Thus, the three digitized images can be combined into one RGB digital key where the absence of a signal corresponds to black (R = 0, G = 0, and B = 0 [000]), whereas a signal in only one of the channels gives rise to the primary RGB colors (red [100], green [010], and blue [001]). Because the encoding capacity is defined by the number of pixels imaged (p) and the number of possible responses, this digital key has an encoding capacity of 4p (see the Supplementary Materials for details). By including colocalization in the digitization procedure, the number of responses can be increased to seven with an encoding capacity of 7p. This can be achieved by decreasing the resolution in the image so that more than one taggant is present in each pixel or by including more than one lanthanide(III) ion in each taggant. When including colocalization, the colors are still defined by the number of excitation wavelengths that give rise to a signal, but now, signals in more than one channel are included as additional colors: yellow [110], magenta [101], and cyan [011]. White [111], with emission detected in all three channels, will not occur because of the noise reduction protocol used in the digitization procedure (see the Supplementary Materials). If the resolution or...
Fig. 3. Emission-resolved images of zeolites doped with europium(III), terbium(III), and dysprosium(III) ions. (A) Emission spectra of Eu$^{3+}$-, Tb$^{3+}$-, and Dy$^{3+}$-doped zeolites recorded upon 465-, 488-, or 450-nm excitation, respectively, from a single pixel with the CCD-based spectrometer system using 6.4- to 7.2-$\mu$W excitation power and 20-s integration time. (B) The corresponding confocal fluorescence image of Eu$^{3+}$-, Tb$^{3+}$-, and Dy$^{3+}$-doped zeolites (10 $\mu$m $\times$ 10 $\mu$m, 50 pixels $\times$ 50 pixels, and 1- to 2-s integration time). Intensities in Tb$^{3+}$ and Dy$^{3+}$ images are multiplied by the factor indicated.

taggant loading does not require the digitization to include colocalization, then only combinations involving the pure RGB colors will be present in the images even when the digitization software allow for colocalization.

The exponential law dictates that the encoding capacity quickly rises toward infinity as a function of the number of pixels with both four and seven responses. Because our method grants full control over the size of the imaged area, only data storage and the computing power needed to perform the point-by-point comparison of two digital keys limit the maximum encoding capacity. The actual encoding capacity is determined by the full system. As an example, we use the RGB-CMYK approach with seven responses and an RGB+K approach with four responses and 60 pixels $\times$ 60 pixels images resulting in maximum encoding capacities of $7^{6000}$ and $4^{3600}$, respectively. Primarily due to the physical dimensions of the taggants, the actual encoding capacity is reduced to $6 \times 10^{104}$ and $2.1 \times 10^{103}$ (see the Supplementary Materials). If higher encoding capacities are required, then these can be achieved by imaging larger areas or by matching the physical dimensions of the taggants to the pixel size used. By optimizing the full system, the number of responses becomes less important. For example, using only europium and terbium with taggants matched to the pixel size of a video graphics array (VGA) image sensor will result in an actual encoding capacity of $4^{307200}$.

To form the digital key from the raw readout, we used a process involving several steps (see Fig. 5). Several sets of parameters are used in the digitization process. These add another layer of security to the authentication system, because authentication can only be achieved by using the correct parameters. If one parameter is changed, then a different digital key is produced. The input is the three raw images of total emission intensity versus pixel recorded following excitation at one of the three selected wavelengths. Each data set is individually noise-reduced using a relative and an absolute threshold value resulting in three noise-reduced images (Fig. 5A). Below the thresholds, the intensity of pixels is forced to be zero: The relative threshold sets all the pixels of an image that are below a certain percent of the maximum intensity of the image to zero, and the absolute threshold sets all the pixels with less than a certain number of counts per second to zero. The latter avoids considering noise as signal if the image has a poor signal-to-noise ratio. The noise reduction reduces the encoding capacity but is crucial for a proper digitization (see the Supplementary Materials).

In the next step of the process, the three noise-reduced image sets are considered together in a digitization process that results in three binary images (Fig. 5B). The color condition [RGB] of a given pixel depends on the intensity determined in the pixel in all three noise-reduced images and is locked to a hardware-specific level of cross-talk between the laser lines. The cross-talk limits are unique for a given system and add another layer of protection. In the authentication system demonstrated here, we require that the corresponding signal in the Tb$^{3+}$ channel (G) AND/OR Dy$^{3+}$ channel (B) is less than 0.1 times the intensity of the Eu$^{3+}$ channel (R) for a pixel to be [1**]. Otherwise, the pixel is considered [0**]. If we require both conditions to be true (AND operator), then we are using the RGB+K approach, whereas the OR operator allows for colocalization, and is used in the RGB-CMYK approach. By merging the three digitized images, the digital key (Fig. 5C) is created. Note that pixels with colocalization appear black in the RGB+K approach. The file sizes of the corresponding digital keys in either scheme are only 21.09 kilobytes, and the size of the digital file depends only on the number of pixels in the data set (see the Supplementary Materials).

**Authentication**

The full authentication system is outlined in Fig. 6. To realize the example in Fig. 6, we suggest that the taggants are included in the polymer used for the blister pack; thus, the physical key is simply a selected area of the pack. The full authentication system contains three levels of security: the physical key, the digitization software including noise reduction and cross-talk definitions, and the acceptance criteria for comparing two digital keys from the same physical key. The acceptance criteria will depend strongly on the reader hardware. When using our setup and the RGB+K scheme, we suggest an acceptance criterion, where an error margin of 40% in each channel is tolerated. This gives rise to a false-positive probability of $3.6 \times 10^{-8}$, which is acceptable for all practical purposes (see the Supplementary Materials). The error margin allows small differences between the individual readers used at separate points in the supply chain. Because the read time is short and digital processing is fast, the false positives can be fully eliminated...
by performing the authentication operation in triplicate. Note that the acceptance criteria must be tailored to the actual anticounterfeiting tags and hardware used. To demonstrate the authentication system as an anticounterfeiting measure, we have implemented and tested one set of two acceptance criteria. Figure 6 summarizes the requirements of an anticounterfeiting system, where products must be authenticated at all points in the supply chain (41, 42), and includes an example where we have challenged our system with two products with an authentic and a fake anticounterfeiting tag. The PUF tag was registered at the point of origin by reading the physical key and storing a copy of the digital key. The digital key was then used to authenticate the physical key, which was reread four times to illustrate the different points in the supply chain. Physical keys that did not match the digital key were not authenticated (see the Supplementary Materials).

In summary, we have demonstrated an optical authentication system, exploiting the unique optical properties of trivalent lanthanide ions, PUFs, state-of-the-art optical technology, and cryptographic approaches. The optical authentication system can be used for unbreakable encryption but was demonstrated for anticounterfeiting purposes. When used as an anticounterfeiting system, the manufacturer tags a product with a unique physical key and records the digital key corresponding to the PUF key in a read-only public database. The number of unique physical keys is near infinite, and coincidentally identical anticounterfeiting tags will not occur. In addition, because the PUF key is unique and cannot be copied, there is no need for secrecy. Merchants and end users can then verify the authenticity of the product using shop-based or personal readers that, knowing the type of product, look up the digital key in the corresponding manufacturers’ section of the database. The large parameter space of the randomly generated PUF keys made from affordable materials enables a simple approach to authentication of consumer goods, medicine, passports, or electronic components subjected to counterfeiting. The robust physical keys can either be grafted onto the product or supplied as thin films. The fundamental properties of the lanthanide ions exploited in excitation-selected imaging cannot be emulated, the structures cannot be printed, and product keys are registered by trusted manufacturers. All three facts would individually make the method tamper-proof. The economic benefit in upholding trademark and intellectual property rights is substantial, and using the excitation-selected imaging of lanthanide-doped zeolites to ensure the authenticity of medicine will save lives.

MATERIALS AND METHODS

Tb(III) acetate hydrate (99.9%) and Eu(III) acetate hydrate (99.9%) were purchased from Sigma-Aldrich, and Dy(III) acetate hydrate (99.9%) was purchased from Strem Chemicals. LTA zeolites were a gift from UOP Antwerpen PVA (98% hydrolyzed; average Mw, 13,000 to 23,000) was purchased from Sigma-Aldrich. All chemicals were used as received. Milli-Q water was used to prepare all reagents.

Loading of zeolites with lanthanides

To exchange the Ca2+ cations within the pores and cavities of the LTA zeolite with Ln3+ cations (Dy3+, Eu3+, or Tb3+), 200 mg of LTA was mixed with 800 μl of 0.25 M Ln3+ acetate hydrate dissolved in Milli-Q water and mixed overnight (IKA Vortex 3) at room temperature. The Ln3+-exchanged zeolites were recovered and washed three times with 1 ml of Milli-Q water by centrifugation (1000 rpm, 2 min; Force 12, Denver Instrument) and then dispersed into 1 ml of Milli-Q water. For the model system validation, 1 mg of each Ln3+-doped zeolites in 3% (w/v) PVA/water was spin-coated on a 22-mm × 22-mm microscope glass slide (Menzel-Gläser no. 1.5) for ~1 min to form a thin film.

Fig. 6. An optical authentication system based on imaging of excitation-selected lanthanide luminescence used as an anticounterfeiting system. A product is authenticated using a physical key and readers at critical points in the supply chain. The physical key is read, digitized (second to fourth read) (B to D), and matched to the digital key (first read) (A) that was stored in the cloud by the manufacturer. Counterfeit products can enter at all points in the supply chain but will be eliminated by trusted retailers (green arrow). Counterfeits may be introduced directly to the end user (red arrow), who then must authenticate the product using a personal reader (fifth read (E) or random pattern (F)) or consult a trusted retailer.
**Supplementary Materials**

Supporting Information for this article is available at http://advances.sciencemag.org/cgi/content/full/4/1/e1701384/DC1.

Validation of the physical key.

**References and Notes**

1. R. R. Gosline, Forbes, 12 February 2010; http://forbes.com/2010/02/11/luxury-goods-counterfeit-fakes-chanel-gucci-cmo-network-renee-richardson-gosline.html.

2. J. Rogn, The Daily Beast, 12 February 2014; http://thedailybeast.com/articles/2014/02/12/the-u-s-tells-you-where-to-buy-the-best-fake-designer-handbags-pirated-movies-and-counterfeit-fakes-chanel-gucci-cmo-network-renee-richardson-gosline.html.

3. Organization for Economic Cooperation and Development (OECD)/European Union Intellectual Property Office, Trade in counterfeit and pirated goods: Mapping the economic impact (OECD Publishing, 2016).
1. U.S. Food and Drug Administration, Counterfeit Medicine (U.S. Department of Health and Human Services, 2016; http://FDA.gov/Drugs/ResourcesForYou/Consumers/BuyingUsingMedicineSafely/CounterfeitMedicine/default.htm)

2. T. K. Mackey, B. A. Liang, The global counterfeit drug trade: Patient safety and public health risks. J. Pharm. Sci. 100, 4571–4579 (2011).

3. P. N. Newton, M. D. Green, F. M. Fernández, N. P. J. Day, N. J. White, Counterfeit anti-infective drugs. Lancet Infect. Dis. 6, 602–613 (2006).

4. P. Althous, Counterfeit pharmaceuticals: Murder by medicine. Nature 434, 132–136 (2005).

5. C. Sheridan, Bad medicine. Nat. Biotechnol. 25, 707–709 (2007).

6. R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit, C. Yang, Physical unclonable features. Nat. Rev. Chem. 5, 5581 (2008).

7. R. Arppe, T. J. Sørensen, Physical unclonable functions generated through chemical self-assembly. Adv. Mater. 28, 2083–2089 (2015).

8. R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical one-way functions. Adv. Funct. Mater. 24, 5029–5036 (2014).

9. J. Andres, R. D. Hersch, J.-E. Moser, A.-S. Chauvin, A new anti-counterfeiting feature relying on invisible luminescent full color images printed with lanthanide-based inks. Adv. Funct. Mater. 29, 2026–2030 (2002).

10. F. A. Smith, P. Patton, S. E. Skrabalak, Plasmonic nanopillars as a physically unclonable function for responsive anti-counterfeit nanofingerprints. Adv. Funct. Mater. 26, 1315–1321 (2016).

11. R. Arppe, T. J. Sørensen, Physical unclonable functions generated through chemical methods for anti-counterfeiting. Nat. Rev. Chem. 1, 0031 (2017).

12. Y. Geng, J. H. Noh, I. Drevansek-Olenik, R. Rupp, G. Lenzini, J. P. F. Lagerwall, High-fidelity spherical cholesteric liquid crystal Bragg reflectors generating unclonable patterns for secure authentication. Sci. Rep. 6, 26840 (2016).

13. Z. Hu, J. M. M. Lobez Comeras, H. Park, J. Tang, A. Afzali, G. S. Tulevski, J. B. Hannon, M. Lieh, S.-J. Han, Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. Nat. Nanotechnol. 11, 559–565 (2016).

14. J. Kim, J. M. Yun, J. Jung, H. Song, J.-B. Kim, H. Hee, Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires. Nanotechnology 25, 155303 (2014).

15. L. Tian, K-K. Liu, M. Fei, S. Tadepalli, S. Cao, J. A. Geldmeyer, V. V. Tsukruk, S. Singamaneni, Plasmonic nanogels for unclonable optical tagging. ACS Appl. Mater. Interfaces 8, 4031–4041 (2016).

16. T. A. W. Wolterink, R. Uppu, G. Cistis, W. L. Vos, K-J. Boller, P. W. H. Pinkse, Programmable two-photon quantum interference in 105 channels in opaque scattering media. Phys. Rev. A 93, 053817 (2016).

17. J. D. R. Buchanan, R. P. Cowburn, A-V. Jaoueve, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, M. T. Bryan, Forgyree: “Fingerprinting” documents and packaging. Nature 436, 475 (2005).

18. C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, Physical unclonable functions and applications: A tutorial. Proc. IEEE 102, 1126–1141 (2014).

19. Y. Zheng, C. Jiang, S. H. Ng, Y. Lu, F. Han, U. Bach, J. J. Gooding, Unclonable plasmonic security labels achieved by shadow-mask-lithography-assisted self-assembly. Adv. Mater. 28, 2330–2336 (2016).

20. M. Wang, B. Duong, H. Fenniri, M. Su, Nanomaterial-based barcodes. Nanoscale 7, 11240–11247 (2015).

21. J. M. Meruga, W. M. Cross, P. S. May, Q. Lui, G. A. Crawford, J. I. Kellar, Security printing of covert quick response codes using upconverting nanoparticle inks. Nanotechnology 23, 359201 (2012).

22. Y. Lu, J. Zhao, R. Zhang, Y. Liu, D. Liu, E. M. Goldys, X. Yang, P. Xi, A. Sunna, J. Lu, Y. Shi, R. C. Leif, Y. Hoo, J. Shen, J. A. Piper, J. P. Robinson, D. Jin, Tunable lifetime multiplexing using lanthanide nanocrystals. Nat. Photonics 8, 32–36 (2014).

23. D. J. Chandler, B. A. Lambert, J. J. Reber, S. L. Phipps, “Precision fluorescently dyed particles and methods of making and using,” U.S. Patent 6,514,295 (2003).

24. S. Fournier-Bidoz, T. L. Jennings, J. M. Klostranec, W. Fung, A. Rhee, D. Li, W. C. W. Chan, Facile and rapid one-step mass preparation of quantum-dot barcodes. Angew. Chem. Int. Ed. 47, 5577–5581 (2008).

25. X.-H. Ji, N.-G. Zhang, W. Cheng, F. Guo, W. Liu, S.-S. Guo, Z.-K. He, X.-Z. Zhao, Integrated parallel microfluidic device for simultaneous preparation of multiplex optical-encoded microbeads with distinct quantum dot barcodes. J. Mater. Chem. 21, 13380–13387 (2011).

26. Q. Wang, Y. Liu, C. Lin, H. Yan, Layer-by-layer growth of superparamagnetic, fluorescent barcode nanoparticles. Nanotechnology 18, 405604 (2007).

27. M. Han, X. Gao, J. Z. Su, S. Nie, Quantum-dot-tagged microbeads for multiplexed optical coding of biomolecules. Nat. Biotechnol. 19, 631–635 (2001).

28. J.-C. Bünzli, S. V. Eliseeva, In Lanthanide Luminescence: Photophysical, Analytical and Biological Aspects, P. Hänninen, H. Hämä, Eds. (Springer-Verlag, 2010), vol. 7, pp. 1–46.

29. K. A. White, D. A. Chengelis, K. Gogick, J. Stehman, N. L. Rossi, S. Petoud, Near-infrared luminescent lanthanide MOF barcodes. J. Am. Chem. Soc. 131, 18069–18071 (2009).

30. M. J. Dejnkea, A. Streltsov, S. Pal, A. G. Frutos, C. L. Powell, K. Yost, P. K. Yuen, U. Müller, J. Lahiri, Rare earth-doped glass microparticles. Nat. Protoc. 6, 3543 (2011).

31. Q. Wang, Y. Liu, C. Lin, H. Yan, Layer-by-layer growth of superparamagnetic, fluorescent barcode nanoparticles. Nanotechnology 18, 405604 (2007).

32. M. Lehtonen, in Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks, C. D. Ranasinghe, Z. Q. Sheng, S. Zeedaly, Eds. (Springer-Verlag, 2011), pp. 331–351.

33. L. Li, Technology designed to combat fakes in the global supply chain. Bus. Horiz. 56, 167–177 (2013).

Acknowledgments: We thank UOP Antwerpen for donating the LTA zeolites.

Funding: This work was supported by the Villum Fonden (grant no. 14922), Villum Fonden block stipends, bioSYNERGY University of Copenhagen’s Excellence Programme for Interdisciplinary Research, the “Center for Synthetic Biology” at Copenhagen University funded by the Danish Ministry of Higher Education and Science (grant no. 09-065274), and the Danish Council of Independent Research (grant no. DFF-1323-00352). Author contributions: M.R.C.-T. and R.A. manufactured the PUF-tags and performed the experiments and the initial data analysis. M.R.C.-T. wrote the software and did the mathematical modeling. R.A. and T.J.S. wrote the first draft of the paper. T.V. and T.J.S. came up with the idea and supervised the experiments. All authors contributed to the final version of the manuscript. Competing interests: All authors of this paper are inventors of a patent application related to this work that has been filed with the European Patent Office by the University of Copenhagen (application no. EP17152670.0, filed 23 January 2017). Data and materials availability: All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper may be requested from the authors.

Submitted 10 May 2017
Accepted 15 December 2017
Published 26 January 2018

Citation: M. R. Carro-Temboury, R. Arppe, T. Vosch, T. J. Sørensen, An optical authentication system based on imaging of excitation-selected lanthanide luminescence. Sci. Adv. 4, e1701384 (2018).
An optical authentication system based on imaging of excitation-selected lanthanide luminescence
Miguel R. Carro-Temboury, Riikka Arppe, Tom Vosch and Thomas Just Sørensen

Sci Adv 4 (1), e1701384.
DOI: 10.1126/sciadv.1701384

http://advances.sciencemag.org/content/4/1/e1701384

http://advances.sciencemag.org/content/suppl/2018/01/22/4.1.e1701384.DC1

This article cites 33 articles, 1 of which you can access for free
http://advances.sciencemag.org/content/4/1/e1701384#BIBL

http://www.sciencemag.org/help/reprints-and-permissions

Use of this article is subject to the Terms of Service