Physically secure and fully reconfigurable data storage using optical scattering

Roarke Horstmeyer*‡, Sid Assawaworrarit*‡, Ulrich Rührmair†, and Changhuei Yang*

*Department of Electrical Engineering
California Institute of Technology, Pasadena, CA 91125, USA
Email: roarke@caltech.edu

† Technische Universität München, Arcisstr. 21, 80333 München, Germany
Email: ruehrmair@ilo.de

‡ Authors contributed equally to this work

***Abstract*—This paper presents an optical method of storing random cryptographic keys within a reconfigurable volume of polymer-dispersed liquid crystal (PDLC). We suggest a PDLC-based device that functions as an integrated optical physical unclonable function (PUF). Our device can selectively access a dense set (up to 10 Gb/mm^3 in theory) of non-electronically saved random bits. Furthermore, this optical PUF can fully erase and transform these bits into a new random configuration in less than one second, via a simple *electrical* signal. When a short voltage spike is applied across the PDLC film interface, its optical scattering potential completely decorrelates. We confirm this phenomenon with detailed experiments on a proof-of-concept device, thereby suggesting the security use of a new class of optical materials as (i) securely and efficiently reconfigurable PUFs, and (ii) an erasable storage medium for random cryptographic keys. Our work can eventually help address the challenge of quickly and completely erasing sensitive digital electronic memory and/or key material. It also establishes a new and hopefully fruitful connection between security questions and the material sciences.**

I. Introduction

A common problem facing all cryptographic systems is how to secure their secret keys against malicious attacks. Ideally, an effective key storage medium should be (i) difficult for adversaries to read-out or tamper with, and (ii) quickly erasable in an irrecoverable fashion whenever necessary. Both requirements represent a non-trivial challenge to system designers. First, a host of physical attacks on digital electronic memories have been reported in the past, including non-volatile memories like EEPROM [1] as well as volatile forms like SRAM [2] and DRAM [3]. Second, data remanence in electronic storage media, along with the problem of quickly erasing large amounts of data, are just two of several issues surrounding secure data deletion [4].

Physical unclonable functions (PUFs) could be seen as a new, emerging class of key storage devices that increase the difficulty of copying, modeling or probing their saved contents [5], [6]. They use the inherent microscopic physical disorder within a device, often in the form of variations induced during fabrication, to form a unique "fingerprint" that is extremely challenging to copy or model. Examples include timing offsets in integrated circuits [7], instabilities in volatile memory cells [8], [9], variations in resistance values [10], [11], capacitances of perturbed films [12], and scattering potentials of volumetric materials [5], [13]. Random but stable keys are typically derived from these physical fingerprints after additional digital processing and error correction.

Most PUFs to date remain electronic-based. Unfortunately, recent work has demonstrated that the majority of digital electronic PUFs are not as physically secure as originally imagined. Recent attacks have been successful in physically cloning and invasively reading out SRAM PUFs [14], [15], as well as in establishing modeling attacks and side channels on Arbiter PUF [16], [17] and Silicon PUF [18] variants. These attacks negate many of the original assumptions supporting the electronic PUF's physical and digital unclonability. Currently, it appears that optical PUFs are one of the few remaining candidates for a "strongly unclonable" random bit storage medium (i.e., as a so-called "Strong PUF" [16]). Although more challenging to directly integrate into conventional electronic devices, their multiple orders-of-magnitude larger memory capacity and their extremely high input-output complexity have so far prevented a successful attack. Optical methods thus maintain high promise for future secure PUF generations.

Besides unclonability, two highly desirable attributes of secure key storage are total erasability (i.e., that key data can be safely and irrecoverably deleted) and reconfigurability (i.e., that the PUF or other storage medium can be made to contain a new, random key that is uncorrelated to the old one). These two features may not just help prevent the abuse of a cryptographic device that falls into adversarial hands. They can also increase the strength of various communication protocols by limiting the amount of data available for cryptanalysis (e.g., by periodic erasure/reconfiguration of PUF keys [19]). Furthermore, an effective reconfiguration operation supports commercial PUF usages, in which a single PUF-carrying hardware unit can be refreshed and employed by multiple users in sequence [19], [20].

Unfortunately, as we detail later, fully erasing large data sets in a short amount of time still remains a serious challenge [4], [21]. In addition, currently existing suggestions for reconfigurable PUFs [9], [20], [22] each have certain limitations. For example, logically reconfigurable PUFs [22] depend upon an additional module that manages access to the PUF, as well as a hardware-internal counter that cannot be manipulated (i.e., reduced). Both introduce new security assumptions on top of those required by the PUF: for example, one must assume that the module cannot be circumvented or disconnected from the PUF. In addition, existing optical reconfigurable PUFs [20] require application of significant heat to the PUF volume to change its internal configuration. However, such heating is practically awkward, only changes the PUF locally, and will not fully refresh its stored randomness. Most problematically, the repeated application of heat will eventually warp the PUF structure into an energy-minimized state, reducing the PUF's internal entropy and eventually producing little to no change in the PUF outputs.

This paper designs and implements a reconfigurable optical scattering-based storage (ROSS) mechanism, which is a specific type of reconfigurable optical PUF. It functions like an integrated version of Pappu et al.'s optical PUF [5]: to read a fixed number of random bits, we shine patterned light onto a disordered volume of particles (Fig. 1). The light and its pattern serve as the PUF input, or "challenge". We patterned the light using an integrated spatial light modulator (SLM), in which certain subregions can be switched on and off independently. Unlike in [5], [20], this SLM mechanism functions without any moving parts, now enabling an exponential number of different PUF challenges. The distributed volume of particles will scatter the input light into a unique speckle interference pattern, which we measure with an attached digital detector and form into a random key. This random output key forms one PUF "response". Compared to existing work, we make the following new contributions:

- Our system is the first *integrated* reconfigurable optical PUF, meaning that it operates without any moving components inside a small package, unlike previous designs [5], [20]. It can hence operate at comparably faster frequencies (up to 10 challenges/sec, 10^5 random bits per challenge) and is more stable. While [23] suggests a similar prototype layout, our PUF is miniaturized and is thus more convenient to integrate with microelectronics. Unlike classical optical PUFs [5], [20], it has an exponential, as opposed to a polynomial, number of challenges.
- Our optical system uses an *electrical* reconfiguration operation, which can be triggered by a simple short voltage pulse. In opposition to [20], our reset alters the system completely within less than one second. The operation furthermore upholds — and does not diminish — the entropy and complexity in the system, and can thus be applied many times in sequence without wearing out the PUF. Earlier approaches based on heating and melting the PUF material do not possess this feature [20].
- We build a full prototype of our suggestion. We use it to evaluate, for the first time on large scales, the input-output complexity of an integrated optical PUF by applying the NIST random number generator test suite to optical input-output data. The prototype, which was not optimized in this respect, already demonstrates that more than 10^6 256-bit keys can be derived safely, with the potential being yet much larger: 1 Tb/mm^3 is predicted in theory, while 10 Gb/mm^3 has been demonstrated in related experiments [24].
- The electrical reconfiguration operation becomes possible via a new active scattering medium, polymer-dispersed liquid crystal (PDLC), which is very simple to use and can be sprayed onto security hardware and systems. It can hence easily be used to encapsulate security hardware and as a tamper-detecting mechanism. The medium is sensitive to electrical voltage, which enables its reconfiguration mechanism. Our work here establishes a new and interesting connection between security and the material sciences.
- Due to the volumetric and three-dimensional nature of the suggested optical system, and the complexity of the optical scattering, we argue that its achieved security level is higher than for reconfigurable electronic PUFs. What's more, its gigabit-scale storage is orders-of-magnitude larger than previously demonstrated integrated PUFs, enabling unique future applications.

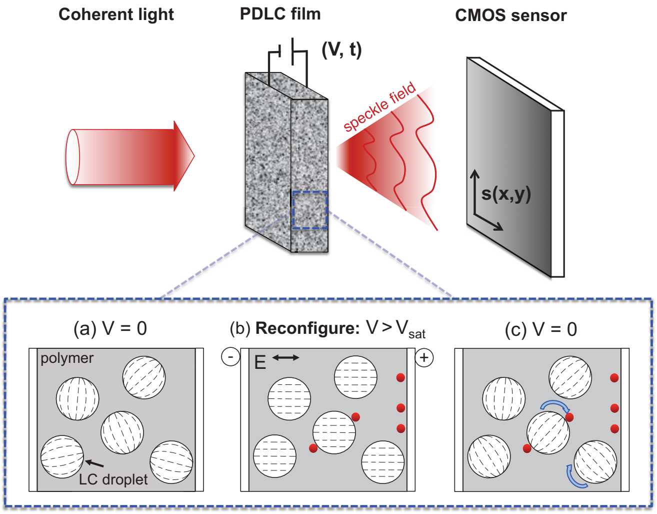


Fig. 1. The optical scattering response of PDLC film may be reconfigured with temporary application of a large voltage V, which introduces both an electric field E and mobile ions (red) within the material. After V is removed, liquid crystals (LCs) shift to produce a new scattering response.

The remainder of this paper is outlined as follows. In Section 2, we first experimentally demonstrate how the optical scattering response of PDLC film may be reset with an applied voltage. In Section 4, we experimentally show the ROSS device can store over 10^6 256-bit random keys with minimal error, which can be fully erased (i.e., re-randomized) in one second. Section 5 discusses and analyzes our findings and also suggests future research opportunities.

II. Electrically Reconfigurable Optical Scattering Material

PDLC is a well-studied material whose optical transmission properties change with the introduction of a voltage across the film interface. The films employed in this study exhibit a 400 μm-thick optically transparent polymer substrate containing a

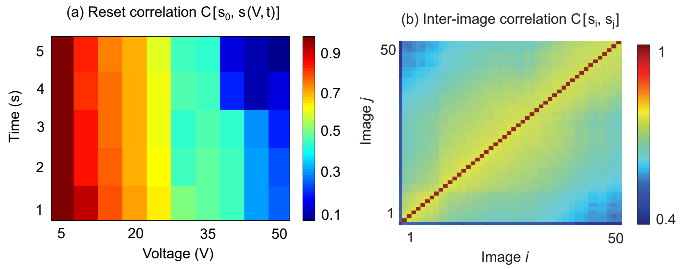


Fig. 2. Reconfiguring PDLC with an applied voltage. (a) Experimental optical scattering response of PDLC decorrelates to different values as a function of DC voltage V and application time t. (b) Experimental cross-correlation C of different speckle images after repeated application of fixed voltage $V = 40$ V for duration $t = 1$ second shows continued decorrelation.

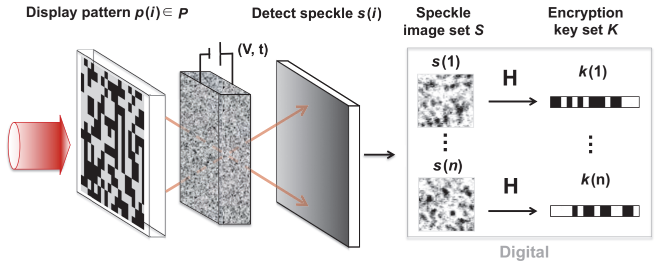


Fig. 3. The schematic of the ROSS device, where an SLM is used to probe the PDLC material in Fig. 1. Many uncorrelated speckle image resposes s may be detected as many unique binary challenges p are displayed on the SLM, from which our total key set K is derived (H denotes whitening).

20 μm-thick active layer of sub-micron sized liquid crystal (LC) droplets distributed randomly throughout. This substrate is sandwiched between a transparent anode and cathode. In the off state (no voltage between anode and cathode), the birefringent LC molecules randomly align themselves between various dislocations (i.e., anchor points) along each droplet's surface (Fig. 1(a)). The boundary of each droplet thus exhibits a random index of refraction mismatch, causing an incident optical field to scatter within the film. The optical response of such a material dense with wavelength-scale particles is conveniently described by a scattering matrix T, containing complex random Gaussian entries [25]. In the "on" state (voltage V applied between anode and cathode), the LC molecules orient themselves along the voltage gradient, aligning the dielectric tensor of all droplets (Fig. 1(b)). When $V \approx$ 2-3V/μm, the film becomes nearly transparent, changing T into an optical transformation that closely resembles the identity matrix.

When the direct current (DC) voltage V used to keep PDLC in an on-state is above a certain critical saturation value V_{sat}, its LC molecules undergo an electrochemical reaction [26]. This DC-induced reaction effects both the LCs within each droplet [27] as well as the liquid-polymer and polymer-electrode boundaries, where charge instabilities build up. Specifically, [28] has shown that the prolonged application of DC voltage to an LC cell introduces mobile ions that selectively adsorb at droplet boundaries. Likewise, [29] has derived how free ions at a substrate-LC boundary can shift the LC anchoring energy, thus rotating its local dielectric tensor. We hypothesize that a combination of the above electrochemical effects can shift the scattering response of a PDLC film after application of a large DC voltage. Mathematically, this scattering response shift is represented by a change in a given PDLC film's original off-state random scattering matrix T into a new and unpredictable off-state matrix T'. As we demonstrate next, the transformation of T into T' effectively "resets" our cryptographic keys in an irreversible manner, thus completely and simultaneously erasing all previously stored content.

To experimentally demonstrate PDLC reconfiguration, we first illuminate a film with a coherent plane wave of 532 nm light and measure its optical response, $s_0(x, y)$, which is the intensity of the speckle field at a directly adjacent digital detector (Fig. 1, top). Then, we apply a DC voltage $V > V_{sat}$ for a fixed time t across the film surface, during which the film becomes optically transparent. After removing the voltage we measure a new optical scattering response $s_t(x, y)$, which is significantly different from the original measurement, s_0. We compare s_0 and s_t with a cross-correlation. Performing this experiment for many different values of V and t yields the data in Fig. 2(a), indicating the scattering response of the film decorrelates after several seconds of applied DC (a new film was used for each measurement to remove any bias). To demonstrate the induced potential continues to produce a random optical response within one film, we repeat this experiment 50 times with the same film, fixing $V = 40$ V and $t = 1$ second. All response images are significantly (yet not fully) uncorrelated, showing the scattering state does not momentarily leave and return to an original configuration or approach a steady-state molecular configuration, but continues to vary in a semi-random fashion (Fig. 2(b)). Increasing the thickness of the active PDLC material, stacking multiple films along the optical axis, or executing multiple reset operations sequentially over time helps enhance decorrelation. We demonstrate that a single reset of two stacked films leads to nearly ideal re-randomization of all stored random bits.

III. Design of the Prototypical ROSS Device

The random distribution and orientation of sub-micron PDLC droplets will serve as the centerpiece of our prototype. To selectively address a subset of its stored random bits, we attach an amplitude SLM screen (1920 x 1080 pixel Epson HDTV LCD) directly in front of our PDLC volume and sensor (Fig. 3). These three elements joined together form our ROSS key storage device, which is an integrated and reconfigurable optical PUF. We physically attach the SLM and film with a half-ball lens (radius = 1 cm), and the film to the sensor with a quartz disc (McMaster-Carr 1357T62) to minimize movement. A small microprocessor controls our data input-output and reconfigurable switch.

To efficiently present our experimental results in the next section, we now summarize our reconfigurable PUF with a brief mathematical model. The SLM controllably varies an input "challenge" wavefront incident upon the scatterer, to sequentially induce many mutually random speckle intensity pattern "responses". If we consider our SLM and CMOS array extend along one dimension for simplicity, we may mathematically denote the ith pattern displayed on the SLM as vector $p(i)$ and the corresponding detected speckle image as vector $s(i)$. When illuminated with a plane wave, the ith SLM challenge and detected speckle response are connected by the matrix-vector product, $s(i) = |Tp(i)|^2$, where T is the unique random scattering matrix of the PDLC volume. Any small change in the SLM challenge will produce a significant, random change in speckle response.

T contains all of the inherent randomness that imparts our detected keys with their security. A sufficiently large set of many independent speckle measurements $s(i) \in S$ efficiently transfers all of the stored randomness in T to the digital detector. In practice, we probe T with a set of mutually random binary SLM patterns $p(i) \in P$ (i.e., half of the pixels in each $p(i)$ absorb light). A stack of 2 separate layers of PDLC film, which is 1.5 mm thick, ensures T is a fully random matrix. In our experiments, T contains approximately 10^{12} entries. Finally, as discussed in Section 2, reconfiguration completely re-randomizes each of these entries.

IV. Experimental Demonstration

Here, we experimentally test the ability of our ROSS device to save a large set of random 256-bit keys. This demonstration of random key memory easily generalizes to secure storage of any sensitive content (discussed in the following section). We begin by displaying $n = 4300$ random binary SLM screen challenges $p(i)$ to create and capture the same number of uncorrelated 4.85 MB speckle responses $s(i)$. The number of challenges n is selected to efficiently extract all the randomness contained within our PDLC scattering volume (i.e., its matrix T) without introducing unwanted correlations [24]. Each response image $s(i)$ is transformed via a digital whitening operation into a 2.42 MB vector. The same whitening operation transforms all images.

We then implement key creation with fuzzy commitment [12], [30], which is required to remove any possible noise from each key, as outlined in Fig. 4(a). First, each whitened speckle sequence $s(i)$ is split into two segments: a key vector k and a "witness" vector w. At the end of the fuzzy commitment process, we will only use k for security purposes, and effectively discard w. Second, we encode the key k as a longer "codeword" k'. This encoding step simply introduces redundant bits to k, to help with a subsequent error correction step. Third, we XOR k' with w to create an encrypted blob b, which is information-theoretically secure (i.e., may be publicly shared). We then save b in digital memory.

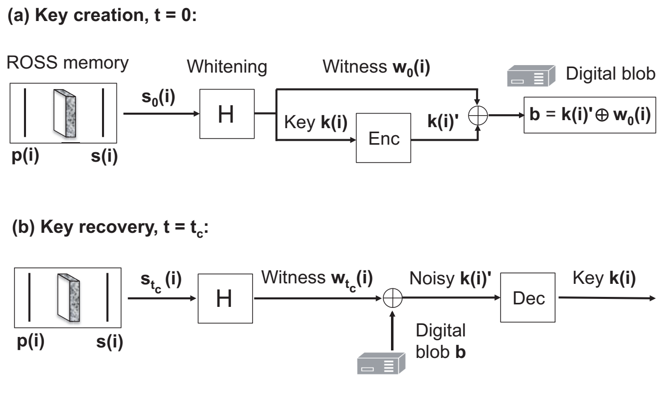


Fig. 4. The fuzzy commitment protocol. (a) A key k and witness w are created from the same whitened speckle image s_0, which we XOR ($\oplus$) to create a secure, publicly sharable blob b. (b) The key is recovered at any later time t_c by using the ROSS to re-create a noisy witness w_{t_c}, XORing it with b and applying error correction to recover a noiseless key k.

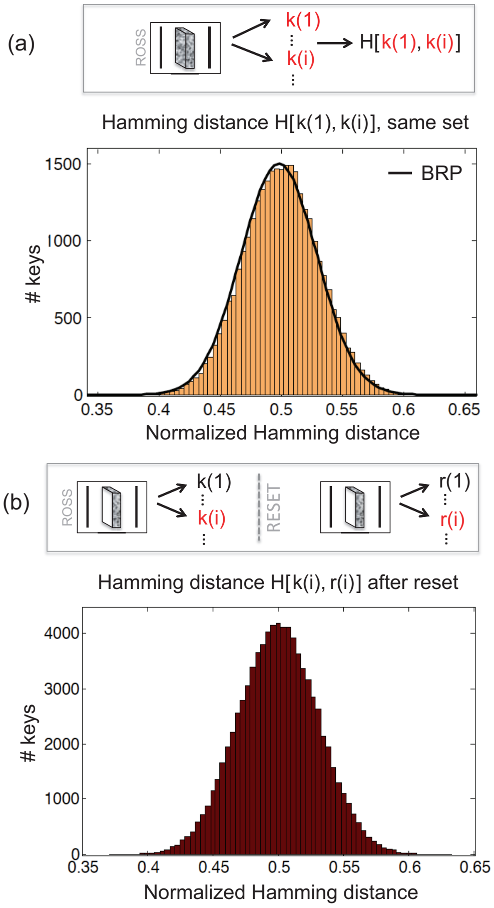
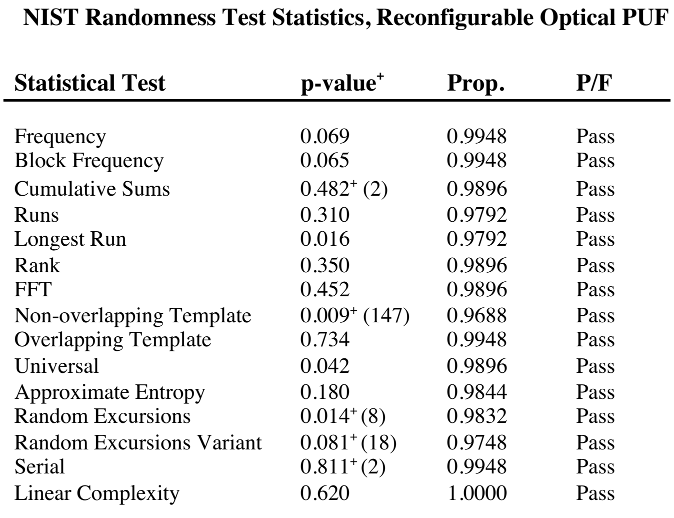


Fig. 5. (a) Experimental Hamming distance between one key $k(1)$ and 3×10^5 other keys from the same device follows an uncorrelated binomial random process (BRP) curve. (b) Experimental Hamming distance between one key $k(i)$ and the corresponding key $r(i)$, creating using the same screen input $p(i)$ but after PDLC reset, similarly demonstrates complete key reconfiguration.

At a later time $t_c = 24$ hours, we attempt to access our saved keys using fuzzy commitment key recovery, as outlined in Fig. 4(b). First, we use the same SLM screen challenge $p(i)$ to regenerate a noisy speckle response $s'(i)$. Second, we XOR $s'(i)$ with the saved blob b. Third, we apply a modified (255, 9) Hamming error correction with an additional 12.5% data reduction factor to the XOR result, which recovers the key vector k with minimal error. The measurement and recovery process for one k takes less than one second.

After a period of 24 hours, we successfully extract 1.43 million 256-bit keys from our ROSS device, of which 90.2% are error-free. During practical operation, erroneous keys must be discarded and regenerated, which will delay any associated protocol. In Fig. 5(a), we demonstrate that each of our 256-bit ROSS keys are minimally correlated by plotting their normalized inter-key Hamming distance. Here, each distance is measured with respect to the first generated key. We find nearly identical distances when comparing to the ith generated key. A Gaussian fit of the histogram of these Hamming distances finds a mean of 0.50 and variance of 9.81×10^{-4}. Comparing this variance to the predicted variance of an independent, identically distributed binomial process (9.77×10^{-4}) suggests each key is comprised of nearly 256 independent variables, as



NIST Randomness Test Statistics, Reconfigurable Optical PUF

Statistical Test	p-value^{+}	Prop.	P/F
Frequency	0.069	0.9948	Pass
Block Frequency	0.065	0.9948	Pass
Cumulative Sums	0.482^{+} (2)	0.9896	Pass
Runs	0.310	0.9792	Pass
Longest Run	0.016	0.9792	Pass
Rank	0.350	0.9896	Pass
FFT	0.452	0.9896	Pass
Non-overlapping Template	0.009^{+} (147)	0.9688	Pass
Overlapping Template	0.734	0.9948	Pass
Universal	0.042	0.9896	Pass
Approximate Entropy	0.180	0.9844	Pass
Random Excursions	0.014^{+} (8)	0.9832	Pass
Random Excursions Variant	0.081^{+} (18)	0.9748	Pass
Serial	0.811^{+} (2)	0.9948	Pass
Linear Complexity	0.620	1.0000	Pass

Fig. 6. NIST statistical randomness test performance for 24 MB of PUF-based key data. We test 192 unique 1 megabit data sequences. For success using 192 samples of 10^6 bit sequences and a 0.01 significance level, the p-value (uniformity of p-values) should be larger than 0.001 and the minimum pass rate is 0.968458. Tests with multiple p-values have a (+), followed by the number of different test values. This table displays the lowest generated p-values and proportions in the set (all tests pass).

we expect for an ideally random bit source. We additionally verify that our ROSS key set is random by ensuring an arbitrarily selected 24 MB sequence of 750,000 concatenated keys passes all tests contained within the Diehard and NIST statistical random number generator test suites. Example NIST test statistics are in Fig. 6.

Next, we demonstrate the quick and complete reconfiguration of all the stored keys in our new optical PUF prototype. We now use the ROSS device to generate 250 speckle responses S, from the same set of 250 SLM challenges P, applied at four separate times: t_1-t_4. At t_1, we execute key creation to form key vector k_1 containing 8.4 x 10^4 individual 256-bit random keys. At t_2, two hours later, we perform key recovery to access 98% of the keys in k_1 without any error. We then apply 40 V DC for 0.8 seconds across the PDLC interface to reconfigure its scattering potential. At t_3, one minute after reset, we again display each SLM challenge in set P, but now record a different set of speckle responses, S'. Attempting to use S' for key recovery of k_1 leads to the error histogram in Fig. 5(b), which closely matches the curve of an uncorrelated binomial random process. A Gaussian fit of this histogram yields a mean of 0.50 and variance of 9.79×10^{-4}, again matching the histogram of an independent binomial random process. We thus conclude that all random bits are completely reset into a new uncorrelated configuration. The reset material's new optical response offers effectively zero information about the original key set (i.e., achieving total erasure). However, we can use S' to generate a new set of 8.4 x 10^4 keys, which we again recover two hours later at t_4 with 98% accuracy. Thus, our PUF prototype continues to offer distinctly random key sets after each reset (i.e., showing successful reconfiguration). Given this reconfiguration operation is quick, repeatable and complete, we now conclude with a brief discussion of how our integrated optical PUF may securely store and quickly erase large datasets.

V. Summary, Discussion and Future Work

We demonstrated in this paper that our reconfigurable optical PUF device is capable of storing over one million 256-bit keys within a 1 mm^3 physically disordered volumetric structure. Keys may be reset into new, nearly perfectly uncorrelated sequences of random bits in less than one second with a briefly applied DC voltage. To the best of our knowledge, no other device offers such physically unclonable key storage and direct electronic reconfiguration. Beyond this first prototype, there are substantial possibilities to further improve information densities: the high potential for stored randomness in similar material has been thoroughly analyzed in previous work (currently 10 Gb/mm^3, can be extended to 1 Tb/mm^3 [24]).

Let us quickly compare our approach to current electronic techniques once more. One desirable property of an erasable storage medium clearly should be a quick and efficient option to completely destroy its contents. Since all electronic-based memory keeps each of its bits localized at a specific spatial location (e.g., within a gate), complete destruction of large amounts of key material is challenging. If an attacker obtains a fraction of either a volatile or non-volatile chip, they may still extract whatever saved bits remain across the fractional surface. Each random bit extracted from of our optical PUF, on the other hand, is not localized. Every detected speckle results from scattering interactions across the entire memory volume. Due to this non-locality, a small fragment of the PUF cannot be used to obtain partial information for an attack. Device fragmentation, such as in tampering attempts or caused by any other phenomena, thus directly and permanently destroys all saved bits.

Second, as discussed in [21], a full "erasure" of non-volatile digital electronic (e.g. magnetic or flash) memory is only achieved when each and every saved bit is re-written with various bit patterns [31]. This re-write period can take up to several days, preventing its widespread adoption. Furthermore, other forms of data sanitization (e.g., reformatting) may leave behind partial information in overlooked hard drive sections [32]. As discussed above, the entire multi-gigabit PUF volume may be effectively re-written in one second, altering all volume areas simultaneously and uncontrollably. This represents an important asset of our approach and is unprecedented by other methods in the literature.

One particularly interesting and noteworthy application of our optical PUF would hence be memory encryption in connection with large datasets, using the PUF responses as one-time pads for the memory data. Due to the high information densities of our optical PUF, this would promise information-theoretically secure data encryption. Furthermore, tampering with the optical PUF (which could encapsulate the hardware) would result in destruction of all key material, following from its property of non-locality mentioned above. Finally, the entire memory can be effectively erased in less than one second by reconfiguring the PUF, a feature that is currently not shared by any current electronic approaches. Due to the information-theoretic secrecy of the mentioned one-time pad scheme, future decryption of the encrypted memory content, e.g. with increased computational power or improved crypt-analytic techniques, would not be possible. This advantage is unique to our optical approach. Electronic PUFs used in other memory encryption schemes exhibit a lower PUF information content, and can thus only promise computationally secure encryption [33].

A. Future Work

Future efforts will primarily focus on improving the somewhat high error rate of the current ROSS prototype (e.g., 10% of saved 256-bit keys currently exhibit at least 1 flipped bit). Error is caused by noise introduced into the key generation and readout process. Over the course of our experiment, we believe that laser source fluctuations, temperature variations, and small movements all potentially contributed noise that corrupted a small percentage of our bits before re-measurement. Temperature variations were on the order of several degrees. Furthermore, we believe a fixed fraction of this noise currently increases slowly with device lifetime.

Three future improvements will help reduce the ROSS device error rate to match the error of current electronic PUFs. First, we are now investigating alternative optical setups that better stabilize the scattering process. Integrating the illumination, scattering and detection mechanisms onto a single silicon substrate is possible and will form a very stable package. Using an integrated photonic circuit, we may also combine any electronic controls onto the same chip. This packaged design may thus lead to a general strategy for securely interfacing each ROSS component with any required digital logic.

Second, an alternative embedding material besides polymer, ideally with a lower coefficient of heat expansion, may prove more stable in the presence of temperature fluctuations. Spraying liquid crystal droplets into more a rigid material like a silicon gel or even a carbon nanotube structure [34] should better anchor the scatterers in place. This effort connects cryptographic hardware to the material sciences – an ideally designed reconfigurable optical material will require input from both fields. Third, a new error correction procedure (within the fuzzy commitment protocol) that is well-suited to fix higher bit rate errors will clearly lead to more repeatable keys. In combination with optical techniques to increase random bit output [35], we believe this may improve device reliability without sacrificing storage capacity. All of these observations open the door for fruitful future research opportunities.

References

[1] R. Anderson and M. Kuhn, "Low cost attacks of tamper resistant devices," Lect. Notes Comput. Sc. **1361**, 125 DOI:10.1007/BFb0028165 (1998).

[2] S. Skorobogatov and R. Anderson, "Optical fault induction attacks," Lect. Notes Comput. Sc. **2523**, 2 (2003).

[3] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Caladrino, A. J. Feldman, J. Appelbaum and E. W. Felten, "Lest we remember: cold boot attacks on encryption keys". Proc. 2008 USENIX Security Symposium (2008).

[4] J. Reardon, D. Basin and S Capkun, "SoK, Secure data deletion," In 2013 IEEE Sym. Security and Privacy (SP), pp. 301–315 (2013).

[5] R. Pappu, B. Recht, J. Taylor and N. Gershenfeld, "Physical one-way functions," Science **297**, 2026 (2002).

[6] U. Rührmair and D. E. Holcomb, "PUFs at a glance," Design Automation & Test in Europe (DATE) 2014, pp. 1–6 (2014).

[7] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Trans. VLSI Syst. **13**, 1200 (2005).

[8] J. Guajardo, S. S. Kumar, G. Schrijen & P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," Lect. Notes Comput. Sc. **4727**, pp. 63–80 (2006).

[9] M. Majzoobi, F. Koushanfar and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," ACM Trans. Reconfig. Technol. Syst. **2**, 5 (2009).

[10] R. Helinski, D. Acharyya and J. Plusquellic, "A physical unclonable function defined using power distribution system equivalent resistance variations," In ACM Proc. 46th Annual Design Automation Conf., pp. 676–681 (2013).

[11] U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba and M. Stutzmann, "Security applications of diodes with unique current-voltage characteristics," In Financial Cryptography and Data Security, Springer pp. 328–335 (2010)

[12] P. Tuyls, B. Škorić and T. Kevenaar, *Security with Noisy Data* (Springer-Verlag, London, 2007).

[13] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić and P. W. H. Pinske, "Quantum-secure authentication of a physical unclonable key," Optica **1**, pp. 421–424 (2014).

[14] D. Nedospasov, J. P. Seifert, C. Helfmeier and C. Boit, "Invasive PUF analysis," Proc. 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography (2013).

[15] C. Helfmeier, C. Boit, D Nedospasov, and J. Seifert, "Cloning physically unclonable functions," In 2013 IEEE Int. Symp. Hardware-Oriented Security and Trust (HOST), pp. 1–6 (2013).

[16] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas and J. Schmidhuber, "Modeling attacks on physical unclonable functions," Proc. ACM Conference on Computer and Communications Cecurity, 237 (2010).

[17] U. Rührmair, X. Xu, J. Sölter, A. Mahmoud, M. Majzoobi, F. Koushanfar, and W. Burleson, "Efficient Power and Timing Side Channels for Physical Unclonable Functions," In Cryptographic Hardware and Embedded Systems (CHES) 2014, Springer pp. 476–492 (2014).

[18] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson and S. Devadas, "PUF Modeling attacks on simulated and silicon data," IEEE Trans. Info. Forensics Security **8**(11), 1876–1891 (2013).

[19] U. Rührmair and M. van Dijk, "PUFs in security protocols: attack models and security evaluations," IEEE Symposium on Security and Privacy, pp. 286–300 (2013).

[20] K. Kursawe, A. R. Sadeghi, D. Schellekens, B. Škorić and P. Tuyls, "Reconfigurable physical unclonable functions - enabling technology for tamper-resistant storage," Proc. IEEE Workshop Hardware Oriented Security & Trust (2009).

[21] R. Canetti, D. Eiger, S. Goldwasser and D. Y. Lim, "How to protect yourself without perfect shredding," Lect. Notes Comput. Sc. **5126**, pp. 511–523 (2008).

[22] S. Katzenbeisser, U. Kocabas, V. van der Leest, A. R. Sedeghi, G. J. Schrijen and C. Wachsmann, "Recyclable PUFs: logically reconfigurable PUFs," J. Cryptogr. Eng. **1**, pp. 177–186 (2011).

[23] U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, C. Jirauschek, "Optical PUFs Reloaded," IACR Cryptology ePrint Archive 2013, 215 (2013).

[24] R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit and C. Yang, "Physical key-protected one-time pad," Scientific Reports **3**, 3543 (2013).

[25] M. C. W. van Rossum and T. M. Nieuwenhuizen, "Multiple scattering of classical waves: microscopy, mesoscopy and diffusion," Rev. Mod. Phys. **71**, 313 (1999).

[26] S. C. Jain and D. K. Rout, "Electrooptic response of polymer dispersed liquid crystal films," J. Appl. Phys. **70**, 6988 (1991).

[27] A. Sussman, "Dynamic scattering life in the nematic compound p-methoxybenzylidene-p'-amino phenyl acetate as influenced by current density," Appl. Phys. Lett **21**,126 (1972).

[28] S. H. Perlmutter, D. Doroski and G. Moddel, "Degredation of liquid crystal device performance due to selective adsorption of ions," Appl. Phys. Lett. **69**(9), 1182 (1996).

[29] G. Barbero and G. Durand, "Selective ions adsorption and nonlocal anchoring energy in nematic liquid crystals," J. Appl. Phys. **67**, 2678 (1990).

[30] M. D. Yu and S. Devadas, “Secure and robust error correction for physical unclonable functions,” IEEE Des. Test Comput. **27**, pp. 48–65 (2010).

[31] Department of Defense, “National Industrial Security Program Operating Manual,” DOD 5220.22-M (2006).

[32] S. Garfinkel. Design principles and patterns for computer systems that are simultaneously secure and useable. PhD Thesis, MIT (2005).

[33] P. Tuyls, G. J. Schijen, B. Škorić, J. van Geloven, N. Verhaegh and R. Wolters, “Read-Proof Hardware from Protective Coatings,” Lect. Notes Comput. Sc. **4249**, pp. 369–383 (2006).

[34] R. Basu and G. S. Iannacchione, “Carbon nanotube dispersed liquid crystal: a nano electromechanical system,” Appl. Phys. Lett. **93**, 183105 (2008).

[35] R. Horstmeyer, R. Y. Chen, B. Judkewitz and C. Yang, “Markov speckle for efficient random bit generation,” Opt. Express **20**, pp. 26394–26410 (2012).