RSA Laboratories Cryptobytes
Volume 6, No.2 — Summer 2003

III. Physical One-Way Functions

Ravikanth S. Pappu *

Abstract

How can we assign unique, tamper-resistant, and unforgeable identifiers to everyday objects at a very low cost? Physical One-Way Functions (POWFs) provide a novel approach to answering this question. POWFs can be obtained from the inherent three-dimensional microstructure of a large class of physical systems known as mesoscopic systems. They are inexpensive to fabricate and prohibitively difficult to duplicate; they admit no compact mathematical representation and are intrinsically tamper-resistant. In this paper, we show how POWFs are obtained by using coherent scattering of visible laser radiation from inhomogeneous structures and experimentally demonstrate their properties. We also discuss potential attacks on POWFs and possible applications.

1 Introduction

Humans have long used physical structures to authenticate objects of value. As early as the 4th millennium BC, the Mesopotamian civilization was using cylindrical seals to certify the contents of envelopes, waybills, ceramics, and bricks. These seals, small cylindrical stones carved with a decorative pattern, were rolled over wet clay to mark the target object. Their use was contemporaneous with the use of clay tablets in everyday life and lasted over two thousand years [4].

Modern banknotes incorporate a variety of different structural features that aid the goals of authentication and anti-counterfeiting. Among these are security threads, hologram foils, iridescent stripes, color-shifting inks, and as proposed recently, radio-frequency identification tags [25]. The number and complexity of security features included on banknotes is an indication of the increasing capability of forgers to reproduce highly specialized features with very low cost equipment. While forgers of yesteryear needed access to expensive printing equipment and skilled engravers, highly sophisticated two-dimensional reprographic systems are easily available to the general public today.

Fundamentally, two major changes have occurred since ancient Mesopotamia. First, the creation of complicated two-dimensional structures with specific properties no longer requires the skill that it once did. Second, the manufacturing and digital revolutions have allowed forgers to stop worrying about the structural features and focus on the logical content (e.g., the denomination of currency as opposed to the physical banknote) of the forged object. Because it is much easier to work with bits than it is with atoms, the asymmetry in effort between the ”good guys” and ”bad guys” and the time lag between the original object and a high-quality forgery has decreased substantially.

The search for uncloneable and tamper-evident physical structures leads ultimately to the theoretically compelling concept of Quantum Money [1]. The key idea here is to augment banknotes with a number of isolated two-state quantum systems, such as spin 1/2 nuclei or photons with orthogonal polarizations,

*Research carried out at the MIT Media Laboratory; author may be reached at ravi@thingmagic.com

which are encoded with the identity of the note. In order to successfully forge the note, a forger has to prepare a counterfeit banknote in the same quantum state as the original. This is theoretically impossible [24]. There are two principal attributes of Quantum Money that make it substantially different from all previous methods of physical authentication. First, the security is provable via the quantum no-cloning theorem which states that an arbitrary, unknown quantum state cannot be cloned with certainty. Second, it makes an explicit connection between physical authentication and the framework of modern cryptography. Practically speaking, however, quantum decoherence, i.e., the loss of the quantum identity of isolated quantum monetary systems by interacting with the environment, prevents any useful realization of the concept. While Quantum Money is not a POWF, it does provide a clear example of a physical authentication system whose non-clonability is provable.

This is the context in which we situate POWFs.

2 Motivation: arms control treaties

In this section, we provide an example where POWFs may be used with benefit.

Arms control treaties typically place numerical limits on treaty-limited weapons systems. As opposed to treaties which ban certain types of weapons outright, treaty-limited items (TLIs) require a tagging system to ensure that more than the allowed number of items exist at any given time [9, 10]. Treaty verification then consists of verifying that the total number of items is below the limit established for that item under the treaty.

The goals of the tagging system are unique: it must provide unambiguous verification of TLIs without allowing the monitoring party undue advantage in tracking the weapons systems for purposes of intelligence gathering and espionage. The requirements on the tag system are discussed at length in [10] and are reproduced here: (a) it must be impossible to copy the tag without detection (b) it must be impossible to spoof the tagging system or to fool it into thinking that a valid tag exists where there actually is none (c) it must not be possible to move the tag from one weapon to another without the knowledge of the monitoring party (d) the tagging system must not aid the monitoring party in locating the weapons in real time (e) the tag should only reveal information required for purposes of verification (f) the system must be reliable and have a low false alarm rate (g) the physical size and the power requirements of the tag must be minimal (h) the tag must be reliable in the range of environments that the weapon is exposed to (i) the system should be inexpensive.

Further, the process of creating and reading tags cannot contain any secrets and a complete description of the tag reading process must be written into the language of the treaty so that tags can be read in an objective way.

In this article, we will show how POWFs can be employed in situations where complete transparency is required at the system level while providing all the requisite features at the tag level.

3 The physics of POWFs

A typical POWF embodiment is a token (e.g., a credit card, access control fob) encapsulating a small, optically translucent three-dimensional microstructure which contains inhomogeneities (also referred to as scatterers) that have features at the scale of the wavelength of visible light. The token is probed using a laser beam as shown in Figure 1 below. The scattering of such coherent radiation from an inhomogeneous medium produces laser speckle fluctuations, which is the result of interference of light that has taken a multitude of paths through the token. This speckle pattern is a complicated function of the microstructure of the

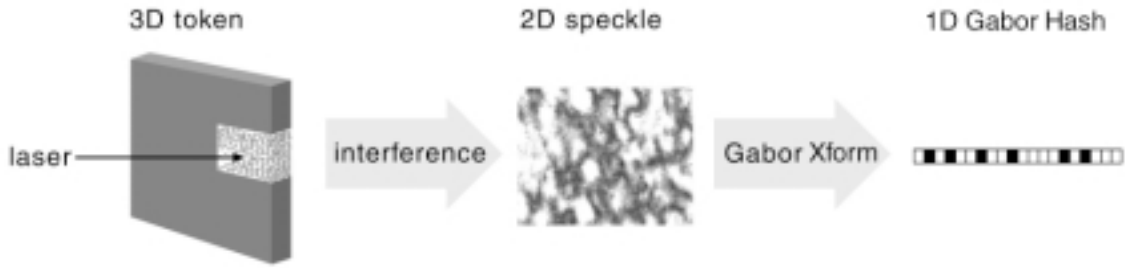

Figure 1: Coherent multiple scattering from an inhomogeneous structure results in a laser speckle pattern that can be reduced to a binary string. This string can be used as a unique identifier for the structure. This process may be viewed as physically hashing the complicated 3D structure down to a fixed-length key. The Gabor Transform is a means of filtering noisy speckle patterns and reducing them to a fixed-length bitstring called a Gabor Hash. Both these terms are defined in the text.

token and is used to derive a unique identifier for the structure.

We will show in the rest of this article that

- each token can produce not one but a very large number of identifiers. The availability of a large number of identifiers allows its deployment in challenge-response protocols.
- under certain conditions, each of these identifiers is a string of random bits.
- making small changes to the token's structure causes a given identifier to completely decorrelate

Before we press on into the physics of POWFs, consider a general model for the underlying physical mechanism. Typically, we have a physical system S encapsulated in a token and a physical probe P that interacts with S to produce an output O which is recorded by a detector D (Figure 2). How can we build a system that allows us to repeatably and robustly distinguish S from others in its class? Clearly, there are several choices for each of the elements in the system: S could be drawn from a large number of physical systems (e.g., regular vs. disordered, 2D vs. 3D); the probe P could possess several attributes (electromagnetic vs. acoustic, single frequency vs. broadband); and the detector could be anything from a voltmeter to a digital camera to X-ray film depending on the nature of S and P.

The long list of candidate systems, probes, and detectors may be narrowed down by considering the crucial properties they must have in order to meet our requirements.

- *Uniqueness* requires that the output O as recorded by D have a large number of statistically independent degrees of freedom
- *Tamper resistance* requires that the output O have a sensitive dependence on the state of S
- *Unforgeability* requires that the system S be difficult and expensive to clone regardless of the prior knowledge a forger has of P and O

Mesoscopic systems are a large class of physical systems that possesses all these properties. They are so named because they lie in a region between *macroscopic systems*, which are governed by the laws of classical physics, and *microscopic systems*, which

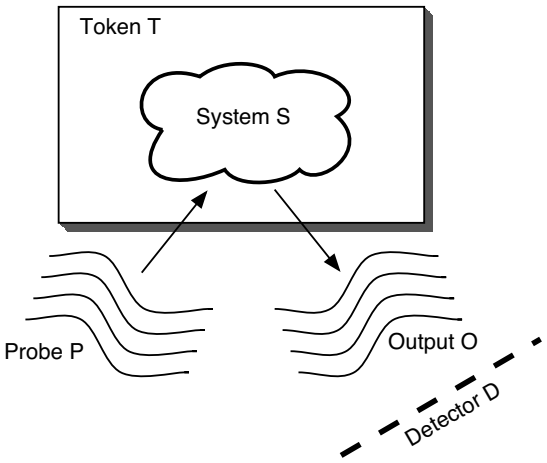

Figure 2: A general model for a physical authentication system

are governed by *quantum physics*. The fundamental distinguishing feature of mesoscopic systems is the preservation of coherence as radiation travels through the system i.e., the wavelength of the radiation is unchanged and its phase relative to that of the incident radiation is predictable after it exits the system. When *disordered* mesoscopic systems are probed with coherent radiation, the interference pattern after the radiation has passed through the structure is called a speckle pattern or a conductance fluctuation [13, 22]. By contrast, ordered mesoscopic systems produce regular diffraction patterns which are easily predictable given knowledge of the structure and the probe. In fact it is possible to predict the structural configuration by observing the diffraction patterns, a fact that is commonly used in X-ray crystallography. Hereafter, we will focus our attention on disordered mesoscopic systems.

There are generally four length scales of importance in these systems. The first is the wavelength λ of the incident probe. The second is the mean free path l which is the average distance between scattering events within the physical system S. The third is the size of the physical system itself denoted by L and finally, we have the coherence length[1] of the probe radiation L_c. The mesoscopic regime is governed by the inequality $\lambda \ll l \ll L \ll L_c$. In the mesoscopic limit of scattering in a three-dimensional structure [7, 8], the mean free path l between elastic collisions with scatterers is much larger than the wavelength λ of the radiation, but the thickness L of the structure is much smaller than the coherence length of the probe. In this regime of *coherent multiple scattering*, if the cross-sectional area of a beam is A, then moving $A/(Ll)$ scatterers will produce an uncorrelated speckle pattern, as will rotating the incident beam by an angle $\delta\theta = \lambda/(2\pi L)$ [2]. This phenomenon is the physical basis for POWFs.

We have thus narrowed down the choices of system components to:

- *Physical system S* - a 3D structure in the mesoscopic regime i.e., whose size L lies between the wavelength of the probe radiation and the coherence length of the radiation. This structure contains numerous scatterers which have features at the scale of the wavelength of the physical probe.
- *Physical probe P* - coherent radiation at a given wavelength λ
- *Interaction mechanism* between the P and S is coherent multiple scattering i.e., the interaction of coherent radiation with multiple scatterers in the disordered microstructure

The choice of detector D depends intimately on the wavelength of radiation. We note that although mesoscopic behavior is observed at all wavelengths, our requirement for unforgeability places an upper bound on the wavelength. Specifically, the size (in units of λ) of the structure L and its disorder characterized by the mean free path l must be such that it is prohibitive to

[1]The coherence length is defined as the distance light is able to travel from the laser before its phase becomes unpredictable relative to that at the laser.

clone the disordered mesoscopic system. Practically speaking, given the state of the art in 3D microfabrication, this restricts the range of wavelengths to be below one micron.

4 Implementation

In the embodiment described here [20, 21], we used a $\lambda = 632.8$ nm HeNe laser beam to illuminate $10 \times 10 \times 2.5$ mm^3 optical epoxy tokens containing 500-800 μm glass spheres. This represents about a penny's worth of materials; the cost of the reader can be anything from a few dollars to several hundreds of dollars depending on the precision of the laser pointing system. The density of spheres was chosen to give an average spacing on the order of 100 μm, which equals the photon mean free path in the limit of strong scattering applicable here [22]. The resulting speckle patterns were recorded with an inexpensive 320×240 pixel CCD camera. Repeatable positioning, i.e., mechanical registration, of the token with respect to the probe and the detector is achievable without recourse to high-precision (and expensive) systems.

Although it is possible to use the speckle patterns directly as identifiers, this is error-prone owing to the noisy readings of speckle patterns and their inherent sensitivity to small changes in the state of the probe. Figure 3 provides an example of the noise that can occur in a POWF system. In order to reduce the effects of noise, we transform the speckle pattern into a bit string using a multiscale Gabor Transform [11, 6]. The Gabor Transform is a complex-valued transform that represents speckle image intensity as a linear combination of oriented, modulated Gaussian filters at multiple scales. The parameters of the transform [19] are dependent on geometry of the specific optical implementation [20] and were experimentally determined in the embodiment discussed in this article.

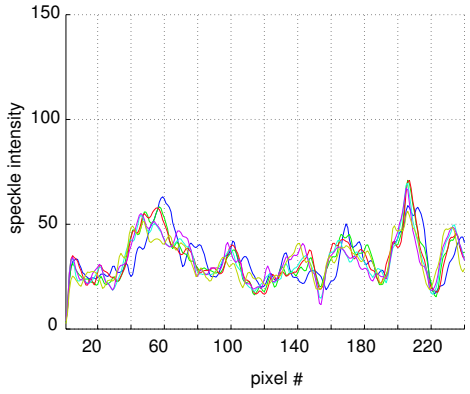

Figure 3: Noise sources in a speckle image. The plot shows six overlaid traces of speckle image intensity taken along a single row of a 320×240 raw speckle image before it was Gabor-transformed. Each trace was obtained after the token was removed and replaced in the reader after routine handling. First, there is pixel-scale noise, which is either due to the optical system or induced by the CCD detector. Then, there is noise at the scale of several pixels, which occurs at the physical interaction level. A third source of noise is due to misregistration of the token, shown as a trace horizontally displaced from the rest by about 10 pixels. Another source of noise, not shown in the figure, is due to changes in average illumination levels which would manifest itself as a vertical displacement of one trace from the other.

To summarize what we have said so far, a single probe of the 3D microstructure results in a 320×240 pixel speckle intensity image that is reduced to a bitstring of length 2400. This string is the unique identifier of the 3D microstructure when interrogated with a probe beam in a given state. Hereafter, we will refer to this bitstring as a *Gabor Hash*.

5 Experiments

In this section we present several experimental results that elucidate the properties of POWFs. The first

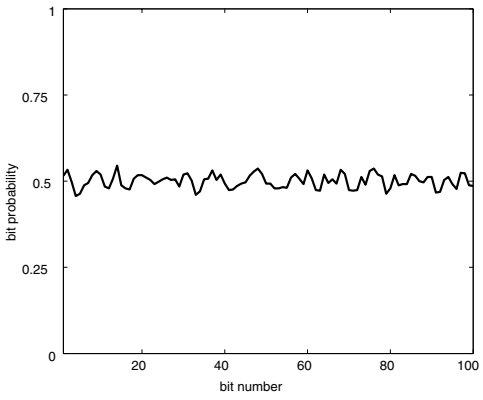

Figure 4: The plot depicts the probability that a bit in any given location of a Gabor Hash is set or cleared. Although only a 100-bit window is shown for clarity, this behavior is observed over all the bits.

experiment explores the average probability that a bit in any given location is either *0* or *1*. The average is taken over 576 Gabor Hashes which were derived from four different tokens, each of which was probed at 144 distinct locations. Figure 4 plots this probability, which hovers around 0.5. This result clearly indicates that each bit is equally likely to be set or cleared i.e., the bitstring derived from a POWF is a bit-wise maximum entropy code.

The second experiment focuses on how effective the Gabor Hash is at distinguishing one token from another. To ascertain this, we used the Gabor Hashes gathered in the previous experiment in an enrollment/authentication scenario. The bitstrings were enrolled in a database and candidate bitstrings were (a) matched to corresponding enrolled bitstrings and (b) matched to all 575 non-corresponding enrolled bitstings. The metric used for matching was a normalized Hamming Distance (i.e, every bit being different equals a distance of 1). The *like distribution*, which is the Hamming Distance distribution obtained from matching Gabor Hashes which had the same origin and the *unlike distribution* obtained by matching Gabor Hashes which had distinct origins are shown in Figure 5.

We learn several facts about POWFs from Figure 5. The distance between Gabor Hashes that have the same origin is usually smaller than the distance between hashes that have different origins. The average Hamming Distance between Gabor Hashes that have different origins is 0.5 implying that one can do no better at guessing one from the other than coin-flipping. The fact that the like distribution may be modeled by a binomial distribution with 233 independent degrees of freedom implies that this implementation of POWFs is capable of distinguishing between $2^{233} \approx 10^{70}$ Gabor Hashes. However, only a small subset of these Gabor Hashes are available from the same token. The number of available Gabor Hashes from any given token is calculated below.

From theory, we know that moving the probe beam by a small angle or displacing a small number of scatterers (see section 3) causes the speckle pattern to decorrelate completely. For our implementation the theoretically calculated value of angular displacement of the probe beam required to cause decorrelation of the speckle pattern is $\delta\theta = \lambda/(2\pi L) = 4 \times 10^{-5}$ rad. In practice, this value is ~ 40 times greater and equal to 1.7×10^{-3} rad. Linear sensitivity is challenging to calculate theoretically, but was experimentally determined to be 60μm. These results place constraints on the mechanical system that must be used to register the tokens with respect to the probe beam. Figure 6 shows the linear and angular sensitivity plots. For our 100 mm^2 token, assuming that the range of possible probe angles are bounded by $\Delta\theta = \pi/2$, we have a total of $2.37 \times 10^{10} \approx 2^{34}$ available Gabor Hashes from any given token. This number may be made larger by using higher precision probe positioning equipment. Obviously, using such equipment would increase the cost of the reader substantially.

One final point to note is the crossover point between distributions in Figure 5. The two distributions intersect at a Hamming Distance of 0.41. This means that up to $2400 * 0.41 = 984$ bits can be wrong in a given Gabor Hash before we reject it as being unre-

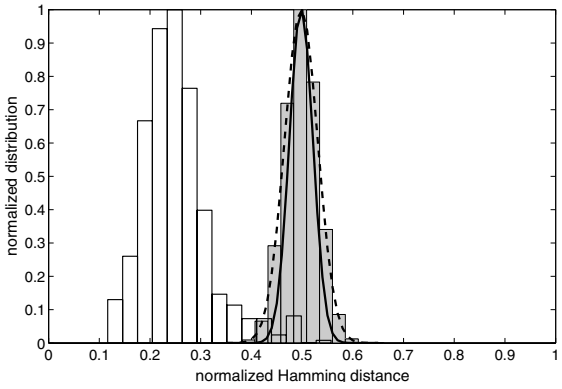

Figure 5: The normalized Hamming distances measured for Gabor Hashes. The unlike distribution, in gray, shows the distribution of 165,600 distances between unlike bitstrings; the mean of the dashed Gaussian fit is 0.50 - half the bits differ on average - and the variance is 1.07×10^{-3} (equivalent to 233 independent binomial trials). Doubling the length of the bitstring to 4800 bits by concatenating readings from two angles produces a distribution with a Gaussian fit shown by the solid curve, reducing the variance to 5.42×10^{-4}, corresponding to 461 independent binomial trials. The like distribution, in white, shows the errors in rereading 576 like bitstrings after candidates are presented to the enrolled database; the mean of 0.25 equals 1800 bits being matched correctly.

lated to a previously enrolled one. While this amount of noise tolerance is essential to keep the cost of the readers low, it offers increased probability of successful spoofing for an attacker. We will have more to say about this later. The final experiment demonstrates tamper-resistance. One Gabor Hash was enrolled in a database, and a second one was obtained from the same token after it was intentionally damaged by drilling a 1 mm deep hole in its surface with a drill of diameter 533μm. The distance between the two hashes was 0.46, thereby physically demonstrating avalanche. Figure 7 shows the results of this experiment.

Thus far, we have experimentally characterized both uniqueness - a large number of independent degrees of freedom in the Gabor Hash - and tamper-resistance - a sensitive dependence on the state of the system and the probe - in our embodiment of POWFs. We leave the discussion of unforgeability to a later section.

6 Abstraction

From a cryptographic point of view, it is useful to model POWFs as follows [17]. A (k, n)-POWF Π comprises a set of values $\{\Pi(i)\}_{i=1}^{n}$, where each $\Pi(i) \in \{0,1\}^k$ is generated independently and uniformly at random. Π may be conceptualized as a tape consisting of n cells, each of which contains a k-bit string. The value n will in general be finite in a POWF, as a reflection of practical limitations on the number of possible ways in which the underlying physical object may be read. This representation assumes that it is possible to go from a 2400-bit Gabor Hash with correlations between bits to a shorter 233-bit sequence of uncorrelated bits. This may be accomplished by one of the many available methods of entropy coding [5].

In response to a challenge $i \in \{1, 2, \ldots, n\}$ to POWF Π, the response $\Pi(i)$ is returned. This value, however, is communicated through a noisy channel ν. In other words, the response received by the challenger is a random variable $\Pi_\nu(i)$ over the space $\{0,1\}^k$ that models the effects of various types of noise on the underlying value $\Pi(i)$.

The POWF we consider has $k = 2400$ bits, although this number would go down to 233 if some form of entropy coding were used to compress a Gabor Hash. As we saw above, the number of cells (i.e., unique challenges) supported by any token is $n \approx 10^{10} \approx 2^{34}$. We note that k may be increased in practice by (a) reducing the noise in the system through better engineering and (b) using a larger detector. n can be increased by increasing the size L of the structure, decreasing the mean free path l be-

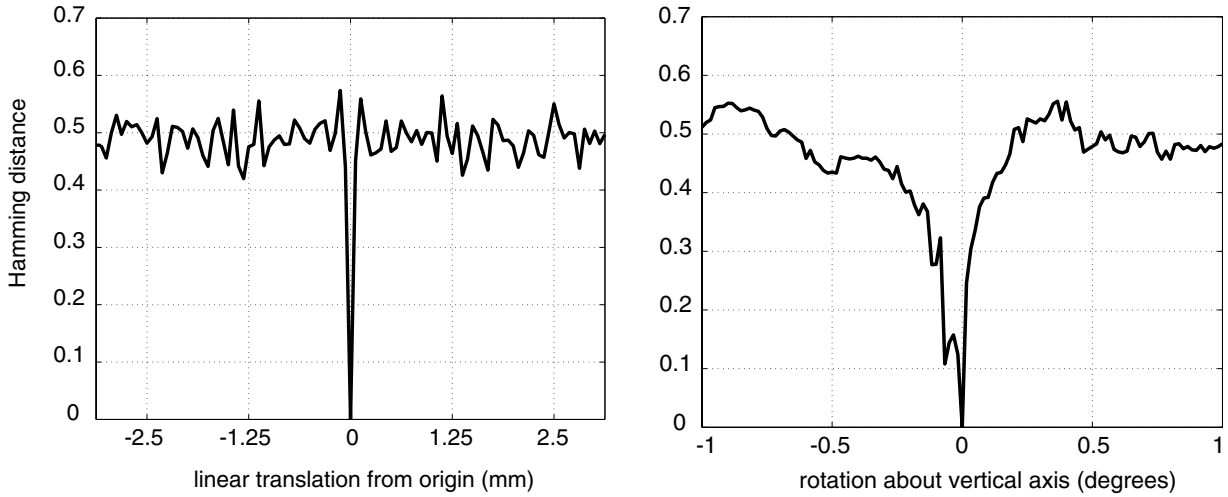

Figure 6: The plot on the left shows the Hamming distance between a reference key obtained from a central location and keys obtained as the laser is translated linearly across the surface of the token. A translation of approximately 60 microns causes the key to decorrelate completely. Data obtained for angular sensitivity show that a rotation of approximately 1.7 mrad causes full decorrelation of the key.

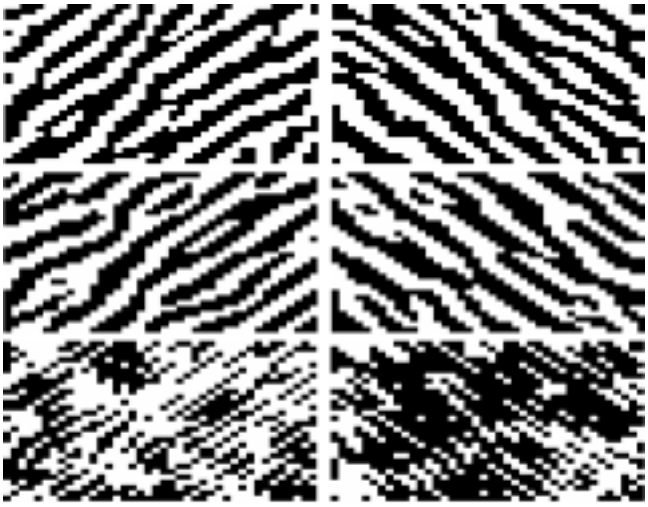

Figure 7: Demonstration of tamper resistance. The top row shows a segment of the enrolled Gabor Hash (represented as two adjacent binary images for ease of visualization), the middle row shows the same segment from the hash of an intentionally damaged token, and the bottom row shows the XOR of the previous two rows. The Hamming Distance between the top two rows is 0.46.

tween scatterers up to a limit equal to the wavelength of probe radiation, decreasing the wavelength λ of the probe radiation, and engineering higher precision probe positioning systems. One final point to note is that, from an economic point of view, increasing the size of the structure or decreasing the mean free path adds very little cost, if any, to the system.

7 Attacks

POWFs, as described here, may be used in an authentication protocol as described in Figure 8. The protocol is based on generating challenge-response pairs on secure terminals and consuming them on unsecure terminals. During the enrollment stage, several challenge-response pairs (denoted by (θ, k)) are acquired at a trusted terminal. During the verification stage of the protocol, the server challenges the token with a specific θ_i and compares the noisy response k_i' with the known k_i. The token is authenticated if the Hamming distance between k_i' and k_i is below a previously set threshold T. The challenge-response pair

(θ_i, k_i), grayed out in Figure 8, is not reused in any future transactions. As we saw earlier, the number of challenges per token is $\approx 2^{34}$. Given that up to 41% of the bits can be incorrect before we reject a spoofed Gabor Hash as having not originated in the same token, the probability that an attacker can guess the corresponding response is $2^{-233*0.59} \approx 2^{-137}$.

An attack on a POWF-based authentication system is successful if an attacker can demonstrate possession of the POWF without actually having physical access to the token. Stated more formally, we would like to enumerate the subset of cells of a (k, n)-POWF an attacker can spoof when challenged with queries $i \in \{1, 2, \ldots, n\}$. There are two classes of attacks on POWFs - physical and computational - each offering varying degrees of ease of spoofing to the attacker. Physical attacks are of interest in environments where the reader requires the presence of a 3D structure as part of the authentication process while computational attacks are relevant in scenarios where the Gabor Hashes, rather than the 3D structure itself, are used.

7.1 Physical attacks

These attacks involve creating a physical structure that emulates all or part of a (k, n)-POWF. The spectrum of attacks ranges from a static image that spoofs a single cell to holograms that spoof a small subset of cells to cloning the entire structure down to the scale of λ. The former attack may be thwarted by using the POWF in a challenge-response protocol as described in Figure 8. The holographic attack is practically infeasible owing to limitations in the ability of holographic film to store and reproduce a large number of images with no crosstalk [16]. The most difficult attack of all is the cloning attack. The principal difference between that holographic attack and the cloning attack is that the hologram aims to emulate the optical behavior of the 3D microstructure without actually creating a replica of the structure itself. The state of the art in 3D microfacrication is far behind the difficulty presented by a macroscopic 3D structure with λ-scale inhomogeneities [18]. This difficulty is further enhanced because probe samples not just the token's physical structure but also its material properties (e.g. dielectric constant) of the medium as well as those of the scatterers. This implies that in order for a cloning attack to succeed, it would have to not only recreate the structure but also its local electromagnetic attributes. Given the fact that 3D microfabrication is currently possible with only a small library of materials, it appears that a full-fledged cloning attack is infeasible using know 3D microfacrication technology. Finally, we remark that spoofing a single token does not affect the integrity of any other token.

7.2 Computational attacks

This class of attacks involves spoofing the (k, n)-POWF computationally. The simplest of these attacks is a replay attack - observe and store all possible challenges and corresponding responses for replay later. This attack is the most feasible of all and involves storage of a large amount of data. For a spoofing success probability of 100%, our (2400, $\sim 10^{10}$)-POWF requires storing 2400×2^{34} bits $\approx 2^{45}$ bits i.e., about 32 terabytes of data, which is not infeasible, but it *is* expensive. If the attacker were satisfied with a lower success rate, the storage requirements would decrease accordingly. This decrease in storage could be offset by requiring the verifying server to challenge the prover multiple times. Storage requirements drop to about 4 terabytes if the Gabor Hashes were compressed to 233 bits. Further, assuming a 10 ms acquisition time per response, it would take an attacker over 3 years to acquire responses to all possible challenges. Note that the verifier's database can be much smaller because it can select the subset of challenge-response pairs that it wants to query on in advance.

A second attack would be simulate the response to any given challenge. Assume that the volume of the token is 1 cm^3 and it is probed by light with a wave-

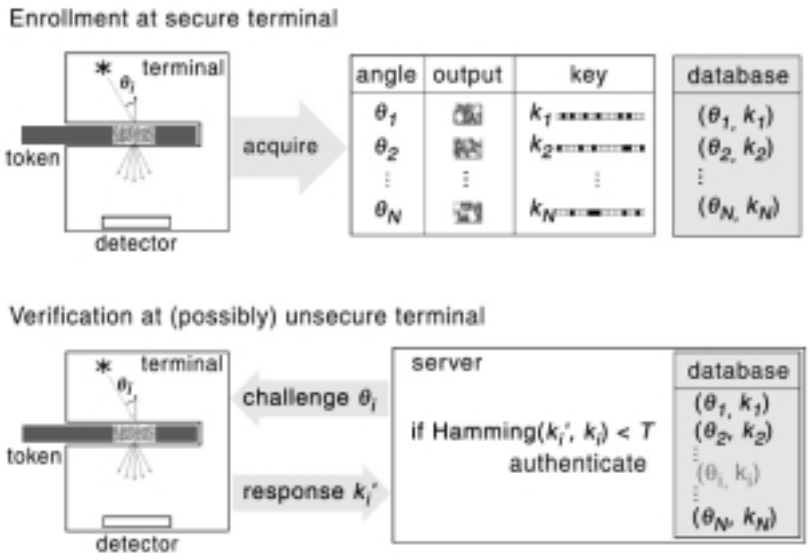

Figure 8: A challenge-response authentication protocol

length on the order of 1 μm, then its structure is specified by up to $(10^{-2}/10^{-6})^3 = 10^{12} \approx 2^{40}$ bits if the composition of each cubic block of wavelength size is random, as it would be for microscopically inhomogeneous scatterers. These bits could be used to computationally simulate the output instead of storing all possible outputs in advance. In the mesoscopic limit, a photon passing through the structure performs a random walk with a step size given by the mean free path l, covering a distance $l\sqrt{N}$ after N scattering events [23]. For the photon to emerge from the thickness L of the token requires that $L = l\sqrt{N}$ and so $N = (L/l)^2$ scattering events. At each of these steps, in a simulation it is necessary to propagate forward paths linking all pairs of scatterers, giving an total of $\sim 10^{12} \times 10^{12} \times 10^2 = 10^{26} \approx 2^{86}$ scattering simulations per scattering event. In our embodiment, $N = 625$ scattering events. In practice, simulating the scattering from even a single arbitrarily-shaped particle in the limit that its dimension is several times the wavelength presently requires a supercomputer [15]. Although simulating the response to any arbitrary challenge is not provably difficult, it does require complete knowledge of local structural and electromagnetic properties of the microstructure at the scale of λ and access to extremely high-performance computing. This presents a substantial challenge to any attacker.

Successfully spoofing a POWF involves technical measures, effort and expense which are extremely disproportional to the effort and expense of creating the POWF. This physical asymmetry is akin to the computational asymmetry encountered in cryptographic one-way functions.

8 Discussion

POWFs are expected to find utility in physical authentication systems where challenge-response protocols are employed. A typical application could be in access control, where the number of tokens is small and the data system employed usually relies on a

trusted central computer to keep track of the challenges and responses. Another potential application is in arms control treaty verification. Unlike more familiar challenge-response protocols, this one relies on the enormous amount of information that is committed in advance to the token that is read out over a long period. Beyond this, applications exist in tamper resistant packaging either as externally monitored free-standing structures or through the use of self-contained packages containing a laser, a detector which are potted in optical epoxy containing inhomogeneities. It is also worth noting that POWFs can be built at any wavelegth as long as the system is in the mesoscopic regime. Speckle patterns have been observed mesoscopic all-electronic systems by using the scattering of electrons from atomic-scale inhomogeneities [14]. Although the temperature at which these effects are observed is too low to be practically used, this line of thinking opens up new approaches to uniquely identifying electronic structures based solely on their physical structures. One area where this kind of identification is becoming increasingly important is in assigning identity to silicon chips. Recent work in silicon POWFs, Physical Unknown Functions (PUFs) and Physical Random Functions (PRFs) [3, 12] points to interesting opportunities in using the actual physical structure of silicon chips for identification, certified execution, and digital rights management.

We have shown how coherent multiple scattering in inexpensive 3D structures performs a mapping that satisfies all of the attributes of a physical source of data with properties akin to those of a noisy random oracle [17]. The value of POWFs lie in the fact that they, unlike prior physical authentication methods, makes an explicit connection with the framework of modern cryptography and thus may be viewed as another primitive in the cryptographer's toolbox, albeit one that has a physical manifestation. In cases where cryptographic authentication is neither economically nor practically feasible, POWFs offer an alternative approach.

Acknowledgements

The author thanks Ari Juels for several insightful discussions. Markus Jakobsson, Burt Kaliski, and Ari Juels also provided a large number of comments during review which greatly improved the content and readability of this article.

References

[1] C. Bennet, G. Brassard, S. Breidbard, and S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Proceedings of Crypto '82*, pages 267–275, 1982.

[2] R. Berkovits. Sensitivity of the multiple-scattering speckle pattern to the motion of a single scatterer. *Physical Review B*, 43:8638–40, 1991.

[3] D. Clarke, B. Gassend, M. van Dijk, and S. Devadas. Secure hardware processors using silicon physical one-way functions. In R. Sandu, editor, *ACM CCS '02*, 2002.

[4] D. Collon. *First Impressions: Cylinder seals in the Ancient Near East*. British Museum, London, 1987.

[5] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, New York, 1991.

[6] J. G. Daugman. Uncertainty relation for space, spatial frequency, and orientation optimized by two dimensional visual cortical filters. *Journal of the Optical Society of America*, 2:1160–9, 1985.

[7] S. Feng, C. Kane, P.A. Lee, and A.D. Stone. Correlations and fluctuations of coherent wave transmission through disordered media. *Physical Review Letters*, 61:834–7, 1988.

[8] S. Feng and P.A. Lee. Mesoscopic conductors and correlations in laser speckle patterns. *Science*, 251:633–9, 1991.

[9] Steve Fetter and Thomas Garwin. Using tags to moniitor numerical limits in arms control agreements. In Barry M. Blechman, editor, *Technology and the Limitation of International Conflict*, pages 33–54, Washington, DC, 1989. The John's Hopkins Foreign Policy Institute.

[10] Steve Fetter and Thomas Garwin. Tags. In Richard Kokoski and Sergey Koulik, editors, *Verification of Conventional Arms Control In Europe: Technological Constraints and Opportunities*, pages 139–154, Boulder, CO, 1990. Westview Press.

[11] D. Gabor. Theory of communication. *Journal of the Institute of Electrical Engineers*, 93:429–457, 1946.

[12] B. Gassend. Physical random functions. Master's thesis, Massachusetts Institute of Technology, 2003.

[13] J.W. Goodman. Statistical properties of laser speckle patterns. In J.C. Dainty, editor, *Laser Speckle and Related Phenomena*, pages 9–75, Berlin, 1975. Springer-Verlag.

[14] D. Hoadley, P. McConville, O. Norman, and N.O. Birge. Experimental comparison of the phase-breaking lengths in weak localization and universal conductance fluctuations. *Physical Review B*, 60:5617–25, 1999.

[15] A.G. Hoekstra, M.D. Grimminck, and P.M.A. Sloot. Large scale simulations of elastic light scattering by a fast discrete dipole adapproximation. *International Journal of Modern Physics C*, 9:87–102, 1998.

[16] K.M. Johnson, L. Hesselink, and J.W. Goodman. Holographic reciprocity law failure. *Appl. Optics*, 23:218–227, 1984.

[17] A. Juels and R. Pappu. Physical random oracles, 2003. manuscript in preparation.

[18] C. Marxer and N.E. de Rooij. Silicon micromechanics for the fiber-optic information highway. *Sensors and Materials*, 10:351–62, 1998.

[19] O. Nestares, R. Navarro, J. Portilla, and A. Tabernero. Efficient spatial-domain implementation of a multiscale image representation based on gabor functions. *Journal of Electronic Imaging*, 7:166–73, 1998.

[20] R. Pappu. *Physical One-Way Functions*. PhD thesis, Massachusetts Institute of Technology, 2003.

[21] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical one-way functions. *Science*, 297:2026–2030, 2002.

[22] M.C.W. van Rossum and Th.M. Nieuwenhuizen. Multiple scattering of classical waves: Microscopy, mesoscopy, and diffusion. *Reviews of Modern Physics*, 71:313–371, 1999.

[23] Bart van Tiggelen. *Multiple Scattering and Localization of Light*. PhD thesis, University of Amsterdam, 1992.

[24] W. K. Wootters and W. Zurek. A single quantum cannot be cloned. *Nature*, 299:982–83, 1982.

[25] J. Yoshida. Euro bank notes to embed RFID chips by 2005. *EE Times*. 19 December 2001. Available at www.eetimes.com/story/OEG20011219S0016.