rests on the difficulty of recreating the microstructure of macroscopic objects down to atomic length scales. This approach replaces the number-theoretical conjectures of current cryptosystems with technological constraints that have no theoretical grounding, but that do present daunting practical challenges to adversaries. Such practical limits are perhaps the most important point of all: Cryptosystems don't protect information if they're not used. The introduction of physical one-way functions greatly expands where, and how, information can be protected.

### References and Notes


1. R. L. Rivest, A. Shamir, L. Adleman, *Commun. ACM* **21**, 120 (1978).
2. W. Diffie, M. Hellman, *IEEE Trans. Inf. Theory* **IT-22**, 644 (1976).
3. M. V. Wilkes, *Time-Sharing Computer Systems* (American Elsevier, New York, 1972).
4. R. Rivest, RFC 1321: The MD5 message-digest algorithm (1992).
5. D. Atkins, M. Graff, A. K. Lenstra, P. C. Leyland, *Advances in Cryptology–ASIACRYPT'94*, J. Pieprzyk, R. N. Safavi, Eds. (Springer-Verlag, Berlin, 1995), pp. 263–277.
6. R. Anderson, M. Kuhn, *Security Protocols, 5th International Workshop*, B. Christianson, B. Crispo, M. Lomas, M. Roe, Eds. (Springer-Verlag, Berlin, 1998), pp. 125–136.
7. P. W. Shor, *SIAM J. Comput.* **26**, 1484 (1997).
8. J. R. Smith, A. V. Sutherland, *Proceedings of AutoID'99, the Workshop on Automatic Identification Advanced Technologies* (IEEE, New York, 1999), pp. 79–83.
9. R. van Renesse, *European Convention on Security and Detection* (Institution of Electrical Engineers London, 1995), pp. 45–49.
10. N. Amer, D. DiVincenzo, N. Gershenfeld, U.S. Patent 5,790,025 (1998).
11. W. K. Wootters, W. Zurek, *Nature* **299**, 982 (1982).
12. J. W. Goodman, *Laser Speckle and Related Phenomena*, J. C. Dainty, Ed. (Springer-Verlag, Berlin, 1975), pp. 9–75.
13. S. Feng, C. Kane, P. A. Lee, A. D. Stone, *Phys. Rev. Lett.* **61**, 834 (1988).
14. S. Feng, P. A. Lee, *Science* **251**, 633 (1991).
15. R. Berkovits, *Phys. Rev. B* **43**, 8638 (1991).
16. R. Pappu, thesis, Massachusetts Institute of Technology, Cambridge, MA (2001).
17. M. C. W. van Rossum, T. M. Nieuwenhuizen, *Rev. Mod. Phys.* **71**, 313 (1999).
18. A. Slocum, *Precis. Eng.* **14**, 67 (1992).
19. O. Nestares, R. Navarro, J. Portilla, A. Tabernero, *J. Electron. Imaging* **7**, 166 (1998).
20. D. Gabor, *J. Inst. Electr. Eng.* **93**, 429 (1946).
21. J. G. Daugman, *J. Opt. Soc. Am.* **2**, 1160 (1985).
22. H. V. Poor, *An Introduction to Signal Detection and Estimation* (Springer-Verlag, New York, 1994).
23. B. A. Ridley *et al.*, *Nanophase and Nanocomposite Materials III* (Materials Research Society, Warrendale, PA, 2000), pp. 115–120.
24. J. H. Smith *et al.*, *Proc. SPIE* **3514**, 42 (1998).
25. K. M. Johnson, L. Hesselink, J. W. Goodman, *Appl. Opt.* **23**, 218 (1984).
26. B. van Tiggelen, thesis, University of Amsterdam, Netherlands (1992).
27. A. G. Hoekstra, M. D. Grimminck, P. M. A. Sloot, *Int. J. Mod. Phys. C* **9**, 87 (1998).
28. B. Spivak, A. Zyuzin, *Phys. Rev. Lett.* **84**, 1970 (2000).
29. C. Marxer, N. E. de Rooij, *Sens. Mater.* **10**, 351 (1998).
30. D. Hoadley, P. McConville, O. Norman, N. O. Birge, *Phys. Rev. B* **60**, 5617 (1999).


31. Supported by the Center for Bits and Atoms (NSF grant CCR-0122419) at the MIT Media Labs and an IBM Research Fellowship (R.P.). For many helpful discussions, we thank N. Amer, I. Chuang, D. DiVincenzo, J. Jacobson, W. Plesniak, R. Rivest, D. Simon, J. Smith, and members of the Physics and Media Group. We are especially grateful to A. Juels for several insightful comments and constructive criticism.

28 May 2002; accepted 7 August 2002


REPORTS

# Quantum Solvation of Carbonyl Sulfide with Helium Atoms


**Jian Tang,[1] Yunjie Xu,[2] A. R. W. McKellar,[1]* Wolfgang Jäger[2]***



**High-resolution infrared and microwave spectra of $He_N$–carbonyl sulfide ($He_N$-OCS) clusters with $N$ ranging from 2 to 8 have been detected and unambiguously assigned. The spectra show the formation of a solvation layer beginning with an equatorial "donut" of five helium atoms around the OCS molecule. The cluster moment of inertia increases as a function of $N$ and overshoots the liquid droplet limit for $N > 5$, implying that even atoms in the first solvation shell are decoupled from the OCS rotation in helium nanodroplets. To the extent that this is due to superfluidity, the results directly explore the microscopic evolution of a phenomenon that is formally macroscopic in nature.**


One of the fundamental goals of cluster research is the interpretation of the properties of condensed phases in terms of those of their constituent atoms and molecules (*1*). However, the clusters that can be investigated systematically in detail are limited in size. In the area of superfluidity, the recent development of He nanodroplet isolation spectroscopy (*2*) helps to close the gap between cluster and bulk studies. It offers possibilities for synthesizing, stabilizing, and characterizing novel chemical species (*3*) and also constitutes an important step toward detailed microscopic understanding of superfluidity, a collective bulk property.

In an elegant nanomatrix study, the microscopic Andronikashvili experiment, Toennies and co-workers (*4*) used the appearance of sharp infrared (IR) spectral features of dopant molecules in He nanodroplets (consisting of several thousand He atoms) as an indicator of the onset of the superfluidity. Carbonyl sulfide (OCS) was used as the dopant molecule in $^3$He droplets in these experiments. Line widths in the OCS spectrum were monitored as a function of the number of captured $^4$He atoms. About 60 $^4$He atoms, corresponding to roughly two solvation layers of $^4$He around OCS, were required to induce sharp gas-phase–like spectral features indicative of nearly free rotation of the molecule. Various models have been advanced to explain the observation (*5–7*). Explicit simulations (*8*) show that the decoupling of the solvent from the molecule is associated with the onset of superfluidity (*5*).

Can the onset of superfluidity be fully traced using high-resolution spectroscopy in the small to intermediate cluster size regime, and which observables can be used as indicators of superfluidity? Advances in theoretical models and computing power may give answers to the latter question. Simulations provide predictions of observable properties such as frequency shifts and rotational constants, along with nonobservables, such as He density profiles and superfluid character. Gianturco, Whaley, and co-workers (*5*, *9*, *10*) performed diffusion Monte Carlo calculations for $He_N$-OCS clusters with $N = 1$ to 100 and found a sharp energy signature upon completion of the first solvation shell at $N \approx 20$. The CO vibrational frequency saturated at $N \approx 20$ and reached a value in qualitative agreement with nanodroplet experiments (*4*). Simulations also suggest that the rotational constant $B$ (proportional to the inverse moment of inertia) of $He_N$-molecule systems saturates at relatively small $N$; for example, $N = 8$ for the $SF_6$ molecule (*5*), attaining the limiting nanodroplet value (*11*).

An ideal experiment would isolate small- to medium-sized $He_N$-molecule clusters and characterize them sequentially until dramatic changes in spectroscopic observables indicated the onset of superfluidity. $He_N$-OCS is an ideal test system because OCS is a strong chromophore in both the IR and the microwave regions. In addition, the $He_1$-OCS complex is well characterized spectroscopically (*12*, *13*) and several high-quality potential energy surfaces (PESs) have been constructed for it (*12*, *14*, *15*).

We have measured and assigned rotationally resolved microwave and IR spectra of $He_N$-OCS clusters with $N = 2$ to 8 and observed IR spectra of larger clusters with $N$ up to about 20. The experiments were carried out using an IR diode laser spectrometer and a molecular beam Fourier-transform microwave spectrometer, as described previously (*16–18*). Clusters were generated using pulsed supersonic jet expansions of trace amounts (<0.1%) of OCS in He at backing pressures ranging from 10 to 30 atm. For the larger clusters, the jet nozzles were cooled to temperatures as low as −80°C. Microwave spectra of the singly substituted minor isotopomers were observed in natural abundance,


[1]Steacie Institute for Molecular Sciences, National Research Council of Canada, Ottawa, Ontario K1A 0R6, Canada. [2]Department of Chemistry, University of Alberta, Edmonton, Alberta T6G 2G2, Canada.

*To whom correspondence should be addressed. E-mail: robert.mckellar@nrc.ca (A.R.W.M.); wolfgang.jaeger@ualberta.ca (W.J.)

25. M. R. Singleton, D. B. Wigley, *J. Bacteriol.* **184**, 1819 (2002).
26. J. M. Caruthers, D. B. McKay, *Curr. Opin. Struct. Biol.* **12**, 123 (2002).
27. J. P. Abrahams, A. G. Leslie, R. Lutter, J. E. Walker, *Nature* **370**, 621 (1994).
28. L. Holm, C. Sander, *Trends. Biochem. Sci.* **20**, 478 (1995).
29. S. S. Velankar, P. Soultanas, M. S. Dillingham, H. S. Subramanya, D. B. Wigley, *Cell* **97**, 75 (1999).
30. R. M. Story, H. Li, J. N. Abelson, *Proc. Natl. Acad. Sci. U.S.A.* **98**, 1465 (2001).
31. E. R. Johnson, D. B. McKay, *RNA* **5**, 1526 (1999).
32. J. M. Caruthers, E. R. Johnson, D. B. McKay, *Proc. Natl. Acad. Sci. U.S.A.* **97**, 13080 (2000).
33. C. van der Does *et al.*, *Mol. Microbiol.* **22**, 619 (1996).
34. J. Eichler, W. Wickner, *Proc. Natl. Acad. Sci. U.S.A.* **94**, 5574 (1997).
35. P. Fekkes, J. G. de Wit, A. Boorsma, R. H. Friesen, A. J. Driessen, *Biochemistry* **38**, 5111 (1999).
36. P. Fekkes, C. van der Does, A. J. Driessen, *EMBO J.* **16**, 6105 (1997).
37. E. Breukink *et al.*, *J. Biol. Chem.* **270**, 7902 (1995).
38. V. Ramamurthy, D. Oliver, *J. Biol. Chem.* **272**, 23239 (1997).
39. V. Dapic, D. Oliver, *J. Biol. Chem.* **275**, 25000 (2000).
40. S. Snyders, V. Ramamurthy, D. Oliver, *J. Biol. Chem.* **272**, 11302 (1997).
41. C. van der Does, E. H. Manting, A. Kaufmann, M. Lutz, A. J. Driessen, *Biochemistry* **37**, 201 (1998).
42. T. Rajapandi, D. Oliver, *Biochem. Biophys. Res. Commun.* **200**, 1477 (1994).
43. R. Salavati, D. Oliver, *J. Mol. Biol.* **265**, 142 (1997).
44. H. Nakatogawa, K. Ito, *Mol. Cell* **7**, 185 (2001).
45. S. Korolev, J. Hsieh, G. H. Gauss, T. M. Lohman, G. Waksman, *Cell* **90**, 635 (1997).
46. J. L. Kim *et al.*, *Structure* **6**, 89 (1998).
47. R. L. Woodbury, S. J. Hardy, L. L. Randall, *Protein Sci.* **11**, 875 (2002).
48. R. I. Menz, J. E. Walker, A. G. Leslie, *Cell* **106**, 331 (2001).
49. N. D. Ulbrandt, E. London, D. B. Oliver, *J. Biol. Chem.* **267**, 15184 (1992).
50. V. Ramamurthy, V. Dapic, D. Oliver, *J. Bacteriol.* **180**, 6419 (1998).
51. H. Ding, I. Mukerji, D. Oliver, *Biochemistry* **40**, 1835 (2001).
52. M. Schmidt, H. Ding, V. Ramamurthy, I. Mukerji, D. Oliver, *J. Biol. Chem.* **275**, 15440 (2000).
53. K. Nishiyama, T. Suzuki, H. Tokuda, *Cell* **85**, 71 (1996).
54. G. Matsumoto, H. Nakatogawa, H. Mori, K. Ito, *Genes Cells* **5**, 991 (2000).
55. J. R. Lakowicz, *Principles of Fluorescence Spectroscopy* (Plenum, New York, 1983).
56. J. J. Fak, J. Benach, A. Itkin, L. Gierasch, J. F. Hunt, in preparation.
57. M. Song, H. Kim, *J. Biochem.* **122**, 1010 (1997).
58. J. D. Fikes, P. J. Bassford Jr., *J. Bacteriol.* **171**, 402 (1989).
59. J. L. Huie, T. J. Silhavy, *J. Bacteriol.* **177**, 3518 (1995).
60. J. Drenth, *Principles of Protein X-ray Crystallography* (Springer-Verlag, New York, 1994).
61. We thank T. Rajapandi for construction of the N96C mutant of *B. subtilis* SecA; H. Ding for advanced access to the single-tryptophan substitution mutants of *E. coli* SecA; and M. Machius, D. Xia, R. Krishnaraj, and other members of the Deisenhofer, Sprang, and Goldsmith lab groups for advice and for assistance with crystallographic data collection. We also thank W. Hendrickson for a critical review of the manuscript and L. Gierasch, G. Wittrock, R. Chou, A. Driessen, T. Economu, and B. DeKruijff for insightful conversations. We acknowledge support during synchrotron data collection from M. Capel, T. Langdon, and C. Ogata of the National Synchrotron Light Source (NSLS); W. Miller, M. Szebenyi, and D. Thiel of Cornell High Energy Synchrotron Source (CHESS); and A. Thompson and B. Rassmussen of the European Synchrotron Radiation Facility (ESRF). We particularly thank A. Weaver and R. Cabelli for their pioneering efforts in initiating this project using *E. coli* SecA. The Howard Hughes Medical Institute supported this project in J.D.'s laboratory, and a startup grant from Columbia University and a grant from NIH General Medical Sciences supported the continuation of this project in J.F.H.'s laboratory. Coordinates and structure factors for the nucleotide-free and Mg-ADP–bound structures have been deposited in the PDB under accession codes 1M6N and 1M74, respectively.

**Supporting Online Material**

www.sciencemag.org/cgi/content/full/297/5589/2018/DC1
Materials and Methods
SOM Text
Figs. S1 to S8
References and Notes

28 May 2002; accepted 5 August 2002

REPORTS

# Physical One-Way Functions

**Ravikanth Pappu,*† Ben Recht, Jason Taylor, Neil Gershenfeld**

**Modern cryptographic practice rests on the use of one-way functions, which are easy to evaluate but difficult to invert. Unfortunately, commonly used one-way functions are either based on unproven conjectures or have known vulnerabilities. We show that instead of relying on number theory, the mesoscopic physics of coherent transport through a disordered medium can be used to allocate and authenticate unique identifiers by physically reducing the medium's microstructure to a fixed-length string of binary digits. These physical one-way functions are inexpensive to fabricate, prohibitively difficult to duplicate, admit no compact mathematical representation, and are intrinsically tamper-resistant. We provide an authentication protocol based on the enormous address space that is a principal characteristic of physical one-way functions.**

Information security requires a mechanism that provides significant asymmetry in the effort required to make intended and unintended uses of encoded information. Such protection is growing in importance as an increasing fraction of economic activity is communicated electronically; sending credit card numbers over the Internet or spending money stored in a smart card's memory assumes that these data cannot easily be duplicated.

Modern cryptographic practice rests on the use of one-way functions. These are functions that are easy to evaluate in the forward direction but infeasible to compute in the reverse direction without additional information. For example, multiplying large prime numbers can be done in a time that is a polynomial function of their size, but finding the prime factors of the product is believed to require exponential time (*1*). Another important example is the ease of modular exponentiation (evaluating $a = b^c \bmod d$ for integers $b$, $c$, and $d = 2p + 1$, where $d$ and $p$ are large primes) versus the difficulty of taking discrete logarithms (finding the integer $c$, given $a$, $b$, and a prime $d$) (*2*).

Cryptographic applications that have variable-length inputs, such as storing computer passwords (*3*) or digitally signing secure electronic documents (*4*), use one-way hash functions as a cryptographic primitive. A hash function compresses an arbitrary-length input to a fixed-length output and has the avalanche property that changing one bit in the input flips roughly half the bits in the output. A one-way hash function has preimage resistance (it is infeasible to find an input that produces a given output), and it can also have collision resistance (it is difficult to find two inputs that produce the same output).

Although algorithmic one-way functions are widely used, they are facing a number of challenges. The first is technological, as massively parallel networks of computers break codes that had been considered safe (*5*) and secure processors containing keys are reverse-engineered (*6*). The second is fundamental, because the cryptographic primitives used are believed to be secure, but there is no proof that efficient attacks don't exist. Such attacks are in fact known using quantum computers; it is shown in (*7*) that factoring the product of two large prime numbers can be accomplished in polynomial time on a quantum computer. The third and perhaps most serious challenge is practical: The demands placed on the physical embodiments

Center for Bits and Atoms, The MIT Media Labs, 20 Ames Street, Cambridge, MA 02139, USA.

*Present address: ThingMagic, One Broadway, 14th Floor, Cambridge, MA 02142, USA.
†To whom correspondence should be addressed. E-mail: ravi@thingmagic.com

of one-way functions by emerging embedded applications such as smart cards and authenticated devices go beyond the cost and packaging constraints of conventional semiconductor technology.

We show here that all of these issues can be addressed by using coherent multiple scattering from inhomogeneous structures rather than number theory to implement one-way functions. Two-dimensional (2D) (*8*) and 3D inhomogeneous structures (*9*) have been used as tokens that are difficult to forge, and coherent scattering has been used to detect tampering of secure structures (*10*), but these approaches did not consider the effective computation performed by the physical probe. We describe the use of that capability to create authentication systems. The use of physical mechanisms for cryptography is well known in quantum cryptography, which is based on the impossibility of cloning quantum information (*11*). Unlike quantum cryptography, however, the approach described here can be used over a classical communications channel.

Laser speckle fluctuations (*12*) are a familiar demonstration of the sensitivity of the scattering of coherent radiation to the structure of inhomogeneous media. In the mesoscopic limit of scattering in a 3D structure (*13*, *14*), the mean free path $l$ between elastic collisions with scatterers is much larger than the wavelength $\lambda$ 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 $\delta\theta = \lambda/(2\pi L)$ (*15*).

Because any changes in the microstructure of a disordered medium cause an order unity change in its speckle pattern, a discretely sampled image of speckle intensity provides a fixed-length key that hashes the specification of the 3D spatial distribution of the scatterers. In the embodiment described here, we used a $\lambda$ = 632.8 nm HeNe laser beam to illuminate optical epoxy tokens measuring 10 by 10 by 2.5 mm$^3$, containing glass spheres 500 to 800 $\mu$m in diameter (representing about \$0.01 worth of materials) (*16*). The density of spheres was chosen to give an average spacing on the order of 100 $\mu$m, which equals the photon mean free path in the limit of strong scattering applicable here (*17*). The resulting speckle patterns were recorded with a 320 × 240 pixel charge-coupled device camera (Fig. 1A). The tokens were mechanically registered with an inexpensive kinematic mount, which allows submicron positional accuracy in six degrees of freedom (*18*), providing repeatability of the registration system (Fig. 1B).

The speckle patterns were then filtered by a Gabor transform to produce a 2400-bit key. This transform represents the image intensity as a discrete multiscale decomposition over oriented filter kernels with varying spatial frequency

$$g(x,y) = e^{-[\pi(a2(x-x_0)2+b2(y-y_0)2)]}$$

$$e^{[2\pi if(x\cos\theta+y\sin\theta)]}$$

where the filter parameters were selected according to (*19*) to reject both pixel-scale noise and average image intensity variations, while rendering the key relatively insensitive to mechanical misregistration. The 1D version of this transform was proposed by Gabor (*20*), and it was extended to 2D by Daugman (*21*), who showed that these filters are jointly optimal in providing the maximum possible resolution for information about the orientation and spatial frequency content of local image structure simultaneously with its 2D location.

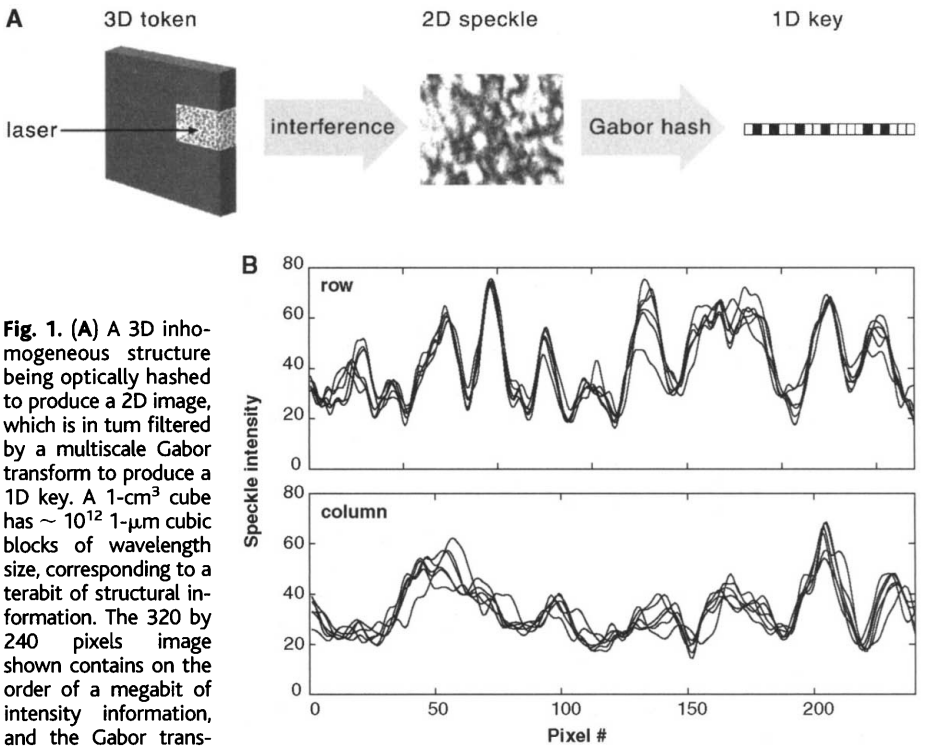


**Fig. 1.** (**A**) A 3D inhomogeneous structure being optically hashed to produce a 2D image, which is in turn filtered by a multiscale Gabor transform to produce a 1D key. A 1-cm$^3$ cube has ~ $10^{12}$ 1-$\mu$m cubic blocks of wavelength size, corresponding to a terabit of structural information. The 320 by 240 pixels image shown contains on the order of a megabit of intensity information, and the Gabor transform reduces this to a 2400-bit key. (**B**) The two plots show intensity variation along a specific row and column of the speckle pattern as a function of repeated removal and reinsertion of the token into the kinematic mount. The repeatability of the registration system is demonstrated by the overlaid traces; the remaining variability between measurements is filtered with a multiscale Gabor transform.

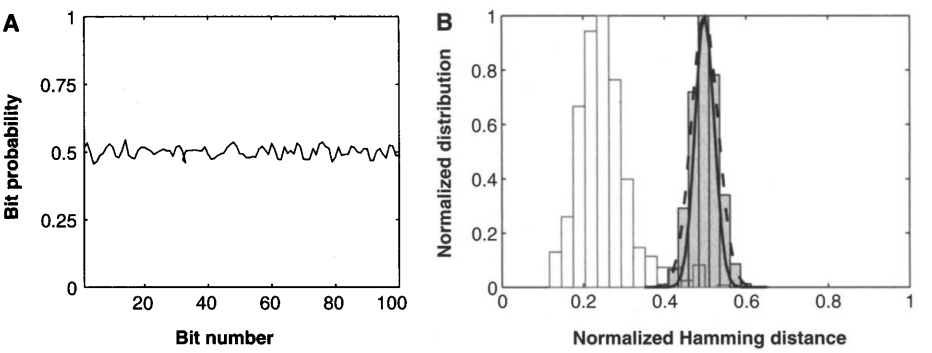


**Fig. 2.** (**A**) The probability of a bit being set in the key, determined by averaging over an ensemble of 576 keys. For clarity, only the first 100 bits are shown. The average value is 0.50. (**B**) The normalized Hamming distances measured for 2400-bit keys. The unlike distribution, in gray, shows 165,600 distances between unlike keys; the mean of the dashed Gaussian fit is 0.50 (half the bits differ), and the variance is 1.07 $10^{-3}$ (equivalent to 233 independent binomial trials). Doubling the key length to 4800 bits by pairing 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 keys after routine handling of the tokens; the mean of 0.25 equals 1800 bits being matched correctly.

To experimentally determine the behavior of the physical one-way function (POWF), four physical tokens were produced, and speckle patterns were recorded at 144 distinguishable angles for each token, giving 576 keys. Plotting the probability of each of the bits in the key being set (Fig. 2A), we see that the average probability is approximately 0.50, indicating that this is a bitwise maximum entropy code. There are, however, correlations among the bits. Figure 2B shows the distribution of Hamming distances (the number of bits that differ, normalized in the plot so that 1.0 represents a difference in all 2400 bits) among these keys and between the keys when they were remeasured after the tokens were subjected to routine handling. In the ensuing discussion, "like keys" are keys that have the same origin (that is, keys derived from a token interrogated under identical conditions), whereas "unlike keys" are those that have distinct origins. We also refer to the distribution of Hamming distances between like keys as the like distribution. The corresponding term for unlike keys is the unlike distribution.

The mean distance between the unlike key pairs is 0.5 (a 1200-bit difference), with a variance of $1.07 \times 10^{-3}$, and the mean distance between like key pairs is 0.25, with a variance of $4.7 \times 10^{-3}$. The Hamming distance at which the two distributions intersect is 0.41. If the unlike distribution were binomial, this would correspond to 233 independent identically distributed variables. This experimental value does not change if half of the keys are discarded, as expected for a data set size that is adequate for estimating a distribution. Hence, our POWF provides a theoretical key space size on the order of $2^{233}$ distinguishable keys.

The overlap between the like and unlike distributions can be made as small as desired by reading each token from more than one angle, because each angle generates essentially independent information. To demonstrate this, readings from pairs of angles were combined to form 4800-bit keys in a data set with 165,600/2 = 82,800 entries. The resulting distribution of the interkey distances had the same mean (0.5) and a variance of $5.42 \times 10^{-4}$, corresponding to $0.5(1 - 0.5)/5.42 \times 10^{-4} \approx 461$ independent variables, effectively doubling the previous number by doubling the key size used.

To decide whether a candidate token placed in a terminal is the same as a token previously enrolled in the database, the minimum probability-of-error decision rule is to reject the candidate when the probability that tokens are the same is less than or equal to the probability that the tokens are different (*22*). By fitting a Gaussian probability density function to the like and unlike distributions, we arrive at a decision rule that rejects a token's authenticity if the keys differ by more than $0.41 \times 2400 = 984$ bits. For our data, the probability that this corresponds to a false reject is $9.8 \times 10^{-3}$. Because each measurement is independent of the others, this probability may be made exponentially small by taking measurements from multiple angles and applying the same decision rule.

Under normal handling, the dimensional stability of the materials used provides the repeatability shown in Fig. 1B, but the measurement should fail if the token is intentionally modified. A test of this tamper resistance was performed by drilling a small hole with a no. 75 drill (533 μm in diameter) approximately 1 mm deep into the token. The keys produced before and after the tampering had a normalized Hamming distance of 0.46 (differing in roughly half their bits), thereby demonstrating the avalanche property for our POWF. To protect the token from accidental damage, it can be encapsulated in a scratch-resistant material, and the multiscale Gabor transform can be tuned to reject speckle features arising from surface scratches while preserving features that originate from the internal microstructure.

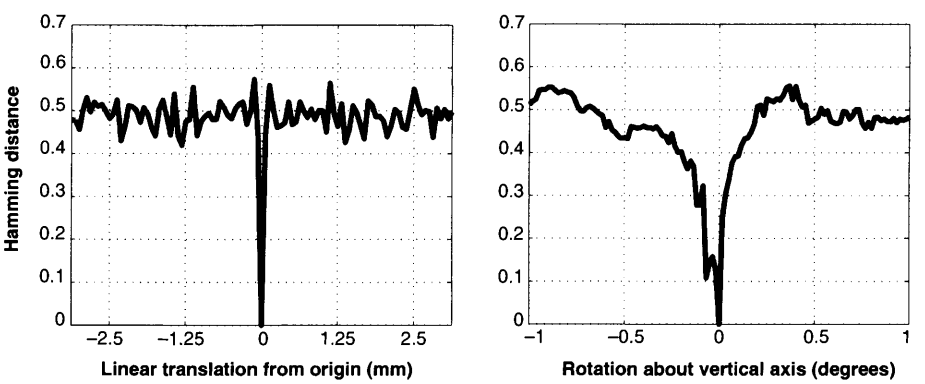


**Fig. 3.** These data quantify the sensitivity of the key as the probe is moved relative to the token. The plot on the left shows the Hamming distance between a reference key obtained from a central location and keys obtained as the laser is translated linearly across the surface of the token. A translation of approximately 60 μm 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.

An even greater concern than tampering is the possibility of duplication of the token. A number of mature techniques could be used to determine the 3D structure of the scatterers, including invasive microscopic sectioning or polishing, and noninvasive tomographic imaging. Given such a description, however, cloning the token is still quite daunting. As noted above, submicron changes in scatterer location can cause order unity changes in output speckle intensity. Thus, a cloning scheme would need to be able to reproduce submicron feature sizes. Tabletop printing techniques now make it possible to produce arbitrary 2D structures with submicron feature sizes (*23*), but the state of the art in 3D microelectromechanical systems fabrication is still a five-layer process (*24*). Although this number will no doubt increase over time, it is still many orders of magnitude away from the tens of thousands of layers that would be needed to make arbitrary centimeter-scale objects with submicron feature sizes, and the capital expenditure for the facilities presently used for microfabrication is even more orders of magnitude away from the economic value that is protected by a typical authentication token.

An alternative to copying the physical structure of a token is to try to reproduce its behavior under arbitrary illumination. Using the numbers given above, in theory an angle change of $\delta\theta = \lambda/(2\pi L) = 4 \times 10^{-5}$ rad will produce an independent speckle pattern. If the range of accessible angles is bounded by $\Delta\theta = \pi/2$, across the input solid angle there is a total of $(\Delta\theta/\delta\theta)^2 = 10^9$ distinct patterns. Translating the 1-mm$^2$ beam over the 100-mm$^2$ token surface multiplies that by a factor of 100, producing $10^{11}$ distinguishable patterns, and that number can be increased still further by varying the amplitude, phase, and wavelength distribution of the illumination. This value will be reduced slightly by spatial correlations in the speckle pattern that are removed by the hash (*13*). Figure 3 shows the measured sensitivity of a key under translation and rotation of the token. We obtained a linear sensitivity of 60 μm and an angular sensitivity of 1.7 mrad, giving a total of $2.37 \times 10^{10}$ 2400-bit keys available from the 100-mm$^2$ token surface.

Another attack would be to emulate these speckle patterns by a hologram or diffractive optical element. Beyond the obvious constraint of having to record $10^{11}$ or more distinct interference patterns in order to produce the hologram, the incoherent superposition of these $N$ patterns decreases the overall diffraction efficiency of the hologram by $1/N$, making them all effectively unobservable (*25*).

Because the coherent optical output is detected as an incoherent image, which is then reduced to a key, an adversary with access to a terminal may be able to read an incoming query and then respond from a table of acquired keys; this is a replay attack. Here, the

problem is one of storage: With $10^{11}$ or more possible queries, even a $10^3$-bit key requires at least $10^{14}$ bits of storage for all possible measurements. The physical structure itself does not contain that much information, however; if its volume is on the order of 1 $cm^3$ and it is probed by light with a wavelength on the order of 1 μm, then its structure is specified by up to $(10^{-2}/10^{-6})^3 = 10^{12}$ 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 (*26*). For the photon to emerge from the thickness $L$ of the token requires that $L = l\sqrt{N}$ and so $N = (L/l)^2$, which equals 625 steps using the numbers given above. At each of these steps, it is necessary in a simulation to propagate forward paths linking all pairs of scatterers, giving an infeasible total of $\sim 10^{12} \times 10^{12} \times 10^2 = 10^{26}$ operations. Practically, 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 (*27*).

The reason why the preceding approaches to compromising the token or terminal are infeasible is that the space of possible pairs of input illumination and output keys is so large. This can be viewed as a functional mapping, producing a response to a challenge specifying the parameters of the illumination. Unlike more familiar challenge-response protocols, however, this one uses an enormous amount of information that is committed in advance to the token. This precommitted information can be used to read the token on an unsecure terminal that is completely controlled by an untrusted user (Fig. 4). First, when the token is read on a trusted terminal, several randomly chosen illumination-key pairs are acquired and stored at a secure site. Later, when an authentication request is made from an unknown or unreliable terminal, it can be challenged with one of the previously stored illuminations and asked to produce a key. Because that pair will not have been seen outside of the trusted terminal, the only way to reproduce it is by having access to the physical token. Further, as the pair is used only once, the challenge and response can be sent over a public channel. This process can continue as needed, generating illumination-key pairs on secure terminals and consuming them on unsecure terminals, without ever needing to repeat a measurement over the useful lifetime of the token.The generation of the key establishes a shared secret between the secure site and the holder of the token; beyond authentication, this mechanism can be used for key distribution for use in conventional cryptosystems.

The security of this scheme rests on the infeasibility of storing all illumination-key pairs. The parameterization of the illumination by its orientation, location, and wavelength leads to an enormous address space, but one that is still linear in the input degrees of freedom because independent illumination patterns add linearly (but coherently) so they could be expanded in such a basis. However, this space can be made exponentially large by using a nonlinear scattering medium that is excited with a two-photon process (*28*). The address space then becomes that of all possible complex-valued illumination patterns, up to a resolution set by the mesoscopic scale. Because the number of these patterns is exponential in $(L/l)^3$, this number can easily exceed not just technological but cosmological limits.

The preceding discussion has assumed a distinction between the token and the terminal, but the scattering medium can itself be embedded in a larger system to authenticate the system's identity. Further, it could be used to encapsulate essential elements of the system to guard against tampering. For example, a sensor used in treaty verification could be potted with scatterers so that both the identity and integrity of the sensor could be queried along with the value of its readings. The only secret information required (the illumination-key pairs to be used) is stored at a remote secure site; unlike existing tamper-proof chips, the workings of the POWF can be openly disclosed.

An optical scheme does require means to generate, modulate, and record the radiation, adding substantial functionality to what might otherwise be an all-electronic system. Although integrated micromechanical optics (*29*) could be used to simplify the terminal, it may become possible to employ a similar mesoscopic approach in an electronic system by using the scattering of electrons from atomic-scale inhomogeneities within their coherence length (*30*). This would also push the length scale for attempting to fabricate a duplicate token down to the same atomic scale.

Building on the mature practice of using complex physical structures for authentication, we have shown that coherent multiple scattering in the mesoscopic regime performs a mapping that satisfies all of the attributes of a noisy one-way function, and that the enormous difference between the amount of information available in such a structure and what is actually used provides an address space that can be used like a one-time pad that is generated as needed. The real value of such a scheme comes when it is embedded as a primitive in a larger distributed cryptographic system, viewing the physical interaction as a part of the overall computation that is distinguished by the speed with which it can transform an enormous amount of information at very low cost. Given the infeasibility of compactly representing this process, the security ultimately

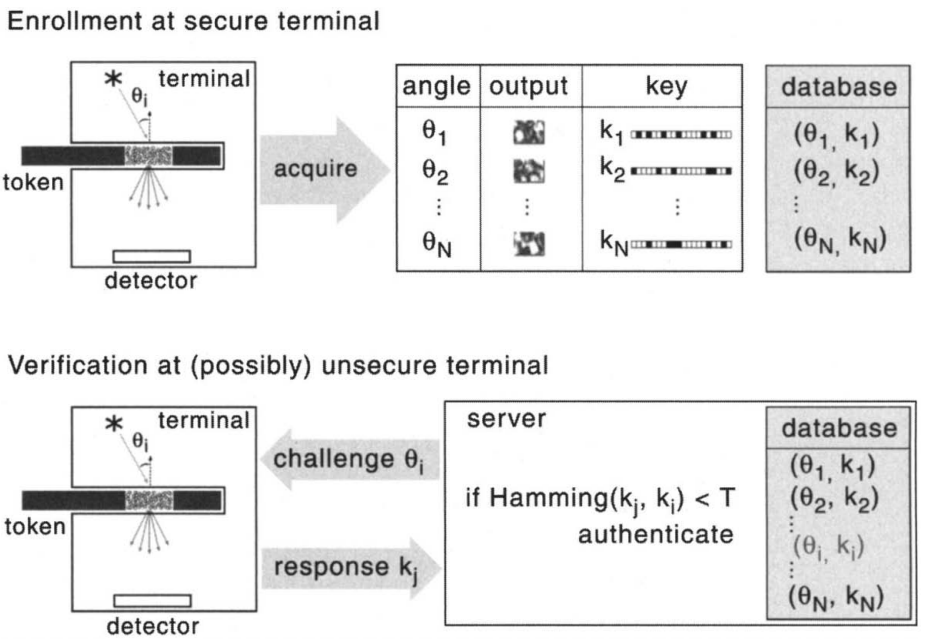


**Fig. 4.** A simple authentication protocol based on generating illumination-key pairs on secure terminals and consuming them on unsecure terminals. During the enrollment stage, several illumination-key pairs [denoted by $(\theta, k)$] are acquired at a trusted terminal. During the verification stage of the protocol, the server challenges the token with a specific $\theta_j$ and compares the response $k_j$ with the known $k_i$. The token is authenticated if the Hamming distance between $k_j$ and $k_i$ is below a previously set threshold $T$. The illumination-key pair $(\theta_i, k_i)$, grayed out in the figure, is not reused in any future transactions.