Physical Unclonable Functions for Secure Communication

Roarke Horstmeyer[1], Benjamin Judkewitz[1], Ivo Vellekoop[2] and Changhuei Yang[1]

[1]Department of Electrical Engineering, California Institute of Technology, Pasadena, CA, USA [2]University of Twente, Enschede, The Netherlands

Abstract: All encryption schemes rely on the use of suitably random keys to ensure security. Here, the feasibility of using an object's microscopic randomness to generate these communication keys is experimentally investigated. The physical disorder of a volumetric material can be converted into a one-way hash function through a simple optical probe-and-detect setup. Benefits of physical randomness storage over algorithmic constructions include efficiency, resilience against characterization or modeling, and the near-impossibility of cloning. Noise is accounted for using a fuzzy commitment-based communication scheme. Future work is focused on jointly optimizing the physical and digital post-processing steps required of a successful device.

Background

-Sending coherent light through a volumetric scattering medium generates a highly randomized interference pattern – "speckle".

-Slightly changing the incident light wave can create an equally random yet independent speckle pattern.

-Digitally detecting many independent speckle patterns generates a large set of random numbers.

-Experiments indicate the total useful randomness of a volumetric scatterer is on the order of 10^{10} bits in the absence of noise.

References

1. R. Pappu, B. Recht, J. Taylor and N. Gershenfeld, Physical one-way functions, Science 297, 2002
2. B. Skoric, On the entropy of keys derived from speckle, J. Opt. A: Pure App. Opt. 10, 055304 (2008)
3. P. Tuyls, B. Skoric and T. Kevenaar, Security with Noisy Data: Private Biometrics, Secure Key Storage and Anit-Counterfeiting. Springer 2007
4. Y. Dodis, L. Reyzin and A. Smith, Fuzzy Extractors: a brief survey of results from 2004-2006, (chapter in above)
5. P. Elias, The efficient construction of an unbiased random sequence, Ann. Math Stat. 43 (3), 1972
6. M. Matsui, Linear Cryptanalysis method for DES cipher, EUROCRYPT 1993: 386-397
7. G. Marsaglia, DieHard Battery of Tests of Randomness, http://www.stat.fsu.edu/pub/diehard

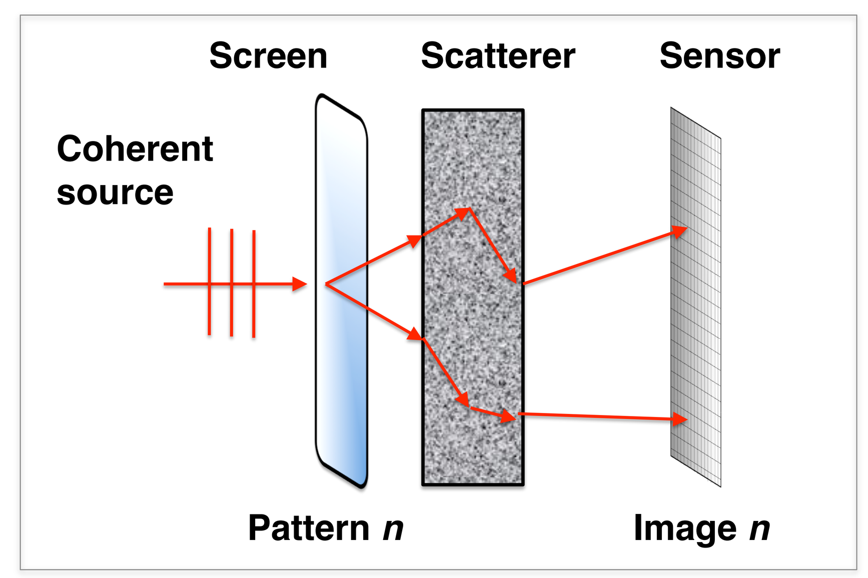
Acknowledgements

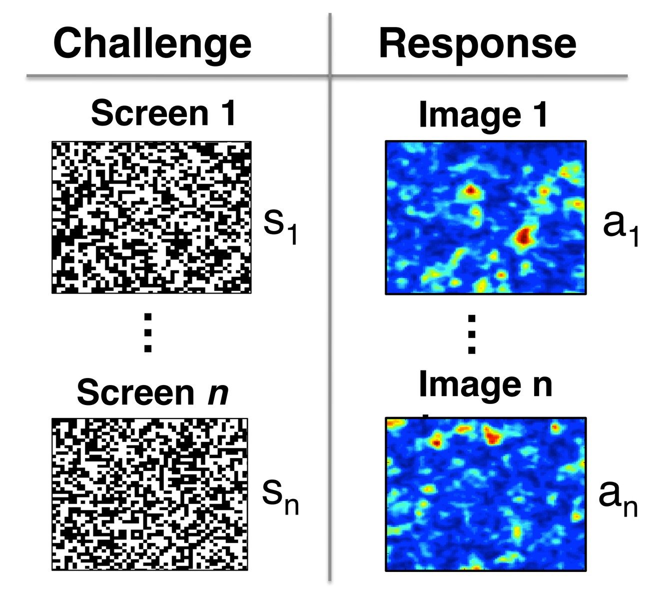
This work is supported in part by an NDSEG Scholarship

Contact: Roarke Horstmeyer, roarke@caltech.edu
Webiste: http://www.biophot.caltech.edu

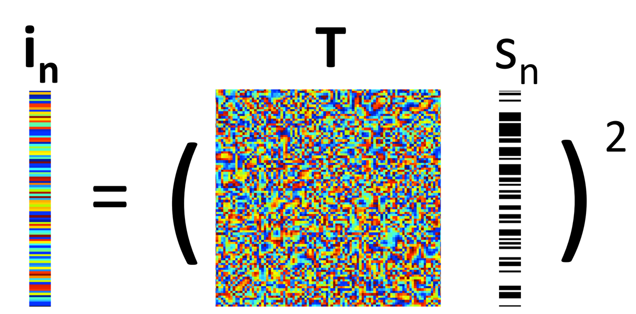
Setup and Theory

-Randomly vary phase of input light with an SLM screen
-Digitally detect output interference pattern (intensity)
-Generate many random [*Challenge*, *Response*] key pairs[1,2]





A. Transmission matrix formulation



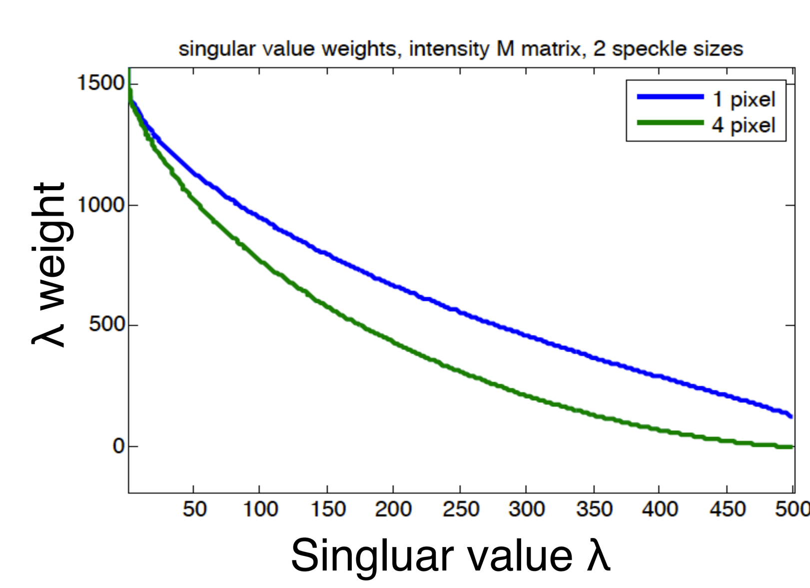
i_n = image ~ 10^6 pixels
s_n = screen pattern ~ 10^6 pixels
T = scattering matrix ~ $(10^6)^2$ (complex)

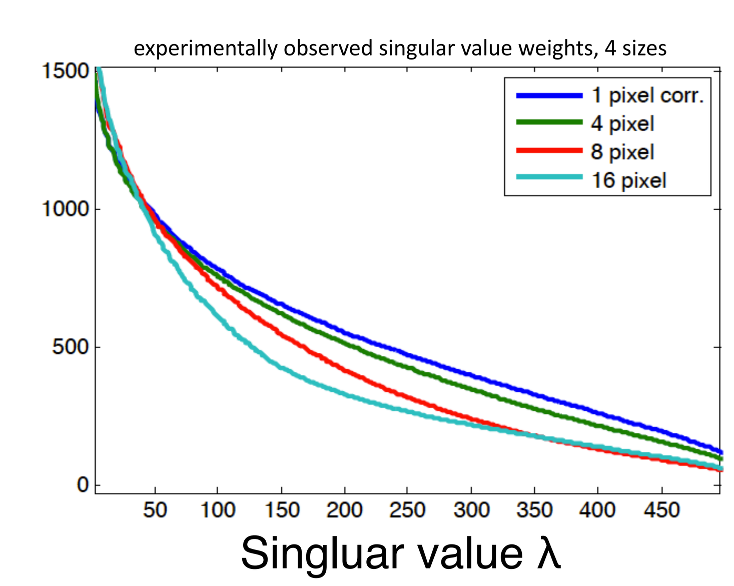
B. Size of key space

$$\frac{\#\text{ useful random bits}}{\text{device}} = \frac{\#\text{ useful random bits}}{1\text{ speckle image}} \times \frac{\#\text{ independent speckle images}}{\text{device}}$$

random bits / image = speckle entropy ≈ $|i_n|$/speckle size ≈ 10^5

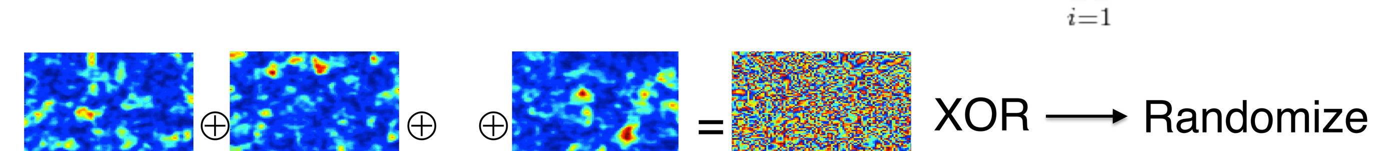
independent images / device ~ addressable column space of T = $-\sum_{n=1}^{N}\frac{\lambda_n}{N}\log\left(\frac{\lambda_n}{N}\right) \approx 10^5$





C. Removing correlation

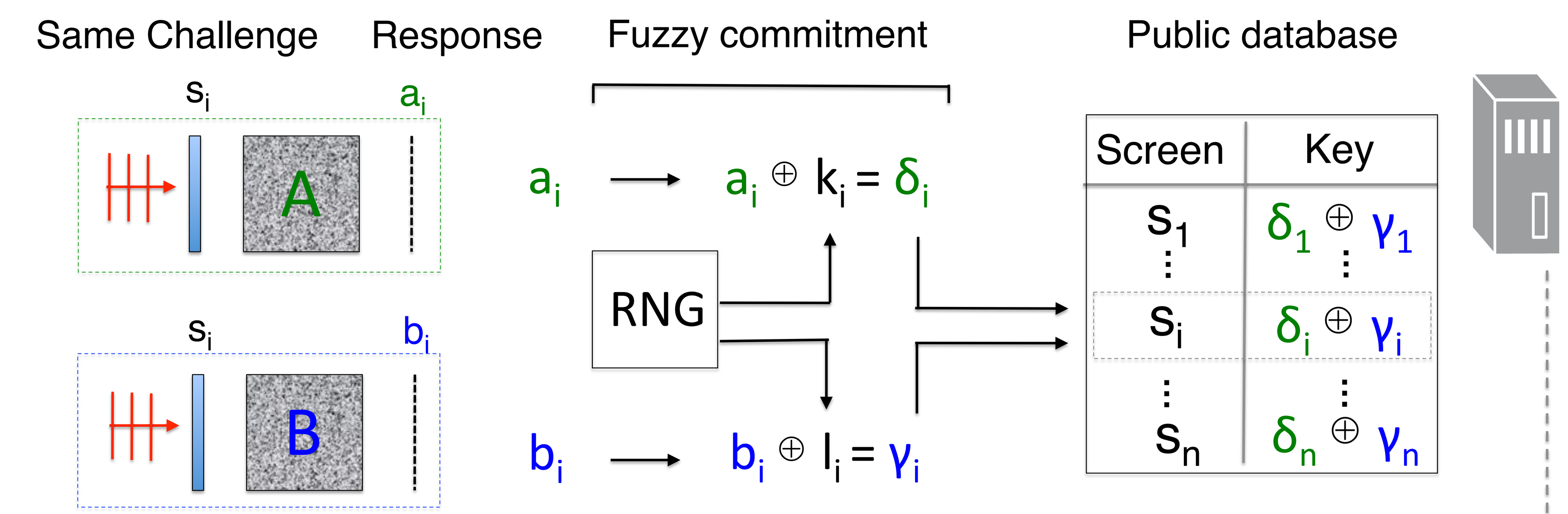
1. Digital whitening methods[4]
2. Piling up lemma[5]: $P(X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0) = 1/2 + 2^{n-1}\prod_{i=1}^{n}\epsilon_i$



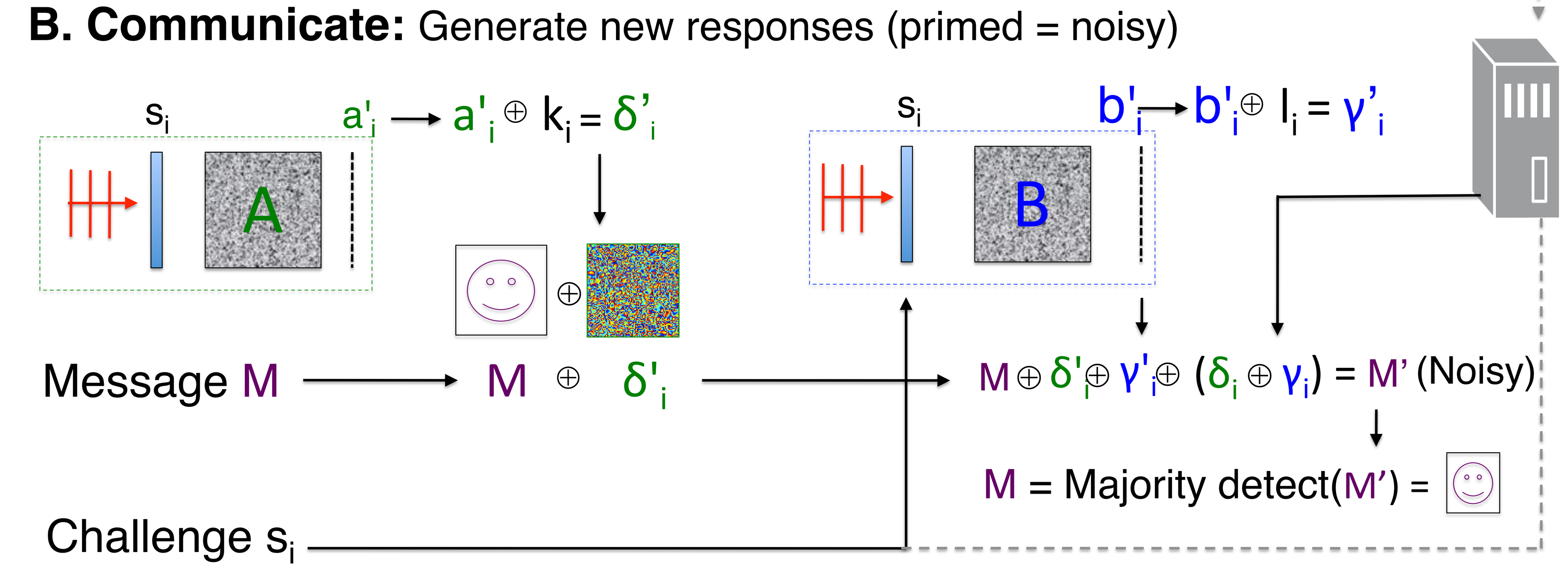
Example Communication Protocol

- Alice and Bob each have an optical-PUF device, A and B
- Use fuzzy commitment[2,3] to help with information leakage, account for noise
- Passes DieHard tests[7] after fuzzy commitment/whitening

A. Register: Show same challenge, detect different response, build database



B. Communicate: Generate new responses (primed = noisy)



1. Alice randomly selects challenge s_i and creates δ_i from response a_i
2. Alice encrypts up-sampled message M with δ_i, sends to Bob along with s_i
3. Bob uses s_i to create γ_i w/device, get $\delta_i \oplus \gamma_i$ from database, decrypt message
4. Bob uses majority detection to remove errors in $M' = M$

C. Experimental Noise Analysis