Optical Engineering

OpticalEngineering.SPIEDigitalLibrary.org

Remote key establishment by random mode mixing in multimode fibers and optical reciprocity

Yaron Bromberg
Brandon Redding
Sebastien M. Popoff
Ningbo Zhao
Guifang Li
Hui Cao

SPIE.

Yaron Bromberg, Brandon Redding, Sebastien M. Popoff, Ningbo Zhao, Guifang Li, Hui Cao, "Remote key establishment by random mode mixing in multimode fibers and optical reciprocity," *Opt. Eng.* **58**(1), 016105 (2019), doi: 10.1117/1.OE.58.1.016105.

Remote key establishment by random mode mixing in multimode fibers and optical reciprocity

Yaron Bromberg,[a,b,*] Brandon Redding,[a] Sebastien M. Popoff,[a,†] Ningbo Zhao,[c] Guifang Li,[c,d] and Hui Cao[a]
[a]Yale University, Department of Applied Physics, New Haven, Connecticut, United States
[b]The Hebrew University of Jerusalem, Racah Institute of Physics, Jerusalem, Israel
[c]Tianjin University, College of Precision Instrument and Opto-Electronic Engineering, Tianjin, China
[d]University of Central Florida, CREOL, College of Optics and Photonics, Orlando, Florida, United States

Abstract. Disorder and scattering in photonic systems have long been considered a nuisance that should be circumvented. Recently, disorder has been harnessed for a rapidly growing number of applications, including imaging, sensing, and spectroscopy. The chaotic dynamics and extreme sensitivity to external perturbations make random media particularly well-suited for optical cryptography. However, using random media for distribution of secret keys between remote users still remains challenging since it requires the users have access to the same scattering sample. Here, we utilize random mode mixing in long multimode fibers to generate and distribute keys simultaneously. Fast fluctuations in fiber mode mixing provide the source of randomness for key generation, and optical reciprocity guarantees that the keys at the two ends of the fiber are identical. We experimentally demonstrate the scheme using classical light and off-the-shelf components, opening the door for a practically secure key establishment at the physical layer of fiber-optic networks. [DOI: 10.1117/1.OE.58.1.016105]

Keywords: optical communications; key distribution; optical cryptography; fiber optics; reciprocity; random media.

Paper 181386SS received Sep. 26, 2018; accepted for publication Nov. 28, 2018; published online Jan. 9, 2019.

1 Introduction

Complex photonic systems, such as scattering media, chaotic cavities, aperiodic photonic crystals, and biological tissue, are composed of a large number of spatial, spectral, temporal, and polarization degrees of freedom. The strong coupling of these degrees of freedom provides exceptional opportunities for numerous applications. For example, spatial–temporal coupling was utilized for dynamic light scattering and diffusive wave spectroscopy,[1,2] spatial–spectral coupling for spectroscopy[3,4] and imaging,[5,6] and spatial-polarization coupling for polarimetry.[7] For optical cryptography, complex random media have been utilized for several cryptographic functions, including authentication,[8,9] identification,[10] encryption,[11] random number generation,[12,13] and secure key storage.[14] An optical fiber that supports hundreds or thousands of guided modes can also be considered as a complex photonic system. Random mode mixing arises naturally due to local index inhomogeneities and cross section variations, producing speckle patterns at the output of the fiber. Since the mixing depends on ambient temperature fluctuations and mechanical strains,[15] the output speckle pattern is extremely sensitive to environmental perturbations and therefore constantly changes in time. This poses a serious challenge for many applications such as telecommunication and imaging, as the transmitted information quickly gets scrambled. Here, we take advantage of the random fluctuations in a long multimode fiber to generate and distribute random keys. Most importantly, the remote users at the two ends of the fiber can share identical copies of the keys, by virtue of the optical reciprocity principle. The keys, which are constantly updated due to intrinsic fluctuations of the fiber, can then be used to encode and decode information being sent over a standard unsecure communication channel.

Our method of distributing keys at the physical-layer of communication networks can only be hacked in real-time, in contrast to the computational keys that are widely used in today's telecommunications. Compared to quantum key distribution (QKD), our scheme does not provide an unconditional security. However, since it uses classical light and off-the-shelf fiber components, it is much simpler and can be easily integrated with current communication networks, potentially at Gb/s rates. While other classical key distribution (CKD) approaches, e.g., the ones using chaotic lasers,[16] require a precise tuning of system parameters, ours is alignment-free and naturally robust, making it especially attractive for real-world applications. Recently, several key distribution methods based on single-mode fibers have been developed,[17,18] including CKD at rates of 100 bits per second over a distance of 500 km.[19] In our approach, the complexity of a multimode fiber forces an adversary to simultaneously probe all fiber modes to extract information, and the measurements must be done quickly to track the rapid fluctuations of the fiber. The additional noise introduced by such exhaustive measurements sets the security of the key.

2 Proof of Principle Demonstration

Let us consider two users, Alice and Bob, who simultaneously couple laser light of identical frequency into both ends of a multimode fiber (Fig. 1). As an example, we assume that the input beam from Alice (Bob) has a well-defined

*Address all correspondence to Yaron Bromberg, E-mail: yaron.bromberg@mail.huji.ac.il

†Present address: PSL University, CNRS, Institut Langevin, ESPCI Paris, Paris, France

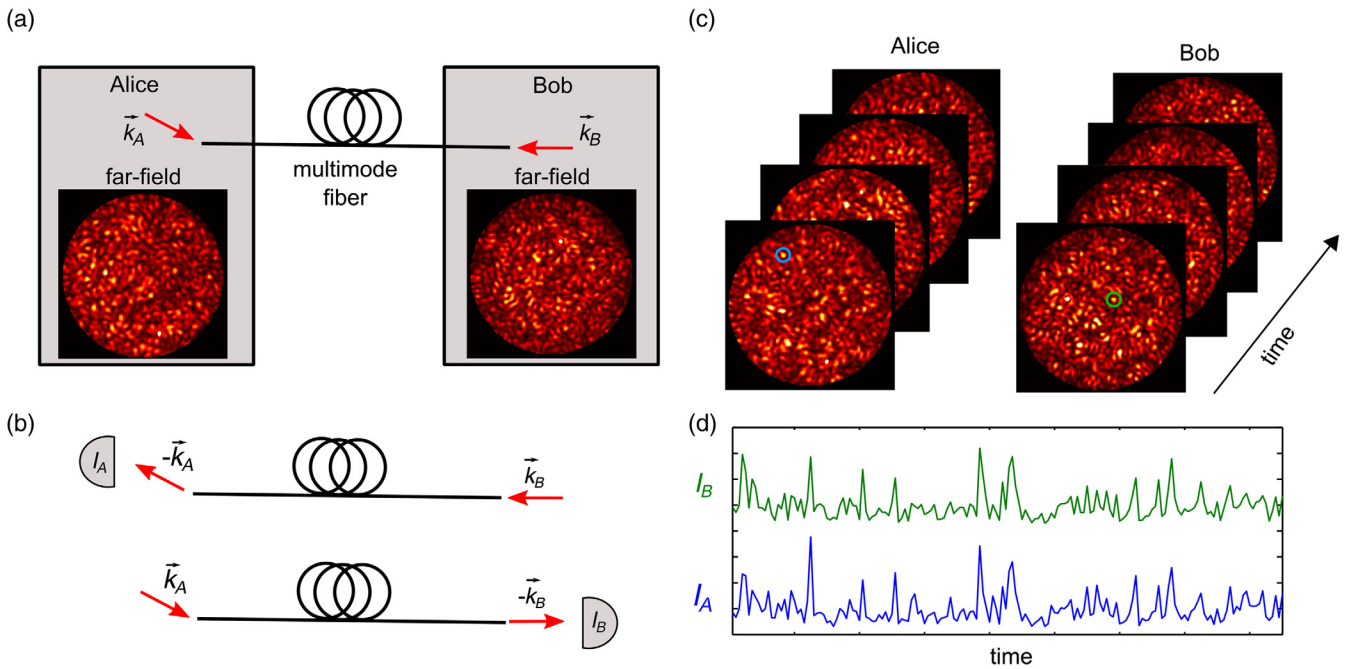

Fig. 1 A proof of principle demonstration of classical key establishment with a multimode fiber. (a) Alice and Bob couple a laser beam into the multimode fiber with wavevectors $\vec{k}_A$ and $\vec{k}_B$, respectively. Due to mode mixing in the fiber, speckle patterns appear at the output. (b) According to the optical reciprocity theorem, when the positions of a detector and a source are interchanged, the intensity measured by the detector in the two different configurations (I_A and I_B) is identical. Thus, at the channels that correspond to $-\vec{k}_A$ and $-\vec{k}_B$, Alice and Bob measure exactly the same intensities. (c) Due to changes in the environmental conditions of the fiber, the output speckles constantly fluctuate. Nevertheless, at channel $-\vec{k}_A$ (blue circle) and $-\vec{k}_B$ (green circle) the intensities are always correlated, as verified experimentally in (d) with a 6-m long step-index fiber (core diameter = 105 m, numerical aperture = 0.22) that supports $M \approx 4000$ guided modes. The probe laser wavelength is $\lambda = 640$ nm.

wavevector $\vec{k}_A$ ($\vec{k}_B$). In the presence of strong mode mixing, by the time the light exits the fiber all the guided modes are excited. Thus, at the far-field of the output facet a speckle pattern emerges, with no trace of the input wavevector [Fig. 1(a)]. The patterns Alice and Bob observe result from exactly the same mode mixing and phase shifts across the fiber but in a reversed order. Since the order of the coupling events is not interchangeable, the output patterns at the opposite ends are different even when the input channels of Alice and Bob are the same ($\vec{k}_A = \vec{k}_B$). Nevertheless, there is a unique pair of output channels that will be perfectly correlated. Optical reciprocity guarantees that the intensity measured by Alice at the output channel $-\vec{k}_A$ is identical to the intensity measured by Bob in the output channel $-\vec{k}_B$ [Fig. 1(b)]. Remarkably, not only does this hold even when the two input channels are not identical ($\vec{k}_A \neq \vec{k}_B$), but Alice and Bob do not need to know which channel the other user couples light into at the opposite end of the fiber. All they need to do is to measure the output intensity from the same channel that they have coupled light into. As the environmental conditions of the fiber change, the speckle patterns and the intensities measured in the $-\vec{k}_A$ and $-\vec{k}_B$ channels will fluctuate. However, since reciprocity holds for any configuration of the fiber, the intensities measured in the $-\vec{k}_A$ and $-\vec{k}_B$ channels will remain perfectly correlated [Fig. 1(c)], as long as the fiber remains static during the time it takes the light to traverse it. This is demonstrated experimentally in Fig. 1(d). Since the input and output channels are specified not only by the wavevector but also by the polarization, we have placed linear polarizers at both ends of the fiber. Note, however, that the two polarizers do not need to select the same polarization state but can be oriented at any arbitrary angle. To emulate changes in the environmental conditions of long fibers, the fiber was constantly shaken while speckle patterns were recorded. The synchronized fluctuations of the intensities measured by Alice and Bob allow them to share a common random signal from which they can extract a key.

While the above demonstration is performed in the wavevector (k) space, the reciprocity principle is not restricted to the wavevector space, and Alice and Bob can use channels in other spaces, e.g., the guided-mode space or the position space. Moreover, either of them can use a channel in a different space without knowing which space is used by the other. The position space is convenient for fiber-network applications, because Alice and Bob can simply couple light to each end of the multimode fiber via single-mode fibers. The single-mode fibers, together with an in-line fiber polarizer, automatically guarantee that the illumination and detection are conducted in the same channels, enabling an all-fiber, alignment-free configuration that is compatible with optical fiber networks. Furthermore, in contrast to QKD, our method does not have to operate at the single photon level and can easily be implemented using standard telecommunication lasers. Figure 2(a) is a schematic of an all-fiber setup we built with off-the-shelf elements. Using this setup,

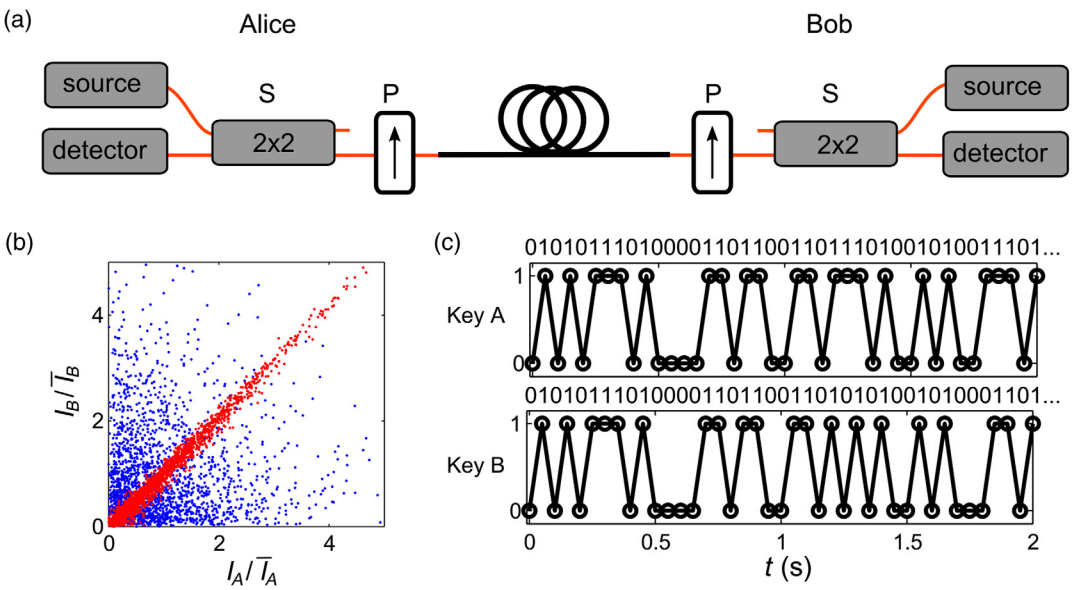

Fig. 2 Telecommunication-compatible implementation of remote key distribution. (a) Each node contains a laser source, a photodetector, a 2×2 splitter (S), and an in-line fiber polarizer (P). In our experiment, a single laser source operating at the telecommunication C-band ($\lambda = 1550$ nm) is used with a splitter (not shown) to mimic two sources at both ends of the fiber. The laser light is coupled into the multimode fiber (black) via a single-mode fiber (orange) to ensure that the illumination and detection channels are identical at each end of the fiber. The multimode fiber is a 1-km long graded-index fiber with a core diameter of 62.5 m, supporting about $M \approx 100$ guided modes. The environmental changes on the fiber are induced by shaking a 5-m portion of the fiber (out of the 1 km spool). (b) Scatter plot of the intensity measured by Alice versus the intensity measured by Bob, exhibiting a correlation of 0.99 (red dots). To verify that the high level of correlation does not result from fluctuations in the total transmitted light, we added a free-space beamsplitter between the single-mode fiber and the multimode fiber at Bob's end (not shown), and measured the intensity at an arbitrary position across the beam, yielding a correlation of 0.01 (blue dots). (c) A fraction of the digitized key, showing a raw bit rate of 20 Hz, and a bit error rate of 0.05.

we demonstrated that the intensities measured by Alice and Bob exhibit a correlation of 0.99 [Fig. 2(b)]. Such a high degree of correlation allows digitization of the analog signal, by associating a bit value "1" to all the intensities above the median, and "0" to all the intensities below the median. After digitization, the correlation between the stream of bits Alice and Bob obtained is 0.90, and the bit error rate is 0.05 [Fig. 2(c)], which can be further reduced with error correction protocols.[20] The key rate is determined by the rate of the fiber fluctuations, which in our case was only 20 Hz since we perturbed just 5 m out of a 1-km long fiber. However, the reported fluctuation rates of long-haul fibers in optical networks are much higher, typically in the range of 1 to 100 KHz,[21,22] enabling high key generation rates. The key rates can be further increased via parallelization, for example, using wavelength division multiplexing (WDM), as two spectral channels separated by the spectral correlation width of the fiber yield two uncorrelated speckle patterns at the output of the fiber. The spectral correlation width, determined by the modal dispersion in the fiber, scales inversely with the fiber length, and a merely 100-m long standard step-index multimode fiber has the spectral correlation width well below the frequency spacing required for WDM (see Sec. 5.3).

The contrast of the speckle pattern is determined by the laser linewidth and the spectral correlation width of the fiber. It is maximal for linewidths that are smaller than the spectral correlation width, and scales such as one over the square root of the linewidth for linewidths larger than the spectral correlation width. Since even under these circumstances reciprocity is not broken, Alice and Bob will still measure two correlated signals, yet with a lower level of fluctuations.

3 Eavesdropping and Security Analysis

Next, we analyze possible attacks by an eavesdropper, Eve. The attacks fall under two categories, passive ones where Eve only probes the light that is transmitted between the users, and active ones where Eve can also inject light into the system and use additional modulators to deceive Alice and Bob. In this section, we focus on passive attacks and briefly discuss active attacks at the end. We specifically consider the so-called beamsplitter attack, in which Eve places a beamsplitter at some intermediate point along the fiber. Eve can then measure the speckle intensity patterns incident at the beamsplitter, traveling from Alice to Bob and from Bob to Alice [Fig. 3(a)]. These two patterns are uncorrelated since they have traveled through two different sections of the multimode fiber and experienced different mode mixing. Hence, none of the spatial channels measured by Eve will be correlated with the signals Alice and Bob measure. We experimentally emulated a beamsplitter attack and confirmed that the intensities in all the channels measured by Eve are uncorrelated with the intensity measured by Alice and Bob [Fig. 3(b)]. Note that, as in any cryptographic system, we assume the nodes of Alice and Bob are in a secure area which Eve cannot access. Alice and Bob can therefore make sure that the sufficient mode mixing is introduced to the portion of the multimode fiber within the secure area so

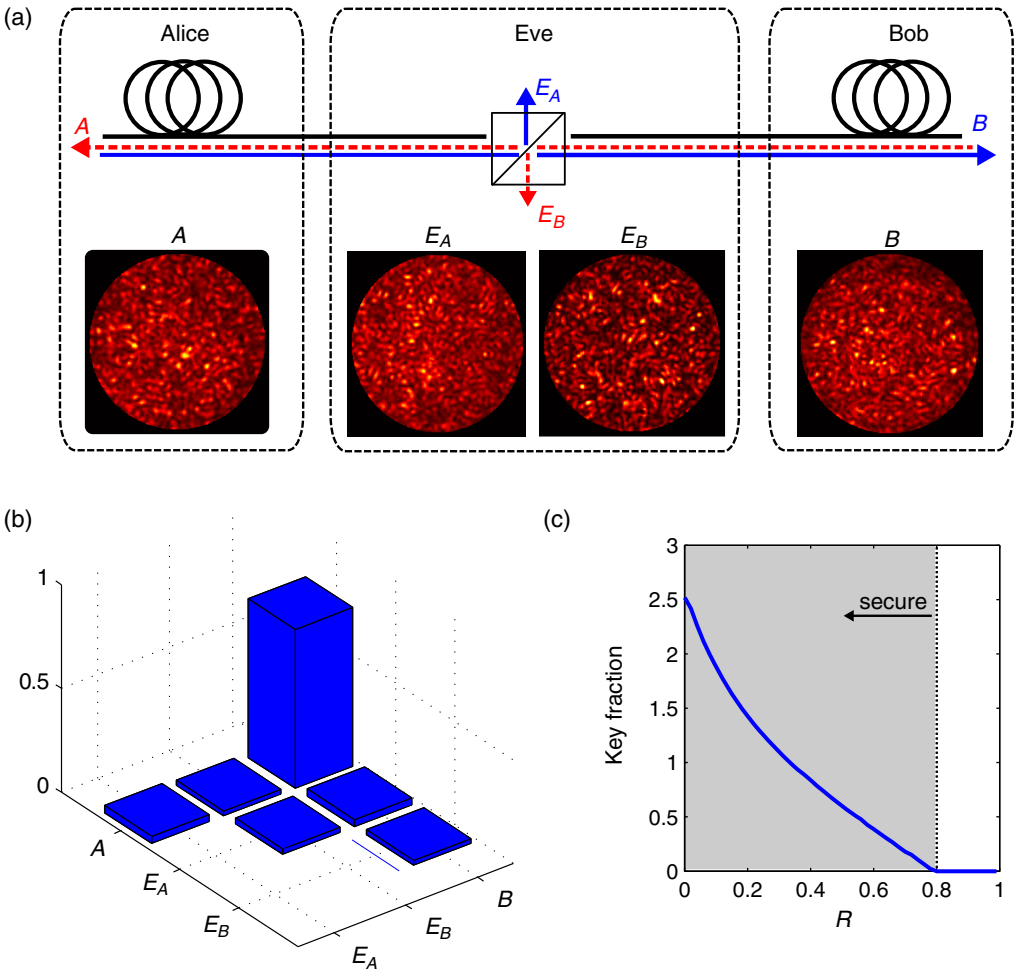

Fig. 3 Experimental emulation of a direct beamsplitter attack on the system shown in Fig. 1. (a) Eve picks up a fraction of the light propagating between Alice and Bob by intersecting the fiber with beamsplitter. The light which arrives to E_A and E_B passes through different parts of the fiber and therefore experiences completely different mode mixing. (b) The cross-correlations of measured intensities between the speckle grains from the four patterns A, B, E_A, and E_B. The cross-correlation between *A* and *B* corresponds to the input modes. Due to strong mode mixing, all the speckles in patterns E_A and E_B are equivalent, and two of them are selected from E_A and E_B for the other five cross-correlations. (c) Secure key fraction *K* as a function of the beamsplitter reflectivity *R*, for a simulated full-field attack by Eve. For $R < 0.8$, a secure key is established.

that when the light exits the secure area, all channels are excited and the intensity measured by Eve in any channel will be uncorrelated with the signal sent by Alice and Bob.

The random mode mixing along the fiber prevents Eve from extracting the key via direct intensity measurements. However, even in the presence of strong mode mixing, the complex fields at the output ports of Eve's beamsplitter carry information about the key. To illustrate this, let us denote the complex field distribution at the output port of Eve's beamsplitter from Alice by $E_{A,p}(x,y)$, where $p = H$, and V denotes the polarization state. Since at a single frequency phase conjugation corresponds to the time-reversal operation, a complex conjugate field $E^*_{A,p}(x,y)$ will send the light back to Alice's channel. Thus, the projection of field distribution that Eve measures at the output port from Bob $E_{B,p}(x,y)$ onto $E^*_{A,p}(x,y)$, gives the fraction of the light that actually reaches Alice's channel. Hence, Eve can extract the key by computing the complex overlap of the field distributions:

$$I_E = \left| \sum\nolimits_{p=H,V} \iint \mathrm{d}x\,\mathrm{d}y E_{A,p}(x,y) E_{B,p}(x,y) \right|^2 . \tag{1}$$

While it is theoretically possible that Eve directly measures the fields $E_{A,p}(x,y)$ and $E_{B,p}(x,y)$, and numerically computes the signal using Eq. (1), such a full-field beamsplitter attack requires a complex measurement apparatus. First, it is extremely challenging to accurately measure the amplitude and phase of all the modes inside a multimode fiber without being detected. In contrast to single-mode fibers that can be tapped by simply bending the fiber and collecting the scattered light, or via evanescently coupling an additional fiber to the single-mode fiber, for multimode fibers these methods do not work. The reason is that the scattering strength and the evanescent coupling lengths are very sensitive to the spatial field distributions of the modes close to the boundary of the core. Such distributions depend not only on the local index inhomogeneities and cross-section

variations of the fiber but also on the external perturbations such as bending and temperature fluctuations. Thus, different modes will acquire very different amplitudes and phases as they couple out of the core, and thus it will be practically impossible to measure the exact amplitude and phase of each mode. The only practical way to measure the field inside the core of a multimode fiber is to splice into the fiber a multimode fiber coupler, or to cut the fiber and insert a bulk beamsplitter. Both methods require shutting down the data traffic and, more importantly, will induce a reflection back into the fiber that can easily be detected by standard optical time-domain reflectometer testing.[23] Second, for every spatial channel, Eve needs a local oscillator to coherently detect the two quadratures of the field, at two orthogonal polarizations, for the two counter propagating fields. These can add up to thousands of channels that need to be measured faster than the fluctuation rate of the field. Despite of recent advances in the spatial division multiplexing (SDM) in multimode fibers,[24] such a measurement is still out of reach of current technology.

We next show that the multimode fiber not only imposes a technical challenge on the attacker, Eve, but it also guarantees security under the passive beam splitter attack. By analyzing the fundamental noise that is associated with such an attack, we extract system parameters that will guarantee security. In our analysis, we assume that Eve cannot intrude the secure areas of Alice and Bob, and that the only information that leaks out of the secure areas are the fields propagating through the multimode fiber. We also assume Alice and Bob have access to an authenticated public communication channel for performing, privacy amplification and error correction protocols, and for eliminating the so-called man-in-the-middle attack.

To prove security under the beamsplitter attack, we analyze the fundamental noise associated with the measurements of Alice, Bob, and Eve. We assume the laser light is in a coherent state with a large mean photon number. In this limit, Alice and Bob can perform a direct intensity measurement, which is limited only by shot-noise.[25] Eve, however, needs to first coherently detect the fields $E_{A,p}(x,y)$ and $E_{B,p}(x,y)$, and then compute the intensity I_E according to Eq. (1). Noise is added to her signal at two levels (see Sec. 5.2). First, for coherent states, the standard deviation in the simultaneous measurement of the two field quadratures is $\sqrt{2}$ larger than that of a single quadrature measurement.[26] Thus, the standard deviation of the intensity computed from the sum of the squares of the quadratures is $\sqrt{2}$ larger than that of a direct, shot-noise limited, intensity measurement. A second source of noise in Eve's signal is the multiplication of the fields $E_{A,p}(x,y)$ and $E_{B,p}(x,y)$ in the right-hand side of Eq. (1). Due to error propagation, multiplication of two random variables increases the standard deviation of the product by another factor of $\sqrt{2}$. Thus, if Eve detects N_E photons per channel, her signal-to-noise ratio (SNR) is $\sqrt{N_E/4}$, whereas the SNR of Alice and Bob for a shot-noise limited detection of N photons per channel is $\sqrt{N}$. We therefore conclude that as long as the number of photons per channel that Eve measures is a factor of 4 (6 dB) lower than the number of photons that Alice or Bob measure, Eve's SNR will be lower than that of Alice and Bob.

Our security claims are based on SNR analysis. Previous information theoretic security analysis has proven that the security of key distribution at the physical-layer is guaranteed as long as the legitimate users (Alice, Bob) have access to a common source of randomness, through channels that are less noisy than the channel of the eavesdropper (Eve). Thus, the superior SNR of their measurements enables Alice and Bob to generate a secure key, provided that they also have access to an unsecure yet authenticated public channel for privacy amplification protocols. For example, Alice and Bob can reveal a fraction of their bits and compare them over the public channel. In this way, they can estimate their error rate and compare it to the expected error rate of the system. In a conservative approach, any increase in the error rate is attributed to photons that Eve extracts from the channel, as the reduction in the number of photons that Alice and Bob measure increases their shot-noise and thus increases their bit error rate. Eve cannot compensate for this by using an amplifier, because shot-noise limited signals amplification cannot improve the SNR.[27] Alice and Bob can therefore get an upper bound on the ratio between the number of photons per channel that Eve measures and the number of photons they measure. If this upper bound is higher than 3 dB, they stop the communication since they know the fiber might have been hacked. If the ratio is lower than 3 dB, they can use a standard privacy amplification protocol to extract a secure key from the raw bits[33]. We conduct a quantitative analysis based on mutual information and numerically calculate the secure key fraction (K), defined by the ratio of the secure bit rate and the raw bit rate (See Sec. 5.2 for further details). Figure 3(c) shows the secure key fraction K as a function of the fraction of the beamsplitter reflectivity R. The simulations confirm that for the beamsplitter attack, as long as Eve measures less than 80% of the photons in the fiber, security is guaranteed.

Thus far we analyzed the SNR and the security of the system as a function of the number of photons that arrive to Alice, Bob, and Eve. Since this number depends on the transmission loss in the fiber, the security of the system depends on the fiber length. Transmission loss benefits Eve since we assume she has the capability to transmit light from her location to Alice and Bob without any loss. Specifically, the error rate that Alice and Bob expect already takes into account that there is loss in the fiber all along the link between the two of them. If Eve replaces parts of this fiber by a loss-less fiber, she can use all the photons that would have otherwise been lost in the lossy fiber, without Alice and Bob noticing an increase in the error rate. The mutual information analysis illustrates that the optimal position for Eve to place the beamsplitter is at the midpoint of the fiber. Then, Alice and Bob can establish a secure key only if the transmission from the midpoint of the fiber to its ends is higher than −6 dB. For typical fibers with transmission loss of 0.2 dB/km,[28] this corresponds to a maximum fiber length of 60 km.

Finally, we briefly discuss a few potential active attacks. An active Eve can try to perform the so-called man-in-the-middle attack, where she blocks the light that Alice and Bob send, and couples her own light into the fiber. However, by comparing part of the keys they obtain over a public channel, Alice and Bob can immediately notice that their keys are no longer correlated and stop the communication. If Eve tries to inject light to the fiber without blocking the light that Alice

and Bob send, they can notice a reduction in the contrast of the intensity fluctuations they measure. To prevent Eve from inducing correlations by modulating the total intensity of the light passing through the fiber, Alice and Bob can measure the total intensity that arrives to their end of the fiber and verify that it is not modulated.

4 Discussion and Conclusions

Below, we briefly compare our approach to the ones developed previously based on reciprocity (more comparisons are given in Sec. 5.1). Our approach to spread the transmitted signal over multiple spatial channels bares similarity with key distribution methods in the wireless domain, which rely on the scattering and fading of radio-frequency waves.[29] In the optical domain, a recent work demonstrated key distribution by free-space propagation through turbulent media, but in this configuration the legitimate users measure the reciprocal phase using a complex detection apparatus.[30] Our scheme is much simpler and more robust as it relies on a direct intensity measurement. Compared to the previous key-distribution schemes based on single-mode fibers,[17,18] the complexity of the multimode fiber forces the hacker to use a significantly more complex detection apparatus and perform additional computational processing. The asymmetry between the complex detection of the adversary and the simple direct detection of the legitimate users imposes excess noise in the adversary's measurements, which the legitimate users can utilize via privacy amplification protocols to distil a secure key.[31]

In this work, we used the natural fluctuations of the fiber as the source of randomness required for generating secure keys. Since the fiber fluctuations are inherent to the system, the implementation of our method in real world applications is greatly simplified. However, since the fiber has to be static during the time it takes the light to traverse the fiber, the key rate is limited by the length of the fiber. To overcome this limitation, we are currently developing a configuration in which Alice (or Bob) can add fast modulators at one end of the multimode fiber.

In conclusion, we have developed a key establishment protocol that relies on classical light and off-the-shelf telecommunication components. We experimentally demonstrated the method using an all-fiber and alignment-free system, which is compatible with optical fiber networks. The method is readily available for applications that are based on multimode fibers, such as local area networks. This method is also compatible with long-distance SDM networks, which has experienced rapid advances in recent years in the optical communication research community. The security of our method is based on the complexity of multimode fibers and on the fundamental noise limits of coherent laser light. Our method currently relies on the standard privacy amplification protocols to reduce uncertainties in the correlation measurements between Alice and Bob, yet it would be interesting to explore in the future advanced protocol tailored for our specific application. While this work has focused on classical light and does not provide unconditional security, we notice an analogy between our method and continuous variable quantum key distribution (CVQKD), as described in Sec. 5.2. This analogy may allow a future extension of our security analysis to more general security proofs that were recently developed for CVQKD.[32] The analogy to CVQKD may also help developing a new protocol for overcoming the maximal distance limit discussed above, similar to the way CVQKD has been extended beyond the 3-dB loss limit using postselection.[33] In addition, spreading quantum light over multiple spatial channels may open new opportunities for QKD in the spirit of the recent proposals to utilize multiple temporal channels for advanced QKD protocols.[34]

5 Appendix A

5.1 *Comparison with Other Key Distribution Methods*

Our scheme is inspired by the on-going effort to distribute keys between remote users at the physical-layer of communication networks. To date, the security of telecommunication networks depends on computational security, which is based on unproven assumptions that some computational tasks cannot be computed efficiently using a classical computer.[35] However, an adversary can tap the communication channel, save all the encrypted bits, and decrypt the information once a new computational paradigm or a quantum computer becomes available. In contrast, key distribution at the physical layer can be compromised only if it is hacked in real-time.[36] QKD is one such physical-layer approach, which relies on the fundamental laws of quantum mechanics to guarantee that an eavesdropper cannot extract the key without being exposed. However, a quantum channel requires transmission and detection of quantum states of light, which is technically challenging and expensive, and thus has not been widely implemented yet.

Over the years several classical alternatives to QKD have been proposed. A common approach is to rely on pre-established secret information, for example, the parameters of a chaotic laser[16] or the configuration of the encoder and decoder.[37] This approach typically requires accurate tuning by the end users so that their system parameters will match. More importantly, to guarantee security these settings have to be constantly updated, and therefore require an additional key distribution method for securely sharing the updated parameters. In an alternative approach, the entire channel between the users is turned to a giant fiber laser, with switchable cavity mirrors.[17] From the lasing characteristics, each user knows what mirror was used at the other end of the fiber and utilizes this information to generate a key. However, an eavesdropper can directly measure the reflectivity from the mirrors and extract the key since the key is deterministically set by the configuration of the cavity mirrors. It is therefore essential that the key will not be determined by the settings of just a few elements, which the adversary can measure. Toward this end, it was recently demonstrated that the relative phase between two fluctuating single-mode fibers can be used for generating a key.[18] Since the phase difference between the two fibers is accumulated along the entire length of the fibers, it is significantly more challenging for an eavesdropper to measure. Nevertheless, by splitting each fiber and measuring the phase accumulated at each of the four segments, the eavesdropper can compute the total phase difference between the fibers and extract the key.[18] In our multimode fiber configuration, an equivalent attack would require coherent detection of hundreds of spatial channels, simultaneously, featuring the complexity of multimode fibers. It forces the adversary to use a

significantly more complex detection apparatus than the apertures of the legitimate users, and additional computational processing, which as we further discuss in the next section, sets the security of the key.

5.2 *Detailed Security Analysis*

The fact that some information can leak to the eavesdropper is common to all physical-layer key distribution methods, including QKD.[38] Nevertheless, security of the key can still be guaranteed provided that the amount of information that has leaked is smaller than the amount of information that is exchanged between the legitimate users, by processing the raw signals using privacy amplification protocols.[31] The analysis of physical-layer systems is therefore based on notions from information theory that quantify the amount of information between the users. A central result in information theoretic security was derived by Csiszar and Korner,[39] who proved that the security of key distribution at the physical-layer is guaranteed as long as the legitimate users have access to a common source of randomness, through channels that are less noisy than the channel of the eavesdropper. Thus, we next perform a noise analysis of the full-field attack.

5.2.1 *Noise analysis of the full-field beamsplitter attack*

In this section, we consider the full-field beamsplitter attack and compare the SNR of the intensity reconstructed by Eve, with the SNR of the intensity measured by Alice and Bob. Let us denote by A_m (B_m) the projection of the complex field $E_{A,p}(x,y)$ [$E_{B,p}(x,y)$]), which gets from Alice (Bob) to Eve, onto the output channel $m = 1..2M$. Here m denotes the output spatial and polarization channels at Eve's beamsplitter, M is the number of spatial channels the fiber supports and $p = H, V$ denotes the polarization state. From Eq. (1) in the main text, Eve can reconstruct the intensity that is measured by Alice and Bob, by computing the intensity $I = |\sum_m A_m B_m|^2$. The signal reconstructed by Eve, however, will have an additional noise that originates from the noise in her measurements. We model the noise in the quadratures of each of the channels she measures by additive, uncorrelated, Gaussian random variables, with a variance σ^2. By plugging the random variables into the sum that Eve computes and averaging over the noise realizations, we get the signal-to-noise ratio (SNR) of Eve's reconstructed intensity:

$$\mathrm{SNR}_E = \sqrt{\frac{N_A N_B}{8M\sigma^2(N_A + N_B)}}, \tag{2}$$

where $N_A(N_B)$ is the number of photons that get to Eve from Alice (Bob). Here, we assumed the high SNR limit $N_A, N_B \gg \sigma^2$ and that all the photons detected by Alice and Bob contribute to the signal. We note that if the linewidth of the source is larger than the spectral correlation width of the fiber, one must subtract from the signal the photons in the nonfluctuating part of the signal. Nevertheless, since typical telecom lasers can have linewidths of 100 KHz, and typical fibers in optical communication networks have a bandwidth-distance product in the range of 0.1 to 5 GHz · km (see Sec. 5.3), this assumption is valid even if the fiber is thousands of kilometers long.

We further assume that Alice and Bob send the same number of photons per bit, N_0, then the average number of photons that arrive to Eve is $N_A = N_0\eta e^{-\gamma(L/2+z)}$ and $N_B = N_0\eta e^{-\gamma(L/2-z)}$, γ is the fiber attenuation coefficient, L is the fiber length, z is the distance of Eve's beamsplitter from the fiber midpoint, and η is the reflectivity of the beamsplitter. We thus get

$$\mathrm{SNR}_E = \sqrt{\frac{N_0 R e^{-\gamma L/2}}{8M\sigma^2}\frac{1}{2\cosh(\gamma z)}}. \tag{3}$$

To maximize her SNR, Eve needs to place her beamsplitter at the midpoint of the fiber ($z = 0$). The SNR is then given as

$$\mathrm{SNR}_E = \sqrt{\frac{N_E}{8\sigma^2}}, \tag{4}$$

where $N_E = N_0\eta e^{-\gamma L/2}/2M$ is the average number of photons per channel that get to Eve. For computing the fundamental limit on Eve's SNR, we need to evaluate the variance of the noise in the measurement of the two quadratures of the field. According to the quantum theory of photodetection, the fundamental noise associated with coherent detection of the two quadratures of a coherent state, simultaneously, is Gaussian noise with $\sigma^2 = 1/2$,[26] and therefore $\mathrm{SNR}_E < \sqrt{N_E/4}$. In contrast to Eve, Alice, and Bob can perform a direct shot-noise-limited intensity measurement, and therefore their SNR is giving by $\mathrm{SNR}_{A/B} = \sqrt{N}$, where $N = N_0(1-\eta)e^{-\gamma L}/2M$. We therefore conclude that as long as the number of photons per channel that Eve measures is a factor of 4 lower than the number of photons that Alice or Bob measure, Eve's SNR will be lower than that of Alice and Bob.

5.2.2 *Mutual information analysis*

The noise in the signal reconstructed by Eve limits the amount of information she can extract. To obtain a quantitative relation between the amount of information obtained by Eve and the security of the key, we use the result of Csiszar and Korner, who proved that the key fraction, defined by the ratio of the secret key and the raw bit rate, is given by[39]

$$K = I(A,B) - \min[I(A,E), I(B,E)]. \tag{5}$$

Here, $I(A,B)$ is the mutual information between Alice and Bob, and $I(A,E)$ [$I(B,E)$] is the mutual information between Eve and Alice (Bob).

To study the effect of the excess noise on the key fraction, we performed a numerical simulation of Eve's attack and computed the mutual information of the simulated signals measured by Alice, Bob, and Eve. The channel projections of the complex fields at Eve's output channel, A_m and B_m, are simulated by circular complex Gaussian random numbers, and the intensity at the output channel of Alice and Bob is computed using $I_0 = |\sum_m A_m B_m|^2$.

We next simulated Eve's noisy measurements by adding a Gaussian noise to the real and imaginary parts of the complex fields A_m and B_m with variance $\sigma^2 = 1/2$. We denote the fields with the additional Gaussian noise by a_m and b_m.

Eve's signal was simulated by computing $I_E = |\sum_m a_m b_m|^2$. The noisy measurement of Alice and Bob is simulated by a Poissonian random number with mean I_0. We repeat this procedure for 10^6 realizations of the fiber configuration (i.e., 10^6 realizations of A_m and B_m). Finally, we compute the mutual information between the simulated intensities of Alice, Bob, and Eve, and using Eq. (5), we obtain the secret key fraction K.

5.2.3 *Analogy to continuous variable quantum key distribution*

A promising route to extend the above security analysis to more general attacks is via the analogy between our method and CVQKD. In CVQKD Alice encodes a random key in the amplitude and phase of a coherent state using modulators, and sends it to Bob, who measures the two quadrature of the field using coherent detection.[40,41] Conceptually, one can think of our multimode fiber as the amplitude and phase modulator, which one of the users, say Alice, uses to send a random coherent state to Bob. Since Alice does not know the modulation that the multimode fiber has applied, she receives that information from the light Bob sends her. We encoded the key by the intensity measured by Alice and Bob, but similarly to CVQKD, the key can also be encoded by the quadratures of the fields. This analogy may allow a future extension of our security analysis to more general security proofs that were recently developed for CVQKD.[32]

5.3 *Increasing the Key Rate Using Wavelength Division Multiplexing*

The key rate can be further increased via parallelization, using WDM. Due to modal dispersion in multimode fibers, the field at the output of long fibers is wavelength dependent. In order to increase the key rates, it is critical that fields at wavelengths that are separated by the WDM spectral spacing will yield uncorrelated keys. Thus, the bandwidth over which the fields at the output of the fiber are correlated (the spectral correlation width Δ) must be smaller than the WDM spectral spacing. Since the spectral correlation width scales inversely with the fiber length, for long enough fibers this is indeed the case. We have recently shown experimentally that the spectral correlation width of a 100-m long standard step-index multimode fiber is 3 pm.[4] Graded index (GRIN) fibers, which are more commonly used in fiber communication networks, exhibit wider spectral correlation widths, typically in the range of 5 to 250 pm for 100 m long fiber (corresponding to a bandwidth-distance product in the range of 0.1 to 5 GHz · km). These widths are well below the spacing required for dense WDM (800 pm for the ITU frequency grid with 100 GHz spacing).

To quantify the amount of information Eve can extract from different spectral channels, we simulate numerically the fields measured by Eve at different wavelengths. We use the concatenated waveguide model to simulate the propagation through a GRIN fiber with a core diameter of 50 μm and a 0.19-numerical aperture, supporting 110 modes.[42] The fiber we simulate is 1 km long and is composed of 200 segments. Mode coupling is introduced by modeling random bending and orientations for each segment.[42] Figure 4 shows two speckle patterns at the output of the fiber at two different wavelengths that are separated by $\delta\lambda = 200$ pm. The patterns are clearly uncorrelated. To quantify the degree of spectral correlation, we compute the spectral correlation function of the fields, defined as

$$\rho(\delta\lambda) \equiv \frac{|\langle E(x,y,\lambda_0)E^*(x,y,\lambda_0+\delta\lambda)\rangle|}{\sqrt{\langle|E(x,y,\lambda_0)|^2\rangle}\sqrt{\langle|E(x,y,\lambda_0+\delta\lambda)|^2\rangle}}. \tag{6}$$

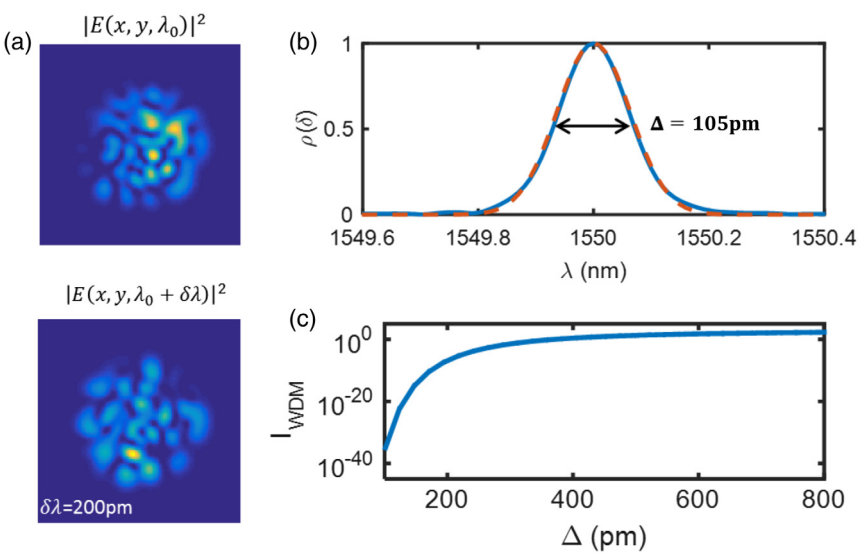

Fig. 4 (a) Numerical simulation of the wavelength dependence of the fields at the output a 1-km long multimode fiber. Due to modal dispersion, two speckle patterns at wavelengths separated by $\delta\lambda = 200$ pm are completely uncorrelated. (b) The degree of spectral correlation between the speckle field at $\lambda_0 = 1550$ nm and the field at wavelength λ (blue solid line), and a Gaussian fit (red dashed line). (c) The mutual information I_{WDM} as a function of the spectral correlation width of the multimode fiber. I_{WDM} sets an upper bound on the amount of information that Eve can extract by measuring all the spectral channels in a standard WDM frequency grid. The amount of information Eve can extract is negligible for spectral correlation widths that are smaller than 300 pm, which correspond to fibers that are longer than just a few centimeters.

Here $\langle\,\rangle$ denotes spatial and ensemble averaging. Figure 4 shows the spectral correlation function $\rho(\delta\lambda)$ (dashed blue line), where the spectral correlation width, which is defined by the full width half maximum of $\rho(\delta\lambda)$, is in this example $\Delta = 105$ pm.

To relate the spectral correlation width to the amount of information Eve can extract on the key from different spectral channels, we compute the mutual information between speckle fields at different wavelengths. Since speckle fields follow Gaussian statistics, we can use the results from information theory which quantify the mutual information between two circular complex random variables with a degree of correlation $(\delta\lambda)$: $I(\rho) = -\log_2(1-\rho^2)$.[43] For long multimode fibers $\rho(\delta\lambda)$ can be approximated by a Gaussian function (dashed red line in Fig. 4). Assuming the multimode fiber supports N guided modes, the fields arriving to Eve from Alice and Bob $[E_A(x,y,\lambda)$ and $E_B(x,y,\lambda)]$ can be decomposed into $2N$ independent spatial channels. Hence, the amount of information on the fields at λ_0 that Eve can extract from measuring the fields at $\lambda_0+\delta\lambda$ is given by $I(\lambda_0,\lambda_0+\delta\lambda) = -2N\log_2[1-\rho(\delta\lambda)^2]$. Thus, if Alice and Bob decide to use WDM with M spectral channels with a frequency spacing $\delta\lambda$, the amount of information Eve can extract on the key at wavelength λ_0 is bounded as

$$I_{\mathrm{WDM}}(\delta\lambda) = -2N\sum_{m=1}^{M}\log_2[1-e^{-(m\delta\lambda)^2/(2\ln 2\Delta^2)}]. \tag{7}$$

Figure 4 plots the mutual information I_{WDM} as a function of the spectral correlation width of the fiber Δ, for a typical WDM frequency grid with $M = 72$ channels and $\delta\lambda = 800$ pm. These grid parameters correspond to the ITU frequency grid with a 100-GHz spacing. It is clear that for spectral correlation widths smaller than $\Delta = 300$ pm, the amount of information that Eve can extract from all the spectral channels of the WDM grid is negligible. A spectral correlation width of 300 pm corresponds to GRIN fibers that are hundreds of meters or shorter. We therefore conclude that WDM can be safely used with multimode fibers that are longer than hundreds of meters without compromising the security of the key.

We note that principle measurements at different wavelengths could have added some information on the instantaneous configuration of the fiber. But the critical point is that Eve's attack cannot be based on figuring out the fiber's instantaneous configuration. The reason is that the number of instantaneous configurations of a long multimode fiber is innumerable. For example, let us assume that for every 1-m long segment of the fiber there are N configurations that yield uncorrelated fields at the output (here by configuration we mean geometrical setting and temperature profile across the fiber), then for a 1-km long fiber there would be N^{1000} different configurations, which are obviously intractable. Hence, an attack that is based on learning the fiber configuration is unrealistic.

Acknowledgments

This work has been supported in part by the US National Science Foundation (NSF) under Grant Nos. ECCS-1509361, -1808976, and -1809099 and by the United States-Israel Binational Science Foundation (BSF) Grant No. 2017694. The authors declare no competing financial interests.

References

1. G. Maret and P. E. Wolf, "Multiple light scattering from disordered media. The effect of Brownian-motion of scatterers," *Z. Phys. B Con. Matter* **65**, 409–413 (1987).
2. D. J. Pine et al., "Diffusing wave spectroscopy," *Phys. Rev. Lett.* **60**, 1134–1137 (1988).
3. B. Redding et al., "Compact spectrometer based on a disordered photonic chip," *Nat. Photonics* **7**, 746–751 (2013).
4. B. Redding et al., "High-resolution and broadband all-fiber spectrometers," *Optica* **1**, 175–180 (2014).
5. R. Barankov and J. Mertz, "High-throughput imaging of self-luminous objects through a single optical fibre," *Nat. Commun.* **5**, 5581 (2014).
6. S. M. Kolenderska et al., "Scanning-free imaging through a single fiber by random spatio-spectral encoding," *Opt. Lett.* **40**, 534–537 (2015).
7. J. Ellis and A. Dogariu, "Optical polarimetry of random fields," *Phys. Rev. Lett.* **95**, 203905 (2005).
8. R. Pappu et al., "Physical one-way functions," *Science* **297**, 2026–2030 (2002).
9. S. A. Goorden et al., "Quantum-secure authentication of a physical unclonable key," *Optica* **1**, 421–424 (2014).
10. J. D. R. Buchanan et al., "Forgery: 'fingerprinting' documents and packaging," *Nature* **436**, 475–475 (2005).
11. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**, 767–769 (1995).
12. P. Lalanne et al., "2-D generation of random numbers by multimode fiber speckle for silicon arrays of processing elements," *Opt. Commun.* **76**, 387–394 (1990).
13. D. G. Marangon, G. Vallone, and P. Villoresi, "Random bits, true and unbiased, from atmospheric turbulence," *Sci. Rep.* **4**, 5490 (2014).
14. R. Horstmeyer et al., "Physical key-protected one-time pad," *Sci. Rep.* **3**, 3543 (2013).
15. K. Ho and J. Kahn, "Mode coupling and its impact on spatially multiplexed systems," *Opt. Fiber Telecommun.* VI(B), 491–568 (2013).
16. M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nat. Photonics* **9**, 151–162 (2015).
17. J. Scheuer and A. Yariv, "Giant fiber lasers: a new paradigm for secure key distribution," *Phys. Rev. Lett.* **97**, 140502 (2006).
18. K. Kravtsov et al., "Physical layer secret key generation for fiber-optical networks," *Opt. Express* **21**, 23756–23771 (2013).
19. A. El-Taher et al., "Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser," *Laser Photonics Rev.* **8**, 436–442 (2014).
20. B. Azimi-Sadjadi et al., "Robust key generation from signal envelopes in wireless networks," in *Proc. of the 14th ACM Conf. on Computer and Communications Security*, pp. 401–410 (2007).
21. J. Minář et al., "Phase-noise measurements in long-fiber interferometers for quantum-repeater applications," *Phys. Rev. A* **77**, 052325 (2008).
22. S. Ö. Arik, J. M. Kahn, and K. P. Ho, "MIMO signal processing for mode-division multiplexing: An overview of channel models and signal processing architectures," *IEEE Signal Process. Mag.* **31**, 25–34 (2014).
23. ID Quantique, *White Paper Fiber Optic Networks: Your Weakest Link* (2011).
24. N. K. Fontaine et al., "30 × 30 MIMO transmission over 15 spatial modes," in *Optical Fiber Communication Conf. Post Deadline Papers*, p. Th5C.1 (2015).
25. P. Lodahl and A. Lagendijk, "Transport of quantum noise through random media," *Phys. Rev. Lett.* **94**, 153905 (2005).
26. J. Shapiro, "6.453 quantum optical communication," Lecture 16, Quantum Cryptography, http://ocw.mit.edu (2016).
27. C. M. Caves, "Quantum limits on noise in linear amplifiers," *Phys. Rev. D* **26**, 1817–1839 (1982).
28. R. Ryf et al., "Mode-multiplexed transmission over conventional graded-index multimode fibers," *Opt. Express* **23**, 235–246 (2015).
29. N. Patwari et al., "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mob. Comput.* **9**, 17–30 (2010).
30. M. D. Drake et al., "Optical key distribution system using atmospheric turbulence as the randomness generating function: classical optical protocol for information assurance," *Opt. Eng.* **52**, 055008 (2013).
31. C. H. Bennett et al., "Generalized privacy amplification," *IEEE Trans. Inf. Theory* **41**, 1915–1923 (1995).
32. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Phys. Rev. Lett.* **114**, 070501 (2015).
33. C. Silberhorn et al., "Continuous variable quantum cryptography: beating the 3 dB loss limit," *Phys. Rev. Lett.* **89**, 167901 (2002).
34. T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature* **509**, 475–478 (2014).
35. B. Schneier, *Applied Cryptography*, 2nd ed., John Wiley & Sons (1996).
36. R. Alleaume et al., "Using quantum key distribution for cryptographic purposes: a survey," *Security* **560**, 62–81 (2009).
37. M. P. Fok et al., "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Secur.* **6**, 725–736 (2011).

38. V. Scarani et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
39. T. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory* **18**, 339–348 (1972).
40. F. Grosshans et al., "Quantum key distribution using Gaussian-modulated coherent states," *Nature* **421**, 238–241 (2003).
41. A. M. Lance et al., "No-switching quantum key distribution using broadband modulated coherent light," *Phys. Rev. Lett.* **95**, 1–4 (2005).
42. M. B. Shemirani et al., "Principal modes in graded-index multimode fiber in presence of spatial- and polarization-mode coupling," *J. Lightwave Technol.* **27**, 1248–1261 (2009).
43. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, Somerset (1991).

Yaron Bromberg is a senior lecturer at the Physics Department, Hebrew University of Jerusalem. He received his PhD in 2010 from Weizmann Institute of Science working on quantum walks in correlated photons. His research interests are in the fields of quantum optics and complex photonic media.

Brandon Redding is currently a research physicist at the US Naval Research Laboratory, where he works on fiber optic sensors, computational sensing, and coherent LIDAR. He received his PhD from the University of Delaware, working on integrated silicon photonics before working as a postdoc at Yale University on light generation and sensing in complex and disordered systems.

Sebastien M. Popoff received his PhD from the University of Paris (Université Paris Diderot) for his work on wavefront shaping in complex media. He is now a CNRS (French Research Agency) Research Scientist at the Langevin Institute (ESPCI Paris, France). His current research interests involve the control of light propagation in complex media for various applications, including optical imaging through inhomogeneous media, fundamental investigations of mesoscopic correlations in scattering samples, and telecommunications in multimode fibers.

Ningbo Zhao: Biography is not available.

Guifang Li received his PhD from the University of Wisconsin at Madison. His research interests include optical communication and networking, RF photonics, all-optical signal processing and imaging. He received the NSF CAREER Award and the Office of Naval Research Young Investigator Award. He is a fellow of the National Academy of Inventors, IEEE, The Optical Society, and SPIE. He currently serves as an associate editor of *Optica* and the *IEEE Photonics Journal*.

Hui Cao is the Frederick W. Beinecke professor of applied physics and professor of physics at Yale University. She received her PhD in applied physics from Stanford University in 1997. Her technical interests and activities are in the areas of mesoscopic optics, complex photonic materials and devices, nanophotonics, and biophotonics. She is a fellow of the AAAS, APS, and OSA.