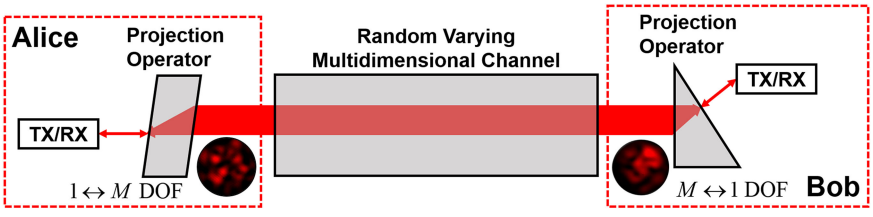
IEEE Photonics Journal
An IEEE Photonics Society Publication

High-Speed Random-Channel Cryptography in Multimode Fibers

Volume 13, Number 1, February 2021

Rachel Sampson
He Wen
Bin Huang
Rodrigo Amezcua Correa, *Member, IEEE*
Yaron Bromberg
Hui Cao, *Fellow, IEEE*
Guifang Li, *Fellow, IEEE*



Random channel cryptography is a classical key distribution method that uses random variations in a multidimensional shared channel to establish a high-speed key.

DOI: 10.1109/JPHOT.2021.3049253

High-Speed Random-Channel Cryptography in Multimode Fibers

Rachel Sampson,[1] **He Wen**,[1] **Bin Huang**,[1] **Rodrigo Amezcua Correa**,[1] ***Member, IEEE***, **Yaron Bromberg**,[2] **Hui Cao**,[3] ***Fellow, IEEE***, **and Guifang Li**,[1] ***Fellow, IEEE***

[1]CREOL, The College of Optics & Photonics, University of Central Florida, Orlando, FL 32816-2700 USA
[2]Racah Institute of Physics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel
[3]Department of Applied Physics, Yale University, New Haven, CT 06511-8499 USA

DOI:10.1109/JPHOT.2021.3049253

Manuscript received November 25, 2020; accepted December 30, 2020. Date of publication January 5, 2021; date of current version January 21, 2021. This work was supported in part by National Science Foundation (NSF) (1649522, ECCS-1808976 and -1809099) and in part by United States-Israel Binational Science Foundation (BSF) (2017694). Corresponding author: Rachel Sampson (e-mail: rachel.sampson@knights.ucf.edu).

Abstract: We propose and experimentally demonstrate high-speed operation of random-channel cryptography (RCC) in multimode fibers. RCC is a key generation and distribution method based on the random channel state of a multimode fiber and multi-dimension to single-dimension projection. The reciprocal intensity transmittance of the channel shared between the two legitimate users is used to generate and distribute correlated keys. In previous work, RCC's key rate-distance product was limited by the speed of light. In this work, we show that adding a fast modulator at one end of the channel decouples the key rate and distance, resulting in a significant improvement in the key rate-distance product, limited only by the fiber's modal dispersion. Error-free transmission at a key rate-distance product of 64.7 Mbps $\times$ 12 km, which is seven orders of magnitude higher than the previous demonstration, was achieved. The proposed method's security arises from a fundamental asymmetry between the eavesdroppers' and legitimate users' measurement complexity.

Index Terms: Electro-optical systems, fiber optic systems, security and encryption.

1. Introduction

Many public-key cryptography methods, which are widely used for encryption over the internet, offer computational security [1]–[3]. A disadvantage of computational security is that it allows an eavesdropper to save encrypted data and decrypt it later following advances in computing power or with a new computational paradigm [1]–[3]. The anticipated arrival of quantum computers has made encryption an area of active research, as many modern encryption algorithms will be rendered obsolete by quantum computation [4]–[6]. In response to this impending problem, several physical-layer key distribution methods have been proposed. One physical-layer key distribution method that has received considerable attention is quantum key distribution (QKD), whose security is based on the laws of quantum physics [7]–[11]. QKD is attractive because, in principle, it offers unconditional security and thereby immunity to any attack regardless of an eavesdropper's computational capabilities [12]. There are still practical challenges facing deployment of QKD

though, including security in real implementations and increasing the key rate-distance product [12]–[18]. Furthermore, QKD is currently a costly and complicated solution [15].

Another physical-layer key-distribution method that has received less attention is classical key distribution (CKD). Most CKD methods employ hacking asymmetry, a large disparity in measurement complexity between the legitimate users and eavesdroppers, to make their system technologically secure. One such approach forms a fiber laser out of the communication link between the legitimate users and the resultant lasing properties are used to distribute a key [19]–[22]. Alternative CKD methods employ a large-scale fiber-based interferometer between the legitimate users and phase fluctuations within the interferometer are used to establish a key [23]–[26]. Since the phase is accumulated over the entire interferometer, recovering the signal is significantly more challenging for an eavesdropper than for the legitimate users. However, this method relies on slow-varying external fluctuations to produce the key, which has limited key rates to 100 s bps, many orders of magnitude below communication system bit rates [23]–[27]. Therefore, there still exists a desire for a simple low-cost, high key rate, long-distance physical key distribution method.

We previously demonstrated a CKD method, in which random variations in the transmittance of a shared channel between the legitimate users were used to establish a key [28]–[30]. We call this CKD method random channel cryptography (RCC). In [28]–[30], external perturbations distributed along the fiber act as the source of the random fluctuations in the channel transmittance. As a result, the key rate-distance product of RCC in [28]–[30] was limited by the speed of light. A key rate of 20 bps over 1 km was demonstrated in [28], which is orders of magnitude lower than the transmission capacity of optical fiber communication systems. In this work, we increase the key rate and distance of RCC by adding a fast modulator at one end of the link, thereby decoupling the key rate and distance and enabling higher key rate-distance products. The high-speed RCC technique presented here preserves the security properties of the RCC method originally presented in [28]. Error-free transmission at a key rate of 64.7 Mbps over 12 km of commercial OM4 fiber was demonstrated using only commercial off-the-shelf components. This represents a seven orders of magnitude increase in the key rate-distance product compared to the previous result of 20 bps·km [28].

2. Principle of Operation of RCC

In its simplest form, the RCC channel consists of two projection operators and a random spatially-, spectrally-, and temporally-varying multidimensional channel, as shown in Fig. 1(a). The two passive paths between the legitimate users, from Alice to Bob and from Bob to Alice, are reciprocal and therefore, the intensity transmission properties are identical, creating a mechanism for key distribution between Alice and Bob. The concept of using channel properties to establish a shared key was originally proposed for wireless communication systems, using radio waves over free-space [31], [32]. RCC offers a fiber-based analog to this wireless key distribution method. Furthermore, projection operators reduce the degrees of freedom (DOFs) at the receiver, allowing Alice and Bob to make one-dimensional measurements, while an eavesdropper, Eve, will have to measure M DOFs, where M is the number of dimensions supported by the channel. It is assumed that Alice and Bob's transceivers, shown by dashed red boxes in Fig. 1, are located in secure areas that are inaccessible to Eve.

A concrete example of RCC is shown in Fig. 1(b) [28]–[30]. In the forward direction, Alice sends one-dimensional light (plane wave in the direction $\boldsymbol{k}_A$) which is projected onto the M DOFs of the multimode fiber (MMF). This produces a speckle pattern S_2 at the fiber facet on Bob's end. In the reverse direction, Bob sends a plane wave in the direction $\boldsymbol{k}_B$ and a speckle pattern S_1 forms at the fiber facet on Alice's end. Both speckle patterns, S_1 and S_2, are a superposition of many plane waves with different wave vectors. In general, the two speckle patterns will be completely different because the input plane wave at each end will excite different modal content in the MMF [33]. Even if the same input plane wave is used at each end, since MMF is a coupled multipath channel and the order of coupling is not commutable, the speckle patterns will be different [28]–[30], [34], [35]. Alice and Bob should also require that the signal is sufficiently spread over many DOFs within their

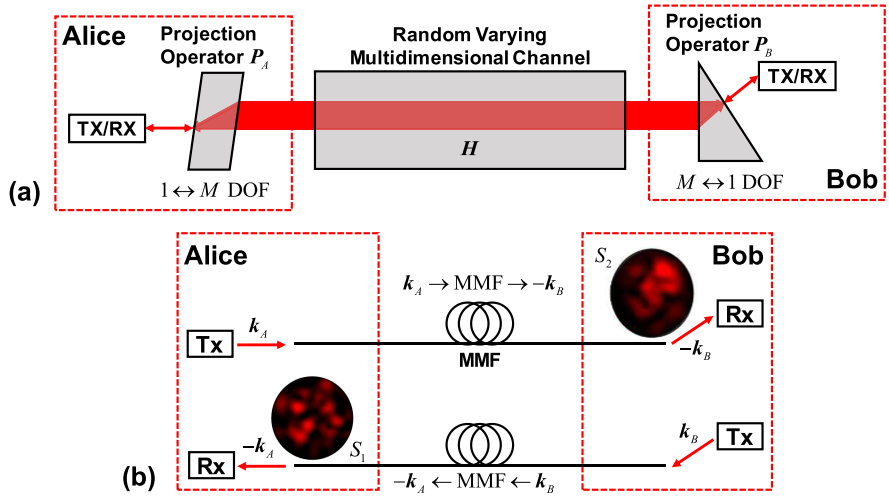


Fig. 1. (a) Schematic of RCC. Single degree-of-freedom (DOF) light is produced at the transmitters (TX) and projected onto the M DOFs of the multidimensional channel ($\mathbf{H}$) using projection operators $\mathbf{P}_A$ and $\mathbf{P}_B$. Within the channel, the light is scrambled among the M DOFs, and at the receivers (RX), M DOF light is projected onto a single DOF. The reciprocal paths produce correlated intensities, which can be used to form a shared key. (b) An example of RCC using a multimode fiber (MMF) and plane-wave inputs having wavevectors $\boldsymbol{k}_a$ and $\boldsymbol{k}_b$.

secure areas, through mode mixing, so that the outgoing light excites all modes and any mode measured by Eve will have no correlation to the light sent by Alice and Bob [28]. At each receiver, the multidimensional signal is then projected into a plane wave in the $-\boldsymbol{k}_A$ or $-\boldsymbol{k}_B$ direction at Alice or Bob, respectively, and its intensity is measured.

Even though the speckle patterns at the two ends of the fiber are different, there is a correlation between them because they are produced by transmission through the same reciprocal medium (although in opposite directions). As a condition of reciprocity, the intensity transmission properties for the opposite-direction paths must be the same [36]. The correlated intensity received at Alice and Bob is used to establish a shared key. A novel property of RCC worth noting is that neither Alice nor Bob generates the key, instead, it is created in a distributed fashion during transmission through the shared channel. Additionally, Alice and Bob do not need any knowledge of the projection operator used by the other user; Alice (and Bob) just need to use the *same* projection operator for their *own* transmission and reception.

The identical transmission characteristics of the two reciprocal paths between Alice and Bob in RCC can be expressed mathematically as follows. From Fig. 1(a), the electric field transmittances for forward and backward propagation are

$$t_{A\rightarrow B} = \boldsymbol{P}_B^T \boldsymbol{H} \boldsymbol{P}_A \tag{1}$$

$$t_{B\rightarrow A} = \boldsymbol{P}_A^T \boldsymbol{H}^T \boldsymbol{P}_B \tag{2}$$

where $\boldsymbol{H}$ is the $M \times M$ unitary transfer matrix of the MMF, $\boldsymbol{P}_A$ and $\boldsymbol{P}_B$ are the $M \times 1$ vectors describing the $M \leftrightarrow 1$ projection operators at Alice and Bob, and T denotes transpose [34]. Since transmittance is a complex scalar, $t_{A\rightarrow B} = t_{A\rightarrow B}^T$, leading to

$$t_{A\rightarrow B} = t_{A\rightarrow B}^T = \boldsymbol{P}_A^T \boldsymbol{H}^T \boldsymbol{P}_B = t_{B\rightarrow A}. \tag{3}$$

This illustrates that the link is reciprocal, and the transmittances of forward and backward propagation are equivalent, therefore the intensity received by Alice and Bob will be correlated.

The transfer matrix $\boldsymbol{H}$ of a MMF is, in general, randomly time-varying as its environment changes [28]. As a result, the random, time-varying, but identical transmittance

$$t_{A\to B}(t) = \boldsymbol{P}_A^T \boldsymbol{H}^T(t)\boldsymbol{P}_B = t_{B\to A}(t) \tag{4}$$

can serve as a common key between Alice and Bob. To obtain the key, Alice and Bob use direct detection to measure the time-dependent intensity at their receivers. The received intensities are related to the transmittance through $I_{(A,B)} = |t_{A\to B}|^2 I_{i(B,A)}$, where $I_{i(A,B)}$is the transmitted intensity from Alice and Bob, respectively. This was demonstrated experimentally in [28]–[30].

However, when key generation and distribution relies on the changing MMF characteristics, the key rate (BW) scales inversely with transmission distance (L). In order for Alice and Bob to obtain the same key, the fiber's transmittance should not change during a bit's fiber transit time to ensure that the same distributed mode coupling is experienced by light traveling in opposite directions [23], [28]. Therefore, the key rate cannot exceed the inverse of the fiber transit time, and the key rate-distance product is limited to

$$(\text{BW} \times L)_{\max} = \frac{c}{n} \approx 200\ \text{kbps} \cdot \text{km} \tag{5}$$

where c is the speed of light and n is the index of refraction, which is many orders of magnitude below the bit rate-distance product of telecommunication systems [27]. Previous experimental demonstrations of RCC that used fluctuations in MMF transmittance only achieved a key rate-distance product of 20 bps·km [28]–[30].

The key rate-distance product of RCC can be dramatically enhanced if the transmittance of the shared path is changed locally by modulating DOFs within one of the projection operators through the addition of a fast modulator. The transmittance with a time-varying projection operator is

$$t_{A\to B}(t) = \boldsymbol{P}_A^T \boldsymbol{H}^T(\delta \cdot t)\boldsymbol{P}_B(t) = t_{B\to A}(t-\tau) \tag{6}$$

where τ is a delay due to the difference in propagation distance between the modulator and the receivers and δ is a small parameter indicating that the fiber's transmittance $\boldsymbol{H}$ fluctuates slowly relative to the projection operator $\boldsymbol{P}_B$ and can be treated as constant within a bit interval [37]. Similar to the previous method, key generation is derived from the transmittance of the entire shared channel. However, high-speed RCC based on modulating the projection operator decouples the key rate and transmission distance since high-speed fluctuations occur locally, rather than distributed over the full fiber. While the fast-varying element must remain static during a bit's transit through the modulating section, this transit time is short relative to that of the MMF and allows for a key rate that is independent of the fiber length. This enables RCC to achieve much higher key rates, limited only by the bandwidth available in bidirectional modulators.

Modulators can only be added to one end of the link because adding modulators to both ends would lead to uncorrelated transmittance. For a channel with modulators at both ends, the transmittances for forward and backward propagation would be $t_{A\to B}(t) = \boldsymbol{P}_B^T(t)\boldsymbol{H}^T(\delta \cdot t)\boldsymbol{P}_A(t+\tau)$ and $t_{B\to A}(t) = \boldsymbol{P}_A^T(t)\boldsymbol{H}^T(\delta \cdot t)\boldsymbol{P}_B(t+\tau)$, respectively. The time arguments of the projection operators are different for the two paths. Thus, light travelling in the two directions will experience different modulations at the projection operators and the transmittances will no longer allow for key generation.

The transmitted intensity from the projection operator should be kept constant to prevent Eve from extracting key information from total intensity fluctuations in the shared channel. Therefore, in the case of intensity modulation, an additional parallel channel should be added to the modulated projection operator that maintains constant transmitted intensity by applying the inverse of the summation of the modulation applied to the other DOFs.

It was previously shown that it might be possible for Eve to extract the key using the full-field beamsplitter attack in RCC [28], [30]. Using the full-field beamsplitter attack, as shown in Fig. 2, Eve can measure the M-dimensional field from Alice, $\boldsymbol{E}_{EA} = \boldsymbol{H}_1\boldsymbol{P}_A e_{iA}$, and from Bob, $\boldsymbol{E}_{EB} = \boldsymbol{H}_2^T\boldsymbol{P}_B e_{iB}$, at Eve's location, where $\boldsymbol{H} = \boldsymbol{H}_2\boldsymbol{H}_1$ and e_{iA} and e_{iB} are the one-dimensional input electric field at

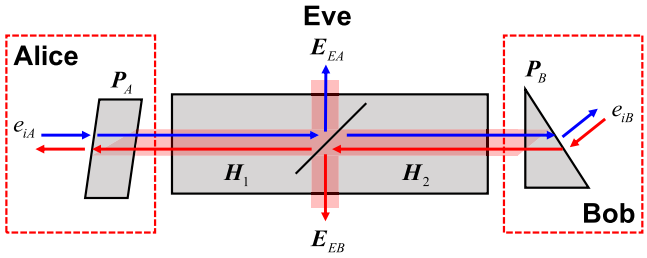


Fig. 2. Schematic of the full-field beamsplitter attack. Eve intercepts and diverts a portion of the field being transmitted from Alice to Bob ($\boldsymbol{E}_{EA} = \boldsymbol{H}_1\boldsymbol{P}_A e_{iA}$) and from Bob to Alice ($\boldsymbol{E}_{EB} = \boldsymbol{H}_2^T\boldsymbol{P}_B e_{iB}$), where $e_{iA}$and $e_{iB}$are the input fields at Alice and Bob, and $\boldsymbol{H}_1$($\boldsymbol{H}_2$) is the channel transfer matrix between Alice and Eve (Eve and Bob). From these measurements, Eve can extract the key.

Alice and Bob, respectively. If Eve performs the dot product between $\boldsymbol{E}_{EA}$ and $\boldsymbol{E}_{EB}$,she obtains

$$\boldsymbol{E}_{EB}^T\boldsymbol{E}_{EA} = \left[\boldsymbol{P}_B^T\boldsymbol{H}\boldsymbol{P}_A\right] e_{iA}e_{iB} \tag{7}$$

which is proportional to $t_{A\to B}$ and $t_{B\to A}$, allowing Eve to extract the key.

However, Eve's required measurements to obtain the key are substantially more complex than Alice and Bob's, thereby establishing technological security. First, using classical measurements, Eve must coherently detect the *M*-dimensional fields and then multiply the fields, $\boldsymbol{E}_{EA}$ and $\boldsymbol{E}_{EB}$. This requires Eve to perform *2M* coherent measurements. For MMF, *M* is typically on the order of hundreds. By contrast, Alice and Bob perform a single intensity measurement. Second, Eve must obtain the full-field $\boldsymbol{E}_{EA}$ and $\boldsymbol{E}_{EB}$ from the MMF core. This is considerably more difficult than for single-mode fiber (SMF), and practically requires the use of a MMF coupler or bulk beam-splitter [28]. Both methods force the eavesdropper to add an additional splice or break to the link, which will temporarily shut down traffic and produce a reflection point that can be detected by the legitimate users using standard optical time domain reflectometry [28]. Additionally, the system should be precisely characterized prior to and after deployment as changes in the system's loss or delay could be the result of devices added by the eavesdropper. This disparity in measurement complexity forms the basis of RCC's technological security, which is similar to the security currently offered by digital encryption methods but implemented at the physical layer.

Furthermore, [28] claims that RCC can be made information-theoretically secure under the full-field beamsplitter attack and classical coherent detection for link loss less than 12 dB, due to signal-to-noise degradation as a result of the increased number of measurements and additional signal processing required for the eavesdropper [28], [38]. A more detailed discussion of the information-theoretic security proof for RCC, as well as the security of RCC against both active and passive attacks, can be found in [28].

3. Experimental Setup and Results

The experimental set-up, shown in Fig. 3, utilized a 12-kilometer commercial MMF (OM4) as the random multidimensional channel. For our proof-of-concept high-speed RCC experiment, a laser operating at $\lambda = 1550$ nm with a linewidth of 100 kHz was split into two by a polarizing beamsplitter (PBS) and injected into both ends of the link. For practical deployment, independent, frequency-locked lasers should be used at Alice and Bob [28]. There are a range of remote laser frequency-locking techniques that Alice and Bob can implement, including injection locking, locking to external references, and direct measurements [39]–[41]. Optical circulators (OC) were used to separate the outgoing and incoming light at the transceivers. For the projection operators, Alice used a 6 LP mode photonic lantern (PL) and a PBS, while Bob's projection operator was composed of a PL, (an) electro-optic modulator(s), and a PBS [42]. While the conceptual demonstration presented in Fig. 1(b) used the wave-vector basis set for its projection operators, Alice and Bob may use any

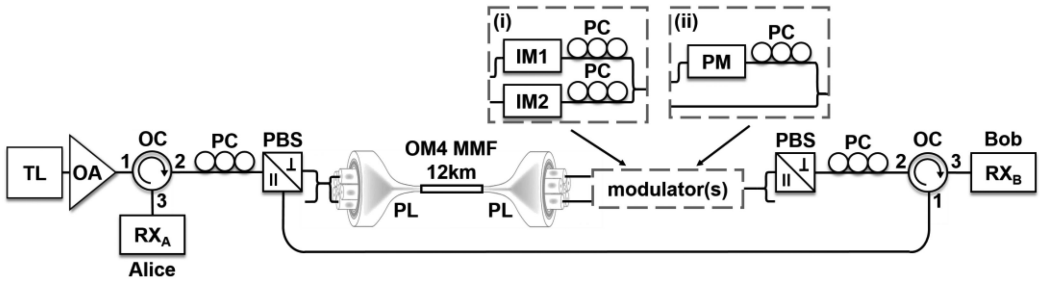


Fig. 3. RCC experimental setup using (i) intensity and (ii) phase modulation to vary the projection operator at Bob; TL: tunable laser, OA: optical amplifier, OC: optical circulator, PC: polarization controller, PBS: polarizing beamsplitter, PL: photonic lantern, IM: intensity modulator, PM: phase modulator, RX: receiver.

basis set. For this demonstration, the LP spatial mode basis set was used. Pre-amplified receivers were used by the legitimate users to measure the received intensity.

Experimental demonstrations using both amplitude and phase modulation were performed, as shown in Fig. 3(i) and (ii), respectively. Since the modulated light should be spread over all DOFs, via coherent mixing (represented by a complex unitary matrix) prior to entering the unprotected channel, either intensity or phase modulation will, in general, be coupled to both the amplitude and phase of all the DOFs. Therefore, to recover the key, Eve must measure both quadratures for all DOFs, whereas Alice and Bob make single quadrature measurements on a single DOF.

By adding a modulator to the projection operator at Bob's end, the transmission characteristics of the reciprocal path become time-varying at high speeds, thus generating and distributing a key. For this proof-of-concept experiment, the Mersenne-Twister algorithm was used to generate the pseudo-random number sequences that were applied to the modulators [43]. The Mersenne-Twister algorithm has been shown to have good statistical randomness and passes the Diehard and NIST SP800-22 test suites [43]–[45]. For practical deployment, a cryptographically secure pseudo-random or random number generator should be used to generate the signal applied to the modulators, as is required in QKD [46]–[48]. Since the light modulated at the projection operator must travel through the fiber to reach Alice's end, there is a delay between the signal received by Alice and Bob, and temporal alignment of their signals is needed. To determine the time delay, a cross-correlation between the signal received by Alice and Bob was performed. Calibration of this correction only needs to be performed once and this temporal alignment was applied in the digital domain to the results presented in Fig. 4. Differential detection was used during post-processing to minimize the effect of laser phase noise, which was slow-varying compared to the key rate.

Fig. 4(a) presents a portion of the matched analog sequence received by Alice and Bob at a raw modulation rate of 100 Mbps with a correlation coefficient of 0.97. The binary decision threshold was chosen as the mid-point and data points with amplitudes less than 10% of the maximum above and below the threshold (i.e., between the two dotted lines in Fig. 4(a) and within the dashed box in Figs. 4(c,d)) were excluded. After removing data points near the threshold and down sampling, 63 000 and 323 000 bits were detected for phase and intensity modulation, respectively. A portion of the digital signal is shown in Fig. 4(b). A net key rate-distance product of 63.4 Mbps and 64.7 Mbps $\times$ 12 km with no errors were achieved using phase and intensity modulation, respectively. For the RCC system described here where binary decoding was performed at the receiver, the upper limit on the key rate-distance product of the system was correlated to the MMF's bandwidth-distance product. It is possible to employ multi-level and/or quadrature decoding, for example pulse-amplitude modulation (PAM) or quadrature-amplitude modulation (QAM), to increase key bits per symbol and thus the key-rate-distance product. In that case, the BER will be determined by the signal-to-noise ratio, which will in turn be limited first by detector noises, and eventually by fiber nonlinearity. For practical deployment, Alice and Bob can use an authenticated public channel to perform information reconciliation and privacy amplification protocols to obtain the final key.

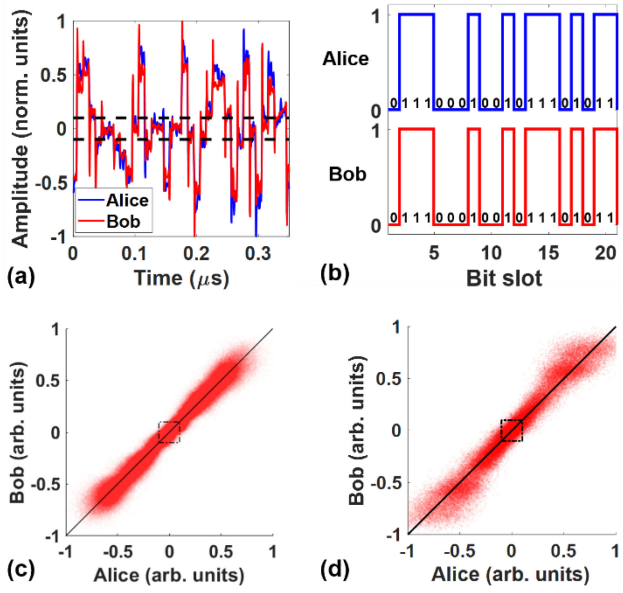


Fig. 4. (a) Well-correlated analog and (b) digital signals, with the corresponding bit sequence, received by Alice (blue) and Bob (red). (c,d) Intensity measured by Alice and Bob when using (c) intensity and (d) phase modulation, respectively. Data is distributed close to the solid black line which denotes perfect correlation. Data points near the threshold, within the dashed lines (a) and box (c,d), were removed during processing.

4. Discussion and Conclusions

We proposed and demonstrated a simple high-speed RCC that offers a much higher key rate-distance product than our initial demonstration while preserving its security properties [28]. A key rate of 64.7 Mbps over 12 km of MMF with no errors was achieved, corresponding to a seven orders of magnitude improvement in the key rate-distance product. For the RCC system described here where binary decoding was performed at the receiver, the upper limit on the system's key rate-distance product was correlated to the fiber modal bandwidth-distance product [49]. Further improvements in the key-rate distance product can be made using techniques from traditional optical communications, such advanced modulation formats and wavelength-division multiplexing [28]. Our demonstration made use of commercial off-the-shelf components and was fiber-based. These properties make RCC an attractive and simple key distribution method that can be readily deployed in applications based on few-mode or MM fiber, such as local area networks (LAN) or space-division multiplexed (SDM) networks [28]. SDM is one of the most active areas of research in telecommunications [27], [35], [50].

RCC possesses a significant hacking asymmetry due to Alice and Bob having access to one-dimensional fields, while Eve only has access to *M*-dimensional fields [28]. This allows Alice and Bob to perform a single direct measurement, while Eve must employ *2M* coherent measurements to characterize single-input multiple-output systems. Compared to previous fiber-based channel-state CKD methods which utilized SMF, RCC offers an increase in the DOFs through the use of MMF and thereby additional hacking asymmetry [24]–[26], [51]; an eavesdropper must characterize the *M*-dimensional complex field supported by the MMF, where the number of vector modes, *M,* is typically on the order of hundreds, compared to a 2-dimensional field in SMF. Measurement complexity and cost scales with the DOFs. With RCC, SDM networks can not only provide transmission capacity but also potentially key distribution.

References

[1] B. Scheier, *Applied Cryptography*. New York, NY, USA: Wiley, 1995.
[2] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov 1976.
[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Comm. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[4] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Secur. Privacy*, vol. 16, no. 5, pp. 38–41, Sep./Oct. 2018.
[5] L. Chen *et al.*, "Report on Post-Quantum Cryptography," National Inst. Standards Techn., Gaithersburg, MD, USA, Tech. Rep. 8105, Apr. 2016.
[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.
[7] R. Alleaume, "Using quantum key distribution for cryptographic purposes: A survey," *Security*, vol. 560, pt. 1 pp. 62–81, 2009.
[8] H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, no. 8, pp. 595–604, 2014.
[9] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, no. 2, pp. 513–577, 2005.
[10] F. Grousshan, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.
[11] C. H. Bennett, G. Brassard, C. Crepeau, U. M. Maurer, and S. Member, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
[12] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Info.*, vol. 2, no. 1, 2016, Art. no. 16025.
[13] Q. Zhang, F. Xu, Y. A. Chen, C. Z. Peng, and J. W. Pan, "Large scale quantum key distribution: Challenges and solutions," *Opt. Exp.*, vol. 26, no. 18, pp. 24260–24273, 2018.
[14] H. P. Yuen, "Security of quantum key distribution," *IEEE Access*, vol. 4, pp. 724–749, 2016.
[15] National Cyber Security Centre, Quantum security technologies. Victoria, London, 2020.
[16] K. I. Yoshino *et al.*, "Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses," *npj Quantum Info*, vol. 4, no. 1, pp. 1–8, 2018.
[17] H. Qin, R. Kumar, V. Makarov, and R. Alleaume, "Homodyne-detector-blinding attack in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 98, no. 1, 2018, Art. no. 012312.
[18] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial cryptography systems by tailored bright illumination," *Nat. Photon.*, vol. 4, no. 10, pp. 686–689, 2010.
[19] J. Scheuer and A. Yariv, "Giant fiber lasers: A new paradigm for secure key distribution," *Phys. Rev. Lett.*, vol. 97, no. 14, 2006, Art. no. 140502.
[20] A. El-Taher, O. Kotlicki, P. Harper, S. Turitsyn, and J. Scheuer, "Secure key distribution over a 500 km long link using a raman ultra-long fiber laser," *Laser Photon. Rev*, vol. 8, no. 3, pp. 436–442, 2014.
[21] A. Tonello *et al.*, "Secret key exchange in ultralong lasers by radiofrequency spectrum coding," *Light: Sci. Appl.*, vol. 4, no. 4, pp. 276, 2015.
[22] O. Kotlicki and J. Scheuer, "Dark states ultra-long fiber laser for practically secure key distribution," *Quantum Inf. Process.*, vol. 13, no. 10, pp. 2293–2311, 2014.
[23] K. Kravtsov, Z. X. Wang, W. Trappe, and P. R. Prucnal, "Physical layer secret key generation for fiber-optical networks," *Opt. Exp.*, vol. 21, no. 20, pp. 23756–23771, 2013.
[24] B. Wu, Y. Huang, S. Zhang, B. J. Shastri, and P. R. Prucnal, "Long range secure key distribution over multiple amplified fiber spans based on environmental instabilities," in *Proc. CLEO*, 2016, Paper SF1F.4.
[25] A. Hajomer, X. Yang, A. Sultan, and W. Hu, "Key distribution based on phase fluctuation between polarization modes in optical channel," *IEEE Photon. Tech. Lett.*, vol. 30, no. 8, pp. 704–707, Apr. 2018.
[26] L. Zhang, A. A. E. Hajomer, X. Yang, and W. Hu, "Error-free secure key generation and distribution using dynamic stokes parameters," *Opt. Exp.*, vol. 27, no. 20, pp. 29207–29216, 2019.
[27] P. Bayvel *et al.*, "Maximizing the optical network capacity," *Phil. Trans. A Math. Phys. Eng. Sci.*, vol. 374, no. 2062, 2016.
[28] Y. Bromberg, B. Redding, S. M. Popoff, N. Zhao, G. Li, and H. Cao, "Remote key establishment by random mode mixing in multimode fibers and optical reciprocity," *Opt. Eng.*, vol. 58, no. 1, 2019, Art. no. 016105.
[29] Y. Bromberg, B. Redding, S. M. Popoff, N. Ofek, and H. Cao, "Secure optical communication using random mode mixing and time-reversal symmetry in multimode fibers," in *Proc. CLEO*, 2014, vol. 4, Paper FTh5A.
[30] G. Li, Y. Bromberg, B. Redding, S. Popoff, N. Zhao, and H. Cao, "Classical key distribution in optical communication," in *Proc. Photon. West*, 2017, Art. no. 1013002.
[31] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Info. Forensics Secur.*, vol. 5, no. 2, pp. 240–254, Jun. 2010.
[32] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mob. Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.
[33] U. Levy, H. Kobrinsky, and A. A. Friesem, "Angular multiplexing for multichannel communication in a single fiber," *IEEE J. Quantum Elec.*, vol. 17, no. 11, pp. 2215–2224, Nov. 1981.
[34] K. P. Ho and J. M. Kahn, "Linear propagation effects in mode-division multiplexing systems," *J. Lightw. Tech.*, vol. 32, no. 4, pp. 614–628, 2014.
[35] G. Li, N. Bai, N. Zhao, and C. Xia, "Space-division multiplexing: The next frontier in optical communication," *Adv. Opt. Photon.*, vol. 6, no. 4, pp. 413–487, 2014.
[36] R. J. Potton, "Reciprocity in optics," *Rep. Prog. Phys.*, vol. 67, no. 5, pp. 717–754, 2014.

[37] C. R. Menyuk, "Application of multiple-length-scale methods to the study of optical fiber transmission," *J. Eng. Math.*, vol. 36, no. 1, pp. 113–136, 1999.
[38] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[39] M. Giunta, W. Hänsel, M. Fischer, M. Lezius, T. Udem, and R. Holworth "Real-time phase tracking for wide-band optical frequency measurements at the 20th decimal place," *Nat. Photon.*, vol. 14, no. 1, pp. 44–49, 2020.
[40] L. Hollberg *et al.*, "Optical frequency/wavelength references," *J. Phys. B: At. Mol. Opt. Phys.*, vol. 38, no. 9, 2005, Paper S469.
[41] S. M. Foreman, K. W. Holman, D. D. Hudson, D. J. Jones, and J. Ye, "Remote transfer of ultrastable frequency references via fiber networks," *Rev. Sci. Instruments*, vol. 78, no. 2, 2007, Art. no. 021101.
[42] A. M. Velazquez-Benitez *et al.*, "Six mode selective fiber optic spatial multiplexer," *Opt. Lett.*, vol. 40, no. 8, pp. 1663–1666, 2015.
[43] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudorandom number generator," *ACM Trans. Model. Comput. Simul.*, vol. 8, no. 1, pp. 3–30, 1998.
[44] Y. Wang and T. Nicol, "On statistical distance based testing of pseudo random sequences and experiments with PHP and debian OpenSSL," *Comput. Secur.*, vol. 53, pp. 44–64, 2015.
[45] A. Uchida, *Optical Communication with Chaotic Lasers: Applications of Nonlinear Dynamics and Synchronization*. Weinheim, Germany: Wiley-VHC Verlag & Co. KGaA, 2012.
[46] L. E. Bassham *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, PA, USA, Special Publication 800-22 rev. 1a, 2010.
[47] M. Stipcevic, "Quantum random number generators and their applications in cryptography," in *Proc. SPIE*, 2012, Art. no. 837504.
[48] A. Boaron *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, 2018, Art. no. 190502.
[49] G. Agrawal, *Fiber-optic Communication Systems*. Hoboken, NJ, USA: Wiley, 1992.
[50] D. J. Richardson, "Filling the light pipe," *Science*, vol. 330, no. 6002, pp. 327–328, 2010.
[51] I. U. Zaman, A. B. Lopez, M. A. Al Faruque, and O. Boyraz, "Physical layer cryptographic key generation by exploiting PMD of an optical fiber link," *J. Lightw. Tech.*, vol. 36, no. 24, pp. 5903–5911, 2018.