Optical Engineering

SPIEDigitalLibrary.org/oe

Optical key distribution system using atmospheric turbulence as the randomness generating function: classical optical protocol for information assurance

Marvin D. Drake
Christophe F. Bas
David Gervais
Priscilla F. Renda
Daniel Townsend
Joseph J. Rushanan
Joe Francoeur
Nick Donnangelo
Michael D. Stenner

SPIE

Optical key distribution system using atmospheric turbulence as the randomness generating function: classical optical protocol for information assurance

Marvin D. Drake
Christophe F. Bas
David Gervais
Priscilla F. Renda
Daniel Townsend
Joseph J. Rushanan
Joe Francoeur
The MITRE Corporation
202 Burlington Road
Bedford, Massachusetts 01730
E-mail: mddphd@mitre.org

Nick Donnangelo
Michael D. Stenner
The MITRE Corporation
7525 Colshire Drive
McLean, Virginia 22102

Abstract. We describe an experimental laboratory system that generates and distributes random binary sequence bit streams between two optical terminals (labeled Alice and Bob). The random binary sequence is generated through probing the optical channel of a turbulent atmosphere between the two terminals with coincident laser beams. The two laser beams experience differential phase delays while propagating through the atmospheric optical channel. The differential phase delays are detected and sampled at each terminal to yield raw random bit streams. The random bit streams are processed to remove bit errors and, through privacy amplification, to yield a bit stream known only to Alice and Bob. The same chaotic physical mechanism that provides randomness also provides confidentiality. The laboratory system yielded secret key bit rates of a few bits/second. For external optical channels over longer channel lengths with atmospheric turbulence levels, secret bit rates of 10 s of bits/second are predicted. [DOI: 10.1117/1.OE.52.5.055008]

Subject terms: optical key distribution; secret key generation; atmospheric randomness; optical protocol for information assurance; optical communication.

Paper 130253 received Feb. 15, 2013; revised manuscript received Apr. 25, 2013; accepted for publication Apr. 29, 2013; published online May 29, 2013.

1 Introduction

Since the beginning of warfare and politics, transmitting secret messages between two parties in a secure manner has been an ongoing activity and concern. The methods of generating and distributing the codes have evolved over the centuries, culminating in modern times with the invention and development of the public key encryption method known as RSA,[1] which is used over the Internet. However, it is generally accepted that encryption method based on algorithmic complexity could be broken as larger computers are built, or new computing paradigms are developed. An unbreakable method, called the Vernam cipher,[2] relies for its "unbreakableness" on a completely random encryption/decryption key being used by the two communicating parties, labeled Alice and Bob. But the encryption/decryption key must be kept secure when it is distributed to the communicating parties. Distributing the key electronically or by courier means the key could be compromised. A key distribution method based on the uncertainty principle of quantum mechanics, called quantum key distribution (QKD), has been developed.[3–8] In QKD, random number generators are used to determine both the state of the photon that is to be transmitted from Alice to Bob and the choice of the measurement that Bob will make on that photon. In theory QKD is secure against computational attacks, but in practice the security of QKD rests on having a source of single photons and high-speed single photon detectors.

We have developed a method of generating and distributing a random secret bit stream that leverages physical layer randomness, like QKD, but does not require exotic components that might not perfectly reflect theory. More specifically we have developed a method and system that uses the randomness of the turbulent atmosphere as the generating function and the exclusivity of the optical modes that are propagated between Alice and Bob as the security feature of this method. Since this method does not rely on quantum principles but instead uses only classical transmission and detection methods and components, we have labeled it classical optical protocol for information assurance (COPIA).

COPIA then is a method of generating and confidentially distributing random bits that may be used to encrypt communications. The method of generating the secret bits is based on measurements of the differential phase imparted to optical beams that traverse the turbulent atmosphere between the terminals of the two users, Alice and Bob. Alice and Bob each simultaneously send an optical beam toward each other's terminal, which is then reflected back toward the sender. Alice and Bob each measure the differential phase imparted to their individual transmitted and reflected optical beam. The differential phase that they each measure is due in part to the random variation of the index of refraction of the atmospheric channel through which the beams pass and, in part, to the delay in the measurement of phase. This random variation of the index of refraction is caused by the turbulence present in the atmosphere due to heating and cooling of the atmosphere, by differences in the atmospheric pressure and by wind velocity—all random physical processes. Alice and Bob measure substantially the same differential phase because their individual beams pass through the same volume of the atmosphere at the same time. The security of the COPIA protocol comes from (1) the secret bits are immune from crypto-analysis because they are derived

from a collection of independent physical random processes; (2) an eavesdropper cannot effectively sample the random phase disturbance, even with sensors placed in the middle of the optical channel; and (3) the distribution of random bits is only between Alice and Bob since only they will be able to measure the same differential phase. A valuable feature of the COPIA system is that the components were all developed for use in the optical telecommunications industry and are commercially available. The COPIA system does not require specialized components such as the single photon sources or detectors that are necessary in quantum key distribution systems. In the COPIA system, the optical power levels are such that standard optical sources and detectors can be used.

This paper describes the experimental results of generating random raw bit streams utilizing the turbulence of an atmospheric channel as the randomness generating function. The raw bit streams are processed by upper layers of the COPIA protocol through bit reconciliation and privacy amplification algorithms, which result in secret bit streams that are shared only between Alice and Bob. The sections of this paper will, in brief, describe the basic COPIA system concept (Sec. 2), the theory of atmospheric turbulence and induced phase variations (Sec. 3), the public channel used in COPIA (free space optical communication links) (Sec. 4), the measurements of the turbulent optical channel made by the COPIA system (Sec. 5), the randomness generation layer (Sec. 6), the COPIA experimental setup (Sec. 7), the phase extraction challenges (Sec. 7), the experimental results (Sec. 8), the expectation of bit rate versus C_n^2 and L (Sec. 9), the analysis of experimental data streams (Sec. 10), the processing of random bits to secret bits (Sec. 11), and conclusions and acknowledgments (Sec. 12).

2 COPIA System Concept

The basic layout of the COPIA system is shown in Fig. 1. Alice and Bob interact with each other over a terrestrial, free-space optical channel that exhibits nondeterministic, time-varying variations in the index of refraction consequential to thermodynamically driven turbulent mixing from which they generate mutual secret bits. Alice and Bob also use a public channel to exchange messaging for the secret sharing protocol. This public channel is assumed to be authenticated in that Alice and Bob can each confirm the sender of the messages. An eavesdropper, Eve, is assumed to observe all messages on the public channel. The levels of the COPIA protocol stack are shown in Fig. 2. The bottom layer in the COPIA protocol stack use the randomness generation physical channel and upper layers use the public messaging channel. In the next level of the protocol stack above the bottom level, software implements information reconciliation including random interleaving and interactive parity checks.

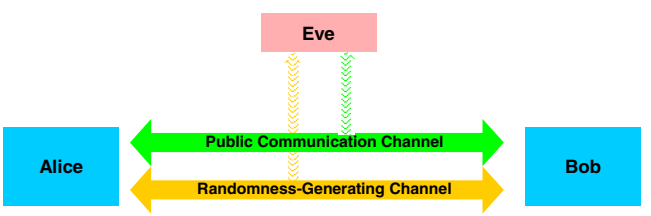

Fig. 1 COPIA optical channels.

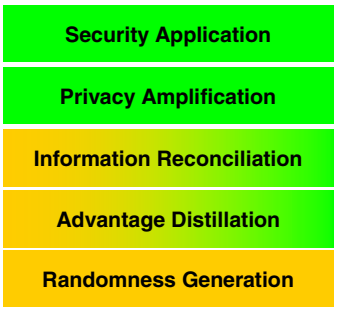

Fig. 2 COPIA protocol stack.

After Alice and Bob generate their separate random bit strings, the strings should agree at most corresponding time intervals. Even so, there will be values where the bit strings disagree, due to random independent transmitter and receiver noise and minor channel fluctuations. The next two steps to resolve these disagreements are advantage distillation and information reconciliation.

For advantage distillation, Alice and Bob use side information to decide which values are less likely to agree. These values are discarded, so that the following step of information reconciliation is only performed on those values where they have higher confidence that they agree. The discarding is coordinated using an interactive protocol over a public channel.

The second step, information reconciliation, is essentially an error-correction procedure. For input, Alice and Bob each have a string of bit values that may disagree in places. The output of the information reconciliation procedure is a common binary bit string shared by Alice and Bob. Alice and Bob may use several error-correction techniques for this step.

At this point in the protocol, Alice and Bob each possess the same random bit string. Eve may possess some knowledge of this string, perhaps from listening in on parity checks or just being lucky in her measurements. Following that, the protocol software performs privacy amplification including entropy estimation and application of a universal or cryptographic hash. By using privacy amplification, the negotiated binary string is reduced to a smaller string by hashing such that Eve's knowledge of the resulting smaller string is vanishingly small. The output of the privacy amplification step is a binary string that is random, secret from Eve, and shared by Alice and Bob. Finally, the protocol software performs randomness testing of the generated secret key bits as assurance that the terminals and the software are performing correctly.

3 Theory of Atmospheric Turbulence and Induced Phase Variations

In the classical theory, light is treated as an oscillation in a field ψ. For monochromatic plane waves arriving from a distant point source with wave-vector $\mathbf{k}$:

$$\psi_0(\mathbf{r}, t) = A_u e^{i(\phi_u + 2\pi v t + \mathbf{k}.\mathbf{r})}, \tag{1}$$

where ψ_0 is the complex field at position $\mathbf{r}$ and time t, with real and imaginary parts corresponding with the electric and magnetic field components, φ_u represents a phase offset, v is the frequency of the light determined by $\nu = x|\mathbf{k}|/(2\pi)$, and A_u is the amplitude of the light.

The photon flux in this case is proportional to the square of the amplitude A_u, and the optical phase corresponds to the complex argument of ψ_0. As wave fronts pass through the earth's atmosphere, they are perturbed by refractive index variations in the atmosphere. The perturbed wave front ψ_p may be related at any given instant to the original planar wave front $\psi_0(\mathbf{r})$ in the following way:

$$\psi_p(\mathbf{r}) = (\chi_a(\mathbf{r})e^{i\phi_a(\mathbf{r})})\psi_0(\mathbf{r}), \tag{2}$$

where $\chi_a(\mathbf{r})$ represents the fractional change in wave front amplitude and $\phi_a(\mathbf{r})$ is the change in wave front phase introduced by the atmosphere. It is important to emphasize that $\chi_a(\mathbf{r})$ and $\phi_a(\mathbf{r})$ describe the effects of atmospheric turbulence. The time scales for any changes in these functions are set by the speed of refractive index fluctuations in the atmosphere. This will be described in a later section.

3.1 *Kolmogorov Turbulence Model*

A description of the nature of the wave front perturbations introduced by the atmosphere is provided by the Kolmogorov model developed by Tatarski,[9] based partly on the studies of turbulence by the Russian mathematician Andreï Kolmogorov.[10,11] This model is supported by a variety of experimental measurements and is widely used in simulations of astronomical seeing and remote sensing. The model assumes that the wave front perturbations are brought about by variations in the refractive index of the atmosphere. These refractive index variations lead directly to phase fluctuations described by $\varphi_a(\mathbf{r})$ from the perturbing atmospheric layer to the terminal optics. For all reasonable models of the earth's atmosphere at optical and infrared wavelengths the instantaneous imaging performance is dominated by the phase fluctuations $\phi_a(\mathbf{r})$.

The phase fluctuations in Tatarski's model have a Gaussian random distribution with the following second order structure function:

$$D_{\varphi_a}(\rho) = \langle|\phi_a(\mathbf{r}) - \phi_a(\mathbf{r}+\rho)|^2\rangle_{\mathbf{r}}, \tag{3}$$

where $D_{\varphi_a}(\rho)$ is the atmospherically induced variance between the phase at two parts of the wave front separated by a distance ρ in the aperture plane, and the bracketed quantity represents the ensemble average. The structure function of Tatarski can be described in terms of a single parameter r_0:

$$D_{\varphi_a}(\rho) = 6.88\left(\frac{|\rho|}{r_0}\right)^{5/3}, \tag{4}$$

where r_0 indicates the strength of the phase fluctuations as it corresponds to the diameter of a circular optical aperture at which atmospheric phase perturbations begin to seriously limit the image resolution (the primary application for theoretical description of atmospheric turbulence in the literature is astronomical seeing). Fried[12] and Noll[13] noted that r_0 also corresponds with the aperture diameter, d, for which the variance σ^2 of the wave front phase is defined as:

$$\sigma^2 = 1.0299\left(\frac{d}{r_0}\right)^{5/3}. \tag{5}$$

This equation represents a commonly used definition for r_0, a parameter frequently used to describe the atmospheric conditions at astronomical observatories. The refractive index structure parameter is given by:

$$\langle[n'(\mathbf{r}_1) - n'(\mathbf{r}_2)]^2\rangle = {C_n}^2\rho^{2/3}, \quad \rho = |\mathbf{r}_1 - \mathbf{r}_2| < L_0. \tag{6}$$

The timescale t_0 is proportional to r_0 divided by the mean wind speed. For the optical system postulated for COPIA, the Fried parameter, r_0 is about 10 cm and timescale t_0 is one millisecond. It should be noted that the longer the optical path in the atmosphere, the shorter the timescale t_0.

Normal wind motion carrying temperature gradients vary with a log normal distribution.[14] These fluctuations cause a mishmash of random eddies of all length and scales to occur along the optical channel, with each eddy having a refractive index variation. The refractive index variations, $n'(r)$, have a Kolmogorov structure function across a wide range of scales from a few millimeters to an "outer scale" L_o of 1 kilometer or more. Turbulence induced eddies evolve and move with the mean wind speed V causing small centimeter-scale eddies to traverse a several centimeter wide laser beam in one to ten milliseconds while large, hundred meter scale eddies traverse the nominal several centimeter laser beam in tens of seconds.

4 Free-Space Optical Communication Links

Free space optical (FSO) links are typically used to fill in the gaps where optical fiber or wired communication links cannot be placed or are impractical. FSO links are capable of providing connectivity at data rates above 2.5 Gbps over distances of many kilometers, subject to atmospheric turbulence, absorption and scattering.[15] Examples include links between office buildings in major cities, office parks, college campuses, and on military bases.[16] FSO links have also been investigated between airborne and satellite platforms, between ships at sea to enhance communication data rate and security and for land-based combat units that require rapid setup and takedown of line-of-sight point-to-point links.[17] FSO links are also applicable to rapid deployment in disaster situations as well as backup for optical fiber.

We contemplate that the COPIA system uses a FSO communication link as its public channel, but there is no reason the public channel could not be wired, radio frequency or even IP based.[15] The implementation of COPIA physical layer draws heavily on the components that are currently used for both FSO as well as optical fiber communication links. The telescopes, the pointing-acquisition-tracking systems, the differential phase transmitter/receiver terminals, optical amplifiers as well as other components are all well developed and are available commercially from many suppliers. The wide presence of existing free space optical communication systems could allow COPIA to be colocated or mounted directly on the existing terminals.

5 COPIA Measurements

COPIA uses time varying changes in refraction of near infrared wavelength laser beams between the two communicating parties, Alice and Bob, as the source of the random values

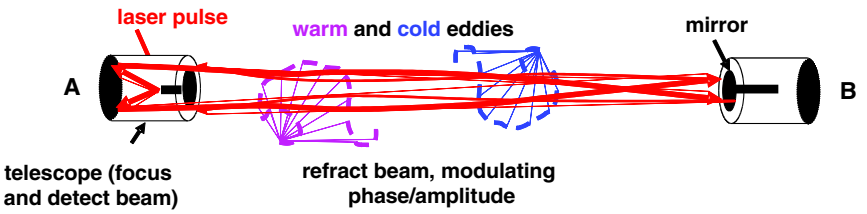

Fig. 3 COPIA channel model.

from which they are able to generate secure binary sequences. This is illustrated in Fig. 3.

Alice sends a CW laser beam from a telescope toward an identical telescope at Bob. This laser beam reflects off an internal retro reflector at Bob's terminal and returns back to Alice. Alice also stores a copy of the phase of her transmitted beam. Alice then continually measures the differential phase delay on her reflected signal. Bob also transmits a CW laser beam along a coincident beam path and measures the differential phase delay on his reflected signal. Since the optical channel turbulence is stationary during the time it takes for each of these beams to travel from Alice to Bob and back to Alice (or Bob to Alice and back to Bob), they will, given reciprocity, see almost identical total differential phase delay histories.

Each COPIA terminal incorporates an internal means to reflect the other terminal's transmitted beam back to the original sender (with field-of-view matched to the telescope). The COPIA system includes these reflectors at Alice and Bob's terminals. In this manner, the system samples the atmosphere's index of refraction variations in both directions and thereby eliminates asymmetries in the measurements of the propagation channel.

6 Randomness Generation Layer

To extract randomness from the turbulent free space optical channel, Alice and Bob perform a series of measurements. The steps are given from Alice's perspective, but they are identically described by switching the roles of Alice and Bob. In particular, each laser beam travels from Alice to Bob and from Bob to Alice through the same optical path.

1. Alice transmits a CW laser beam with slowly varying phase function.
2. Alice detects, samples, and stores a copy of the transmitted laser beam's phase history.
3. The transmitted beam travels through the atmosphere to Bob's telescope and is reflected back to Alice's receiver.
4. The transmitted and reflected laser beam undergoes a differential phase delay due to the index of refraction variations in the atmosphere.
5. At the receiver, the phase history of the transmitted and reflected beam is detected, sampled, and stored.
6. The stored copy of the transmitted phase history at Alice is delayed and then used as the local reference for homodyne detection of Alice's laser beam transmitted to and reflected from Bob's terminal.
7. The stored (and delayed) phase history and the reflected phase history are combined and coherently detected using a balanced pair of photodetectors.

The optical channel is considered stationary for the time required for the laser beam to travel back and forth through the atmosphere optical path. This detection of the differential phase of the atmospheric path is done by subtracting the phase history of the internal interferometer path from that of the external atmospheric path. This can be written in terms of coherent detection as:

$$V \propto E_{\text{inner}} E_{\text{outer}} \cos(\phi_{\text{outer}} - \phi_{\text{inner}}), \tag{7}$$

where V is the output voltage signal from the digital processing of the two coherently detected and sampled phase histories. In a simplistic discretion procedure, the sign of the coherently detected optical signal differential phase, $(\varphi_{\text{outer}} - \varphi_{\text{inner}})$, is periodically sampled and yields a random bit stream from these sampled values of the differential phase. For example, the value of phase delay qk' of each sampled differential phase value is detected and will yield a binary bit stream, sk, from the following:

$$\text{sk} = 1 \text{ if } 0 < qk'(\text{mod } 2\pi) < \pi, \tag{8}$$

$$\text{sk} = 0 \text{ if } -\pi < qk'(\text{mod } 2\pi) < 0. \tag{9}$$

For typical variations in C_n^2 (about 10^{-14} $\text{m}^{-2/3}$), the measured differential phase qk' changes by thousands of degrees a second, meaning that Alice and Bob can make an independent measurement roughly every 10^{-2} s. Higher precision incremental phase detection such as 0, $\pi/4$, $\pi/2$, $3\pi/4$ instead of just $+\pi$, $-\pi$ as used above may make possible more frequent measurements of the differential phase stream which would effectively increase bit rate.

7 Experimental Setup

The COPIA laboratory system has two optical terminals, Alice and Bob, as shown in the diagrams for the COPIA optical system in Figs. 4 and 5. The optical system was constructed on an optical table as shown in the photograph in Fig. 6. Each optical terminal has two lasers and corresponding interferometers, one that samples the atmospheric optical channel by transmission toward and reflection from the other terminal, and another laser that samples the internal optical phase of the terminal. The internal interferometer serves as the reference for the measurement of the differential phase disturbance induced by the atmospheric channel. The two lasers are closely spaced in wavelength and have very narrow line widths. In the laboratory system, the transmitted laser beam, or probing beam, passes through a simulated turbulent atmospheric optical channel to the other terminal, is reflected there and returns along the same path to the originating terminal where it is coupled back into the optical system. The simulated turbulent atmospheric optical channel is produced

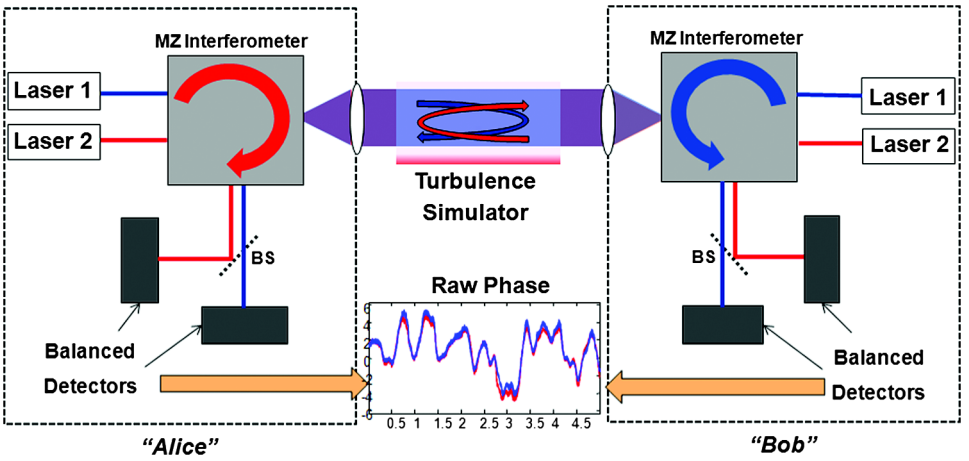

Fig. 4 Diagram of the COPIA optical system.

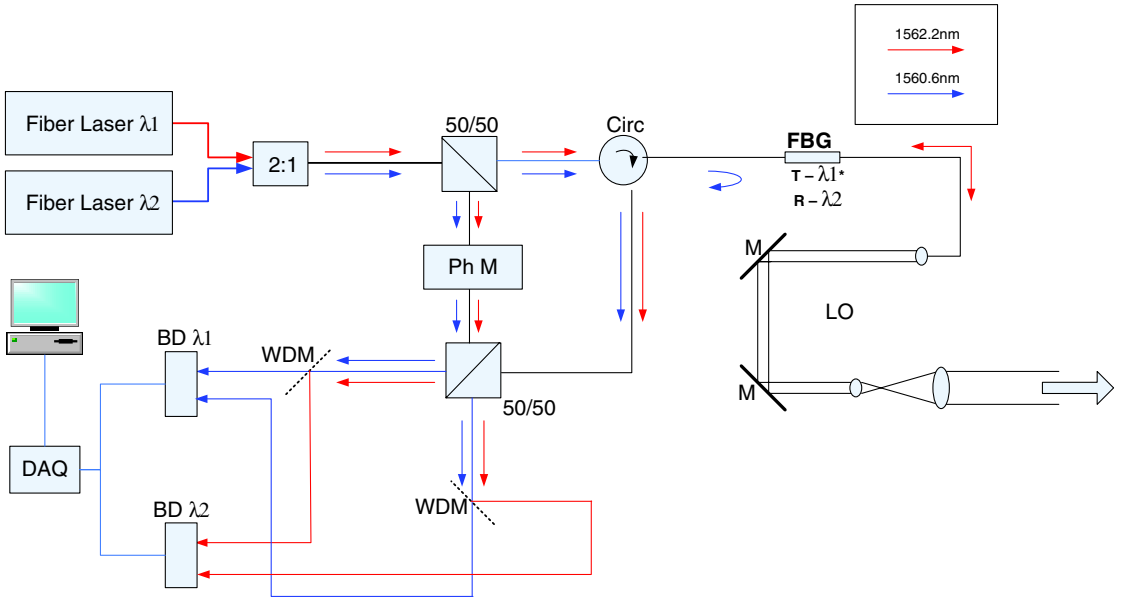

Fig. 5 COPIA terminal schematic: FBG = fiber Bragg grating; Ph *M* = phase modulator; WDM = wavelength division demultiplexer; BD = balanced detector; DAQ = data ac quisition.

by locally heating the air in the optical channel, as shown in Fig. 7, to simulate a C_n^2 of about 10^{-13} $m^{-2/3}$.

At the originating terminal, the probe interferometer and the internal interferometer signals are detected by a pair of balanced detectors such that the electrical signals out of the detector pair reflect the phase fluctuations induced by the atmospheric channel and the internal phase fluctuations, respectively. These electrical signals are sampled in analogue to digital converters and the digital signals stored and processed. The processing consists of calculating the optical phase of each signal, subtracting the phase of the reference signal from that of the transmitted signal, converting the continuous phase measurements into a bit stream and then decimating the raw bit stream at a rate commensurate with the randomness inherent in the atmospheric refractive index change.

A detailed schematic of the components in Alice's terminal of the COPIA system are shown in Fig. 5. The main fiber components make up two interferometer systems. All fiber components use single-mode polarization maintaining fiber. Two lasers are used to produce two closely spaced wavelengths, in our case 1562.2 and 1560.6 nm. Both wavelengths are combined using a 2×1 coupler at the entrance of the fiber optic system. They are then split using a 2×2 fiber coupler. The top output (as shown in Fig. 5) of this coupler is sent through a circulator to a fiber Bragg grating (FBG). At the FBG the two wavelengths of light are split. $\lambda 1$ is transmitted through the FBG while $\lambda 2$ is reflected from the fiber Bragg grating. $\lambda 1$ is then launched into free space, transmitted through the air to the opposite terminal where it is then reflected back to the original terminal by a FBG in Bob's terminal and enters into Alice's system through the launching optics and FBG. The separation of the wavelengths by the FBG allows the system to measure the phase changes of the external air path and the internal fiber path using $\lambda 1$, while separately measuring the phase changes of the internal fiber path alone using $\lambda 2$.

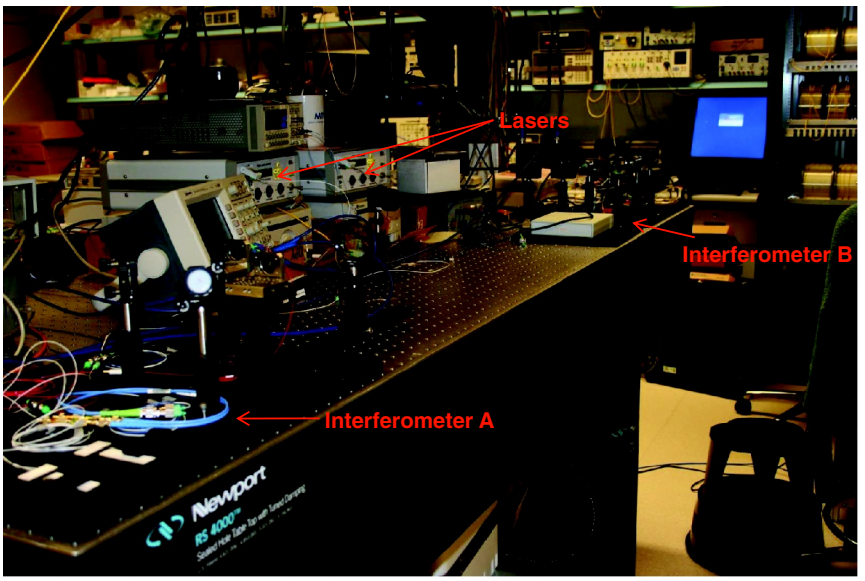

Fig. 6 COPIA laboratory system.

The light returning through the circulator (either $\lambda 1$ that has been reflected from the opposite terminal or $\lambda 2$ that was reflected from the FBG) is then sent to a second 2×2 coupler where it is combined with the light from the second arm of the initial 2×2 coupler. Before the light from the lower arm of the initial 2×2 coupler enters the second 2×2 coupler, it is sent through a phase modulator. The phase modulator imparts a modulation signal on the light, which aids in the extraction of the phase data in post-processing as discussed further in Sec. 7.

Once the optical signals in the two arms of the interferometer are combined in the second 2×2 coupler, the outputs of the coupler are passed through wave division multiplexer units to separate the two wavelengths. One of the balanced detectors measures $\lambda 1$ and thus the phase change of the air path plus the internal fiber path. The other balanced detector measures $\lambda 2$ and thus measures the phase change of the internal path alone. The outputs of the balanced detectors are recorded using a data acquisition system connected to the computer where the post-processing for phase extraction occurs.

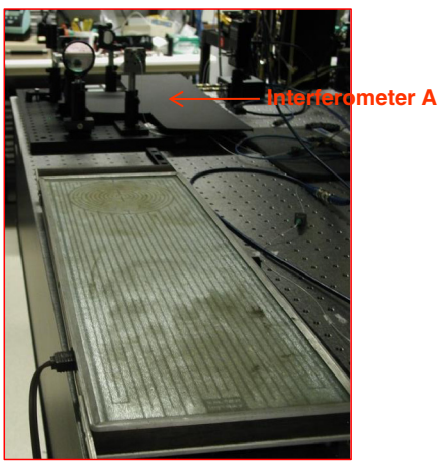

Fig. 7 Heater plate used to create simulated atmospheric turbulence.

The FBG on the terminal opposite Alice's has opposite wavelength characteristics: it transmits $\lambda 2$ while reflecting $\lambda 1$. The two wavelengths are therefore used for opposite purposes on the opposing (Bob's) terminal: $\lambda 2$ is used to monitor the phase fluctuations of the air path plus the internal fiber path while $\lambda 1$ monitors the internal path only. This switch in optical characteristics allows the two opposing terminals to keep the optical beam that they use to measure the air path phase separate from each other since they have different wavelengths. The FBG has a secondary purpose in that it acts as a mirror for the beam from the opposite terminal reflecting it back to the terminal that transmitted it. The choice of the two wavelengths used in these experiments—in our case 1562.2 and 1560.6 nm—must balance two requirements: (1) both wavelengths must experience essentially the same phase delay as they travel through the optical channel, and (2) they must be separated in wavelength sufficiently so that one will pass through the FBG and the other one will be reflected. The FBGs used also had to have the capability to perform both the pass-through and the reflection of these two wavelengths.

The two-way laboratory COPIA system was constructed and exercised between two two-way terminals (Alice and Bob) as shown in Fig. 6. A turbulent atmosphere was simulated by heating the air of the optical path using a heating plate as shown in Fig. 7. The heating resulted in a high level of turbulence ($C_n^2 \approx 10^{-10}$) over an approximately 1 m optical path. This level of turbulence simulated atmospheric turbulence levels of $C_n^2 \approx 10^{-14}$ to 10^{-12} over a 1 km optical path. Two channels of differential phase data were taken over many data runs and showed strong correlation between Alice and Bob's phase data. This is shown in the plot at the bottom of Fig. 4 where the red and blue traces are the differential phase data from Alice and Bob, respectively. The differential phase data streams were processed to yield random bit streams with bit rates $\approx a$ few bits/second. Analysis of the random bit streams will be discussed in Sec. 10.

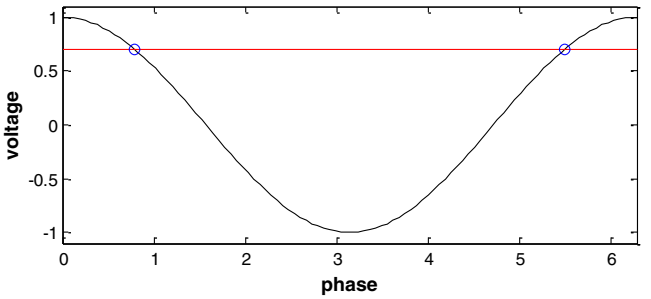

Fig. 8 Voltage from detectors versus differential phase (radians).

8 Phase Extraction Challenges

The differential phase is multivalued with voltage; that is, the voltage resulting from the coherent detection of the differential phase cannot be uniquely converted to a single value of phase (see Fig. 8). The output voltage of the matched detectors can be written as Eq. (7).

Also, the measured voltage depends on the field amplitude, E_{outer}, as well as phase, so amplitude fluctuations (also caused by turbulence) will masquerade as phase variations (see Fig. 9).

Both of these challenges can be addressed by introducing a deliberate phase dither onto the internal field. A phase modulator is inserted in the internal interferometer path (see Fig. 5), and a large ($>2\pi$) phase oscillation (dither) is added to the phase history in the internal path such that:

$$\phi_{\text{inner}} \rightarrow [\phi_{\text{inner}} - D\cos(\omega t)]. \tag{10}$$

By introducing the oscillating dither onto the internal field, the voltage measurement becomes:

$$V \propto E_{\text{inner}} E_{\text{outer}} \cos[\phi_{\text{outer}} - \phi_{\text{inner}} + D\cos(\omega t)]. \tag{11}$$

By comparing the oscillation of the detector voltage, V, to the known dither oscillation, ωt, the phase contribution to V from $(\varphi_{\text{outer}} - \varphi_{\text{inner}})$ can be uniquely determined. The dither signal also helps avoid errors from amplitude fluctuations. If the dither amplitude D is large enough ($>\pi$), the cosine will always "hit the rails" for each dither cycle (see Fig. 10). The envelope then provides a measure of the amplitude, which can be normalized out, leaving a clean phase measurement.

The final challenge to accurate phase measurement is that the phase of the optical path inside the terminals varies slowly with mechanical and thermal changes. This challenge is addressed in several ways: (1) all fiber and optical components are polarization-maintaining; (2) the phase is set to zero at a fixed interval shared by both terminals—this does not affect the probability of 0/1, but it removes accumulated drift between the two terminals; and (3) a second interferometer of a similar wavelength is included in each optical terminal (see Fig. 5). The two interferometers are identical except that the reference interferometer reflects at the output coupler and does not follow the shared atmospheric path. The differential phase caused by the turbulent atmosphere can then be extracted by the following:

$$\varphi_{\text{sig}} = \varphi_{\text{outer}} - \varphi_{\text{inner}} \tag{12}$$

$$\varphi_{\text{ref}} = \varphi_{\text{outer}} - \varphi_{\text{inner}} - \varphi_{\text{atmosphere}} \tag{13}$$

$$\varphi_{\text{atmosphere}} = \varphi_{\text{sig}} - \varphi_{\text{ref}}. \tag{14}$$

The reference interferometer can then be used to compensate for fluctuations in the devices of the terminal optical paths.

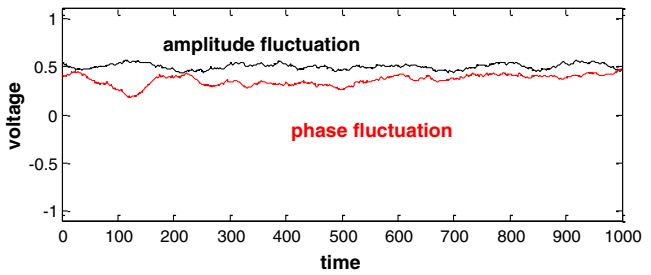

Fig. 9 Amplitude fluctuations may mask phase fluctuations.

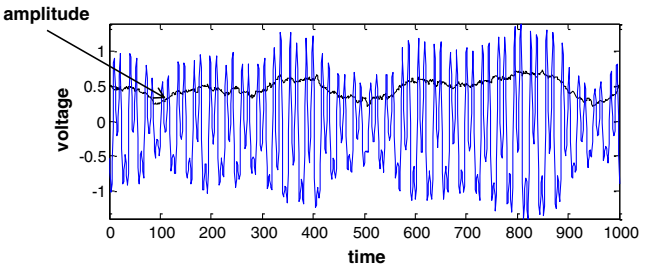

Fig. 10 Amplitude and dithered phase variations.

9 Results

The results of typical measurements of the shared differential atmospheric phase, as measured by the two terminals, are shown in Fig. 11 [red trace is Terminal 1 (Alice) and the blue trace is Terminal 2 (Bob)].

From the shared atmospheric phase measurement, Alice and Bob each generate a string of raw binary bits. The binary values, b, are assigned to each phase measurement according to the formula:

$$\mathbf{b} = 1 \qquad \text{when} \quad \left[\frac{\phi(\text{mod}\,2\pi)}{\pi}\right] = [0 < \phi < +\pi], \tag{15}$$

$$\mathbf{b} = 0 \qquad \text{when} \quad \left[\frac{\phi(\text{mod}\,2\pi)}{\pi}\right] = [-\pi < \phi < 0]. \tag{16}$$

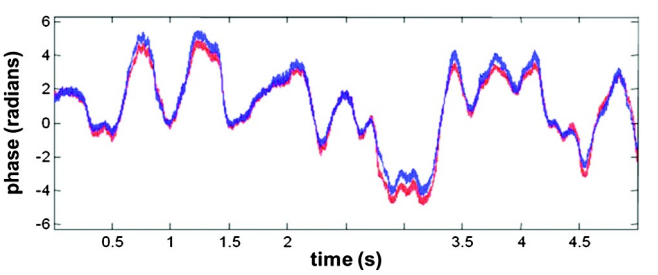

Fig. 11 Shared atmospheric phase measurement.

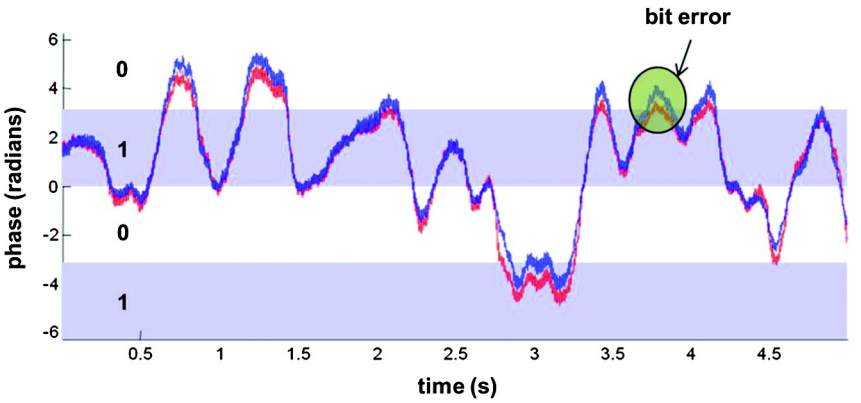

Fig. 12 Bit errors at inflection points of differential phase measurements.

This is shown graphically in Fig. 12, which also shows where bit errors may occur at the inflection points of the cosine curve.

Each phase measurement is converted to a raw bit, b, resulting in a raw bit-stream. However, if the phase measurements of the optical channel are oversampled (i.e., sampled faster than the rate at which the turbulence is changing the differential phase of the channel), then the raw bits will be correlated. Raw samples must be decimated so final bits are uncorrelated and fully random. Final decimation bit-rate is chosen to ensure randomness by observing C_n^2 (the degree of atmospheric turbulence) and the phase coherence time (temporal separation at which phase values are unrelated).

A plot of the autocorrelation of the bit stream in Fig. 12 is shown is Fig. 13. This plot indicates that the raw bit stream shown in Fig. 12 de-correlates after 0.5 to 1 s. Thus the raw bit stream is uncorrelated when the differential phase plot is decimated ≤ 2 samples/second.

10 Expectation of Bit Rate Versus C_n^2 and L

The expected bit rate will vary and will increase as C_n^2 and/or path length L increases. This variation is caused by the decrease in spatial coherence length, r_o, of the optical wave front. In addition, the wind velocity, V, will cause r_o-sized regions of turbulence (eddies) to pass through the optical path as shown in Fig. 14. Then uncorrelated phase measurements can be taken at a bit rate, $R = V/r_o$, where:

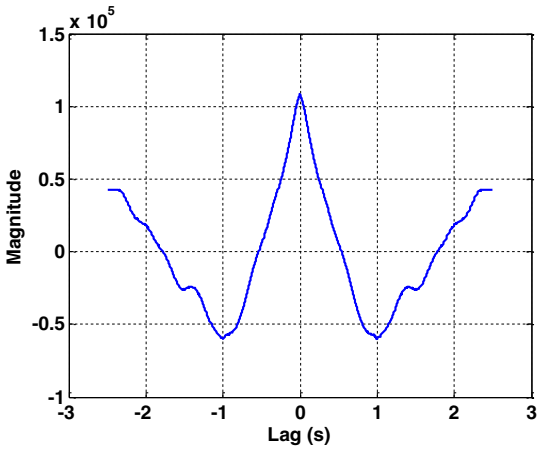

Fig. 13 Autocorrelation plot of raw bit stream samples from Fig. 12.

$$r_0 = 0.185\lambda^{6/5}[C_n^2 L]^{-3/5} \tag{17}$$

$$\frac{1}{R} \asymp \frac{r_0}{V} = 0.185\frac{\lambda^{6/5}}{V}[C_n^2 L]^{-3/5}. \tag{18}$$

To compare the physical measurements in the lab with the theory of $R = V/r_0$, the following parameters from the laboratory conditions were used to calculate R and used in a simulation of the differential phase measurements: $C_n^2 = 10^{-10}$, $L = 1$ m, $V = 0.1$ m/s and $r_0 = 2$ cm.

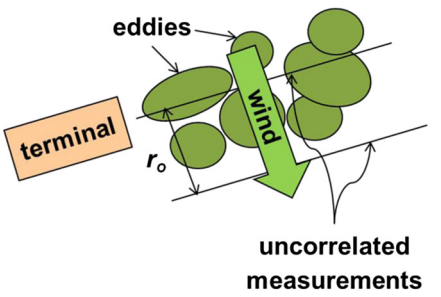

Fig. 14 Movement of r_0 sized turbulent eddies through the optical path.

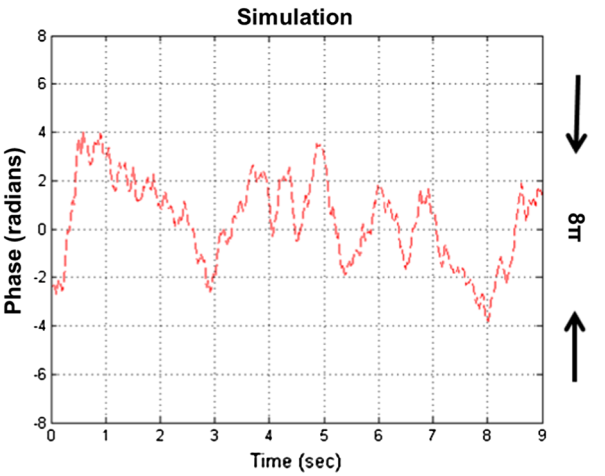

Fig. 15 Simulation of differential phase with laboratory parameter values (compare to the lab experimental measurements shown in Fig. 11).

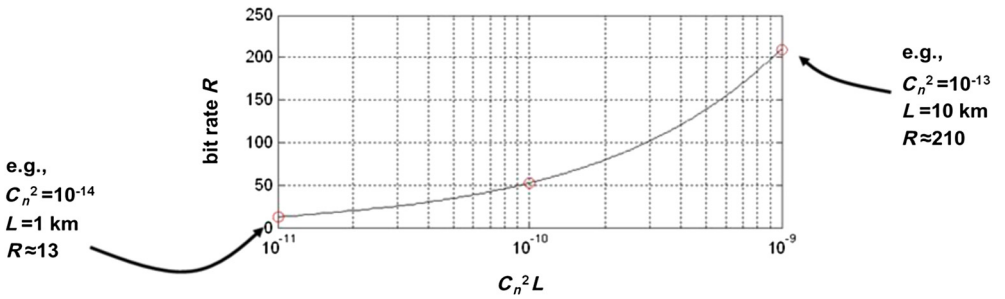

Fig. 16 Random bit rate versus product of $C_n^2 L$ (simulation).

The results are: $R \approx 5$ Bits per second (theoretical) compared with $R \approx 2$ Bits per second (laboratory measurements). The results of the simulation are plotted in Fig. 15, which shows excellent quantitative and qualitative agreement between the theoretical simulation and the laboratory experiment results, which are shown in Fig. 11.

When the above laboratory parameters values were extended to those that would be typical in a field experiment; namely, $C_n^2 = 10^{-13}$, $L = 1$ km, $V = 1$ m/s and $r_0 = 2$ cm, and the simulation run with these values, the result was $R \approx 50$ Bits per second, a much higher secret bit rate. The simulation was then run for R as a function of the product of $C_n^2 \times L$ with the results shown in Fig. 16. Increasing the separation, L, of the two terminals will increase the time of flight of the optical beams and slightly slow down the generation of the raw bit streams, but this will at the same time increase the amount of phase change occurring in the two beams. This increase in the amount of phase change will enable the system to sample the phase change at a higher rate and thus increase the secret bit rate generation as shown in Fig. 16.

11 Analysis of Experimental Data Streams

The experimental setup was exercised by capturing 5 s blocks of data (this was limited to 5 s blocks of data by the data storage capability of the experimental setup). A total of 514 blocks of data were captured for each terminal (Alice and Bob) and analyzed. Comparing the data blocks of bit streams of Alice and Bob yielded a minimum bit error rate between these two data sets of 5% and a maximum of 10%. When the data was reduced by decimation of 10 bits/s, the data blocks yielded 25,700 bits but yielded 12,850 bits and 5,140 bits when decimated by 5 bits/s and 2 bits/s, respectively. These three groups of bits were further analyzed for randomness using the NIST Statistical Test Suite (v. 2.0b).[18] This test suite includes 16 tests designed to detect nonrandomness. However, we used only a subset of seven of these tests due to the small size of the data sets from our experiments. These tests yields a p-value as a measure of success, where "success" is defined as consistent with randomness if the p-value is larger than 0.01 in each test in the suite. The results of the tests are shown in Fig. 17 for the seven different tests and the three levels of decimation of the data blocks. As mentioned earlier, the bit streams then are uncorrelated when decimated at ≈2 bits/s for the experimental conditions experienced in the laboratory. Conditions outside the laboratory will be with longer optical path lengths and higher levels of turbulence, resulting in higher $C_n^2 L$ products, in which case both the decimation rate, and the resulting bit rate will be higher (see Fig. 16).

12 Random Bits to Secret Bits

The random bits streams, R_{random} generated in the laboratory must be further processed for information reconciliation by any of several different error correction routines. One well-know interactive error correction method used in the laboratory instantiation of COPIA is CASCADE. In this process, we expect to lose about half the bits as parity if the BER is between 5% and 10% but less than half for smaller BERs. After the reconciliation process, the bit stream must also undergo privacy amplification, which will be based on a security parameter S. A block of bits of size M bits is hashed to a block of bits sized $M - 2 \times S$ bits where $M = (R_{\text{random}}/2) \times N$, and $N =$ of seconds. The final average secret bit rate will then be:

$$R_{\text{secret}} = \frac{R_{\text{random}}}{2} - \frac{2 \times S}{N}. \tag{19}$$

For example, if $R_{\text{random}} = 50$ bits/s $N = 600$ s $M = 15000$ $S = 160$ (typical) then $R_{\text{secret}} = 24.47$ bits/s after both reconciliation and privacy amplification.

Test	Bits per second		
	2	5	10
Frequency (Monobit)	0.418517	0.216820	0.032897
Frequency (Block)	0.450938	0.410315	0.000001
Runs	0.852312	0.000501	0.000000
Longest Run of 1s in a Block	0.816628	0.823224	0.000000
FFT	0.077580	0.920206	0.008021
Cumulative Sums (Forward)	0.794046	0.249578	0.023053
Cumulative Sums (Backward)	0.352028	0.174016	0.012824

Pass (≥ 0.05)
Borderline (between 0.01 and 0.05)
Fail (< 0.01)

Fig. 17 P-values for experimental data sets.

13 Conclusions

A two-way laboratory COPIA optical system has been constructed and exercised that generates and distributes random bit streams between two terminals (Alice and Bob).[19] The random generating function is the atmospheric turbulence along the optical path between the two terminals. The optical path between these two terminals had lab-simulated turbulence levels of C_n^2 of 10^{-17} to 10^{-15} scaled to an optical path length of 1 km. Differential phase data was taken simultaneously at Alice and Bob's terminals over many data runs. These differential phase data showed strong correlation between Alice and Bob's phase data. The differential phase data streams were processed to yield raw key bit streams at several different decimation rates and gave bit rates of a few bits/second at a decimation rate of 2 bit/s. The raw bit streams were analyzed by NIST methods to show randomness of >99% ($p > 0.01$). Extrapolation of the laboratory C_n^2 levels and path length to atmospheric C_n^2 levels and path lengths predict secret key rates of 10s of bits/second. Further experiments are planned with longer path lengths to increase the secret key bit stream rates.

Acknowledgments

The authors wish to thank Department Head Ira Shapiro for his continued support and encouragement of this work and thank Eric Case and Mike Richey for their support of the mathematical analysis of the data streams.

References

1. R. L. Rivest, A. Shamir, and L. M. Adelman, "On digital signatures and public-key cryptosystems," *Comm. ACM* **21**(2), 120–126 (1978).
2. G. Vernam and J. Mauborgne, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *J. Amer. Inst. Elect. Eng.* **XLV**, 295–301 (1926).
3. Ch. H. Bennett et al., "Experimental quantum cryptography," *J. Cryptol* **5**(1), 3–28 (1992).; N. Gisin et al., "Quantum cryptograpy," *Rev. Modern Phys.* **74**(1), 145–195 (2002).
4. id Quantique SA, rue Cingria 10, CH-1205 Geneva, Switzerland, http://www.idquantique.com.
5. MagiQ, Somerville, MA, USA, http://www.magiqtech.com.
6. QinetiQ Ltd., Malvern Tech. Center, Malvern, UK, http://www.QinetiQ.com.
7. D. Stucki et al., "Quantum key distribution over 67 km with a plug & play system," *New J. Phys.* **4**, 41.1–41.8 (2002).
8. C. Kurtsiefer et al., "Quantum cryptography: a step towards global key distribution," *Nature* **419**, 450 (2002).
9. V. I. Tatarski, *Wave Propagation in a Turbulent Medium*, McGraw-Hill Books, New York, NY (1961).
10. A. N. Kolmogorov, "Dissipation of energy in the locally isotropic turbulence," *Comptes rendus (Doklady) de l'Académie des Sciences de l'U.R.S.S.* **32**, 16–18 (1941).
11. A. N. Kolmogorov, "The local structure of turbulence in incompressible viscous fluid for very large Reynold's numbers," *Comptes rendus (Doklady) de l'Académie des Sciences de l'U.R.S.S.* **30**, 301–305 (1941).
12. D. L. Fried, "Statistics of a geometric representation of wavefront distortion," *Opt. Soc. Am. J.* **55**(11), 1427–1435 (1965).
13. R. J. Noll, "Zernike polynomials and atmospheric turbulence," *Opt. Soc. Am. J.* **66**(3), 207–211 (1976).
14. R. R. Beland, Chapter 2, "Propagation through atmospheric optical turbulence," *The Infrared & Electro-Optical Systems Handbook*, Vol. 2—Atmospheric Propagation of Radiation, F. G. Smith, Ed., Co-published by ERIM-Infrared Information Analysis Center and SPIE Optical Engineering Press, Ann Arbor, MI; Bellingham, WA (1993).
15. Sonabeam, fSONA optical wireless, http://www.fsona.com.
16. P. Yan et al., "Enhancing mobile ad hoc networks with free-space optics," *Opt. Eng.* **46**(8), 085008 (2007).
17. J. G. Rarity et al., "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.* **4**, 82.1–82.9 (2002).
18. Randomness Testing of the Advanced Encryption Standard Candidate Algorithms," NIST IR 6390, http://www.nist.gov/publication-portal.cfm# (September 1999).
19. N. Donnangelo et al., "Method of generating and securely distributing cryptographic bit sequences using naturally occurring chaotic processes," U.S. Patent NO 8189785 (2012).

Marvin D. Drake is a lead engineer with the MITRE Corporation in Bedford, Massachusetts. He received the BSEE-cum laude from the University of Toledo in 1960 and a PhD from the Johns Hopkins University in 1970. He has published in the areas of optical processing, optical communications, fiber optics, fingerprint devices, and ferroelectrics. His continuing interest is in optical communication and photonics.

Christophe F. Bas received his MS in electrical engineering from the Université de Nantes (France) in 1991 and a PhD in electrical engineering (with a minor in meteorology) from the Pennsylvania State University (USA) in 2002. Since his employment with the MITRE Corporation in 2001, he has been contributing engineering solutions to many U.S. government agencies, such as the Defense Advanced Research Projects Agency (DARPA), the Air Force Weather Agency (AFWA), and the Department of Justice (DoJ). His interests encompass any form of sensing, weather phenomena, and biometrics.

David Gervais received BS and MS degrees in electrical engineering from the College of Engineering at Boston University in 2001 and 2004, respectively. His research interests include quantum nonlinear optics and photonic-based communication systems. He has been working at the MITRE Corporation since 2001 engaged in various projects spanning sensing, communication, and navigation.

Priscilla F. Renda received her BS in physics from Bates College and her MS in electrical engineering from Boston University in 1999 and 2009, respectively. She is a senior integrated electronics engineer at the MITRE Corporation and has been employed there since 1999 performing testing, design, and research for a wide range of programs in the fields of optical communications and sensing.

Daniel Townsend received his BSEE and MSEE from Northeastern University. He is a senior sensors system engineer with the MITRE Corporation, Bedford, Massachusetts.

Joseph J. Rushanan is a principal mathematician in the Signal Processing Department of the MITRE Corporation, where his recent focus has been in navigation and secure systems. He was part of the GPS M-code Signal and L1C Signal Design Teams and is currently helping to define the next generation security architecture for military GPS user equipment. He has published in various areas of discrete mathematics, especially in binary sequences. He received a BS and

MS from the Ohio State University and a PhD from Caltech, all in mathematics, and has been with MITRE since 1986.

Joe Francoeur is a senior software engineer at the MITRE Corporation. He develops software involving mathematical algorithms from diverse areas of science and engineering, including digital signal processing, cryptography, discrete mathematics, and bioinformatics. He earned his BS and MS degrees, both in applied mathematics, from Purdue University. He is the author of a paper describing an implementation of spreadsheet recomputation and the coauthor of a bioinformatics paper describing a new approach for the detection of single nucleotide polymorphisms (SNPs).

Nick Donnangelo joined the MITRE Corporation in 2001. He authored nine patents and patent applications, on topics as diverse as bistatic radar, cryptography and dielectric sensing. Before joining MITRE he was the founding partner of NCD Management Solutions and the president and CEO of Avion Systems, Inc. In addition to advising numerous technology companies on advanced research and development, he served as a director of the Center for Law and Accountability. Nick is an aerospace engineer by training with advanced study in control theory and applied mathematics.

Michael D. Stenner received his PhD in physics from Duke University in 2004 for the study of fast- and slow-light pulse propagation. He has since worked at the University of Arizona and (currently) the MITRE Corporation where he develops novel optical sensing and communication devices.