Secure Key Distribution Using Correlated Randomness in Lasers Driven by Common Random Light

Kazuyuki Yoshimura,[1] Jun Muramatsu,[1] Peter Davis,[1] Takahisa Harayama,[1] Haruka Okumura,[2]
Shinichiro Morikatsu,[2] Hiroki Aida,[2] and Atsushi Uchida[2]

[1]*NTT Communication Science Laboratories, NTT Corporation 2-4, Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237, Japan*
[2]*Department of Information and Computer Sciences, Saitama University, 255, Shimo-Okubo,*
Sakura-ku, Saitama City, Saitama 338-8570, Japan

(Received 2 March 2011; published 14 February 2012)

We propose a secure key distribution scheme based on correlated physical randomness in remote optical scramblers driven by common random light. The security of the scheme depends on the practical difficulty of completely observing random optical phenomena. We describe a particular realization using the synchronization of semiconductor lasers injected with common light of randomly varying phase. We experimentally demonstrate the feasibility of the scheme over a distance of 120 km.

DOI: 10.1103/PhysRevLett.108.070602 PACS numbers: 05.40.−a, 05.45.Xt, 42.55.Px, 42.79.Sz

Secure key distribution is of crucial importance for the security of information systems. In a cryptosystem, secure communication between two users is based on a secret key, which is known only to them. A secure key distribution scheme is necessary for the two users to share this secret key. It is known that there are two different notions of security, i.e., computational and information theoretic security. The former assumes a limitation on the computational ability of the attacker, while the latter does not. The issue of secure key distribution based on physical principles concerns the latter one and it has been of increasing interest. Quantum key distribution (QKD) [1,2] is important from the point of view of ultimate physical security but it is difficult to implement in practice, especially over long distances. Thus, it is important to also consider alternative methods with less limitations.

Recently, some schemes based on classical optical phenomena have been proposed [3–5] and they have attracted interest from the point of view of practical feasibility (e.g., [6]). However, the security of these schemes has not yet been analyzed quantitatively.

The notion of generating secret keys from correlated physical randomness has strong information theoretical foundations. Maurer proved that, when two users are able to sample correlated random sources, it is possible for them to create a shared secret key from the samples by exchanging messages over a public channel [7]. Recently, Muramatsu *et al.* generalized this approach, introducing conditions for the security of shared keys based on physical limitations called ‘‘bounded observability’’ [8]. In nature, there exist physical phenomena that are too fast, or too large, or too noisy, or too complex to be completely observed with current technology. One typical example is a light wave with broad bandwidth, which has a fast randomly fluctuating phase or amplitude. The approach of bounded observability relies on the limits of observation technology for such physical phenomena.

In this Letter, we propose and demonstrate a new method for secure key distribution, which uses correlated physical randomness in remote optical scramblers driven by a common random broadband light delivered over optical fiber. The security of the method is based on information theory and the physical property of bounded observability, which ensures that no one, neither the legitimate users nor the attackers, can completely observe the common random broadband light. To implement a scrambler, we propose the use of semiconductor lasers. Recently, it has been revealed that a common random input could give rise to synchronization between two independent limit-cycle or chaotic systems [9]. This phenomenon has been experimentally observed in semiconductor lasers driven by common light with a randomly fluctuating amplitude and phase [10,11]. In this Letter, we experimentally show that common light with constant amplitude and randomly varying phase (CARP) can also induce the synchronization of two lasers; i.e., phase information is sufficient for the synchronization, as numerically predicted in [12]. Our implementation of the scrambler is based on this finding.

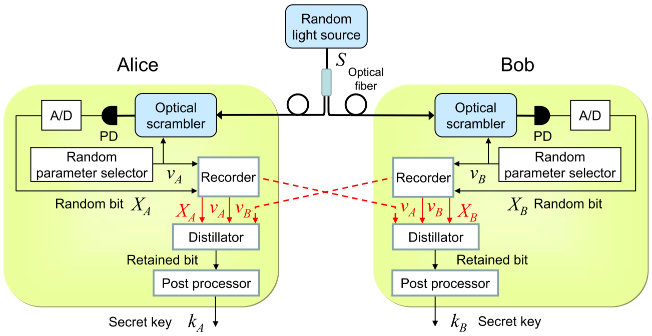

FIG. 1 (color online). General scheme for secure key distribution.

The general form of the scheme is illustrated in Fig. 1. Two legitimate users, Alice and Bob, have identical optical scramblers. Each optical scrambler has a set v of adjustable parameters, which takes one of M different sets of values. A random broadband light S is broadcast to the users. They receive identical copies of S and inject it into their optical scrambler. Each scrambler generates an optical output, which depends on both S and v and has the following property of correlated randomness: the output intensity waveforms are identical if the parameter settings of Alice and Bob are the same and mutually uncorrelated if the parameter settings are different; i.e., $C \equiv \langle (I_A - \mu_A) \times (I_B - \mu_B) \rangle / \sigma_A \sigma_B \simeq 0$, where $I_{A,B}$ are the output intensities; $\mu_{A,B}$ and $\sigma_{A,B}$ are their averages and standard deviations, respectively; and $\langle\rangle$ represents averaging over the realizations of S. Alice and Bob independently select their own parameter values v_A and v_B at random and simultaneously sample and quantize their scrambler outputs to extract bits X_A and X_B, respectively. Alice and Bob then store the pairs (v_A, X_A) and (v_B, X_B) in their data recorders. They repeat this procedure many times, injecting the continuously varying nonrepeating random light S to their scramblers with parameters randomly selected each time, to acquire sequences of the pairs $(v_{A,i}, X_{A,i})$ and $(v_{B,i}, X_{B,i})$, $i = 1, 2, \ldots, n$, respectively. Next, they distill common bits from the sequences by exchanging the parameter sequences, $\{v_{A,i}\}$ and $\{v_{B,i}\}$, $i = 1, 2, \ldots, n$, through an authenticated public channel (dashed line in Fig. 1) and retaining only the bits $X_{A,i}$ and $X_{B,i}$ for i such that $v_{A,i} = v_{B,i}$. These retained common bits are then used to generate a secret key $k_A = k_B$ via privacy amplification [13] in post processors [14]. In privacy amplification, information from multiple retained bits is combined in each key bit, in a way that reduces attacker Eve's chances of guessing the key from partial information about retained bits.

In order to assess the security of this scheme, we assume a passive attacker, Eve, that can use the broadcast light S—for example, inject it into one or more scrambler modules—and also obtain any information exchanged through a public channel between Alice and Bob. For any type of passive attack in which Eve does not alter S and the exchanged information, it has been proven that Alice and Bob can generate a key which is completely secret from Eve if and only if there is no way for Eve to *perfectly*, i.e., with no error, infer the bits generated by Alice and Bob [8]. Our goal is to make it practically impossible for Eve to obtain a perfect copy of Alice or Bob's bits by exploiting physical limitations.

The goal can be achieved by ensuring two physical limitations. (i) The common random light S has a fluctuation bandwidth which is too broad to completely observe its fast temporal variation with current technology; i.e., no one, neither a legitimate user Alice or Bob nor an attacker Eve, can continuously measure and record the entire S, so Eve cannot reproduce and reinject the entire common light to repeat the observations of Alice or Bob *after* the parameter settings have been exchanged. (ii) The number M_E of scramblers that Eve can operate simultaneously is limited ($M_E < M$), so Eve cannot simultaneously observe the outputs for all possible parameter values while S is being broadcast.

Because of (ii), it sometimes happens that Alice and Bob use the same set of parameter values, i.e., $v_A = v_B$, while Eve uses different sets. In such a case, Alice and Bob obtain common bits which Eve does not know: the bits cannot be inferred from the output intensities of Eve's scramblers, since they are uncorrelated with those of Alice and Bob; it is also impossible, because of (i), to infer the bits by completely repeating the observations of Alice or Bob. Note that Alice and Bob do not have to observe the entire temporal variation of S but only have to read the outputs of their scramblers with an injection of S. The latter is technologically much easier than the former, so limitation (i) does not prevent the key generation by Alice and Bob.

The above effects are manifest in the key generation rate, which is the ratio of the number of secret key bits to the number of raw sample bits:

$$R = \frac{1}{M}\left(1 - \frac{M_E}{M}\right)(1 - I_E), \tag{1}$$

where $1/M$ represents the probability of parameter matching $v_A = v_B$between Alice and Bob while $1 - M_E/M$ is the probability for Eve to use M_E sets of parameter values different from v_A and v_B under the condition $v_A = v_B$. I_E is the information per bit known by Eve about the common bits of Alice or Bob when Eve's set of parameter values does not match that of Alice and Bob. It is possible to generate keys up to rate R, with security guaranteed. I_E is ideally zero. However, secure keys can still be generated; i.e., $R > 0$, even if I_E is not zero, so long as $I_E < 1$. In order to generate keys which are secure with respect to a powerful attacker Eve capable of a large number M_E, it is necessary to use a large M, which results in a small rate R. Hence, it is necessary to achieve a large raw sampling rate in order to achieve practical key generation rates. In the remainder of the Letter, we show that this scheme for secret key generation is feasible through using fast semiconductor laser devices as optical scramblers driven by light with fast random-phase modulations and exploiting their synchronization phenomenon.

Figure 2(a) illustrates a method of constructing a scrambler module. Each scrambler consists of a cascade of laser units. Each unit U_i has a variable parameter θ_i comprising the parameter set $v = (\theta_1, \theta_2, \ldots, \theta_N)$ of the module. When injected with the same random input light, the outputs of the modules exhibit the correlated randomness property: the outputs of modules driven by the same injected light will be highly correlated with each other, $C \simeq 1$, when all the unit parameters are identical, but uncorrelated

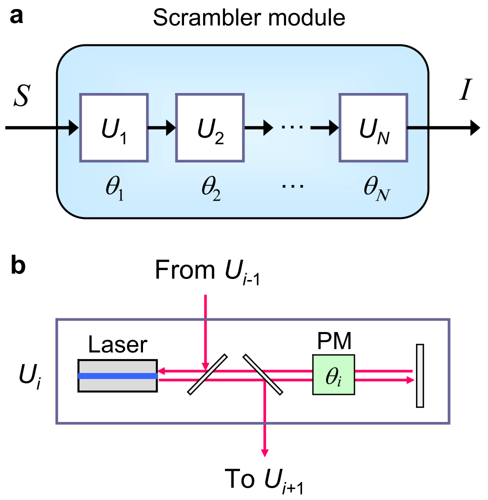

FIG. 2 (color online). Implementation of the optical scrambler. (a) Scrambler module consisting of a cascade of laser units. (b) Realization of a laser unit.

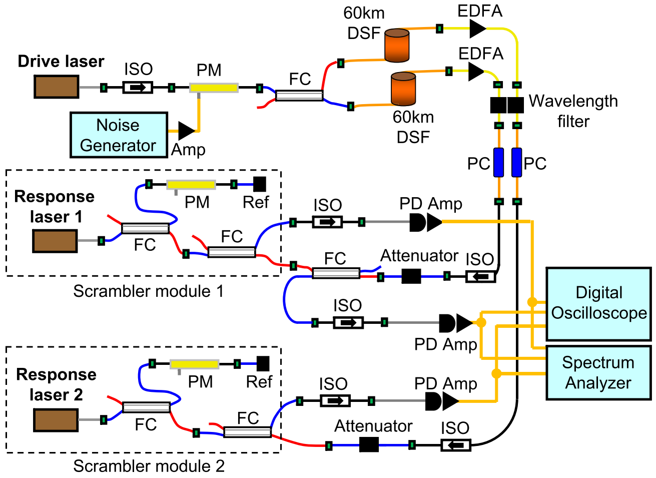

FIG. 3 (color online). Experimental setup for generation of correlated random bits.

with each other, $C \simeq 0$, when any of their unit parameters are not identical. Figure 2(b) shows how the laser units could be realized. Each laser unit has an optical self-feedback containing an optical phase modulator (PM). The amount of phase shift imposed by the phase modulator is used as the parameter θ_i. The output of each unit is input to the next unit in the cascade, so all feedback phase parameters affect the final output of the module. Hence, all the phase parameters must be matched between separate modules in order to achieve correlated oscillation.

The use of a common light with broadband random-phase modulation ensures condition (i), due to the difficulty of detecting the fast temporal variation of optical phase. In addition, condition (ii) can be ensured by using a large number N of laser units per module. The number M of parameter values increases exponentially with N: for example, if the phase parameter values are binary, then $M = 2^N$, so that the attack by completely mimicking Alice and Bob's observations using $M_E = M$ scrambler modules can be made practically impossible by making N large.

We have confirmed the feasibility of the scheme experimentally in the fundamental case of $N = 1$. Figure 3 shows our experimental setup. Laser light with CARP modulation was used as the common random light S, so there is no information available in the intensity of S, and the only information is in the phase of the light, which is harder to continuously detect and record. A portion of light from a distributed-feedback (DFB) semiconductor laser, which we call the drive laser, is injected into a fiber isolator (ISO) and a phase modulator. The phase of the laser light is randomly modulated in the phase modulator, driven by a noise generator with a bandwidth of 1.5 GHz, to generate the CARP light used as S. This CARP light is split into two branches by a fiber coupler (FC) and delivered through a single-mode dispersion-shifted fiber (DSF) with amplification by an erbium-doped fiber amplifier (EDFA), propagating over 60 km from the branch point, achieving a distance of 120 km between two scrambler modules, each of which is a DFB laser unit. A polarization controller (PC) is used to adjust the polarization direction of the CARP light. The CARP light is injected into the laser unit in each scrambler module through an optical isolator to ensure unidirectional coupling from the drive to the scrambler modules. Each DFB laser (response laser 1 or 2) in the scrambler modules has a variable fiber reflector (Ref) to form an optical self-feedback loop. The loop includes a phase modulator, and the phase of the feedback light comprises the parameter to control the degree of synchronization between the two scrambler modules. The optical wavelengths of all the DFB lasers are matched to each other by injection locking. The outputs of the two scrambler modules are detected by photodiodes (PD), amplified by electronic amplifiers (Amp), and observed using a digital oscilloscope.

Each feedback phase parameter is switched between two values (0 and π) by a random return-to-zero (RZ) binary voltage signal. So, the number M of possible values of the parameter set is $M = 2$. Figure 4(a) shows the temporal waveforms of the random RZ signals for the phase modulation and the short-term cross-correlation value for the optical output intensity waveforms between the two scrambler modules. When the parameters are matched, the short-term cross-correlation value becomes close to 1, whereas it changes to near 0 when the parameters are mismatched. Figure 4(b) shows examples of the laser output waveforms and their correlation plots. The average correlation is 0.934 and 0.0182 for parameter-matched and parameter-mismatched data, respectively. This result is consistent with the required correlated randomness property and confirms that we succeeded in realizing robust sources of correlated randomness over large distances in optical fibers.

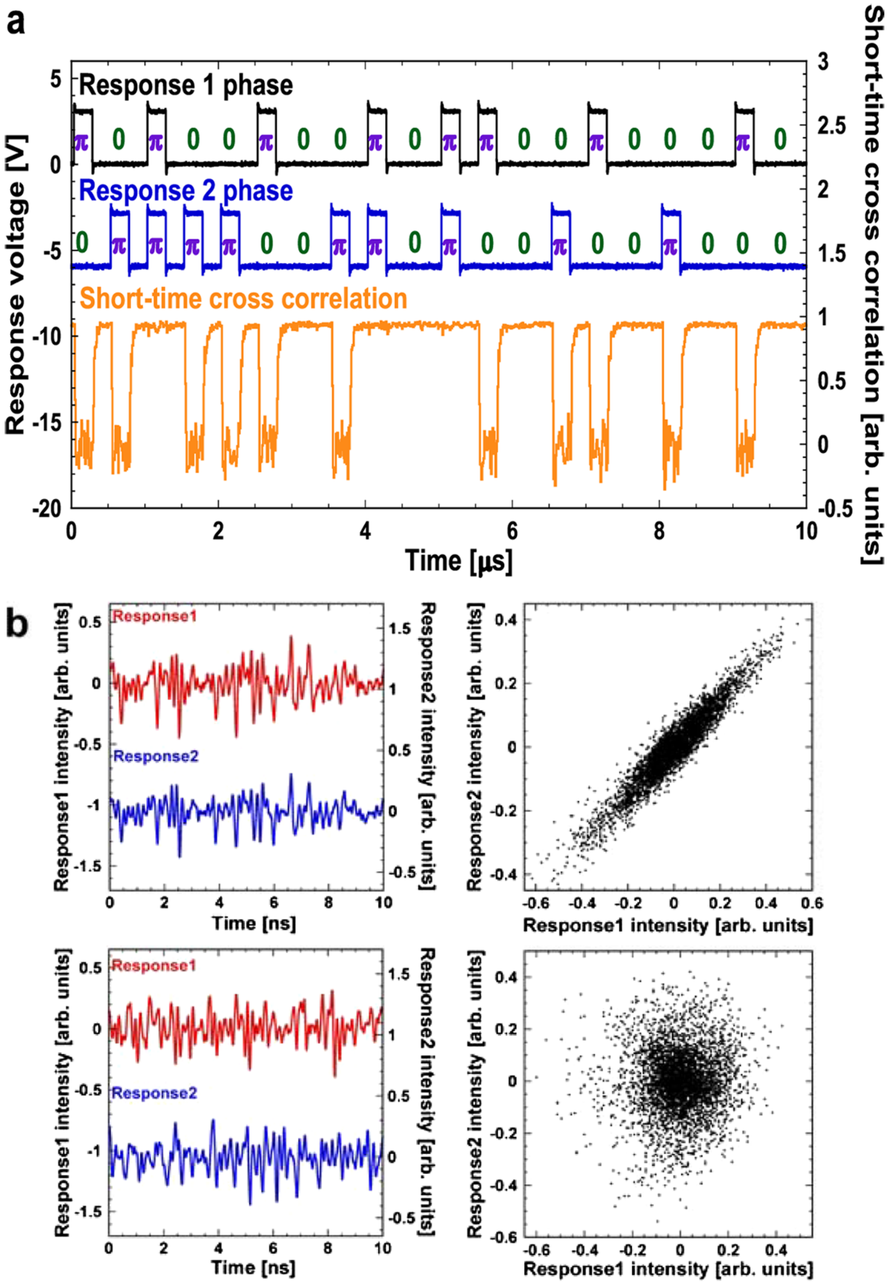

FIG. 4 (color online). (a) Temporal waveforms of random RZ signals for the phase modulation and the short-term cross correlation for outputs of two scrambler modules. (b) Temporal output waveforms of two scrambler modules (response lasers 1 and 2) and their correlation plots for parameter-matched (upper panels) and -mismatched (lower panels) cases.

A binary bit is extracted from the temporal waveform by sampling at a predetermined timing and comparing the sampled value with thresholds. A robust sampling technique (using two thresholds) is used to reduce the bit error rate (BER), the probability of bits being different even when the parameters are matched. So, only a proportion r of the bits in parameter-matched cases is retained after robust sampling. We calculated the statistical results for typical sequences of bits obtained in our experiment. For our threshold values, $r = 0.37$ and the achieved BER is a very low value of 0.000 164. The frequency of occurrence of bit “1” in the retained-bit sequence is 0.493, close to the ideal value of 0.5. Now, consider the key generation rate R. Allowing for the robust sampling and finite BER value e, $R = rM^{-1}[(1 - M_E/M)(1 - I_E) - h(e)]$. Here, $h(x)$ is the binary entropy function defined by $h(x) = -x\log_2 x - (1 - x)\log_2(1 - x)$. A rough estimate for Eve’s information I_E in this experiment was less than 0.01 bit. Assuming that Eve has no more than one laser module, i.e., $M_E < M = 2$, we have $R \geq 0.091$ for $M = 2$, $M_E = 1$, $I_E \leq 0.01$, $e = 0.000\,164$, and $r = 0.37$. An estimate of the real-time key generation rate is obtained by multiplying

R by the raw sampling rate 2 Mbit/s, giving 182 kbit/s. Most importantly, no significant degradation of the statistical properties due to the propagation and amplification operations was observed in our experiment over 120 km of optical fiber. This indicates that this scheme is feasible for stable operation over distances much longer than 120 km in large scale optical fiber networks, which is a practical important advantage over QKD.

We now discuss the feasibility of the scheme for larger N. Consider the scrambler module shown in Fig. 2(a). The major difference between the first unit and the others is the type of injected light: CARP light is injected to U_1, while light with both amplitude and phase fluctuation is injected to U_i, $i \geq 2$. It has been shown in [11] that the laser unit in Fig. 2(b) has the required correlation property also when driven by a common light of randomly fluctuating amplitude and phase. Thus, it is reasonably expected that, when all θ_i's are matched between two scrambler modules, their final outputs are highly correlated. In contrast, if θ_i's are matched for $i = 1, \ldots, n - 1$ but mismatched for $i = n$ between the two modules, the outputs of the nth units are uncorrelated. The units for $i > n$ have uncorrelated injected lights and so generate uncorrelated outputs, independent of whether their phase parameters are matched or mismatched. Consequently, the final outputs of the two scrambler modules will be uncorrelated. To confirm this correlation property, we carried out numerical simulations using the Lang-Kobayashi equation [17] with reasonable parameter values. For $N = 8$, we confirmed that the correlation of the final outputs is larger than 0.993 in the parameter-matched cases while it is smaller than 0.184 in the parameter-mismatched cases.

It has been shown that semiconductor lasers can be used for fast random bit generation [18–21]. In the near future, it is reasonably expected that the raw-bit generation rate in our scheme could be increased at least beyond 1 Gbit/s, by using lasers integrated with short feedback loops which require less time for synchronization [20–22]. For example, assuming $I_E = 0$, $M = 2^{28}$, and a powerful attacker with $M_E = 200$ million modules, then generating secure keys at a rate of 1 bit/s requires a raw sampling rate of at least 1.05 Gbit/s from Eq. (1). Moreover, the feasibility of modules with large numbers of laser units, as considered in the numerical analysis, is supported by the recent demonstration of lasers with on-chip optical feedback [20–22].

The authors would like to thank the members of the NTT Communication Science Laboratories for their continuous encouragement and support. A. U. gratefully acknowledges support from a Grant-in-Aid for Young Scientists from the Ministry of Education, Culture, Sports, Science, and Technology in Japan, and the NTT Corporation.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984* (IEEE, Bangalore, India, 1984), p. 175.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] J. Scheuer and A. Yariv, Phys. Rev. Lett. **97**, 140502 (2006); A. Zadok, J. Scheuer, J. Sendowski, and A. Yariv, Opt. Express **16**, 16 680 (2008).

[4] R. Vicente, C. R. Mirasso, and I. Fischer, Opt. Lett. **32**, 403 (2007).

[5] I. Kanter, M. Butkovski, Y. Peleg, M. Zigzag, Y. Aviad, I. Reidler, M. Rosenbluh, and W. Kinzel, Opt. Express **18**, 18 292 (2010); I. Kanter, E. Kopelowitz, and W. Kinzel, Phys. Rev. Lett. **101**, 084102 (2008).

[6] G. S. Kanter and P. Kumar, Nature Photon. **1**, 15 (2007).

[7] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).

[8] J. Muramatsu, K. Yoshimura, and P. Davis, Lect. Notes Comput. Sci. **5973**, 128 (2010).

[9] J. N. Teramae and D. Tanaka, Phys. Rev. Lett. **93**, 204103 (2004); R. Toral, C. R. Mirasso, E. Hernandez-Garcia, and O. Piro, Chaos **11**, 665 (2001); C. Zhou and J. Kurths, Phys. Rev. Lett. **88**, 230602 (2002); K. Yoshimura, I. Valiusaityte, and P. Davis, Phys. Rev. E **75**, 026208 (2007).

[10] T. Yamamoto, I. Oowada, H. Yip, A. Uchida, S. Yoshimori, K. Yoshimura, J. Muramatsu, Shin-itiro Goto, and P. Davis, Opt. Express **15**, 3974 (2007).

[11] I. Oowada, H. Ariizumi, M. Li, S. Yoshimori, A. Uchida, K. Yoshimura, and P. Davis, Opt. Express **17**, 10 025 (2009).

[12] S. Goto, P. Davis, K. Yoshimura, and A. Uchida, Opt. Quantum Electron. **41**, 137 (2009).

[13] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[14] In practice, there may be some errors between retained bits of Alice and Bob. To eliminate the errors, Alice and Bob need to perform a form of error correction, known as "information reconciliation" [15,16], through an authenticated public channel, before the privacy amplification.

[15] G. Brassard and L. Salvail, Lect. Notes Comput. Sci. **765**, 410 (1994).

[16] J. Muramatsu, K. Yoshimura, K. Arai, and P. Davis, NTT Tech. Rev. **6**, No. 2, 1 (2008).

[17] R. Lang and K. Kobayashi, IEEE J. Quantum Electron. **16**, 347 (1980).

[18] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nature Photon. **2**, 728 (2008).

[19] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nature Photon. **4**, 58 (2010).

[20] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Opt. Express **18**, 18 763 (2010).

[21] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, Phys. Rev. A **83**, 031803 (2011).

[22] A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, Phys. Rev. Lett. **100**, 194101 (2008).