IEICE Proceeding Series

Secure key distribution using correlated randomness in optical devices

Kazuyuki Yoshimura, Jun Muramatsu, Peter Davis, Atsushi Uchida, Takahisa Harayama

Vol. 1 pp. 336-339
Publication Date: 2014/03/17
Online ISSN: 2188-5079

2012 International Symposium on Nonlinear Theory and its Applications
NOLTA2012, Palma, Majorca, Spain, October 22-26, 2012

Secure key distribution using correlated randomness in optical devices

Kazuyuki Yoshimura[1], Jun Muramatsu[1], Peter Davis[1,2], Atsushi Uchida[3], and Takahisa Harayama[1,4]

[1]NTT Communication Science Laboratories, NTT Corporation
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto 619–0237 Japan
[2]Telecognix Corporation, 58–13 Shimooji-cho, Yoshida, Sakyo-ku, Kyoto 606–8314 Japan
[3]Department of Information and Computer Sciences, Saitama University
255 Shimo-Okubo, Sakura-ku, Saitama city, Saitama 338–8570 Japan
[4]Toyo University, 2100 Kujirai, Kawagoe-shi, Saitama 350–8585 Japan
Email: yoshimura.kazuyuki@lab.ntt.co.jp

Abstract—We propose a secure key distribution scheme based on correlated physical randomness in remote optical scramblers driven by common broadband random light. Moreover, we propose a particular realization of the scheme using synchronization of semiconductor lasers injected with common broadband random light.

1. Introduction

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 when they do not share any secret information in advance.

It is known that there are two different notions of security, i.e., computational and information theoretic security. The former assumes a limitation on computational ability of the attacker while the latter does not. So, the latter implies the security against the attacker with infinite computational power. In order to achieve the information theoretic security, it is necessary to introduce another assumption such as physical one, instead of the computational one. Of course, this assumption has to be reliable enough and hold in long-term future, being not influenced by advance in technology.

The issue of secure key distribution based on physical principles concerns the information theoretic security, and it has been of increasing interest. Quantum key distribution (QKD) [1] 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 [2, 3, 4], and they have attracted interest from the point of view of practical feasibility (e.g. [5]). However, the security of these schemes has not yet been analysed 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 [6]. Recently, Muramatsu et al. generalized this approach, introducing conditions for security of shared keys based on physical limitations called ”bounded observability” [7]. 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 fast randomly fluctuating phase or amplitude. The approach of bounded observability relies on the limit of observation technology for such physical phenomena.

We propose 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 (cf. [8]). The security of the method is based on information theory and the physical property of bounded observability, which ensures that no one, not 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. This phenomenon has been experimentally and numerically observed in semiconductor lasers driven by common random light [9, 10, 11]. We propose an implementation of the scrambler based on this phenomenon.

2. General scheme

The general form of the scheme is illustrated in Fig. 1. Two legitimate users, Alice and Bob, have identical optical scramblers. The scrambler itself has nothing in secrecy and it is also available to the attacker, Eve. Each optical scrambler has a set v of adjustable parameters, which takes one of M different sets of values. In general, v is a vector consisting of several parameters. A random broadband light S is broadcast to the users. Alice and Bob independently select their own parameter values v_A and v_B at random, receive identical copies of S, and inject it into their optical

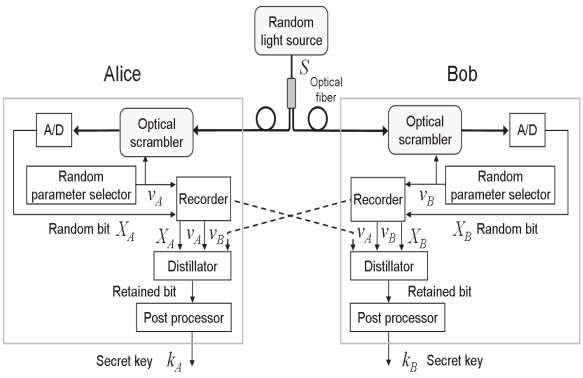

Figure 1: General scheme for secure key distribution.

scramblers.

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. Let C be defined by $C \equiv \langle (I_A - \mu_A)(I_B - \mu_B)\rangle / \sigma_A \sigma_B \simeq 0$, where $I_{A,B}$ are the output intensities at an instant, $\mu_{A,B}$ and $\sigma_{A,B}$ are their averages and standard deviations respectively, and $\langle\ \rangle$ represents averaging over the realizations of S. In terms of C, the above property means that $C = 1$ for $v_A = v_B$ while $C = 0$ for $v_A \neq v_B$.

Alice and Bob simultaneously sample at a prescribed timing and quantize their scrambler outputs via A/D converters 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 the above procedure many times, injecting the continuously varying non-repeating 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 $v_{A,i} = v_{B,i}$. Because of the output correlation property of the scramblers, these retained bits satisfy $X_{A,i} = X_{B,i}$. These retained common bits are then used to generate a secret key $k_A = k_B$ via privacy amplification [12] in post processors [13]. In general, Eve could have partial information about the retained bits. The privacy amplification is a technique that reduces attacker Eve's chances of guessing the key from her partial information to almost zero.

3. Security

In order to assess the security of this scheme, we assume a passive attacker, Eve, such that

(a) Eve can use the broadcast light S identical with that of Alice and Bob, for example inject it into one or more scrambler modules;

(b) Eve can 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 proved 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 [7]. 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 the following two physical limitations:

(i) The common random light S has fluctuation bandwidth which is too broad to completely observe its fast temporal variation with current technology i.e., no one, not a legitimate user Alice or Bob, nor an attacker Eve, can continuously measure and record the entire S;

(ii) The number M_E of scramblers that Eve can operate simultaneously is limited, and M is set large enough so that $M_E < M$ will hold.

Due to (i), Eve cannot reproduce and reinject the entire common light S to repeat the observations of Alice or Bob *after* the parameter settings have been exchanged. So, it is impossible for Eve 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 measure the outputs of their scramblers with injection of S in a prescribed manner. The latter is technologically much easier than the former, so limitation (i) does not prevent the key generation by Alice and Bob.

There could be a possibility of using a long delay line to keep S until Alice and Bob exchange their parameter settings. We note that this is practically impossible because of the following reason. The duration time of Alice and Bob's random bit generation can be made arbitrarily long, for example, 100 sec. or more. To keep the entire non-repeating random light S, a very long delay line is necessary, for example, the length is 3×10^{10} m for the duration time of 100 sec.. Therefore, the use of a delay line is impractical.

Due to (ii), Eve also cannot simultaneously observe the outputs for all possible parameter values while S is being broadcast. It sometimes happens with nonzero probability that Alice and Bob use the same set of parameter values, $v_A = v_B$, while Eve uses different sets. In such a case, Alice and Bob obtain a common bit which Eve does not know: the bit cannot be inferred from the output intensities of Eve's scramblers since they are uncorrelated with those of Alice and Bob's scramblers.

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:

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

where $1/M$ represents the probability of parameter matching between Alice and Bob, $v_A = v_B$, 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. i.e., $v_{E,i} \neq v_A = v_B$ for any $i = 1, \ldots, M_E$, where $v_{E,i}$ is Eve's set of parameter values. 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 paper we show that this scheme for secret key generation is feasible using fast semiconductor laser devices as optical scramblers driven by light with fast random phase modulations, and exploiting their synchronization phenomenon.

4. Implementation

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. 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 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.

Based on the results in Refs. [9, 10, 11], it is reasonably expected that when all θ_is are matched between two scrambler modules driven by the same injected light, their final outputs are highly correlated, i.e., $C \simeq 1$. In contrast, if θ_is 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, i.e., $C \simeq 0$. That is, the outputs of the two modules will be uncorrelated with each other, $C \simeq 0$, when *any* of their unit parameters are not identical. To confirm this correlation property, we carried out numerical simulations using the Lang-Kobayashi equation [16] 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.

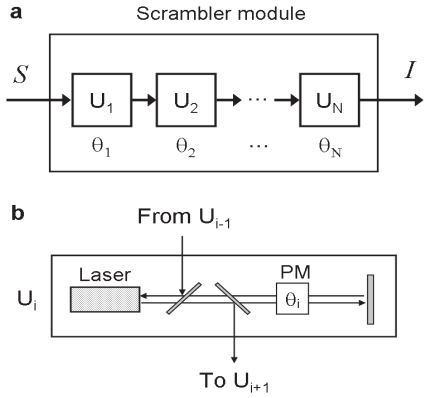

Figure 2: Implementation of optical scrambler. (a) Scrambler module consisting of a cascade of laser units. (b) Realization of a laser unit.

The use of a common light with broadband random phase and/or amplitude modulation ensures condition (i), due to the difficulty of detecting the fast temporal variation of optical phase and/or amplitude. 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's and Bob's observations using $M_E = M$ scrambler modules can be made practically impossible by making N large.

It has been shown that semiconductor lasers can be used for fast random bit generation [17, 18, 19]. 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 [18, 19, 20]. For example, assuming $I_E = 0$, $M = 2^{28}$, and a powerful attacker with $M_E = 200$ million modules, then generating secure keys at rate of 1 bit/s requires a raw sampling rate of at least 1.05 Gbit/s from Eq. (1). The raw-bit generation rate of this order could be achieved by using fast semiconductor lasers. 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 [18, 19, 20].

Acknowledgment

The author would like to thank the members of the NTT Communication Science Laboratories for their continuous encouragement and support.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proc. of the IEEE Int. Conf. on Comp. Syst. and Sig. Process.*, pp.175–179 (1984).

[2] J. Scheuer and A. Yariv, "Giant fiber lasers: a new paradigm for secure key distribution," *Phys. Rev. Lett.*, vol.97, 140502, 2006.

[3] R. Vicente, C. R. Mirasso, and I. Fischer, "Simultaneous bidirectional message transmission in a chaos-based communication scheme," *Opt. Lett.*, vol.32, pp.403–405, 2007.

[4] I. Kanter, M. Butkovski, Y. Peleg, M. Zigzag, Y. Aviad, I. Reidler, M. Rosenbluh, and W. Kinzel, "Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography," *Optics Express*, vol.18, pp.18292–18302, 2010.

[5] G. S. Kanter and P. Kumar, "Fibre lasers: keeping cryptographic keys safe," *Nature Photonics*, vol.1, pp.15–16, 2007.

[6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol.39, pp.733–742, 1993.

[7] J. Muramatsu, K. Yoshimura, and P. Davis, "Information theoretic security based on bounded observability," *Lecture Notes in Computer Science*, vol.5973, pp.128–139, 2010.

[8] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, "Secure key distribution using correlated randomness in lasers driven by common random light," *Phys. Rev. Lett.*, vol.108, 070602, 2012.

[9] T. Yamamoto, I. Oowada, H. Yip, A. Uchida, S. Yoshimori, K. Yoshimura, J. Muramatsu, Shin-itiro Goto, and P. Davis, Optics Express **15**, 3979 (2007).

[10] I. Oowada, H. Ariizumi, M. Li, S. Yoshimori, A, Uchida, K. Yoshimura, and P. Davis, "Synchronization by injection of common chaotic signal in semiconductor lasers with optical feedback," *Optics Express*, vol.17, pp.10025–10034, 2009.

[11] S. Goto, P. Davis, K. Yoshimura, and A. Uchida, "Synchronization of chaotic semiconductor lasers by optical injection with random phase modulation," *Optical and Quantum Electronics*, vol.41, pp.137–149, 2009.

[12] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol.41, pp.1915–1923, 1995.

[13] 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" [14, 15] through an authenticated public channel, before the privacy amplification.

[14] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," *Lecture Notes in Computer Science*, vol.765, pp.410-423, 1994.

[15] J. Muramatsu, K. Yoshimura,K. Arai, and P. Davis, "Some results on secret key agreement using correlated sources," *NTT Technical Review*, vol.6, no.2, 2008.

[16] R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection properties," *IEEE J. Quantum Electron.*, vo.16, pp.347–355, 1980.

[17] 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, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics*, vol.2, pp.728–732, 2008.

[18] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, "Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit," *Optics Express*, vol.18, pp.18763–18768, 2010.

[19] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast nondeterministic random-bit generation using on-chip chaos lasers," *Phys Rev. A*, vol.83, 031803, 2011.

[20] A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, "Photonic Integrated Device for Chaos Applications in Communications," *Phys Rev. Lett.*, vol.100, 194101, 2008.