IEICE Proceeding Series

# Experiment on secure key distribution using correlated random phenomenon in semiconductor lasers

Hayato Koizumi, Shinichiro Morikatsu, Hiroki Aida, Masaya Arahata, Takahiro Nozawa, Atsushi Uchida, Kazuyuki Yoshimura, Jun Muramatsu, Peter Davis

Vol. 1 pp. 340-343
Publication Date: 2014/03/17
Online ISSN: 2188-5079

# Experiment on secure key distribution using correlated random phenomenon in semiconductor lasers

Hayato Koizumi†, Shinichiro Morikatsu†, Hiroki Aida†, Masaya Arahata†, Takahiro Nozawa†, Atsushi Uchida†, Kazuyuki Yoshimura‡, Jun Muramatsu‡, and Peter Davis‡*

†Department of Information and Computer Sciences, Saitama University
255 Simo-okubo, Sakura-ku, Saitama City, Saitama, 338-8570 Japan
‡NTT Communication Science Laboratories
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0237 Japan
* Telecognix Corporation
58-13 Shimooji-cho, Yoshida, Sakyo-ku, Kyoto, 606-8314 Japan
Email: {s11mm312, auchida}@mail.saitama-u.ac.jp

**Abstract–** Optical devices can be used to generate correlated random bit sequences and that secure key distribution is possible using the correlated random bit sequences. We report the experimental demonstration of a scheme for generating correlated random bit sequences, using semiconductor lasers synchronized by common random optical signals. The correlated random bit sequences generated in this scheme can be used by two legitimate users to create information-theoretically secure keys.

## 1. Introduction

The information security technologies are very important in recent communication and computer systems. There are two main security paradigms, namely computational security and information-theoretic security. Computational security is based on the assumed hardness of computational problems such as the integer-factoring or discrete logarithm problems. Information-theoretic security [1,2] on the other hand is based on probability theory and on the fact that an adversary's information is limited. Such a limitation can come from classical uncertainty in communication channels or from the laws of quantum mechanics. Information theoretic security avoids the reliance on unproven assumptions about the complexity of computations, and is future-proof in the sense that the security of keys generated today will not be compromised by improvements in computing technology, including quantum computing, in the future.

One approach to information theoretic security assumes that there is public source of randomness and that all parties have limited storage so that they cannot record all the randomness from the source [2]. Recently, a new scheme for information-theoretically secure key distribution based on bounded observability, which means the practical difficulty of completely observing physical phenomena, has been proposed [3]. It has been shown that this method can be implemented in optical systems [4] by using common-signal-induced synchronization [5, 6].

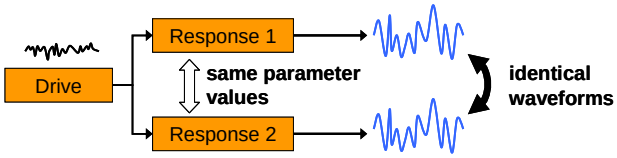


Fig. 1 Concept of common-signal-induced synchronization

The concept of common-signal-induced synchronization is shown in Fig. 1. A drive signal from a dynamical laser system (called Drive laser) is injected to two laser systems (called Response 1 and 2 lasers) that are independent and have different initial conditions. The outputs from the two different Response lasers injected from the common drive signal are identically synchronized, even though the outputs of the Drive and Response lasers are different. The outputs of the two Response lasers are identical because the Responses are driven by the common drive signal. The common-signal-induced synchronization has been experimentally demonstrated in coupled semiconductor lasers with a chaotic drive signal [5, 6]. Moreover, the common-signal-induced synchronization using constant-amplitude and random-phase (CARP) light as a driving signal has been demonstrated experimentally [7]. Also, some schemes based on synchronization of chaotic lasers have been proposed for secure key distribution [8-11].

In this study we experimentally demonstrate secure key distribution based on the information theoretical security using common-signal-induced synchronization in semiconductor lasers with a CARP drive signal. We estimate the bit error rate (BER) and bit generation rate (BGR) of secure keys generated by two legitimate users.

## 2. Experimental Setup

Our experimental setup is shown in Fig. 2. The experimental system is the same as in [4]. In this paper we show more detail configuration of the experimental setup. We use three semiconductor lasers as Drive, Response 1, and Response 2 lasers, respectively. The output light from the Drive laser (LD) is injected to an optical isolator (ISO) to transmit the light unidirectionally. We use a noise signal generated by an electronic noise generator and a phase

modulator (PM), where the phase of the drive signal is modulated randomly, and CARP light is generated. The CARP light indicates that the light has constant amplitude and randomly modulated optical phase. The CARP light is divided into two beams at a fiber coupler (FC). One of the beams is used for signal detection. The other beam is divided into two beams at another FC. Each beam is attenuated by an optical attenuator and injected into Response 1 and 2, respectively. The Response 1 and 2 lasers are subject to self-optical feedback from fiber reflectors (i.e., closed-loop configuration). The relative phase of the optical feedback lights from each Response laser is modulated by an arbitrary waveform generator, according to two randomly-selected parameter values, π or 0. Note that each Response laser has an independent phase modulation generator. If π is selected, the phase is modulated by a half period of the wavelength. If the parameter 0 is selected, the phase is not modulated. The outputs of the two Response lasers are transformed into electric signals by photodiodes (PD) and amplified by electric amplifiers (Amp), then detected by a digital oscilloscope.

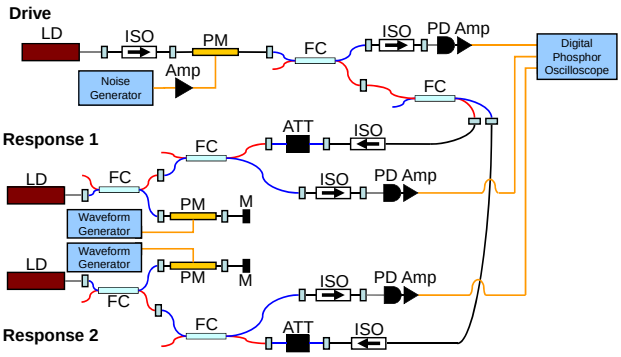


Fig. 2 Experimental setup of common-signal-induced synchronization. Amp, electric amplifier; ATT, attenuator; FC, fiber coupler; ISO, optical isolator; LD, laser diode; M, mirror; PD, photodiode; PM, phase modulator.

## 3. Common-signal-induced synchronization with CARP light

We show that common-signal-induced synchronization can be achieved experimentally when the phases of the optical feedback lights of the two Response lasers are set to be identical. The temporal waveforms and corresponding correlation plots of the two Response lasers are shown in Fig. 3 when the optical phases of the feedback lights are matched and mismatched, respectively. For Fig. 3(a) and 3(b), when the phases are matched, the temporal waveforms of the two Response lasers are strongly correlated and synchronized. On the other hand, for Fig. 3(c) and 3(d), when the phases are mismatched, the temporal waveforms of the two Response lasers are not correlated at all.

We introduce a measure of analog cross-correlation to evaluate synchronization accuracy quantitatively. The analog cross-correlation value is calculated as follows.

$$C_A = \frac{\left\langle \left(I_1 - \bar{I}_1\right)\left(I_2 - \bar{I}_2\right)\right\rangle}{\sigma_1 \cdot \sigma_2} \qquad (1)$$

where, $I_1, I_2$ are the amplitudes of the temporal waveforms of the two Response laser outputs, $\bar{I}_1, \bar{I}_2$ are the means of $I_1, I_2$, $\sigma_1, \sigma_2$ are the standard deviations of $I_1, I_2$, $\langle\ \rangle$ indicate time averaging. $C_A = 1.0$ indicates identical synchronization, whereas $C_A = 0.0$ indicates no synchronization.

The analog cross-correlation value of Fig. 3(b) is 0.935 and high-quality synchronization is achieved. On the other hand, the correlation value of Fig. 3(d) is 0.011 and no synchronization is observed. Therefore, the degree of synchronization can be controlled by the optical phases of the feedback lights of the two Response lasers.

For reference, we measure the cross-correlation value between the Drive and Response 1 lasers. The amplitude of drive signal is much smaller than that of Response 1 and nearly constant because the CARP light is used as a drive signal. The correlation value between the Drive and Response 1 is ~0.19 and almost no correlation is found between the Drive and Response 1 lasers [8]. The cross correlation value is not sensitive to the parameter change in the optical feedback phases of the Response lasers, unlike the case in Fig. 3.

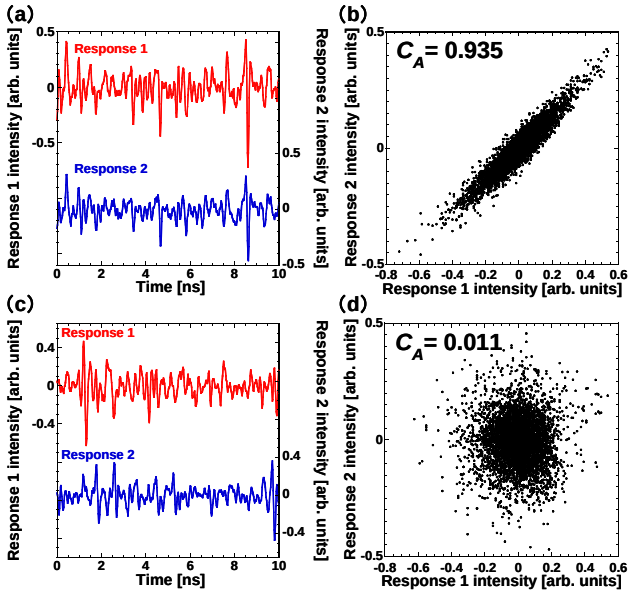


Fig. 3 (a),(c) Temporal waveforms of the Response 1 and Response 2 lasers. (b),(d) Corresponding correlation plots. The optical phases of the feedback lights of the two Response lasers are (a),(b) matched and (c),(d) mismatched.

We observe short-term cross-correlation between the two Response lasers when the feedback phases are modulated independently by random parameter choices of the optical phases (0 or π). In this experiment, we set the period of 0.5 μs for one parameter choice (i.e., the modulating speed is 2.0 MHz). The Return to Zero (RZ) format is used for the parameter modulation.

We show the time evolution of the randomly-selected parameter values and the short-term analog cross-correlation between the Response 1 and 2 lasers in Fig. 4. The upper and middle rows in Fig. 4 correspond to the

parameter modulation of the feedback phases and the lower row shows the short-term cross-correlation. When the same parameter values are selected, the short-term correlation becomes high. On the other hand, low correlation values are obtained when the different parameter values are selected. This synchronization switching phenomenon can be utilized for secure key distribution.

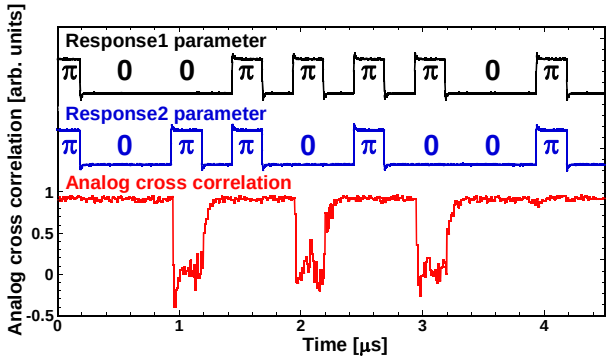


Fig. 4 Temporal waveforms of the two randomly-selected parameter values of the optical feedback phases for the Response 1 and 2 lasers and the corresponding short-term cross-correlation between the Response 1 and 2 lasers as a function of time.

## 4. Secure Key Generation Based on Common-Signal-Induced Synchronization

We propose a scheme for secure key distribution based on common-signal-induced synchronization. A schematic diagram of the proposed secure key distribution scheme is shown in Fig. 5. Let us assume that a drive signal source (Drive) is provided to legitimate users, Alice and Bob. The following assumption is used in this protocol. The two users receive a common drive signal and one of the parameter values (0 or π) is selected randomly by each user. The users obtain analog signals from their Response systems, and the output signals depend on both the drive signal and the selected parameter values. If the common drive signal is used and the selected parameter values are matched, the two users can share synchronized analog signals.

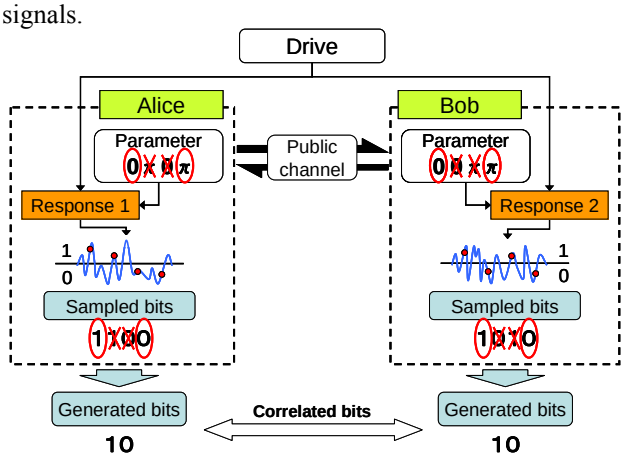


Fig. 5 Schematic diagram of the secure key distribution scheme based on correlated randomness phenomena.

Next the two users extract a bit by sampling their analog signals. A bit can be shared by the two users with the common drive signal when they selected the same parameter value, because the output from the Response system is determined by both the parameter and the drive signal. If an eavesdropper cannot preserve the drive signal due to the difficulty of detecting fast optical phase fluctuations, the eavesdropper cannot estimate the output obtained from the opposite parameter value at the same time. This is an important property to avoid sampling attack for this security system [4, 5].

The secure key generation protocol is shown as follows (see also Fig. 5):

1. Two legitimate users select the parameter values of their Response systems independently.
2. The common signal from the Drive system is injected into the two Response systems for the two legitimate users.
3. Bits are generated by sampling the outputs from the Response systems. A pair of the bit and the corresponding parameter value is stored.
4. The task 1~3 is executed repeatedly.
5. When the task 4 is finished and a sequence of bits is generated, the legitimate users exchange the information on the parameter values each other.
6. The bits are preserved as correlated random bits when the corresponding parameter values are matched between the two Response systems, otherwise the bits are discard. After this process is executed repeatedly, a secure key is obtained from the correlated random bits by using the secure key sharing protocol [9].

In the above protocol, we use a robust sampling method to improve the bit error rate (BER). The concept of the robust sampling method is shown in Fig. 6. We set two threshold values $I_{th,u}$ and $I_{th,l}$ as follows.

$$I_{th,u} = m + C_{+}\sigma \qquad (2)$$

$$I_{th,l} = m - C_{-}\sigma \qquad (3)$$

where, $I_{th,u}$, $I_{th,l}$ are the upper and lower threshold values for random bit generation, $m$ is the mean of the temporal waveform, $\sigma$ is the standard deviation of the temporal waveform. $C_{+}, C_{-}$ are constant values to determine the threshold values. Here, we set $C_{+} = 0.70$ and $C_{-} = 0.69$, respectively. A bit '1' is obtained when a sampled value excesses the upper threshold $I_{th,u}$. A bit '0' is obtained when a sampled value is lower than the lower threshold $I_{th,l}$. When a sampled value is between $I_{th,u}$ and $I_{th,l}$, a bit is discarded. Two thresholds are shown on the temporal waveforms in Fig. 6(a) and on the correlation plot in Fig. 6(b). The waveforms outside the two thresholds are similar to each other between the two Response signals in Fig. 6(a). For Fig. 6(b), there are four regions denoted as 00, 01, 10 and 11. The first number corresponds to the bit generated by Alice, and the second number corresponds to

the bit generated by Bob. The same bits are generated by the robust sampling in the regions of 00 and 11. On the other hand, the bits are different in the regions of the 01 and 10. To increase the threshold values, the points in 01 and 10 regions are negligible and the bit error rate can be improved.

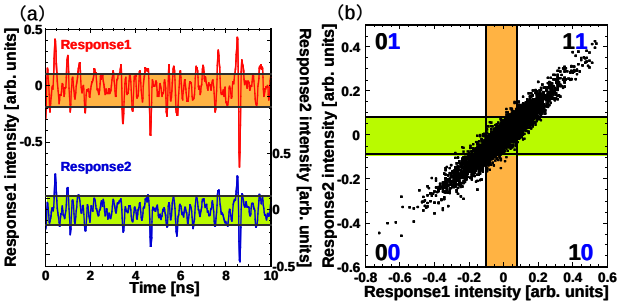


Fig. 6 Examples of the robust sampling method with two threshold values. (a) Temporal waveforms and (b) corresponding correlation plot. The two bits indicate Alice's and Bob's bits. 11 and 00 indicate that the same bit can be shared.

### 2.4. Estimation of the Generated Bit

We investigated statistical evaluation of generated bit sequences. We used measures of analog and digital cross-correlations, the number of generated bits, bit generation rate (BGR), bit error rate (BER), and 0 frequencies of Alice's and Bob's bit sequences. We evaluated the generated bit streams when the selected parameter values are matched between the legitimate users. The results are shown in Table 1. The analog cross-correlation is 0.9249 and the digital cross correlation is 0.9996. This result indicates that the robust sampling generates higher correlated bit streams than the analog waveforms. BGR is 0.3312. In this experiment, the parameter modulation frequency is 2.0 MHz. The probability of parameter matching is nearly 0.5 because the two parameter values are randomly modulated. Therefore, the bit generation speed is estimated as 2.0 Mb/s × 0.331 × 0.5 = 331 kb/s. Also, BER is $1.78\times10^{-4}$. This value indicates that all the errors can be corrected using the practical secure key sharing protocol [12]. In addition, the occurrence of the frequency of bit 0 generated by Alice and Bob are 0.5009 and 0.5011, respectively. These values are close to the ideal value of 0.5. From these results, we succeed in the experiment on secure key distribution with common-signal-induced synchronization.

Table 1 Statistical evaluation of the results of secure key distribution.

| Evaluation item | Value |
|---|---|
| Analog cross correlation | 0.9249 |
| Digital cross correlation | 0.9996 |
| Number of generated bits | 11264 |
| Bit generation rate (BGR) | 0.3312 |
| Bit error rate (BER) | $1.78\times10^{-4}$ |
| 0 frequency of Alice's bits | 0.5009 |
| 0 frequency of Bob's bits | 0.5011 |

## 6. Conclusion

We have experimentally demonstrated secure key distribution using common-signal-induced synchronization in semiconductor lasers. The security of this system relies on information theoretic security. In our experiment, we have succeeded in common-signal-induced synchronization in semiconductor lasers. When the phases of optical feedback lights of the Responses lasers are randomly modulated, two legitimate users can share highly correlated random bit streams. One can generate secure keys by executing the key sharing protocol. Our implementation is promising as a new secure key distribution scheme.


## Acknowledgments

We gratefully acknowledge support from a Grant-in-Aid for Young Scientists and Management Expenses Grants from the Ministry of Education, Culture, Sports, Science and Technology in Japan, and NTT Corporation.


## References


[1] C. E. Shannon, Bell System Technical Journal, Vol. 28, pp. 656-715 (1949).

[2] C. Chachin, U. M. Maurer, CRYPTO 1997, Lecture Notes on Computer Science (LNCS), Vol. 1294, pp. 292-306, Springer, Heidelberg (1997).

[3] J. Muramatsu, K. Yoshimura, and P. Davis, ICITS 2009, Lecture Notes on Computer Science (LNCS), Vol. 5973, pp. 128-139, Springer (2010).

[4] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, Physical Review Letters, Vol. 108, No. 7, pp. 070602-1-5 (2012).

[5] T. Yamamoto, I. Oowada, H. Yip, A. Uchida, S. Yoshimori, K. Yoshimura, J. Muramatsu, S. Goto, and P. Davis, Optics Express, Vol. 15, No. 7, pp. 3974-3980 (2007).

[6] I. Oowada, H. Ariizumi, M. Li, S. Yoshimori, A. Uchida, K. Yoshimura, and P. Davis, Optics Express, Vol. 17, No. 12, pp. 10025-10034 (2009).

[7] H. Aida, M. Arahata, H. Okumura, H. Koizumi, A. Uchida, K. Yoshimura, J. Muramatsu, and P. Davis, Optics Express, Vol. 20, No. 11, pp. 11813-11829 (2012).

[8] E. Klein, N. Gross, E. Kopelowitz, M. Rosenbluh, L. Khaykovich, W. Kinzel, and I. Kanter, Physical Review E, Vol. 74, No. 4, pp. 046201 (2006).

[9] R. Vincente, C. R. Mirasso, and I. Fischer, Optics Letters, Vol. 32, No. 4, pp. 403-405 (2007).

[10] I. Kanter, E. Kopelowitz, and W. Kinzel, Physical Review Letters, Vol. 101, No. 8, pp. 084102 (2008).

[11] I. Kanter, M. Butkovski, Y. Peleg, M. Zigzag, Y. Aviad, I. Reidler, M. Rosenbluh, and W. Kinzel, Optics Express, Vol. 18, No. 17, pp. 18292-18302 (2010).

[12] J. Muramatsu, IEICE Transactions on Fundamentals, Vol. E89-A, pp. 2036-2046 (2006).