Public channel cryptography based on synchronization of chaotic lasers

Ido Kanter† Yitzhak Peleg†, Meital Zigzag† and Wolfgang Kinzel‡

† Department of Physics, Bar-Ilan University, Ramat-Gan,52900 Israel
‡ Institute for Theoretical Physics, University of Wuerzburg, Am Hubland, 97074 Wuerzburg, Germany
Email: kanter@mail.biu.ac.il

Abstract– Recently, physical random number generators (RBGs) based on chaotic semiconductor lasers were shown to exceed Gbit/s rates. Whether secure synchronization of two high rate physical RBGs is possible remains an open question. Here we propose a method, whereby two fast RBGs based on mutually coupled chaotic lasers, are synchronized. Using information theoretic analysis we demonstrate security against a powerful computational eavesdropper, capable of noiseless amplification, where all parameters are publicly known. The method is also extended to secure synchronization of a small network of three RBGs.

1. Introduction

In a typical scenario of a secure channel the communicating parties have to hold a common key in the form of a bit string which is known only to the two parties [1]. A secure deterministic key-exchange protocol between two parties over a public channel was discovered in 1976 by Diffie and Hellman based on number theory, and paved the road for modern cryptography [1]. Alternative physical mechanisms based on quantum mechanics have been suggested more recently for a secure key-exchange protocol with the important and unique ability of the two communicating parties to detect the presence of any third party trying to gain knowledge of the key [2]. The first layer of the quantum protocol is based on quantum ingredients such as entangled pairs of photons and results in *correlated keys* for both partners. A second, classical layer, consists of information reconciliation and privacy amplification (error correcting code and source coding). These result in *identical keys* for the communicating pair while leakage of information to an eavesdropper is eliminated, however, these procedures lower the rate at which random bits can be generated.

An intriguing possibility for a non-deterministic, physical RBG that is appropriate to all of these applications, is a semiconductor laser (SL) in the presence of external feedback, whose output consists of large chaotic intensity fluctuations, characterized by pulses with typical width of 100 ps [3-6]. Indeed great progress has been made recently in demonstrating an RBG based on such lasers, with rates from a few Gbit/s [4,5] towards tera-bits/s [6,7]. A secure synchronization method, however, which is essential for utilization of the fast generation rate of the physical RBGs in a multiple node public channel cryptography network, remains to be demonstrated [8].

The focus of this work is to demonstrate secure synchronization of two high bandwidth RBGs over a public channel using a classical mechanism zero lag synchronization (ZLS) of two mutually coupled chaotic lasers [9]. The ZLS mechanism is not sufficiently secure in its simple form to act as a key-exchange protocol [10], and it serves only as an information carrier to generate *correlated* random bit sequences. Identical random bit sequences can be constructed from these correlated sequences via information reconciliation and privacy amplification [2,8]. Furthermore, the presented mechanism allows the secure generation of a synchronized random bit string amongst a small network of communicating parties.

2. Results

2.1. Synchronization of two RBGs

We have numerically investigated the scenario of Fig. 1(a) where two mutually coupled lasers, A and B, are subject to both optical feedback and mutual coupling in a symmetric configuration. In general, ZLS can be achieved when that the sum of the self-coupling delay times of lasers A and B equals twice the mutual coupling delay time [11]. For simplicity of the discussion we first investigate the case where the optical self-feedback time delays, τ_A and τ_B, and the mutual coupling time delay, τ, are all equal to 10 ns in the examples below. The strength of self-feedback and the mutual coupling are denoted by κ and σ, respectively. The injection current to the threshold current ratio is selected to be 1.5, so that the lasers operate in the coherence collapse regime. In simulations, we use the Lang-Kobayashi (LK) equations which are a good model for the intensity dynamics of coupled semiconductor lasers and are explicitly given in references [12,13]. For each point in the phase space, (κ,σ), the cross correlation at zero time lag was measured over a window of 20 ns and averaged over 1 μs.

There are mainly two phases as shown in Fig. 2(a). For small $\kappa+\sigma$, A and B are not synchronized, whereas for larger values, ZLS emerges as the cross correlation gradually increases towards one. The cross correlation between A or B and a third laser, C, coupled unidirectionally (Fig. 1(a)) with the same time delays, $\tau_C=\tau_A=\tau_B=\tau$ and coupling strengths, $\sigma_C=\sigma$, $\kappa_C=\kappa$, is depicted in Fig. 2(b). A comparison of Fig. 2(a) and 2(b) indicates that ZLS of mutually coupled chaotic lasers is superior to the unidirectional coupling of laser C in a large

fraction of the phase space (κ,σ) [9], however, laser C can achieve the same level of synchronization as the mutually coupled lasers by amplifying the coupling signal, $\sigma_C>\sigma$, while maintaining its total input $\kappa_C+\sigma_C\sim\kappa+\sigma$. In what follows, we first describe the utilization of ZLS as a carrier synchronizing the RBGs of A and B and then we analyze the security of the channel

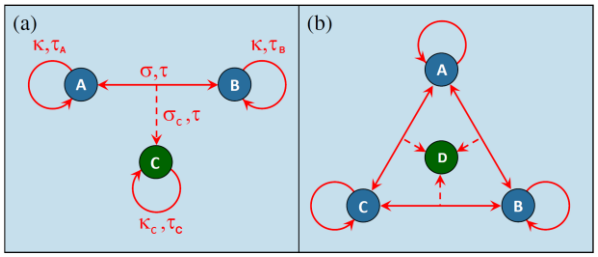

Fig. 1. Zero lag synchronization scheme for two and three lasers and an attacker. (a) Two mutually coupled SLs, A and B, where a third SL, C, is unidirectionally coupled to the mutually transmitted signals. The self-coupling delays for A and B are τ_A and τ_B, mutual coupling delay is τ, κ and σ are the strengths of self and mutual couplings. and similarly κ_C and σ_C for C. (b) A small network of three symmetrically mutually coupled SLs, A, B and C, where all coupling delays are equal to τ and a fourth laser, D, is coupled unidirectionally to each of the three transmitted signals. All delay times are equal.

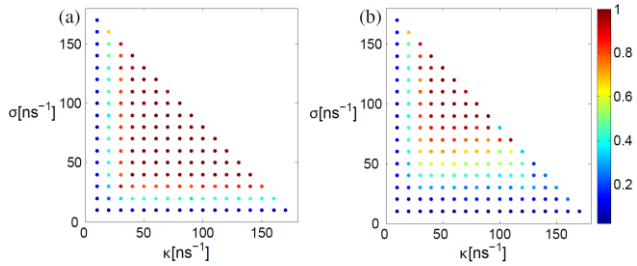

Fig. 2. Cross correlation for mutual and unidirectional coupling. (a) Cross correlation at zero time lag is calculated for two mutually coupled SLs (Fig. 1(a)) for a range of parameter values: κ, feedback strength and σ, coupling strength. (b) Cross correlation at zero time lag between a third SL coupled unidirectionally to one of the parties (Fig. 1(a)), using identical κ and σ as the parties.

In the first step, each partner encodes a random binary sequence by modulating the chaotic intensity of its laser. The modulated intensity is thus M^2I, where M=1 corresponds to the transmission of "1" while $M=M_0$ corresponds to the transmission of "-1". In simulations we modulate the intensity by changing the field and in the examples below M_0 is set to 0.9 with a bandwidth of 1 Gbit/s, the explicit equations are given in [10]. Our simulations indicate that the ZLS between the communicating pair remains robust even in the presence of such independent modulation by each of the parties. B for instance, decodes the massage transmitted from A by dividing the intensity received from A with its own synchronized laser output, prior to his modulation, $<I_A^R>/<I_B>$, where the average, <…>, is over a predetermined duration of one bit transmission time. If this fraction is larger than $(1+M_0^2)/2$ then the estimated received bit is "1", otherwise "-1". The encoding/decoding procedures are implemented simultaneously at both lasers and are known as a mutual chaos pass filter (MCPF) mechanism [10]. The average bit error rate (BER) as a function of (κ,σ) is presented in Fig. 3(b).

2.2. Protocol

Parties A and B encode different random bit sequences, hence, the decoded bits are uncorrelated and independent of BER level. An identical random binary sequence is obtained using the following protocol:

- The two partners start with an identical public random binary sequence of length L, $S_A=S_B=S$.
- A compares his estimated received bit at time interval m, $R_A(m)$, to his random transmitted bit at the same time interval, $T_A(m)$. If $R_A(m)=T_A(m)$, $S_A(m)$ is set equal to $R_A(m)$, otherwise $S_A(m)$ remains unchanged. Similarly, in the event $R_B(m)=T_B(m)$, $S_B(m)$ is set equal to $R_B(m)$.
- At the end of the MCPF procedure the average fraction of identical bits between S_A and S_B is given by

$$P_{AB} = 1 - p + 0.5p^2 \qquad (1)$$

where p stands for the BER of the MCPF procedure [8]. The meaning of p=0 is that A and B acted identically on the initial vectors S and $P_{AB}=1$, whereas for p=1 only when the partners send different bits, S is altered differently by the two partners, hence $P_{AB}=0.5$. For simplicity of discussion we assume statistically independent errors in the decoding procedure of A and B. However, it is expected that both decoders are correlated, since in the event the two lasers are temporally desynchronized the probability for an error bit for both of them increases in comparison to time slots of enhanced synchronization, as was indeed observed in simulations and is analyzed using symbolic mathematics in [8]. The two partners now possess *correlated bit sequences*.
- To achieve the goal of two identical random bit sequences, an information reconciliation procedure is performed, a form of error correcting code, as for protocols of quantum cryptography [2]. At the end of this procedure the two partners hold *identical random bit sequences*.
- Inevitably, leakage of information occurs during the information reconciliation procedure and is eliminated by a privacy amplification procedure which is also utilized in quantum cryptography for similar reasons [2].

The identical random bit sequences can serve as a common key generated over a public channel. The main question is whether a passive, unidirectionally coupled attacker, C, is capable of deducing the key, when all details of the protocol are publicly known.

Fig. 2 indicates that it is possible to select sets of parameters (κ,σ) such that the ZLS of A and B, is superior to the ZLS of C. For instance, for κ=90 ns^{-1} and σ=40 ns^{-1} the cross correlation at zero time lag between the parties is much higher, ~0.94, than correlation between the attacker and the parties ~0.5. An attacker using the same set of parameters as A and B would obtain a very high BER in his CPF mechanism [21], q~0.4 in our simulations (Fig. 3(a)), in comparison to p~0.07 for A and B (Fig. 3(b)). In order to minimize his BER, the attacker can amplify σ_C while decreasing κ_C so that $\kappa_C+\sigma_C\sim\kappa+\sigma$. Fig. 3(a) indicates that the minimum BER for the attacker, q~0.15, is obtained for (κ=40 ns^{-1} ,σ_C = 90 ns^{-1}) while the parties are operating with (κ=90 ns^{-1} ,σ=40 ns^{-1}). Though this is a much lower BER then C would obtain without the use of amplification, it remains more than twice as high as the BER of A and B

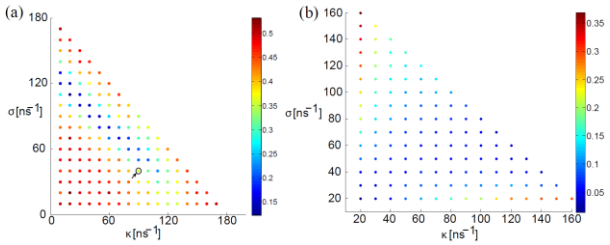

Fig. 3. Bit error rate for the attacker and the parties. (a) BER is calculated for laser C in the setup of Fig. 1(a) as a function of (κ, σ), when A and B are operating with κ=90ns^{-1} and σ= 40ns^{-1} (indicated by the arrow) (b) BER among the parties in the setup of Fig. 1(a) as a function of (κ, σ). The BER for each (κ, σ) is averaged over 1 μs and the modulation bandwidth is 1 Gbit/s.

Information theory analysis

The MCPF procedure is based on the synchronization of lasers A and B on the unmodulated portion of the mutual signal, while the modulated part can be considered as "noise". The noise to signal ratio for A and B is given by

$$\frac{\sigma M^2}{I(\sigma+\kappa)} \qquad (2)$$

and this is larger for the attacker

$$\frac{\sigma_C M^2}{I(\sigma_C+\kappa_C)} \qquad (3)$$

since $\sigma_C>\sigma$ and as a result q>p. A higher BER for C, however, does not necessarily indicate that the fraction of identical bits between S_C and S_A is reduced in comparison to the fraction of identical bits between S_A and S_B. One can show, using symbolic mathematics [8], that the average fraction of identical bits between S_C and S_A (or S_B) is given by

$$\boldsymbol{P_{AC}} = 1-0.5\boldsymbol{p}-\boldsymbol{q}(1-1.5\boldsymbol{p})+\boldsymbol{q}^2(0.5-\boldsymbol{p}) \qquad (4)$$

A comparison between equations (1) and (4) yields the range of (p,q) values where $P_{AC}<P_{AB}$, indicated by the blue and red colored region in Fig. 4(a). Note that for p=q and also for a limited region where p<q, one finds $P_{AC}<P_{AB}$.

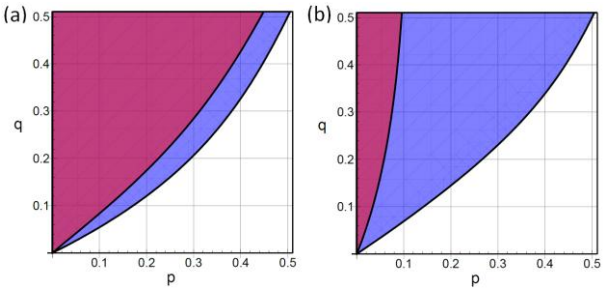

Fig. 4. Secure regions for two and three synchronized RBGs. (a) Two mutually coupled lasers as in the setup of Fig. 1(a) where all delays are equal. (b) Three mutually coupled lasers as in schematic Fig. 1(b). The BER of the MCPF procedure between a pair of parties, p, and between a party and the attacker, q, is calculated assuming uncorrelated decoded bits by the parties and by the attacker. The colored regions (blue or red) indicate a necessary condition for the failure of an attacker before the reconciliation procedure, $P_{AC}<P_{AB}$. The region where an attacker cannot succeed in recovering the key, even when using the leakage of information of the reconciliation procedure, is indicated in red.

A reconciliation procedure sets P_{AB}=1, resulting in identical random bit sequences for A and B. The leakage of information in the reconciliation procedure for the case $P_{AC}< P_{AB}$, can be also expected to be usable for enhancing P_{AC}, but it cannot be boosted to one. The exact bound for when A and B can be considered secure from attack by C is given by

$$I(S_A,S_B) > I(S_C,S_A)+I(S_C,S_B\,|\,S_A) \qquad (5)$$

where $I(S_C,S_B)$ and $I(S_C,S_B|S_A)$ stands for the mutual information and the conditional mutual information [14], respectively, and S_A, S_B and S_C stand for the binary sequences before the reconciliation procedure. Equation (5) states that in case the minimum required exchange of information for the reconciliation procedure, $1-I(S_A,S_B)$, is less than the total missing information C possesses about S_A and S_B, $1- I(S_C,S_A)-I(S_C,S_B|S_A)$, the attacker fails to recover the random bits sequence. Condition (5) as a function of p and q is calculated using symbolic mathematics and depicted by the red region of Fig. 4(a). In the above-mentioned example the point (p=0.07,q=0.15) lies in the red region of Fig. 4(a) and thus indicates that a secure synchronization of two RBGs over a public channel is achieved. The case of correlated decoded bits is also found to be secure [8].

2.3. Synchronization of three RBGs

Key-exchange protocols based on number theory are fundamentally limited to only two users [1]. Our proposed protocol, however, can be generalized to secure synchronization of RBGs among a small network of three mutually coupled lasers, as shown in Fig. 1(b). Each party starts with a given public random binary sequence. In case the estimated two received bits, using MCPF procedure, are equal to the party's transmitted bit, the corresponding bit in the public random binary sequence is set to the value of this common bit. An attacker represented by the fourth, middle laser in Fig. 1(b), is assumed to be capable of noiseless amplification of the transmitted signal and eavesdropping to each of the three communicating signals and to estimate the transmitted bit using a CPF procedure.

The average number of identical bits between any pair of (S_A, S_B, S_C) is calculated using symbolic mathematics and is given by $P=1-p+7/4p^2-3/2p^3+1/2p^4$ whereas between the attacker and a party $P_{attacker}=1-p/2+p^2/4-(3/4-2p+5/4p^2)q+(3/4-5/2p+2p^2)q^2-(1/4-p+p^2)q^3$ [8]. The region where $P>P_{attacker}$ is denoted by the colored (both blue and red) regions of Fig. 4(b), indicating a similar lower bound as for the two lasers case, Fig. 4(a). The exact condition for a secure synchronization of three RBGs is given by

$$I(S_D,S_A) + I(S_D,S_B \mid S_C) + I(S_D,S_C \mid S_A,S_B) - 2I(S_A,S_B) - I(S_A,S_C \mid S_B) + 1 > 0 \qquad (6)$$

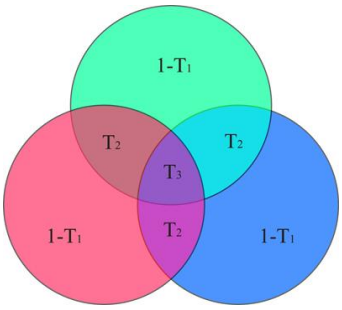

Fig. 5. Venn diagram for the mutual information of three communicating parties. The entropy of a transmitted bit of each party is represented by a circle normalized to 1. T_3–common information for all parties, T_2–common information for each pair of parties and $1-T_1$ stands for the independent information of each party.

where S_D is the binary recovered sequence of the attacker. This inequality was derived using a Venn diagram, Fig. 5. $1-T_1=1-I(S_A,S_B)-I(S_A,S_C|S_B)$ stands for the independent information of one party, $T_2= I(S_A,S_C|S_B)$ stands for the common information of two parties only and $T_3=T_1-2T_2$ is the common information for the three parties. The total entropy of the three parties is $3+T_2-2T_1$, hence the required exchange of information in the reconciliation procedure is $2+T_2-2T_1$. Failure of the attacker requires that the leakage of information in the reconciliation procedure plus the mutual information of the attacker with the three parties, $I(S_D,S_A)+I(S_D,S_B|S_C)+I(S_D,S_C|S_A,S_B)$, is less than 1 and results in inequality (6). The region of secure synchronization is indicated by the red region of Fig. 4(b) and is limited by $p \lesssim 0.1$ for $q \to 0.5$. Is it realistic to create such a gap between the BER of the parties and the attacker? Simulation results, averaged over transmission of 20,000 bits, with $\kappa=\sigma=60$ ns^{-1} for the parties indicate $p=0.025$, whereas an exhaustive search of the attacker indicates that the minimum $q=0.145$ is obtained for $\kappa_{attacker}=50$ ns^{-1} and $\sigma_{attacker}=120$ ns^{-1}. Fig. 4(b) shows that ($p=0.025$,$q=0.145$) is in the red region, hence a secure synchronization of three RBGs over a public channel is achieved.

References

[1] D. R. Stinson, *Cryptography : Theory and Practice.* (CRC Press, Boca Raton, 1995).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).

[3] T. E. Murphy, and R. Roy, "Chaotic lasers: The world's fastest dice," Nature Photon. **2**, 714-715 (2008).

[4] A. Uchida, et al., "Fast physical random bit generation with chaotic semiconductor lasers," Nature Photon. **2**, 728-732 (2008).

[5] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-Speed Random Number Generation Based on a Chaotic Semiconductor Laser," Phys. Rev. Lett. **103**, 024102 (2009).

[6] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nature Photon. **4**, 58–61 (2010).

[7] K. Hirano, et al., "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," Optics Express, **18**, 5512-5524 (2010).

[8] I. Kanter et. al., "Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography", Optics Express **18,** 18292 (2010).

[9] E. Klein, N. Gross, M. Rosenbluh, L. Khaykovich, and I. Kanter, "Stable isochronal synchronization of mutually coupled chaotic lasers," Phys. Rev. E **73**, 066214 (2006).

[10] I. Kanter, E. Kopelowitz, and W. Kinzel, "Public Channel Cryptography: Chaos Synchronization and Hilbert's Tenth Problem," Phys. Rev. Lett. **101**, 084102 (2008).

[11] M. Zigzag, M. Butkovski, A. Englert, W. Kinzel, and I. Kanter, "Zero lag synchronization of chaotic units with time-delayed couplings," Euro. Phys. Lett. **85** 60005 (2009).

[13] E. Klein, N. Gross, E. Kopelowitz, M. Rosenbluh, L. Khaykovich, W. Kinzel, and I. Kanter, "Public-channel cryptography based on mutual chaos pass filters," Phys. Rev. E **74**, 046201 (2006).

[14] T. M. Cover, and J. A. Thomas, *Elements of Information Theory* (John Wiley and Sons, New York, 1991).