On chaos synchronization and secure communication

BY W. KINZEL¹, A. ENGLERT¹,* AND I. KANTER²

¹Institute of Theoretical Physics, University of Wuerzburg, Wuerzburg, Germany
²Department of Physics, Bar-Ilan University, Ramat Gan 52900, Israel

Chaos synchronization, in particular isochronal synchronization of two chaotic trajectories to each other, may be used to build a means of secure communication over a public channel. In this paper, we give an overview of coupling schemes of Bernoulli units deduced from chaotic laser systems, different ways to transmit information by chaos synchronization and the advantage of bidirectional over unidirectional coupling with respect to secure communication. We present the protocol for using dynamical private commutative filters for tap-proof transmission of information that maps the task of a passive attacker to the class of non-deterministic polynomial time-complete problems.

Keywords: chaos synchronization; secure communication; delayed complex systems

1. Introduction

Chaos synchronization is a counterintuitive phenomenon. On one hand, a chaotic system is unpredictable, since its trajectory is extremely sensitive to its initial state (Schuster & Just 2005). On the other hand, two identical chaotic units that are coupled to each other may synchronize to a common chaotic trajectory (Pikovsky 1984; Pecora & Carroll 1990; Pikovsky et al. 2001). The system is still chaotic, but after a transient time the two chaotic trajectories are locked to each other in finite precision. This coupling may be unidirectional so that one sender is driving a receiver, and is then called a master–slave configuration. It may also be bidirectional with both units influencing each other.

The phenomenon of chaos synchronization is attracting a lot of research, partly because it has the potential to be applied for novel secure communication systems (Cuomo & Oppenheim 1993; Kocarev & Parlitz 1995; Boccaletti et al. 2002; Kinzel & Kanter 2008). In this regard, synchronization between coupled chaotic lasers is vitally important (Colet & Roy 1994; VanWiggeren & Roy 1998; Uchida et al. 2005). In fact, a private key secure communication system over a distance of 120 km in a public fibre-optic communication network has recently been demonstrated with chaotic semiconductor lasers in a master–slave configuration (Argyris et al. 2005).

*Author for correspondence (aenglert@physik.uni-wuerzburg.de).

One contribution of 13 to a Theme Issue ‘Delayed complex systems’.
When a message is added in the master–slave configuration with a tiny amplitude to the chaotic carrier of the sender Alice,¹ it is not easily—if at all—extractable from the transmitted laser beam unless its undisturbed chaotic signal is known (Cuomo & Oppenheim 1993; Kocarev & Parlitz 1995; Kinzel & Kanter 2008). The undisturbed chaotic signal, however, can only be known from a system that synchronizes with the sender, e.g. the receiver Bob. Thus, chaos synchronization opens up the possibility for a private key secure communication with high bit rates of the order of GHz. Is it possible to generalize this concept to the realm of public channel communication?

In this report, we focus on a passive attacker, Eve, who can only record the transmitted signals but does not send her signals to either one of the communicating partners, Alice and Bob. For a passive attacker, one has to distinguish between two possible scenarios. Either Eve consists of a similar set-up to that of Alice and Bob and her input is the mutually transmitted signals. If Eve is a software attacker, she can manipulate the recorded transmitted signal with various mathematical methods.

However, this communication protocol is secure only if the two partners, Alice and Bob, have agreed on identical private laser parameters. If an attacker, Eve, can use identical equipment, she can synchronize as well and extract the message by subtracting her laser output from the transmitted signal. Therefore, public cryptography is not possible with a unidirectional configuration.

For bidirectional couplings, however, the situation is different. When the two lasers of Alice and Bob are interacting, they may have an advantage over a hardware attacker, Eve, who is only recording the signal. As mentioned above, here we assume that Eve cannot send her own signal to Alice and Bob without being discovered. Eve has to amplify the signal she is listening to in order to synchronize; her signal-to-noise ratio will be worse than that of the communicating partners, which may be used for secure communication. Here, we found a quantitative difference in the bit error rate of Eve compared with the bit error rate of the communicating partners. It is possible, however, that Eve synchronizes with the communicating partners and we cannot prove this method to be secure.

Therefore, another approach to provide public cryptography is to prevent a hardware or software attacker, Eve, from synchronizing with the communicating partners at all. In the case of a software attacker, Eve has knowledge about all details of the equipment and the methods, and she is able to record the transmitted signals and to apply any mathematical tools to them. Alice and Bob are not allowed to agree on secret parameters and protocols prior to the communication. The question is: can Eve synchronize her laser with Bob and extract the information Alice sent?

Public cryptography with chaos synchronization based on mutual coupling was recently suggested and investigated by our research groups (Klein et al. 2005). In this report, we give an introduction and an overview of chaos synchronization and its potential for public cryptography with emphasis on our recent work (Klein et al. 2006a,b; Kanter et al. 2007, 2008a,b; Kestler et al. 2007, 2008; Rosenbluh et al. 2007; Aviad et al. 2008; Zigzag et al. 2009).

¹In this report, we commonly refer to the communicating units (sender) A and (receiver) B as Alice and Bob and to the eavesdropping unit E as Eve.
Chaos synchronization and communication

The work is based on the chaotic Bernoulli map as well as on ordinary differential equations (ODEs), namely the Lang–Kobayashi equations that are used to describe chaotic semiconductor lasers (Lang & Kobayashi 1980; Ahlers et al. 1998). All phenomena that we found for the simple discrete time map could be found in the ODEs as well (Kestler et al. 2008).

Our report is structured as follows: in §2, we describe the origin of our Bernoulli model that originates in the structure of a coupled chaotic laser system with focus on unidirectional coupling. In §3, we give an overview of two possibilities to transmit information via chaos synchronization, namely chaos pass filter and chaos modulation. Bidirectional coupling will be presented in §4 with a note on the restraint given by the correct adjustment of the time delays and the possibility of avoiding this restraint by multiple self-feedbacks. In this section, we also present the difference between uni- and bidirectional coupling. We describe methods for secure communication in §5, namely using static and dynamical private filters. Finally, we summarize our work in §6 and give a short outlook for further research.

2. Unidirectional coupling

Most of the phenomena that have been observed for synchronized chaotic lasers have been described by a simple mathematical model: coupled Bernoulli maps (Kestler et al. 2007; Aviad et al. 2008; Kanter et al. 2008a). Hence in this overview, we restrict the mathematics to this simple case. But we keep in mind that many details of coupled lasers depicted by rate equations, in particular the Lang–Kobayashi equations for semiconductor lasers (Lang & Kobayashi 1980; Ahlers et al. 1998), are the same as for the Bernoulli case. An isolated laser is not chaotic; chaos stems from time-delayed feedback of the laser itself or from its partners. In the simplest case, a laser becomes chaotic by feeding its beam back to its resonator by an external mirror. When this chaotic laser beam is inserted into a second laser, it may synchronize it. This unidirectional coupling, shown in figure 1, has the corresponding equations for the Bernoulli maps with $f(x) = (\alpha x) \mod 1$ that is chaotic for $\alpha > 1$,

$$a_t = (1 - \epsilon)f(a_{t-1}) + \epsilon f(a_{t-\tau})$$
$$b_t = (1 - \epsilon)f(b_{t-1}) + \epsilon f(a_{t-\tau}).$$

(2.1)

The Bernoulli system allows an analytical calculation of the stability of the synchronization manifold (Kestler et al. 2007, 2008). Here we find that

— the unit $A$ is chaotic for all parameters $\epsilon \in [0, 1]$ and
— $B$ synchronizes to $A$ for $(1 - \epsilon)\alpha < 1$. 

Figure 1. Scheme of two unidirectional coupled units A and B with an attacker E recording the transmitted signal.

Phil. Trans. R. Soc. A (2010)
When B synchronizes to A, the isolated units A and B without coupling and feedback are not chaotic. In this case, chaos is generated by the feedback, and only a non-chaotic unit can be synchronized by a signal from its partner. Note that, although the signal is transmitted with a time-delayed signal with an arbitrary large delay time $\tau$, B synchronizes to A without any time shift, $a_t = b_t$. This holds because we have used identical delay times for feedback and coupling, otherwise the trajectories would be synchronized with a time shift.

For shorter coupling delays, even anticipating chaos is possible: B can predict the chaotic trajectory of A (Voss 2000).

3. Transmission of information

How can Alice hide and transmit her secret message with synchronized laser beams? In principle, there are two possibilities: (i) the message is modulating only the transmitted signal (chaos masking or chaos pass filter) and (ii) the message is modulating the sending unit as well as the transmitted signal (chaos modulation) (Cuomo & Oppenheim 1993; Kocarev & Parlitz 1995; Kinzel & Kanter 2008). These two principles may be demonstrated with our Bernoulli systems. The first case corresponds to adding a message $m_t$ to the transmitted signal

$$b_t = (1 - \varepsilon)f(b_{t-1}) + \varepsilon f(a_{t-1} + m_{t-1}). \quad (3.1)$$

Since the unit of Bob is driven by the signal plus the message, Alice cannot completely synchronize with Bob. Surprisingly, Bob can recover the message by substracting the incoming signal from its own time-shifted trajectory

$$\tilde{m}_t = a_t + m_t - b_t. \quad (3.2)$$

It seems that the dynamic of B filters out the message, therefore the name chaos pass filter was coined (Fischer et al. 2000; Murakami & Shore 2005). The message is a perturbation that drives the unit B away from the synchronization manifold.

It turns out that this mechanism is more complex than the simple explanation (Kinzel et al. 2008). The tiny perturbation $m_t$ is amplified by the chaotic dynamics. In fact, the distribution of $\tilde{m}_t$ can have power-law tails, so extremely large excursions away from the synchronization manifold are possible. But if the message is encoded with bits, $m_t = \pm 1$ the bit error rate, the probability of $\tilde{m}_t m_t < 0$ can be very small. In fact, a bit error rate of $10^{-7}$ is reported for the laser demonstration (Argyris et al. 2005).

For the second scenario, chaos modulation, even error-free transmission is possible. One example is feeding the message back to the sender

$$a_t = (1 - \varepsilon)f(a_t) + \varepsilon f(a_{t-\tau} + m_{t-\tau}) \quad \text{and} \quad b_t = (1 - \varepsilon)f(b_t) + \varepsilon f(a_{t-\tau} + m_{t-\tau}). \quad (3.3)$$

It is immediately obvious that $a_t = b_t$ is still a solution of these equations, hence from equation (3.2) one finds $\tilde{m}_t = m_t$. Another possibility of chaos modulations is to modulate one parameter of the sending unit, e.g. the pump current of the laser of Alice (Uchida et al. 2005). This may be easier than modulating the beam, but it generates bit errors. In this case, one can even transmit signals with a chain
of identical units with arbitrary transmission delays and extract the message just by the difference of the trajectories of the last two units. However, the length of the chain is limited by convective instabilities (Schmitzer et al. 2009).

4. Bidirectional coupling

As mentioned before, unidirectional configurations allow any attacking unit to synchronize as well, if the attacker uses an identical dynamical unit. For bidirectional coupling, however, this is not obvious; hence, in this section we discuss chaos synchronization with mutually interacting units.

For lasers, chaos can be generated by coupling two lasers via their time-delayed laser beams. But they will not synchronize until one includes a self-feedback or another coupling with certain constraints to the delay times (Fischer et al. 2006; Klein et al. 2006). For the inclusion of a self-feedback, a scheme can be seen in figure 2 and the corresponding Bernoulli system has the equations

\[
\begin{align*}
a_t &= (1 - \varepsilon)f(a_{t-1}) + \varepsilon \kappa f(a_{t-\tau}) + \varepsilon (1 - \kappa) f(b_{t-\tau}) \\
b_t &= (1 - \varepsilon)f(b_{t-1}) + \varepsilon \kappa f(b_{t-\tau}) + \varepsilon (1 - \kappa) f(a_{t-\tau}).
\end{align*}
\]

(4.1)

For all parameters \(\varepsilon, \kappa \in [0, 1]\), the system is chaotic. Complete synchronization, \(a_t = b_t\), is a solution of these equations, but its stability has to be calculated. The analytic solution for large values of the delay time \(\tau\) is shown in figure 3. In fact, the stability of synchronization is determined by the roots of a polynomial of degree \(\tau\), and general symmetry considerations do not allow synchronization without feedback, \(\kappa = 0\). This is different for a triangular configuration of three units or they can synchronize without feedback (Kestler et al. 2007).

These results have been derived for a simple Bernoulli network. But, in fact, complete synchronization for semiconductor lasers with feedback and mutual coupling has been demonstrated experimentally (Klein et al. 2006b). The phase diagram is similar to that of figure 3. Of course, there are differences to iterated maps: if we are operating close to the threshold current, the laser will generate quasi-periodic spike patterns, as can be seen in figure 4, interrupted by sudden intensity breaks, known as low-frequency fluctuations. Almost complete synchronization of the intensity has been observed on a picosecond time scale (Rosenbluh et al. 2007), corresponding to a 10 ns delay time, and even optical phase synchronization on a femtosecond scale has been measured (Aviad et al. 2008).

For both systems, the system consisting of iterated Bernoulli maps and the chaotic semiconductor lasers usually described by ODEs, it turns out that synchronization is extremely sensitive to a careful adjustment of delay times.
Figure 3. Phase diagram for Bernoulli units. Regions II + III, synchronization of A and B for unidirectional coupling; regions I + II, synchronization for bidirectional coupling. Adapted from Kestler et al. (2008).

Figure 4. A trace of 15 ns duration of the intensity of one laser followed by plots of the same laser intensity after a time $\tau$, $2\tau$ and $3\tau$ with $\tau = 23.55$ ns. In the bottom panel, the intensity trace at time $t + \tau$ and at time $t + 2\tau$, demonstrating the slowly decaying periodicity of the spiking pattern. Adapted from Rosenbluh et al. (2007).
Chaos synchronization and communication

Figure 5. Even for small differences between the coupling delay time $\tau_c$ and feedback time $\tau_f$, the synchronization area can be reduced significantly compared with an exact adjustment. (a) Synchronization area for two chaotic coupled units with $\tau_c = \tau_f = 50$. (b) Synchronization area for $\tau_c = 50$ and $\tau_f = 49$.

The previous results have been derived with identical delay and coupling times. For the Bernoulli system, an analytical calculation shows that, for the minimal possible difference of one time step between delay and feedback time, synchronization is destroyed for large delay times, as can be seen in figure 5. Analogous to this, a careful adjustment of delay times of less than a picosecond, which means less than a millimetre distance in the laser experiments, is necessary. But, recently, we have shown how to avoid this sensitivity of the coupling delay. If the two partners use identical multiple feedback delays, the system synchronizes in broad intervals of the coupling delay (Zigzag et al. 2009).

Is there any difference between bi- and unidirectional coupling? Our simple model shows (figure 3) that the phase diagrams are different. Two identical units with bidirectional coupling synchronize in regions I and II, whereas with a unidirectional coupling they synchronize in regions II and III. Thus, with identical units, Alice and Bob synchronize in regions I and II, whereas with a unidirectional coupling they synchronize in regions II and III. Thus, with identical units, Alice and Bob can select their parameters in region I, and Eve does not synchronize her unit in the Bernoulli system as well as in the lasers. It was shown, however, that Eve can always find parameters for her unit that lead to synchronization (Kanter et al. 2008b). This may be a serious problem for realizations with lasers as negative coupling parameters are needed, which requires optical phase synchronization in the order of femtoseconds. Hence we find a quantitative difference between the bit error rate of an attacker Eve and the communicating partners (Klein et al. 2006a). However, in principle, this configuration does not allow secure communication and therefore an approach that prevents Eve from synchronization is preferable.

5. Secure public synchronization

Let us repeat the initial problem related to public cryptography: Alice and Bob want to synchronize their dynamical systems to a common chaotic trajectory. Eve has as much knowledge about Bob’s systems as Alice has and vice versa. Eve can
record and manipulate the transmitted signals between Alice and Bob, but she cannot influence their dynamics. How can Alice and Bob ensure that Eve does not synchronize as well?

For this problem, we focus on the chaos pass filter not on chaos modulation. It turns out that we can add a new mechanism to the configuration of the previous section to not only raise the bit error rate of Eve, but also to prevent her from synchronization—secret commutative filters (Kanter et al. 2008a, b), as can be seen in figure 6. Both Alice and Bob transmit their signals via a private filter which is not known to their partners. Since these filters commute, both receive an identical signal if they are synchronized. Eve knows the two transmitted signals only after passing through one filter and thus cannot synchronize as a hardware attacker.

Let us specify this principle for the Bernoulli systems. The dynamical equations of Alice and Bob are

\[
\begin{align*}
    a_t &= (1 - \varepsilon)f(a_{t-1}) + \varepsilon\kappa f(a_{t-\tau}) + \varepsilon(1 - \kappa)f(F_A(F_B(b_t))) \\
    b_t &= (1 - \varepsilon)f(b_{t-1}) + \varepsilon\kappa f(b_{t-\tau}) + \varepsilon(1 - \kappa)f(F_B(F_A(a_t))).
\end{align*}
\]

(5.1)

\(F_B(b_t)\) and \(F_A(a_t)\) are the signals transmitted from Alice and Bob, respectively. They consist of the variables that are filtered with private kernels \(K^A_r\) and \(K^B_r\).

\[
\begin{align*}
    F_A(a_t) &= \sum_r K^A_r a_{t-\tau} \\
    F_B(b_t) &= \sum_r K^B_r b_{t-\tau}.
\end{align*}
\]

(5.2)

If \(a_t = b_t\), then the two driving signals \(F_A(F_B(b_t))\) and \(F_B(F_A(a_t))\) are identical, since convolutions commute. In fact, for randomly chosen filter parameters Alice and Bob can still synchronize the units, as shown in figure 7. But Eve as an hardware attacker receives only \(F_A(a_t)\) and \(F_B(b_t)\), thus she cannot synchronize her unit. Any hardware attack fails.

We now analyse the situation with an idealized software attacker that can record the signal with infinite precision. In principle, when enough information is transmitted, it may be possible to calculate the private filters \(K^A_r\) and \(K^B_r\) for \(r = 1, \ldots, N\) with \(N\) being the number of filter parameters. This is due to the counting argument as with each time step the attacker gets two additional equations for \(F_A(a_t)F_B(a_t)\) and only one additional unknown new variable \(a_t\). To avoid this, an additional protocol has been suggested.

— When the number of time steps is about the number of unknowns \(a_t = b_t\), \(K^A_r, K^B_r\), the transmission is interrupted, and we have a period of silence and Alice and Bob select new filter parameters.

Figure 6. Scheme of two bidirectional coupled units A and B each with a private commutative filter. Adapted from Kanter et al. (2008b).
Chaos synchronization and communication

Figure 7. Analytical results for the fraction of the phase space \((\varepsilon, \kappa)\), where synchronization is achieved for a Bernoulli map with \(\tau = 40\) and \(\alpha = 1.5\). (a) With the absence of filters, synchronization is achieved only in the red region. (b) The probability of synchronizing in the phase space in the case of static filters with \(N = 2\).

— The transmitted signals as well as the filter parameters are discretized to integers.
— A nonlinear term of the past signal is added to the transmitted signal and its effect vanishes as the partners are synchronized.

The first point avoids an exact calculation of the filter parameters. The second point maps the problem to the solution of equations with integers (Diophantine problems). These problems belong to the class of non-deterministic polynomial time (NP) problems; hence, in principle, it should be impossible to solve these equations that a number of calculations, which increases with a power of \(N\), the number of filter parameters, only.

6. Summary and outlook

In this paper, we have presented recent work from our research group on secure communication based on chaos synchronization. Chaos synchronization is a promising field of research concerning public cryptography. The isochronal synchronization of two chaotic units can be used to transmit messages with small bit error rate by using the configuration of the chaos pass filter, or even error-free by using chaos modulation. In both cases, bidirectional coupling has the potential to be used in secure communication, whereas unidirectional coupling has been proved not to be secure.

When we are dealing with a hardware attacker, static filters can be used to ensure a secure public channel communication. A software attacker can record the transmitted signal of both units and try to adjust its own parameters to achieve the private filters and then the hidden message. However, it was shown that, by using private commutative filters with parameters that are changed after a certain time, the problem of adjusting the parameter of the attacker correctly can be mapped to a known NP-complete problem. Therefore, our presented protocol provides a way to transmit information securely over a public channel.

Phil. Trans. R. Soc. A (2010)
To avoid the restriction that exactly identical delay times must be used for self-feedback and coupling, we presented the method of using multiple self-feedback. This approach increases the range of coupling delay times where synchronization between two units is possible. The question of how Eve may react to such a change is the subject of further research.

References


