Public Channel Cryptography: Chaos Synchronization and Hilbert's Tenth Problem

Ido Kanter,[1] Evi Kopelowitz,[1] and Wolfgang Kinzel[2]

[1]*Department of Physics, Bar-Ilan University, Ramat-Gan, 52900 Israel*

[2]*Institute for Theoretical Physics, University of Würzburg, Am Hubland, 97074 Würzburg, Germany*

(Received 14 February 2008; published 22 August 2008)

The synchronization process of two mutually delayed coupled deterministic chaotic maps is demonstrated both analytically and numerically. The synchronization is preserved when the mutually transmitted signals are concealed by two commutative private filters, a convolution of the truncated time-delayed output signals or some powers of the delayed output signals. The task of a passive attacker is mapped onto Hilbert's tenth problem, solving a set of nonlinear Diophantine equations, which was proven to be in the class of NP-complete problems [problems that are both NP (verifiable in nondeterministic polynomial time) and NP-hard (any NP problem can be translated into this problem)]. This bridge between nonlinear dynamics and NP-complete problems opens a horizon for new types of secure public-channel protocols.

DOI: 10.1103/PhysRevLett.101.084102 PACS numbers: 05.45.Vx, 89.70.Hj

Chaotic systems are very unpredictable, and two chaotic systems, starting from almost identical initial states, end in completely uncorrelated trajectories [1]. Nevertheless, two chaotic systems which are coupled by some of their internal variables may synchronize to a common identical chaotic motion [2,3]. Unpredictability [4] or chaos synchronization, of coupled chaotic systems have attracted a lot of attention, mainly because of the potential to build a secure communication protocol based on artificial chaotic systems [3,5–7] or coupled chaotic lasers [8–10].

The security of a public-key encryption protocol based on chaos synchronization relies on the fact that two chaotic systems, A and B, synchronize by bi-directional interaction whereas a third unit E, which is only driven by the transmitted signal, cannot synchronize. However, it is not obvious that this is possible at all. On one hand, the two mutually coupled chaotic systems influence the dynamics of each other and can accelerate the synchronization by enhancing coherent moves, whereas the unidirectionally coupled system, an attacker, cannot influence the synchronization process. On the other hand, the attacker is allowed to record and to manipulate his recorded signals, without affecting the synchronization process [5,6,11,12]. Note that the two partners, A and B, are not allowed to exchange any secret information; the attacker E knows all the details which A knows about the system of B and vice versa.

For identical partners which synchronize by a bi-directional signal, we recently presented a proof that an attacking unit coupled unidirectionally can synchronize as well [13]. The proof is valid for any type of transmitted signals, for instance, a nonlinear function of the time-delayed output signals. For nonidentical partners which can synchronize, using for instance private commutative filters, it may be difficult for the attacker to synchronize and to reveal the time-dependent output signal of the parties [13], but one cannot exclude efficient advanced software or hardware attacks. A hardware attacker consists of a similar chaotic setup to those of the synchronized chaotic partners, whereas a software attacker is able to mathematically manipulate the recorded signal.

In order to exclude any possible software advanced attack, we map the task of the attacker onto one of the NP-Complete (NPC) problems [14]. The NPC problems are the most difficult problems in NP (nondeterministic polynomial time) and at present, all known deterministic algorithms for NPC problems require running time that is exponential with some tunable parameters of the problem. The main goal of this Letter is to bridge between two different disciplines, synchronization in nonlinear dynamics and the realm of the NPC problems. The establishment of such a bridge proves the lack of any possible efficient software attack, while the mutually coupled chaotic partners are synchronized. Note that the definition of the known NPC problems is static [14], and here we map a dynamical process onto an NPC problem.

Hilbert's tenth problem is the tenth on the list of Hilbert's problems of 1900 [15]. Its statement is as follows: given a set of Diophantine equations (DEs), polynomials with integer coefficients, finding an integer solution that satisfies the set. The solution of a general set of DEs is known to be undecidable [16–18]. However, some subsets of the DEs are known to be decidable and belong to the class of NPC problems [16,18]. A class of Hilbert's tenth problem is to find an integer solution of the following set of DEs [18]

$$D\vec{y} = \vec{\sigma}(z), \tag{1}$$

where D is an $m \times n$ matrix of rational constants, $\vec{y} = (y_1, \ldots, y_n)$, and $\vec{\sigma} = (\sigma_1(z), \ldots, \sigma_m(z))$ is a column vector. The $\{\sigma_i(z)\}$ are polynomials with a finite degree greater than one. Finding a non-negative integer solution $(y_1, \ldots, y_n, z)$ to the above set was proven to belong to the class of NPC problems [18]. In this Letter, we map the task of an attacker in the scenario of two synchronizing chaotic units onto this NPC problem.

We start by defining our synchronization process of two interacting units. Consider two iterated chaotic maps x^A and x^B, which their dynamics are controlled by a general self-feedback function S_f and a general coupling function S_c which are both nonlinear functions of the history τ steps back

$$x_t^A = S_f(\vec{x}_t^A) + S_c(\vec{x}_t^B) \qquad x_t^B = S_f(\vec{x}_t^B) + S_c(\vec{x}_t^A) \quad (2)$$

where $\vec{x}_t = (x_{t-1}, \ldots, x_{t-\tau})$.

Do the two mutually coupled chaotic maps synchronize under such circumstances? The positive answer is demonstrated below for the simplest chaotic maps, the Bernoulli map [2]. The dynamics of the two mutually coupled units x_t^A and x_t^B can be analyzed analytically and is given by

$$\begin{aligned} x_t^A &= (1-\varepsilon)f(x_{t-1}^A) + \varepsilon[\kappa f(x_{t-\tau}^A) + (1-\kappa)R^A(\vec{x}_t^B)] \\ x_t^B &= (1-\varepsilon)f(x_{t-1}^B) + \varepsilon[\kappa f(x_{t-\tau}^B) + (1-\kappa)R^B(\vec{x}_t^A)] \end{aligned} \quad (3)$$

where $f(x) = (ax) \bmod 1$, and a Bernoulli map is chaotic for $a > 1$ [19]. The parameter ε indicates the weight of the delayed terms, κ stands for the strength of the self-coupling term, and $R^{A,B}(\vec{x}_t^{B,A})$ are the received signals of each partner. Note that [0, 1] is the allowed range for ε and κ. For the simple case of $R^{A,B}(\vec{x}_t^{B,A}) = f(x_{t-\tau}^{B,A})$, a linear expansion of the distance $d_t = x_t^A - x_t^B$ leads to $d_t = (1-\varepsilon)ad_{t-1} + \varepsilon a(2\kappa - 1)d_{t-\tau}$ [19,20]. By assuming that the distance converges/diverges exponentially in time, $d_t \propto c^t$, we find that the largest conditional Lyapunov exponent is negative and synchronization is achieved for $(a-1)/2a\varepsilon < \kappa < (2a\varepsilon + 1 - a)/2a\varepsilon$ as is depicted in Fig. 1(a).

In order to map the task of an attacker on this synchronization process to the presented NPC problem, we have to include the following four adjustments to the system: (a) private commutative filters, (b) transmission of integer signals, (c) additional nonlinear terms to the transmitted signal, and (d) periods of cutoffs in communication. Our next goal is to explain each one of these adjustments and to show that synchronization is still maintained when applying all of the adjustments simultaneously, and finally to show that the task of the attacker is mapped onto the NPC problem, Eq. (1).

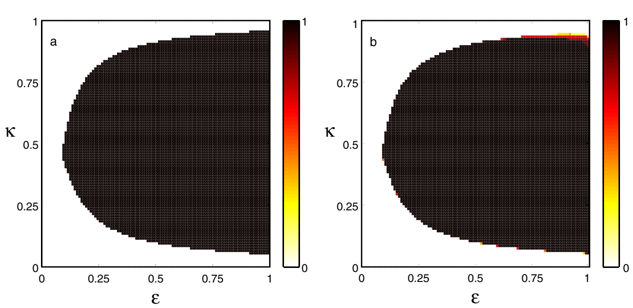

FIG. 1 (color online). Semianalytic results for the fraction of the phase space, (ε, κ), where synchronization is achieved for a Bernoulli map with $\tau = 100$ and $a = 1.1$. (a) With the absence of filters, synchronization is achieved only in the black regime. (b) The probability to synchronize in the case of unclipped filters with $N = 10$ and $\phi = 2$.

The first adjustment is extending the configuration, Eq. (3), to the case of nonidentical units x^A and x^B. Both units are using different functions (filters) g_A and g_B, and the two transmitted signals are $g_A(\vec{x}_t^A)$ and $g_B(\vec{x}_t^B)$, see Fig. 2. These functions are private, only x^A knows g_A and x^B knows g_B. The coupling functions $S_c(\vec{x}_t^B)$, $S_c(\vec{x}_t^A)$ are simply the received signals which are $g_A(g_B(x_t^B))$ and $g_B(g_A(x_t^A))$, respectively. In order to preserve synchronization as a fix point of the dynamics, we only use filters that commute, $g_A(g_B(\vec{x})) = g_B(g_A(\vec{x}))$. Since an attacker does not know the filters, he cannot use them for his hardware attack.

The most simple *commutative* filter one can consider is convolution. The transmitted signal is defined by

$$T_t^{A,B} = g_{A,B}(\vec{x}_t^{A,B}) = \sum_{\nu=0}^{N-1} K_{A,B}^{\nu} f(x_{t-\nu}^{A,B}) \quad (4)$$

where $K_A^\nu, K_B^\nu \in [0, 1]$ are the private filters chosen randomly by each one of the partners and $\nu = 0, 1, \ldots, N-1$. We demand that $\sum_{\nu=0}^{N-1} K_{A,B}^\nu = 1$, in order to ensure that the convolved signal is limited by [0, 1].

Before arriving at the other end of the channel, the transmitted signal T encounters the second filter. Therefore, the received signal for units A and B is

$$R_t^{A,B} = g_{A,B}(\vec{T}_t^{B,A}) = \sum_{\mu,\nu=0}^{N-1} K_B^\nu K_A^\mu f(x_{t-\nu-\mu}^{B,A}). \quad (5)$$

We measured the synchronization time t_{synch} as a function of τ and found that in order to achieve linear synchronization time for $N \gg 1$, the strengths of the filter coefficients, the keys, have to follow a power-law $K_A^\nu, K_B^\nu \propto \frac{\xi_{A,B}^\nu}{(1+\nu)^\phi}$, where $\xi_{A,B}^\nu$ is a random number between [0, 1]. Figure 3(a) exemplifies the linear scaling of $t_{\text{synch}}(\tau)$ for $N = 10$ and $\phi = 2$. Since the values of the private keys K_A, K_B are random, we calculate the probability of achieving synchronization in the phase space of (ε, κ) using sampling of random sets of keys. In Fig. 1, we compare the semianalytic results for the regimes of synchronization for the basic setup without filters (a) and with filters (b). We

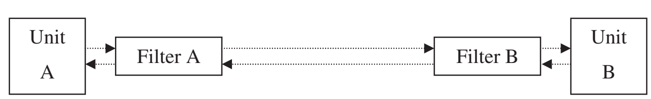

FIG. 2. A setup of two time-delayed mutually coupled units, where each unit has a filter influencing both transmitted and received signals.

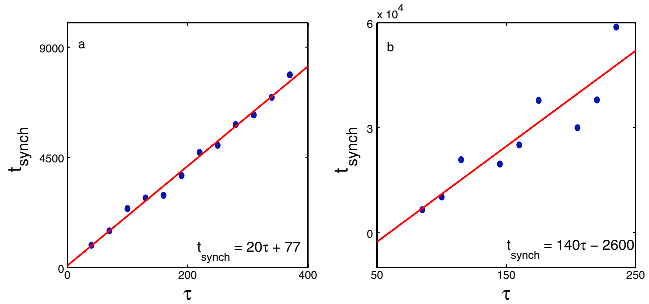

FIG. 3 (color online). Simulation results for the synchronization time, $t_{\rm synch}$, as a function of τ for $a = 1.1$, $N = 10$, and $\phi = 2$: (a) linear filters, and (b) with quantization $m = 6$, and an additional quantized nonlinear term. $\rho_t = 2, 3, 4, 5$ with equal probability, $C_t \in [0, 0.1]$, $N_0 = 40(t \bmod 40) - 5$, $N_1 = 20$, and $N_2 = 20$, solid lines were obtained by linear fitting.

found that even in this case, the regime of synchronization is almost unchanged.

The next two adjustments [(b) and (c)] to the synchronization process is modifying the transmitted signal to be composed of clipped output keys and signals, and also to include a nonlinear term of the past output signal. Practically, the precision of the computer is m_0 decimal digits, and the key filters and output signals consist of only $m \ll m_0$ most significant decimal digits (or integers after multiplying by 10^m). Adopting these two adjustments, the transmitted signal has the following form:

$$T_t^{A,B} = \sum_{\nu=0}^{N-1} K_{A,B}^{\nu} f(x_{t-\nu}^{A,B}) + C_t[f(x_{N_0}^{A,B})]^{\rho_t} \tag{6}$$

where $K_{A,B}$ are the clipped keys and $f(x_{t-\nu}^{A,B})$ are the clipped output signals. $C_t[f(x_{N_0}^{A,B})]^{\rho_t}$ is the nonlinear term which is not convolved in the current filters, C_t, ρ_t, and N_0 are public constants used simultaneously by both partners. $C_t \in [0, 1]$ and is also clipped, the power ρ_t is an integer, and $N_0 (< t - N)$ is a time step from the past. Since the partners are using different private keys (filters), synchronization is a fix point of the dynamics only when each partner subtracts his own nonlinear term before applying the convolution using his key. Therefore, the received signal in case of synchronization is

$$\begin{aligned} R_t^{A,B} &= g_{A,B}(\vec{T}_t^{B,A} - C_t[f(x_{N_0}^{A,B})]^{\rho_t}) \\ &= \sum_{\mu,\nu=0}^{N-1} K_B^{\nu} K_A^{\mu} f(x_{t-\nu-\mu}^{B,A}). \end{aligned} \tag{7}$$

It is clear that synchronization is a fixed point of the dynamical process, since after the convolution at the receiver, the nonlinear terms appear only in the form $C_t[f(x_{N_0}^B)^{\rho_t} - f(x_{N_0}^A)^{\rho_t}]$ which vanishes when the partners are synchronized. It is worthy to note that since the keys are normalized and $C_t > 0$, it is possible that the received signal is greater than one; however, in practice it does not affect the synchronization process, and alternatively one can apply mod 1 again on the received signal. Both methods give the same regime of synchronization.

For the case of clipped keys and output signals, simulations with $m_0 = 32$ indicate that the regime in the phase space where synchronization exists is only slightly affected by the quantization of the keys and the transmitted signals. A typical result for different values of m is depicted in Fig. 4(a).

The last adjustment [(d)] of our setup is the implementation of dynamical filters. For N_1 steps, the partners are using the above-mentioned prescription. For the next N_2 steps, no communication between the partners occurs, and each partner is updating his states following his own history of continuous signals with $\kappa = 1$ in Eq. (3). After each period of silence, N_2, each partner is selecting a new set of private filters, and in addition, they select the nonlinear contribution to the transmitted signal to be a function of the signal at a time step, N_0, belonging to the previous silence period [21].

Simulations indicate that while the synchronization time and phase space are affected by the nonlinear additional term in Eq. (6) and by the silence periods, $t_{\rm synch}$ still scales linearly with τ as depicted in Fig. 3(b), and synchronization is achieved in a non-negligible fraction of the phase space. For instance, synchronization for $\rho_t = 2, 3, 4, 5$ with equal probability, $C_t \in [0, 0.1]$, $N = 10$, $N_1 = 20$, $N_2 = 20$, and $N_0 = 40(t \bmod 40) - 5$ is depicted in Fig. 4(b).

We now turn to discuss the complexity of a unidirectional listener. To avoid any software attacks or any other advanced attacks, we map the task of the attacker to the NPC problem, Eq. (1). Assuming a synchronization state, $\vec{x}_t^A = \vec{x}_t^B \equiv \vec{x}_t$. In one time step, the transmitted signals on both directions, $T_t^{A,B}$, consist of $3N - 2$ unknown variables: $\{K_{A,B}^{\nu}\}, f(x_t), \ldots, f(x_{t-N+1})$. On the next time step, two new equations emerge: $T_{t+1}^{A,B}$. These equations consist of previously unknown variables and one new unknown variable $f(x_{t+1})$. Therefore, by adding more time steps, we

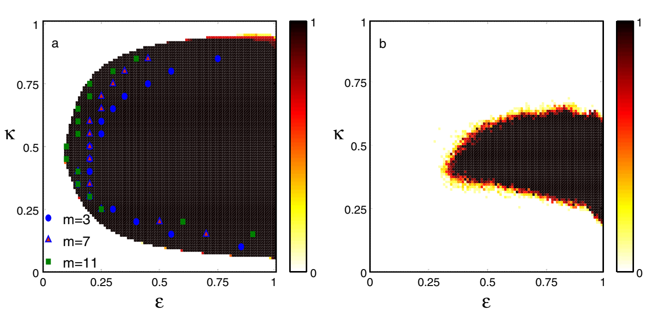

FIG. 4 (color online). Simulation results for the fraction of the phase space, (ε, κ), where synchronization is achieved for $\tau = 100$, $a = 1.1$, $N = 10$, and $\phi = 2$. (a) With quantized linear filters for $m = 3, 7, 11$ (b) with quantization $m = 6$ and the same parameters as for Fig. 3(b).

are adding more equations than new variables. Actually, the number of required equations to decode the keys of length N is $6(N-1)$. Therefore, the number of required iterations is $3(N-1)$. In order for a passive attacker to construct the entire signal, he needs to eavesdrop over at least $3(N-1)$ successive time steps. His task is therefore to solve a set of nonlinear DEs [16,17]. The nonlinearity emerges since the attacker does not know either the integer keys, $K^{\nu}_{A,B}$, or the history of the clipped output signals of the partners.

In order to map our synchronization problem to the proven NPC problem, Eq. (1), we choose N_1 to be in the range of $N < N_1 < 3(N-1)$ [see for instance Fig. 4(b)]. Hence, the task of the attacker is to find the complete set of solutions for the nonlinear DEs (unknown clipped keys and history of clipped signals), and next to find the correct solution for the observed dynamical synchronization process. The number of solutions is at least one, but can be unbounded; hence, the complexity of the attacker is at least NPC, where the complexity of the problem increases with N. The silence regime, $N_2 > N$, was selected to guarantee that the set of DEs the attacker has to solve consists of nonlinear terms of only one past clipped output signal [as formally required by Eq. (1)]. Note that the use of time-dependent filters eliminates any approximated reconstruction of the trajectory based on Takens embedding theorem [22] since the transmitted signal is a discontinuous function of the chaotic variables.

Note that also with the lack of adjustment (c) [the nonlinear term in Eq. (6)], the problem reduces to the solvability of linear DEs which belongs to the class of NPC [17,18,23]. However, finding a solution of a set of linear DEs may be feasible in practice, in polynomial time using heuristic or probabilistic methods [24].

We prove semianalytically that the security of the simplest synchronization process (Bernoulli map) consists of τ *time-independent* local Lyapunov exponents. In simulations, we obtained similar results also for the Lang-Kobayashi differential equations governing the behavior of semiconductor lasers, where the transmitted signal in lasers is quantized.

We thank Johannes Kesstler, Uri Feige, and Aviezri Fraenkel for many fruitful discussions.

[1] H. G. Schuster and W. Just, *Deterministic Chaos* (Wiley VCH, New York, 2005).

[2] A. Pikovsky, M. Rosenblum, and J. Kurths, *Synchronization: A Universal Concept in Nonlinear Sciences* (Cambridge Univ. Press, N.Y., 2001).

[3] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).

[4] A. Abel and W. Scharz, Proc. IEEE **90**, 691 (2002).

[5] G. Perez and H. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).

[6] K. M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 959 (1994).

[7] E. Klein, R. Mislovaty, I. Kanter, and W. Kinzel, Phys. Rev. E **72**, 016214 (2005).

[8] G. D. VanWiggeren and R. Roy, Science **279**, 1198 (1998).

[9] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, Nature (London) **437**, 343 (2005).

[10] E. Klein, N. Gross, E. Kopelowitz, M. Rosenbluh, W. Kinzel, L. Khaykovich, and I. Kanter, Phys. Rev. E **74**, 046201 (2006).

[11] M. Rosen-Zvi, E. Klein, I. Kanter, and W. Kinzel, Phys. Rev. E **66**, 066135 (2002).

[12] A. Klimov, A. Mityagin, and A. Shamir, ASIACRYPT 288–298 (2002).

[13] I. Kanter, E. Kopelowitz, W. Kinzel, and J. Kestler, arXiv:0712.2712v1.

[14] M. R. Garey and D. S. Johnson, *Computers and Intractability* (W. H. Freeman Corporation, New York, 1979).

[15] M. Davis, Am. Math. Mon. **80**, 233 (1973).

[16] http://mathworld.wolfram.com/DiophantineEquation.html, and references therein.

[17] C. H. Papadimitriou, *Computational Complexity* (Addison Wesley, Reading, MA, 1994).

[18] E. M. Gurari and O. H. Ibarra, J. Assoc. Comput. Mach. **26**, 567 (1979).

[19] J. Kestler, W. Kinzel, and I. Kanter, Phys. Rev. E **76**, 035202 (2007).

[20] S. Lerpi, G. Giacomelli, A. Politi, and F. T. Arecchi, Physica D (Amsterdam) **70**, 235 (1994).

[21] Synchronization under a scenario of silence periods is based on the fact that resycnhronization time of two mutually coupled chaotic maps is shorter in comparison to desynchronization time, as was observed in I. Kanter, N. Gross, E. Klein, E. Kopelowitz, P. Yoskovits, L. Khaykovich, W. Kinzel, and M. Rosenbluh, Phys. Rev. Lett. **98**, 154101 (2007).

[22] F. Takens, in *Dynamical Systems and Turbulence (Warwick 1980)*, edited by D. A. Rand and L.-S. Young, Lecture Notes in Mathematics Vol. 898 (Springer-Verlag, Berlin, 1980), pp. 366–381.

[23] C. H. Papadimitriou, JACM **28**, 765 (1981) proves that this problem is in NP. A proof that this problem is in NPC was offered by Uri Feige based on the following reduction from SAT. For every variable z in the input SAT formula, introduce two variables in the system of equations, z_0 for a positive literal corresponding to the variable, z_1 for a negative literal and add the equation $z_0 + z_1 = 3$. This constraint forces exactly one of these literals to have value 1 (interpreted as "true") and the other to have value 2 (interpreted as "false"). For every clause C_i, add the equation stating that the sum of the literals in the clause plus a new variable c_i is equal to twice the number of variables in the clause. This can be satisfied by setting c_i to be equal to the number of satisfied literals in the clause, which is positive if and only if the formula is satisfiable.

[24] I. Borosh and A. S. Fraenkel, Math. Comput. **20**, 107 (1966).