Coupling Functions Enable Secure Communications

Tomislav Stankovski, Peter V. E. McClintock, and Aneta Stefanovska*

Department of Physics, Lancaster University, Lancaster LA1 4YB, United Kingdom

(Received 16 August 2013; revised manuscript received 30 October 2013; published 26 February 2014)

Secure encryption is an essential feature of modern communications, but rapid progress in illicit decryption brings a continuing need for new schemes that are harder and harder to break. Inspired by the time-varying nature of the cardiorespiratory interaction, here we introduce a new class of secure communications that is highly resistant to conventional attacks. Unlike all earlier encryption procedures, this cipher makes use of the coupling functions between interacting dynamical systems. It results in an unbounded number of encryption key possibilities, allows the transmission or reception of more than one signal simultaneously, and is robust against external noise. Thus, the information signals are encrypted as the time variations of linearly independent coupling functions. Using predetermined forms of coupling function, we apply Bayesian inference on the receiver side to detect and separate the information signals while simultaneously eliminating the effect of external noise. The scheme is highly modular and is readily extendable to support different communications applications within the same general framework.

DOI: 10.1103/PhysRevX.4.011026

Subject Areas: Complex Systems, Nonlinear Dynamics, Statistical Physics

I. INTRODUCTION

It is often the case that great scientific and technological discoveries are made by mimicking biological methods and the systems already found in nature [1–3]. The complexity and phenomena associated with these natural structures and functions have been accumulated over a very long period of evolution and optimization, and they can lead to a diversity of designs and applications for solving contemporary human problems [4–7]. Recently, it was discovered that the cardiorespiratory coupling function can be decomposed into a number of independent functions and that it is of a time-varying nature [8]. This highly complex biomedical function has inspired and motivated us to create a new class of secure communications characterized by high efficiency and modularity.

Secure communications [9–17] can be based on different technologies, each characterized by its particular speed, size, energy consumption, and so on. Ideally, one seeks basic communication concepts that are applicable not only to existing technologies, e.g., magnetic vortex oscillators, graphene circuits, analogue electronic systems, quantum oscillators, and optical lasers [14,18–22], but also to the foreseeable technologies of the future. However, the question of where and how best to encrypt the information is far from trivial. If one chooses to encrypt in terms of the properties of a system, then the limited and small number of properties means that the security can be broken by conventional attack. The use of coupling functions, on the other hand, brings great freedom in the encryption process without changing the qualitative state of the system, and thereby increases security. Our proposal of coupling-function encryption, therefore, amounts to a significant conceptual advance that is likely to be important in many different technologies.

Although we take advantage of recent advances in the *understanding* of time-variable, nonautonomous, dynamics in, e.g., geophysics, biology, and astrophysics [23–26], our present aims are quite different in that we consider how to *apply* the corresponding theory [27] and methods to secure communications. As we see below, the decrypting receiver takes advantage of Bayesian inference. Its ability to infer multidimensional, time-evolving and coupled dynamical systems [8,28–30] makes it ideally matched to such applications. Additionally, the fact that coupled systems typically span a large volume of state space yields easier, faster, inference and higher precision.

A common characteristic of dynamical systems in nature is that they mutually interact, exerting influence and transferring energy and/or matter between each other. The interaction between two such systems is described by their coupling function and coupling amplitude. Coupling functions prescribe the physical rule specifying how the interactions occur and defining the possibility of qualitative transitions between the systems. They have played an important role in studies of interaction in diverse areas, including biology [31], geophysics [32], cosmology [33], and chemistry [34]. Much progress has been made towards being able to detect and quantify the causality,

*Corresponding author.
aneta@lancaster.ac.uk

direction, and strength of the coupling amplitude [35–38] based on the analysis of measured time series. More recently, however, efforts have focused on how to extract and reconstruct the coupling functions themselves [8,39–42], but many aspects still remain to be investigated, e.g., the problem of treating more than two independent and nonlinear coupling functions, each describing a relationship between the two systems, which we describe below.

These developments have unexpectedly opened the door to a novel class of secure communications [43]. In what follows, we introduce the new scheme, explain how it works, present examples of encryption and decryption in action, and point out some of the considerable advantages of the new cipher. Section II provides a succinct description of the underlying protocol and Sec. III discusses how it is implemented. In Sec. IV, we provide a detailed description of an exemplary realization of the scheme in terms of coupled Rossler and Lorenz oscillators and quantify its high noise tolerance. We discuss the results obtained and the advantages of the scheme in Sec. V. The Appendix describes a second and more complicated example of the new scheme: we demonstrate the use of pairs of coupled Lorenz systems for the encryption and decryption of ten independent binary information signals in parallel and very briefly discuss the results.

II. PROTOCOL

We illustrate the central concepts of our new communication framework in Fig. 1. A number of information signals coming from different channels or communications devices (e.g., mobile phone, sensor networks, or wireless broadband) are to be transmitted simultaneously. Each of the signals s_i is encrypted in a coupling function; i.e., they serve as coupling scale parameters in the nonlinear coupling functions between two self-sustained systems in the transmitter. Two signals, one from each system, are transmitted through the public channel. At the receiving end, two similar systems are enslaved, i.e., completely synchronized, by the two transmitted signals. Finally, by applying time-evolving Bayesian inference to the reconstructed systems, one can infer the model parameters and decrypt the information signals s_i. An important feature of the scheme is the private key holding information about the particular coupling functions in use—which, in principle, has an unbounded continuum of possible combinations. The number of coupling functions in use will always be finite, depending on the specific number of information channels that are needed; the choice of *forms* available for the coupling functions (forming the private key) is, however, unbounded.

III. IMPLEMENTATION

A. Systems model

Starting from a time series, the model to be inferred consists of two noisy M-dimensional interacting systems given by the following stochastic differential equation:

$$\begin{aligned}\dot{\mathbf{x}}_i &= \mathbf{f}(\mathbf{x}_i, \mathbf{x}_j|\mathbf{c}) + \sqrt{\mathbf{D}}\xi_i \\ &= \mathbf{g}(\mathbf{x}_i|\mathbf{c}_1) + \mathbf{q}(\mathbf{x}_i, \mathbf{x}_j|\mathbf{c}_2) + \sqrt{\mathbf{D}}\xi_i, \end{aligned} \tag{1}$$

where $i \neq j = 1, 2$, $\mathbf{c}$ is the parameter vector, and $\mathbf{f}(\mathbf{x}_i, \mathbf{x}_j|\mathbf{c})$ are base functions describing both the autonomous dynamics $\mathbf{g}(\mathbf{x}_i)$ and the coupling functions $\mathbf{q}(\mathbf{x}_i, \mathbf{x}_j)$. The noise is assumed to be white, Gaussian, and parametrized by a noise diffusion matrix $\mathbf{D}$.

For optimal security, the systems to be coupled need to be self-sustained, e.g., limit-cycle or chaotic oscillators. Chaotic systems are convenient for inference within a communications framework and confer the additional security associated with conventional chaotic communication [9,13,14,44,45] by exploiting the unpredictable, randomlike but deterministic [46] nature of chaotic signals to encrypt the transmitted information. The latter approach

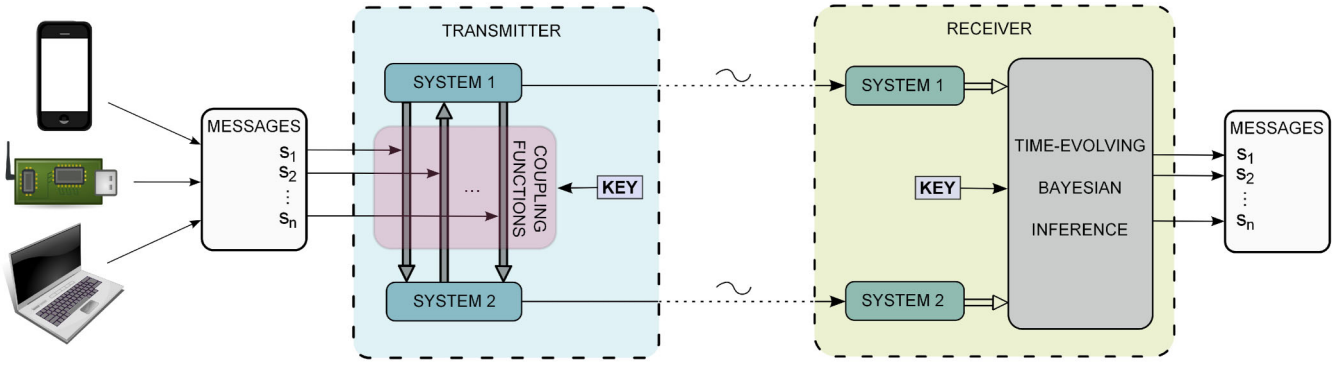

FIG. 1 Schematic of the communications scheme. Messages $s_1, \ldots, s_n$ are encrypted through their modulation of the coupling functions connecting the two oscillators of the transmitter. Only two signals are transmitted through the public domain. For the particular realization of the cipher discussed in the text, Eqs. (5) and (6), they are x_1 and y_2. The receiver consists of the same kind of oscillators and the same coupling functions (effectively forming the privately shared key) as the transmitter and uses time-evolving Bayesian inference to reconstruct $s_1, \ldots, s_n$.

has been popular mainly because of the high controllability of chaos and the concept of complete synchronization [47,48]. We emphasize, however, that the use of chaotic systems here is inessential. Parameter modulation of an attractor has been used in a number of earlier communication methods [13,49]; however, the modulation of different coupling functions as applied here provides for a much larger number of parameter encryption possibilities.

B. Time-evolving Bayesian inference

We outline succinctly the application of time-evolving Bayesian inference [8] for the reconstruction of the information encrypted within the interactions between the dynamical systems. The model to be inferred is described by the stochastic differential equation [Eq. (1)].

The inference is performed in state space, and the base functions $\mathbf{f}(\mathbf{x}_i, \mathbf{x}_j|\mathbf{c})$ consist of the systems base functions $\mathbf{g}(\mathbf{x}_i)$ and the all-important coupling functions $\mathbf{q}(\mathbf{x}_i, \mathbf{x}_j)$, which are specified by the encryption key. Inferential methods are conventionally used to treat physical problems where the model (i.e., its base functions) is hidden or unknown. In contrast to this, in our proposed application to secure communication, we know the model and the base functions *a priori*.

If $2 \times M$ time series $\mathcal{X} = \{\mathbf{x}_n \equiv \mathbf{x}(t_n)\}$ $(t_n = nh)$ are provided as inputs, the fundamental task for the Bayesian dynamical inference [8,30] is to reveal the unknown model parameters $\mathcal{M} = \{\mathbf{c}, \mathbf{D}\}$. The inference relies on the application of the Bayes theorem, which is used to calculate the so-called *posterior* density $p_{\mathcal{X}}(\mathcal{M}|\mathcal{X})$ of the unknown parameters $\mathcal{M}$, given a *prior* density $p_{\text{prior}}(\mathcal{M})$ that encloses previous knowledge of the unknown parameters based on observations, and the *likelihood* function $\ell(\mathcal{X}|\mathcal{M})$, i.e., the conditional probability density to observe $\mathcal{X}$ given choice $\mathcal{M}$ of the dynamical model:

$$p_{\mathcal{X}}(\mathcal{M}|\mathcal{X}) = \frac{\ell(\mathcal{X}|\mathcal{M}) p_{\text{prior}}(\mathcal{M})}{\int \ell(\mathcal{X}|\mathcal{M}) p_{\text{prior}}(\mathcal{M}) d\mathcal{M}}.$$

If the sampling is dense enough, the problem can conveniently be solved using the Euler midpoint $\mathbf{x}^*_n = (\mathbf{x}_{n+1} + \mathbf{x}_n)/2$ discretization of Eq. (1):

$$\mathbf{x}_{i,n+1} = \mathbf{x}_{i,n} + h f(\mathbf{x}^*_{i,n}, \mathbf{x}^*_{j,n}|\mathbf{c}) + h\sqrt{\mathbf{D}}\mathbf{z}_n, \tag{2}$$

where $\mathbf{z}_n$ is the stochastic integral of the noise term over time: $\mathbf{z}_n \equiv \int_{t_n}^{t_{n+1}} \mathbf{z}(t)dt = \sqrt{h}\mathbf{H}\boldsymbol{\xi}_n$, for the $\mathbf{H}$ matrix that satisfies the Cholesky decomposition $\mathbf{H}\mathbf{H}^{\mathbf{T}} = \mathbf{D}$.

The noise under consideration $\mathbf{z}_n$ is statistically independent and the likelihood is given by a product over n of the probability of observing $\mathbf{x}_{n+1}$ at each time. The joint probability density of $\mathbf{z}_n$ is used to find the joint probability density of the process in respect to $\mathbf{x}_{n+1} - \mathbf{x}_n$ by imposing $P(\mathbf{x}_{n+1}) = \det(J^{\mathbf{x}}_{\boldsymbol{\xi}}) P(\xi^i)$, where $J^{\mathbf{x}}_{\boldsymbol{\xi}}$ is the Jacobian term of the transformation of variables that can be calculated from the known polynomial base functions. For high sampling rates ($h \to 0$), the determinant of the Jacobian can be well approximated by the product of its diagonal terms: $\det(J^{\mathbf{x}_k(t_n)}_{\xi_k(t_n)}) \approx \prod_l \frac{\partial \mathbf{f}_k(\mathbf{x}_{\cdot,n})}{\partial \mathbf{x}}$. Here, and in what follows, the dot index in $\mathbf{x}_{\cdot}$ is substituted with the relevant index. The base functions are linearly parametrized as $\mathbf{f}(\mathbf{x}_{\cdot}|\mathbf{c}) = \mathbf{c}\mathbf{f}(\mathbf{x}_{\cdot})$. The negative log-likelihood function $S = -\ln \ell(\mathcal{X}|\mathcal{M})$ is then expressed as

$$S = \frac{N}{2}\ln|\mathbf{D}| + \frac{h}{2}\sum_{n=0}^{N-1}\Bigg(\mathbf{c}_k \frac{\partial \mathbf{f}_k(\mathbf{x}_{\cdot,n})}{\partial \mathbf{x}} + [\dot{\mathbf{x}}_n - \mathbf{c}_k\mathbf{f}_k(\mathbf{x}^*_{\cdot,n})]^T(\mathbf{D}^{-1})[\dot{\mathbf{x}}_n - \mathbf{c}_k\mathbf{f}_k(\mathbf{x}^*_{\cdot,n})]\Bigg), \tag{3}$$

with $\dot{\mathbf{x}}_n = (\mathbf{x}_{n+1} - \mathbf{x}_n)/h$ and implicit summation over the repeated index k.

Next, we assume the prior probability to be a multivariate normal distribution. This, together with the specific form of the log-likelihood [Eq. (3)], ensures that the posterior probability will be a multivariate normal distribution. Given such a distribution as a prior for the parameters $\mathbf{c}$, with mean $\bar{\mathbf{c}}$, and covariance matrix $\Sigma_{\text{prior}} \equiv \Xi^{-1}{}_{\text{prior}}$, the stationary point of S is calculated recursively from

$$\begin{aligned}
\mathbf{D} &= \frac{h}{N}(\dot{\mathbf{x}}_n - \mathbf{c}_k\mathbf{f}_k(\mathbf{x}^*_{\cdot,n}))^T(\dot{\mathbf{x}}_n - \mathbf{c}_k\mathbf{f}_k(\mathbf{x}^*_{\cdot,n})),\\
\mathbf{c}_k &= (\Xi^{-1})_{kw}\mathbf{r}_w,\\
\mathbf{r}_w &= (\Xi_{\text{prior}})_{kw}\mathbf{c}_w + h\mathbf{f}_k(\mathbf{x}^*_{\cdot,n})(\mathbf{D}^{-1})\dot{\mathbf{x}}_n - \frac{h}{2}\frac{\partial \mathbf{f}_k(\mathbf{x}_{\cdot,n})}{\partial \mathbf{x}},\\
\Xi_{kw} &= (\Xi_{\text{prior}})_{kw} + h\mathbf{f}_k(\mathbf{x}^*_{\cdot,n})(\mathbf{D}^{-1})\mathbf{f}_w(\mathbf{x}^*_{\cdot,n}),
\end{aligned} \tag{4}$$

where summation over $n = 1, \ldots, N$ is assumed and the summation over repeated indices k and w is again implicit. The initial prior is set to be the noninformative flat normal distribution given by $\Xi_{\text{prior}} = 0$ and $\bar{\mathbf{c}}_{\text{prior}} = 0$. For a given sequential block of data $\mathcal{X}$, one applies Eq. (4) to evaluate the posterior multivariate probability $\mathcal{N}_{\mathcal{X}}(c|\bar{c}, \Xi)$, which explicitly defines the probability density of each parameter set of the model [Eq. (1)].

The main idea of our communication scheme is to encrypt the information in a specific time evolution of the parameters. Therefore, the inference technique needs to follow the time evolution of the parameter set $\mathbf{c}$ while separating these effects from the unavoidable noise. In order to achieve this, we modify [8] the propagation procedure between the covariance of the current posterior Σ^n_{post} and the next prior $\Sigma^{n+1}_{\text{prior}}$. We define a squared symmetric positive definite matrix Σ_{diff}, which prescribes how much each parameter diffuses normally. Thus, the next prior probability of the parameters is the convolution of two current normal multivariate distributions, Σ_{post} and Σ_{diff}:

$\Sigma^{n+1}_{\text{prior}} = \Sigma^{n}_{\text{post}} + \Sigma^{n}_{\text{diff}}$. The diffusion matrix is expressed as $(\Sigma_{\text{diff}})_{i,j} = \rho_{ij}\sigma_i\sigma_j$, where σ_i is the standard deviation of the diffusion of c_i in the time window t_w, and ρ_{ij} is the correlation between the change in parameters c_i and c_j. We consider Σ_{diff} to be such that there is no change of correlation between parameters ($\rho_{ij} = \delta_{ij}$) and that each σ_i is a known fraction of the relevant standard deviation from the posterior $\sigma_i = p_w(\sigma^n_{\text{post}})_i$, where p_w indicates that the parameter p refers to a window of length t_w. Moreover, in the proposed communication scheme, it is known beforehand that some, but not all, of the parameters are time evolving. Thus, one can use selective propagation where not all, but only the selected correlations ρ_{ii} from the diagonal, have nonzero values.

IV. AN EXAMPLE

As an example of the cipher [50] in action, we take the transmitter to consist of a Rössler oscillator [Eq. (5), left] coupled to a Lorenz [Eq. (5), right] system:

$$\begin{aligned} \dot{x}_1 &= 2 + x_1(x_2 - 4) + \xi_1, & \dot{y}_1 &= 10y_2 - 10y_1 + \xi_2, \\ \dot{x}_2 &= -x_1 - x_3, & \dot{y}_2 &= -y_1y_3 - y_2 + s_0(t)y_1 \\ & & & \quad + s_1(t)x_2x_3 + s_2(t)x_3^2 \\ \dot{x}_3 &= x_2 + 0.45x_3, & \dot{y}_3 &= y_1y_2 - 2.67y_3 + \xi_3. \end{aligned} \tag{5}$$

Only the signals x_1 and y_2 are transmitted, and they completely synchronize [47] the Rössler and Lorenz systems at the receiver:

$$\begin{aligned} u_1 &= x_1, & \dot{w}_1 &= 10y_2 - 10w_1 + \xi_4, \\ \dot{u}_2 &= -x_1 - u_3, & w_2 &= y_2, \\ \dot{u}_3 &= u_2 + 0.45u_3, & \dot{w}_3 &= w_1y_2 - 2.67w_3 + \xi_5. \end{aligned} \tag{6}$$

The information signals acting as time-dependent nonautonomous terms are given by binary pseudorandom sequence signals $s_0(t) = \{0, 28\}$, $s_1(t) = \{1.6, 2.4\}$, and $s_2(t) = \{0, 0.6\}$. We note in passing that continuous signals can be encrypted with equal facility. The noise sources $\xi_1, ..., \xi_5$, acting on different levels, are assumed to be white, Gaussian, and of the same intensity $D = 0.05$. The differentiation was rescaled to $d/d\tau$, with $\tau = t/2000$ for the Rössler and $\tau = t/1000$ for the Lorenz oscillator. The signals are generated by numerical simulation, but analogue electrical circuits [21] can equally be used. Bayesian inference was applied to the receiver signals $\mathbf{u}$ and $\mathbf{w}$ using the same base functions as the right-hand side of the transmitter model [Eq. (5)].

The Rössler and Lorenz oscillators are unidirectionally coupled through the information signals s_1 and s_2 and, depending on signal s_0, they can be either nonsynchronized or synchronized. In Figs. 2(a)–2(c), the driven oscillator $\mathbf{y}$ for $s_0\{0\} = 0$ is asymptotically stable and the two oscillators can undergo generalized synchronization [51]. The latter statement can be proved by application of the second Lyapunov stability method to the dynamical error system $\mathbf{e} = \mathbf{y} - \mathbf{y}'$, where $\mathbf{y}'$ is an identical copy of $\mathbf{y}$ with different initial conditions. By using the Lyapunov function $L = 1/2(e_1^2/10 + e_2^2 + e_3^2)$, one can show that $\dot{L} = -(e_1 - \frac{e_2}{2})^2 - \frac{3}{4}e_2^2 - 2.67e_3^2 < 0$, which proves that the driven system $\mathbf{y}$ is globally asymptotically stable and the two oscillators $\mathbf{x}$ and $\mathbf{y}$ are synchronized. The same phenomenon can be detected by evaluation of the largest Lyapunov exponent [52] (or alternatively by basin stability [53]) of the driven oscillator model [Eq. (5)] using the inferred parameters. If the exponents λ are negative, the system $\mathbf{y}$ is asymptotically stable and generalized synchronization occurs. By evaluating the Lyapunov exponents for each sequential block of data from the Bayesian inference,

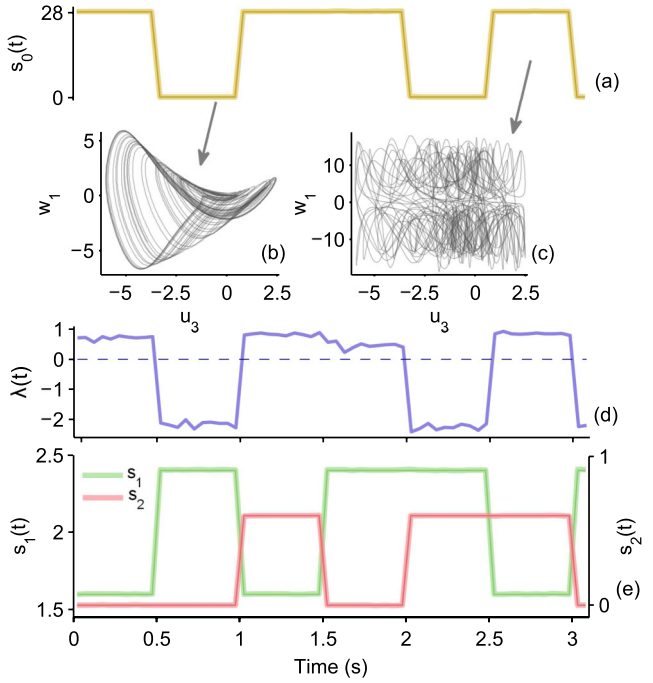

FIG. 2 The communication procedure based on coupled chaotic oscillators [Eqs. (5) and (6)]. (a) The transmitted binary signal $s_0(t)$ acting as a ρ variable in the Lorenz oscillator. Lissajous curves qualitatively indicating the existence of generalized synchronization during (b) synchronized and (c) nonsynchronized intervals. The gray arrows point to synchronization intervals in the $s_0(t)$ signal. (d) The largest Lyapunov exponent detected from the driven Lorenz oscillator serves as an index of time-evolving generalized synchronization. (e) Simultaneously transmitted signals $s_1(t)$ and $s_2(t)$. For comparison, the original signals $s_0(t)$, $s_1(t)$, and $s_2(t)$ are presented in dark color below the received ones shown in light transparent color in (a) and (e)—note that in some intervals they are indistinguishable.

one can follow the evolution of the synchronization and the associated transitions as illustrated in Fig. 2(d).

The binary information signal $s_0(t)$ acts on and changes the attractor properties of the Lorenz oscillator alone. Hence, this communication information is insecure and can be broken by the use of standard attack procedures [54]. In this way, the $s_0(t)$ signal serves more as decoy information and a control signal that takes the two oscillators through qualitative transitions of generalized synchronization. The two information signals $s_1(t)$ and $s_2(t)$, on the other hand, are encrypted through the weak and nonlinear interactions, providing a complicated dynamical mixing that is highly resistant to the standard attacks [54,55]. On top of this, the transitions in or out of generalized synchronization bring additional impediments to potential attacks on the interactions via which the information is being conveyed. Despite these complexities, Bayesian inference can detect and separate the two signals precisely, as shown for $s_1(t)$ and $s_2(t)$ in Fig. 2(e).

Note that the proposed communication technique can transmit more than one information signal simultaneously. This can be used to provide a higher level of security or inherently to allow multiplexing.

Of crucial importance is the fact of an intruder being ignorant of the form and number of the coupling functions (in particular) and, thus, being unable to decrypt the signals in any simple way. The choice of the form of coupling functions comes from a set of functions that is *not bounded*. This property is highly desirable for constructing a private encryption key. In theory, it enables the communications framework to resist brute-force attacks, and in practice [43], it allows for the use of dynamical keys or dynamical physical unclonable functions (PUFs). The latter could be implemented with analogue technology, exploiting the unbounded continuum of the key. At relatively small computational expense, one could include additional nonlinear coupling functions (see the Appendix, showing the coupling-function encryption of ten binary information signals), thereby increasing the complexity in the encryption and making the communications even harder to break.

A. Noise tolerance

In practical applications, there will be noise from various sources that is potentially damaging to the communication. The proposed Bayesian framework is by definition stochastic inference, Eq. (1), and naturally separates the effect of the noise from what is inferred to be internal deterministic dynamics. To illustrate this advantage, we first used the communication model [Eqs. (5) and (6)] for sending only one pseudorandom binary signal $s_1(t) = \{-2.5, 2.5\}$. The modified terms at the transmitter are now expressed as $\dot{y}_2 = -y_1 y_3 - y_2 + 28 y_1 + s_1(t) x_2 x_3$. The effect of channel noise on the success of the information transfer is shown in Figs. 3(a) and 3(b). It is evident from the appearance of small errors that corruption of the two binary states occurs at around and below ~4 dB. This is well below the 15 dB SNR of a digital transmission or the 40 dB SNR of a wireline communication channel in a real environment [55], thereby demonstrating the high noise tolerance of our scheme.

Second, in order to confirm the high noise resistance of our scheme compared to that of other known encryption schemes, we investigate how noise affects signal-masking [13] communication. This case can act as a general example of a whole class of secure communications schemes based on complete synchronization [47]. It also corresponds to how we transmit and recover the systems in the coupling-function scheme, before the Bayesian inference is applied. For this reason, we masked the y_2 signal at the transmitter with a binary signal $s_3(t) = \{0, 5\}$ as $\dot{y}_2 = -y_1 y_3 - y_2 + 28 y_1 + s_3(t)$, and we applied the relevant recovery procedure [13]. The effect of channel noise on the success of information transmission is shown in Fig. 3(c):

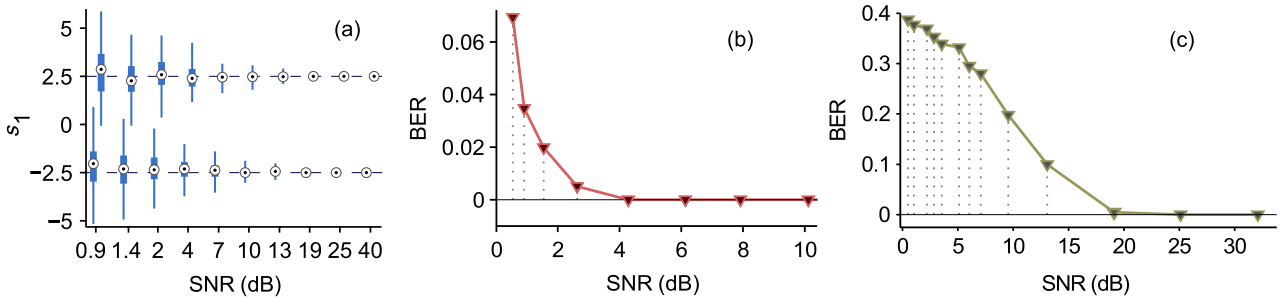

FIG. 3 Example of how noise affects the communication of a binary signal using the model [Eqs. (5) and (6)]. (a) Deviations of the demodulated signal from the initial binary states due to noise, presented as compact box plots (in terms of descriptive statistics: median, quartiles, max, and min) as a function of signal-to-noise ratio (SNR). (b) Bit-error rate (BER) of the coupling-function scheme as a function of SNR. (c) For comparison, BER of the signal-masking scheme as a function of SNR. In (a) and (b) the transmitted signal for coupling-function encryption has the two binary values $s_1(t) = \{-2.5, 2.5\}$, while in (c) for signal-masking encryption, $s_3(t) = \{0, 5\}$. In each run, 10^3 randomly ordered binary symbols are sent.

erroneous detection of the binary information occurs at around and below ∼20 dB. The fact that the coupling-function scheme is noise resistent down to 4 dB points to its superiority over signal-masking schemes and emphasizes the benefit of the Bayesian inference used within our scheme.

V. DISCUSSION AND CONCLUSION

The specific model used here is just as an illustrative example of the cipher, while the scheme itself is inherently modular. The choice that the oscillators be self-sustained provides optimal conditions for encryption and dynamical mixing, but it is not essential. The Bayesian inference can function regardless. Limit-cycle oscillators (e.g., Van der Pol oscillators) can be used, with the information messages encrypted in a number of different nonlinear coupling functions. Using chaotic systems can add to the difficulties experienced by an intruder because the transmitted chaotic signals have randomlike characteristics. This chaotic mixing is additional to the encryption provided by the coupling functions; we again emphasize that the use of chaos is not essential for our new scheme, but just a potentially useful addition that can add further difficulty for an illicit decryptor. Similarly, one might choose to use chaotic maps in order to provide for faster transfer with reduced resource requirements. Within the Bayesian framework, Eq. (2) is already discrete, which would allow the inference to be adjusted for use with discrete maps. Finally, the transmitter and receiver could consist of more than two systems, and bidirectional multivariate coupling can also be used (see the Appendix).

We anticipate that coupling-function encryption—thus far just a theoretical concept—will have great impact on a diversity of experimental implementations, e.g., on those mentioned above [14,18,20–22]. Such systems can themselves be very complex, and changing some of their intrinsic properties can easily lead to qualitative changes in their nature. This can be avoided by encrypting the information through weak couplings. In this way, a number of information signals can be encrypted simultaneously while not affecting qualitatively the existence or function of the systems that are being used. The proposed decryption method can then safely and reliably recover the transmitted information.

In summary, our new class of communications enables the secure transfer of several information signals simultaneously. Inspired by cardiorespiratory interactions [8,25,30,56], it is made possible by recent developments in Bayesian inference. These enable us to follow the time evolution of the modulation of different nonlinear coupling functions to which a potential intruder does not have access. The encrypting key space is unbounded. The facility of sending multiple signals simultaneously allows the multiplexing and sharing of the same resources. Because the Bayesian procedure involves stochastic inference, the communications scheme is inherently resistent to external noise. This makes it suitable for implementation not only for landline (e.g., telephone) but also for mobile and wireless communications, where the level of external interference tends to be higher. Our scheme is highly modular and is readily extendable to support far more complex and diverse communications applications than the examples discussed here, within the same general framework.

ACKNOWLEDGMENTS

Our grateful thanks are due to P. Clemson, L. Kocarev, Y. A. Pashkin, A. Risteski, and R. J. Young for valuable discussions. This work was supported by the Engineering and Physical Sciences Research Council (UK) (Grant No. EP/100999X1).

APPENDIX: ENCRYPTION AND DECRYPTION OF TEN BINARY INFORMATION SIGNALS

We now present an additional example, based on the use of two coupled Lorenz systems for simultaneous transmission of ten binary signals encrypted in separate, linearly independent, coupling functions. We use this example to demonstrate some points and generalizations about the application and the modularity of the communications framework. We also discuss some of its properties and preferred modes of operation.

The main concept that facilitates the security of our scheme is the form of the coupling functions. For clarity of presentation, the example in the main text shows only two unidirectional coupling functions. In general, however, there can be a larger number of bidirectional and multivariate coupling functions. In the following example, we use ten nonlinear coupling functions, each of different form: $Q=\{\cos(y_1)x_2, y_2^2/y_3, x_1y_2/y_3, \sqrt{y_3}, x_2^2/y_3, x_2x_3, x_1^3, \sin(x_3), x_3^2, x_2^2\}$. Note that the form of a coupling function refers to the algebraic *function*, e.g., as in Q, and not just to the parameter value scaling a particular function. The number of coupling functions depends on the specific application (i.e., on the number of information channels and devices connected to the transmitter), and will always be finite, e.g., 10, 20, …. In contrast, the form of the coupling functions can be very different, and their choice is unbounded. For example, one can add to the Q set the function combinations $\cos(y_1)x_2\sin(x_3)$, $x_3^2x_1y_2/y_3$, …, or one can include some entirely new functions—again leading to choice from an unbounded set of functions. This choice of which particular functions are to be used acts as a key that is privately shared between the transmitter and the receiver. The information about the choice of coupling functions can be stored on a chip, similarly to the subscriber identity module (SIM) card for mobile phones, and can be shared exclusively between the transmitter and the receiver in each individual device realization.

We consider implementation of the cipher with two coupled chaotic Lorenz systems. The transmitter is thus given by the first Lorenz system with five coupling functions acting in x_1:

$$\begin{aligned}\dot{x}_1 &= 10x_2 - 10x_1 + s_1(t)\cos(y_1)x_2 + s_2(t)y_2^2/y_3 \\ &\quad + s_3(t)x_1y_2/y_3 + s_4(t)\sqrt{y_3} + s_5(t)x_2^2/y_3, \\ \dot{x}_2 &= 28x_1 - x_1x_3 - x_2, \\ \dot{x}_3 &= x_1x_2 - 2.67x_3, \end{aligned} \tag{A1}$$

together with the second Lorenz system with five coupling functions acting in y_2:

$$\begin{aligned}\dot{y}_1 &= 10y_2 - 10y_1 + \xi_1, \\ \dot{y}_2 &= 28y_1 - y_1y_3 - y_2 + s_6(t)x_2x_3 + s_7(t)x_1^3 + \\ &\quad + s_8(t)\sin(x_3) + s_9(t)x_3^2 + s_{10}(t)x_2^2, \\ \dot{y}_3 &= y_1y_2 - 2.67y_3. \end{aligned} \tag{A2}$$

Only the signals x_1 and y_2 are transmitted through the public channel. On the receiver side, the two chaotic systems are completely synchronized [47]: the system **u**, through x_1, becomes effectively identical to the system **x**,

$$\begin{aligned} u_1 &= x_1, \\ \dot{u}_2 &= 28x_1 - x_1u_3 - u_2, \\ \dot{u}_3 &= x_1u_2 - 2.67u_3 + \xi_2, \end{aligned} \tag{A3}$$

and the system **w**, through y_2, becomes effectively identical to system **y**,

$$\begin{aligned} \dot{w}_1 &= 10y_2 - 10w_1, \\ w_2 &= y_2, \\ \dot{w}_3 &= w_1y_2 - 2.67w_3 + \xi_3. \end{aligned} \tag{A4}$$

The binary information signals acting as time-dependent nonautonomous terms are given by the two level values, $s_4(t) = \{0, 1.5\}$, $s_5(t) = \{0, 0.4\}$, and the rest are equal, $s_1(t) = s_2(t) = s_3(t) = s_6(t) = s_7(t) = s_8(t) = s_9(t) = s_{10}(t) = \{0, 0.6\}$. The noise sources $\xi_1, ..., \xi_3$ are assumed to be white and Gaussian $\langle \xi(t)\xi(\tau)\rangle = \delta(t-\tau)D$ and of the same noise intensity $D = 0.05$. To speed up the systems, we change the frequency of oscillation by rescaling the differentiation to $d/d\tau$ with $\tau = t/1000$ for the first Lorenz and $\tau = t/1300$ for the second Lorenz oscillator. The different rescaling ensures that the two chaotic systems have different frequencies and are harder to mutually (in the generalized sense) synchronize. This allows the couplings for the $s_i(t)$ signals to have larger values, without mutually synchronizing the transmitter's two oscillators. Bayesian inference [8,30,57,58] is applied to the received signals **u** and **w** on the receiver side using the same polynomial base functions as the right-hand side of the transmitter model [Eqs. (A1)) and (A2)], with $p_w = 0.2$ and a window of $t_w = 25$ ms.

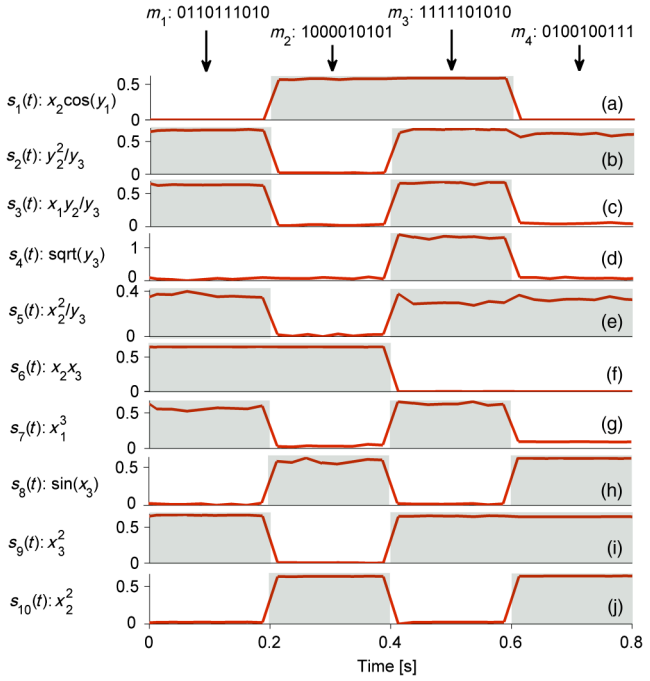

FIG. 4 Transmission of ten pseudorandom binary signals encrypted in different coupling functions. The high values (binary '1') at the transmitter, prior to encrypting, are indicated by grey shading. The received signals, after decrypting, are shown by red lines, each of which (a-j) represents one information signal $s_i(t)$. The particular coupling functions that were used for encrypting each signal are indicated on the ordinate axis. Each bit is transmitted during an interval of 0.2 s, and four bits are transmitted in total for each signal e.g., $s_7(t) \rightarrow 1010$. The information could correspond either to ten separate serially-encoded messages, or to a single 10-bit parallel-encoded message, but all of it is being transmitted simultaneously. The bits are indicated by $m_1 - m_4$ on the top of the figure.

The results of the 10-bit binary transmission are demonstrated in Fig. 4. We send four pseudorandom 10-bit messages $m_1 = 0110111010$, $m_2 = 1000010101$, $m_3 = 1111101010$, and $m_4 = 0100100111$. For every message, we send ten signals $s_1(t)$–$s_{10}(t)$ simultaneously. Therefore, each signal has a length of four bits, for example, $s_{10}(t) \rightarrow 0101$. The detected signals after transmission (Fig. 4) indicate that the communication is accurate, with consistent and precisely detected messages.

Thus, the communication technique is able to transmit more than one (in this case ten) information signals simultaneously. This property is very beneficial for any real application because, inherently, it allows multiplexing —multiplexing being the conventional method of sharing an expensive resource by sending multiple information signals simultaneously [59]. Similarly, in our scheme, as

long as the coupling base functions are linearly independent, Bayesian inference is able to separate the simultaneously sent signals $s_i(t)$ at the receiver end.

One should note that, for the example in the main text, we have generalized synchronization [51] within the transmitter (receiver), and not complete synchronization [47]. The latter is also used for the transmission procedure in this example, and it only applies between the transmitter and the receiver. The transmission does not have to be exclusively through complete synchronization. With the use of chaotic maps, this mode can be avoided or one could use a key function for coding and decoding the chaotic signals before and after transmission. The onset of generalized synchronization between the coupled systems within the transmitter can be excluded totally. In fact, the nonsynchronized case, where the coupled systems do not form an attractor, is to be preferred for secure transmission. In such cases, methods of attack based on attractor properties will fail.

Another important property for practical applications is the speed of communication. In our framework, this depends on the time scales of the coupled systems and the speed of the Bayesian inference. Unlike other statistical methods (e.g., Granger causality or transfer entropy), which detect statistical effects, the Bayesian technique infers dynamical mechanisms and requires substantially less data. With each sequential block, the Bayesian inference exploits the dynamical model and the acquired prior knowledge, allowing the use of smaller blocks of data and better time resolution. The time scale of the "carrier signal" should, in general, be longer than the time scales of the information signals. The relationship between them has to be determined on a case-by-case basis [60]. For the proposed communication scheme, however, this does not pose a problem because the time scales are known *a priori*.

[1] J. F. V. Vincent, O. A. Bogatyreva, N. R. Bogatyrev, A. Bowyer, and A. Pahl, *Biomimetics: Its Practice and theory*, J. R. Soc., Interface **3**, 471 (2006).

[2] B. Bhushan, *Biomimetics: Lessons from Nature—An Overview*, Phil. Trans. R. Soc. A **367**, 1445 (2009).

[3] M. Sarikaya, *Biomimetics: Materials Fabrication Through Biology*, Proc. Natl. Acad. Sci. U.S.A. **96**, 14183 (1999).

[4] D. Lentink, *Biomimetics: Flying Like a Fly*, Nature (London) **498**, 306 (2013).

[5] M. Sarikaya, C. Tamerler, A. K. Jen, K. Schulten, and F. Baneyx, *Molecular Biomimetics: Nanotechnology through Biology*, Nat. Mater. **2**, 577 (2003).

[6] L. P. Lee and R. Szema, *Inspirations from Biological Optics for Advanced Photonic Systems*, Science **310**, 1148 (2005).

[7] A. R. Parker and H. E. Townley, *Biomimetics of Photonic Nanostructures*, Nat. Nanotechnol. **2**, 347 (2007).

[8] T. Stankovski, A. Duggento, P. V. E. McClintock, and A. Stefanovska, *Inference of Time-Evolving Coupled Dynamical Systems in the Presence of Noise*, Phys. Rev. Lett. **109**, 024101 (2012).

[9] G. D. Van Wiggeren and R. Roy, *Communication with Chaotic Lasers*, Science **279**, 1198 (1998).

[10] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, *Secure Communication: Quantum Cryptography with a Photon Turnstile*, Nature (London) **420**, 762 (2002).

[11] C. C. Wen Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, *Device-Independent Quantum Key Distribution with Local Bell Test*, Phys. Rev. X **3**, 031006 (2013).

[12] X. Liu, S. Chandrasekhar, P. J. Winzer, A. R. Chraplyvy, R. W. Tkach, B. Zhu, T. F. Taunay, M. Fishteyn, and D. J. DiGiovanni, *Scrambled Coherent Superposition for Enhanced Optical Fiber Communication in the Nonlinear Transmission Regime*, Opt. Express **20**, 19088 (2012).

[13] K. M. Cuomo and A. V. Oppenheim, *Circuit Implementation of Synchronized Chaos with Applications to Communications*, Phys. Rev. Lett. **71**, 65 (1993).

[14] 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, *Chaos-Based Communications at High Bit Rates Using Commercial Fibre-Optic Links*, Nature (London) **438**, 343 (2005).

[15] L. B. Kish, *Totally Secure Classical Communication Utilizing Johnson(-like) Noise and Kirchoff's Law*, Phys. Lett. A **352**, 178 (2006).

[16] C. H. Bennett, *Quantum Information and Computation*, Nature (London) **404**, 247 (2000).

[17] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber*, Phys. Rev. X **2**, 041010 (2012).

[18] S. Petit-Watelot, J. Kim, A. Ruotolo, R. M. Otxoa, K. Bouzehouane, J. Grollier, A. Vansteenkiste, B. Van de Wiele, V. Cros, and T. Devolder, *Commensurability and Chaos in Magnetic Vortex Oscillations*, Nat. Phys. **8**, 682 (2012).

[19] X. Liu, A. R. Chraplyvy, P. J. Winzer, R. W. Tkach, and S. Chandrasekhar, *Phase-Conjugated Twin Waves for Communication beyond the Kerr Nonlinearity Limit*, Nat. Photonics **7**, 560 (2013).

[20] E. Lee, K. Lee, C. Liu, G. S. Kulkarni, and Z. Zhong, *Flexible and Transparent All-Graphene Circuits for Quaternary Digital Modulations*, Nat. Commun. **3**, 1018 (2012).

[21] D. G. Luchinsky and P. V. E. McClintock, *Irreversibility of Classical Fluctuations Studied in Analogue Electrical Circuits*, Nature (London) **389**, 463 (1997).

[22] Y. A. Pashkin, T. Yamamoto, O. Astafiev, Y. Nakamura, D. V. Averin, and J. S. Tsai, *Quantum Oscillations in Two Coupled Charge Qubits*, Nature (London) **421**, 823 (2003).

[23] D. Rudrauf, A. Douiri, C. Kovach, J. P. Lachaux, D. Cosmelli, M. Chavez, C. Adam, B. Renault, J. Martinerie, and M. L. Van Quyen, *Frequency Flows and the Time-Frequency Dynamics of Multivariate Phase Synchronization in Brain Signals*, NeuroImage **31**, 209 (2006).

[24] K. C. Creager, *Inner Core Rotation Rate from Small-Scale Heterogeneity and Time-Varying Travel Times*, Science **278**, 1284 (1997).

[25] Y. Shiogai, A. Stefanovska, and P. V. E. McClintock, *Nonlinear Dynamics of Cardiovascular Ageing*, Phys. Rep. **488**, 51 (2010).

[26] D. Khodagholy *et al.*, *In Vivo Recordings of Brain Activity Using Organic Transistors*, Nat. Commun. **4**, 1575 (2013).
[27] Y. F. Suprunenko, P. T. Clemson, and A. Stefanovska, *Chronotaxic Systems: A New Class of Self-Sustained Nonautonomous Oscillators*, Phys. Rev. Lett. **111**, 024101 (2013).
[28] K. J. Friston, *Bayesian Estimation of Dynamical Systems: An Application to fMRI*, NeuroImage **16**, 513 (2002).
[29] U. von Toussaint, *Bayesian Inference in Physics*, Rev. Mod. Phys. **83**, 943 (2011).
[30] V. N. Smelyanskiy, D. G. Luchinsky, A. Stefanovska, and P. V. E. McClintock, *Inference of a Nonlinear Stochastic Model of the Cardiorespiratory Interaction*, Phys. Rev. Lett. **94**, 098101 (2005).
[31] A. T. Winfree, *Biological Rhythms and the Behavior of Populations of Coupled Oscillators*, J. Theor. Biol. **16**, 15 (1967).
[32] T. Murayama, *Coupling Function Between Solar-Wind Parameters and Geomagnetic Indexes*, Rev. Geophys. **20**, 623 (1982).
[33] R. G. Cai and A. Z. Wang, *Cosmology with Interaction Between Phantom Dark Energy and Dark Matter and the Coincidence Problem*, J. Cosmol. Astropart. Phys. 3 (2005) 2.
[34] I. Z. Kiss, C. G. Rusin, H. Kori, and J. L. Hudson, *Engineering Complex Dynamical Structures: Sequential Patterns and Desynchronization*, Science **316**, 1886 (2007).
[35] M. G. Rosenblum and A. S. Pikovsky, *Detecting Direction of Coupling in Interacting Oscillators*, Phys. Rev. E **64**, 045202 (2001).
[36] K. Hlaváčkováá-Schindler, M. Paluš, M. Vejmelka, and J. Bhattacharya, *Causality Detection Based on Information-Theoretic Approaches in Time Series Analysis*, Phys. Rep. **441**, 1 (2007).
[37] M. Staniek and K. Lehnertz, *Symbolic Transfer Entropy*, Phys. Rev. Lett. **100**, 158101 (2008).
[38] A. Bahraminasab, F. Ghasemi, A. Stefanovska, P. V. E. McClintock, and H. Kantz, *Direction of Coupling from Phases of Interacting Oscillators: A Permutation Information Approach*, Phys. Rev. Lett. **100**, 084101 (2008).
[39] B. Kralemann, L. Cimponeriu, M. Rosenblum, A. Pikovsky, and R. Mrowka, *Uncovering Interaction of Coupled Oscillators from Data*, Phys. Rev. E **76**, 055201 (2007).
[40] I. T. Tokuda, S. Jain, I. Z. Kiss, and J. L. Hudson, *Inferring Phase Equations from Multivariate Time Series*, Phys. Rev. Lett. **99**, 064101 (2007).
[41] J. Miyazaki and S. Kinoshita, *Determination of a Coupling Function in Multicoupled Oscillators*, Phys. Rev. Lett. **96**, 194101 (2006).
[42] I. Z. Kiss, Y. Zhai, and J. L. Hudson, *Predicting Mutual Entrainment of Oscillators with Experiment-Based Phase Models*, Phys. Rev. Lett. **94**, 248301 (2005).
[43] Subject to U. K. patent application No. GB1314114.8, Lancaster University, filed 7 2013.
[44] L. Kocarev and U. Parlitz, *General Approach for Chaotic Synchronization with Applications to Communication*, Phys. Rev. Lett. **74**, 5028 (1995).
[45] Y. C. Hung and C. K. Hu, *Chaotic Communication via Temporal Transfer Entropy*, Phys. Rev. Lett. **101**, 244102 (2008).
[46] J. P. Crutchfield, *Between Order and Chaos*, Nat. Phys. **8**, 17 (2012).
[47] L. M. Pecora and T. L. Carroll, *Synchronization in Chaotic Systems*, Phys. Rev. Lett. **64**, 821 (1990).
[48] S. Boccaletti, C. Grebogi, Y. C. Lai, H. Mancini, and D. Maza, *The Control of Chaos: Theory and Applications*, Phys. Rep. **329**, 103 (2000).
[49] U. Parlitz and L. Kocarev, *Multichannel Communication Using Autosynchronization*, Int. J. Bifurcation Chaos Appl. Sci. Eng. **06**, 581 (1996).
[50] Note that the nature of our secure communications scheme is that of a cipher rather than a secure key exchange protocol.
[51] L. Kocarev and U. Parlitz, *Generalized Synchronization, Predictability, and Equivalence of Unidirectionally Coupled Dynamical Systems*, Phys. Rev. Lett. **76**, 1816 (1996).
[52] J. P. Eckmann and D. Ruelle, *Ergodic Theory of Chaos and Strange Attractors*, Rev. Mod. Phys. **57**, 617 (1985).
[53] P. J. Menck, J. Heitzig, N. Marwan, and J. Kurths, *How Basin Stability Complements the Linear-Stability Paradigm*, Nat. Phys. **9**, 89 (2013).
[54] G. Pérez and H. A. Cerdeira, *Extracting Messages Masked by Chaos*, Phys. Rev. Lett. **74**, 1970 (1995).
[55] G. Alvarez and S. Li, *Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems*, Int. J. Bifurcation Chaos Appl. Sci. Eng. **16**, 2129 (2006).
[56] D. Iatsenko, A. Bernjak, T. Stankovski, Y. Shiogai, P. J. Owen-Lynch, P. B. M. Clarkson, P. V. E. McClintock, and A. Stefanovska, *Evolution of Cardio-Respiratory Interactions with Age*, Phil. Trans. R. Soc. A **371**, 20110622 (2013).
[57] D. G. Luchinsky, V. N. Smelyanskiy, A. Duggento, and P. V. E. McClintock, *Inferential Framework for Nonstationary Dynamics. I. Theory*, Phys. Rev. E **77**, 061105 (2008).
[58] A. Duggento, D. G. Luchinsky, V. N. Smelyanskiy, I. Khovanov, and P. V. E. McClintock, *Inferential Framework for Nonstationary Dynamics. II. Application to a Model of Physiological Signaling*, Phys. Rev. E **77**, 061106 (2008).
[59] R. J. Bates and D. W. Gregory, *Voice and Data Communications Handbook* (McGraw-Hill, New York, 2007), 5 ed.
[60] A. Duggento, T. Stankovski, P. V. E. McClintock, and A. Stefanovska, *Dynamical Bayesian Inference of Time-Evolving Interactions: From a Pair of Coupled Oscillators to Networks of Oscillators*, Phys. Rev. E **86**, 061126 (2012).