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.

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,
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 consists of two noisy $M$-dimensional interacting systems given by the following stochastic differential equation:

$$
\begin{align*}
\dot{x}_i &= f(x_i, x_j | \mathbf{c}) + \sqrt{D} \xi_i, \\
&= g(x_j | \mathbf{c}_1) + q(x_i, x_j | \mathbf{c}_2) + \sqrt{D} \xi_f,
\end{align*}
$$  

(1)

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

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, random-like but deterministic [46] nature of chaotic signals to encrypt the transmitted information. The latter approach

![Schematic of the communications scheme](image)

**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 $x_2$. 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 $s_1, \ldots, s_n$. 

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:

$$
\begin{align*}
\dot{x}_i &= f(x_i, x_j | \mathbf{c}) + \sqrt{D} \xi_i, \\
&= g(x_j | \mathbf{c}_1) + q(x_i, x_j | \mathbf{c}_2) + \sqrt{D} \xi_f,
\end{align*}
$$  

(1)

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

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, random-like but deterministic [46] nature of chaotic signals to encrypt the transmitted information. The latter approach
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)].

\[ x(t) = x_i(t) + h f(x_i(t), x_j(t)) + \sqrt{D}\xi(t), \]

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

The noise under consideration \( z_n \) is statistically independent and the likelihood is given by a product over \( n \) of the probability of observing \( x_{n+1} \) at each time. The joint probability density of \( z_n \) is used to find the joint probability density of the process in respect to \( x_{n+1} - x_n \) by imposing \( P(X_{n+1}) = \det(J_X^i)P(\xi^i) \), where \( J_X^i \) 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: \( \det(J_X^i(x_n)) \approx \prod_i \frac{\partial f_i(x_n)}{\partial x_n} \).

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 \( \epsilon \), with mean \( \bar{\epsilon} \), and covariance matrix \( \Sigma_{\text{prior}} = \Sigma^{-1} \), the stationary point of \( S \) is calculated recursively from

\[ S = \frac{N}{2} \ln |D| + h \sum_{n=0}^{N-1} \left( c_k \frac{\partial f_i(x_n)}{\partial x} \right)^T \left( D^{-1} \right) \left( x_n - f_i(x_n) \right), \]

with \( x_n = (x_{n+1} - x_n) / h \) and implicit summation over the repeated index \( k \).

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 \( \epsilon \) 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 \( \Sigma_{\text{post}}^n \) and the next prior \( \Sigma_{\text{prior}}^{n+1} \). We define a squared symmetric positive definite matrix \( \Sigma_{\text{diff}} \), 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, \( \Sigma_{\text{post}}^n \) and \( \Sigma_{\text{diff}} \).
\( \Sigma_{\text{prior}}^{n+1} = \Sigma_{\text{post}}^{n} + \Sigma_{\text{diff}}^{n} \). The diffusion matrix is expressed as 
\( (\Sigma_{\text{diff}})^{ij} = \rho_{ij} \sigma_{i} \sigma_{j} \), where \( \sigma_{i} \) is the standard deviation of the diffusion of \( c_{i} \) in the time window \( \tau_{w} \), and \( \rho_{ij} \) is the correlation between the change in parameters \( c_{i} \) and \( c_{j} \). We consider \( \Sigma_{\text{diff}} \) to be such that there is no change of correlation between parameters \( (\rho_{ij} = \delta_{ij}) \) and that each \( \sigma_{i} \) is a known fraction of the relevant standard deviation from the posterior \( \sigma_{i} = p_{w}(\sigma_{i}^{\text{post}})_{i} \), where \( p_{w} \) indicates that the parameter \( p \) refers to a window of length \( \tau_{w} \). 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 \( \rho_{ii} \) 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:

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

(5)

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

\[
\begin{align*}
\dot{u}_1 &= x_1, & \dot{w}_1 &= 10y_2 - 10w_1 + \xi_4, \\
\dot{u}_2 &= -x_1 - u_3, & \dot{w}_2 &= y_2, \\
\dot{u}_3 &= u_2 + 0.45u_3, & \dot{w}_3 &= w_1y_2 - 2.67w_3 + \xi_5.
\end{align*}
\]

(6)

The information signals acting as time-dependent non-autonomous terms are given by binary pseudorandom sequence signals \( s_0(t) = \{0, 28\} \), \( s_1(t) = \{1, 6, 2, 4\} \), and \( s_2(t) = \{0, 6\} \). 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 \( d/dt \), 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 \( u \) and \( w \) 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 \( y \) for \( s_0(t) = 0 \) 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 \( e = y - y' \), where \( y' \) is an identical copy of \( y \) with different initial conditions. By using the Lyapunov function \( L = 1/2(e_1^2 + e_2^2 + e_3^2) \), one can show that \( L = -(e_1 - e_2'^2 - e_3'^2) - 2.67e_1^2 < 0 \), which proves that the driven system \( y \) is globally asymptotically stable and the two oscillators \( x \) and \( y \) 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 \( \lambda \) are negative, the system \( y \) is asymptotically stable and generalized synchronization occurs. By evaluating the Lyapunov exponents for each sequential block of data from the Bayesian inference,
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 dynamical mixing that is highly resistant to the standard attacks [54,55].

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 $y_2 = -y_1y_3 - y_2 + 28y_1 + s_1(t)x_2x_3$. 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 $\sim 4$ 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 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 $y_2 = -y_1y_3 - y_2 + 28y_1 + s_3(t)$, 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 \(\sim 20 \text{ dB}\). The fact that the coupling-function scheme is noise resistant 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 resistant 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: 

\[ Q = \{ \cos(y_1)x_2, y_2^2/y_3, x_1y_2/y_3, \sqrt{y_3}, x_2^3/y_3, x_2x_3, x_1^3, \sin(x_3), x_2^3, x_3^2 \} \]

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 \( \cos(y_1)x_2 \sin(x_3), x_2^3x_1y_2/y_3, \ldots \), 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 $x_1$:

\[ x_1 = 10x_2 - 10x_1 + s_1(t) \cos(y_1)x_2 + s_2(t)y_2^2/y_3 + s_3(t)x_1y_2/y_3 + s_4(t)\sqrt{y_3} + s_5(t)x_2^2/y_3, \]

\[ x_2 = 28x_1 - x_1x_3 - x_2, \]

\[ x_3 = x_1x_2 - 2.67x_3, \quad (A1) \]

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

\[ \dot{y}_1 = 10y_2 - 10y_1 + \xi_1, \]

\[ \dot{y}_2 = 28y_1 - y_1y_3 - y_2 + s_6(t)x_2x_3 + s_7(t)x_1^3 + s_8(t)\sin(x_3) + s_9(t)x_2^2 + s_{10}(t)x_2^2, \]

\[ \dot{y}_3 = y_1y_2 - 2.67y_3, \quad (A2) \]

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 $\mathbf{u}$, through $x_1$, becomes effectively identical to the system $\mathbf{x}$,

\[ u_1 = x_1, \]

\[ u_2 = 28x_1 - x_1u_3 - u_2, \]

\[ u_3 = x_1u_2 - 2.67u_3 + \xi_2, \quad (A3) \]

and the system $\mathbf{w}$, through $y_2$, becomes effectively identical to system $\mathbf{y}$,

\[ \dot{w}_1 = 10y_2 - 10w_1, \]

\[ w_2 = y_2, \]

\[ w_3 = w_1y_2 - 2.67w_3 + \xi_3, \quad (A4) \]

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 $\xi_1, \ldots, \xi_3$ 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 $\mathbf{u}$ and $\mathbf{w}$ 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.

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.

References:

COUPLING FUNCTIONS ENABLE SECURE COMMUNICATIONS

PHYS. REV. X 4, 011026 (2014)


[28] U. von Toussaint, Y.F. Suprunenko, P.T. Clemson, and A. Stefanovska, Note that the nature of our secure communications scheme is that of a cipher rather than a secure key exchange protocol.


[42] Subject to U.K. patent application No. GB1314114.8, Lancaster University, filed 7 2013.


[49] Note that the nature of our secure communications scheme is that of a cipher rather than a secure key exchange protocol.


