Distributed Dynamics Encryption (DDE)- Questions and Answers

1 Question: The history of crypto algorithms shows that errors and deficiencies are found much later after the initial design of the method. Is there any guarantee for the security of this the new public key encryption scheme ?

Answer: Indeed, no cryptoanalysis of any method can be complete, as there is always a chance that a new cryptographical attack will emerge in the future. The only way to achieve a certain level of confidence is to publish a method and let people try to find a way to break it. Our analysis may have additional value: To the best of our knowledge the security of conventional chaotic synchronization and chaotic shift key encoding have been cryptoanalyzed using rather intuitive and and heuristic methods, whereas our analysis attempts to create tools and methods that will provide more rigorous and general analytic analysis of breaking continuous state nonlinear dynamics systems.

2 Question: The whole system attractor can be reconstructed from the (public) transmitted signal $s_t(n)$ based on the time-delay embedding method. By detecting the shift of the attractor due to the message encryption ($m = 0$ and $m = 1$), it is possible to extract the message without the knowledge of the receiver dynamics (e.g., PRL 74, p.1970 1995).

Answer: In conventional chaotic switch keying, the receiver and transmitter have identical structure that has to remain the same from bit to bit. That allows an unauthorized receiver to reconstruct the attractor in the embedding space of $s_t(n)$ using familiar phase space embedding technique. Our public key system allows us to change the secret dynamics of the receiver at any time, in particular at the beginning of every transmitted bit. Since for a single bit transmission we only need to send a short transient from a random initial condition to the attractor (different for every bit), an eavesdropper simply does not have sufficient data to reconstruct the dynamics. Furthermore, even if the attractor position could be identified, an eavesdropper cannot tell whether the end point lies on the '0' attractor or the '1' attractor, and the position of the attractor would change for the next bit.

3 Question: In the case where $s_r(n)$ is compromised, any unauthorized receiver can readily reproduce the transmitter output signal (at $m = 0$) without the knowledge of the receiver dynamics.

Answer: $s_r(n)$ is public and assumed to be known to all, yet the system is secure. The transmitter dynamics is chaotic, and neither the transmitter state nor the signal $s_t(n)$ is completely determined by $s_r(n)$. In order to reproduce the transmitted signal $s_t(n)$, an eavesdropper in addition to $s_r(n)$ needs to know the initial conditions,$\mathbf{t}(0)$, for the internal state of the transmitter system with impractically large precision. The state of the transmitter is randomized at the beginning of every bit, and this state is unknown to everybody (including the receiver). For different random initial states of the transmitter, the transmitter will produce different outputs $s_t(n)$, which will be the input of the receiver. The receiver will have different output $s_r(n)$ which will be a new input to the transmitter and so on. Hence, in order to reconstruct and converge to the correct attractor position in the reconstructed delays embedding space for $m = 0$ knowing the sequence $s_r(n)$ is not enough. The dynamics of the receiver is essential in order to know the position of the attractor. Still, an eavesdropper can use other methods that are discussed in the paper to compute the transmitted bit m knowing $s_r(n)$, $s_t(n)$ and the receiver dynamics, and without knowing neither the attractor position, the transmitter initial state, nor the receiver dynamics. We show in the paper that these methods can be made computationally unfeasible.

4 Question: How easy/difficult it is to properly detect (separate) possible chaotic attractors ("1" and "0") by using the received signals. How does the presence of noise influence the detection? How much does the receiver dynamics change from one symbol to another?

Answer : The separation between attractors depends on many factors, primarily on the noise level in the channel. The larger the noise level in the channel - the harder it is to separate between the attractors. The presence of noise makes the attractors 'thicker' and blur the border between them. The amount of blurring depends both on the noise level. Illustration of the blurring effect can be found in Fig-

ure. 5 on the following link:
http://inls.ucsd.edu/ roy/DDE/MainPage
/ViterbiStatesNumberDerivation.pdf On Fig. 3 of our paper (not at the above link) we demonstrate that due to blurring of the border between the attractors, the closer they are (the smaller modulation parameter A is) the larger the decoding error. Larger noise level will shift the graph upwards. In Fig. 4 of our paper, we illustrate the dependence of the security of the system measured by N_s as a function of the transmitter state noise level variance V. The graph shows that with the increase of noise (in this case noise in the transmitter state, however the phenomena in the presence of noise in the channel is similar), the decoding becomes harder due to blurring and 'thickening' of the attractors. In order to avoid detection errors the separation between the attractors has to be increased by increasing the parameter A, and therefore based on Eq.11 the security (measured by N_s) is decreased. The separation between the attractors also depends on the complexity of the attractor shape. This is illustrated in our web page:
http://inls.ucsd.edu/ roy/DDE/MainPage
/Chaotic_attractor_simulation.html The attractor at the top of the page, which is the one we used for simulations in our paper, is simpler for detection than the attractor at the bottom of the page.

Changing the dynamics of the receiver changes the position of the attractor, as illustrated in our web page:
http://inls.ucsd.edu/ roy/DDE/MainPage
/LimitCycleExample.html Any change of the receiver dynamics which results in a significant change of the position of the attractor will suffice. A significant change is the one that results in a shift in the attractor position of the order of the separation between the '0' and '1' attractor. This will result in a total confusion between the attractors of '0' and '1' transmitted at different times. In our simulation we kept the receiver dynamics constant in order to obtain the graphs in Fig. 3 and Fig. 4.

5 Question: How much will the transmitter-receiver system be affected by the lack of the proper synchronization, i.e. what if $s_t(n-1)$ is processed instead of $s_t(n)$.

Answer: A lack of proper synchronization may affect the decoding capability by altering the position of the attractor. For some dynamics, a severe lack of synchronization may even cause the system state trajectory to diverge. There are two main reasons for de-synchronization: loss of symbols due to noise and round-trip time delay. The former can be mitigated by adding a synchronization protocol that makes sure that no symbols are lost in the transmission, or if a symbol is lost, forces the system to re-transmit it. The latter can be improved either by including the time delay in the simulated dynamics of the system to determine the positions of attractor, or by limiting the bandwidth so the time delay becomes negligible.

6 Question: What is the "coding efficiency" of this encryption scheme. How many extra bits of information have to be exchanged between a receiver and a transmitter before a useful message bit "0" or "1" is properly detected. This is very important since $s_t(n)$ and $s_r(n)$ are real valued signals that have to be coded themselves.

Answer: The coding efficiency, which is measured in the information bits per transmitted bit is given by: $E = log2(M)/(n_1 * T_{bit})$, where M is the number of transmitted symbols, i.e. the number of attractors (we can use more than 2 attractors), n_1 is the number of bits representing a single sample of s_r or s_t, and T_{bit} is the number of samples until the system converges to the attractor. Note: the system does not need to accurately converge to the attractor. It only has to make sure that the trajectory is closer to the correct attractor than to the wrong one. Large separation between the attractors will require smaller T_{bit}. T_{bit} is also determined by the rate of convergence of the dynamical system, which is pretty much determined by the largest negative Lyapunov exponent.

In general, the efficiency of any chaotic switch keying is degraded by the factor of convergence to the attractor time. However, there may be ways to extend DDE to use other modulation methods than may be more efficient.

7 Question: What is the performance of the system? The combined dynamical system is iterated long enough to ensure that the system moves from the random initial state to one of the two attractors that correspond to the transmission of '0' or '1'. How long does this take? How large are the "keys" (private and public)?

Answer: A detailed answer to the convergence issue and the resulting efficiency was addressed in our answer to comment - III . Regarding the key sizes: The advantage of DDE is mainly in case of analog implementation. We assume that at least the transmitter is implemented using analog components. In such a case the public key is determined at the manufacturing. The key is named public since a series of (possibly identical) transmitters are distributed to all (and an eavesdropper may easily get/buy one). In this case the key is public since all the features of the transmitter are public. The public key is the structure of the transmitter that is available to all, and is not necessarily a stream of bits that needs to be transmitted. Of course, the hardware transmitter can have several public parameters that may determine the transmitter dynamics, but this is only an option.

Still, assuming that the dynamics equations are repre-

sented digitally, and needs to be transmitted, then the length of the keys given by the number of bits required to represent the structure and the coefficients of the dynamical equations (depends on the sensitivity to coefficients accuracy). The coefficients of the transmitter are used to determine the public key length, and the coefficients of the receiver determine the secret key length.

8 Question: Altering the dynamics of the receiver $\mathbf{F}_R(0)$; $G_R(0)$ at the beginning of each transmitted bit seems to reduce too much the performance. Is it possible to change them only at 1 Byte or 64 Bytes boundaries?

Answer: It is possible to change them at any desirable time interval. The factor that determines the maximal number of bytes that is transmitted before the dynamics of the receiver is altered is the security. In particular, long transmission without altering the dynamics of the transmitter may enable an eavesdropper to reconstruct the attractors of '0' and '1' in the embedding phase space, even without knowing the secret dynamics of the receiver. The allowed length of transmission is mainly determined by the complexity of the attractor in the high dimensional space: the more complex is the attractor, the more samples will be required to reconstruct it so a longer transmission is possible without altering the dynamics of the receiver. Also, the closer the attractors that correspond to transmission of '0' and '1', the more accurate the reconstruction has to be in order to differentiate between the two, and therefore more samples are needed for reconstruction, which again implies that longer sequences (more bits) can be transmitted before altering the dynamics of the transmitter. However, a more quantitative answer to this question goes beyond the scope of this Letter, and it is one of our future research goals. Note: at the beginning of each transmitted bit not only the dynamics of the receiver $\mathbf{F}_R(\bullet)$, $G_R(\bullet)$ are altered, but also the initial state of the transmitter $t(0)$ is initiated with a random value, so our answer relates to both.

9 Question: There seems to be a contradiction: Solving Eq.(7),for the initial transmitter state can be computationally infeasible. However, the transmitter initial state is not required to recover the message by the authorized receiver. The transmitted bit is decoded by the receiver by choosing the attractor that is closer to the endpoints of the trajectory.

Answer: Indeed,seemingly, there is a contradiction: On one hand the authorized receiver can reconstruct the the secret message m applying time-delay embedding method using the scalar signal s_t and does not need to calculate the initial state $t_i(0)$. On the other hand, our system is secure since the unauthorized receiver does need to calculate $t_i(0)$, which can be made computationally unfeasible for large transmitter state dimension D_T. However, there is no contradiction: The reason the authorized receiver does not need to calculate the initial state $t_i(0)$ is that no matter what the initial state $t_i(0)$ is, the end of the trajectory converge to one of the two attractors ($m = 0$ and $m = 1$). Therefore, regardless of the initial state $t_i(0)$, the authorized receiver can determine to which attractor the end of the trajectory is closer, and choose the message m to be the one that correspond to that attractor. On the other hand, the unauthorized receiver does not know the position of the attractors (details are in our paper and in our previous reply to referee B) and needs to find other methods that do not rely on any knowledge of the position of the attractors nor of the secret receiver dynamics. One such method is the one discussed in Eq. (7), which does require computation of the initial state $\mathbf{t}(0)$, and which is computationally unfeasible for large transmitter dimension D. To summarize, knowledge of the secret dynamics enables knowledge of position of the attractors, which in turn saves the need to know the initial state $\mathbf{t}(0)$. The unauthorized receiver does not know the position of the attractor, and therefore needs to use methods that compute implicitly or explicitly the initial state $\mathbf{t}(0)$, computation that is unfeasible for large transmitter dimension D.

10 Question: The attractor is reconstructed by the time-delay embedding method using the scalar signal $\mathbf{s}_t$ from the transmitter which is public and requires no knowledge of t($\mathbf{D}_T$). Why can the authorized receiver use the time-delay embedding method while the unauthorized receiver can not ?

Answer: The authorized receiver can reconstruct the position of the attractor using time-delay embedding of s_t and the unauthorized can not since they use different sequences of s_t obtained at different situations.
The authorized receiver reconstructs the position of the attractor using a sequence s_t obtained by simulating (running) off-line the entire dynamical system (transmitter+receiver) before the real transmission begins. The system will converge to the attractor, no matter what the state **t** is. After converged, the the off-line simulations continues until the trajectory (represented in reconstructed phase space using the sequence s_t) covers the entire attractor surface. The position of the attractor will be stored as points in memory (as we did in our simulation) or in any other efficient way. The same simulation takes place twice: once for $m = 0$ and then form $m = 1$. Each will produce a collection of points that represent the surface of each of the

two attractors separately.
On the other hand, the sequence s_t that is available to the unauthorized receiver is of a single converging trajectory, obtained during real transmission. Only the end of this trajectory lies on one of the two attractors that correspond to $m = 0$ or $m = 1$, and does not cover the whole surface of the attractor. Therefore, an unauthorized receiver can only determine that the end of the sequence s_t lies on one of the two attractors, but not which of the two. The authorized receiver can tell using the sequences s_t that were simulated off-line and covers the entire surface of the attractor (and are not available to the unauthorized receiver) to which of the two attractors the currently transmitted sequence is closer.

11 Question: How does the authorized receiver choose the closer attractor ? Since the authorized receiver does not know the full information of the transmitter, even the endpoints of the trajectory is on the attractor, it is not trivial to make the decision.

Answer: The authorized receiver simulates off-line and stores two sets of points that covers the entire surface of the two possible attractors ($m = 0$, $m = 1$). The unauthorized receiver can not obtain those points since he does not know the receiver dynamics and therefore can not run the system off-line. Once real transmission takes place, the end of the monitored trajectory is compared to the two stored sets of points (which are not available to the unauthorized receiver). The set of points that is closer to the trajectory end (we used euclidean distance) is chosen to be the attractor to which the trajectory converged to, and the corresponding value of m is chosen to be the decoded message.

12 Question: There seems to be a contradiction: On one hand, neither an unauthorized nor an authorized receiver knows the complete transmitter state t(n). On the other hand, using the public information s_r, F_T, and G_T, an unauthorized receiver can also regenerate the transmitter output signal s_t' corresponding to m(n)=0 at the receiver side. By comparing the attractors reconstructed from s_t and s_r, it is also possible for the unauthorized receiver to decode the message.

Answer: The attractors position can be reconstructed only by using the sequences s_t and s_r obtained during the off-line simulation that covers the entire attractor surface and is performed for each attractor separately. During real transmission (non off-line), the transmission ends once the trajectory converges to the relevant attractor but it does not cover the whole surface of the attractor. Further, the trajectory converges only one attractor out of the two. The other attractor is not transmitted at all and during transmission of the next bit the receiver dynamics changes and so does the position of both attractors. Only the off-line simulation which requires knowledge of the receiver secret dynamics, and is performed twice (once for each attractor) and long enough, provides the position of BOTH attractor, and covers the entire surface of each of the two attractors .

13 Question: One approach to attack the system is to assume that an attacker knows everything about the scheme and only lacks the information which constitutes the "read key." Can an unauthorized receiver develop a method (perhaps iterative) which could converge on the read key using some sort of complexity measure of the dynamics of each intermediate system. In other words, are the holes representing the read keys "deep".

Answer: As far as the transmitter is concerned, it is assumed that the exact transmitter dynamics is known to all, and the "read key" is the secret accurate initial state of the transmitter. As we have shown in our cryptanalysis, calculation of the initial transmitter state, $\mathbf{t}(0)$ can be made computationally unfeasible by using a nonlinear dynamics system with large transmitter dimension D_{tr}. Regarding the receiver, there are two cases to consider: In one case, the dynamics is assumed to be completely unknown. Reconstruction of the secret receiver dynamics can be made unfeasible by changing frequently the receiver dynamics. Frequent changes in the receiver dynamics will not allow a large enough amount of data to be monitored and to enable the reconstruction of the secret dynamics of the receiver during the period it remains constant. In the second case, the attacker knows the general structure of the secret receiver dynamics, and the "read key" would be the specific parameters used to implement the known "type" of dynamics. The difficulty in reconstructing the secret dynamics of the receiver will depend on the sensitivity of the dynamics to changes in parameters, and the size of the possible parameters space. Cryptanalysis in this case will be similar to the cryptanalysis of conventional chaotic secret key encryption scheme. Yet, in our scheme is more secure, since we are able to alter the secret receiver's parameters at will, while in conventional secret key chaotic encryption scheme the dynamics remains constant.
We are also conducting an analysis for quantifying the number of transmitted samples that will enable to reconstruct the secret dynamics of a secret key chaotic encryption scheme. The result of this research may be applicable

also to determine the number of samples that can be transmitted before the secret ”read key” which is the secret dynamics of receiver in our public key encryption scheme can be reconstructed.
It is possible that iterative methods for converging to the ”read key” will be developed in the future. Once a specific method is developed, we will do our best to develop a counter-measure, i.e. a specific scheme that will be robust to the specific kind of attack.

14 Question: An important issue with any encryption system is traffic analysis. Can an attacker assess the ”type” of information being sent (text, imagery, database records, noise), even if they cannot decrypt it. All key-based encryption systems are subject to this potential weakness. Can an unauthorized receiver induce about the character of the encrypted bitstream given a specific source model for the plaintext?

Answer: In the case of continuous state and discrete time transmission, which is the the type of system we implemented so far, protection against traffic analysis is relatively simple: For instance, the ability to alter the secret receiver dynamics at the beginning of each transmitted bit/symbol, enables the complete altering of the shape of the waveform at the output of the transmitter. This in turn can prevent attempts to use various global properties of the transmitted signal to induce about the transmitted data. However, in the near future we plan to extend DDE so it can transmit continuous state and continuous time signals (such as continuous video streams), and in that case the issue of traffic analysis might turn to be more problematic. Once we develop an encryption scheme version which is continuous in time we intend address the issue of traffic analysis.