Methods of Attacking Chaotic Encryption and Countermeasures

Mohamed I. Sobhy and Alaa-eldin R. Shehata
The Electronic Engineering Laboratory
The University of Kent at Canterbury
Canterbury Kent CT2 7NT, UK
Phone +441227 823236 Fax +44 1227 456084 email: M.I.Sobhy@ukc.ac.uk

Abstract: Methods of attacking chaotic encryption algorithms have been developed. These methods have been applied to all the published chaotic encryption systems and all these systems are broken in very short computer times. Counter measures have also been developed in order to make chaotic encryption secure. Several examples and results are given.

1. INTRODUCTION

Many papers have been published describing chaotic encryption algorithms and analogue encryption systems [1-4]. None of the papers adequately discusses the problem of security or estimate the computational effort required to break the system. Almost all papers assume that the system security is derived from the fact that a cryptanalist does not know the encryption system and hence it is very difficult to attack it with knowledge of the ciphertext alone. Systems that derive their security in this way are not worth very much as sooner or later the system will be known. Worse still, is that the user will not be aware that the system has been known and all the messages sent will be easily attacked. In any encryption system one must assume that the cipher is well known but the message cannot be retrieved without the key used. This fact is well known to cryptographers but apparently not to researchers in chaotic systems. Most papers in chaotic encryption do not even identify the key. This lead to researchers in methods of attack to concentrate on processing the ciphertext alone without knowledge of the cipher itself [5-7].

In this paper we shall show that the first step in attack must be the determination of the system used. This can be done from processing the ciphertext. The second step is to build the system and minimise the output to obtain the key. These two processes are relatively easy to achieve especially that a 'thumb print' can be produced from the ciphertext to identify the chaotic system that produced it.

The developed method has been applied to all published systems known to us and all of them have been broken with very little computational effort.

The next question to be asked is 'Does this mean that no chaotic encryption method is secure?' To answer this question we introduced non-linear functions to change the system keys dynamically. In this case the method of attack requires knowledge of the non-linear functions used and all their parameters. So far we are unable successfully to attack such systems.

2. SYTEM IDENTIFICATION

The first step of attack is to identify the chaotic system from the ciphertext. Chaotic time series possess a high level of information that point to the type of generating system. That information could be obtained by two ways:

- Plotting the signal iterates. This is a plot of the signal versus a delayed version of itself. Several delay values could be used. For a discrete time series the delay is an integer larger than unity. This step produces a plot similar to a strange attractor and every chaotic system produces a different strange attractor.
- The auto-correlation function of the time series is plotted. Again every chaotic system produces a different auto-correlation plot.

From the above two relatively simple processes a 'thumb print' of the system is produced which when compared to already compiled library of plots, will identify the chaotic system used.

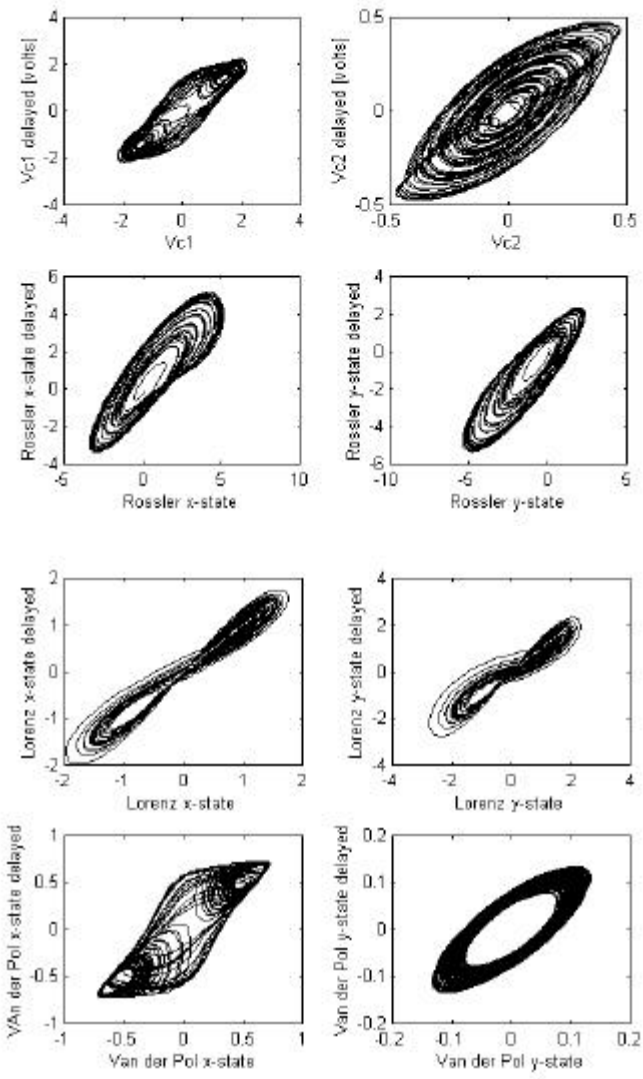

Fig 1 Examples of iterates of chaotic signals produced by the Chua, Rössler, Lorenze and Van der Pol systems

Fig 1. Shows iterates of continuos chaotic systems. The examples shown were produced by the Chua, Rössler, Lorenz and Van der Pol systems. It is easily seen that each system produces a unique pattern that can be readily identified.

Fig 2. shows examples of iterates of discrete chaotic systems. The examples shown are for the Henon map and the Yamakawa systems. Again each system produces a distinctly identifiable plot.

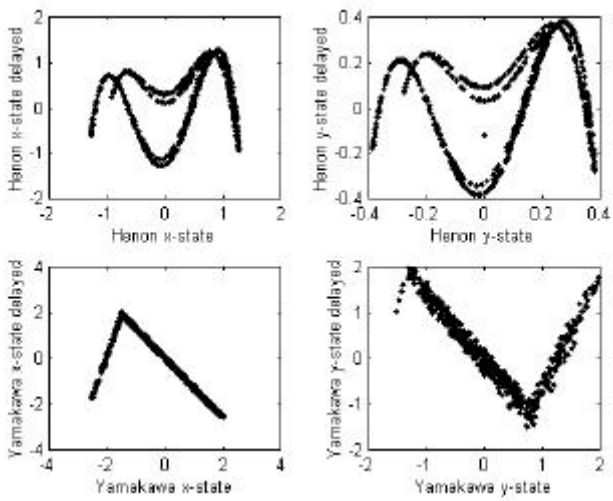

Fig 2. Iterates of the Henon map and the Yamakawa system.

The plot of the auto-correlation function produces a similar result. Fig 3 shows the auto-correlation function for the Chua, Henon, Lorenz and Rössler systems.

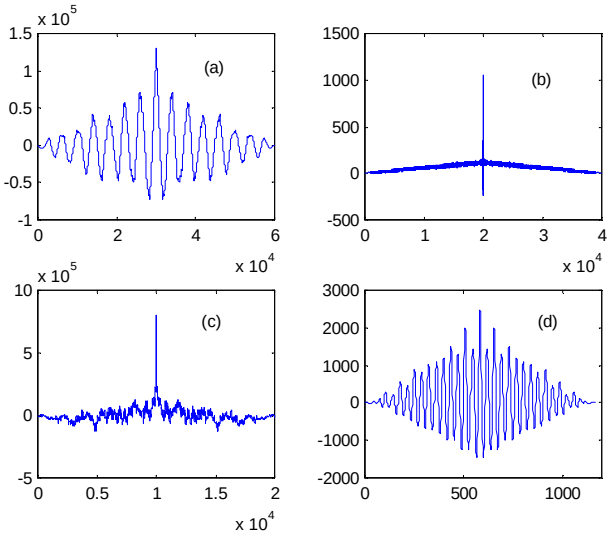

Fig 3. The auto-correlation function for the (a) Chua (b) Henon (c) Lorenz and (d) Rössler systems.

We can conclude that the iterates and the auto-correlation function can identify the chaotic system that produced the intercepted ciphertext.

Of course knowledge of the system alone is not enough to decipher the message. In the next section we shall describe how the key is found.

3. FINDING THE KEY

Once the system is identified, the system and its inverse are constructed to retrieve the information once the key is found.

All chaotic encryption systems rely on hiding the information in the chaotic signal. The higher the chaos to signal ratio the more secure the system is considered, as simple signal processing such as filtering will not retrieve the information. Some systems simply add the signal to chaos linearly while in others a process of linear or non-linear modulation is used. Paradoxically, the mere fact that the signal is very small makes the system prone to attack. Once the system and its inverse are known the system parameters (keys) are then optimised to minimise the output and thus remove the masking chaotic signal. The keys are the parameters of the chaotic system and the initial conditions of the integrators. The keys have to be found to an accuracy of about one part in 10^{15}. Furthermore the parameters have to be kept within a certain range so that the system does not come out of chaos. This means that we must use a very accurate, constrained minimisation routine. The routines used are standard functions in the MATLAB© optimisation toolbox. However we find that we have to use two different routines in succession in order to obtain the required accuracy. First routine **E04AJF** is used to obtain preliminary results for the keys. This is then followed by routine **fminsearch** . The process of finding the keys and displaying the recovered information signal are illustrated in the flow chart of Fig 4.

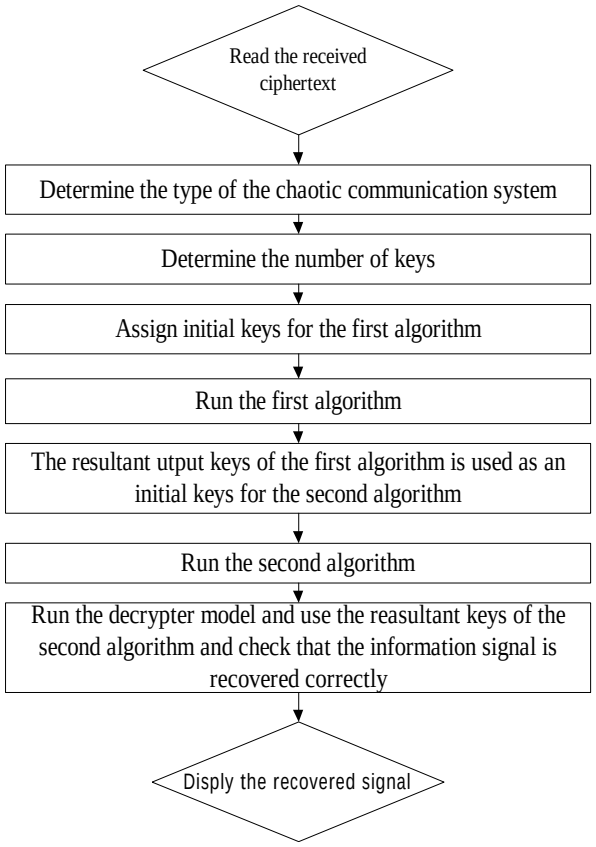

Fig 4. Flow chart of the attack to recover the information signal.

4. EXAMPLES OF SUCCESSFUL ATTACK

As mentioned before all published systems known to us have been successfully attacked using the above method. We shall give examples of these methods.

a. Attacking the Yamakawa chaotic communication system

Itoh *et al.* [8] have presented a chaotic communication system based Yamakawa's chaos chip. The chaos chip contains three basic units for constructing chaotic systems. Those are a nonlinear delay unit, a linear delay unit and a summing unit. The transmitter state equations are given by

$$\begin{aligned} x_{n+1} &= f(x_n) + e s_n \\ y_{n+1} &= g(y_n) - a z_n + d x_n \\ z_{n+1} &= y_n - b z_n \end{aligned} \qquad (1)$$

where,

$$f(x) = \begin{cases} k_1(x - E_1) + k_2 E_1, & x < E_1 \\ k_2 x, & E_1 \le x \le E_2 \\ k_3(x - E_2) + k_2 E_2, & x \ge E_2 \end{cases}$$

k_1, k_2, k_3, E_1 and E_2 are constants.

y_{n+1} is the transmitted signal and S_n is the information signal.

The function $g(y_n)$ has the same form of $f(x)$ but with different constants k_1, k_2, k_3, E_1 and E_2

The receiver state equations are given by

$$\begin{aligned} z'_{n+1} &= y_n - b z'_n \\ x'_n &= \frac{y_{n+1} - g(y_n) + a z'_n}{d} \\ r_n &= \frac{x'_{n+1} - f(x'_n)}{e} \end{aligned} \qquad (2)$$

where r_n is the recovered signal.

The attack took 345.8 seconds to determine the system parameters (keys) after 1219 iterations.

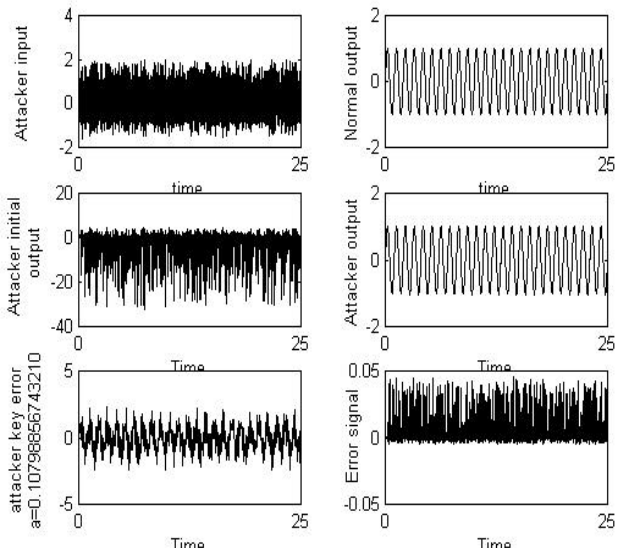

Fig 5. Result of attacking the Yamakawa system

Fig 5. shows the results of the attack. In this figure the 'Attacker input' is the ciphertext, 'The attacker initial output' is the output with the initial values of the keys, the 'Normal output' is the output with the exact keys and 'The attacker output' is the output with the keys found by the optimisation procedure. The figure shows that the analogue signal was correctly recovered with an error of less than 5%.

b. Attacking the system based on 'the general approach for chaotic synchronisation'

Kocarev and Parlitz [9] presented a secure communication system based on the general synchronisation approach. The system uses the well-known Lorenz model. The state equations of the transmitter are given by

$$\begin{aligned} \dot{x}_1 &= -a x_1 + s(t) \\ \dot{x}_2 &= b x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 &= x_1 x_2 - c x_3 \end{aligned} \qquad (3)$$

where a, b and c are constants and $s(t)$ is the transmitted signal and it is given by

$$s(t) = 10 x_2 + i x_3 \qquad (4)$$

and i is the information signal.

The state equations of the receiver are

$$\begin{aligned} \dot{y}_1 &= -a y_1 + s(t) \\ \dot{y}_2 &= b y_1 - y_2 - y_1 y_3 \\ \dot{y}_3 &= y_1 y_2 - c y_3. \end{aligned} \qquad (5)$$

The information signal is recovered by

$$i_R = (s(t) - 10 y_2) / y_3. \qquad (6)$$

The attack took 222.6 seconds to determine the system parameters (keys) after 1760 iterations

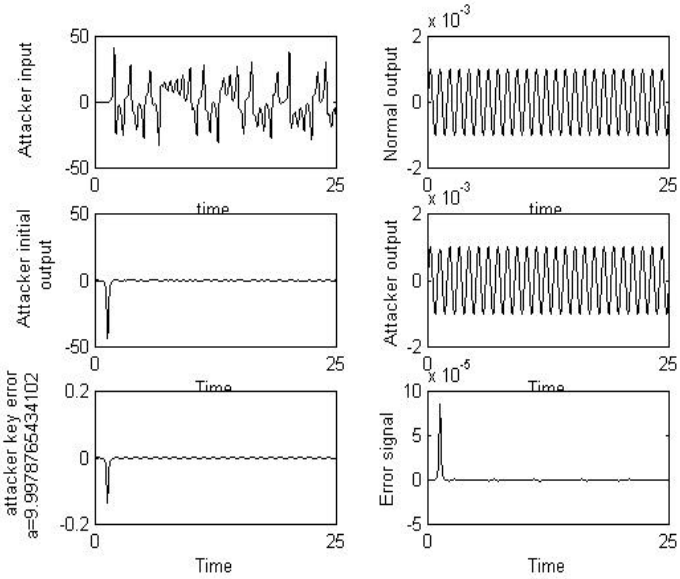

Fig 6. Result of attacking the 'general approach for chaotic synchronisation'.

Fig 6. is represented in a similar manner to Fig 5 and for explanation of the various signals see above.

Fig 6 shows that in this case the keys are calculated exactly and the final error is zero to the accuracy of the computer used.

5. COUNTER MEASURES

We have presented [10] a chaotic encryption algorithm that realises signal to chaos ratios of −240 dB. We shall now describe methods of making this algorithm secure against the methods of attack described in section 4 above.

- We convert all fixed parameters (keys and the initial conditions) to non-linear bounded functions of time and the state variables. Bounded functions are used to ensure that the system still has a chaotic behaviour. The attacker must first finds out what the functions used in the system are and then finds the parameter values.
- We use a multi-system encryption algorithm. In this algorithm a combination of Chua, Lorenz and R`ssler algorithms are used to encrypt the information signal. The signal flow diagram of the algorithm using SIMULINK© is shown in Fig. 7 and Fig. 8

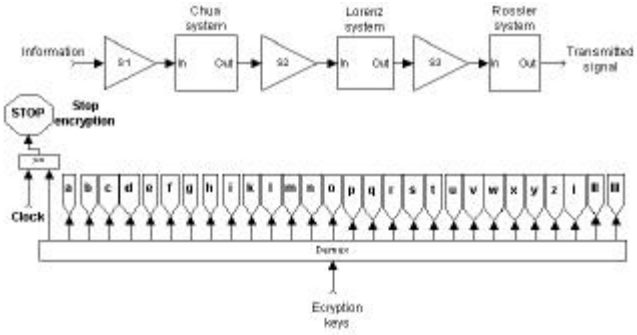

Fig. 7 Multi-system encryption algorithm. The lower diagram shows the key distribution system.

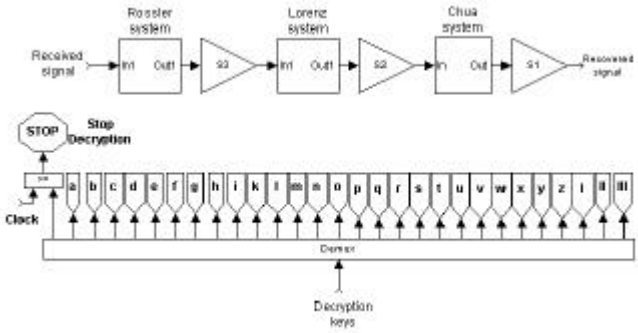

Fig. 8 Multi-system decryption algorithm. The lower diagram shows the key distribution system.

- The security is further improved by making the non-linear key functions of one system dependent on the state variables of the other systems.

The above counter measures will change the keys dynamically in a way that is extremely difficult to predict by the cryptanalyst. The next level of attack is to attack the algorithms symbol by symbol. We apply this method to attack to out system and the result is shown in Fig. 9

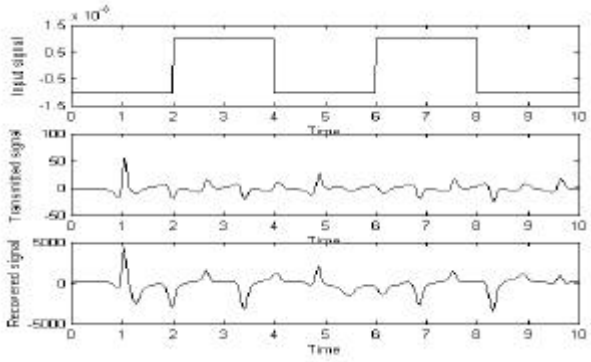

Fig 9. Result of the symbol by symbol attack

It is clear from Fig. 9 that it is not possible to retrieve the information signal.

6. CONCLUSION

We conclude that all chaotic encryption algorithms using constant keys are prone to attack. The only way to make these systems secure is to have the system parameters (keys) non-linear functions of time and the state variables. Further security could be added using a multi-system algorithm consisting of different individual algorithms. So far no known method of attack exists for such systems.

7. REFERENCES

[1] M. Itoh and H. Murakami, "New communication system via chaotic synchronisations and modulations," *IEICE Trans. Fundamentals*, vol. E78-A, No. 3, Mar. 1995.

[2] A. Sato and T. Endo, "Experiments of secure communications via chaotic synchronisation of phase-locked loops," *IEICE Trans. Fundamentals*, vol. E78-A, No. 10, Mar. 1995.

[3] R. Frey," Chaotic digital encoding an approach to secure communication," *IEEE Trans. Circuits Syst. II*, vol. CAS-40, pp. 660-666, Oct. 1993.

[4] L. M. Pecora, "Overview of chaos and communications research," *Proc. SPIE in Chaos in Communications*, vol 2038, pp. 2-25, July 1993

[5] K. M. Short, "Steps toward unmasking secure communications," *Int. J. Bifurcation and Chaos*, vol. 4, No. 4, pp. 959-977, 1994.

[6] Stark and B. V. Arumugam, "Extracting slowly varying signals from a chaotic background," *Int. J. Bifurcation and Chaos*, vol. 2, No.2, pp. 413-419, 1992.

[7] T. Yang, L. B. Yang and C. M. Yang, "Breaking chaotic switching using generalised synchronisation: examples," *IEEE Trans. Circuits Syst. I*, vol. CAS-45, No. 10, 1998.

[8] M. Itoh, H. Murakami and L. O. Chua, "Secure communication via Yamakaw's chaotic chips and Chua's circuits," *IEEE Int. Symposium. on Circuit and System (ISCAS 94)*, pp. 1293-1296, 1994.

[9] L. Kocarev and U. Parlitz, "General approach for chaotic synchronisation with applications to communications," *Phys. Rev. Lett.*, vol. 74, No. 25, pp. 5028-503 June 1995.

[10] M.I. Sobhy and A.R. Shehata "Chaotic Algorithms for Data Encryption" Submitted for presentation at this conference.