Assessing the Security of Subsampling Process Using Modified EKF and Nonlinear Least Squares Methods

Léa D. Cot
ICA: Institut Clément Ader
Université Toulouse ; INSA, UPS, Mines Albi, ISAE;
ICA; 135, avenue de Rangueil, F-31077 Toulouse, France

René Lozi
Laboratoire J.A. Dieudonné, UMR CNRS 7351
Université de Nice Sophia-Antipolis
Parc Valrose, F-06108 Nice Cedex 02

Abstract—**Since the theory of chaos was introduced in cryptography, the use of chaotic dynamical systems to secure communications has been widely investigated, particularly to generate chaotic pseudorandom numbers as cipher-keys. The emergent property of the ultra-weak multidimensional coupling of p one-dimensional dynamical systems lead to randomness preserving chaotic properties of continuous models in numerical simulations. This paper focuses on such families called multiparameter chaotic pseudo random number generators (M-p CPRNG) and proposes algorithm approach to test the robustness of time series generated by M-p CPRNG. First, a single one-dimensional chaotic map to construct a regular chaotic subsampling is considered. Parameters on which depends the map are estimated using only the sequences generated by this map to cipher a message. A previous study [1] using the Extended Kalman Filter (EKF) has shown that a necessary minimum shift value corresponding to a particular subsampling of a chaotic cubic map is obtained from which it is not possible to estimate the parameters. In this paper, new cipher breaking methods are considered for the same purpose: assessing the security of the time series. These methods are investigated in the same way than EKF one and compared to the results provided by EKF. The EKF was first improved by introducing a modified Gram-Schmidt method and the nonlinear least squares method was also tested. The one-dimensional cubic map was again considered and a new parameter leading to EKF oscillations is especially studied.**

Keywords; security; chaos; cryptography; time series; parameter estimation; pseudo random number generation; subsampling.

I. INTRODUCTION

Pseudorandom or chaotic numbers are used in many areas of contemporary technology such as modern communication systems and engineering applications. Significant researches have been made using chaotic dynamical systems in order to benefit of the high sensitivity of chaos to initial conditions. Efficient Chaotic Pseudo Random Number Generators (CPRNG) have been recently introduced. The emergent property [2] of the ultra-weak multidimensional coupling of p one-dimensional dynamical systems is used and chaotic properties of continuous models in numerical simulations are preserved. Noteworthy CPRNG families based on the sampling and mixing of chaotic sequences have been proposed in [3], [4]. This method is very efficient in numerical calculations using floating point numbers. Moreover, only additions and multiplications are considered in a computation process and no division is required.

In [5], [6], these CPRNG families are improved using a double threshold chaotic sampling instead a single one. The performances of such families called multiparameter chaotic pseudo random number generators (M-p CPRNG) are increased, especially to compute very long time series. Both the high number of parameters and the high sensitivity of their values allow to choose these parameters as cipher-keys. Their applications can be, for example, generation of Gaussian noise, computation of hash functions or chaotic cryptography.

Our paper focuses on the field of chaotic cryptography which has been widely investigated in an effort to improve the security of transmissions. An approach is proposed to test the robustness of time series generated by the M-p CPRNG process defined in [6] and used to cipher a message. First, a particular case of M-p CPRNG using a single one-dimensional chaotic map to construct a regular chaotic subsampling is considered. The idea is to estimate the chaotic map parameters using only the sequences generated by this map to cipher a message and to reconstruct the sequences to decipher the message. In [1], such a study has been carried out to test the robustness of an enhanced chaos shift keying (CSK) system based on the estimation of chaotic map parameters using the Extended Kalman Filter (EKF). Instead of using the sequences generated by the chaotic map directly, a subsampling of sequence terms is extracted so that no transmission of consecutive terms occurs. A large number of simulations has been performed using three different chaotic attractors of a cubic map corresponding to three parameter sets. Various regular subsampling were considered. It was obtained a necessary condition, different in each case, expressed by a different threshold value, related to the subsampling chosen, from which it was not possible to estimate the parameters. Consequently, the chaotic sequences used to cipher a message cannot be reconstructed and the message cannot be deciphered. This study has shown that by placing themselves under the conditions that lead to the divergence of EKF, the security of a transmitted message is guaranteed. The threshold value should be part of the secret key with the corresponding initial condition and parameter. Moreover, as various initial

condition, parameter and shift sets lead to the divergence of EKF, the secret key can be changed very often.

Regarding the study of M-p CPRNG families, these results are of a great interest. However, the behavior of EKF was also studied by taking into account different values of the measurement and state noises and the results obtained have shown that sometimes the EKF algorithm cannot converge nor diverge. In these cases, the iteration maximum number is reached and the estimation error on the parameters is greater than the required precision.

In this paper, new cipher breaking methods are considered for the same purpose: assessing the security of the time series. These methods are investigated in the same way than EKF one and compared to the results provided by EKF. The EKF was first improved by introducing a modified Gram-Schmidt method and the nonlinear least squares method was also tested. The one-dimensional cubic map was again considered and a new parameter leading to EKF oscillations is especially studied.

This paper is organized as follows. In section II, the method to construct the chaotic subsampled sequence of a map is described. The estimation methods are explained in section III. Simulations and results are presented in section IV, followed by the conclusion section.

II. SUBSAMPLING CHAOTIC MAP

A chaotic map is represented by a nonlinear deterministic model with function F defined on $IR^p \times IR^q$ by $\forall k \in IN$, $U_{k+1} = F(U_k, \Lambda)$ where $\Lambda \in IR^q$ is the parameter vector to be determined. Initial condition vector U_0 is also unknown.

To avoid the transmission of consecutive terms, we retain a state trajectory every Δ states. This integer value Δ is called a shift. This means that a sub-sampled $(U_{\varphi(k)})_{k \in IN}$ where $\varphi(k) = \Delta k$ is extracted from $(U_k)_{k \in IN}$. Accordingly, the chaotic model is now represented by the function G expressed by successive compositions of F

$$U_{(k+1)\Delta} = G(U_{k\Delta}, \Lambda), \ \forall k \in IN \tag{1}$$

As a chosen plaintext attack is considered, the system and its encryption algorithm are known and any plaintext can be ciphered, especially, a sequence of 0 or a sequence of 1. The sequences therefore taken into account in our study to determine the map parameters are of the form $u_0 u_\Delta u_{2\Delta} u_{3\Delta} u_{4\Delta} u_{5\Delta} u_{6\Delta} \ldots$ corresponding to real numbers at non successive times. These real numbers define the measurement vectors which we call Z_k , $0 \le k \le m-1$, $m \in IN$. We just use the EKF usual notations. Assuming that m measurements are used for the parameter estimation process, the chaotic sequence at non successive times k is $Z_0 Z_1 Z_2 \ldots Z_{k-1} Z_k Z_{k+1} \ldots Z_{m-1}$. Moreover, we suppose that a symmetric secret key is used and the chaotic map is known but not the initial conditions nor the parameters nor the shift value, which will be part of the secret key.

The cubic map model F on $IR^2 \times IR^2$ in IR^2 we use in our study is defined, for all integer k, by

$$\begin{cases} u_{k+1} = v_k \\ v_{k+1} = \lambda^{(1)}(u_k - u_k^3) + \lambda^{(2)}(v_k - v_k^3) \end{cases} \tag{2}$$

where $U = (u, v)$ and $\Lambda = (\lambda^{(1)}, \lambda^{(2)})$. Here F is linear in Λ but in the problem with shift, G is nonlinear in Λ . Because of the relationship between the two components of vector U, this map can be expressed as the following one-dimensional map

$$v_{k+1} = \lambda^{(1)}\left(v_{k-1} - v_{k-2}^3\right) + \lambda^{(2)}\left(v_k - v_k^3\right) \tag{3}$$

III. ESTIMATION METHODS

A. Modified Extended Kalman Filter (MEKF)

The estimation method first chosen to estimate the chaotic map parameters was the Extended Kalman Filter which provides real-time utilization.

The estimation problem of the state-parameter vector $X_{k\Delta} \in IR^{p+q}$ at time $k\Delta$ using the EKF formulation is expressed by the following equations

$$\begin{cases} U_{k\Delta} = G(U_{(k-1)\Delta}, \Lambda_{(k-1)\Delta}) + W_{(k-1)\Delta}, \forall k \in N^* \\ \Lambda_{k\Delta} = id(\Lambda_{(k-1)\Delta}) + W_{(k-1)\Delta} = \Lambda_{(k-1)\Delta} + W_{(k-1)\Delta}, \forall k \in N^* \\ Z_k = HX_{k\Delta} + V_{k\Delta}, \forall k \in N \end{cases} \tag{4}$$

where $X_{k\Delta} = \begin{pmatrix} U_{k\Delta} \\ \Lambda_{k\Delta} \end{pmatrix}$ is also called joint EKF, G is a continuous differentiable nonlinear function and $H \in M_{m,p+q}(IR)$ is a matrix modeling the measurement equation. W and V are state and measurement noises of covariance matrices $Q \in M_{p+q}(IR)$ and $R \in M_m(IR)$ respectively, assumed to be white, Gaussian, centred $\forall i, j, E[W_i] = 0, E[W_i W_j^T] = Q_i \delta_{ij}, E[V_i] = 0, E[V_i V_j^T] = Q_i \delta_{ij}$ where δ_{ij} is the Kronecker symbol. For more details, see [1].

The usual prediction-updating EKF equations providing the state-parameter estimation $\hat{X}_{k\Delta}$ and the estimation covariance matrix $\hat{P}_{k\Delta}$ are recalled here after

$$\begin{cases} P_{k\Delta}^- = J_{k\Delta}(\hat{X}_{(k-1)\Delta}) \hat{P}_{(k-1)\Delta} J_{k\Delta}(\hat{X}_{(k-1)\Delta})^T + Q_{(k-1)\Delta} \\ K_{k\Delta} = P_{k\Delta}^- H^T (H P_{k\Delta}^- H^T + R_{k\Delta})^{-1} \\ \hat{X}_{k\Delta} = \hat{X}_{k\Delta}^- + K_{k\Delta}(Z_k - H\hat{X}_{k\Delta}^-) \\ \hat{P}_{k\Delta} = (I - K_{k\Delta} H) P_{k\Delta}^- . \end{cases} \tag{5}$$

The calculation of the Kalman gain requires the inverting of the matrix $(HP_{k\Delta}^- H^T + R_{k\Delta})$. In the case of ill-conditioned matrix, round-off numerical errors can arise and lead to the divergence of the algorithm. To avoid this problem, a matrix

French National Research Agency: COSINUS program.
PEPS INS2I 2012: COIG project.

factorization is applied using a modified Gram-Schmidt process. Results obtained with the modified Gram-Schmidt EKF (MEKF) are shown in section IV.

B. Nonlinear least squares (NLS)

Another approach consists in using nonlinear least square-based methods. Let us define the residual function S of IR^q in IR^m twice continuously differentiable where its kth component $s^{(k)}$ is expressed as

$$s^{(k)}(\Lambda) = \|Z_k - U_{k\Lambda}\|_2 = \left[\sum_{j=1}^{p}\left(z_k^{(j)} - u_k^{(j)}(\Lambda)\right)^2\right]^{1/2}. \quad (6)$$

The NLS problem consists in determining the parameters that minimize the criterion C of IR^q in IR, i.e. find Λ such that

$$\min_{\Lambda\in IR^q} C(\Lambda) = \frac{1}{2}S(\Lambda)^T S(\Lambda) = \frac{1}{2}\sum_{k=0}^{m-1} s^{(k)}(\Lambda)^2 \quad (7)$$

where

$$C(\Lambda) = \frac{1}{2}\sum_{k=0}^{m-1}\|Z_k - U_{k\Lambda}\|_2^2 = \frac{1}{2}\sum_{k=0}^{m-1}\sum_{j=1}^{p}\left(z_k^{(j)} - u_k^{(j)}(\Lambda)\right)^2. \quad (8)$$

After making an affine approximation of function S and assuming that the Jacobian matrix $J(\Lambda)$ of S at point Λ is full rank, the solution of the estimated parameters $\hat{\Lambda}$ to the NLS is

$$\hat{\Lambda} = \Lambda - \left[J(\Lambda)^T J(\Lambda)\right]^{-1} S(\Lambda) \quad (9)$$

where $\forall k \in [0, m-1],\ \forall j \in [1, q],\ J(\Lambda_{kj}) = \dfrac{\partial s^{(k)}(\Lambda)}{\partial \lambda^{(j)}}$. (10)

Among the methods based on nonlinear least squares, an iterative method for finding the minimum of the cost function C is the Gauss-Newton method. The solution Λ_{k+1} at time k+1 in the descent direction d_{k+1} is obtained by solving the linear system

$$J(\Lambda_k)^T J(\Lambda_k) d_{k+1} = -J(\Lambda_k)^T S(\Lambda_k) \quad (11)$$

where $\Lambda_{k+1} = \Lambda_k + \alpha_k d_k$ and α_k is the descent step provided by a line-search algorithm. This method has similar properties than Newton method; in particular, the convergence is quadratic but requires an initial parameter estimation Λ_0 chosen near the exact solution of the parameters. Here again, ill-conditioned matrix $J(\Lambda_k)^T J(\Lambda_k)$, which is approximately the Hessian matrix $H(\Lambda_k)$ of the cost function C, can occur. Indeed, this matrix may not be symmetric positive definite. In this case, a standard method to get a symmetric positive definite matrix is to define $H(\Lambda_{k+1}) = H(\Lambda_k) + \alpha I$ where I is the identity matrix. The method therefore obtained is called the Lebenberg-Marquardt method.

IV. SIMULATIONS AND RESULTS

All the simulations were done using the cubic map (2) and we developed our own program in Matlab (version 7.9 0.529 (R2009b)).

In [Léa], results presented are obtained from simulations using the EKF to estimate the cubic map parameters. Our own Matlab program (version 7.9 0.529 (R2009b)) was developed. Three parameters $\Lambda \in IR^2$ were first chosen to be estimated for which the exact values are $\Lambda_e = (2.2, -0.91)$, $\Lambda_e = (2.2, -0.95)$ and $\Lambda_e = (-2., 1.7)$ according to the Lyapunov exponent values. The initial condition vectors U_0 are taken in the basin of the corresponding chaotic attractor, i.e. the initial condition sets which allow to generate the sequences converging towards the attractor. Regarding the EKF, only a very small measurement noise was first considered, i.e. no state noise, corresponding to the accuracy of the real sequence terms in Matlab 10^{-16}. The diagonal coefficients of the covariance matrix R, representative of the variances, were therefore taken to be 10^{-16}. The state-parameter estimation error initial covariance matrix P_0 was always initialized with the identity matrix. Finally, to be sure that the sequence terms correspond to the chaotic regime, the transient regime was skipped. The measurements were therefore considered from the 1000^{th} sequence term. The parameter estimation precision required was 10^{-10}.

Many simulations were done scanning the basin of these attractors and searching the shift value from which the EKF algorithm diverged. Similar results are obtained for the three parameters. For each parameter and for each initial condition set, a necessary minimum value of the shift was found from which it is not possible to estimate the parameters. This appears to result from numerical considerations where accumulated round-off errors in the calculations increase with the shift and become so large that the EKF diverge. However, simulations also show that sometimes the maximum iteration number authorized, i.e. iteration number 2000, was reached so that the EKF algorithm neither converged nor diverged. Even by increasing this maximum value up to 10000, the convergence or the divergence of EKF cannot be obtained.

The EKF behavior was also studied by increasing the measurement and process noises. In many cases tested and for the three parameters, we obtained that the necessary minimum shift also increased. These results showed that the higher the noise, the better the EKF works. We also observed that more cases appeared for which the EKF neither converges nor diverges and oscillates.

This phenomenon has been confirmed by the study of another cubic map chaotic parameter which exact value is $\Lambda_e = (-2.55, 0.24)$. As for the three others parameters, we systematically scaned the basin of this attractor and gradually increased the shift value. For all the initial conditions, i.e. 100 different cases, the maximum iteration number was reached, even if the iteration number is 10000, and it is impossible to make EKF diverge as the other previous parameters.

In this paper, we focuse on the study of this particular parameter in the aim to avoid the oscillations of the EKF filter

and to obtain the divergence of the method used. The MEKF and the NLS methods have been implemented and tested in the same conditions. The EKF Matlab program already developed has been adapted to use the Gram Schmidt modified method. Nsqnonlin Matlab function was used to test the NLS approach because this function is very robust and efficient. It is based on a trust region method and the algorithm automatically switches to the Lebenberg-Marquardt method in case of ill-conditioned Hessian matrix.

Compared to the results obtained with EKF, the MEKF method improves the results in 60% of initial conditions. This means that MEKF diverges for a specific shift value, different for each initial condition, which is the threshold from which the parameter cannot be estimated. In other cases, the maximum iteration number is reached again.

TABLE I. NECESSARY MINIMUM SHIFT FOR PARAMETER $(-2.55,0.24)$ AND VARIOUS INITIAL CONDITION SETS, $R = Q = 10^{-16} I_2$, $\varepsilon = 10^{-10}$

MEKF			NLS		
U_0	Δ_{min}	N	U_0	Δ_{min}	N
(-0.9,-0.9)	22	246	(-0.9,-0.9)	9	7
(-0.7,-0.9)	17	46	(-0.7,-0.9)	5	6
(-0.5,-0.3)	17	907	(-0.5,-0.3)	7	6
(-0.3,-0.1)	17	916	(-0.3,-0.1)	8	6
(-0.1,-0.9)	15	381	(-0.1,-0.9)	7	6
(-0.9,0.9)	20	1019	(-0.9,0.9)	9	7
(-0.7,0.9)	18	928	(-0.7,0.9)	7	6
(-0.5,0.9)	17	93	(-0.5,0.9)	7	5
(-0.3,0.3)	16	107	(-0.3,0.3)	8	7
(-0.1,0.9)	19	514	(-0.1,0.9)	8	8
(0.1,-0.3)	18	895	(0.1,-0.3)	7	6
(0.3,-0.9)	19	32	(0.3,-0.9)	9	8
(0.5,-0.7)	18	53	(0.5,-0.7)	9	7
(0.7,-0.1)	16	8	(0.7,-0.1)	9	6
(0.9,-0.1)	19	146	(0.9,-0.1)	7	7
(0.1,0.7)	18	95	(0.1,0.7)	7	6
(0.3,0.3)	16	587	(0.3,0.3)	7	7
(0.5,0.3)	15	103	(0.5,0.3)	7	6
(0.7,0.5)	18	680	(0.7,0.5)	7	6
(0.9,0.7)	18	904	(0.9,0.7)	7	7

Moreover, the NLS method lead to the divergence of the algorithm for all initial conditions of the basin of the attractor and a necessary minimum shift is obtained, different in each case.

Table I shows a part of the results obtained for the parameter $(-2.55,0.24)$ respectively using MEKF and NLS methods. Five initial condition sets are selected in four domains of $[-1,1]^2$. For each initial condition, the corresponding necessary minimum shift $\Delta_{\min}$ obtained and the iteration number N are given.

As seen in Table I, the parameter can be estimated until the minimum shift value and not beyond. For instance, for initial condition $(-0.9,-0.9)$, MEKF and NLS don't estimated the parameter from $\Delta_{\min} = 22$ and $\Delta_{\min} = 9$ respectively. These minimum shift values are therefore necessary conditions corresponding to the method used. In all simulations, results show that higher minimum shift values are obtained with MEKF than NLS but the iteration number required by MEKF, and consequently, the time computing, are greater than that of NLS.

Regarding the EKF oscillations, this problem has been solved in more than half of the cases by using MEKF. But the NLS method is more efficient because it provides a necessary minimum shift whereas MEKF does not work as shown in Table II.

TABLE II. NECESSARY MINIMUM SHIFT FOR PARAMETER AND VARIOUS INITIAL CONDITION SETS, $R = 10^{-16} I_2$, $\varepsilon = 10^{-10}$

MEKF			NLS		
U_0	Δ_{min}	N	U_0	Δ_{min}	N
(-0.9,-0.7)	22	2000	(-0.9,-0.7)	7	7
(-0.5,-0.5)	18	2000	(-0.5,-0.5)	8	8
(-0.5,0.3)	18	2000	(-0.5,0.3)	7	8
(-0.3,0.5)	13	2000	(-0.3,0.5)	7	8
(0.7,-0.5)	14	2000	(0.7,-0.5)	10	6
(0.5,-0.1)	16	2000	(0.5,-0.1)	11	13
(0.5,0.5)	20	2000	(0.5,0.5)	8	8
(0.9,0.5)	12	2000	(0.9,0.5)	9	9

Table II shows some cases where the maximum iteration number is reached and the EKF filter still oscillates despite the use of MEKF. On the contrary, the NLS algorithm works until a necessary minimum shift, $\Delta_{\min}$, from which it is not possible to estimate the map parameters.

The security of the time series used to estimate the chaotic map parameter is therefore guaranteed by taking the highest value of the necessary minimum shift obtained among all the simulations performed, i.e. 100 cases corresponding to 100 initial conditions of the basin of the considered attractor. Additional safety factor can also be applied to the value chosen.

V. CONCLUSION

These simulations have shown that both MEKF and NLS behaviour depends on regular subsamplings of chaotic sequence terms considered. The two algorithms diverge for a particular subsampling corresponding to a necessary minimum shift, different for each parameter and each initial condition, from which it is not possible to estimate the parameter. The divergence of MEKF and NLS can be explained by round-off errors in the calculations, their accumulation and their propagation as the shift value is increased. Consequently, the estimated parameter precision decreases and finally, the algorithms diverge.

Moreover, this study carried out to test a single one-dimensional chaotic map to generate regular subsamplings shows that this particular case of M-p CPRNG is efficient in cryptography applications to choose cipher-keys. The security of a transmitted message is guaranteed by the shift value which must be chosen greater than the necessary minimum shift obtained. This shift value should be part of the secret key with the corresponding initial condition and parameter. Moreover, various initial condition, parameter and shift sets lead to the divergence of MEKF and NLS so that the secret key can be changed very often. Consequently, by using a such appropriate secret key and by changing it regularly, the cipher-key is immune against attack using the MEKF and NLS.

Finally, this study provides areas for future investigation on M-p CPRNG families.

ACKNOWLEDGMENT

This work has been partially supported by the French National Research Agency (ANR) through the COSINUS program under the grant ANR-09-COSI-005 and by the PEPS INS2I 2012 program through the COIG project.

We would also like to thank Adrien Gamot, Camille Desjardins, Hichem Ayadi, Karim Benizeri, Guillaume Jacob, Sophie Coquan, Claire Beigbeder, Pierre Gangneux and Paul Escande for their fruitful contribution.

REFERENCES

[1] L.D. Cot and C. Bès, “Study of the robustness of an enhanced CSK system by using the Extended Kalman Filter,” IEEE ICITST, 2011, pp. 202–207.

[2] M.A. Aziz-Alaoui and C. Bertelle, “From system complexity to emergent properties (Understanding complex systems),” Springer-Verlag, Berlin.

[3] S. Hénaff, I. Taralova and R. Lozi, “Statistical and spectral analysis of a newly weakly coupled maps system,” Indian J. Industr. Appl. Math., 2009b, vol. 2, pp. 1–17.

[4] S. Hénaff, I. Taralova and R. Lozi, “Exact and asymptotic synchronization of a new weakly coupled maps system,” J. Nonlin. Syst. Appl. , 2010, vol. 1, pp. 87–95.

[5] R. Lozi, “New enhanced chaotic number generators,” Indian J. Industr. Appl. Math., 2008a, vol. 1, pp. 1–23.

[6] R. Lozi, “Emergence of randomness from chaos,” Int. J. Bifurcation and Chaos, 2012, vol. 22, 2, pp. .

