Estimating Secret Parameters of a Random Number Generator from Time Series by Auto-synchronization

Salih Ergün
ERGTECH Research Center
Zürich, Switzerland
Email: salih.ergun@ergtech.ch

***Abstract*—A novel estimate system is proposed to discover the security weaknesses of a chaos based random number generator (RNG). Convergence of the estimate system is proved using auto-synchronization. Secret parameters of the target RNG are recovered where the available information are the structure of the RNG and a scalar time series observed from the target chaotic system. Simulation and numerical results verifying the feasibility of the estimate system are given such that, next bit can be predicted while the same output bit sequence of the RNG can be regenerated.**

***Index Terms*—Estimation, security weaknesses, random number generator, continuous-time chaos, time series, synchronization of chaotic systems, auto-synchronization**

I. Introduction

Nowadays, technological developments emphasize the importance of innovations in the following field of circuits and systems: Small area occupation, hardware security, low power consumption and high speed operation. In relation to this, the fast and low power consuming random number generators (RNG) are positioned more clearly in the heart of the research as the main components of the security systems. Although most of the people are unaware that they use them, we use RNGs in our day-to-day work. We use RNG if you withdraw money from a bank's cash machine, order goods with a credit card on the internet, or watch pay TV. Public/private keys for asymmetric crypto algorithms, keys for hybrid and symmetric encryption systems, one-time pad, nonces and padding bytes are created by using RNGs [1].

Being aware of any knowledge about the structure of the RNG must not provide a useful estimate of the output bit sequence of the RNG. Even so, fulfilling the requirements for the confidentiality of security systems using RNG requires three privacy criteria as a must: 1. The RNG must fulfill all statistical randomness tests; 2. The preceding and following random bits can not be predicted [2] and; 3. Anyone should not generate the same output bit sequence of the RNG [3].

One of the basic principle of the cryptography is that according to Kerckhoff's hypothesis [1], it is assumed that the overall security of any crypto system is completely dependent on the security of the key, and that all other parameters of the crypto system are publicly observable. Vulnerability analysis is complementary to cryptography. The interaction between these two cryptology branches creates a contemporary cryptography that becomes stronger due to the vulnerability analysis that reveals the weaknesses of the existing crypto systems.

Although the use of discrete-time chaotic maps in random number generation has been acknowledged over a long period of time [4], [5], [6], it has been shown nowadays that continuous-time chaotic oscillators can be used to implement RNGs [7], [8], [9], [10], [11]. In particular, a "truly" RNG based on a continuous-time chaotic oscillator has been proposed in [8]. In this article, we target the RNG reported in [8], and propose an estimate system to analyze security vulnerabilities of the targeted RNG.

The robustness of a crypto system depends on the key used, or in other words, the attacker's ability to estimate the key. The target RNG [8] defines the deterministic chaos as the true source of randomness, contrary to the latest RNG designs [10], [11] in which the equivalent noise generated by circuit components is analyzed.

The organization of the article is as follows. In Section II the targeted RNG is explained in detail; In the next Section III an estimate system is proposed for vulnerability analysis of the target RNG and its feasibility is verified; Section IV describes the numerical and simulation results that are followed by the noise analysis and the conclusion section.

II. Target System

Chaotic systems can be categorized into two groups: In relation to the evolution of underlying dynamical system, one is discrete time and the other is continuous time.

In the target paper [8], a simple autonomous continuous-time chaotic system is utilized, as the seed of the RNG, which is derived from a simple model. The analysis of the system yields the state equations given in [8] which transforms into the following equation:

$$\begin{aligned} \dot{x_1} &= y_1 \\ \dot{y_1} &= z_1 \\ \dot{z_1} &= a_1(-x_1 - y_1 - z_1 + sgn(x_1)) \end{aligned} \tag{1}$$

The equations in 1 generate chaos for the single-parameter a_1 in a large region ($0.48 < a_1 < 1$). The chaotic attractor used for numerical analysis is obtained for $a_1 = 0.666$ using a 4^{th}-order Runge-Kutta algorithm with an adaptive step size.

ISBN 978-90-827970-1-5

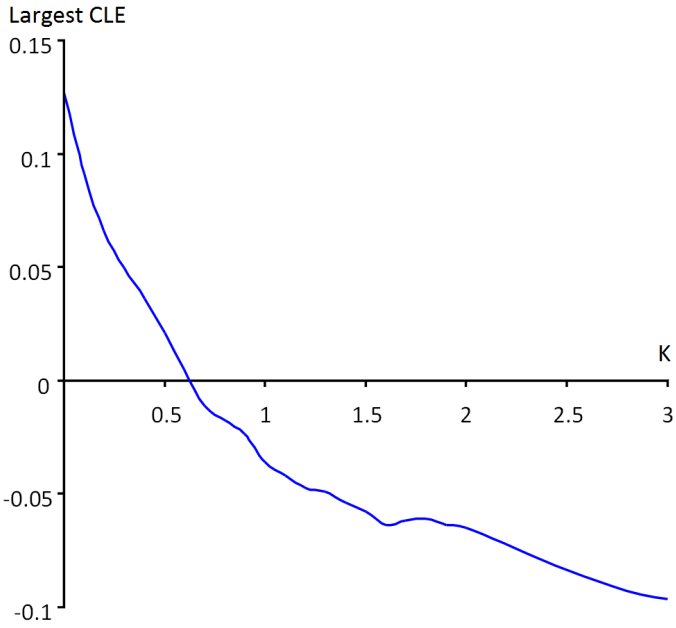

Fig. 1. Largest Conditional Lyapunov Exponents as a function of coupling strength K.

Random number generation method was explained in [8] where the mechanism fundamentally characterize the jumps in chaotic signal from one scroll to the other or staying at the same scroll. Because of this reason, the chaotic state-space is partitioned into three subspaces, P_0, P_M and P_1 divided by two planes located at p_2 and p_1. The binary sequence generated by this method is biased and do not fulfill the statistical tests. In order to remove the unknown bias in this sequence, the Von Neumann's de-skewing technique is employed.

The post-processed bit sequence given at http://www.esat.kuleuven.ac.be/∼mey/Ds2RbG/Ds2RbG.html does not also fulfill Block-frequency, Runs, Nonperiodic templates, ApEn and Random excursions variant tests of NIST-800-22 test suite [12]. Note that, the target RBG [8] do not fulfill the first secrecy criteria, which states that "TRNG must pass all the statistical tests of randomness."

III. Estimate System

Since the ground-breaking paper of Pecora and Carroll, the synchronization of chaotic systems has become an increasingly sought-after field of research [13]. In this article, the convergence of the estimate and target systems is proven using the auto-synchronization, (synchronization of chaotic systems with unknown parameters) [14]. In order to analyze vulnerability of the target RNG, an estimate system given by the following equation 2 is proposed:

$$\begin{aligned} \dot{x_2} &= y_2 \\ \dot{y_2} &= z_2 + K(y_1 - y_2) \\ \dot{z_2} &= a_2(-x_2 - y_2 - z_2 + sgn(x_2)) \\ \dot{a_2} &= -x2(y1 - y2) \end{aligned} \tag{2}$$

where K is the coupling strength between the target and estimate systems and a_2 is the unknown control parameter of the target system to be estimated. The information available are the structure of the target RNG system and a scalar time series given by a observable where $y_1 = \dot{x_1}$ is the observable chaotic signal given in 2.

For analyzing the stability of auto-synchronization, we numerically calculate the Conditional Lyapunov Exponents (CLE) using standard 4th-order Runge-Kutta algorithm with fixed step size. CLEs for the estimate system are calculated from the set of ordinary differential equations given in Eqn. 2 where QR decomposition method [15] is used. Numerical Jacobian is exploited which is calculated numerically by using finite differences. Offset for numerical Jacobian = $10^{-0.008}$ and integration time step is 0.004 while integration steps per Jacobian map is 50.

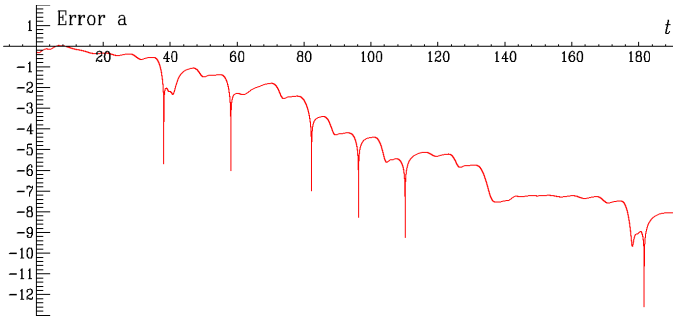

Fig. 2. Synchronization error Log $|e_a(t)|$ (red line).

In Fig.1, we plot largest CLEs as a function of coupling strength K. As shown in this figure, when K is greater than 0.63 then the largest CLE is negative and hence auto-synchronization of target and estimate systems is achieved and stable. For any K less than 0.63, largest CLE is positive and auto-synchronization is unstable.

IV. Numerical Results

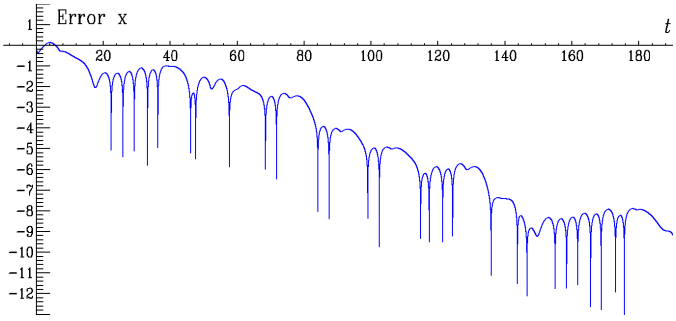

Fig. 3. Synchronization error Log $|e_x(t)|$ (blue line).

In this article, we numerically demonstrate the proposed estimate system using standard 4th-order Runge-Kutta algorithm with fixed step size. The estimate system expressed by the Eqn. 2 is designed that converges to target system as $x_2 \to x_1$ where $t \to \infty$ and t is the normalized time. Error signal a, x, y, and z of the auto-synchronization are defined as $e_a = a_1 - a_2$,

ISBN 978-90-827970-1-5 © EURASIP 2018

$e_x = x_1 - x_2$, $e_y = y_1 - y_2$ and $e_z = z_1 - z_2$ respectively. Here proposed estimate system aims to find out appropriate coupling strengths such that $|e(t)| \to 0$ when $t \to \infty$.

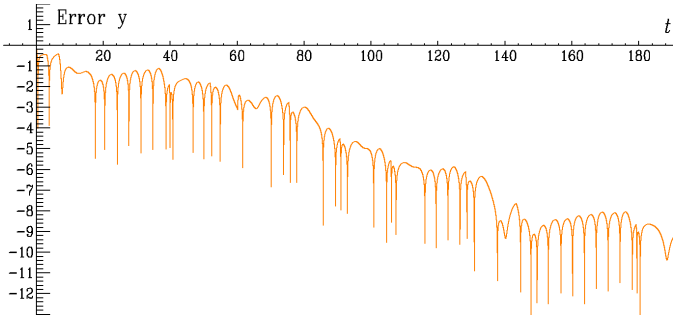

Fig. 4. Synchronization error Log $|e_y(t)|$ (orange line).

Log $|e_a(t)|$, Log $|e_x(t)|$, Log $|e_y(t)|$ and Log $|e_z(t)|$, are given as a function of normalized time t in Fig.2, Fig.3, Fig.4 and Fig.5 respectively, for $K = 3$. It is observed from the given figure that the auto-synchronization is achieved in less than $90t$, where the synchronization effect is better than that of $K = 0.64$.

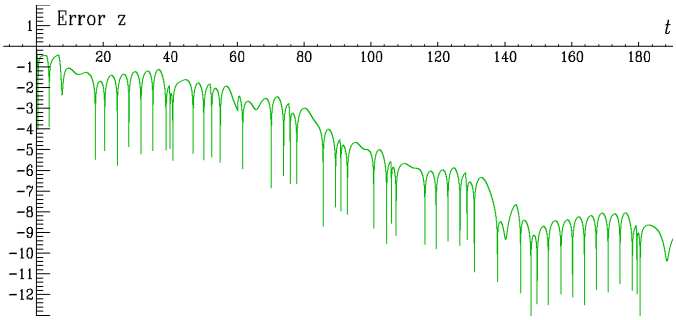

Fig. 5. Synchronization error Log $|e_z(t)|$ (green line).

Auto-synchronization of the estimate system is shown in Fig.6 where the convergence of the recovered parameter values a2 of the estimate systems to the known values a1 of the target system is illustrated. As shown from the given figure that, the proposed estimate system converges to the parameter a1 of the target system for $0.48 < a_1 < 1$ and auto-synchronization is achieved in less than $90t$.

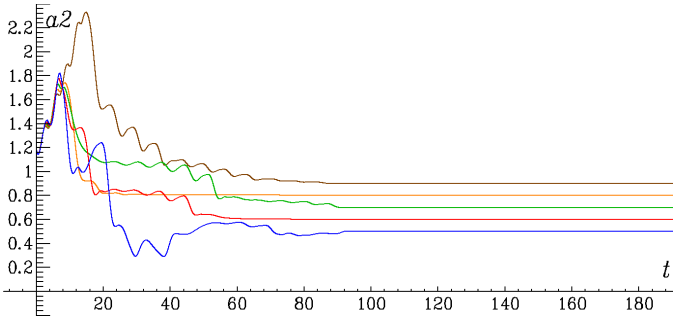

Fig. 6. Convergence of the parameter value a_2 of the estimate system to the fixed value a_1 of the target system for $0.48 < a_1 < 1$.

On the other hand, we have reported the other cryptanalysis results in [16] and [17] where [16] use master slave synchronization scheme. In this work, we propose a novel chaotic system and further focus on estimating the secret parameters from time series where auto-synchronization scheme is used. It should be also noted that the proposed estimate system is twice as fast as the previous one [17] where time to reach $Log(errorsignals) = -12$ error levels was reduced by half and it has been decreased from $280t$ [17] to $140t$ here.

Simulation results of $x_1 - x_2$, $y_1 - y_2$ and $z_1 - z_2$, are depicted in Fig. 7, Fig. 8 and Fig. 9, which show non-synchronized behavior and synchronization of target and estimate systems.

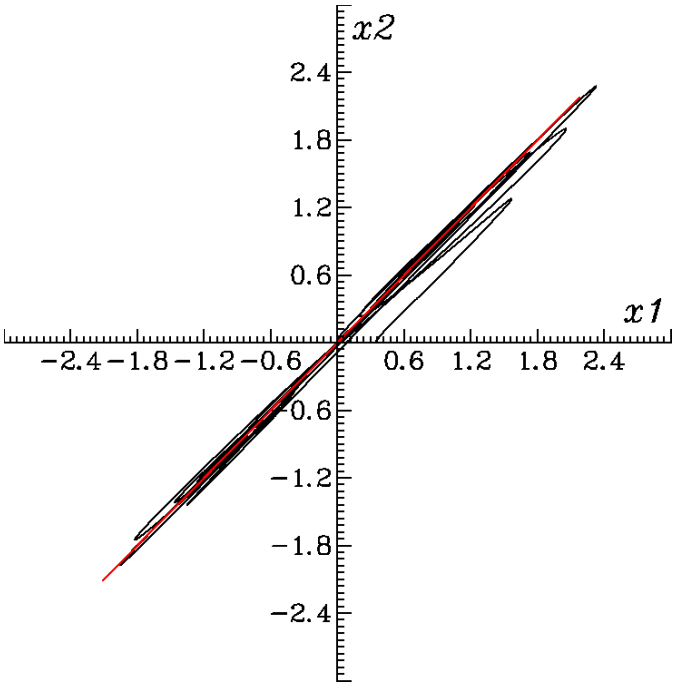

Fig. 7. Numerical results of $x_1 - x_2$ showing the synchronized and unsynchronized behaviors of target and estimate systems.

From the figures it is observed that stable identical synchronization can be achieved. In these figures, a synchronized phenomenon has not been observed initially as shown by the black lines. The proposed estimate system approaches the target system in less than $90t$ and the stable identical synchronization is obtained where these synchronized phenomenon are shown by colored lines in Fig. 7, 8 and Fig. 9, respectively.

Since the identical synchronization of estimate and target systems is achieved in less than $90t$ ($x_2 \to x_1$), the unknown parameters of the target random number generation system are accurately recovered and the estimated values of x_1, and S_i bit converge to their corresponding fixed values. As a result, it is clear that chaotic systems have achieved the identical synchronization and therefore the output bitstreams of the target and estimate systems are completely synchronized.

As a result, the proposed estimate system has not only reached the identical synchronization at the level of the chaotic state variables but also synchronized at the level of the

ISBN 978-90-827970-1-5 © EURASIP 2018

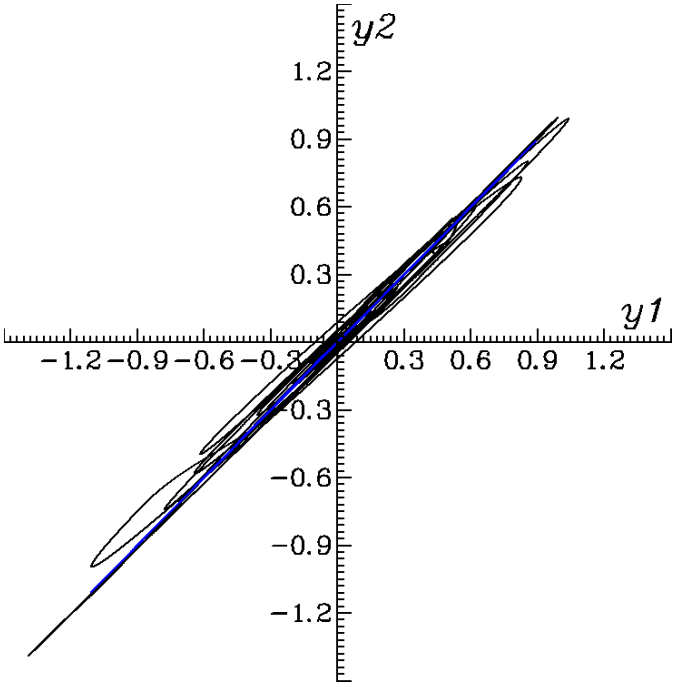

Fig. 8. Numerical results of $y_1 - y_2$ showing the synchronized and unsynchronized behaviors of target and estimate systems.

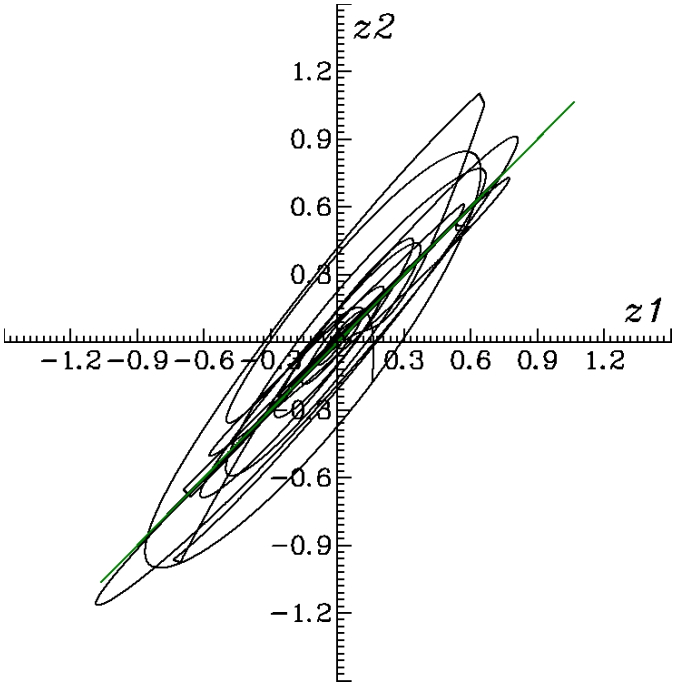

Fig. 9. Numerical results of $z_1 - z_2$ showing the synchronized and unsynchronized behaviors of target and estimate systems.

generated bit sequence. Proposed system not only estimates the preceding and following bits of the target RNG but also shows that the estimate system can generate the same output bit sequence of the target RNG. The target RNG [8] satisfies neither the second nor third secrecy criteria that an RNG must fulfill. In conclusion, it has been verified that deterministic chaos can not be the true source of randomness.

V. Conclusions

In this paper, an estimate system is proposed to discover the security weaknesses of a chaos based random number generator (RNG). It is shown that secret parameters of the RNG can be recovered by the proposed estimate system using auto-synchronization scheme. Although the only information available is the structure of the target RNG and a scalar time series, auto-synchronization of the estimate system is achieved and hence not only next bit but also whole output bit sequences are synchronized.

References

[1] Martin., K.: Everyday Cryptography: Fundamental Principles and Applications, 2^{nd} Edition, Oxford University Press (2017)

[2] N.C. Göv, M.K. Mıhçak, and S. Ergün, "True Random Number Generation Via Sampling From Flat Band-Limited Gaussian Processes," IEEE Trans. Circuits and Systems I, vol. 58, no. 5, pp. 1044-1051, May 2011.

[3] Schneier, B.: Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley Publishing, Inc. (2015)

[4] F. Pareschi, G. Setti, R. Rovatti, "Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems", IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 57, 12 (2010) 3124-3137.

[5] J. L. Valtierra, E. Tlelo-Cuautle, A. Rodrguez-Vzquez, "A switched-capacitor skew-tent map implementation for random number generation", International Journal of Circuit Theory and Applications, Vol. 45, 2 (2017) 305315.

[6] M. Kim, U. Ha, K. J. Lee, Y. Lee, H.J. Yoo, "A 82-nW Chaotic Map True Random Number Generator Based on a Sub-Ranging SAR ADC", IEEE Journal of Solid-State Circuits, Vol. 52, 7 (2017) 1953-1965.

[7] S. Ergün, "Modeling and Analysis of Chaos-Modulated Dual Oscillator-Based Random Number Generators," Proc. European Signal Processing Conference (EUSIPCO '08) pp. 1-5, Aug. 2008.

[8] M.E. Yalcin, J.A.K. Suykens, and J. Vandewalle "True Random Bit Generation from a Double Scroll Attractor.", IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 51(7). pp. 1395-1404, 2004.

[9] S. Ergün, S. Özoğuz, "A Chaos-Modulated Dual Oscillator-Based Truly Random Number Generator," Proc. IEEE International Symposium on Circuits and Systems (ISCAS '07), pp. 2482-2485, May 2007.

[10] S. Ergün, Ü. Güler, and K. Asada, "A High Speed IC Truly Random Number Generator Based on Chaotic Sampling of Regular Waveform" IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E94-A, no.1, pp.180-190, Jan. 2011

[11] S. Ergün, Ü. Güler, and K. Asada, "IC Truly Random Number Generators Based on Regular & Chaotic Sampling of Chaotic Waveforms" Nonlinear Theory and Its Applications, IEICE transactions, vol. 2, no. 2, pp. 246-261, 2011.

[12] L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, N. Heckert, J. Dray , "SP 800-22 Rev. 1a A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", Apr. 2010, http://doi.org/10.6028/NIST.SP.800-22r1a

[13] L.M. Pecora, T.L. Carroll, "Synchronization of chaotic systems," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 25, no. 9, 097611 pp. 1-12, Apr. 2015.

[14] Y. Liu, W. Tang, and L. Kocarev, "An Adaptive Observer Design for Auto-Synchronization of Lorenz System," International Journal of Bifurcation and Chaos, vol. 18, no. 8, pp. 2415-2423, Aug. 2008.

[15] J. P. Eckmann and D. Ruelle, "Ergodic theory of chaos and strange attractors," American Physical Society, Reviews of Modern Physics, vol. 57, no. 3, 1, (1985), pp. 617-656.

[16] S. Ergün, "On the security of a double-scroll based "true" random bit generator," 23^{rd} European Signal Processing Conference (EUSIPCO), Nice, 2015, pp. 2058-2061

[17] S. Ergün, "Cryptanalysis of a double scroll based "True" random bit generator," IEEE 58^{th} International Midwest Symposium on Circuits and Systems (MWSCAS), Fort Collins, CO, 2015, pp. 1-4.

ISBN 978-90-827970-1-5 © EURASIP 2018