Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–5.
ISSN-0037-8712
doi:10.5269/bspm.77855

FHE cryptographic systems with using chaotic secret key generation

Nibras Hadi Jawad

ABSTRACT: Security is a fundamental characteristic sought by researchers and sought by users above all else. Any system balances efficiency with application and information security as one of its most important prerequisites. No matter how efficient a service system is and the features it provides, security is paramount. Cryptography systems achieve the highest level of security. Among the modern encryption methods that help raise security and increase user confidence are homomorphic encryption schemes, which help complete tasks and conduct operations in an encrypted form. These systems operate by generating secret keys, which underlie the system's strength. This research discusses the integration of chaotic systems with fully homomorphic encryption to produce strong secret keys it is called DUff-skg. The idea uses a chaotic duffing scheme to provide high-quality randomness for FHE keys, combining key unpredictability with mathematical security. The results confirm effectiveness of the DUff-skg proposed key in homomorphic encryption systems.

Key Words: FHE, chaotic systems, duffing equations, secret key.

Contents

1. Introduction

Cryptographic systems require unpredictable, safe secret keys. Conventional key generation uses pseudorandom number generators to generate statistically random keys. Using secret key generators for encryption using chaotic dynamic systems methods gives more complex and better results. Chaotic systems are deterministic nonlinear systems that behave pseudo-randomly due to their sensitivity to initial conditions and parameters. A little change in the initial condition causes diverse trajectories, making the system's output uncertain without exact understanding [1]. These traits can create high-entropy cryptographic keys. This work discusses using the classical chaotic Duffing oscillator to generate secret keys in Fully Homomorphic Encryption (FHE) systems. FHE is a complex encryption algorithm that calculates on ciphertexts to provide encrypted outputs that match plaintext activities [2]. FHE security, like most encryption, depends on private keys. The idea uses a chaotic Duffing system to provide high-quality FHE key randomness, combining physical unpredictability with mathematical security. This work analyses FHE secret key creation using Duffing equations. We use first-order differential equations from the Duffing oscillator to build a key generator and study the translation of chaotic output into a binary secret key. the aim from this research is to demonstrate that Duffing chaos can produce statistically random, unreproducible cryptographic keys suitable for use in contemporary encryption techniques like FHE. Modern literature shows that chaos can be successfully integrated into encryption methods, such as hybrid chaos-based key generators with high entropy and standard randomness evaluations [3]. the

2010 *Mathematics Subject Classification:* 68P25, 68P27.
Submitted July 14, 2025. Published September 01, 2025

research links continuous-time chaotic dynamics to encryption technology by using these insights for FHE secret key creation.

2. Related work

In the paper of Challa R., and Gunta V. [4] (2021) proposes Reed-Muller-based symmetric key fully homomorphic encryption (FHE) to improve efficiency and security. Reed-Muller codes' algebraic features effectively compute homomorphic functions while preserving data in the preferred way. Experimental results reveal that the method outperforms current FHE systems in security. The work of Mortajez S., et al [5] (2020) improves DICOM picture encryption key generation using confusion and chaotic systems. Use a chaotic map with enhanced randomization and initial condition sensitivity to generate safe secret keys. These keys are coupled with a confusion-based permutation approach to confound DICOM picture pixel coordinates. The improved key generation method is computationally efficient and secure for medical imaging applications, according to experiments. Important medical data storage and transfer security issues are addressed. While Mohammed S. J., and Taha D. B. [6] (2021) presented a study that introduces a Chao-scattering-based privacy-preserving technique for partial homomorphic encryption (PHE). In this research, the Lorenz chaotic system is used to generate pseudo-random sequences to improve the encryption. The algorithm claims that key length and randomization determine encryption effectiveness. Imtiaz Ahamed, S., and Ravi, V. [7] (2022) Privacy A Privacy-Preserving Chaotic Extreme Learning Machine (ELM) utilizing Fully Homomorphic Encryption is proposed in the work. The recommended method generates weights and biases using a chaotic logistic map, improving model efficacy and data privacy. Chaotic ELM outperforms normal ELM in many datasets, especially healthcare applications, but somewhat poorer in finance datasets. The work reveals that chaotic dynamics with homomorphic encryption secure and optimize machine learning models. Su Y., Wang X., and Gao, H. [8] (2024) The purpose of this paper is bit-level feedback modification-based disordered picture encryption to secure data. The method uses chaotic systems, which are sensitive to starting conditions, to generate a secure key stream for visual data encryption. The research shows the algorithm's speed and durability, making it suitable for real-time applications. Jawad N. H., and Abdulhadi, S. [9] (2025) This work strengthens the Brakerski-Fan-Vercauteren (BFV) homomorphic encryption technique through chaos-based key generation. The suggested method generates secret keys using a modified 3D Lorenz chaotic system. Using chaotic trajectories, the key has a wider range (0 to 2^{279}) , making it resistant to brute-force attacks. This technique uses dynamic, unpredictable keys to secure BFV without reducing efficiency.

3. The Chaotic Behavior of Duffing Equations

Duffing equations are nonlinear. When applied, they produce complex, chaotic, nonlinear behavior with a cubic relationship between displacement and restoring force [10]. They are a two-dimensional, second-order nonlinear equation and their formula is as follows :
$x'_i = y_i$, $y'_i = Gama.Sin(Omega.t)–Delta.y_i–Alpha.x_i–Beta.x_i^3$, where i= 1...n. As Duffing shows a chaotic behavior according to pre -defined primary conditions (x_0, y_0) that are highly sensitive to it, thus giving a complex behavior with irregular paths. Duffing attractive also has a fractal dimension that shows complex repeated patterns based on specific parameters, each representing (Gama is amplitude, Omega is forcing, Delta is damping, Alpha is linear stiffness, Beta is nonlinear stiffness), [11].

4. Fully Homomorphic Encryption Algorithms

Fully homomorphic encryption techniques use a different approach to encrypt data. These techniques generate manipulable ciphertexts for calculations and operations. This technique protects consumer data when service providers process and encrypt it without decryption. Data is fundamentally secure, regardless of service provider confidence [12]. FHE relies on two types of homogeneous operations: addition and multiplication, which allows for more complex operations to be performed on encrypted data, with unlimited number of operations. Like other algorithms, FHE relies on a secret key known only to the data owner. This key is not shared with any other party (the server) for data processing, as the data is processed encrypted. Therefore, no one can decipher the plaintext without the secret key. Given the importance of this key and the strength and security it provides for FHE, it must be generated using

a sophisticated and random method, making it difficult for an attacker to identify or predict the secret key. There are several types of FHE algorithms to which the secret key can be applied, the most common of which in terms of speed and performance are BFV [13], CKKS [14], and TFHE [15], among others.

5. The Method of Generate Secret Key DUff-skg by Duffing Equations

The first component of the proposed key DUff-skg is parameter selection. The dynamic chaotic system uses parameters to build its routes. The initial parameter values must be carefully chosen for favorable outcomes. The tiniest change in initial values indicates a chaotic system's power, intricacy, and capacity to wander along dispersed paths. Secret keys (sk) for encryption techniques benefit from this sensitivity. The system analysis section demonstrates that the proposed system can utilize any initial values (x0, y0) to achieve satisfactory, convergent results. The values of the parameters that were adopted and gave the best results are as follows: (Gama=0.5, Omega= 2, Delta=0.1, Alpha= -1, Beta=2). The second component of the proposed system DUff-skg is numerical solution method used to solve Duffing equations is Runge-Kutta4, it depends on fixed step size (st= 0.01 for 1000 iterations) to ensure the system's dynamism, so you should choose carefully. The design of the two-dimensional chaotic system DUff-skg is based on the Duffing equations, whose equations were used after modification as follows:

$$x_i' = y_i + 0.5, \quad y_i' = x_i + \text{Gamma. } \cos(\text{Omega}\, t) - \text{Delta}.y_i - \text{Alpha}.x_i - \text{Beta}.x_i^3 \tag{5.1}$$

Where i=1...n, with initial values = (1.5, 1.0). The third part is extracting the sk from the values resulting by applying the modified Duffing equations, which yields a sk with chaotic values that are not repeated over the long term and are not related to each other. As acquiring a point is unattainable, it is difficult to know the prior points or predict the upcoming values. Then the sk calculate as follows:

$$sk = integer((x + y + 0.5).1000) \tag{5.2}$$

The values resulting from applying the modified Duffing equations are fractional values. To get an integer, we multiplied the result (x + y + 0.5) by 1000, then took the integer part and ignored the fraction. 0.5 was added to further complicate the equation. This sk as shown in Algorithm 1 was implemented in the BFV and CKKS algorithms. It can also be used with algorithms that effectively support bootstrapping operations. The original algorithms are mostly based on choosing random binary values, which makes the secret key weak and easy to guess. Instead of using a binary secret key, the proposed unpredictable key was used.

Algorithm 1 Secret Key Generation

Input: n (number of sk), chaotic parameters (Gamma, Omega, Delta, alpha, beta)
Output: set of sk with n numbers

procedure SECRETKEYGENERATION(n, Gamma, Omega, Delta, alpha, beta, initial values)
  $List\_sk \leftarrow \emptyset$
  for $i = 1, \ldots, n$ **do**
    $(x, y) \leftarrow$ duffing_sk(st, Gamma, Omega, Delta, alpha, beta, initial values)
    $sk \leftarrow$ integer$((x + y + 0.5) \times 1000)$
    $List\_sk \leftarrow$ append(sk, $List\_sk$)
  end for
  return $List\_sk$ with length n
end procedure

6. Experimental Result

The proposed key generator DUff-skg, which used the two modified Duffing equations, yielded good results based on the results provided by the NIST statistical tests, as shown in Table 1, which demonstrate the degree of randomness of the key. Key generation also relied on the use of seven parameters (Gama,

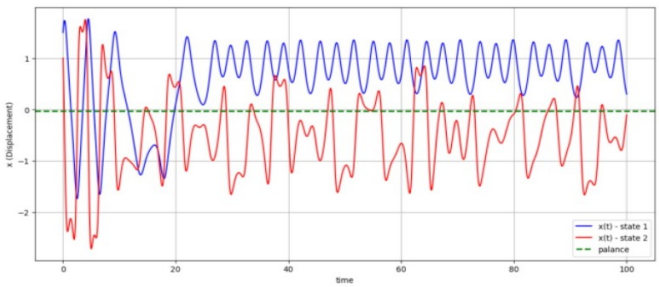

Figure 1: Proposed sk Behavior

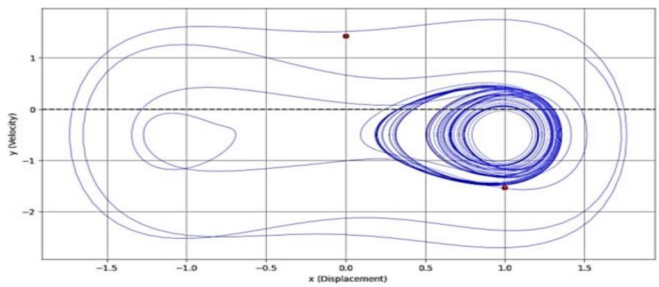

Figure 2: Hidden Attractor in Modified Duffing Oscillator

Omega, Delta, Alpha, Beta, x, y), meaning that the resulting key length would be $(10^{14})^7 \approx 2^{325}$ (where 10^{14} is computer computational power), which is much larger than the recommended minimum key size of 2^{128} bits. This large size of the key provides greater security than that provided by the traditional method of symmetric encryption algorithms, which are 21 in length. The system is sensitive to the slightest change in the initial values of x_0, y_0, which subsequently leads to significant changes in the key values in the long run, see in Figure 1. This is further confirmed by the amount of chaos achieved by the Lyapunov exponent, which yields a positive power of one (0.02701202947), which is evidence of the system's instability and its chaotic nature towards the hidden attractor see in Figure 2. The secret key generation DUff-skg took 1.43 seconds to execute, compared to traditional random binary number generators that take less than a fraction of a second, the security provided by this algorithm is much higher and stronger than the traditional method.

Table 1: Secret Key Testing Using NIST

Test	Input length	value
run	1000	0.71642507
Frequency (bit)	1000	0.22949314
Serial	100000	0.17024183
Linear complexity	1000000	0.55014026
Frequency (block)	1000	0.51811936
Discrete Fourier transform	1000	0.14679308
Binary matrix rank	38912	0.20495777
Overlapping template matching	1000000	0.01113558
Non-Overlapping	100	0.99999433
Cumulative sums	1000	0.16045173
entropy	1000	0. 9999999

7. Conclusion

This paper presents a novel method for generating secret keys DUff-skg that combines the strength of homomorphic encryption algorithms with the power of dynamic chaotic systems, the Duffing equations. It uses the chaotic Duffing approach to securely generate non-repeating secret keys with a randomness that is difficult for an attacker to know or predict. This method provides greater strength and security, despite consuming slightly more computational cost than traditional random number generators.

References

1. Hameed, B. A., and Gbashi, E. K. *A review of Chaotic Maps used for Generating Secure Random Keys*. In BIO Web of Conferences (Vol. 97, p. 00070). EDP Sciences, (2024).
2. Sharma, I. *Fully Homomorphic Encryption Scheme with Symmetric Keys*. arXiv Preprint arXiv:1310.2452, (2013).
3. Rukhin, A., Soto, J., and Nechvatal, J. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. NIST Special Publication, vol. 22, no. April, pp. 1/1-G/1, (2010).
4. Challa, R., and Gunta, V. *A modified symmetric key fully homomorphic encryption scheme based on Reed-Muller Code*. Baghdad Science Journal, 18(2), 42, (2021).
5. Mortajez, S., Tahmasbi, M., Zarei, J., and Jamshidnezhad, A. *A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential DICOM images*. Informatics in Medicine Unlocked, 20, 100396, (2020).
6. Mohammed, S. J., and Taha, D. B. *Privacy preserving algorithm using Chaos-scattering of partial homomorphic encryption*. In Journal of Physics: Conference Series (Vol. 1963, No. 1, p. 012154). IOP Publishing, (2021).
7. Imtiaz Ahamed, S., and Ravi, V. *Privacy-Preserving Chaotic Extreme Learning Machine with Fully Homomorphic Encryption*. arXiv e-prints, arXiv:2208, (2022).
8. Su, Y., Wang, X., and Gao, H. *Chaotic image encryption algorithm based on bit-level feedback adjustment*. Information Sciences, 679, 121088, (2024).
9. Jawad, N. H., and Abdulhadi, S. *Efficient Brakerski-Fan-Vercauteren Algorithm Using Hybrid-Position-Residues Number System*. International Journal of Mathematics and Computer Science, 20(2), (2025).
10. Ueda, Y. *Duffing's equation. Chaotic Oscillators: Theory and Applications*. 20, 26, (1992).
11. Kovacic, I., and Brennan, M. J. *The Duffing equation: nonlinear oscillators and their behavior*. John Wiley and Sons, (2011).
12. Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C. A., and Strand, M. *A guide to fully homomorphic encryption*, Cryptology ePrint Archive, (2015).
13. Iliashenko, I., and Zucca, V. *Faster homomorphic comparison operations for BGV and BFV*. Proceedings on Privacy Enhancing Technologies, (3), 246-264, (2021).
14. Lv, Y., Han, Y., and Wang, Z. *Fast CKKS Algorithm in the SEAL Library*. In International Conference of Pioneering Computer Scientists, Engineers and Educators (pp. 139-152). Singapore: Springer Nature Singapore, (2024).
15. Chillotti, I., Gama, N., Georgieva, M., and Izabachene, M. *TFHE: Fast Fully Homomorphic Encryption Over the Torus*. (pp. 0–62), (2023).

Nibras Hadi Jawad,
Department of Mathematics,
University of Al-Qadisiyah,
Al-Qadisiyah, Iraq.
E-mail address: nibras.hadi@qu.edu.iq