

FPGA CENTRIC ATTENTION BASED DEEP LEARNING
NETWORK EVOKED CHAOTIC ENCRYPTION
TO MITIGATE SIDE CHANNEL ATTACKS

Mani Karthikeyan[#], Vediappan Ponniyin Selvan

Received on February 24, 2023

Presented by S. Margenov, Corresponding Member of BAS, on April 25, 2023

Abstract

Security concerns are growing, especially in applications where sensitive information is sent (such as health care devices, credit cards, and even Internet of Things (IoT) nodes), even while these developments bring in a modern revolution. This is due to the constant scaling of technologies, which has now been incredibly useful for delivering the new trend of development in the numerous domains such as communications, semiconductors, health care, and automation. Even when cutting-edge standard encryption algorithms are used in smart devices, the principal threats, such as Side-Channel Attacks (SCA) and Correlation Power Analysis (CPA), increase the susceptibility of encrypted cipher text to attacks. In order to defend against side channel assaults, the usefulness of deep learning algorithms combined with chaotic principles is examined in this paper. Scroll Mapping (SM) and Attention-Evoked Long Short-Term Memory (AE-LSTM) are used in the proposed study to effectively safeguard sensitive data while consuming little power. The most promising advancements in terms of all security metrics and hardware capabilities for obtaining high-speed performances are shown by experimental findings on an FPGA implementation of a suggested framework.

Key words: side channel attacks, deep learning algorithm, attention evoked long short-term memory, scroll maps, FPGA

[#]Corresponding author.

DOI:10.7546/CRABS.2023.06.14

Introduction. In the era of pervasive computing, penetration of Internet in the people's life zone has become unavoidable. This leads to a number of benefits, including ubiquitous communication and simple activity tracking. On the other hand, this scenario reveals the darker side in which the securing and protecting the user data against the growing attacks seems to be more complex. To brighten this darker side, several encryption schemes were embedded in the hardware processors to safeguard the sensitive data against the multiple attacks. But still, tricky attacks such as Side Channel Attacks (SCA) and Correlation Power Analysis (CPA) pose serious threats in which the data are hacked through the physical emissions from the physical devices. Apart from that, under SCA, an adversary would not exploit the physical emissions, or side channels, directly from the device, including power consumption [1], execution time [2], and electromagnetic emission [3], to retrieve meaningful data while taking advantage of a cryptographic algorithm's mathematical flaws. These physical emissions' potential connection to the data processed by the gadget serves as the foundation for the SCA theory.

Recently, machine and deep learning algorithms are integrated with the encryption techniques to form the hybrid schemes that overcome the SCA attacks. But integrating the complete integration again leads to the computational overhead that results in the high power consumption that makes SCA a super threat to the sensitive data. SCA has unquestionably grown in importance over the past 20 years, posing a severe threat to security and a serious problem for cryptographic hardware designers, making it a key area of focus for the creation of secure devices.

Motivated by this aforementioned problem, this research article proposes the hardware centric intelligent encryption schemes which integrate the high performance and complexity aware deep learning model triggered Chaotic Scroll Encryption technique (CSE). Note that, to the best of our knowledge, hardware centric intelligent cryptographic processors with low computational overhead have not been designed to safeguard the user data against the SCA complications. The following are the paper's primary contributions:

1. Proposes the low complexity and hardware deployable deep learning model based scroll encryption technique to safeguard the SCA attacks. The principles of AE-LSTM are employed to defend the SCA which also aids for the strong countermeasures against the SCA measures.
2. Employs the Strong Hybrid Scroll Chaotic algorithm to produce the high randomness keys to mitigate the SCA scenario. Also to ensure the data protection against SCA, traditional mathematical operations are replaced with the DNA operations to form the protective cover for the sensitive data against the SCA.
3. Hardware implementation was done on a Xilinx XC7Z020 PYNQ-Z2 FPGA

platform, and performance was assessed in terms of computational complexity and security analysis.

The paper outline is presented as follows. Section 2 covers the brighter insights of the proposed intelligent cryptographic frameworks. The experimental implementation, performance analysis and results discussion are presented in Section 3. Finally the paper is concluded with the future enhancements in Section 4.

Proposed methodology. The suggested encrypted architecture used in the FPGA for forging side channel assaults is explained in full in this section's operational mechanism. Figure 1 shows the general architectural layout. The suggested design takes into consideration the vulnerabilities foreseen by SCA in other studies while also drawing inspiration from some of our earlier work [4]. The suggested system is made up of a sophisticated deep learning model, as seen in Fig. 1 that operates on the idea of self-attention maps combined with lengthy short-term memory. The chaotic maps' beginning conditions are the output features from the deep learning model. Then the chaotic maps are constructed using Multi-Scroll principles which are then used to encrypt the plain text data. The working mechanism of each and every layer deployed for building the encryption scheme is explained in the preceding section.

Attention evoked long short-term memory (AELSTM). This section presents the working principle of Long Short-term memory (LSTM), Self-attention maps and attention evoked LSTM networks.

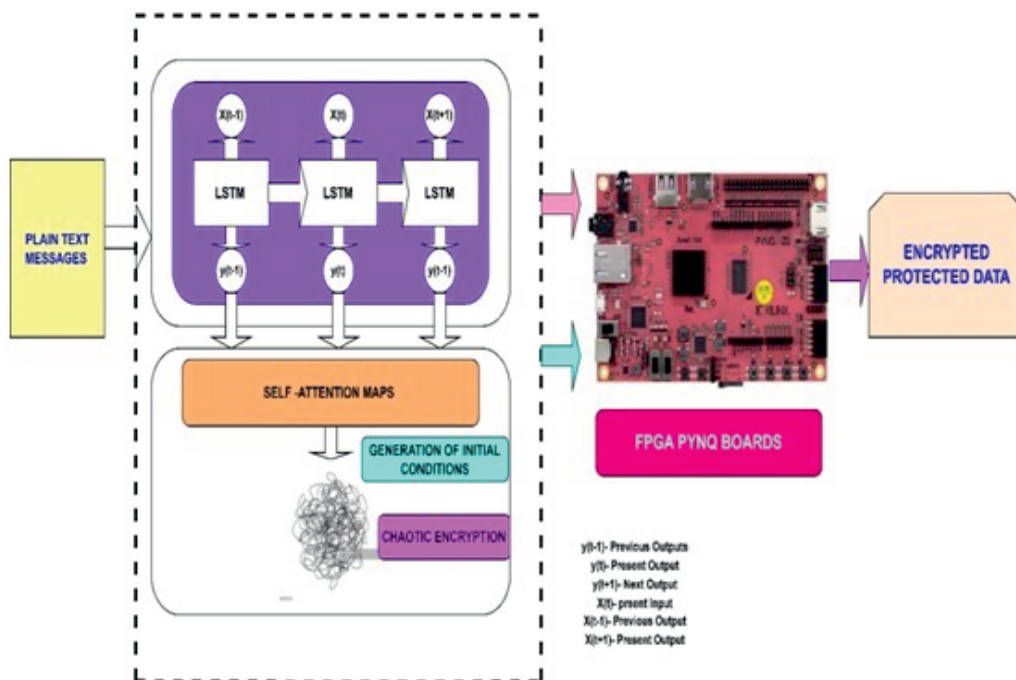


Fig. 1. Overall systematic framework for the proposed encryption architecture

LSTM Layers. Initially the LSTM layer is introduced as a form of Recurrent Neural Network (RNN) [5]. In [6] and the references therein, more contemporary formalisms and investigations of LSTM RNN are discussed. Speech processing and language translation [7] are a few successful examples of uses. Input, forget, and output gate (j_t, T_f, T_o) are the three gates that make up the common LSTM layer. A duplicate of the RNN's "input block" exists in each gate. The main equations for this common LSTM layer are provided in [8] and the references therein. The memory is updated by the output and forget gates of an LSTM by combining the output of the prior unit with the current input state. Calculate the states of the three gates and the input gates for the cell first. The proposed encryption architecture's overarching systematic structure is shown in Fig. 1.

The following equation presents the input gate

$$(1) \quad j_t = \theta(G_l^i \cdot O_t + G_h^i \cdot e_{t-1} + s_i).$$

The following equation represents the forget gate

$$(2) \quad T_f = \theta(G_l^f \cdot O_t + G_h^f \cdot e_{t-1} + s_f).$$

The following equation calculates the output gate

$$(3) \quad T_o = \theta(G_l^o \cdot O_t + G_h^o \cdot e_{t-1} + s_o).$$

The following equation calculates the cell input

$$(4) \quad \tilde{T}_C = \tanh(G_l^C \cdot O_t + G_h^C \cdot e_{t-1} + s_C).$$

Here $G_l^0, G_l^f, G_l^i, G_l^C$ are the weight matrices connecting the input gates to the output layers whereas $G_h^i, G_h^f, G_h^o, G_h^C$ are the weight matrices connecting the gate inputs to the hidden layers. Also s_i, s_f, s_o, s_C are the bias vectors and $\tanh$ is considered to be hyperbolic function.

To help the LSTM layers to extract only effective features that can aid for the encryption, attention maps are integrated at the LSTM cell. The detailed description of self-attention maps and its characteristics are described in [9]. The most useful elements that may be used to create the very unpredictable beginning circumstances that aid in improved protection are determined by this module. To identify the most efficient features, it constructs a probabilistic distribution of channels and multiplies them by input. Correspondingly, each feature extracted by LSTM is assigned with an appropriate weight and features are integrated to form the final features. As described in [10], overall self-attention based LSTM features are given as follows:

$$(5) \quad F(t) = \sum_{t=1}^T \text{Softmax}(w^t \tanh(\beta W + B_x)).$$

For an effective extraction of features from sensitive data, three layers of LSTM units are integrated with self-attention layers which are driven by activation ReLu function.

AE-LSTM based scroll chaotic encryption. The extracted features are then selected randomly and fed to the dynamic scroll attractors. Multi-scroll attractors are dynamic systems that can exhibit more complex characteristics than the other traditional scroll attractors. The main advantage the scroll maps that triggered to formulate this research is mentioned in [11,12]. The characteristics equation for automatic chaotic system is given by

$$(6) \quad \dot{x}_1 = -ax_1 + bx_2x_3,$$

$$(7) \quad \dot{x}_2 = -cx_2^3 + dx_1x_3,$$

$$(8) \quad \dot{x}_3 = ex_3 - fx_1x_2.$$

The above equations (1)–(3) can be modified by adding the hyperbolic equation $p_1 \tanh(x_2 + g)$ which is given in

$$(9) \quad \dot{x}_1 = -ax_1 + bx_2x_3,$$

$$(10) \quad \dot{x}_2 = -cx_2^3 + dx_1x_3,$$

$$(11) \quad \dot{x}_3 = ex_3 - fx_1x_2 + p_1 \tanh(x_2 + g).$$

Chaotic attractor is obtained when $a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, $g = 2$, and the chosen initial conditions are $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$. Figure 2 illustrates the proposed architecture's (a) bifurcation diagram and (b) phase portrait components.

Proposed encryption process. As discussed in Section 2, AE-LSTM features are then randomly selected and used as the initial conditions for formulating the high randomness encrypted data. Algorithm-1 (see next page) presents the whole operational framework for the suggested encryption procedure.

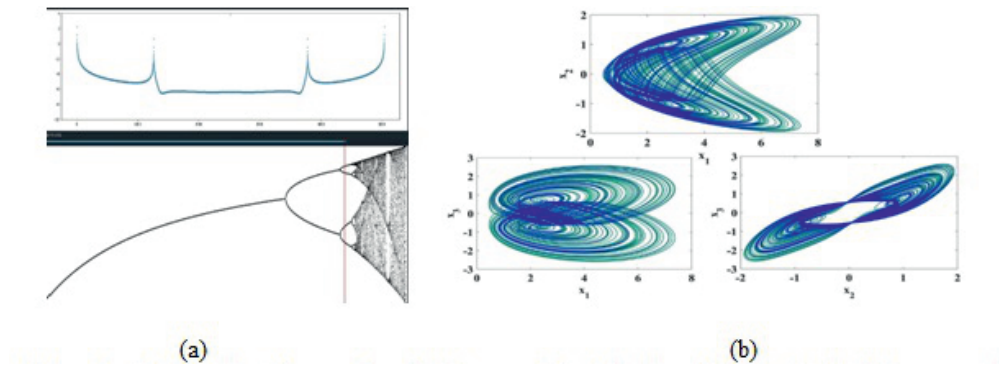


Fig. 2. a) Bifurcation diagram for the proposed architecture; b) Phase portrait components

Algorithm-1. Working principle of the proposed encryption process

Step 1: As the first step, initial conditions for the scroll maps have been generated. In this case, proposed research employs the deep learning algorithm as mentioned in Section 2. The LSTM and attention maps are used to generate the features which are randomly selected for the initial conditions to design the scroll maps.

Step 2: Deep learning Scroll Maps (DLSM) are created based on the initial conditions formed in previous step.

Step 3: To form the high randomness keys, DLSM and medical data are then computed by DNA operation D to form the high randomness key (R_k)

$$R_k = D(I, \text{DLSM}(X, Y, Z))$$

I = IoT Sensor values and X, Y, Z are the Scroll based Chaotic matrix Values.

Step 4: The keys R_k which are formulated in Step 4 are then diffused (D) with DLSM maps to form their strong encryption keys. Since ID's and chaotic matrix are different in size, these values are scaled in accordance with the IoT devices' address length L

$$\text{Encrypted Data} = D(R_k, \text{DLSM}(X, Y, Z)) \text{ scaled to } L.$$

FPGA implementation of the proposed encryption process. The proposed learning-based chaotic process was implemented using the Xilinx PYNQ Z-2 FPGA board. Hardware and software co-design methodologies have been used for the implementation of both learning networks and chaotic encryption processes. The suggested encryption model was created in Verilog using a 32-bit floating-point data format and implemented on a PFPGA utilizing Xilinx VIVADO 2022.2.13 design suites.

In this deployment, hardware-software partition methodology is followed in which the deep learning models are implemented in soft processors and chaotic encryption technique is deployed in programmable FPGAs. The initial conditions are pre-computed using AE-LSTM which runs on the software processors and is transmitted to the PFPGA using the DMA (Direct Memory Access) Ports which interconnect with the chaotic countermeasure architecture. In PFPGA, the proposed scroll maps are synthesized using Pipelined Configurable Distributed Arithmetic Architectures (PCDAA) in which the configurable LUTs are used instead of traditional LUTs for storing the pre-computed initial conditions. Thus better area utilization is achieved with less delay and low power consumption. The inner permutation and diffusion operations are calculated by an N-cycle of shift accumulation followed by the memory-read operation.

Results and discussion. This section evaluates the efficiency, speed (throughput and maximum frequency), and performance of the recommended encryption scheme. Also, the effectiveness of the suggested method is evaluated in comparison

T a b l e 1

Speed performances for the different encryption model implemented
on the FPGA

Performance	Encryption model [13]	Encryption model [14]	Encryption model [15]	Proposed encryption model
WNS	-19.45	-18.32	-19.55	-19.89
Max. frequency (Hz)	300	320	204	375
Throughput (Mbps)	1180.45	1167.56	1189.44	1290.00
Efficiency (Mbps/Slices)	70%	73%	76%	95%

with the other encryption approach in terms of hardware resources, throughput, and statistical robustness (NIST test). Our total understanding of the hardware metrics performance of the implementation is provided by the efficiency parameter. The numerical representations of the experiment's metrics are given in following equations

$$(12) \quad \text{Max Frequency(Max.Fre)} = 1/(T - W),$$

where $T \rightarrow$ Target based Clock Cycles, $W \rightarrow$ Worst Negative Slack of the clock period

$$(13) \quad \text{Throughput} = N * \text{Max.Fre (Mbps)},$$

where N – Clock period

$$(14) \quad \text{Efficiency} = \text{Throughput/Slices (Mbps/Slices)}.$$

In Table 1, the hardware metrics of several chaotic and non-chaotic systems that are currently in use are compared. The suggested model has produced hardware performance that is more competitive than that of current chaotic and non-chaotic systems when taking into account the FPGA's clock rate, throughput, and efficiency.

The complete Structure was implemented in the FPGA with the proposed architectures. Since the Scroll maps and Deep learning algorithms are implemented in the FPGA, performance of the proposed model is identified to even single bit changes when implementing the FPGA architecture. Even one bit change in the inputs will change the location of bits in LUT in which it may become highly impossible for the intruder to track the data. When ported to the FPGA, it may be useful for mitigating the side channel attacks.

➤ NIST standard tests:

A secure pseudo-chaotic number generator must also be able to create sequences that pass the 188-test statistical NIST test, which assesses the randomness of lengthy binary sequences. This is a crucial critical characteristic of a safe

pseudo-chaotic number generator. The beginning circumstances and the chaotic system's characteristics were used to create 100 pseudo-chaotic sequences with a 256-bit length for the NIST test. Each test result was represented by a set of 100 p -values that were computed.

A p -value more than or equal to 0.01 (the test's threshold of significance) infers that the sequence must be random, while a p -value less than or equal to 0.01 shows that the sequence is not random. The number of p -values divided by 100 determines the percentage of 100 sequences that pass a test. The findings, which are shown in Table 2, infer that the sequences produced cleared all 15 statistical tests and demonstrated their high unpredictability property, which is necessary to fend off side channel attacks.

T a b l e 2
NIST standard test results for the proposed model

Sl. No	NIST test specification	Status of test	p -value	Proportion %
1	DFT Test	PASS	0.7884	100
2	Run Test	PASS	0.65363	99.45
3	Long Run Test	PASS	0.76733	99.92
4	Frequency Test	PASS	0.542920	99.90
5	Block Frequency Test	PASS	0.66234	100
6	Frequency Mono Test	PASS	0.64556	100
7	Overlapping Template of All One's Test	PASS	0.67893	99.45
8	Linear Complexity Test	PASS	0.75640	99.67
9	Matrix Rank Test	PASS	0.80393	100
10	Lempel-ZIV Compression Test	PASS	0.780202	100
11	Random Excursion Test	PASS	0.89034	100
12	Universal Statistical Test	PASS	0.88320	99.75
13	Cumulative Sum Test	PASS	0.39202	99.80
14	Linear Complexity Test	PASS	0.7563	99.80

The Logistic Maps and LSTM networks are used for which the encrypted data are subjected to the partial verification of NIST standard tests and consume more resources which may fit partially in the FPGA to counterfeit the side channel attack. In our research, the modified Logistic maps with the powerful and more dynamic scroll maps which can even more exhibit the randomness and strong counterfeit activities against the side channel attacks. Moreover, FPGA resource consumption is also low when compared with the existing work. The novelty of the work is proved in replacing the existing counterfeits and deep learning algorithm with our newly combined algorithm that has been proved in the results by using NIST and FPGA resources [4].

Conclusion and future enhancement. In this paper, hardware centric intelligent and high randomness chaotic encryption implemented on Xilinx PYNQ platforms are proposed. The proposed scheme includes powerful features of deep learning model that triggers high randomness chaotic systems to produce the high

defensive encrypted data that can counterfeit the side channel attacks. Cryptographic strength and hardware metrics for the proposed model were examined and contrasted with those of the other encryption methods currently in use to demonstrate its superiority. The suggested encryption model is the best option for encrypting sensitive data, as shown by all of the results that were collected. The suggested model's future work will concentrate on innovation in terms of building the light-weight intelligent chaos-based encryption to protect the Internet of Things (IoT) data and to be implemented in small processors to fight side channel assaults in real-world applications.

REFERENCES

- [1] SAAD A., H. FOUAD, H. ALGINAHI YASSER, W. SAID (2022) Connection adjustable network slicing process for heterogeneous service handling in real-time applications, *J. Nanoelectron. Optoelectron.*, **17**(1), 158–169.
- [2] SRIVASTAVA A., P. GHOSH (2019) An efficient memory zeroization technique under side-channel attacks. In: *Proc. Int. Conf. Embedded Systems*, Delhi, India, 76–81, <https://doi.org/10.1109/VLSID.2019.00032>.
- [3] ANTOGNAZZA F., A. BARENGHI, G. PELOSI (2021) Metis: an integrated morphing engine CPU to protect against side channel attacks, *IEEE Access*, **9**, 69210–69225.
- [4] KARTHIKEYAN M., V. PONNIYIN SELVAN (2022) A novel hybrid reconfigurable architecture for prediction of side channel attacks with its countermeasure mechanism, *J. Nanoelectron. Optoelectron.*, **17**(7), 1056–1067.
- [5] HU F., H. WANG, J. WANG (2021) Deep-learning side-channel attack against STM32 implementation of AES. In: *Proc. Int. Conf. Comput. Sci. Comput. Intell.*, Las Vegas, NV, USA, 844–847, <https://doi.org/10.1109/CSCI54926.2021.00030>.
- [6] CHANG L., Y. WEI, S. HE, X. PAN (2022) Research on side-channel analysis based on deep learning with different sample data, *Appl. Sci.*, **12**, 8246, <https://doi.org/10.3390/app12168246>.
- [7] KORIYAMA T., H. SARUWATARI (2020) Utterance-level sequential modeling for deep Gaussian process based speech synthesis using simple recurrent unit. In: *IEEE Int. Conf. Acoustics, Speech & Signal Processing*, Barcelona, Spain, 7249–7253, <https://doi.org/10.1109/ICASSP40776.2020.9052935>.
- [8] HOU H., Z. DI, M. ZHANG, D. YUAN (2022) An intrusion detection method for cyber monitoring using attention based hierarchical LSTM. In: *IEEE 8th Intl Conf. Big Data Security on Cloud (BigDataSecurity)*, *IEEE Intl Conf. High Performance and Smart Computing, (HPSC)* and *IEEE Intl Conf. Intelligent Data and Security (IDS)*, Jinan, China, 125–130, <https://doi.org/10.1109/BigDataSecurityHPSCIDS54978.2022.00032>.
- [9] SHARMA D., C. DHIMAN, D. KUMAR (2022) Automated image caption generation framework using adaptive attention and bi-LSTM. In: *IEEE Delhi Section Conf. (DELCON)*, New Delhi, India, 1–5, <https://doi.org/10.1109/DELCON54057.2022.9752859>.

- [10] QIN G., X. NIU, J. WANG, Q. QIAN (2021) Traffic flow prediction based on JANet and attention mechanism. In: 2021 6th Int. Conf. Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 131–134, <https://doi.org/10.1109/ICSP51882.2021.9408777>.
- [11] YANG Y., L. HUANG, J. XIANG, Q. GUO (2022) Three-dimensional sine chaotic system with multistability and multi-scroll attractor, IEEE Trans. Circuits and Systems II: Express Briefs, **69**(3), 1792–1796, <https://doi.org/10.1109/TCSII.2021.3126227>.
- [12] DENG J., K. DENG (2021) Design of multi-scroll chaotic attractors based on tempered fractional differential systems. In: 2021 7th Int. Conf. Systems and Informatics (ICSAI), Chongqing, China, 1–6, <https://doi.org/10.1109/ICSAI53574.2021.9664115>.
- [13] HUANG X., M.M. WONG, A.T. DO, W.L. GOH (2021) A backpropagation extreme learning machine approach to fast training neural network-based side-channel attack. In: 2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Shanghai, China, 1–6, <https://doi.org/10.1109/AsianHOST53231.2021.9699677>.
- [14] ALIPOUR A., A. PAPADIMITRIOU, V. BEROLLE, E. AERABI, D. HÉLY (2020) On the performance of non-profiled differential deep learning attacks against an AES encryption algorithm protected using a correlated noise generation based hiding countermeasure. In: 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 614–617, <https://doi.org/10.23919/DATE48585.2020.9116387>.
- [15] YU. H, H. SHAN, M. PANOFF, Y. JIN (2021) Cross-device profiled side-channel attacks using meta-transfer learning. In: 2021 58th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 703–708, <https://doi.org/10.1109/DAC18074.2021.9586100>.

*Department of Electronics
 and Communication Engineering
 Mahendra College of Engineering
 Salem, Anna University
 636106, India
 e-mails: ramkartik9@gmail.com
 vponniyinselvan@gmail.com*