Chaotic-based Security for Near Field Communication in Internet of Things Devices

Colin Sokol Kuka
Department of Electronic Engineering
University of York
Heslington
York YO10 5EZ
United Kingdom
sk1759@york.ac.uk

James Chandler
The City of Liverpool College
Liverpool L3 6BN
United Kingdom
James.Chandler@liv-coll.ac.uk

Mohammed Alkahtani
University of Liverpool
Liverpool L69 3BX
United Kingdom
m.alkahtani@liverpool.ac.uk

***Abstract*—The security of wireless systems has become a growing challenge resulting from the expansion of the Internet of Things (IoT) into everyday life. Despite the many advantages driving the adoption of IoT devices, their proliferation increases the surface susceptible to advanced attacks that aim to misuse their resources and cause interruptions, delays, losses and degradation of the offered services in IoT. This paper introduces a chaotic transmission for Near Field Communication (NFC) Topology, based on the Wireless Power Transfer (WPT) systems. Traditional WPT circuits are based on inverters to create an oscillation for the transmitter coil. This results in systems relying only on software security. Therefore, we have introduced this topology which adopts chaotic encryption for NFC security. Furthermore, the proposed system is immune to Man-in-the-Middle (MitM) attacks. The simulation results and tests prove the functionality of the chaotic WPT based on the Chua's diode and their synchronisation between transmitter and receiver. The chaos generated is sampled by an electronic board and can be used for cryptography coding based on Python. The application for this system is a new NFC digital code for accessing the IoT services.**

Keywords–Cryptography, Chaotic transmission, Digital key, High Security, Chua diode, Man-in-the-Middle (MitM) attack immune, Near Field Communication (NFC), Wireless Power Transfer (WPT), Internet of Things (IoT).

I. INTRODUCTION

The Internet of Things (IoT) is the product of recent developments in energy and cost-efficient computing and cloud/wireless infrastructure. The IoT has been a major driver of scientific, technological, economic, and social change 1. IoT also comes with a set of requirements [1]: ultra-low power consumption for long-term autonomous operation without the ability to recharge the battery; the need to communicate with other devices; the need to operate efficiently in harsh environments; and the ability to withstand malicious cyber-attacks (including both: remote attacks mounted through network connections and physical attacks by adversaries) [2]. Our everyday lives are intertwined with modern cryptographic schemes. The majority of available cyber-defenses are based on securing electronic systems' software or their communication interfaces [3].

Most everyday IoT devices use the Near-Field Communication (NFC), which is a recent short-range communication system that can be used for anything from physical access control to contactless payments [4]. The NFC transponder is the most important part of the device because it enables data to be read and written. There are several different types of NFC tags, each with its own form, scale, and construction material, but they all fall into two categories [5], [6]. One group is the active NFC, in which the system uses its own power source, which is normally a long-lasting battery. The other type is passive, which means they don't have their own energy source and instead rely on the electromagnetic field produced by the transponder [7], [8]. To relay information over a short distance, NFC uses electromagnetic induction between two loop antennas at a particular frequency. The data is stored in tiny microchips (or tags) and sent to readers within a certain physical range [9].

NFC devices using the WPT operating principle rely on the resonance by magnetic means of an alternating current in coupled LC circuits. In near-field, the mutual inductance at high frequency of both antenna coils acts as a loosely (roughly) magnetically coupled transformer, where energy is magnetically induced and propagated from the primary to the secondary coil. For short-range tasks such as a gap of few centimetres, the working frequency of the resonant circuit is generally in the range from 10 kHz to a few MHz [10], [11].

In this work, we present a WPT topology with advanced security capabilities based on the Chua's diode. The circuit exhibits a typical two attractor chaotic behaviour. Thanks to this unique non-linearity, it is possible to adopt a mutual authentication key based on the last state and its subsequent encryption and decryption. Furthermore the WPT system is immune to man-in-the-middle (MitM) attacks.

The memristor or Chua's diode is a circuit element based on the electrical charge q and the magnetic flux φ. Its constitutive relationship is theorised by Prof. Leon Chua [12]. This device can create chaos from the well known Chua's circuit shown in Fig. 2. Memristors with their non-linearities are properly integrated into existing electronic circuits to create several new chaotic behaviour circuits [13], [14] as depicted in Fig. 3. Dynamic behaviours, such as chaos and hyper-chaos [15], [16], coexisting multiple attractors [17], [18], hyper-chaotic multi-wing [19], [20] and hidden attractors [21], [22] have been studied and analysed by numerical simulations and hardware experiments.

 ISBN: 978-1-61208-838-9

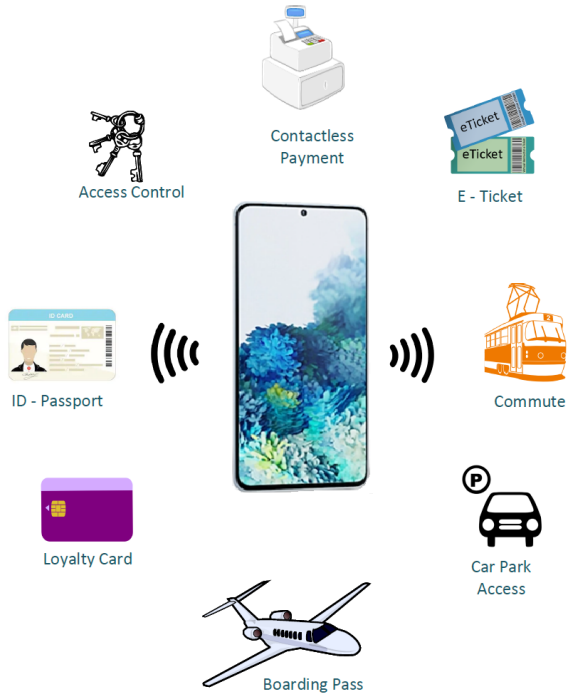

Figure 1. Example of IoT devices used in everyday life which rely on the NFC and the WPT techniques.

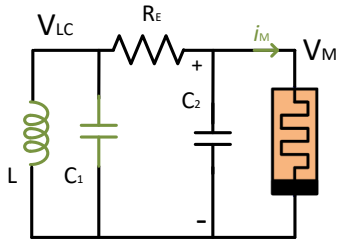

Figure 2. Traditional Chua's circuit

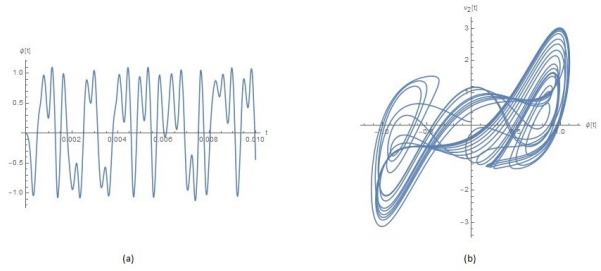

Figure 3. Typical chaotic behaviour waveform of the voltages in the inductor (**a**) and capacitor in a XY mode representation (**b**).

In this work, we therefore propose a low power Chua's diode circuit architecture for WPT systems. The system has the quality of transmitting power and data wirelessly. In addition, the system has the ability to achieve the highest level of encryption due to the chaotic behaviour. One of the biggest advantage for this system is the low power consumption. The rest of the document is organized as follows. The wireless power transmission circuit and encryption and decryption capabilities are shown in the next section. In Section III, there is an analysis of the WPT based on memristor. System functionality and simulation results are presented in Section IV. Finally, Section V concludes the document.

II. Wireless Power Transfer and Chua's Diode

Near Field Communication (NFC), which is commonly used in smartphones as presented in Figure 1. The NFC are also used contactless credit cards and digital keys, is a special form of WPT device that is very sensitive to the problem of cryptography [23], [24]. NFC is a low-bandwidth, two-way wireless communication technology that uses electromagnetic induction to transfer data between devices separated by up to ten centimeters. Internal user data on access cards and digital keys is encrypted by software and stored in a computer. The Hash function has historically been used to encrypt data. This form of algorithm is well-known and subject to a number of attacks easily accessible through the Internet [25]–[27]. This confidential information must be secured by an internal electronic system in high-security applications. We present an NFC device based on a chaotic communication between two circuits in this paper. By adopting this technology, there are three major advantages:

- Ability to develop chaotic behaviour.
- Avoid man-in-the-middle (MitM) attack.
- Provides less power consumption than transistors or switches.

In this way, the WPT device with Chua diode can create highly encrypted security without the use of external circuits to drive their synchronisation. It is not based on a tamper-proof algorithm. The developed waveform is chaotic and is based on the state variables' most recent state. Every time the device reads from the memristor, the internal state of the memristor changes to a new point of stability that is completely random and unrelated to the previous one.

There is no such method in the literature [28]. The cryptography suggested in the reference [29] is based on a shift in transmission frequency that knocks out other receivers. The frequency and correspondence with the receiver are generated by causal variation of the capacitor array according to the algorithm for maximum power output. The transmitted power can then be packed with various frequencies and delivered to the receiver in a predetermined time interval. Nonetheless, discrete algorithm adjustments, finite choices, and simple cloning affect these types of switched capacitor cryptography. In contrast, the memristor has been successfully used in imaging and communication encryption, achieving the highest degree of encryption. Circuit instability is crucial in deciding on chaotic encryption and decryption in a chaotic model of memristor-based cryptography. A user key, for example, has a chaotic generation of sequences because its initial values triggered the chaos of the memristor circuit. Encryption and decryption was built from this series. As a result, WPT technology and a chaotic memristor-based circuit can be used together.

A. Wireless Communication

Figure 4 depicts a WPT device made of memristors. Since the inductor is a reciprocal inductance the memristive Chua's

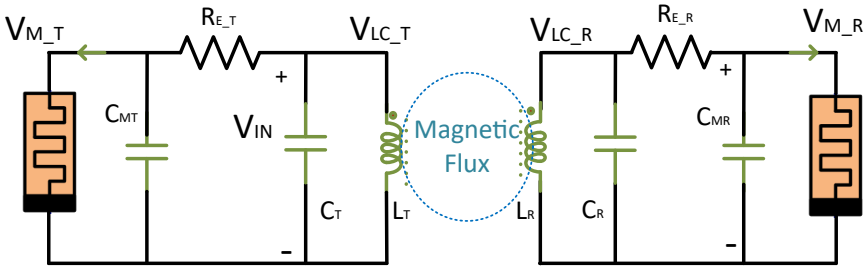

Figure 4. Symmetric Chua circuit proposed in the article.

TABLE I. PARAMETERS OF THE SYSTEM PROPOSED.

Parameter	Transmitter	Receiver	Value
C_1	C_{MT}	C_{MR}	6.8 nF
C_2	C_T	C_R	68 nF
R_E	R_T	R_R	2.18 kΩ
L	L_T	L_R	8 mH
M			4 mH

circuit introduced has been strengthened. The system is totally symmetric with two copies of the Chua circuit, as shown in Fig. 4. The above circuit produces an oscillation that may result in equilibrium, disorder, or instability. The parameter values shown in Table I have been considered in reference to a memristive Chua's circuit. As can be shown, the inductors have a value of 8 mH, which is lower than the typical value of 12 mH in Chua memristive circuits due to the use of the mutual inductance of the coupled circuits. The current flowing through L_T, the transmitter coil, generates a magnetic field around it, with some of these magnetic field lines going through the receiver coil, resulting in reciprocal inductance. Since the square root of two equal values is the same as one single value, when the inductances of the two coils are the same and equal, L_T and L_R are equal to L, the reciprocal inductance between the two coils would equal the value of one single coil, as shown:

$$M = k\sqrt{L_T L_R} = kL \tag{1}$$

where k denotes the coupling coefficient as a fractional number between 0 and 1, with 0 denoting no inductive coupling and 1 denoting complete or maximum inductive coupling. Since one coil induces a voltage in the next, the transmitter L induces a voltage V in the receiver, and vice versa. The oscillation of the circuit is not possible with more than one receiver at the same time because it will create an over mutual inductive M load as shown in the equation below.

$$\begin{cases} v_R^{in} = L_R \frac{dL_R}{dt} + M \frac{dL_T}{dt} \\ v_T^{in} = L_T \frac{dL_T}{dt} + M \frac{dL_R}{dt} \end{cases} \tag{2}$$

Using these relationships, lower inductances can be used than in Chua's circuit, and the circuitry's symmetry allows the chaotic behaviour to be transmitted. The transmitter and receiver would have the same resonant frequency:

$$f_0 = \frac{1}{2\pi\sqrt{LC_T}} = \frac{1}{2\pi\sqrt{LC_R}} \tag{3}$$

When the values in Table I are used, the result is 6.8 kHz. It is important to note that high efficiency is not needed for this application. The receiver only requires a small amount of power to begin its own oscillation and the chaotic actions needed for encryption.

B. Memristor state variables

Moreover, it is crucial to demonstrate that the device has no difference when compared to the typical Chua's diode circuit equations. When both sides of the system are in close proximity to each other, they must be capable of engaging in disorderly actions. The circuit's behaviour is derived from the classic third order Chua circuit by adopting the ideal voltage regulated active memristor shown in Fig. 5. Since the two circuits are symmetric, we will only look at the transmitter in this study. For the study, we call $C_{MT} = C_1$, $C_T = C_2$ and $L_T = L$ in series with a resistor (resistance of the coil) R_0. Let us consider that the state equations are obtained by computing the currents through the two voltage at the capacitors and the voltage across the inductor and remembering that $i_1 = C_1 \frac{dv_1}{dt}$, $i_2 = C_2 \frac{dv_2}{dt}$ and $V_3 = L \frac{di_3}{dt}$. We obtain:

$$\begin{cases} \frac{dv_1}{dt} = \frac{1}{C_1}[(v_2 - v_1)G - f(v_d)] \\ \frac{dv_2}{dt} = \frac{1}{C_2}[(v_2 - v_1)G - i_L] \\ \frac{di_3}{dt} = -\frac{1}{L_T}[v_2 - R_0 i_3] \end{cases} \tag{4}$$

where the $f(v_d)$ is the diode function:

$$f(v_d) = G_b v_1 + 0.5(G_a - G_b)[|v_1 + B_p| - |v_1 - B_p|] \tag{5}$$

To plot these equations,, usually we are sizing the time, voltages, and currents by RC_2, B_p, and B_pG, respectively. Assuming the variables $\tau = \frac{t}{RC_2}$, $x = \frac{v_1}{B_p}$, $y = \frac{v_2}{B_p}$ and $z = \frac{i_3}{GB_p}$, we obtain the following dimensionless state equations:

$$\begin{cases} \frac{dx}{d\tau} = \alpha(-x + y - f(x)) \\ \frac{dy}{dt} = x - y + z \\ \frac{dz}{dt} = -\beta y - \gamma z \end{cases} \tag{6}$$

where $\alpha = \frac{C_2}{C_1}$, $\beta = \frac{R^2 C_2}{L}$ and $\gamma = RR_0 \frac{C_2}{C_1}$. These are the typical equations for the Chua circuit computed in almost all computer simulators analysing the chaotic behaviours.

 ISBN: 978-1-61208-838-9

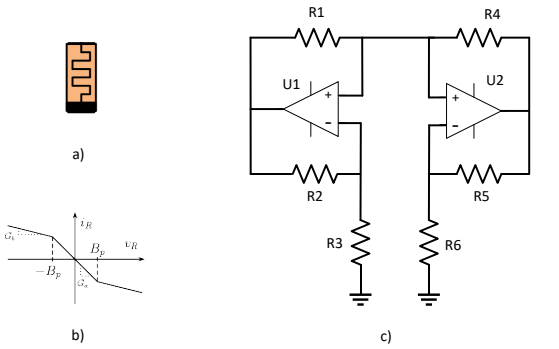

Figure 5. Chua‘s diode (**a**) typical I-V characteristic (**b**) and the equivalent circuit used in this article.

TABLE II. Circuit Parameters in reference to the Chua‘s diode equivalent circuit.

Circuit Parameters			
Resistor	Value	Resistor	Value
R_1	220 Ω	R_4	22 kΩ
R_1	220 Ω	R_4	22 kΩ
R_1	2.2 kΩ	R_4	3.3 kΩ

III. Communication Sequence

In this Section, we list all the steps and a flowchart of the new chaotic NFC procedure. The system is described as a door opening mechanism but can be adopted in all the IoT applications mentioned above such as payment.

A. NFC procedure proposed

Memristor-based chaotic cryptography system model consists of two parts shown in Fig. 4, which are two symmetrical Chua‘s circuits, Transmitter and Receiver respectively. In a typical Chua circuit, the initial condition is applied on the Capacitor C_T from external digital source. Therefore, in the L_TC_T and L_RC_R there is a connection to A/D or D/A converters. According to the cryptosystem model shown in Fig. 6, the process of chaotic encryption key data generation for opening an access door is described as follows:

1) The high security lock has a database of customers and each lock has in internal memory the ID of the customer.
2) The digital key or Access Card has an internal ID encrypted by the last Memristor chaotic status.
3) At the attempt to open the door, the lock and digital key (Receiver) are connected to each other. Both Memristors will develop a chaotic behaviour.
4) The chaotic behaviour generated in the transmitter circuit depends on the receiver status because it induces a voltage in the transmitter coil and consequently giving a new initial condition V_{IN}. In this way, the security lock’s digital logic can immediately recognise the authenticity of the user decrypting the data received.
5) If the Memristor status of the digital key is the same as the last status check, the digital logic can convert data. Otherwise, the receiver will bring the transmitter Memristor into a state with unknown variables, and hence the lock will be prevented from opening.

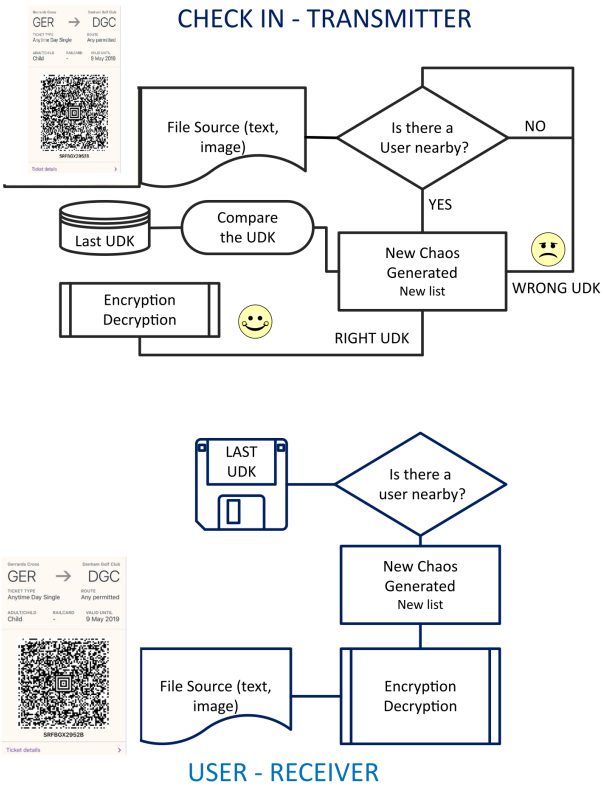

Figure 6. Flowchart of the entry system described in steps.

6) When the WPT system has reached an End Of File, both digital logic stages will disconnect the Memristor storing their last status.

Furthermore, any attempt to forge the digital key or smartphone would leave an indelible mark, as it will cause the memristor internal status for the authentication key to change irreversibly to an unexpected value from which their is no way to derive the previous value. True, the electronic system can be duplicated, but the internal value of the memristor can never be estimated, and there is no algorithm that can do so.

IV. System Performance Results

The system has been simulated with the advanced software NI multisim 14.2 with commercial devices and Labview functionality. The coils are designed as coupled inductors with a variable coupling factor. In order to start the chaotic behaviour memristors develop the chaotic waveform following the Chua’s memristive circuit. The key design specifications and parameters are listed in Tables I and II. The whole system has been verified showing a chaotic behaviour. The time plot can only partially give an understanding of the chaotic behaviour, therefore the system has been plotted with an oscilloscope in X-Y mode. We have shown the waveforms in the receiver as XY plot in 0.2 V/div and 1 V/div in Fig. 7 for V_{M_R} vs V_{LC_R} , respectively. In Fig. 8 is shown V_{M_R} vs i_{LC_R} in XY mode in 1 V/div and 1 V/div, respectively. In Fig. 9 is shown the v_{LC_R} vs i_{LC_R} in 0.2 V/div and 1 V/div, respectively.

The synchronisation of the phase portraits of the chaotic

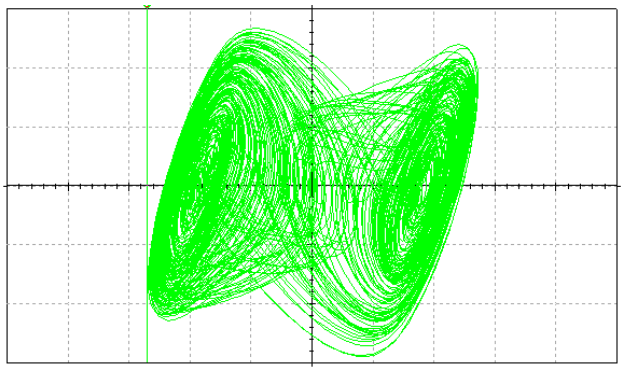

Figure 7. Receiver V_{M_R} vs V_{LC_R} shown in XY mode in 0.2 V/div and 1 V/div, respectively.

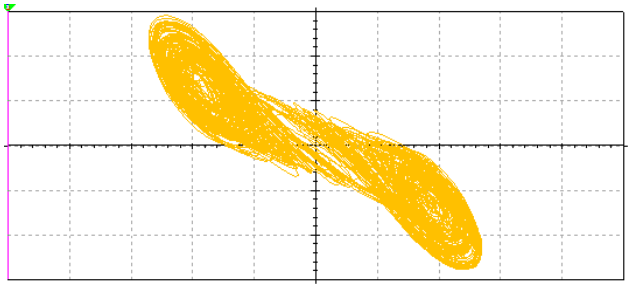

Figure 8. Receiver V_{M_R} vs i_{LC_R} shown in XY mode in 1 V/div and 1 V/div, respectively.

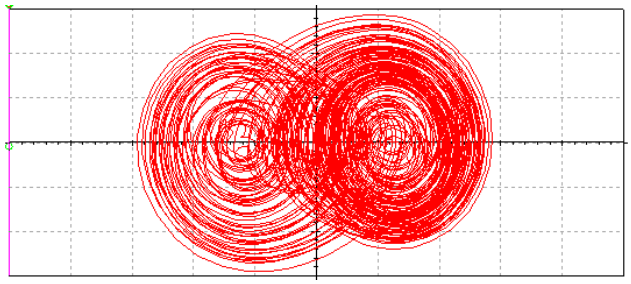

Figure 9. Receiver v_{LC_R} vs i_{LC_R} shown in XY mode in 0.2 V/div and 1 V/div, respectively.

attractors are fully synchronised as shown in all the plots of the transmitter (left) and the receiver (right) in Fig. 10.

A. *Experiment*

A prototype of the system has been built, as shown in Figure 11, on two different electronic breadboards which are jointed by a transformer representing the two coils. The memristor model has been built using the the ideal voltage regulated active Chua's diode introduced in Figure 5. The physical design of the memristors and the coils require advanced manufacturing technology which is outside of the scope of this article. In place of the coils a 6 mH 1:1 transformer has been used (resulting in a total inductance of 12 mH). The chaotic behaviour developed by the system is visualised on the transmitting side using a Tektronix 465 analogue oscilloscope and at the receiver with a Voltcraft digital storage oscilloscope and is in accordance with our simulations.

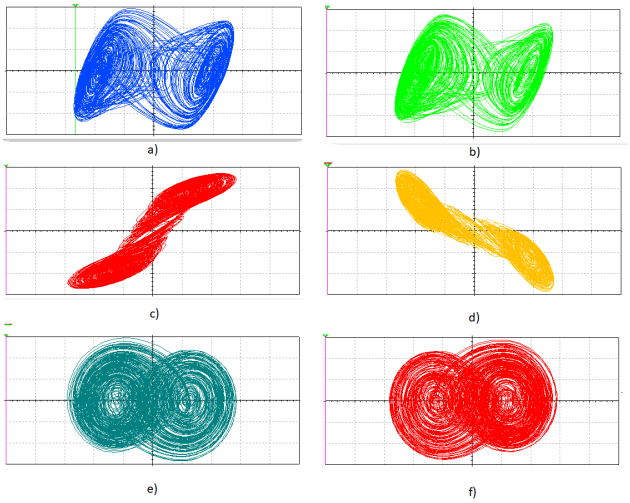

Figure 10. Synchronisation of the phase portraits of a chaotic attractor: voltage in the inductor V_{LC} referred to the memristor voltage V_M in the transmitter (a) and receiver(b) coil; current in the inductor i_L referred to the memristor voltage V_M in the transmitter (c) and receiver (d) coil; the memristor voltage V_M referred to its internal voltage status V_0 in the transmitter (e) and receiver (f).

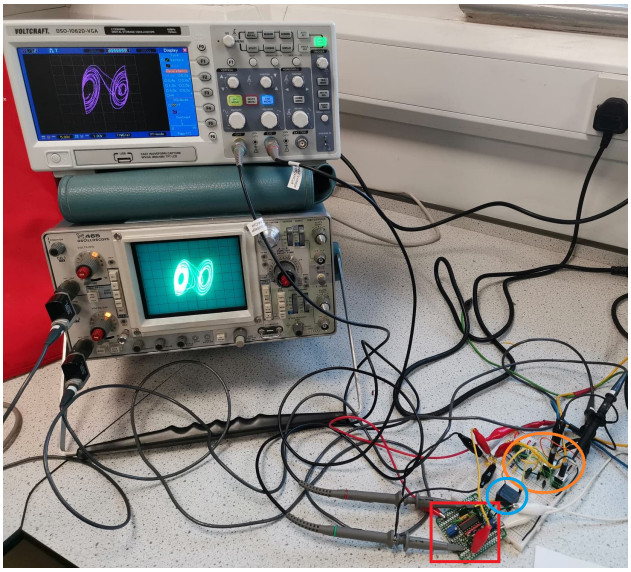

Figure 11. The prototype transmitter highlighted in orange, the receiver in red and the coupling transformer in blue.

For the IoT application, we have sampled the waveforms and used the Arduino Firmata library and Python to record the data on a host PC and an online service, as shown in Figure 12. In this way the chaotic behaviour is available online. The chaotic data is used in a Python code by using Flask libraries and HTML Python. We have created a database and webpage by using Python and sampling data by arduino.

V. Conclusions

The security of the new electronic and Internet of Things devices has become a great challenge. The data protection of these devices are only based on the web or on well-known algorithms and software. Therefore, the unique behaviour of the

 ISBN: 978-1-61208-838-9

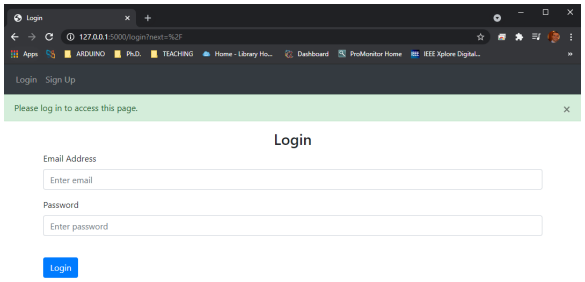

Figure 12. Use of Python and use chaotic encryption for web resources.

Chua's diode has attracted a lot of research studies and interest in developing new encryption characteristics. Furthermore, the memristor in a modified Chua's circuit is able to facilitate power and data transmission, provided that the inductors are mutually coupled. For this reason, we created two symmetrical Chua circuits able to transmit chaos. This new technique is an interesting solution, due to the fact it can be used to implement near-field wireless communication and encryption using a true random number generator. We are introducing an innovative implementation of the Chua circuit, which is applied in the NFC. In the article we have not mentioned the algorithm used in Python.

Future work will be focused on improving the data encryption and the realisation of multi-coil synchronisation, because they show a great and interesting advantage in comparison with the traditional Chua's circuit.

REFERENCES

[1] D. Minoli, K. Sohraby, and B. Occhiogrosso, "Iot considerations, requirements, and architectures for smart buildings—energy optimization and next-generation building management systems," IEEE Internet of Things Journal, vol. 4, no. 1, 2017, pp. 269–283.

[2] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, 2018, pp. 3453–3495.

[3] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," IEEE Internet of Things Journal, vol. 5, no. 6, 2018, pp. 4829–4842.

[4] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in 2010 seventh international conference on information technology: new generations. Ieee, 2010, pp. 804–809.

[5] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (nfc) technology," Wireless personal communications, vol. 71, no. 3, 2013, pp. 2259–2294.

[6] G. Jain and S. Dahiya, "Nfc?: Advantages, limits and future scope," vol, vol. 4, 2015, pp. 1–12.

[7] F. Di Rienzo, A. Virdis, C. Vallati, N. Carbonaro, and A. Tognetti, "Evaluation of nfc-enabled devices for heterogeneous wearable biomedical application," IEEE Journal of Radio Frequency Identification, vol. 4, no. 4, 2020, pp. 373–383.

[8] I. Yoon and H. Ling, "Investigation of near-field wireless power transfer under multiple transmitters," IEEE Antennas and Wireless Propagation Letters, vol. 10, 2011, pp. 662–665.

[9] Y. Sun, S. Kumar, S. He, J. Chen, and Z. Shi, "You foot the bill! attacking nfc with passive relays," IEEE Internet of Things Journal, 2020.

[10] J. I. Cairó, J. Bonache, F. Paredes, and F. Martín, "Reconfigurable system for wireless power transfer (wpt) and near field communications (nfc)," IEEE Journal of Radio Frequency Identification, vol. 1, no. 4, 2017, pp. 253–259.

[11] S. Kuka, K. Ni, and M. Alkahtani, "A review of methods and challenges for improvement in efficiency and distance for wireless power transfer applications," Power Electronics and Drives, 2019.

[12] R. Barboza and L. O. Chua, "The four-element chua's circuit," International Journal of Bifurcation and Chaos, vol. 18, no. 04, 2008, pp. 943–955.

[13] T. Matsumoto, "A chaotic attractor from chua's circuit," IEEE Transactions on Circuits and Systems, vol. 31, no. 12, 1984, pp. 1055–1058.

[14] Q. Xu, Q. Zhang, B. Bao, and Y. Hu, "Non-autonomous second-order memristive chaotic circuit," IEEE Access, vol. 5, 2017, pp. 21 039–21 045.

[15] B. Bao, T. Jiang, Q. Xu, M. Chen, H. Wu, and Y. Hu, "Coexisting infinitely many attractors in active band-pass filter-based memristive circuit," Nonlinear Dynamics, vol. 86, no. 3, 2016, pp. 1711–1723.

[16] A. L. Fitch, D. Yu, H. H. Iu, and V. Sreeram, "Hyperchaos in a memristor-based modified canonical chua's circuit," International Journal of Bifurcation and Chaos, vol. 22, no. 06, 2012, p. 1250133.

[17] Q. Xu, Y. Lin, B. Bao, and M. Chen, "Multiple attractors in a non-ideal active voltage-controlled memristor based chua's circuit," Chaos, Solitons & Fractals, vol. 83, 2016, pp. 186–200.

[18] J. Kengne, Z. Njitacke Tabekoueng, V. Kamdoum Tamba, and A. Nguomkam Negou, "Periodicity, chaos, and multiple attractors in a memristor-based shinriki's circuit," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 25, no. 10, 2015, p. 103126.

[19] P. Zaiping, W. Chunhua, L. Yuan, and L. Xiaowen, "A novel four-dimensional multi-wing hyper-chaotic attractor and its application in image encryption," Acta Physica Sinica, vol. 63, no. 24, 2014, p. 240506.

[20] H. Wu, Y. Ye, B. Bao, M. Chen, and Q. Xu, "Memristor initial boosting behaviors in a two-memristor-based hyperchaotic system," Chaos, Solitons & Fractals, vol. 121, 2019, pp. 178–185.

[21] B. Bao, H. Bao, N. Wang, M. Chen, and Q. Xu, "Hidden extreme multistability in memristive hyperchaotic system," Chaos, Solitons & Fractals, vol. 94, 2017, pp. 102–111.

[22] M. Chen, M. Li, Q. Yu, B. Bao, Q. Xu, and J. Wang, "Dynamics of self-excited attractors and hidden attractors in generalized memristor-based chua's circuit," Nonlinear Dynamics, vol. 81, no. 1, 2015, pp. 215–226.

[23] P. Pourghomi and G. Ghinea, "A proposed nfc payment application," arXiv preprint arXiv:1312.2828, 2013.

[24] M. Q. Saeed and C. D. Walter, "Off-line nfc tag authentication," in 2012 International Conference for Internet Technology and Secured Transactions. IEEE, 2012, pp. 730–735.

[25] D. Schürmann, S. Dechand, and L. Wolf, "Openkeychain: an architecture for cryptography with smart cards and nfc rings on android," Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 1, no. 3, 2017, pp. 1–24.

[26] V. Coskun, K. Ok, and B. Ozdenizci, Near field communication (NFC): From theory to practice. John Wiley & Sons, 2011.

[27] N. Ramya, U. Sandhya, and L. Gayathri, "Biometric authentication to ensure security in epassports," in 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), Feb 2018, pp. 342–346.

[28] C. S. Kuka, Y. Hu, Q. Xu, and M. Alkahtani, "An innovative near-field communication security based on the chaos generated by memristive circuits adopted as symmetrical key," IEEE Access, vol. 8, 2020, pp. 167 975–167 984.

[29] Z. Zhang, K. T. Chau, C. Qiu, and C. Liu, "Energy encryption for wireless power transfer," IEEE Transactions on Power Electronics, vol. 30, no. 9, Sep. 2015, pp. 5237–5246.

 ISBN: 978-1-61208-838-9