# An Innovative Memristor-Based Near Field Communication Topology Adopted as Security Key

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

Mohammed Alkahtani and Gor Poliposyan
University of Liverpool
Liverpool L69 3BX
m.alkahtani@liverpool.ac.uk
Gor.Poliposyan@liverpool.ac.uk

Muflah Alahammad
University of Cranfield
Bedford MK43 0AL
m.s.alhammad@cranfield.ac.uk

***Abstract*—In recent years, the security of power systems has become a growing challenge resulting from the expansion of the use of wireless power and data transmission. This paper introduces a new circuit topology for Near Field Communication (NFC) Topology which are based on the Wireless Power and Data Transfer (WPDT) systems. Traditional WPDT circuits are based on inverters to create an oscillation for the transmitter coil. By adopting switches, the traditional WPDT circuitry has intrinsic sources of power loss and requires an extra switching time control circuit for the correct commutation. In addition, these systems have low data cryptography capabilities. Therefore, a new WPDT system has been developed which utilises memristors without adopting switches. In addition, this topology is as advantageous it is possible to adopt chaotic encryption for NFC security. The simulation results and tests prove the functionality of the WPDT based on Memristor and their quality of data generation and storage. The major application for this type of circuitry is the NFC digital code for the opening of the high security block.**

***Keywords–Decryption, Digital key, Encryption, High Security, Memristor, Near Field Communication (NFC), Wireless Power and Data Transfer, Security Lock;***

## I. INTRODUCTION

The growing request for wireless technology has quickly attracted a lot of attention in the investigation of Wireless Power and Data Transfer (WPDT) systems for different uses. Unlike RF transmission, the operating principle of WPDT is based on the resonance of magnetic and electric fields by means of an alternating current in the LC circuit. This AC power is created by switches activated in external control system. 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 [1]. Typically, the power dissipation in the inverter grows with the operating frequency. As the air gap increases, less connection of the magnetic flux is caught by the receiver winding [2], [3]. Most of the research results in WPT systems focus on effective transfer mode, operating principles and circuit topology [4], [5], [6].

In the near future, the inductive WPDT connection will gradually eliminate charging and communication cables as power and data can be integrated simultaneously [7]. On the other hand, it inevitably entails the hazards of theft or loss of power and data. While a selective WPDT technology can achieve a power transmission oriented to specific receivers through multiple receivers [8], [9], illegal receivers can track and block the operating frequency to steal power and data.

In this work, we present a new WPDT topology with advanced security capabilities. We use the memristor to create LC resonance oscillation instead of traditional switches and therefore less power dissipation. Also, there is no need to add an external circuit to operate the switches, and there will be no timing problems. In addition, thanks to the unique non-linearity and memory characteristics of the memristor, it is possible to adopt a mutual authentication key based on the last state and its subsequent encryption and decryption.

### A. Memristor

The memristor is a circuit element based on the electrical charge q and the magnetic flux $\varphi$ constitutive relationship theorized by Prof. Leon Chua [10]. This component (short for memory resistor) was manufactured for the first time by Hewlett Packard laboratories [11]. This device has a pinched $I - V$ hysteresis cycle with switching mechanism and has the ability to remember its last state [12], [13]. Details on the history, device, manufacturing and characterization of the memristor are available in the following references [14], [15], [16]. Memristors with their non-linearities are properly integrated into existing linear or non-linear electronic circuits to create several new chaotic circuits [17]. Dynamic behaviors, such as chaos and hyper-chaos [18], [19], coexisting multiple attractors [20], [21], hyper-chaotic multi-wing [22], [23] and hidden attractors [24], [25], [26] have been studied and analyzed by numerical simulations and hardware experiments.

In this work, we therefore propose a memoristor-based architecture for WPT systems. The system has the quality of transmitting power and data wirelessly without using any switch and driver circuitry. In addition, the system is not predictable by the algorithm and therefore has the ability to achieve the highest level of encryption due to the last state of the memristor that cannot be predicted and measured. The rest of the document is organized as follows. The main functionality and encryption and decryption capabilities are shown in the next paragraph. In the section III, there is an analysis of the WPT based on memristor and its stability. System functionality and simulation results are presented in the section IV. Finally, the section V concludes the document.

 ISBN: 978-1-61208-771-9

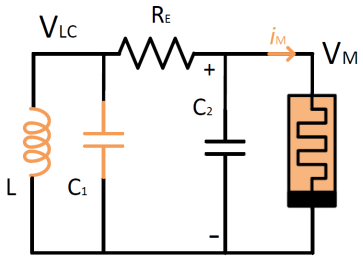


Figure 1. Memsistive circuit developed by L. Chua[10].

## II. Wireless Power Transfer and Memristor

A special type of WPT system very sensitive to the problem of cryptography is the Near Field Communication (NFC) which is widely used in contactless credit cards, smartphones and digital keys. NFC is a low-bandwidth, two-way wireless communication technology that utilises electromagnetic induction to transmit information and allows data to be exchanged between devices separated by up to 4 inches [27]. Access cards and digital keys have internal user data encrypted by software and stored in the device. This encryption is traditionally based on the Hash function [28], [29]. This type of algorithm is well known and is widely available on the Internet. For high security applications, this important data must be protected by an internal electronic device. In this work, we introduce an NFC system based on a memory circuit capable of producing chaotic waveforms. There are three great benefits of memristors, which are used in this WPT application:

- Provides less heat than transistors or switches.
- Able to store charge and remember its last state.
- Ability to develop chaotic behaviour.

In this way, the WPT system with memristor does not require external circuits to drive the times and is able to create highly encrypted protection. It is not based on an algorithm that can be hacked. The generated waveform is chaotic and is based on the last state of the state variables. Each time the system reads from the memristor, it will take the internal state of the memristor to a different point of stability, which is completely chaotic and unrelated to the previous one.

In literature, there is no such system. The cryptography proposed in the references [30], [31] is built on the change in transmission frequency that makes other receivers out of resonance. Causal variation of the capacitor array according to the algorithm creates the frequency and correspondence with the receiver for maximum power output. Then, the transmitted power can be packed with different frequencies and delivered to the receiver in a specific time interval [32], [33], [34]. Nevertheless, these types of switched capacitor cryptography are affected by discrete algorithm adjustment, finite selections and are easy to clone. In comparison, the memristor has been used efficiently in imaging and communication encryption [35], [36] providing the highest level of encryption achieved. In a chaotic model of memristor-based cryptography, circuit chaos is critical to deciding on chaotic encryption and decryption. For example, a user key, which is defined as the initial values caused the chaos of the memristor circuit, has a chaotic generation of sequences. From this sequence, encryption and decryption is developed. Therefore, it is possible to combine WTP technology and the chaotic memristor-based circuit together.

Figure 2. Commercial product of a security safe lock with a NFC system opening key. Image collected from source [37].

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 |

### A. Typical Functionality

Memristor-based chaotic cryptography system model consists of two parts shown in Fig. 3 and 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. 3, the process of chaotic encryption key for opening safety data is described as follows:

1) The high security lock has a database of customers and each lock has in the internal memory the ID of the customer.
2) The digital key or Access Card has internal ID encrypted by the last Memristor chaotic status.
3) At the attempt to open the safe, 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 from 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 safe security lock digital part can immediately recognise the authenticity of the user decrypting the data received.
5) If the Memristor status of the digital key is the same of the last status check, the digital part can convert data. Otherwise, the receiver will bring the transmitter Memristor in an unknown variables status, hence not allowing to open the lock.

 ISBN: 978-1-61208-771-9

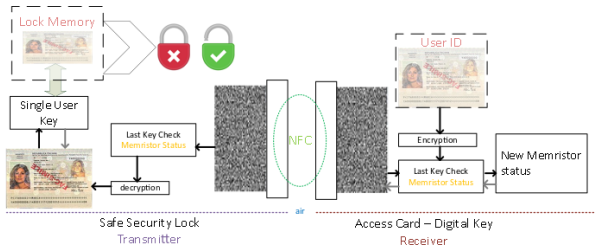


Figure 3. The crypto-system model: on the left the transmitter lock and the receiver in the Access Card Key.

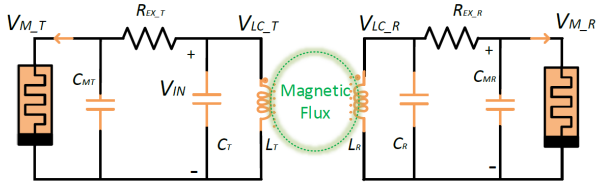


Figure 4. The wireless power and data transfer system built with Memristors.

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

Moreover, any forgery attempt to the digital key or smartphone will leave an indelible mark as it will bring the memristor internal status in unexpected value for the authentication key in safe security lock. There is no possibility to come back. It is true that the electronic system can be cloned but the internal value of the memristor can never be predicted and there is not an algorithm that could predict this value.

## III. Stability and Chaotic Behaviour

In this Section, we analyse the principles of inductive coupling and Memristor state valiable in order to integrate them for the developed Memristor-based Wireless Power and Data Transfer system.

### A. Wireless Power Transmission

The WPT system built with memristors is shown in Fig. 4. The memristive Chua's circuit introduced in 1 has been improved as the inductor is a mutual inductance and $C_R$ is the compensation capacitor. As depicted in Fig. 4, the system is completely symmetric as two copies of the Chua circuit. The latter circuit creates an oscillation which can bring to equilibrium, chaos or unstability. In reference of memristive Chua's circuit, it has been considered the parameters' values shown in Table I. As notices, the inductors values $L_T$ and $L_R$ are 8 mH which is lower of the usual values in Chua memristive circuits around 12 mH. It is possible to use a lower value because of mutual induction. The current flowing in $L_T$ or the transmitter coil sets up a magnetic field around itself with some of these magnetic field lines passing through the receiver coil $L_R$ giving us mutual inductance. When the inductances of the two coils are the same and equal, $L_T$ is equal to $L_R$, the mutual inductance that exists between the two coils will equal the value of one single coil as the square root of two equal values is the same as one single value as shown:

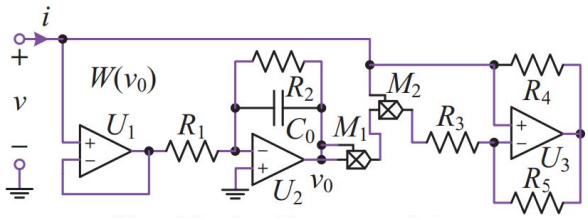


Figure 5. Non-ideal active voltage-controlled memristor equivalent realisation. This circuit is active and only $C_0$ has charge storing qualities. The real memristor has similar behaviour and possesses all the qualities mentioned in the paper but it not available in any simulation library.

TABLE II. Memristor model internal values.

| Memristor equivalent | | | |
|---|---|---|---|
| Parameter | Value | Parameter | Value |
| $R_1$ | 4 kΩ | $R_5$ | 2 kΩ |
| $R_2$ | 10 kΩ | $C_0$ | 1 nF |
| $R_3$ | 1.4 kΩ | $g_1$ | 1 |
| $R_4$ | 2 kΩ | $g_2$ | 0.1 |

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

where $k$ is the coupling coefficient expressed as a fractional number between 0 and 1, where 0 indicates zero or no inductive coupling, and 1 indicating full or maximum inductive coupling. In our application, the coupling coefficient is an range between 0.4 to 0.6. A lower value of coupling is not enough to start chaotic behaviour and to change the status of the memristor. One coil induces a voltage in an adjacent coil, therefore the transmitter $L_T$ induces a voltage $v_R^{in}$ in the receiver, and viceversa.

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

Using this relationships, it is possible to adopt lower inductances than the Chua's circuit and the symmetry of the circuitry allows to transmit the chaotic behaviour. This chaotic behaviour is necessary for the encryption. The transmitter and receiver will resonate at the same frequency :

$$f_0 = \frac{1}{2\pi\sqrt{LC_2}} \tag{3}$$

which adopting the values reported in II gives 6.8 kHz. It is important to notice that this application it is not necessary to achieve high efficiency. The receiver needs just enough power to start its own oscillation and the chaotic behaviour necessary for the encryption.

### B. Memristor state variables

Therefore, it is important to show that the system has no variation compared to the Chua memristive circuit and is therefore stable. Either side of the system must be capable of engaging in chaotic behaviour whenever they are in close proximity to each other. The behaviour of the circuit derives from the classic third order Chua circuit replacing it with the non-ideal voltage controlled active memristor shown in Fig. 5. The latter is composed by a buffer $U_1$, an integrator

 ISBN: 978-1-61208-771-9 

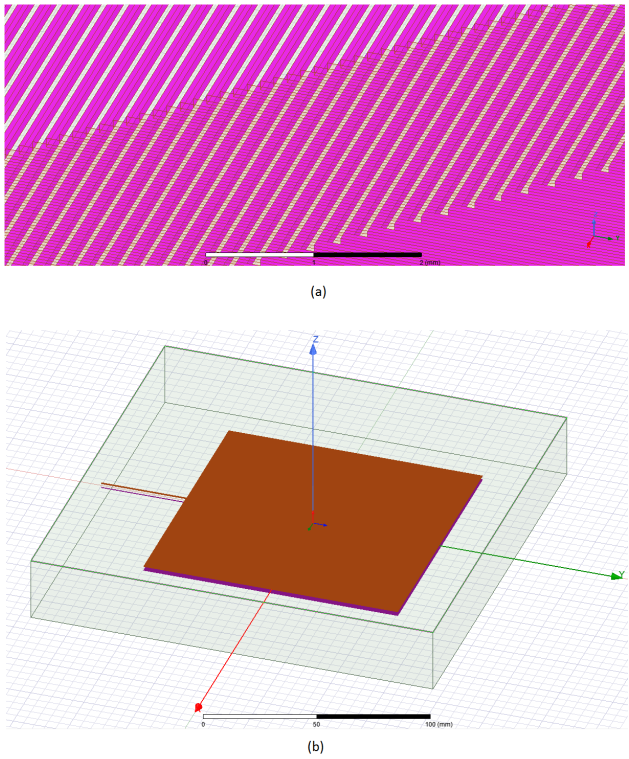


Figure 6. (a) Magnification of the 8 mH coils. Structure of the receiver (brown) and transmitter (purple) in the ANSYS analysis.

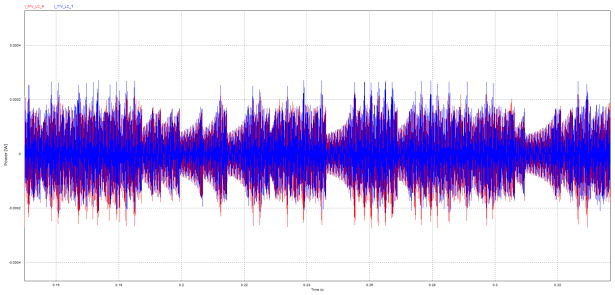

Figure 7. The power transmitted (blue) and received (red) are around 2 mW and they have also a chaotic behaviour.

$U_2$ connected two resistors $R_1$, $R_2$, the capacitor $C_0$, the multipliers $M_1$ and $M_2$ and a current inverter $U_3$ connected to the resistors $R_3$, $R_4$ and $R_5$. This model is characterised by two equations:

$$i_M = (-G_a + G_b \cdot v_0^2) v_M \tag{4}$$

$$\frac{dv_0}{dt} = -\frac{v_M}{R_1 C_0} - \frac{v_0}{R_2 C_0} \tag{5}$$

where $i_M$ is the current flowing in the memristor, $v_M$ is the voltage on the memristor and $v_0$ the voltage on its internal capacitor $C_0$. In addition, the scale factors of the multipliers $M_1$ and $M_2$ are indicated as $g_1$ and $g_2$ in order to have $G_a = \frac{1}{R_3}$ and $G_b = \frac{g_1 g_2}{R_3}$. These relationships give the memristor input-output characteristic and the pinched $I - V$ relationship [21].

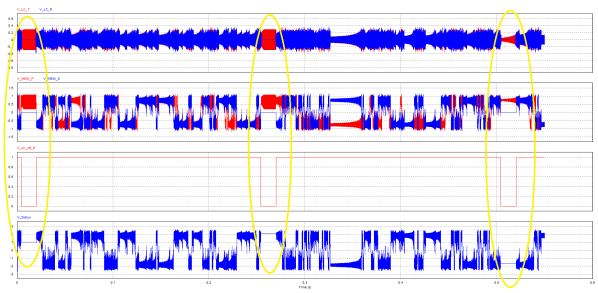

Figure 8. Time step of the chaotic behaviour when the receiver is disconnected (highlighted in yellow): the LC and memristor voltage $V_{LC}$ and $V_M$ in receiver and transmitter, respectively in blue and red. At the disconnection (in the $3^{rd}$ graph), the receiver memristor holds its last status shown in the $4^{rd}$ graph.

## IV. System Performance Results

To assess the design, stability and performance of the proposed memristor based WPT system, finite element analysis (FEA) and system simulation are performed. Initially, it has been designed the coils using ANSYS Maxwell v19 as it is is one of the challenging part of this design. It is possible design the size of the coil in the actual size of a passport 88 x 125 mm. In order to achieve the mutual inductance of 6.4 mH, simulation results has shown that is necessary a gap of 2 mm (air, plastic or any material with relative permeability $\mu_R = 1$) between coils. As shown in the simulation design in Fig. 6a the spiral of the inductors has a thickness of 0.1 mm merely visible in a larger scale as Fig. 6b. In purple is the transmitter coil and the brown is the receiver one. By using PSIM simulations, it is possible to plot the power transferred and the system to working power as shown in Fig. 7. When the receiver has finished the communication, it will stop the oscillation in blu in the first two graphs of Fig. 8, and it will keep it last status in the $4^{th}$ graph for a certain period of disconnection circled in yellow in Fig. 8. Just for illustration, the disconnection is periodic and we have shown only three times.

### A. Experiment

The system has been build with the advanced software NI multisim 14.2 with commercial devices and Labview functionality. The coils are designed as coupled inductors with the 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 Table I and II. The whole system has been verified showing a chaotic temporal behaviour as plot in Fig. 9. The time plot can only partially give an understanding of the chaotic behaviour, therefore the system has been plot with an oscilloscope in X-Y mode. The results are the phase portraits of the chaotic attractors fully synchronised between the transmitter (left) and the receiver (right) in a time representation in milliseconds (10 ms/div). as shown in Fig. 10. The two circuits can generate multistability and have the same behaviours because they have the same circuit parameters. Thus, the initial conditions can be used as a chaotic key sequence in encryption and decryption which is transmitted in a synchronisation process.

 ISBN: 978-1-61208-771-9 

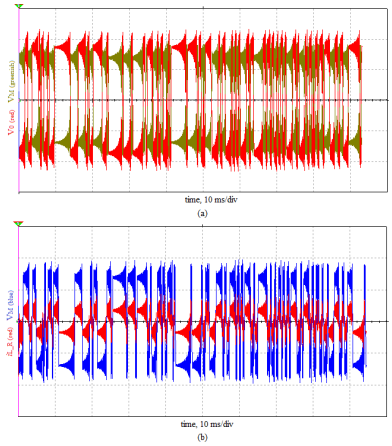

Figure 9. Time step of the chaotic behaviour in the receiver: the memristor voltage $V_M$ in greenish and internal status $V_0$ in red(a) and coil current $i_L$ in red and memristor voltage $V_M$ in blue (b).

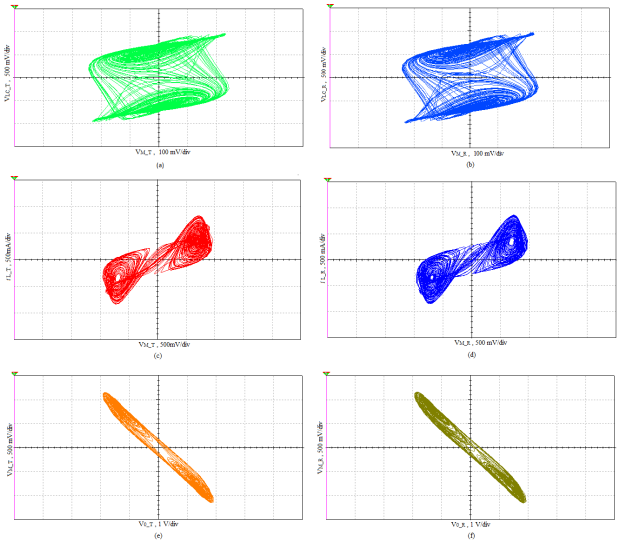

Figure 10. Synchronisation of the phase portraits of a chaotic attractor: voltage in the inductor $V_{LC}$ referred to the memristor voltage $V_M$ in the receiver (a) and transmitter (b) coil; current in the inductor $i_L$ referred to the memristor voltage $V_M$ in the receiver (c) and transmitter (d)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

## V. Conclusions

In the future, security on power systems will play a critical role in all electronic devices. This is the main consequence of the elimination of wires and the deployment of wireless power and data transmission. This growing challenge is met with the extreme use of software and algorithms leading to data encryption and decryption. Unfortunately, once the type of algorithm is known, it is often violated because it is based in the programming code. An advanced circuit topology for wireless power and data transmission using the memory circuit has been introduced in this article. Traditional WPT circuits are based on inverters in order to generate an oscillation for the transmitter coils. By adopting switches, the system has intrinsic energy dissipation sources and requires an additional control circuit for the correct switching time. The memristor is able to create a chaotic oscillation without adopting switches. The oscillation makes the system transmit power and chaotic behaviour is very advantageous for high security encryption. The functionality of the system has been experimented and verified. In future works, the system will be experimented with data transmission performance and improved cryptography capabilities.

## References


[1] 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.

[2] V. Vijayakumaran Nair and J. R. Choi, "An efficiency enhancement technique for a wireless power transmission system based on a multiple coil switching technique," Energies, vol. 9, no. 3, 2016. [Online]. Available: https://www.mdpi.com/1996-1073/9/3/156

[3] 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.

[4] Z. Wang, X. Wei, and H. Dai, "Principle elaboration and system structure validation of wireless power transfer via strongly coupled magnetic resonances," in 2013 IEEE Vehicle Power and Propulsion Conference (VPPC). IEEE, 2013, pp. 1–6.

[5] R. Jay and S. Palermo, "Resonant coupling analysis for a two-coil wireless power transfer system," in 2014 IEEE Dallas Circuits and Systems Conference (DCAS). IEEE, 2014, pp. 1–4.

[6] T. C. Beh, T. Imura, M. Kato, and Y. Hori, "Basic study of improving efficiency of wireless power transfer via magnetic resonance coupling based on impedance matching," in 2010 IEEE International Symposium on Industrial Electronics. IEEE, 2010, pp. 2011–2016.

[7] J. Wu, C. Zhao, Z. Lin, J. Du, Y. Hu, and X. He, "Wireless power and data transfer via a common inductive link using frequency division multiplexing," IEEE Transactions on Industrial Electronics, vol. 62, no. 12, Dec 2015, pp. 7810–7820.

[8] C. Jiang, K. Chau, C. Liu, and W. Han, "Wireless dc motor drives with selectability and controllability," Energies, vol. 10, no. 1, 2017. [Online]. Available: https://www.mdpi.com/1996-1073/10/1/49

[9] Y. Zhang, T. Lu, Z. Zhao, F. He, K. Chen, and L. Yuan, "Selective wireless power transfer to multiple loads using receivers of different resonant frequencies," IEEE Transactions on Power Electronics, vol. 30, no. 11, Nov 2015, pp. 6001–6005.

[10] L. Chua, "Memristor-the missing circuit element," IEEE Transactions on circuit theory, vol. 18, no. 5, 1971, pp. 507–519.

[11] R. Stanley Williams, "How we found the missing memristor," in Chaos, CNN, Memristors and Beyond: A Festschrift for Leon Chua With DVD-ROM, composed by Eleonora Bilotta. World Scientific, 2013, pp. 483–489.

[12] O. A. Olumodeji, A. P. Bramanti, M. Gottardi, and S. Iannotta, "A memristor-based pixel implementing light-to-resistance conversion," Optical Engineering, vol. 55, no. 2, 2016, p. 020501.

[13] O. A. Olumodeji, A. P. Bramanti, and M. Gottardi, "A memristive pixel architecture for real-time tracking," IEEE Sensors Journal, vol. 16, no. 22, 2016, pp. 7911–7918.

[14] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," nature, vol. 453, no. 7191, 2008, p. 80.

[15] D. Lin, L. Chua, and S.-Y. Hui, "The first man-made memristor: Circa 1801 [scanning our past]," Proceedings of the IEEE, vol. 103, no. 1, 2014, pp. 131–136.

[16] L. O. Chua and S. M. Kang, "Memristive devices and systems," Proceedings of the IEEE, vol. 64, no. 2, 1976, pp. 209–223.

[17] 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.

[18] I. Petras, "Fractional-order memristor-based chua's circuit," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 57, no. 12, 2010, pp. 975–979.

[19] 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.


 ISBN: 978-1-61208-771-9 

[20] 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.

[21] 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.

[22] J. Ma, Z. Chen, Z. Wang, and Q. Zhang, "A four-wing hyper-chaotic attractor generated from a 4-d memristive system with a line equilibrium," Nonlinear Dynamics, vol. 81, no. 3, Aug 2015, pp. 1275–1288. [Online]. Available: https://doi.org/10.1007/s11071-015-2067-4

[23] L. Zhou, C. Wang, and L. Zhou, "Generating hyperchaotic multi-wing attractor in a 4d memristive circuit," Nonlinear Dynamics, vol. 85, no. 4, 2016, pp. 2653–2663.

[24] 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.

[25] H. Bao, N. Wang, H. Wu, Z. Song, and B. Bao, "Bi-stability in an improved memristor-based third-order wien-bridge oscillator," IETE Technical Review, vol. 36, no. 2, 2019, pp. 109–116.

[26] H. Bao, N. Wang, B. Bao, M. Chen, P. Jin, and G. Wang, "Initial condition-dependent dynamics and transient period in memristor-based hypogenetic jerk system with four line equilibria," Communications in Nonlinear Science and Numerical Simulation, vol. 57, 2018, pp. 264–275.

[27] A. Alzahrani, A. Alqhtani, H. Elmiligi, F. Gebali, and M. S. Yasein, "Nfc security analysis and vulnerabilities in healthcare applications," in 2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Aug 2013, pp. 302–305.

[28] 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.

[29] F. Hamad, J. Zraqou, A. Maaita, and A. A. Taleb, "A secure authentication system for epassport detection and verification," in 2015 European Intelligence and Security Informatics Conference, Sep. 2015, pp. 173–176.

[30] W. Liu, K. T. Chau, C. H. T. Lee, C. Jiang, and W. Han, "A switched-capacitorless energy-encrypted transmitter for roadway-charging electric vehicles," IEEE Transactions on Magnetics, vol. 54, no. 11, Nov 2018, pp. 1–6.

[31] 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.

[32] Z. Zhang, K. Chau, C. Liu, C. Qiu, and F. Lin, "An efficient wireless power transfer system with security considerations for electric vehicle applications," Journal of Applied Physics, vol. 115, no. 17, 2014, p. 17A328.

[33] M. Sadzali, A. Ali, M. Azizan, and M. Albreem, "The security energy encryption in wireless power transfer," in AIP Conference Proceedings, vol. 1885, no. 1. AIP Publishing, 2017, p. 020242.

[34] E. Ahene, M. Ofori-Oduro, and B. Agyemang, "Secure energy encryption for wireless power transfer," in 2017 IEEE 7th International Advance Computing Conference (IACC), Jan 2017, pp. 199–204.

[35] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, "Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit," IEEE Access, vol. 7, 2019, pp. 58 751–58 763.

[36] H. Abunahla, D. Shehada, C. Y. Yeun, C. J. OKelly, M. A. Jaoude, and B. Mohammad, "Novel microscale memristor with uniqueness property for securing communications," in 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), Oct 2016, pp. 1–4.

[37] Aliexpress. Nfc door lock. [Online]. Available: http://aliexpress.com

 ISBN: 978-1-61208-771-9 