An Innovative Near-Field Communication Security Based on the Chaos Generated by Memristive Circuits Adopted as Symmetrical Key

COLIN SOKOL KUKA1, YIHUA HU1, (Senior Member, IEEE), QUAN XU2, (Member, IEEE), AND MOHAMMED ALKAHTANI3, (Graduate Student Member, IEEE)

1Department of Electronic Engineering, University of York, York YO10 5DD, U.K.
2School of Information Science and Engineering, Changzhou University, Changzhou 213164, China
3Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, U.K.

Corresponding author: Quan Xu (xuquan@cczu.edu.cn)

ABSTRACT The new technology solutions are playing an important role in the hardware security. One of the latest techniques is the use of the Memristor as an encryption element. In this paper, it has been introduced a two-column array inductor for Memristor-Based Wireless Power Transfer (M-WPT) systems. The traditional WPT circuits are based on switches, which do require a control circuit for timing and have low data encryption factor. By adopting the memristive Chua’s circuit with the chaotic behaviour characteristic, it is possible to create a symmetrical dual-key cryptography. Furthermore, in this innovative solution, the high inductance value of the traditional Chua circuit can be further reduced by using the dynamic effects of the coils flux linkage. The simulation results exhibit the dual-scroll attractors phase portrait, which is available for encryption features. Therefore, the data collected from the phase portrait are used as true random number generator in Python code. Instead of using algorithms, the code can create a symmetrical key for an unique chaotic cryptography. In order to build a prototype, it has been created a PCB design for the whole system. The experiment highlights the unpredictable voltage and current and validates the chaotic behaviour of the transmitter and receiver.

INDEX TERMS Decryption, data transmission, encryption, security, memristor, near field communication (NFC), true random number generator, symmetrical encryption, wireless power transfer.

I. INTRODUCTION

The concept of the Internet of Things is based on the ability of physical objects with embedded technology to communicate with each other or with other systems, transmit data and work in a synchronised way. Due to its disruptive potential in several segments, such as agriculture, industry and payment methods, the topic has received a lot of attention. The IoT security survey by Granjal et al. [2] further suggests the importance of security, privacy and trust. Near Field Communication (NFC) [3] is a low energy wireless transfer technology operating at 13.56 MHz frequency, with few centimetres of access distance particularly used in IoT devices. It can assist for a secure on-demand connecting, as well as controlling and commissioning of IoT devices through proximity, in order to assure that only the two devices are communicating as shown in Fig. 1. It can also help for a secure device configuration, firmware update, cryptographic keys setup and access to logs. NFC has the advantage that due to proximity, it is hard to perform eavesdropping and man in the middle (MITM) attack. However, it uses an untrusted communication channel and does not ensure the authenticity, authorisation and trustful state of the devices [4].

The standard NFC access to the IoT unit comprises of a user’s device (typically a mobile device, unique cards or maybe Key fob) to get into the IoT unit via NFC tags. These devices utilise the unreliable FC Data Exchange Format (NDEF) communications [5] or maybe Peer-to-Peer mode [6], which is not ready to accept designers for a two way communication. Hence, it is important to develop new NFC modes that can overcome these security issues. On user devices, such as certain commercially available mobile devices, the NFC uses a component Secure Element (SE) [7]. The SE is a tamper-resistant platform (typically a one chip secure
microcontroller) capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities. It can also be used for hardware card emulation of a small-sized contact-less smart card on a mobile device [3], as well as to store credentials and identities. In order to increase this security, the Host Card Emulation (HCE) provides the emulation of a smart card using the ISO 7816 standard [6] at a software level. The HCE [7], [8] is the software architecture that provides accurate virtual representation of different electronic identification cards (access, transit and banking). This technology makes it easier for retailers to deliver payment card through mobile closed-loop contact-less payment solutions, as well as provides real-time payment card delivery, and enables a simple implementation scenario that does not require changes to the software within payment terminals. This can be accessed by a traditional card reader or a HCE reader application on another user device using the Application Protocol Data Unit (APDU) packets [9]. However, since the HCE is totally software-based, it is vulnerable to threats and requires additional mechanisms to secure the interaction [10], [11].

Therefore, it is necessary to increase the level of security in smart cards and to reduce the HCE vulnerability in the user device. In this article, in order to improve the security in IoT devices, we introduce the memristor. The memristor is a circuit element based on the electrical charge \( q \) and the magnetic flux \( \phi \). 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 a. Memristors with their non-linearities are properly integrated into existing electronic circuits to create several new chaotic circuits [12] as depicted in Fig. 3. Dynamic behaviours, such as chaos and hyper-chaos [13], [14], coexisting multiple attractors [15], [16], hyper-chaotic multi-wing [13], [17] and hidden attractors [18]–[20] have been studied and analysed by numerical simulations and hardware experiments.

The cryptography proposed for WPT systems in the references [21], [22]. is built upon 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 [23]–[25]. Nevertheless, these types of switched capacitor cryptography are affected by a discrete algorithm adjustment, finite selections and are easy to clone [26]. In comparison, the memristor has been used efficiently in imaging and communication encryption [27]–[29] providing the highest level of encryption achieved.

In this work, we therefore propose an array memristor-based architecture for WPT systems. This is a new research study adopting the memristor in wireless power transfer, therefore there are no other references for this system. The system is a Near Field Communication (NFC), a particular form of WPT which harvests energy to transfer data. In the chaotic model of memristor-based cryptography, the chaos of the circuit is critical to determine the encryption and decryption. These systems are build on the Chua’s memristive circuit, which has a large inductance that is usually difficult to build in coil windings. Therefore, we have introduced an array which reduces the large inductance in two smaller coupled inductors and at the same time improves the quality of the WPT. 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 organised as follows below.

The circuit design and the main functionality are shown in the section II and in the paragraph II-A we have explained the memristor model. In the section III, there is an analysis of the cryptography. The system simulation and the synchronisation results are presented in the section IV. The experiment results
WIRELESS POWER TRANSFER SYSTEM

The NFC (Near-field Communication) is based on the WPT system. The NFC transponder is the main element of the whole system, as it allows to read and write data on it. There are a large number of NFC tags that vary in shape, size, construction material [30], but all of these can be grouped into two main categories. One category is Active, when the device draws energy from their own power supply usually consisting of a long-lasting battery. The other category is Passive, when they do not have their own source of energy, but derive it from the electromagnetic field generated by the transponder.

The Passive devices are the majority of NFC tags. When the reader passes, the electromagnetic field transmits the power necessary to operate and activates the microchip inside the tag. Although the range of NFC is limited to a few centimetres, plain NFC does not guarantee secure communications. NFC technology was developed with particular attention to data and transaction security. In fact, there are various levels of security that allow you to move from a completely open and unencrypted model to a complex system with DES encryption [31].

In this work we built an WPT system based on a Memristive circuit capable of producing chaotic waveform. By adopting Memristors, there are three great advantages: the ability to store charge like a memory, the ability to develop chaotic behaviour, and the ability to provide less heat than transistors or switches. The Memristive WPT (M-WPT) system created has features similar to the NFC, as shown in Table 2. Theoretical analysis on WPT system are based on the maximum efficiency, maximum load power transfer, compensation and coil design. The similar system is the NFC, which is based on energy harvesting and transmission of data. The NFC analysis are usually based on the power harvested from the periodic signal from the transmitter. In the M-WPT, the system is chaotic, so we can only give an estimation on the maximum power transmitted. By adopting the Chua circuit, the M-WPT can create a chaotic waveform that can be used for a highly encrypted communication. The waveform generated is based on the last configuration of the state variables. Each time the system reads from the memristor, the internal state variable of the memristor will bring the system to a different, chaotic and unrelated stabilisation point. As the chaos is not based on a known algorithm, it cannot be replicated. In addition, the system is able to create chaotic behaviour only for a certain inductive value. Therefore, two receivers at the same time will create a surplus inductive value which will unable the system to have a chaotic behaviour.

ARRAY OF INDUCTORS

In this paper, we use the mutual inductance of the primary and secondary coil to transmit power and data. Analogous
to the NFC system, the power is harvested when the two parts of the system are in proximity. Once both parts power themselves, they synchronise chaotically. Without using the array, the inductors $L_P$ and $L_S$ values could be approximately 8 mH, which is much lower than the usual 12 mH values in the Chua memristive circuits. The $L_{TOT}$ total inductance is equal to $L_P + 2 * M_{12}$, which is still 12 mH, but the coil design is only for a 8 mH. It is also possible to have a much lower value using the other mutual induction, as it will be shown in the next paragraph. This value is necessary to obtain the Chaotic Behaviour (CB), which will be used for the encryption. The transmitter and receiver will oscillate chaotically and resonate at the same frequency:

$$f_0 = \frac{1}{2\pi \sqrt{L_{TOT} C_1}}$$

and by adopting the values reported in Table 3, it gives 6.8 kHz. The current flowing in $L_P$, the transmitter coil, sets up a magnetic field around itself. Some of these magnetic field lines are passing through the receiver coil $L_S$ giving mutual inductance. When the inductances of the two coils are the same and equal, $L_P$ is equal to $L_S$, the mutual inductance that exists, will equal the value of one single coil, as the square root of two equal values.

$$M = k \sqrt{L_P L_S} = kL$$

$M$ also depends on the coupling coefficient as an inductive fraction number from 0 to 1, where zero is indicates no inductive coupling, and 1 indicates full or maximum inductive coupling. Values lower than 0.8 are not sufficient to initiate a chaotic behaviour and subsequently not able to change the memristor variable state. The transmitter coil $L_P$ induces a voltage in the adjacent coil $v_{in}^{p2}$ and $v_{in}^{p3}$, and viceversa $v_{in}^{p}$. Using these relationships, it is possible to adopt lower inductances compared to the Chua’s circuit and the symmetry of the circuitry allows to transmit the chaotic behaviour. As mentioned above, the total inductance value for the circuit will be very high for each side. For this reason, we have developed the secondary coil as two mutually coupled inductors in series, which are both coupled to the primary as well. In this way, we use the mutual inductance between the two coils in the secondary to further reduce all the inductances of the coils. In the simulation results section IV, more details will be given about the values that can be adopted for each side.

### B. MEMRISTOR MODEL

In reference to the Chua memristive circuit, the internal relationship of the memristor mode is the same. The circuit’s behaviour stems from the classic Chua circuit, substituting it

### TABLE 2. Comparison of traditional WPT and a M-WPT system.

|                  | WTP (NFC)       | M-WPT          |
|------------------|-----------------|----------------|
| Power            | Transmitted (Harvested) | Harvested     |
| Data             | Oscillation     | Chaos          |
| Distance         | Over 30 cm (10 cm) | 10 cm          |
| Operating Frequency | Up to 13.5 MHz  | Up to 7 KHz    |
| Control          | Timing, Switches and Data Algorithm | Data |
| Receivers        | Many            | Only one       |

In the secondary, the two coils mutually induce themselves, as shown in the third part of the equation by the value of $M_{23}$. Using these relationships, it is possible to adopt lower inductances compared to the Chua’s circuit and the symmetry of the circuitry allows to transmit the chaotic behaviour. As mentioned above, the total inductance value for the circuit will be very high for each side. For this reason, we have developed the secondary coil as two mutually coupled inductors in series, which are both coupled to the primary as well. In this way, we use the mutual inductance between the two coils in the secondary to further reduce all the inductances of the coils. In the simulation results section IV, more details will be given about the values that can be adopted for each side.

### FIGURE 4. The system of wireless power transfer built with Memristors.

### FIGURE 5. The induced voltage in each coil as show in Equation 3.
C. S. Kuka et al.: Innovative NFC Security Based on the Chaos Generated by Memristive Circuits Adopted as Symmetrical Key

III. CRYPTOGRAPHY

The cryptography model of the Memristor-based chaotic system consists of two parts, which are the two symmetrical Chua’s circuits, the Transmitter and the Receiver respectively, as shown in Fig. 4. The initial condition is applied on the Capacitor $C_{1P}$ from an external digital source, exactly as in a typical Chua circuit. Therefore, in the $L_pC_{1P}$ there is a connection to A/D or D/A converters, as the system is a both way communication. In the cryptosystem model, the memristor-based chaotic circuit is critical in deciding the encryption and decryption. When the user device key (UDK), which is defined as the internal state value of the memristor, is given, then a new CB is generated from the UDK. The digital sequence of the chaotic encryption (ECB) and decryption (DCB) is developed once the CB has been obtained. The information can be encoded/decoded according to the cryptosystem model.

The system adopts the symmetrical key, which involves only one secret key to cipher and decipher information sent to both parts. The key is the chaos generated from the circuits. The great advantage is that the key can be applied only and exclusively at the transmitter and the receiver at the same time. If a third party tries to join, the CB in the circuits will stop immediately because the inductive load will change. This type of encryption is a step over the most widely used symmetric algorithms such as AES, RC5 and DES, which support multiple receivers.

A. ENCRYPTION

According to the cryptosystem model shown in Fig. 7, the process of chaotic encryption of text/image is described as follows.

1) Step 1 The data (text/image) is applied to the primary as the input of the cryptosystem. Within the user proximity, the UDK input, the memristor-based chaotic system generates the CB. Hence, the UDK maps ECB which is an analogue voltage in the range of $-2.5$ to $+2.5$ Volt (depending on the memristor equivalent).

2) Step 2 The ECB is mapped to the value from zero to one for random function compatibility.

3) Step 3 From the ECB sequence, the random generator is created with NumPy and the chaotic key CK) sequence is generated.

4) Step 4 The CK encrypt the information and achieves the cipher data sequence (CDT).

with the non-ideal active controlled voltage memristor model shown in Fig. 2 b. This model is the most developed in application circuits [33], as well as the diode bridges cascaded with RC, LC or RLC filters [34]. The latter is composed of a buffer $U_1$, an integrator $U_2$ connected to two resistors $R_1$, $R_2$, a 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 $R_5$. 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 $G_a = \frac{1}{R_2}$ and $G_b = \frac{R_2}{R_5}$. This model is characterised by the two equations:

$$i_M = (-G_a + G_b \cdot v_0^2) v_M$$

$$\frac{dv_0}{dt} = -\frac{v_M}{R_1C_0} - \frac{v_0}{R_2C_0}$$

where $i_M$ is the current flowing in the memristor, $v_M$ is the voltage on the memristor and $v_0$ is the voltage on its internal capacitor $C_0$. When the two parts of the system are nearby each other, either side of the system will be capable of developing a CB. In the simulation results, the Chua’s circuit adopting this model develops a double-scroll phase portrait, as shown in Fig. 8.
When the WPT system has reached the end of the information (End Of File), both digital parts will disconnect the Memristor. The Memristor last status will be stored as a memory.

B. DECRYPTION

According to the cryptosystem model shown in Fig 7, the process of chaotic decryption of text/image is described as follows.

1) Step 1 The CDT is applied to the secondary as the input of the cryptosystem. Within the user proximity, the UDK input, the memristor-based chaotic system generates the CB. Hence, the UDK maps DCB, which is an analogue voltage in the range of $-2.5$ to $+2.5$ Volt (depending on the memristor equivalent).

2) Step 2 The DCB is mapped to the value from zero to one for random function compatibility.

3) Step 3 From the ECB sequence, the random generator is created with NumPy and the chaotic key CK) sequence is generated.

4) Step 4 The CK decrypts the information, and obtains the original data (text/image).

Furthermore, any falsify attempt on the device will leave an indelible mark, because it will make the internal memristor value a new value, which will create a new CB for the authentication key. It is not possible to return in the previous internal variable state. Despite the fact that the electronic system can be cloned, the internal value of the memristor can never be predicted and there is no algorithm capable of predicting this value.

IV. SIMULATIONS AND EXPERIMENT

In order to simulate the system created, we have initially started from the design of the coils. ANSYS Maxwell v19 software has been used to test the coils design and to study the energy harvested, as well as the coupling coefficient between the coils. It is possible to design the primary coil of 5 mH value in the dimensions of 90 x 130 mm. For the secondary, we have fit the two coils of 2.5 mH value at the same size and achieved a small gap between the two coils. The value of 2.5 mH is one of the lowest inductive values in a Chua circuit design, which is one of the main novelties in this paper. Successively, we have started the simulation for different medium gaps (air, plastic or any material with relative permeability $\mu_R = 1$) between coils. In a close distance of 2-3 mm, the coupling reaches the value of nearly 0.9, which assures a chaotic behaviour. As shown in figure 9a, the system is able to achieve energy harvesting up to 100 mm with a low coupling down to 0.4. As highlighted in the yellow cloud in figure 9b, the secondary is still able to receive energy.

The system is close similar to the NFC system. An analysis on the power efficiency is not equitable because the system harvests energy and we are using a active memristor model instead of a real memristor. Therefore, both the transmitter and the receiver side are powered by external power sources. It is important to notice that the primary is transmitting the chaotic behaviour which has encrypted digital values. In reality, the power necessary is much higher than what a real memristor would require. By using a circuit simulator,
we confirm the development of a chaotic waveform typical of the Chua’s memristive circuit, where the system developed double-scroll phase attractors in the transmitter (in blue) and the receiver (purple), shown in figure 8. The maximum power at the primary coil is obtained by $P_{\text{MAX}} = I_{\text{MAX}} \times V_{\text{MAX}}$, and extracting the values from the simulations of the graphs in figure 8, the maximum power transmitted is close to 0.6 W. Because the receiver waveform has a short delay, the efficiency will always be under 1. In addition, the coils are considered pure inductive, which are not applied in a practical experiment.

The graphs in figure 10 show the simulation of the system with two synchronisation signals. This situation is a typical encoding in which a synchronisation is sent before the payload transmission. The transmitter sends a synchronising signal through the Vin, which is the voltage on the capacitance C1. The first graph shows the voltage on the parallel of the capacitance and coil. As can be seen in the second graph, the voltage on the receiver coil continues to vary randomly, maintaining encryption. As it can be seen in the first graph, this is the signal transmitted on air, which is completely chaotic. The synchronisation, circled in red, is not perceptible on air and is hidden in the waveform. This does not happen in the memristor. In the third and fourth graphs, the synchronising signal has no effect on the status of the transmitter memristor, but on the receiver memristor instead. The latest recognises the value and keeps it constant for about the duration of the signal (in reality it lasts less for the transient “rise” and “fall” time). This internal voltage of the memristor is unique, not recognisable externally and represents an indispensable factor for coding. The fifth graph shows the synchronisation signal.

After the system produced the desired chaotic behaviour on both sides, we proceeded to use values obtained from the coding simulations. To carry out the coding, it is necessary to quantify the values of this chaotic behaviour. The results obtained from the simulations are lists that the software plots. This list is simply a sequence of numbers representing the
chaotic behaviour. So the encryption can be done by taking the list of simulations and using this data in a python code.

The python code generates a CK encoding key from the ECB sequence. In addition to the chaotic behaviour sequence, the data to be encoded must also be entered. In the example, an old Italian identity document, made up of text and images, is inserted as input data in the code. As seen in the figure 7, both data are encrypted according to the CK key obtaining the gray image in the scrambled data. The decryption takes place with the same CK key obtained from a chaotic ECB sequence.

A. EXPERIMENT RESULTS
The system is comparable to the NFC system. We are also adopting an equivalent memristor circuit rather than the real memristor. Therefore, measurements such as power transferred and distance are not significant, because the primary and the secondary are both active and the system is not transferring power in distance. The significant test is the development of chaos in the circuits using only 2.5 mH. A PCB model of the system has been built to verify functionality. In order to build the non-ideal active voltage-controlled memristor, it has been used the AD711JRZ operational amplifier and the AD633JRZ multiplier. For the physical experiment, a PCB has been built. The size of printed circuit is very small and not clear in real pictures, because is covered by probes and wires. Therefore, we have shown the schematic of the PCB (as shown in the figure 11) from the manufacturer website. As schematized in figure 11, the inductors are not included in the PCB design. They will be added in the connectors that are left open to test different solutions. In 12 a, there are shown the voltages of the inductors coils in the transmitter $V_{LP}$ (yellow) and receiver $V_{LS}$ (blue). There is a small delay time between the two waveforms which is caused by the transmission. The consistency of the information is assured by the digital data encrypted on it such as the synchronisation signal. In the 12 b, we have depicted the memristor voltages at the transmitter $V_{MP}$ (yellow) and receiver $V_{MS}$ (blue). In proximity of the coils, it has been added an external shunt resistor of 1 Ω and measured the voltage in order to obtain the current values, shown in yellow (transmitter) and blue (receiver) 12 c.

Instead of using coils for the power transmission, it has been adopted the Tamura 5 mH 2:1:1 transformer. Unfortunately, because of the parasitic effects, the system did not oscillate. So we adopted a Tamura 6 mH 2:1:1 transformer and the system developed the chaotic behaviour, as depicted in the figure 12. It has also been tried a 8 mH 2:1:1, but there was no advantages observed, as the system developed a similar behaviour. Using a 6 mH transformer (6 mH primary and 3 mH secondaries) the two circuits can have the same chaotic behaviours because they have the same parameters and initial conditions, as shown in figure 8. Due to the non-ideal active voltage-controlled memristor, a single phase portrait is obtained in the figure 12 d, differently from the simulation results obtained in the figure 8. In order to verify

the circuit functionality under non ideal conditions, it has been used non-ideal memristor emulator as it is the key element for the synchronisation and the integrity of the signal. There are other non ideal parameters that could be considered but they do not affect (under certain limits) the possibility of the circuits to chaotically oscillate or to transmit chaos wirelessly.

V. CONCLUSION
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 in the well-known algorithms and software. Therefore, the unique behaviour of the memristor has attracted a lot of research studies and interests in developing new encryption characteristics. Furthermore, the memristor in a modified Chua’s circuit is able to generate a power and data transmission, provided that the inductors are mutually coupled. For this reason, we created a two symmetrical Chua circuits able to transmit chaos. This new technique is an interesting solution, due to the fact it can achieve a near-field wireless communication, which can create encryption using a true number generator. There are many algorithms based on chaos and a new algorithm requires a cryptanalysis, but this is not the aim of the article. For this reason, in the article we have not mentioned the algorithm used in Python. We are introducing an innovative design of the Chua circuit, which is applied in the NFC. In addition, the system can store the previous values as a memory and cannot be cloned. An attempt of forgery will leave an indelible trace in the memristor memory.

Future work will be focused on improving the data encryption and the realisation of multi-coils production,
because they show a great and interesting advantage in comparison with the traditional Chua’s circuit. A further improvement on the Python true number generator will be required, in order to enhance the performance. The interesting property of the memristor creates many possibilities of future work, particularly if we increase the order of the chaos to hyperchaos.

**REFERENCES**

[1] M. Integrated. Max66242. Accessed: May 2020. [Online]. Available: https://www.maximintegrated.com/en/products/embedded-security/secure-authenticators/MAX66242.html

[2] J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the Internet of Things: A survey of existing protocols and open research issues,” *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[3] V. Coskun, B. Ozdenizci, and K. Ok, “A survey on near field communication (NFC) technology,” *Wireless Pers. Commun.*, vol. 71, no. 3, pp. 2259–2294, 2013.

[4] D. Sethia, D. Gupta, and H. Saran, “NFC secure element-based mutual authentication and attestation for IoT access,” *IEEE Trans. Consum. Electron.*, vol. 64, no. 4, pp. 470–479, Nov. 2018.

[5] V. Odelu, A. K. Das, and A. Goswami, “SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms,” *IEEE Trans. Consumer Electron.*, vol. 62, no. 1, pp. 30–38, Feb. 2016.

[6] M. Roland and J. Langer, “Comparison of the usability and security of NFC’s different operating modes in mobile devices,” in *Elektrotechnik und Informationstechnik*, vol. 130, no. 7, pp. 201–206, 2015.

[7] R. Toegel and M. Hutter, “An approach to introducing locality in remote attestation using near field communications,” *J. Supercomput.*, vol. 55, no. 2, pp. 207–227, Feb. 2011.

[8] F. Dang, E. Zhai, Z. Li, P. Zhou, A. Mohaisen, K. Bian, Q. Wen, and M. Li, “Pricing data tampering in automated fare collection with NFC-equipped smartphones,” *IEEE Trans. Mobile Comput.*, vol. 18, no. 5, pp. 1159–1173, May 2019.

[9] D. Sethia, D. Gupta, V. Kumar, and H. Saran. Technical Report for Implementation of Secure NFC-Based IoT Prototype Using Mobile Devices. [Online]. Available: https://sites.google.com/site/divyashikhasethia/home/securitynfc-based-iot-access/IoTPrototypeTechReport.pdf

[10] M. A. Bouazzoumi, E. Conchon, and F. Peyrand, “Trusted mobile computing: An overview of existing solutions,” *Future Gener. Comput. Syst.*, vol. 80, pp. 596–612, Mar. 2018.

[11] S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S. P. Mohanty, and S. Ghosh, “A survey on NFC’s different operating modes in mobile devices,” *IEEE Access*, vol. 6, pp. 66055–66061, 2018.

[12] H. Bao, K. T. Chau, C. Qiu, and C. Liu, “Energy encryption for wireless power transfer,” *IEEE Trans. Power Electron.*, vol. 30, no. 9, pp. 5237–5246, Sep. 2015.

[13] Z. Zhang, K. T. Chau, C. Qiu, and F. Lin, “An efficient wireless power transfer system with security considerations for electric vehicle applications,” *J. Appl. Phys.*, vol. 115, no. 17, 2014, Art. no. 17A328.

[14] S. Kuka, K. Ni, and M. Alkahtani, “A review of methods and challenges to precharged buses: A general analysis for symmetric-key cryptographic algorithms,” *IEEE Trans. Dependable Secure Comput.*, vol. 7, no. 3, pp. 226–239, Jul. 2010.

[15] D. Yu, C. Zheng, H. H.-C. Iu, T. Fernando, and L. O. Chua, “A new circuit for emulating memristors using inductive coupling,” *IEEE Access*, vol. 5, pp. 1284–1295, 2017.

[16] Z. Zhang, K. T. Chau, C. Qiu, and F. Lin, “An efficient wireless power transfer system with security considerations for electric vehicle applications,” *IEEE Access*, vol. 7, pp. 58751–58763, 2019.

[17] J. Sun, Y. Shen, Q. Yin, and C. Xu, “Compound synchronization of four memristor chaotic oscillator systems and secure communication,” *Chaos, Interdiscip. J. Nonlinear Sci.*, vol. 23, no. 1, Mar. 2013, Art. no. 013140.

[18] H. Eun, H. Lee, and H. Oh, “Conditional privacy preserving security protocol for NFC applications,” *IEEE Trans. Consum. Electron.*, vol. 59, no. 1, pp. 153–160, Feb. 2013.

[19] 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, pp. 58751–58763, 2019.

[20] H. Bao, N. Wang, H. Wu, Z. Song, and B. Bao, “Bi-stability in an improved memristor-based third-order wiener-bridge oscillator,” *IETE Tech. Rev.*, vol. 36, no. 2, pp. 109–116, Mar. 2019.

[21] H. Bao, N. Wang, B. Bao, M. Chen, P. Jin, and G. Wang, “Initial condition-dependent dynamics and transient period in memristor-based hyperbolic jerk system with four line equilibria,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 57, pp. 264–275, Apr. 2018.

[22] 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 Trans. Magn.*, vol. 44, no. 1, pp. 1–6, Nov. 2018.

[23] Z. Zhang, K. T. Chau, C. Qiu, and C. Liu, “Energy encryption for wireless power transfer,” *IEEE Trans. Power Electron.*, vol. 30, no. 9, pp. 5237–5246, Sep. 2015.

[24] Z. Zhang, K. T. Chau, C. Qiu, and F. Lin, “An efficient wireless power transfer system with security considerations for electric vehicle applications,” *J. Appl. Phys.*, vol. 115, no. 17, 2014, Art. no. 17A328.

[25] J. Goodman, A. P. Dancy, and A. P. Chandrakasan, “An energy/security scalable encryption processor using an embedded variable voltage DC/DC converter,” *IEEE J. Solid-State Circuits*, vol. 33, no. 11, pp. 1799–1809, 1998.

[26] E. Ahene, Z. Qin, A. K. Adusei, and F. Li, “Efficient signcryption with proxy re-encryption and its application in smart grid,” *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9722–9737, Dec. 2019.

[27] H. Eun, H. Lee, and H. Oh, “Conditional privacy preserving security protocol for NFC applications,” *IEEE Trans. Consum. Electron.*, vol. 59, no. 1, pp. 153–160, Feb. 2013.

[28] 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, pp. 58751–58763, 2019.

[29] J. Sun, Y. Shen, Q. Yin, and C. Xu, “Compound synchronization of four memristor chaotic oscillator systems and secure communication,” *Chaos, Interdiscip. J. Nonlinear Sci.*, vol. 23, no. 1, Mar. 2013, Art. no. 013140.

[30] S. F. Wang, “Dynamical analysis of memristive unified chaotic system and its application in secure communication,” *IEEE Access*, vol. 6, pp. 66055–66061, 2018.

[31] 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 Electron. Drives*, vol. 1, no. ahead-of-print, 2020.

[32] A. S. Butter, C. Y. Kao, and J. P. Kuruts, “Des encryption and decryption unit with error checking,” U.S. Patent 5,432,848, Jul. 11, 1995.

[33] M. Alioto, M. Poli, and S. Rocchi, “Differential power analysis attacks to precharged buses: A general analysis for symmetric-key cryptographic algorithms,” *IEEE Trans. Dependable Secure Comput.*, vol. 7, no. 3, pp. 226–239, Jul. 2010.

[34] D. Wu, B. Bao, Z. Liu, Q. Xu, and P. Jiang, “Chaotic and periodic bursting phenomena in a memristive Wien-bridge oscillator,” *Nonlinear Dyn.*, vol. 83, nos. 1–2, pp. 893–903, Jan. 2016.
YIHUA HU (Senior Member, IEEE) received the B.S. degree in electronic motor driver and the Ph.D. degree in power electronics and drives from the China University of Mining and Technology, China, in 2003 and 2011, respectively. From 2011 to 2013, he was with the College of Electrical Engineering, Zhejiang University, as a Postdoctoral Fellow. From 2012 to 2013, he was an Academic Visiting Scholar with the School of Electrical and Electronic Engineering, Newcastle University, Newcastle upon Tyne, U.K. From 2013 to 2015, he was a Research Associate with the Power Electronics and Motor Drive Group, University of Strathclyde. He is currently a Lecturer with the Department of Electrical Engineering and Electronics, University of Liverpool. He has authored over 35 peer reviewed technical articles in leading journals. His research interests include PV generation systems, power electronics converters and control, and electrical motor drives.

QUAN XU (Member, IEEE) was born in Lianyun-gang, China, in 1983. He received the B.S. degree in physics from the School of Huaiyin Teachers College, in 2005, and the M.S. and Ph.D. degrees in optical engineering from the University of Electronics Science and Technology of China, in 2011. Since 2011, he has been a Teacher with Changzhou University, China. He is the author of more than 30 articles, and more than ten inventions. His research interests include memristor and its applications and memristive chaotic circuit/systems.

MOHAMMED ALKAHTANI (Graduate Student Member, IEEE) was born in Ar Rayn, Saudi Arabia. He received the B.Eng. degree (Hons.) in electrical and electronics engineering and the M.Sc. degree in electrical power and control engineering from Liverpool John Moores University, Liverpool, U.K., in 2014 and 2016, respectively. He is currently pursuing the Ph.D. degree with the University of Liverpool. His research interests include soil management of photovoltaic and PV array efficiency improvement.