Second Harmonic Generation Exploiting Ultra-Stable Resistive Switching Devices for Secure Hardware Systems

Ziang Chen, Nan Du, Mahdi Kiani, Xianyue Zhao, Ilona Skorupa, Stefan E. Schulz, Danilo Bürger, Massimiliano Di Ventra, *Member, IEEE*, Ilia Polian, *Senior Member, IEEE*, and Heidemarie Schmidt

***Abstract*—In the era of Big Data and Internet of Things (IoT), information security has emerged as an essential system and application metric. The information exchange among the ubiquitously connected smart electronic devices requires functioning reliably in harsh environments, which highlights the need for securing the hardware root of trust. In this work, by leveraging the uniform nonlinear resistive switching of emerging electroforming-free analog memristive device based on $BiFeO_3$ (BFO) thin film, the security-oriented hardware primitive (SoHP) system is developed and optimized with high-security level. The SoHP system utilizes the distinguishable power conversion efficiency generated at second and higher harmonics in low resistance state (memristor with diodelike behavior) and high resistance state (memristor with high resistive behavior) of memristive devices. By exploring the significant influence of writing bias and operational frequency in sourcing input voltage on the dynamic switching behavior of memristive device, the novel 2-memristor encoding scheme and 1-memristor decoding scheme are developed for SoHP system, which realizes a frequency enhancement of 4000 times in comparison to 1-memristor encoding scheme and 2-memristor decoding scheme. The encoded data bits that generated from physically implemented SoHP system pass diverse statistical test suites (i.e. ENT, BSI, and NIST SP-800.22 statistical test suites), which indicates the high randomness distribution of the encoded data and the high-security level of the proposed memristive encoding system.**

***Index Terms*—Ultra-stable resistive switching, second harmonic generation, hardware security, power conversion efficiency.**

Manuscript received October 9, 2021; accepted December 9, 2021. Date of publication December 15, 2021; date of current version February 10, 2022. The work of Ziang Chen, Nan Du, Xianyue Zhao, and Ilia Polian was supported by the German Research Foundation (DFG) Priority Program Nano Security, Project MemCrypto under Grant DFG439827659. The work of Nan Du, Danilo Bürger, and Heidemarie Schmidt was supported by the Fraunhofer Internal Programs under Grant 600768. The review of this article was arranged by Associate Editor Amit Acharyya. *(Corresponding authors: Nan Du; Heidemarie Schmidt.)*

Ziang Chen, Nan Du, Mahdi Kiani, Xianyue Zhao, Stefan E. Schulz, and Danilo Bürger are with Department Nano Device Technology, Fraunhofer-Institut for Elektronische Nanosysteme ENAS, Chemnitz 09126, Sachsen, Germany (e-mail: ziang.chen@enas-extern.fraunhofer.de; nan.du@enas.fraunhofer.de; mahdi.kiani@enas-extern.fraunhofer.de; xianyue.zhao@enas-extern.fraunhofer.de; Stefan.Schulz@enas.fraunhofer.de; danilo.duerger@enas.fraunhofer.de).

Ilona Skorupa is with the Institute of Ion Beam Physics and Materials Research, Helmholtz-Zentrum Dresden-Rossendorf, Dresden 01328, Sachsen, Germany (e-mail: i.skorupa@hzdr.de).

Massimiliano Di Ventra is with the Department of Physics, University of California San Diego, La Jolla, CA 92093 USA (e-mail: diventra@physics.ucsd.edu).

Ilia Polian is with the Institute of Computer Engineering and Computer Architecture, University of Stuttgart, Stuttgart 70174, Baden-Württemberg, Germany (e-mail: ilia.polian@informatik.uni-stuttgart.de).

Heidemarie Schmidt is with the Department of Quantum Detection, Leibniz Institute of Photonic Technology, Jena 07745, Thüringen, Germany (e-mail: heidemarie.schmidt@enas.fraunhofer.de).

This article has supplementary downloadable material available at https://doi.org/10.1109/TNANO.2021.3135713, provided by the authors.

Digital Object Identifier 10.1109/TNANO.2021.3135713

I. Introduction

With the widespread application of electronic systems in communication devices, the demand for secure hardware and secure data transmission has been dramatically increased. The majority of available classical mathematical or algorithmic cyber-defenses in the software-based security system concentrate on protecting the software part of electronic systems or their communication interfaces, which are not only high-energy consuming, but also vulnerable to brute force and malicious code [1], [2]. With the advent of smart homes, smart cities, smart transportation, and infrastructure, etc, the need for securing the hardware root of trust in the Internet of Things (IoT) becomes incredibly anxious [3], [4]. Several studies on hardware-oriented security applications have demonstrated the robustness of functional systems based on nano-electronic technology and their preliminary security capabilities, i.e. memristors [5]–[7], spin-torque devices [8], [9], phase change materials [10], [11], silicon nanowires [12], [13], and etc.. The memristor, as one promising candidate among nano-electronic devices, have the potential to construct innovative computing systems with nanoscale miniaturization [14], [15] and low-power consumption [16].

In the recent years, forming-free $BiFeO_3$ (BFO) memristors have drawn much attention due to highly uniform switching performance with excellent endurance and retention properties [17]–[19] and their promising applications in neuromorphic computing [16], [20]–[22], reconfigurable Boolean logics [23], [24], and in our previous work [25], we have demonstrated the hardware security system by exploiting the second of harmonic generation functionality of analog BFO memristive devices. In this work, based on the nonvolatile nonlinear switching dynamic of BFO memristive devices, we study the impact of writing bias and operational frequency on the generated second harmonic power efficiency, and further optimized the design schematics of the BFO memristor based security-oriented hardware primitive (SoHP) on PCB board, i.e. SoHP-PCB system with 2-memristor

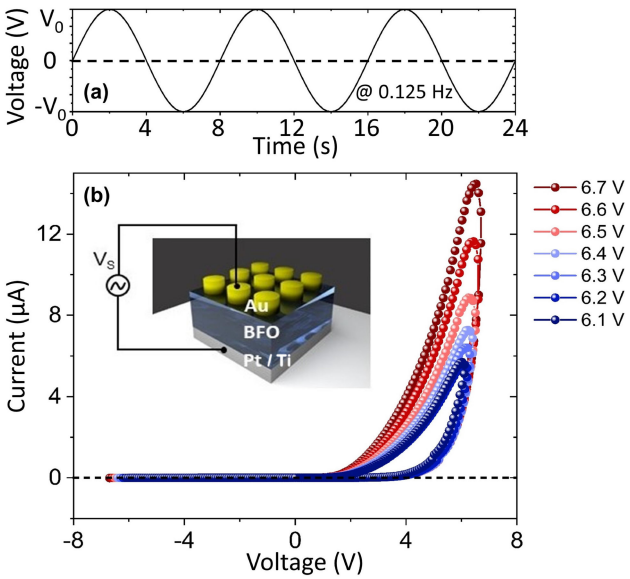


Fig. 1. (a) Sequence of sinusoidal ramping voltage $V_S(t) = V_0 \sin(2\pi f_1 \cdot t)$ with amplitude V_0 ranging from 6.1 V to 6.7 V and frequency $f_1 = 0.125$ Hz and (b) corresponding current voltage characteristics on a logarithmic scale of BFO memristive device with thickness 500 nm and top electrode size 1E5 μm^2. The inset of (b) shows the schematic sketch of the BFO memristive device.

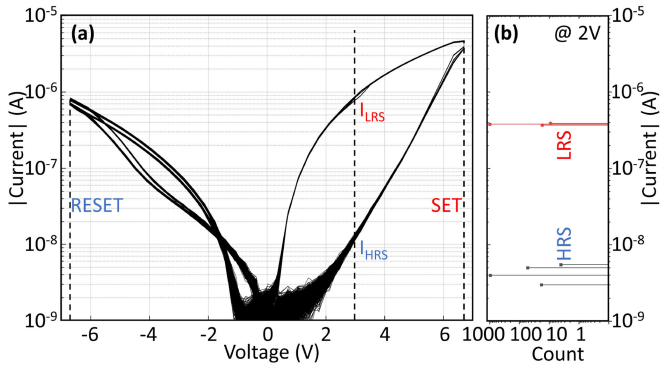


Fig. 2. (a) Endurance tests result for BFO memristor by exploiting 1000 cycles of sinusoidal ramping voltage $V_S(t) = V_0 \sin(2\pi f_1 \cdot t)$ with amplitude $V_0 = 6.7$ V and frequency $f_1 = 0.125$ Hz. The LRS and HRS current are defined at smaller reading bias V_r ($V_{r,max} = 3$ V). (b) Histogram of reading current at $V_r = 2$ V as an example. The concentrated reading currents prove the ultra-uniformity of the Current-Voltage performance of the BFO memristor.

encoding scheme and 1-memristor decoding scheme, which has realized the improvement of encryption speed by 4000 times in comparison to the SoHP implementation in previous work [25].

The work is organized as follows: After the introduction of the ultra-stable switching behavior of BFO memristor in Section I, the writing bias and frequency-dependent power conversion efficiencies of the BFO memristor are analyzed in Section II. By investigating the optimization progress of the laboratory implementation for BFO memristor-based SoHP systems, the optimized circuit block diagram of memristive SoHP system is finalized (Section III). For investigating the security level of the implemented SoHP system, the randomness test result of encrypted data by using NIST SP-800.22 statistical test suite reveals the security level of the optimized memristive SoHP system.

II. High Efficient Second Harmonic Generation Exploiting BFO Memristive Devices

By revealing the nonvolatile nonlinear high uniform switching behavior of BFO memristive devices, high efficient second harmonic can be generated. The writing voltage and frequency dependence of the testing signal play an essential role in the encoding and decoding performance of SoHP system.

A. BFO Memristive Devices With Nonlinear High Uniform Switching Behavior

Polycrystalline BFO thin film with the thickness of 500 nm was deposited by pulsed laser deposition (PLD) on Pt/Ti/SiO_2/Si substrate with Pt/Ti layer thickness of 100 nm /50 nm. The schematic sketch of the Au-BFO-Pt/ Ti MIM structure is depicting in the inset of Fig. 1. The physical mechanism underlying resistive switching of BFO memristive devices is related with the nonvolatile change of flexible barriers at Ti-containing bottom electrode region. Circular Au top electrodes with an area of 1E5 μm^2 and a thickness of 150 nm were fabricated by DC magnetron sputtering at room temperature using a metal shadow mask for the following current-voltage and higher harmonic generation tests. The downscaling of the thickness of BFO thin films, i.e. from 500 nm to 100 nm, has been investigated in our previous work [26]. With downscaled BFO thin film thickness the writing bias of BFO memristive device can be further reduced with maintained switching behavior. Due to its reliable and uniform switching behavior, the BFO memristor with BFO thin film thickness of 500 nm is chosen for the second harmonic generation in this work.

For operating the BFO memristive device, the large writing biases with opposite polarity are required to switch the device into the valid low resistance state (LRS) or high resistance state (HRS) for the application-oriented purpose. As demonstrated in Fig. 1 the current voltage characteristics of BFO memristive device are recorded under the sinusoidal sourcing voltage $V_S(t) = V_0 \sin(2\pi f_1 \cdot t)$ with diverse amplitudes V_0. During the IV testing, the sinusoidal sourcing input voltage (with 80 testing points and 0.1 s time width per testing point) is applied to the top electrode of the memristive device. Thus the testing frequency of sinusoidal sourcing input voltage for recording IV characteristics amounts to 0.125 Hz. As demonstrated in Fig. 2, by applying large positive input bias, e.g. +6.7 V, to the Au top electrode of BFO memristive device, the device is switched to LRS. This process is identified as SET process, thus the LRS current I_{LRS} can be recorded at a small reading bias, e.g. 3 V. By sourcing large negative input voltage, e.g. −6.7 V, to the Au top electrode, the device can be then switched to HRS, and the switching process is identified as RESET process. Thus the HRS current I_{HRS} can be recorded at a small reading bias, e.g. 3 V. The analog hysteresis is recognizable within the positive bias range in the IV characteristics of BFO memristor. It reveals the self-rectifying nonlinear switching behavior of BFO memristive device. The nonvolatile property of BFO memristive device ensures that the device remains in LRS or

HRS under a small reading bias V_r ($V_{r,max} = 3$ V). The Off/On ratio of corresponding analog hysteresis at 3 V under voltage amplitude V_0 of $|\pm 6.7|$ V amounts to 91.60, which is calculated by using the following equation: I_{LRS}/I_{HRS} or R_{HRS}/R_{LRS}. Hence the Off/On ratio is unitless. By applying the sinusoidal sourcing voltage with decreasing voltage amplitudes V_0 from 6.7 V to 6.1 V, the Off/On ratio of analog hysteresis at reading bias 3 V is shrinking due to the decreasing LRS current, i.e. from 91.60 to 25.38. It further reveals that multi-level resistive switching states of BFO memristive device are realizable under different V_0. By applying 1000 cycles of sinusoidal ramping voltage $V_S(t)$ with amplitude $V_0 = 6.7$ V and frequency $f_1 = 0.125$ Hz, the endurance performance of the BFO memristor is explored in Fig. 2. The concentrated reading currents at small reading bias, e.g. at 2 V, in LRS and HRS from 1000 cycles of IV characteristic reveal ultra-uniform switching behavior of BFO memristor in comparison to other types of memristive devices [27]–[29], which fundamentally ensures the stability of the second harmonic generation in the BFO memristor based SoHP system.

The self-rectifying behavior and its nonlinear switching dynamics of BFO memristive device makes it feasible for generating the second and higher harmonics which can be used for hardware-oriented encoding and decoding system with higher security level. As shown in the inset of Fig. 1(b), a sinusoidal sourcing voltage $V_S(t)$ is applied between the Au top and Pt bottom electrodes of BFO memristive device as the excitation stimuli for the second and higher harmonic generation. The power ratio between the average power at k-th harmonics and average source power is defined as the power conversion efficiency P_k/P_s (PCE), which is the crucial parameter for data encoding and decoding procedures. The corresponding second and higher harmonic signals are translated into frequency domain by Fast Fourier Transform (FFT) transformation for further computing the PCE values.

B. Power Conversion Efficiency Based on Memristive Device

For generating the distinguishable second and higher harmonic, the memristive device is initialized to LRS (HRS) by applying single 100 ms writing pulse with pulse amplitude $V_w = +6.7$ V ($V_w = -6.7$ V) to the top electrode of device, and the PCE values at different harmonics are recorded under the sinusoidal sourcing voltage $V_S(t) = V_0 \sin(2\pi f_1 \cdot t)$ with $V_0 = 3$ V and $f_1 = 0.125$ Hz. PCE values are generated and computed based on the circuit topology with BFO memristor in series of a variable linear load resistor R_L (from 100 Ω to 1 GΩ). Take the second harmonic generation as an example, the PCE diagram in Fig. 3 demonstrates the PCE values at 2nd harmonic $P_{L,2}/P_S$ recorded from BFO memristive device in both LRS and HRS under sinusoidal sourcing voltage in dependence of load resistor R_L. Due to an application of large positive writing bias, fixed Ti donors close to the bottom electrode can effectively trap mobile oxygen vacancies in BFO thin film, thus the barrier height near to the bottom electrode becomes non-rectifying and BFO memristive device is in LRS. By applying the large negative writing bias, the mobile donors, i.e. oxygen vacancies, in BFO thin film are redistributed between the top and the bottom electrode. The barrier height near the bottom electrode becomes rectifying and the device is in HRS. It is noteworthy that the barrier height in Au top electrode region remains rectifying under both positive and negative writing biases. Due to the different functional behaviors of BFO memristive device in LRS (diode like behavior) and in HRS (high-ohmic behavior), the distinguishable sets of PCE diagrams can be recorded in both LRS and HRS, thus the input data '0' and '1' can be encoded and transmitted, respectively.

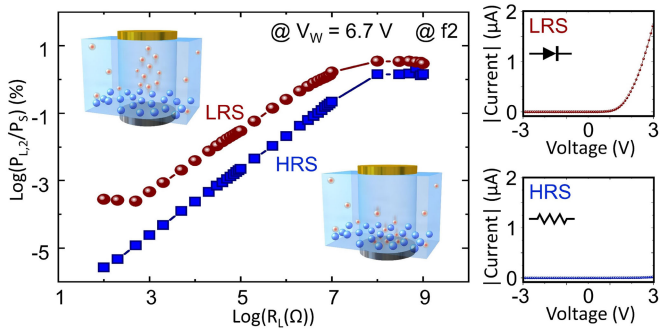


Fig. 3. Power conversion efficiency $P_{L,2}/P_s$ (PCE) curve of the BFO memristor between the average power at second harmonics and average source power under the sinusoidal sourcing voltage $V_S(t) = V_0 \sin(2\pi f_1 \cdot t)$ with $V_0 = 3$ V and $f_1 = 0.125$ Hz and prior to the PCE measurements, the memristor was initialized by writing voltages with pulse amplitude $V_W = 6.7$ V. With the positive writing bias $V_W = 6.7$ V, fixed Ti donors close to the bottom electrode can effectively trap mobile oxygen vacancies in BFO thin film, thus the barrier height near to the bottom electrode becomes non-rectifying and BFO memristor is set in LRS. By applying negative writing bias $V_W = -6.7$ V, the oxygen vacancies, in BFO thin film are redistributed between the top and the bottom electrode. The barrier height near the bottom electrode becomes rectifying and the device is set in HRS.

For the sake of the performance improvement of SoHP system, in this work the study on the PCE diagrams with BFO memristive devices in LRS or HRS in dependence on the sinusoidal sourcing voltage with various amplitudes V_0 is carried out, and their perspective influences on the SoHP system are analyzed. As demonstrated in Fig. 4(a), after the initialization process with pulse amplitude $V_W = 6.7$ V, the PCE value recorded in LRS at 2nd harmonic $P_{L,2}/P_S$ is significantly larger than that in HRS for the specific load resistor R_L (PCE values $\log(P_{L5,2}/P_S)$ in LRS and HRS are -1.51959 and -2.64771, respectively). This is because the BFO memristive device is functioning as a diode in LRS, and as a high-ohmic resistor in HRS. After the initialization process with pulse amplitude $|V_W| = 6.1$ V (Fig. 4(b)), the BFO memristive device is not fully switched to LRS or HRS, and it is predictable that the corresponding Off/On ratio will be smaller than that switched by writing bias $V_W = 6.7$ V. Thus, the hysteresis and nonlinearity of IV characteristics are depressed under initialization pulse amplitude $|V_W| = 6.1$ V, which results in the undistinguishable power ratios between LRS and HRS as shown in (Fig. 4(b)). Only the two clearly distinguishable sets of power ratio curves in LRS and HRS can be used for designing the hardware-oriented security primitives.

As next, the PCE diagrams recorded under various V_W are analyzed. As shown in Fig. 4(d), we exam the opening area between PCE curves in LRS and HRS by evaluating the minimal

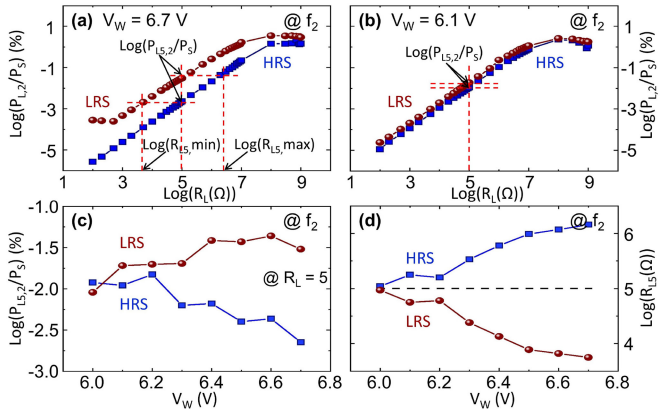


Fig. 4. Comparison of PCE curves of BFO memristive device in both LRS and HRS at 2nd harmonic under sinusoidal input voltage with amplitudes $V_0 = 3$ V and prior to the PCE measurements, the device was initialized by writing voltages with pulse amplitude (a) $V_W = 6.7$ V and (b) $V_W = 6.1$ V. (c) Interface PCE values $\log(P_{L5,2}/P_S)$ and (d) load resistor range for detecting LRS and HRS with $R_{L5,min} < R_L$ and $R_{L5,max} > R_L$ with $R_L = 100\ k\Omega$ at 2nd harmonic in dependence on sinusoidal input voltage.

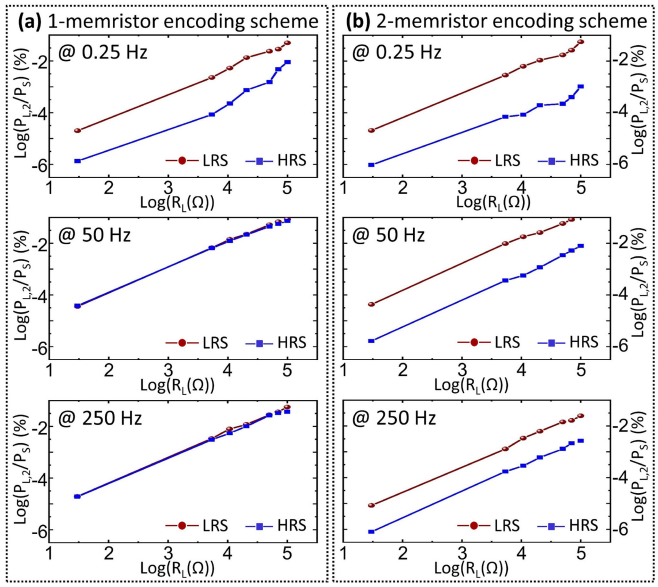


Fig. 5. Frequency dependent power conversion efficiency diagrams in (a) one-memristor encoding scheme and (b) two-memristor encoding scheme. The PCE curves in both LRS and HRS under sinusoidal input voltage with voltage bias of $V_0 = 3$ V and frequencies f = 0.25 Hz, 50 Hz, and 250 Hz are examined. The memristive devices were initialized by the writing bias with amplitude $|V_W| = 6.7$ V.

and maximal PCE values at $R_L = 100\ k\Omega$, i.e. $\log(P_{L5,min})$ and $\log(P_{L5,max})$, respectively. $\log(R_{L5})$ values, difference between $\log(P_{L5,max})$ and $\log(P_{L5,min})$, in LRS and HRS at $V_W = 6.0$ V are 4.97 and 5.04. The cross points between the load resistor at $\log(R_L) = 5$ and PCE curves at 2nd harmonic are defined as interface PCE values $\log(P_{L5,2}/P_S)$ in both LRS and HRS, respectively. The interface PCE values are analyzed in Fig. 4(c) in dependence on the pulse amplitudes of writing voltages V_W, i.e. the Off/On ratio in the corresponding resulted IV characteristics. With decreasing pulse amplitude V_W, the corresponding PCE values in LRS and HRS at 100 $K\Omega$ $\log(P_{L5,2}/P_S)$ converge at $V_W = 6.03$ V, which reveals decreased nonlinear dynamics in IV characteristics of memristive device. As illustrated in Fig. 4(a), the load resistor region used for encoding input data is defined between the minimum load resistor value in LRS $\log(R_{L5}$,min) and maximum load resistor value in HRS $\log(R_{L5}$,max). The minimum and maximum load resistor values $\log(R_{L5}$,min) and $\log(R_{L5}$,max) at 2nd harmonic in dependence on pulse amplitude of writing voltage V_W are derived from PCE diagrams and plotted in Fig. 4(d). With decreasing V_W, the opening area between $\log(R_{L5}$,min) and $\log(R_{L5}$,max), which is used for encoding input data, decreases. Thus the encoding system is theoretically no longer functioning if the pulse amplitude lower than $V_W = 6.03$ V according to the crossing point in Fig. 4(d).

In the SoHP system, the frequency of input sinusoidal voltage $V_S(t)$ is the key parameter which limits the encoding and decoding velocity. Thus the impact of the input sinusoidal voltage $V_S(t)$ is experimentally investigated for the SoHP-system. In Fig. 5(a) the frequency influence on 1-memristor encoding scheme is demonstrated. In 1-memristor encoding scheme, the load resistor R_L is connected in series with one single BFO memristive device, which is continuously switched between LRS and HRS according to the input data. We can see that at 0.25 Hz, the opening area between LRS and HRS PCE curves can be adopted in the SoHP system, but at 50 and 250 Hz, LRS and HRS PCE curves become indistinguishable, which can not be used anymore. Such phenomenon is caused by the intrinsic high frequeny switching property of memristive devices, i.e. the input voltage at high frequency eliminates the hysteresis characteristic of the memristive devices.

For the sake of high encrypting and decrypting efficiency, the 2-memristor encoding scheme is developed and the PCE diagrams are recorded as demonstrated in Fig. 5(b) under input sinusoidal voltage $V_S(t)$ with frequencies 0.25 Hz, 50 Hz, and 250 Hz, respectively. In the 2-memristor encoding scheme, the load resistor R_L was separately connected in series with two BFO memristive devices, which are permanently switched to LRS and HRS under pulse amplitude $V_W = 6.7$ V and -6.7 V, respectively. The average power ratio over load resistor was recorded under the sinusoidal testing input voltage $V_S(t) = V_0 \sin(2\pi f_1 \cdot t)$ with amplitude $V_0 = 3$ V at frequencies $f_1 = 0.25, 50$ and 250 Hz, which is insufficient to corrupt the well-defined LRS or HRS memristive states. The power ratio efficiency $P_{L,2}/P_S$ is then demonstrated in Fig. 5(b). In the 2-memristor encoding scheme, under the input voltage testing with amplitude 3 V, the LRS memristor remains rectifying and working as a diode device, whereas the HRS memristor functions as high resistive resistor (as shown in Fig. 3). Thus it is expectable that the distinguishable PCE curves can be recorded even at an elevated frequency, e.g. at 250 Hz, in Fig. 5(b). Therefore, the nonvolatile high uniform rectifying switching behavior of BFO memristor plays a role in generating distinguishable PCE curves over the memristor, which maintains the opening area between LRS and HRS PCE region under input sinusoidal voltage with high frequency. Thus the 2-memristor encoding scheme is adopted in the circuit design of the encoder in the SoHP system as demonstrated in Fig. 6(b).

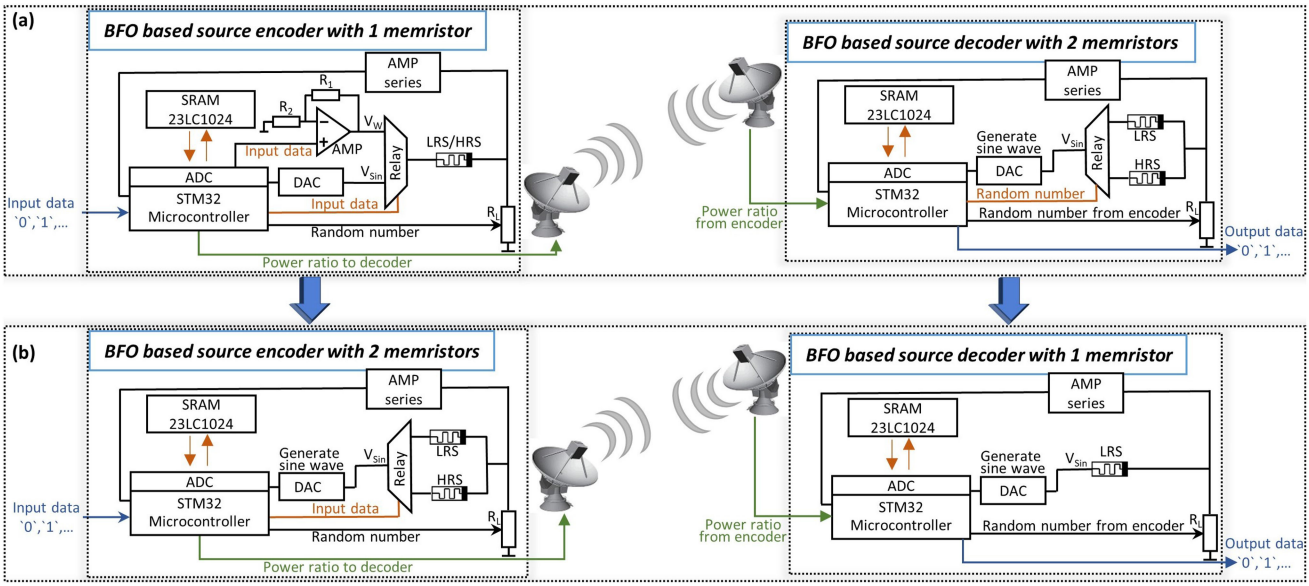


Fig. 6. Block diagrams of BFO memristor based SoHP systems: (a) The SoHP system with 1-memristor encoding scheme and 2-memristor decoding scheme requires one BFO memristor continues switchable between LRS and HRS during data encryption, and requires two BFO memristors with well-defined LRS and HRS in the decoder. (b) The improved SoHP system with 2-memristor encoding scheme and 1-memristor decoding scheme requires two BFO memristors with well-defined LRS and HRS in the encoder and one BFO memristor in LRS in the decoder which enables the higher frequency implementation of data encoding and decoding processes. Both encoders encrypt the input binary data into modulated data by measuring the power ratio $P_{L,2}/P_S$ (between the average source power and the 2nd harmonic power) on the memristor with ADC via an amplifier series. At the same time, a sinusoidal voltage generated by DAC as the excitation signal is applied on the corresponding memristive device, under the control of STM32 microcontroller.

III. BFO Memristor Based Security-Oriented Hardware System

With nonvolatile switching performance, the memristor was proposed to be applied to various fields: next generation nonvolatile resistive memories [30]–[32], neuromorphic system [33], [34], chaotic circuits [35], [36], and etc. In this work, we extend the application of memristor for higher harmonic generation to security-oriented applications.

The block diagrams for constructing BFO memristor based SoHP systems with 1-memristor encoding scheme and 2-memristor encoding scheme are illustrated in Fig. 6(a) and Fig. 6(b), respectively. The SoHP system with 1-memristor encoding scheme in Fig. 6(a) requires two BFO memristors with well-defined LRS and HRS in the decoder, whereas the SoHP system with 2-memristor encoding scheme in Fig. 6(b) requires one BFO memristors in LRS in the decoder, which enables the higher frequency implementation of data encoding and decoding.

The 1-memristor encoding scheme of SoHP system is advanced based on the system design in Ref. [25]. The BFO memristor in 1-memristor encoding should be continuously switched between LRS and HRS according to the input binary data '0' and '1', respectively. The encoding process is designed as follows: The input binary data are firstly stored in the embedded SRAM to coordinate the speed difference between the data reception and the data encoding. The single one BFO memristor is connected in series with load resistor R_L, resulting in a series M-R_L circuit. For the transmission of the input binary data '0' ('1'), the memristive device has to be correspondingly set to LRS (HRS) by applying writing voltage with pulse amplitude $V_W = +6.7$ V and $V_W = -6.7$ V to the top electrode of device via an amplifier. The sine wave source voltage $V_S(t)$ is activated by a MC controlled digital to analog converter (DAC), and applied to the M-R_L circuit for generating second and higher harmonics. The relay determines, based on the input binary data, whether the writing voltage V_W or the excitation sinusoidal voltage $V_S(t)$ is applied to the memristor: If the input binary data is '0' ('1'), the memristor is first set in LRS (HRS) by the writing voltage V_W, then switched memristor accesses excitation sinusoidal voltage $V_S(t)$ generated by DAC. The power at second harmonic $P_{L,2}$ over load resistor R_L is then extracted by an analog to digital converter (ADC) integrated inside STM32 MC with adopting an amplifier series and transformed into the frequency domain by FFT transformation. The encrypted power ratios at second harmonic $P_{L,2}/P_S$ are transmitted via an antenna to the BFO memrsitor based decoder. In the 1-memristor encoder scheme, the continuous switching process of BFO memristor between LRS and HRS is the bottleneck for the encoding velocity. For the sake of high encrypting efficiency in the SoHP system, the 2-memristor encoding scheme is proposed (Fig. 6(b)).

In the optimized 2-memristor encoding scheme, two BFO memristors are utilized, which are set to LRS and HRS respectively by applying writing voltage with pulse amplitude $V_W = +6.7$ V and $V_W = -6.7$ V to the top electrode of device, before transmission of the input data. Here the relay determines the selection between the memristors in LRS and HRS according to the DAC converted input binary data: If the input data is '0', the memristor in LRS accesses to the circuit, otherwise for '1', HRS memristor is selected. In this way, the second and higher harmonic signals are generated by utilizing pre-defined LRS or HRS memristor in series with load resistor R_L upon a sinusoidal voltage source $V_S(t)$. The flowchart in

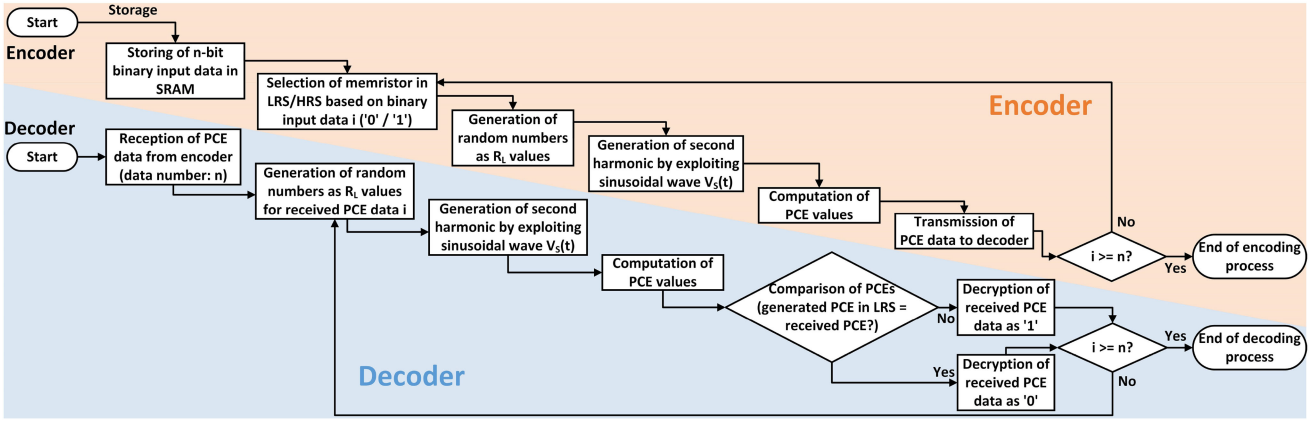


Fig. 7. Flowchart for depicting the encryption and decryption processes of n-bit input data of 2-memristor encoder scheme and 1-memristor decoder scheme in the SoHP-PCB system.

Fig. 7 (marked with orange background color) illustrates the aforementioned encryption process for the 2-memristor encoder scheme. In the encoding process of each bit of input data, the switching process of the BFO memristor is omitted, and the encoding time is not limited by the switching process of the BFO memristor anymore. The encoding time is extremely shortened in the optimized 2-memristor encoding scheme. Thus without the requirement of the memristive switching process, it highlights the potential of 2-memristor encoding scheme in terms of high efficiency encoding: the encoding frequency of SoHP system with 2-memristor encoding scheme can reach 1 kHz, which is 4000 times higher than 1-memristor encoding scheme. The 1 kHz encoding frequency of improved 2-memristor encoding scheme is further limited by the operation frequency of the analog circuitry STM32 MC, DAC and ADC. It is thus expectable with more advanced electronic components bring even higher frequency. Eventually, the encrypted power ratios at second harmonic $P_{L,2}/P_S$ in the encoder are transmitted from sender to the receiver via an antenna.

At receiver, the SoHP system with 2-memristor decoding scheme (Fig. 6(a)) [25] has been optimized and upgraded to 1-memristor decoding scheme (Fig. 6(b)). Instead of using two BFO memristive devices in 2-memristor decoding scheme, which are permanently set to LRS and HRS, respectively, the single one BFO memristor in LRS is utilized in 1-memristor decoding scheme. The 1-memristor decoding scheme simplifies the data decrypting process, while ensuring the functionality of the decoder. The same random sequence of load resistor values for R_L is generated simultaneously by the random number generator integrated inside STM32 MC. Thus the secondary power efficiency is computed according to the second harmonic signal generated from series combination circuit of LRS BFO memristor and load resistor R_L. By comparing the secondary power efficiency with the received one from encoder, the output binary data of the decoder is determined: '0' is transmitted, if the power efficiencies are equal to each other; otherwise, data '1' is transmitted. The aforementioned decryption process for 1-memristor decoding scheme is depicted in Fig. 7 (marked with blue background color). Without the selection process between LRS and HRS memristors realized by relay, the design of 1-memristor decoding scheme simplifies the functional structure of the decoding circuit, boosts the decrypting efficiency and shrinks the system cost in terms of power consumption and operation latency. The 2-memristor encoding scheme and the 1-memristor decoding scheme (Fig. 6(b)) are adopted in the final version of SoHP-PCB system, and its laboratory realization is demonstrated in Fig. 8.

The three-step optimization approaches for implementing the BFO memristor based security-oriented hardware primitive (SoHP) system is illustrated in Fig. 8, including SoHP system exploiting off-the-shelf devices (SoHP-OTSD) (Fig. 8(a)), SoHP system exploiting microcontroller (SoHP-MC) (Fig. 8(b)), and integrated SoHP system on PCB board (SoHP-PCB) (Fig. 8(c)). Each implementation of the SoHP system consists of the encoder and decoder schemes based on BFO memristors. The SoHP-OTSD implementation is based on the system block diagram Fig. 8(a)), where the combined design of a MC based hardware system controlled by LabVIEW software with the support from off-the-shelf Keithley 2400 source meter is adopted. In the MC based hardware system of SoHP-OTSD version, the memristive devices are connected with the load resistor in series as the basic circuit topology. The LabVIEW software is responsible for providing the excitation source signal via the Keithley 2400 source meter and extracting the power efficiency at second harmonic $P_{L,2}$ over load resistor, which is used for data encryption and decryption according to input binary data. Both SoHP-MC (Fig. 8(b)) and SoHP-PCB implementations (Fig. 8(c)) are sharing the same circuit topology, i.e. consisting of 2-memristor encoding and 1-memristor decoding schemes with higher operational speed. For the sake of higher integrality of the encryption system, the off-the-shelf devices (LabVIEW and Keithley 2400) from SoHP-OTSD implementation have been substituted by the STM32 microcontroller (MC) with required DAC, ADC and a couple of operational amplifiers in order to convert the measuring voltage range. The further SoHP-PCB implementation is integrated into a custom-made electronic PCB board with size of 80 $mm \times 68$ mm to bestow the SoHP system a higher level of integration and stability. In comparison to SoHP-OTSD, the optimized SoHP-MC and SoHP-PCB with 2-memristor encoding scheme and 1-memristor decoding scheme has improved the frequency from 0.25 Hz to 1 KHz, thus the encryption/decryption speed is increased

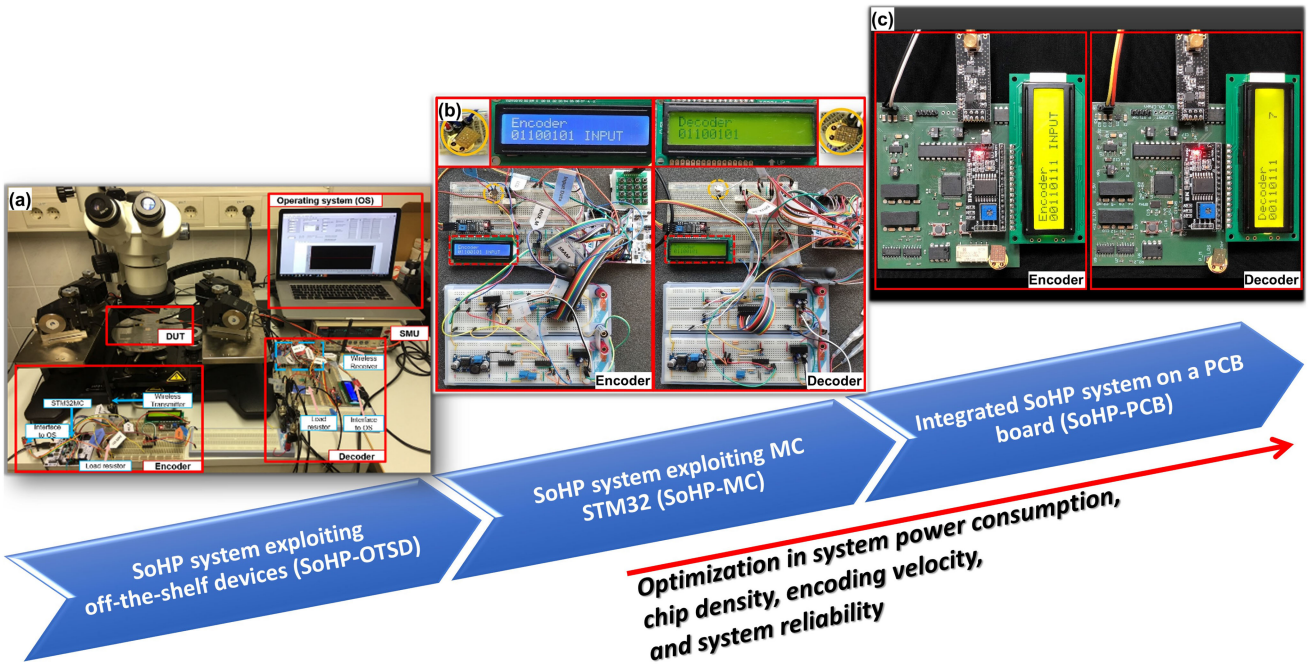


Fig. 8. Three-step optimization of system power consumption, chip density, encoding velocity, and system reliability for a BFO memristor based security-oriented hardware primitive (SoHP) system: (a) SoHP system exploiting off-the-shelf devices (SoHP-OTSD); (b) SoHP system exploiting microcontroller STM32 (SoHP-MC); (c) Integrated SoHP system on a PCB board (SoHP-PCB). The first version SoHP-OTSD adopts the combined design of a hardware system and a LabVIEW software system with the support from off-the-shelf Keithley 2400 source meter. For higher encryption/decryption speed and the integrability of the system, the off-the-shelf devices (LabVIEW and Keithley 2400) are substituted by the STM32 microcontroller and other electronic components, in the improved version SoHP-MC. The final version SoHP-PCB bestows the SoHP system a higher level of integration and stability.

by 4000 times. By omitting the switching process of the BFO memristor for each bit of input data in the encoding scheme and simplifying the decoding scheme, the power consumption of the SoHP system is substantially reduced. The video of encryption and decryption processes for optimized SoHP-PCB system is provided as supplementary material. The encrypted data are transferred from the encoder through a wireless transceiver to decoder. Note that, the further higher operational frequency than 1 KHz is possible, if the electrical peripheral circuits, i.e. MC, DAC and ADC with higher operating frequency are adopted.

Randomness is a probabilistic property and the properties of a random sequence can be characterized and described in terms of probability [37]. For a cryptographic algorithm or system, the randomness of its encrypted sequence is an important aspect of its security. For testing the security level of the SoHP system, a randomness test has been executed with the NIST SP-800.22 statistical test suite [38], which is one of the most reliable randomness test suit currently with 15 tests utilized for the evaluation of random number generator (RNG). Fig. 9 depicts the randomness test results for the hardware oriented SoHP-PCB security system with writing bias $V_W = 6.7$ V and sinusoidal frequency $f_1 = 0.125$ Hz at second harmonic. In the specific statistical test for randomness, 5.12×10^7 power ratio data transferred between the security system with the bit stream with the length of 5.12×10^5 are analyzed. According the NIST publication [38], the output of the statistical test called P-value represents the level of randomness: Data sequence with higher P-Value P (maximal 1) indicates higher level of randomness. Given the significance level $\alpha = 0.01$, a test is interpreted as

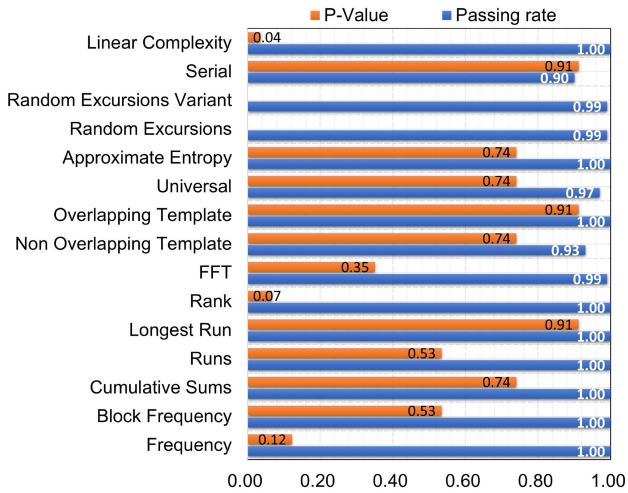


Fig. 9. Randomness test result of NIST SP800-22 for the hardware oriented security system. All 15 tests with P-Value ≥ 0.01 (significance level) pass the randomness test. The larger P-Value (maximal 1.00) of the PCE data sequence, which are recorded from the SoHP system, indicates the improved randomness. The passing rates (blue) are calculated by NIST test suite for 5.12×10^7 PCE data transferred between the hardware oriented security system with the bit stream of 5.12×10^5 bit length.

follows:

$$\begin{aligned} P &< \alpha \quad \text{the test is failed} \\ P &\geq \alpha \quad \text{the test is passed} \end{aligned} \tag{1}$$

All 15 tests with P-Value $P \geq 0.01$ (α) are considered passed. The passing rates (blue) are calculated by NIST test suite for

100 PCE data sequences as demonstrated in the Fig. 9. The test results provide evidences for the strong randomness of the encrypted data and for the extremely low possibility of the BFO memristor-based security system being cracked. Beside the higher security level, the flexible freedom parameters and the low power consumption performance grant the BFO memristor-based SoHP system a wide application potential in various fields. Moreover, for further randomness verification of the encrypted data, two more randomness tests have been conducted, i.e. the ENT (A Pseudorandom Number Sequence Test Program), which is an entropy estimator and the BSI's (German Federal Office for Information Security) statistical test suite, which puts an emphasis on forward/backward secrecy and other security properties. The extensive detailed results of the BSI suite and ENT random number sequence test are exhibited as supplementary materials. The encrypted data from BFO memristor based SoHP system have passed the NIST, ENT and BSI test suits.

IV. Summary and Outlook

In this work, the high efficient security-oriented hardware system by exploiting the emerging electroforming-free $BiFeO_3$ (BFO) based ultra-stable memristive devices has been developed. With the help of untra-stable switching behavior of BFO based memristive devices, the impact of writing voltage V_W on the switching dynamics and on the efficiency of second harmonic generation is revealed, i.e. the larger the V_W, the more distinguishable PCE curves in both LRS and HRS can be generated. In SoHP system, the PCE curves in LRS and HRS are used for encoding binary input data '1' and '0'. Based on the BFO memristor in LRS with diode-like behavior and in HRS with high resistive behavior, the SoHP-PCB system with 2-memristor encoding scheme is developed, and alleviates the issue of limited operating frequency caused by the unswitchable memristive dynamic behavior at elevated frequency. The operating frequency of SoHP system is thus improved by 4000 times (from 0.25 Hz to 1 kHz). Furthermore, the design of 1-memristor decoding scheme simplifies the functional structure of the decoding circuit, boosts the decrypting efficiency and shrinks the system cost in terms of power consumption and operation latency. The PCB implemented SoHP system has passed all 15 statistical randomness tests of NIST SP-800.22 test suite, which proves the random distribution of encrypted data and highlights its high security level.

A clear benefit of the proposed hardware security solution over software-based system lies in its insensitivity to malicious code and brute force attacks. It is also noteworthy that not only BFO memristive devices, but also other types of memristive devices with nonlinear analog switching behavior can be applied in the proposed SoHP system. The analysis of the energy efficiency of the designed system is highly dependent on the operational efficiency of the applied memristive devices. Compared to a logic-level EXOR cipher (implemented in hardware or software) followed by transmission of the ciphertexts, the BFO memristor-based SoHP system is an integrated solution that avoids overheads for synchronization and contains more freedom parameters, due to their influence on the PCE map, i.e. pulse amplitude of writing voltage V_W, maximum sine wave amplitude V_0 and harmonic k, which give the SoHP system degrees of freedom that are not available for the standard solution. Additionally, being a hardware encryption device, the SoHP system can be encapsulated to prevent tampering, whereas software or hardware implementations of the EXOR cipher can be prone to physical attacks (die-channel analysis and fault injections). For even higher frequency applications, the current SoHP system can be combined with a linear-feedback shift register, reaching a generation rate in the GHz range. The proposed memristor based SoHP system with high security level is suitable for communication encryption in the daily communication equipment, i.e. mobile phone and laptop, etc., as an embedded implant system.

References

[1] M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega-García, and J. Siguenza, "Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification," in *Proc. IEEE 40th Annu. Int. Carnahan Conf. Secur. Technol.*, 2006, pp. 151–159.

[2] M. Lindorfer, A. Di Federico, F. Maggi, P. M. Comparetti, and S. Zanero, "Lines of malicious code: Insights into the malicious software industry," in *Proc. 28th Annu. Comput. Secur. Appl. Conf.*, 2012, pp. 349–358.

[3] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018.

[4] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Serv.-Oriented Comput. Appl.*, 2014, pp. 230–234.

[5] G. S. Rose, N. McDonald, L.-K. Yan, and B. Wysocki, "A write-time based memristive PUF for hardware security applications," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Des.*, 2013, pp. 830–833.

[6] G. S. Rose, N. McDonald, L.-K. Yan, B. Wysocki, and K. Xu, "Foundations of Memristor Based PUF Architectures," in *Proc. IEEE/ACM Int. Symp. Nanoscale Architectures*, 2013, pp. 52–57.

[7] S. Kannan, N. Karimi, and O. Sinanoglu, "Secure memristor-based main memory," in *Proc. 51st ACM/EDAC/IEEE Des. Automat. Conf.*, 2014, pp. 1–6.

[8] J. Rajendran *et al.*, "Nano meets security: Exploring nanoelectronic devices for security applications," *Proc. IEEE*, vol. 103, no. 5, pp. 829–849, May 2015.

[9] A. S. Iyengar, S. Ghosh, and K. Ramclam, "Domain wall magnets for embedded memory and hardware security," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, vol. 5, no. 1, pp. 40–50, Mar. 2015.

[10] B. Duong, H. Liu, C. Li, W. Deng, L. Ma, and M. Su, "Printed multilayer microtaggants with phase change nanoparticles for enhanced labeling security," *ACS Appl. Mater. Interfaces*, vol. 6, no. 11, pp. 8909–8912, 2014.

[11] L. Zhang, Z. H. Kong, C.-H. Chang, A. Cabrini, and G. Torelli, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 6, pp. 921–932, Jun. 2014.

[12] Y. Bi, P.-E. Gaillardon, X. S. Hu, M. Niemier, J.-S. Yuan, and Y. Jin, "Leveraging emerging technology for hardware security-case study on silicon nanowire fets and graphene symfets," in *Proc. IEEE 23rd Asian Test Symp.*, 2014, pp. 342–347.

[13] R. R. Katti, J. L. Tucker, and A. Kohli, "Magnetoresistive random access memory (MRAM) package including a multilayer magnetic security structure," U.S. Patent 8,811,072, Aug. 19, 2014.

[14] C. Du, F. Cai, M. A. Zidan, W. Ma, S. H. Lee, and W. D. Lu, "Reservoir computing using dynamic memristors for temporal information processing," *Nature Commun.*, vol. 8, no. 1, pp. 1–10, 2017.

[15] C.-C. Hsieh, A. Roy, Y.-F. Chang, D. Shahrjerdi, and S. K. Banerjee, "A sub-1-volt analog metal oxide memristive-based synaptic device with large conductance change for energy-efficient spike-based computing systems," *Appl. Phys. Lett.*, vol. 109, no. 22, 2016, Art. no. 223501.

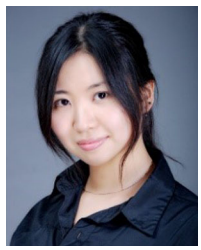
[16] N. Du *et al.*, "Single pairing spike-timing dependent plasticity in $BiFeO_3$ memristors with a time window of 25 ms to 125 μs," *Front. Neurosci.*, vol. 9, p. 227, 2015.

[17] T. You *et al.*, "Bipolar electric-field enhanced trapping and detrapping of mobile donors in $BiFeO_3$ memristors," *ACS Appl. Mater. Interfaces*, vol. 6, no. 22, pp. 19 758–19765, 2014.

[18] Y. Shuai *et al.*, "Coexistence of memristive and memcapacitive effects in oxide thin films," *Japanese J. Appl. Phys.*, vol. 57, no. 12, 2018, Art. no. 121502.

[19] N. Du *et al.*, "Field-driven hopping transport of oxygen vacancies in memristive oxide switches with interface-mediated resistive switching," *Phys. Rev. Appl.*, vol. 10, no. 5, 2018, Art. no. 0 54025.
[20] N. Du *et al.*, "Synaptic plasticity in memristive artificial synapses and their robustness against noisy inputs," *Front. Neurosci.*, vol. 15, p. 696, 2021.
[21] N. Du, H. Schmidt, and I. Polian, "Low-power emerging memristive designs towards secure hardware systems for applications in Internet of Things," *Nano Mater. Sci.*, vol. 3, no. 2, pp. 186–204, 2021.
[22] G. Indiveri, B. Linares-Barranco, R. Legenstein, G. Deligeorgis, and T. Prodromakis, "Integration of nanoscale memristor synapses in neuromorphic computing architectures," *Nanotechnology*, vol. 24, no. 38, 2013, Art. no. 384010.
[23] T. You *et al.*, "Exploiting memristive $BiFeO_3$ bilayer structures for compact sequential logics," *Adv. Funct. Mater.*, vol. 24, no. 22, pp. 3357–3365, 2014.
[24] Y. Zhou, Y. Li, L. Xu, S. Zhong, H. Sun, and X. Miao, "16 Boolean logics in three steps with two anti-serially connected memristors," *Appl. Phys. Lett.*, vol. 106, no. 23, 2015, Art. no. 233502.
[25] N. Du *et al.*, "Novel implementation of memristive systems for data encryption and obfuscation," *J. Appl. Phys.*, vol. 115, no. 12, 2014, Art. no. 124501.
[26] L. Jin *et al.*, "Resistive switching in unstructured, polycrystalline BiFeO3 thin films with downscaled electrodes," *Physica Status Solidi (A)*, vol. 211, no. 11, pp. 2563–2568, 2014.
[27] X. Yan *et al.*, "Self-assembled networked PbS distribution quantum dots for resistive switching and artificial synapse performance boost of memristors," *Adv. Mater.*, vol. 31, no. 7, 2019, Art. no. 1805284.
[28] D. Kim *et al.*, "Retention of resistance states in ferroelectric tunnel memristors," *Appl. Phys. Lett.*, vol. 103, no. 14, 2013, Art. no. 142908.
[29] S. Kumar *et al.*, "Oxygen migration during resistance switching and failure of hafnium oxide memristors," *Appl. Phys. Lett.*, vol. 110, no. 10, 2017, Art. no. 103503.
[30] D.-H. Kwon *et al.*, "Atomic structure of conducting nanofilaments in TiO_2 resistive switching memory," *Nature Nanotechnol.*, vol. 5, no. 2, pp. 148–153, 2010.
[31] R. Waser and M. Aono, "Nanoionics-based resistive switching memories" in *Nanoscience and Technology: A Collection of Reviews from Nature Journals*. Singapore: World Scientific, 2010, pp. 158–165.
[32] Y. V. Pershin and M. Di Ventra, "Memory effects in complex materials and nanoscale systems,"*Adv. Phys.*, vol. 60, no. 2, pp. 145–227, 2011.
[33] M. D. Pickett, G. Medeiros-Ribeiro, and R. S. Williams, "A scalable neuristor built with mott memristors," *Nat. Mater.*, vol. 12, no. 2, pp. 114–117, 2013.
[34] A. Wu, Z. Zeng, X. Zhu, and J. Zhang, "Exponential synchronization of memristor-based recurrent neural networks with time delays," *Neurocomputing*, vol. 74, no. 17, pp. 3043–3050, 2011.
[35] S. Kumar, J. P. Strachan, and R. S. Williams, "Chaotic dynamics in nanoscale NbO_2 Mott memristors for analogue computing," *Nature*, vol. 548, no. 7667, pp. 318–321, 2017.
[36] Z. Qi-Shui, Y. Yong-Bin, and Y. Jue-Bang, "Fuzzy modeling and impulsive control of a memristor-based chaotic system," *Chin. Phys. Lett.*, vol. 27, no. 2, 2010, Art. no. 0 20501.
[37] U. Hahn and P. A. Warren, "Perceptions of randomness: Why three heads are better than four," *Psychol. Rev.*, vol. 116, no. 2, p. 454, 2009.
[38] R. Andrew and S. Juan, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol. NIST, 2010.

Ziang Chen received the bachelor's degree in microelectronics manufacturing engineering from the Guilin University of Electronic Technology, Guilin, China, in 2004, and the M.S. degree in microsystems and microelectronics from the Technical University of Chemnitz, Chemnitz, Germany, in 2019. He is currently working toward the Ph.D. degree with the Center for Microtechnologies, Technical University of Chemnitz. His research interests include memristive devices, digital and analog electronic circuit design using the memristors and transistors, and development of Advanced-Encryption-Standard (AES) security system exploiting resistive switching devices.



Nan Du received the Diploma degree in electrical engineering from the Faculty of Electrical Engineering and Information Technology, Technical University of Dresden, Dresden, Germany, in 2011, and the Ph.D. degree in electrical engineering from the Technical University of Chemnitz, Chemnitz, Germany, in 2016.

Since 2008, she has been a Member of the Scientific Staff of Prof. Dr. Heidemarie Schmidt. Between 2017 and 2019, she was a Postdoc with Fraunhofer ENAS, Chemnitz, Germany. In October 2019, she became a Group Leader for Research Group 'MemDevice, Friedrich-Schiller-Universität Jena, Jena, Germany, and with Fraunhofer ENAS. She is the Corresponding Author or Co-Author of more than 30 publications and 12 inventions (information from depatisnet.dpma.de). Her research interests include development of innovative security-oriented primitives and unconventional computing systems exploiting resistive switching devices, such as, brain-inspired neuromorphic computing, in-memory computing, and probabilistic computing. Since 2020, has been a Member of Coordination Board of Priority Program NanoSecurity in Deutsch Forschungsgemeinschaft.

Mahdi Kiani received the B.S. degree in electrical engineering from Shiraz University, Shiraz, Iran, in 2012, and the M.S. degree in micro and nano systems in 2016, from the Technical University of Chemnitz, Chemnitz, Germany, where he is currently working toward the Ph.D. degree. His research interests include the development of digital and analog electronic circuits using the memristors and transistors.

Xianyue Zhao received the B.S. degree in electrotechnical science and technology from Yanshan University, Qinhuangdao, China, in 2013, and the M.S. degree in microelectronics from the Chemnitz University of Technology, Chemnitz, Germany, in 2019. He is currently working toward the Ph.D. degree in nanosemiconductor with the Center for Microtechnologies (ZfM), Chemnitz University of Technology, Chemnitz, Germany. From 2019 to 2020, he was a Research Assistant with the Institute of ZfM, Chemnitz, Germany. His research interests include characterization of wafer-level memristive components and circuit design for analog memristor-based hardware security.

Ilona Skorupa has successfully passed the apprenticeship as a Physics Laboratory Assistant in 1978, with the ZfK Rossendorf. In 1985, she became an Engineer for materials technology and materials science in distance learning. She is currently a Laboratory Engineer with Helmholtz-Zentrum Dresden-Rossendorf, Dresden, Germany, and a Fabricating Memristive BFO with pulsed laser deposition.

Stefan E. Schulz studied microelectronics and received the Doctoraal degree in the field of interconnect systems from the Chemnitz University of Technology, Chemnitz, Germany, in 1996. Until 2008, he was a Scientific Assistant, later as a Senior Engineer with the Center for Microtechnologies,Technische Universität (TU) Chemnitz, Chemnitz, Germany. From 2003 to 2008, he was the Expert in micro- and nanoelectronics with the former Chemnitz Department of Fraunhofer IZM, today's Fraunhofer ENAS. He is currently the Deputy Director with the Institute and the Head of the Nano Device Technologies Department, Fraunhofer ENAS. Since November 2008, he has been appointed as Honorary Professor of "Nanoelectronics Technologies" with the Faculty of Electrical Engineering and Information Technology, TU Chemnitz, and has been involved in the training of junior scientists.

Danilo Bürger received the Diploma degree in physics from the Technical University of Dresden, Dresden, Germany, in 2008, and the Doctoral degree in 2012 from the Technical University of Dresden in scientific collaboration with the Helmholtz-Zentrum Dresden-Rossendorf. Since 2007, he has been a Member of the Scientific Staff of Prof. Dr. Heidemarie Schmidt. Between 2013 and 2016, he was a Postdoc on explosive crystallization phenomena in Ge:Mn with the Technical University of Chemnitz, Chemnitz, Germany. Since 2017, he has been using his expertise about deposition technologies for preparing memristive devices based on the material system $BiFeO_3$ with Fraunhofer ENAS in Chemnitz.

Massimiliano Di Ventra (Member, IEEE) received the undergraduate degree in physics (*summa cum laude*) from the University of Trieste, Trieste, Italy, in 1991 and the Ph.D. degree from the Swiss Federal Institute of Technology in Lausanne, Lausanne, Switzerland, in 1997. He is currently a Professor of physics with the University of California, San Diego, San Diego, CA, USA. He was invited to deliver more than 300 talks worldwide, including 15 plenary/keynote presentations. He has authored or coauthored more than 200 papers in refereed journals (he was named 2018 Highly Cited Researcher by Clarivate Analytics), has four granted patents, co-edited the textbook *Introduction to Nanoscale Science and Technology* (Springer, 2004) for undergraduate students, he is the single author of the graduate-level textbook *Electrical Transport in Nanoscale Systems* (Cambridge University Press, 2008), and of the trade book *The Scientific Method: Reflections from a Practitioner* (Oxford University Press, 2018). His research interests include condensed-matter theory and unconventional computing. He is the Co-Founder of MemComputing, Inc.

Ilia Polian (Senior Member, IEEE) received the Diploma (M.Sc.) and Ph.D. degrees from the University of Freiburg, Breisgau, Germany, in 1999 and 2003, respectively. He is currently a Full Professor and the Director of the Institute for Computer Architecture and Computer Engineering with the University of Stuttgart, Stuttgart, Germany. He has coauthored more than 200 scientific publications. His scientific interests include hardware-oriented security, emerging architectures, test methods, and quantum computing. He was the recipient of two best paper awards.

Heidemarie Schmidt studied physics from the Technical University Leipzig, Leipzig, Germany, where she graduated in 1999 with a dissertation on band structures in ultrathin semiconductors. At the Institute for Experimental Physics II, University of Leipzig, Leipzig, Germany, she headed the BMBF Junior Research Group Nano-Spintronics from 2003 to 2007. Since 2007, she has been established as Junior Research Group of the same name with the Institute for Ion Beam Physics and Materials Research, Helmholtz Center Dresden-Rossendorf. In 2012, she received the Heisenberg Scholarship from the Deutsche Forschungsgemeinschaft (DFG) and started to work on electroforming-free hardware materials for AI, namely $BiFeO_3$ and $YMnO_3$, Faculty of Electrical Engineering and Information Technology, Chemnitz University of Technology. Since 2016, she and her BFO4ICT-ATTRACT Group develop the technology for an industrial production of BFO memristors with Fraunhofer Institute ENAS, Chemnitz, Germany. In September 2017, she became a Professor with focus on quantum detection with the Institute of Solid State Physics, Friedrich Schiller University Jena Jena, Germany, and took over the management of the Quantum Detection Department, Leibniz Institute for Photonic Technology, Jena, Germany.