Exploiting Memristive Crossbar Memories as Dual-Use Security Primitives in IoT Devices

Garrett S. Rose, Md. Badruddoja Majumder, and Mesbah Uddin

IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Bochum, Germany, July 2017.

Citation Information (BibTex):

```
@INPROCEEDINGS{RoseISVLSI:2017,
  author="Garrett S. Rose and Md. Badruddoja Majumder and
      Mesbah Uddin",
  title="Exploiting Memristive Crossbar Memories as Dual-Use
      Security Primitives in IoT Devices",
  booktitle="Proceedings of {IEEE} Computer Society Annual
      Symposium on {ISVLSI}"
  month="July",
  year="2017",
  address="Bochum, Germany"
}
```

Exploiting Memristive Crossbar Memories as Dual-Use Security Primitives in IoT Devices

Garrett S. Rose, Md. Badruddoja Majumder, and Mesbah Uddin
Department of Electrical Engineering and Computer Science
University of Tennessee, Knoxville
Knoxville, Tennessee 37996-2250
Email: {garose, majumde, muddin}@utk.edu

***Abstract*—As the internet-of-things (IoT) paradigm emerges, digital system designers are pressed with ever challenging design requirements necessitating smaller, more energy efficient systems. Such requirements for lightweight IoT devices apply first and foremost to the primary functionality of the devices themselves. However, as IoT devices and systems become more prevelant in society, designers also must include strong security measures within a very limited area and power budget. Thus, approaches to lightweight security primitives are needed to address challenges such as reliable device authentication, side-channel analysis, and memory integrity, to name a few. In this paper, we consider nanoelectronic circuit designs that provide robust security with minimal area and power overhead. We focus specifically on memristor based circuits that offer reasonable levels of security with low energy and area overhead. For example, memristive crossbars are attractive in and of themselves as candidates for dense on-chip non-volatile memory in IoT devices. We show how such memristive crossbar structures can be leveraged in the implementation of (1) crossbar-based physical unclonable functions (PUF) useful for authentication and (2) sneak path integrity checking for data stored in the memory itself. These functions also demonstrate the potential dual-use nature of memristive crossbar structures (e.g. use as a memory and as a PUF). Early analysis of the nanoelectronic security primitives considered suggest very low power operation with minimal area footprint, making these solutions reasonable candidates for providing security and a hardware root of trust in emerging IoT devices.**

I. Introduction

The emerging "internet of things" (IoT) paradigm leads to new opportunities that can help improve overall quality of life. This improvement comes in part as the "things" in IoT are increasingly being interconnected to provide increased connectivity as part of an ever-swelling IoT system (see Fig. 1). This connectivity enables many functions in everyday personal devices such as smart phones and smart watches. Furthermore, very simple embedded sensor systems are being developed that necessitate the use of persistent, non-volatile memory that can survive across recharge cycles. Such systems have proven to be useful for applications ranging from agriculture to medicine [1]. From a security perspective, non-volatile memory poses several security challenges, many relating to the possibility of information leakage or malicious memory modification. However, emerging non-volatile memory provides important power and performance benefits that must be balanced against security needs in the implementation of secure IoT systems.

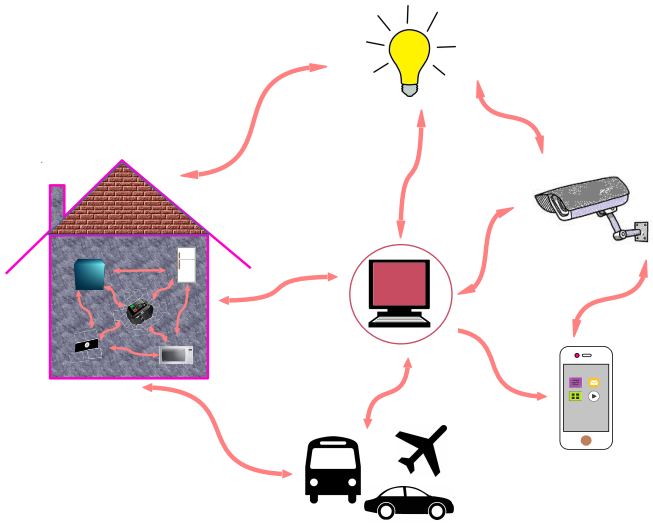

Fig. 1. The Internet of Things (IoT)

IoT devices are small, battery powered or even "batteryless" devices. For a batteryless IoT system, a temporary storage device (e.g. supercapacitor) is recharged via sources available, such as solar, wind, or vibration. The basic idea is the IoT function is simple so power is only needed in small bursts. However, some functions may require programming that survives recharge cycles in the sense that system state is maintained such that the program can pick up once a new charge is available. Thus, persistent, non-volatile memory is required to maintain system state and other important data used during computation. From a performance perspective, a major challenge is the power required for such non-volatile memory. The solution suggested here for these IoT device applications is the use of memristor-based crossbar memories that utilize little area and consume very little power.

The term memristor, a concatenation of "memory resistor", is used broadly in this work to refer to any hysteretic resistive switching device with memory. Many memristors considered in the literature are based on transition metal-oxides and are primarily considered for the implementation of resistive RAM (RRAM or ReRAM) [2]. For example, in past work our group and others have considered the use of TiO_2, HfO_2,

and other metal-oxide materials for the implementation of such memory systems. Given the advantages in terms of non-volatility, device density and low-power, memristor based memory technologies are very well suited for IoT systems. This is especially true for batteryless IoT.

Several memristor related security primitives have been considered in recent years, many of which are implemented using crossbar array structures similar to what is required for memory. Memristors have often be considered for the implementation of physical unclonable function (PUF) architectures. In [3] we introduced a simple PUF concept that leverages the entropy generated from variable memristor switching times. This concept was later verified experimentally by Mazady *et al.* [4]. The basic idea behind the simple write-time based memristive PUF was later expanded into a memristive crossbar PUF (XbarPUF) [5]. Kavehei *et al.* also presented a combination of RRAM structures and ring oscillators used to implement mrPUF[6]. Several other works have also focused on the security benefits of memristor-based PUF architectures [7], [8], [9], [10], [11], [12], [13].

Another security primitive important for IoT, especially batteryless systems requiring frequent recharge cycles, is memory integrity checking. In recent work, we've considered a memristor-based approach that leverages the data dependency of sneak path currents in memristive crossbar memory systems [14]. In prior work, related lightweight CMOS-based methods for integrity checking methods have been explored [15], [16]. However, even though such sytems are lightweight in terms of power and area, fitting them into resource constrained IoT devices remains a challenge. Thus, the memristor based integrity checking method is promising in this regard due to significantly low overhead in terms of area, power and delay [14]. This sneak path based integrity checking technique also uses the memristive memory array itself to compute the tags, providing a dual-use feature (memory and security) for these systems.

The remainder of this paper is organized as follows. In section II we provide background discussion on the IoT systems considered and memristor-based memory. Section III provides greater detail regarding expected security vulnerabilities in IoT systems requiring persistent memory. Sections IV and V provide details for dual-use memristive security primitives for integrity checking and authentication, respectively. Finally, concluding remarks are provided in section VI.

II. Background

A. IoT Systems & Devices

IoT broadly defines the networks of embedded computer systems, often including networking systems, processors, actuators, and sensors. The "things" in IoT are usually everyday devices and components that do not typically include compute capabilities, let alone networking capabilities. Examples include supply chain management systems, health monitors and agricultural management systems. Major challenges as IoT continues to grow are very large network loads (trillions of interconnected devices) and low power requirements during operation.

Being embedded systems, IoT devices are vulnerable to several potential security threats, including counterfeiting, tampering, power analysis attacks, and malicious memory modifications. Many of these threats are applicable because IoT systems exist "in the field" where authorized users might see limited physical access while the systems remain exposed to unauthorized tampering. As one example, infrastructure monitoring systems for some civil engineering tasks often include very few security safe guards. The reason security features are often lacking in these types of IoT devices is the need to design with limited resources (size, weight, area and power). Thus, sound approaches to design for IoT devices are required that provide sufficiently strong security with small area and very low power consumption.

TABLE I
Memristor Device Parameter Values Considered

Properties	VO_2 Nanowire [17]	Chalcogenide [18], [19]	Desired
Switching Time (s)	~ 0.25 m	~ 10 m	~ 100 p [20]
Threshold Voltage (V)	$\sim$1	$\sim 0.24(-0.32)$	$\sim 0.24(-0.32$)
Lowest resistance (Ω)	$\sim 10^7$	$\sim 10^4$	$\sim 10^5$
Highest Resistance (Ω)	$\sim 10^{11}$ - 10^{12}	$\sim 10^7$	$\sim 10^8$
Filament Formation	N/A	not required	not required

B. Memristor-based Persistent Memory

Several two-terminal memristive switching device technologies have emerged in recent years that can be leveraged for IoT applications. Many of these devices are based on transition metal-oxide (TMO) materials, such as TiO_2, TaO_2, and HfO_2. Other interesting material families that could be leveraged for IoT include magnetic tunnel junctions, chalcogenides, and hybrid ferroelectrics. For IoT, low-power operation is particularly important such that reliable operation (e.g. resistance switching) should be possible for relatively low supply voltages. Put another way, it is desirable that the threshold voltages be as small as possible. Other important device parameters include: persistence (non-volatility), fast switching times, relatively high resistance levels, and memristive behavior without the need for filament formation. Table I summarizes important memristor device properties, including desired behavior and published properties for existing experimental devices.

Two memristor types that would seem to work well for IoT are chalcogenides [21] and VO_2 [17] based devices. One important feature of both of these materials is the lack of a formation step. This formation step is common for TMO materials where a high voltage (3 V or more) must be applied to form the device and set the stage for memristor switching. Not having formation for chalcogenides and VO_2 means the voltage supply (and thus power) could be maintained at a low value. Forming also requires additional circuitry that

may degrade performance by introducing additional delay and power dissipation.

Since memristors have at least two stable and reachable resistance states these states can be interpreted as two logic levels and can thus act as a memory element (resistive RAM or ReRAM or RRAM). The high resistance state (HRS) can be considered logic '0' and low resistance state (LRS) can be considered as logic '1'. High separation between HRS and LRS offers higher noise margin between the two logic levels. There are many advantages of memristors as memory elements over traditional memory technologies. Memristors are non-volatile with high retention time meaning they can retain their resistance states even when the power supply is turned off, unlike the case where continuous power is needed for refresh cycles in DRAM. Memristors can be very small in size and thus can offer the build-up of a ultra-high density memory, denser even than DRAM. The switching rates of a memristor could potentially be very fast for some materials and thus memory read/write operation of a RRAM would be faster than existing memory technology. Moreover, many memristos exhibit more than two stable resistance states and thus can lead to more dense and faster multilevel memory technology [22].

III. Expected Security Vulnerabilities of Non-Volatile IoT Memory

IoT devices are often powered from a battery. Batteryless schemes have also been proposed in recent works [1]. Such schemes primarily depend on energy harvested from different sources such as solar cells, piezoelectric generators, vibration, and/or thermoelectric generators [23]. These sources of energy do not exhibit constant discharge-recharge cycles. Rather, they largely depend on environmental conditions that are always fluctuating. Thus, the IoT device relying on such a power supply must have the ability to stop and start through the duration of any computation. Thus, non-volatile memory is required for batteryless IoT devices such that the system state can be held persistently over different discharging and recharging cycles of the power supply.

Any non-volatile memory is vulnerable to a variety of different attacks. Adversaries can simply disconnect the device during a recharge cycle of the power supply and either read or manipulate memory content using energy from another power supply. The manipulated data in the memory often causes the application running on the embedded processor in the IoT devices to perform malicious functionality. Therefore, integrity checking of data stored in the memory of an IoT device is an essential security requirement.

Adversaries may also replace the original device with a counterfeit device. The counterfeit device may contain hardware Trojans which can cause malicious functioning of the device. Malicious activity may violate fundamental security properties of the system such as confidentiality, integrity and availability of the system. Therefore, every device in the IoT system should be authenticated against its hardware signature scheme, potentially using a physical unclonable function (PUF).

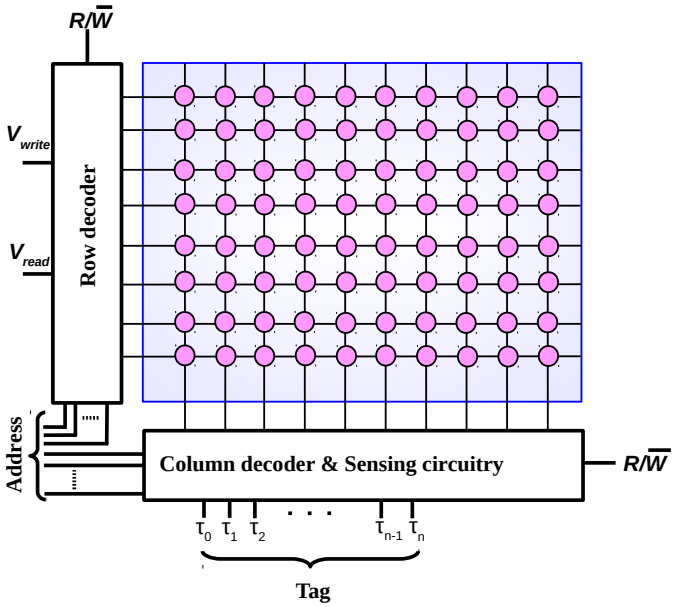

Fig. 2. Memristive crossbar memory enabling tag generation using sneak path currents for integrity checking purposes.

IV. Dual-Use Integrity Checking

A. Memristor-based Integrity Checking

The memristive crossbar is a well known nanoelectronic architecture which has already shown its great promise for high density non-volatile memory. Sneak path currents in memristive crossbar memory has been an intriguing topic for nanoelectronics researchers. The term "sneak path" refers to the current leakage through unselected memory cells along with the selected one in crossbar memory. Primarily it is identified as a deterrent for memory performance as sneak path currents affect the reliability of the read and write process of the memory. However, there are different modified versions of the crossbar architecture such as $1D1M$, $1T1M$ which mitigate sneak path problems by using a selector device [24]. The selector device minimizes the current leakage through unselected memory cells.

Interestingly, researchers have also found applications where sneak path currents can be leveraged for different memory based security applications. Majumder *et. al.* proposed a sneak path based memory integrity checking protocol where the data dependency of sneak path currents are used to generate authenticating tags for memory data. Since such sneak path based integrity checking has been presented as more lightweight than most of existing methods. Thus, the technique can be thought as an aggressive candidate for integrity checking in IoT systems and devices. The idea of integrity checking with sneak path currents in memristive crossbars is that the output current read from a crossbar memory while sneak paths

are enabled is dependent on the memristive states of every memristor in the crossbar and hence reflect the overall state of the memory. If the memory is overwritten, the new tag would be different from the previous one. Thus, every state of the memory can be represented with a tag generated using sneak path currents from multiple columns of the crossbar. Every time the integrity of memory data needs to be verified, tags are regenerated and compared with the reference tag. Fig. 2 illustrates the sneak path based tag generation method.

Device researchers have been proposing a variety of materials for making the memristive devices faster, more compact and energy efficient. Since IoT devices require extremely low power, low area and faster operation, Such exploration in memristor devices is bringing newer opportunities for them. Lower switching threshold voltage, faster switching operation, high value of low and high resistance state while maintaining a larger on/off ratio are some of the desirable properties that would perfectly fit memristor devices (e.g. memristive crossbar) in building IoT hardwares. IoT devices often cannot afford strong security protection due to limited resources but it is crucial that trust and reliability IoT applications be verified. While, no single memristive device has proven to be sufficient for all desired parameters, some materials are close. Here, a hypothetical memristive devices with desirable properties is listed in Table I to show the potential for memristive crossbar memory for multi-use applications in IoT devices. We present the comparison between sneak path based integrity checking method described in [14] and the same approach simulated with a hypothetical memristor device having properties fitting the low resource criteria of IoT devices. For the comparison we consider the same structure of crossbar memory presented in [14].

Table II shows the overhead of sneak path enabled tag generation method by considering the memristive device parameters mentioned in [14] and those provided in table I under the column of "desired" device properties. The predicted improvements are inferable from the scaled values of device parameters considered assuming applications for IoT devices and systems. Improvement in energy consumption results from threshold voltage reduction by almost half and switching time by one hundredth from the similar device parameters considered in [14]. Since the overhead of the peripheral circuitry does not scale down proportionately, the energy consumption value is not proportionate with the corresponding device parameters scaling. Delay is measured in terms of required number of clock cycles and clock frequency while clock frequency is chosen according to the switching time.

TABLE II
INTEGRITY CHECKING OVERHEAD COMPARISONS

Overhead	Majumder *et al.* [14]	Desired Device
Energy (pJ)	53.66	1.60
Delay (ns)	40.00	0.40

B. Checking for Batteryless IoT Devices

The integrity of data stored in the memory is one of the fundamental properties of a secure system. We have pointed out some of the security vulnerabilities of an IoT system, especially for batteryless systems that harvest energy from different environmental sources. Memristive crossbars being non-volatile memory devices are more vulnerable to unauthorized modification when powered off. This happens because the memory devices can simply be powered from another source and the contents be modified bypassing all security protection. Thus, it is important that for every cycle where the supply voltage is about to go below a certain predefined threshold level a tag is generated from the present memory state. Again when the power supply is recharged from the energy harvesting mechanism and the system is ready to function, the tag is regenerated from the memory data and compared with what was saved immediately before the device was nearly out of energy. If the tags do not match, an unauthorized modification in the memory data is likely and should be addressed immediately before any possible damage to the system.

In this paper, we do not consider any run time memory manipulation attack which occurs during the power supply of IoT devices are above the charging threshold voltage. Considering the higher chances of attack during the dead period (i.e below charging threshold) of power supply, we can reasonably assume that integrity checking is sufficient immediately after every recharge of the power supply.

V. PUF-BASED AUTHENTICATION

A. The Memristive Crossbar PUF

As an alternative to CMOS based physical unclonable functions, memristor based PUFs have been gaining attention for the past few years due to their very low size, low switching energy and fast switching rates of memristors. The memristor based crossbar PUF or the XbarPUF was first presented by Rose *et al* in 2015 [5]. The crossbar architecture offers a very dense array with memristors located at each of the cross-points. The XbarPUF is functionally a re-imagining of the arbiter PUF [25] in the sense that memristors are used in place of delay switch boxes of arbiter PUF. Binary memristors have primarily two stable resistive states which can be reached by applying set/reset voltages across them. Variations of threshold voltages, switching times and resistive states exist among different memristors which may give rise to differences in the overall resistances detected by read/write circuitries. A functional illustration of a XbarPUF is shown in Fig. 3.

The XbarPUF has three primary operational phases. First, all the memristors of a column are RESET using a high negative voltage pulse to ensure that all the memristors reach their high resistance or OFF state (HRS). Then, during the PUF's CHALLENGE phase, a positive voltage pulse is applied across each row to switch the memristors to low resistance or OFF state (LRS). The current through the memristors are measured at the end of each column. Due to process variations, not all memristors switch at the same time. Whenever, all the memristors of a column reach to their OFF states faster than

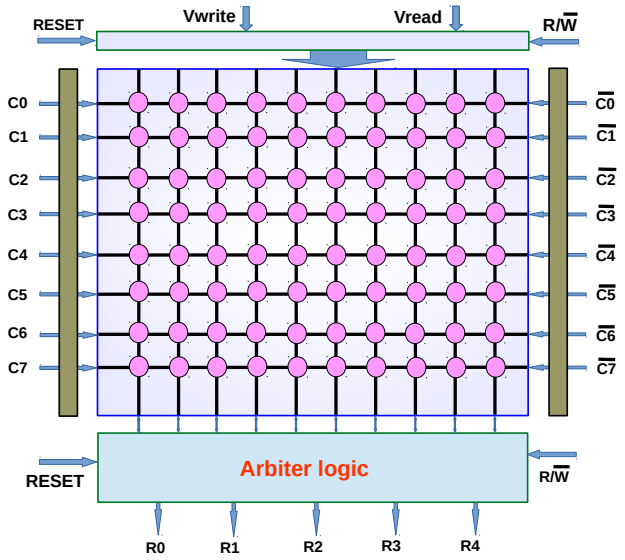

Fig. 3. Conceptual schematic of a 8×5 (in terms of no. of challenge-response bits) memristive crossbar PUF.

memristors of its adjacent column, CHALLENGE is stopped. During the last or READ phase, a small voltage, which wouldn't alter the memristors' current resistance, is applied. A load resistance is connected in series at the end of each crossbar column. Whichever column's memristors are faster in switching than its adjacent column, would have relatively higher voltage drop at the load. Thus that column would be faster in reaching high logic or '1'. An arbiter, which may be a flip-flop or a latch, is connected with both the columns to determine whichever is faster. These three phases constitute one challenge-response collection stage. Afterwards, a different challenge could be applied to collect a new response.

Since memristors are very small in size and the crossbar architecture offers a very dense implementation, the XbarPUF offers much smaller area requirement than other traditional PUFs as shown in [5]. By using appropriate memristors, the power dissipation could be very low too [13]. Besides, memristors such as TiO_x memristors offer switching rates on the order of tens of picoseconds [20] and thus memristor PUF can offer real-time security as well. Any PUFs could be vulnerable to machine learning based modeling attacks too. The basic XbarPUF could be modified further by including XORing [12], column shuffling and thus can provide a strong resiliency against those modeling attacks as analyzed in [13].

B. IoT Device Authentication

Device authentication is an important step for emerging IoT devices to avoid, among other things, spoofing attacks where an attacker may pretend to be an authentic IoT device and provide invalid or even dangerous results to a base server. PUF based authentication makes use of the challenge-response pairs to generate unique "fingerprints" for an integrated circuit [26]. When a device needs to be authenticated, the user presents a set of challenges for which the expected responses have been determined during an earlier enrollment phase. Assuming the challenge-response space is relatively large, which challenges are actually used make up a secret that should be hard for the attacker to uncover. Once the challenges are applied, the device issues the corresponding response which is then compared against the known response determined during enrollment. If the responses match, the device can be said to be authenticated [26].

In the context of IoT device authentication using a memristor based PUF, the protocol is much the same as for any CMOS based PUF. Since the memristor based PUF considered is constructed from a crossbar array, it is possible that the same structure used for main system memory (including integrity checking) can also be used for authentication. This would extend the dual-use nature of the memristive memory to a triple-use scenario where the memristive crossbar provides (1) efficient, low power memory, (2) built-in integrity checking, and (3) authentication capabilities via a PUF operation mode. The major caveat for PUF operation is that the XbarPUF, as designed thus far, requires that data be overwritten in order to generate proper responses to a given challenge.

For a batteryless IoT device, we envision authentication could occur at the end of a run cycle where data has recently been collected and processed. After data has been processed, the result can either be stored in a smaller local memory or transmitted to the receiving device (e.g. base station) where it would be held in protected memory until authentication has completed. In both scenarios, the data has already been removed from the memristive memory allowing the mode of operation to be switched to a PUF for authentication, at the request of the receiving device. At this point, challenges are presented to the XbarPUF and corresponding responses are determined, just as is done for any PUF based authentication [26].

Another possible research direction for batteryless IoT device authentication is that power may not be sufficient to complete an entire authentication request. In this case, the temporary state of the crossbar is stored due to the persistent nature of the system. Further, integrity checking could occur at the boundaries of recharge cycles to help improve trust that the PUF function has completed properly. More detailed analysis of such a scenario is left for future research.

VI. Conclusion

In this work we've considered some security implications of limited power supply IoT systems, including batteryless devices. One consideration is that batteryless systems require persistent data that can survive across recharge cycles, allowing the system to pick up once recharged. Given the nature of non-volatile memory, such systems are vulnerable to outside attacks, including malicious memory modifications. We propose the use of a memory integrity checking scheme that utilizes sneak path currents in the memristive memory array to generate tags for checking. Early results presented suggest that emerging memristive devices are well suited to

such applications and can operate with very low energy (~ 1.6 pJ) and fast enough speeds (~ 400 ps).

Further building on the concept of dual-use memory (use as for storage and security), we propose the use of a crossbar based memristive PUF for device authentication. One important consideration for using the memory array as a PUF is the likely requirement for the PUF to overwrite data during an authentication session. Thus, the dual-use XbarPUF would need to be used at a point when data can be destroyed. However, as is the case for integrity checking, the XbarPUF has shown to be particularly efficient in terms of area, speed, and power consumption, all necessary requirements for resource limited IoT systems.

ACKNOWLEDGMENT

The authors would like to thank Himanshu Thapliyal of the University of Kentucky for interesting discussions relating to this topic.

This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-16-1-0301. Any opinions, finding, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Air Force.

REFERENCES

[1] J. Hester, N. Tobias, A. Rahmati, L. Sitanayah, D. Holcomb, K. Fu, W. P. Burleson, and J. Sorber, "Persistent clocks for batteryless sensing devices," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 15, no. 4, p. 77, 2016.

[2] H.-S. P. Wong, H.-Y. Lee, S. Yu, Y.-S. Chen, Y. Wu, P.-S. Chen, B. Lee, F. T. Chen, and M.-J. Tsai, "Metal–oxide rram," *Proceedings of the IEEE*, vol. 100, no. 6, pp. 1951–1970, 2012.

[3] G. S. Rose, N. McDonald, L. Yan, and B. Wysocki, "A write-time based memristive PUF for hardware security applications," in *Proc. of the IEEE/ACM Int. Conf. on Computer-Aided Design (ICCAD)*, November 2013, pp. 830–833.

[4] A. Mazady, H. Manem, M. Rahman, D. Forte, and M. Anwar, "Memristor PUF - a security primitive: Theory and experiment," *IEEE J. on Emerging and Selected Topics in Circuits and Syst.*, vol. 5, no. 8, pp. 222–229, June 2015.

[5] G. Rose and C. Meade, "Performance analysis of a memristive crossbar PUF design," in *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2015, pp. 1–6.

[6] O. Kavehei, C. Hosung, D. Ranasinghe, and S. Skafidas, "mrPUF: A Memristive Device based Physical Unclonable Function," *ArXiv e-prints*, Feb. 2013.

[7] A. Chen, "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions," *IEEE Electron Device Lett.*, vol. 36, pp. 138–140, February 2015.

[8] H. Abunahla, B. Mohammad, and D. Homouz, "Effect of device, size, activation energy, temperature, and frequency on memristor switching time," in *26th Int. Conf. on Microelectronics (ICM)*, December 2014, pp. 60–63.

[9] P. Y. Chen, , Tempe, R. Fang, R. Liu, C. Chakrabarti, Y. Cao, and S. Yu, "Exploiting resistive cross-point array for compact design of physical unclonable function," in *IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST)*, May 2015, pp. 26–31.

[10] R. Liu, H. Wu, Y. Pang, H. Qian, and S. Yu, "Experimental characterization of physical unclonable function based on 1 kb resistive random access memory arrays," *IEEE Electron Device Lett.*, vol. 36, pp. 1380–1383, October 2015.

[11] K. Beckmann, H. Manem, and N. Cady, "Performance enhancement of a time-delay PUF design by utilizing integrated nanoscale ReRAM devices," *IEEE Transactions on Emerging Topics in Computing*, p. 1, 2016.

[12] M. Uddin, M. B. Majumder, G. S. Rose, K. Beckmann, H. Manem, Z. Alamgir, and N. C. Cady, "Techniques for improved reliability in memristive crossbar PUF circuits," in *IEEE Comp. Society Annual Symp. on VLSI*, July 2016.

[13] M. Uddin, M. B. Majumder, and G. S. Rose, "Robustness analysis of a memristive crossbar puf against modeling attacks," *IEEE Transactions on Nanotechnology*, vol. PP, no. 99, pp. 1–1, March 2017.

[14] M. B. Majumder, M. Uddin, G. S. Rose, and J. Rajendran, "Sneak path enabled authentication for memristive crossbar memories," in *Hardware-Oriented Security and Trust (AsianHOST), IEEE Asian*. IEEE, 2016, pp. 1–6.

[15] M. Hong, H. Guo, and S. X. Hu, "A cost-effective tag design for memory data authentication in embedded systems," in *Proceedings of the 2012 international conference on Compilers, architectures and synthesis for embedded systems*. ACM, 2012, pp. 17–26.

[16] T. Liu, H. Guo, S. Parameswaran, and X. S. Hu, "Improving tag generation for memory data authentication in embedded processor systems," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, Jan 2016, pp. 50–55.

[17] S.-H. Bae, S. Lee, H. Koo, L. Lin, B. H. Jo, C. Park, and Z. L. Wang, "The memristive properties of a single vo2 nanowire with switching controlled by self-heating," *Advanced Materials*, vol. 25, no. 36, pp. 5098–5103, 2013.

[18] A. S. Oblea, A. Timilsina, D. Moore, and K. A. Campbell, "Silver chalcogenide based memristor devices," in *Neural Networks (IJCNN), The 2010 International Joint Conference on*. IEEE, 2010, pp. 1–3.

[19] M. Escudero-López, E. Amat, A. Rubio, and P. Pouyan, "An experience with chalcogenide memristors, and implications on memory and computer applications," in *Design of Circuits and Integrated Systems (DCIS), 2016 Conference on*. IEEE, 2016, pp. 1–6.

[20] A. C. Torrezan, J. P. Strachan, G. Medeiros-Ribeiro, and R. S. Williams, "Sub-nanosecond switching of a tantalum oxide memristor," *Nanotechnology*, vol. 22, no. 48, p. 485203, 2011.

[21] A. S. Oblea, A. Timilsina, D. Moore, and K. A. Campbell, "Silver chalcogenide based memristor devices," in *Proceedings of The 2010 International Joint Conference on Neural Networks (IJCNN)*, July 2010, pp. 1–3.

[22] H. Kim, M. P. Sah, C. Yang, and L. O. Chua, "Memristor-based multilevel memory," in *2010 12th International Workshop on Cellular Nanoscale Networks and their Applications (CNNA 2010)*, Feb 2010, pp. 1–6.

[23] S. Chalasani and J. M. Conrad, "A survey of energy harvesting sources for embedded systems," in *Southeastcon, 2008. IEEE*. IEEE, 2008, pp. 442–447.

[24] H. Manem, J. Rajendran, and G. S. Rose, "Design considerations for multilevel cmos/nano memristive memory," *J. Emerg. Technol. Comput. Syst.*, vol. 8, no. 1, pp. 6:1–6:22, Feb. 2012. [Online]. Available: http://doi.acm.org/10.1145/2093145.2093151

[25] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. of the 9th ACM Conf. on Comput. and Commun. Security*, 2002, pp. 148–160.

[26] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *44th ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2007, pp. 9–14.