This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

Design, Analysis and Application of Embedded Resistive RAM based Strong Arbiter PUF

Rekha Govindaraj, Swaroop Ghosh, and Srinivas Katkoori

Abstract— Resistive Random Access Memory (RRAM) based Physical Unclonable Function (PUF) designs exploit either the probabilistic switching or the resistance variability during forming, SET and RESET processes of RRAM. Memory PUFs using RRAM are typically weak PUFs due to fewer number of challenge response pairs. We propose a strong arbiter PUF based on 1T-1R bit cell which is designed from conventional RRAM memory array with minimally invasive changes. Conventional voltage sense amplifier is repurposed to act like an arbiter and generate the response. Similarly, address and data lines are repurposed to act as challenge and response bits respectively. The PUF is simulated using 65nm predictive technology models for CMOS and Verilog-A model for a hafnium oxide based RRAM. The proposed PUF architecture is evaluated for uniqueness, uniformity and reliability for various number of stages. It demonstrates mean intra-die Hamming Distance (HD) of 0.135% and inter-die HD of 51.4%, and passes the NIST tests. We study the vulnerability of proposed PUF to machine learning attacks. We also present an application of proposed PUF for data attestation in the internet of things. Proposed PUF-based data attestation consumes 9.88pJ of total energy per data block of 64-bits and offers a speed of 120.7kbps.

Index Terms—Physical Unclonable Function; Resistive RAM; Hardware security; Non-volatile memory; Arbiter PUF; ML attacks; Data attestation.

1 Introduction

Cybersecurity is becoming a growing concern with evolution of Internet-of-Things (IoT). The conventional cybersecurity techniques are devoted to secure the upper layer of software stack assuming the underlying hardware to be secure. However, that assumption is not true anymore and hardware itself is subjected to variety of attacks such as cloning, reverse engineering, Trojan insertion, side channel attack, recycling/counterfeiting, and so on. New methodologies are being developed to ensure the security and integrity of hardware systems. At Integrated Circuit (IC) level, various security primitives are proposed such as Physically Unclonable Functions (PUF) [1-3], recycling sensor [4], True Random Number Generator [5], tamper detection sensor and encryption engines [6]. At Printed Circuit Board (PCB) level, techniques such as Trojan detection have been proposed [7]. Although CMOS-based security solutions [1-3] are promising they offer limited security-specific properties such as process variations, noise and chaos. Emerging technologies such as memristor [8-9] and spintronics [10-11] have demonstrated significant promise because in addition to low-power, high-density and high-speed they also offer new sources of noise and randomness.

PUF is one of the widely accepted hardware security primitives that finds application in authentication as well as random number generation. It generates a secured key by the physical nature of an electronic system. Physical structure of every electronic system is unique due to inherent differences during manufacturing by the same process technology [2]. Several PUFs based on CMOS [2] [3], memristor [8] and spintronic technologies [10-11] have been proposed in the literature. The CMOS PUFs include SRAM based memory PUF, arbiter PUF and ring oscillator based PUFs [1]. Memristor and spintronic PUFs are the memory PUFs that offer good Hamming Distance (HD) due to inherent variations. Domain Wall Memory (DWM) based arbiter PUFs are also proposed to exploit exponential Challenge Response Pairs (CRP) and resilience to machine learning attacks due to non-linearity [10]. Resistive Random Access Memory (RRAM) is another non-volatile memory technology [12-13] based on binary metal electrodes that have been explored for memory and cross-bar array based PUFs [13-17]. The responses are generated by comparing the resistance of memory bits from two symmetric columns of an array. The existing RRAM PUFs are weak due to linear number of CRPs. Extension to strong PUFs (such as arbiter PUF) while staying within the array structure is a non-trivial problem due to requirements such as arbiter circuits and multiplexers.

We proposed design of RRAM based arbiter PUF within 1T-1R memory architecture for the first time [18]. Compared to [18] we make following additional contributions in this paper.

- We evaluate the proposed Arbiter PUF (APUF) characteristics in terms of inter- and intra-HD for various number of stages.
- We propose an APUF architecture resilient to Machine Learning (ML) based model building attacks with few additional modifications.
- We also investigate the application of proposed PUF architecture in data attestation and signature in IoT devices.

The **novelty** of the proposed approach include: (i) realization of APUF within the memory array. In-memory realization of secure hardware security primitives is an attractive solution to complement in-memory computing.; (ii) ability of the proposed APUF to be configured for different number of stages. Configurability feature can be used to camouflage the actual

This paper is based on work supported by Semiconductor Research Corporation (#2442.001) and NSF CNS 1441757. We sincerely thank Dr. Puglisi for help on thorough understanding of the RRAM model.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

number of bits used as challenge in the APUF for response generation. This can be used to provide an additional layer of protection against adversary attacks. For instance, 24-stage APUF accepts all 24 bits of challenge while internally using only 16 address bits with 16-stage APUF configuration.

The remainder of this paper is organized as follows. Section 2 provides the background of PUF, RRAM model for process variation and RRAM-based PUF. Section 3 describes the proposed PUF architecture and Section 4 presents simulation results. Section 5 discusses the potential adversary attacks on proposed APUF with results of ML based model building and side channel attack based on power information. In Section 6, the proposed APUF architecture is leveraged for ML attack resilient design. Section 7 presents the application of APUF for data attestation in IoTs when integrated with a Logic in Memory (LiM) encryption platform. Finally, Section 8 draws conclusions.

2 Background

We discuss the details of PUF, RRAM model and existing RRAM-based PUFs in this section.

2.1 Physically Unclonable Function

PUFs are promising security primitives that find applications in authentication and key generation for secure operation. PUFs can be categorized based on the circuit topologies and the characteristics such as CRPs. Based on circuit topology, PUFs can be categorized as memory PUFs and delay based PUFs [1-3] whereas based on the characteristic property PUFs can be categorized as weak and strong PUFs.

Memory PUFs exploit the random initialization of the SRAM bits in an array due to process variations in CMOS memory cell. The address bits are used as challenge and the bits read from the SRAM array with the address is the response of the PUF. The number of CRPs are limited by the number of address bits of the memory. APUF (Fig. 1) comprises of two symmetric electrical paths and the delay difference between the paths is digitized by an arbiter. The arbiter output is the response of an APUF. The symmetric paths consist of gates and multiplexer circuits. Multiplexer select lines are used as challenge bits. At every stage multiplexer select lines connect the two incoming paths to one of the outputs. The randomness in the path delay due to process variation makes the delay parameters unclonable which makes an APUF stronger. Further, with exponential increase in the number of CRPs and multiple delay paths while employing XOR gate as arbiter makes APUF more secure and resilient against potential adversary attacks such model building.

2.2 Resistive RAM Technology

RRAM is a promising candidate for future non-volatile memory applications [12]. It is designed by sandwiching an oxide material between two metal electrodes i.e., Top Electrode (TE) and Bottom Electrode (BE). RRAM resistive switching is primarily due to the mechanism of oxide breakdown and reoxidation which modifies a Conduction Filament (CF) in the oxide. The conduction through the CF is primarily due to the transportation of electrons in the oxygen vacancies. The oxygen

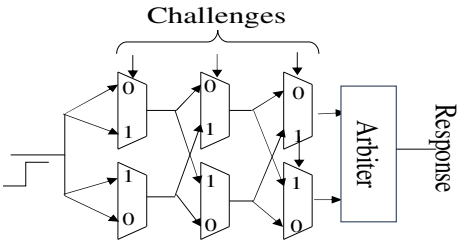

Fig. 1 CMOS APUF

vacancies in the oxide filament are created under the influence of electric field due to applied voltage. The two states of the RRAM in low resistance and high resistance are termed as Low Resistance State (LRS) and High Resistance State (HRS). The process of switching the state of RRAM to LRS is known as SET process while the process of switching the state to HRS is known as RESET process shown in Fig. 2. The resistance switching of RRAM involves three elementary processes such as formation, SET and RESET. Fig. 3 shows the voltage and current transfer characteristics during the SET and RESET process cycles. The minimum resistance of the filament depends on the current compliance used in the process of forming. We have used the expressions from [8-10] as the basis to model the resistance of hafnium oxide based RRAM at different voltages applied at the top electrode.

The forming voltage is applied across the electrodes to create an electric field in the oxide material. Oxygen atoms are knocked out of oxide material forming oxygen vacancies under the influence of high electric field, typically as high as 10MV/cm (Fig. 2). The conduction through the CF is primarily due to the transportation of electrons in these oxygen vacancies. After the process of forming the resistance of the RRAM is at the lowest (LRS). Resistance in LRS depends on the current compliance as shown in characteristic plot Fig. 3. Equations for RRAM resistance after forming and RESET operation are as tabulated in Table 1. The SET process is same as forming except that only a part of CF is recovered as compared to forming process (Fig. 2). Also, SET is performed following a RESET process and SET voltage depends linearly

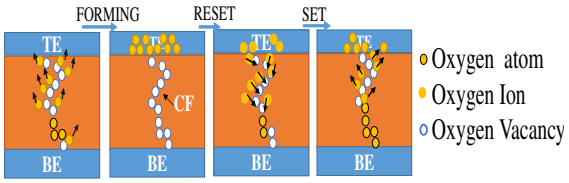

Fig. 2 Resistive RAM forming, SET and RESET mechanism.

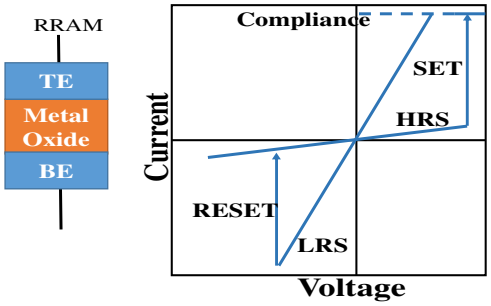

Fig. 3. RRAM device and resistance transfer characteristics.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

Table 1

Equations governing the RRAM resistance

Eqn.	Value
1	$R_{set}=\rho(H_f,CF)*t_{ox}/S$
2	$R_{reset} = \rho(H_f,CF) * (t_{ox}-x)/S + R_{set} (\exp(x/k)-(x/t_{ox}))$
3	$\frac{dx}{dt} = R_{set} * C_{xv} * \lvert V-V_{reset}\rvert$ if $V>V_{reset}$; $\frac{dx}{dt} = 0$ otherwise
4	$I(x,V) = I_0(x) * \sinh(\frac{V}{V0})$
5	$I_0(x) = V_0/R(x)$
6	$R(x,T) = R_{set}*(t_{ox}-x)/t_{ox} + R_{set} * [\exp(x/k)-1]* \exp(E_r/K_b*T)$

$\rho(H_f,CF)$ is the resistivity of the CF, t_{ox} is the hafnium oxide thickness and S is the cross section of the CF. $\rho(H_f,CF)$ depends on the current compliance used during forming (Fig. 3). It is evident that higher current compliance induces a larger CF.
V_{reset} is the function of time and ramp voltage with the peak of 1.3V is applied for RESET. C_{xv} is the proportionality coefficient. V_0 is experimentally measured quantity.
x is the barrier length created by reoxidation of CF by the reset voltage. E_r is the activation energy, K_b is Boltzmann constant and T is the temperature of the device.

on the RESET voltage [19, 20]. The LRS state can be changed by applying a high negative voltage typically greater than 300mV [12]. A read voltage of 100mV is used to read without disturbing the stored data in RRAM. The process of setting state to high resistive state is called RESET process. During RESET, the oxygen ions drifted to the anode return back to the bulk to combine with the oxygen vacancies or to oxidize the metal precipitates. The rate of reoxidation depends on the magnitude of the RESET voltage [20].

2.3 RRAM Model and Process Variation

We have used the model parameters and the equations from [20] that are calibrated with experimental data. The model is based on TiN/Ti/HfOx/TiN RRAM device having a physical oxide thickness t_{ox} of 5nm. Current compliance of 100uA is used for modeling the SET resistance. Table 1 summarizes the equations used in RRAM Verilog-A model. RESET process is performed by negative ramp voltage and the differential barrier length with the voltage is modeled by Eqn. 3. The current during RESET and SET process is given by Eqn. 4. RESET is a thermally activated process and the temperature increases with the electric power and overcomes the activation energy to switch the state of the device. Switching of the device at an applied reset voltage is probabilistic activity [14]. The resistance after RESET process follows lognormal distribution probability characteristics. To model the variation in the resistance of the RRAM due to defects in the oxide material (Fig. 4) we assume Gaussian distribution in the SET resistance of RRAM with the variance 0.08 [20]. The RESET resistance is calculated using the equations Eqns. 4-6 by assuming Gaussian distribution of the proportionality coefficient C_{xv} with variance of 0.034. Due to exponential dependence of RESET resistance on the barrier length HRS exhibits lognormal distribution characteristics as shown in Fig. 4. RESET resistance observed is in the range of 3MΩ- 5MΩ during PUF operation.

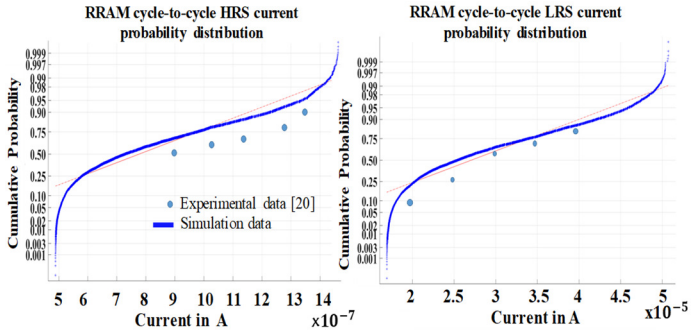

Fig. 4 Defects in the CF, cumulative probability distribution of LRS and HRS resistance from [20] and simulated data.

2.4 Background on RRAM PUFs

The resistance of RRAM after SET and RESET follow probability distribution due to defects in the CF and the thermal voltage fluctuations. The variability in cycle-to-cycle resistance switching which is a source of randomness can be exploited for security applications. RRAM PUF proposed are based on 1T-1R bit cell and crossbar array. In 1T-1R architecture, the input to row decoder and column multiplexer is used as a challenge to select and read two cells of a row randomly. The response is generated by a current sense amplifier by comparing the resistance of two cells. This forms a weaker PUF for array size of NxN, with $N*N*\log_2(N)$ number of CRPs [16]. This PUF becomes unreliable as the technology node shifts below 50nm due to interconnect resistance of crossbar array. Crossbar array PUF proposed in [42] implements APUF by serially connecting the memristors in crossbar array. Responses are XORed to generate a final response which is a classical technique for improving non-linearity in APUF response. MrPUF [43] is a Ring Oscillator (RO) based PUF that uses delay-controlled inverters. Delay of the inverters is varied as a function of resistance variation across the memory array. RO based PUFs are vulnerable to non-invasive frequency injection attack [47]. Also, RO external to memory array incurs an additional area overhead in the PUF.

3 Proposed PUF architecture

In this section, we propose an APUF using regular 1T-1R RRAM array architecture. This is a stronger PUF with exponential number of CRPs. Motivation for the proposed architecture is to achieve desirable PUF characteristics for hardware security while improving the area efficiency of APUF staying with 1T-1R memory architecture. We provide the details of the PUF architecture and performance analysis as well for various number of stages and reconfigurability.

3.1 Summary of Proposed PUF Architecture

Fig. 5(a) shows the proposed the architecture of 1T-1R bit cell based APUF. Design is obtained by making minimally invasive changes to existing RRAM memory array. The column circuitry is modified by including two 2:1 multiplexers (inset in Fig. 5(a)). MUXes connect two selected bit cells from a global column (GC2) to the other bit cells selected from another global

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

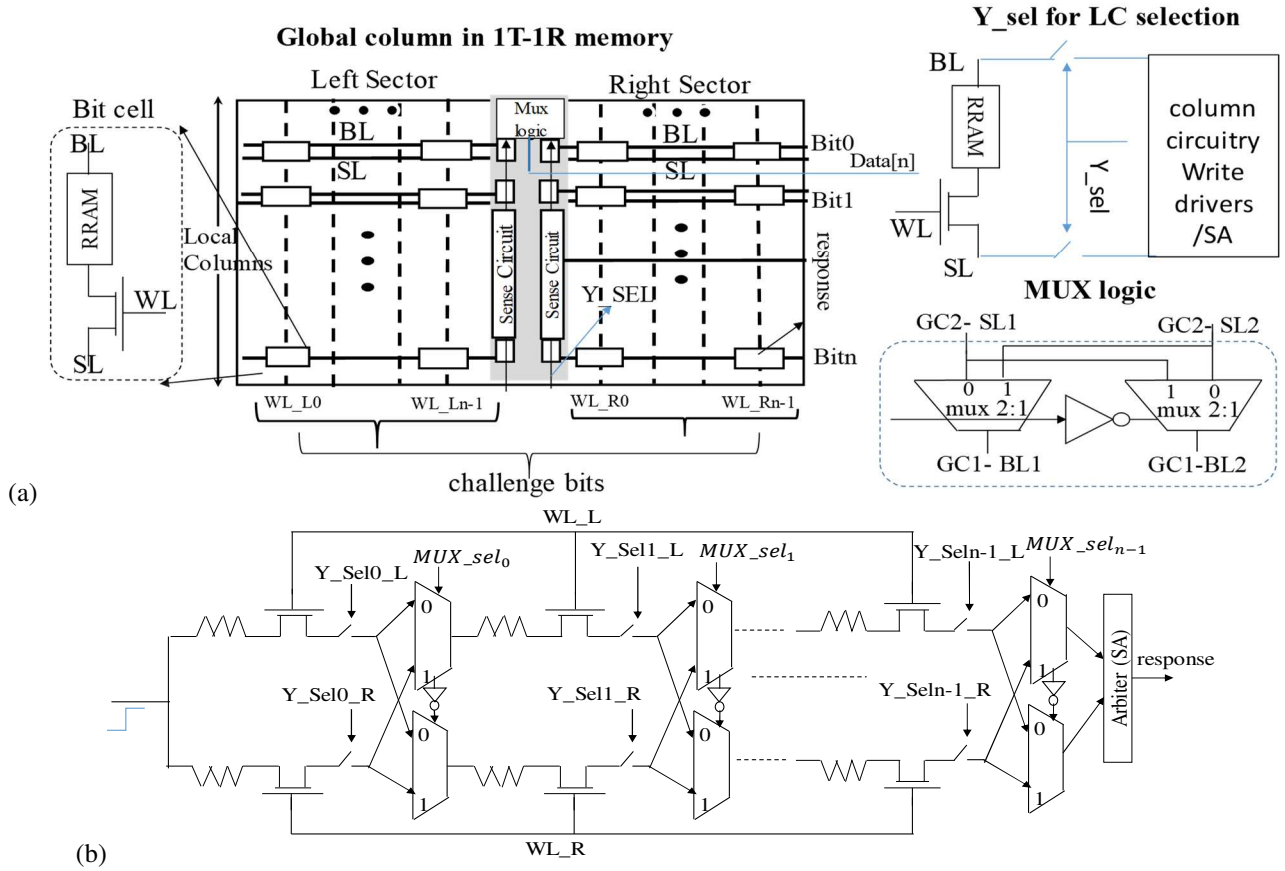

Fig. 5 (a) High level architecture of proposed APUF; and, (b) Conceptual schematic of the proposed APUF

column (GC1). Two bit cells selected in a GC are from two different sectors by Word Line (WL), and column select (Y_sel) signal selects one of the local columns in each of the sectors. Selected bit from local columns is connected to sense amplifier during read or to the write drivers during write in a conventional memory as shown in Fig.5 (a). Source Lines (SL) from GC2 and Bit Lines (BL) from GC1 of the selected bit cells are selectively connected through the MUXs. Select signal to the MUXs in each of the GC forms challenge bit in association with address bits (i.e., sector select and Y_sel) used for bit addressing in every global column. The scheme effectively pairs up any two bit cells of GC1 with other bit cells of GC2 and the connecting path is controlled by the challenge bits (which could be address bits and MUX selects). This type of architecture provides an exponential increase in the number of CRPs with size of memory array.

We repurpose sense amplifier as arbiter in the architecture. Two symmetric paths of APUF are connected as two inputs of a differential sense amplifier. This is evident from conceptual schematic of the PUF shown in Fig. 5(b). Instead of measuring delay between signals racing in two paths to determine the response we measure the voltage difference at a given sense time. This enables the implementation of the PUF architecture from a conventional RRAM memory array minimally invasive. Multiplexers of the arbiter path are placed in column area of

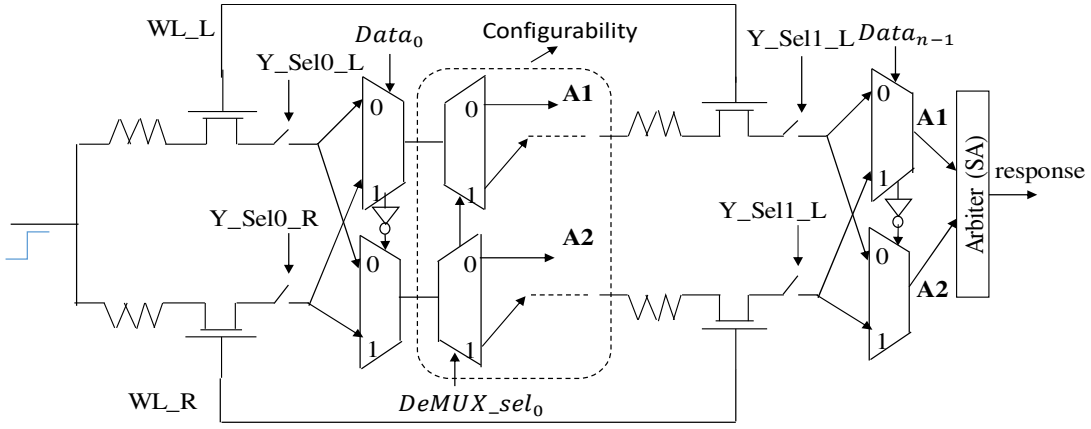

Fig. 6 Configurability for the number of stages in proposed APUF

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

the memory subarray (Fig. 5(a)-(b)). The variability in sense amplifier adds another source of entropy in the PUF response.

3.2 Implementation of APUF

Fig. 5(a) illustrates the implementation of APUF and Fig. 5 (b) depicts conceptual view of RRAM APUF. RRAM bit cells are connected in daisy chain fashion selectively between two symmetric paths. Inset in the right-hand side of Fig. 5(a) shows the MUX circuit placed in column area of the PUF architecture. The state of select signals controls the selected bit cell connection between two symmetric paths. An arbiter is used to produce final response depending on the delay difference between the signals arriving from these two paths. Process variations in the access transistor, MUX circuit and RRAM bit cell are the sources of entropy in such an APUF. We use the access transistors of minimum size. MUX circuit transistors are chosen for optimal speed of the delay paths and smaller ON resistance. Smaller ON resistance ensures that process variation in RRAM RESET resistance is not suppressed in path delay contribution.

3.3 Implementation of Challenges

Fig. 5 demonstrates the APUF implementation along with the challenge bits. Bit cell addressing from the row decoder (WL) and column decoder (Y_sel) along with MUX select lines are used as challenge bits. Such an implementation offers an exponential growth in the number of CRPs with the size of memory array and arbiter stages. Number of arbiter stages should be optimized for larger number of CRPs.

3.4 Implementation of Arbiter

We repurpose sense amplifier present in a conventional memory architecture as arbiter. The implementation is minimally invasive in the memory architecture. Sense amplifier is designed to measure the available sense margin between the two symmetric paths. The method is based on the fact that the delay difference between the signals on two symmetric paths is proportional to the voltage difference at any instant of time before settling. Multiple sense amplifiers are connected in parallel to suppress the effect of noise on sense margin.

3.5 Number of CRPs

The number of MUXes in the paths of APUF varies proportionally with number of global columns in the memory subarray. For N number of global columns, 'M' number of local columns for a memory of word length 'W', the number of CRPs are $(2^N)*(2^M)*(2^W)$. The combination synthesizes a delay path with 'N' 1T-1R bit cells and MUXes in two symmetric delay paths. The area overhead of the proposed PUF is very minimal due the addition of only two MUXes and a select line in each of the GCs. APUF architecture with large number of CRPs yields a stronger PUF compared to RRAM memory PUFs proposed in the literature. By choosing 'X' number of GCs out of 'N' number of GCs in each arbiter path one can have 'N/X' number of symmetric paths. The number of CRPs in such a case would be $(2^{(N/X)})*(2^X)*(2^M)*(2^W)$ for a memory of word length 'W' with 'M' number of local columns. The number of CRPs grow exponentially with size of the memory subarray and number of bit cells in an arbiter path.

Table 2

Number of CRPs with and without configurability

Number of PUF stages 'N'	No. of CRPs with configurable stages ($2^{GC}*2^{LC}*\sum_{K=4}^{N} 2^K$)	No. of CRPs with non-configurable PUF stages ($2^{GC}*2^{LC}*2^N$)
8	32505856	16777216
12	535822336	268435456
16	8588886016	4.295E+09
20	1.37438E+11	6.872E+10
32	5.6295E+14	2.815E+14
40	1.44115E+17	7.206E+16
52	5.90296E+20	2.951E+20
64	2.41785E+24	1.209E+24

3.6 Configurability

Number of multiplexer stages in each path of APUF can be dynamically configured. This is accomplished by using DEMUX at every stage of MUX. 2:1 DEMUX is used to selects one of the two paths, either to generate final response with sense amplifier or direct it the next stage of APUF. Fig. 6 shows the DeMUX stage integrated with the multiplexer stages in the architecture to facilitate configurability. DeMUX_sel signal is used for configuration at each stage. When DeMUX_sel is '0' the path breaks bypassing further stages. A1 and A2 are connected to the arbiter. When DeMUX_sel is '1' outputs from the MUX is connected to on-coming path. It should be noted that A1, A2 inputs of the arbiter should be multiplexed at the input of single arbiter or exclusive arbiters should be employed after each of DeMUX stage. However, sense amplifiers in each of the GCs are utilized to generate response by connecting to DeMUX in respective GC. Therefore, arbiter is readily available at every stage of MUX and DeMUX. Further, configurability also increases the number of CRPs as discussed in the next subsection.

3.7 CRPs with Configurability

Configurability in the proposed architecture offers various advantages along with the ability to dynamically select the number of APUF stages. To completely exploit the rich features in the proposed architecture, DeMUXs can be utilized to increase the number of CRPs exponentially yielding a much stronger APUF. For instance, 'N' bit arbiter with DeMUX in each of the GCs, CRPs available from the configuration for 'N-

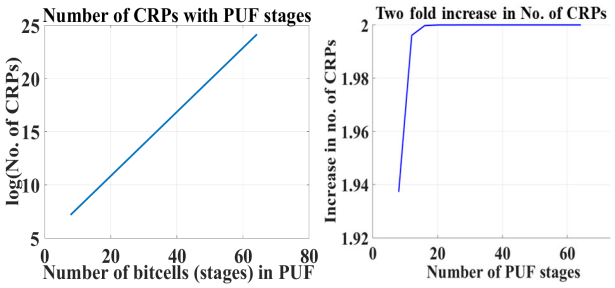

Fig. 7 (a) Number of CRPs with respect to number of stages; and, (b) Two-fold increase in the number of CRPs with configurable PUF stages.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

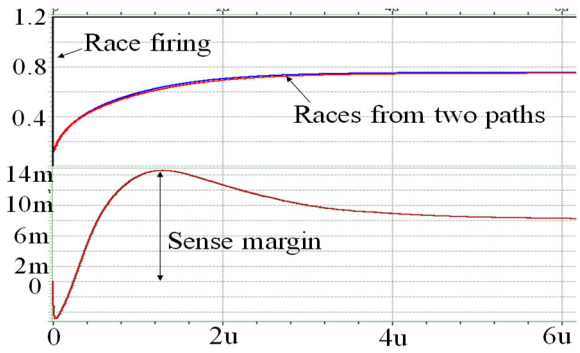

Fig. 8 Race firing and sense margin development at differential SA.

1', 'N-2',… 5,4… so on could be combined together to obtain $2^N+2^{N-1}+2^{N-2}+\cdots\cdots 2^4$ number of CRPs. The total number of bits in a challenge in such case is 'M_N+D_N' where M_N is the number of multiplexers in the arbiter and D_N is the number of DeMUXs. D_N bits remain constant while M_N bits follow regular binary number pattern for a fixed configuration. For example, in a 16-stage APUF for up to 8-stage configuration total number of CRPs is '$2^8+2^9+2^{10}+\ldots.2^{16}$'. D_N bits in the first configuration are '1111111100000000' likewise in the last configuration for all 16-stages in the APUF D_N bits are '1111111111111111'. By approximating summation in the equation, we get $2^{GC}*2^{LC}*\sum_{K=4}^{N} 2^K$. The number of CRPs is twice compared to $2^{GC}*2^{LC}*2^N$ with non-configurable PUF stages. Total number of CRPs with minimum of 4 stages in APUF configuration with 8 GCs and 8 LCs in the memory array are as tabulated in Table 2.

The number of CRPs with respect to the number of PUF stages is shown in Fig. 7. It can be observed that exponential number of CRPs can be obtained from the proposed PUF by altering the number of global columns employed in the path. Number of CRPs in the proposed grow exponentially with the number of stages in APUF (Fig. 7(a)) and can be increased further by exploiting the feature of configurability. The number of CRPs with minimum of 4 stages in APUF configuration with 8 GCs and 8 LCs in the memory array is shown in Fig. 7(b).

4 Simulation Results

We present simulation results of the proposed APUF with 8 GCs. We have used 65nm predictive technology models [21] and Verilog-A model of RRAM for simulations. All bit cells are initially set by forming process. Then a RESET voltage of -1.3V is applied at the BL of RRAM while the SLs are connected to ground. HRS and LRS are modeled as explained in Section 2.3. The LRS is assumed to have gaussian distribution with mean 3.65kOhm and variance of 0.034 [20]. Cxv is a model parameter and is assumed to have gaussian distribution with variance of 0.08 in compliance with experimental results [20] of hafnium oxide based RRAM. We evaluate PUF for three metrics namely, uniqueness, reliability, and uniformity. It should be noted that the responses are not uniformly distributed unlike in a RRAM based memory PUFs proposed so far [17]. This is because the delay is used as response in a path composed of multiple 1T-1R bit cells and MUXes. The address bits used to select the bit cells in each of the global columns and subarrays is used as challenge along with the multiplexer select line inputs. Voltage across the RRAM in the memory cell for more than 8 1T-1R cells connected in series is less than 100mV of read voltage. This

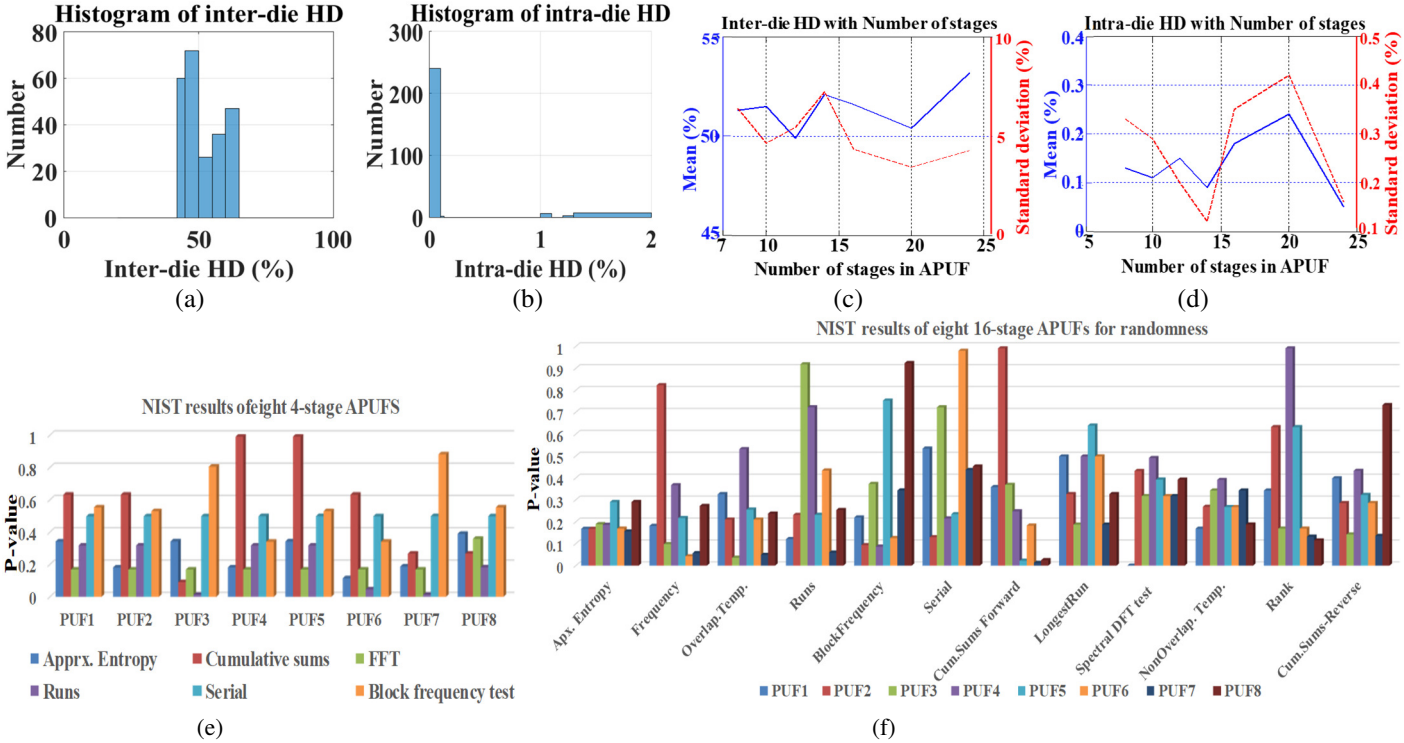

Fig. 9 (a) & (b) Histogram of the PUF responses such as inter-die HD and intra-die HD for 8 stage APUF; (c) & (d) Inter-HD and intra-HD of APUF with various number of stages mean and standard deviation; and, NIST results of eight: (e) 4-stage; and (f) 16-stage APUFs. Passed all the tests with P-value > 0.01.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

ensures that the cells are not read disturbed during evaluation of response in an APUF with >8 stages.

Fig. 8 shows the firing of race and the race signals from two paths in the simulation waveform. Race firing refers to the application of input transition to PUF's symmetric paths. Race signals from paths are fed to the differential sense amplifier which resolves to generate a response. The sense margin is the maximum voltage difference measured between the race signals at the end of delay path is also shown in the diagram. A peak sense margin of 14.5mV is developed when the sense amplifier can be fired. Approximately 10mV of continuous difference between the signals of the race is due to potential drop difference across the resistance of RRAMs in the path.

Uniqueness: Uniqueness in the PUF response enables the identification of different chips uniquely. Uniqueness is measured by inter-die HD. 50% of inter-die HD indicates better uniqueness of PUF response [22]. Fig. 9(a) shows the plot of percentage inter-HD of the proposed APUF. We have measured inter-die HD by varying the threshold voltage of access transistor by ±10% and process variation in RRAM array as explained in Section 2.3. It is evident from the graph that inter-HD is close to 50% with the mean of 51.3% which indicates desired quantity of uniqueness for practical applications. Fig. 9(c) shows the mean and SD of inter-die HD for APUF with various APUF, which demonstrates desirable inter-die properties with mean in the range of 49%-53% and SD range of 3.45%-7.23%.

Reliability: Reliability is the measure of the dependency of PUF response to the intra chip parameter variations such as voltage and temperature. The reliability of a PUF can be measured by its intra-die HD which should be close to 0% for all the possible challenges of a PUF for all responses [22]. Intra-die HD is measured by XORing the responses of the PUF at various conditions of voltage (+/-10% variations) and temperature (-10C to 90C). In our measurements HD is close to 0% for most of the challenges and is less than 2% with the mean of 0.13% (Fig. 9(b)). Fig. 9(d) illustrates the intra-die HD of APUF with various stages. It can be observed that most of the responses have zero intra-die HD with mean in the range of 0.05%-0.24% and SD in the range of 0.12%-0.42% for all the responses.

Uniformity: For uniformity in the PUF response, the probability of 1s and 0s in the response for possible challenges should be 50%. We evaluate the uniformity by the frequency metric in the NIST benchmark for all the possible 256 CRPS of 8 RRAM bits in an APUF. The test showed 50-53% of probability of 1s and 0s with block frequency test, which guarantees a desired uniformity in the PUF responses. NIST test results for eight different 4-stage and 16-stage PUFs are shown in the graph Fig. 9. Entropy test on the responses show p-value greater than 0.01 which ensures randomness. 16-stage PUF is chosen to have sufficient length of bitstream to apply all the tests in NIST test suite [22].

Aging: We study the effect of aging after 10 years by modeling degradation in resistance with shifted median by ±20% (0.64uA-0.96uA HRS current in Fig. 4) in the HRS distribution [44]. Bit Error Rate (BER) of response is calculated

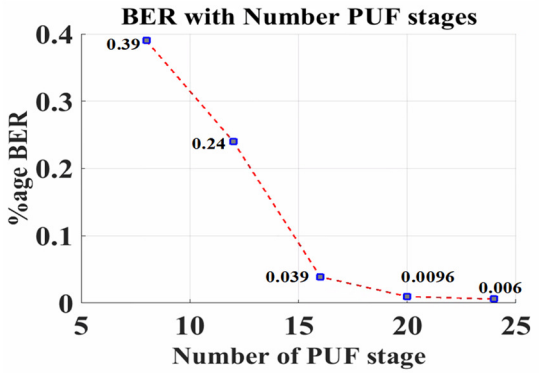

Fig. 10 BER of APUF with number of stages after 10 years of aging.

for different stages in APUF (Fig. 10) as the ratio of number of incorrect responses to total number of CRPs due to aging. Incorrect responses are associated with the shift in the sense margin at the arbiter. Variations in symmetric paths tend to cancel out with each other resulting in BER less than 0.01% in 20 stage APUF. With increase in the number of stages net variation in RRAMs connected in series tend to be lower compared to net variation with fewer number of stages.

Attacks on Proposed APUF

In this section, we discuss the adversary attacks on APUF and present the results of vulnerability analysis on the proposed APUF architecture. Model building attacks based on ML algorithms, side channel attack, hybrid ML and side channel attacks [23-27] have been proposed in the literature. We investigate ML algorithms for model building and side channel attack based on power information of the APUF in this paper.

4.1 ML based model building attacks

ML attacks are based on using computer algorithms to model the behavior of PUF. Output of PUF is a binary response for a given challenge which is solved as a classification problem in ML. ML algorithms for PUF modeling use the classifiers with supervised learning. A percentage of CRPs are used to train the ML classifier and the model developed on the training data set is used to predict the remaining responses of PUF [23]. Logistic Regression (LR) and Support Vector Machine are two machine learning frameworks investigated extensively in PUF modelling attacks.

We investigate LR based ML attacks using data mining tool from the University of Waikato [28-29], Waikato Environment for Knowledge Analysis (WEKA). We use WEKA to model the proposed APUF using ML algorithms. We also investigate Multi-Layer Perceptron (MLP) which is another LR classifier for ML attack on the proposed PUF. The ability of MLP neural network algorithm to model non-linear behavior is the motivating factor for this study [30]. Performance of ML attack is measured as percentage of correctly predicted instances with given percentage of training samples, termed as success rate in the rest of this paper. ML model predicts single bit response generated by APUF. For instance, in a 16-stage APUF, out of 2^{16} samples, 20% ($0.2x2^{16}$= 13107) samples were used as test samples to build model. And if 10% were correctly predicted, we have $0.1x(2^{16}$-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

13107) = 5243 samples were correctly predicted. This is achieved in WEKA by selecting percentage split of samples for model building. This is achieved in WEKA by using percentage split in the samples for model building.

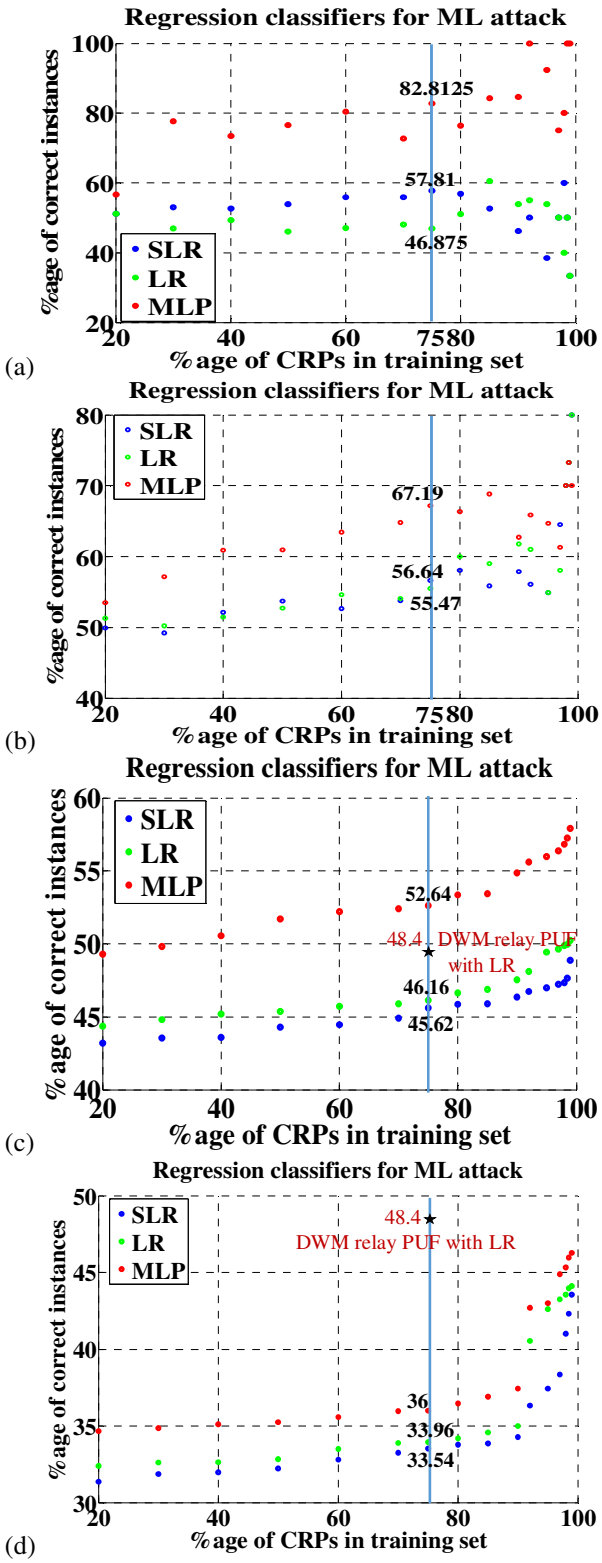

Fig. 11 Performance of regression classifiers SLR, LR, and MLP for machine learning attack on RRAM APUF: (a) 8-stage; (b) 10-stage; (c) 16-stage; and, (d) 24-stage.

Fig. 11 shows the results of using Simple Logistic Regression (SLR), LR and MLP data mining algorithms for model building of the APUF with 8, 10, 16 and 24 stages. SLR is a conventional LR algorithm where the predicted variable takes only two values (0/1, TRUE/FALSE in PUF) with binary logit function [31]. LR in WEKA includes ridge estimator implemented into LR to reduce the error in predictions [45-46]. We measure success rate with various percentage of test instances from 10% to 99%. success rate of various ML attacks is compared at 75% of test instances to establish comparison with other APUFs in the literature. SLR algorithm performed better than LR algorithm for smaller training samples. With 75% training set the correctly predicted instances were as low as 46.87% in LR while in SLR and MLP the correctly predicted instances 57.81% and 82.81% respectively (Fig. 11(a)). Percentage of correctly predicted instances in 8-stage APUF using LR (46.87%) is smaller than that in SRAM (65.6%) and DWM PUFs (48.4%) proposed in literature [10]. Also, the percentage of instances correctly predicted vary in non-linear fashion with the percentage of training samples (Fig. 11) which could be associated with the non-linear behavior of proposed APUF. Observing the performance of LR and SLR algorithms motivates us to use MLP which can be used to build models predicting non-linearity. MLP is a logistic regression based multi-layer neural network algorithm with non-linear activation functions used in the hidden layers [30]. MLP performed well in predicting non-linear behavior of RRAM APUF and yields more than 72% of correctly predicted instances in most of the percentage splits of training and test samples from 30-85% which demonstrates the weakness of APUF to model building attacks by choosing a suitable ML algorithm [23]. However, to get 100% of correct instances using MLP we had to use training set size of 92%. ML attacks SLR, LR and MLP performed well on 10-stage APUF (Fig. 11(b)). With 75% of training set 56.64%, 55.47% and 67.19% of test instances were predicted correctly with SLR, LR and MLP regression classifiers respectively.

For 16-stage and 24-stage even with MLP only 52.64% and 36% of the instances were correctly predicted with 75% training and test sample split (Fig. 11(c, d)). The improvement in the resilience of APUF is due to increased number of samples with non-linearity to be predicted with fewer training samples. Given millions (2^{24}) of CRPs with 24-stage APUF, adversary will be able to efficiently observe only smaller percentage of samples for training. Therefore, limiting the training samples to less than 50% at most 35% of the test samples were predicted correct with LR, SLR and MLP. With longer paths and larger CRPs proposed APUF is robust to ML attacks compared to SRAM and, DWM PUFs. CMOS APUFs are vulnerable to ML attacks; with <20% training set in 64-stage APUF Support Vector Machine and Artificial Neural Network (with multilevel hidden layer suitable to binary classification problem in non-linear data set) provide success rate of greater than 65% successfully [24]. We leverage the proposed architecture to improve the resilience of RRAM APUF with fewer stages against ML attacks (Section. 6).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

4.2 Analysis of Side Channel Attack

APUF is a strong PUF with large number of CRPs. APUFs can be designed to safeguard against the ML attacks [1] which can be achieved by selection of an arbiter function to minimize the correlation between the CRPs and path delay. Side channel attacks [25] are based on analyzing correlation between the dynamic powers consumed by the PUF with respective CRPs. The correlation coefficient indicates vulnerability of the circuit to power analysis attacks such as side channel attack [26]. We calculate the correlation coefficient by calculating the power consumed for each of 256 CRPs in an 8-stage APUF. correlation coefficient between the logic values (R) and power (P) is calculated by using the equation:

$$\text{correlation-coefficient(R, P)} = \frac{E[(R-\mu R)(P-\mu P)]}{\sigma R * \sigma P}$$

where, μR and μP are the mean of R and P, σR and σP are the standard deviation of R and P respectively.

Correlation coefficient between CRPs and power gets closer to zero with the number of CRPs (Fig.12(a)) which indicates that there exists no strong correlation exists between the response bits and the power drawn by the APUF circuit. The correlation coefficient decreases with number of CRPs examined in the proposed PUF. The proposed APUF is resilient against the side channel attack. We also calculate the correlation coefficient between the sense margin of all the CRPs and the power for generating the PUF response for 8-stage APUF. The correlation coefficient plot is shown in Fig.12(b). This indicates no strong correlation between the challenges and sense margin which is amplified by the sense amplifier to generate the response. Hence, it is not feasible to model the PUF response from a known set of CRPs by the method of side channel attack.

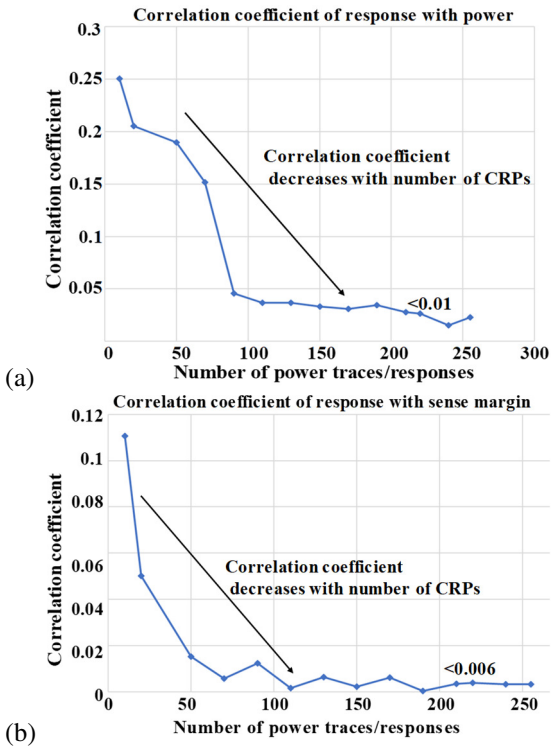

Fig. 12 Correlation coefficient with number of CRPs. CC decreases with the larger number of CRPs.

5 Proposed APUF Architecture for Resiliency to ML Attacks

To improve the resilience against ML based model building attacks we employ the classical approach of using XOR operation to generate final PUF response. XOR APUFs are simplest realization of ML attack resilient design of APUFs [1, 32]. We leverage the proposed architecture to generate APUF response by 'XOR'ing the responses from multiple APUFs. RRAM cells in the paths of multiple APUFs are selected simultaneously by shorting their 'Y_sel' signals. Fig. 13 shows the architecture of RRAM APUF leveraged for ML attack resilience with XOR of responses from two APUFs. We select two cells from same row and different local columns of a GC to establish four paths for two APUFs. Responses from the two APUFs are XOR'ed to generate final response. MUX selects for the two MUXes are generated from a single MUX (Data[n]) select signal by complementing it. This minimizes the routing complexity of interface signals and simplifies implementation from a conventional 1T-1R memory architecture.

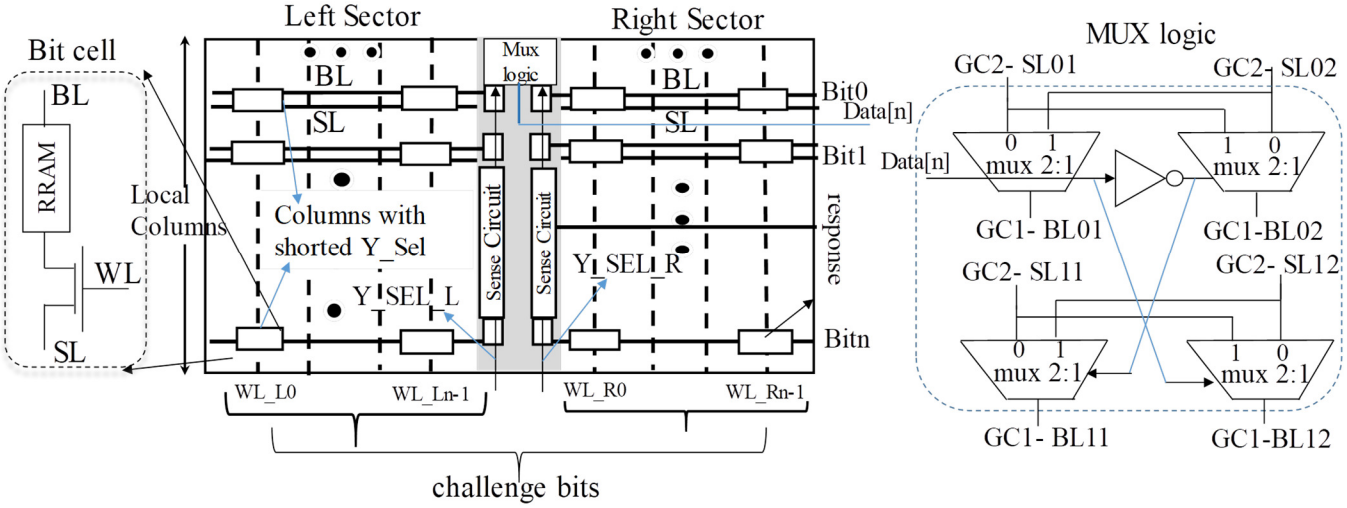

Fig. 13 RRAM APUF architecture resilient to ML attacks. Two local columns are selected simultaneously from two sectors.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

The technique can be extended by using different Y_sel lines to select more than two local columns simultaneously. 'XOR' of all the responses (more than 2 APUFs) is calculated at the final stage to generate the PUF response. However, it adds the overhead of additional interconnects and input ports in the 1T-1R array. This is due to separate MUX selects and Y_sel signals required for each of the APUFs. Also, additional area overhead due to growth in the number of MUXes in the column area at each stage of APUFs.

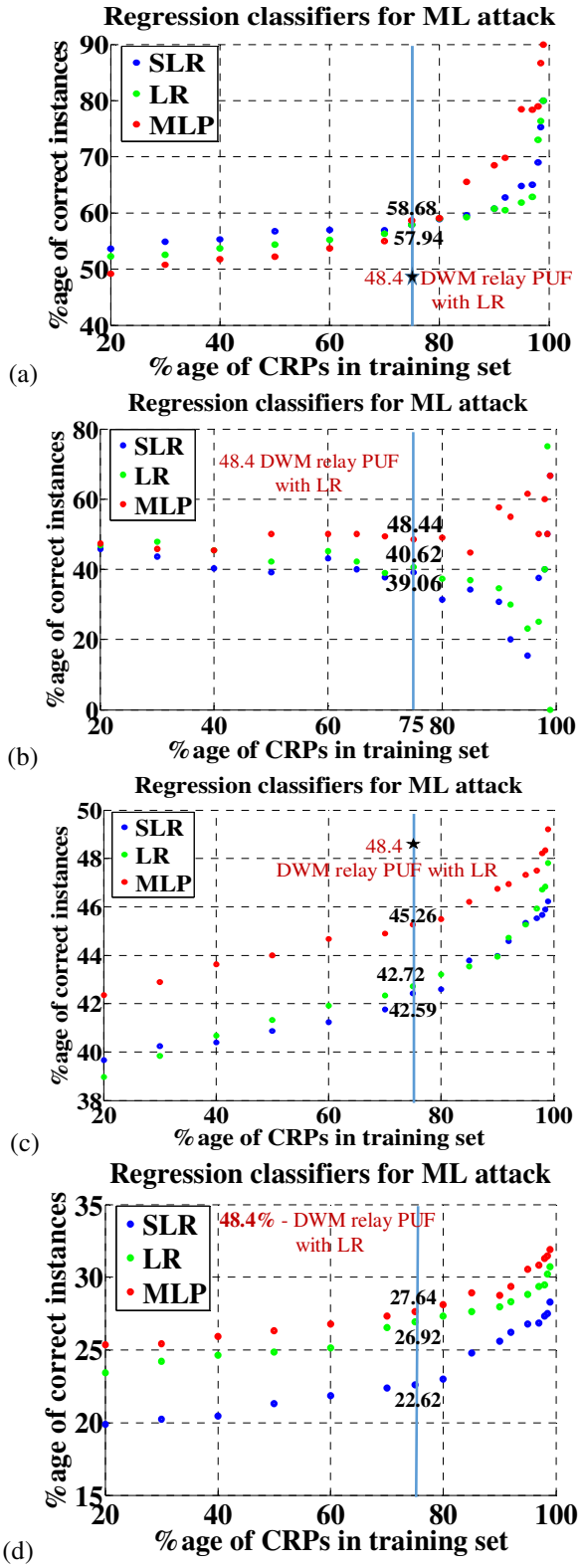

Fig. 14 Performance of regression classifiers SLR, LR and MLP for ML attack on proposed ML resilient architecture with (a) 8-stage; (b) 10-stage; (c) 16-stage; and, (d) 24-stage.

Fig. 14 presents the results of regression classifiers SLR, LR and MLP for ML attack on the proposed ML resilient architecture for 8-stage, 10-stage, 16-stage and 24-stage APUF. PUF response is produced by XORing the response from two APUFs. Significant reduction in the number of correctly predicted instances is observed from the plots. With 75% of the test vectors only less than 50% of the instances were predicted correctly in 10-stage PUF. In 8-stage APUF less than 60% with (less compared to SRAM PUFs 65.6%) of instances were predicted correctly using LR and SLR classifiers. In ten or more number of stages of APUF success rate of ML algorithms including MLP lowers below that in DWM PUF using LR (48.4%) with 75% of training data. This demonstrates appreciable improvement in resilience to ML attacks with the proposed 'XOR' based APUF architecture.

The proposed APUF is strong and can be leveraged to be ML attack resilient with minimal implementation, and area overhead from 1T-1R memory architecture. Table 3 summarizes the comparative analysis of the proposed PUF with other RRAM based memory and cross bar array PUFs in the literature [42-43].

We present an application of the proposed APUF for data attestation in the IoTs in the next section along with the qualitative analysis of the proposed attestation technique.

6 Application in Hardware Attestation

6.1 Basics of Hardware Attestation

IoTs is a system consisting of various computing and non-computing, living and non-living things connected to interact with each other. In such an environment, establishing the integrity of each of the connected objects is a challenge [33]. Attestation is a method of establishing the trust and integrity of a remote device. Attestation ensures the security by establishing trust in operations performed on remote device. Various techniques based on software, hardware and hybrid have been proposed in the literature [33-39]. Sensor nodes in an IoT system are light weight with minimal or almost no software application layer. Integrity of the sensor hardware is an important requirement for establishing trust in its data. The sensor nodes in IoT system where hardware plays vital role in sensing and sending the data to the base station, hardware implementation of attestation algorithm is viable. Unlike in a computing device running various software applications in which software needs attestation, in an IoT system data sent from the sensor node should be attested by its hardware.

Proposed APUF demonstrates good statistical properties and resilience to adversary attacks. We propose a method of attestation using the proposed PUF architecture. This is achieved by integrating a data encryption algorithm that uses the key generated from the APUF. A light weight attestation module implementation is proposed. Attestation in light weight sensor nodes consist of a sensor which is registered with the base station prior to its deployment. Therefore, base station is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2018.2866425, IEEE Transactions on Dependable and Secure Computing

Table 3
Comparison of RRAM based PUFs

	[14]	[15]	[16, 42]	Proposed
Topology	1T-1R Memory PUF	1T-1R Memory PUF	Cross bar array	APUF with 1T-1R memory
No. of CRPs	Quadratic: $N*N*\log_2(N)$	Quadratic: $N*N*\log_2(N)$	Linear: $Cn^2*N*\log_2(N)$ Cn: No. of cols	Exponential: $2^{GC}*2^{LC}*2^N$ GC: No. of GCs, LC: No. of LCs N: No. of MUX stages
% Inter HD	50% with SD=3.2%	NA	49-50%	51.3% mean; SD=6.41%
% Intra HD	0%	NA	1.7-2.3%	0.13% mean; SD=0.33%
ML attack success rate	NA	NA	NA	<=36% without XOR; <28% with XOR given 75% training set

aware of hardware and in specific PUF CRPs of a registered sensor node. The proposed PUF has large number of CRPs, only a few CRPs for each of the registered sensor nodes are used for attestation. Challenge is a public key and respective response is the secret key used for encryption (Fig. 15). We will discuss the implementation of encryption hardware and data attestation in the coming subsections.

6.2 Implementation of Encryption Hardware

Design for data attestation uses a Programmable Logic in Memory (PLiM) computer [40]. In [40], a technique is proposed where the computaion is done within RRAM memory. It employs a light weight finite state machine for instruction execution on the data stored in memory. The principle of computation within memory is based on the RESET and SET operation of RRAM. With '1' stored in the RRAM , it switches to '0' or remains '1' depending on the polarity of the voltage applied across its terminals. SET state is read as '1' and RESET state is read as '0'. Combining the operations in the two cases: a) switching when '1' is stored; and b) switching when '0' is stored, operation on memory location can be written as shown below:

$Z_n = A.Z + B'.Z+B'.A$

where, Z is the initial value stored in the memory. Z_n is the value stored in the memory location after operation with A and B are the signals applied to top and bottom electrodes respectively. A' and B' are complement of A and B respectively. For computation A, B and Z are stored in memory locations initially. Instructions are executed in terms of read and write operations initiated from an external Finite State Machine (FSM) based light weight processor.

Implementation of PRESENT encryption algorithm in the PLiM computer is also presented in [40]. Data is encrypted with the response as key stored in the user register using PRESENT or by simple operation between data and key such as XOR.

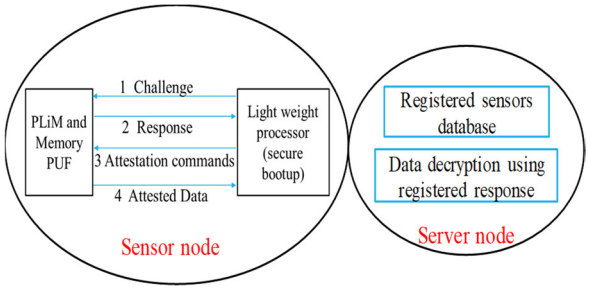

Fig. 15 Sensor nodes and server node in IoT network.

6.3 Data Attestation in Sensor Node

Sensor node is registered with the base station during installation. Base station selects a set of CRPs to be used for data attestation from the sensor node. Likewise, each of the sensor nodes in the network are registered with selected number of CRPs for attestation of the data sent. Sensor nodes encrypt using the attestation algorithm with response of its registered challenge and records the challenge. While sending the data, sensor node sends the challenge along with encrypted data. Different challenges are used in random order to encrypt different data blocks. Base station when it receives the encrypted data with the challenge, it looks up for respective response from its database and decrypt with response as secret key to read the data transferred.

6.4 Performance Analysis of Proposed Attestation Technique

RRAM write time of 1ns and write energy of 0.1fJ/bit is assumed for the write performance of RRAM with maturity of RRAM technology [41]. We measure energy/bit of key generation from PUF. Proposed APUF can generate a bit of response every 0.8us. Speed of 80-bit key generation is 156.25kbps by using 10 APUFs to generate 8-bits of 80-bit key in parallel. Each of the ten PUFs generate 8-bit response. The responses are appended to form an 80-bit key for attestation. Energy/bit generation of APUF response is 50fJ. For 80bit key generation 4pJ of energy is consumed. Attesting a 64-bits block of data with 80-bit key consumes ~5.88pJ of energy. Total energy for attestation of a block of data is 9.88pJ for 64-bits data block. Proposed architecture with PRESENT encryption together can offer a speed of 120.7kbps [40].

7 Conclusion

We propose 1T-1R RRAM APUF using hafnium oxide based RRAM. Multiplexers in the symmetric paths of APUF could be placed in the column area of the memory subarray. Sense circuits in the conventional memory architecture is employed as arbiter. Overall, the implementation of the proposed PUF is minimally invasive from a 1T-1R memory subarray. Proposed PUF is evaluated by systematic PUF evaluation methodology demonstrates 0% intra HD for most of CRPs with the mean of 0.13% and inter HD of mean 51.3% with sufficient randomness in the response. Number of CRPs in proposed APUF increase exponentially with the array size and number of global columns in the subarray. The proposed APUF is strong and resilient against possible adversary attacks

compared to RRAM memory PUFs proposed in the literature. Potential application for data attestation in IoTs is also presented. Speed of 120.7kbps can be achieved with 9.88pJ of total energy for 64-bits block data attestation.

REFERENCES

[1] Herder, Charles, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. "Physical unclonable functions and applications: A tutorial." Proceedings of the IEEE 102, no. 8 (2014): 1126-1141.

[2] Suh, G. Edward, and Srinivas Devadas. "Physical unclonable functions for device authentication and secret key generation." In Proceedings of the 44th annual Design Automation Conference, pp. 9-14. ACM, 2007.

[3] Maes, Roel, and Ingrid Verbauwhede. "Physically unclonable functions: A study on the state of the art and future research directions." In Towards Hardware-Intrinsic Security, pp. 3-37. Springer Berlin Heidelberg, 2010.

[4] Shakya, Bicky, Ujjwal Guin, Mark Tehranipoor, and Domenic Forte. "Performance optimization for on-chip sensors to detect recycled ICs." In *Computer Design (ICCD), 2015 33rd IEEE International Conference on*, pp. 289-295. IEEE, 2015.

[5] https://en.wikipedia.org/wiki/Hardware_random_number_generator

[6] Miura, Noriyuki, Daisuke Fujimoto, Daichi Tanaka, Yu-ichi Hayashi, Naofumi Homma, Takafumi Aoki, and Makoto Nagata. "A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor." In *2014 Symposium on VLSI Circuits Digest of Technical Papers*, pp. 1-2. IEEE, 2014.

[7] Ghosh, Swaroop, Abhishek Basak, and Swarup Bhunia. "How secure are printed circuit boards against trojan attacks?." IEEE Design & Test 32, no. 2 (2015): 7-16.

[8] Mazady, Anas, Md Tauhidur Rahman, Domenic Forte, and Mehdi Anwar. "Memristor puf—a security primitive: Theory and experiment." *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 5, no. 2 (2015): 222-229.

[9] Chen, An, X. Sharon Hu, Yier Jin, Michael Niemier, and Xunzhao Yin. "Using Emerging Technologies for Hardware Security Beyond PUFs." In *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1544-1549. IEEE, 2016.

[10] Iyengar, Anirudh, Swaroop Ghosh, Kenneth Ramclam, Jae-Won Jang, and Cheng-Wei Lin. "Spintronic PUFs for Security, Trust, and Authentication." ACM Journal on Emerging Technologies in Computing Systems (JETC) 13, no. 1 (2016): 4.

[11] Ghosh, Swaroop, and Rekha Govindaraj. "Spintronics for associative computation and hardware security." In 2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1-4. IEEE, 2015.

[12] Wong, H-S. Philip, Heng-Yuan Lee, Shimeng Yu, Yu-Sheng Chen, Yi Wu, Pang-Shiu Chen, Byoungil Lee, Frederick T. Chen, and Ming-Jinn Tsai. "Metal–oxide RRAM." Proceedings of the IEEE 100, no. 6 (2012): 1951-1970.

[13] Chen, An, and Ming-Ren Lin. "Reset switching probability of resistive switching devices." Electron Device Letters, IEEE 32, no. 5 (2011): 590-592.

[14] Chen, An. "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions." Electron Device Letters, IEEE 36, no. 2 (2015): 138-140.

[15] Zhang, Le, Xuanyao Fong, Chip-Hong Chang, Zhi Hui Kong, and Kaushik Roy. "Feasibility study of emerging non-volatilememory based physical unclonable functions." In *2014 IEEE 6th International Memory Workshop (IMW)*, pp. 1-4. IEEE, 2014.

[16] Chen, Pai-Yu, Runchen Fang, Rui Liu, Chaitali Chakrabarti, Yu Cao, and Shimeng Yu. "Exploiting resistive cross-point array for compact design of physical unclonable function." In Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on, pp. 26-31. IEEE, 2015.

[17] Chen, A. "Reconfigurable physical unclonable function based on probabilistic switching of RRAM." *Electronics Letters* 51, no. 8 (2015): 615-617.

[18] Govindaraj, Rekha, and Swaroop Ghosh. "A strong arbiter PUF using resistive RAM within 1T-1R memory architecture." In Computer Design (ICCD), 2016 IEEE 34th International Conference on, pp. 141-148. IEEE, 2016.

[19] Puglisi, Francesco, Luca Larcher, Gennadi Bersuker, Andrea Padovani, and Paolo Pavan. "An empirical model for RRAM resistance in low-and high-resistance states." Electron Device Letters, IEEE 34, no. 3 (2013): 387-389.

[20] Puglisi, Francesco Maria, Paolo Pavan, Andrea Padovani, and Luca Larcher. "A compact model of hafnium-oxide-based resistive random access memory." In Proceedings of 2013 International Conference on IC Design & Technology (ICICDT). 2013.

[21] http://ptm.asu.edu/

[22] Maiti, Abhranil, Vikash Gunreddy, and Patrick Schaumont. "A systematic method to evaluate and compare the performance of physical unclonable functions." In Embedded systems design with FPGAs, pp. 245-267. Springer New York, 2013.

[23] Rührmair, Ulrich, Frank Sehnke, Jan Sölter, Gideon Dror, Srinivas Devadas, and Jürgen Schmidhuber. "Modeling attacks on physical unclonable functions." In Proceedings of the 17th ACM conference on Computer and communications security, pp. 237-249. ACM, 2010.

[24] Hospodar, Gabriel, Roel Maes, and Ingrid Verbauwhede. "Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability." In Information Forensics and Security (WIFS), 2012 IEEE International Workshop on, pp. 37-42. IEEE, 2012.

[25] Delvaux, Jeroen, and Ingrid Verbauwhede. "Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise." In Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on, pp. 137-142. IEEE, 2013.

[26] Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008.

[27] Xu, Xiaolin, and Wayne Burleson. "Hybrid side-channel/machine-learning attacks on PUFs: a new threat?." In Proceedings of the conference on Design, Automation & Test in Europe, p. 349. European Design and Automation Association, 2014.

[28] http://www.cs.waikato.ac.nz/ml/weka

[29] Hall, Mark, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H. Witten. "The WEKA data mining software: an update." ACM SIGKDD explorations newsletter 11, no. 1 (2009): 10-18.

[30] http://deeplearning.net/tutorial/mlp.html

[31] http://www.biostathandbook.com/simplelogistic.html

[32] Ganji, Fatemeh, Shahin Tajik, and Jean-Pierre Seifert. "Why attackers win: on the learnability of XOR arbiter PUFs." In International Conference on Trust and Trustworthy Computing, pp. 22-39. Springer International Publishing, 2015.

[33] Haider, Ihtesham, Michael Höberl, and Bernhard Rinner. "Trusted sensors for participatory sensing and iot applications based on physically unclonable functions." In Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, pp. 14-21. ACM, 2016.

[34] Seshadri, Arvind, Adrian Perrig, Leendert Van Doorn, and Pradeep Khosla. "SWATT: Software-based attestation for

embedded devices." In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pp. 272-282. IEEE, 2004.

[35] Anati, Ittai, Shay Gueron, Simon Johnson, and Vincent Scarlata. "Innovative technology for CPU based attestation and sealing." In Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy, vol. 13. 2013.

[36] Tan, Hailun, Wen Hu, and Sanjay Jha. "A remote attestation protocol with Trusted Platform Modules (TPMs) in wireless sensor networks." Security and Communication Networks 8, no. 13 (2015): 2171-2188.

[37] Premarathne, Uthpala Subodhani, Ibrahim Khalil, and Mohammed Atiquzzaman. "Secure and reliable surveillance over cognitive radio sensor networks in smart grid." Pervasive and Mobile Computing 22 (2015): 3-15.

[38] Steiner, Rodrigo Vieira, and Emil Lupu. "Attestation in Wireless Sensor Networks: A Survey." ACM Computing Surveys (CSUR) 49, no. 3 (2016): 51.

[39] Abera, Tigist, N. Asokan, Lucas Davi, Farinaz Koushanfar, Andrew Paverd, Ahmad-Reza Sadeghi, and Gene Tsudik. "Invited-things, trouble, trust: on building trust in iot systems." In Proceedings of the 53rd Annual Design Automation Conference, p. 121. ACM, 2016.

[40] Gaillardon, Pierre-Emmanuel, Luca Amarú, Anne Siemon, Eike Linn, Rainer Waser, Anupam Chattopadhyay, and Giovanni De Micheli. "The programmable logic-in-memory (plim) computer." In Proceedings of the 2016 Conference on Design, Automation & Test in Europe, pp. 427-432. EDA Consortium, 2016.

[41] Emerging Research Devices (ERD) report, International Technology Roadmap for Semiconductors (ITRS), 2013.

[42] Uddin, Mesbah, Md Badruddoja Majumder, and Garrett S. Rose. "Robustness analysis of a memristive crossbar PUF against modeling attacks." IEEE Transactions on Nanotechnology 16, no. 3 (2017): 396-405.

[43] Kavehei, Omid, Chun Hosung, Damith Ranasinghe, and Stan Skafidas. "mrPUF: A memristive device based physical unclonable function." arXiv preprint arXiv:1302.2191 (2013).

[44] Yoshimoto, Y., Y. Katoh, S. Ogasahara, Z. Wei, and K. Kouno. "A ReRAM-based physically unclonable function with bit error rate< 0.5% after 10 years at 125° C for 40nm embedded application." In VLSI Technology, 2016 IEEE Symposium on, pp. 1-2. IEEE, 2016.

[45] Le Cessie, S., and J. C. Van Houwelingen. "Ridge Estimators in Logistic Regression." Journal of the Royal Statistical Society. Series C (Applied Statistics) 41, no. 1 (1992): 191-201. doi:10.2307/2347628.

[46] http://weka.sourceforge.net/doc.dev/weka/classifiers/functions/Logistic.html

[47] Markettos, A. Theodore, and Simon W. Moore. "The frequency injection attack on ring-oscillator-based true random number generators." In Cryptographic Hardware and Embedded Systems-CHES 2009, pp. 317-331. Springer Berlin Heidelberg, 2009.