AFRL-RI-RS-TR-2018-128

PHYSICS OF INFORMATION ASSURANCE

MAY 2018

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2018-128 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
JOSEPH A. CAROLI
Chief, High Performance Systems Branch

/ S /
JOHN D. MATYJAS
Technical Advisor, Computing
& Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAY 2018	FINAL TECHNICAL REPORT	DEC 2016 – SEP 2017

4. TITLE AND SUBTITLE

PHYSICS OF INFORMATION ASSURANCE

5a. CONTRACT NUMBER
IN-HOUSE (R1XX)

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62788F

6. AUTHOR(S)

Donald Telesca

5d. PROJECT NUMBER
T2MD

5e. TASK NUMBER
IN

5f. WORK UNIT NUMBER
HO

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RITB
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RITB
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2018-128

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. PA# 88ABW-2018-1740
Date Cleared: 10 APR 2018

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Free Space Optical Data Transmission for Secure Computing patent application has a provisional application serial number 62/322,391 and was filed in the United States Patent and Trademark Office on April 14, 2016. HfO memristor devices were measured over a range of temperatures up to 250C. They showed stability in performance at these elevated temperatures.

15. SUBJECT TERMS

HfO, memristors, free space optical data transmission, integrated photonics

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Donald Telesca
U	U	U	UU	19	19b. TELEPHONE NUMBER (*Include area code)*

TABLE OF CONTENTS

Section **Page**

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

1. SUMMARY

The focus of this work was to explore 3 different technologies at the nano-scale that can increase information assurance in DoD cyber systems. First, this work attempted to investigate the most suitable material stack for pursuing future memristor device technologies. Second, a standardized method to define Physically Unclonable Function (PUF) quality and a broadly accepted computation standard for PUFs was under consideration. Finally, the feasibility of utilizing optical data transmission for board to board information transmission and isolation was considered.

2. INTRODUCTION

Mission Assurance (MA), as defined by DoD Directive 3020.40 is "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan.[1] It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy."

Information Assurance (IA) is the application of this directive in the cyber domain. IA activities include measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. IA is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.[2] It can use physical, technical and administrative controls to accomplish these tasks.

In accordance with this directive, a principal responsibility of a commander is to assure mission execution in a timely manner. The reliance of a Mission Essential Function (MEF) on cyberspace makes cyberspace a center of gravity an adversary may exploit and, in doing so, enable that adversary to directly engage the MEF without the employment of conventional forces or weapons.

Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers," and cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."

The U.S. Department of Defense (DoD) depends increasingly on cyberspace to execute critical missions that are vital to maintaining American military superiority in the traditional domains of land, sea, air, and space. The U.S. is arguably more at risk to an asymmetric attack vector launched by an adversary that cannot, or chooses not to, confront the U.S. in a conventional conflict. In the end, the military advantages that net-centricity provides the U.S. military concomitantly offer an adversary affordable attack vectors through cyberspace against critical missions and advanced weapon systems.

2.1. Free Space Optical Data Transmission for Secure Computing

An additional research area for nano-scale hardware based mission assurance will be investigating the feasibility of developing a board to board air-gapped optical data transmission mechanism as a physical security layer. An air gap is a network security measure that consists of ensuring that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network. It is often employed for computers and networks that must be extraordinarily secure. Frequently the air gap is not completely literal, such as via the use of dedicated cryptographic devices that can tunnel packets over untrusted networks while avoiding packet rate or size variation. This is the current state-of-the-art. In this case, however, the goal is to develop an interface between two boards which (a) are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control or at the minimum there is an interlock mechanism in place).

The concept of an air gap represents nearly the maximum protection one network can have from another (save turning the device off). It is not possible for packets or datagrams to "leap" across the air gap from one network to another.

Free Space Optics were originally developed by the military and NASA and have been used for more than three decades in various forms to provide fast communication links in remote locations[3]. Free-Space Optical Communications (FSOC) have already been explored for next-generation military networks[4]. FSOCs were recognized as having the potential to provide fundamental improvement to the ability to support high-capacity links for network-centric operational concepts like widespread sensor data dissemination. Additionally, it has been shown that data can be encoded using the orbital angular momentum of the light. Optical encoding is now being applied to free-space communication links and can potentially lead to improved security implemented at the classical and single photon level[5].

2.2. Entropy Sources in Metal Oxide Memristive Devices for use in Security Primitives

The security primitives, Physical Unclonable Functions (PUFs) and True Random Number Generators (TRNGs) are pieces of the overall security and trust puzzle. Physical Unclonable Functions have been used to mitigate a variety of potential threats and attacks including integrated circuit (IC) piracy, counterfeiting, malicious Trojan insertion and side-channel analysis. Additionally, random number generators are needed for cryptographic applications. Memristors have security relevant characteristics that make them a logical future foundation to generate these primitives. In addition, previous research has shown that memristors are more difficult to reverse engineer and are tamper evident.

A PUF can be described as a fingerprint that can be used to uniquely identify individual integrated circuits (ICs). PUFs are unique in that no two devices will have the same signature and are unclonable due to the inherent infeasibility required to create two devices with the same signature. In the literature, both uniqueness and unclonability have been attributed to intrinsic variations resulting from non-uniform manufacturing process. There is variability in the complex physical processes associated with IC design and manufacturing. This creates a natural defense to an attacker whom now must either control the noise, or selectively and predictively change manufacturing parameters without disrupting the functional correctness of the resulting ICs. This

portion of research will seek to gain a better understanding of whether these fundamental assumptions are valid, and formalize standards that define what makes a suitable PUF.

2.3. ReRam material study

A thorough study that compares metal oxide for use in as a RRAM switching layer has not been performed. This study tries to address this lack of comparison. From the literature, high-k materials seem to be the most promising candidate to serve as the oxide in these metal-insulator-metal (MIM) devices. There are two mechanisms that are competing against each other, one is the electrochemical metallization model creating a conductive filament by moving cations from an active electrode through the insulator and second, the vacancy change mechanism model moving oxygen anion within a sub-stoichiometric insulator and by this forming a filament of the metal inherently available within the metal oxide. The later mechanism is more strongly dependent on the switching layer and preferably used to the superior performance with respect to endurance and reliability. Currently, two materials are leading this field with respect to endurance, data retention, reliability and on/off ratio. These materials are Ta2O5 and HfO2, both showing superior performance by reaching endurance levels of over 1e11 cycles and retention of over 10 years[6,7]. However, these studies only show their best performing device and do not touch on yield and whether or not other materials could perform better.

3. METHODS, ASSUMPTIONS, AND PROCEDURES

3.1. Free Space Optical Data Transmission for Secure Computing

An architecture was proposed and submitted as a patent. Funding was never obtained to build a concept demo from this work. The architecture was found to be novel and following minor revisions, should be receiving a full patent in the summer of 2018.

3.2. Entropy Sources in Metal Oxide Memristive Devices for use in Security Primitives

The research outlined in this work sought to understand the sources of variability in metal-oxide memristive devices and determine whether they are suitable for use in PUFs and TRNGs. There are three components to the research: physical characterization, statistical modeling, and TRNG/PUF circuit design. Statistical analysis of current device operative properties in conjunction with the physical (material) characterization of the same devices will be used to reveal correlations between device variability and certain physical parameters. This will allow for proper understanding of the nature and viability of the entropy afforded by these devices. The statistical data will also be used to develop more accurate device models on which TRNG and PUF circuits can be designed and evaluated.

3.3. ReRam material study

Switching in oxide materials has been encountered in most metal oxides but the characteristic varies largely. The list of metal oxides in which switching was shown includes: TiO2, SiO2, ZrO2, CuO2 Al2O3, WO2, Gd2O3, La2O3, NiO, Ta2O5 and HfO2[8]. In addition, claims have been made that by combinations of lanthanides a better performance can be achieved like with SmxGdxOx. With respect to the study that will be performed the focus was made to be

on easy to fabricate binary metal oxides. The current most studied oxides with the best performance are HfO2 and Ta2O5. From their material characteristic additional metal oxides that fit into the same category and might achieve the same or even a better performance were chosen. The following categories were considered: dielectric constant, atomic number of metal, atomic weight of metal, band gap, number of oxide phases and the free energy for oxide formation at 300C. These numbers are shown in **Table 1** for various high-k materials.

Table 1. Dielectric constant, atomic number, atomic weight, band gap, number of stable oxide states, gibbs free energy and metal price is shown for various high-k and rare earth metals.

	Dielectric constant [4]	Atomic number	Atomic weight (u)	Band gap (eV)	# of oxide states	Free energy (at 300C) in kJ/mol	Metal Price[1] (US$/g)
HfO2	23	72	179	5.6	1	1010	4
Ta2O5	25	73	181	4.6	2	760	9
La2O3	15	57	139	5.5	2	1120	9
Gd2O3	14	64	157	5.3	1	1150	12
Y2O3	15	39	89	5.5	1	1220	13
ZrO2	20	40	91	6	2	1025	2.5
Nd2O3	14.3	60	144	4.4	1	≈1100	13
Yb2O3	13	70	173	4.9	1	≈1100	14
Dy2O3	13	66	162	4.9	1	≈1100	13

Previous results show the superior behavior of HfO2 and Ta2O5 in comparison to TiO2, CuO2 and Al2O3 with respect to endurance, on/off ratio and retention. Following properties contribute to this performance:

1. The high dielectric constant which exceeds 20 for HfO2 as well as Ta2O5 results in a high force applied to these ultra-thin materials. Because of this, in particular the lighter oxygen ions within the materials need a lower electric field to be moved. This movement eventually enables the switching of our material stack in the first place.
2. To ensure a high retention we solely want to move oxygen ions. Fortunately, the movement of ions (metal or oxygen) is statistically dependent on the mass of the ion. A high atomic weight of the metal in comparison to the oxygen would decrease the chance of moving metal ions within the insulating layer. HfO2 as well as Ta2O5 are probably the heaviest metals with such a high dielectric constant.
3. A large band gap is wishful to suppress leakage current in this category HfO2 has a clear advantage in comparison to Ta2O5. The oxide will be weekend till the edge of collapse to reduce forming voltage and eventually build forming free devices. In this case the larger bandgap reduces the trap assisted tunneling and theoretically allows for a comparably lower power operation.
4. The number of stable and semi-stable oxides states have an impact on the resistance state reliability. Due to statistical variations in the filament and the tremendous heat dissipated in the nanostructure it is possible to create different kind of oxide states in the filament during different

[1] Metal prices come from Sigma Aldrich

cycles. These phases have different resistances and negatively affect the reliability. In example Ta2O5 has a very stable TaO2 phase which is a conductor. If this phase is formed in the vicinity of the filament it would cause a drop in HRS for a certain cycle or if formed in the LRS a spike in resistance because it has a higher resistance than metallic Ta. On the other hand, HfO2 does not have such a phase and therefore only switches between Hf and HfO2.

5. The Gibbs free energy for oxide formation determines how thick the oxygen getter layer need to be to enable good switching performance. As of now, an in depth study has not been performed on what impact this value has on the switching characteristic but ideally we want to keep our oxygen getter layer as thin as possible. In example, if we use titanium we might break the filament in the titanium itself and our RRAM inherits the bad characteristics of a TiO2 device.

To investigate the change in switching characteristic of the films, the electrodes and oxygen getter layer were kept the same throughout the study. Initially, due to the large number of publications and therefore a pool to compare our devices against, titanium was used as the oxygen getter layer and ruthenium was chosen as the passive electrode layer.

A total sample number of 6 metal oxides was chosen as a feasible workload for the first phase of the project including HfO2, Ta2O5 and ZrO2 as standard materials, with the following more exotic oxides being selected as novel device structures:

1. La2O3 [9]
2. Ga2O3 [10]
3. Yb2O3 [11]

All three oxides have been shown to work for at least 10^5 cycles by operating with the VCM model in the bipolar switching mode. In addition they spread through the rare earth metals with Z numbers of 57, 64 and 70 for 1, 2 and 3, respectively. The dielectric constant varies slightly from 13 – 15 but this is for a bulk and fully stoichiometric material and will vary in the ultra-thin films. Titanium has been shown to work as an oxygen getter layer for ZrO2 which has a similar free energy[12].

Besides the properties mentioned above there are a number of material properties that impact RRAM switching performance and might be traced down by comparing these similar rare earth oxides:

- Crystallinity
- Unit cell structure
- Cation radius (density)
- Film stress
- Interaction with oxygen getter

4. RESULTS AND DISCUSSION

4.1. Free Space Optical Data Transmission for Secure Computing

The following is the detailed description of the preferred embodiment of the free space optical data transmission invention as submitted to the US Patent office.

Referring to **Figure** 1, the key components of the FSOI security architecture include a network card **110**, printed circuit boards **120, 130, 140** and **150**, transmitters **112, 122, 124, 132,**

142, and **152**, which are described in greater detail later in this document, receivers **111, 121, 123, 125, 127,** and **141**, which are described in greater detail later in this document, a shutter **200** and **202** capable of blocking all transmission of the emitted coherent light, and a mechanical connection system **201** that interlocks the two shutters **200** and **202**, which is can only be manually operated.

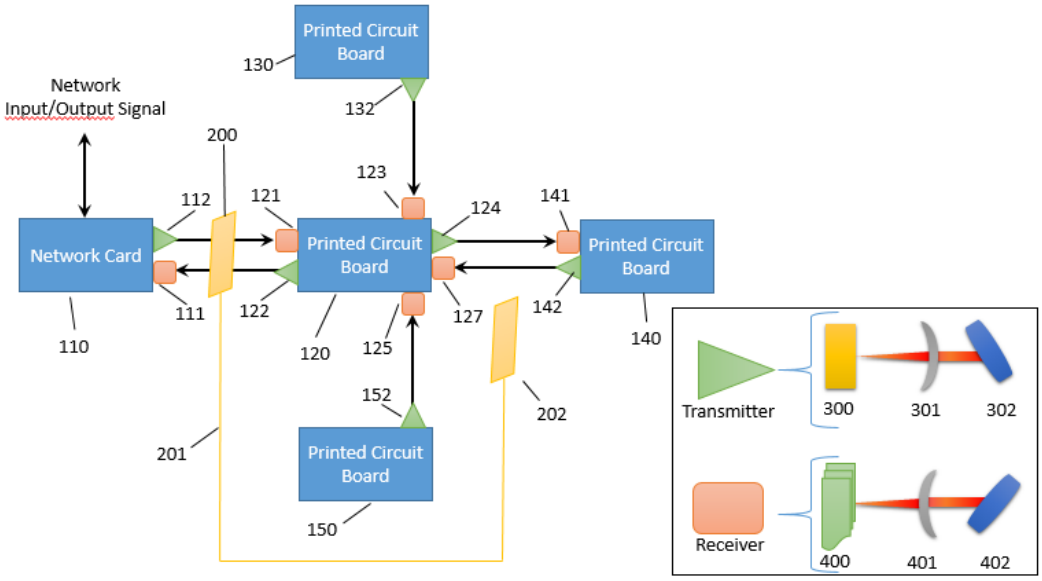

Figure 1: Proposed novel security architecture

Still referring to **Figure** 1, the key components of all the transmitter units include a vertical-cavity surface-emitting laser (VCSEL) **300,** focusing lens **301,** and steering mirrors **302**. The key components of all the receiver units include a photo diode array **400,** focusing lens **401,** and steering mirrors **402.**

Still referring to **Figure** 1, the network card **110** receives and transmits any network traffic as required by the user. In the case of receiving data, the network card uses transmitter **112** to communicate to printed circuit board **120** via receiver **121.** Printed circuit board (PCB) **120** will be capable of, but is not limited to, allowing the user to perform internet browsing, email generation and consumption, and any network connectivity requirements. The user is free to execute any code on PCB **120** as there is no storage allowed on this board. If the user wishes to save a file, they must activate the manually controlled, interlocked shutter system **201**, which uses shutter **200** to block all communication between transmitter **112** and receiver **121.** The network card **110** and PCB **120,** while simultaneously opening communication between PCB **120** and PCB **140**, by removing shutter **202** from their communication path**.** PCB **140** will have any functionality required by the user for file read/write, file edit capabilities and to execute any code. The manual, interlocked shutter system completely isolates PCB **140** from the network, rendering it impossible for nonuser authorized transmission of data or communication back to the network card **110.**

Still referring to **Figure** 1, PCB **130** and **150** are equipped with only a transmitter, **132** and **152** respectively. PCB **130** will have any functionality required by the user for file read/write, file edit capabilities and to execute any code. The exclusively unidirectional nature of the transmitter **132** ensures that dissemination of any information from PCB **130** can only be authorized by the user, making it impossible for any unauthorized access or exfiltration of data from an external

network. PCB **150** works in the same manner as described above for PCB **130**, but differs in the information that is stored on it. PCB **150** will store, but is not limited to, all necessary registry and operating system information necessary to scrub PCB's **120** and **130.**

Referring to **Figure** 2, the first action is for the user to initiate a request for an internet resource. The user will be able to complete this task pending the position of the manually controlled interlocked shutter system **201**. If the shutter system **201** is positioned and verified by the system that the network card **110** cannot communicate with the hub workstation **120** then the user will receive a notification informing them that there is no communication path to external networks. If the shutter system **201** is positioned and verified that the network card **110** is capable of communicating with the hub workstation **120** then the user is free to interact with external networks via the hub workstation **120**.

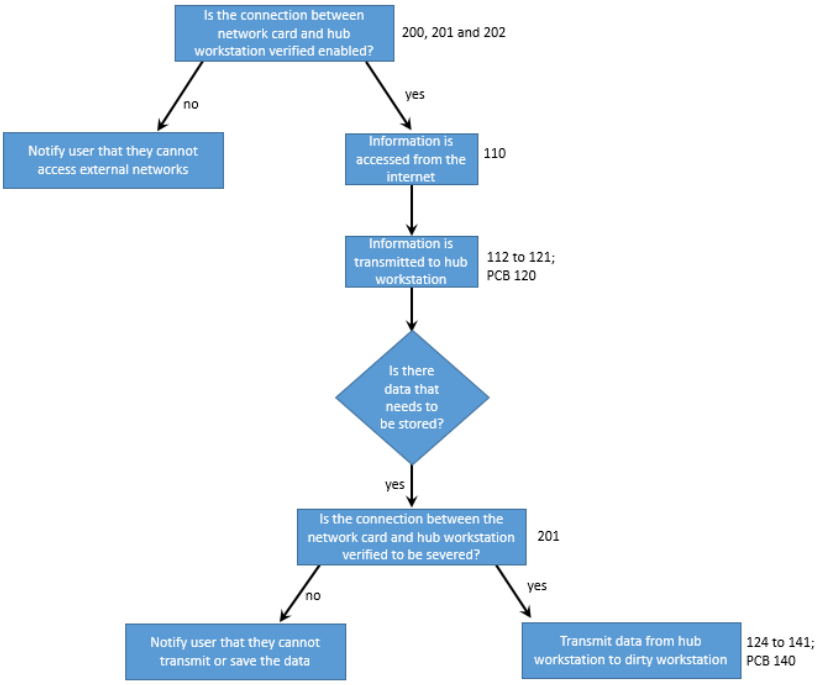

Figure 2: Process flow for internet browsing and storage of network accessed data

Still referring to **Figure** 2, if the user is required to save network accessed data, then they must switch the position of the shutter system **201**, so that the network card **110** cannot communicate with the hub workstation **120**, but the hub workstation **120** can communicate with the dirty workstation **140.** Prior to any write actions being completed, the system must verify that the shutter system **201** is in the correct position: blocking communication between the network card **110** and the hub workstation **120**, and enabling communication between the hub workstation **120** and the dirty workstation **140**. If this is not verified to be true, the user will receive a notification informing them that data cannot be written to the dirty workstation **140**. If the shutter system **201** is verified to be in the correct position (as described above), then the user will be allowed to write to the dirty work station **140**.

Referring to **Figure 3**, the first action is for the user to initiate a request to transmit data to an external network. The user will be able to complete this task pending the position of the manually controlled interlocked shutter system **201**. If the user is required to transmit data to an external network, then they must first switch the position of the shutter system **201**, so that the network card **110** cannot communicate with the hub workstation **120**, but the hub workstation **120** can communicate with the dirty workstation **140.** Prior to any data transmissions being completed, the system must verify that the shutter system **201** is in the correct position: blocking communication between the network card **110** and the hub workstation **120**, and enabling communication between the hub workstation **120** and the dirty workstation **140**. If this is not verified to be true, the user will receive a notification informing them that data cannot be transmitted to the hub workstation **120**. If the shutter system **201** is verified to be in the correct position (as described above), then the user will be allowed to transmit data to the hub workstation **120**.

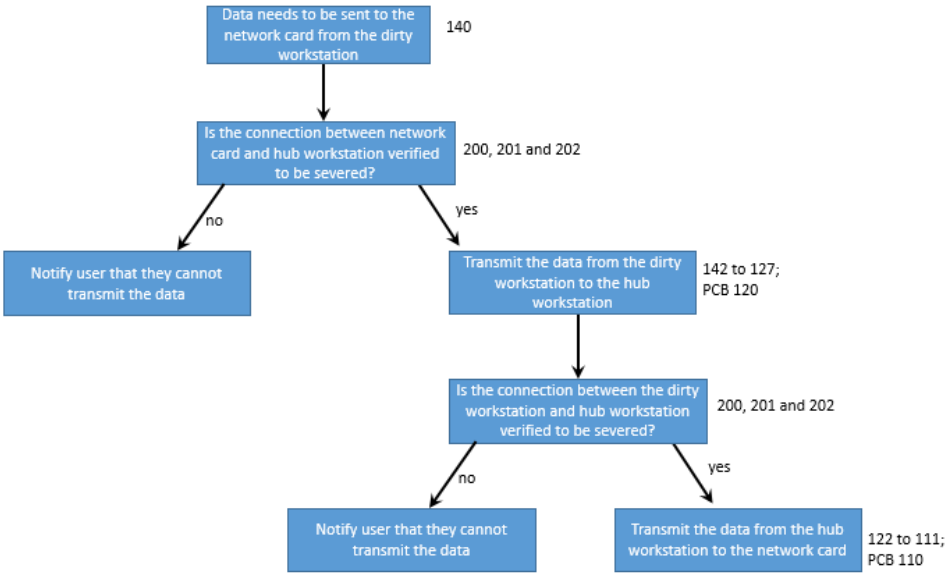

Figure 3: Process flow for data transmission from the dirt workstation 140 to an external network

Still referring to **Figure 3,** the user must now switch the shutter system **201** so that the network card **110** can communicate with the hub workstation **120**, but the hub workstation **120** cannot communicate with the dirty workstation **140.** If shutter system **201** is positioned and verified by the system that the network card **110** can communicate with the hub workstation **120** then the user will be able to complete the transmission of data to external networks. If the shutter system **201** is positioned and verified that the network card **110** cannot communicate with the hub workstation **120** then the user will receive a notification informing them that there is no communication path to external networks.

Referring to **Figure 4**, any data created on the clean workstation **130**, is completely secure from external networks due to the uni-directional nature of the communication hardware **132** and **123** as described in **Figure** 1. If the user must transmit any secure data from the clean workstation **130**, the first action is for the user to initiate a request to transmit data to an external network. The

user will be able to complete this task pending the position of the manually controlled interlocked shutter system **201**. The user must first switch the position of the shutter system **201**, so that the network card **110** cannot communicate with the hub workstation **120,** and subsequently, the system must verify that the shutter system **201** is in the correct position. If this is not verified to be true, the user will receive a notification informing them that data cannot be transmitted to the hub workstation **120**. If the shutter system **201** is verified to be in the correct position (as described above), then the user will be allowed to transmit data to the hub workstation **120.**

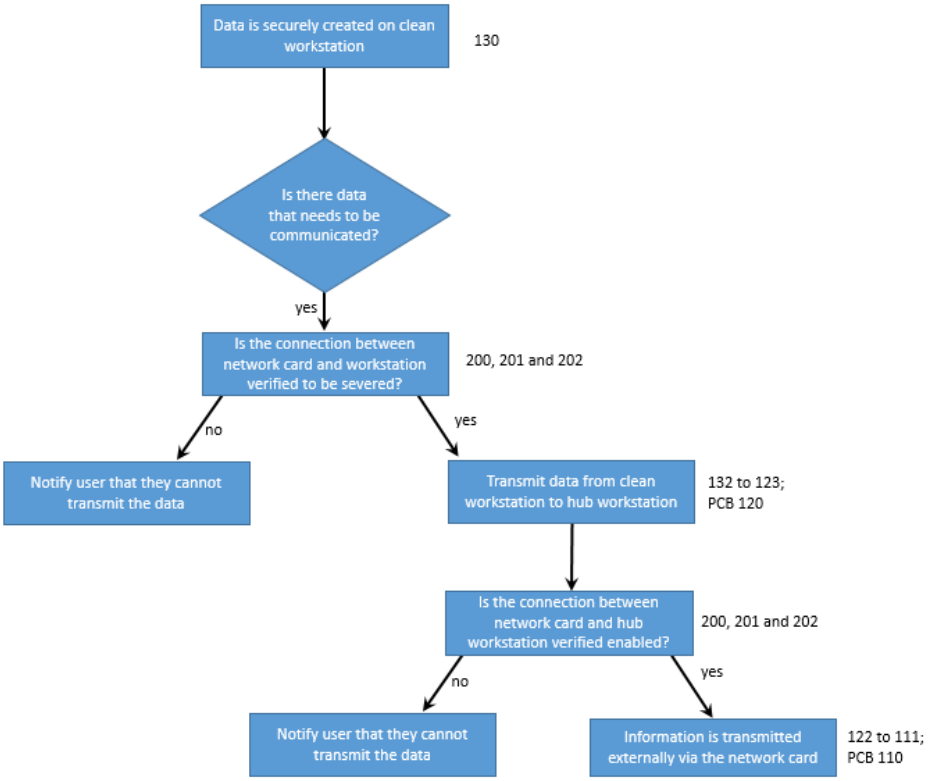

Figure 4: Process flow for data transmission from the clean workstation 130 to an external network

Still referring to **Figure 4**, the user must now switch the shutter system **201** so that the network card **110** can communicate with the hub workstation **120**, but the hub workstation **120** cannot communicate with the dirty workstation **140.** If shutter system **201** is positioned and verified by the system that the network card **110** can communicate with the hub workstation **120** then the user will be able to complete the transmission of data to external networks. If the shutter system **201** is positioned and verified that the network card **110** cannot communicate with the hub workstation **120** then the user will receive a notification informing them that there is no communication path to external networks.

Referring to **Figure** 5, the safe repository **150** holds any necessary registry, OS or other data required for completely reformatting and reconstituting the hub workstation **120.** The safe repository **150** is completely secure from external networks due to the uni-directional nature of the communication hardware **152** and **125** as described in **Figure** 1. First, a periodic time to push the secure registry/OS data onto the hub workstation **120** must be established. The periodic time in the preferred embodiment of this invention is envisioned to be, but is not limited to, once

every 24 hours. In addition, a time delay for initiation of the scrub should be established. The time delay resides on the safe repository and is not accessible by the user. The time delay in the preferred embodiment of this invention is envisioned to be, but is not limited to, 2 minutes.

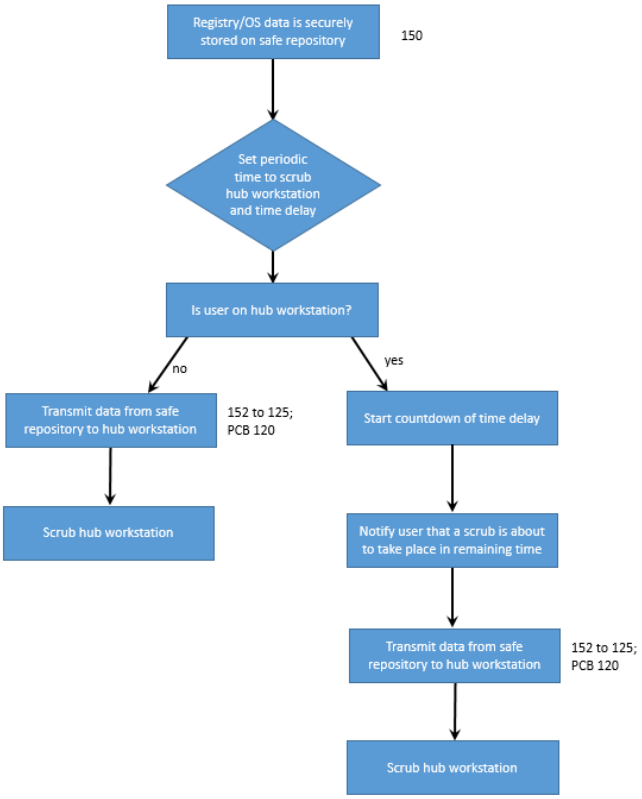

Figure 5: Process flow for scrub of hub workstation 120 and transmission of secure registry/OS from the secure repository 150

Still referring to **Figure** 5**,** prior to pushing the registry/OS data, the system should verify if any users are presently using the hub workstation **120**. If it is verified that no users are present, then the registry/OS data will be transmitted from the safe repository **150** to the hub workstation **120**. The complete wipe and rebuild of the hub workstation will then take place. If a user is verified to be using the hub workstation **120**, then the delay clock begins counting down and a notification is sent to the user informing them of the imminent reformatting, along with the remaining time on the countdown clock. When time expires on the clock, the user loses all access to the hub workstation **120**. The registry/OS data will then be transmitted from the safe repository **150** to the hub workstation **120**. The complete wipe and rebuild of the hub workstation **120** will then take place.

Referring to **Figure** 6, the basic components can be arranged as shown. The preferred embodiment of this invention is envisioned to be, but is not limited to, PCBs mounted in a standard PC desktop configuration. The preferred embodiment is meant to demonstrate a method for air-gaping mission critical components used for processing, read/write, and storage from a direct connection to outside networks. The preferred embodiment demonstrates a method for mitigating the unwanted access and exfiltration of secure data, minimizing/mitigating the damage of executed

malicious code, and prohibiting executed malicious code from communicating back to the threat actor. This method will have applications that scale up from the preferred embodiment, such as server racks and rooms, as well as applications that are scaled down from the preferred embodiment, such as portable electronic devices.

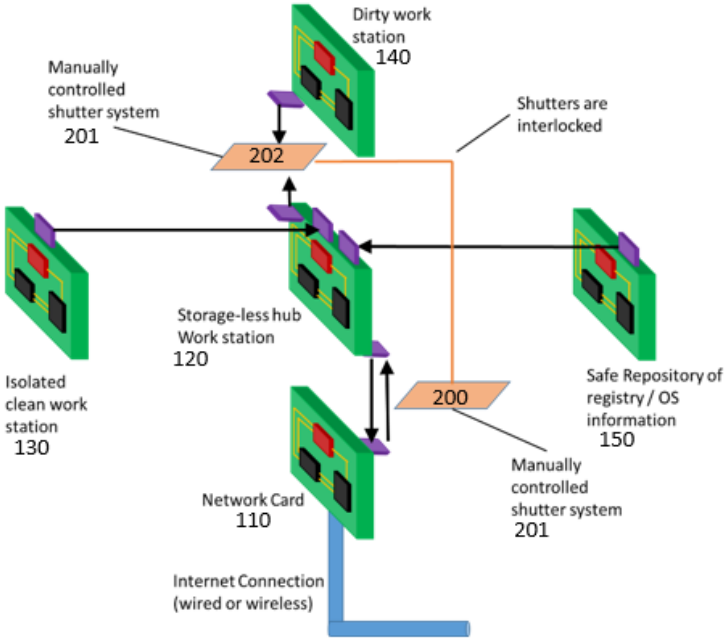

Figure 6: Proposed novel security architecture

4.2. ReRam material study

Memristor Samples were ordered in November 2015, however, the first samples were delivered for measurement in September of 2016. These were HfO2 memristor devices and were the only samples to be characterized for inclusion in this report.

Figure 7 shows the top down view of the single device geometry and range of sizes of the HfO2 devices. In addition, the bottom figure depicts the growth structure from a side view of the devices. This is the generalized structure for all the different lateral geometries shown above it.

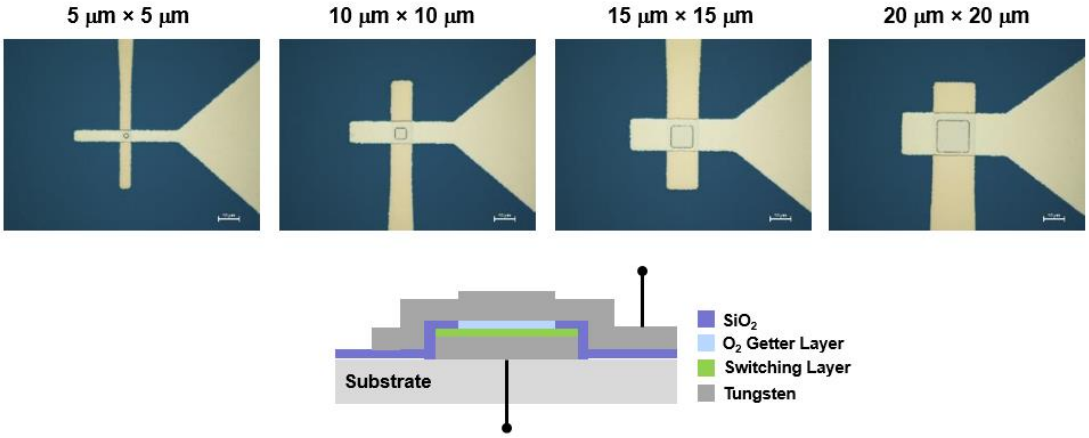

Figure 7: HfO2 memristor device sizes (top) and growth structure (bottom)

Figure 8 shows the results of pulsed voltage measurements of a 15 um x 15 um HfO2 device. The resistance is shown as a function of variable temperature, where the temperature was cycled between room temperature and increasing high temperature measurements. The low resistance (LRS) and high resistance (HRS) states of the device is shown to be stable both at high temperature and during high temperature cycling. In addition, the one to two orders of magnitude difference between the LRS and HRS remains stable through temperature cycling up to 125°C. At 150°C the spread between LRS and HRS decreases, but still remains large enough for two distinct resistance states to be present.

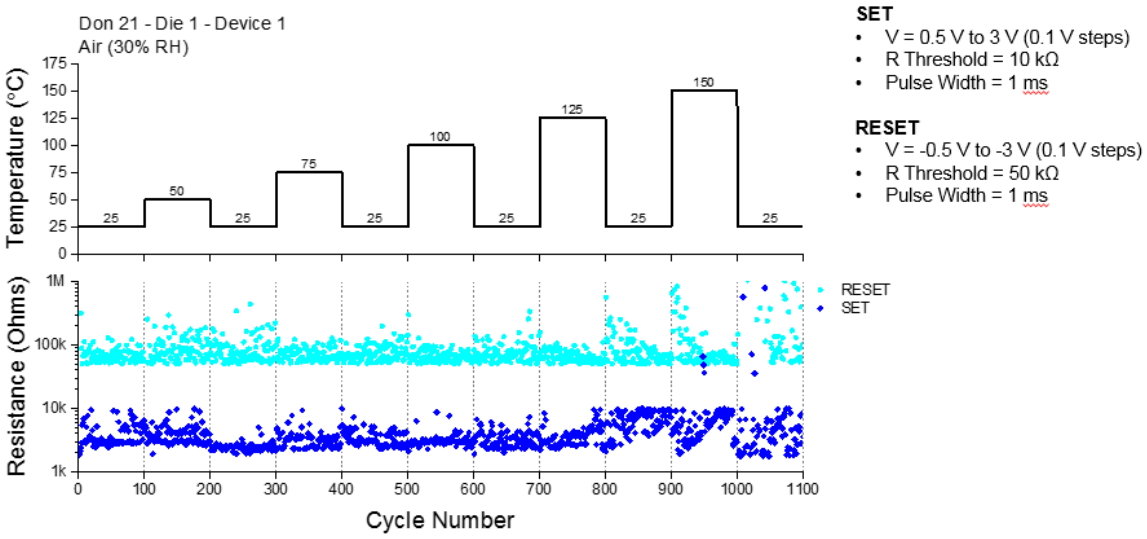

Figure 8: Resistance values from pulsed voltage measurements as a function of temperature cycling

Figure 9 and **Figure 10** show resistance values from two different HfO2 samples, Device 2 and Device 6, from pulsed voltage measurements as function of increasing temperature. Both data sets show the LRS and HRS states of these devices are stable as a function of increasing temperature. In addition, the one to two orders of magnitude difference between the LRS and HRS remains stable through increasing temperature up to 15°C. The small dissimilarities and fluctuations differing between the two data sets are interpreted as being a result of the manufacturing variations between devices.

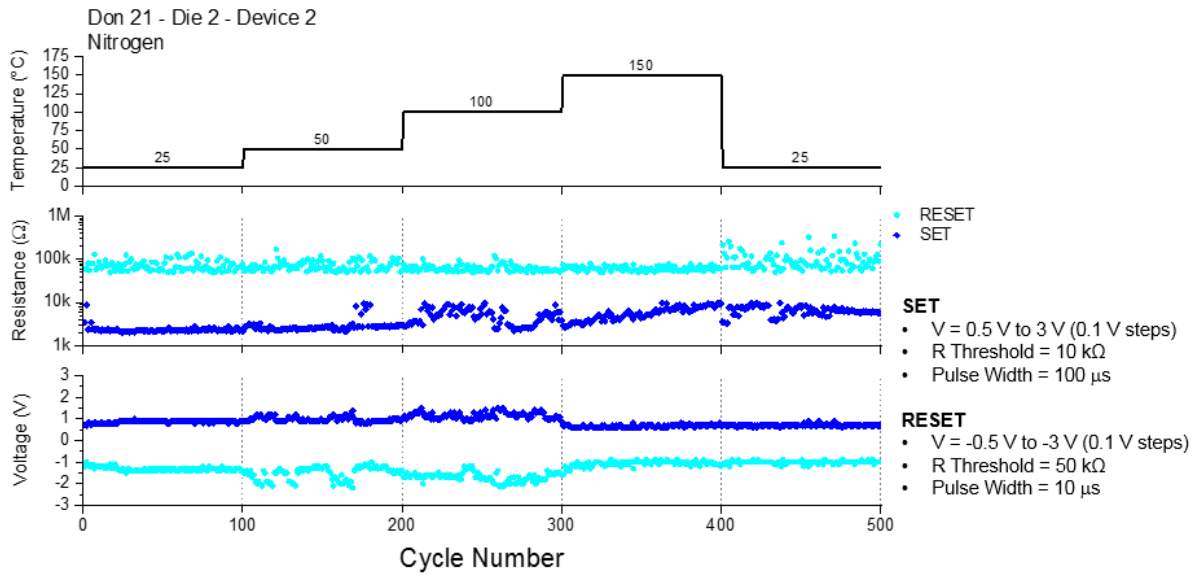

Figure 9: Resistance values of Device 2 from pulsed voltage measurements as a function of increasing temperature

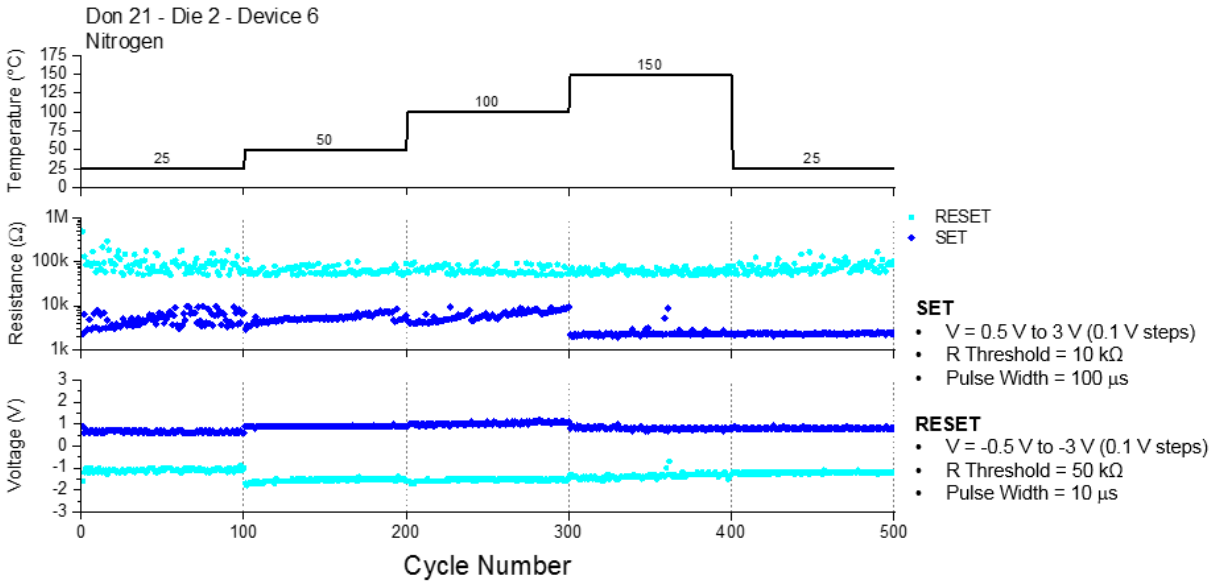

Figure 10: Resistance values of Device 6 from pulsed voltage measurements as a function of increasing temperature

5. CONCLUSION

5.1. Free Space Optical Data Transmission for Secure Computing

Use of VCSELs for board to board free space optical data transmission was determined to be a novel invention, as determined by the US Patent office. However, due to a lack of funding, a concept demo was never able to be built and this remains an untested idea.

5.2. Entropy Sources in Metal Oxide Memristive Devices for use in Security Primitives

This project underwent three changes in management before being assigned to Dr. Telesca. He spent the remainder of FY 15 familiarizing himself with the original proposal and after assessing his strengths, determined that he would not be successful at completing the stated research objectives. He reformulated the technical work to suit his background and stay within the framework of the original proposal. The purchase of a variable temperature probe station was required in order to accomplish said goals and was the defining budgetary and time consuming event of the remainder of FY15.

5.3. ReRam material study

Unforeseen difficulties related to the reliable, robust and reproducible fabrication of the more exotic oxide memristor devices discussed in 3.3 resulted in an extremely large schedule slip. As a result, the reminder of the proposed work was deemed not worth pursuing.

6. REFERNCES

[1] Department of Defense DoD Directive 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, July 2010, available at: *http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf*.

[2] Department of Defense Instruction (DoDI) 8500.01E, *DoD Policy and Responsibilities for Critical Infrastructure*, July 2010, available at: *http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf*.

[3] http://www.freespaceoptics.org/

[4] Juarez, J.C.; Dwivedi, A.; Hammons, A.R.; Jones, S.D.; Weerackody, V.; Nichols, R.A. Communications Magazine, IEEE, Issue Date: November 2006, 46 -51.

[5] Jian Wang, Jeng-Yuan Yang, Irfan M. Fazal, Nisar Ahmed,Yan Yan, Hao Huang, Yongxiong Ren, Yang Yue, Samuel Dolinar, Moshe Tur & Alan E. Willner, Nature Photonics 6, 488–496 (2012)

[6] M.-J. Lee, C. B. Lee, D. Lee, S. R. Lee, M. Chang, J. H. Hur, Y.-B. Kim, C.-J. Kim, D. H. Seo, S. Seo, U.-I. Chung, I.-K. Yoo, and K. Kim, "A fast, high-endurance and scalable non-volatile memory device made from asymmetric Ta2O(5-x)/TaO(2-x) bilayer structures.," Nat. Mater., vol. 10, no. 8, pp. 625–630, 2011.

[7] S. Deora, G. Bersuker, M. G. Sung, D. C. Gilmer, P. D. Kirsch, H. Chong, and S. Gausepohl, "Statistical assessment of endurance degradation in high and low resistive states of the HfO2-based RRAM," IEEE Int. Reliab. Phys. Symp., p. MY.2.1 – MY.2.5, 2013.

[8] F. Pan, S. Gao, C. Chen, C. Song, and F. Zeng, "Recent progress in resistive random access memories: Materials, switching mechanisms, and performance," Mater. Sci. Eng. R Reports, vol. 83, pp. 1–59, 2014.

[9] L. Chen, W. Yang, Y. Li, Q.-Q. Sun, P. Zhou, H.-L. Lu, S.-J. Ding, and D. W. Zhang, "Resistive switching properties of plasma enhanced-ALD La2O3 for novel nonvolatile memory application," J. Vac. Sci. Technol. A Vacuum, Surfaces, Film., vol. 30, no. 1, p. 01A148, Dec. 2012.

[10] H. Zhao, H. Tu, F. Wei, Z. Shi, Y. Xiong, Y. Zhang, and J. Du, "High mechanical endurance RRAM based on amorphous gadolinium oxide for flexible nonvolatile memory application," J. Phys. D. Appl. Phys., vol. 48, no. 20, p. 205104, May 2015.

[11] S. Mondal, H.-Y. Chen, J.-L. Her, F.-H. Ko, and T.-M. Pan, "Effect of Ti doping concentration on resistive switching behaviors of Yb2O3 memory cell," Appl. Phys. Lett., vol. 101, no. 8, p. 083506, Aug. 2012.

[12] S.-Y. Wang, C.-H. Tsai, D.-Y. Lee, C.-Y. Lin, C.-C. Lin, and T.-Y. Tseng, "Improved resistive switching properties of Ti/ZrO2/Pt memory devices for RRAM application," Microelectron. Eng., vol. 88, no. 7, pp. 1628–1632, Jul. 2011.