REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
31-08-2022	Final Report	9-May-2016 - 8-May-2017

4. TITLE AND SUBTITLE
Final Report: Research Instrumentation for Advanced Hardware Reverse Engineering and Integrated Circuit Imaging

5a. CONTRACT NUMBER
W911NF-16-1-0301

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
New York University
665 Broadway
Suite 801
New York, NY 10012 -2331

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
68558-NS-RIP.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Siddharth Garg
UU	UU	UU	UU		19b. TELEPHONE NUMBER 646-997-3656

RPPR Final Report
as of 15-Dec-2022

Agency Code: 21XD

Proposal Number: 68558NSRIP **Agreement Number: W911NF-16-1-0301**
INVESTIGATOR(S):

Name: Davood Shahrjerdi
Email: davood@nyu.edu
Phone Number: 7182604140
Principal: N

Name: PhD Ramesh Karri
Email: rkarri@nyu.edu
Phone Number: 6469973596
Principal: N

Name: Siddharth Garg
Email: sg175@nyu.edu
Phone Number: 6469973656
Principal: Y

Organization: **New York University**
Address: 665 Broadway, New York, NY 100122331
Country: USA

DUNS Number: 041968306 EIN: 135562308
Report Date: 08-Aug-2017 Date Received: 31-Aug-2022
Final Report for Period Beginning 09-May-2016 and Ending 08-May-2017
Title: Research Instrumentation for Advanced Hardware Reverse Engineering and Integrated Circuit Imaging
Begin Performance Period: 09-May-2016 **End Performance Period:** 08-May-2017
Report Term: 0-Other

Submitted By: PhD Ramesh Karri Email: rkarri@nyu.edu
Phone: (646) 997-3596

STEM Degrees: **STEM Participants:**

Major Goals: The requested equipment will form the centerpiece of the hardware reverse engineering laboratory at NYU and used to study several aspects of this emerging and critical threat model. It will contribute towards two broad research efforts that are already underway at NYU. These are:

1. IC camouflaging, an approach used to defend against attackers who try to extract the IC logic details using optical microscopy. Recently, in response to a call from DARPA, we have been investigated camouflaged cells whose functionality is doping concentration dependent. The security of our solution is intrinsically linked to the attackers' ability to extract doping concentrations using SCM or SSRM. However, this question is poorly addressed in literature and is the second motivation behind our request for the equipment.

2. IoT Security: Next generation devices, particularly those used in energy constrained environments are likely to use different types of non-volatile memory solutions. The data stored in these memories will include secret keys, biometrics, and other proprietary information. Can the data on these memories be extracted even if, for security reasons, the JTAG port and other access ports are protected? If so, what are the implications for security and forensics? And finally, if it is possible to extract secret bits based on microscopy, what can we do to defend against such attacks. To answer this final question, we need to have a good understanding of the attackers' capabilities.

Accomplishments: Described in the uploaded pdf file.

Training Opportunities: Nothing to Report

RPPR Final Report
as of 15-Dec-2022

Results Dissemination: 1- A. Alharbi, D. Shahrjerdi, “Analyzing the Effect of High-k DielectricMediated Doping on Contact Resistance in Top-Gated Monolayer MoS2 Transistors,” IEEE Transactions on Electron Devices, 65, pp. 4048-4092 (2018) - Invited contribution to the special issue on 2D Materials.

2- A. Alharbi, D. Armstrong, S. Alharbi, D. Shahrjerdi, “Physically Unclonable Cryptographic Primitives by Chemical Vapor Deposition of Layered MoS2,” ACS Nano, 11, pp. 12772-12779 (2017) Research highlight in Nature Nanotechnology.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Siddharth Garg
Signature Date: 8/31/22 4:39PM

Abstract and Objectives

The requested equipment will form the centerpiece of the hardware reverse engineering laboratory at NYU and used to study several aspects of this emerging and critical threat model. It will contribute towards two broad research efforts that are already underway at NYU. These are:

1. IC camouflaging, an approach used to defend against attackers who try to extract the IC logic details using optical microscopy. Recently, in response to a call from DARPA, we have been investigated camouflaged cells whose functionality is doping concentration dependent. The security of our solution is intrinsically linked to the attackers' ability to extract doping concentrations using SCM or SSRM. However, this question is poorly addressed in literature and is the second motivation behind our request for the equipment.
2. IoT Security: Next generation devices, particularly those used in energy constrained environments are likely to use different types of non-volatile memory solutions. The data stored in these memories will include secret keys, biometrics, and other proprietary information. Can the data on these memories be extracted even if, for security reasons, the JTAG port and other access ports are protected? If so, what are the implications for security and forensics? And finally, if it is possible to extract secret bits based on microscopy, what can we do to defend against such attacks. To answer this final question, we need to have a good understanding of the attackers' capabilities.

Findings

The experimental capabilities through this DURIP enabled the study of emerging two-dimensional (2D) materials and devices and their applications for hardware security. Below is a summary of two main findings enabled by this DURIP grant.

Project 1. Physically Unclonable Cryptographic Primitives by Chemical Vapor Deposition of Layered MoS_2

Physically unclonable cryptographic primitives are promising for securing the rapidly growing number of electronic devices. In this project, we introduced physically unclonable primitives from layered molybdenum disulfide (MoS_2) by leveraging the natural randomness of their island growth during chemical vapor deposition (CVD). We synthesized a MoS_2 monolayer film covered with speckles of multilayer islands, where the growth process is engineered for an optimal speckle density. Using the Clark−Evans test, we confirmed that the distribution of islands on the film exhibits complete spatial randomness, hence indicating the growth of multilayer speckles is a spatial Poisson process. Such a property is highly desirable for constructing unpredictable cryptographic primitives. The security primitive is an array of 2048 pixels fabricated from this film. The complex structure of the pixels makes the physical duplication of the array impossible (i.e., physically unclonable). A unique optical response is generated by applying an optical stimulus to the structure. The basis for this

unique response is the dependence of the photoemission on the number of MoS_2 layers, which by design is random throughout the film. Using a threshold value for the photoemission, we converted the optical response into binary cryptographic keys. We showed that the proper selection of this threshold is crucial for maximizing combination randomness and that the optimal value of the threshold is linked directly to the growth process. This study reveals an opportunity for generating robust and versatile security primitives from layered transition metal dichalcogenides.

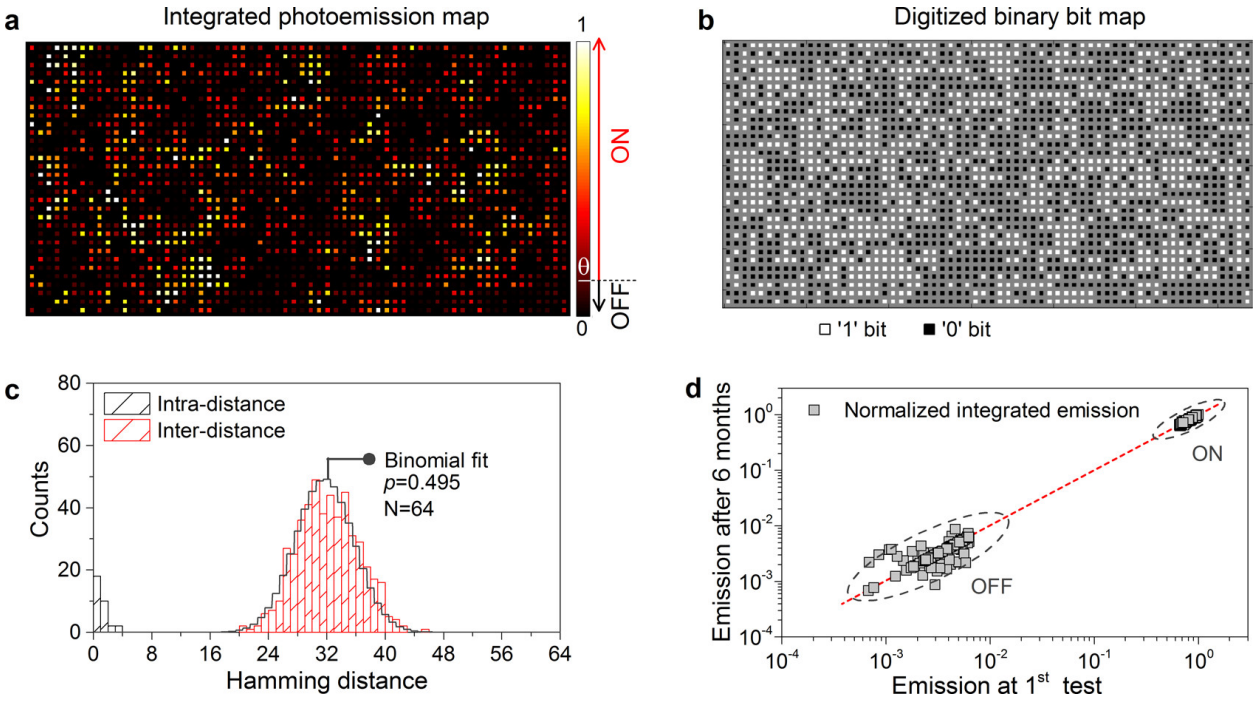

Fig. 1. Optical response and security metrics of the MoS_2 primitive: (a) Stimulating the 2D MoS_2 array with a laser light produces an optical response that is unique to this primitive. (b) The photoemission spatial map was converted to a 2D binary array by comparing each pixel with the ON/OFF threshold. (c) Standard security tests confirm uniqueness and repeatability of the security keys. (d) By studying the aging properties of the photoemission for multiple MoS_2 pixels, we confirm that the MoS2 primitives are highly stable. The red dashed line is guide to the eye and has a slope of 1.

Project 2. Analyzing the Effect of High-k Dielectric-Mediated Doping on Contact Resistance in Top-Gated Monolayer MoS_2 Transistors

A scalable process that can yield low resistance contacts to transition metal dichalcogenides is crucial for realizing a viable device technology from these materials. In this project, we systematically examined the effect of high-k dielectric-mediated doping on key device metrics including contact resistance and carrier mobility. Specifically, we used top-gated transistors from monolayer MoS_2 as a test vehicle and varied the MoS_2 doping level by adjusting the amount of oxygen vacancies in the HfO_x gate dielectric. To understand the effect of doping on the contact resistance, from a fundamental standpoint, we first estimated the doping level in monolayer MoS_2. The

results of our device studies quantitatively showed that the reduction in contact resistance with an increase in doping is due to the doping-induced lowering of the Schottky barrier height (SBH) at the metal–semiconductor interface. Furthermore, our temperature dependent measurements revealed that a mixture of thermionic and field emissions, even at high carrier densities, dominates carrier conduction at the contact. While our study revealed the effectiveness of dielectric-induced doping in lowering SBH, it suggested that a further reduction of SBH using alternative methods is necessary for achieving an ohmic-like contact to monolayer MoS_2.

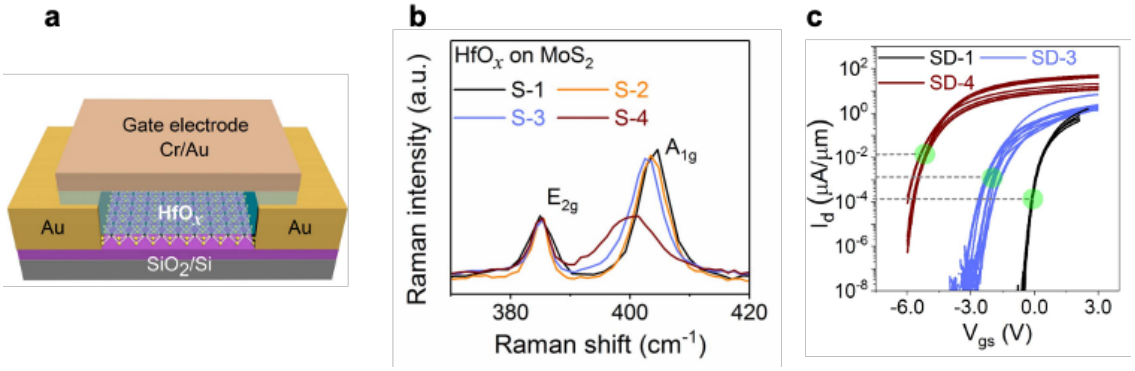

Fig. 2. High-k mediated doping for contact engineering. (a) Schematic illustration of a top-gated MoS_2 transistor. By varying the stoichiometric oxygen content of the HfO_x gate dielectric, we produced device samples with different doping levels. (b) Raman spectroscopy was used for estimating the high-k induced doping in MoS_2. S-1 had the lowest doping level and S-4 the highest. (c) Electrical measurements of the devices with different doping levels.