The Pennsylvania State University

The Graduate School

LOGIC LOCKING OF INTEGRATED CIRCUITS ENABLED BY 2D MATERIALS BASED MEMTRANSISTORS

A Thesis in

Electrical Engineering

by

Shakya Chakrabarti

© 2022 Shakya Chakrabarti

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Master of Science

December 2022

The thesis of Shakya Chakrabarti was reviewed and approved by the following:

Saptarshi Das
Associate Professor of Engineering Science and Mechanics
Thesis Advisor

Abhronil Sengupta
Joseph and Janice M. Monkowski Career Development Assistant Professor
School of Electrical Engineering and Computer Science

Rongming Chu
Associate Professor of Electrical Engineering and Computer Science

Thomas La Porta
Evan Pugh Professor, William E. Leonhard Endowed Chair and Director of EECS
Head of Electrical Engineering Department

ABSTRACT

Ever since the advent of two-dimensional (2D) van der Waals (vdW) layered materials, the likes of graphene, hexagonal boron nitride (h-BN) and the semiconducting family of transition metal dichalcogenides (TMDCs), have received immense attention as an alternative platform to sustain Moore's Law and promote post-Silicon electronics. Notably, TMDCs have captured significant interest, and have been intensely investigated on, as they exhibit novel electronic, optical, mechanical, electrochemical and physical properties. Compelled by the quest of developing low power and high-performance devices for electronics industry, 2D-field effect transistors (FETs) and logic designs with impressive performances were demonstrated. Subsequently, these 2D-based devices were successfully employed in developing impressive analog, digital, memory, sensing and neuromorphic applications.

Yet another domain that has become increasingly important in today's data driven world is hardware security. The emergence of a globalized semiconductor manufacturing model has raised serious concerns involving security and trust of the information systems on which the modern-day society has become increasingly reliant. Threats such as intellectual property (IP) piracy, reverse engineering, IP overbuilding and counterfeiting have crept into this supply chain and compromised the security of these hardware components. Logic Locking (LL) can mitigate these threats by locking a given IC with a secret key. The chip can then only be unlocked if an adversary has prior knowledge of the correct key sequence.

In this work, we demonstrate MoS_2 based two-dimensional (2D) memtransistors as in-memory compute primitives to realize LL in 2D Integrated Circuits (ICs) comprising of programmable logic gates the likes of AND, $NAND$, OR, XOR, and NOT gates. The 2D memtransistors are three-terminal devices unlike the two-terminal memristor counterparts; thus, having an additional gate terminal providing both non-volatile and analog programming of conductance states along with electrostatic control of the 2D channel. Earlier demonstrations of LL based on traditional silicon complementary metal oxide semiconductor (CMOS) technology as well as emerging memristors require extensive hardware peripherals and additional input gates, creating a logical overhead making them area as well as energy inefficient. By harnessing the in-memory compute capability, demonstration of LL on the aforementioned logic gates have been performed, which can be locked/unlocked without any additional area overheads and at a miniscule energy expenditure of < 1 picojoules. It must be noted that in recent years, other hardware security solutions such as camouflaging, true random number generators (TRNG), physically unclonable functions (PUFs), watermarking, and anticounterfeiting based on 2D-materials have also been successfully demonstrated.

With the increasing attention of chip manufacturing corporations to replace and/or augment silicon with aggressive scaling in lower technology process nodes, our demonstration of area and energy efficient LL illustrates how such secure ICs can be implemented by enabling the unique properties of the 2D memtransistors.

TABLE OF CONTENTS

LIST OF FIGURES v

LIST OF TABLES vii

ACKNOWLEDGEMENTS viii

Chapter 1 Introduction 1

1.1 Introduction 1
1.2 Two-dimensional materials as post-Silicon alternatives 2
1.3 Application of Two-dimensional materials in Integrated Circuits (ICs) 3

Chapter 2 Hardware Security 5

2.1 Introduction 5
2.2 Logic Locking 6
2.3 Motivation behind the thesis 7
2.4 Objective of the thesis 7

Chapter 3 Logic Locking using 2D-material-based memtransistors 9

3.1 Characterization of monolayer MoS_2-based 2D memtransistors 9
3.2 Programmability in MoS_2 memtransistors 11
3.3 Logic locking in 2D-memtransistor-based logic families 13
3.4 Endurance and retention of MoS_2 memtransistors 19

Chapter 4 Benchmarking Results 21

Chapter 5 Conclusion and Future Work 23

5.1 Conclusion 23
5.2 Future Work 24

Bibliography 25

LIST OF FIGURES

Figure **1**: Atomic arrangement of transition metal dichalcogenide materials. Each layer is covalently bonded while interlayer bond is Van der Waals bond..2

Figure **2**: (a) Raman spectra and (b) photoluminescence (PL) spectra of a representative MoS_2 channel using a 532 nm laser. (c) A 3D schematic and (d) optical image of monolayer MoS_2 based 2D memtransistor with a local back-gate stack comprising of atomic layer deposition (ALD) grown 50 nm Al_2O_3 with a 40/30 nm Pt/TiN deposited using sputtering on SiO_2/p^{++}-Si substrate. Transfer characteristics, i.e., source to drain current (I_{DS}) versus back-gate voltage (V_{BG}) for different drain to source bias (V_{DS}) in (e) logarithmic and (f) linear scale, respectively for a representative MoS_2 memtransistor with a channel length of 1μm and a channel width of 5 μm. (g) Mobility versus V_{BG} extracted using the peak transconductance method. (h) Output characteristics, i.e., I_{DS} versus V_{DS} for different V_{BG} for the same MoS_2 memtransistor..9

Figure **3(a-b)**: Programmability in MoS_2 memtransistors (a) programming and (b) erase operations in a representative 2D memtransistor when subjected to negative "Write" (V_P) and positive "Erase" (V_E) voltage pulses of different magnitudes ranging from 7V to 15V that are applied to the local back gate. Pulse widths were fixed for a duration of 100ms. 11

Figure **3(c-d)**: Respective shifts in the threshold voltages (V_{TH}) is attributed to the carrier de-trapping/ trapping at the MoS_2 and the local gate stack interface. Non-volatile retention for 4 representative (c) programmed and (d) erased states are shown for a duration of 100 seconds. 11

Figure **4**: Band diagrams explaining the underlying mechanism of charge trapping and de-trapping in our MoS_2 memtransistor. 12

Figure **5**: Demonstration of logic locking in MoS_2 inverter: (a) Optical image and (b) circuit diagram of an inverter consisting of two memtransistors MT_1 and MT_2. Note that MT_1 operates in depletion mode (the gate is shorted to the source) whereas MT_2 operates in enhancement mode. (c) Baseline transfer characteristics of MT_2 and (d) corresponding output characteristics of an inverter showing normal operation where the V_{OUT} represents the opposite logic of the V_{IN}. (e) Transfer characteristics of MT_2 post application of a program pulse of -12V and (f) corresponding locked inverter output where V_{OUT} is clamped to V_{GND}.. 13

Figure **6**: Demonstration of logic locking for 2D memtransistor-based AND, NAND and OR gates: (a-c) Optical images and (d-f) corresponding circuit diagram of AND, NAND and OR gates comprising of three monolithic integrated MoS_2 memtransistors, MT_1, MT_2 and MT_3. Output characteristics for the respective logic functionalities under (g-i) normal (unlocked) and (j-l) locked operations... 15

Figure **7**: Transfer characteristics of enhancement-mode MT_1 for a AND gate (a) before and (b) after the application of an erase voltage pulse of magnitude of 15V... 16

Figure **8**: Transfer characteristics of MT_1 and MT_2 for a NAND gate (a,c) before and (b,d) after the application of a programming voltage pulse of magnitude -14V... 17

Figure **9**: Transfer characteristics of MT_1 and MT_2 for an OR gate (a,c) before and (b,d) after the application of an erase voltage pulse of magnitude 15V..18

Figure **10**: Demonstration of logic locking for 2D memtransistor-based XOR gate: (a) Optical image and (b) corresponding circuit diagram of XOR gate comprising of 9 monolithic integrated MoS_2 memtransistors. Output characteristics for the XOR logic functionality under (c) normal (unlocked) and (d) locked operations...19

Figure **11**: (a) Retention and (b) Memory ratio plots for a representative memtransistor for a total of 10^4 seconds or ~ 3 hours. Based on the decay observed, we estimate the two memory states will converge after ~ 16 hours c) Endurance plot of a representative memtransistor for a total of 10^3 cycles showing minimal change between the post-programmed V_P = -11V and post-erase V_E = 15V conduction states..20

LIST OF TABLES

Table **1**: Benchmarking 2D-memtransistor based logic locking with existing alternatives 22

ACKNOWLEDGEMENTS

The accomplishment and penultimate outcome of this thesis required significant guidance and assistance from many people.

First, I would like to thank my academic advisor, Prof. Saptarshi Das for the immense guidance and encouragement throughout the entire duration of my graduate studies. I am particularly indebted to him for providing me an opportunity to work in his research group, as well as to get a hands-on exposure on state-of-the-art facilities for semiconductor device research. This thesis would not have been possible without his continuous support and supervision.

I offer my sincerest appreciation to the committee members- Prof. Abhronil Sengupta and Prof. Rongming Chu, to learn a lot of things which in due course of time helped me with my research.

Besides my advisor and committee members, I would like to thank my fellow graduate students- Akshay Wali for co-operation and assistance during the development of this work, Thomas F. Schranghamer for performing the fabrication and characterization of the devices used for this work, and, Dipanjan Sen as well as Satwik Kundu for being a constant pillar of support and keeping me motivated throughout this journey. I would also like to thank all my colleagues from Das Research Group.

I would like to thank the collaborators of this project Prof. Kanad Basu and Shamik Kundu, a graduate student of the group, from the Electrical and Computer Engineering Department at University of Texas at Dallas, for generously offering their time with the SAT-attack simulation model pertaining to this thesis.

I would like to also thank Prof. Joan M. Redwing and Nicholas Trainor a graduate student from the group for growing the materials used in this work.

Finally, I would like to acknowledge The Pennsylvania State University 2D Crystal Consortium-Materials Innovation Platform (2DCCMIP) under NSF cooperative agreement DMR-1539916 for providing the material support for this work. Any opinions, findings, and conclusions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).

Chapter 1

Introduction

1.1 Introduction

The unprecedented success of the semiconductor technology over last several decades can single-handedly be attributed to the landmark invention of transistor by William Shockley and his colleagues in 1947 [1]. From that point onwards, miniaturization of the devices primarily driven by aggressive scaling of conventional silicon-based complementary metal-oxide-semiconductor (CMOS) features became the hallmark of all the successive technological nodes. Popularly known as the Moore's law, this downscaling enabled faster, cheaper and more reliable computational capabilities by exponentially increasing the number of transistors that could be placed within a given chip area. Furthermore, the scaling of supply voltage with the shrinking geometrical dimensions of the planar devices has also ensured the corresponding scaling of power and energy consumption requirements [2]. Introduction of high-*k* dielectrics, different contact metal gates, and strain have also led to significant improvements in transistor performances [3]. However, these technological nodes have witnessed significant hardships in recent years, with stagnation of voltage and dimension scaling due to the fundamental bottlenecks arising from the thermodynamic limitations governed by Boltzmann statistics, and quantum mechanical tunneling at the nanoscale level, respectively [4]. In particular, ensuring good gate electrostatics and device performance beyond 10-nm nodes has become increasingly difficult due to the requirement of aggressive channel length reduction which results in severely degraded mobility as a result of increased charge carrier scattering at the channel-dielectric interface [5]. Therefore, in order to sustain Moore's law

and reinstate the scaling paradigm, new materials and device geometries must be adopted for development of the next generation of ultra-low-power devices and processes technologies [6].

1.2 Two-dimensional materials as post-Silicon alternatives

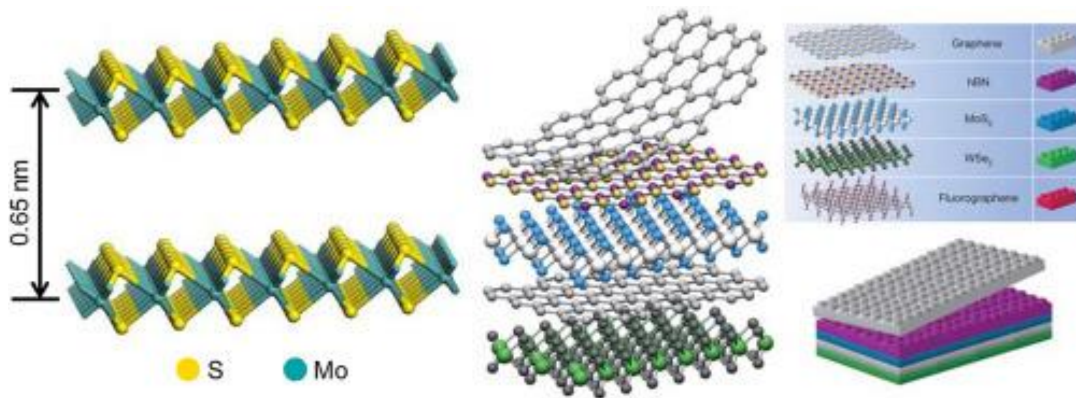

Figure 1: Atomic arrangement of molybdenum disulfide (MoS_2), a two-dimensional (2D) transition metal dichalcogenide (TMDC) material. (Adapted from Ref. [80]).

In this context, low-dimensional materials such as graphene [7-9], semiconducting nanowires [10, 11], nanotubes [12, 13], and more recently, the family of transition metal dichalcogenides (TMDCs) consisting of MoS_2, WSe_2, $MoTe_2$, and WS_2 amongst others have been intensely investigated as an alternative solution to sustain the Moore's law [14-18]. TMDCs, in particular are layered materials with a general formula of MX_2, where M is a transition metal (such as Mo, W, etc.) and X is a chalcogen atom (such as S, Se, Te) [19-24] that exhibit novel electronic, optical and electrochemical properties [25]. With their strong in-plane covalent bonds and weak out-of-plane van der Waals (vdW) interaction [19], TMDCs have emerged as promising candidates for the next generation of low-cost, low-power and area efficient post- CMOS technologies since their ultrathin body (~ 0.7 nm thick) allows aggressive channel scaling, offers superior gate electrostatic control,

and is resilient to the quantum confinement and short channel effects thereby ensuring good device performance [3, 26, 27]. Moreover, better channel-to-dielectric interfaces as a result of the absence of dangling bonds can mitigate the mobility bottleneck as described earlier. The progress of TMDC-based electronics over the past few years has been rather impressive. From earlier realizations of bulk [28, 29] and monolayer [14] based field effect transistors (FETs), to the development of NMOS [30-32] and CMOS [33, 34] based technologies in addition to demonstration of electronic circuits such as microprocessors [35] [6] has been monumental. This has largely been possible due to intensive efforts geared towards the development of growth techniques for large scale fabrication of TMDC films and devices [36-38]. Further discourse on implementation of electronic Integrated Circuits (ICs) using TMDC-based devices have been discussed in the following section.

1.3 Application of Two-dimensional materials in Integrated Circuits

2D-material-based semiconductors have prospective applications in mainstream logic design from analog circuits to more-than-Moore applications [39]. Among the TMDC-family of semi conductive materials, MoS_2 is the most widely studied [40-41]. To date, functional circuitry comprising of 115 MoS_2 field-effect transistors (FETs) fabricated using a gate-first technology have also been reported [42]. Furthermore, ICs based on MoS_2 2D field-effect transistors (2D FETs) have been demonstrated for a plethora of analog, digital, memory, sensing, neuromorphic applications [43-45]. Therefore, the above discussions indicate that commercial application of TMDC-material based 2D technology is quite imminent. For the execution of the former and

making it viable at large-scale, it is of utmost preeminence to mitigate the security threats that these 2D FETs will encounter. The following chapter would delve into the intricacies of how security aspects play a major role in the semiconductor industry, and how hardware security acts as a major pervasive in the businesses involved.

Chapter 2

Hardware Security

Portions of this chapter are reproduced from: Chakrabarti, S., ***et. al.*** *"Logic Locking of Integrated Circuits Enabled by Nanoscale MoS_2 Based Memtransistors."* ***ACS Applied Nano Materials (DOI: 10.1021/acsanm.2c02807).***

2.1 Introduction

The increasing cost and complexity of ICs have spawned an era of fabless semiconductor companies with extensive reliance on globalized and distributed IC design flows [46]. In this highly interconnected yet physically dispersed ecosystem, untrusted parties can easily obtain access to intellectual properties (IPs), giving rise to major security threats such as IP piracy, counterfeiting, and overbuilding [47-49]. As a result, such hardware compromised chips are becoming more pervasive in the semiconductor industry, raising significant concerns for the governments, consumers, and businesses involved [50-52]. As per a report published by the Senate Armed Services Committee, the presence of more than a million counterfeit components in US military defense systems has severely impacted their security and reliability in mission critical applications involving military airplanes, missiles and warfare systems and communications [53]. Furthermore, ICs may be recycled, remarked, reverse engineered or even sold illegally [54]. Additional threats involving trojan insertion and illegal ownership claims over an IP further compound the problem. Therefore, protecting an IC/IP design from potentially unscrupulous groups and above-mentioned attack threats present within the supply chain is of paramount importance. One of the potential panaceas to assuage these security threats is Logic Locking (LL),

which will be discussed in the subsequent section.

2.2 Logic Locking

LL is a potential solution to the above discussed security threats, wherein a circuit design is locked using a secret key. In order to retrieve the correct circuit functionality (correct logical outputs), a valid key must be provided to this locked design, one which is only known to the original designer. While a number of alternative countermeasures such as IC camouflaging [55], split manufacturing [56] and IC metering [57] have also been proposed, LL, in particular has received significant attention from the hardware-security research community due to its versatility in protecting the IP. Conventional literature has implemented LL by introducing additional logic elements such as XOR/XNOR [58] and AND/OR [59] gates into the original design at random locations thus maximizing the hamming distance between the incorrect and correct outputs. Yet another technique involves introducing additional logic (black) states into the state transition graph where only the correct sequence of key-bits derived by an on-chip tamper-proof memory allows the design to operate correctly [60, 61]. Recently, a key destruction scheme based on a Ta/HfO_2 memristive crossbar array was also demonstrated for logic locking/unlocking [62].While promising, nearly all of the above-mentioned approaches employ additional peripheral logic elements which ultimately increases the area overhead and consumes significant amounts of energy. Additionally, most of the proposed schemes have only been simulated, with few experimental demonstrations. In order to keep up with ever-shrinking technological nodes as per the International Technology Roadmap for Semiconductors (ITRS) [63] and continued outsourcing of IC manufacturing to reduce development costs, innovative area and energy efficient security solutions are critical for securing

ICs in this highly globalized and untrustworthy fabrication.

2.3 Motivation behind the thesis

In this regard, TMDC-based materials have been intensely investigated in recent years for a plethora of diverse nanoelectronics applications beyond Moore's law as discussed in detail in Section 1.3. Furthermore, a wide range of security primitives including true random number generators, physically unclonable functions, IC camouflaging, watermarking, and anticounterfeit solutions based on 2D materials and devices [64-68]. However, LL of 2D ICs is yet to be accomplished.

2.4 Objective of the thesis

This work introduces 2D nanoscale memtransistors as in-memory compute primitives for the realization of LL in 2D ICs. Unlike two-terminal memristors, 2D memtransistors are three-terminal devices with the additional gate terminal permitting both non-volatile and analog programming of conductance states and electrostatic control of the 2D channel. By exploiting this in-memory compute capability we were able to demonstrate LL of different logic gates, including NOT, AND, $NAND$, OR and XOR gates, with no additional overhead, thereby offering an efficient hardware security solution to thwart IC piracy and overbuilding. The locking mechanism within these circuits results from the intentional application of a programming or erase pulse $\left(V_{P/E}\right)$ to the local back-gate of our 2D nanoscale memtransistors which shifts the threshold voltage (V_{TH}) and thereby clamp the output of the circuit in either a logic '1' or logic '0' state. The correct functionalities of these locked circuits can then only be recovered when the 2D memtransistor is reset back to its

original baseline state through the application of an opposite polarity of voltage pulse $\left(V_{E/P}\right)$ compared to the one used to originally lock the circuit. We have also provided the background for necessitating innovations at the materials and the device level in light of the bottlenecks imposed by the scaling limitations of the present-day state-of-the-art silicon technologies.

Chapter 3

Logic Locking using 2D-material-based memtransistors

Portions of this chapter are reproduced from: Chakrabarti, S., ***et. al.*** *"Logic Locking of Integrated Circuits Enabled by Nanoscale* MoS_2 *Based Memtransistors."* ***ACS Applied Nano Materials (DOI: 10.1021/acsanm.2c02807).***

3.1 Characterization of monolayer MoS_2-based 2D memtransistors:

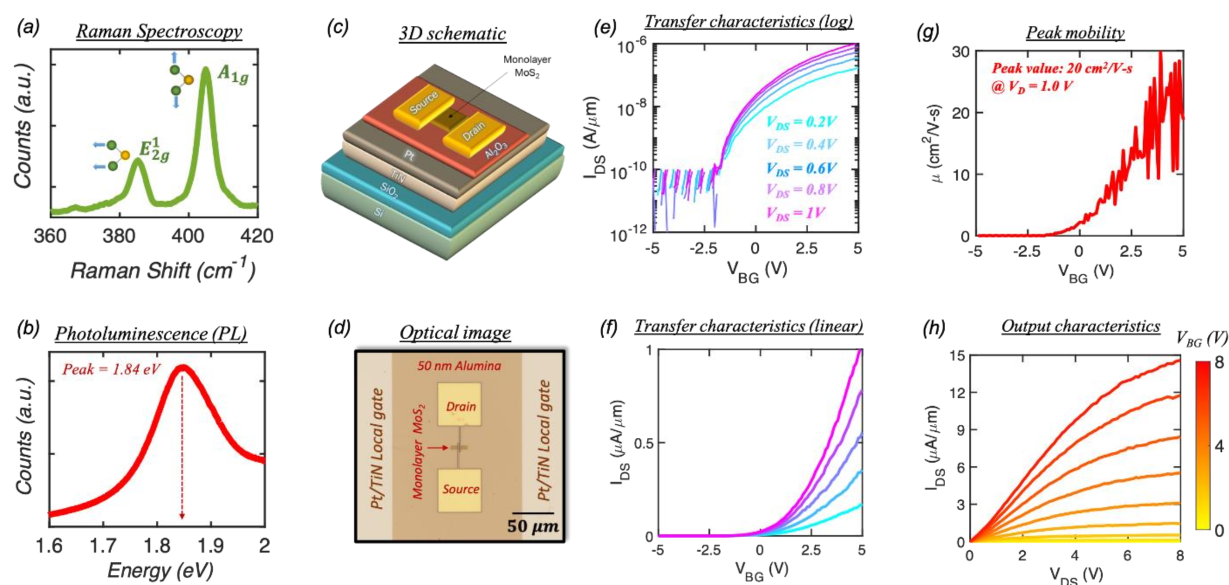

Figure 2: Characterization of MoS_2 2D memtransistors.

MoS_2 is a layered semiconductor from the TMDC family having a general formula of MX_2 where M represents the transition metal (M= Mo, W) and X represents a chalcogen (X=S, Se, Te). With a weak out-of-plane van der Waals (vdW) coupling between successive layers and a strong in-plane bonding within each layer, monolayers can be easily separated from their bulk crystal with

unparalleled electronic properties, thus making them attractive for developing the next-generation of area and energy efficient circuits. While prior studies on TMDCs have been primarily based on exfoliated multilayer and single-crystal flakes, practical realization of high-volume manufacturing of 2D-based dense logic integration technology requires high quality large area growth of these materials. The large area monolayer MoS_2 used in our work was grown on a sapphire substrate at 950 °C via a metal-organic chemical vapor deposition (MOCVD) technique [81]. The use of an epitaxial substrate and elevated growth temperatures allowed for the formation of a uniform, high-quality 2D film, which is critical for ensuring good device performance and low device-to-device variation. Raman and photoluminescence (PL) spectroscopy were used to assess the material quality using a 532 nm laser. **Fig. 2a** shows the Raman spectra of a representative MoS_2 channel. The two characteristic peaks i.e., the in-plane E_{2g}^{1} peak and the out-of-plane A_{1g} peak, were observed at 385 cm^{-1} and 405 cm^{-1}, respectively; the peak separation of ~20 cm^{-1} is characteristic of a monolayer MoS_2 film. Furthermore, as shown in **Fig. 2b**, a PL peak was observed at 1.85 eV; this was attributed to the direct bandgap transition at the K-point in the Brillouin zone in monolayer MoS_2 and is completely subdued in bulk MoS_2.

Fig. 2c-d, respectively, show the 3D schematic and optical image of a representative 2D MoS_2 memtransistor with a channel length (L) of 1 µm and a channel width (W) of 5 µm. **Fig. 2e-f**, respectively, show the transfer characteristics i.e., source to drain current (I_{DS}) as a function of applied back-gate voltage (V_{BG}), of a representative MoS_2 FET measured at different source to drain biases (V_{DS}) in the logarithmic and linear scales. Clearly, n-type dominated carrier transport is observed due to the pinning of the metal Fermi level near the conduction band facilitating

enhanced electron injection; this observation is consistent with our earlier reports [73]. In addition, an excellent ON/OFF current ratio of ~ 10^5 is observed. A threshold voltage (V_{TH}) of ~ 0 V was extracted using linear scale estimation and the field effect mobility (μ_{FE}) in **Fig. 2g** extracted from the peak trans-conductance $\left(g_m = \frac{dI_{DS}}{dV_{BG}}\right)$ was 20 cm^2/V-s. Finally, **Fig. 2h** shows the output characteristics i.e., I_{DS} versus V_{DS} for different V_{BG}. I_{ON} was found to be ~ 15 µA/µm for V_{DS} = 8 V at a V_{BG} = 8 V indicating the superior performance of our 2D memtransistors.

3.2 Programmability in MoS_2 memtransistors

In this section, we demonstrate the ability of our MoS_2 FETs to be programmed to any given desirable conduction state, which is central to our LL scheme, as a result of the application of two

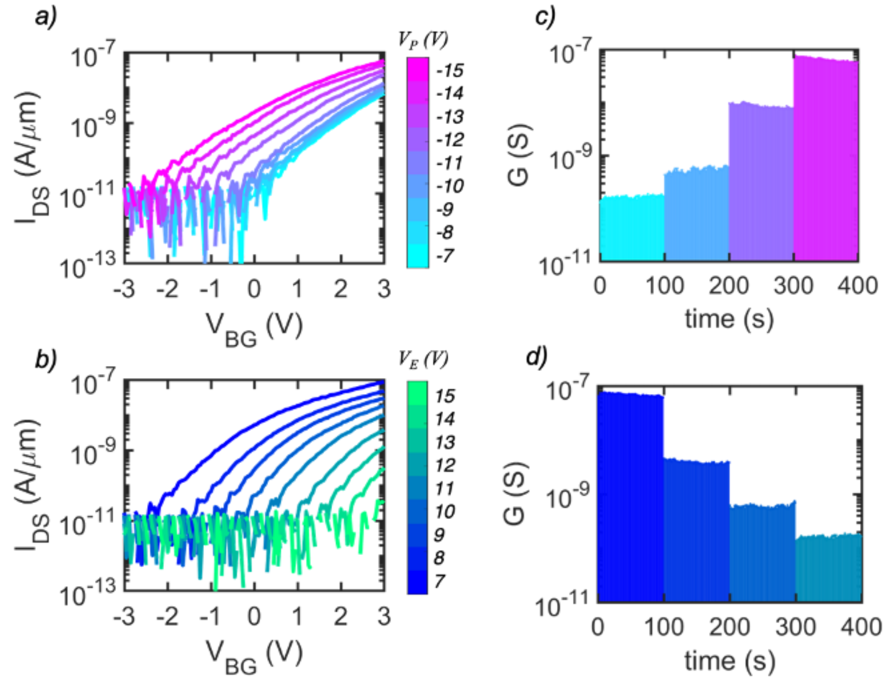

Figure 3: Programmability in MoS_2 2D memtransistors.

types of voltage pulses to the local back-gate: a negative programming pulse (V_P) and a positive erase pulse (V_E). **Fig. 3a-b** show the transfer characteristics of a representative MoS_2 FET following the application of V_P and V_E, respectively, at magnitudes ranging from 7 V

to 15 V and with the same pulse width $(\tau_{P/E})$ of 100 ms. The respective negative and positive shifts observed in the V_{TH} of the memtransistor are the result of charge trapping and de-trapping at and/or near the MoS_2/ Al_2O_3 interface, as has been described in our earlier works [69-74]. Note that the increase in the shift of V_{TH} with increasing magnitude of V_P and V_E is attributed to the greater number of charges getting trapped and detrapped, respectively, at the channel/dielectric interface. Analysis of the stability of the programmed memory states clearly shows the non-volatile retention of our devices, as evident from the plots in **Fig. 3c-d**. Additionally, the

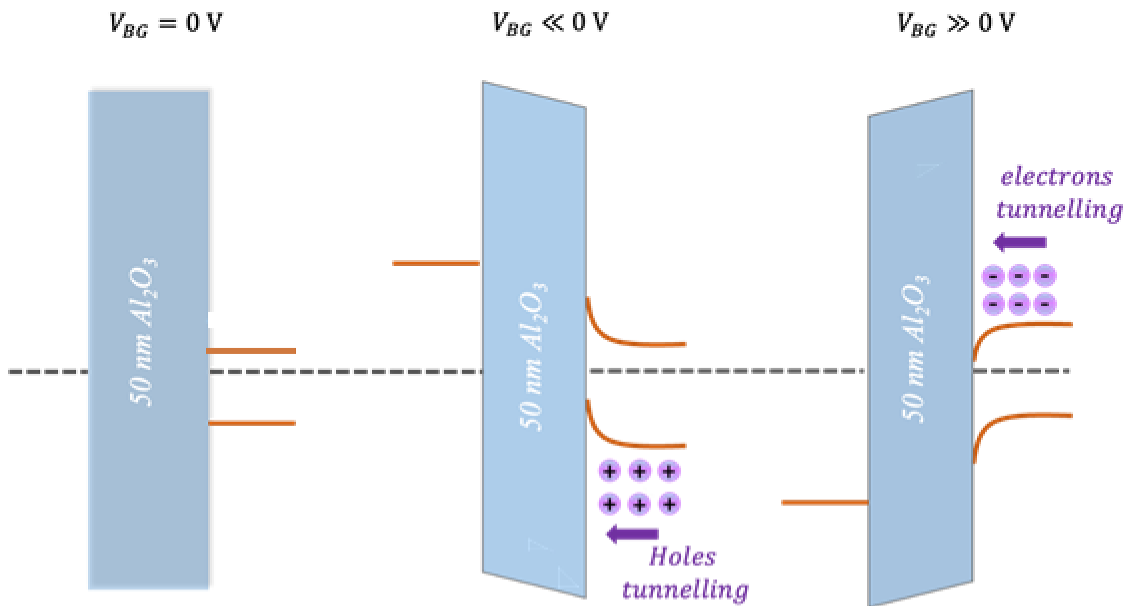

Figure 4: Band diagrams explaining the underlying mechanism of charge trapping and de-trapping in our MoS_2 memtransistors.

programming/erase energy expenditure, calculated based on $E_W = \frac{1}{2} C_g \left(V_{P/E}\right)^2$, where $C_g = {WL\varepsilon_0\varepsilon_{ox}}/{t_{ox}}$ is the gate capacitance, ε_0 = 8.85×10^{-12} F/m is the vacuum permittivity, ε_{ox} = 10 and t_{ox} = 50 nm are the relative dielectric constant and thickness of Al_2O_3 dielectric gate, respectively, was found to be miniscule (<1 picojoule). **Fig. 4.** shows the associated band diagrams explaining the charge trapping and de-trapping process.

3.3 Logic locking in 2D-memtransistor-based logic families

Logic gates are fundamental building blocks of digital integrated circuits (ICs) and play a critical role in modern computing architectures and microprocessors. Here, we successfully integrate MoS_2 memtransistors fabricated on separate local back-gate islands to create five different logical functionalities (inverter, AND gate, $NAND$ gate, OR gate, and XOR gate) and demonstrate their

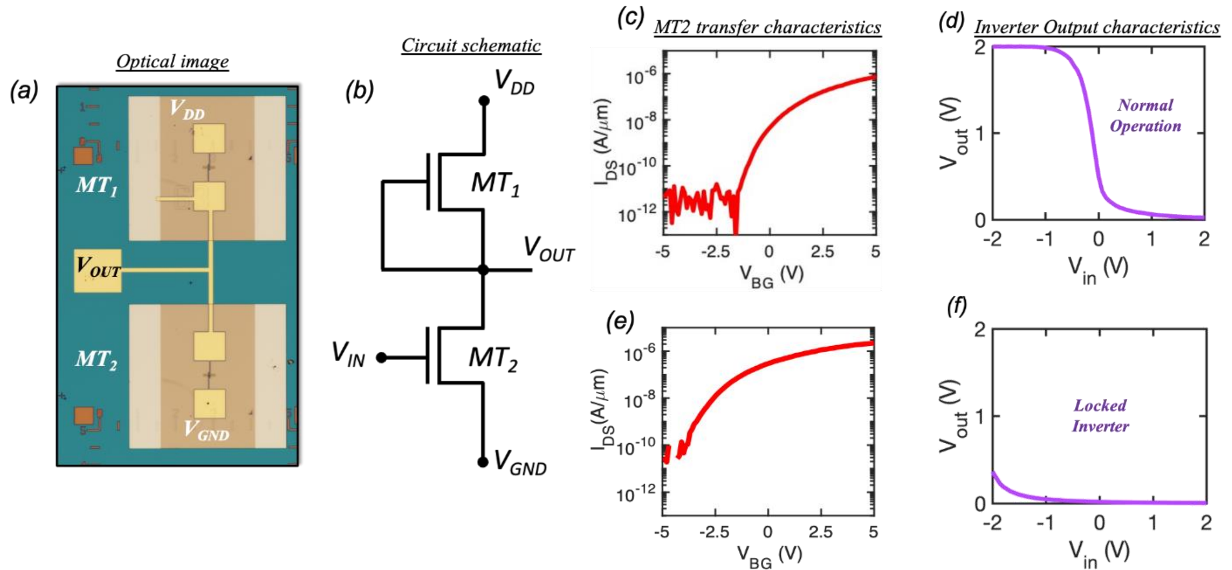

Figure 5: Demonstration of logic locking in a 2D memtransistor-based inverter (NOT gate).

respective locking schemes. **Fig. 5a-b** show an optical image and a circuit diagram, respectively, of our fabricated inverter. An inverter is a logic circuit that outputs a voltage representing the opposite logic-level to its input. The inverter demonstrated in this work was constructed using a depletion-mode (*D*-mode) memtransistor ($MT1$), formed by shorting the gate and source terminals, and an enhancement-mode (*E*-mode) memtransistor ($MT2$). For our demonstration, a specific supply voltage, V_{DD} = 2 V, was chosen for operating the circuits. Thus, a voltage level close to 2 V represents the logic state '1' while a voltage level close to 0 V represents the logic state '0'. We first determined the baseline state of $MT2$ by measuring its transfer characteristics as shown in **Fig. 5c.** Next, we evaluated the logic functionality of the inverter by plotting the input (V_{in}) versus the output (V_{out}) voltage transfer curve as shown in **Fig. 5d**. When V_{in} = 0 V (logic state '0') is applied to the gate terminal of $MT2$, the *E*-mode memtransistor becomes non-conductive in comparison to the *D*-mode memtransistor, resulting in $V_{out} = V_{DD}$ = 2 V (logic state '1'). However, for V_{in} = 2 V (logic state '1'), the *E*-mode memtransistor, $MT2$, becomes more conductive than the *D*-mode memtransistor, $MT1$, effectively clamping the V_{out} to 0 V (logic state '0'). Thus, in order to lock the inverter, it is evident that $MT2$ must remain more conductive than $MT1$ at all times. This is achieved by applying V_P = -14 V to the gate terminal of $MT2$, which shifts its V_{TH} to a more negative value as shown in **Fig. 5e**. This ensures that $MT2$ remains in the ON-state irrespective of V_{in}; as a result, the V_{out} from the inverter remains permanently clamped to 0 V (logic level '0'), as shown in **Fig. 5f.** Once locked, the inverter can only be unlocked by bringing $MT2$ back to its original baseline state through the application of a positive V_E.

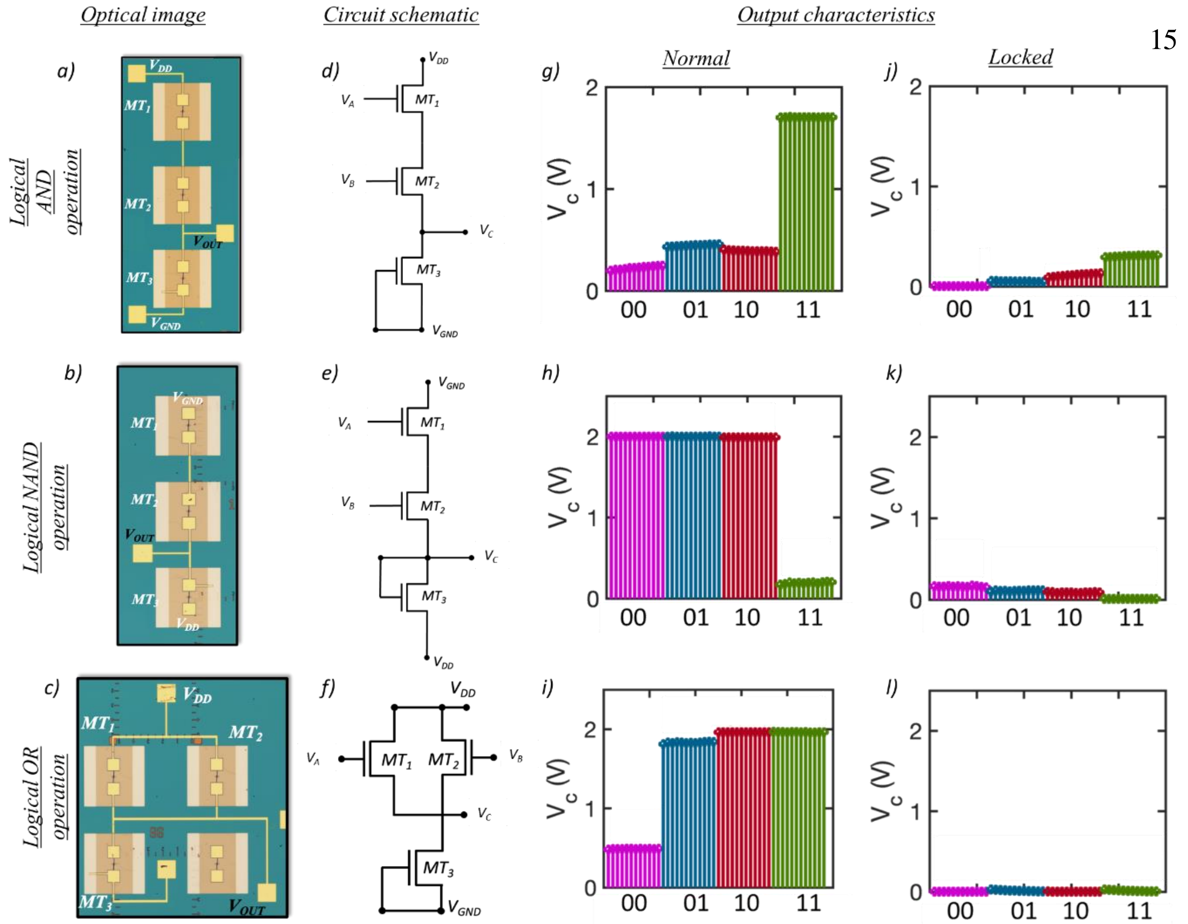

Figure 6: Demonstration of logic locking for 2D memtransistor-based AND, NAND and OR gates.

Fig. 6a-c show the optical images and **Fig. 6d-f** show the corresponding circuit diagrams for 2D memtransistor-based AND, $NAND$, and OR gates, respectively. Each circuit consists of two *E*-mode memtransistors ($MT1$ and $MT2$) and one *D*-mode memtransistor ($MT3$). **Fig. 6g-i** show the output characteristics of all three logic gates under standard operating conditions and **Fig. 6j-l** show their corresponding locked states. For an AND gate, operating on logical multiplication rule, the output, V_C, will always remain at a low level (logic state '0') when the input for any one of the *E*-mode transistors ($MT1$ and $MT2$), $V_{A/B}$ = 0 V, as shown in **Fig. 6g**. This is because $MT3$ is highly

conductive when either $MT1$ and $MT2$ is in a low conductive state, clamping V_C to 0 V. In contrast, V_C will only be clamped to V_{DD} = 2 V (logic state '1') when both $MT1$ and $MT2$ have $V_{A/B}$ = 2 V, i.e., are in a high conductance state. Thus, in order to lock the circuit functionality as shown in **Fig. 6j**, we provide a V_P of magnitude 15 V to the local back-gate of $MT1$, shifting its V_{TH} to a high positive value (**Fig. 7)** for the transfer characteristics of $MT1$ in unlocked and locked states) and setting it to a high resistance state. This is equivalent to having an open circuit condition for $MT1$ since it always remains OFF, irrespective of the input provided. As a result, all $V_{A/B}$ combinations for the AND gate provide a low V_C values (logic state '0'), thereby locking the circuit.

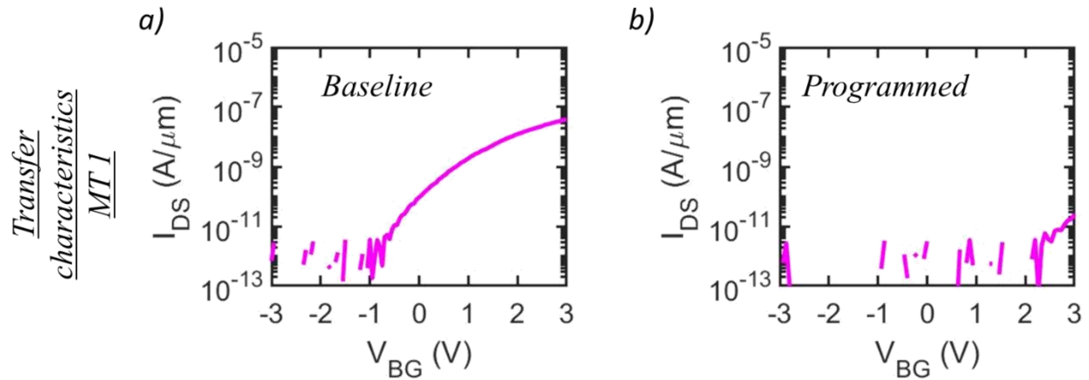

Figure 7: Transfer characteristics of enhancement-mode MT_1 for a AND gate with programming.

The LL mechanism of a $NAND$ gate is inverse of that of an AND gate stemming from the fact that a standard $NAND$ operation is nothing more than inverted AND logic. As shown in **Fig. 6h**, the V_C of the circuit is clamped to V_{DD} = 2 V (logic state '1') when either or both $MT1$ and $MT2$ remains non-conductive, i.e., for $V_{A/B}$ = 0 V; only when $V_{A/B}$ is high (logic state '1') for both $MT1$ and $MT2$, V_C = 0 V. In order to lock the $NAND$ gate, V_E = -14 V is applied to the local back-gates of

$MT1$ and $MT2$ (**Fig. 8**) since both need to be highly conductive to clamp V_C to 0 V as shown in **Fig. 6k**.

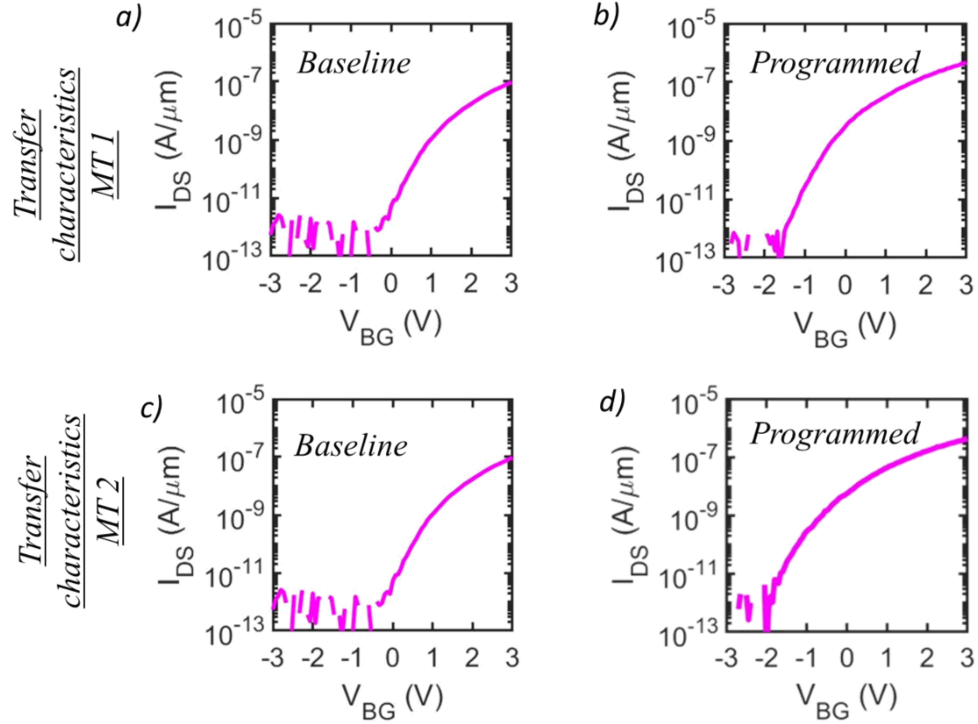

Figure 8: Transfer characteristics of MT_1 and MT_2 for a NAND gate with programming.

Next, for an OR gate that operates on logical addition rule, $MT1$ and $MT2$ are connected in series with $MT3$. As shown in **Fig. 6i**, the V_C of this circuit remains at 0 V (logic state '0') when $V_{A/B}$ = 0 V (logic state '0') for both $MT1$ and $MT2$. When either of the two input is high, V_C becomes clamped to V_{DD} (logic state '1') because one of the two E-mode memtransistors ($MT1$ and $MT2$) gets connected to $MT3$. This circuit can thus be locked by providing a V_P to both $MT1$ and $MT2$, making them highly resistive (**Fig. 9**). The locked OR gate is shown in **Fig. 6l**. The original logic functionality can then only be restored by providing an erase pulse V_E

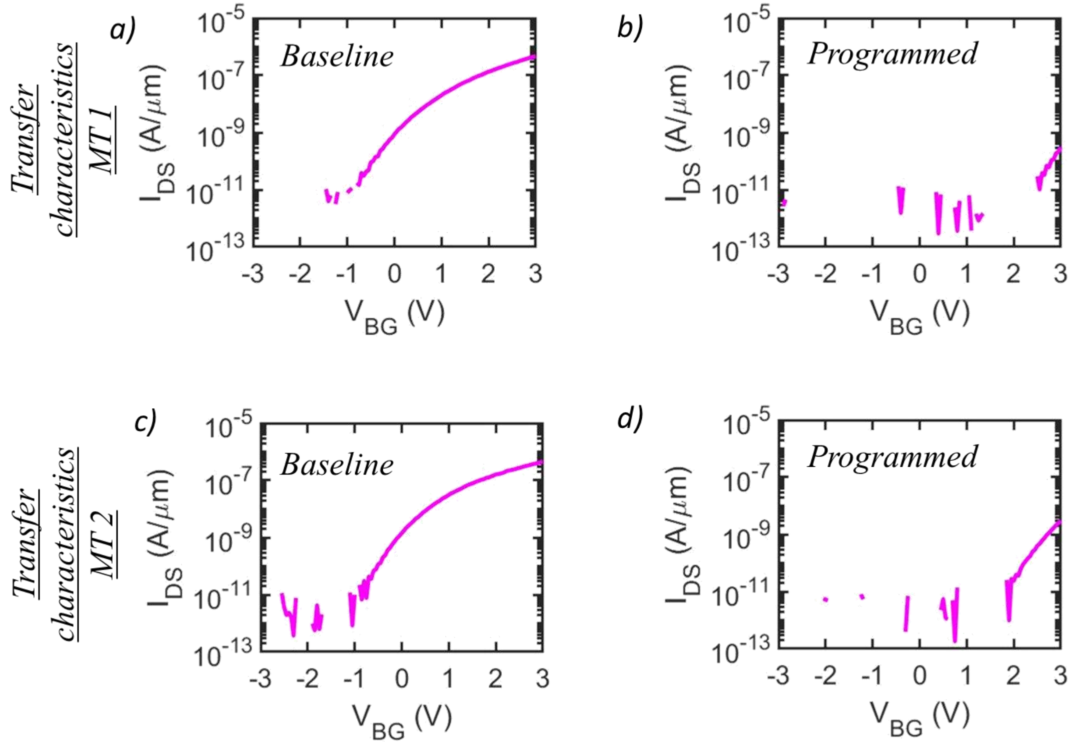

Figure 9: Transfer characteristics of MT_1 and MT_2 for an OR gate with programming.

to both $MT1$ and $MT2$, as described earlier for the other gates.

Finally, **Fig. 10a-b**, respectively, show the optical image and corresponding circuit schematic for a XOR gate that operates on the exclusive OR rule, i.e., a true output is obtained when the two inputs are dissimilar. Note that the circuit comprises of 9 2D memtransistors. The memtransistor pairs $MT1$ and $MT2$, and $MT5$ and $MT6$ operate as NOT gates. These NOT gates are employed to invert the bits A and B into $\bar{A}$ and $\bar{B}$, respectively. Next, the inputs A and $\bar{B}$ are applied to the gates of $MT3$ and $MT4$ whereas $\bar{A}$ and B are applied to the gates of $MT7$ and $MT8$, respectively. Also note

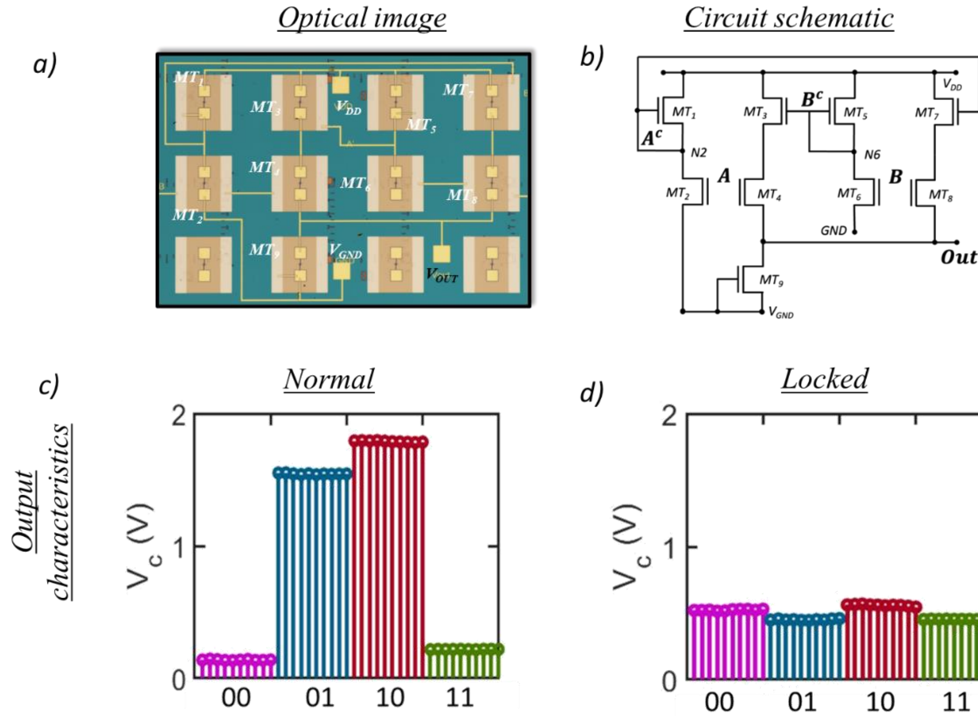

Figure 10: Demonstration of logic locking for a 2D memtransistor-based XOR gate.

that the series connections of $MT3$ and $MT4$ and $MT7$ and $MT8$ are connected in parallel and the entire block is connected in series with $MT9$. The overall circuit accomplishes XOR logic for inputs A and B, i.e., $V_C = \bar{A}B + A\bar{B}$, as shown in **Fig. 10c**. V_C = 2 V (logic state '1') when input logics are different. However, when the input logics are similar, V_C = 0V (logic 0). This circuit can be locked by providing a V_E = -14 V to both $MT2$ and $MT6$, making them highly conductive, thus clamping V_C to 0 V as shown in **Fig. 10d**.

3.4 Endurance and Retention of MoS_2 memtransistors

We have also experimentally demonstrated the long-term retention of our memtransistor devices for a total of 10^4 seconds or ~ 3 hours. **Fig. 11a-b**, respectively, show the retention, and the

memory ratio (MR) plot as a function of time for a representative memtransistor. MR is the time taken for the two states to eventually converge and become indistinguishable. Based on the fitting parameters and the decay observed, we estimated the convergence time of ~ 16 hours. Note that although, our MR window frame may not seem optimal, we believe that it is sufficient given today's ultra-competitive globalized chip design supply chain which is aggressively driven by time to market demands and shorter design time. However, we do agree that further improvements in the memtransistor design by including a floating gate (FG) architecture will certainly be a significant improvisation in terms of retention time. The endurance of our memtransistor has also been experimentally tested for up to 10^3 cycles. As shown in **Fig. 11c**, there is a minimal change observed in the ratio between the post-programmed and post-erase conduction states measured at a V_{BG} = 0V which is significant for our LL demonstration.

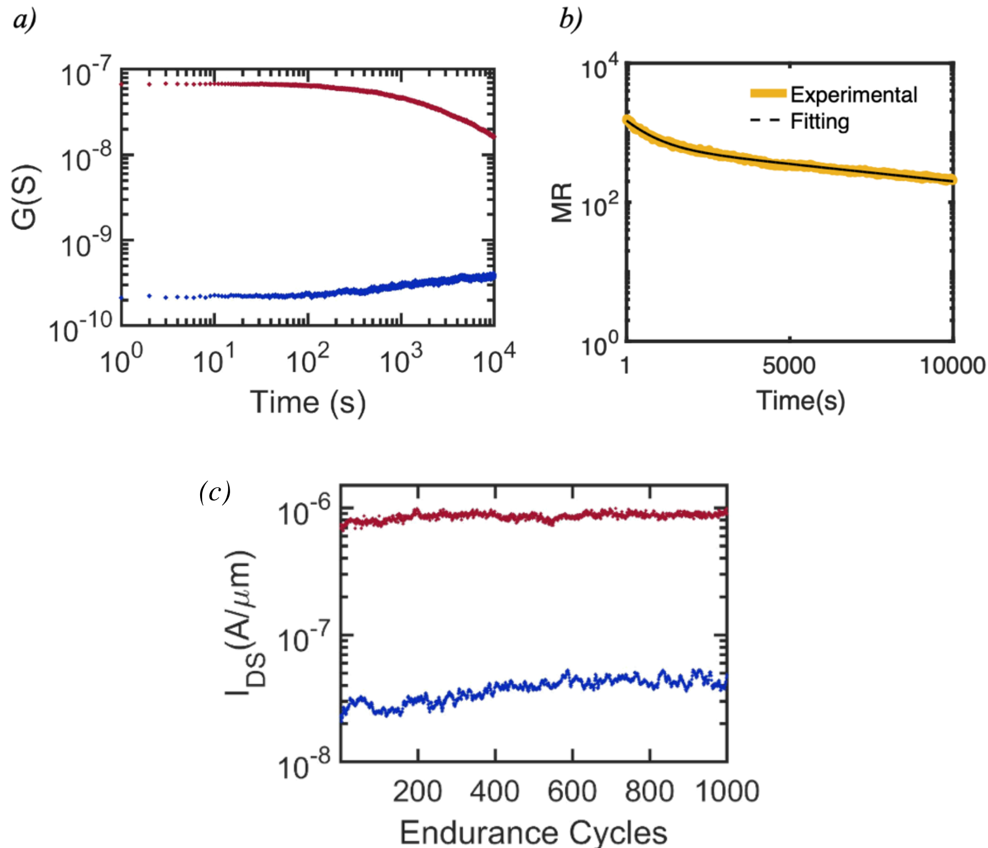

Figure 11: Endurance and retention plots of MoS_2 memtransistors.

Chapter 4

Benchmarking Results

Portions of this chapter are reproduced from: Chakrabarti, S., ***et. al.*** *"Logic Locking of Integrated Circuits Enabled by Nanoscale* MoS_2 *Based Memtransistors."* ***ACS Applied Nano Materials (DOI: 10.1021/acsanm.2c02807).***

In this chapter we discuss the benchmarking results and highlight the superiority of our proposed LL technique against the existing solutions. While LL techniques over the years have primarily focused on providing efficient hardware security solutions by eliminating their vulnerability to several attack models, they have often come at the cost of requiring additional peripheral components. For example, the recently proposed SARlock[76] and Anti-SAT[77] techniques have demonstrated impressive resilience against SAT-attacks. However, these techniques require integration of comparator/mask blocks and/or multiple XOR/XNOR/multiplexer key gates as peripheral elements to achieve the required resilient obfuscation. In comparison, the proposed LL scheme based on programmable 2D memtransistors eliminates the need of any peripheral components by enabling individual device-level locking of all the gates in any given circuit. **Table 1.** compares and summarizes our proposed technique against some of the present state-of-the-art LL solutions in terms of the locking mechanism, requirement of peripheral components and their resilience to SAT-attacks.

Table 1. Benchmarking 2D-memtransistor based LL with existing alternative solutions

LL technique	***Mechanism***	***Peripheral components***	***Resilience to SAT-attacks***
Random logic locking (RLL)[58]	*Inserting XOR key gates at random locations*	*Yes*	*No*
Fault based logic locking (FLL)[55]	*Inserting XOR key gates at lower testable points*	*Yes*	*No*
Strong logic locking (SLL)[56]	*Interference based key-gate insertion*	*Yes*	*No*
SARlock[53]	*Flipping circuit to corrupt input pattern*	*Yes*	*Yes*
Anti-SAT[54]	*Additional Anti-SAT combination blocks*	*Yes*	*Yes*
TT-Lock[57]	*Flipping output pattern for a wrong key*	*Yes*	*Yes*
2D-memtransistor based logic locking (this work)	***Individual device programmability***	***No***	***Yes***

Chapter 5

Conclusion and Future Work

5.1 Conclusion

The work presented in this thesis highlights the importance of securing IP cores from an untrustworthy adversary within the confines of a globalized and highly inter-connected semiconductor manufacturing supply chain ecosystem. The significance and importance of novel materials such as TMDCs in terms of providing low power and area efficient hardware security solutions in comparison to CMOS and memristive based technologies are also discussed. A new LL technique involving locking of basic digital logic gates such as AND, $NAND$, OR, XOR and NOT, fabricated using programmable monolayer MoS_2-based memtransistors is demonstrated. The area efficiency stems from the programmability aspect of the 2D memtransistors which is attributed to the phenomenon of charge trapping and de-trapping at the Al_2O_3/MoS_2 interface. The logic gates are locked/unlocked *via* the application of either a programming pulse V_P or an erase pulse V_E to their respective local back-gates at a miniscule energy expense of < 1 picojoules. The 2D memtransistors exhibit an excellent long-term retention and stability. By exploiting the unique material properties and intrinsic device phenomena of MoS_2 based 2D memtransistors, the LL technique developed in this work is a step forward in providing critical solutions for solving critical hardware security problems such as IP overbuilding and piracy. Furthermore, by evading the requirement of any additional logic or peripherals, the proposed LL technique has also shown resilience to SAT-attack model. Therefore, to conclude, this work delineates the background for warranting innovations underlying at the materials and device level to circumvent impediments

imposed by present day silicon-based CMOS technology.

5.2 Future Work

With promising preliminary results, it is evident that 2D-material based technologies will be brought to fruition in the near future. However, certain key challenges at the device level such as reducing contact resistance, enhancing carrier mobility, integrating high-*k* dielectrics, achieving a stable doping strategy and improving device stability must be overcome first for ensuring good reliability. Since the technology more or less still stands at its inception point, recent efforts collimated towards the large-area growth of the 2D materials using CVD and MOCVD techniques with minimum device-to-device variation and superior electrostatic performances offer a promising ambition geared towards developing large scale VLSI applications. Therefore, along these lines, future research direction will be geared towards implementing LL of complex sequential and combinational logic circuits. Moreover, prolonging the retention of 2D memtransistor memory by including a thin tunneling layer of HfO_2 along with a charge trapping layer in the fabricated gate stack would also be yet another major goal. This would undoubtedly be a significant milestone leading to a more practical realization of secure ICs.

Bibliography

[1] R. R. Schaller, "Moore's law: past, present and future," *IEEE spectrum,* vol. 34, no. 6, pp. 52-59, 1997.

[2] D. J. Frank, R. H. Dennard, E. Nowak, P. M. Solomon, Y. Taur, and H.-S. P. Wong, "Device scaling limits of Si MOSFETs and their application dependencies," *Proceedings of the IEEE,* vol. 89, no. 3, pp. 259-288, 2001.

[3] G. Fiori *et al.*, "Electronics based on two-dimensional materials," *Nature nanotechnology,* vol. 9, no. 10, pp. 768-779, 2014.

[4] B. Yu *et al.*, "FinFET scaling to 10 nm gate length," in *Digest. International Electron Devices Meeting*, 2002: IEEE, pp. 251-254.

[5] K. Uchida, J. Koga, R. Ohba, T. Numata, and S. Takagi, "Experimental evidences of quantum-mechanical effects on low-field mobility, gate-channel capacitance, and threshold voltage of ultrathin body SOI MOSFETs," in *International Electron Devices Meeting. Technical Digest (Cat. No. 01CH37224)*, 2001: IEEE, pp. 29.4. 1-29.4. 4.

[6] K. Zhu *et al.*, "The development of integrated circuits based on two-dimensional materials," *Nature Electronics,* vol. 4, no. 11, pp. 775-785, 2021.

[7] Y. Wu, D. B. Farmer, F. Xia, and P. Avouris, "Graphene electronics: Materials, devices, and circuits," *Proceedings of the IEEE,* vol. 101, no. 7, pp. 1620-1637, 2013.

[8] F. Torrisi *et al.*, "Inkjet-printed graphene electronics," *ACS nano,* vol. 6, no. 4, pp. 2992-3006, 2012.

[9] K. C. Yung, W. Wu, M. Pierpoint, and F. Kusmartsev, "Introduction to graphene electronics–a new era of digital transistors and devices," *Contemporary Physics,* vol. 54, no. 5, pp. 233-251, 2013.

[10] W. Lu, P. Xie, and C. M. Lieber, "Nanowire transistor performance limits and applications," *IEEE transactions on Electron Devices,* vol. 55, no. 11, pp. 2859-2876, 2008.

[11] J. Appenzeller, J. Knoch, M. T. Bjork, H. Riel, H. Schmid, and W. Riess, "Toward nanowire electronics," *IEEE Transactions on electron devices,* vol. 55, no. 11, pp. 2827-2845, 2008.

[12] P. L. McEuen, M. S. Fuhrer, and H. Park, "Single-walled carbon nanotube electronics," *IEEE transactions on nanotechnology,* vol. 1, no. 1, pp. 78-85, 2002.

[13] P. Avouris, J. Appenzeller, R. Martel, and S. J. Wind, "Carbon nanotube electronics," *Proceedings of the IEEE,* vol. 91, no. 11, pp. 1772-1784, 2003.

[14] B. Radisavljevic, A. Radenovic, J. Brivio, V. Giacometti, and A. Kis, "Single-layer MoS2 transistors," *Nature nanotechnology,* vol. 6, no. 3, pp. 147-150, 2011.

[15] S. Kim *et al.*, "High-mobility and low-power thin-film transistors based on multilayer MoS2 crystals," *Nature communications,* vol. 3, no. 1, pp. 1-7, 2012.

[16] W. Liu, J. Kang, D. Sarkar, Y. Khatami, D. Jena, and K. Banerjee, "Role of metal contacts in designing high-performance monolayer n-type WSe2 field effect transistors," *Nano letters,* vol. 13, no. 5, pp. 1983-1990, 2013.

[17] Q. H. Wang, K. Kalantar-Zadeh, A. Kis, J. N. Coleman, and M. S. Strano, "Electronics and optoelectronics of two-dimensional transition metal dichalcogenides," *Nature nanotechnology,* vol. 7, no. 11, pp. 699-712, 2012.

[18] S. Larentis *et al.*, "Reconfigurable complementary monolayer MoTe2 field-effect transistors for integrated circuits," *ACS nano,* vol. 11, no. 5, pp. 4832-4839, 2017.

[19] S. Manzeli, D. Ovchinnikov, D. Pasquier, O. V. Yazyev, and A. Kis, "2D transition metal dichalcogenides," *Nature Reviews Materials,* vol. 2, no. 8, pp. 1-15, 2017.

[20] D. Akinwande *et al.*, "Graphene and two-dimensional materials for silicon technology," *Nature,* vol. 573, no. 7775, pp. 507-518, 2019.

[21] M. Chhowalla, D. Jena, and H. Zhang, "Two-dimensional semiconductors for transistors," *Nature Reviews Materials,* vol. 1, no. 11, pp. 1-15, 2016.

[22] F. Schwierz, J. Pezoldt, and R. Granzner, "Two-dimensional materials and their prospects in transistor electronics," *Nanoscale,* vol. 7, no. 18, pp. 8261-8283, 2015.

[23] G. Iannaccone, F. Bonaccorso, L. Colombo, and G. Fiori, "Quantum engineering of transistors based on 2D materials heterostructures," *Nature nanotechnology,* vol. 13, no. 3, pp. 183-191, 2018.

[24] Y. Liu, X. Duan, H.-J. Shin, S. Park, Y. Huang, and X. Duan, "Promises and prospects of two-dimensional transistors," *Nature,* vol. 591, no. 7848, pp. 43-53, 2021.

[25] G. R. Bhimanapati *et al.*, "Recent advances in two-dimensional materials beyond graphene," *ACS nano,* vol. 9, no. 12, pp. 11509-11539, 2015.

[26] A. P. Jacob, R. Xie, M. G. Sung, L. Liebmann, R. T. Lee, and B. Taylor, "Scaling challenges for advanced CMOS devices," *International Journal of High Speed Electronics and Systems,* vol. 26, no. 01n02, p. 1740001, 2017.

[27] R.-H. Yan, A. Ourmazd, and K. F. Lee, "Scaling the Si MOSFET: From bulk to SOI to bulk," *IEEE Transactions on Electron Devices,* vol. 39, no. 7, pp. 1704-1710, 1992.

[28] V. Podzorov, M. Gershenson, C. Kloc, R. Zeis, and E. Bucher, "High-mobility field-effect transistors based on transition metal dichalcogenides," *Applied Physics Letters,* vol. 84, no. 17, pp. 3301-3303, 2004.

[29] A. Ayari, E. Cobas, O. Ogundadegbe, and M. S. Fuhrer, "Realization and electrical characterization of ultrathin crystals of layered transition-metal dichalcogenides," *Journal of applied physics,* vol. 101, no. 1, p. 014507, 2007.

[30] B. Radisavljevic, M. B. Whitwick, and A. Kis, "Integrated circuits and logic operations based on single-layer MoS2," *ACS nano,* vol. 5, no. 12, pp. 9934-9938, 2011.

[31] H. Wang *et al.*, "Integrated circuits based on bilayer MoS2 transistors," *Nano letters,* vol. 12, no. 9, pp. 4674-4680, 2012.

[32] L. Yu *et al.*, "Design, modeling, and fabrication of chemical vapor deposition grown MoS2 circuits with E-mode FETs for large-area electronics," *Nano Letters,* vol. 16, no. 10, pp. 6349-6356, 2016.

[33] M. Tosun *et al.*, "High-gain inverters based on WSe2 complementary field-effect transistors," *ACS nano,* vol. 8, no. 5, pp. 4948-4953, 2014.

[34] L. Yu *et al.*, "High-performance WSe2 complementary metal oxide semiconductor technology and integrated circuits," *Nano letters,* vol. 15, no. 8, pp. 4928-4934, 2015.

[35] S. Wachter, D. K. Polyushkin, O. Bethge, and T. Mueller, "A microprocessor based on a two-dimensional semiconductor," *Nature communications,* vol. 8, no. 1, pp. 1-6, 2017.

[36] K.-K. Liu *et al.*, "Growth of large-area and highly crystalline MoS2 thin layers on insulating substrates," *Nano letters,* vol. 12, no. 3, pp. 1538-1544, 2012.

[37] Y. Zhan, Z. Liu, S. Najmaei, P. M. Ajayan, and J. Lou, "Large-area vapor-phase growth and characterization of MoS2 atomic layers on a SiO2 substrate," *Small,* vol. 8, no. 7, pp. 966-971, 2012.

[38] D. Dumcenco *et al.*, "Large-area epitaxial monolayer MoS2," *ACS nano,* vol. 9, no. 4, pp. 4611-4620, 2015.

[39] Fiori, G. *et al.*, "Electronics based on two-dimensional materials", *Nat.Nanotechnol.*, 9, 768–779 (2014).

[40] Wang, H. *et al.,* "Integrated circuits based on bilayer MoS2 transistors", *Nano Lett.*, 12, 4674–4680 (2012).

[41] Polyushkin, D. K. *et al.,* "Analogue two-dimensional semiconductor electronics", *Nat. Electron.*, 3, 486–491 (2020).

[42] Yu, L. *et al.,* "Design, modeling, and fabrication of chemical vapor deposition grown MoS2 circuits with E-mode FETs for large-area electronics" *Nano Lett.*, 16, 6349–6356 (2016).

[43] S. Das, A. Sebastian, E. Pop, C. J. McClellan, A. D. Franklin, T. Grasser*, et al.*, "Transistors based on two-dimensional materials for future integrated circuits," *Nature Electronics,* vol. 4, pp. 786-799, 2021/11/01 2021.

[44] S. Das, A. Dodda, and S. Das, "A biomimetic 2D transistor for audiomorphic computing," *Nature Communications,* vol. 10, p. 3450, 2019/08/01 2019.

[45] T. F. Schranghamer, A. Oberoi, and S. Das, "Graphene memristive synapses for high precision neuromorphic computing," *Nature Communications,* vol. 11, p. 5474, 2020/10/29 2020.

[46] T. Force, "High performance microchip supply," *Annual Report. Defense Technical Information Center (DTIC), USA,* 2005.

[47] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the IEEE,* vol. 102, pp. 1283-1295, 2014.

[48] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," in *Proceedings of the 48th Design Automation Conference*, 2011, pp. 333-338.

[49] R. James, "Intel's 22-nm Trigate Transistors Exposed," *Chipworks Real Chips Blog, http://www.electroiq.com/blogs/chipworks_real_chips_blog/2012/04/intel-s-22-nm-trigate-transistors-exposed. html,* 2012.

[50] E. Oriero and S. R. Hasan, "Survey on recent counterfeit IC detection techniques and future research directions," *Integration,* vol. 66, pp. 135-152, 2019.

[51] M. Tehranipoor and C. Wang, *Introduction to hardware security and trust*: Springer Science & Business Media, 2011.

[52] S. Sethumadhavan, A. Waksman, M. Suozzo, Y. Huang, and J. Eum, "Trustworthy hardware from untrusted components," *Communications of the ACM,* vol. 58, pp. 60-71, 2015.

[53] "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain.," Washington DC2012.

[54] M. Yasin, J. J. Rajendran, O. Sinanoglu, and R. Karri, "On improving the security of logic locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 35, pp. 1411-1424, 2015.

[55] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 709-720.

[56] R. W. Jarvis and M. G. Mcintyre, "Split manufacturing method for advanced semiconductor circuits," ed: Google Patents, 2007.

[57] Y. Alkabani and F. Koushanfar, "Active Hardware Metering for Intellectual Property Protection and Security," in *USENIX security symposium*, 2007, pp. 1-20.

[58] J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending piracy of integrated circuits," *Computer,* vol. 43, pp. 30-38, 2010.

[59] S. Dupuis, P.-S. Ba, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans," in *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*, 2014, pp. 49-54.

[60] R. S. Chakraborty and S. Bhunia, "HARPOON: An obfuscation-based SoC design methodology for hardware protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 28, pp. 1493-1502, 2009.

[61] R. S. Chakraborty and S. Bhunia, "Security against hardware Trojan through a novel application of design obfuscation," in *2009 IEEE/ACM International Conference on Computer-Aided Design-Digest of Technical Papers*, 2009, pp. 113-116.

[62] H. Jiang, C. Li, R. Zhang, P. Yan, P. Lin, Y. Li*, et al.*, "A provable key destruction scheme based on memristive crossbar arrays," *Nature Electronics,* vol. 1, pp. 548-554, 2018.

[63] B. Hoefflinger, "ITRS: The international technology roadmap for semiconductors," in *Chips 2020*, ed: Springer, 2011, pp. 161-174.

[64] A. Oberoi, A. Dodda, H. Liu, M. Terrones, and S. Das, "Secure Electronics Enabled by Atomically Thin and Photosensitive Two-Dimensional Memtransistors," *ACS nano,* 2021.

[65] A. Wali, S. Kundu, A. J. Arnold, G. Zhao, K. Basu, and S. Das, "Satisfiability Attack-Resistant Camouflaged Two-Dimensional Heterostructure Devices," *ACS nano,* vol. 15, pp. 3453-3467, 2021.

[66] P. Wu, D. Reis, X. S. Hu, and J. Appenzeller, "Two-dimensional transistors with reconfigurable polarities for secure circuits," *NATURE electronics,* vol. 4, pp. 45-53, 2021.

[67] A. Wali, H. Ravichandran, and S. Das, "A Machine Learning Attack Resilient True Random Number Generator Based on Stochastic Programming of Atomically Thin Transistors," *ACS Nano,* vol. 15, pp. 17804-17812, 2021/11/23 2021.

[68] A. Dodda, S. Subbulakshmi Radhakrishnan, T. F. Schranghamer, D. Buzzell, P. Sengupta, and S. Das, "Graphene-based physically unclonable functions that are reconfigurable and resilient to machine learning attacks," *Nature Electronics,* vol. 4, pp. 364-374, 2021.

[69] Wali, A.; Ravichandran, H.; Das, S. "A Machine Learning Attack Resilient True Random Number Generator Based on Stochastic Programming of Atomically Thin Transistors," *ACS Nano,* vol. 15, no. 11, pp. 17804-17812, 2021/11/23 2021, doi: 10.1021/acsnano.1c05984.

[70] A. Dodda, A.; Subbulakshmi Radhakrishnan, S.; Schranghamer, T.F.; Buzzell, D.; Sengupta, P.; Das, S."Graphene-based physically unclonable functions that are reconfigurable and resilient to machine learning attacks," *Nature Electronics,* vol. 4, no. 5, pp. 364-374, 2021.

[71] Feng, G.; Jiang, J.; Zhao, Y.; Wang, S.; Liu, B.; Niu, D.; Li,X.; Chen, Y.; Duan,H.; Yang, J.; He, J.; Gao, Y.; Wan, Q."A sub-10 nm vertical organic/inorganic hybrid transistor for pain-perceptual and sensitization-regulated nociceptor emulation," *Advanced Materials,* vol. 32, no. 6, p. 1906171, 2020.

[72] Xie, D.; Wei, L.; Xie, M.; Jiang, L.; Yang, J.; He, J.; Jiang, J. "Photoelectric visual adaptation based on 0D-CsPbBr3-quantum-dots/2D-MoS2 mixed-dimensional heterojunction transistor," *Advanced Functional Materials,* vol. 31, no. 14, p. 2010655, 2021.

[73] Das, S.; Chen, H.Y.; Penumatcha, A.V.; Appenzeller, J."High performance multilayer MoS2 transistors with scandium contacts," *Nano Lett,* vol. 13, no. 1, pp. 100-5, Jan 09 2013, doi: 10.1021/nl303583v.

[74] Sebastian, A.; Das, S.; Das, S."An Annealing Accelerator for Ising Spin Systems Based on In-Memory Complementary 2D FETs," *Advanced Materials,* vol. 34, no. 4, p. 2107076, 2022.

[75] Yasin, M.; Mazumdar, B.; Rajendran, J.J.; Sinanoglu, O. "SARLock: SAT attack resistant logic locking," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2016: IEEE, pp. 236-241.

[76] Xie,Y.; Srivastava, A."Mitigating SAT attack on logic locking," in *International conference on cryptographic hardware and embedded systems*, 2016: Springer, pp. 127-146.

[77] Rajendran, J.; Zhang, H.; Zhang, C.; Rose, G.S.; Pino, Y.; Sinanoglu , O.;. Karri, R."Fault analysis-based logic encryption," *IEEE Transactions on computers,* vol. 64, no. 2, pp. 410-424, 2013.

[78] Rajendran, J.; Pino, Y.; Sinanoglu, O.; Karri, R."Security analysis of logic obfuscation," in *Proceedings of the 49th Annual Design Automation Conference*, 2012, pp. 83-89.

[79] Yasin, M.; Sengupta, A.; Schafer, B.C.; Makris, Y.; Sinanoglu, O.; Rajendran, J. "What to lock? Functional and parametric locking," in *Proceedings of the on Great Lakes Symposium on VLSI 2017*, 2017, pp. 351-356.

[80] Xiao, L.; Hongwei Z.; "Two-dimenstional MoS_2: Properties, preparation, and applications", in Journal of Materiomics, Vol 1., Issue 1, Pages 33-34.

[81] Sebastian, A.; Pendurthi, R.; Choudhury, T.H.; Redwing, J.M.;Das, S. Benchmarking monolayer MoS2 and WS2 field-effect transistors. Nature Communications. 2021, 12, 693.