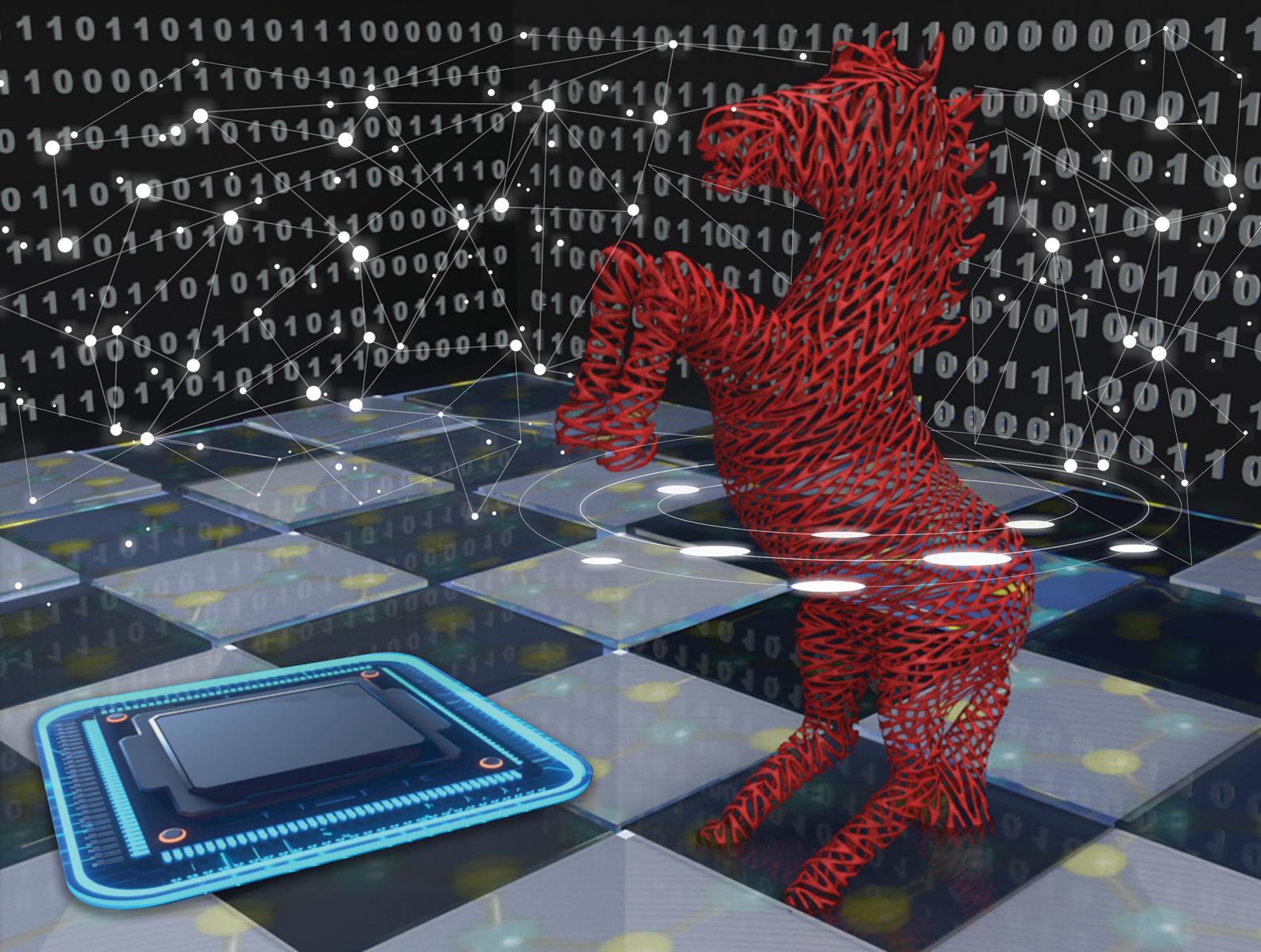


Nanoscale Horizons

The home for rapid reports of exceptional significance in nanoscience and nanotechnology
rsc.li/nanoscale-horizons



ISSN 2055-6756



Cite this: *Nanoscale Horiz.*, 2023, 8, 603

Received 7th December 2022,
Accepted 25th January 2023

DOI: 10.1039/d2nh00568a

rsc.li/nanoscale-horizons

Hardware Trojans based on two-dimensional memtransistors†

Akshay Wali, ^a Harikrishnan Ravichandran ^b and Saptarshi Das ^{*abc}

Hardware Trojans (HTs) have emerged as a major security threat for integrated circuits (ICs) owing to the involvement of untrustworthy actors in the globally distributed semiconductor supply chain. HTs are intentional malicious modifications, which remain undetectable through simple electrical measurements but can cause catastrophic failure in the functioning of ICs in mission critical applications. In this article, we show how two-dimensional (2D) material based in-memory computing elements such as memtransistors can be used as hardware Trojans. We found that logic gates based on 2D memtransistors can be made to malfunction by exploiting their inherent programming capabilities. While we use 2D memtransistor-based ICs as the testbed for our demonstration, the results are equally applicable to any state-of-the-art and emerging in-memory computing technologies.

Introduction

The monumental success of nearly all present day computing and information technology platforms brought about by the von Neumann architecture used in integrated circuits (ICs) has

New concepts

Here we show, for the first time, that logic circuits constructed using two-dimensional memtransistors can be used as Hardware Trojans (HTs). Existing research has not explored this aspect inherent to in-memory computing elements. Therefore, while we use two-dimensional memtransistor-based ICs as the testbed for our demonstration, the results are equally applicable to any state-of-the-art and emerging in-memory computing technologies such as FeFETs, RRAMs, FPGAs, etc.

been truly remarkable.¹ However, with the ever-increasing demands of data-intensive applications such as artificial intelligence, machine learning, signal processing, optimization, etc., the separation between processing and memory units in the conventional von Neumann architecture has lead to a worsening performance bottleneck in a phenomenon widely known as the “Memory Wall”.² Despite the introduction of improved architectures such as high bandwidth memory (HBM),³ hybrid memory cubes (HMCs),⁴ and high-parallel graphics processing units (GPUs),⁵ moving massive amounts of information between the logic and memory units results in significant latency and energy consumption.⁶ The emergence of non-von-Neumann architectures, most notably in-memory computing, mitigates this problem by allowing computational tasks to be performed within the confines of the computational memory,⁷ thus eliminating the aforementioned energy and latency limitations.^{8,9} In this context, successful demonstrations of in-memory computing architectures implemented on programmable heterogenous microprocessors,¹⁰ static random access memory (SRAM),¹¹ integrated optics,¹² and resistive switching devices¹³ offer a new way forward.

However, as expected, newer technologies are subjected to newer challenges and given that the semiconductor supply chain is a globally distributed ecosystem with likely involvement of untrustworthy actors, it is worthwhile to study the susceptibility of in-memory computing technology to emerging security threats. In this context, hardware Trojans (HTs) have been identified as one of the most pervasive security threats to ICs used in military, government, and industrial operations in recent years.^{14,15} HTs are undesirable malicious modifications at the device, circuit, or

^a Electrical Engineering and Computer Science, Penn State University, University Park, PA 16802, USA. E-mail: sud70@psu.edu

^b Engineering Science and Mechanics, Penn State University, University Park, PA 16802, USA

^c Materials Science and Engineering, Penn State University, University Park, PA 16802, USA

† Electronic supplementary information (ESI) available: Transfer characteristics of 16 MoS₂-based memtransistors on a logarithmic scale and linear scale for examining device to device variation along with a histogram plot of the threshold voltage (V_{TH}) extracted from the linear scale. Band diagram profile of our 2D memtransistor architecture demonstrating the mechanism of charge trapping and detrapping. Normal inverter output characteristics for a supply voltage $V_{DD} = 5$ V. Degradation of the subthreshold slope (SS) for three different 2D memtransistors in a cascaded three-stage inverter (TSI) circuit module. Output inverter plots post V_{HT} application showing a clear shift in the switching voltage V_m for all the three stages of a TSI circuit module. Normal NOR functionality for a $V_{DD} = 5$ V. Normal NAND functionality for a $V_{DD} = 5$ V. Long term retention of two representative analog resistance states for a total of 10^4 seconds or 3 hours along with a memory ratio (MR) plot showcasing the eventual merging of the two resistance states. See DOI: <https://doi.org/10.1039/d2nh00568a>

architecture level which alter the intended IC functionalities. HTs can be inserted at various stages of the design and manufacturing process flow, including fabrication, testing, assembly, and packaging. Such modifications remain unknown to the original designer and can result in catastrophic consequences in critical applications such as defense, transportation and communications.^{16,17} In fact, as per a report, malicious HTs present in electronic systems recently resulted in severe military mishaps.^{14,18}

Unlike software-based Trojans (STs) which steal, erase or corrupt information and cause harm to the host by gaining access to the operating system,¹⁹ HTs cannot be removed once inserted into the intellectual property (IP). While Trojans exist in many forms, they are most commonly activated by a specific mechanism, called a trigger, and deliver a specific function, called a payload.²⁰ HTs can be small or large in size with respect to the overall circuit.¹⁹ Although the intention is to compromise the integrity, authenticity, and functionality of the underlying IC, HTs can also be designed with the sole intention of shortening the operational lifetime or causing the failure of the entire hardware system upon their activation. Trojans are stealthy, undetectable, and inserted into rare circuit nodes so as to reduce the likelihood of their activation during normal operations. It must be emphasized that an HT is an intentional insertion by an adversary and not a flaw arising from design or manufacturing variability.

While the majority of the research efforts collimated towards studying HTs have focused on their detection, few have highlighted their deliberate inclusion in an IP.^{21–24} In this article, we adopt a radical approach by placing ourselves in the role of an adversary who is knowledgeable about circuit designs and address a scenario where an HT is locally inserted within the IP core. We utilize in-memory computing to engineer our hardware designs so as to deliberately produce faulty or corrupt circuit outputs, thereby compromising and degrading their overall circuit functionality. Note that, contrary to earlier studies^{25–30} which have focused on securing the IPs against a variety of security threats such as reverse engineering (RE), piracy, counterfeiting, and illegal cloning, our demonstration aims to expose the hardware security vulnerabilities of the emerging in-memory computing paradigm. We have used logic circuits such as NOT, AND, NAND, NOR and a three-stage inverter (TSI) based on memtransistors fabricated from atomically thin two-dimensional (2D) materials such as monolayer molybdenum disulfide (MoS₂) as a testbed for HT insertion. However, the results and HT insertion strategies adopted in this work are equally applicable to any other state-of-the-art in-memory computing technologies such as CMOS-based static random access memories (SRAMs),^{31,32} resistive RAM (RRAM)^{33,34} phase-change materials (PCMs),^{35,36} spintronics,^{37,38} floating gate memories,^{39,40} ferroelectric field-effect transistors (FETs),^{41,42} and memristive arrays.^{43,44}

Monolayer MoS₂ characterization and device fabrication

Our choice of MoS₂ stems from the growing interest in 2D materials as a post-Si solution as indicated by IC manufacturing

giants such as Intel and TSMC. It is also noteworthy that there are several recent reports on high-performance, high-density, and low power 2D device technologies^{45–52} as well as on 2D-based in-memory and in-sensor computing technologies.^{53–59} In order to ensure the high quality of the material, the monolayer MoS₂ used in our study was grown using a metal-organic chemical vapor deposition (MOCVD) technique on an epitaxial sapphire substrate at a temperature of 950 °C.⁵¹ The material growth was followed by the fabrication of the memtransistor-based IC as the IP. Fig. 1a shows the optical image of the as-fabricated MoS₂-based IP which comprises several logic circuits such as NAND, NOR, AND, and a three-stage inverter (TSI) module. Fig. 1b and c, respectively, show the optical image and the corresponding 2D schematic of a representative individual 2D-memtransistor with monolayer MoS₂ as the semiconducting channel, Pt/Ti as local back-gate electrodes (CG), 40 nm alumina (Al₂O₃) as the gate dielectric, a 3 nm hafnia (HfO₂) as a charge trapping layer in a floating gate (FG) configuration, and a 7 nm Al₂O₃ as the tunnelling layer along with Ni/Au (40/30 nm) as the source and drain electrodes. All our memtransistors have a fixed channel length (L) of 1 μm and a channel width (W) of 5 μm. Details on the MoS₂ synthesis, film transfer, and memtransistor-based circuit fabrication can be found in the Methods section.

Fig. 1d and e, respectively, show the Raman and the photoluminescence (PL) spectra obtained from a representative MoS₂ film where the characteristic in-plane E_{2g}¹ mode and out-of-plane A_{1g} mode were observed at 385 cm⁻¹ and 403 cm⁻¹, respectively, and the PL peak was found to be at 1.81 eV; these results are consistent with a monolayer film. Fig. 1f shows the transfer characteristics of a representative MoS₂ memtransistor where the source-to-drain current (I_{DS}) is plotted in the linear and logarithmic scales with respect to the local back-gate voltage (V_{BG}) when measured at different source-to-drain biases (V_{DS}). A clear n-type dominated carrier transport is observed due to the pinning of the metal Fermi level near the conduction band facilitating enhanced electron injection.^{60,61} In addition, an excellent ON/OFF current ratio of ~10⁷ and a subthreshold slope (SS) of ~350 mV per decade obtained over three orders of magnitude change in I_{DS} are also observed. The deviation of the SS from the ideal value of 60 mV per dec can be attributed to the presence of interface traps. Next, the output characteristics (Fig. 1g) where I_{DS} is plotted against V_{DS} as a function of different V_{BG} also show excellent I_{ON} values of 10 μA μm⁻¹ for V_{DS} = 5 V at V_{BG} = 5 V. Note that further enhancement in the device characteristics can be accomplished through the optimization of metal contacts, as well as scaling the oxide thickness and the channel length⁶²

The device-to-device (D2D) variation was also examined due to our intention to fabricate ICs involving multiple memtransistors. Fig. 1h and i show the histogram plots of the obtained threshold voltage (V_{TH}) at an iso-current of 100 nA μm⁻¹ and the peak electric field mobility (μ_n) obtained from the transconductance ($g_m = \frac{dI_{DS}}{dV_{BG}}$) method, respectively, with the corresponding mean values of 1.5 V and 17.5 cm² V⁻¹ s⁻¹ for 16 different MoS₂ memtransistors. Fig. 1j and k show the colormaps of the on/off ratio and I_{ON} measured at V_{DS} = 5 V

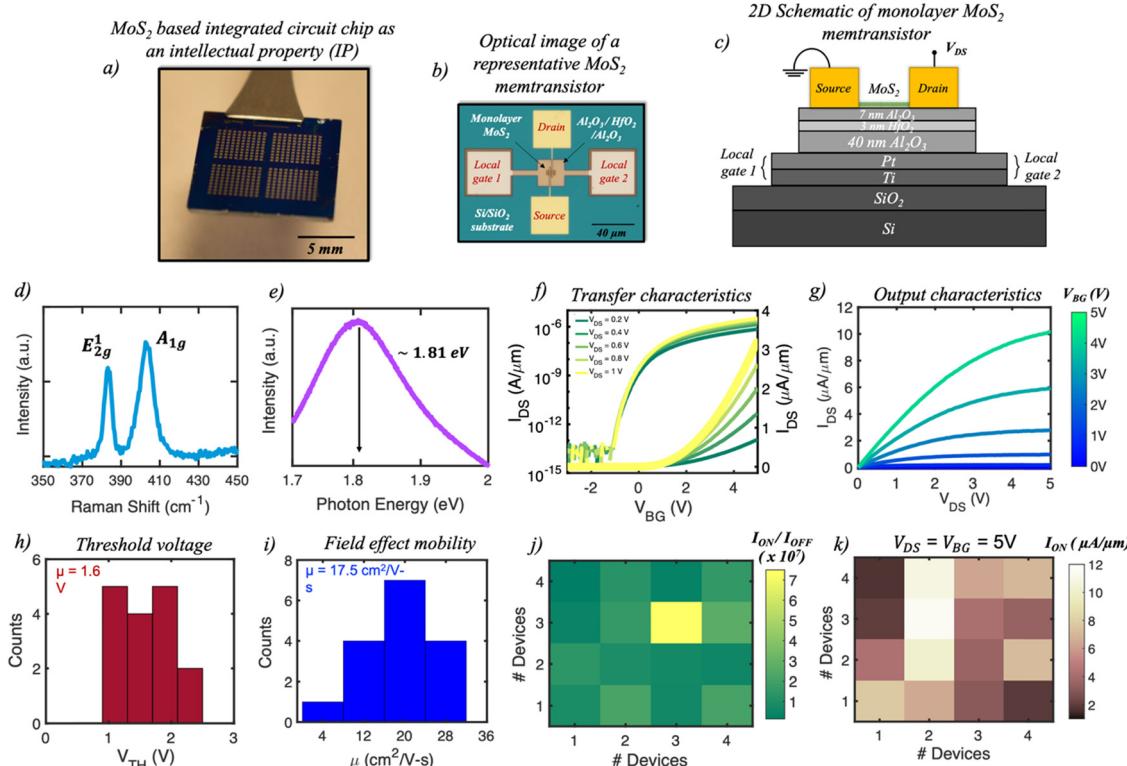


Fig. 1 Monolayer MoS₂ characterization and memtransistor fabrication: (a) An optical image of a MoS₂-based integrated intellectual property (IP) comprising several logic circuits such as NAND, NOR, AND, and a three-stage inverter (TSI) module. (b) An optical image along with a corresponding (c) 2D schematic of a representative individual MoS₂-memtransistor. The device structure comprises Platinum/Titanium (Pt/Ti) local gates, a 7 nm Alumina (Al₂O₃) tunnelling layer, a 3 nm Hafnia (HfO₂) charge-trapping layer, and a 40 nm Al₂O₃ blocking layer as the gate dielectric stack with Ni/Au (40/30 nm) as the source and drain contact pads. All the memtransistors have a channel length (L) of 1 μ m, a channel width (W) of 5 μ m, and two local gates from either side for better accessibility. (d) Raman and (e) photoluminescence (PL) spectra, respectively, obtained from a representative MoS₂ film where the characteristic in-plane E_{2g}^1 mode and out-of-plane A_{1g} mode were observed at 385 cm^{-1} and 403 cm^{-1} , respectively, with the PL peak at 1.83 eV. (f) Transfer characteristics of a representative MoS₂ memtransistor in the logarithmic and linear scales where the source-to-drain current (I_{DS}) is plotted with respect to the local back-gate voltage (V_{BG}) and measured at different source-to-drain (V_{DS}) biases. A clear n-type dominated carrier transport is observed. (g) A plot of the output characteristics where I_{DS} is plotted against V_{DS} as a function of different V_{BG} biases with excellent I_{ON} values of 10 $\mu\text{A } \mu\text{m}^{-2}$ for $V_{DS} = 5$ V at $V_{BG} = 5$ V. Histogram plots for the extracted (h) threshold voltage (V_{TH}) at an iso-current of 100 $\text{nA } \mu\text{m}^{-2}$ with a mean of 1.6 V and (i) peak electric field mobility (μ) extracted using the transconductance method with a mean of 17.5 $\text{cm}^2 \text{V}^{-1} \text{s}^{-1}$ along with the colormap plots of (j) I_{ON}/I_{OFF} ratio and (k) I_{ON} values at a $V_{DS} = V_{BG} = 5$ V for a population of 16 MoS₂ memtransistors; these results further confirm the high quality of our channel material.

and $V_{BG} = 5$ V for the same devices. These results confirm the high quality and uniform growth of MoS₂, which is critical for successful realization of memtransistor-based ICs. ESI† S1 shows D2D variation across the transfer characteristics and linear V_{TH} obtained for all 16 MoS₂ memtransistors. Although a deterrent, these variations are often unavoidable due to factors such as growth and transfer-related defects, adsorbed water molecules, and resist residues originating from the fabrication process. However, they do not hinder or limit our ability as an adversary to insert HTs into chip designs.

Basis of in-memory computing inspired hardware Trojans (HTs) in MoS₂ intellectual property (IP)

In this section, we demonstrate the non-volatile electrical programmability of our 2D memtransistors as the basis for

inserting HTs into the IP core. Fig. 2a shows the pre-Trojan baseline transfer characteristics of a representative memtransistor in both the logarithmic and linear scales with expected carrier transport behavior. Trojans are inserted by applying a voltage pulse to the local gate of the MoS₂ memtransistor which results in an altered device characteristic. Fig. 2b and c, respectively, show the transfer characteristics (logarithmic and linear scales) for the same representative memtransistor post Trojan insertion. It can be clearly seen that the application of a negative voltage pulse shifts the device threshold voltage (V_{TH}) towards a more negative value, thereby making it less resistive (more conductive), whereas a positive voltage pulse shifts V_{TH} towards a more positive value, making it more resistive (less conductive). This shift is attributed to the tunnelling of charge carriers across the 7 nm Al₂O₃ into the HfO₂ charge-trapping layer. The ability to draw the carriers into the FG is enabled by Fowler-Nordheim tunnelling⁶³ applying a large negative/positive voltage pulse to the CG facilitates the

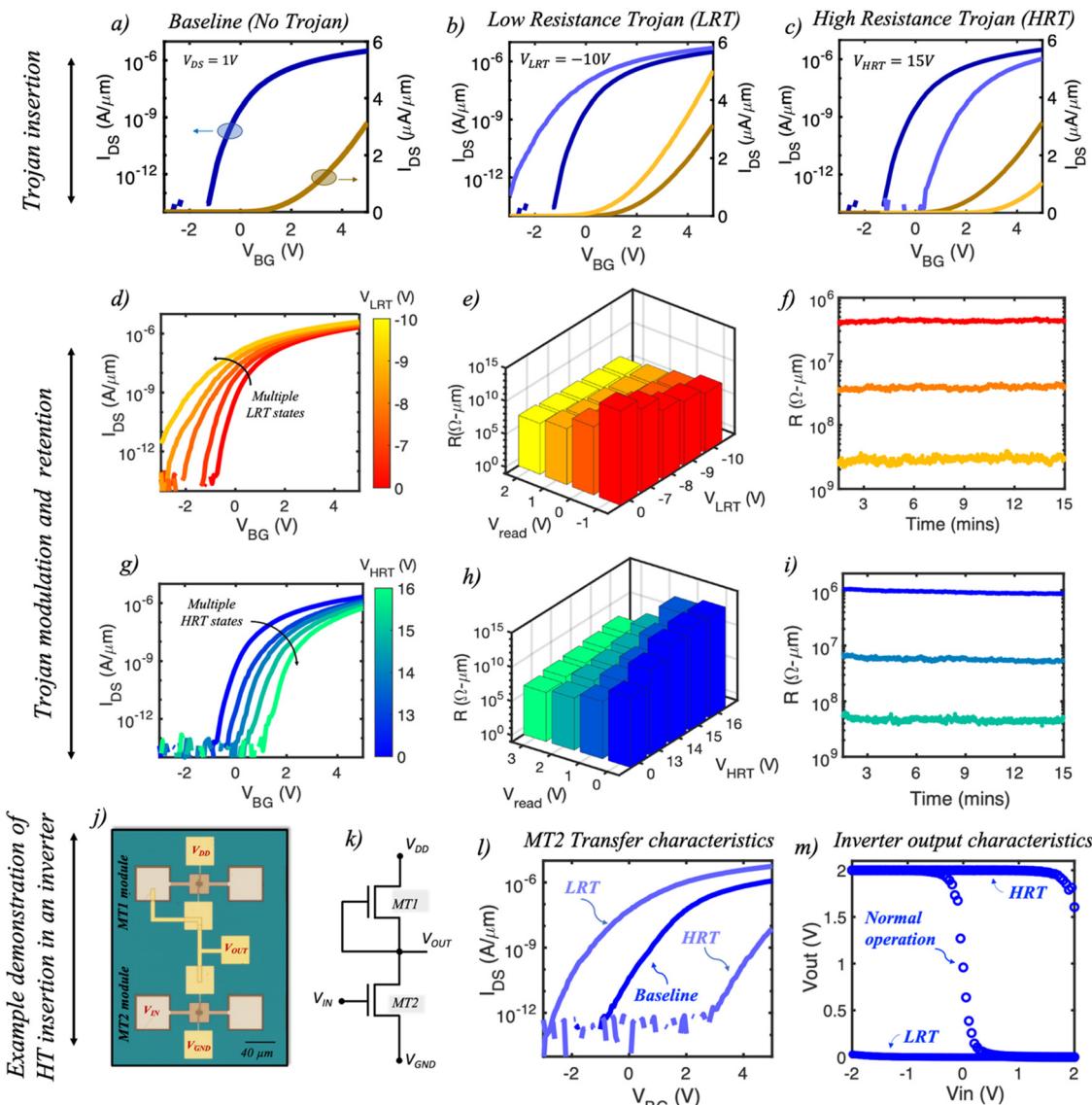


Fig. 2 Basis of non-von-Neumann-based hardware Trojans (HTs) in monolayer MoS₂ memtransistors: (a) Transfer characteristics of a representative memtransistor in three different scenarios: (a) no Trojan, (b) post low resistance Trojan (LRT) insertion and (c) post high resistance Trojan (HRT) insertion. (d) Transfer characteristics of a representative MoS₂ memtransistor for different V_{LRT} magnitudes ranging from -7 V to -10 V and their (e) corresponding resistance values extracted at different $V_{read} = V_{BG}$ values. (f) Retention plot for three different LRT states which were found to be stable over 15 minutes. (g) Transfer characteristics of the same MoS₂ memtransistor for different V_{HRT} magnitudes ranging from 13 V to 16 V and their (h) corresponding resistance values extracted at different $V_{read} = V_{BG}$. (i) Retention plot for three different HRT states which were also stable over 15 minutes. (j) An optical image and a (k) circuit diagram of an inverter, fabricated using a depletion-mode (D-mode) memtransistor (MT1) and an enhancement-mode (E-mode) memtransistor (MT2). (l) Transfer characteristics of MT2, measured pre-Trojan (baseline), post $V_{LRT} = -10\text{ V}$ (LRT) insertion, and post $V_{HRT} = 15\text{ V}$ (HRT) insertion. (m) Inverter output characteristics showing normal operation along with post LRT and HRT operations with clear performance degradation.

tunnelling of electrons/holes, respectively, through the thin tunneling oxide layer (7 nm Al₂O₃) and into the FG, thereby screening the electric field and accounting for the observed V_{TH} shifts. ESI† S2 shows the band diagram associated with the described tunnelling phenomenon. Note that a similar charge trapping phenomenon with a different gate stack has also been extensively discussed in our earlier reports.^{30,53,54} While similar V_{TH} shifts are also observed due to the long-term drifts of the device characteristics as a result of bias-temperature instability (BTI),⁶⁴ the slow and often prolonged nature of the process

renders it infeasible for timely insertion of HTs from an adversary's perspective. Due to their distinct effect on memtransistor characteristics, we have defined the negative voltage pulse as low resistance Trojan voltage (V_{LRT}) and the positive voltage pulse as high resistance Trojan voltage (V_{HRT}). We applied a -10 V and a 15 V bias pulse as V_{LRT} and V_{HRT} , respectively, with a pulse width (τ_w) of $100\text{ }\mu\text{s}$ each, which remains constant for all subsequent discussions. Note that, for our demonstration, V_{LRT} and V_{HRT} are defined as trigger mechanisms whereas the affected logic designs are defined as the payload. Also note that similar

resistive memories have also been demonstrated earlier for memristive^{65,66} and oxide nanosheet materials.⁶⁷

It is also interesting to note that our MoS_2 memtransistors offer the unique capability of modulating both the low resistance Trojan (LRT) and high resistance Trojan (HRT) states as a function of the applied magnitude of V_{LRT} and V_{HRT} , respectively. Although the overall aim is to corrupt or provide faulty logic at the output, the modulation becomes important from a D2D variation point of view which is generally observed across a large population of 2D-memtransistors and can necessitate application of higher or even lower magnitudes of V_{LRT} and V_{HRT} . Fig. 2d shows the transfer characteristics of a representative MoS_2 memtransistor for different V_{LRT} magnitudes ranging from -7 V to -10 V and their corresponding resistance values (Fig. 2e) obtained at different $V_{\text{read}} = V_{\text{BG}}$ values. Two observations can be made from these plots. First, for any given V_{LRT} , the values of LRT states decrease as V_{read} increases. This is expected since the V_{read} values gradually shift from the sub-threshold region towards the ON state. Second, the LRT values also decrease as a function of the magnitude of V_{LRT} at any given V_{read} value. This phenomenon can be attributed to the higher number of electrons tunnelling into the FG with increasing V_{LRT} which results in a larger negative V_{TH} shift. The LRT states were found to be very retentive (Fig. 2f) when measured for over 15 minutes. Similarly, Fig. 2g and h, respectively, show the transfer characteristics for different V_{HRT} magnitudes ranging from 13 V to 16 V and their corresponding resistance values (Fig. 2h) obtained at different $V_{\text{read}} = V_{\text{BG}}$. While following the similar trend as a function of V_{read} values, the HRT states show the converse effect with increasing V_{HRT} magnitude. Once again, this is expected due to the larger positive V_{TH} shift with increasing V_{HRT} magnitude, which would suggest a larger amount of electron tunnelling out of the FG. Note that this ability to electrostatically alter the channel conductance through application of V_{BG} , which acts as the third terminal, is what differentiates our memtransistor architecture from other similar prototypes such as metal-insulator-metal (MIM) structures or memristors, which are simple two terminal devices offering limited tunability and electrostatic control. Like the LRT states, the HRT states were also found to be retentive (Fig. 2i).

Next, as an example demonstration, we successfully inserted a Trojan into an inverter module and corrupted its functionality. An inverter is one of the most fundamental and well-known logic circuits whose output reflects the opposite logic-level of its input. Fig. 2j and k, respectively, show an optical image and a circuit diagram of the inverter, which was using a depletion-mode (D-mode) memtransistor (MT1) and an enhancement-mode (E-mode) memtransistor (MT2). Note that the gate and source terminals of MT1 in our design are shorted in order for it to act as an n-type depletion load in the absence of a p-type memtransistor. Fig. 2l shows the transfer characteristics of MT2, measured as-fabricated (baseline), post $V_{\text{LRT}} = -10\text{ V}$ (LRT) application, and post $V_{\text{HRT}} = 15\text{ V}$ (HRT) application; Fig. 2m shows the inverter output characteristics considering all three scenarios for a representative applied voltage (V_{DD}) of 2 V . For the baseline state, application of $V_{\text{in}} = 0\text{ V}$ (logic state '0') to the gate of MT2 results in $V_{\text{out}} = V_{\text{DD}} = 2\text{ V}$ since, at $V_{\text{BG}} = 0\text{ V}$,

MT2 is highly resistive compared to MT1 (logic state '1'). Conversely, applying $V_{\text{in}} = 2\text{ V}$ (logic state '1') clamps the V_{out} to 0 V (logic state '0') since MT2 is now less resistive than MT1 at $V_{\text{BG}} = 2\text{ V}$. However, post HT insertion, faulty inverter behavior is observed. For both the LRT and the HRT states, respectively, V_{out} always remains clamped to 0 V and 2 V with no apparent transition or switching point. This is because MT2 now remains either always 'ON' (the LRT state) or always 'OFF' (the HRT state) compared to MT1. Interestingly, despite the HRT state of MT2, the inverter exhibits normal operation for $V_{\text{DD}} = 5\text{ V}$ (ESI† S3). Therefore, assuming it continually functions at this higher supply voltage, the presence of HTs remains hidden at $V_{\text{DD}} = 2\text{ V}$ (rare node). It must be noted that, for the LRT state, V_{out} always remains clamped to 0 V regardless of the V_{DD} value. We would also like to point out that for this particular case and the subsequent discussions, the adversary attack model relies on accelerated aging of the IC. Since HT insertion techniques continue to evolve, there is no guarantee that every attack mechanism is addressed. Therefore, run-time monitors are often deployed in ICs as the last line of defense, with the aim to switch the IC operating conditions to a safe mode if an HT is detected.^{68,69} For our MoS_2 IC, this safe mode can only be enabled through higher V_{DD} operations which inevitably lead to higher power consumption and energy dissipation, both of which are detrimental for any circuit/chip operation in terms of its operational lifetime.

Demonstration of in-memory HTs in a three-stage inverter (TSI) circuit

Continuing from the discussion above, here we exploit the degradation observed in the SS of a 2D memtransistor in a cascaded three-stage inverter (TSI) circuit module as a form of HT. Fig. 3a and b, respectively, show the optical image and the corresponding circuit schematic of our TSI design which consists of three inverters connected in series; the V_{out} from a single inverter is fed as the V_{in} to the next stage inverter. Fig. 3c shows the process flow of HT insertion, which begins by first measuring the baseline transfer characteristics of the MT2 from stage 1. Thereafter, the HT is inserted in two steps. First, a V_{HRT} pulse of magnitude 15 V is applied to one of the local gates of MT2, the effect of which can be seen through a large positive V_{TH} shift in the device characteristics. This is followed by the application of a large V_{LRT} pulse of -12 V in an attempt to bring the device back to its baseline state. Interestingly, the device never fully recovers, the evidence of which can be clearly seen through the SS degradation from 243 mV per dec to 420 mV per dec. In order to support this finding, we repeated the experiment with three different individual 2D memtransistors and analyzed their SS both before and after HT insertion with similar results as shown in the 3D bar plot in Fig. 3d. This degradation in SS can be attributed to the development of permanent damage in the underlying Al_2O_3 oxide due to repeated high magnitude voltage stressing of the devices. ESI† S4 shows the transfer characteristics for the three memtransistors pre- and post-HT insertion.

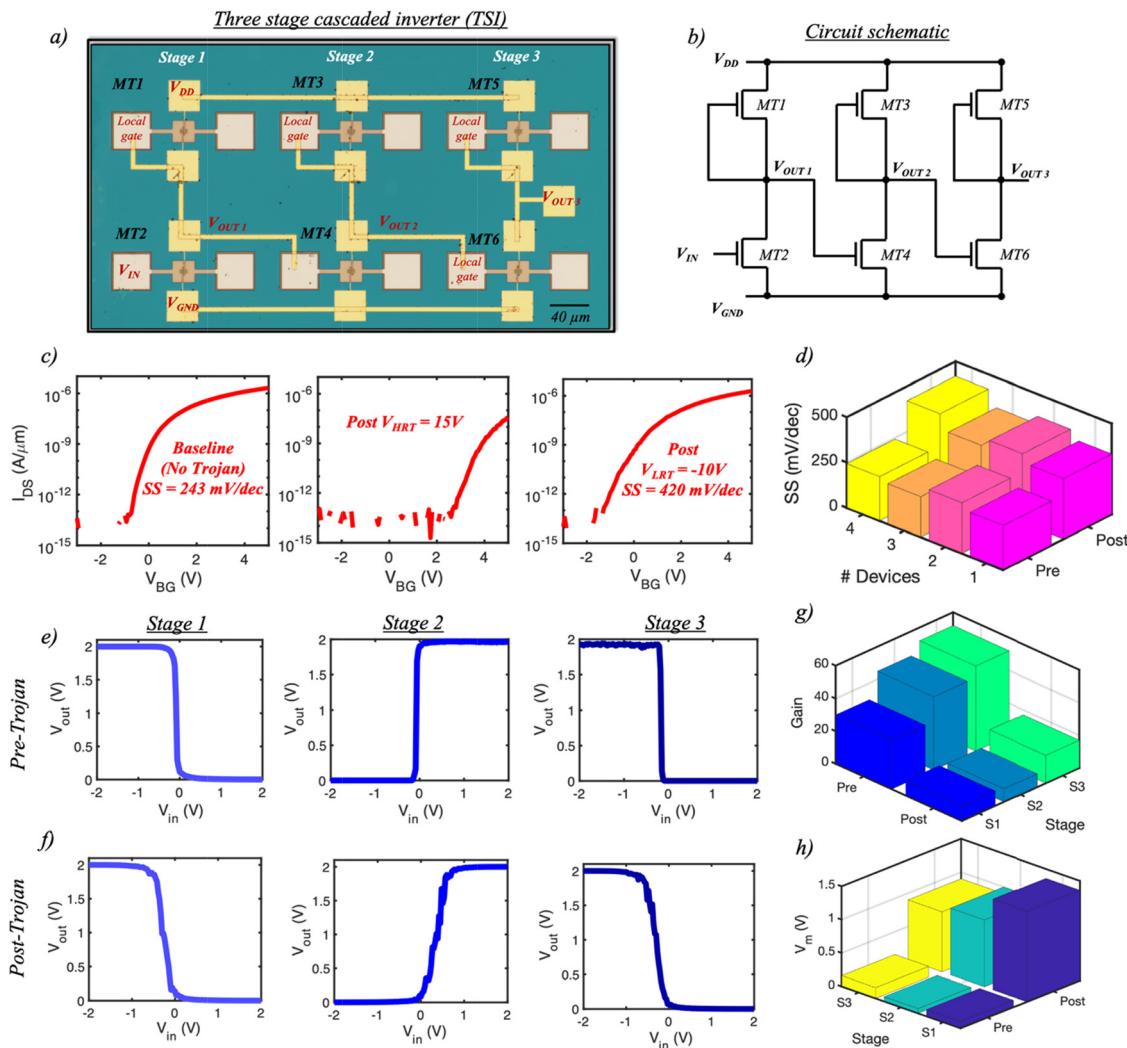


Fig. 3 Demonstration of in-memory HTs in a cascaded three-stage inverter (TSI) circuit: (a) An optical image and the (b) corresponding circuit schematic of our TSI design consisting of three inverters connected in-series where the V_{out} from a single inverter is fed as the V_{in} to the next stage inverter. (c) Evolution of the degradation in subthreshold slope (SS) of MT2 through application of a V_{HRT} pulse of 15 V followed by a V_{LRT} pulse of -10 V to bring the device back to its baseline state. Both the voltage pulses are applied to one of the local gates of MT2 from stage 1. (d) A 3D bar plot showing similar SS degradation for four separate 2D memtransistors which is attributed to permanent damage caused to the underlying Al_2O_3 oxide due to repeated high magnitude voltage stressing of the devices. Inverter output characteristics plots for (e) pre-HT and (f) post-HT clearly showing the deterioration of the overall gain as a result of HT insertion which is further confirmed by (g) analyzing the maximum gain as shown using the 3D bar plot. (h) A 3D bar plot of the extracted V_m which clearly shows a significant positive V_m shift as compared to the original pre-HT state of the inverters.

Next, Fig. 3e and f, respectively, show the inverter output characteristics plots for all the three stages of the cascaded TSI both before and after the HT insertion. The degradation in the gain is clearly visible from the plots. Note that the inverter gain, defined as the slope of the inverter characteristics, *i.e.*, $\frac{dV_{out}}{dV_{in}}$, increases with the number of stages prior to HT insertion. The overall reduction in the maximum gain for all the three stages post-Trojan insertion, as shown using the 3D bar plot in Fig. 3g, is attributed to the degraded SS of MT2. This is because a steeper SS would signify a more rapid change in the corresponding current values as a function of the applied gate-bias, which would, in turn, imply a more abrupt transition between the two logic levels, *i.e.*, $V_{DD} = 2$ V and 0 V. In addition to the SS and the corresponding gain degradation, we also evaluated the

change in the switching voltage (V_m), which is defined as the magnitude of V_{in} for which V_{out} reaches $V_{DD}/2$, for all the inverters by applying a single V_{HRT} pulse of 15 V and length $\tau_w = 100$ μs to MT2. Fig. 3h shows the 3D bar plot of the extracted V_m which clearly shows a significant positive V_m shift as compared to the original pre-HT state of the inverters. ESI† S5 shows the corresponding output inverter plots following V_{HRT} application to MT2 for all the stages.

Demonstration of in-memory HTs in a NOR logic design

Fig. 4a and b, respectively, show the optical image and the circuit schematic of a NOR gate fabricated using our 2D

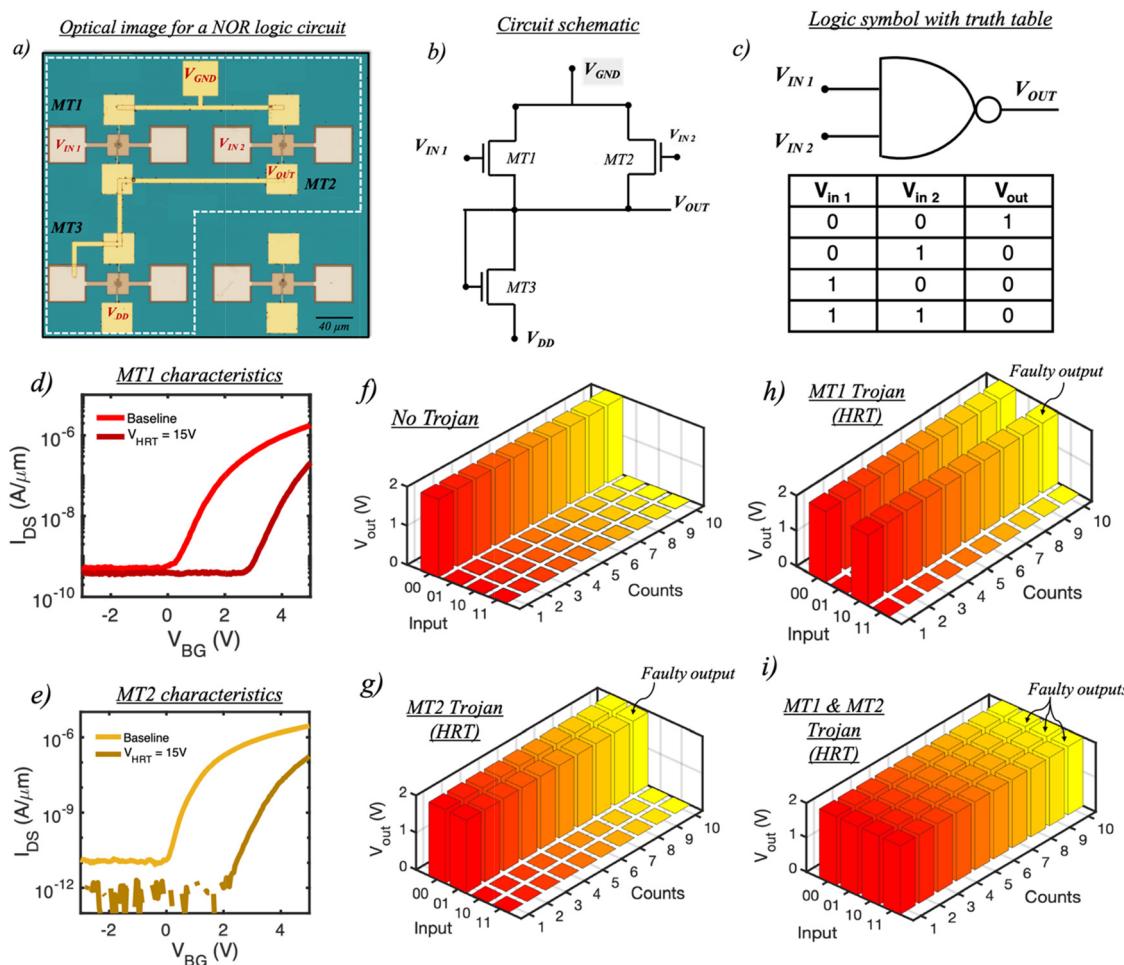


Fig. 4 Demonstration of in-memory HTs in a NOR logic design: (a) An optical image and the (b) circuit schematic of a NOR gate fabricated using two E -mode memtransistors, MT1 and MT2, with a D -mode memtransistor, MT3, along with its (c) logic symbol and truth table. Note that the NOR design is shown within the demarcated white dashed line in the optical image. Transfer characteristics of (d) MT1 and (e) MT2 memtransistors for both the baseline and post $V_{HRT} = 15$ V HT insertion. Output characteristics of the NOR gate for all the possible input combinations under (f) normal operating conditions, which are in agreement with the truth table, (g) post MT2 HT insertion resulting in a corrupt $V_{out} = V_{DD} = 2$ V (logic '1') value for the specific input combination of '01', (h) post MT1 HT insertion resulting in a corrupt $V_{out} = V_{DD} = 2$ V (logic '1') value for the specific input combination of '10', and (i) post MT1 and MT2 HT insertion resulting in a totally corrupt NOR logical operation where, regardless of any input combinations, $V_{out} = V_{DD} = 2$ V.

memtransistors. Note that in the optical image our design is shown within the demarcated white dashed line. A NOR is the negation of the logical OR operation and is also a universal logic gate which operates as per the truth table shown in Fig. 4c. In our design, we have combined two *E*-mode memtransistors, MT1 and MT2, with a *D*-mode memtransistor, MT3. Prior to HT insertion, we first measure the baseline transfer characteristics of both MT1 and MT2 as shown in Fig. 4d and e, respectively. This is followed by measuring the output characteristics of the NOR gate under normal operating conditions for all possible input combinations. As shown in Fig. 4f, $V_{out} = V_{DD} = 2$ V (logic '1') only when both V_{in1} and V_{in2} are at logic '0'. This behavior can be attributed to the highly resistive state of both MT1 and MT2 at $V_{BG} = 0$ V, which effectively clamps the V_{out} to the V_{DD} supply. For all the other input combinations, V_{out} always remains at logic '0' since, at $V_{BG} = 2$ V, either MT1 or MT2, or both, remain at a lower resistance state than MT3, thereby clamping V_{out} to V_{GND} . These results are in agreement

with the truth table shown earlier. Note that to ensure correct logical operations (without HTs), the *E*-mode memtransistors must initially remain OFF at $V_{BG} = 0$ V. Therefore, any memtransistor which conducts at this V_{BG} as a result of the D2D variation must be biased properly through application of a programming pulse.

Next, we demonstrate our capability as an adversary to produce corrupt V_{out} values for specific combinations of $V_{\text{in}1}$ and $V_{\text{in}2}$. For example, it is possible to engineer a faulty V_{out} value for the input combination '01' by simply inserting an HT in MT2 by applying a V_{HRT} pulse of 15 V while keeping MT1 in its baseline state (refer to Fig. 4d and e). In this case, MT2 remains in an HRT state when $V_{\text{BG}} = 2$ V; therefore, for an input combination '01', both MT1 and MT2 now act as an open circuit path which ensures $V_{\text{out}} = V_{\text{DD}} = 2$ V (logic '1') as seen in Fig. 4g. Following a similar logic, applying a V_{HRT} pulse of 15 V to MT1 while keeping MT2 in its baseline state ensures $V_{\text{out}} = V_{\text{DD}} = 2$ V for the input combination '10' as seen in

Fig. 4h. However, in this case, MT1 remains in an HRT state when $V_{BG} = 2$ V. Finally, applying a V_{HRT} pulse of 15 V to both MT1 and MT2 results in a totally corrupt NOR logical operation where, regardless of any input combinations, $V_{out} = V_{DD} = 2$ V as shown in Fig. 4i, which is due to the HRT state of both MT1 and MT2 at $V_{BG} = 2$ V. Once again, when the V_{DD} is scaled to 5 V, the NOR gate resumes its normal functionality, as shown in ESI† S6, while the Trojan remains hidden at a lower V_{DD} supply of 2 V (rare node).

Demonstration of in-memory HTs in a NAND logic design

Fig. 5a and b, respectively, show the optical image and the circuit schematic of a NAND gate fabricated using two *E*-mode memtransistors, MT1 and MT2, that are in series with one *D*-mode memtransistor, MT3. Another universal gate, a NAND produces low output (logic '0') only when all of its inputs are high (logic '1'). Therefore, its output is complemented to that of an AND gate as shown in the truth table in Fig. 5c. Moving along similar lines, we first begin with measuring the baseline transfer characteristics of both MT1 and MT2 as shown in Fig. 5d and e, respectively, followed by the output characteristics (Fig. 5f) prior to HT insertion. Clearly, the expected NAND logic functionality is observed where $V_{out} = V_{DD} = 2$ V (logic '1')

for the input combinations of '00', '01', and '10' due to the high resistive state of both MT1 and/or MT2 compared to MT3. However, for the input combination '11', $V_{out} = V_{GND} = 0$ V (logic '0') since now both MT1 and MT2 become more conductive than MT3. Note that this is in line with the truth table shown earlier. The HT is then inserted by applying a V_{HRT} pulse of 15 V ($\tau_w = 100$ μ s) to the local gate of MT1, which results in the positive shift in the MT1 device characteristics. On remeasuring the NAND, we now see a faulty V_{out} for the input combination of '11'. This behavior is attributed to the HRT state of MT1 which will now always clamp the V_{out} to $V_{DD} = 2$ V. Note that, unlike the NOR logic, our NAND logic design requires HT insertion in only one of the two *E*-mode memtransistors (MT1 or MT2). Once again, despite the presence of HT at the rare node ($V_{DD} = 2$ V), normal NAND functionality is observed for $V_{DD} = 5$ V as shown in ESI† S7.

Demonstration of in-memory HTs in an AND logic design

Finally, Fig. 6a and b, respectively, show the optical image and the circuit schematic of an AND gate with a similar memtransistor configuration to that of a NAND gate except for the switching of the V_{DD} and V_{GND} polarities along with the shorting of the gate terminal of MT3 to V_{GND} . The AND logic can be

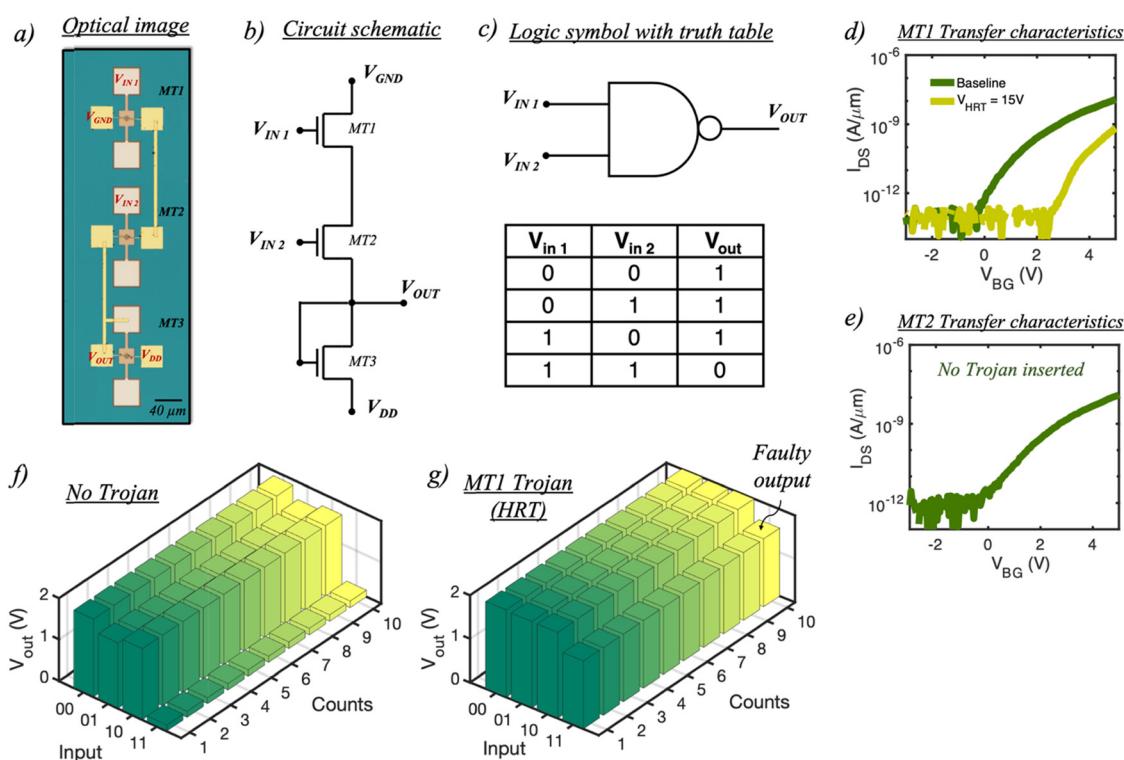


Fig. 5 Demonstration of in-memory HTs in a NAND logic design: (a) An optical image and the (b) circuit schematic of a NAND gate fabricated using two *E*-mode memtransistors, MT1 and MT2, with a *D*-mode memtransistor, MT3, along with its (c) logic symbol and truth table. Transfer characteristics of (d) MT1 for both the baseline and post $V_{HRT} = 15$ V HT insertion along with the baseline transfer characteristics of (e) MT2. Note that for our NAND logic design only one of the two memtransistors require insertion of HT. Output characteristics of the NAND gate for all the possible input combinations under (f) normal operating conditions, which are in agreement with the truth table, and (g) post MT1 HT insertion, resulting in a corrupt $V_{out} = V_{DD} = 2$ V (logic '1') value for the specific input combination of '11'.

summarized using the truth table shown in Fig. 6c where V_{out} remains high (logic 1') only when both $V_{\text{in}1}$ and $V_{\text{in}2}$ are high. Fig. 6d and e, respectively, show the baseline transfer characteristics of MT1 and MT2. Prior to HT insertion, a normal AND logic functionality is observed as shown in Fig. 6f where, for the input combinations of '00', '01', or '10', $V_{\text{out}} = V_{\text{GND}} = 0 \text{ V}$ (logic '0') since either one or both MT1 and MT2 are more resistive than MT3. However, for the input '11', MT1 and MT2 become more conductive than MT3, which clamps V_{out} to $V_{\text{DD}} = 2 \text{ V}$ (logic '1'). Next, the HT is inserted by applying a V_{LRT} pulse of -15 V ($\tau_w = 100 \mu\text{s}$) to both MT1 and MT2, resulting in a negative V_{TH} shift as seen in Fig. 6d and e. The effect of inserting this HT can be understood by once again observing the output characteristics, as shown in Fig. 6g where now regardless of the input combination, $V_{\text{out}} = V_{\text{DD}} = 2 \text{ V}$ (logic '1') since both MT1 and MT2 are in the LRT state and offer a more conductive path compared to MT3.

Enabling complete failure of logic designs with in-memory HTs

In addition to corrupting the circuit outputs for a particular set of input combinations, it is also possible for an adversary to engineer a complete failure or malfunction of the logic designs using the

described in-memory HT insertion technique. In this context, we define a complete logic failure as a scenario where V_{out} always remains low (logic '0') regardless of the input combination. In other words, the chip becomes completely non-functional. Fig. 7a and c, respectively, show the transfer characteristics of MT1 and MT2 in the NOR, NAND, and AND logic designs measured for both baseline and post-HT configurations. Note that in each case, the type of HT inserted (V_{LRT} or V_{HRT}) would be different. For example, in order to make the NOR and NAND logic malfunction, a V_{LRT} pulse of -15 V ($\tau_w = 100 \mu\text{s}$) is applied to both MT1 and MT2, whereas the AND logic malfunctioning requires an application of a V_{HRT} pulse of 15 V ($\tau_w = 100 \mu\text{s}$). On observing their respective output characteristics, as shown in Fig. 7d-f, it is evident that each logic design has malfunctioned since $V_{\text{out}} = V_{\text{GND}} = 0 \text{ V}$ (logic '0') for all input combinations. In the case of the NOR and NAND logic design, this can be attributed to the LRT state of both MT1 and MT2, whereas for the AND logic design, both MT1 and MT2 are in the HRT state compared to MT3.

Trojan lifetime and detection countermeasures avoidance

From the above discussions, it is abundantly clear that from an adversary's perspective, the ultimate goal is to enable an HT

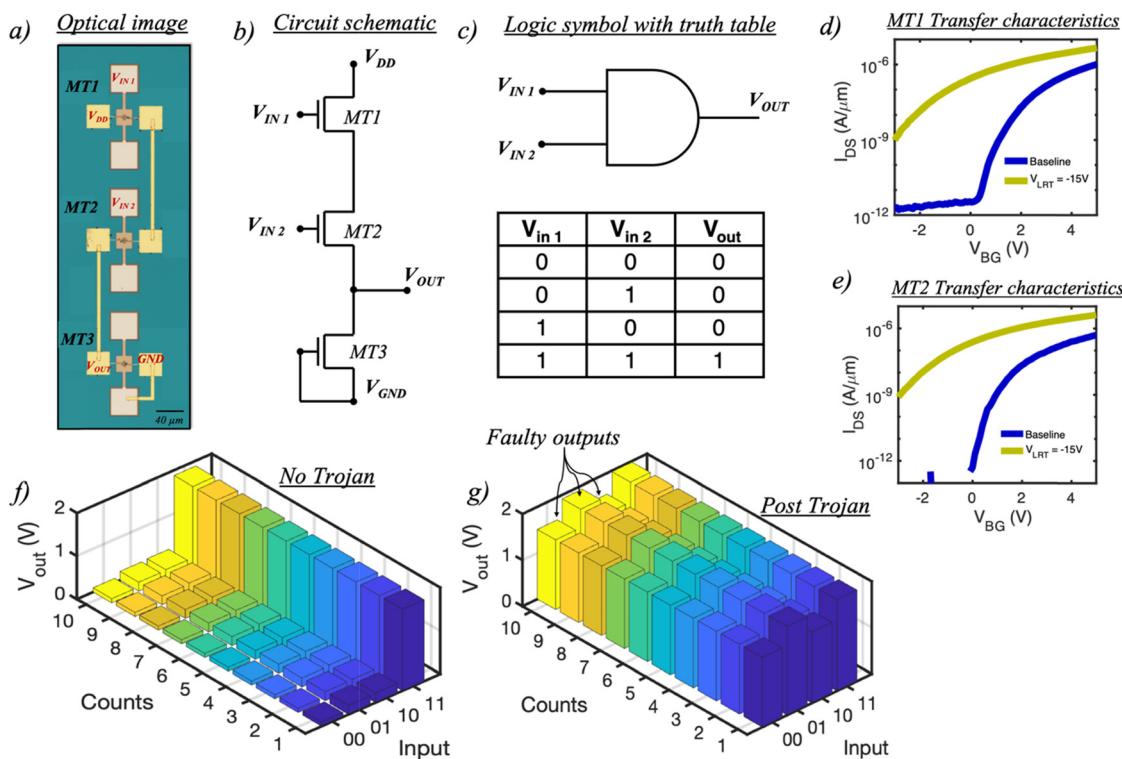


Fig. 6 Demonstration of in-memory HTs in an AND logic design: (a) An optical image and the (b) circuit schematic of a NAND gate fabricated using two E-mode memtransistors, MT1 and MT2, with a D-mode memtransistor, MT3, along with its (c) logic symbol and truth table. Transfer characteristics of (d) MT1 and (e) MT2 at both the baseline and post $V_{\text{LRT}} = -15 \text{ V}$ HT insertion. Note that for our AND logic design both memtransistors require insertion of HT. Output characteristics of the AND gate for all possible input combinations under (f) normal operating conditions where, for the input combinations of '00', '01', or '10', $V_{\text{out}} = V_{\text{GND}} = 0 \text{ V}$ (logic '0') since either one or both MT1 and MT2 are more resistive than MT3 and (g) post MT1 and MT2 HT insertion where, regardless of the input combination, $V_{\text{out}} = V_{\text{DD}} = 2 \text{ V}$ (logic '1') since both MT1 and MT2 are now in the LRT state and offer a more conductive path compared to MT3.

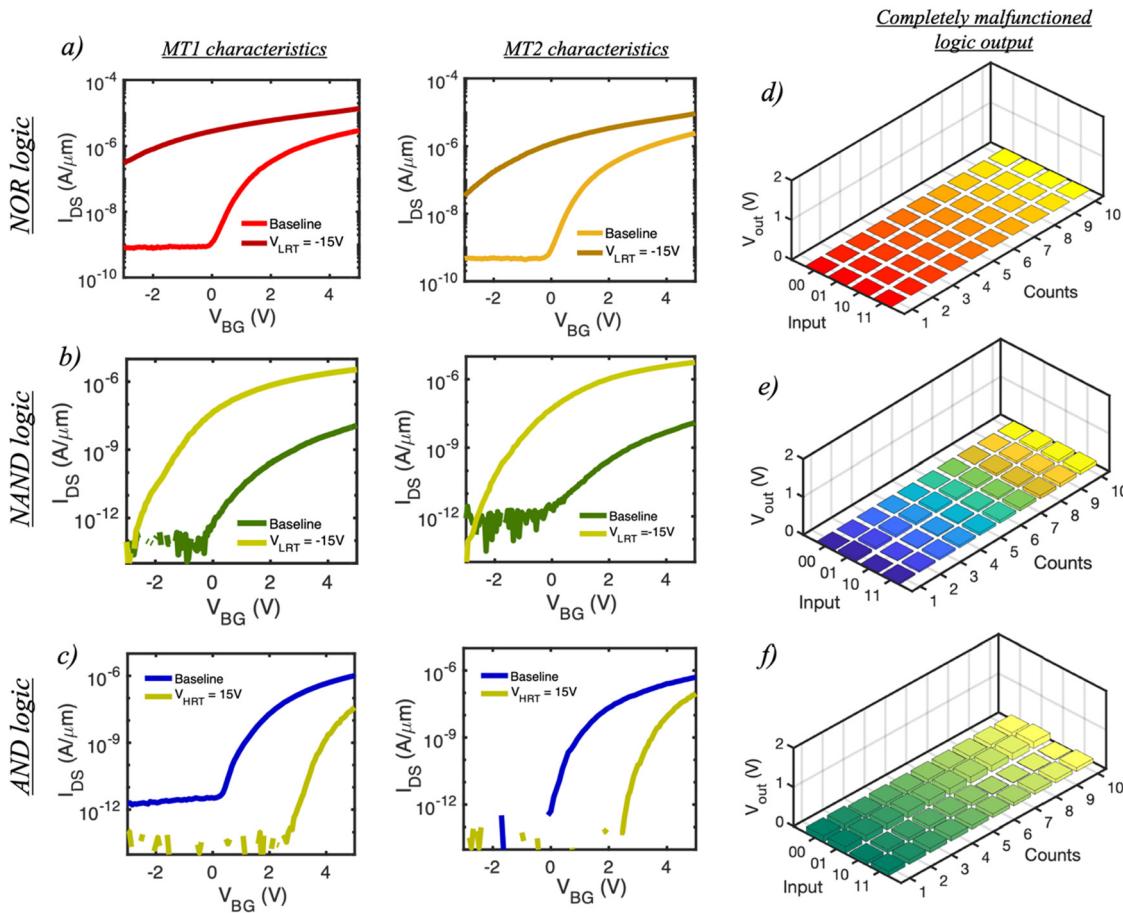


Fig. 7 Enabling complete failure of logic designs with in-memory HT: Transfer characteristics of MT1 and MT2 measured for the (a) NOR, (b) NAND, and (c) AND logic designs under both baseline and post-HT configurations. (d–f) Malfunctioned output characteristics for each respective logic design since $V_{\text{out}} = V_{\text{GND}} = 0$ V (logic '0') regardless of the input combinations. In case of the NOR and NAND logic design, this can be attributed to the LRT state of both MT1 and MT2, whereas for the AND logic design, both MT1 and MT2 are in the HRT state compared to MT3. It must be noted the type of HT inserted (V_{LRT} or V_{HRT}) is different for each individual design. For example, in order to make the NOR and NAND logic malfunction, a V_{LRT} pulse of -15 V ($\tau_w = 100$ μ s) is applied to both MT1 and MT2, whereas the AND logic malfunctioning requires an application of a V_{HRT} pulse of -15 V ($\tau_w = 100$ μ s).

attack mechanism which is precise and stealthy, with a small footprint such that it is capable of evading detection countermeasures.⁷⁰ For our in-memory HT demonstration, we have achieved all of the aforementioned requirements. First, despite the V_{TH} shifts observed as a result of V_{LRT} or V_{HRT} application, the presence of the HT is obscured since the electrical measurements of the affected individual 2D memtransistor do not offer any additional information. Although it can be argued that the device performance parameters such as SS and I_{ON} values degrade slightly, these parameters are more likely to be attributed to fabrication constraints and D2D variation related factors. Furthermore, our HT injection scheme also fulfills the criteria of having a small footprint since the HT can be triggered (V_{LRT} and V_{HRT} application) without requiring any additional peripheral components within the design.

Additionally, from our point of view as an adversary, a good retention of both LRT and HRT states is desirable for delivering the payload. Therefore, we examined the extended retention of our memtransistors for two different states over a total of 10^4 seconds, or ~ 3 hours (ESI† S8). Although the two memory states

will eventually converge after ~ 15 hours, as evident through the slow collapse of the memory ratio (MR) due to an exponential decay, an adversary can employ this attribute to cause catastrophic malfunctions and failures in critical technological infrastructure such as military equipment and aircraft navigation and still evade detection since the presence of HTs can only be confirmed if the black box retrieved from the failed equipment is analyzed within the MR retention time frame. As soon as the MR window vanishes and the HT disappears, no evidence of a Trojan ever being inserted can be recovered. Note that this decay might seem counterintuitive as far as deliberately aging or causing a total logic malfunction of the IC is concerned. This is because both of these adversarial intentions would ideally require the HT to be present within an IC at all times. However, in the present day's era of stiff market competition and time-to-market demands requiring increased productivity and shorter design time, any degradation or malfunction observed within this global supply chain will likely result in the affected IP being discarded completely, leading to severe monetary loss in addition to reputational dissolution for the involved parties.

Conclusions

In conclusion, we have exploited and exposed the vulnerability of the in-memory computing architecture to insert hardware Trojans (HTs) within basic digital logic designs such as AND, NAND, NOR and NOT gates fabricated using monolayer MoS₂ memtransistors. In addition, we have also exploited the degradation in subthreshold slope (SS) due to the presence of HTs to drastically compromise the performance of a cascaded three stage inverter (TSI). The HT is inserted by applying an electrical voltage pulse (V_{HRT} or V_{LRT}) to the local gate of our memtransistor devices, programming them into either HRT or LRT states which significantly corrupts and even causes complete logic malfunction within our circuit. This ability to enable both the LRT and HRT states as a function of the applied magnitude of V_{LRT} and V_{HRT} can be attributed to the tunnelling of charge carriers across the 7 nm Al₂O₃ into the HfO₂ charge-trapping layer due to the Fowler Nordheim tunneling process. Moreover, the Trojan remains hidden within the rare node during the normal operation of the logic designs at a higher $V_{\text{DD}} = 5$ V and only gets activated when the supply voltage is scaled down ($V_{\text{DD}} = 2$ V). These results are not just limited to 2D-based technologies but are applicable to any state-of-the-art in-memory computing architecture. Our approach in the role of an adversary offers a rather unconventional, uncomfortable, and eye-opening insight into the vulnerabilities of in-memory computing in today's highly complex and globalized IP supply chain system, which can be exploited in unimaginable ways to compromise the security, reliability, and even the lifetime of electronic components.

Methods

Large area monolayer MoS₂ film growth

The metal-organic chemical vapor deposition (MOCVD) technique was used to deposit monolayer MoS₂ on an epi-ready 2" c-sapphire substrate. A cold-wall horizontal reactor with an inductively heated graphite susceptor and a wafer rotation was utilized to assist in achieving a uniform monolayer deposition.⁷¹ Molybdenum hexa-carbonyl (Mo (CO)₆) and hydrogen sulfide (H₂S) were used as precursors. Prior to the material growth, the substrate was heated to 1000 °C in H₂ and maintained for 10 min. (Mo (CO)₆). For the growth process, Mo (CO)₆ was maintained at 10 °C and 650 Torr in a stainless-steel bubbler to deliver 1.1×10^3 sccm of the metal precursor along with 400 sccm of H₂S. The monolayer MoS₂ deposition was achieved in 18 min at 950 °C in 50 Torr H₂ ambient. Following the growth of the MoS₂ film, the substrate was cooled down to 300 °C in H₂S to prevent its decomposition. More details can be found in our earlier work.^{51,72,73}

Fabrication of local back-gate islands

To define the features with local gate island configuration, the 285 nm SiO₂ on the p⁺⁺-Si substrate (commercially purchased) was first spin-coated with a bilayer poly(methyl methacrylate) or PMMA resist in a two-step process and subsequently baked at 185 °C and 95 °C for 60 s and 90 s, respectively. Next, an EBPG

5200 Vistec Electron Beam Lithography tool was used to pattern the individual islands. The exposed resist was developed using a 4-methyl-2-pentanone (MIBK) and 2-propanol (IPA) solution in a 1:1 mixture. Following a sputter cleaning of the substrate with O₂ plasma, the local-gate electrodes comprising Ti/Pt (20/50 nm) layers were deposited using a Temescal e-beam evaporator. This was followed by lifting off the excess metal in a cold acetone bath. Next, the atomic layer deposition (ALD) process was performed to grow the Al₂O₃/HfO₂/Al₂O₃ layers. Subsequently, a Heidelberg Maskless Aligner (MLA 150) was utilized to pattern and subsequently define the access points to the local back-gate electrodes. The excess oxide in the exposed areas was subsequently removed using BCl₃ based reactive ion etch (RIE) chemistry.

MoS₂ film transfer to local back-gate islands

In order to fabricate the MoS₂ memtransistors, transfer of monolayer MoS₂ films from the growth substrate (sapphire) to the application substrate (SiO₂/p⁺⁺-Si) with local back-gate islands is the first step. This was achieved using a polymethyl-methacrylate (PMMA) assisted wet transfer process. First, the sapphire substrate with the monolayer film was spin-coated with PMMA and left idle for 24 hours in order to ensure good adhesion between PMMA and MoS₂. Next, the corners of the spin-coated film were lightly scratched with a razor blade followed by its immersion in a 2 M NaOH solution at 90 °C. Owing to the hydrophilic and hydrophobic nature of sapphire and MoS₂/PMMA, respectively, NaOH is drawn towards the substrate/MoS₂ interface due to the capillary action thereby separating the PMMA/MoS₂ stack from the sapphire substrate. Using a clean glass slide, the separated film is then carefully taken out from the NaOH solution and rinsed in three separate water baths for 15 minutes each before being finally transferred onto the application substrate. Post-transfer, the substrate is baked at 50 °C and 70 °C for 10 min each in order to remove the excess moisture and promote good film adhesion. This ensures a pristine interface. Finally, the PMMA is removed using acetone followed by a final cleanse with IPA.

Fabrication of 2D memtransistors

For fabricating MoS₂ memtransistors, the substrate with MoS₂ on-top was spin-coated with PMMA and baked at 180 °C for 90 s. Electron beam (e-beam) lithography was used to define the features by exposing the resist which was subsequently developed using a 1:1 mixture of 4-methyl-2-pentanone (MIBK) and IPA for 60 seconds and 45 seconds, respectively. The exposed monolayer MoS₂ film was etched using a sulfur hexafluoride (SF₆) RIE at 5 °C for 30 s followed by an acetone and IPA rinse to remove the e-beam resist. Next, the sample was again spin-coated with methyl methacrylate (MMA) and A3 PMMA resist which was accompanied by E-beam lithography to define the source and drain contacts. The subsequent developing was once again carried out using a 1:1 mixture of MIBK and IPA for the same times as previously described. Finally, nickel/gold (40/30 nm) metal contacts were deposited using e-beam evaporation followed by a lift-off process to remove the evaporated

Ni/Au except from the source/drain patterns by immersing the sample in acetone for 30 min followed by IPA for another 30 min.

Multidevice integration

The connections between individual memtransistors were achieved using similar resist, e-beam lithography, and development processes as discussed previously. The interconnect metals Ni/Au (60/30 nm) were deposited using an E-beam evaporator. A greater metal thickness was required compared to the source/drain contacts due to the requirement for a conformal metal coating over/along the sidewalls. Finally, the e-beam resist was removed using a lift-off process with acetone and IPA.

Electrical characterization

The electrical measurements for devices and circuits were performed in a Lake Shore CRX-VF probe station in air using a Keysight B1500A parameter analyzer.

Data availability

The experimental data generated in this study and codes used to analyze them are available from the corresponding author on reasonable request.

Author contributions

A. W. and S. D. conceived the idea, designed the experiments and wrote the manuscript. H. R. fabricated the logic circuits. A. W., and H. R. performed the experiments. A. W., H. R., and S. D. analyzed the data, discussed the results and agreed on their implications. All authors contributed to the preparation of this manuscript.

Conflicts of interest

The authors declare no conflicts of interest.

Acknowledgements

This work was supported by the National Science Foundation (NSF) through CAREER Award under Grant Number ECCS-2042154. The authors also acknowledge the support from The Pennsylvania State University 2D Crystal Consortium-Materials Innovation Platform (2DCCMIP) for the material growth under NSF cooperative agreement DMR-2039351.

References

- 1 L. Yin, R. Cheng, Y. Wen, C. Liu and J. He, *Adv. Mater.*, 2021, **33**, 2007081.
- 2 O. Mutlu, S. Ghose, J. Gómez-Luna and R. Ausavarungnirun, *Microprocess. Microsyst.*, 2019, **67**, 28–41.
- 3 D. U. Lee, K. W. Kim, K. W. Kim, H. Kim, J. Y. Kim, Y. J. Park, J. H. Kim, D. S. Kim, H. B. Park and J. W. Shin, IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014, pp. 432–433.
- 4 J. T. Pawlowski, IEEE Hot chips 23 symposium (HCS), 2011, pp. 1–24.
- 5 S. W. Keckler, W. J. Dally, B. Khailany, M. Garland and D. Glasco, *IEEE micro*, 2011, **31**, 7–17.
- 6 M. Horowitz, 2014.
- 7 A. Sebastian, M. Le Gallo, R. Khaddam-Aljameh and E. Eleftheriou, *Nat. Nanotechnol.*, 2020, **15**, 529–544.
- 8 G. Indiveri and S.-C. Liu, *Proc. IEEE*, 2015, **103**, 1379–1397.
- 9 M. Di Ventra and Y. V. Pershin, *Nat. Phys.*, 2013, **9**, 200–202.
- 10 H. Jia, H. Valavi, Y. Tang, J. Zhang and N. Verma, *IEEE, J. Solid State Circ.*, 2020, **55**, 2609–2621.
- 11 Z. Jiang, S. Yin, J.-S. Seo and M. Seok, *IEEE, J. Solid State Circ.*, 2020, **55**, 1888–1897.
- 12 C. Ríos, N. Youngblood, Z. Cheng, M. Le Gallo, W. H. Pernice, C. D. Wright, A. Sebastian and H. Bhaskaran, *Sci. Adv.*, 2019, **5**, eaau5759.
- 13 D. Ielmini and H.-S. P. Wong, *Nat. Electron.*, 2018, **1**, 333–343.
- 14 S. Adey, *IEEE Spectrum*, 2008, **45**, 34–39.
- 15 J. Kumagai, *IEEE Spectrum*, 2000, **37**, 43–48.
- 16 R. S. Chakraborty, S. Narasimhan and S. Bhunia, IEEE International high level design validation and test workshop, 2011, pp. 166–171.
- 17 M. Tehranipoor and F. Koushanfar, *IEEE Des. Test comput.*, 2010, **27**, 10–25.
- 18 Y. Alkabani and F. Koushanfar, Proceedings of the 2009 international conference on computer-aided design, 2009, pp. 123–127.
- 19 S. Bhunia, M. S. Hsiao, M. Banga and S. Narasimhan, *Proc. IEEE*, 2014, **102**, 1229–1247.
- 20 S. Bhunia and M. Tehranipoor, *The hardware trojan war*, Springer, Cham, Switzerland, 2018.
- 21 R. S. Chakraborty, I. Saha, A. Palchaudhuri and G. K. Naik, *IEEE Des. Test*, 2013, **30**, 45–54.
- 22 M. Potkonjak, Proceedings of the 47th Design Automation Conference, 2010, pp. 633–634.
- 23 L. Lin, W. Burleson and C. Paar, IEEE/ACM International Conference on Computer-Aided Design-Digest of Technical Papers, 2009, pp. 117–122.
- 24 S. S. Ali, R. S. Chakraborty, D. Mukhopadhyay and S. Bhunia, Design, Automation & Test in Europe, 2011, pp. 1–4.
- 25 A. Wali, S. Kundu, A. J. Arnold, G. Zhao, K. Basu and S. Das, *ACS Nano*, 2021, **15**, 3453–3467.
- 26 P. Wu, D. Reis, X. S. Hu and J. Appenzeller, *Nat. Electron.*, 2021, **4**, 45–53.
- 27 A. Dodd, S. S. Radhakrishnan, T. F. Schranghamer, D. Buzzell, P. Sengupta and S. Das, *Nat. Electron.*, 2021, **4**, 364–374.
- 28 C. Wen, X. Li, T. Zanotti, F. M. Puglisi, Y. Shi, F. Saiz, A. Antidormi, S. Roche, W. Zheng and X. Liang, *Adv. Mater.*, 2021, 2100185.
- 29 A. Oberoi, A. Dodd, H. Liu, M. Terrones and S. Das, *ACS Nano*, 2021, **15**, 19815–19827.
- 30 A. Wali, H. Ravichandran and S. Das, *ACS Nano*, 2021, **15**, 17804–17812.

31 A. Biswas and A. P. Chandrakasan, *IEEE International Solid-State Circuits Conference-(ISSCC)*, 2018, pp. 488–490.

32 A. Jaiswal, I. Chakraborty, A. Agrawal and K. Roy, *IEEE Trans. VLSI Syst.*, 2019, **27**, 2556–2567.

33 C.-X. Xue, Y.-C. Chiu, T.-W. Liu, T.-Y. Huang, J.-S. Liu, T.-W. Chang, H.-Y. Kao, J.-H. Wang, S.-Y. Wei and C.-Y. Lee, *Nat. Electron.*, 2021, **4**, 81–90.

34 H.-S. P. Wong, H.-Y. Lee, S. Yu, Y.-S. Chen, Y. Wu, P.-S. Chen, B. Lee, F. T. Chen and M.-J. Tsai, *Proc. IEEE*, 2012, **100**, 1951–1970.

35 W. Zhang, R. Mazzarello, M. Wuttig and E. Ma, *Nat. Rev. Mater.*, 2019, **4**, 150–168.

36 C. D. Wright, P. Hosseini and J. A. V. Diosdado, *Adv. Funct. Mater.*, 2013, **23**, 2248–2254.

37 X. Fong, Y. Kim, K. Yogendra, D. Fan, A. Sengupta, A. Raghunathan and K. Roy, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2015, **35**, 1–22.

38 D. Fan, S. Angizi and Z. He, 2017.

39 D. W. Graham, E. Farquhar, B. Degnan, C. Gordon and P. Hasler, *IEEE Trans. Circuits Syst. I*, 2007, **54**, 951–963.

40 L. Danial, E. Pikhay, E. Herbelin, N. Wainstein, V. Gupta, N. Wald, Y. Roizin, R. Daniel and S. Kvatin斯基, *Nat. Electron.*, 2019, **2**, 596–605.

41 J. Hoffman, X. Pan, J. W. Reiner, F. J. Walker, J. Han, C. H. Ahn and T. Ma, *Adv. Mater.*, 2010, **22**, 2957–2961.

42 A. I. Khan, A. Keshavarzi and S. Datta, *Nat. Electron.*, 2020, **3**, 588–597.

43 C. E. Graves, C. Li, X. Sheng, D. Miller, J. Ignowski, L. Kiyama and J. P. Strachan, *Adv. Mater.*, 2020, **32**, 2003437.

44 C. Li, D. Belkin, Y. Li, P. Yan, M. Hu, N. Ge, H. Jiang, E. Montgomery, P. Lin and Z. Wang, *IEEE International Memory Workshop (IMW)*, 2018, pp. 1–4.

45 D. Akinwande, C. Huyghebaert, C.-H. Wang, M. I. Serna, S. Goossens, L.-J. Li, H.-S. P. Wong and F. H. Koppens, *Nature*, 2019, **573**, 507–518.

46 N. Li, Q. Wang, C. Shen, Z. Wei, H. Yu, J. Zhao, X. Lu, G. Wang, C. He and L. Xie, *Nat. Electron.*, 2020, **3**, 711–717.

47 Z. Lin, Y. Liu, U. Halim, M. Ding, Y. Liu, Y. Wang, C. Jia, P. Chen, X. Duan and C. Wang, *Nature*, 2018, **562**, 254–258.

48 C. Liu, H. Chen, S. Wang, Q. Liu, Y.-G. Jiang, D. W. Zhang, M. Liu and P. Zhou, *Nat. Nanotechnol.*, 2020, **15**, 545–557.

49 K. S. Novoselov, A. K. Geim, S. V. Morozov, D.-E. Jiang, Y. Zhang, S. V. Dubonos, I. V. Grigorieva and A. A. Firsov, *Science*, 2004, **306**, 666–669.

50 W. Cao, J. Kang, D. Sarkar, W. Liu and K. Banerjee, *IEEE Trans. Electron Devices*, 2015, **62**, 3459–3469.

51 A. Sebastian, R. Pendurthi, T. H. Choudhury, J. M. Redwing and S. Das, *Nat. Commun.*, 2021, **12**, 1–12.

52 S. Das, A. Sebastian, E. Pop, C. J. McClellan, A. D. Franklin, T. Grasser, T. Knobloch, Y. Illarionov, A. V. Penumatcha and J. Appenzeller, *Nat. Electron.*, 2021, **4**, 786–799.

53 A. Sebastian, S. Das and S. Das, *Adv. Mater.*, 2022, **34**, 2107076.

54 A. Dodd, N. Trainor, J. Redwing and S. Das, *Nat. Commun.*, 2022, **13**, 1–12.

55 R. Cheng, L. Yin, F. Wang, Z. Wang, J. Wang, Y. Wen, W. Huang, M. G. Sendeku, L. Feng and Y. Liu, *Adv. Mater.*, 2019, **31**, 1901144.

56 M. Wang, S. Cai, C. Pan, C. Wang, X. Lian, Y. Zhuo, K. Xu, T. Cao, X. Pan and B. Wang, *Nat. Electron.*, 2018, **1**, 130–136.

57 Y. Wang, E. Liu, A. Gao, T. Cao, M. Long, C. Pan, L. Zhang, J. Zeng, C. Wang and W. Hu, *ACS Nano*, 2018, **12**, 9513–9520.

58 R. Cheng, F. Wang, L. Yin, Z. Wang, Y. Wen, T. A. Shifa and J. He, *Nat. Electron.*, 2018, **1**, 356–361.

59 X. Zhu, D. Li, X. Liang and W. D. Lu, *Nat. Mater.*, 2019, **18**, 141–148.

60 S. Das, H. Y. Chen, A. V. Penumatcha and J. Appenzeller, *Nano Lett.*, 2013, **13**, 100–105.

61 S. Das, H.-Y. Chen, A. V. Penumatcha and J. Appenzeller, *Nano Lett.*, 2013, **13**, 100–105.

62 P.-C. Shen, C. Su, Y. Lin, A.-S. Chou, C.-C. Cheng, J.-H. Park, M.-H. Chiu, A.-Y. Lu, H.-L. Tang, M. M. Tavakoli, G. Pitner, X. Ji, Z. Cai, N. Mao, J. Wang, V. Tung, J. Li, J. Bokor, A. Zettl, C.-I. Wu, T. Palacios, L.-J. Li and J. Kong, *Nature*, 2021, **593**, 211–217.

63 M. Lenzlinger and E. Snow, *J. Appl. Phys.*, 1969, **40**, 278–283.

64 Y. Y. Illarionov, K. K. Smithe, M. Waltl, T. Knobloch, E. Pop and T. Grasser, *IEEE Electron Device Lett.*, 2017, **38**, 1763–1766.

65 A. C. Khot, T. D. Dongale, K. A. Nirmal, J. H. Sung, H. J. Lee, R. D. Nikam and T. G. Kim, *ACS Appl. Mater. Interfaces*, 2022, **14**, 10546–10557.

66 W. Huh, D. Lee and C. H. Lee, *Adv. Mater.*, 2020, **32**, 2002092.

67 A. C. Khot, T. D. Dongale, J. H. Park, A. V. Kesavan and T. G. Kim, *ACS Appl. Mater. Interfaces*, 2021, **13**, 5216–5227.

68 A. Valdes-Garcia, R. Venkatasubramanian, J. Silva-Martinez and E. Sánchez-Sinencio, *IEEE Trans. Instrum. Meas.*, 2008, **57**, 1470–1477.

69 H. Le Gall, R. Alhakim, M. Valka, S. Mir, H.-G. Stratigopoulos and E. Simeu, 20th IEEE European Test Symposium (ETS), 2015, pp. 1–6.

70 A. Pavlidis, E. Faehn, M.-M. Louérat and H.-G. Stratigopoulos, 40th IEEE VLSI Test Symposium, 2022.

71 Y. Xuan, A. Jain, S. Zafar, R. Lotfi, N. Nayir, Y. Wang, T. H. Choudhury, S. Wright, J. Feraca and L. Rosenbaum, *J. Cryst. Grow.*, 2019, **527**, 125247.

72 A. Dodd, A. Oberoi, A. Sebastian, T. H. Choudhury, J. M. Redwing and S. Das, *Nat. Commun.*, 2020, **11**, 1–11.

73 D. Jayachandran, A. Oberoi, A. Sebastian, T. H. Choudhury, B. Shankar, J. M. Redwing and S. Das, *Nat. Electron.*, 2020, **3**, 646–655.