SAT-Attack Resistant Hardware Obfuscation using Camouflaged Two-Dimensional Heterostructure Devices

Akshay Wali
Pennsylvania State University https://orcid.org/0000-0002-4632-687X
Andrew Arnold
Pennsylvania State University
Shamik Kundu
University of Texas at Dallas
Soumyadeep Choudhury
University of Texas at Dallas
Kanad Basu
University of Texas at Dallas
Saptarshi Das (sud70@psu.edu)
Pennsylvania State University https://orcid.org/0000-0002-0188-945X

Article

Keywords: Reverse engineering, integrated circuit, TMO/TMD heterostructures, SAT-attack resistant hardware

Posted Date: September 30th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-81183/v1

SAT-Attack Resistant Hardware Obfuscation using Camouflaged Two-Dimensional Heterostructure Devices

Akshay Wali[1], Andrew Arnold[1], Shamik Kundu[2], Soumyadeep Chowdhury[2], Kanad Basu[2] and Saptarshi Das[3,4,5,]*

[1]Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802, USA

[2]Department of Electrical and Computer Engineering, University of Texas at Dallas, Richardson, TX 75080, USA

[3]Department of Engineering Science and Mechanics, Pennsylvania State University, University Park, PA 16802, USA

[4]Department of Materials Science and Engineering, Pennsylvania State University, University Park, PA 16802, USA

[5]Materials Research Institute, Pennsylvania State University, University Park, PA 16802, USA

Abstract: Reverse engineering (RE) is one of the major security threats to the semiconductor industry due to the involvement of untrustworthy parties in an increasingly globalized chip manufacturing supply chain [1-5]. RE efforts have already been successful in extracting device level functionalities from an integrated circuit (IC) with very limited resources [6]. Camouflaging is an obfuscation method that can thwart such RE [7-9]. Existing work on IC camouflaging primarily uses fabrication techniques such as doping and dummy contacts to hide the circuit structure or build cells that look alike but have different functionalities. While promising these Si complementary metal oxide semiconductor (CMOS) based obfuscation techniques adds significant area overhead and are successfully decamouflaged

by the Satisfiability solver (SAT)-based reverse engineering techniques [9-13]. Emerging solutions, such as polymorphic gates based on giant spin Hall effect (GSHE) are promising but adds delay overhead in hybrid CMOS-GSHE designs restricting the camouflaging to a maximum of 15% of all the gates in the circuit. Here, we harness the unique properties of two-dimensional (2D) transition metal dichalcogenides (TMDs) including MoS_2, $MoSe_2$, $MoTe_2$, WS_2, and WSe_2 and their optically transparent transition metal oxides (TMOs) to demonstrate novel area efficient camouflaging solutions that are resilient to SAT-attack and automatic test pattern generation (ATPG) attacks. We show that resistors with resistance values differing by 8 orders of magnitude, diodes with variable turn-on voltages and reverse saturation currents, and field effect transistors (FETs) with adjustable conduction type, threshold voltages and switching characteristics can be optically camouflaged to look exactly similar by engineering TMO/TMD heterostructures allowing hardware obfuscation of both digital and analog circuits. Since this 2D heterostructure devices family is intrinsically camouflaged, NAND/NOR/AND/OR gates in the circuit can be obfuscated with significantly less area overhead allowing 100% logic obfuscation compared to only 5% for CMOS-based camouflaging. Finally, we demonstrate that the largest benchmarking circuit from ISCAS'85, comprised of more than 4000 logic gates when obfuscated with the CMOS-based technique are successfully decamouflaged by SAT-attack in less than 40 minutes; whereas, it renders to be invulnerable even in more than 10 hours, when camouflaged with 2D heterostructure devices thereby corroborating our hypothesis of high resilience against RE. Our approach of connecting unique material properties to innovative devices to secure circuits can be considered as one of its kind demonstrations, highlighting the benefits of cross-layer optimization.

Today, the semiconductor industry is a global ecosystem involving thousands of specialized companies all around the world engaged in activities that range from the supply of raw materials to chip design, manufacturing, testing, assembly, packaging, and ultimately distribution and sales of the final product i.e. the integrated circuits (ICs) which are the "brains" of all modern electronic devices. As these ICs become more complex and multifunctional, the semiconductor supply chain becomes more granular. While this physically dispersed but highly interconnected value chain continues to reduce the developmental cost and design time, it brings forth new challenges such as counterfeiting, cloning, overproduction, Trojan insertion, as well as piracy of intellectual property (IP) due to the involvement of untrustworthy parties [1]. One of the major threats arises from reverse engineering (RE), a process that can be used to identify the device technology, or extract gate level circuit layout, or infer the functionality of an IC [2-5]. For instance, Intel's 22nm Xeon processor was successfully reverse engineered revealing the use of trigate transistors [6]. The tools and techniques used for hardware RE can range from simple mechanical delayering and optical or X-ray photography, to more involved electrical micro probing of key buses, pins, and connectors, to resource intensive microscopy involving scanning electron microscope (SEM) or transmission electron microscope (TEM) [5]. A more recent threat to hardware obfuscation is the SAT-attack, that can reverse engineer camouflaged gates of complementary metal oxide semiconductor (CMOS) based circuits with more than 4000 logic gates in less than an hour [9, 10]. Since it is unlikely that ICs can be made foolproof against RE, the strategy is to enhance the complexity of the required RE effort so that the resources necessary such as time, work force, tool, cost, etc. outweighs the reward.

Camouflaging has emerged as a hardware obfuscation method that can thwart RE by hiding the functionality of a circuit. The inspiration is derived from nature, where countless animals camouflage themselves within their surroundings to conceal their presence from predators or catch unsuspecting preys. For example, Fig. 1a, appears to be the bark of a tree. However, a closer inspection reveals a camouflaged tree spider. Camouflaging adaptations have been proposed for ICs as shown in Fig. 1b. For an observer, the circuit functionality appears to be $Y = ABC$, however, the true functionality is $Y = AB$, since the connection from the input C to the output Y is camouflaged. IC camouflaging primarily involves fabrication of dummy contacts or threshold engineering through the alteration of channel doping [14-18] to make the circuits look alike but differ in functionalities. Gate netlist level camouflaging has also been proposed where camouflaging cells or camouflaging connections are inserted to maximize the resilience of the circuit netlist against RE techniques [13, 19, 20]. While innovative, these IC obfuscation techniques add significant area overhead and are easily decamouflaged when the reverse engineer launches SAT-attacks [9, 10, 13]. Furthermore, these obfuscation methods are based on the aging Si technology which is experiencing stagnation in energy, size, and complexity scaling [21, 22] and at the same time does not offer low-cost, low-power, flexible, and printable solutions for the edge devices in the emerging era of Internet of Things (IoT) [23]. Finally, most of the proposed schemes have been implemented and tested at the simulation level with limited experimental demonstrations.

Here, we exploit unique material properties of two-dimensional (2D) transition-metal dichalcogenides (TMDs) and their corresponding transition metal oxides (TMOs) to obfuscate device and circuit level functionalities using TMO/TMD heterostructures as shown in Fig. 1c.

TMDs are layered compounds with strong in-plane covalent bonding and weak out-of-plane van der Waals (vdW) interaction which allows thinning of the material down to monolayer with thicknesses < 1 nm [24]. TMDs have the general formula of MX_2, where M represents the transition metal atom, i.e. molybdenum (Mo) and tungsten (W) and X represents the chalcogen atom i.e. sulfur (S), selenium (Se), and tellurium (Te). Unlike, graphene which is a gapless 2D semimetal, TMDs offer finite bandgap in the range of 0.5 – 3 eV making them promising candidates for post-Si nanoscale devices [25-30]. Note that even at atomically thin body thicknesses, TMDs are robust to detrimental quantum confinement effects observed in Si, which allows field effect transistors (FETs) based on mono or few-layers of TMDs to reinstate aggressive length scaling [31, 32]. Moreover, the mechanical flexibility [33], optical transparency [34], and availability of TMD inks [35] make them attractive for IoT edge devices. Manufacturable solutions are also being developed through large area growth of TMDs using chemical vapor deposition (CVD) and other techniques [36]. TMOs on the other hand offer three unique properties: 1) TMOs are insulating in nature, 2) TMOs are optically transparent, and 3) TMOs are p-type dopants for TMDs [37-39]. Furthermore, when TMDs (MX_2) are exposed to mild oxygen plasma, the top few layers can be transformed to corresponding sub-stoichiometric TMOs (MO_{3-y}) through a self-limiting and highly anisotropic oxidation process that favors lateral oxidation within layers of MX_2 with minimal vertical propagation [40-42]. This allows optical camouflaging of the TMO/TMD hetero-stack as shown schematically in Fig. 1d.

For experimental demonstration of optical camouflaging of TMO/TMD hetero-stack, WSe_2 flakes were mechanically exfoliated on a 50nm alumina (Al_2O_3) substrate using the scotch-tape technique followed by imaging using an optical microscope. A random flake with a thickness ~ 35 nm,

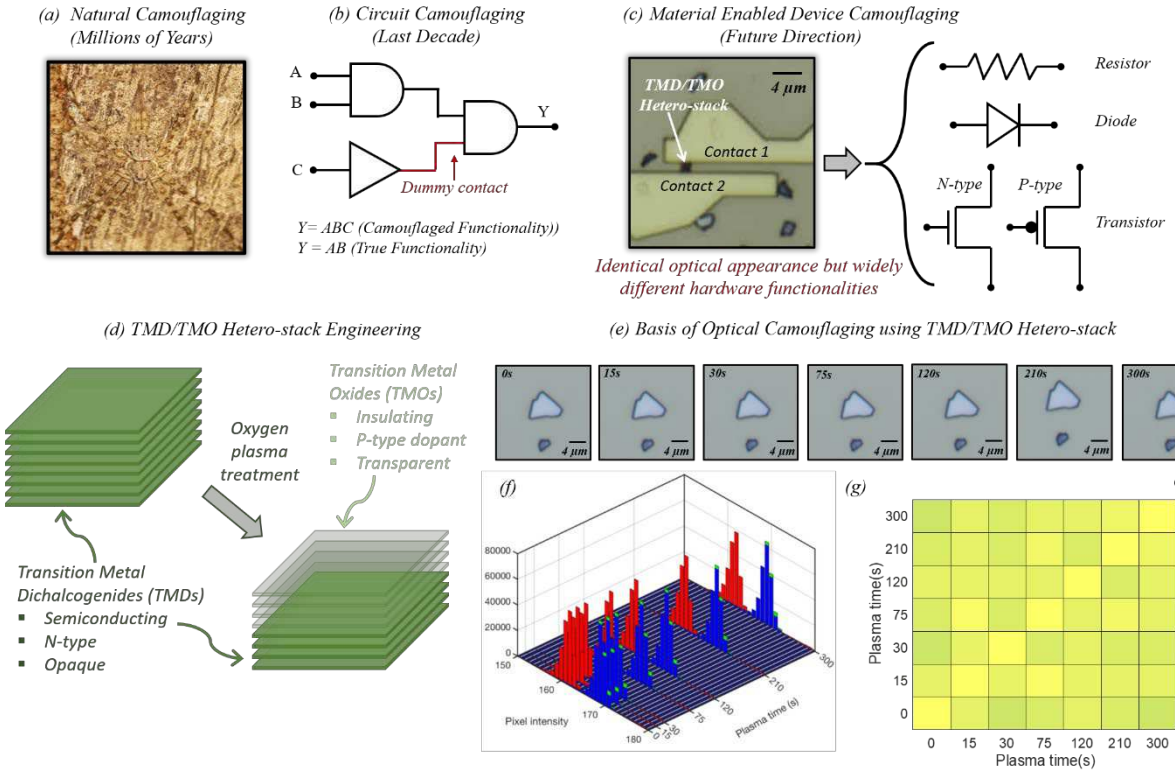

Figure 1. Camouflaged two-dimensional (2D) heterostructure for hardware obfuscation. *a) Natural camouflaging for survival. Photograph of a camouflaged tree spider. b) IC camouflaging using dummy contact to thwart reverse engineering. For an observer, the circuit functionality appears to be $Y = ABC$, however, the true functionality is $Y = AB$, since the connection from the input C to the output Y is camouflaged. c) Proposed camouflaging enabled by unique material properties of transition metal dichalcogenides (TMDs) and their corresponding transition metal oxides (TMOs). The optical image shows a camouflaged TMO/TMD hetero-stack device that can be either a resistor or a diode or a transistor. d) Schematic showing that when the TMDs are exposed to mild oxygen plasma, the top few layers can be transformed to corresponding sub-stoichiometric TMOs through a self-limiting and highly anisotropic oxidation process that favors lateral oxidation within layers of TMDs with minimal vertical propagation. TMOs are insulating, optically transparent and are p-type dopant for TMDs, whereas, TMDs are semiconducting, opaque, and intrinsically n-type. e) Optical images of a 35 nm thick WSe_2 flake taken sequentially following exposer to mild oxygen plasma at 50 watts RF power for the indicated amount of times. f) Histograms of the red, green, and blue (RGB) color spectrum for the optical images in (e) show no significant changes in any of the three-color channels indicating that the images are practically indistinguishable. g) Color map of correlation coefficient (CC) between the binarized optical images from (e). CC values close to '1' indicate perfect similarity between the images. These findings suggest that the plasma treatment process and hence the presence of TMO on top of the TMD is concealed from the adversary. Furthermore, the thickness of the TMO layer, which depends on the plasma exposure time, as well as the region of its presence (i.e. partial or complete covering of the TMD) are also not revealed in the optical images.*

confirmed using an atomic force microscopy (AFM) was selected to analyze the impact of the oxygen plasma on its visual appearance. The flake was then sequentially exposed for the following time intervals: 15s, 30s, 75s, 120s, 210s and 300s to oxygen plasma at 50 watts RF power. Fig. 1e shows the images acquired between every exposure step. The minimum power setting needed to

generate a stable plasma was used for the plasma etch tool to minimize physical damage to the 2D flakes and also to establish a reliable, controllable and reproducible method for obtaining the TMO/TMD hetero-stack (see ***Method*** sections for details). Fig. 1f shows the histogram of the red, green, and blue (RGB) color spectrum in the optical images of the WSe_2 flake corresponding to different plasma exposure times. Clearly, there is no significant changes in any of the three-color channels indicating that the images are practically indistinguishable. Furthermore, Fig. 1g shows the color map of the correlation coefficient (CC) between the binarized optical images from Fig. 1e. The binarization was done using standard MATLAB coding. A CC value of '1' indicates perfect similarity between the images, whereas '0' indicates that the images are completely different. CC values in Fig. 1g are found to be near 1 with a mean ~ 0.85, which ensures that the plasma treatment process and hence the presence of TMO on top of the TMD is concealed from the adversary (see ***Supplementary Information 1*** for camouflaged TMO/TMD hetero-stack of various thicknesses). Furthermore, the thickness of the TMO layer, which depends on the plasma exposure time, as well as the region of its presence (i.e. partial or complete covering of the TMD), are also not revealed in the optical images. However, as we will describe next, such camouflaged and lithographically patterned TMO/TMD hetero-stacks offer a wide range of device functionalities, which can revolutionize hardware obfuscation to prevent RE efforts without adding any area or energy overhead that makes it attractive for smart and secure technologies of the future.

Camouflaged Resistors: Fig. 2a shows the schematic of a camouflaged resistor based on TMO/TMD hetero-stack, whose resistance value can be adjusted in three possible ways: 1) by controlling the oxygen plasma exposure time, 2) by using different TMD flake thicknesses and 3) by changing the TMD material. Fig. 2b shows the optical images of a camouflaged resistor based

on 10 nm thick WO_{3-y}/WSe_2 hetero-stack before and after 30s of oxygen plasma exposure and Fig. 2c shows the corresponding current *versus* voltage characteristics. The change in resistance of the stack is attributed to the change in the surface charge doping introduced by the sub-stoichiometric WO_{3-y} in the underlying WSe_2. The oxygen deficient WO_{3-y} captures electron from intrinsic WSe_2 and thereby moves the equilibrium Fermi level close to the valence band resulting in p-type doping of WSe_2 as shown using the energy band diagrams in Fig. 2d. Fig. 2e shows the bar plot for the extracted resistance values for camouflaged WO_{3-y}/WSe_2 hetero-stack resistors for different initial thicknesses of the exfoliated WSe_2 flakes as a function of plasma exposure time. Note that the current is normalized to the width of the resistor and hence the resistance values are indicated in Ω-μm. All resistors had 1μm channel length and 40 nm Ni/ 30 nm Au as the contact metal. The resistance value changes by more than 8 orders of magnitude without changing the device footprint and at the same time remains optically indistinguishable. The non-monotonic trend in the resistance values for the thinner flakes can be attributed to the fact that thin WSe_2 flakes are found to be intrinsically n-type doped (low resistance). Short plasma exposure times induce p-type doping through sub-stoichiometric WO_{3-y}, which compensates for the n-type doping and makes the stack intrinsic (high resistance). With continued plasma exposure, p-type doping keeps increasing and the stack becomes more conductive (low resistance). On the other hand, thicker WSe_2 flakes are more intrinsic (high resistance) in nature and therefore show monotonic decrease in resistance with increased plasma exposure time. Finally, Fig. 2f-i show the bar plot for extracted resistance values for representative thin and thick MoS_2, $MoSe_2$, $MoTe_2$ and WS_2 based camouflaged resistors pre- and post-exposure to oxygen plasma for 75s. The increase in resistance for post-plasma treated MoS_2, $MoSe_2$, and WS_2 is due to the fact that all of these materials exhibit intrinsic n-type doping which is compensated by the p-type doping introduced by their

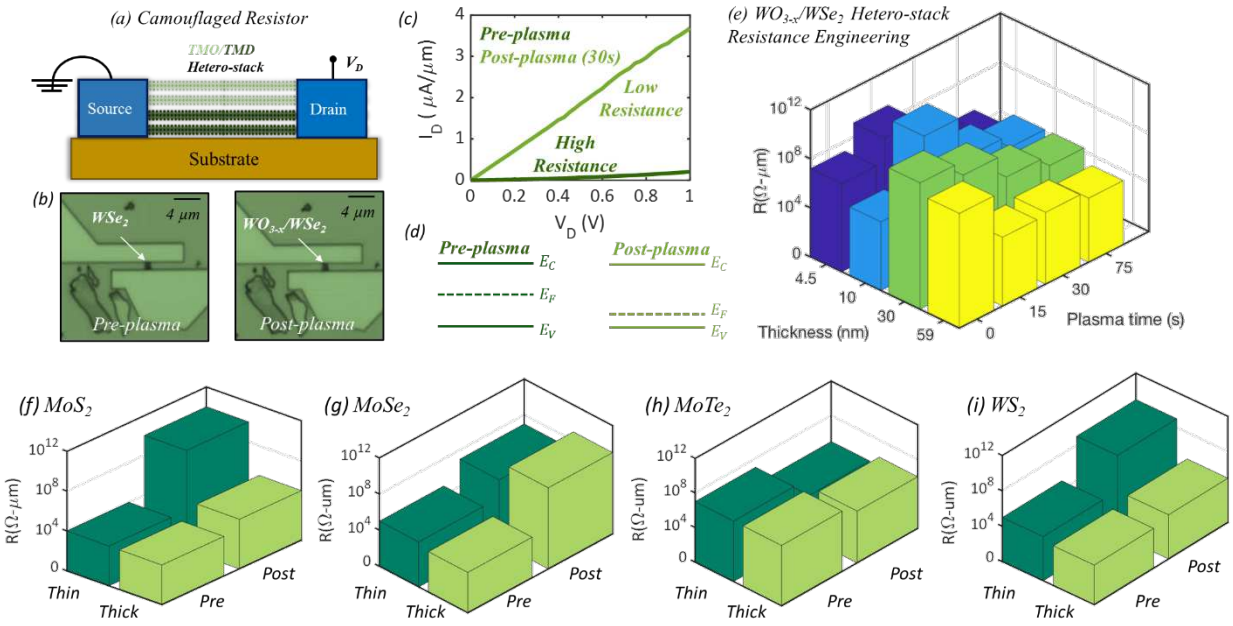

Figure 2. Camouflaged resistors*. a) Schematic of a camouflaged resistor based on TMO/TMD hetero-stack. b) Optical images and c) corresponding current versus voltage characteristics of a 10 nm thick WO_{3-y}/WSe_2 hetero-stack resistor before and after 30s of oxygen plasma exposure. While the optical appearances remain identical the resistances differ significantly. The change in resistance can be attributed to the change in the surface charge doping introduced by the sub-stoichiometric WO_{3-y} in the underlying WSe_2. d) Energy band diagrams showing the transition in the Fermi level (E_F) towards the valence band since the oxygen deficient WO_{3-y} acts like an electron acceptor introducing p-type doping in WSe_2. e) Bar plot showing the extracted resistance values (normalized to width) for camouflaged WO_{3-y}/WSe_2 hetero-stack resistors for different initial thicknesses of the exfoliated WSe_2 flakes as a function of plasma exposure time. All resistors had 1μm channel length and 40 nm Ni/ 30 nm Au as the contact metal. The resistance value changes by more than 8 orders of magnitude without changing the device footprint or their optical appearances. Similar results are obtained for f) MoS_2, g) $MoSe_2$, h) $MoTe_2$ and i) WS_2 based camouflaged resistors pre- and post-exposure to oxygen plasma for 75s. While any semiconducting material will form insulating and transparent surface oxide when exposed to mild oxygen plasma, what makes TMOs unique is their capability to dope the underlying TMDs and thereby change the resistance values by orders of magnitude. These TMO/TMD hetero-stack resistors can, therefore, be used to camouflage connections between devices and circuits in an IC to increase the complexity of RE without adding any area or energy overhead.*

corresponding sub-stoichiometric oxides irrespective of the thickness. On the contrary, post plasma treated $MoTe_2$ stack shows decrease in resistance, similar to WSe_2 owing to the lack of any intrinsic n-type doping. The resistance values are also impacted by the Schottky barrier (SB) that exists at the metal/TMD interface [43, 44]. For Schottky injection, the barrier height and width play a critical role in determining the contact resistance. The barrier height depends on the choice of metal, position of metal Fermi level pinning, pinning factor etc. and barrier width is determined by the flake thickness and doping [45]. Nevertheless, for any given TMD and for any choice of

thickness, it is possible to achieve orders of magnitude difference in the resistance values in the TMO/TMD hetero-stack resistors through controlled oxygen plasma treatment without compromising their optical indistinguishability which is the key for the success of resistance camouflaging against RE efforts. While most semiconducting materials will form insulating and transparent surface oxides when exposed to mild oxygen plasma, what makes TMOs unique is their capability to dope the underlying TMDs and thereby change the resistance values by orders of magnitude. These TMO/TMD hetero-stack resistors can, therefore, be used to camouflage connections between devices and circuits in an IC to increase the complexity of RE without adding any area or energy overhead.

Camouflaged Diodes: Diodes are non-linear passive components essential for any IC design. Both analog and digital circuits require diodes. Therefore, camouflaged diodes can add significant challenge to any RE effort. Fig. 3a shows the schematic of a camouflaged diode based on TMO/TMD hetero-stack. Camouflaged diodes require an additional processing step where one side of the fabricated WSe_2 resistors are protected by PMMA which is patterned using electron beam lithography before exposure to the oxygen plasma (see ***Method*** sections for details). The PMMA is striped off afterwards. This fabrication step ensures that the protected area remains intrinsic, whereas the exposed area becomes p-type due to the formation of sub-stoichiometric MO_{3-y}. Fig. 3b shows the optical images of the device before and after the fabrication of the diode based on WSe_2. Clearly, the images appear identical making it difficult for an adversary to recognize the functionality of the device through visual inspection. Fig. 3c-f show the current *versus* voltage characteristics of a thin and a thick diode in linear and logarithmic scales, respectively. These plots show rectifying behaviors. Since the diodes were fabricated on a back-

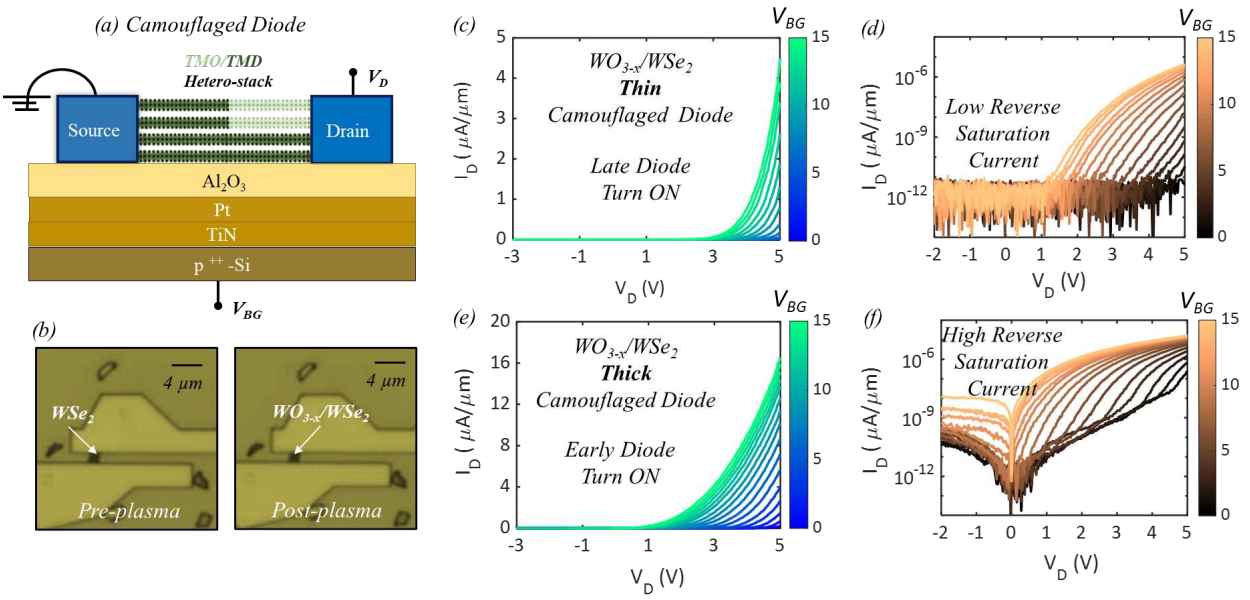

Figure 3. Camouflaged Diodes. *a) Schematic of a camouflaged diode based on TMO/TMD hetero-stack. Camouflaged diodes require an additional processing step where one side of the fabricated TMD resistors are protected by PMMA which is patterned using electron beam lithography before exposure to the oxygen plasma. The PMMA is striped off afterwards. This fabrication step ensures that the protected area remains intrinsic, whereas the exposed area becomes p-type doped due to the formation of sub-stoichiometric TMO. b) Optical images of the device before and after the fabrication of the diode based on WSe_2. Clearly, the images appear identical making it difficult for an adversary to recognize the functionality of the device through visual inspection. Current versus voltage characteristics of a thin diode in c) linear and d) logarithmic scales. Clearly, rectifying behaviors are observed. Since the diodes were fabricated on a back-gate stack comprising of 50 nm Al_2O_3 as the back-gate oxide and Pt/TiN/p^{++}-Si as the back-gate electrode, dynamic reconfiguration of the diode characteristics is possible through electrostatic doping using the back-gate voltage (V_{BG}). Current versus voltage characteristics of a thick diode in e) linear and f) logarithmic scales. The thin diode shows late turn on since the built-in-potential is higher between the undoped region which is intrinsically n-type doped and the p-type doped region compared to the thick diode where the undoped region is more intrinsic. Also, the thin diode offers significantly low reverse saturation current, whereas, the reverse saturation current depends strongly on the applied V_{BG} for the thick diode. This is expected since for thicker diodes, the phenomenon of Thomas-Fermi charge screening restricts the doping effect to only top few layers, while the layers at the bottom of the stack i.e. the layers close to the oxide are under firm back-gate control. For $V_{BG} \gg 0$, these layers become electrostatically n-doped and offer a parallel conduction path for the current to flow between the two metal contacts. The tunability of camouflaged diode characteristics through back-gating adds one more level of complexity to RE.*

gate stack comprised of 50 nm Al_2O_3 as the back-gate oxide and Pt/TiN/p^{++}-Si as the back-gate electrode (Fig. 3a), dynamic reconfiguration of the diode characteristics is possible through electrostatic doping using the back-gate voltage (V_{BG}). ***Supplementary Information 2*** shows the tunability in diode turn on voltage and reverse saturation current using V_{BG} for thin and thick WO_{3-y}/WSe_2 stacks. The thin diode (Fig. 3c) shows late turn on since the built-in-potential is higher between the undoped region which is intrinsically n-type doped and the p-type doped region

compared to the thick diode (Fig. 3e) where the undoped region is more intrinsic. Also note that the thin diode offers significantly lower reverse saturation current (Fig. 3d), whereas, the reverse saturation current depends strongly on the applied V_{BG} for the thick diode (Fig. 3f). This is expected, since for thicker diodes, the phenomenon of Thomas-Fermi charge screening restricts the doping effect to only top few layers [46], while the layers at the bottom of the stack i.e. the layers close to the oxide are under firm back-gate control. For $V_{BG} \gg 0$, these layers become electrostatically n-doped and offer a parallel conduction path for the current to flow between the two metal contacts. The tunability of camouflaged diode characteristics through back-gating adds one more level of complexity to RE.

Camouflaged Transistors: FETs are the elementary building blocks for any digital logic and analog computational circuits. Camouflaging their conduction type i.e. electron (n-type) or hole (p-type) dominance, threshold voltage, ON-current, current ON-OFF ratio, and switching characteristics will make any RE effort significantly more challenging. Fig. 4a shows the schematic of a camouflaged FET based on TMO/TMD hetero-stack. The device structure is identical to the camouflaged resistors shown in Fig. 2a, except for the use of the back-gating capability shown in Fig. 3a. Fig. 4b shows the optical images of a representative FET based on WO_{3-y}/WSe_2 hetero-stack before and after the oxygen plasma exposure. Clearly, the images appear identical making it difficult for an adversary to recognize the FET functionality through visual inspection. Fig. 4c demonstrates how the oxygen plasma exposure time and the initial flake thickness can be used to obfuscate the WSe_2 FET transfer characteristics i.e. the functional dependence of source to drain current (I_{DS}) on the back-gate voltage (V_{BG}) for a constant source to drain voltage (V_{DS}) of 1V without changing either the visual appearance or the footprint of the

FET. Fig. 4d shows a table summarizing the transition of pristine WSe_2 based FETs from dominant n-type to ambipolar to p-type transport characteristics as the plasma exposure time increases for various flake thicknesses (see ***Supplementary Information 3*** for the evolution of the transfer characteristics for 30 nm and 59 nm thick flakes). The change in dominant carrier transport from electron conduction (n-type) to hole conduction (p-type) with increasing plasma exposure time is consistent with the fact that the sub-stoichiometric WO_{3-x} introduces p-type doping in the underlying WSe_2. Note that thinner flakes switch their conduction type even with short plasma exposures, whereas thicker flakes require longer exposure time. This can be explained using the physics of electrostatic gating and Thomas-Fermi charge screening [46, 47]. The sub-stoichiometric WO_{3-x} induces p-type doping in the WSe_2 layers which are right underneath and thereby promoting hole conduction in the WSe_2 layers near the top surface. The impact of this doping diminishes in the WSe_2 layers away from the surface owing to the Thomas-Fermi charge screening. Simultaneously, the back-gate voltage (V_{BG}) produces a charge near the oxide-semiconductor interface which alters the surface potential and creates a conductive channel near that interface. If the channel is thin, these two charges can combine to locally move the Fermi level in the channel more than either could individually. This creates large positive shift in the threshold voltages seen in the thinner WSe_2 flakes switching the conduction type even for short plasma exposure times. However, if the channel is thick, the back-gate is too far away to modify the potential near the top of the channel and hence similar shift requires longer plasma exposure. Fig. 4e shows the color map for the threshold voltages (V_{TH}) extracted from the linear transfer characteristics for the dominant conduction type. Clearly, our approach offers tremendous flexibility for camouflaging the threshold voltage of the FET. However, beyond a certain plasma exposure time, the self-limiting nature of the oxidation process does not add any extra charges and

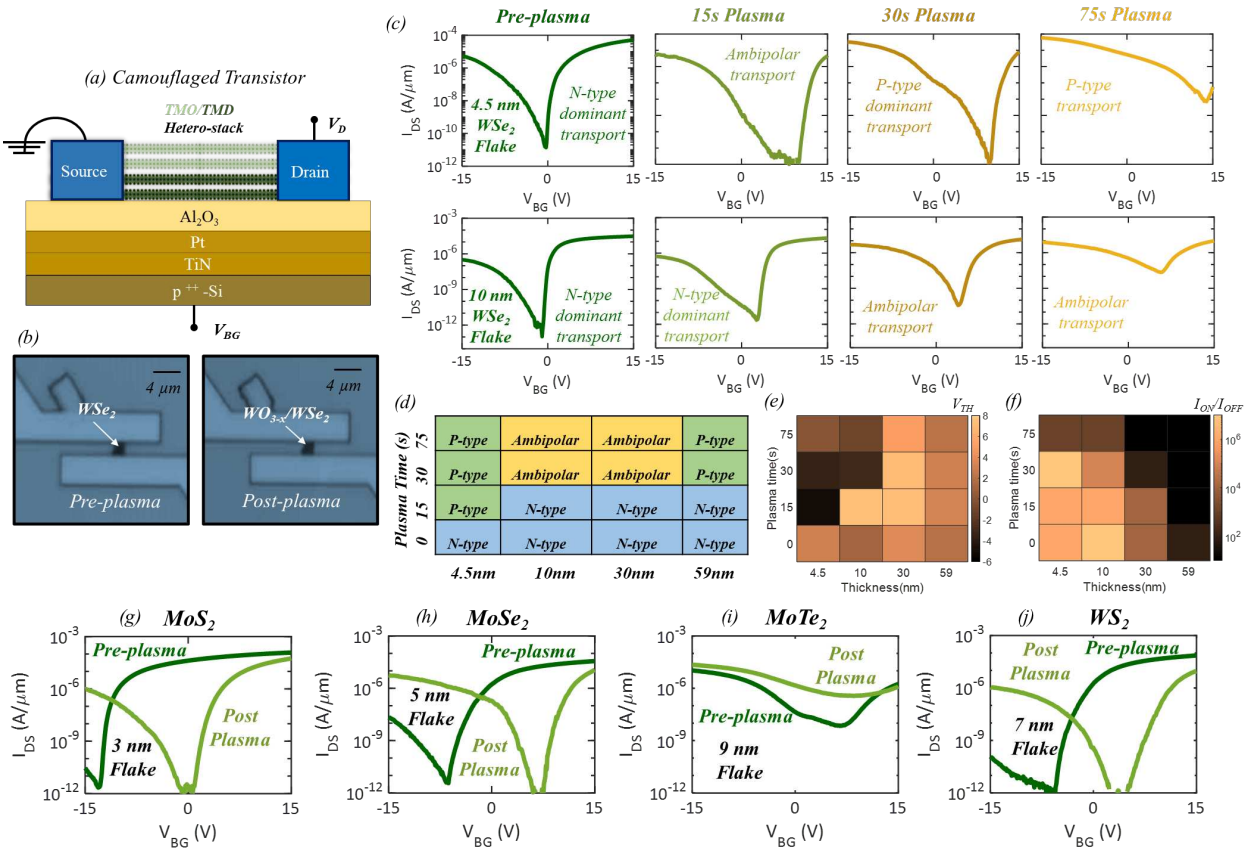

Figure 4. Camouflaged Transistors: *a) Schematic of a camouflaged FET based on TMO/TMD hetero-stack. b) Optical images of WO_{3-y}/WSe_2 hetero-stack FET before and after the oxygen plasma exposure. Clearly, the images appear identical making it difficult for an adversary to recognize the FET functionality through visual inspection. c) Evolution of the transfer characteristics for WO_{3-y}/WSe_2 hetero-stack FET as a function of oxygen plasma exposure time for two different initial flake thicknesses. d) A table summarizing the transition of pristine WSe_2 based FETs from dominant n-type to ambipolar to p-type transport characteristics as the plasma exposure time increases for various flake thicknesses. The change in dominant carrier transport from electron conduction (n-type) to hole conduction (p-type) with increasing plasma exposure time is consistent with the fact that the sub-stoichiometric WO_{3-x} introduces p-type doping in the underlying WSe_2. Color map for e) threshold voltages (V_{TH}) and f) current ON/OFF ratio for the dominant branch. Similar observations can be made in the transfer characteristics of g) MoS_2, h) $MoSe_2$, i) $MoTe_2$ and j) WS_2 based camouflaged FETs before and after exposure to oxygen plasma for 75s. Irrespective of the choice of material, p-type conduction is enhanced. These results indicate that TMO/TMD hetero-stack FETs can be camouflaged with tunable device parameters through oxygen plasma exposure irrespective of their thickness and composition and without compromising their optical indistinguishability which is critical for defying the RE efforts. What is more attractive is that these camouflaged TMO/TMD hetero-stack devices do not add any area overhead which is unavoidable for the state-of-the-art layout level camouflaging approaches.*

the threshold shift saturates. Moreover, longer plasma exposure can physically damage the flake degrading the FET characteristics. Fig. 4f shows the color map for the current ON/OFF ratio for the dominant branch. Note that the OFF state current increases with the plasma exposure time and the increase is more substantial for the thicker flakes leading to significant reduction in the current

ON/OFF ratio. Since gating in our devices occur form the back, for thicker flakes the p-type channel near the top surface is weakly modulated by the back-gate voltage and hence continues to conduct significant amount of current even in the OFF state resulting in lower ON/OFF current ratio. However, in thinner flakes, the back-gate can fully compensate the p-type doping induced by the surface charge due to better electrostatic control which allows the device to reach lower OFF state current and hence higher current ON-OFF ratio. Finally, Fig. 4g-j show the transfer characteristics for representative MoS_2, $MoSe_2$, $MoTe_2$, and WS_2 based camouflaged FETs before and after exposure to oxygen plasma for 75s. It is clear that irrespective of the choice of material, p-type conduction is enhanced. For MoS_2 FET (Fig. 4g), the electron conduction dominates even after 75s of plasma exposure. This is due to that fact that MoS_2 shows a high level of intrinsic n-type doping, which is evident from the large negative threshold voltage seen in its pre-plasma treatment characteristics. Furthermore, the phenomenon of metal Fermi level pinning close to the conduction band of MoS_2 facilitates easier electron injection and limits hole conduction [45]. For WS_2 FET (Fig. 4i) and $MoSe_2$ FET (Fig. 4j), the post plasma treatment characteristics show ambipolar conduction i.e. the presence of nearly symmetric electron and hole transport. This suggests a lesser extent of n-type doping in intrinsic WS_2 and $MoSe_2$. Finally, $MoTe_2$ FET (Fig. 4k) appears different compared the other TMD FETs, with a higher OFF state current and a stronger ambipolar behavior. This is consistent with earlier findings that $MoTe_2$ is significantly more sensitive to oxidation than other TMDs [48] and hence the pristine device may already have sub-stoichiometric MoO_{3-x} on the top surface. ***Supplementary Information 4*** summarizes the relative strength of electron and hole conduction in various TMO/TMD hetero-stack. Nevertheless, TMD FETs can be camouflaged with tunable device parameters through oxygen plasma exposure irrespective of their thickness and composition and without compromising their

optical indistinguishability which is critical for defying the RE efforts. What is more attractive is that these camouflaged TMO/TMD hetero-stack devices do not add any area overhead which is unavoidable for the state-of-the-art layout level camouflaging approaches.

Camouflaged Circuits and Logic Gates: In conventional digital and analog circuit designs the basic hardware elements such as resistor, diode, n-type, and p-type FETs have unique footprints, which allow the adversary to seamlessly identify the devices through optical inspection and thereby reconstruct the circuit functionality. State-of-the-art camouflaging approaches prevent such RE effort by introducing dummy contacts which increases the area overhead. However, our camouflaged resistors, diodes, and FETs are optically indistinguishable since their layouts are identical making the RE through visual inspection to be futile. In this case, the reverse engineer has to adopt a trial and error approach to identify the circuit functionality. If there are M hardware components in an IC, each with P possibilities, the number of trials will be equal to the number of unique functionalities (F), which will be given by, $F = M^P$. Fig. 5a shows the number of RE trials as a function of M and P, which becomes astronomical when one considers billions of camouflaged devices on a chip, each with many possibilities, i.e. resistance values that differs by more than 8 orders of magnitude for camouflaged resistors, turn on voltages and reverse saturation current that can be adjusted for camouflaged diodes, and conduction type, threshold voltage, current ON-OFF ratio, etc. that can be tuned for camouflaged FETs. Even for relatively small, M = 1000 and P = 6, the number of RE trials become $F = 10^{40}$. Fig. 5b shows the layout of a camouflaged analog circuit. Here both layouts are visually identical but the one functions as a voltage divider, while the other functions as a half-wave rectifier. Similarly, Fig. 5c shows a camouflaged digital to analog mapping circuit with multiple digital input and one analog output. This circuit functions as a digital

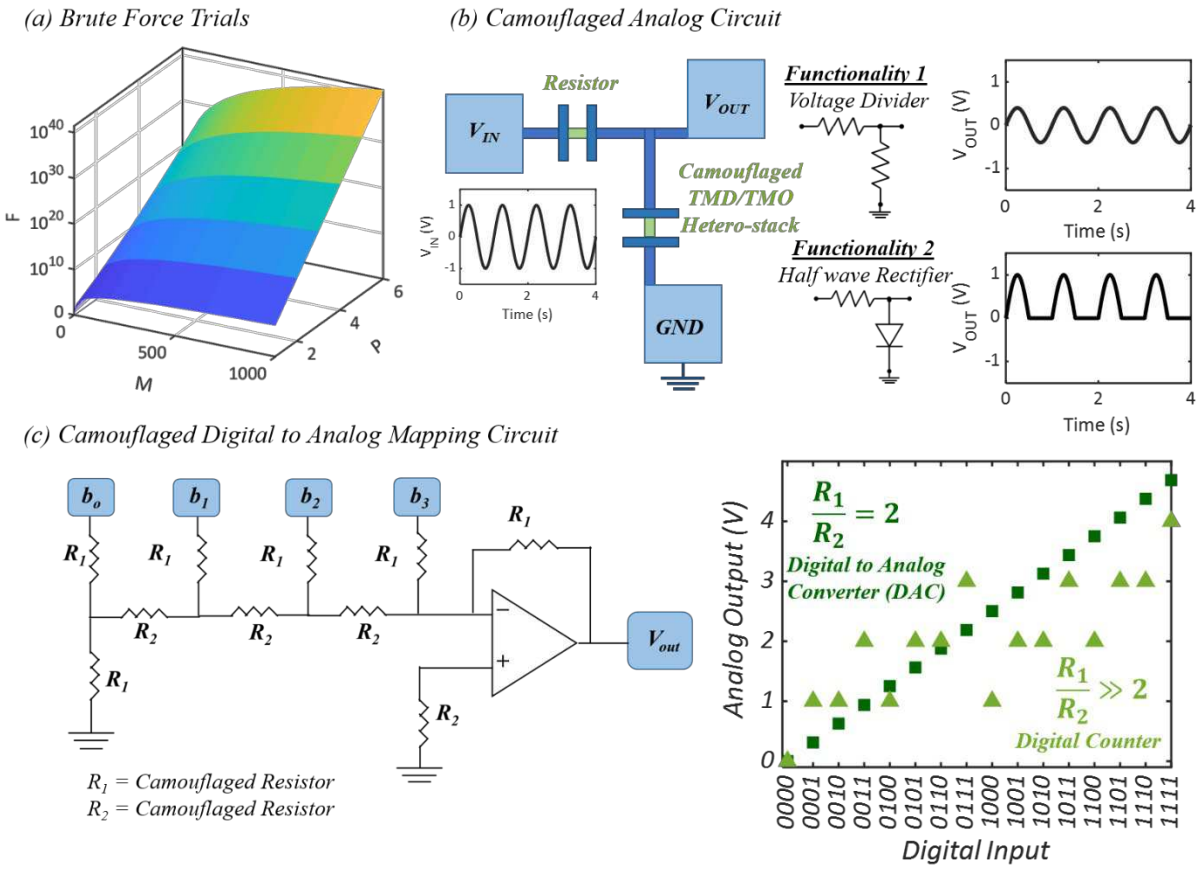

Figure 5. Camouflaged analog circuits. *a) Number of trials (F) for reverse engineering an integrated circuit (IC) with M hardware components, each with P possibilities. Even for relatively small, M = 1000 and P = 6, the number of RE trials becomes astronomical, F = 10^{40}. b) Camouflaged circuit layout exploiting TMO/TMD hetero-stack devices. Both layouts are visually identical but the one functions as a voltage divider, while the other functions as a half wave rectifier. c) A camouflaged digital to analog mapping circuit with multiple digital input and one analog output. This circuit functions as a digital to analog converter (DAC) for* $^{R_1}/_{R_2} = 2$ *but transforms into a digital bit counter (DBC) that counts the number of ones in a digital sequence for* $^{R_1}/_{R_2} \gg 2$.

to analog converter (DAC) for $^{R_1}/_{R_2} = 2$, but transforms into a digital bit counter (DBC) that counts the number of ones in a digital sequence for $^{R_1}/_{R_2} \gg 2$.

Next, we show that conventional combinational logic gates – NAND, NOR, AND, and OR can be camouflaged using 2D heterostructure device-based circuit elements, thereby obfuscating the gate functionality. Fig. 6a models the template of the camouflaged representation of a logic circuit,

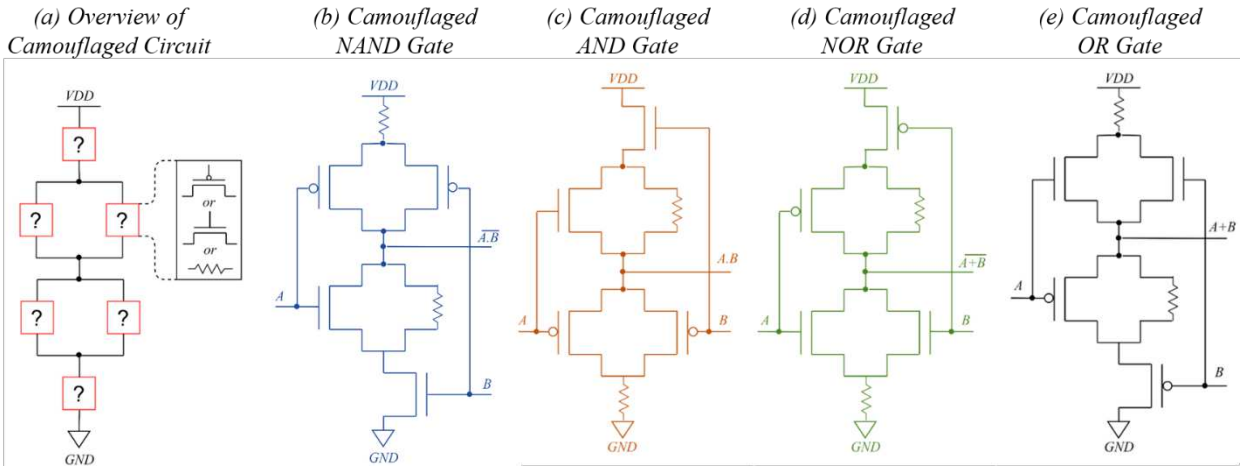

Figure 6. Camouflaged logic gates. *a) Overview of a digital logic circuit with camouflaged elements. Actualization of b) NAND gate, c) AND gate, d) NOR gate, and e) OR gate with TMO/TMD hetero-stack based camouflaged p-FET, n-FET, and resistor. Since the camouflaged devices are physically identical to each other, the gates developed using those elements also look the same.*

where each boxed element can be either a p-type FET or an n-type FET or a resistor. Different instances of these camouflaged elements are mapped onto a box of the model circuit to devise multi-functional logic gates. The realization of NAND gate operation based on CMOS logic is shown in Fig. 6b. The corresponding representations of AND, NOR and OR gates are shown in Fig. 6c, 6d, and 6e, respectively. Since the camouflaged devices are physically identical to each other, the gates developed using those elements also look exactly the same. Hence, the reverse engineer gaining access to the top-view representation of the visually indistinguishable multi-functional gates cannot infer the logic functionality and is obfuscated from the knowledge about the operation of the circuit. The value of the resistors should be as low as possible to minimize the voltage drop but should be higher than the intrinsic device resistance of the individual FETs to direct the current to flow through the transistors. In fact, by using gated camouflaged resistors as shown in ***Supplementary Information 5***, it is possible to dynamically change the resistance value, which is unprecedented for current state-of-the-art Si technology.

Resilience to SAT-Attack: To analyze the prowess of our proposed circuit level camouflaging scheme, these visually identical logic gates are employed to camouflage the ISCAS'85 benchmark circuits. The ISCAS'85 benchmark suite is comprised of 11 circuits with multi-input gates from multiple logic families, which is traditionally used by existing research to evaluate their proposed camouflaging schemes [9, 11, 12]. Each circuit has been decomposed into two-input gates. All the NAND, NOR, AND, and OR gates in the circuit are then camouflaged according to the respective camouflaging techniques as discussed, and the cumulative increase in area overhead incurred to accommodate the camouflaged gates is calculated for each circuit. Table 1 represents the total number of gates, the gate count for each camouflaged logic family and the corresponding increase in area overhead for each circuit in the benchmark. Since this device family is intrinsically camouflaged, all the NAND/NOR/AND/OR gates in the circuit can be inherently obfuscated with significantly less area overhead as compared to camouflaging with CMOS logic, where dummy contacts are forcibly introduced to obfuscate the circuit operation [9]. Hence, CMOS-based camouflaging technique incurs enormous area overhead metrics, thereby restricting the circuit designer to camouflage only 5% of the logic gates, as compared to 100% obfuscation using 2D heterostructure devices. Consequently, the proposed circuit-level camouflaging scheme is expected to be notably more resilient against reverse engineering attacks compared to the CMOS-based camouflaging technique. Efficiency of a circuit obfuscation technique is traditionally evaluated by its resilience against SAT-attack. SAT-attack is a supplement to the Boolean Satisfiability Solver, that attempts to reverse engineer the camouflaged gates of a circuit by retrieving the key-value pairs to replicate the oracle functionality [10]. Each of the obfuscated netlist from the ISCAS'85 benchmark is executed on the SAT-solver for more than 10 hours. Although the SAT-attack is successful in breaking the c17 and c432 benchmark, the other nine

Table 1. Resiliency of ISCAS'85 Benchmarks Decomposed into 2-input Gates

Circuit	*Total Number of Gates*	*Number of Gates*				*Area Overhead*	*Decamouflaged by SAT (?)*
		AND	*OR*	*NAND*	*NOR*		
c17	*6*	*0*	*0*	*6*	*0*	*50%*	*Yes*
c432	*216*	*60*	*0*	*79*	*19*	*36.91%*	*Yes*
c499	*246*	*96*	*6*	*0*	*0*	*15.45%*	*Yes*
c880	*435*	*169*	*29*	*87*	*61*	*44.30%*	*Yes*
c1355	*590*	*96*	*6*	*416*	*0*	*46.75%*	*No*
c1908	*1057*	*240*	*0*	*377*	*1*	*36.23%*	*No*
c2670	*1400*	*488*	*129*	*254*	*12*	*38.67%*	*No*
c3540	*1983*	*631*	*273*	*298*	*68*	*39.04%*	*No*
c5315	*2973*	*1178*	*420*	*454*	*27*	*41.5%*	*No*
c6288	*2406*	*256*	*0*	*2118*	*0*	*49.66%*	*No*
c7552	*4042*	*1146*	*404*	*1028*	*54*	*39.43%*	*No*

benchmarks are resilient against the attack, even with inexhaustive resource space. The resilience of the proposed camouflaging approach is compared with state-of-the-art circuit obfuscation scheme in CMOS-based implementations [9, 10]. The two largest benchmarks, c5315 and c7552 when obfuscated with the CMOS-based technique are successfully decamouflaged by SAT-attack in less than 40 minutes, whereas, these benchmarks render to be unbreakable even in more than 10 hours, when camouflaged with 2D heterostructure devices. Since the largest benchmarks are vulnerable to SAT-attacks under CMOS-based obfuscation, it can be inferred that the benchmarks with lower gate counts can also be easily decamouflaged in lesser amounts of time. However, smaller benchmarks camouflaged with the proposed obfuscation scheme exhibit to be unbreakable, even with extensive resource space, as shown in Table 1. Since the benchmarks in ISCAS'85 manifest strong resiliency to SAT-attacks, we restrict ourselves from analyzing larger benchmarks

(e.g. ISCAS'89) used in [9, 10]. It is imperative that ISCAS'89 benchmarks will certainly be invulnerable to SAT attacks, when camouflaged with the proposed technique, unlike dummy contact-based CMOS camouflaging. Hence, this camouflaging technique with 2D heterostructure device furnishes significantly less vulnerability against SAT-attacks with much reduced reasonable area overhead metrics, thereby corroborating our hypothesis of high resilience against reverse engineering.

Resilience to ATPG Attack: The efficacy of our proposed circuit-level camouflaging scheme is further explored by evaluating the resilience against Automatic Test Pattern Generation (ATPG) attacks. Given an obfuscated netlist, an attacker, with the ATPG tool, generates a set of input patterns to the black-box circuit. Following this, the adversary aims to resolve the camouflaged gates by analyzing the corresponding output patterns from the circuit. Resolving an unknown logic gate involves two steps – activation and propagation. In order to activate a particular logic gate, at least one of the two inputs should be controllable. Either the gate should be controlled by primary inputs or by resolved/non-camouflaged gates in the fan-in cone that are controlled by the primary inputs. Subsequently, the tool aims to propagate the output of this missing gate to one of the primary outputs through a clean path in its fan-out cone. A clean path is defined as a path that is not passing through any other missing gate. An analysis of the observable outputs after a successful activation and propagation aids the adversary in resolving each camouflaged gate in the logic circuit. The ATPG attack is launched on each of the camouflaged netlist from the ISCAS'85 benchmarks. Owing to a successful obfuscation of all the NAND, NOR, AND and OR gates in each circuit by our proposed camouflaging scheme, the ATPG tool fails to execute the activation and propagation operation. As a result, the ATPG attack is incapable of breaking any of the benchmark circuits. Even the smallest benchmark, c17 is resilient against the ATPG attack, the obfuscated netlist of which is demonstrated in Figure 7. Although gate G4 can be activated by the primary input E, the fan-out cone is devoid of a clean path to propagate to any of the observable

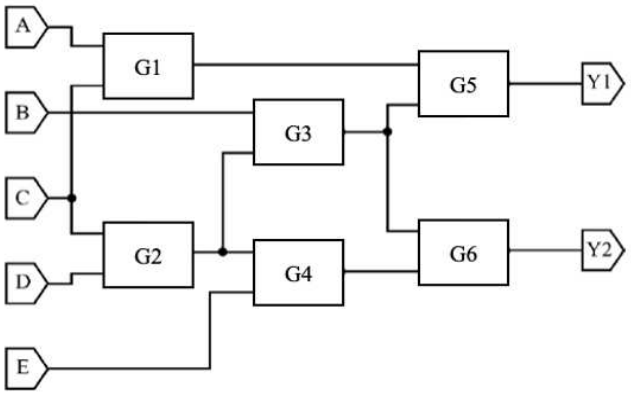

Figure 7. Camouflaged digital circuit. *The c17 benchmark circuit consisting of 6 camouflaged gates (G1 to G6), in order to demonstrate resilience against ATPG attacks.*

outputs. On the contrary, gate G6 despite having a clean path to the primary output Y2 contains missing gates in its fan-in cone. Hence, G6 cannot be activated by any of the primary inputs and therefore, cannot be resolved by the adversary. Thus, the proposed obfuscation scheme proves to be strongly resilient against ATPG attacks, thereby bolstering the security of the camouflaged circuits against reverse engineering.

Resilience to Brute-Force Attack: De-camouflaging an obfuscated circuit is often accomplished by brute-force attack. The adversary accomplishing this attack enumerates all the possible combinations for each camouflaged gate in a circuit. The corresponding logic is simulated to eliminate the false functionalities until the entire circuit is resolved. As a result, the complexity of the brute-force attack increases exponentially with the number of camouflaged gates. Our proposed obfuscation scheme with 2D heterostructure devices can camouflage four logic families – NAND, NOR, AND and OR. Therefore, the c17 benchmark from ISCAS'85 with 6 gates furnishes an attack complexity of 4^6, which increases exponentially to 4^{2632} for the c7552 benchmark. Hence, the brute-force attack suffers from scalability issue, thereby inferring the non-feasibility of this attack under the proposed camouflaging technique.

Comparative Analysis between Polymorphic Spin-Hall Effect Devices and 2D Heterostructure Devices: Among the emerging devices that offer to enhance hardware security, polymorphic gates

Table 2. Number of Camouflaged Gates in ISCAS'85 Benchmarks under Multiple Obfuscation Schemes

Circuit	*Total Number of Gates*	*Number of Gates Camouflaged*	
		Spin-Hall Effect Device	*2D Heterostructure Device*
c17	*6*	*1*	*6*
c432	*216*	*32*	*158*
c499	*246*	*37*	*102*
c880	*435*	*65*	*346*
c1355	*590*	*88*	*518*
c1908	*1057*	*159*	*618*
c2670	*1400*	*210*	*883*
c3540	*1983*	*297*	*1270*
c5315	*2973*	*446*	*2079*
c6288	*2406*	*361*	*2374*
c7552	*4042*	*606*	*2632*

appear to render a promising solution with respect to circuit obfuscation. In this regard, devices based on giant spin-hall effect (GSHE) furnish the most cost-effective and robust versatile security primitive. GSHE devices are capable of camouflaging all the basic logic gates in a circuit – AND, OR, NAND, NOR, XOR, XNOR, NOT and BUF [49]. However, due to the formidable delay overhead of the GHSE switch arising in hybrid CMOS-GSHE designs, camouflaging is restricted to a maximum of 15% of all the gates in the circuit. On the contrary, we implement all the logic gates in a circuit with 2D heterostructure devices, thereby eliminating the need for a hybrid design. As a result, our proposed camouflaging technique with these devices is capable to obfuscate 100% of all the possible gates that can be camouflaged in the circuit. Table 2 outlines the approximate number of gates under each camouflaging scheme for all the ISCAS'85 benchmarks. For each benchmark circuit, obfuscation with 2D heterostructure device furnishes higher number of camouflaged gates as compared to the Spin-Hall effect device, thereby significantly enhancing the resilience of the circuit against reverse engineering attacks.

Optical Decamouflaging Approaches: Simple RE efforts such as mechanical delayering followed by optical imaging to recognize the hardware elements will be unsuccessful for camouflaged 2D material-based devices and circuits. If the reverse engineer has access to advance instrumentations such as parameter analyzers, signal generators, oscilloscopes etc., then it is possible to identify the circuit functionality through electrical probing of key connections. However, most of these connections are made using narrow metallic interconnects with dimensions less than 100nm making it challenging to access even using advanced micro probe technologies. A reverse engineering attacker with access to advanced characterization tools such as SEM, AFM, and Raman may be able to gather some critical information. For example, Fig. 8a shows the SEM images of a WSe_2 based TMO/TMD hetero-stack device before and after the exposure to the oxygen plasma. The two channels look remarkably similar, however, on a closer look, one can observe slight alterations of the surface due to mild physical damage of the flake introduced by the plasma. While the SEM image indicates additional processing of the channel, it does not reveal any information regarding the thickness and composition of the 2D material, plasma type, exposure time, and the pattern design that determines if the device is a resistor or a diode or a transistor. The flake thickness can be measured using AFM as shown in Fig. 8b for a representative WSe_2 flake. The height histograms in Fig. 8c show few nanometers decrease in the flake thickness following 300s of oxygen plasma exposure. However, without having any knowledge of pre-plasma exposure flake thickness, the reverse engineer is unlikely to extract any meaningful information about the device functionality from the AFM image. Finally, Fig. 8d shows the Raman spectroscopy of a 10nm thick WSe_2 flake using the 532nm ULF laser before and after 300s of plasma exposure. Few-layer WSe_2 is characterized by two dominant vibrational modes: the in-plane E_{2g}^1 mode at 247.2 cm^{-1} and the out-of-plane A_{1g} mode at 257.4 cm^{-1}. The small observable

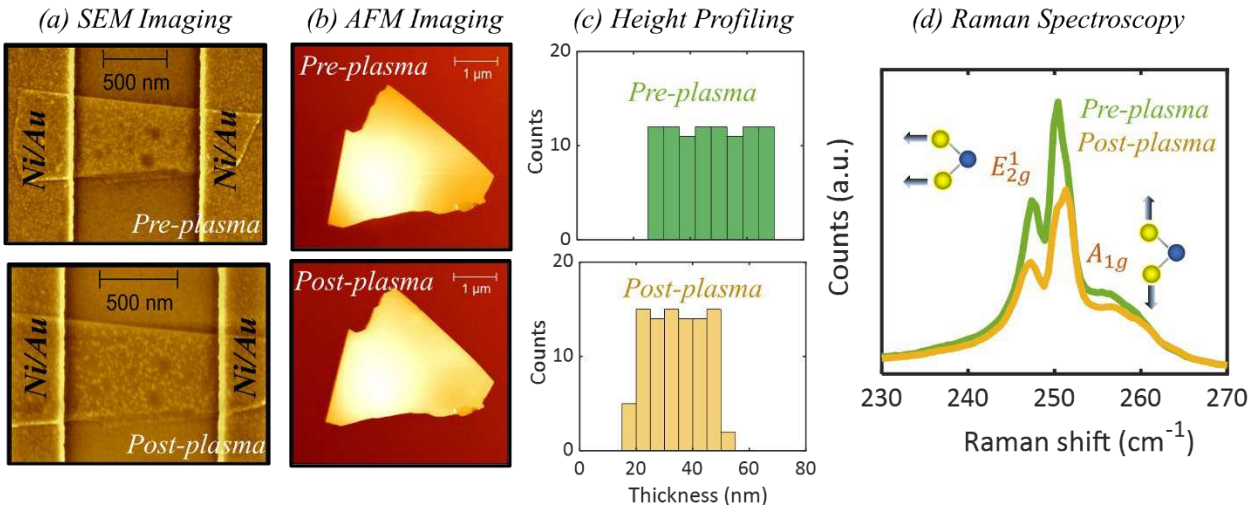

Figure 8. Optical decamouflaging solutions. *a) SEM images, b) AFM images, c) AFM height histograms, and d) Raman measurements of a WSe_2 based TMO/TMD hetero-stack device before and after the exposure to the oxygen plasma. In the SEM image the two channels look remarkably similar, however, on a closer look, one can observe slight alterations of the surface due to mild physical damage of the flake introduced by the plasma. While the SEM image indicates additional processing of the channel, it does not reveal any information regarding the thickness and composition of the 2D material, plasma type and exposure time, and the pattern design that determines if the device is a resistor or a diode or a transistor. The height histograms (c) show few nanometers decrease in the flake thickness following 300s of oxygen plasma exposure. However, without having any prior knowledge of the pre-plasma exposure flake thickness, the reverse engineer is unlikely to extract any meaningful information about the device functionality from the AFM image. Raman spectroscopy (d) shows small observable shift in the E^1_{2g} mode, which can be attributed to the lateral oxidation of the flake and can be used for RE. While the above-mentioned characterization techniques are powerful for decamouflaging a single device, they are mostly non scalable to billions of devices on a chip. As such the RE risk will remain significantly low for TMO/TMD hetero-stack camouflaged devices and circuits.*

shift in the E^1_{2g} mode can be attributed to the lateral oxidation of the flake and can be used for RE. Reverse engineer with access to even more advanced tools such as TEM and energy dispersive X-ray spectroscopy (EDS) can obtain the elemental information and precise thicknesses of the TMD and TMO in the device stack from the cross-section imaging. While the above-mentioned characterization techniques are powerful for decamouflaging a single device, they are mostly non scalable to billions of devices on a chip. As such the RE risk will remain significantly low for TMO/TMD hetero-stack camouflaged devices and circuits.

In the conclusion, we have successfully demonstrated a novel camouflaging technique that allows obfuscation of logic gates and benchmarking circuits with unprecedented area efficiency and

resilience to SAT and ATPG attacks by exploiting 2D heterostructure devices that harness the unique material properties of 2D TMDs and their corresponding TMOs. We show that TMO/TMD hetero-stack devices can be made optically indistinguishable but functionally diverse by using lithographic patterning and mild oxygen plasma exposure. We have also shown that by changing the initial thickness of the exfoliated multilayer TMD material and by controlling the plasma exposure time the resistance values can be tuned by more than 8 orders of magnitude for camouflaged resistors, the turn on voltages and reverse saturation current can be adjusted for camouflaged diodes and conduction type, threshold voltage, and current ON-OFF ratio can be regulated for camouflaged FETs. We have used 5 different semiconducting TMDs: WSe_2, MoS_2, $MoSe_2$, $MoTe_2$, and WS_2 to show the generic nature of our approach offering tremendous flexibility for device and circuit designers. Furthermore, we show that our inherently camouflaged 2D heterostructure devices allow obfuscation of both digital and analog circuits with significantly less area overhead and higher resilience to reverse engineering compared to corresponding CMOS-based camouflaging. Our hypothesis has been corroborated with empirical results obtained by performing experiments using ISCAS'85 benchmark circuits. Our implementation also eliminates the need for a hybrid design when compared to other emerging solutions, such as polymorphic gates based on giant spin Hall effect (GSHE). As a result, our proposed camouflaging technique with 2D heterostructure devices is capable to obfuscate 100% of all the possible gates that can be camouflaged in the circuit. Our novel approach of connecting unique material properties to innovative devices, in order to secure circuits highlights the benefits of cross-layer optimization.

Methods

Device Fabrication: Multilayer TMD flakes were mechanically exfoliated on a 50nm alumina substrate. The transferred flakes were mapped in terms of their location and dimensions using an optical microscope. The plasma doping was performed in a Tepla M4L plasma etching tool. Before placing the sample inside the tool, a conditioning step was performed to prepare the chamber. The radiofrequency (RF) power was set to 300 W and the pressure inside was set to 500-mTorr. The O_2 and He flow rates were adjusted to 150 and 50 standard cubic centimeters (sccm) respectively and the conditioning was done for 5 minutes. For doping the flakes, the chamber pressure and gas flow rates were set to the same values with the RF power adjusted to 50W. These conditions represent the minimum power and gas flow rates for a reliable and consistent plasma in this particular tool. The RF power was kept at a minimum to mitigate any damaging effects to the flake. Various WSe_2 flakes with a mean thickness ranging from 8nm to 45nm were selected and subsequently exposed to the oxygen plasma for varying time intervals of 15s, 30s, 75s, 120s, 210s and 300s. Optical images were acquired between each time step using a Nikon L200ND microscope with a 100x lens objective and the flake thicknesses were measured prior to and after 300s of exposure with atomic force microscopy (AFM) to observe any visible changes in their appearances and thickness reduction respectively as a result of prolonged plasma exposure. For defining the contacts, the substrate was first spin-coated with MMA/PMMA bilayer stack, and electron-beam lithography (EBPG 5200 Vistec e-beam with Raith software) was used to pattern the source and drain pads. The exposed PMMA was removed using a 1:1 methyl isobutyl ketone and isopropanol (MIBK: IPA) developer. Thereafter, 40 nm Ni/30 nm Au metal stack was deposited at the rate of 2 Å/s using the Temescal FC2000 metal evaporator. A second lithography step was performed where the flakes were exposed for subsequent plasma doping and form a

WSe_2/WO_{3-y} hetero-stack. For the resistance and transistor camouflaging, the entire flake region along the channel length and width was exposed whereas for diode camouflaging, half of the region was kept protected by the PMMA resist and the other half was exposed to the plasma. The total exposure time was 75s for all the five different TMDs and the devices were characterized electrically both before and after the plasma using a Keysight B1500A parameter analyzer in a lakeshore CRX-VF probe station. The excess PMMA was finally stripped off using standard lift-off procedure in acetone and IPA for the final optical imaging.

Electrical Measurements: Electrical measurements were performed in air inside a Lakeshore probe station using a B1500A Keysight semiconductor parameter analyzer.

Data Availability: The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Code Availability: The codes used for plotting the data are available from the corresponding authors on reasonable request.

References

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

[2] 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.

[3] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang*, et al.*, "A survey on chip to system reverse engineering," *ACM journal on emerging technologies in computing systems (JETC),* vol. 13, pp. 1-34, 2016.

[4] P. Subramanyan, N. Tsiskaridze, W. Li, A. Gascón, W. Y. Tan, A. Tiwari*, et al.*, "Reverse engineering digital circuits using structural and functional analyses," *IEEE Transactions on Emerging Topics in Computing,* vol. 2, pp. 63-80, 2013.

[5] R. Torrance and D. James, "The state-of-the-art in IC reverse engineering," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2009, pp. 363-381.

[6] Chipworks. (2012). *Intel's 22-nm Trigate Transistors Exposed*.

[7] M. Li, K. Shamsi, T. Meade, Z. Zhao, B. Yu, Y. Jin*, et al.*, "Provably secure camouflaging strategy for IC protection," *IEEE transactions on computer-aided design of integrated circuits and systems,* 2017.

[8] J. Rajendran, O. Sinanoglu, and R. Karri, "VLSI testing based security metric for IC camouflaging," in *2013 IEEE International Test Conference (ITC)*, 2013, pp. 1-4.

[9] 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.

[10] M. El Massad, S. Garg, and M. V. Tripunitara, "Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes," in *NDSS*, 2015, pp. 1-14.

[11] C. Yu, X. Zhang, D. Liu, M. Ciesielski, and D. Holcomb, "Incremental SAT-based reverse engineering of camouflaged logic circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 36, pp. 1647-1659, 2017.

[12] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "CamoPerturb: Secure IC camouflaging for minterm protection," in *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2016, pp. 1-8.

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

[14] M. I. M. Collantes, M. El Massad, and S. Garg, "Threshold-dependent camouflaged cells to secure circuits against reverse engineering attacks," in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2016, pp. 443-448.

[15] B. Erbagci, C. Erbagci, N. E. C. Akkaya, and K. Mai, "A secure camouflaged threshold voltage defined logic family," in *2016 IEEE International symposium on hardware oriented security and trust (HOST)*, 2016, pp. 229-235.

[16] A. Iyengar and S. Ghosh, "Threshold voltage-defined switches for programmable gates," *arXiv preprint arXiv:1512.01581,* 2015.

[17] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware trojans," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2013, pp. 197-214.
[18] L.-W. Chow, W. M. Clark Jr, and J. P. Baukus, "Covert transformation of transistor properties as a circuit protection method," ed: Google Patents, 2007.
[19] K. Shamsi, M. Li, T. Meade, Z. Zhao, D. Z. Pan, and Y. Jin, "Cyclic obfuscation for creating sat-unresolvable circuits," in *Proceedings of the on Great Lakes Symposium on VLSI 2017*, 2017, pp. 173-178.
[20] Y.-W. Lee and N. A. Touba, "Improving logic obfuscation via logic cone analysis," in *2015 16th Latin-American Test Symposium (LATS)*, 2015, pp. 1-6.
[21] H. Esmaeilzadeh, E. Blem, R. S. Amant, K. Sankaralingam, and D. Burger, "Dark silicon and the end of multicore scaling," in *2011 38th Annual International Symposium on Computer Architecture (ISCA)*, 2011, pp. 365-376.
[22] W. Haensch, E. J. Nowak, R. H. Dennard, P. M. Solomon, A. Bryant, O. H. Dokumaci*, et al.*, "Silicon CMOS devices beyond scaling," *IBM Journal of Research and Development,* vol. 50, pp. 339-361, 2006.
[23] C. P. Kruger and G. P. Hancke, "Benchmarking Internet of things devices," in *Industrial Informatics (INDIN), 2014 12th IEEE International Conference on*, 2014, pp. 611-616.
[24] S. Manzeli, D. Ovchinnikov, D. Pasquier, O. V. Yazyev, and A. Kis, "2D transition metal dichalcogenides," *Nature Reviews Materials,* vol. 2, p. 17033, 2017.
[25] G. Fiori, F. Bonaccorso, G. Iannaccone, T. Palacios, D. Neumaier, A. Seabaugh*, et al.*, "Electronics based on two-dimensional materials," *Nat Nanotechnol,* vol. 9, pp. 768-79, Oct 2014.
[26] 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, p. 699, 11/06/online 2012.
[27] G. R. Bhimanapati, Z. Lin, V. Meunier, Y. Jung, J. Cha, S. Das*, et al.*, "Recent Advances in Two-Dimensional Materials beyond Graphene," *ACS Nano,* vol. 9, pp. 11509-11539, 2015/12/22 2015.
[28] S. Das, J. A. Robinson, M. Dubey, H. Terrones, and M. Terrones, "Beyond Graphene: Progress in Novel Two-Dimensional Materials and van der Waals Solids," *Annual Review of Materials Research, Vol 45,* vol. 45, pp. 1-27, 2015.
[29] A. Sebastian, A. Pannone, S. S. Radhakrishnan, and S. Das, "Gaussian synapses for probabilistic neural networks," *Nature communications,* vol. 10, pp. 1-11, 2019.
[30] S. Das, A. Dodda, and S. Das, "A biomimetic 2D transistor for audiomorphic computing," *Nature Communications,* vol. 10, p. 3450, 2019/08/01 2019.
[31] L. Liu, Y. Lu, and J. Guo, "On Monolayer ${\rm MoS}_{2}$ Field-Effect Transistors at the Scaling Limit," *IEEE Transactions on Electron Devices,* vol. 60, pp. 4133-4139, 2013.
[32] S. B. Desai, S. R. Madhvapathy, A. B. Sachid, J. P. Llinas, Q. Wang, G. H. Ahn*, et al.*, "MoS2 transistors with 1-nanometer gate lengths," *Science,* vol. 354, pp. 99-102, Oct 07 2016.
[33] S. J. Kim, K. Choi, B. Lee, Y. Kim, and B. H. Hong, "Materials for Flexible, Stretchable Electronics: Graphene and 2D Materials," *Annual Review of Materials Research,* vol. 45, pp. 63-84, 2015.

[34] S. Das, R. Gulotty, A. V. Sumant, and A. Roelofs, "All two-dimensional, flexible, transparent, and thinnest thin film transistor," *Nano Lett,* vol. 14, pp. 2861-6, May 14 2014.

[35] D. McManus, S. Vranic, F. Withers, V. Sanchez-Romaguera, M. Macucci, H. Yang*, et al.*, "Water-based and biocompatible 2D crystal inks for all-inkjet-printed heterostructures," *Nature nanotechnology,* vol. 12, p. 343, 2017.

[36] K. Kang, S. Xie, L. Huang, Y. Han, P. Y. Huang, K. F. Mak*, et al.*, "High-mobility three-atom-thick semiconducting films with wafer-scale homogeneity," *Nature,* vol. 520, p. 656, 2015.

[37] S. Wang, W. Zhao, F. Giustiniano, and G. Eda, "Effect of oxygen and ozone on p-type doping of ultra-thin WSe2 and MoSe2 field effect transistors," *Phys Chem Chem Phys,* vol. 18, pp. 4304-9, Feb 14 2016.

[38] P. Bolshakov, C. M. Smyth, A. Khosravi, P. Zhao, P. K. Hurley, C. L. Hinkle*, et al.*, "Contact Engineering for Dual-Gate MoS2 Transistors Using O2 Plasma Exposure," *ACS Applied Electronic Materials,* vol. 1, pp. 210-219, 2019.

[39] A. N. Hoffman, M. G. Stanford, M. G. Sales, C. Zhang, I. N. Ivanov, S. J. McDonnell*, et al.*, "Tuning the electrical properties of WSe2 via O2 plasma oxidation: towards lateral homojunctions," *2D Materials,* vol. 6, 2019.

[40] C.-S. Pang, T. Y. T. Hung, A. Khosravi, R. Addou, Q. Wang, M. J. Kim*, et al.* (2019, October 01, 2019). Atomically Controlled Tunable Doping in High Performance WSe2 Devices. *arXiv e-prints*. Available: https://ui.adsabs.harvard.edu/abs/2019arXiv191008619P

[41] M. Yamamoto, S. Nakaharai, K. Ueno, and K. Tsukagoshi, "Self-Limiting Oxides on WSe2 as Controlled Surface Acceptors and Low-Resistance Hole Contacts," *Nano Lett,* vol. 16, pp. 2720-7, Apr 13 2016.

[42] N. M. D. Brown, N. Cui, and A. McKinley, "An XPS study of the surface modification of natural MoS2 following treatment in an RF-oxygen plasma," *Applied Surface Science,* vol. 134, pp. 11-21, 1998.

[43] S. Das, H. Y. Chen, A. V. Penumatcha, and J. Appenzeller, "High performance multilayer MoS2 transistors with scandium contacts," *Nano Lett,* vol. 13, pp. 100-5, Jan 09 2013.

[44] S. Das and J. Appenzeller, "WSe2 field effect transistors with enhanced ambipolar characteristics," *Applied Physics Letters,* vol. 103, Sep 2 2013.

[45] D. S. Schulman, A. J. Arnold, and S. Das, "Contact engineering for 2D materials and devices," *Chem Soc Rev,* Mar 2 2018.

[46] D. Saptarshi and A. Joerg, "Screening and interlayer coupling in multilayer MoS2," *physica status solidi (RRL) – Rapid Research Letters,* vol. 7, pp. 268-273, 2013.

[47] S. Das and J. Appenzeller, "Where does the current flow in two-dimensional layered systems?," *Nano Lett,* vol. 13, pp. 3396-402, Jul 10 2013.

[48] B. Chen, H. Sahin, A. Suslu, L. Ding, M. I. Bertoni, F. M. Peeters*, et al.*, "Environmental Changes in MoTe2 Excitonic Dynamics by Defects-Activated Molecular Interaction," *ACS Nano,* vol. 9, pp. 5326-32, May 26 2015.

[49] S. Patnaik, N. Rangarajan, J. Knechtel, O. Sinanoglu, and S. Rakheja, "Advancing hardware security using polymorphic and stochastic spin-hall effect devices," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2018, pp. 97-102.

Supplementary Information

Supplementary Information file includes evolution of optical images of WO_{3-y}/WSe_2 hetero-stacks of two different thicknesses as a function of the plasma exposure time, tunability in camouflaged diode turn-on voltage and reverse saturation current using V_{BG} for thin and thick WO_{3-y}/WSe_2 stacks, evolution of the transfer characteristics for 30 nm and 59 nm thick WSe_2 flakes as a function of the plasma exposure times, relative strength of electron and hole conduction in various TMO/TMD hetero-stacks pre- and post-plasma exposure and gated camouflaged resistors.

AUTHOR INFORMATION

Corresponding Author

sud70@psu.edu, das.sapt@gmail.com

Author Contributions

S.D conceived the idea. A.W and A.J.A performed the device fabrication, material characterization and electrical measurements. S.K, S.C and K.B designed the camouflaged gates and tested the SAT-attack and ATPG-attacks. All authors analyzed the data, discussed the results, agreed on their implications. All authors contributed to the preparation of the manuscript.

Competing Interest

The authors declare no competing interests

Acknowledgement

None.

Figure Captions

Figure 1. Camouflaged two-dimensional (2D) heterostructure for hardware obfuscation. a) Natural camouflaging for survival. Photograph of a camouflaged tree spider. b) IC camouflaging using dummy contact to thwart reverse engineering. For an observer, the circuit functionality appears to be $Y = ABC$, however, the true functionality is $Y = AB$, since the connection from the input C to the output Y is camouflaged. c) Proposed camouflaging enabled by unique material properties of transition metal dichalcogenides (TMDs) and their corresponding transition metal oxides (TMOs). The optical image shows a camouflaged TMO/TMD hetero-stack device that can be either a resistor or a diode or a transistor. d) Schematic showing that when the TMDs are exposed to mild oxygen plasma, the top few layers can be transformed to corresponding sub-stoichiometric TMOs through a self-limiting and highly anisotropic oxidation process that favors lateral oxidation within layers of TMDs with minimal vertical propagation. TMOs are insulating, optically transparent and are p-type dopant for TMDs, whereas, TMDs are semiconducting, opaque and intrinsically n-type. e) Optical images of a 35 nm thick WSe_2 flake taken sequentially following exposer to mild oxygen plasma at 50 watts RF power for the indicated amount of times. f) Histograms of the red, green and blue (RGB) color spectrum for the optical images in (e) show no significant changes in any of the three-color channels indicating that the images are practically indistinguishable. g) Color map of correlation coefficient (CC) between the binarized optical images from (e). CC values close to '1' indicate perfect similarity between the images. These findings suggest that the plasma treatment process and hence the presence of TMO on top of the TMD is concealed from the adversary. Furthermore, the thickness of the TMO layer, which depends on the plasma exposure time, as well as the region of its presence (i.e. partial or complete covering of the TMD) are also not revealed in the optical images.

Figure 2. Camouflaged resistors. a) Schematic of a camouflaged resistor based on TMO/TMD hetero-stack. b) Optical images and c) corresponding current *versus* voltage characteristics of a 10 nm thick WO_{3-y}/WSe_2 hetero-stack resistor before and after 30s of oxygen plasma exposure. While the optical appearances remain identical the resistances differ significantly. The change in resistance can be attributed to the change in the surface charge doping introduced by the sub-stoichiometric WO_{3-y} in the underlying WSe_2. d) Energy band diagrams showing the transition in the Fermi level (E_F) towards the valence band since the oxygen deficient WO_{3-y} acts like an electron acceptor introducing p-type doping in WSe_2. e) Bar plot showing the extracted resistance values (normalized to width) for camouflaged WO_{3-y}/WSe_2 hetero-stack resistors for different initial thicknesses of the exfoliated WSe_2 flakes as a function of plasma exposure time. All resistors had 1μm channel length and 40 nm Ni/ 30 nm Au as the contact metal. The resistance value changes by more than 8 orders of magnitude without changing the device footprint or their optical appearances. Similar results are obtained for f) MoS_2, g) $MoSe_2$, h) $MoTe_2$ and i) WS_2 based camouflaged resistors pre- and post-exposure to oxygen plasma for 75s. While any semiconducting material will form insulating and transparent surface oxide when exposed to mild oxygen plasma, what makes TMOs unique is their capability to dope the underlying TMDs and thereby change the resistance values by orders of magnitude. These TMO/TMD hetero-stack resistors can, therefore, be used to camouflage connections between devices and circuits in an IC to increase the complexity of RE without adding any area or energy overhead.

Figure 3. Camouflaged Diodes. a) Schematic of a camouflaged diode based on TMO/TMD hetero-stack. Camouflaged diodes require an additional processing step where one side of the fabricated TMD resistors are protected by PMMA which is patterned using electron beam

lithography before exposure to the oxygen plasma. The PMMA is striped off afterwards. This fabrication step ensures that the protected area remains intrinsic, whereas the exposed area becomes p-type doped due to the formation of sub-stoichiometric TMO. b) Optical images of the device before and after the fabrication of the diode based on WSe_2. Clearly, the images appear identical making it difficult for an adversary to recognize the functionality of the device through visual inspection. Current *versus* voltage characteristics of a thin diode in c) linear and d) logarithmic scales. Clearly, rectifying behaviors are observed. Since the diodes were fabricated on a back-gate stack comprising of 50 nm Al_2O_3 as the back-gate oxide and Pt/TiN/p^{++}-Si as the back-gate electrode, dynamic reconfiguration of the diode characteristics is possible through electrostatic doping using the back-gate voltage (V_{BG}). Current *versus* voltage characteristics of a thick diode in e) linear and f) logarithmic scales. The thin diode shows late turn on since the built-in-potential is higher between the undoped region which is intrinsically n-type doped and the p-type doped region compared to the thick diode where the undoped region is more intrinsic. Also the thin diode offers significantly low reverse saturation current, whereas, the reverse saturation current depends strongly on the applied V_{BG} for the thick diode. This is expected since for thicker diodes, the phenomenon of Thomas-Fermi charge screening restricts the doping effect to only top few layers, while the layers at the bottom of the stack i.e. the layers close to the oxide are under firm back-gate control. For $V_{BG} \gg 0$, these layers become electrostatically n-doped and offer a parallel conduction path for the current to flow between the two metal contacts. The tunability of camouflaged diode characteristics through back-gating adds one more level of complexity to RE.

Figure 4. Camouflaged Transistors: a) Schematic of a camouflaged FET based on TMO/TMD hetero-stack. b) Optical images of WO_{3-y}/WSe_2 hetero-stack FET before and after the oxygen

plasma exposure. Clearly, the images appear identical making it difficult for an adversary to recognize the FET functionality through visual inspection. c) Evolution of the transfer characteristics for WO_{3-y}/WSe_2 hetero-stack FET as a function of oxygen plasma exposure time for two different initial flake thicknesses. d) A table summarizing the transition of pristine WSe_2 based FETs from dominant n-type to ambipolar to p-type transport characteristics as the plasma exposure time increases for various flake thicknesses. The change in dominant carrier transport from electron conduction (n-type) to hole conduction (p-type) with increasing plasma exposure time is consistent with the fact that the sub-stoichiometric WO_{3-x} introduces p-type doping in the underlying WSe_2. Color map for e) threshold voltages (V_{TH}) and f) current ON/OFF ratio for the dominant branch. Similar observations can be made in the transfer characteristics of g) MoS_2, h) $MoSe_2$, i) $MoTe_2$ and j) WS_2 based camouflaged FETs before and after exposure to oxygen plasma for 75s. Irrespective of the choice of material, p-type conduction is enhanced. These results indicate that TMO/TMD hetero-stack FETs can be camouflaged with tunable device parameters through oxygen plasma exposure irrespective of their thickness and composition and without compromising their optical indistinguishability which is critical for defying the RE efforts. What is more attractive is that these camouflaged TMO/TMD hetero-stack devices do not add any area overhead which is unavoidable for the state-of-the-art layout level camouflaging approaches.

Figure 5. Camouflaged analog circuits. a) Number of trials (F) for reverse engineering an integrated circuit (IC) with M hardware components, each with P possibilities. Even for relatively small, $M = 1000$ and $P = 6$, the number of RE trials becomes astronomical, $F = 10^{40}$. b) Camouflaged circuit layout exploiting TMO/TMD hetero-stack devices. Both layouts are visually identical but the one functions as a voltage divider, while the other functions as a half wave

rectifier. c) A camouflaged digital to analog mapping circuit with multiple digital input and one analog output. This circuit functions as a digital to analog converter (DAC) for $^{R_1}/_{R_2} = 2\ but$ transforms into a digital bit counter (DBC) that counts the number of ones in a digital sequence for $^{R_1}/_{R_2} \gg 2$.

Figure 6. Camouflaged logic gate. d) Overview of a digital logic circuit with camouflaged elements. Actualization of e) NAND gate, f) AND gate, g) NOR gate, and h) OR gate with TMO/TMD hetero-stack based camouflaged p-FET, n-FET, and resistor. Since the camouflaged devices are physically identical to each other, the gates developed using those elements also look exactly the same.

Figure 7. Camouflaged digital circuit. Camouflaged representation of c17 benchmark circuit consisting of 6 camouflaged gates (G1 to G6), in order to demonstrate resilience against ATPG attacks.

Figure 8. Optical decamouflaging solutions. a) SEM images, b) AFM images, c) AFM height histograms, and d) Raman measurements of a WSe_2 based TMO/TMD hetero-stack device before and after the exposure to the oxygen plasma. In the SEM image the two channels look remarkably similar, however, on a closer look, one can observe slight alterations of the surface due to mild physical damage of the flake introduced by the plasma. While the SEM image indicates additional processing of the channel, it does not reveal any information regarding the thickness and composition of the 2D material, plasma type and exposure time, and the pattern design that

determines if the device is a resistor or a diode or a transistor. The height histograms (c) show few nanometers decrease in the flake thickness following 300s of oxygen plasma exposure. However, without having any prior knowledge of the pre-plasma exposure flake thickness, the reverse engineer is unlikely to extract any meaningful information about the device functionality from the AFM image. Raman spectroscopy (d) shows small observable shift in the E_{2g}^{1} mode, which can be attributed to the lateral oxidation of the flake and can be used for RE. While the above-mentioned characterization techniques are powerful for decamouflaging a single device, they are mostly non scalable to billions of devices on a chip. As such the RE risk will remain significantly low for TMO/TMD hetero-stack camouflaged devices and circuits.

Figures

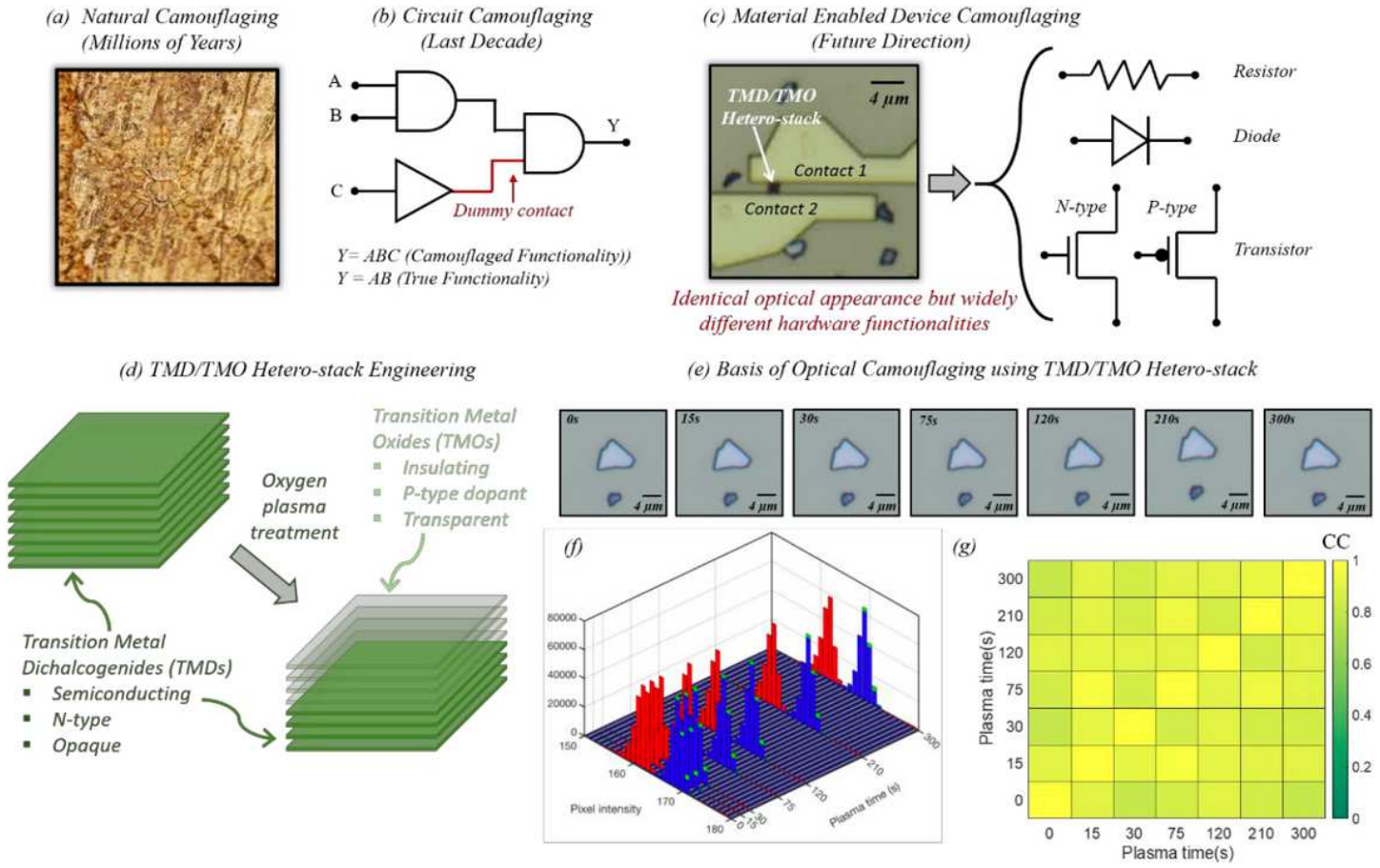

Figure 1

Camouflaged two-dimensional (2D) heterostructure for hardware obfuscation. a) Natural camouflaging for survival. Photograph of a camouflaged tree spider. b) IC camouflaging using dummy contact to thwart reverse engineering. For an observer, the circuit functionality appears to be ▯▯=▯▯▯▯▯ , however, the true functionality is ▯▯=▯▯▯▯, since the connection from the input ▯ to the output ▯▯ is camouflaged. c) Proposed camouflaging enabled by unique material properties of transition metal dichalcogenides (TMDs) and their corresponding transition metal oxides (TMOs). The optical image shows a camouflaged TMO/TMD hetero-stack device that can be either a resistor or a diode or a transistor. d) Schematic showing that when the TMDs are exposed to mild oxygen plasma, the top few layers can be transformed to corresponding sub-stoichiometric TMOs through a self-limiting and highly anisotropic oxidation process that favors lateral oxidation within layers of TMDs with minimal vertical propagation. TMOs are insulating, optically transparent and are p-type dopant for TMDs, whereas, TMDs are semiconducting, opaque, and intrinsically n-type. e) Optical images of a 35 nm thick WSe2 flake taken sequentially following exposer to mild oxygen plasma at 50 watts RF power for the indicated amount of times. f) Histograms of the red, green, and blue (RGB) color spectrum for the optical images in (e) show no significant changes in any of the three-color channels indicating that the images are practically

indistinguishable. g) Color map of correlation coefficient (CC) between the binarized optical images from (e). CC values close to '1' indicate perfect similarity between the images. These findings suggest that the plasma treatment process and hence the presence of TMO on top of the TMD is concealed from the adversary. Furthermore, the thickness of the TMO layer, which depends on the plasma exposure time, as well as the region of its presence (i.e. partial or complete covering of the TMD) are also not revealed in the optical images.

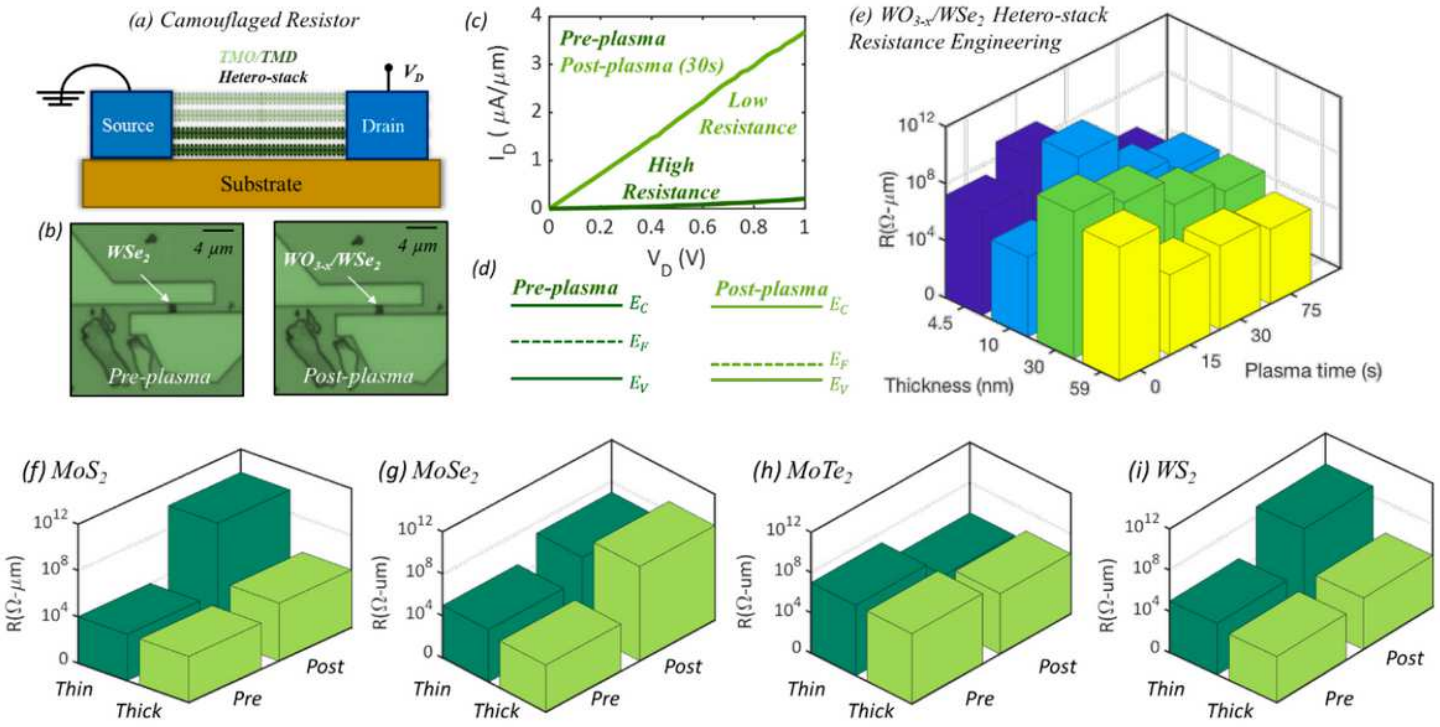

Figure 2

Camouflaged resistors. a) Schematic of a camouflaged resistor based on TMO/TMD hetero-stack. b) Optical images and c) corresponding current versus voltage characteristics of a 10 nm thick WO3-y/WSe2 hetero-stack resistor before and after 30s of oxygen plasma exposure. While the optical appearances remain identical the resistances differ significantly. The change in resistance can be attributed to the change in the surface charge doping introduced by the sub-stoichiometric WO3-y in the underlying WSe2. d) Energy band diagrams showing the transition in the Fermi level (□□□□) towards the valence band since the oxygen deficient WO3-y acts like an electron acceptor introducing p-type doping in WSe2. e) Bar plot showing the extracted resistance values (normalized to width) for camouflaged WO3-y/WSe2 hetero-stack resistors for different initial thicknesses of the exfoliated WSe2 flakes as a function of plasma exposure time. All resistors had 1μm channel length and 40 nm Ni/ 30 nm Au as the contact metal. The resistance value changes by more than 8 orders of magnitude without changing the device footprint or their optical appearances. Similar results are obtained for f) MoS2, g) MoSe2, h) MoTe2 and i) WS2 based camouflaged resistors pre- and post-exposure to oxygen plasma for 75s. While any semiconducting material will form insulating and transparent surface oxide when exposed to mild

oxygen plasma, what makes TMOs unique is their capability to dope the underlying TMDs and thereby change the resistance values by orders of magnitude. These TMO/TMD hetero-stack resistors can, therefore, be used to camouflage connections between devices and circuits in an IC to increase the complexity of RE without adding any area or energy overhead.

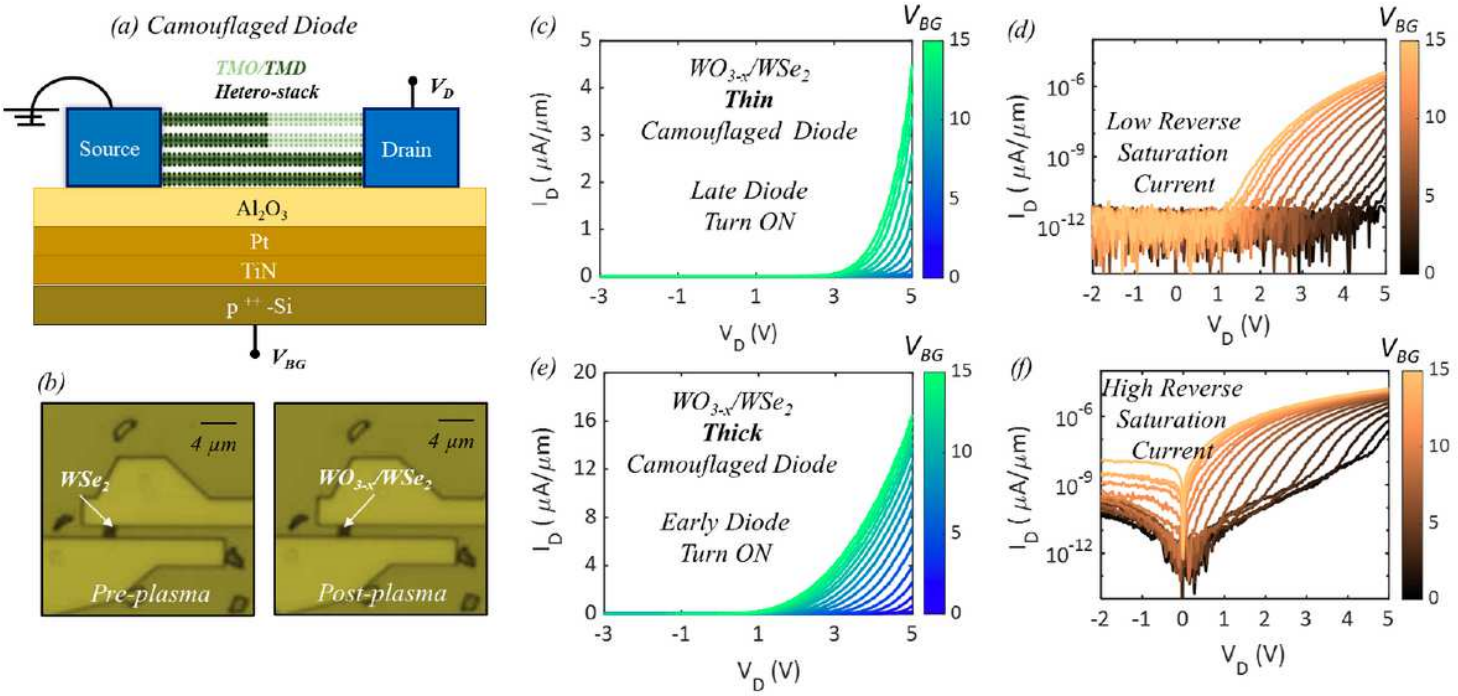

Figure 3

Camouflaged Diodes. a) Schematic of a camouflaged diode based on TMO/TMD hetero-stack. Camouflaged diodes require an additional processing step where one side of the fabricated TMD resistors are protected by PMMA which is patterned using electron beam lithography before exposure to the oxygen plasma. The PMMA is striped off afterwards. This fabrication step ensures that the protected area remains intrinsic, whereas the exposed area becomes p-type doped due to the formation of sub-stoichiometric TMO. b) Optical images of the device before and after the fabrication of the diode based on WSe2. Clearly, the images appear identical making it difficult for an adversary to recognize the functionality of the device through visual inspection. Current versus voltage characteristics of a thin diode in c) linear and d) logarithmic scales. Clearly, rectifying behaviors are observed. Since the diodes were fabricated on a back-gate stack comprising of 50 nm Al2O3 as the back-gate oxide and Pt/TiN/p++-Si as the back-gate electrode, dynamic reconfiguration of the diode characteristics is possible through electrostatic doping using the back-gate voltage (□□□□□□). Current versus voltage characteristics of a thick diode in e) linear and f) logarithmic scales. The thin diode shows late turn on since the built-in-potential is higher between the undoped region which is intrinsically n-type doped and the p-type doped region compared to the thick diode where the undoped region is more intrinsic. Also, the thin diode offers significantly low reverse saturation current, whereas, the reverse saturation current depends strongly on the applied □□□□□□ for the thick diode. This is expected since for thicker diodes, the phenomenon of Thomas-Fermi charge screening restricts the doping effect to only top few layers, while the layers at the

bottom of the stack i.e. the layers close to the oxide are under firm back-gate control. For □□□□□□□0, these layers become electrostatically n-doped and offer a parallel conduction path for the current to flow between the two metal contacts. The tunability of camouflaged diode characteristics through back-gating adds one more level of complexity to RE.

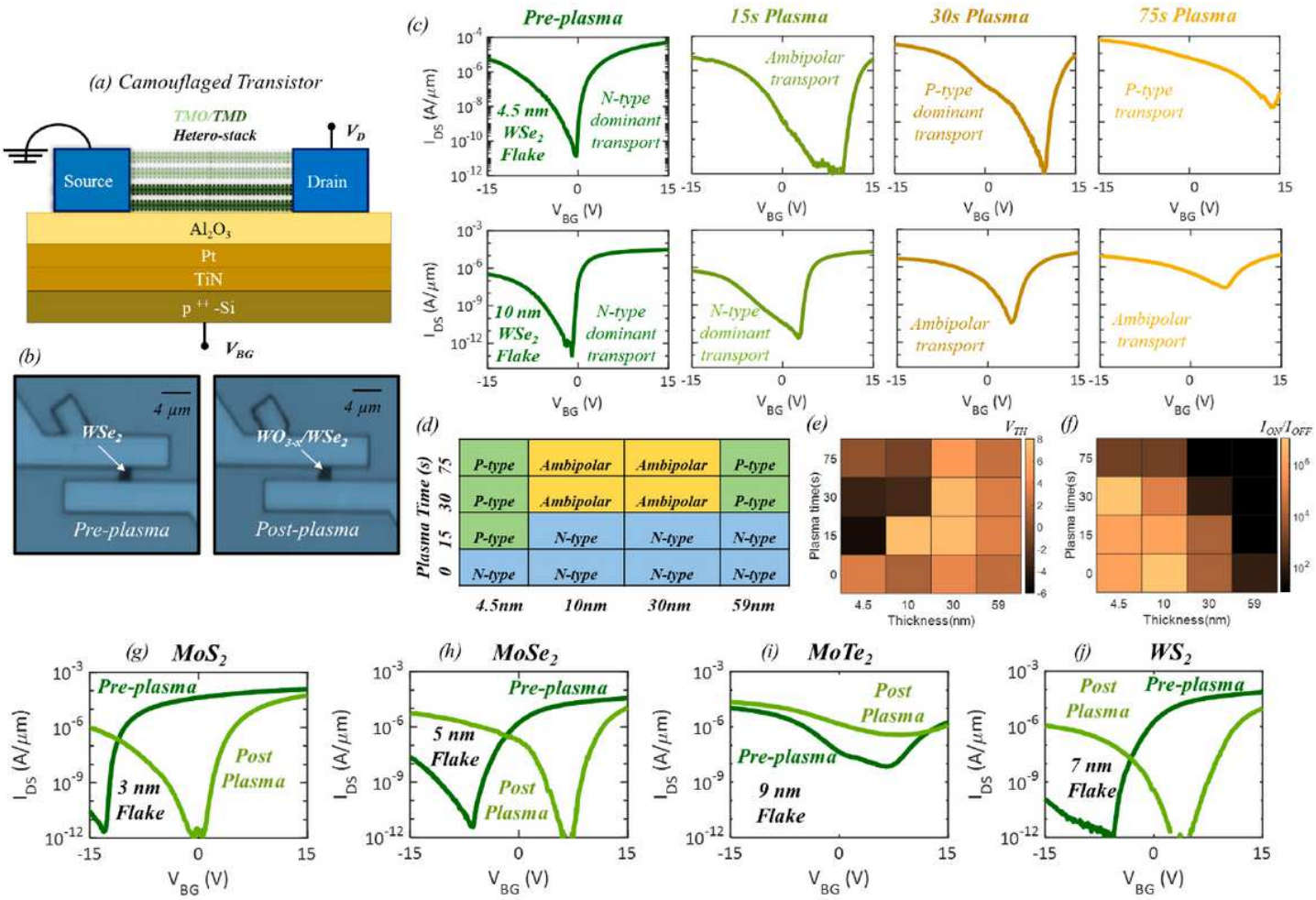

Figure 4

Camouflaged Transistors: a) Schematic of a camouflaged FET based on TMO/TMD hetero-stack. b) Optical images of WO3-y/WSe2 hetero-stack FET before and after the oxygen plasma exposure. Clearly, the images appear identical making it difficult for an adversary to recognize the FET functionality through visual inspection. c) Evolution of the transfer characteristics for WO3-y/WSe2 hetero-stack FET as a function of oxygen plasma exposure time for two different initial flake thicknesses. d) A table summarizing the transition of pristine WSe2 based FETs from dominant n-type to ambipolar to p-type transport characteristics as the plasma exposure time increases for various flake thicknesses. The change in dominant carrier transport from electron conduction (n-type) to hole conduction (p-type) with increasing plasma exposure time is consistent with the fact that the sub-stoichiometric WO3-x introduces p-type doping in the underlying WSe2. Color map for e) threshold voltages (□□□□□□) and f) current ON/OFF ratio for the dominant branch. Similar observations can be made in the transfer characteristics of g) MoS2, h) MoSe2, i) MoTe2 and j) WS2 based camouflaged FETs before and after exposure to oxygen

plasma for 75s. Irrespective of the choice of material, p-type conduction is enhanced. These results indicate that TMO/TMD hetero-stack FETs can be camouflaged with tunable device parameters through oxygen plasma exposure irrespective of their thickness and composition and without compromising their optical indistinguishability which is critical for defying the RE efforts. What is more attractive is that these camouflaged TMO/TMD hetero-stack devices do not add any area overhead which is unavoidable for the state-of-the-art layout level camouflaging approaches

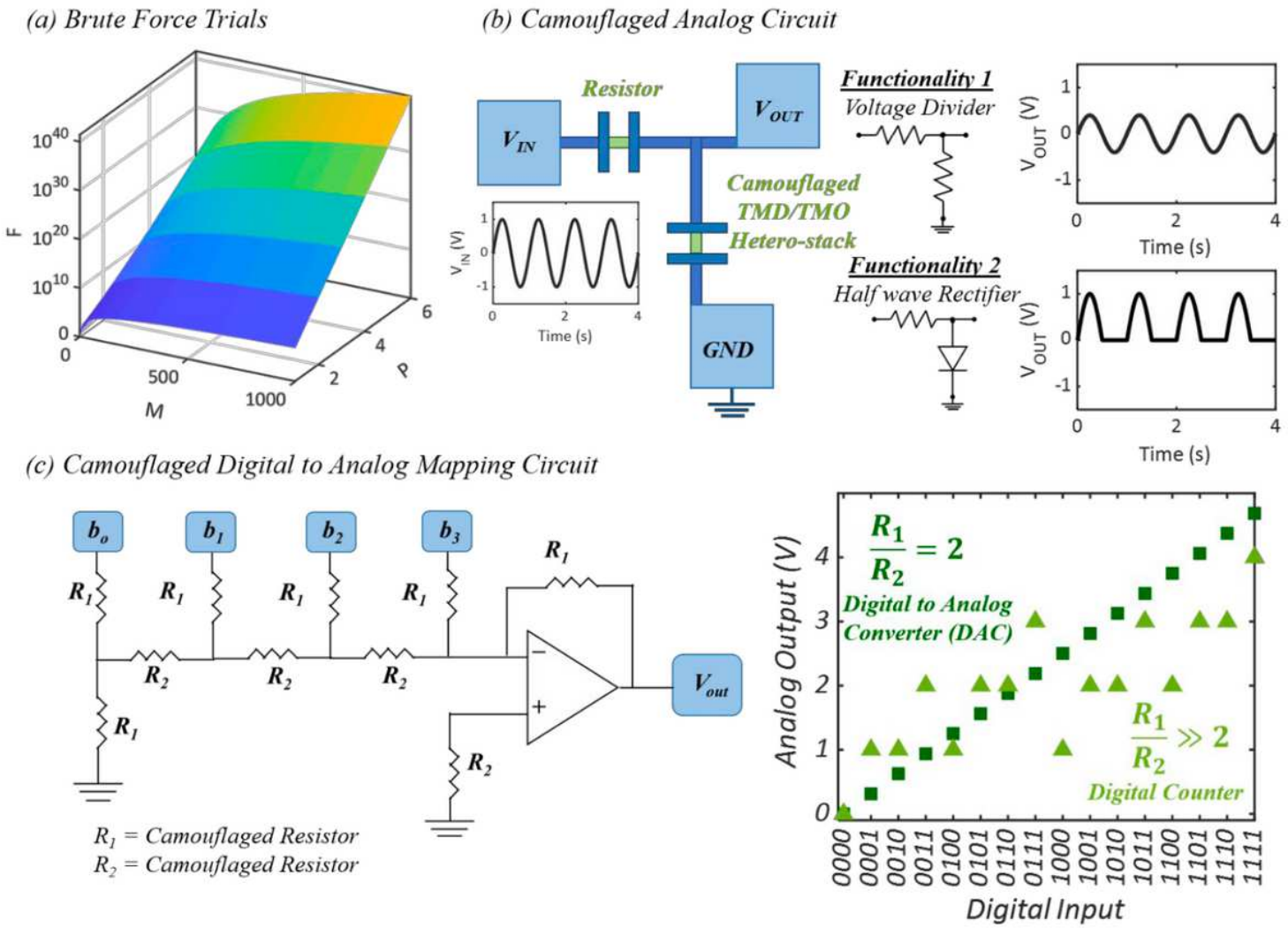

Figure 5

Camouflaged analog circuits. a) Number of trials (□□) for reverse engineering an integrated circuit (IC) with □□ hardware components, each with □□ possibilities. Even for relatively small, □□ = 1000 and □□ = 6, the number of RE trials becomes astronomical, □□ = 1040. b) Camouflaged circuit layout exploiting TMO/TMD hetero-stack devices. Both layouts are visually identical but the one functions as a voltage divider, while the other functions as a half wave rectifier. c) A camouflaged digital to analog mapping circuit with multiple digital input and one analog output. This circuit functions as a digital to analog converter (DAC) for □□1□□2 =2 □□□□□□ transforms into a digital bit counter (DBC) that counts the number of ones in a digital sequence for □□1□□2 □2.

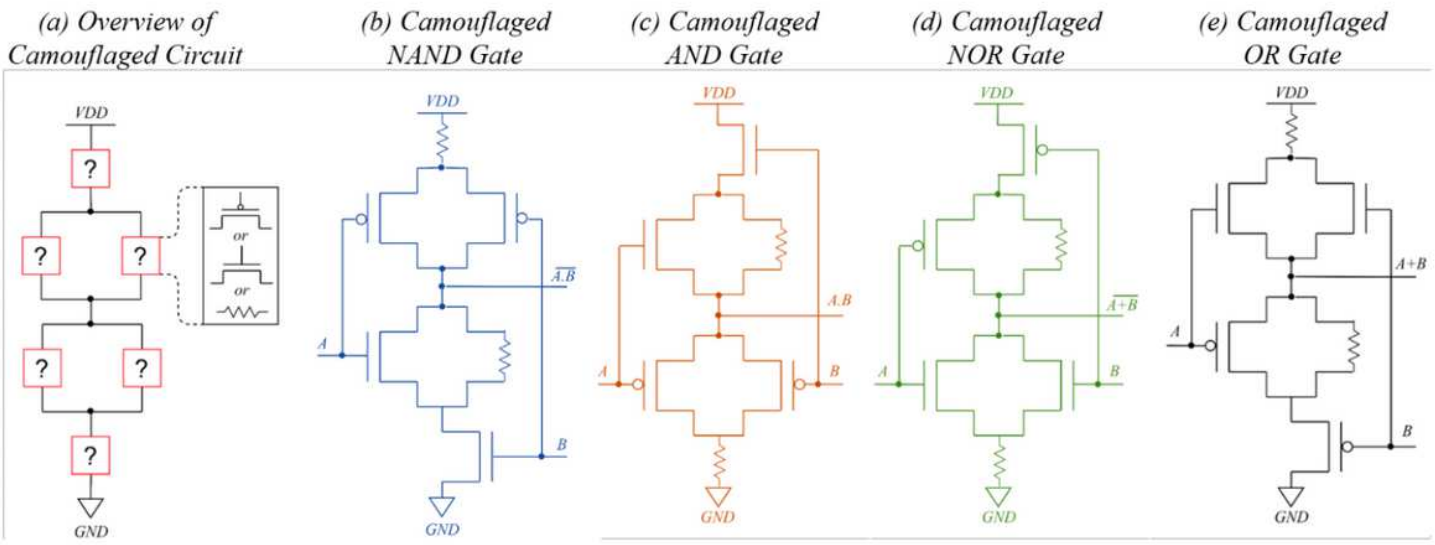

Figure 6

Camouflaged logic gates. a) Overview of a digital logic circuit with camouflaged elements. Actualization of b) NAND gate, c) AND gate, d) NOR gate, and e) OR gate with TMO/TMD hetero-stack based camouflaged p-FET, n-FET, and resistor. Since the camouflaged devices are physically identical to each other, the gates developed using those elements also look the same.

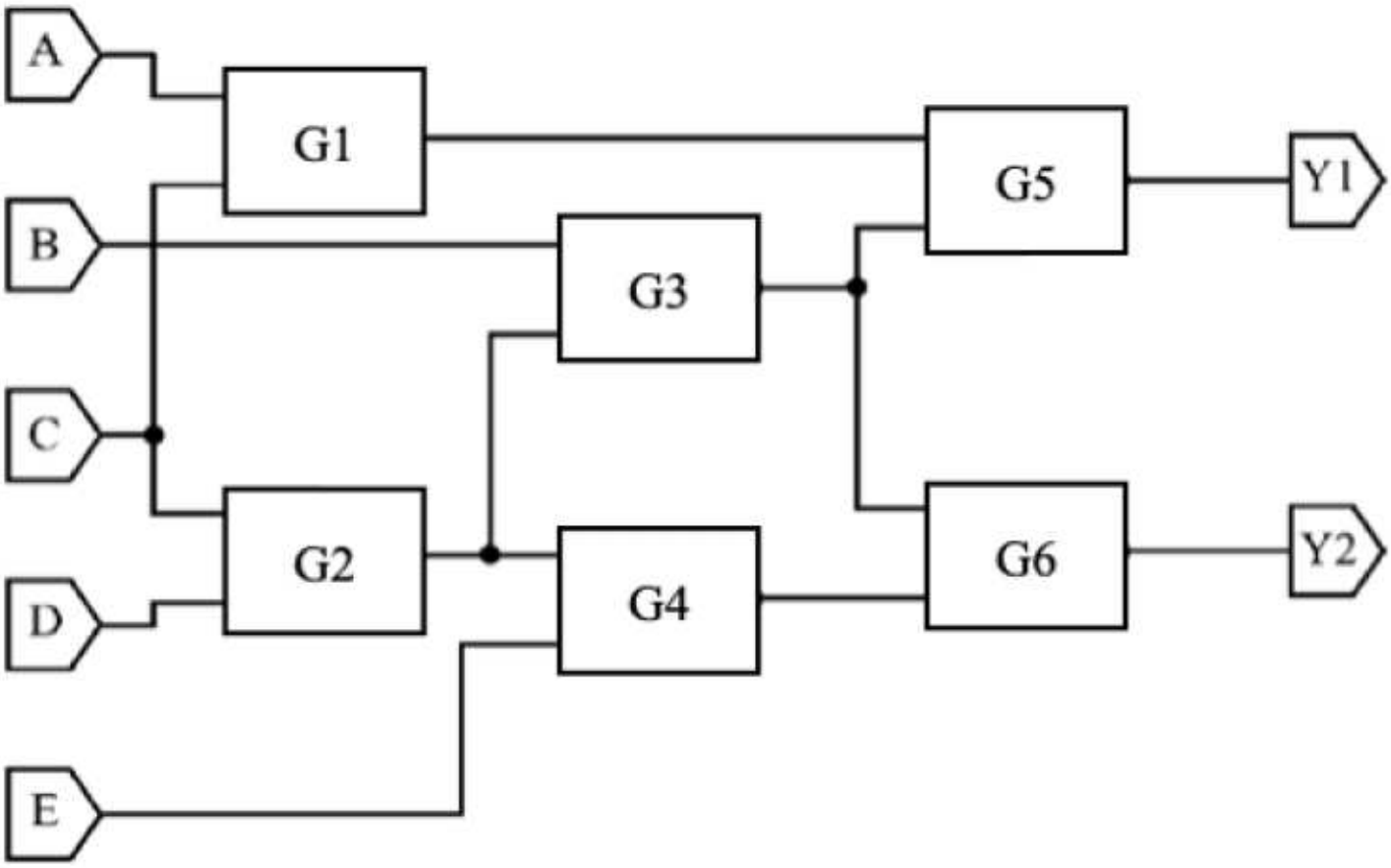

Figure 7

Camouflaged digital circuit. The c17 benchmark circuit consisting of 6 camouflaged gates (G1 to G6), in order to demonstrate resilience against ATPG attacks.

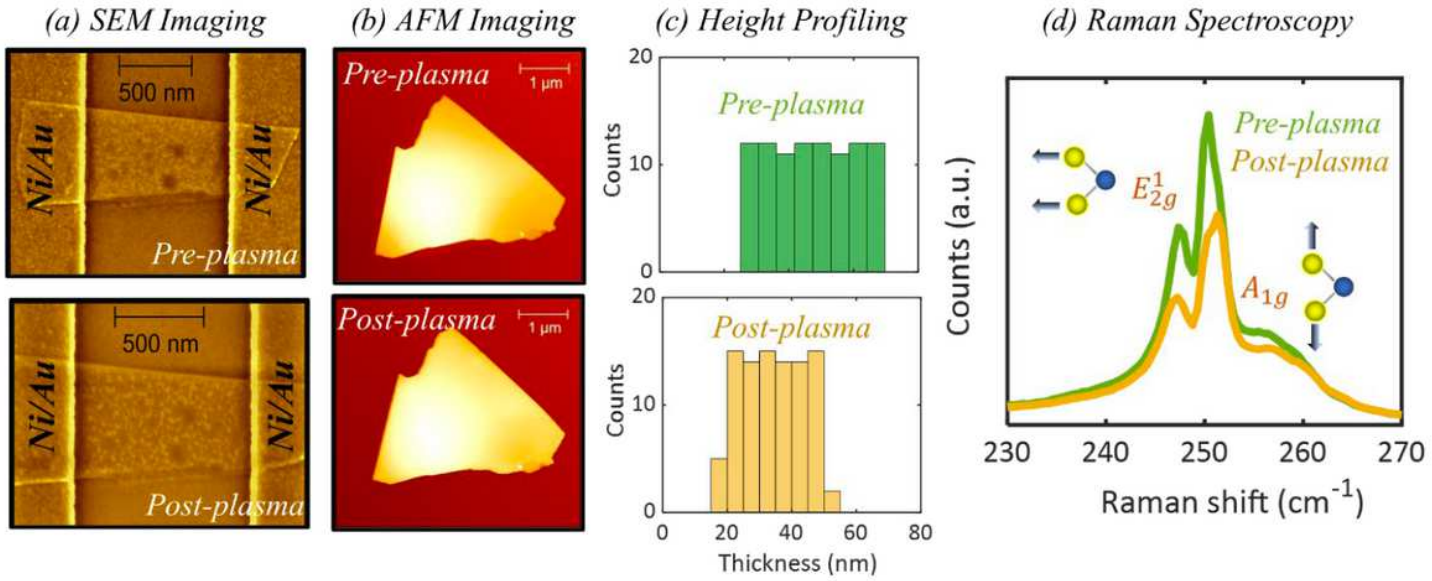

Figure 8

Optical decamouflaging solutions. a) SEM images, b) AFM images, c) AFM height histograms, and d) Raman measurements of a WSe2 based TMO/TMD hetero-stack device before and after the exposure to the oxygen plasma. In the SEM image the two channels look remarkably similar, however, on a closer look, one can observe slight alterations of the surface due to mild physical damage of the flake introduced by the plasma. While the SEM image indicates additional processing of the channel, it does not reveal any information regarding the thickness and composition of the 2D material, plasma type and exposure time, and the pattern design that determines if the device is a resistor or a diode or a transistor. The height histograms (c) show few nanometers decrease in the flake thickness following 300s of oxygen plasma exposure. However, without having any prior knowledge of the pre-plasma exposure flake thickness, the reverse engineer is unlikely to extract any meaningful information about the device functionality from the AFM image. Raman spectroscopy (d) shows small observable shift in the □□2□□1 mode, which can be attributed to the lateral oxidation of the flake and can be used for RE. While the above-mentioned characterization techniques are powerful for decamouflaging a single device, they are mostly non scalable to billions of devices on a chip. As such the RE risk will remain significantly low for TMO/TMD hetero-stack camouflaged devices and circuits.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SupplementaryInformation.pdf