A Low-Power Biomimetic Crypto Engine for All-In-One IoT based on Programmable and Multifunctional MoS₂ FETs

Akhil Dodda¹ and Saptarshi Das¹,²,³,*

¹Department of Engineering Science and Mechanics, Pennsylvania State University, University Park, PA 16802, USA
²Department of Materials Science and Engineering, Pennsylvania State University, University Park, PA 16802, USA
³Materials Research Institute, Pennsylvania State University, University Park, PA 16802, USA

Abstract: In the emerging era of internet of things (IoT), ubiquitous sensors continuously collect, consume, store, and communicate an astonishing volume of information, which are becoming increasingly vulnerable to theft and misuse. Modern software crypto systems are powerful but require extensive computational infrastructure for implementing ciphering algorithms making it difficult to be adopted by IoT edge sensors that operate with limited hardware resources and at miniscule energy budgets. Here we propose, and experimentally demonstrate a low-power, biomimetic, crypto system integrated with IoT edge sensor based on an array of atomically thin, multifunctional, and programmable MoS₂ field effect transistors (FETs). We show that the information received by a MoS₂ photodetector and encrypted by a population of MoS₂ based reconfigurable artificial neural encoders is secure from an eavesdropper with finite resources. We also show that our all-in-one IoT platform consumes miniscule energy in the range of tens to hundreds of pico Joules, has a small hardware footprint, and combines sensing, non-volatile storage, and security, for the first time.
Introduction

Information security is key for sustainable growth and development of any modern society that thrives on global connectivity in this new era of Internet of Things (IoT). Today, information is collected, stored, and communicated continuously by IoT sensors and edge devices that are found ubiquitously in our homes, workplaces, industrial manufacturing plants, transportation, health sectors, agricultural fields, and so on and so forth. However, there is an escalating threat of information loss, misuse, and manipulation owing to the involvement of untrustworthy parities [1]. While the state-of-the-art crypto systems offer powerful security solutions based on complex ciphering algorithms [2-4] that can be implemented using hardware accelerators [5], IoT edge devices have many restrictions in terms of computational capabilities due to limited hardware and energy resources. Furthermore, low-cost design needs, large-scale deployments, and heterogeneous nature of the IoT sensors limit direct adoption of traditional security solutions, including the widely used public key scheme. Due to inadequate security, IoT devices used in smart-cars, and smart-homes have shown tremendous vulnerability in the recent times [6]. Therefore, wider adoption of IoT technology can be greatly hindered if cryptosystems and security protocols which require less computational resources are not developed and integrated with the IoT edge sensor in a timely manner.

Here, we exploit a new paradigm, namely, in-memory biomimetic computing to offer an integrated sensing, storage, and security solution for IoT edge devices with minimal hardware investments and at frugal energy expenditure. Our demonstration is based on atomically thin and multifunctional MoS$_2$ field effect transistors (FETs) with a programmable gate stack that can be used as sensor, i.e. photodetector (PD), as well as various components of the proposed cryptographic engine or artificial neural encoder. The encryption is done by a finite population ($P$)
of encoders with reconfigurable encoding threshold ($V_{TH}$) using a zero mean white Gaussian noise (WGN) of finite standard deviation ($\sigma$). The decryption requires an optimum number of voting mandate ($V_M$) that is determined by $P$, $V_{TH}$, and $\sigma$ without the knowledge of which an eavesdropper requires an astronomical number of brute force trials (BFTs) for deciphering the information. In fact, the information remains concealed even if the eavesdropper has access to a trained artificial neural network (ANN). Note that our inspiration is derived from the organization of peripheral and central nervous system which employ similar cell type i.e. neurons with different functionalities that transduce external sensory information into electrical impulses and then communicate with each other as a group through successive encoding and decoding processes in the presence of a wide range of synaptic noise. To the best of our knowledge, this is the first demonstration of an all-in-one biomimetic IoT hardware platform based on multifunctional MoS$_2$ FETs that integrates sensing, non-volatile storage, and security. See Extended Data 1 for a benchmarking table summarizing earlier works based on 2D materials and memristors that combine either sensing and storage or security and storage.

Fig. 1a shows the schematic of our proposed all-in-one IoT platform. The IoT sensor collects the information, which is encrypted using an array of encoders. Each encoder comprises of a white Gaussian noise adder (WGNA) and an artificial neuron (AN). Fig. 1b shows the associated hardware based on programmable and multifunctional MoS$_2$ field effect transistor (FET) arrays, which are used as photodetectors (PDs) for sensing, and WGNA and ANs for encryption. Fig. 1c shows an example experimental demonstration of sensing and ciphering. Information, for example, an 8×8 pixelated image of the letter ‘N’ obtained by illuminating a blue light emitting diode (LED) is presented to the IoT sensor, i.e. MoS$_2$ PD. The photocurrent ($I_{PH}$) in response is superimposed
Figure 1. Hardware realization of all-in-one IoT platform based on programmable and multifunctional MoS$_2$ field effect transistor (FET) arrays. a) Schematic representation of our proposed all-in-one IoT platform that involves sensing, storage, and security. The IoT sensor collects the information, which is encrypted using an array of encoders. Each encoder comprises of a white Gaussian noise adder (WGNA) and an artificial neuron (AN). b) Associated hardware based on programmable and multifunctional MoS$_2$ FET arrays, which are used as photodetector (PD) for sensing, and WGNA and AN for encryption. c) An example experimental demonstration of sensing and ciphering. Information, for example, an 8×8 pixelated image of the letter ‘N’ obtained by illuminating a blue light emitting diode (LED) is presented to the IoT sensor, i.e. MoS$_2$ PD. The photocurrent ($I_{PH}$) in response is superimposed with zero mean white Gaussian noise (WGN) of desirable standard deviation and transduced to subthreshold presynaptic voltage ($V_{RSV}$) using MoS$_2$ WGNA and presented to MoS$_2$ ANs with pre-programmed threshold voltages. The information is revealed by a decoder through a voting process if the encoding knowledge is accessible.
with zero mean WGN of desirable standard deviation and transduced to subthreshold presynaptic voltage ($V_{PSV}$) using MoS$_2$ WGNAs and presented to MoS$_2$ ANs with pre-programmed threshold voltages. The information is revealed by a decoder through a voting process if the encoding knowledge is accessible. see **Extended Data 2** for the description of the experimental setup and measurement procedures.

The use of MoS$_2$ for our *all-in-one* IoT platform is motivated by recent studies demonstrating various low-power sensors based on MoS$_2$ that can benefit the IoT technology [7-13]. In addition, MoS$_2$ offers compatibility with flexible [14] and printable technologies [15] and shows promise for neuromorphic and biomimetic applications [16-18]. MoS$_2$ used in this study was grown epitaxially on a sapphire substrate using metal organic chemical vapor deposition (MOCVD) technique at 1000 °C and subsequently, transferred from the growth substrate to the device fabrication substrate using the PMMA-assisted wet transfer process [19]. The large area MOCVD growth allows for the fabrication of low-power and programmable monolayer MoS$_2$ FET arrays that can be used for sensing, storage, and ciphering information. See **Methods** section for further details on the synthesis, film transfer, and fabrication of MoS$_2$ FETs. Fig. 2a-b show the schematic and optical image of arrays of such MoS$_2$ FETs used for our *all-in-one* IoT platform. Fig. 2c shows the transfer characteristics, i.e. source to drain current ($I_{DS}$) as a function of the back-gate voltage ($V_{BG}$) at different drain biases ($V_{DS}$) for a representative MoS$_2$ FET with 1 μm channel length, 5 μm channel width, and a stack of 40 nm Ni/30 nm Au as the source and drain contacts. The back-gate stack for the FET comprised of atomic layer deposition (ALD) grown 50 nm Al$_2$O$_3$ on Pt/TiN/p$^{++}$-Si. As we will discuss next, this gate stack allows realization of analog, non-volatile, and programmable memory states in MoS$_2$ FETs, which is the key towards the realization of crypto
engine for IoT security. In addition, the use of thin and high-k gate oxide such as Al₂O₃ compared to conventional 300 nm of SiO₂ facilitates better electrostatic control of the MoS₂ channel and allows operation below 5 V, which is critical for achieving low-power IoT platform. As seen in Fig. 2c MoS₂ FET is a unipolar, and n-type thresholding device with $V_{TH} = 0.8$ V, extracted for $I_{DS} = 10$ pA/µm, which is 10 times higher than the average noise floor, i.e. 1 pA/µm. In other words the device is considered to be ON if $I_{DS} \geq 10$ pA/µm. The device also exhibits excellent ON/OFF current ratio of $\sim 10^7$ and subthreshold slope (SS) of less than 225 mV/decade. The electron field effect mobility ($\mu_{FE}$) value extracted from the peak transconductance was found to be $\sim 10$ cm²/V-s. Fig. 2d shows the output characteristics of the MoS₂ FET, i.e. $I_{DS}$ versus $V_{DS}$ for different $V_{BG}$. Relatively high ON current of $\sim 37$ µA/µm at $V_{DS} = 5$ V for an inversion charge carrier density of $\sim 6.2 \times 10^{12}$/cm² confirms high quality of our MOCVD grown monolayer MoS₂. Note that while our mobility and ON current values are on par with the state-of-the-art literature on large area grown MoS₂, these do not play a significant role in our proposed IoT platform as we will exploit subthreshold device operation to achieve energy efficiency.

Next, we demonstrate the capability of programming our monolayer MoS₂ FETs in any desirable conductance state with non-volatile retention characteristics. The results are shown in Fig. 2e-h. When “Write” programming pulses of different amplitudes, $V_p$, are applied to the back-gate electrode, each for a total duration of $t_p = 1$ s, the transfer characteristics of the device shifts towards the right as illustrated in Fig. 2e. During programming, the source and drain terminals were grounded. Fig. 2f shows the extracted iso-current ($\sim 10$ pA) threshold voltages, $V_{TH}$, corresponding to each state measured multiple times, post-programming, to ensure non-volatile retention. Similar observations are made when “Write” programming pulses of same amplitude,
$V_p = 10\ V$, but different $t_p$, are applied to the back-gate electrode as shown in Fig. 2g. Fig. 2h shows the corresponding non-volatile shift in $V_{TH}$. The shift in $V_{TH}$ can be attributed to our back-gate stack that closely resembles floating gate (FG) configuration used in non-volatile flash memory [20]. See Extended Data 3 explaining the memory operation using energy band diagrams.

In short, the $p^{++}$-Si/TiN/Pt interface in the stack is characterized by a Schottky barrier (SB), whereas, the gate dielectric, i.e. 50 nm Al$_2$O$_3$, acts as an oxide barrier (OB). The OB is much wider and taller compared to the SB. When a large positive back-gate voltage, $V_{BG} = V_p$, i.e. “Write” pulse is applied to the control gate (CG), i.e. $p^{++}$-Si, carriers tunnel from the $p^{++}$-Si into the Pt/TiN floating gate (FG) and remains trapped even when the $V_p$ is released. These negative fixed charges on the FG screen the electric field from CG and thereby makes the $V_{TH}$ more positive. The total amount of charge injected into the FG, and hence shift in $V_{TH}$ of the MoS$_2$ FET can be controlled by the amplitude, and duration, of the “Write” programming pulse as shown in Fig. 2e and 2g, respectively. Note that once programmed, the devices continue to remain in the programmed state as evident from the retention measurements displayed in Fig. 2f and 2h. This is critical for non-volatile memory operation. Furthermore, the device can be programmed in any desired state indicative of analog memory operation, which we will exploit later for the realization of look-up-table based Gaussian random number generator for the ciphering operation. It is also possible to restore the device from any programmed state to its initial state by applying negative voltage pulses of certain magnitude and duration (see Extended Data 4 for preset, set, and reset of a representative MoS$_2$ FET). It is also important to mention here that although our back-gate stack is global, programming and erase operations can be performed on individual MoS$_2$ FETs without impacting the adjacent devices (see Extended Data 5). Finally, the “Write” energy ($E_W$) was found to be in the range of 500 -1000 fJ calculated based on $E_W = \frac{1}{2} C_v V_p^2$.
Figure 2. MoS 2 FET for compute, storage, and sensing. a) Schematic of MoS 2 FET with programable back-gate stack comprised of atomic layer deposition (ALD) grown 50 nm Al2O3 on Pt/TiN/p++-Si. b) Optical image of arrays of MoS 2 FETs used for our all-in-one IoT platform. c) Transfer characteristics, i.e. source to drain current ($I_{DS}$) versus back-gate voltage ($V_{BG}$) at different drain biases ($V_{DS}$) for a representative MoS 2 FET with 1 μm channel length ($L$), 5 μm channel width ($W$), and a stack of 40 nm Ni/30 nm Au as the source and drain contacts. d) Output characteristics of the MoS 2 FET, i.e. $I_{DS}$ versus $V_{DS}$ for different $V_{BG}$. e) Shift in transfer characteristics of MoS 2 FET when “Write” programming pulses of different amplitudes, $V_p$, are applied to the back-gate electrode, each for a total duration of $t_p = 1$ s. f) Extracted iso-current (~10 pA) threshold voltages, $V_{TH}$, corresponding to each state in (e) measured multiple times, post-programming to demonstrate non-volatile retention. g) Shift in transfer characteristics of MoS 2 FET when “Write” programming pulses of same amplitude, $V_p = 10$ V, but different $t_p$, are applied to the back-gate electrode. g) Corresponding non-volatile shift in $V_{TH}$. The device can be programmed to any desired conductance state indicative of analog memory operation. i) Transfer characteristics of MoS 2 FET in dark and under the illumination of a blue LED, placed at ~ 1 cm distance. The device shows reasonable photoresponse and hence can be used as a photodetector (PD). j) Photoresponse ($I_{PH}$) of the device, measured at $V_{BG} = 1.5$ V to different input stimulus, i.e. 8×8 pixelated images of the letters, ‘L’, ‘M’, ‘N’, and ‘P’, obtained through the LED illumination. Each pixel corresponds to 1 ms LED illumination. k) Corresponding photocurrent maps demonstrate that the MoS 2 PD can accurately translate optical information into electrical response. Note that the MoS 2 PD was biased in the subthreshold regime to enable exponential reduction in the dark current (~1 pA) and thereby making $I_{PH} = I_{DS}$ under illumination. This also allows ultra-low-power photodetection with energy expenditure in the range $E_{PD}$ ~25-30 pJ/pixel, averaged over all pixels.
Next, we demonstrate the photosensing capability of monolayer MoS$_2$ FET. Fig. 2i shows the transfer characteristics of a representative MoS$_2$ FET in dark and under the illumination of a blue LED, which is placed at ~ 1 cm distance operating at its maximum rated brightness (5 V). Clearly, the device shows reasonable photoresponse and hence can be used as a photodetector (PD). Note that unlike most studies that use LASER excitation to evaluate the photoresponse of MoS$_2$ FETs, we have used LED as the optical source to resemble more realistic lighting ambience where most IoT sensors will be deployed. The phototransduction mechanism in MoS$_2$ PD is extensively studied in the literature including our previous reports and can be ascribed to a combination of photocarrier generation in the MoS$_2$ channel as well as photogating effect arising due to charge trapping/detrapping at the MoS$_2$/gate-dielectric interface [21]. Fig. 2j shows the photoresponse ($I_{PH}$) of the device, measured at $V_{BG} = 1.5$ V to different input stimulus, i.e. 8×8 pixelated images of the letters, ‘L’, ‘M’, ‘N’, and ‘P’, obtained through the LED illumination. Each pixel corresponds to $t_L = 1$ ms LED illumination. The corresponding photocurrent maps in Fig. 2k demonstrate that the MoS$_2$ PD is able to accurately transcribe the optical information into electrical response. Note that the MoS$_2$ PD was biased in the subthreshold regime to enable exponential reduction in the dark current (~ 1 pA) and thereby making $I_{PH} = I_{DS}$ under illumination. This also allows ultra-low-power photodetection with energy expenditure in the range $E_{PD} \sim$25-30 fJ/pixel, averaged over all pixels.

Fig. 3 shows the implementation of the biomimetic crypto engine or artificial neural encoder based on programmable MoS$_2$ FETs. Fig. 3a show the circuit diagram for the MoS$_2$ WGNA, which comprises of a current adder (CA) and a look-up-table based white Gaussian Noise (WGN) generator. The CA adds white Gaussian noise ($I_{NOISE}$) obtained from the WGN generator to the
photocurrent ($I_{PH}$) obtained from the MoS$_2$ PD using a simple resistor network and convert it to presynaptic voltage ($V_{PSV}$) to be applied to the MoS$_2$ AN. The WGN generator is an array of $M = 64$ MoS$_2$ FETs with preprogrammed threshold voltages such that their conductance values ($G_M$) follow random Gaussian distribution. Fig. 3b shows the transfer characteristics of MoS$_2$ FETs corresponding to a representative WGN generator. Fig. 3c shows the histogram of output current values ($I_M = G_M V_{DS}$) read at $V_{BG} = 0$ V with $V_{DS} = \pm 1$ V that constitute the $I_{NOISE} = [I_1 I_2 I_3 \ldots I_M]$. Clearly, $I_{NOISE}$ follow a zero mean Gaussian distribution with a standard deviation of $\sigma_I = 50$ pA/µm. Note that different arrays can be preprogrammed to obtain $I_{NOISE}$ with different $\sigma_I$. While it can be argued that on-chip WGN generators are more desirable solutions, these are often power hungry, pose integration challenges, and mostly lack reconfiguration capabilities based on application needs. Instead, our in-memory look-up-table based WGN is reconfigurable and inherently energy efficient since during the field operation the noise current is simply read from the memory. Although our approach adds area overhead and utilizes storage resources, it integrates well with our *all-in-one* IoT platform. Fig. 3d shows the transduction of the photocurrent map for the letter ‘N’ to $V_{PSV}$ for different noise standard deviation ($\sigma_V$). Note that the resistive network used by the CA allows linear transformation of the noise current into noise voltage with $\sigma_V = R_L \sigma_I$. Fig. 3e shows the corresponding $V_{PSV}$ maps. The average energy expenditure for the transduction of $I_{PH}$ to $V_{PSV}$ was found to be in the range of $E_T = 160$ fJ/pixel, which includes the read energy consumed by the in-memory WGN generator, calculated using Eq. 1.

$$E_T = \sum_{i=1}^{M} [(I_{PH} + I_{NOISE})V_{PSV} + I_{NOISE}V_{DS}]t_L$$  \[1\]

*Extended Data 6* shows the schematic and transfer characteristics of the MoS$_2$ FET used as AN mimicking biological neurons with pre-synaptic voltage ($V_{PSV}$) applied to the back-gate terminal.
Figure 3. Programmable MoS$_2$ FET based biomimetic cryptography engine for IoT security. 

a) Circuit diagram for the MoS$_2$ FET based white Gaussian noise adder (WGNA) comprising of a current adder (CA) and a look-up-table based white Gaussian Noise (WGN) generator. The WGN generator is an array of $M = 64$ MoS$_2$ FETs with preprogrammed threshold voltages such that their conductance values ($G_N$) follow random Gaussian distribution. 

b) Transfer characteristics of array elements of a representative WGN generator and c) corresponding histogram of output current values ($I_{NOISE}$) read at $V_{BG} = 0$ V with $V_{DS} = \pm 1$ V constituting the $I_{NOISE} = [I_1, I_2, I_3, \ldots, I_M]$. 

$I_{NOISE}$ follows a zero mean Gaussian distribution with standard deviation of $\sigma_N = 50$ pA/µm. Note that different arrays can be preprogrammed to obtain $I_{NOISE}$ with different $\sigma_N$. The CA adds WGN to the photocurrent and converts it into presynaptic voltage ($V_{PP}$) to be applied to the MoS$_2$ based artificial neuron (AN). Since we use resistive network, the noise current transforms into noise voltage with standard deviation, $\sigma_P = R_L \sigma_N$. 

d) $V_{PP}$ and e) corresponding color map for the letter 'N' after the transduction process using MoS$_2$ WGNA for different $\sigma_P$. 

f) Corresponding post-synaptic current ($I_{PSC}$) and g) $I_{PSC}$ map obtained from MoS$_2$ AN with a preprogrammed threshold voltage of $V_{TH} = 1.5$ V. Note that, for $V_{PP} < V_{TH}$ the MoS$_2$ AN does not invoke any observable current response as in the case of low $\sigma_P$. For higher $\sigma_P$, there are more threshold crossing events resulting in more brighter pixels in the 8×8 encrypted image of the letter ‘N’.
and post-synaptic current ($I_{PSC}$) measured at the drain terminal with a drain bias, $V_{DS} = 1 \text{ V}$. The encoding threshold was programmed to be $V_{TH} = 1.5 \text{ V}$, such that the presynaptic voltage pulses ($V_{PSV}$) obtained from the MoS$_2$ WGNA (Fig. 3d) are primarily subthreshold with occasional threshold crossing events due to the addition of the WGN. Note that, for $V_{PSV} < V_{TH}$ the MoS$_2$ AN does not invoke any observable current response greater than the noise floor of the measurement ($\sim 1 \text{ pA}/\mu\text{m}$). Fig. 3f and Fig. 3g, respectively, show the $I_{PSC}$ and the corresponding map for different $\sigma_V$ for the letter ‘N’. As evident, for lower $\sigma_V$, there are none to limited threshold crossing events resulting in sporadic bright pixels in the 8×8 encrypted image of the letter ‘N’, whereas, for higher $\sigma$ values, there are more frequent threshold crossing events resulting in greater number of bright pixels in the 8×8 encrypted image of the letter ‘N’. Nevertheless, the $I_{PSC}$ map constitute the encoded information for the letter ‘N’.

Next, to analyze the strength of the encryption process, we define true positive (TP) as an event when a bright pixel in the encoded image corresponds to a bright pixel in the original image, and false positive (FP) as an event when a bright pixel in the encoded image corresponds to a dark pixel in the original image. The likelihood of identifying the letter ‘N’ by an eavesdropper from the encrypted image will, therefore, be determined by the detectivity (D), which is defined as $D = p_{TP} - p_{FP}$, where $p_{TP}$ is the probability of TP, and $p_{FP}$ is the probability of FP. Colormaps in Fig. 4a-c, respectively, show $p_{TP}$, $p_{FP}$, and $D$ as a function of $\sigma_V$ obtained by repeating the experiments with a population of $P = 50$ encoders and Fig. 4d shows the corresponding population means. Note that the population mean for $D$ exhibits a non-monotonic behavior. At low noise level, there is hardly any FP, i.e. low $p_{FP}$, but the likelihood of detecting the letter ‘N’ remains low due to limited threshold crossing events for the original bright pixels, i.e. low $p_{TP}$. At high noise level, both bright
and dark pixels corresponding to the original image cross the spiking threshold resulting in high $p_{TP}$, and $p_{FP}$, and, therefore, low $D$. However, at an intermediate noise, the detectivity reaches its maximum value. Fig. 4e shows the number of brute force trials (BFTs) by the eavesdropper, necessary to identify the letter ‘N’ as a function of $\sigma_V$. Note that we computed $\text{BFT} = \frac{1}{D} \cdot S$, where $S = 8 \times 8 = 64$ is the size of the image. The number of BFTs are found to be astronomical irrespective of $\sigma_V$. Furthermore, the number of BFTs increases exponentially with $S$ (see Extended Data 7). Therefore, the encryption can be considered to be secure from an eavesdropper with finite resources. Fig. 4f shows the average energy expenditure by a MoS$_2$ AN for the encryption of the letter ‘N” as a function of $\sigma_V$. Note that the energy expenditure is less than 10 pJ/pixel even for the highest $\sigma_V$.

The encryption strength is also tested assuming that the eavesdropper has access to a trained artificial neural network (ANN) and the information being communicated are encrypted MNIST data set for digit classification. Fig. 4g shows a fully connected two-layered ANN with 100 neurons in the hidden layer and 10 neurons in the output layer. The 10 output neurons correspond to digits from 0 to 9. MNIST images (28×28 pixels) are flattened to obtain corresponding 784×1 vectors, which are fed to the input layer. Gradient decent algorithm is used to train the ANN using 60,000 images with a learning rate of 0.001 and rectified linear unit (ReLU) as the activation function to ensure high convergence accuracy of 90.6% beyond 300 epochs. Following this, a testing accuracy of 92.2% was achieved using the remaining 10,000 images. Note that higher training and testing accuracies can be achieved by optimizing the network, which is not the primary focus of this work. Next, we added white Gaussian noise to 10,000 MNIST images and binarized them at a threshold of 1.5 mimicking our MoS$_2$ based artificial neural encoder. Fig. 4h shows some example of
Figure 4. Strength of biomimetic encryption. Colormaps of likelihood or probability of (a) true positive ($p_{TP}$), (b) false positive ($p_{FP}$), and (c) detectivity ($D = p_{TP} - p_{FP}$) as a function of $\sigma_y$ for $P = 50$ encoders. (d) Corresponding population means. True positive (TP) is an event when a bright pixel in the encoded image corresponds to a bright pixel in the original image, and false positive (FP) is an event when a bright pixel in the encoded image corresponds to a dark pixel in the original image. At low noise level, there is hardly any FP, i.e. low $p_{FP}$, but the likelihood of detecting the letter ‘N’ remains low due to limited threshold crossing events for the original bright pixels, i.e. low $p_{TP}$. At high noise level, both bright and dark pixels corresponding to the original image cross the encoder threshold resulting in high $p_{TP}$ and $p_{FP}$, and, therefore, low $D$. However, at an intermediate noise, the detectivity reaches its maximum value. Note that the population mean for $D$ exhibits a non-monotonic trend. e) The number of brute force trials (BFTs) by the eavesdropper, necessary to identify the letter ‘N’ as a function of $\sigma_y$. Note that $BFT = 1/D^2$, where, $S = 8 \times 8 = 64$, is the size of the image. The number of BFTs are found to be astronomical irrespective of the amount of noise. f) The average energy expenditure for the encryption process as a function of $\sigma_y$. g) A fully connected artificial neural network (ANN) with 100 neurons in the hidden layer and 10 neurons in the output layer, trained using gradient decent algorithm with learning rate of 0.001 to recognize MNIST data set for digit classification. Rectified linear unit is used as the activation function. The training and testing sets consisted of 60,000 and 10,000 images, respectively. High convergence accuracy of 90.6% and inference accuracy of 92.2% is achieved. h) Representative MNIST images with white Gaussian noise (WGN) of different standard deviation ($\sigma$) binarized at a threshold of 1.5 mimicking our MoS$_2$ based artificial neural encoder. i) Average inference accuracy for 10,000 encrypted images as a function of $\sigma$. A non-monotonic trend is seen. However, irrespective of $\sigma$, the inference accuracy remains low indicating the robustness of our biomimetic encryption to trained ANNs.
encoded MNIST images for different standard deviation ($\sigma$) of the WGN. Fig. 4i shows the inference accuracy for the encrypted images as a function of $\sigma$, which follows a non-monotonic behavior. Interestingly, the accuracy values are found to be significantly low irrespective of $\sigma$, indicating the robustness of our proposed encryption scheme to trained ANNs.

In order to retrieve the information, we adopt population voting-based algorithm. We assume that the encoded images of the letter ‘N’ are transmitted over different communication channels by $P$ encoders. The receiver at the other end receives $P$ encoded images and counts the number votes corresponding to each pixel. Fig. 5a shows the vote counts for each pixel when $P = 50$ for different $\sigma_v$. A vote is registered when the encoded pixel is bright, i.e. $I_{PSC} > 10$ pA. The vote is considered to be a true positive vote (TPV) if the corresponding pixel in the original image is also bright, whereas the vote is considered to be a false positive vote (FPV) if the corresponding pixel in the original image is dark. Fig. 5b and 5c, respectively, show the probability distribution for TPVs ($p_{TPV}$) and FPVs ($p_{FPV}$) for $P = 50$ for different $\sigma_v$. At low noise levels, the probability of crossing the encoding threshold ($V_{TH}$) is low and hence only a few encoders fire simultaneously resulting in lower expected number of encoders for TPV, i.e. $\langle N_{TPV} \rangle = \sum_{n=1}^{P} np_{TPV}(n)$. The expected number of encoders for FPV, i.e. $\langle N_{FPV} \rangle = \sum_{n=1}^{P} np_{FPV}(n)$, is even lower. Similarly, at high noise level, the probability of crossing the threshold of the encoder is high and hence more encoders fire synchronously resulting in larger $\langle N_{TPV} \rangle$ and $\langle N_{FPV} \rangle$. However, as seen in Fig. 5b-c for any $\sigma_v$, $\langle N_{TPV} \rangle$ is higher than $\langle N_{FPV} \rangle$. Extended Data 8 shows the decoding of the images of the letter ‘N’ for different $\sigma_v$ for different number of mandated votes ($M_v$) to mark a pixel as bright for $P = 50$. Fig. 5d shows the corresponding colormap of correlation coefficient (CC) between the original and the decrypted image as a function of $\sigma_v$ and $M_v$. Note that for a given $\sigma_v$, there is an
Figure 5. Voting-based decryption of encrypted information. a) Number of votes corresponding to each pixel of the encoded images of the letter ‘N’ received from $P = 50$ encoders for different $\sigma_v$. A vote is registered when the encoded pixel is bright, i.e., $I_{DSC} > 10$ pA. The vote is a true positive vote (TPV) if the corresponding pixel in the original image is also bright, whereas the vote is a false positive vote (FPV) if the corresponding pixel in the original image is dark. Probability distribution for b) TPVs ($p_{TPV}$) and c) FPVs ($p_{FPV}$) corresponding to (a). Insets show the expected number of TPV, i.e., $\langle N_{TPV} \rangle = \sum_{n=1}^{P} n p_{TPV}(n)$, and FPV, i.e., $\langle N_{FPV} \rangle = \sum_{n=1}^{P} n p_{FPV}(n)$. d) The colormap of correlation coefficient (CC) between the original and the decrypted images of the letter ‘N’ as a function of $\sigma_v$ and $M_v$, when encryption is done by $P = 50$ encoder with encoding threshold of $V_{TH} = 1.5$ V. Here, $M_v$ is the minimum number of votes required to mark a pixel as bright. Note that for a given $\sigma_v$, there is an optimum $M_v$, that allows accurate decryption of the encoded image, i.e., CC = 1. e) The colormap of CC between the original and the decrypted image of the letter ‘N’ as a function of $V_{TH}$ and $M_v$ for $\sigma_v = 0.8$ V and $P = 50$. Note that without prior knowledge of $\sigma_v$, $P$, and $V_{TH}$ it is difficult to determine $M_v$ and hence decode the information.
optimum $M_V$, that allows accurate decryption of the encoded image, i.e. $CC = 1$. *Extended Data 9* shows similar results for CC when different encoding population sizes ($P$) are used. As expected, the optimum number of $M_V$ for accurate decryption is found to be different for similar $\sigma_V$. Therefore, without the prior knowledge of the $\sigma_V$ and $P$, used by the biomimetic encoder it is difficult to decode the information. The strength of encoding can be further enhanced by exploiting the programming capability of our MoS$_2$ based ANs. Here we reconfigure the encoding threshold ($V_{TH}$) similar to neuroplasticity in biological neurons allowing adaptation to changing environment and stimuli. *Extended Data 10* shows the encryption of the letter ‘N’, by encoders with different $V_{TH}$, for different $\sigma_V$. As obvious if $V_{PSV} > V_{TH}$, the encryption process is pointless or in other word the communication is insecure. For $V_{TH}$ values slightly greater than $V_{PSV}$, there are more threshold crossing events even for low $\sigma_V$, whereas, for $V_{TH}$ values further from $V_{PSV}$, there are limited threshold crossing events even for high $\sigma_V$. Fig. 5e shows the colormap of CC between the original and the decrypted image of the letter ‘N’ as a function of $V_{TH}$ and $M_V$ for $\sigma_V = 0.8$ V and $P = 50$ (see *Extended Data 11* for similar results with different $\sigma_V$). Clearly, the optimum $M_V$ for accurate decryption is found to be different for different $V_{TH}$. Therefore, not only $\sigma_V$ and $P$, but also prior knowledge of $V_{TH}$ is required for decoding the information, which makes the system more robust from the eavesdropper.

Conclusion

In conclusion, we have experimentally demonstrated an *all-in-one* hardware IoT platform based on programmable and multifunctional MoS$_2$ FETs, which is capable of sensing, storing, and securing information. Since a single material and similar device structures are used the hardware footprint is minimal, $\sim 5 \mu m \times 2 \mu m$ for each photodetector, $\sim 5 \mu m \times 3 \mu m$ for each CA, $5 \mu m \times$
64 µm for each WGN generator, and ~5 µm X 2 µm for each AN. The energy expenditure is also miniscule, in the range of few tens to hundreds of pico Joules, as we have primarily exploited subthreshold FET operation. Furthermore, analog, and non-volatile memory capability allows reconfiguration of the IoT platform based on application needs. Finally, the biomimetic IoT platform is shown to be secure.
Methods

Film Growth: Monolayer MoS$_2$ was deposited on epi-ready 2” c-sapphire substrate by metalorganic chemical vapor deposition (MOCVD). An inductively heated graphite susceptor equipped with wafer rotation in a cold-wall horizontal reactor was used to achieve uniform monolayer deposition as previously described [22]. Molybdenum hexacarbonyl (Mo(CO)$_6$) and hydrogen sulfide (H$_2$S) were used as precursors. Mo(CO)$_6$ maintained at 10°C and 950 Torr in a stainless-steel bubbler was used to deliver 0.036 sccm of the metal precursor for the growth, while 400 sccm of H$_2$S was used for the process. MoS$_2$ deposition was carried out at 1000°C and 50 Torr in H$_2$ ambient, where monolayer growth was achieved in 18 min. The substrate was first heated to 1000°C in H$_2$ and maintained for 10 min before the growth was initiated. After growth, the substrate was cooled in H$_2$S to 300°C to inhibit decomposition of the MoS$_2$ films.

Film Transfer: After the growth of monolayer MoS$_2$ on sapphire substrate, the film is then transferred onto the FET gate dielectric substrate by wet transfer technique. Polymethylmethacrylate (A3 PMMA) resist is spin coated onto the growth substrates encapsulating the MoS$_2$ and then immersed into the 1M NaOH solution kept at 90°C. Capillary action draws the NaOH solution to the PMMA/substrate interface, separating the hydrophobic PMMA/MoS$_2$ from the sapphire substrate. The detached film floats on the surface, which is then rinsed for multiple times in deionized water and is finally transferred on to the Alumina/ Pt/TiN/p$^{++}$ Si gate dielectric stack[23].

Fabrication of monolayer MoS$_2$ FET: We have fabricated the back-gated field effect transistors on a 50nm alumina (Al$_2$O$_3$) acting as a gate oxide and a stack of Pt/TiN/p$^{++}$ Si as a back-gate
electrode. First, MOCVD grown MoS$_2$ are transferred onto the alumina sample, then the sample is spin coated with A6 PMMA and followed by electron-beam (e-beam) lithography to specify the channels and then separating them out by sulfur hexafluoride (SF$_6$) etch under 5 degree centigrade for 30s. After etch step, sample is rinsed in Acetone for 30 min followed by 2-propanol (IPA). To define the source and drain contacts, sample is then spin coated with methyl methacrylate (MMA) followed by A3 PMMA. Then using electron-beam lithography source and drain contacts are patterned and further developed by using 1:1 mixture of 4-methyl -2-pentanone (MIBK) and 2 propanol for 60s. 40nm of Nickel (Ni) and 30 nm of Gold (Au) are deposited/ evaporated on to the patterns using E-beam evaporation. Lift- off the evaporated materials is done by immersing the sample in Acetone for 30 min followed by 2-propanol (IPA).

*Electrical Characterization:* Electrical characterization of the fabricated devices are performed using Lake Shore CRX-VF probe station under atmospheric condition using a Keysight B1500A 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


AUTHOR INFORMATION

Corresponding Author

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

Author Contributions

S.D conceived the idea and designed the experiments. S.D, and A.D performed the experiments, 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

The work was partially supported by Army Research Office (ARO) through Contract Number W911NF1920338.
Figure Captions

Figure 1. Hardware realization of all-in-one IoT platform based on programmable and multifunctional MoS2 field effect transistor (FET) arrays. a) Schematic representation of our proposed all-in-one IoT platform that involves sensing, storage, and security. The IoT sensor collects the information, which is encrypted using an array of encoders. Each encoder comprises of a white Gaussian noise adder (WGNA) and an artificial neuron (AN). b) Associated hardware based on programmable and multifunctional MoS2 FET arrays, which are used as photodetector (PD) for sensing, and WGNA and AN for encryption. c) An example experimental demonstration of sensing and ciphering. Information, for example, an 8×8 pixelated image of the letter ‘N’ obtained by illuminating a blue light emitting diode (LED) is presented to the IoT sensor, i.e. MoS2 PD. The photocurrent ($I_{PH}$) in response is superimposed with zero mean white Gaussian noise (WGN) of desirable standard deviation and transduced to subthreshold presynaptic voltage ($I_{PSV}$) using MoS2 WGNAs and presented to MoS2 ANs with pre-programmed threshold voltages. The information is revealed by a decoder through a voting process if the encoding knowledge is accessible.

Figure 2. MoS2 FET for compute, storage, and sensing. a) Schematic of MoS2 FET with programable back-gate stack comprised of atomic layer deposition (ALD) grown 50 nm Al2O3 on Pt/TiN/p++-Si. b) Optical image of arrays of MoS2 FETs used for our all-in-one IoT platform. c) Transfer characteristics, i.e. source to drain current ($I_{DS}$) versus back-gate voltage ($V_{BG}$) at different drain biases ($V_{DS}$) for a representative MoS2 FET with 1 μm channel length ($L$), 5 μm channel width ($W$), and a stack of 40 nm Ni/30 nm Au as the source and drain contacts. d) Output characteristics of the MoS2 FET, i.e. $I_{DS}$ versus $V_{DS}$ for different $V_{BG}$. e) Shift in transfer...
characteristics of MoS2 FET when “Write” programming pulses of different amplitudes, $V_p$, are applied to the back-gate electrode, each for a total duration of $t_p = 1$ s, f) Extracted iso-current ($\sim 10$ pA) threshold voltages, $V_{TH}$, corresponding to each state in (e) measured multiple times, post-programming to demonstrate non-volatile retention. e) Shift in transfer characteristics of MoS2 FET when “Write” programming pulses of same amplitude, $V_p = 10$ V, but different $t_p$, are applied to the back-gate electrode. g) Corresponding non-volatile shift in $V_{TH}$. The device can be programmed to any desired conductance state indicative of analog memory operation. i) Transfer characteristics of MoS2 FET in dark and under the illumination of a blue LED, placed at $\sim 1$ cm distance. The device shows reasonable photoresponse and hence can be used as a photodetector (PD). j) Photoresponse ($I_{PH}$) of the device, measured at $V_{BG} = 1.5$ V to different input stimulus, i.e. 8×8 pixelated images of the letters, ‘L’, ‘M’, ‘N’, and ‘P’, obtained through the LED illumination. Each pixel corresponds to 1 ms LED illumination. k) Corresponding photocurrent maps demonstrate that the MoS2 PD can accurately translate optical information into electrical response. Note that the MoS2 PD was biased in the subthreshold regime to enable exponential reduction in the dark current ($\sim 1$ pA) and thereby making $I_{PH} = I_{DS}$ under illumination. This also allows ultra-low-power photodetection with energy expenditure in the range $E_{PD} \sim 25-30$ pJ/pixel, averaged over all pixels.

Figure 3. Programmable MoS2 FET based biomimetic cryptography engine for IoT security. a) Circuit diagram for the MoS2 FET based white Gaussian noise adder (WGNA) comprising of a current adder (CA) and a look-up-table based white Gaussian Noise (WGN) generator. The WGN generator is an array of $M = 64$ MoS2 FETs with preprogrammed threshold voltages such that their conductance values ($G_N$) follow random Gaussian distribution. b) Transfer characteristics of array
elements of a representative WGN generator and c) corresponding histogram of output current values \((I_M = G_M V_{DS})\) read at \(V_{BG} = 0\) V with \(V_{DS} = \pm 1\) V constituting the \(I_{\text{NOISE}} = [I_1 I_2 I_3 \ldots I_M]\). \(I_{\text{NOISE}}\) follows a zero mean Gaussian distribution with standard deviation of \(\sigma_i = 50\) pA/\(\mu\)m. Note that different arrays can be preprogrammed to obtain \(I_{\text{NOISE}}\) with different \(\sigma_i\). The CA adds WGN to the photocurrent and converts it into presynaptic voltage \((V_{PSV})\) to be applied to the MoS2 based artificial neuron (AN). Since we use resistive network, the noise current transforms into noise voltage with standard deviation, \(\sigma_V = R_L \sigma_i\). d) \(V_{PSV}\) and e) corresponding color map for the letter ‘N’ after the transduction process using MoS2 WGNA for different \(\sigma_V\). f) Corresponding post-synaptic current \((I_{PSC})\) and g) \(I_{PSC}\) map obtained from MoS2 AN with a preprogrammed threshold voltage of \(V_{TH} = 1.5\) V. Note that, for \(V_{PSV} < V_{TH}\) the MoS2 AN does not invoke any observable current response as in the case of low \(\sigma_V\). For higher \(\sigma_V\), there are more threshold crossing events resulting in more brighter pixels in the 8×8 encrypted image of the letter ‘N’.

**Figure 4. Strength of biomimetic encryption.** Colormaps of likelihood or probability of (a) true positive \((p_{TP})\), (b) false positive \((p_{FP})\), and (c) detectivity \((D = p_{TP} - p_{FP})\) as a function of \(\sigma_V\) for \(P = 50\) encoders. (d) Corresponding population means. True positive (TP) is an event when a bright pixel in the encoded image corresponds to a bright pixel in the original image, and false positive (FP) is an event when a bright pixel in the encoded image corresponds to a dark pixel in the original image. At low noise level, there is hardly any FP, i.e. low \(p_{FP}\), but the likelihood of detecting the letter ‘N’ remains low due to limited threshold crossing events for the original bright pixels, i.e. low \(p_{TP}\). At high noise level, both bright and dark pixels corresponding to the original image cross the encoder threshold resulting in high \(p_{TP}\), and \(p_{FP}\), and, therefore, low \(D\). However, at an intermediate noise, the detectivity reaches its maximum value. Note that the population mean
for $D$ exhibits a non-monotonic trend. e) The number of brute force trials (BFTs) by the eavesdropper, necessary to identify the letter ‘N’ as a function of $\sigma_V$. Note that $\text{BFT} = 1/D^5$, where, $S = 8\times8 = 64$, is the size of the image. The number of BFTs are found to be astronomical irrespective of the amount of noise. f) The average energy expenditure for the encryption process as a function of $\sigma_V$. g) A fully connected artificial neural network (ANN) with 100 neurons in the hidden layer and 10 neurons in the output layer, trained using gradient decent algorithm with learning rate of 0.001 to recognize MNIST data set for digit classification. Rectified linear unit is used as the activation function. The training and testing sets consisted of 60,000 and 10,000 images, respectively. High convergence accuracy of 90.6% and inference accuracy of 92.2% is achieved. h) Representative MNIST images with white Gaussian noise (WGN) of different standard deviation ($\sigma$) binarized at a threshold of 1.5 mimicking our MoS$_2$ based artificial neural encoder. i) Average inference accuracy for 10,000 encrypted images as a function of $\sigma$. A non-monotonic trend is seen. However, irrespective of $\sigma$, the inference accuracy remains low indicating the robustness of our biomimetic encryption to trained ANNs.

**Figure 5. Voting-based decryption of encrypted information.** a) Number of votes corresponding to each pixel of the encoded images of the letter ‘N’ received from $P = 50$ encoders for different $\sigma_V$. A vote is registered when the encoded pixel is bright, i.e. $I_{PSC} > 10$ pA. The vote is a true positive vote (TPV) if the corresponding pixel in the original image is also bright, whereas the vote is a false positive vote (FPV) if the corresponding pixel in the original image is dark. Probability distribution for b) TPVs ($p_{TPV}$) and c) FPVs ($p_{FPV}$) corresponding to (a). Insets show the expected number of TPV, i.e. $\langle N_{TPV} \rangle = \sum_{n=1}^{P} n p_{TPV}(n)$, and FPV, i.e., $\langle N_{FPV} \rangle = \sum_{n=1}^{P} n p_{FPV}(n)$. d) The colormap of correlation coefficient (CC) between the original and the
decrypted images of the letter ‘N’ as a function of $\sigma_V$ and $M_V$, when encryption is done by $P = 50$ encoder with encoding threshold of $V_{TH} = 1.5$ V. Here, $M_V$ is the minimum number of votes required to mark a pixel as bright. Note that for a given $\sigma_V$, there is an optimum $M_V$, that allows accurate decryption of the encoded image, i.e. $CC = 1$. e) The colormap of $CC$ between the original and the decrypted image of the letter ‘N’ as a function of $V_{TH}$ and $M_V$ for $\sigma_V = 0.8$ V and $P = 50$. Note that without prior knowledge of $\sigma_V$, $P$, and $V_{TH}$ it is difficult to determine $M_V$ and hence decode the information.