ACS NANO

Cite This: *ACS Nano* 2017, 11, 12772−12779

www.acsnano.org

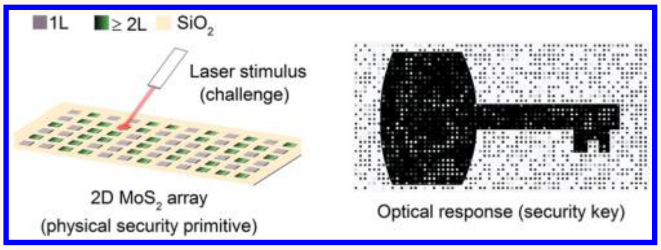
Physically Unclonable Cryptographic Primitives by Chemical Vapor Deposition of Layered MoS_2

Abdullah Alharbi, Darren Armstrong, Somayah Alharbi, and Davood Shahrjerdi*

Department of Electrical and Computer Engineering, New York University, Brooklyn, New York, New York 10003, United States

Supporting Information

ABSTRACT: **Physically unclonable cryptographic primitives are promising for securing the rapidly growing number of electronic devices. Here, we introduce physically unclonable primitives from layered molybdenum disulfide (MoS_2) by leveraging the natural randomness of their island growth during chemical vapor deposition (CVD). We synthesize a MoS_2 monolayer film covered with speckles of multilayer islands, where the growth process is engineered for an optimal speckle density. Using the Clark−Evans test, we confirm that the distribution of islands on the film exhibits complete spatial randomness, hence indicating the growth of multilayer speckles is a spatial Poisson process. Such a property is highly desirable for constructing unpredictable cryptographic primitives. The security primitive is an array of 2048 pixels fabricated from this film. The complex structure of the pixels makes the physical duplication of the array impossible (*i.e.*, physically unclonable). A unique optical response is generated by applying an optical stimulus to the structure. The basis for this unique response is the dependence of the photoemission on the number of MoS_2 layers, which by design is random throughout the film. Using a threshold value for the photoemission, we convert the optical response into binary cryptographic keys. We show that the proper selection of this threshold is crucial for maximizing combination randomness and that the optimal value of the threshold is linked directly to the growth process. This study reveals an opportunity for generating robust and versatile security primitives from layered transition metal dichalcogenides.**


1L
≥ 2L
SiO_2
Laser stimulus
(challenge)
2D MoS_2 array
(physical security primitive)
Optical response (security key)

KEYWORDS: *security, cryptographic primitives, physically unclonable, MoS_2, CVD growth*

Modern society demands information security.[1] Globalization of supply chains has undermined trust in electronic devices, which were once manufactured entirely by a single *trusted* factory. Further, the ubiquity of today's advanced manufacturing poses additional challenges, because such resources are now more accessible to adversaries for developing sophisticated security attacks. A vast number of such attacks are physical[2,3] and range from counterfeiting to unauthorized access. As a result, authentication of electronic devices and information has become increasingly important.

Physically unclonable functions (PUFs) are among promising security primitives for entity identification or cryptographic key generation.[4,5] A variety of PUFs have used manufacturing variability[6,7] or materials disorders[8−13] for generating a security key *on demand*. Specifically, applying a challenge (such as an electrical or an optical stimulus) to a PUF produces a unique response (a security key). Hence, this concept generates security keys that are unique for each electronic device. A PUF construct must be easy to produce at low cost and yet have a physical structure that is impossible to replicate, *i.e.*, physically unclonable. Notably, the uniqueness of the response and the physical unclonability are the core defining properties of a PUF.[5]

Silicon-based PUFs have garnered significant attention as a potential low-cost solution for securing digital systems, due to their compatibility with the complementary metal-oxide-semiconductor (CMOS) technology.[7] These PUFs use the intrinsic variability of the CMOS process, which follows a Gaussian distribution with a mean value close to zero.[14] Because of this attribute of standard CMOS processes, the measured output of all silicon PUFs requires extensive data processing, which aims to enhance the overall robustness and uniqueness of the PUF response.[5,6,15,16] Examples of postprocessing procedures include error correction, masking of unreliable bits, addition of helper data, and fuzzy extraction. Not only does the extensive postprocessing add to the complexity of silicon PUFs, but it might also lead to vulnerability to physical attacks.[17] Hence, there is an

Received: October 25, 2017
Accepted: November 16, 2017
Published: November 16, 2017

DOI: 10.1021/acsnano.7b07568

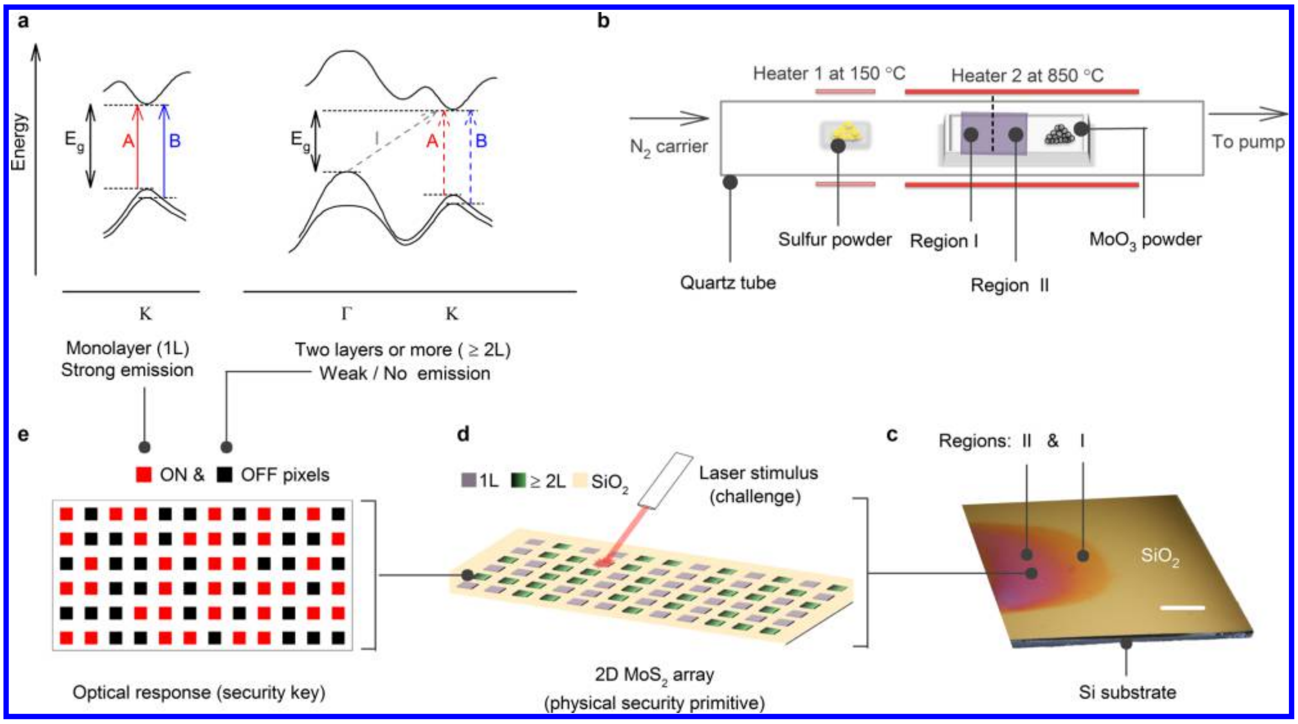


Figure 1. MoS_2-based physically unclonable security primitives: (a) Schematic illustration of the energy band structure of monolayer and multilayer MoS_2, indicating strong dependence of excitonic emission on the number of MoS_2 layers. (b) CVD using solid-phase precursors was used for synthesis of large-area MoS_2 films. (c) Photo of a CVD MoS_2 sample indicating two distinct regions of growth. Scale bar is 5 mm. (d) An array of 32 × 64 pixels was then formed in region II. (e) Stimulating the physical MoS_2 primitive with a laser light produces a unique optical response with randomly distributed ON and OFF pixels.

opportunity for realizing nonsilicon cryptographic primitives that can generate inherently more unique and robust security keys.

A large body of work has reported the natural randomness of nanomaterials,[18,19] which can potentially be leveraged for constructing nonsilicon security primitives. Optimizing the security and reliability of these primitives requires tuning the conditions of the physical process involving nanomaterials (*e.g.*, synthesis or assembly). Further, the scalability of the physical process is important for producing primitives on a large scale and thus realizing a viable nanomaterials-based security technology. A recent work of Hu *et al.* provides a meaningful experimental demonstration of this concept, implementing carbon nanotube (CNT) random bits by leveraging the randomness of a CNT assembly process.[14] Beyond CNTs, the prospects of two-dimensional (2D) transition metal dichalcogenides (TMDs) for security applications are still unexplored.

Several key advances in the field of 2D materials make this exploration worthwhile. First, many studies have reported the large-scale growth of various TMDs on amorphous substrates with apparent random nucleation.[20−23] A true island growth is known to exhibit complete spatial randomness (CSR),[24] which indicates that the occurrences of nucleations are independent and equally probable everywhere on the substrate. On the basis of these properties, the natural randomness of a true island growth offers a close approximation of true randomness. Hence, a TMD film with CSR nucleations is appealing for constructing highly unpredictable security primitives. However, until now, no study has statistically tested whether TMD island growth is CSR. The second advance relates to discovering the strong thickness dependence of photoemission from most semiconducting TMDs.[25] The illustration in Figure 1a shows this concept. Combining this unique property with the randomness of the TMD growth can result in a PUF that provides a random response to an optical stimulus. Finally, the substrate-agnostic property of these 2D materials[22,26−28] makes the resulting security primitives versatile by allowing their integration with different platforms from conventional digital systems to emerging flexible electronics.

Here, we introduce a physically unclonable security primitive constructed from layered molybdenum disulfide (MoS_2). We used MoS_2 as the model system since it has been studied heavily in the family of 2D layered TMDs.[25,29,30] Figure 1 illustrates the proposed concept. A large-area MoS_2 film is produced using a chemical vapor deposition (CVD) process in a layer-plus-island growth mode (Figure 1b). The details of all CVD growth experiments are given in Supporting Information. Figure 1c shows the photo of a CVD MoS_2 film, illustrating two distinct growth regions on the substrate. The region of interest (*i.e.*, region II) is composed of a continuous MoS_2 monolayer with speckles of multilayer (two layers or more) islands. We engineer the growth process to achieve an optimal island density in this region that aims to yield an equal probability of random zero and one bits. We confirmed CSR of the multilayer islands using the statistical test by Clark−Evans.[31] By confirming CSR, we used the Avrami equation to draw insight into the kinetics of the island growth in region II. The security primitive itself is fabricated as a 2048-pixel array from the film in this region (Figure 1d). Applying an optical (laser) stimulus to the security primitive results in random ON and OFF pixels (Figure 1e), owing to the spatial randomness of the multilayer speckles and the different photoemission strengths of monolayer and multilayer pixels. Using standard security

DOI: 10.1021/acsnano.7b07568

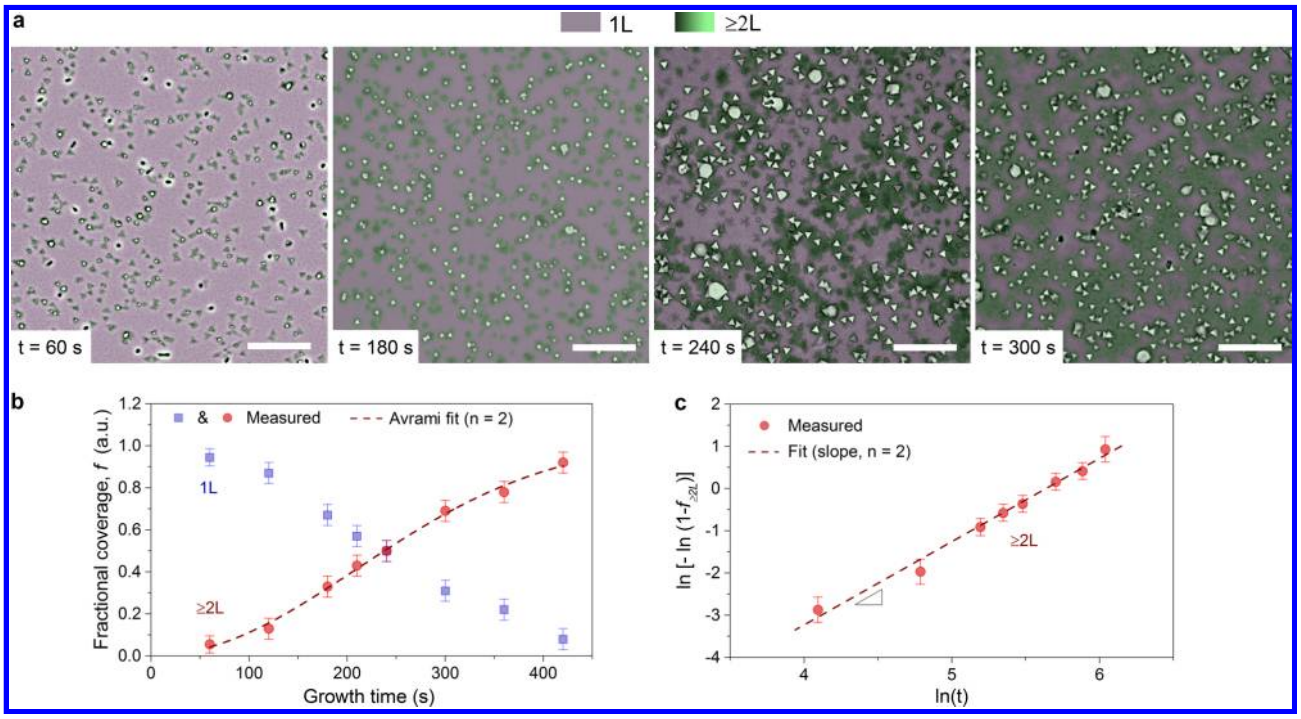


Figure 2. Analyzing the growth randomness: (a) Optical images illustrating the time evolution of the MoS_2 growth in region II, indicating the layer-plus-island growth modes. (b) Time-dependent fractional coverage of monolayer (1L) and multilayer (two or more layers ≥2L) films in region II. The Avrami equation provides a reasonable fit to the data for the fractional coverage of multilayer films, further confirming complete spatial randomness of island nucleation in region II. (c) The fit gives an Avrami exponent n of about 2, suggesting 2D disk-shaped growth governed by the surface diffusion. All scale bars are 30 μm.

tests, we confirm the randomness and stability of the security keys generated from the proposed security primitive.

RESULTS AND DISCUSSION

Layer-Plus-Island Growth of CVD MoS_2. Among the different methods used for growing TMDs, CVD techniques offer better control over thickness on a large scale.[20,32−34] We grew large-area MoS_2 films onto 285 nm SiO_2 on p^+ silicon substrates by CVD from sulfur and MoO_3 precursors.[35] Figure 1b schematically illustrates the CVD reactor based on the solid-phase precursors. Two distinct growth regions are typically evident along the substrate (see Figure 1c), indicating that in this CVD process the growth depends on the distance of the substrate from the MoO_3 powder. Region I is the farthest from the MoO_3 powder in the reactor, where the optimal growth conditions yield a continuous monolayer. Region II, located closer to the MoO_3 powder, is covered by a continuous monolayer film with randomly distributed multilayer islands. According to the surface science of thin film growth, the growth mode strongly depends on the deposition rate of the growth species and the substrate temperature.[24] It is known that the growth mode will deviate from the layer-by-layer mode to the layer-plus-island mode once the deposition rate exceeds a critical value. This explains the presence of these two prominent growth modes along the substrate.[20,24] Indeed, the layer-by-layer growth occurs in region I with low Mo vapor pressure and the growth follows a site-saturated growth kinetics (see Supporting Information). Despite the spatial randomness of the nucleation sites, region I of our samples is suboptimal for constructing a dense array of random binary code because of the relatively sparse spatial distribution of the multilayer films grown mostly at the grain boundaries (spacing from 20 to 80 μm). In contrast, region II (closer to the MoO_3 powder) is exposed to a higher concentration of Mo vapor, resulting in the layer-plus-island growth mode and thus the random nucleation of multilayer islands on the monolayer film, as shown in Figure 2a. To produce the physically unclonable security primitive, we engineer the growth process in this region to achieve an optimal surface coverage of the multilayer islands.

Engineering and Testing the Growth Randomness. Complete spatial randomness is central to constructing strong cryptographic keys in our proposed concept. To test for CSR of the island growth in region II, we apply the statistical test by Clark and Evans[31] on images from this region, taken at an early stage of the multilayer nucleation on the continuous monolayer film, *e.g.*, Figure 2a at $t = 60$ s. If the island growth is CSR, then the distribution of nearest neighbor distances (*i.e.*, the distances between the islands and their nearest neighbor) has a mean $r_{\mathrm{CSR}} = 1/(2\sqrt{\rho})$ and a variance $\sigma^2_{\mathrm{CSR}} = (4 - \pi)/(4\pi\rho)$, where ρ is the particle density per unit area. Therefore, we can test for CSR by testing the null hypothesis that the mean of nearest neighbor distances is equal to r_{CSR}. Using the two-tailed test for the population mean, we compute the standard Z-score given by

$$Z = \frac{\langle r_s \rangle - \langle r_{\mathrm{CSR}} \rangle}{\sqrt{\sigma^2_{\mathrm{CSR}}/N}} \tag{1}$$

where r_s is the sample mean of the nearest neighbor distances computed with N particles. That is,

$$r_s = \sum_{i=1}^{N} \frac{r_i}{N} \tag{2}$$

where r_i is the nearest neighbor distance of the ith island. At a 0.05 significance level, the null hypothesis is to be rejected if Z

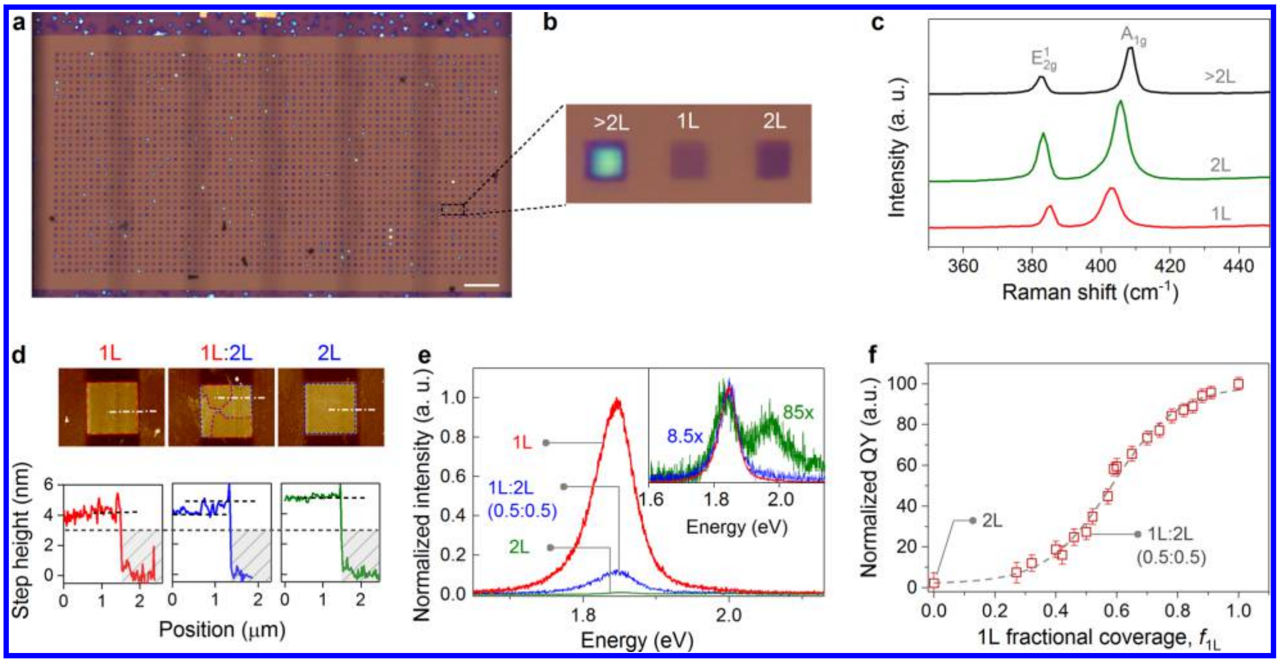


Figure 3. MoS_2 physically unclonable security primitive: (a) Optical image of a 2D array with 2048 MoS_2 pixels. (b) Zoomed-in optical image of three neighboring MoS_2 pixels with different layer thickness: monolayer (1L), bilayer (2L), and more than two layers (>2L). (c) Corresponding Raman spectra of the three pixels in (b). (d) Topographic images of three pixels covered with 1L, 2L, and mixture of 1L:2L MoS_2 and their corresponding step height profiles. The hashed gray boxes inside the step height plots indicate the depth of the SiO_2 film which was overetched during MoS_2 patterning in CF_4/O_2 plasma. (e) Corresponding PL characteristics of these pixels. (f) Using a combination of PL and AFM studies, we determined the normalized QY of several pixels with different fractional surface coverage of monolayer. The data suggests the increase of nonradiative recombinations with decreasing f_{1L}. From the data, we set the ON/OFF classification threshold based on the photoemission properties of a pixel with f_{1L} = 0.5.

≤ -1.96 or $Z \geq 1.96$. We calculated typical Z values of about 0.7−1.0 for our samples (see Supporting Information). Hence, at the 0.05-level of significance, we cannot reject the null hypothesis that the mean nearest neighbor distance is r_{CSR}. This suggests that the island growth in region II exhibits CSR, hence all nucleations are independent and the probability of nucleation is the same everywhere on the surface.

Considering CSR island growth in region II, the Avrami equation[36] can be used to draw insight into the time evolution of the island growth. For a growth time t, the fractional surface coverage f of the multilayer islands (≥2L) is approximated by

$$f_{\geq 2L}(t) = 1 - e^{-kt^n} \tag{3}$$

where the Avrami exponent n gives information about the kinetics of the island growth. To analyze the growth kinetics, we prepared several samples strictly by varying the growth times while keeping the other processing conditions identical—including the quantity of the precursors, the sample size, and the sample position relative to MoO_3. We then imaged the samples to compute the fractional areal coverage of monolayer and multilayer films in region II, as shown in Figure 2a. Assuming time-invariant growth kinetics, this experiment provides a good approximation of the time evolution of the surface coverage.[37] From the optical images, we made two key observations. First, the nucleation is continuous evident from the concurrent presence of thin (mostly bilayer) and thick islands in all different stages of the growth. Second, the growth is mostly 2D, *i.e.*, the lateral dimensions of islands grow faster than the thickness. Figure 2b summarizes the time evolution of the fractional surface coverage for the monolayer film and the multilayer islands. In this plot, t = 0 represents the time at which a monolayer film fully covers the surface in Region II. From our observations, this time corresponds to the beginning of the growth cycle at 850 °C. From the data, the multilayer islands cover 50% of the monolayer film surface at $t \approx 240$ s. In Figure 2c, we plotted $\ln[-\ln(1 - f_{\geq 2L})]$ as a function of $\ln(t)$, where the slope of the fitted line gives the estimate for the Avrami exponent n. We found $n \approx 2$ for our growth experiments, suggesting a 2D disk-shaped growth governed by the surface diffusion. Eq 3 provides a reasonable fit to the experimental data in Figure 2b, further confirming CSR of the multilayer island growth in region II. In addition, the inflection point of the fitted curve at t ≈ 180 s corresponds to the crossover from the isolated island growth to the island overlap growth.

After analyzing the growth kinetics, we adjusted the growth time to obtain MoS_2 films with equal surface areas of exposed monolayer (1L) film and of the multilayer islands, *i.e.*, $f_{1L} = f_{\geq 2L}$ = 0.5. This was done to achieve the maximum combination randomness in the security key responses.

Cryptographic Key Generation. To implement the MoS_2-based security primitives, we fabricated dense arrays consisting of 32 × 64 pixels from the film in region II (see Methods). These arrays have a pixel size of 2 μm × 2 μm and an equal pixel spacing of 2 μm. This pixel size was chosen because it is comparable with the dimensions of the state-of-the-art CMOS image sensors.[38] Figure 3a shows the optical image of a 2D MoS_2 array with 2048 pixels, fabricated on a SiO_2/Si substrate. Due to the randomness of the multilayer island growth on a continuous monolayer film, the content of each pixel is random. A pixel might consist of a monolayer, a multilayer, or a mixture of the two. Figure 3b illustrates the zoomed-in view of three neighboring pixels. These pixels

DOI: 10.1021/acsnano.7b07568
ACS Nano 2017, 11, 12772−12779

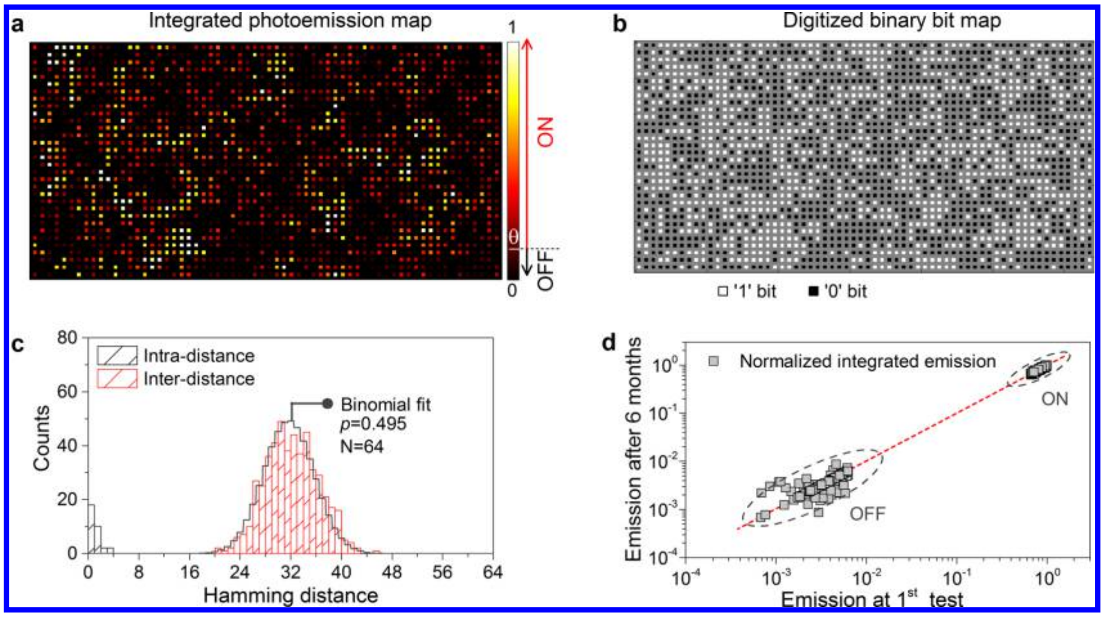


Figure 4. Optical response and security metrics of the MoS_2 primitive: (a) Stimulating the 2D MoS_2 array with a laser light produces an optical response that is unique to this primitive. (b) The photoemission spatial map was converted to a 2D binary array by comparing each pixel with the ON/OFF threshold. (c) Standard security tests confirm uniqueness and repeatability of the security keys. (d) By studying the aging properties of the photoemission for multiple MoS_2 pixels, we confirm that the MoS_2 primitives are highly stable. The red dashed line is guide to the eye and has a slope of 1.

visually look different from one another, indicating their thickness difference. The Raman fingerprint of these pixels in Figure 3c confirms the material type (which is MoS_2 here) and the corresponding thickness, determined from the distance between the peak position of the in-plane (E^1_{2g}) and the out-of-plane (A_{1g}) phonon modes.

After fabrication, the physical security primitive was stimulated using a laser light to generate an optical response. We expect the response to be unique to the security primitive given the random thickness distribution of the CVD MoS_2 and the thickness dependence of the excitonic emissions in MoS_2. Figure 3d and 3e show the topographic images and photoluminescence (PL) spectra of three pixels from the array, which comprise a full monolayer film, a full bilayer film, and a mixture of the two. The PL data illustrate the marked contrast between the full monolayer pixel and the full bilayer one. As a result, the binary (ON or OFF) classification of such pixels in the array is straightforward. In the case of a mixed pixel, however, the photoemission is expected to be a strong function of the monolayer coverage of the pixels. Considering that the growth process was tuned to obtain equal surface coverage by a continuous monolayer film and multilayer speckles, a pixel with monolayer areal coverage of 50% (see Figures 3e) represents the most ambiguous case for classifying a pixel as ON or OFF. Therefore, we use the photoemission of such a mixed pixel as the photoemission threshold θ.

The data in Figure 3e shows clearly that the ratio of the PL intensity of the mixed pixel to that of a full monolayer pixel (about 0.12) is noticeably smaller than the monolayer areal coverage of the mixed pixel (0.5). We noticed that this trend is consistent across the different arrays on the sample. To better understand this observation, we closely examined the PL spectra of multiple pixels with varying monolayer fractional surface coverage, from 0 (full bilayer) to 1 (full monolayer). We selected these pixels at random from different locations within the same array. To accurately determine the surface coverage of the monolayer film within each pixel, we performed atomic force microscopy (AFM). The corresponding AFM images and the PL spectra of these pixels are shown in Supporting Information. We calculated the total area under the PL emission curve for each pixel in the wavelength range of 580−770 nm (the integrated photoemission). Then, the integrated PL of the pixels were normalized with respect to that of a full monolayer pixel. To account for the difference in the monolayer content of these pixels, we divided the normalized integrated photoemission of each pixel by its monolayer fractional coverage. These final values provide a close approximation of the quantum yield (QY)[39−41] of these pixels relative to that of a full monolayer pixel, which we refer to as the normalized QY (Supporting Information). From the normalized QY, we can glean qualitative information about the effective minority carrier lifetime of the pixels. To do so, we plotted the normalized QY of these pixels as a function of their fractional coverage of monolayer f_{1L} in Figure 3f. Interestingly, the normalized QY decreases monotonically with decreasing the monolayer surface coverage of the pixels. This trend suggests an increase in nonradiative carrier recombination in the monolayer portion of the pixels with reducing the monolayer surface coverage, possibly due to the dominance of edge recombination.[42] From the discussion above, it is evident that while the selection of the photoemission threshold is strongly linked to the engineered CVD growth process, the absolute value of the threshold is governed by the physical properties of the material itself.

Figure 4a is the spatial map of the normalized integrated photoemission for a 2D MoS_2 array. We then converted the photoemission map to a 2D array of zero and one binary bits by comparing the normalized integrated emission of each pixel with the photoemission threshold θ of 0.12. The extracted 2D random binary code is shown in Figure 4b. Before we discuss the security test results of the primitive in the next section, we comment on the possible effect of the pixel choice and spacing

DOI: 10.1021/acsnano.7b07568

choice on the behavior of the security primitive. Considering CSR of the island growth and the equal surface coverage by the monolayer and multilayer MoS_2, it is expected that the distribution of the ON and OFF pixels shows no or weak dependency on the pixel size and the pixel spacing in the 2D MoS_2 array. We confirmed this by fabricating multiple arrays with different pixel sizes and spacings, where the arrays demonstrate equal distribution of random ON and OFF pixels (Supporting Information). Hence, the strength of the security primitive is robust to the pixel choice and spacing choice.

Analyzing Security and Stability Metrics. We next analyzed the security metrics of the 2D binary array. Three important metrics are typically used to evaluate the strength of a security primitive:[43] *uniqueness*, *repeatability*, and *uniformity*.

Uniqueness is the ability of a key to be distinguished from other keys. We use the average Hamming interdistance to quantify uniqueness. The Hamming interdistance between two keys is the minimum number of bit substitutions required to transform one key to another. The 32 rows of the 2D binary array are 64-bit security keys to be tested. We compute the Hamming interdistance of all 496 possible pairs of keys (see Supporting Information). Figure 4c shows the Hamming interdistance distribution. A binomial distribution with parameters $p = 0.495$ and $N = 64$ provides a good fit based on the Kolmogorov–Smirnov test. The inverse of the binomial distribution at cumulative probability 0.05 is 25. This means that for two randomly generated 64-bit keys, there is a 95% probability that the keys differ in at least 25 bits. Hence, there is a 95% chance that it will require at least 64 choose 25 (or 4×10^{17}) worst-case number of attempts to guess an unknown key from another known key.

A random key must also produce a consistent response to a given input challenge. The difference in response of a given binary key to the same challenge is quantified by the Hamming intradistance, which represents the *repeatability* of the random binary code. Therefore, the ideal intradistance is zero. Figure 4c shows the results of the Hamming intradistance, indicating high repeatability of the MoS_2 security keys. The observed bit error rates are measurement artifacts and originate from the limited spatial accuracy of the automated sample stage of the PL measurement system. To investigate the long-term stability of our security primitives, we measured a random sample of 200 pixels after 6 months storage in ambient air, as shown in Figure 4d. In this experiment, the candidate pixels had either high fractional areal coverage by a monolayer or a multilayer MoS_2 film. The unchanged emission properties of these pixels indicate that our MoS_2 cryptographic primitives are highly stable.

To maximize the combination randomness of a binary array, each pixel should have an equal probability (*i.e.*, 0.5) of being ON or OFF. This is defined as the *uniformity* property and is quantified by the Hamming weight of the key. Specifically, the Hamming weight indicates the number of bit substitutions to convert the key to an array of all zeros and has an ideal value of 0.5. We calculate the normalized Hamming weight on all 32 64-bit rows of the 2D binary array, and found the average to be 0.48 (see Supporting Information). As described earlier, the measured Hamming weight is directly linked and controlled by selection of the photoemission threshold. This discussion explains a key design parameter, which must be determined properly to achieve maximum combination randomness. Through our observations of the CVD growth process, we can tune the photoemission threshold value, thus taking full advantage of the inherent randomness of the cryptographic primitive.

Lastly, we comment on the physical unclonability of our security primitive. To classify a random physical construct as a security primitive, it must be capable of preventing an unauthorized duplication of its physical structure, even if the adversary has full control of the PUF manufacturing.[5] Figure 5 illustrates the topographic images of several MoS_2 pixels from the 2D array. These images highlight the extreme intricacy of the pixel structures. The heterogeneity of the thickness and the randomness of the spatial distribution of MoS_2 films within the pixels—originating from CSR of the multilayer island growth—make the 2D MoS_2 array physically unclonable. In contrast, we have shown that a physical array of pixels constructed from randomly distributed monolayer islands in Region I (before they coalesce) can be replicated using standard nanofabrication techniques (see Supporting Information). This experiment underscores that the mere randomness of a physical construct, although necessary, is insufficient for realizing a security primitive.

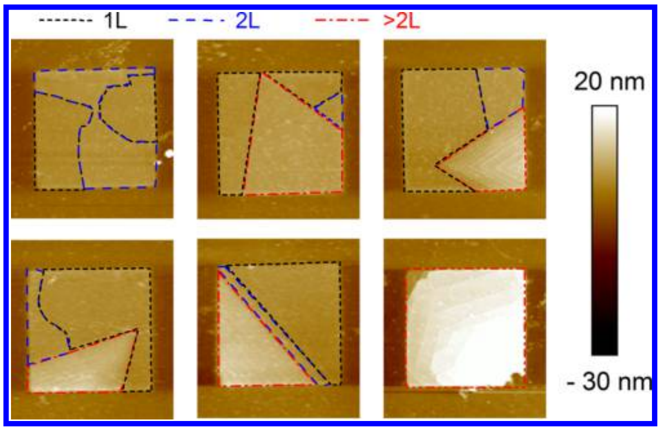


Figure 5. Physical unclonability of the MoS_2 primitive: Representative AFM images of a few MoS_2 pixels, highlighting their complex physical structures. The colored guide lines in these images show the borders of MoS_2 films with one, two, or more layers. It is impossible to physically duplicate such intricate structures.

CONCLUSIONS

We introduce a physically unclonable security primitive based on layered MoS_2. Two fundamental properties underlie this security technology: (i) CSR of multilayer island growth during CVD of MoS_2, confirmed by Clark–Evans test, and (ii) strong thickness dependence of photoemission in MoS_2. Using the Avrami equation, we show that the nucleation is continuous and that the island growth is two-dimensional. We define a photoemission threshold to convert the optical response of the physical 2D array into a binary cryptographic key. Our experiments establish that this threshold is directly linked to the engineered growth process and can be tuned to maximize the combination randomness of the security keys. These security primitives are easy to produce on a large scale using CVD and yet impossible to duplicate because of the intricate physical structures of the pixels. The findings of this study can be readily extended for the development of physically unclonable primitives based on other semiconducting transition metal dichalcogenides.

METHODS

We performed CVD growth using MoO_3 and sulfur solid precursors without requiring a growth promoter. The growth was performed using a custom-made setup at 850 °C with a nitrogen flow of 10 sccm. The optimal quantities of MoO_3 and sulfur precursors are about 6 mg and 100 mg. In all the experiments, the films were grown in the presence of excess sulfur. The details of the growth experiments are given in the Supporting Information. The 2D MoS_2 array was fabricated using an e-beam lithography step followed by patterning in an CF_4/O_2 plasma. The 2D arrays were stimulated using a green laser for producing an optical response.

ASSOCIATED CONTENT

Supporting Information

The Supporting Information is available free of charge on the ACS Publications website at DOI: 10.1021/acsnano.7b07568.

> Details of chemical vapor deposition, analysis of growth in Regions I and II, interpretation of Avrami exponent, normalized quantum yield analysis, physical unclonability experiments, details of PL measurements, studies of pixel size and spacing choices, and analysis of security metrics (PDF)

AUTHOR INFORMATION

Corresponding Author

*E-mail: davood@nyu.edu.

ORCID

Davood Shahrjerdi: 0000-0002-5955-1830

Notes

The authors declare no competing financial interest.

ACKNOWLEDGMENTS

This work was supported in part by NSF Award #1638598 and by U.S. Army Research Office Award #W911NF-16-1-0301. This research used resources of the Center for Functional Nanomaterials, which is a U.S. DOE Office of Science Facility, at Brookhaven National Laboratory under Contract No. DE-SC0012704. The authors acknowledge C. Black and J. Uichanco for helpful discussions.

REFERENCES

(1) Perry, T. S. Why Hardware Engineers Have to Think Like Cybercriminals, and Why Engineers Are Easy to Fool. *IEEE Spectrum*; May 15, 2017; https://spectrum.ieee.org/view-from-the-valley/computing/embedded-systems/why-hardware-engineers-have-to-think-like-cybercriminals-and-why-engineers-are-easy-to-fool.

(2) Rostami, M.; Koushanfar, F.; Rajendran, J.; Karri, R. Hardware Security: Threat Models and Metrics. *Int. Conf. Computer-Aided Design (ICCAD)*; 2013; pp 819−823.

(3) Rostami, M.; Koushanfar, F.; Karri, R. A Primer on Hardware Security: Models, Methods, and Metrics. *Proc. IEEE* **2014**, *102*, 1283−1295.

(4) Herder, C.; Yu, M.-D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. *Proc. IEEE* **2014**, *102*, 1126−1141.

(5) Maes, R. *Physically Unclonable Functions*; Springer, 2016; pp 49−82.

(6) Sadeghi, A.-R.; Naccache, D. *Information Security and Cryptography*; Springer, 2010; pp 39−53.

(7) Gassend, B.; Clarke, D.; Van Dijk, M.; Devadas, S. Silicon Physical Random Functions. *ACM Conf. Comput. Commun. Secur.* **2002**, 148−160.

(8) Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical One-Way Functions. *Science* **2002**, *297*, 2026−2030.

(9) Pham, H. H.; Gourevich, I.; Jonkman, J. E.; Kumacheva, E. Polymer Nanostructured Material for the Recording of Biometric Features. *J. Mater. Chem.* **2007**, *17*, 523−526.

(10) Huang, C.; Lucas, B.; Vervaet, C.; Braeckmans, K.; Van Calenbergh, S.; Karalic, I.; Vandewoestyne, M.; Deforce, D.; Demeester, J.; De Smedt, S. C. Unbreakable Codes in Electrospun Fibers: Digitally Encoded Polymers to Stop Medicine Counterfeiting. *Adv. Mater.* **2010**, *22*, 2657−2662.

(11) Han, S.; Bae, H. J.; Kim, J.; Shin, S.; Choi, S.-E.; Lee, S. H.; Kwon, S.; Park, W. Lithographically Encoded Polymer Microtaggant Using High-Capacity and Error-Correctable QR Code for Anti-Counterfeiting of Drugs. *Adv. Mater.* **2012**, *24*, 5924−5929.

(12) Blumenthal, T.; Meruga, J.; May, P. S.; Kellar, J.; Cross, W.; Ankireddy, K.; Vunnam, S.; Luu, Q. N. Patterned Direct-Write and Screen-Printing of NIR-to-Visible Upconverting Inks for Security applications. *Nanotechnology* **2012**, *23*, 185305.

(13) Kim, J.; Yun, J. M.; Jung, J.; Song, H.; Kim, J.-B.; Ihee, H. Anti-Counterfeit Nanoscale Fingerprints Based on Randomly Distributed Nanowires. *Nanotechnology* **2014**, *25*, 155303.

(14) Hu, Z.; Comeras, J. M. M. L.; Park, H.; Tang, J.; Afzali, A.; Tulevski, G. S.; Hannon, J. B.; Liehr, M.; Han, S.-J. Physically Unclonable Cryptographic Primitives Using Self-Assembled Carbon Nanotubes. *Nat. Nanotechnol.* **2016**, *11*, 559−565.

(15) Böhm, C.; Hofer, M. *Physical Unclonable Functions in Theory and Practice*; Springer Science & Business Media, 2012; pp 105−130.

(16) Škoric, B.; Tuyls, P.; Ophey, W. *Applied Cryptography and Network Security*; Springer, 2005; Vol. *3531*, pp 407−422.

(17) Helfmeier, C.; Boit, C.; Nedospasov, D.; Tajik, S.; Seifert, J.-P. Physical Vulnerabilities of Physically Unclonable Functions. In *Design, Automation, and Test in Europe*; Springer, 2014; p 350.

(18) Franklin, A. D.; Tulevski, G. S.; Han, S.-J.; Shahrjerdi, D.; Cao, Q.; Chen, H.-Y.; Wong, H.-S. P.; Haensch, W. Variability in Carbon Nanotube Transistors: Improving Device-to-Device Consistency. *ACS Nano* **2012**, *6*, 1109−1115.

(19) Park, H.; Afzali, A.; Han, S.-J.; Tulevski, G. S.; Franklin, A. D.; Tersoff, J.; Hannon, J. B.; Haensch, W. High-Density Integration of Carbon Nanotubes *via* Chemical Self-Assembly. *Nat. Nanotechnol.* **2012**, *7*, 787−791.

(20) Kang, K.; Xie, S.; Huang, L.; Han, Y.; Huang, P. Y.; Mak, K. F.; Kim, C.-J.; Muller, D.; Park, J. High-Mobility Three-Atom-Thick Semiconducting Films with Wafer-Scale Homogeneity. *Nature* **2015**, *520*, 656−660.

(21) Najmaei, S.; Liu, Z.; Zhou, W.; Zou, X.; Shi, G.; Lei, S.; Yakobson, B. I.; Idrobo, J.-C.; Ajayan, P. M.; Lou, J. Vapor Phase Growth and Grain Boundary Structure of Molybdenum Disulfide Atomic Layers. *Nat. Mater.* **2013**, *12*, 754−759.

(22) Bilgin, I.; Liu, F.; Vargas, A.; Winchester, A.; Man, M. K. L.; Upmanyu, M.; Dani, K. M.; Gupta, G.; Talapatra, S.; Mohite, A. D.; et al. Chemical Vapor Deposition Synthesized Atomically Thin Molybdenum Disulfide with Optoelectronic-Grade Crystalline Quality. *ACS Nano* **2015**, *9*, 8822−8832.

(23) Wang, S.; Rong, Y.; Fan, Y.; Pacios, M.; Bhaskaran, H.; He, K.; Warner, J. H. Shape Evolution of Monolayer MoS_2 Crystals Grown by Chemical Vapor Ddeposition. *Chem. Mater.* **2014**, *26*, 6371−6379.

(24) King, D. A.; Woodruff, D. *Growth and Properties of Ultrathin Epitaxial Layers*; Elsevier, 1997; Vol. *8*, pp 2−70.

(25) Mak, K. F.; Lee, C.; Hone, J.; Shan, J.; Heinz, T. F. Atomically Thin MoS_2: A New Direct-Gap Semiconductor. *Phys. Rev. Lett.* **2010**, *105*, 136805.

(26) Gong, Y.; Li, B.; Ye, G.; Yang, S.; Zou, X.; Lei, S.; Jin, Z.; Bianco, E.; Vinod, S.; Yakobson, B. I.; et al. Direct Growth of MoS_2 Single Crystals on Polyimide Substrates. *2D Mater.* **2017**, *4*, 021028.

(27) Elías, A. L.; Perea-López, N.; Castro-Beltrán, A.; Berkdemir, A.; Lv, R.; Feng, S.; Long, A. D.; Hayashi, T.; Kim, Y. A.; Endo, M.; et al. Controlled Synthesis and Transfer of Large-Area WS2 Sheets: From Single Layer to Few Layers. *ACS Nano* **2013**, *7*, 5235−5242.

(28) Salvatore, G. A.; Münzenrieder, N.; Barraud, C.; Petti, L.; Zysset, C.; Büthe, L.; Ensslin, K.; Tröster, G. Fabrication and Transfer

of Flexible Few-Layers MoS_2 Thin Film Transistors to Any Arbitrary Substrate. *ACS Nano* **2013**, *7*, 8809−8815.

(29) Splendiani, A.; Sun, L.; Zhang, Y.; Li, T.; Kim, J.; Chim, C.-Y.; Galli, G.; Wang, F. Emerging Photoluminescence in Monolayer MoS_2. *Nano Lett.* **2010**, *10*, 1271−1275.

(30) Wang, Q. H.; Kalantar-Zadeh, K.; Kis, A.; Coleman, J. N.; Strano, M. S. Electronics and Optoelectronics of Two-Dimensional Transition Metal Dichalcogenides. *Nat. Nanotechnol.* **2012**, *7*, 699−712.

(31) Clark, P. J.; Evans, F. C. Distance to Nearest Neighbor as a Measure of Spatial Relationships in Populations. *Ecology* **1954**, *35*, 445−453.

(32) Van Der Zande, A. M.; Huang, P. Y.; Chenet, D. A.; Berkelbach, T. C.; You, Y.; Lee, G.-H.; Heinz, T. F.; Reichman, D. R.; Muller, D. A.; Hone, J. C. Grains and Grain Boundaries in Highly Crystalline Monolayer Molybdenum Disulphide. *Nat. Mater.* **2013**, *12*, 554−561.

(33) Yu, Y.; Li, C.; Liu, Y.; Su, L.; Zhang, Y.; Cao, L. Controlled Scalable Synthesis of Uniform, High-Quality Monolayer and Few-Layer MoS_2 Films. *Sci. Rep.* **2013**, *3*, 1866.

(34) Alharbi, A.; Shahrjerdi, D. Electronic Properties of Monolayer Tungsten Disulfide Grown by Chemical Vapor Deposition. *Appl. Phys. Lett.* **2016**, *109*, 193502.

(35) Alharbi, A.; Zahl, P.; Shahrjerdi, D. Material and Device Properties of Superacid-Treated Monolayer Molybdenum Disulfide. *Appl. Phys. Lett.* **2017**, *110*, 033503.

(36) Avrami, M. Kinetics of Phase Change. I General Theory. *J. Chem. Phys.* **1939**, *7*, 1103−1112.

(37) Starink, M. On the Meaning of the Impingement Parameter in Kinetic Equations for Nucleation and Growth Reactions. *J. Mater. Sci.* **2001**, *36*, 4433−4441.

(38) Fossum, E. R.; Hondongwa, D. B. A Review of the Pinned Photodiode for CCD and CMOS Image Sensors. *IEEE J. Electron Devices Soc.* **2014**, *2*, 33−43.

(39) Yablonovitch, E.; Cody, G. D. Intensity Enhancement in Textured Optical Sheets for Solar Cells. *IEEE Trans. Electron Devices* **1982**, *29*, 300−305.

(40) Crosby, G. A.; Demas, J. N. The Measurement of Photoluminescence Quantum Yields. A Review. *J. Phys. Chem.* **1971**, *75*, 991−1024.

(41) Würth, C.; Grabolle, M.; Pauli, J.; Spieles, M.; Resch-Genger, U. Relative and Absolute Determination of Fluorescence Quantum Yields of Transparent Samples. *Nat. Protoc.* **2013**, *8*, 1535−1550.

(42) Zhao, P.; Amani, M.; Lien, D.-H.; Ahn, G. H.; Kiriya, D.; Mastandrea, J. P.; Ager, J. W.; Yablonovitch, E.; Chrzan, D.; Javey, A. Measuring the Edge Recombination Velocity of Monolayer Semiconductors. *Nano Lett.* **2017**, *17*, 5356.

(43) Mukhopadhyay, D.; Chakraborty, R. S. *Hardware Security: Design, Threats, and Safeguards*; CRC Press, 2014; pp 486−489.