FIELD OF THE INVENTION

This invention is a nanomaterial apparatus, with application to an unconditionally secure method of data encryption. More specifically, a disordered single-electron tunnelling (SET) network, realizing a strong physical unclonable function (PUF) from which one-time pad (OTP) keys are derived. The advantages of this invention are that the OTP key cannot be cracked within its lifetime by brute-force physical attacks and learnt by analytical or computer modelling. This invention has a lower cost of fabrication, a smaller device footprint, and a lower energy consumption in comparison to existing solutions for data encryption.

BACKGROUND OF THE INVENTION

The one-time pad (OTP), was first used in 1882 as a telegraphic code to ensure privacy and secrecy in the transmission of telegrams [1]. OTP uses a random secret-key that is as long as the plaintext. Encryption is done by a bitwise XOR between the plaintext and the secret-key, to generate a ciphertext. Decryption is done by a bitwise XOR of the ciphertext with the secret-key. If an adversary obtains the ciphertext and brute-forces all possible keys, then they would also obtain all meaningful plaintexts of the given length. Hence, OTP encryption is uncrackable in theory. In 1949, Shannon proved that for any cipher to be mathematically uncrackable: it should have a random key, with length at least equal to the plaintext length [2]. Thus, OTP is the most efficient cipher for perfect secrecy.

Unfortunately, implementations of OTP in existing digital hardware is impractical when data is in terabytes. Because storing terabyte sized OTP keys in "protected" memory would be very expensive, and risky against novel physical attacks [3]. As an alternative to key storage in protected memory, there is the emerging technology of physical unclonable function (PUF) [4], where a physically disordered material is measured optically or electrically to derive keys.

The first known PUF was optical and used a transparent material with microbeads [5]. A laser beam is pointed into the

material and results in a speckle pattern which is Gabor transformed to provide a OTP key. It is a PUF where the key is a function of the illumination coordinates, is unique per material, and is unpredictable by mathematical modelling. The key is a bitwise random function of the illumination coordinates, which is a good property for OTP. However, there exists correlations among the bits and thus the key is unsuitable for OTP without a whitening transformation. In another kind of optical PUF [**6**], it was observed that due to the slight drift of scatterers, decryption after a 24-hour delay, resulted in a message noise of 0.4 bit-error rate. Better reliability is observed among electronic PUFs that probe manufacturing variations in silicon [**7**]. SRAM PUF technology is industry leading and proven to be 100% reliable over a span of 2 years and put to use in smartcard, government, automotive, networking and telecom industries to provide authentication technology which require 128 or 256-bit secret key. The startup value of each SRAM bit is uncorrelated and random [**8**], so SRAM PUFs are theoretically suitable for OTP. But, they have a weak bit capacity unlike volumetric optical PUFs, so a terabyte sized SRAM PUF OTP would be expensive and bulky. For a strong PUF capacity, there exists arbiter PUFs that exploit the statistical delay variation in ICs [**9**]. An input transition travels to the arbiter via two parallel delay paths configured by challenge bits $(b_1,b_2,\ldots,b_N)$. The arbiter outputs a 1 or 0 depending on the outcome of this race. Here there are 2^N challenges or race conditions, with device dependent unique responses which is a strong capacity. But, the challenge-response pairs (CRPs) are correlated because two challenges sharing a lot of common bits were likely to have a large path overlap, and hence similar delay responses. In fact, we can train a model for the CRPs by machine learning [**10**].

Thus, none of the PUFs described in the prior-art are practical for OTP, because they are either unreliable or weak or correlated.

OBJECTS OF THE INVENTION

The principal object of this invention is to overcome the limitations of the prior-art and realize a strong physical unclonable function (PUF) which is reliable for generating uncorrelated bits and thus suitable for terabyte sized one-time pad (OTP) encryption.

Another object of this invention is to ensure that the OTP encryption is scalable by employing several PUFs in parallel.

SUMMARY OF THE INVENTION

An aspect of the invention is a nanoelectronic device **300** comprising: a thin film of nanomaterials **101** on an insulating substrate **102** surrounded by a plurality of electrodes; a subset of the surrounding electrodes **103** each connected individually to the plurality of voltage states of a binary counter **401** and the remaining subset of the surrounding electrodes **104** each connected individually to the voltage states of a bit array **402**; a drain electrode **201** in the centre which is connected to the virtual ground of a clocked current mode comparator **403**. Another aspect of the invention is a process to derive a strong physical unclonable function (PUF) **500** from the said device, by considering the challenge as a number which sets the bit array and the response as the comparator output bitstream **404** from reset until the end of counting. A practical application is the derivation of one-time pad (OTP) key from one or more of the said devices carrying out the said process parallely in time, wherein the OTP key is a specified permutation of the response from all the PUFs to a specified challenge. Another novel application is the derivation of a pseudorandom function by the said process on a simulation of the said nanoelectronic device.

DETAILED DESCRIPTION THE INVENTION

The invention is based on the nonlinear interactions due to Coulomb blockade physics in single-electron tunnelling (SET) networks [**11**]. SET networks have been previously fabricated to work at room-temperatures using nanoscale islands distributed randomly in an insulating thin film [**12**], however they could not be utilized in conventional computers because of extreme device-to-device variations in electronic conductivity. Here, we will use such nanomaterial thin films with multiple electrodes to realize multi-input Boolean logic functionality, wherein the functionality is determined by naturally occurring variations during fabrication of the nanoelectronic device.

Figure 1 is a cross-sectional top view of the nanoelectronic device; wherein **101** is a thin film of nanomaterial which is known to act as a SET network for the given operating conditions, **102** is an insulating substrate, **103** and **104** are metallic electrodes (for voltage inputs). **Figure 2** is a cross-sectional side view of the nanoelectronic device; wherein **201** is a metallic electrode (for a current output) and **202** is an insulating layer. **Figure 3** is a top view of the nanoelectronic device. The voltage potential on each island is determined by summing the contributions due to : offset potentials induced by variations in nanofabrication, voltage induced by the electrodes, and the voltage induced by the charge occupancy on the islands. The voltages form a lattice group because the charge occupancy has to be an integer number. So, the stable current output at **201** is zero only if the closest lattice point [**13**] under Chebyshev distance of the said lattice group is robust to thermal fluctuations. Finding the closest lattice point is proven to be a NP-hard problem, and hence so is establishing the stability of random SET networks. The electrode voltages are set by input bits to be each either grounded or at a voltage comparable to the SET network's charging energy, so that SET physics is dominant and the stability of the SET network results in a pseudorandom function. The fact that the SET network is a physically motivated model (i.e. being a natural and not a human-designed algorithm), implies that SET

network simulations (although not an object of this invention) are suitable as backdoor-free pseudorandom functions.

In order to obtain a strong physical unclonable function (PUF) from the nanoelectronic devices, a binary counter **401** applies voltages on a subset of electrodes (**103**), a bit array **402** applying voltages to the remaining subset of electrodes (**104**), a current-mode comparator **403** measures the output at **201**. **Figure 4** is a schematic of the nanoelectronic apparatus. **Figure 5** is a representation of the nanoelectronic apparatus as a PUF, wherein the challenge is a number which sets the bit array and the response is the comparator output bitstream **404** from reset until the end of counting. **Figure 6** is a depiction of the ideal challenge-response behaviour of a PUF (**500**) with *m* electrodes of type **103** and *n-m* electrodes of type **104**, wherein the information entropy increases exponentially with the number of electrodes. For *m*=43, we would obtain terabyte sized OTP. Assuming it takes 2 ns to switch between addresses and measure the output, we would be able to encrypt at a speed of 500 Mbps and match the USB 2.0 transfer rate. Several PUFs can be used to encrypt the same data in parallel, to ensure data integrity or improve data transfer rates.

Figure 7 is a practical scheme for data encryption by using one or more PUF response(s) as a OTP; wherein if there are *x* number of PUFs, the data is split into blocks of *x* bits and each data block of index *i* is encrypted by XORing with the OTP key derived from a specified permutation of the PUF responses to a specified challenge at count number = *i*. By the said method, the time-ratio of a brute-force search against decryption is equal to 2^(*n-m+x*). Thus, we are able to boost the scalability of PUFs for OTP by a factor of 2^*x*.

LIST OF REFERENCES CITED

[1] Miller, F. (1882). *Telegraphic code to insure privacy and secrecy in the transmission of telegrams.* CM Cornwell.

[2] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal,* 28(4), 656-715.

[3] Skorobogatov, S. P. (2005). Semi-invasive attacks: a new approach to hardware security analysis (Doctoral dissertation, University of Cambridge).

[4] Chang, C. H., Zheng, Y., & Zhang, L. (2017). A retrospective and a look forward: Fifteen years of physical unclonable function advancement. *IEEE Circuits and Systems Magazine*, 17(3), 32-62.

[5] Pappu, R., Recht, B., Taylor, J., & Gershenfeld, N. (2002). Physical one-way functions. *Science*, 297(5589), 2026-2030.

[6] Horstmeyer, R., Judkewitz, B., Vellekoop, I. M., Assawaworrarit, S., & Yang, C. (2013). Physical key-protected one-time pad. *Scientific reports,* 3, 3543.

[7] Gassend, B., Clarke, D., Van Dijk, M., & Devadas, S. (2002). Silicon physical random functions. In *Proceedings of the 9th ACM conference on Computer and communications security* (pp. 148-160). ACM.

[8] Schrijen, G. J., & Van Der Leest, V. (2012, March). Comparative analysis of SRAM memories used as PUF primitives. In *Proceedings of the conference on design, automation and test in Europe* (pp. 1319-1324). EDA Consortium.

[9] Lim, D., Lee, J. W., Gassend, B., Suh, G. E., Van Dijk, M., & Devadas, S. (2005). Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13(10), 1200-1205.

[10] Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., & Schmidhuber, J. (2010, October). Modeling attacks on physical unclonable functions. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 237-249). ACM.

[11] Likharev, K. K. (1999). Single-electron devices and their applications. *Proceedings of the IEEE,* 87(4), 606-632.

[12] Yano, K., Ishii, T., Hashimoto, T., Kobayashi, T., Murai, F., & Seki, K. (1994). Room-temperature single-electron memory. *IEEE Transactions on Electron Devices*, *41*(9), 1628-1638.

[13] Agrell, E., Eriksson, T., Vardy, A., & Zeger, K. (2002). Closest point search in lattices. *IEEE transactions on information theory*, *48*(8), 2201-2214.