Firewall with Nano-Helix PUFs For Fiber-Optic Communication

Bertrand Cambou
Northern Arizona University
1(928)5237824
Bertrand.cambou@nau.edu

John Gibbs
Northern Arizona University
1(928)5231916
John.gibbs@nau.edu

ABSTRACT: Complex Nanostructures deposited on transparent substrates with techniques such as Glancing Angle Deposition (GLAD) can be inserted into a fiber-optic cable to create unique patterns similar to DNA helices that can be exploited as Physically Unclonable Functions (PUFs). The resulting PUFs can act as a real "firewall" protecting communications through fiber-optic cables with challenge-response-pair (CRP) authentication. The trusted cables within Cyber-Physical-Systems (CPS) can be part of the cryptographic architecture securing the network.

KEYWORDS: Access control, critical infrastructure, cryptographic primitives, security in grid systems, Physically Unclonable Function, fiber-optics.

INTRODUCTION: The proliferation of connected machines, consumer products, automobiles, the smart grid, and the Internet of Things (IoT) has created new opportunities for criminals, terrorists, and black hat hackers.

Threats and mitigation. Some of the most common cyber-attack threats involve hackers who gain unauthorized access to a user's system or manage to download and execute unauthorized software on a computer connected to the network, as well as the insertion of Trojans and malwares. The first line of defense is to install a strong firewall with trustworthy access control to the CPS and their subsystems. It is always better to prevent malware from penetrating a CPS and contaminating its databases, rather than trying to remove it then mitigate the damages. Effective firewalls, access control, and authentication methods are based on cryptographic methods, passwords, and secret key management.

Physically Unclonable Functions. There is now a growing interest in implementing a new class of PUFs to strengthen the authentication process by using a powerful set of physically derived cryptographic primitives [1-7]. PUFs act as virtual fingerprints for hardware, and thereby provide unique signatures during the authentication processes to effectively block cyber theft, Trojans, and malware. The inherent randomness, uniqueness, secrecy, and physical nature of a PUF makes it extremely hard to inspect for unwelcomed users whereas PUFs are very effective for trusted secure authentications. The underlying mechanism of a PUF is the implementation of a generator, which can produce a large number of challenges (i.e. input) responses (i.e. output) pairs (CRPs). When deployed during the authentication process, a challenge is generated and a PUF-specific response is also generated. The generation of CRPs has to be reproducible, and easy to recognize.

Firewall with PUF. The idea to use a PUF solution to create a firewall at the point of entry has been proposed in previous work [8-11]. In these new structures the PUFs are not inserted in the connecting cable. The concept of securing the optical fiber cables that we are describing in this paper, is inserting Nano-structure based PUFs directly into the cable. This method provides synergistic levels of security and means of access control with existing cyber-systems.

Complex Nano-structures for PUF architectures. The application of complex Nano-structures in the form of Nano-helices to Cyber Security is extremely new and, to the best of our knowledge, has not been studied previously. Their intrinsic physical properties are excellent for the design of a new class of PUF directly integrated into fiber communication because of their relatively high level of randomness, nanoscale dimensions, and unique features that are hard to duplicate, i.e. unclonability. The concept described in this paper is promising, however the full understanding of how Nano-helix materials behave under light transmission is an active field of research. The reproducibility and stability of the Nano-helix, and their transmitting properties are key criteria for the success of the research work. The image detection and processing of the patterns created by the light transmitted through the Nano-structures is rather straightforward; the infrared (IR) absorption spectra of the Nano-helices, which typically have ~50nm critical dimensions, create clusters detectable with existing technologies. Converting the transmitted pattern into challenges and responses is the subject of §4.

1- General description

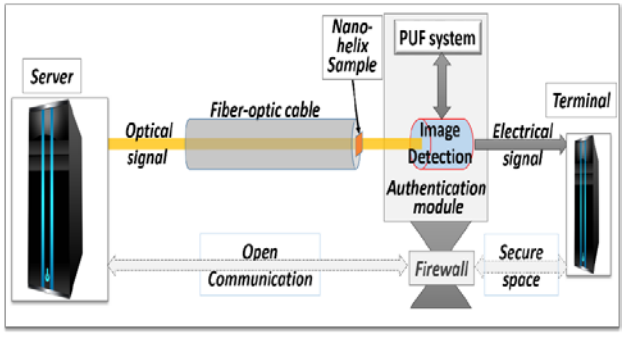


Figure 1. Simplified description of the firewall.

The simplified description of a firewall based upon complex Nano-structures is presented in Fig. 1. The sample, which is inserted at the end of the fiber-optic cable, is a transparent glass containing an array of Nano-helix structures that selectively attenuate the transmitted light. Each sample is unique and distinct. An image detection system captures the transmitted pattern, digitalizes it, and sends the information to the PUF subsystem for authentication. If positive, the PUF

subsystem opens the virtual "gate", allowing secure information to reach the terminal. The cryptographic architecture of the PUF is described in Fig. 2. At first the server receives a reference pattern from the PUF called a "challenge".

To generate this challenge, the server illuminates the optic fiber, the Nano-helix sample selectively transmits light, and the image detection captures the pattern for the PUF subsystem to complete the process. The challenge is then transmitted back, while encrypted, to the secure server for future reference. To trigger a new authentication, the server sends a query with the challenge and the PUF generates a fresh "response". If the challenge-response-pairs (CRPs) match, then the authentication is positive, and the communication gates open between the server and the terminal.

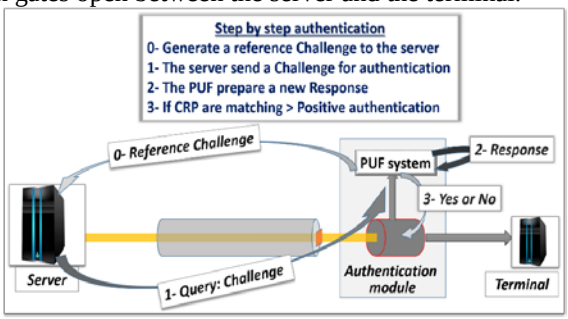


Figure 2. PUF CRP authentication method.

An example of the network system with a Nano-helix-based firewall is shown in Fig. 3, in which the firewalls are inserted within the intranet. The trustworthy authentication offered by the firewall can be put to use to secure data files, applications, and software that are downloaded to each site. It can also prevent a particular site from sending confidential files to a different site without following a process managed by the secure server.

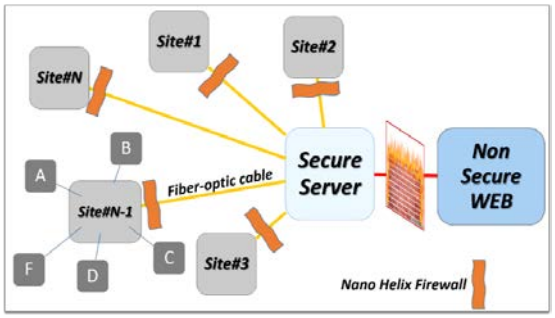


Figure 3. Firewall to secure a networked system.

2- Complex Helix Nano-structure.

2.1 PUF CRPs generation from light scattering

GLAD-grown nanomaterials, including the Nano-Helix, are expected to be an ideal material for the fabrication of PUFs. This is true due to the small variations in the morphology between each structure on the surface, leading the optical properties to be a function of the location on the substrate. Composite insulator/metal nanocomposite structures described above be potentially very useful for PUFs since the spacing between the embedded nanoparticles will have a large effect on the light absorbance as a function of wavelength, as seen in Equation 1. For example, a red laser may absorb strongly in one section of the substrate due to the plasmonic coupling in that region whereas a second region may give rise to a strong plasmonic shift. This second region would then absorb only a fraction of the light absorbed by the first. The inherent variations in the structures, which is a natural part of the fabrication process, would then give rise to a useful PUF. The deposition parameters such as deposition rate, material combinations and other conditions need to be optimized both experimentally and numerically to match the particular wavelength being used in the optical cable. By successfully tuning and characterizing these parameters this unique material can be employed as part of a PUF design.

2.2 Description of complex Nano-structures

Nanomaterials are revolutionizing several branches of materials science and engineering [12-14]. Materials with nanoscale features often exhibit drastically different properties not seen in their bulk counterparts, and it is therefore possible to use nanoengineering to fabricate materials with desired properties and functionalities for targeted applications [15-16]. A particularly interesting nanoscale morphology is the helix, which is very often observed in the natural world especially in biology [17-20]. In everyday macroscale engineering, helical antennae have long been used in radio communications [21]. Not until recent advances in nanoengineering has it been possible to fabricate Nano-helices with feature sizes small enough to exhibit resonance phenomena at visual frequencies [22-25]. The optical properties of a nanomaterial can be tuned by controlling the chemical composition [26] and morphology. [27] The parameters of the helix can also be tuned to exhibit unique properties if the fabrication process allows for a high level of control [28].

2.3 Nano-helix sample fabrication

A physical vapor deposition (PVD) technique termed Glancing Angle Deposition (GLAD), [22,29,30] illustrated in Fig. 4, can be used to fabricate complex 3D nanostructures.

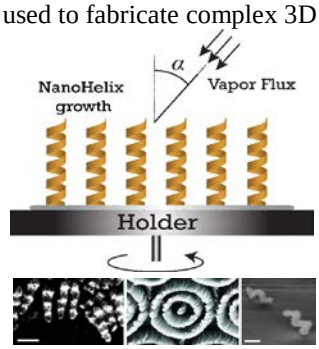


Figure 4. Top: Fabrication of Nano-Helix array, and a few structures by GLAD growth including a Nano-Helix. Scale bar = 200nm - left image and 50nm in the right.

The top of Fig. 4 shows a general schematic in which a physical vapor plume in a vacuum environment (~10^{-7} Torr) impinges upon a substrate at an oblique angle, α, which leads to nanostructured arrays with feature sizes as large as several micrometers (μm) [31] down to as small as tens of nanometers (nm), [34-39] which can be grown onto a variety of surfaces. A few examples are shown in the scanning electron microscopy (SEM) images in the bottom of Fig. 5. Samples can be optimized for desirable PUF characteristics by altering the deposition parameters of the fabrication process and then analyzing the Nano-Helix array's morphology and optical properties. Reproducibility can also be quantified by analyzing the optical measurements of individual PUFs. The particular class of nanomaterial that we expect to be most effective is the nanocomposite Nano-Helix.

Nanocomposites are mixtures of solid materials, which exist in different phases with at least one phase having nanoscale critical dimensions [43-44]. In particular, we can fabricate Nano-Helix arrays made from a transparent electrical insulator with metal nanodots embedded within the insulating matrix. This can be accomplished with a dual-source GLAD system capable of simultaneously depositing the two different materials. The schematic in the left of Fig. 5 illustrates the simultaneous deposition of two materials, which are immiscible and therefore form a multi-phase solid. The way in which the Nano-dots are embedded within the electrically insulating backbone can be controlled by independently altering the deposition rates of each material as well as by controlling the relative ratios. In Fig. 6(a), the ratio, r = (metal deposition rate):(insulator deposition rate) is lower in the top schematic and higher in the bottom showing the controllability of the morphology.

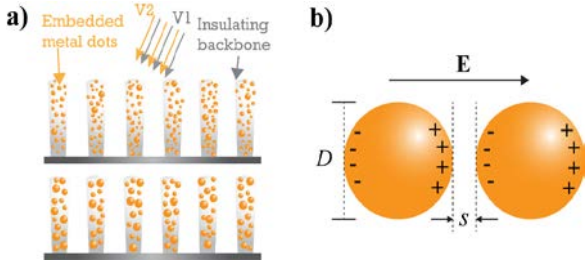


Figure 5. (a) Schematic of the formation of smaller metallic nanodots embedded into larger nanostructures duel deposition, and (b) schematic

Nanocomposites of this type are expected to be particularly useful as possible PUFs. Since the deposition rates control the size and separation between the metal nanodots, the optical properties can be adjusted with the GLAD process. Metal nanoparticles are well known to exhibit surface plasmon resonances [26, 34-40]. That is, the electrons in the metal couple to the electromagnetic wave (Fig. 5(b)), even though the wavelength of the light may be much larger than the size of the particles themselves, leading to collective plasmon oscillations of the electrons. The resonance frequency is in the visible or near infrared (NIR) for many metals leading to high absorbance of light at this frequency. The resonance peak is not only a function of the size and material composition of the nanoparticles, but also the separation between particles [41]. The shift in the peak of the absorbance decays exponentially with distance:

$$\frac{\Delta\lambda}{\lambda_0} \approx \alpha \exp\left(-\frac{s/D}{\beta}\right) \quad (1)$$

where $\Delta\lambda/\lambda_0$, s, and D are the fractional plasmon shift, the edge-to-edge separation, and the diameter of the particle, respectively. Equation 1 describes how particle adjacency affects the collective electron oscillations leading to a shift in the plasmon peak. This phenomena is ideal for a PUF since the small variations between the size and separation of the nanodots have exponentially changing effects on the optical properties.

3- Image detection

The light transmitted by Nanomaterial samples needs to be detected through image detection for the purpose of access control. As illustrated in Fig. 6, the commercial fiber-optic cable is using three infra-red wavelengths to transmit information, 850nm, 1300nm, and 1500nm. The multi-mode fibers, which allow the transmission of multiple signals at once, has a cable with core dimeter d = 62.5µm, and uses a wavelength of 850nm. The mixed-mode fibers, which allows both the transmission of a single signal or multiple ones, has a cable d = 50µm, and use the 1300nm wavelength. The single-mode uses a small d = 9µm core, and 1550nm wavelength.

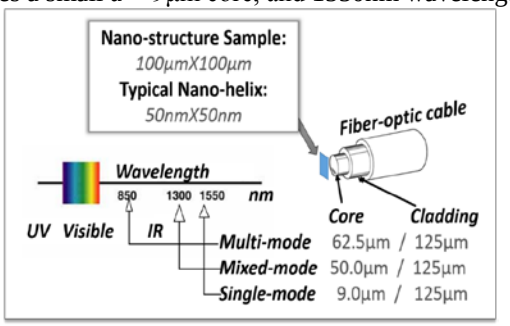
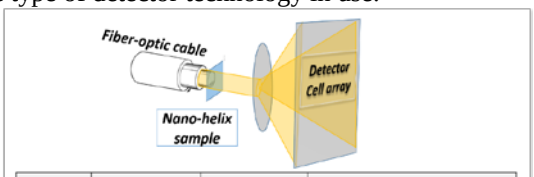


Figure 6: Transmission modes.

In all cases the cladding surrounding the core has a larger diameter d =125µm circular cladding, so it is possible to insert a transparent Nano-structure sample measuring 100µm × 100µm. Assuming that the typical size of a Nano-helix is 50nm × 50nm, and that they are spaced 50nm from each other, the smaller 9µm core can illuminate approximately 5,000 Nano-helices which is already statistically very large. As discussed in § 2 both the size and space between Nanostructures is subject to variations in the manufacturing process, and can eventually be adjusted to maximize the quality of the PUFs. As illustrated in Fig. 7, there is a need to magnify the image transmitted by the Nano-structure for the image detector, and this is a function of the size of the core, and the type of detector technology in use.



Detector	Sensitivity (nm)	Pixel size	Magnification to get 150 pixels With various cable diameter		
			125µm	50µm	9µm
CMOS	200nm-900nm	1µm X 1µm	1:1	1:1	1:3
InGaAs	200nm-5000nm	15µm X 15µm	1:4	1:20	1:500
Quantum	200nm-5000nm	1.5µm X 1.5µm	1:1	1:1	1:6

Figure 7: image detectors for the Nanostructures.

- *CMOS detectors* have small pixel sizes, 1µm × 1µm, and a sensitivity that stops at 900nm which is enough for multi-mode cables but useless at 1300nm and 1550nm for mixed mode and single mode cables.
- *InGaAs detectors* have wide sensitivity in the entire infrared spectrum, however the pixel size is big, at least 15µm X 15µm with current commercially available solutions. A 1:500 magnifying system needs to be inserted so enough pixels are illuminated by the single mode fiber.
- *Quantum dot image sensor* is an emerging technology which is now commercially available [42]. It offers the sensitivity of InGaAs sensors, with smaller pixel sizes of 1.5µm × 1.5µm, nearly as small as CMOS sensors. A 1:6 magnification is enough to illuminate 150 pixels with single mode cables, and can be obtained simply by inserting a small lens into the cable.

Fiber-optic cables need a photodetector to convert the photonic signal into an electronic signal. One of the mainstream photo-detection technologies is based on InGaAs/InP photodiodes. We believe that it is possible to use InGaAs and Quantum dot image detectors to simultaneously drive the PUF for authentication, and convert the photonic signals into electronic signals, and this as suggested in Fig. 1. Such a configuration is very attractive from a cost standpoint, because the added complexity to incorporate a PUF subsystem is low potentially simplifying security protocols; however this could limit the transmission data rate.

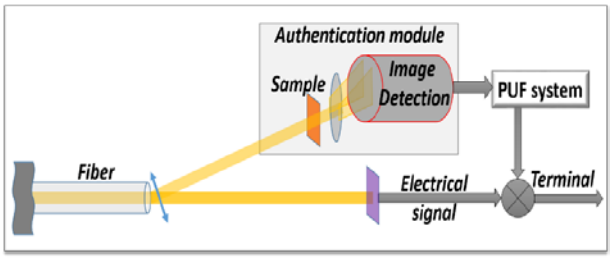


Figure 8. Possible configuration with a separate authentication module.

An alternative architecture, as shown on Fig. 8, is to divert the light coming from the fiber into a separate branch dedicated to security. We see this solution as a good way to develop the PUF technology while keeping the communication route un-touched, with the possibility to develop the integrated solution later.

4- Generation of CRPs

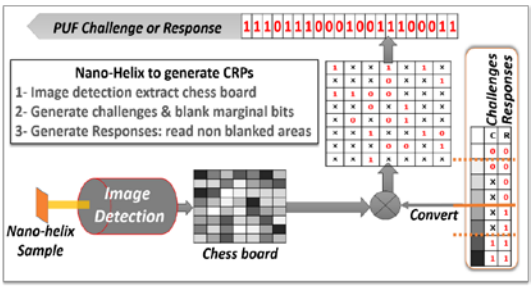


Figure 9. "Chessboard" analysis to generate CRPs.

An example of so called "chessboard" analysis to generate CRPs is shown in Fig. 9. As explained in §4.1 and §4.2, the method to generate challenges differs, from the method to generate responses, however in both cases the level of light transmission through the Nanostructure is the critically differentiating parameter between 0's and 1's.The light cells represent the locations where the Nano-helices do not block the light and are thus converted into 0's, while the dark cells show where the Nano-helices do block the light and are converted into '"'s. In order to reduce CRP error rates, the cells that are neither very light nor very dark are blanked during the challenge generation process, and are ignored during the response generation process [43].

4.1 Challenge generation process

The challenges are usually generated once by the PUF subsystem, and stored by the server as shown in Fig. 2. A method to generate challenges with ternary states has been documented as an effective way to eliminate transitional cells, [44-45], as shown in Fig. 10. The parameter to determine if a challenge is a 0 or a 1 is the "gradient of gray" as measured by the image detector. What is referred as gradient of gray is intended to be a generic term representing variations in transmission of light out of the optical fiber.

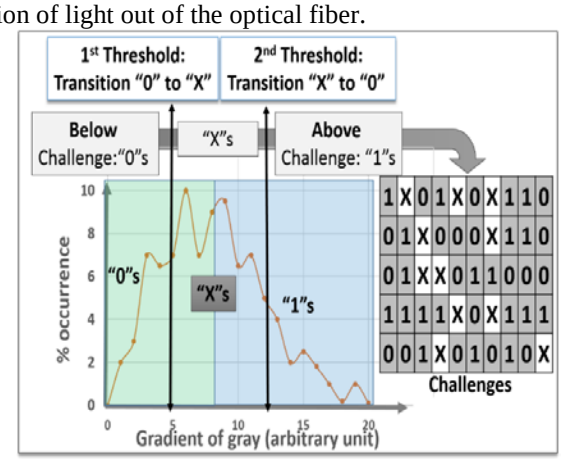


Figure 10. Challenge generation with ternary states.

Considering that commercial fiber-optic communications operate in the infrared range, from 800nm to 1550nm, which is outside the visible spectrum, the intensity of the light transmitted is a relative parameter detectable by the image sensor. The image sensors can sense variations in the transmission of a Nanomaterial with clusters of Nano-Helices that, due to natural manufacturing variations, create random patterns exploitable to generate PUF CRPs. During challenge generation, the position of the blanked "X" cells are kept in a non-volatile memory, while the binary stream of data is sent to the server as the reference Challenge. Both the mapping of the X's and the challenges can be encrypted to enhance security.

4.2 The Response generation process.

The responses are generated similar to the challenges, as shown in Fig. 11. The fiber illuminates the same sample in similar conditions to create a chessboard with several gradients of gray. Only the cell previously used to generate the binary stream of bits for the challenges are considered for response generations, while the blanked cells are ignored. When the blanking is wide enough, the likelihood that a previously tested 0 flips to become a 1 is reduced, and vice versa for 1's becoming 0's, thereby reducing CRP error rates.

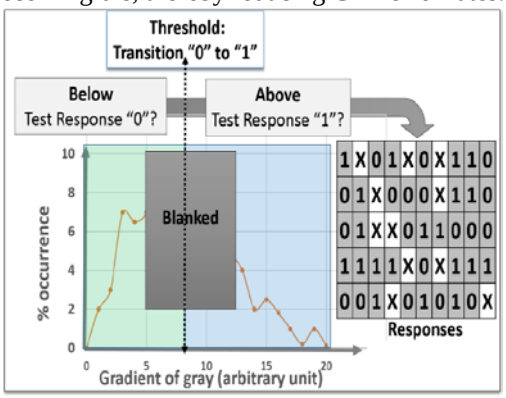


Figure 11. Response generation.

4.3 Authentication algorithms.

An example of authentication was presented in Fig.2, and the algorithm is shown in Fig. 12. To start the authentication process the server sends a challenge (encrypted) to the PUF subsystem, while illuminating the Nanostructure for the response generation process.

- Step-1: the PUF subsystem extracts the raw chessboard pattern from the illuminated Nanostructure. The

gradients of gray are measured only for the non-blanked cells. As presented in § 4.2, a light gradient of gray generates a 0, and dark generates a 1.

- Step-2: the resulting binary data stream of responses in then prepared for authentication and stored in a buffer memory.
- Step-3: the challenges provided by the server are also stored in a buffer memory.
- Step-4: the challenge-response-pairs (CRP) are compared, yielding a Hamming distance between the challenges and the responses.
- Step-5: positive authentication is to be granted when the rate of matching pairs is statistically high enough. Weak PUFs produce high CRP error rates even from the same PUF, creating false rejections.

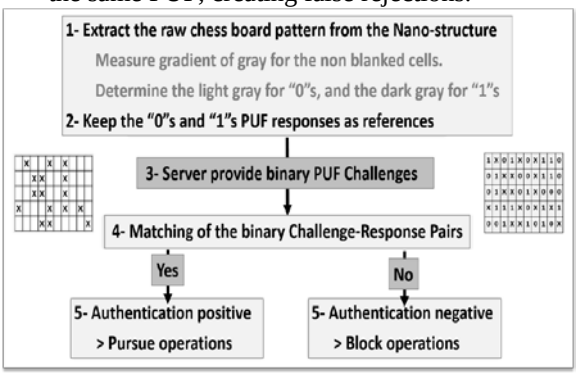


Figure 12: authentication algorithm.

Other important criteria to judge the quality of a PUF are the length of the CRPs, and the robustness of the responses with respect to temperature and voltage, electromagnetic interferences, aging, and other factors. There is an expectation of randomness and uniqueness that should make PUFs hard to extract and identify for unwelcomed users but easy to use for secure authentication. Ways to enhance the Nano-helix based PUFs include the optimization of the manufacturing parameters, image detection technology, CRP generation algorithms, error detection, and authentication methods.

5- System integration

The overall circuitry surrounding the PUF subsystem is not described in detail in this paper because it uses known components, and can vary for different system integration:

- The image detection module and conversion to a chessboard can be driven by a standard Digital Signal Processor (DSP). The DSP can convert the chessboard to a digital chessboard with the gradient of gray measured on each cell.
- A standard secure element includes a crypto-processor, a risk microprocessor, and embedded non-volatile memory. It can directly analyze the digitalized chessboard from the DSP. This secure element can be programmed to communicate with the secure server, generate encrypted challenges, read encrypted challenges from the server, generate responses, and final authentication.
- Eventually a custom ASIC can be designed to integrate the DSP and the secure element into a single component.

The protection of the data circulating though fiber-optic cables is an important topic that has been the subject of prior publications [10-11] in which cryptographic keys and PUFs are inserted after the photodetector, beyond the transmission and reception of the light circulation within the cable. The important aspect addressed in the current paper is to provide PUF authentication at the point of entry of a site communicating via fiber-optics with a secure server prior to the photodetector and receiving circuitry. The Nanomaterials can be inserted into the cable while the image detectors can be located within the receiving board. The Nano-Helix PUF can be inserted anywhere in the cable and, if necessary, at multiple locations. This opens the following examples of functionality (see Fig. 3):

- The secure server can recognized the site N-1 as a valid site through the correct PUF responses. Thereby the terminal can get services, download documents, files, and other software products.
- The server can verify the party transmitting information is site N-1 by sending an authentication challenge before accepting the information.
- The operating system running the computing system of site N-1 can accept running new software products and upgrades from the secure server only if these new software products were downloaded with the correct PUF challenges. This is intended to block malware ability to get in the secure server and to contaminate site N-1.

Industrial and governmental institutions that could take advantage of such a firewall infrastructure include providers of wired communication infrastructure, interconnected CPSs, networked IoTs, multi-site institutions with critical security needs, and content providers wishing to control the delivery of services and products.

Cost considerations: Nanomaterials are produced by using equipment and processes compatible with the microelectronics industry. Wafers can produce tens of thousands of samples with an extremely low cost structure. Others components that are part of the systems described in this paper, such as image detectors, DSPs, and secure elements are also mainstream, low cost, and commercially available. The integration of these components to build the system is novel and is expected to benefit from continuous improvement and further cost reductions.

CONCLUSION and FUTURE WORK

In this paper we did a step-by-step study on the ways to build an effective firewall with Nano-helix PUFs within commercial fiber-optic cables. GLAD can be used to manufacture partially transparent samples that include clusters of uniquely random Nano-helices. Commercially available image detectors can convert the transmitted patterns into digital chessboards that can generate challenge-response pairs. The ternary state method is a way to reduce CRP error rates for trusted authentication. The expected future work will be related to the following three areas:

- Design of experiments to optimize the Nanostructure fabrication. The objective is to increase the clarity of the transmitted image, its contrast to create clear 0s and 1s, and unclonability.
- Optimization of the authentication module, image detector, DSP, secure element, and embedded coding. The objective is to develop a fully integrated system ready for commercialization.

- End-to-end system optimization, protocol of communication between the secure server and the terminal. Enhancement of the cybersecurity of the system to transfer data and secure files.

In summary, firewalls based on Nano-helix PUFs have the potential to drastically enhance the security of connected cyber physical systems at low cost. This development is still at an early stage for commercial deployment; however, we do not see at this point in time any obvious showstopper.

REFERENCES

[1] David. Naccache and Patrice. Frémanteau; Aug. 1992; Unforgeable identification device, identification device reader and method of identification; *Patent US5434917*.

[2] Ravikanth Pappu, Ben. Recht, Jason Taylor, and Neil Gershenfield; 20 Sept 2002; Physical one-way functions; *Science. Vol 297 No5589 pp2026-2030*.

[3] Pravin Prabhu, Ameen Akel, Laura M. Grupp, Wing-Kei S. Yu, G. Edward Suh, Edwin Kan, and Steven Swanson; June 2011; Extracting Device Fingerprints from Flash Memory by Exploiting Physical Variations; *4th international conference on Trust and trustworthy computing*.

[4] Daniel E. Holcomb, Wayne P. Burleson, Kevin Fu; Nov 2008; Power-up SRAM state as an Identifying Fingerprint and Source of True Random Numbers; *IEEE Transactions on Computers, vol 57, No 11*.

[5] Todd A. Christensen, John E Sheets II; Oct. 30, 2012; Implementing Physically Unclonable Function (PUF) utilizing EDRAM memory cell capacitance variation*; Patent No.: US 8,300,450 B2;Assignee IBM.*.

[6] Xiaochun Zhu, Steven Millendorf, Xu Guo, David M. Jacobson, Kangho Lee, Seung H. Kang, Matthew M. Nowak, Daha Fazla; March 2015; PUF based on resistivity of magnetoresistive RAM magnetic tunnel junctions; *Patents. US 2015/0071432 A1*.

[7] Elena I. Vatajelu, Giorgio Di Natale, Mario Barbareschi, Lionel Torres, Marco Indaco, and Paolo Prinetto; July 2015; STT-MRAM-Based PUF Architecture exploiting Magnetic Tunnel Junction Fabrication-Induced Variability; *ACM transactions*.

[8] C.L. Rutledge; Method and apparatus for secure optical links; *US patent No:5,864,625; Jan 1999*.

[9] C.R. Murphy, and all; Intrusion resistant passive fiber optic components; *US patent application No:US2007/0113268 A1; May 2007* .

[10] L.B. Aronson; Anti-counterfeiting means for optical communication components; *US patent application No: US2009/0240945 A1; Sept 2009*.

[11] B. Meyer; System and method for secure transmission of data; *US patent application No:US2014/0189374A1; Jul 2014*.

[12] F. Hussain, M. Hojjati, M. Okamoto, and R. E. Gorga, Journal of composite materials **40**, 1511 (2006).

[13] F. Caruso, R. A. Caruso, and H. Möhwald, Science **282**, 1111 (1998).

[14] F. Caruso, Advanced Materials **13**, 11 (2001).

[15] B. Sepúlveda, P. C. Angelomé, L. M. Lechuga, and L. M. Liz-Marzán, Nano Today **4**, 244 (2009).

[16] V. Wagner, A. Dullaart, A.-K. Bock, and A. Zweck, Nature biotechnology **24**, 1211 (2006).

[17] W. Hol, P. T. Van Duijnen, and H. Berendsen, Nature **273**, 443 (1978).

[18] M. Blaber, X.-J. Zhang, and B. W. Matthews, Science **260**, 1637 (1993).

[19] J. M. Scholtz and R. L. Baldwin, Annual review of biophysics and biomolecular structure **21**, 95 (1992).

[20] F. Crick, Nature **248**, 766 (1974).

[21] H. Nakano, H. Takeda, Y. Kitamura, H. Mimaki, and J. Yamauchi, Antennas and Propagation, IEEE Transactions on **40**, 279 (1992).

[22] K. Robbie and M. Brett, Journal of Vacuum Science & Technology A **15**, 1460 (1997).

[23] A. G. Mark, J. G. Gibbs, T.-C. Lee, and P. Fischer, Nature materials **12**, 802 (2013).

[24] G. Nair, J. H. Singh, and A. Ghosh, Journal of Materials Chemistry C (2015).

[25] S. Eslami, J. G. Gibbs, Y. Rechkemmer, J. van Slageren, M. Alarcón-Correa, T.-C. Lee, A. G. Mark, G. L. Rikken, and P. Fischer, ACS Photonics (2014).

[26] S. Link, Z. L. Wang, and M. El-Sayed, The Journal of Physical Chemistry B **103**, 3529 (1999).

[27] S. Link, M. Mohamed, and M. El-Sayed, The Journal of Physical Chemistry B **103**, 3073 (1999).

[28] J. G. Gibbs, A. G. Mark, T.-C. Lee, S. Eslami, D. Schamel, and P. Fischer, Nanoscale **6**, 9457 (2014).

[29] Y.-P. Zhao, D.-X. Ye, G.-C. Wang, and T.-M. Lu, Nano Letters **2**, 351 (2002).

[30] J. Gibbs, A. Mark, S. Eslami, and P. Fischer, Applied Physics Letters **103**, 213101 (2013).

[31] M. M. Hawkeye and M. J. Brett, Journal of Vacuum Science & Technology A **25**, 1317 (2007).

[32] C. de Julián Fernández *et al.*, Sensors and Actuators B: Chemical **111**, 225 (2005).

[33] F. Croce, G. Appetecchi, L. Persi, and B. Scrosati, Nature **394**, 456 (1998).

[34] J. Homola, S. S. Yee, and G. Gauglitz, Sensors and Actuators B: Chemical **54**, 3 (1999).

[35] C. Sönnichsen and A. P. Alivisatos, Nano letters **5**, 301 (2005).

[36] K.-S. Lee and M. A. El-Sayed, The Journal of Physical Chemistry B **110**, 19220 (2006).

[37] K. A. Willets and R. P. Van Duyne, Annu. Rev. Phys. Chem. **58**, 267 (2007).

[38] L. Sun, W. Luan, S.-t. Tu, and Y. J. Shan, Nano Biomedicine and Engineering **3**, 232 (2011).

[39] V. Amendola, S. Scaramuzza, S. Agnoli, S. Polizzi, and M. Meneghetti, Nanoscale **6**, 1423 (2014).

[40] Z. Pirzadeh, T. Pakizeh, V. Miljkovic, C. Langhammer, and A. Dmitriev, ACS Photonics **1**, 158 (2014).

[41] P. K. Jain, W. Huang, and M. A. El-Sayed, Nano Letters **7**, 2080 (2007)

[42] P. Clark; Quantum-Dot Image Sensor Launch Threatens Silico; *EETimes Europe, Nov. 2015.*

[43] J. Gibbs, B.Cambou; Firewall apparatus with Nano-material PUFs for fiber optic communication; *prov. patent application NAU case No 16-016; Oct. 2015.*

[44] B. Cambou; Physically Unclonable Function Generating Systems and Related Methods; *US Patent application No. 62204912; August 2015.*

[45] D. Yamamoto, K. Sakiyama, K. Ohto, and Masahiko Itoh; 2011; Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches; *Cryptographic Hardware and Embedded Systems – CHES 2011 Lecture Notes in Computer Science Volume 6917, pp 390-406.*