Fighting Fake Goods: How Optical PUFs Provide New Approaches to Anti-Counterfeiting

pufin.id

Fighting Fake Goods: How Optical PUFs Provide New Approaches to Anti-Counterfeiting

The fake goods market continues to grow, costing industries billions in revenue and putting consumer safety at risk. Traditional solutions are generally ineffective against counterfeiting. But an emerging technology safeguards brand trust

TABLE OF CONTENTS

Introduction

In 2019, fake goods accounted for 3.3 percent of global trade, costing industries billions in lost revenue. Meanwhile counterfeit products, like food, alcohol or medicines, often contain toxic substances, putting consumer health and safety at serious risk.

Traditional anti-counterfeiting measures, such as serialization, are not effective enough to combat the rising trend of the fake market. Today's manufacturing capabilities enable counterfeiters to copy these methods and pass off fake goods as legitimate.

To prevent counterfeiting, brands must give products copy-proof unique identifiers, which can trace physical items throughout the entire supply chain. In addition, the solution must be cost-effective and easy to implement on pre-existing hardware, such as a smartphone.

Physical Unclonable Functions (PUFs) offer a reliable option, as they consist of disordered patterns so complex, they are impossible to duplicate, even by the original manufacturer.

Like a fingerprint, physical items receive unique identifiers paired with a digital hash-code. Linking physical items with a digital ID creates a "biometrics of things", an integrated solution to the growing issue with fake goods. At any point in the supply chain, consumers, distributors, retailers and even third party users can validate a product using the scan of a smartphone.

Brands can use optical PUFs as a low-cost method to authenticate an exact product throughout its entire lifecycle using a common smartphone. This whitepaper explores the challenges of traditional anti-counterfeiting methods, and how optical PUFs can better meet the demands of product protection.

Traditional Approaches to Anti-Counterfeiting

Traditional anti-counterfeiting measures fall short because they can be easily copied and passed off as legitimate.

Product authentication requires an identifier, a physical feature that allows validation of a product throughout the entire supply chain. Traditionally, brands use serialization features that are difficult to recreate, such as a QR Code, barcode, data matrix code or RFID, to validate and authenticate a physical item.

However, with today's manufacturing capabilities, counterfeiters have found ways to copy these methods like holograms, special inks, challenging printing techniques and even DNA tags and pass off fake goods as legitimate.

To fully protect products against forgery, brands must use identifiers that are impossible to copy. Identifiers must be unique to each product, as in the FDA mandated serialization of medicine. The technology must be independent of all links in the supply chain and allow the end user or a trusted point-of-sale to perform independent and secure validation of product authenticity.

Each product receives a unique identifier, a physical feature applied directly to the packaging. Then a digital twin of this "unique identifier" is created. Connecting the physical product to a digital twin completes the missing link in the supply chain. Operations in the physical world are tracked in the digital world via the unique identifier of an object, and digital transactions between objects in the physical world can be authenticated using the link between the unique identifier and a corresponding digital ID.

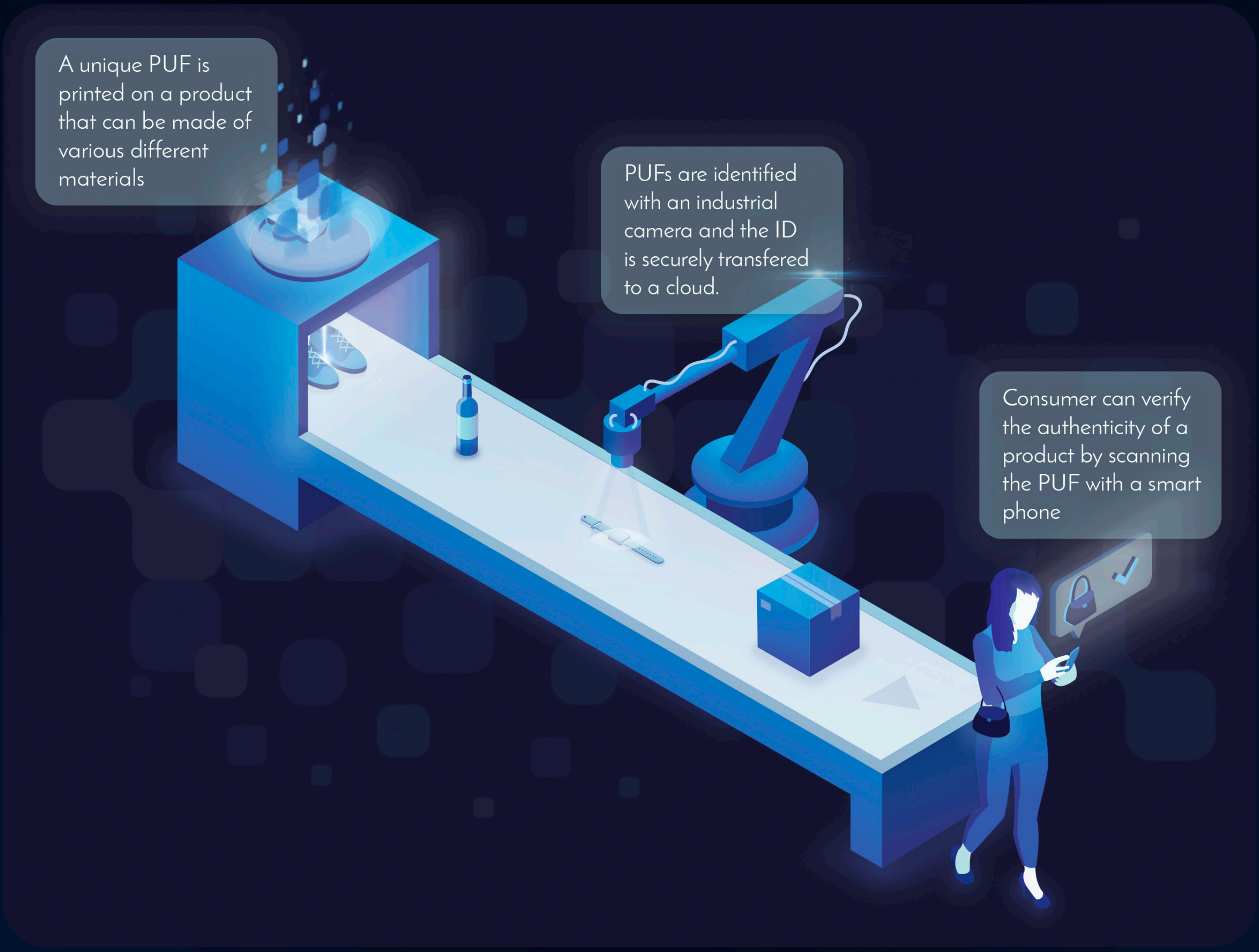
The best example of a unique identifier is a fingerprint. Yet, security researchers have found that even criminals with the right material can spoof fingerprints. The reading and validation of fingerprints are very complex, which is why simple systems typically only allow a low number of attempts of validation. The chance of a false positive is too high for multiple attempts to be made. Further, creating a digital identity based on complex fingerprints is not readily achieved.

A Personal Identification Number is a very simple, yet secure, unique identifier that directly translates into a digital ID. The 4-digit PIN has a very limited capacity with only 9999 unique identifiers, eliminating the chances of false positives if individual keypresses are incorrectly recorded. However, typical credit card systems only allow for three wrong attempts for validation, as the chance of guessing or "brute-forcing" the correct digital ID becomes too high.

In order for a unique identifier to effectively prevent counterfeiting, it will need to meet the following criteria:

- ✓ Copy-proof
- ✓ Zero chance of false positives
- ✓ High capacity
- ✓ Trusted path of software dissemination
- ✓ End-user authentication
- ✓ Validation using readily available resources

Even with the perfect physical unique identifier, there are still unsolved issues in creating a digital ID from the physical unique identifier of the objects. Here, the inherent limitations in linking a physical unique identifier to a digital ID is explored for a system for decentralized validation of authenticity based in Physical Unclonable Functions (PUFs).


A unique PUF is printed on a product that can be made of various different materials
PUFs are identified with an industrial camera and the ID is securely transfered to a cloud.
Consumer can verify the authenticity of a product by scanning the PUF with a smart phone

Introduction to Physical Unclonable Functions

Physical Unclonable Functions (PUFs) consist of complex, disordered patterns that make them impossible to duplicate, even by the original manufacturer. When applied to the material of a product, brands can use PUFs to identify an exact product throughout its entire lifecycle.

PUFs Application in Electronics

While PUFs have recently emerged in the optical authentication of goods, their application has been investigated in detail in electronics. Providing effective anti-counterfeiting solutions within an open authentication systems requires the following demands from PUFs in electronics:

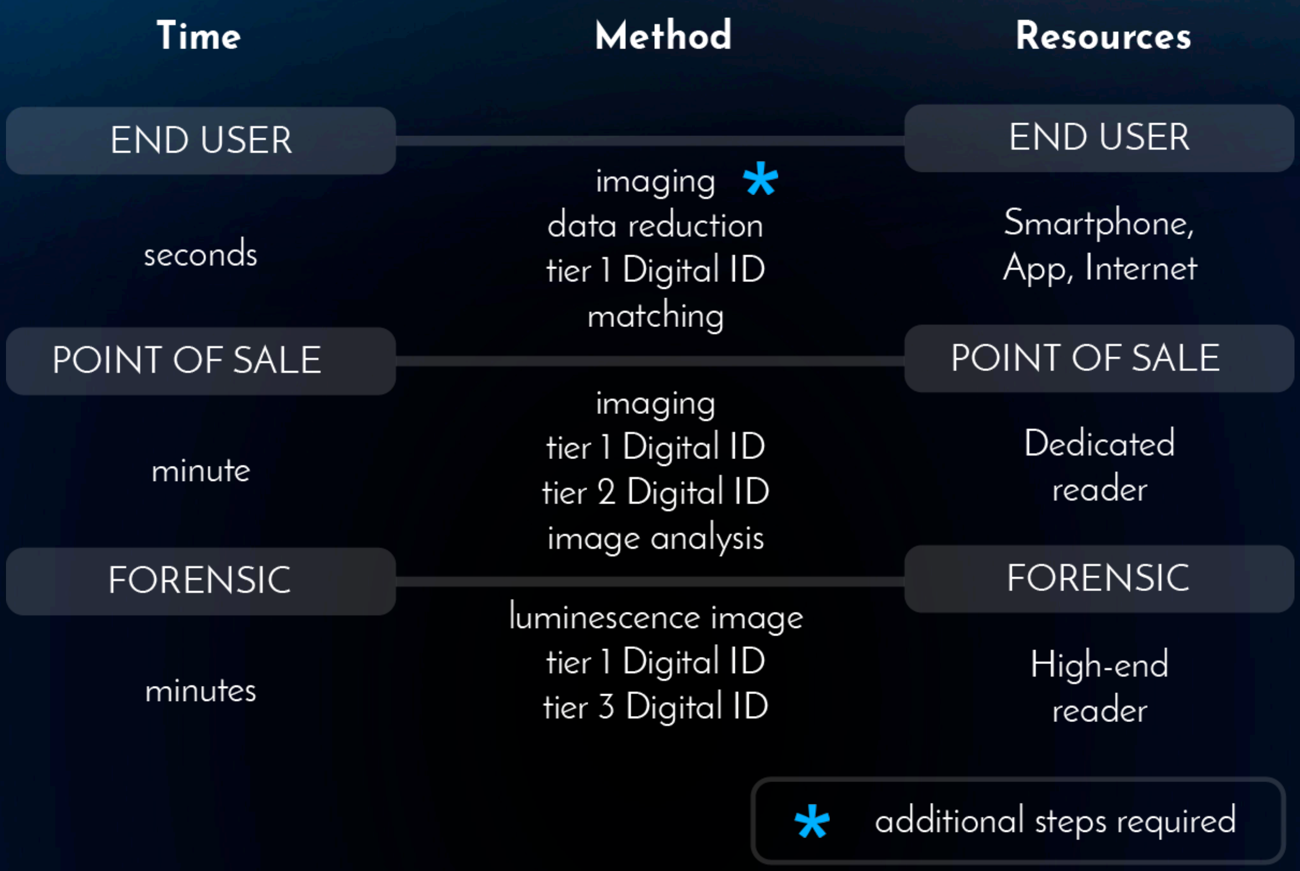
Cost: Brands require cost-effective object identification in which PUFs cost under $0.10 per physical identifier

Accessibility: The system must operate on low cost, accessible hardware, such as a standard smartphone. These demands are given by the problem: ensuring the validity of mass market products such as individual medical devices, packages of medicine, machine parts and similar at the end user.

Copy-proof: Any electronic signal is readily copied—consider the ability of modern smartphones to replicate the RFID tag commonly used in credit cards. Human fingerprints have the same problem, as often illustrated in fiction where latent fingerprints are copied. While a copy of the PUF cannot be created, the output—the measurement used in the authentication, is readily generated. To solve the problem requires an authentication system that only involves and enables two parties, the manufacturer and the end user.

The Three-Tiers of Optical Authentication

Several levels of authentication are available in a single Pufin ID Physical Unclonable Function (see Figure 1). At each level of authentication, a unique identifier and a digital ID is generated from a single physical item.



Time	Method	Resources
END USER		END USER
seconds	imaging * data reduction tier 1 Digital ID matching	Smartphone, App, Internet
POINT OF SALE		POINT OF SALE
minute	imaging tier 1 Digital ID tier 2 Digital ID image analysis	Dedicated reader
FORENSIC		FORENSIC
minutes	luminescence image tier 1 Digital ID tier 3 Digital ID	High-end reader

* additional steps required

Figure 1. *The three-tier optical authentication system is based on PUFs, their derived unique identifiers, corresponding digital identities and the resources required to operate the system.*

The higher levels offer ideal solutions for point-of-sale or forensic use. Identification takes minutes and requires specialized, often expensive hardware, such as a trusted point-of-sale or trusted distributor, to verify an object with its digital twin.

Tier 1 optical authentication offers a better method for product verification as it processes almost instantly and doesn't require pricey hardware. An end user at any point in the supply chain can scan the object identifier to make sure that it matches the digital version to validate the product as genuine.

Users can verify an object in seconds using a low-magnification lens and a common smartphone. The magnification is required to resolve the PUF, which is a random pattern of microparticles. At this tier, optical PUFs offer a level of security sufficient for most mass market products.

Tier 1 optical authentication process works as follows (see Figure 2 below):

1. A physical unclonable function is generated on the product.
2. The manufacturer registers all the unique identifiers from the PUFs storing them as digital IDs of an authentic product in a secure registry,
3. The end user reads the PUF using a smartphone. The client based software converts the read to a digital ID, queries the registry and reports whether the product is authentic or counterfeit.

The process consists of four main components (see Figure 2 below):

A. The tangible components of the authentication system at the site of product manufacture and with the end user including the IT infrastructure

B. The individual components of the minimum viable authentication system

C. The information flow needed from the initial registration of a product to end user validation

D. The different domains of digital and physical unique identifiers

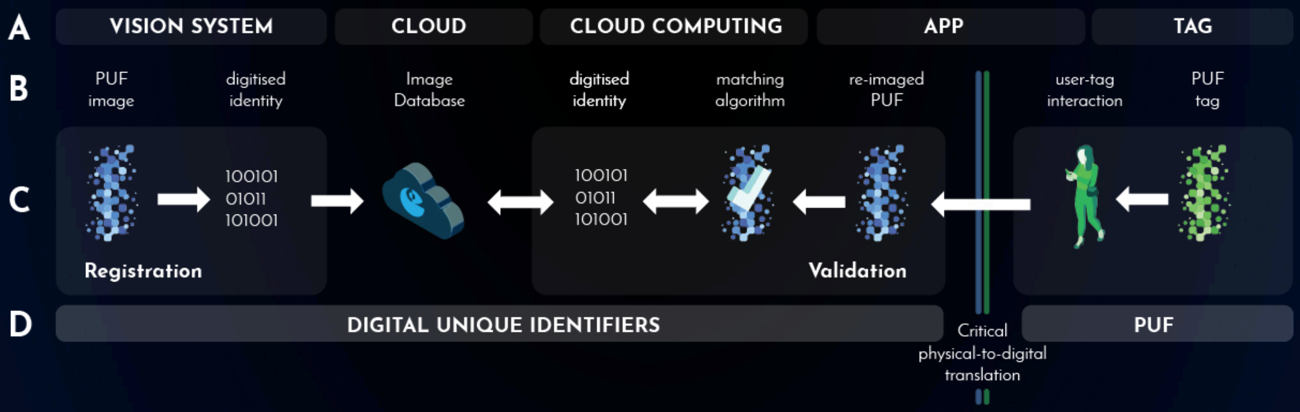
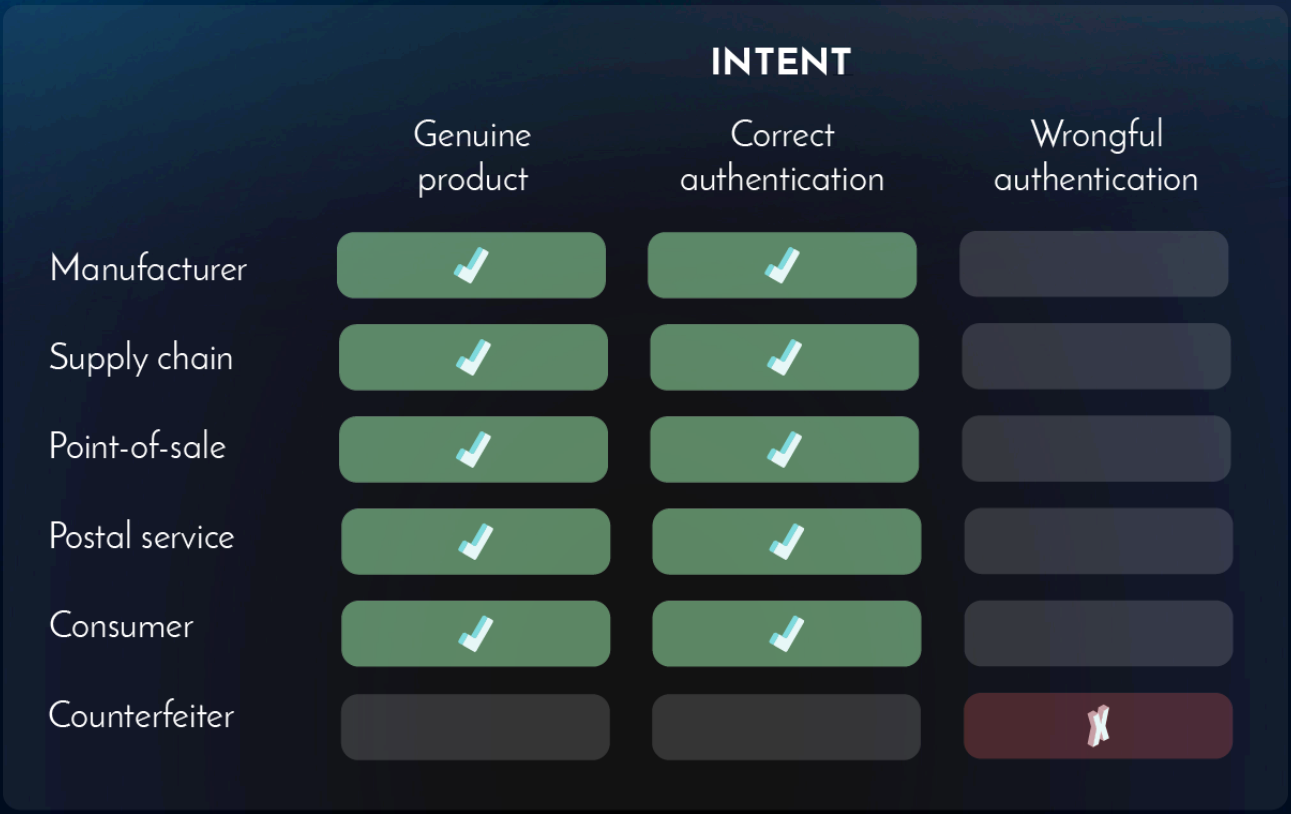


Figure 2. *Optical authentication system based on PUFs, their derived unique identifiers and corresponding digital identities.*

The Tier 1 authentication system creates a direct link from manufacturer and end user, thus bypassing potential tampering from counterfeiters. However, the system implies that all internal parties intend to supply and consume genuine articles and that only the counterfeiter has malicious intent (see Table 1).



	INTENT		
	Genuine product	Correct authentication	Wrongful authentication
Manufacturer	✓	✓	
Supply chain	✓	✓	
Point-of-sale	✓	✓	
Postal service	✓	✓	
Consumer	✓	✓	
Counterfeiter			✗

Table 1. *Parties and the intent of parties involved in manufacturing and distributing goods.*

A decentralized anti-counterfeiting system relies on the intent of both manufacturer and end user. This enables any PUF based solution, as there is no desire to make false validations at these points of the system. Thus, the translation from unique Physical Unclonable Function to digital ID ensures brand trust, and an operational anti-counterfeiting system does not have to include active countermeasures against fraudulent authentication attempts.

Conclusion

Traditional anti-counterfeiting methods depend on decentralized validation of physical unique identifiers. This creates vulnerabilities in a supply chain in which counterfeiters can easily copy identifiers using modern manufacturing capabilities.

Optical PUFs provide a different approach to anti-counterfeiting that matches a unique identifier against its digital ID. Products receive copy-proof unique identifiers, impossible to clone. Authentication doesn't require specialized hardware, and consumers, distributors, retailers and third party users can validate a product with its digital hash code in seconds using a smartphone. Brands can use optical PUFs as a low-cost method to authenticate an exact product throughout its entire lifecycle.

References

Aldhous, P. (2005). Counterfeit pharmaceuticals: Murder by medicine. Nature, 434(7030), 132-136. Retrieved from http://dx.doi.org/10.1038/434132a

Andrews, M., Jones, J. E., Harding, L. P., & Pope, S. J. (2011). Luminescent probes based on water-soluble, dual-emissive lanthanide complexes: metal ion-induced modulation of near-IR emission. Chem Commun (Camb), 47(1), 206-208. doi:10.1039/c0cc00210k

Arppe-Tabbara, R., Tabbara, M., & Sørensen, T. J. (2019). Versatile and Validated Optical Authentication System Based on Physical Unclonable Functions. ACS Applied Materials & Interfaces, 11(6), 6475-6482. doi:10.1021/acsami.8b17403

Arppe, R., & Sørensen, T. J. (2017). Physical unclonable functions generated through chemical methods for anti-counterfeiting. Nature Reviews Chemistry, 1(4), 31. doi:UNSP 0031 10.1038/s41570-017-0031

Boseley, S. (2019). WHO warns of fake cancer drug made from paracetamol The Guardian.

Buchanan, J. D., Cowburn, R. P., Jausovec, A. V., Petit, D., Seem, P., Xiong, G., . . . Bryan, M. T. (2005). Forgery: 'fingerprinting' documents and packaging. Nature, 436(7050), 475. doi:10.1038/436475a

Burzurí, E., Granados, D., & Pérez, E. M. (2019). Physically Unclonable Functions Based on Single-Walled Carbon Nanotubes: A Scalable and Inexpensive Method toward Unique Identifiers. ACS Applied Nano Materials, 2(4), 1796-1801. doi:10.1021/acsanm.9b00322

Carro-Temboury, M. R., Arppe, R., Vosch, T., & Sørensen, T. J. (2018). An optical authentication system based on imaging of excitation-selected lanthanide luminescence. Science Advances, 4(1), e1701384. doi:10.1126/sciadv.1701384

Cowburn, R. (2008). Laser surface authentication – reading Nature's own security code. Contemporary Physics, 49(5), 331-342. doi:10.1080/00107510802583948

Fake Goods Represent 3.3 Percent of Global Trade (2019). Supply and Demand Chain Executive.

FDA. (2016, 05/25/2016). Counterfeit Medicine. Retrieved from http://www.fda.gov/Drugs/ResourcesForYou/Consumers/BuyingUsingMedicin eSafely/CounterfeitMedicine/default.htm

Gao, Z., Han, Y., & Wang, F. (2018). Cooperative supramolecular polymers with anthracene-endoperoxide photo-switching for fluorescent anti-counterfeiting. Nature Communications, 9(1), 3977. doi:10.1038/s41467-018-06392-x

Geng, Y., Noh, J., Drevensek-Olenik, I., Rupp, R., Lenzini, G., & Lagerwall, J. P. (2016). High-fidelity spherical cholesteric liquid crystal Bragg reflectors generating unclonable patterns for secure authentication. Sci Rep, 6, 26840. doi:10.1038/srep26840

Haist, T., & Tiziani, H. J. (1998). Optical detection of random features for high security applications. Optics Communications, 147(1-3), 173-179. doi:10.1016/s0030-4018(97)00546-4

Herder, C., Yu, M.-D., Koushanfar, F., & Devadas, S. (2014). Physical Unclonable Functions and Applications: A Tutorial. Proceedings of the IEEE, 102(8), 1126-1141. doi:10.1109/jproc.2014.2320516

Herder, C., Yu, M., Koushanfar, F., & Devadas, S. (2014). Physical Unclonable Functions and Applications: A Tutorial. Proceedings of the IEEE, 102(8), 1126-1141. doi:10.1109/JPROC.2014.2320516

Horstmeyer, R., Judkewitz, B., Vellekoop, I. M., Assawaworrarit, S., & Yang, C. (2013).Physicalkey-protectedone-timepad. SciRep,3, 3543. doi:10.1038/srep03543

Hu, Z., Comeras, J. M., Park, H., Tang, J., Afzali, A., Tulevski, G. S., . . . Han, S. J. (2016). Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. Nat Nanotechnol, 11(6), 559-565. doi:10.1038/nnano.2016.1

Lehtonen, M., Oertel, N., & Vogt, H. (2007, 4-6 June 2007). Features, identity, tracing, and cryptography in product authentication. Paper presented at the 2007 IEEE International Technology Management Conference (ICE).

Liu, Y., Han, F., Li, F., Zhao, Y., Chen, M., Xu, Z., . . . Qian, L. (2019). Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication. Nature Communications, 10(1), 2409. doi:10.1038/s41467-019-10406-7

Maes, R. (2013). Physically Unclonable Functions.

McGrath, T., Bagci, I. E., Wang, Z. M., Roedig, U., & Young, R. J. (2019). A PUF taxonomy. Applied Physics Reviews, 6(1). doi:10.1063/1.5079407

Mehta, D., Zhou, L., Aono, K., & Chakrabartty, S. (2018, 5-8 Aug. 2018). Self-powered Sensing and Time-Stamping of Tampering Events. Paper presented at the 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS).

Nayyar, G. M. L., Breman, J. G., Mackey, T. K., Clark, J. P., Hajjou, M., Littrell, M., & Herrington, J. E. (2019). Falsified and Substandard Drugs: Stopping the Pandemic. doi:https://doi.org/10.4269/ajtmh.18-0981

Newton, P. N., Green, M. D., Fernández, F. M., Day, N. P. J., & White, N. J. (2006). Counterfeit anti-infective drugs. The Lancet Infectious Diseases, 6(9), 602-613. doi:http://dx.doi.org/10.1016/S1473-3099(06)70581-3

Pappu, R., Recht, B., Taylor, J., & Gershenfeld, N. (2002). Physical one-way functions. Science, 297(5589), 2026-2030. doi:10.1126/science.1074376

Sample, I. (2019). Fake drugs kill more than 250,000 children a year, doctors warn The Guardian.

Sheridan, C. (2007). Bad medicine. Nature Biotech., 25(7), 707-709. Retrieved from http://dx.doi.org/10.1038/nbt0707-707

Suh, G. E., & Devadas, S. (2007, 4-8 June 2007). Physical Unclonable Functions for Device Authentication and Secret Key Generation. Paper presented at the 2007 44th ACM/IEEE Design Automation Conference.

Takahashi, T., Kudo, Y., & Ishiyama, R. (2017). Mass-produced Parts Traceability System Based on Automated Scanning of "Fingerprint of Things". Paper presented at the Fifteenth IAPR International Conference on Machine Vision Applications (MVA), Nagoya University, Nagoya, Japan.

Wigger, B., Meissner, T., Forste, A., Jetter, V., & Zimmermann, A. (2018). Using unique surface patterns of injection moulded plastic components as an image based Physical Unclonable Function for secure component identification. Sci Rep, 8(1), 4738. doi:10.1038/s41598-018-22876-8

Wu, B.-H., Zhang, C., Zheng, N., Wu, L.-W., Xu, Z.-K., & Wan, L.-S. (2019). Grain Boundaries of Self-Assembled Porous Polymer Films for Unclonable Anti-Counterfeiting. ACS Applied Polymer Materials, 1(1), 47-53. doi:10.1021/acsapm.8b00031

Yuan, J., Christensen, P. R., & Wolf, M. O. (2019). Dynamic anti-counterfeiting security features using multicolor dianthryl sulfoxides. Chemical Science, 10(43), 10113-10121. doi:10.1039/C9SC03948A

pufin.id

Today's manufacturing capabilities combined with AI-technology enable unrivaled anti-counterfeit protection throughout the entire product lifespan. Visit **www.pufin.id** to learn more.