Photonic Physically Unclonable Function for the Quantum Era

Tech ID: 34662 / UC Case 2026-397-0

ABSTRACT

Researchers at the University of California, Davis have developed a photonic device that generates unique, unclonable cryptographic keys using light scattering and advanced photodetection for enhanced hardware security.

FULL DESCRIPTION

Current cybersecurity measures are vulnerable to advanced threats, including artificial intelligence-driven attacks and emerging quantum computing capabilities that could break traditional encryption. Furthermore, existing hardware security methods, such as static random-access memory physically unclonable functions (SRAM PUFs), remain vulnerable to environmental sensitivity, aging effects, and side-channel attacks. To address these vulnerabilities, this technology utilizes a light source to emit light into a random optical medium that scatters the light in unpredictable ways. A photodetector with photon-trapping surface textures captures this scattered light, generating an electrical signal that a processor converts into unique, physically unclonable cryptographic keys, one-of-a-kind patterns, much like a digital fingerprint. Because this 'fingerprint' is created by tiny, random variations in the manufacturing process, no two devices are ever the same. Incorporating artificial intelligence to dynamically optimize input parameters and enhance entropy, the system ensures high security and robustness against cyberattacks, environmental variations, and quantum computing threats.

APPLICATIONS

- Secure cryptographic key generation for IoT devices, mobile phones, and embedded systems.
- Authentication and anti-counterfeiting for semiconductor chips and hardware components.
- Resilient hardware security modules (HSMs) in financial and governmental sectors.
- Quantum-resistant security solutions for cloud computing and data centers.
- Secure communication protocols in automotive, aerospace, and defense industries.
- Supply chain security through unclonable device fingerprinting and tamper detection.
- Next-generation cryptographic random number generators for cybersecurity and other cloud (NFT, cryptocurrency, etc.) products.
- Secure communication and operational protocols for autonomous vehicles (V2X communication) to ensure unbreachable navigation systems.
- Enhanced hardware security for biometric systems, including facial recognition and other safety features.

FEATURES/BENEFITS

CONTACT

Andrew M. Van Court
amvancourt@ucdavis.edu
tel: .

INVENTORS

- Ahamed, Ahasan
- Islam, M. Saif
- Rawat, Amita

OTHER INFORMATION

KEYWORDS

AI-based control, avalanche photodiode, challenge-response protocol, cryptographic key generation, physically unclonable function, photon-trapping surface textures, quantum random number, random optical medium, semiconductor photodetector, security hardware

CATEGORIZED AS

- Generates true random and unclonable cryptographic keys leveraging dynamic light scattering.
- Enhances signal quality and reliability by increasing light detection with photon-trapping photodetector surfaces.
- The same system is also engineered to generate unclonable yet repeatable functions for digital fingerprint.
- Mitigates quantum computing threats by utilizing photon's quantum properties for authentic, true random number generation.
- Incorporates artificial intelligence to dynamically optimize parameters and correct errors to ensure robust performance against environmental variations and device aging.
- Operates at high frequencies (1 GHz to 100 or more GHz) to ensure rapid cryptographic bit generation rates, capturing quantum shot noise for authentic randomness.
- Enables multi-state key generation and dynamic power signatures, rendering side-channel and differential power analysis attacks ineffective.
- Supports flexible security deployments by utilizing diverse photodetector technologies and configurable parameters.
- Provides real-time tamper detection and security alerts through transient event monitoring.
- Prevents cloning and prediction of cryptographic keys vulnerable to One-Time-Programmable (OPT) PUF and Static Randon Access Memory (SRAM) PUF methods.
- Closes security gaps caused by environmental sensitivity, device aging, and side-channel attacks in hardware-secured systems.
- Mitigates quantum computing threats by generating quantum-enabled true random numbers and unique identifiers.
- Eliminates vulnerabilities related to static key generation by supporting dynamic, AI-driven key regeneration and adaptation.
- Detects and reports hardware tampering and transient security breaches in real time.

- **Optics and Photonics**
  - All Optics and Photonics
- **Computer**
  - Security
- **Security and Defense**
  - Cyber security

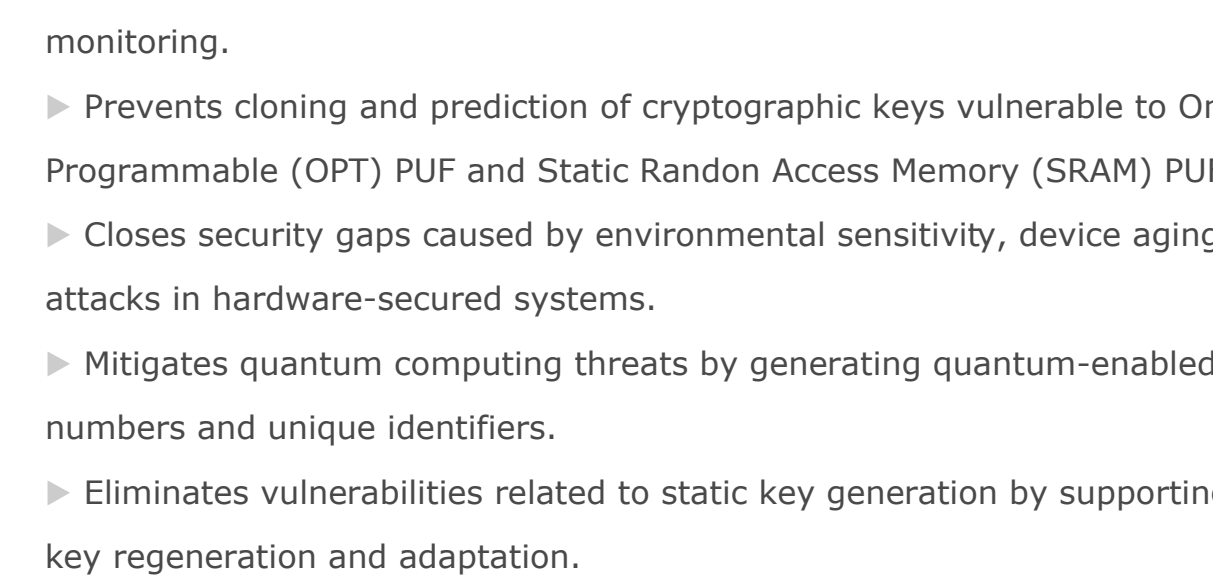
RELATED CASES

2026-397-0

PATENT STATUS

Patent Pending

OTHER INFORMATION



ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

▶ Photonic Physically Unclonable Function for True Random Number Generation and Biometric ID for Hardware Security Applications

University of California, Davis
Technology Transfer Office
1 Shields Avenue, Mrak Hall 4th Floor,
Davis,CA 95616

Tel:
530.754.8649
techtransfer@ucdavis.edu
https://research.ucdavis.edu/technology-transfer/
Fax:
530.754.7620