Security layers for neuromorphic photonic accelerators

openaccessgovernment.org/article/security-layers-for-neuromorphic-photonic-accelerators/195061

Emily Warrender July 3, 2025

Fabio Pavanello and co-authors discuss the importance of security layers in computer systems, particularly in the context of the Horizon Europe NEUROPULS project, which focuses on innovative security solutions based on novel neuromorphic architectures and PUF-based security layers

Security layers are critical to protecting computer systems from threats. They often rely on cryptographic protocols that use secret keys, which are typically stored in memory. However, storing such sensitive data in non-volatile digital memory can pose risks, especially if exploited through hardware vulnerabilities. To address this, the Horizon Europe NEUROPULS project is exploring novel solutions based on integrated photonics

Security layers are critical to protecting computer systems from threats. They often rely on cryptographic protocols that use secret keys, which are typically stored in memory. However, storing such sensitive data in non-volatile digital memory can pose risks, especially if exploited through hardware vulnerabilities. To address this, the Horizon Europe NEUROPULS project is exploring novel solutions based on integrated photonics.

Physical unclonable functions are robust hardware primitives One promising approach is the use of Physical Unclonable Functions (PUFs) – hardware elements that generate secure responses only when needed, removing the need for memory storage. Unlike software-based generators, PUFs derive their strength from physical randomness introduced during the manufacturing process. This makes them hard to duplicate or predict – ideal traits for building secure systems.

Integrated photonics, a key technology for next-generation low-power accelerators, also offers new possibilities for PUFs. Light signals, sensitive to tiny variations in manufacturing, can be harnessed for high-entropy, CMOS-compatible security features. Photonic PUFs could also resist Machine Learning and side-channel attacks more effectively than current solutions.

Simulating security with gem5

The integration of photonic PUFs into the gem5 simulator represents an important opportunity for advancing hardware security research. Given gem5's modular architecture and its capability to simulate complex system architectures, it provides an ideal platform for modeling the unique characteristics of photonic PUFs, including their challenge-response mechanisms. By leveraging gem5's flexible framework, researchers can model the interaction between photonic components and conventional computing elements in terms of timing and power consumption, particularly important for simulating the integration of these PUFs with CMOS-compatible platforms, such as RISC-V.

Looking forward, integrating photonic PUF models into gem5 could be aligned with TPM standards, providing a comprehensive security simulation environment. The TPM's standardized approach to hardware-based security features could serve as a blueprint for implementing photonic PUF functionality within the simulator. This integration would be particularly valuable as it would allow researchers to simulate how photonic PUFs could enhance existing TPM capabilities.

Security protocols and services leveraging PUFs

In NEUROPULS, PUFs are used to deliver a series of services to the photonic accelerator under development. They encompass low-level services, such as key generation and data encryption, as well as high-level protocols, including authentication and software attestation. These security services and protocols leverage PUFs as the root of trust to secure the photonic accelerator, including not only the hardware components (e.g., with authentication) but also the software running on it, for instance, with the possibility to attest that the accelerator only runs firmware and apps that are authentic and not tampered with.

Current challenges

Despite their promise, widespread adoption of photonic PUFs faces hurdles:

1. Co-integration with photonic accelerators –
   Photonic PUFs should seamlessly co-integrate with photonic accelerators to ensure their security without compromising computing flows in terms of energy consumption, latency, or adding excessive hardware constraints that affect overall footprint and costs.
2. ML modeling –
   Photonic circuits often operate in a linear regime. However, to achieve complex behavior in photonic PUFs, optical non-linearities shall be exploited. To trigger such non-linearities, large optical powers, fast time scales, etc., shall be accessed, which imposes tight hardware constraints to address.
3. Photonic PUFs system integration –
   Photonic PUFs shall not only provide a series of properties but also be suitable for integration in real-world computing systems where noise, ambient fluctuations, etc., are present. Besides, their access should be straightforward from a high-level operating system point where security protocols can easily access PUF responses.

Ongoing research

NEUROPULS tackles these challenges by:

- Investigating techniques to co-integrate the photonic accelerator under development with photonic PUFs, leveraging the required hardware for the photonic accelerator operation.

- Developing PUF designs that can be more resilient to ML attacks, e.g., investigating the introduction of non-linearities at different stages of the interrogation flow, but also by coupling photonic and electronic PUFs together.
- Developing security protocols supported by accurate simulation frameworks fully considering photonic PUFs operation flow within a computing system, as well as their performance in terms of, e.g., higher response rate generation (Gbit/s) and reduced latency (~ ns) compared to purely electronic approaches.

By leveraging the novel technologies developed in NEUROPULS, photonic PUFs can become an attractive alternative, enabling real-scenario security layers with higher strength against common attack vectors while offering seamless integration with photonic accelerators.

This project has received funding from the European Union's HORIZON 2020 Research and Innovation programme under the Grant Agreement no. 101070238

Primary Contributor

Fabio Pavanello
University of Savoie Mont-Blanc

Additional Contributor(s)

Ricardo Chaves
INESC-ID

Mariano Ceccato
University of Verona

Alessandro Savino
Polytechnic of Turin

Cedric Marchand
Ecole Centrale de Lyon

Jean-Pierre Seifert
TU Berlin

Ioana Vatajelu
University of Grenoble Alpes