Ring resonator networks as physical unclonable keys
Lars van der Hoeven,1 Matthias C. Velsink,1,* Daan Stellinga,1 Pepijn W.H. Pinkse1
1Faculty of Science & Technology, University of Twente, Drienerloostraat 5, 7522NB, Enschede, NL
2ARCNL, Science Park 106, 1098XG, Amsterdam, NL
Email: d.p.stellinga@utwente.nl

Abstract: We propose an integrated network of ring resonators on a silicon-nitride chip for use as an all-optical single-spatial-mode physical unclonable key, enabling secret-free optical authentication with standard communication channels such as telecom fibres. © 2022 The Author(s)

1. Introduction
Authentication has always been an essential aspect of data security and will continue to be so in the future. The first proposed and arguably most well-known quantum cryptography protocol, quantum key distribution (QKD) [4], is known to rely on the use of an additional authentication method to prevent impersonation attacks [5]. However, well-known cryptography methods such as RSA, elliptic curve cryptography (ECC), and Diffie-Hellman key exchange [1–3] rely on digital keys that are susceptible to untraceable key theft attacks. To provide authenticated channels as well as ensure secure communication, a physical encryption layer has been proposed that relies on the combination of wavefront shaping methods [6] with physical unclonable keys (PUKs) [7]. PUKs rely on the uniqueness of a complex physical structure for security, making recreation of the key near-impossible even with full knowledge of its characteristics. In optics, such a ‘key’ often consists of a scattering medium with unclonable scattering characteristics.

Every optical PUK has a unique set of wavefront shaping phase patterns that can be used to produce a focus in one of two chosen spatial locations after the PUK. This allows for binary communication where the receiving party is intrinsically authenticated [8]. This method is called PUK enabled asymmetric communication (PEAC) [9]. Although functional, the method has a noteworthy drawback. Diffraction makes long-distance transmission of spatially shaped wavefronts difficult in free space. Transmitting these wavefronts through optical fibers is also impractical due to the unstable transmission characteristics of the required multi-mode fibers. To overcome this limitation and enable optical PUK usage over longer distances we demonstrate an alternative class of optical PUKs based on integrated ring-resonator networks operating in the spectral domain with only a single spatial input mode.

2. Integrated PUKs
Our PUK design consists of a network of ring resonators. These networks are chains of individual unit cells that consist of two waveguides connected by two serially coupled ring resonators, as can be seen in figure 1B. Any network made up from such unit cells possesses two input facets and two output facets. A unit cell on its own allows for certain frequencies of light to resonate in the rings and cross from one waveguide to the other [11]. Before forming a chain of unit cells, the nominal lengths of the ring resonators (2 mm) in every unit cell are randomized to a small degree (1%) in a pair-wise fashion, leading to a large variation of resonant characteristics in a chain of such unit cells. This introduces intricate frequency dependent behaviour and effectively scrambles incoming signals in time.

In order for these networks to be considered true PUKs they not only have to scramble an incoming signal in time but they also have to be unclonable. This means that it must be impossible to produce a device that shares a network’s specific time scrambling characteristics. In an attempt to produce a copy, an attacker has two options to consider. One option is to produce a sufficiently precise and efficient spectral shaper [10]. Such a device can shape the phase of an incoming signal allowing an attacker to mimic the effect of the PUK, given a high enough resolution and bandwidth to reproduce the PUK spectrum. However, to reproduce the spectral response of the devices considered here with such a spectral shaper would likely result in high losses, making low intensity signals an effective defense against this type of attack.

Another method of cloning is to directly produce a device that is an exact copy of the original PUK design. In such a copy attempt, the inherent randomness introduced during manufacturing must be small enough to produce a network with the same optical properties. To show that this is unfeasible with current state-of-the-art fabrication technology, PUK ring resonator networks were produced consisting of 1, 13, and 46 unit cells alongside an identical copy of each on the same chip. This represents a best-case scenario for an attempt to copy a network. The photonic chips were manufactured using E-beam lithography in cooperation with LionIX using their TriPleX SiN waveguide platform. A microscope image of the 46-unit cell network in action can be seen in figure 1A.

To compare the transmission characteristics of the produced PUK networks with that of their copies, the throughput power spectra of these networks were studied using a Michelson interferometer. As an input, a pulsed laser source was used with a center wavelength of 800 nm and a bandwidth of 13 nm. A comparison of the power
spectra measured for the two 13-unit cell networks can be viewed in figure 1C. The comparison clearly shows that the two copies of a 13-unit cell network do not produce similar power spectra. The same result is true for the networks consisting of 46-unit cells. Using the Pearson correlation coefficient, the likeness of the network copies can be further quantified. Comparing the power spectra within the frequency range of the laser source yields a Pearson correlation coefficient of 0.37 and 0.17 for the 13-unit cell and 46-unit cell networks respectively. Thus a 13-unit cell network already only shows weak correlation with its copy. These results show that the inherent randomness introduced during manufacturing makes copying a PUK ring resonator system infeasible. The larger the system, the more critical the introduced randomness becomes.

3. Conclusion

Designing functional as well as practical physical unclonable key devices is essential to the development and eventual application of PUK based cryptography methods. Here, we have presented a new spectral-domain PUK design built on an integrated photonics platform using networks of ring-resonators. The new design is small, easy to integrate, and resilient against temperature fluctuations. We have experimentally demonstrated the capabilities of the new design with an investigation of the unclonability of the device.

4. References