JOM Journal of Optical Microsystems

RESEARCH PAPER

Integrated photonic cryptographic key generator using low-power MEMS-on-PIC technology

Martin Blasl,* **Meysam Namdari, Maximilian Wagner, and Jan Grahmann**
Fraunhofer Institute for Photonic Microsystems, Dresden, Germany

ABSTRACT. To improve data security and authentication, we designed and fabricated a cryptographic key generator based on a photonic integrated circuit that converts a digital input key into a digital output key by means of a physical unclonable function (PUF). The PUF is realized by an imperfect multi-mode interferometer controlled by low-power micro-electromechanical system (MEMS) phase shifters. An analytical model was derived and used to prove the randomness of the generated digital keys, and the model was validated by measurements of a first proof-of-concept demonstrator. The demonstrator was fabricated using a silicon nitride photonic integrated circuit (PIC) platform and our recently developed MEMS-on-PIC technology.

Keywords: key generator; photonic integrated circuit; micro-electromechanical systems; silicon nitride

Paper 24012G received May 6, 2024; revised Jul. 5, 2024; accepted Jul. 12, 2024; published Aug. 19, 2024.

1 Introduction

The security of digital information is becoming increasingly important. One approach to enhancing security in cryptographic applications is the use of physical unclonable functions (PUFs). A PUF is a hardware one-way function that is difficult to clone, duplicate, or predict. It produces unique, deterministic results referred to as the response to a certain input, known as the challenge. PUFs are used for identification, authentication, or encryption and can be realized in different physical domains,[1–3] for example, electric,[4,5] magnetic,[6,7] and photonic.[8–10]

For security applications, photonic PUFs are of particular interest because their higher complexity makes them less vulnerable to attack compared with electronic PUFs.[9] The first photonic PUF based on a free-space arrangement, in which a random interference pattern known as speckle is created when coherent light is scattered by the structure of an inhomogeneous medium (token).[11] From this speckle pattern, a digital key that is unique to the token and the beam parameters, such as the angle of incidence, is calculated. Speckle-based approaches remain of high interest and are under further development. Their low probability of cloning, high degree of robustness, and simplicity of production and readout have been demonstrated.[12]

To increase the level of system integration, recent developments utilize photonic integrated circuits (PICs).[13–20] For example, ultrashort pulses, which interact nonlinearly with microcavities to produce a complex, deterministic ultrafast response serving as a fingerprint, are used.[13] Alternatively, digital keys were calculated from the transmission spectrum of an integrated quasicrystal interferometer, in which distributed fabrication-induced imperfections render the digital keys unique.[14] Generating a large number of challenge-response pairs was demonstrated using reconfigurable Mach-Zehnder interferometer (MZI) networks controlled

*Address all correspondence to Martin Blasl, martin.blasl@ipms.fraunhofer.de by thermal phase shifters.[15] Other reconfigurable PUFs were based on tunable multi-mode interferometers (MMI)[16] or scattering slab waveguide regions.[17] Recently, randomly distributed holes in slab waveguide regions in which phase shifters are used to control the mode excitation state were proposed in theoretical work.[18] For the reconfigurable PUFs mentioned here, key generation is based on the optical power measured at the output of the photonic circuit. Using single photons instead of classical light, the authentication mechanism can be enhanced by a quantum readout protocol.[19]

To provide a key generator capable of producing a large number of random-like keys, we present an integrated variant of a speckle-based cryptographic key generator that incorporates low-power micro-electromechanical system (MEMS) phase shifters and a perturbed MMI. The key generator is fabricated using a silicon nitride (SiN) photonic platform and complementary metal-oxide-semiconductor (CMOS)-compatible processes.[21] The combination of the SiN photonic platform and MEMS phase shifters offers several significant advantages. First, SiN exhibits less temperature sensitivity compared with silicon (Si) due to its lower thermo-optic coefficient,[22] ensuring stable operation over varying temperatures. This is particularly beneficial for PUF applications that require consistent performance. Second, SiN's ability to utilize visible light enables higher integration density,[23] particularly in CMOS technologies, through the monolithic integration of photodetectors. In addition, the MEMS phase shifters, with their low power dissipation, small footprint, and negligible crosstalk, further increase the integration density.[24,25] Finally, a simple monochromatic continuous-wave laser source can be used, and the readout process is straightforward. In summary, these features make the key generator highly suitable for portable applications in which low power consumption and compactness are essential.

2 Cryptographic Key Generator

Figure 1 illustrates a free-space optics version of a cryptographic key generator in comparison with our integrated version. In free-space optics, monochromatic light from a laser is directed onto a diffusing plate. The light scattered by the plate creates a random interference pattern known as a speckle on the charge-coupled device (CCD) detector. The speckle pattern is unique to the scattering plate used. Varying the beam parameters, such as the angle of incidence or divergence, results in different speckle patterns. If an input key is associated with the beam

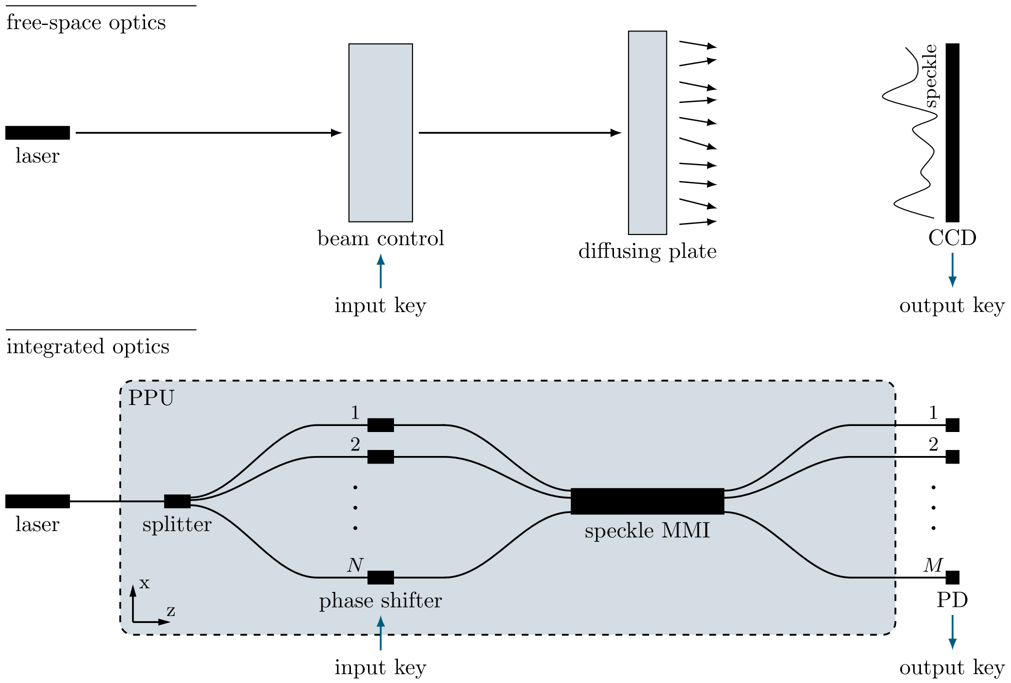

Fig. 1 Comparison between a free-space optics and an integrated optics version of a speckle-based key generator.

parameters and an output key is generated from the CCD signal, an unpredictable but deterministic conversion from the input key to the output key is performed.

In the integrated version, the light emitted by a laser is coupled into the photonic processing unit (PPU) and split into many waveguides. The light in each waveguide is controlled by an individual phase shifter, serving as a physical representation of the digital input key, before it enters an MMI. The MMI modes excited by the input waveguides propagate along the MMI and create an interference pattern at the output. Due to fabrication-induced imperfections or additional modifications to the MMI, the interference pattern becomes unique and unpredictable, similar to a speckle pattern. The MMI output is sampled by waveguides that transmit the light to the photodetectors. From the optical power detected by the photodetectors, a digital output key is generated.

Physically, the speckle MMI is the PUF that generates the challenge-response pairs, in which the optical state at the input is the challenge and the intensity distribution at the output is the response. From the system-side perspective, the challenge is the digital input key, and the response is the digital output key. Phase shifters and photodetectors convert signals between electrical and optical domains. To avoid confusion in distinguishing between physical and system considerations, the term input key or output key is used for the challenge or response related to the system.

3 Theory

To investigate the statistical behavior of the presented key generator, we used an analytical model. The MMI is considered to be a planar structure in the $x-z$ plane (see Fig. 1). The refractive index inside the buried MMI is approximated by the effective refractive index n_{eff} of the corresponding slab waveguide. The MMI modes are described by scalar fields propagating in the z direction.

3.1 Unperturbed MMI

To describe the behavior of the key generator, we start with the electric field propagating along the MMI, given as[26]

$$E(x,z)=\sum_{\nu}a_{\nu}\Psi_{\nu}(x)\mathrm{e}^{-\mathrm{i}\beta_{\nu}z}, \tag{1}$$

as a superposition of the excited MMI modes $\Psi_{\nu}(x)$. $\Psi_{\nu}(x)$ is the normalized electric field amplitude of the ν'th mode, given as

$$\beta_{\nu}=n_{\nu}\frac{2\pi}{\lambda_0}, \tag{2}$$

where the effective refractive is n_{ν} and the vacuum wavelength is λ_0, the corresponding propagation constant, and

$$a_{\nu}=\int_{-\infty}^{+\infty}\Psi_{\nu}^{*}(x)\Psi_{\mathrm{e}}(x)\mathrm{d}x, \tag{3}$$

which is the coupling coefficient between the ν'th MMI mode and the exciting field Ψ_e. Both, the MMI mode and the exciting field are normalized to $\int_{-\infty}^{+\infty}|\Psi(x)|^2\mathrm{d}x=1$.

3.2 Perturbed MMI

Due to naturally occurring or introduced imperfections in the waveguide layer, the varying effective refractive index of the MMI becomes a function of space as

$$\hat{n}_{\mathrm{eff}}(x,z)=n_{\mathrm{eff}}+\Delta n_{\mathrm{eff}}(x,z), \tag{4}$$

where n_{eff} is the effective refractive index of the undisturbed MMI waveguide layer. Assuming that the variations of the effective refractive index $\Delta n_{\mathrm{eff}}(x,z)$ are small and that the shapes of the modes are almost unaffected, we obtain from the relation[27]

$$\Delta n_{\nu}(z)=\int_{-\infty}^{+\infty}\Delta n_{\mathrm{eff}}(x,z)\Psi_{\nu}(x)\mathrm{d}x, \tag{5}$$

the propagation constant of the perturbed MMI

$$\hat{\beta}_\nu = \beta_\nu + \Delta\beta_\nu = \beta_\nu + \frac{2\pi}{\lambda_0}\int_{z=0}^{L} \Delta n_\nu(z)\mathrm{d}z, \tag{6}$$

where β_ν is the propagation constant of the unperturbed MMI belonging to n_{eff} and $\Delta\beta_\nu$ is understood as the phase contribution due to imperfections over the entire length L of the MMI.

3.3 Real MMI

The approximation of unperturbed mode functions neglects the coupling between MMI modes. In terms of mode expansion, this interaction may be considered to be a coupling $a_{\nu\nu'}$ of the modes Ψ_ν and $\Psi_{\nu'}$ between adjacent distinguishable cross sections. $\Delta\beta_\nu$ and $a_{\nu\nu'}$ are unique for each MMI and cause unpredictable interference. Due to the interaction of all modes between adjacent cross sections, the number of variables becomes very large and increases with the size of the MMI. Solving Maxwell's equations as an alternative to calculating light propagation precisely is also numerically very demanding.

3.4 MMI Mode Excitation

The MMI modes are excited by N waveguides at the input of the MMI. Assuming that the input waveguides transmit only their fundamental mode, the excitation field is described as

$$\Psi_{\mathrm{e}}(x) = \sum_n c_n \psi_n(x) \mathrm{e}^{\mathrm{i}(\delta_n + \kappa_n)}, \tag{7}$$

where ψ_n is the normalized fundamental mode of the n'th input waveguide, with $\int_{-\infty}^{+\infty}|\psi_n(x)|^2\mathrm{d}x = 1$. c_n is related to the power $p_n = |c_n|^2$ in each input waveguides, with $\sum_n p_n = 1$. For the same optical power in each waveguide, $c_n = 1/\sqrt{N}$. The phase of the input waveguide at the MMI depends on the phase differences δ_n due to different optical path lengths from the splitter to the MMI and the phase change κ_n controlled by the phase shifter.

3.5 MMI Sampling

The MMI is sampled by M waveguides at the output of the MMI. Assuming single mode waveguides, the proportion of the electric field at the MMI output $E(x, L)$ that is coupled into the fundamental mode $\psi_m(x)$ of the m'th output waveguide is

$$t_m = \int_{-\infty}^{+\infty} \psi_m^*(x) E(x, L)\mathrm{d}x. \tag{8}$$

As before, $\int_{-\infty}^{+\infty}|\psi_n(x)|^2\mathrm{d}x = 1$. With Eqs. (1), (3), (6), and (7), Eq. (8) is rewritten as

$$t_m = \sum_\nu \sum_n \underbrace{c_n \mathrm{e}^{\mathrm{i}(\delta_n + \kappa_n)}}_{k_n} \underbrace{\int_{-\infty}^{+\infty} \Psi_\nu^*(x)\psi_n(x)\mathrm{d}x}_{a_{n\nu}} \underbrace{\mathrm{e}^{-\mathrm{i}(\beta_\nu L + \Delta\beta_\nu)}}_{u_\nu} \underbrace{\int_{-\infty}^{+\infty} \psi_m^*(x)\Psi_\nu(x)\mathrm{d}x}_{a_{\nu m}} \tag{9}$$

$$= \sum_\nu \sum_n k_n a_{n\nu} u_\nu a_{\nu m}, \tag{10}$$

where $a_{n\nu}$ or $a_{\nu m}$ are the coupling coefficients between the MMI and the input waveguides or output waveguides. The input key resulting from the phase shifter and the excitation conditions is represented by k_n. The phase dependence of the MMI design and imperfections, denoted as u_ν, makes the MMI unique and unclonable.

3.6 Output Key Generation

In the case of linear detectors, the electrical output S_m of the m'th detector is proportional to the transmitted optical power, given as

$$S_m \propto T_m = |t_m|^2. \tag{11}$$

To estimate the probability of the occurrence of a certain output signal, we assumed the contribution of a large number of random phasors to the transmitted power with a uniform phase distribution in a range of $[-\pi;\pi]$. Under this condition, the output signal is approximately distributed according to an exponential probability density as[28]

$$p(S) \approx \frac{\mathrm{e}^{-S/S_{\mathrm{mean}}}}{S_{\mathrm{mean}}}, \tag{12}$$

where S_{mean} is the mean value of the signal.

To obtain a digital signal from S, a threshold above which the digit becomes 1 and below which it becomes 0 must be defined. To ensure that the probabilities of 1 and 0 are equally distributed, the median is a more appropriate threshold than the mean. According to the probability density of Eq. (12), the median of S is

$$S_{\mathrm{med}} = \ln(2) S_{\mathrm{mean}}. \tag{13}$$

Assuming a uniform distribution of the averaged optical power at the output of the MMI, the threshold is identical for each signal detector. The S_{med} can be either a constant value, previously determined by a large number of samples, or a variable value determined from the detector signals of the actual reading. The latter compensates for fluctuations in optical input power or wavelength dependencies in the transmission characteristics when using multiple wavelengths.

Figure 2 illustrates the principle of generating an output key from an input key. In this example, a 32-bit input key is used to control the phase in the 32 input waveguides. Neglecting phase differences due to path length differences ($\delta_n = 0$), the phase at the MMI input depends only on the phase shifter. For a zero bit, κ_n is 0, and for a one bit, κ_n is π. Equal power in the input waveguides is assumed. After the light has propagated along the MMI, an interference pattern is created at the output. The interference pattern is sampled by the output waveguides, resulting in

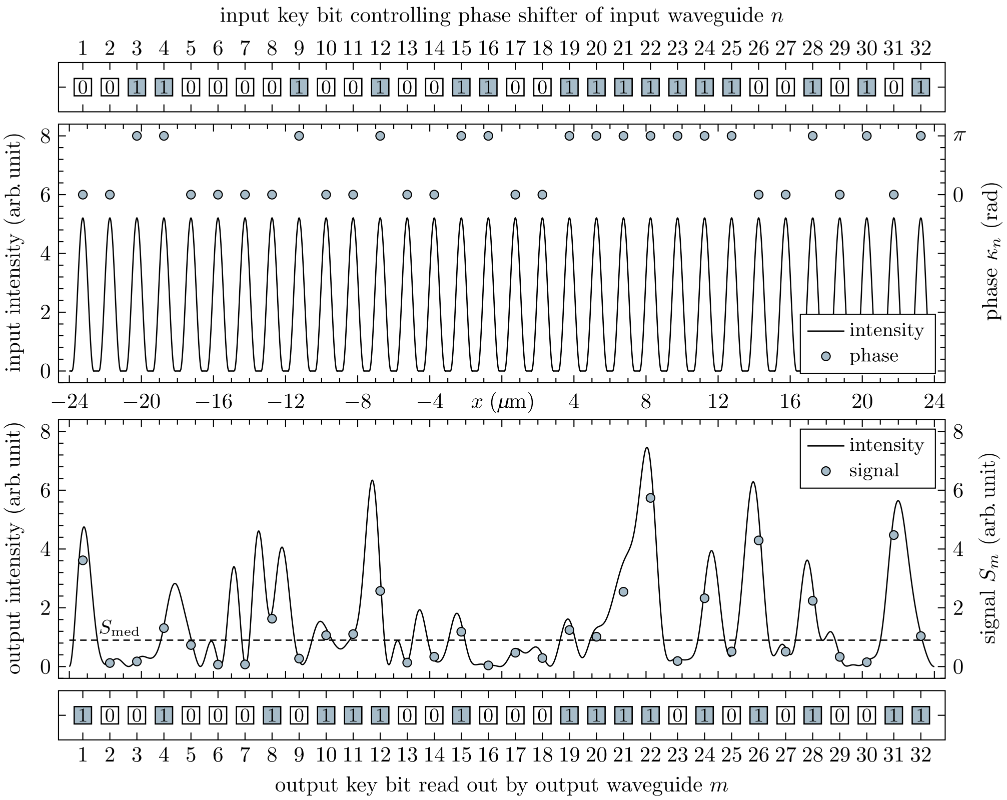

Fig. 2 Principle of the input key to output key conversion for a 32-bit key, according to Eq. (11) and Appendix A, for an MMI with a length of 2000 μm; a width of 48 μm; waveguide width and pitch of 1.2 μm and 1.4 μm, respectively; and a wavelength of $\lambda_0 = 1550$ nm. Equal optical power in the input waveguides as well as $\delta_n = 0$ and $\Delta\beta_\nu = 0$ were assumed, and S_{med} was obtained from 1024 samples.

the output signal S_m. With respect to the threshold value S_{med}, values above S_{med} are treated as one and values below S_{med} are treated as zero in the generated output key.

3.7 Output Key Statistics

To assess the quality of the output key, its statistical behavior is examined. For this purpose, the mean value of the individual bits of the key as well as the Hamming distances (see Appendix B) of the keys were considered.

Figure 3 shows the mean values of the individual bits of 10^5 perfectly random keys in comparison with those of the output keys. These output keys are derived from 10^5 random input keys. A mean value of 0.5 results from an equal probability of the two bit states, 0 and 1. For both the random keys and the output keys, the average over all bits is $\mu_{\mathrm{bit}} = 0.5$. Smaller fluctuations, as seen for the random keys, of approximately ± 0.005 result from the limited number of keys used for the calculation. The standard deviation over all bits is $\sigma_{\mathrm{bit}} = 0.0016$. Compared with the random keys, there are systematic deviations in the center and at the edges of the output key in the range of ± 0.01. This is due to the regularity of the excited modes of the unperturbed MMI. However, the related standard deviation of $\sigma_{\mathrm{bit}} = 0.0034$ represents an almost random behavior.

Figure 4(a) shows the probability distribution for the Hamming distances of the 128-bit output keys for random input keys. Random input keys result in a Gaussian distribution of the Hamming distance of the output key, with an expected value μ_r of 64 bit and a standard deviation

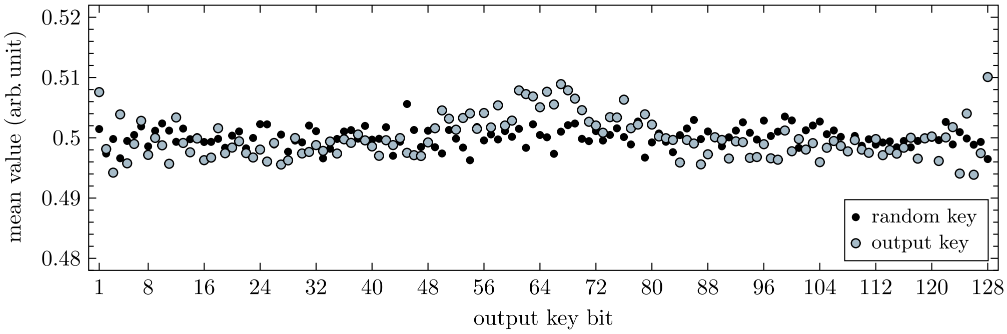

Fig. 3 Mean values of the individual bits of a 128-bit random key in comparison with those of the output key from the MMI, derived from 10^5 samples. Calculations correspond to those in Fig. 2, except for the MMI width of 192 μm, due to the higher number of input or output waveguides.

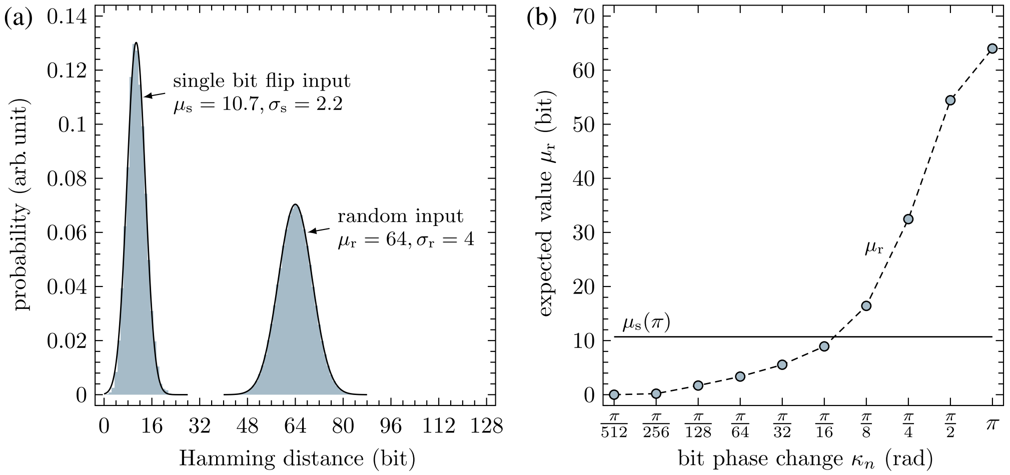

Fig. 4 (a) Hamming distance of the 128-bit output key for random input keys and input keys in which only a single bit is flipped with the phase change of the bit of π and (b) the expected value of the Hamming distance for random input μ_r in dependency of the bit phase change ϕ_c in comparison with the single bit flip expected value $\mu_s(\pi)$ for the bit phase change of π. Calculations correspond to those in Fig. 2, except for the MMI width of 192 μm, due to the higher number of input or output waveguides.

σ_r of 4 bit. This distribution indicates truly random output keys. This statistical behavior is essential for random-like keys and means that, on average, half of the bits of the output change for a different input key.

To get randomly distributed output keys, a phase change of an odd multiple of π is necessary, as shown in Fig. 4(b). For other values of κ_n in the interval of $[0; 2\pi]$, the Hamming distance decreases and becomes 0 at $\kappa_n = 0$ or $\kappa_n = 2\pi$ (not shown, results from periodicity).

Another important aspect that Fig. 4(b) provides is the sensitivity of the output key to the accuracy of the phase setting. For deviations in the phase lower than $\pi/16$, the expected error of the output key is lower than the impact of changing a single input bit [see Fig. 4(a)]. This means that, for a phase accuracy better than $\pi/16$, it is possible to distinguish, on average, between two different output keys even if only one bit of the input key has changed.

Finally, the security of the key generator against attacks, especially emulation, needs to be discussed. To this end, an attempt is made to create a model of the key generator based on a large number of input keys and corresponding output keys. As described in Sec. 3.3, the number of variables required to describe the scattering exactly is very large and increases with the size of the MMI. Although modeling the perturbed MMI is challenging, it is still feasible. To overcome this issue, nonlinearities have to be introduced into the system. The key-generating process, which converts the analogue signal to a digital value, serves as a primary source of nonlinearity that helps to obscure the underlying PUF. To introduce additional nonlinearities, the output key could be utilized in a secondary key-generating loop. This approach is the subject of current investigations using neural networks. Furthermore, as discussed in Ref. 19, the use of a quantum readout protocol is applicable.

The random-like distribution of the output keys, the practically realisable phase accuracy, and the challenges in emulating the key generation process indicate that this approach is promising for a reliable key generator.

4 Design and Fabrication

For the proof of concept, the fabrication of a 16-bit cryptographic key generator, shown in Fig. 5(a), was carried out within the development of the MEMS-on-PIC technology, presented in Ref. 29. The MEMS-on-PIC technology combines an oxide protective layer and an Si sacrificial layer, allowing MEMS functionality to be added subsequently, independent of the photonic material platform. SiN deposited by plasma-enhanced chemical vapour deposition was used to build the waveguide structures.

The key PPU of the key generator consists of a grating coupler array providing 1 input and 16 output waveguides, a 1 × 16 star coupler, 16 MEMS phase shifters, and a 2000 μm long by 170 μm wide MMI. The input and output waveguides are tapered to a width of 9 μm at the MMI. The waveguide pitch is 10 μm. The 1 × 16 star coupler provides a Gaussian power distribution $p_n = 0.45 \exp[(n-8)^2/16]$ at the input, so this influence on the characteristics of the key generator can be analyzed and compared with the theory. The optical path length difference between adjacent waveguides is approximately 50 μm, which allows the input phase to be varied widely

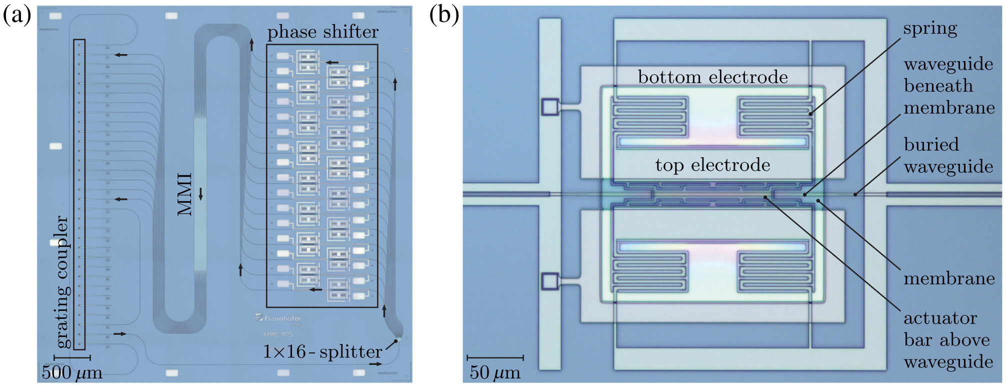

Fig. 5 (a) PPU of a 16-bit cryptographic key generator with (b) MEMS phase shifters fabricated with MEMS-on-PIC technology at Fraunhofer IPMS.

by changing the wavelength. The MMI does not have any additionally fabricated imperfections to evaluate the influence of natural variations.

The MEMS phase shifter shown in Fig. 5(b) and described in Ref. 30 comprises a waveguide beneath an electrostatically driven MEMS actuator. The effective refractive index of a waveguide is changed by varying the gap between the mechanical structure and the waveguide. Because of the fabrication of the PPU as part of the technology development, the gap is 1 μm, which causes pull-in effects and makes the individual adjustment of each phase shifter necessary for the first demonstration.

5 Characterization

The characterization is performed by coupling a swept laser source and 16 detectors to the PPU by means of a fiber array. The 16 detectors are read out simultaneously while the laser performs a wavelength sweep. As an example, Fig. 6 shows four of the 16 signals as a function of wavelength and the change in 2 signals due to the switching of various single phase shifters.

5.1 Wavelength Characteristics

Due to the optical path length differences of the input waveguides (see Sec. 4), the phase difference at the MMI input, given as

$$\delta_n \approx \frac{2\pi}{\lambda_0}(n-1)\cdot 50\ \mu\text{m}, \tag{14}$$

depends on the wavelength. For this reason, the change of the wavelength could be treated as a change of the input key. To compare the sensitivity of the output key toward a change in the wavelength, the Hamming distance of the output key as a function of the wavelength difference is calculated from the measured signals. For a higher amount of data for statistics, an averaging for multiple wavelengths was carried out.

As shown in Fig. 7, the Hamming distance increases with increasing wavelength differences $\Delta\lambda$. Calculations with the theoretical model discussed in Sec. 2 show that the slope for $\Delta\lambda$ close to 0 is dominated by the path length difference and that the trend for larger $\Delta\lambda$ is highly sensitive to the exact value of the optical path length differences δ_n. Considering that the theoretical

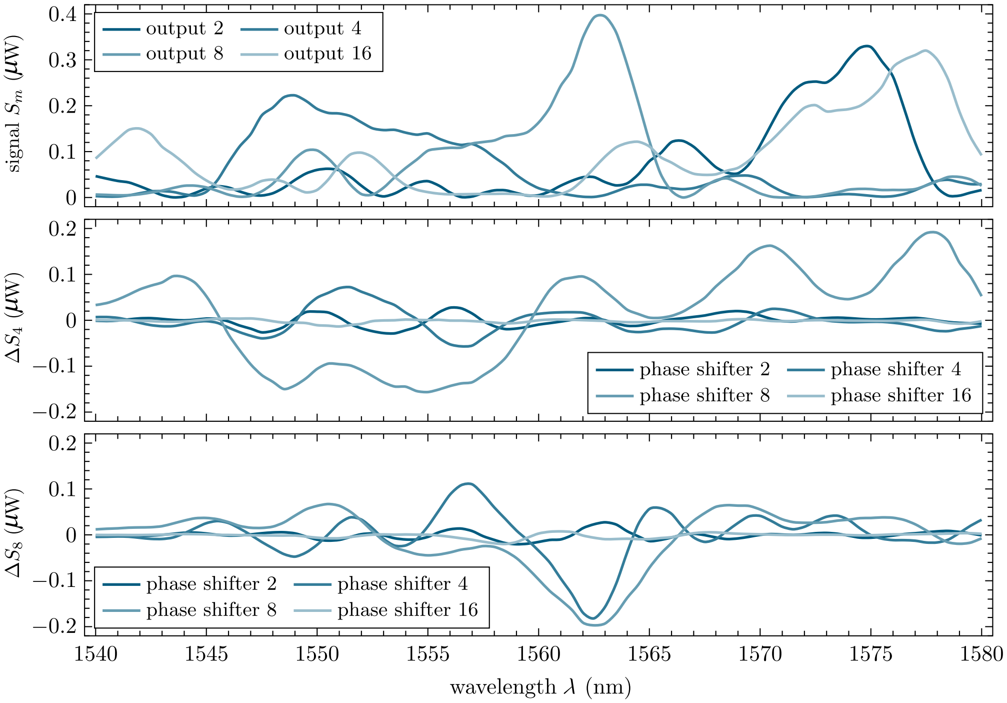

Fig. 6 Signals S_2, S_4, S_8, and S_{16} of the 16 detectors as a function of wavelength and the changes ΔS_4 and ΔS_8 due to switching different single phase shifters with $\kappa_n \approx \pi$.

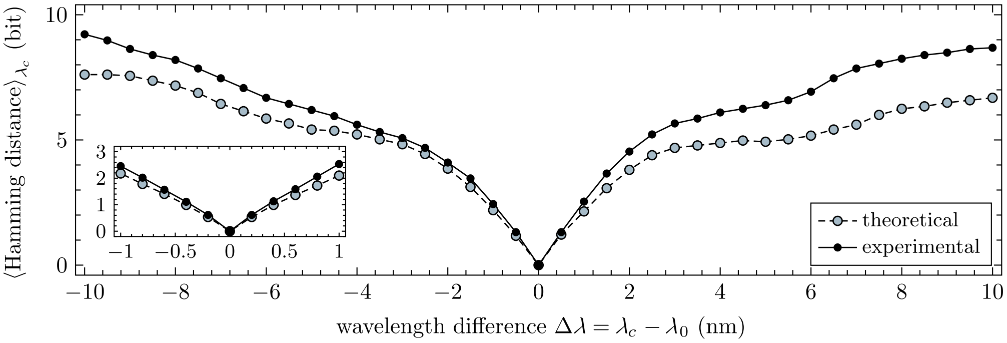

Fig. 7 Hamming distance as a function of wavelength difference $\Delta\lambda$, averaged over multiple central wavelengths λ_c in the range 1550 nm to 1570 nm.

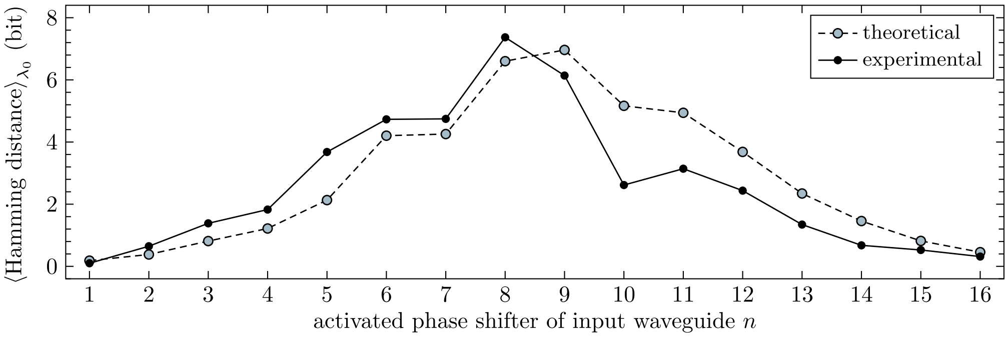

Fig. 8 Hamming distance due to switching of a single input phase shifter n with $\kappa_n \approx \pi$, averaged over the wavelength range 1540 nm to 1580 nm.

calculations are based on the analytic mode definitions from Appendix A, the measurement is in good agreement with the theoretical model. Due to the random-like variation of the phase, it may be expected that the Hamming distance for larger $\Delta\lambda$ converges more strictly to 8 bit. The theoretical investigation indicated that the tapered waveguides cause this behavior, and we found that the Hamming distance converges more strictly to 8 bit as the taper width decreases.

5.2 Single Bit Flip Characteristics

As described in Sec. 4, the MEMS phase shifters are not fully deployable due to the early stage of technology development. However, to perform an initial characterization, a single phase shifter was controlled and carefully set to a value close to π to measure the impact of a single bit flip at the input key on the output key. Again, averaging was performed over multiple wavelengths to generate a larger statistical data set.

The measured response of the output key to a single bit flip of the input key is shown in Fig. 8. A qualitatively good agreement with the theory is observed. Calculations using the theoretical model also show that the exact behavior is strongly dependent on the path length difference at the input of the MMI. However, both theory and measurement show the same correlation between the influence of the switched phase shifter on the Hamming distance and the optical power guided in the corresponding waveguide (see Sec. 4). For an equal distribution of power in the input waveguide, the theoretical calculation yields a Hamming distance of approximately 3.4 bit.

6 Conclusion

In this paper, we have presented the integrated version of a speckle-based cryptographic key generator. An analytical model was derived, and the statistical behavior of the generated output keys was studied. It has been shown that the individual bits of the 128-bit output key are almost random ($\sigma_{\mathrm{bit}} = 0.0034$) and the Hamming distances between the output keys indicate a truly random-like behavior ($\mu_{\mathrm{r}} = 64$). The sensitivity of the output keys to phase shifter errors was also investigated and found to be practically feasible. The analytical model was validated by measurements on a first proof-of-concept demonstrator. Close agreement between the simulation and measurement was observed.

7 Appendix A: MMI Modes

As a rough approximation, we assume that the optical field outside the MMI is zero. Therefore, the analytical solutions for the normalized scalar eigenmodes are

$$\Psi_\nu(x) = \sqrt{\frac{2}{W}} \cos\left(\frac{\pi\nu}{2} + x\sqrt{\beta_{\text{eff}}^2 - \beta_\nu^2}\right), \tag{15}$$

where ν is the mode number and W is the width of the MMI.

$$\beta_\nu = n_\nu \frac{2\pi}{\lambda_0} = \sqrt{\beta_{\text{eff}}^2 - \frac{\pi^2}{W^2}(1+\nu)^2} \tag{16}$$

is the propagation constant, and

$$\beta_{\text{eff}} = n_{\text{eff}} \frac{2\pi}{\lambda_0}, \tag{17}$$

where λ_0 is the vacuum wavelength. The normalization of the eigenmode in Eq. (15) yields $\int_{-\infty}^{+\infty} |\Psi_\nu(x)|^2 \mathrm{d}x = 1$.

For the assumption of the zero field outside the MMI, Eq. (16) gives the number of modes as

$$N_0 = \nu_{\max} + 1 = \text{int}\left(\frac{W}{\pi}\beta_{\text{eff}}\right). \tag{18}$$

The function $\text{int}(x)$ gives the integer part of x, and $\nu_{\max}$ is the highest mode number.

To consider the real condition regarding the refractive index of the surrounding medium n_s, the number of guided modes is[27]

$$N_\text{s} = \nu_{\max} + 1 = \text{int}\left(\frac{W}{\pi}\sqrt{\beta_{\text{eff}}^2 - \beta_\text{s}^2}\right) + 1, \tag{19}$$

with

$$\beta_\text{s} = n_\text{s} \frac{2\pi}{\lambda_0}. \tag{20}$$

For the calculations in this paper, we used the refractive index of silicon dioxide (SiO_2) with $n_\text{s} = 1.444$ and the effective refractive index of the 220 nm SiN slab waveguide with $n_{\text{eff}} = 1.604$ at the wavelength $\lambda_0 = 1550$ nm, and we neglected dispersion.

8 Appendix B: Hamming Distance

The Hamming distance is the number of positions for which two strings or vectors of the same length are different. For two bit vectors $\mathbf{b}_i$ and $\mathbf{b}_j$, the Hamming distance between them is

$$\text{HD}_{ij} = (\mathbf{b}_i - \mathbf{b}_j)^2. \tag{21}$$

Disclosures

The authors have no conflicts of interest.

Code and Data Availability

The data supporting the results of this study are available on request from the corresponding authors.

Acknowledgments

This work was funded by the German Federal Ministry of Education and Research (BMBF) as part of the project, VE-Silhouette (Grant No. 16ME0313K).

References

1. C. Herder et al., “Physical unclonable functions and applications: a tutorial,” *Proc. IEEE* **102**(8), 1126–1141 (2014).
2. Y. Gao, S. F. Al-Sarawi, and D. Abbott, “Physical unclonable functions,” *Nat. Electron.* **3**, 81–91 (2020).
3. H. Ning et al., “Physical unclonable function: architectures, applications and challenges for dependable security,” *IET Circuits Devices Syst.* **14**(4), 407–424 (2020).
4. M.-S. Kim et al., “Investigation of physically unclonable functions using flash memory for integrated circuit authentication,” *IEEE Trans. Nanotechnol.* **14**(2), 384–389 (2015).
5. M. R. Mahmoodi et al., “Ultra-low power physical unclonable function with nonlinear fixed-resistance crossbar circuits,” in *IEEE Int. Electron Devices Meet. (IEDM)*, pp. 30.1.1–30.1.4 (2019).
6. J. Das et al., “MRAM PUF: a novel geometry based magnetic PUF with integrated CMOS,” *IEEE Trans. Nanotechnol.* **14**(3), 436–443 (2015).
7. O. A. Ibrahim, S. Sciancalepore, and R. Di Pietro, “Mag-PUF: Magnetic physical unclonable functions for device authentication in the IoT,” in *Security and Privacy in Communication Networks*, F. Li et al., Eds., pp. 130–149, Springer Nature Switzerland, Cham (2023).
8. C. Mesaritakis et al., “Physical unclonable function based on a multi-mode optical waveguide,” *Sci. Rep.* **8**, 9653 (2018).
9. F. Pavanello et al., “Recent advances in photonic physical unclonable functions,” in *IEEE Eur. Test Symp. (ETS)*, pp. 1–10 (2021).
10. K. Wang et al., “All-silicon multidimensionally-encoded optical physical unclonable functions for integrated circuit anti-counterfeiting,” *Nat. Commun.* **15**, 3203 (2024).
11. R. Pappu et al., “Physical one-way functions,” *Science* **297**(5589), 2026–2030 (2002).
12. A. Anastasiou et al., “Laser fabrication and evaluation of holographic intrinsic physical unclonable functions,” *Sci. Rep.* **12**, 2891 (2022).
13. B. C. Grubel et al., “Silicon photonic physical unclonable function,” *Opt. Express* **25**, 12710–12721 (2017).
14. F. B. Tarik et al., “Scalable and CMOS compatible silicon photonic physical unclonable functions for supply chain assurance,” *Sci. Rep.* **12**, 15653 (2022).
15. A. M. Smith and H. S. Jacinto, “Reconfigurable integrated optical interferometer network-based physically unclonable function,” *J. Lightwave Technol.* **38**(17), 4599–4606 (2020).
16. M. Blasl and F. Costache, “Device and method for generating a key,” European Patent 3679682 B1 (2017).
17. U. Rührmair et al., “Optical PUFs reloaded,” Cryptology ePrint Archive, Paper 2013/215 (2013).
18. M. Liao et al., “On-chip silicon optical scattering physical unclonable function towards hardware security,” *J. Lightwave Technol.* **41**(5), 1487–1494 (2023).
19. H. S. Jacinto, A. M. Smith, and N. I. Rafla, “Utilizing a fully optical and reconfigurable PUF as a quantum authentication mechanism,” *OSA Contin.* **4**, 739–747 (2021).
20. D. Dermanis et al., “Photonic physical unclonable function based on integrated neuromorphic devices,” *J. Lightwave Technol.* **40**(22), 7333–7341 (2022).
21. M. Blasl et al., “Integrated photonic cryptographic key generator using novel low-power MEMS-on-PIC technology,” *Proc. SPIE* **13012**, 1301202 (2024).
22. A. W. Elshaari et al., “Thermo-optic characterization of silicon nitride resonators for cryogenic photonic circuits,” *IEEE Photonics J.* **8**(3), 1–9 (2016).
23. D. J. Blumenthal et al., “Silicon nitride in silicon photonics,” *Proc. IEEE* **106**(12), 2209–2231 (2018).
24. C. Errando-Herranz et al., “Mems for photonic integrated circuits,” *IEEE J. Sel. Top. Quantum Electron.* **26**(2), 1–16 (2020).
25. H. Sun et al., “Silicon photonic phase shifters and their applications: a review,” *Micromachines* **13**(9), 1509 (2022).
26. K. Cooney and F. H. Peters, “Analysis of multimode interferometers,” *Opt. Express* **24**, 22481–22515 (2016).
27. T. Tamir and R. C. Alferness, *Guided-wave Optoelectronics*, Springer series in electronics and photonics, Vol. **26**, Springer-Verlag, Berlin (1988).
28. J. W. Goodman, *Speckle Phenomena in Optics: Theory and Applications*, Roberts & Co., Englewood, Colorado (2007).
29. M. Blasl et al., “MEMS-on-PIC: a cross-platform approach to combine ultra-low-power MEMS-modulators with photonic integrated circuits,” *Proc. SPIE* **12889**, 1288917 (2024).
30. M. Namdari et al., “Phase shifter for silicon nitride photonics using mems-enabled movable cladding,” in *IEEE Silicon Photonics Conf. (SiPhotonics)*, pp. 1–2 (2024).

Martin Blasl received his PhD from BTU Cottbus-Senftenberg for his work on the development of electro-optically induced waveguides in paranematic liquid crystals. Since then, he has been developing active and passive optical waveguide elements as well as micro-(opto)-electro-mechanical systems at the Fraunhofer IPMS Dresden, where he is currently developing a cross-platform approach for the fabrication of MEMS-based integrated photonic devices.

Meysam Namdari received his MS degree in electrical engineering—telecommunications from Amirkabir University of Technology Tehran, Iran, in 2013. He is currently working toward the Dr.-Ing. degree at Fraunhofer Institute for Photonic Microsystems IPMS in Dresden. His thesis topic is focused on the development of MEMS-on-PIC technology on silicon nitride photonics. His research interests include integrated photonics and MOEMS technologies.

Maximilian Wagner earned his BSc degree in electrical engineering in 2017 and MSc degree in microelectronics in 2021, both focusing on microsystem technologies, while working at Fraunhofer ENAS. He now works at Fraunhofer IPMS as an integration and process technologist, developing MEMS technologies, cleanroom processes, and micromirror MOEMS and photonic integrated circuits.

Jan Grahmann received his diploma in microsystem technology from the University of Applied Sciences Berlin in 2002 and his PhD from the University of Chemnitz in 2008. He joined Fraunhofer Institute for Photonic Microsystems in 2007, focusing on micromechanical scanning mirrors. In 2010, he became group manager of Micro Scanner Device Development, and since 2013, he has headed the business unit Active Micro-optical Systems.