Editors' Suggestion

Stable High-Speed Encryption Key Distribution via Synchronization of Chaotic Optoelectronic Oscillators

Fabian Böhm,[1,2,*] Sevada Sahakian,[1] Ann Dooms,[2] Guy Verschaffelt,[1] and Guy Van der Sande[1]

[1] *Applied Physics research group, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium*
[2] *Digital Mathematics research group, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium*

(Received 13 March 2020; revised manuscript received 24 April 2020; accepted 4 May 2020; published 5 June 2020)

Generating and distributing encryption keys via chaos synchronization of optical systems is a promising method for achieving secure and fast real-time encryption of large data volumes. However, current state-of-the-art systems based on lasers subjected to time-delayed feedback have exhibited serious limitations in regard to stability and speed due to their inherent phase sensitivity and their fundamental bandwidth limitation by the laser relaxation oscillation frequency. Here, we propose, simulate, and build a fundamentally different concept based on optoelectronic oscillators (OEOs) to generate and distribute encryption keys. We demonstrate both theoretically and experimentally that by injecting chaotic OEOs with a common external chaotic signal, chaos synchronization can be achieved. The key distribution signal shared between sender and receiver is in the optical domain and can thus be transmitted over a standard fiber-optic network. As the optoelectronic feedback is phase insensitive, stable synchronization becomes possible without any need for active stabilization, resulting in a compact and inexpensive setup. From the chaotic time traces, identical random bit sequences can be generated on the sender's and receiver's sides at rates of up to 6 GBit/s, which is comparable to current state-of-the-art systems of the same bandwidth. Since OEOs are not bandwidth limited by relaxation oscillations, the key generation can be further increased compared to laser-based systems by increasing the OEO bandwidth, thus presenting a promising platform for achieving fast and secure real-time encryption.

DOI: 10.1103/PhysRevApplied.13.064014

I. INTRODUCTION

With recent trends such as cloud computing, Internet of things, and the growth of web services, more and more sensitive data is being transmitted over the Internet. This presents a serious challenge to optical telecommunication networks, not only to accommodate the large throughput of data but also to ensure its security. While encryption is typically handled by symmetric cryptosystems, such as the advanced encryption standard or public key cryptosystems such as the Rivest-Shadmir-Adleman algorithm or combinations thereof, recent cybersecurity attacks have repeatedly demonstrated the vulnerability of preshared encryption keys that are used in symmetric algorithms. This is especially the case when keys are often reused, limited in length, or stolen from central servers [1–3]. The use of unique keys that are used only once, so-called one-time pads, have long been known to resolve these issues and make encryption theoretically unbreakable, given that the key is entirely random, matches the length of the encrypted message, and can be safely shared between sender and receiver [4,5]. However, these requirements have shown to be technically challenging for conventional methods, since new encryption keys have to be constantly generated and securely transmitted alongside the encrypted message.

These shortcomings have generated interest in devising alternative hardware-based concepts for the generation and distribution of one-time pads that rely on synchronization of chaotic systems [6–11]. Here, sender and receiver employ identical chaotic systems that are synchronized by injecting them with an uncorrelated external chaotic seed signal. From the synchronized response, the same encryption key can then be generated on the sender and receiver sides by sampling both chaotic time traces at equal time steps. Since the keys are fully random and can be created indefinitely at high rates, even simple encryption methods such as the Vernam cipher can then be used without compromising security [4,5], hence creating an efficient and secure real-time encryption scheme [12]. Moreover,

* fabian.bohm@vub.be

the key distribution scheme can be readily combined with conventional encryption methods to enhance their security. Seed-mediated synchronization is also fundamentally different from chaos communication schemes that try to hide secure messages in chaotic time traces [13], and presents an improvement in security and ease-of-use since no measures have to be taken to conceal information about the sender and receiver systems in the public channels [14].

First proofs of concept of this scheme have recently been demonstrated with semiconductor lasers [6–8] and analog electronics [9]. Chaotic semiconductor lasers subjected to coherent time-delayed feedback in particular have shown great potential, since they are compatible with optical telecommunication networks and can achieve synchronization over distances of several kilometers [7,13]. However, the timescale of the dynamical response of these system is fundamentally limited by the relaxation oscillation frequency of semiconductor lasers, which limits the key generation rate of current real-world systems to a few MBit/s for oblivious transfer protocols [6,8]. Additionally, the coherent optical feedback in these systems is sensitive to the optical phase of the seed signal as well as the phase of the feedback signal and makes them highly susceptible to external perturbations [15]. This severely limits the time of stable operation and places strict demands on the stability of the optical transmission lines [6–8].

To address these issues, we propose and demonstrate a fundamentally different approach based on optoelectronic oscillators (OEOs) that is more stable and can increase the key generation rate. OEOs are photonic systems that are compatible with telecommunication networks, can be inexpensively built from off-the-shelf components, and are used in various applications due to their rich dynamical properties and high bandwidth [16,17]. When subjected to strong time-delayed feedback, OEOs exhibit chaotic dynamics and can be used for high-speed encryption key generation [18,19]. Since the feedback is optoelectronic rather than coherent, phase sensitivity is removed, which makes OEOs significantly more robust than coherent feedback systems. Based on simulations and experiments with a fiber-based photonic setup, we show that stable chaos synchronization can be achieved by injecting OEOs with a common chaotic seed signal. For an OEO with a 10 GHz bandwidth, we find that matching encryption keys can be generated at rates of up to 6 GBit/s and bit-error ratios of 3.2×10^{-3}. We show that the generated keys fulfill the basic requirements of a one-time pad, thus demonstrating the potential of OEOs as fast and secure key distribution schemes.

II. SIMULATION RESULTS FOR CHAOS SYNCHRONIZATION

To achieve synchronized key generation on the sender and receiver sides, we employ a network of three coupled

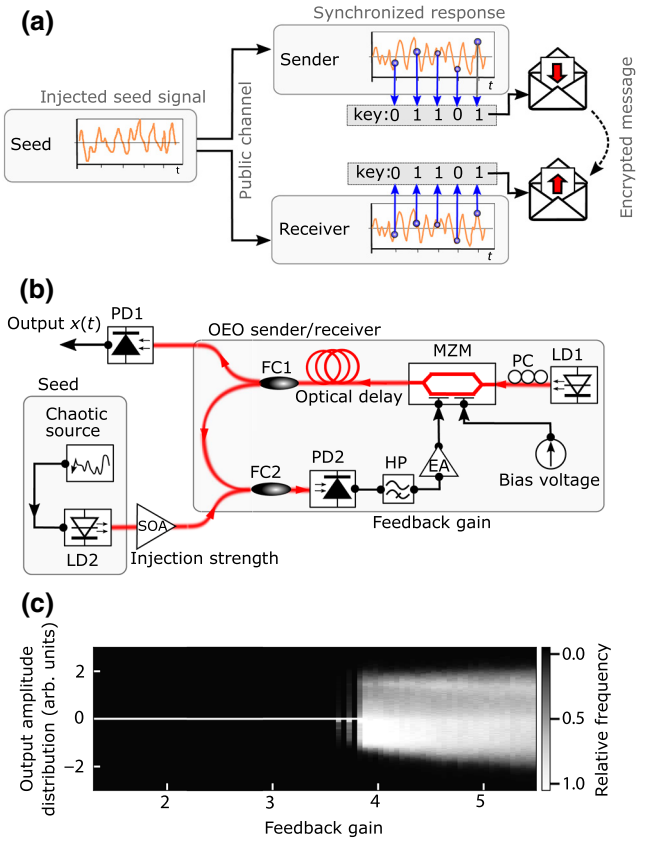

FIG. 1. Scheme for key distribution by chaos synchronization of OEOs. (a) Scheme used for key distribution using chaotic oscillators. (b) Experimental setup of the OEO. Here PD is the photodiode, LD is the laser diode, PC is the polarization controller, AWG is the arbitrary waveform generator, SOA is the semiconductor optical amplifier, FC is the fiber coupler, EA is the electrical amplifier, and HP is the high-pass filter. (c) Simulated distribution of the OEO output as a function of the feedback gain.

chaotic oscillators, namely the sender, the receiver, and the seed, as depicted in Fig. 1(a). The sender and receiver are responsible for generating the encryption key, while the seed is responsible for driving sender and receiver into synchrony. The seed signal $s(t)$ is extracted from the output of the seed and is transmitted via an open public channel to sender and receiver. It is then equally injected into both systems with the injection strength κ. Once the injection becomes strong enough, the seed is able to force them into synchrony. From the synchronized chaotic response, matching keys are generated on both sides by sampling the time traces. These keys are then used to encrypt the secure message on the sender side and decipher it on the receiver side. An important property of this chaos synchronization is that sender and receiver have to be perfectly matched in order to achieve synchrony, meaning that mismatches in even one parameter are enough to destroy the synchronization [7]. This is important in regard to the security of

the key distribution scheme and will be discussed in more detail in Sec. IV.

To attain encryption keys from the chaotic time traces, oblivious transfer [8] or direct sampling [9] are typically used. For direct sampling, the output of the sender and receiver is periodically sampled and random bits are generated based on the output amplitude. The maximum rate at which keys can be generated is primarily determined by the system's autocorrelation time τ_{auto}. If samples are drawn at shorter intervals than the autocorrelation time, successive bits in the key will exhibit strong correlation and they will thus not be fully random anymore. The autocorrelation time is directly linked to the bandwidth of the system, which is limited by the low-pass characteristics of the components. For oblivious transfer on the other hand, both sender and receiver are randomly switched from synchrony to asynchrony by modulating the seed signal with a randomly generated bit sequence [8]. During each of these switches, only a single sample is drawn based on the output's amplitude. By exchanging the information when the sender and receiver are synchronized, the final key is then generated only from samples where both sender and receiver were synchronized simultaneously. This protocol sacrifices key generation rate in favor of security and is fundamentally limited by the transient times of sender and receiver to go from synchrony to asynchrony and back [6–8].

In this work, we consider OEOs as the basis for the chaotic seed, sender, and receiver systems. In Fig. 1(b) we show the setup of our OEO system. Coherent light emitted by a laser diode is passed through a Mach-Zehnder modulator (MZM) that modulates the light intensity. The output propagates through a long optical fiber, which introduces a time delay T, before the signal is detected by a photodiode. The electronic signal then passes through a high-pass filter and is amplified by an electrical amplifier before being injected into the input port of the MZM to close the feedback loop. The dynamics of such an OEO are modeled by an Ikeda-type model, which describes the time evolution of the MZM output $x(t)$ and the filtered feedback signal $y(t)$ [20]:

$$\frac{dx}{dt} = -\left(\frac{1}{\tau_l} - \frac{1}{\tau_h}\right)x - \frac{1}{\tau_h}y + \frac{1}{\tau_l}G\sin^2[x(t-T) + \varphi + \kappa s(t) + \zeta(t)], \quad (1)$$

$$\frac{dy}{dt} = \frac{1}{\tau_h}x. \quad (2)$$

Here, the feedback gain is given by the gain coefficient G, φ is the bias phase of the MZM, and $s(t)$ is the injection signal with injection strength κ. Noise in the OEO is modeled by an additive Gaussian white noise term $\zeta(t)$.

TABLE I. Parameters used in the simulations.

Parameter		Value
φ	Bias phase	1.5
T_{seed}	Feedback delay seed	2.2 ns
$T_{\text{sen,rec}}$	Feedback delay of sender and receiver	2.3 ns
τ_l	Low-pass time constant	15 ps
τ_h	High-pass time constant	1.59 ns
G_{seed}	Feedback gain seed	4
$G_{\text{sen,rec}}$	Feedback gain of sender and receiver	4.5
κ_{seed}	Injection strength seed	0
$\kappa_{\text{sen,rec}}$	Injection strength of sender and receiver	Variable

The frequency response of the system is determined by the low- and high-pass characteristics of the optical and electrical components, which are captured by the characteristic timescales τ_l and τ_h. The full set of parameters used in the simulations is shown in Table I.

Through the interaction of self-feedback and time delay, the OEO can be driven from a steady-state solution to a chaotic regime through a cascade of bifurcations. In Fig. 1(c) we show a simulation of the amplitude distribution of the MZM output $x(t)$ as a function of the feedback gain G for a single OEO without injection signal ($\kappa = 0$). For low feedback gain, the OEO is in a steady state $x^* = 0$ while, for a feedback gain above $G \approx 3.8$, the steady state becomes unstable and the output $x(t)$ evolves into fully chaotic dynamics. In this chaotic regime, the output becomes unpredictable, which makes it possible to generate random encryption keys by sampling the chaotic time trace.

In the following, we consider simulations of the system depicted in Fig. 1(b) with a 10 GHz bandwidth of the OEO. Such a system can be readily built with off-the-shelf components and has demonstrated nonsynchronized encryption key generation at rates of several GBit/s [18,19]. In Fig. 2(a) we show the time traces of the entire system for an injection strength of $\kappa = 7$. At this injection, we can observe how the responses of the sender and receiver become synchronized while the seed time trace is entirely different. To quantify the quality of the synchronization, we calculate the absolute value of the cross-correlation between sender and receiver

$$C_{\text{sen,rec}}(T_0) = \left| \frac{\langle x_{\text{sen}}(t)\, x_{\text{rec}}(t - T_0)\rangle}{\sqrt{\max[C_{\text{auto,rec}}(T_0)]\ \max[C_{\text{auto,sen}}(T_0)]}} \right|, \quad (3)$$

which is normalized with the maximum of the autocorrelation of both signals $C_{\text{auto}}(T_0) = \langle x(t)\, x(t - T_0)\rangle / \langle x(t)\, x(t)\rangle$. We plot $C_{\text{sen,rec}}(T_0)$ in Fig. 2(b) as a function of the time delay T_0. For zero delay, the cross-correlation reaches its maximum value of $C_{\text{sen,rec}}(0) \approx 0.95$, which indicates a

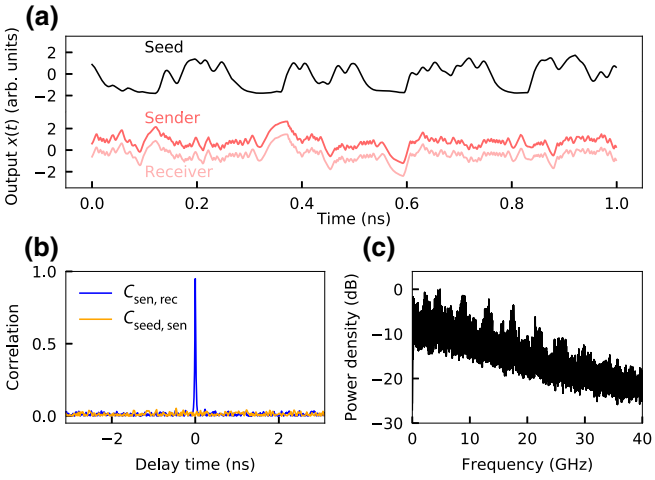

FIG. 2. Properties of chaos synchronized OEOs. (a) Time traces of the seed and the synchronized sender and receiver for $\kappa = 7$. The time traces of the sender and receiver are offset to show their synchronous behavior. (b) Cross-correlation between seed and sender, $C_{\text{seed,sen}}$, and between sender and receiver, $C_{\text{sen,rec}}$. (c) Frequency spectrum of the sender output.

high degree of synchronization and allows us to extract identical bit sequences from the time series of sender and receiver, as will be shown later. At the same time, the correlations between seed and sender and receiver remain very low. This is an important prerequisite for the security of the key generation, since the encryption key becomes impossible to extract from the public channel (this will be discussed in more detail in Sec. IV). The cross-correlation between seed and sender $C_{\text{seed,sen}}$ reaches a maximum value of $\max[C_{\text{seed,sen}}(T_0)] \approx 0.05$, which is comparable to the level of the noise floor. From the plot in Fig. 2(b), we can also observe that no peaks are visible in the cross-correlation, indicating that the shared information between seed and sender is comparable to that of two completely random signals, thus ensuring the security of the generated keys. In Fig. 2(c), we show the frequency spectrum of the sender's response. As expected from a chaotic system, it exhibits a broad frequency spectrum with a bandwidth that corresponds with the low-pass characteristics of our system. Interestingly, we do not observe a peak in the spectrum corresponding to the delay time T, as is typical for many time-delayed feedback systems. This is also corroborated by the autocorrelation in Fig. 2(b) and indicates that repeating patterns are less likely to appear in the generated keys.

Using the chaotic responses of sender and receiver, we extract random encryption keys by direct 1-bit sampling, where every bit $B(t_0)$ corresponds to the sign of the OEO output $B(t_0) = \text{sign}[x(t_0)]$ at the sampling time t_0. To assess the quality of the keys, we calculate the corresponding bit error ratio (BER) between the sequences of sender and receiver, which corresponds to the number of mismatched bits in a 100 bit long sequence. On average, the BER is approximately 0.07 ± 0.01, thus demonstrating that synchronous key generation is possible as this is sufficient to reliably transmit data by using error-correction codes. However, to achieve even lower BERs, the method of robust sampling can be applied [6], which relies on the fact that more errors in the bit generation are created by small values of $x(t)$. This is exemplified by Fig. 3(a), which shows the joint probability distributions of the sender and receiver signals and of the sender and the seed signals. Since the sender and receiver are highly correlated, their joint probability distribution is narrow and follows a linear slope, while the uncorrelated seed and sender exhibit a broad distribution function. Because of the noise in the system, the distribution of sender and receiver is broadened, which, for small amplitudes, can easily lead to cases where one system has a positive amplitude while the other is negative, hence leading to a mismatch in the generated keys. To counteract this, robust sampling applies a threshold η such that values below this threshold will get discarded. In Fig. 3(a), only samples within the white hatched regions will thus be used to generate the keys. This will in turn decrease the BER at the cost of a slower effective sampling rate. In Fig. 3(b), we analyze the BER and the effective sampling rate in our system as a function of the sampling threshold η. We find that by increasing η, the BER can

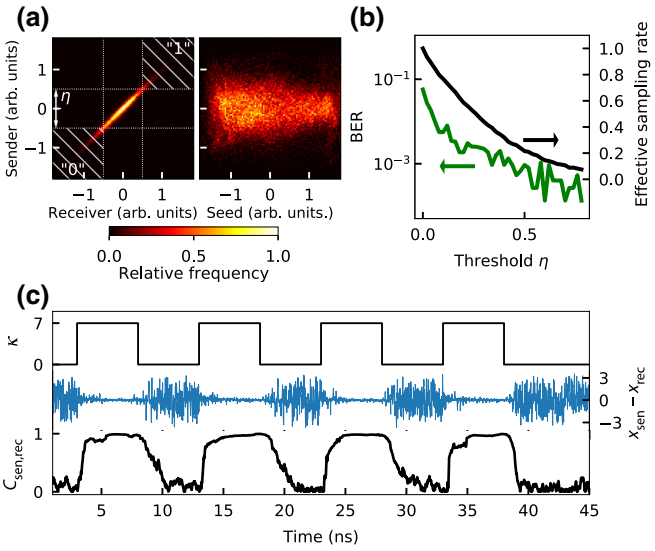

FIG. 3. Methods for robust sampling and for oblivious transfer. (a) Joint probability distribution for sender and receiver outputs with the sampling threshold η (left) and for the seed and sender outputs (right). The hatched regions indicate the part of the distribution that is used to generate 1 and 0 in the key. (b) BER (green line) and effective sampling rate (black line) as a function of the sampling threshold η. (c) Transient of the difference between sender and receiver outputs $x_{\text{sen}} - x_{\text{rec}}$ and maximum of the cross-correlation $C_{\text{sen,rec}}$ as the modulation strength κ is modulated.

be significantly lowered to a minimum of around 10^{-4}, which is comparable to other state-of-the-art systems [6–9,11]. For the lowest BER, between 10% and 20% of the total samples are used for the key generation, which means that the effective sampling rate is slowed down to 0.1 of the original sampling rate. By robust sampling, it is thus possible to decrease the BER by about two orders of magnitude at the cost of around one order of magnitude in the sampling rate.

To estimate the maximal speed at which keys can be generated, we consider the transient behavior of the chaotic signals. From the frequency spectrum in Fig. 2(c) and the time traces in Fig. 2(a), it is apparent that the system possesses a large bandwidth and can thus exhibit chaotic fluctuations at timescales of a few picoseconds. For direct sampling of encryption keys, we estimate the theoretical maximum key generation rate from the autocorrelation time τ_{auto} by fitting the autocorrelation with an exponential decaying function $C_{\text{auto}}(T_0) = \exp(-T_0/\tau_{\text{auto}})$. For the time traces in Fig. 2(a), the autocorrelation time is $\tau_{\text{auto}} =$ 16 ps so that random bits can potentially be sampled at frequencies of up to 60 GHz. This frequency scales linearly with the bandwidth and can thus be increased further by using faster optoelectronic components. With current off-the-shelf equipment, bandwidths of 40 GHz are attainable with OEOs, which could increase the maximum sampling fourfold with respect to the parameters used in our simulations. This is an improvement compared to semiconductor lasers, where the bandwidth is fundamentally limited by the relaxation oscillation frequency of the laser. In current key distribution schemes for example, relaxation oscillation frequencies do not surpass 8 GHz [7,11]. The potential bandwidth of the studied scheme is even more pronounced when compared to analog electronic systems, where key generation rates of just a few kBit/s have been reported [9].

We also estimate the potential maximal key generation rate for oblivious transfer based on the transient time τ_{trans} that the system requires to switch between synchrony and asynchrony. In semiconductor lasers, these timescales become quite long, of the order of around 70 ns, hence limiting the maximal key generation rate to just a few MBit/s [7,8,11]. In Fig. 3(c) we show the difference between the sender and receiver outputs $x_{\text{sen}}(t) - x_{\text{rec}}(t)$ and their cross-correlation during an oblivious transfer. To switch the system between synchrony and asynchrony, the injection strength κ is modulated between $\kappa = 0$ and $\kappa = 7$. We measure the transient time τ_{trans} and compare it against previous studies by measuring the time it takes the system to go from the threshold $C_{\text{sen,rec}} = 0.1$ (asynchrony) to $C_{\text{sen,rec}} = 0.8$ (synchrony) and back. To reach synchronization, we find an average time of around $\tau_{\text{trans}} = 0.5$ ns and, for the reverse process, the transient time is around $\tau_{\text{trans}} =$ 1.3 ns. This is an improvement of around two orders of magnitude compared to semiconductor laser systems and allows us to perform oblivious transfer of encryption keys at much higher rates than what was possible before. In the exemplary time series in Fig. 3(c), a sampling rate of 200 MS/s is easily achieved with a 10 GHz bandwidth OEO.

III. EXPERIMENTAL REALIZATION OF CHAOS SYNCHRONIZATION

Based on our simulations, we want to verify if synchronization of chaotic OEOs can be achieved in an actual photonic setup. For the experimental realization, we utilize a fiber-based OEO as shown in Fig. 1(a). Contrary to our simulations, the seed signal is emitted by a laser diode that is modulated by a chaotic waveform generated from an arbitrary waveform generator (AWG). The chaotic waveform is repeated twice so that comparing the OEO's response to two subsequent repetitions is then equivalent to having two independent but identical OEOs that are injected with the same seed signal. Our experiment hence requires only a single OEO instead of three individual ones, which strongly reduces the complexity and cost for this proof of concept. For future iterations, identical OEOs should be used for sender and receiver. We will discuss the impact of fabrication variations between different MZMs in Sec. IV. Interestingly, using an AWG to generate the chaotic time series is an interesting aspect, since it shows that a large variety of different chaotic systems could be used to generate the seed signal.

In our setup, laser light is emitted by a DFB laser at 1.55 μm and passes through a 12 GHz lithium niobate MZM. The lasers polarization angle is controlled by a polarization controller before entering the MZM. The optical delay line consists of 12 m of optical fiber with a total delay time of around 100 ns. The optical signal is detected by a 150 MHz GaAs photodiode and amplified by a 20 GHz electrical amplifier. The electrical amplifier has an internal high-pass filter with a cutoff frequency of around 50 kHz. It is important to note here that the bandwidth of our system is lower in comparison to our simulations due to the low-pass characteristics of the photodiode. The autocorrelation time of the experimental setup is $\tau_{\text{auto}} = 2.6$ ns, which indicates a possible slowdown of around two orders of magnitude in the key generation rate compared to the simulations. However, since the dynamical timescales of Eqs. (1) and (2) can be arbitrarily rescaled, the general dynamical behavior in the simulations and the experiments remain comparable regardless of the bandwidth. Hence, the same parameters as in Table I are used for the simulations. The output of the OEO is detected by a photodiode that is connected by a fiber coupler to the optical delay line. To generate the chaotic seed signal, we sample the output of the free running chaotic OEO at a sampling rate of 1 GS/s. The recorded waveform is 50 μs long, which ensures that it is both longer than the internal delay time $T = 100$ ns as well as the autocorrelation time of the signal.

This waveform is uploaded to an AWG, which generates the seed signal at the same sampling rate. The seed signal is then injected into the optical feedback line by a fiber coupler. To control the injection strength κ, we use an additional semiconductor optical amplifier that is placed in the injection line.

To compare experiments and simulations, we investigate the scaling of the maximum of the cross-correlation between sender and receiver $C_{\mathrm{sen,rec}}$, the cross-correlation between seed and sender $C_{\mathrm{seed,sen}}$, as well as the BER as a function of the injection strength κ. The results obtained from the simulations are shown in Fig. 4(a) as dashed lines. For low injection strengths, we observe that all OEOs are fully uncorrelated and that the BER is approximately 0.5, which indicates that no chaos synchronization is achieved. As the injection strength is increased, $C_{\mathrm{rec,sen}}$ gradually grows until chaos synchronization is eventually reached for $\kappa > 3$ with the BER decreasing to 0.05 and the cross-correlation increasing to $C_{\mathrm{sen,rec}} = 0.98$ for $\kappa = 4$. It is interesting to note that the cross-correlation between seed and sender will remain constant at a very low level as the injection becomes stronger, which ensures secure key generation on the sender and receiver sides. We compare these findings with our experimental results shown in Fig. 4(a) as black dots and find that, as in the simulations, chaos synchronization is achieved for higher injection strengths. Experimental injection strengths were related to simulations by the ratio between the seed signal amplitude and the amplitude of the free running laser. For the experimental setup, the cross-correlation between sender and receiver reaches levels of up to $C_{\mathrm{sen,rec}} = 0.93$ while the BER is 0.10 for $\kappa = 1.6$. This demonstrates that synchronizing networks of OEOs with an external chaotic seed signal is possible, as predicted by the simulations.

While the general trends for $C_{\mathrm{sen,rec}}$ and the BER are quite comparable, however, we can observe quantitative differences between experimental and simulation results in Fig. 4(a). The experimental injection strength required for chaos synchronization is only about half that of the simulation so that synchronization is already reached for $\kappa > 1.5$. Furthermore, the cross-correlation between seed and sender is significantly higher than in the simulations and reaches a level of around $C_{\mathrm{seed,sen}} \approx 0.4$ for higher injection strengths. These differences can be explained by the MZM used in our experiments. Since the MZM is primarily used as an intensity modulator, the input voltage to the MZM is expected to be in the range $x(t - T) = [0, V_\pi]$. For modulation signals outside this voltage range, the transfer function of MZMs typically evolves to a constant value [21]. This thus limits both the modulation width as well as the maximum injection strength that can be injected in the experiment. To account for this in the simulations, we adapt the MZM transfer function in Eq. (1). In Fig. 4(c) we show a comparison of the transfer function for the full model and our modified

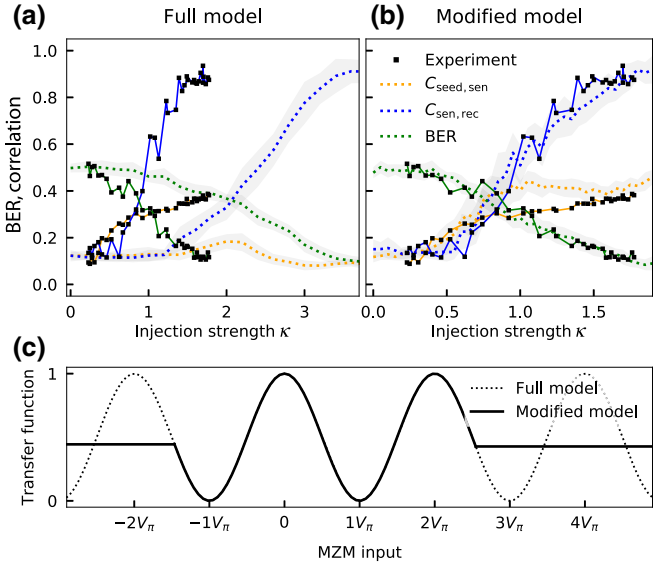

FIG. 4. Comparison of simulations and experiments. (a),(b) BER, cross-correlation between sender and receiver $C_{\mathrm{sen,rec}}$ and between seed and sender $C_{\mathrm{seed,sen}}$ as a function of the injection strength. Comparisons between the experimental data and (a) the full OEO model and (b) the modified OEO model for a limited modulation bandwidth. Grey shades indicate the standard deviation of the simulation results. (c) The MZM transfer function used for the full model and the modified model.

model. For the modified model, the transfer function is set to a constant value for feedback signal strengths outside the range $x(t - T) = [-1.5V_\pi, 2.5V_\pi]$. The simulation results based on this modified model are plotted in Fig. 4(b) as dashed lines and show very good agreement with our experimental data. It is important to note here that the limited voltage range is not inherent to the design of MZMs. By using a longer phase modulator section, for example, a larger modulation width could be achieved.

IV. SECURITY OF THE KEY DISTRIBUTION

The ability to continuously create matching encryption keys on the sender and receiver sides makes it possible to use our key distribution scheme for the creation of one-time pads. However, in order to ensure security, there are four basic requirements that every key has to fulfill in order to be usable as a one-time pad. First, the length of the key has to be at least as long as the secret message. Second, the key may never be reused. Third, the key has to be completely random and not contain predictable patterns. Fourth, the keys have to be shared in a secure manner between sender and receiver. Once these four requirements are met, it is theoretically impossible to crack even simple encryption methods using the one-time pad, such as the Vernam cipher [4,5]. In the following, we investigate whether the keys generated by the OEOs are able to fulfill all of these requirements.

A. Randomness of the keys

Based on our simulations, we assess whether the keys generated by the OEOs fulfill the first three requirements of one-time pads, namely the ability to create arbitrarily long, nonrepeating, and fully random encryption keys. We check these by extracting very long encryption keys from our simulation results and testing them for randomness using the NIST Statistical Test Suite [22]. In total, 187 different tests are performed on 48×10^6 bit long keys that are divided into 120 individual 400 000 bit long bitstreams for testing. To ensure security, two additional stages of delayed bitwise exclusive-OR (XOR) operations are added to the bitstream generator of the OEO, which is a method that is commonly used in photonic physical random number generators [19,23–25]. In the first stage, the bitstream generated by the OEO is delayed by 20 bits and interfered with itself by an XOR operation. In the second stage, we use a delay of 100 bits. In Table II, we show the test results for keys that were generated at different sampling rates. The detailed pass rates and p values for all tests at a 50 GHz sampling rate are also shown in Table II. In order to pass the tests, a pass rate of at least 116 out of 120 bitstreams has to be reached. For the random excursion and random excursion variant tests, the minimum pass rate is 40 out of 42 bitstreams. The corresponding p values have to be larger than 0.001 for all tests. In some cases, multiple instances of a single test are performed (e.g., cumulative sums). In these cases, only the worst results are shown in Table II.

TABLE II. Number of passed tests of the NIST Statistical Test Suite for different bit generation rates (top) and detailed test results for a sampling rate of 50 GHz (bottom). In the case of multiple instances per test, only the worst result is shown.

Sample rate	50 GHz	60 GHz	70 GHz	80 GHz	90 GHz
Pass rate	187/187	186/187	186/187	172/187	166/187
Test at a 50 GHz sampling rate		p value		Pass rate	
Frequency		0.9114		120/120	
Block frequency		0.3371		118/120	
Cumulative sums (worst)		0.7061		119/120	
Runs		0.2327		115/120	
Longest run		0.5174		119/120	
Rank		0.7399		119/120	
FFT		0.0392		117/120	
Nonoverlapping template (worst)		0.0011		116/120	
Overlapping template		0.3925		117/120	
Universal		0.0437		119/120	
Approximate entropy		0.2041		119/120	
Random excursions (worst)		0.0781		41/42	
Random excursions variant (worst)		0.0571		41/42	
Serial (worst)		0.2229		118/120	
Linear complexity		0.8195		119/120	

For sampling rates of up to 50 GHz, the OEO is able to pass all of the 187 tests. This demonstrates that the keys generated by the OEOs are indeed able to fulfill the first three requirements of a one-time pad. With our key distribution scheme, we are thus capable of generating nonrepeating and fully random encryption keys practically indefinitely. Beyond 50 GHz, we find that the failure rate will gradually start to increase, from one failed test at 60 GHz to 21 at 90 GHz. While at 50 GHz, the sampling interval is every 20 ps and thus still above the autocorrelation time of $\tau_{\text{auto}} = 16$ ps, sampling intervals become shorter than the autocorrelation time for higher sampling rates and hence randomness in the generated keys is lost. An OEO with a 10 GHz bandwidth can thus achieve a maximum key generation rate of around 50 GBit/s. By using robust sampling as described in Sec. II, we achieve a final key generation rate of around 6 GBit/s at a BER of 3.2×10^{-3}. We also estimate the maximal key generation rate in the experimental setup from its autocorrelation time and reach a theoretical maximum of around 30 MBit/s with robust sampling applied. This is already a significant improvement when compared to the kBit/s key generation rates reported for analog electronic system [9]. However, we want to remark here once again that the lower experimental key generation rate is due to the lower bandwidth of the detectors used in the experiments and can easily be increased in future iterations of our design.

B. Mutual information with the seed

To assess the fourth and last requirement for one-time pads, we have to ensure that the distribution of the keys is entirely secure from eavesdropping. In our distribution scheme, the only information shared among sender and receiver through the public channel is the seed. An attacker listening to the public channel might then record the seed signal and generate his own key B_{seed} by sampling the seed signal. It is thus important that no information about the key is contained within the seed. From the maximum of $C_{\text{seed,sen}}$ in Fig. 4, it is already apparent that there is little correlation between seed and sender in the synchronized case. To determine how much information about the sender key B_{sen} can be extracted from the injection signal, we calculate the mutual information

$$I(B_{\text{seed}}, B_{\text{sen}}) = \sum_{q,r} P_{B_{\text{seed}}B_{\text{sen}}}(q,r) \log \frac{P_{B_{\text{seed}}B_{\text{sen}}}(q,r)}{P_{B_{\text{seed}}}(q) P_{B_{\text{sen}}}(r)}. \tag{4}$$

The mutual information is a measure of how much information can be obtained about the sender key B_{sen} by observing the seed key B_{seed}, and is calculated from the

joint probability distribution $P_{B_{\text{seed}}B_{\text{sen}}}(q,r) = P(B_{\text{seed}} = q \mid B_{\text{sen}} = r)$ and the corresponding marginal probability distributions $P_{B_{\text{seed}}}(q)$ and $P_{B_{\text{sen}}}(r)$. It is equal to 0 for two uncorrelated signals and equal to one 1 for two identical signals. Using simulation results from the full model, we estimate the joint probability distribution $P_{B_{\text{seed}}B_{\text{sen}}}(q,r) = P(B_{\text{seed}} = q \mid B_{\text{sen}} = r)$ with $q, r \in 0, 1$:

$$P_{B_{\text{seed}}B_{\text{sen}}}(q,r) = \begin{matrix} \textit{case:} \\ r{=}0 \\ r{=}1 \end{matrix} \begin{matrix} q{=}0 & q{=}1 \end{matrix} \begin{pmatrix} 0.2512 & 0.2523 \\ 0.2485 & 0.2480 \end{pmatrix}.$$

The joint probability distribution shows that there is an equal probability of having a matching or a mismatching bit between the seed and sender keys, which is to be expected for two independent random variables. This is also corroborated by the BER between the two keys, which is $\text{BER}_{\text{seed,sen}} = 0.54$ and thus at the same level as randomly guessing the encryption key. For seed and receiver, the mutual information is then $I_{\text{seed,sen}} = 4.3 \times 10^{-4}$. This is very close to the expected value for two independent random variables, where I would become zero and is also comparable with other chaotic key distribution schemes [7,9,11].

We also want to consider the mutual information from the experimental data. From Fig. 4(b), it becomes clear that the limited modulation width of the MZM leads to an increased correlation between the seed and the sender, which raises the question how this increase affects the mutual information and the security of the one-time pad. From the experimental data, we obtain the following joint probability distribution for an injection strength of $\kappa = 1.7$:

$$P_{B_{\text{seed}}B_{\text{sen}}}(q,r)^{\text{expt.}} = \begin{matrix} \textit{case:} \\ r{=}0 \\ r{=}1 \end{matrix} \begin{matrix} q{=}0 & q{=}1 \end{matrix} \begin{pmatrix} 0.3224 & 0.2204 \\ 0.2386 & 0.2070 \end{pmatrix}.$$

The mutual information is then $I^{\text{expt.}}_{\text{seen,sen}} = 0.0213$, hence showing that despite the increase in the correlation, the chances of extracting information about the key from the seed signal are still very low. This is also corroborated by the corresponding BER, which is $\text{BER}^{\text{expt.}}_{\text{seed,sen}} = 0.45$ and thus close to that of two uncorrelated random bit sequences. We can thus conclude that the limited modulation width of the MZM will not significantly affect security. Based on both the simulation and experimental results, we find that no relevant amount of information is shared through the public channel and that reconstructing parts of the key from the seed by an attacker is very unlikely, hence fulfilling the fourth requirement of one-time pads.

C. Difficulty of parameter estimation

Another more serious attack which could compromise the fourth requirement of one-time pads is when an attacker has a large amount of information about the key generation method. Assuming that the attacker knows the type of dynamical system as well as the sampling rate of the key distribution scheme, he could in principle listen to the public channel, record the seed signal, and try to generate his own matching key, either by using his own OEO or by simulating Eqs. (1) and (2). This would require him to estimate all the parameters in Eqs. (1) and (2) and tune them to the same values as in the sender and the receiver to achieve synchronization. To make such an attack scenario unlikely, one has to ensure that the chaos synchronization is sensitive to changes in the parameters, making the parameter space large and the search highly challenging. In Fig. 5, we consider the effect of a mismatch of each parameter on the quality of synchronization under the assumption that all other parameters are perfectly matched. Whenever possible, we study the impact of mismatch both with results obtained from our experimental setup (indicated by black dots) and with data from simulations (indicated by dashed lines). For comparisons against experimental data, we use the modified model introduced in Fig. 4(c), which is in good agreement with the experiments. We also consider comparisons using the full model and find no relevant deviation from the modified model.

In Fig. 5(a), we plot $C_{\text{sen,rec}}$ and the BER as a function of the injection mismatch $\Delta\kappa$. As the injection mismatch becomes larger, we observe that the BER starts to increase

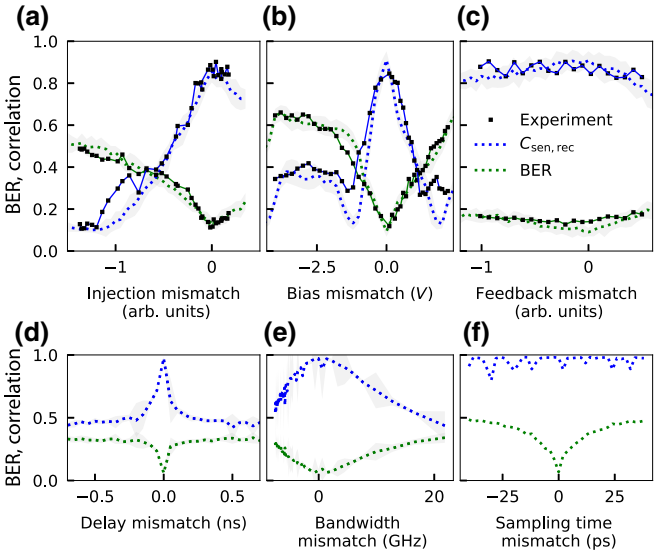

FIG. 5. Sensitivity of synchronization against parameters mismatch. Cross-correlation between sender and receiver $C_{\text{sen,rec}}$ and BER as a function of the parameter mismatch for the injection strength κ (a), the bias phase φ (b), the feedback gain G (c), the time delay T (d), the low pass bandwidth $\omega = 1/(2\pi\tau_l)$ (e), and the sampling time (f). (a)–(c) Results obtained from experiments and simulations using the modified model. (d)–(f) Simulations using the full model. Grey shades indicate the standard deviation of the simulation results.

while the cross-correlation decreases, hence showing the sensitivity of the synchronization to mismatches in the injection strength. We estimate the sensitivity by looking at the parameter range where a BER of less then 30% is achieved. For the injection strength, this mismatch has to be less than $|\Delta I| < 0.45$. In Fig. 5(b), we similarly find for the bias phase φ that the mismatch has to be less than $|\Delta\varphi| < 0.35$ or, equivalently, $|\Delta\varphi| < 0.7V$ in the experimental setup. For the feedback gain, we find in Fig. 5(c) that the synchronization is rather insensitive to changes in G. The mismatch has to be $|\Delta G| > 4$ to drive the system into asynchrony. While not being parameters that are easy to sweep in an experimental setup, we also investigate mismatches in the time delay T in Fig. 5(d), the low-pass bandwidth in Fig. 5(e), and the sampling time in Fig. 5(f) by simulating the full model. We find that the time delay has to be estimated with a precision of $|\Delta\tau| < 15$ ps to reach synchrony. For the bandwidth of the system, which is determined by τ_l, we find that the low-pass cutoff frequency $\omega = 1/(2\pi\tau_l) = 10$ GHz has to be tuned within the range of $\omega > 1.6$ GHz and $\omega < 16.6$ GHz. Lastly, we consider the sampling time in Fig. 5(f). Although the sender and receiver are likely synchronized by an external clock and the sampling frequency might thus be well known to an attacker, the exact point in time at which samples are drawn relative to the clock signal is still unknown. Since the system exhibits a short autocorrelation time, we find that mismatches of 8 ps are enough to increase the BER significantly.

Overall, the chaos synchronization is sensitive to changes in almost all of the OEO's parameters. Including the delay lengths of the bitwise delayed XOR operations introduced in the previous section, this ensures that potential attackers have to scan a very large parameter space if they want to estimate the correct parameters required to generate the same encryption key, hence making this an unlikely method of attack. This high sensitivity to parameter mismatches raises the question of whether fabrication variations between sender and receiver MZMs, such as a different V_π, could make chaos synchronization unfeasible in a real-world system. We have checked the effect of changes in V_π numerically and find that variations can be compensated by adjusting the feedback phase and the injection strength. This is also consistent with experimental results for chaotic key distribution using lasers with self-feedback, where similar issues have been resolved [6–8]. However, we still expect that the same type and model of modulator has to be used for sender and receiver in order to achieve low BERs. This would introduce an additional unknown for an eavesdropper and thus further enhance the security. In addition, the number of parameters that have to be estimated can potentially be increased even further, e.g., by coupling several stages of OEOs or delayed XORs with each other [7,9] or by using oblivious transfer protocols [8].

V. CONCLUSION

We show both theoretically and experimentally how secure encryption key distribution can be achieved by synchronizing chaotic OEOs with an external seed signal. We estimate the performance of a 10 GHz bandwidth OEO system by considering the maximally attainable key generation rate. When using direct sampling, key generation rates of 6 GBit/s at a BER of around 10^{-3} are possible, which outperforms electronic key distribution systems [9] and is comparable to state-of-the-art coherent feedback systems [10]. For oblivious transfer protocols, we are able to demonstrate that OEOs can synchronize up to two orders of magnitude quicker than coherent feedback systems of the same bandwidth, which leads to a significant improvement of the key generation rate. For direct sampling, we are able to show that keys fulfill the basic requirements of one-time pads so that OEOs can be used to create secure encryption keys practically indefinitely. This removes the necessity of using preshared keys and can enhance security by directly integrating the key distribution with existing encryption methods on the software level. Furthermore, since even simple algorithms become theoretically unbreakable using a one-time pad, methods such as the Vernam cipher, which can be efficiently built in hardware [12], can also be employed in combination with our key distribution scheme and thus potentially increase the efficiency and speed of encryption.

An important advantage of using an OEO system is its potential to scale to even higher bandwidths. With current off-the-shelf equipment, OEOs can attain bandwidths of 40 GHz and higher, which is beyond the current capabilities of coherent feedback systems. This will allow key generation rates to increase even further in the future, which is an essential requirement for high-speed data encryption. Another important advantage of OEOs stems from their inherent stability. For chaos synchronization in coherent feedback systems, changes of the optical phase of 180° in the seed signal or in the feedback line suffice to destroy synchrony [15]. In chaotic key distribution, this places strict demands on the phase stability of seed and feedback and will require active stabilization in real-world system to counteract phase shifts due to mechanical vibrations or temperature expansion of the optical fibers. OEOs circumvent this problem since their feedback is optoelectronic rather than coherent and phase sensitivity is thus removed altogether. At the same time, the frequencies of seed, sender, and receiver no longer have to be perfectly matched to achieve synchronization. This simplifies experimental realization, since no active stabilization of the frequencies is required. As a consequence, we report stable operation of our experimental setup over several hours of operation without the need for active stabilization or temperature insulation. Combining this inherent stability with their general ease of use and their high bandwidth, OEOs thus

present an inexpensive platform for achieving high-speed encryption key distribution.

ACKNOWLEDGMENTS

We acknowledge financial support from the Research Foundation Flanders (FWO) under Grants No. G006020N, No. G028618N, and No. G029519N, the Hercules Foundation, and the Research Council of the Vrije Universiteit Brussel.

[1] E. Tews and M. Beck, in *WiSec '09: Proceedings of the Second ACM Conference in Wireless Network Security, Zurich, 2009* (Association for Computing Machinery, New York, NY, United States, 2009), p. 79.

[2] D. Felsch, M. Grothe, J. Schwenk, A. Czubak, and M. Szymanek, in *SEC '18: Proceedings of the 27th USENIX Conference on Security Symposium, Baltimore, 2018* (USENIX Association, Berkeley, CA, United States), p. 567.

[3] S. Pitts, VPN aggressive mode pre-shared key brute force attack, Global Information Assurance Certification Paper, SANS Institute, MD, United States, 2004.

[4] G. S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic telecommunication, Trans. Am. Inst. Electric. Eng. **XLV**, 295 (1926).

[5] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. **28**, 656 (1949).

[6] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, Secure Key Distribution Using Correlated Randomness in Lasers Driven by Random Light, Phys. Rev. Lett. **108**, 070602 (2012).

[7] H. Koizumi, S. Morikatsu, H. Aida, T. Nozawa, I. Kakesu, A. Uchida, K. Yoshimura, J. Muramatsu, and P. Davis, Information-theoric secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers, Opt. Express **28**, 17869 (2013).

[8] T. Ito, H. Koizumi, N. Suzuki, I. Kakesu, K. Iwakawa, A. Uchida, T. Koshiba, J. Muramatsu, K. Yoshimura, M. Inubushi, and P. Davis, Physical implementation of oblivious transfer using optical correlated randomness, Sci. Rep. **7**, 8444 (2017).

[9] L. Keuninckx, M. C. Soriano, I. Fischer, C. R. Mirasso, R. M. Nguimdo, and G. Van Der Sande, Encryption key distribution via chaos synchronization, Sci. Rep. **7**, 43428 (2017).

[10] N. Jiang, C. Xue, D. Liu, Y. Lv, and K. Qui, Secure key distribution based on chaos synchronization of VCSELs subject to symmetric random-polarization optical injection, Opt. Lett. **42**, 1055 (2017).

[11] T. Sasaki, I. Kakesu, Y. Mitsui, D. Rontani, A. Uchida, and S. Sunada, Common-signal-induced synchronization in photonic integrated circuits and its application to secure key distribution, Opt. Express **25**, 26029 (2017).

[12] F. Huo and G. Gong, XOR encryption versus phase encryption, an in-depth analysis, IEEE Trans. Electromagn. Compat. **57**, 903 (2015).

[13] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, Chaos-based communication at high bit rates using commercial fibre-optic links, Nature **438**, 343 (2005).

[14] R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, Digital Key for Chaos Communication Performing Time Delay Concealment, Phys. Rev. Lett. **107**, 034103 (2011).

[15] I. Oowada, H. Ariizumi, M. Li, S. Yoshimori, A. Uchida, K. Yoshimura, and P. Davis, Synchronization by injection of common chaotic signal in semiconductor lasers with optical feedback, Opt. Express **17**, 10025 (2009).

[16] L. Larger, ATITLEComplexity in electro-optic delay dynamics: modelling, design and applications, Philos. Trans. R. Soc. A **271**, 20120464 (2013).

[17] Y. K. Chembo, D. Brunner, M. Jacquot, and L. Larger, Opto-electronic oscillators with time-delayed feedback, Rev. Mod. Phys. **91**, 035006 (2019).

[18] P. Mu, W. Pan, S. Xiang, N. Li, X. Liu, and X. Zou, Fast physical and pseudo random number generation based on nonlinear optoelectronic oscillators, Mod. Phys. Lett. B **29**, 1550142 (2015).

[19] W. Tian, L. Zhang, J. Ding, S. Shao, X. Fu, and L. Yang, Ultrafast physical random bit generation from a chaotic oscillator with a silicon modulator, Opt. Lett. **43**, 4839 (2018).

[20] T. E. Murphy, A. B. Cohen, B. Ravoori, K. R. B. Schmitt, A. V. Setty, F. Sorrentino, C. R. S. Williams, E. Ott, and R. Roy, Complex dynamics and synchronization of delayed-feedback nonlinear oscillators, Philos. Trans. R. Soc. A **368**, 343 (2010).

[21] R. L. Chao, J. W. Shi, A. Jain, T. Hirokawa, A. S. P. Khope, C. Schow, J. E. Bowers, R. Helkey, and J. F. Buckwalter, Forward bias operation of silicon photonic Mach Zehnder modulators for RF applications, Opt. Express **19**, 23181 (2017).

[22] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST special publication 800-22, National Institute of Standards and Technology (NIST), Gaithersburg, MD, United States, 2010.

[23] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Fast physical random bit generation with chaotic semiconductor lasers, Nat. Photonics **2**, 728 (2008).

[24] M. Sciamanna and K. Shore, Physics and applications of laser diode chaos, Nat. Photonics **9**, 151 (2015).

[25] R. M. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijtens, J. Bolk, and G. Van der Sande, Fast random bits generation on a single chaotic semiconductor ring laser, Opt. Express **20**, 28603 (2012).