Secure high-speed key distribution using chaotic opto-electronic feedback systems

F. Böhm[1,2], A. Dooms[2], G. Verschaffelt[1] and G. Van der Sande[1]

[1] Applied Physics Research Group, Vrije Universiteit Brussel, 1050 Brussel, Belgium
[2] Digital Mathematics Research Group, Vrije Universiteit Brussel, 1050 Brussel, Belgium

We present a high-speed key distribution scheme for symmetric encryption algorithms based on chaotic opto-electronic feedback systems. The nonlinear response to a common chaotic seed signal of two identical chaotic feedback systems is used to generate continuous keys in real time systems on the sender and receiver side. Based on simulations, we demonstrate that secure keys can be generated at high rates and that eavesdroppers are unable to extract the key from the open communication channels. We also present ways by which the number of hardware parameters can be extended, so that parameter estimation of the feedback system becomes ineffective to derive the key.

Modern encryption algorithms rely on either symmetric or asymmetric ciphers to securely transmit data between sender and receiver. In asymmetric algorithms, encryption is performed with private and public keys, which provide a high level of security but also require significant computational resources and are thus typically unfit to encrypt large streams of data in real time. Symmetric encryption algorithms on the other hand can provide good performance and sufficient levels of security. However, since sender and receiver are using the same key, generation and exchange of the secure keys poses a major security risk and allows eavesdroppers to decrypt messages once a key has been stolen. We consider an approach for secure key distribution based on chaotic opto-electronic feedback systems, where continuous keys are simultaneously generated on the sender and the receiver side and thus protected from eavesdroppers. In our concept, both receiver and sender have identical chaotic feedback systems, that are injected with a mutual chaotic seed signal (Fig.1a). The nonlinear response of the chaotic feedback systems to the seed is sampled to generate keys of arbitrary length in real time. Since sender and receiver are identical, the response is the same on both sides so that a shared key can be generated without the necessity to exchange it and only the seed signal is transmitted through open communication channels. The chaotic feedback system acts as a complex transfer function, so that the seed signal shares no mutual information with the response and makes it impossible for an eavesdropper to extract the key from any of the open communication channels.

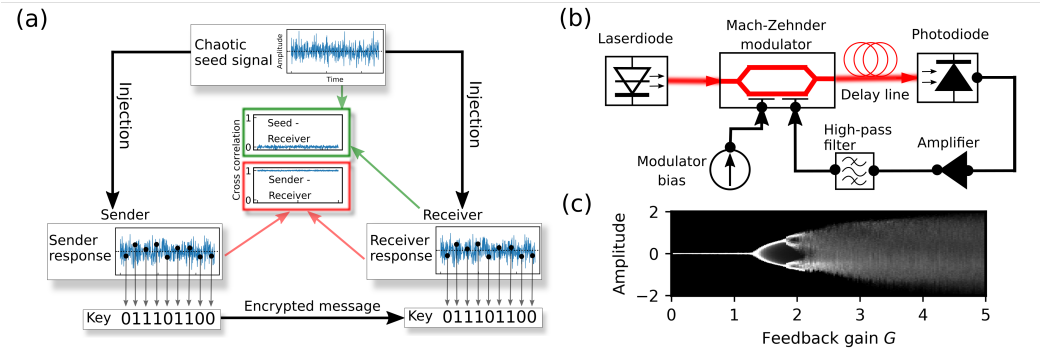

Figure 1. (a) Schematic of the encryption scheme. (b) Schematic of an OEO. (c) Bifurcation diagram of an OEO.

While the above scheme has been studied in semiconductor lasers with optical feedback [1] and electrical circuits [2], we consider opto-electronic oscillators (OEOs). OEOs can easily be integrated with existing telecommunication technology, are easy to control and can be fabricated from off-the-shelf photonic components. OEOs are also widely studied in different fields and well known to exhibit rich chaotic dynamics when subjected to long time-delayed feedback [3] (Fig.1c). In a typical setup (Fig.1b), laser light passes through a nonlinear optical modulator and an optical delay line before being detected by a photodiode. The measured photovoltage is amplified, passed through a high-pass filter and fed back to the modulator, so that a time-delayed feedback system is formed. To model such a system, we use a time-delayed differential equation model, which describes the time evolution of the filtered feedback signal $x(t)$ and the photovoltage $y(t)$ in response to the seed signal $s(t)$ and noise $\xi(t)$ as

$$\dot{x}(t) = -\left(\frac{1}{\tau_l}+\frac{1}{\tau_h}\right)x - \frac{1}{\tau_h}y + \frac{1}{\tau_l}G\cos^2(x(t-T)+\varphi+I\,s(t)+\xi(t)) \quad (1)$$

$$\dot{y}(t) = \frac{1}{\tau_h}x\ . \quad (2)$$

A complete list of all parameters is given in table 1.

parameter		**value**	**parameter**		**value**
G	roundtrip gain	4 [4]	$\frac{1}{2\pi\tau_l}$	low-pass cutoff	10.6 GHz [10.6 GHz]
I	injection strength	5	$\frac{1}{2\pi\tau_h}$	high-pass cutoff	1 GHz [1 GHz]
T	time delay	220ps [230ps]	φ	modulator bias	2 [2]
ξ	Noise (standard deviation)	0.06 [0.06]			

Table 1. List of parameters for the seed source, the sender and the receiver. Parameters for the seed are given in square brackets. Parameters for receiver and sender are identical.

To implement the key distribution scheme, chaotic OEOs are used for the seed, the sender and the receiver. Figure 1c shows a bifurcation diagram of the seed OEO, as the feedback strength is increased. Over a cascade of Hopf and period doubling bifurcations, the system reaches a regime of strong chaos, which is used to emit the seed signal. Sender and receiver are in the same dynamical regime, so that no correlation exists between all signals at $I = 0$. By varying the injection strength and the time delay of sender and receiver, we search for regions, where both systems are able to synchronize. Figure 2b shows the cross correlation between sender and receiver in a parameter sweep. We find that, as the injection strength increases, sender and receiver become locked to the seed signal and synchronize.

Since both signals become identical in this parameter region, continous identical keys can be derived from the response by 1bit sampling, where positive values represent the “1” bit and negative values the “0” bit. Due to the fast dynamics of the OEOs, we can achieve a theoretical sampling rate of 1.7 GSa/s with the given parameters, which is limited by the autocorrelation time of the signal. We analyse the quality of generated keys in regards to noise robustness and randomness. For noise robustness, we measure the bit error ratio

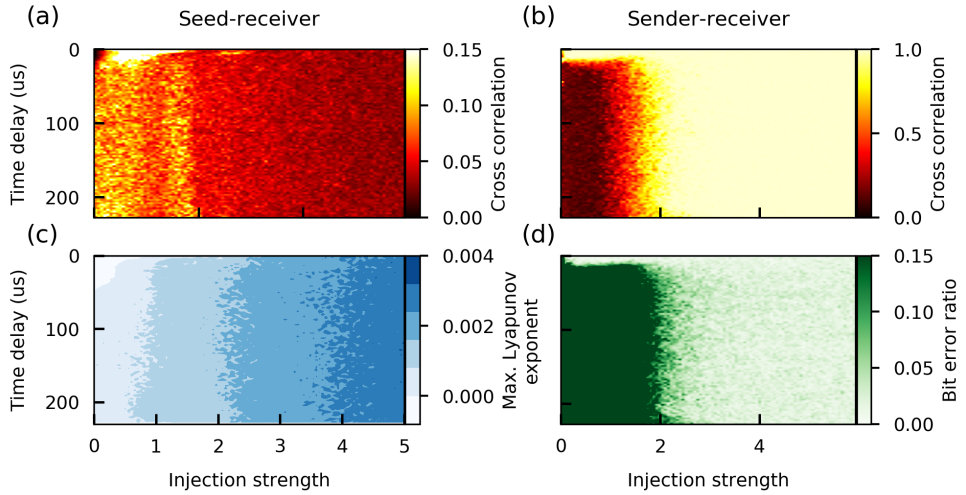

Figure 2. Cross correlation between seed and receiver (a), sender and receiver (b), largest Lyapunov exponent for the receiver (c) and bit error ratio for the receiver (d) in a parameter sweep of injection strength and time delay.

(BER) between keys generated on the sender and the receiver side. The BER measures the percantage of differing bits between both keys, which arise due to optical and electronic noise. Figure 2d shows the BER for 400 bit long keys in a parameter sweep of injection strength and time delay. In the region of synchronization, an optimal BER of around 1 percent is achieved. Since OEOs with narrow bandpass filers can exhibit significantly lower noise levels than those assumed in our simulations [4], we expect that even lower BERs can be expected in an actual setup.

The randomness of a key is an important aspect in regards to security, i.e. entropy should be maximal so that no sequences are correlated. It is thus important that the chaos is fully developed so that very small perturbations will already lead to a diverging of dynamics at small timescales. A good measure for this is the maximum Lyapunov exponent, which has to be positive and large. We find that the Lyapunov exponent increases as the injection strengh is increased (Fig.2c), so that the seed injection drives sender and receiver into a more fully developed chaos. We also directly measure the quality of 10000 bit long random keys with the NIST test suite [5] and find that the generated keys pass all tests, hence corroborating the randomness of sender and receiver.

To ensure security during the key generation, we have to establish that no information about the generated keys are revealed through the public channels. In the following, we consider two likely attack scenarios. In the first, the eavesdropper has no prior knowledge of the system and tries to derive the key directly from the seed signal. In this case, it is important that no correlation exists between both. We test this by analyzing the maximum of the cross correlation between the seed and the receiver (or correspondingly the sender) for 230,000 samples (Fig.2a). We find that with higher injection strength, the correlation between seed and receiver decreases. In the parameter region where $I > 4$, we achieve a minimum value of 0.014 for the maximum of the cross correlation. We compare this value to the cross correlation of two random number sequences of equal length that were generated by a pseudo random number generator, and achieve on average a maximal cross correlation of 0.012. This corroborates that no significant correlation exists between the seed signal and the response of sender and receiver and thus demonstrates that an eavesdropper cannot derive the key from the seed signal alone.

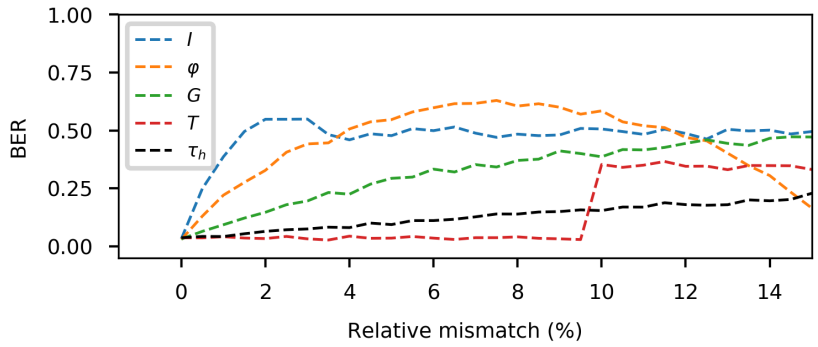

Figure 3. Influence of mismatched parameters (a) and mismatch of the mask (b) on the BER.

As a a second method of attack, we assume that the eavesdropper has prior knowledge about the dynamical system (1) and (2), so that intercepting the key requires an estimation of the system parameters. It is thus important that (i) the system is very sensitive to mismatch of parameters and (ii), the number of parameters to be estimated is large. In figure 3, we test the sensitivity of the BER to changes of the parameters. These parameters can easily be adapted and exchanged between sender and receiver, either on pysical meeting or by secure asynchron encryption methods to ensure security. We find that synchronization between sender and receiver is very sensitive to changes in the injection strength, the modulator bias and the feedback gain. Mismatches of less than 1% already result in a sharp increase of the BER, hence demonstrating that these paramters require very accurate estimation. The BER quickly increases to around 50%, which is equivalent to guessing the key from random numbers. Lesser sensitivity can be observed for the high-pass cutoff. For the the time delay, a sudden increase is seen at 9% relative mismatch. Changes in low-pass cutoff appear to have only very little influence on the BER. For a potential attacker, this leaves 5 parameters that have to be estimated with little tolerance, which does not include the necessity to know the timing of the 1-bit sampling.

In conclusion, we have shown how secure key distribution can be achieved with chaotic OEOs. Based on simulations, we have demonstrated that key generation at rates of up to 1.7 GSa/s can be achieved. We found that a potential attacker without prior knowledge is not able to derive the key directly from the open communication channels. With prior knowledge of the system, a parameter estimation requires to match the actual parameters exactly due to the sensitivity of the synchronization between sender and receiver, hence making it difficult to extract the key. Key distribution with chaotic OEOs thus presents a promising approach to generate indefinetely long key sequences without the necessity to exchange them.

References

[1] H. Koizumi, et.al., “Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers,” Optics Express, vol. 21, 17869-17893, 2013.

[2] L. Keuninckx, et.al., “Encryption key distribution via chaos synchronization,” Scientific Reports, vol. 7, 1992.

[3] T.E. Murphy et.al., “Complex dynamics and synchronization of delayed-feedback nonlinear oscillators”, Phil. Trans. R. Soc. A, vol. 368, 343-366, 2010.

[4] L. Maleki, “The opto-electronic oscillator,” Nature Photonics, vol. 5, 728-730, 2011

[5] A. Rukhin, et.al., “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application”, NIST SP, 800-22, 2010