ARTICLE

Check for updates

Private communication with quantum cascade laser photonic chaos

Olivier Spitz [1,2 ✉], Andreas Herdt[3], Jiagui Wu[4,5], Grégory Maisons[2], Mathieu Carras[2], Chee-Wei Wong[4], Wolfgang Elsäßer[3] & Frédéric Grillot[1,6]

Mid-infrared free-space optical communication has a large potential for high speed communication due to its immunity to electromagnetic interference. However, data security against eavesdroppers is among the obstacles for private free-space communication. Here, we show that two uni-directionally coupled quantum cascade lasers operating in the chaotic regime and the synchronization between them allow for the extraction of the information that has been camouflaged in the chaotic emission. This building block represents a key tool to implement a high degree of privacy directly on the physical layer. We realize a proof-of-concept communication at a wavelength of 5.7 μm with a message encryption at a bit rate of 0.5 Mbit/s. Our demonstration of private free-space communication between a transmitter and receiver opens strategies for physical encryption and decryption of a digital message.

[1] LTCI, Télécom Paris, Institut Polytechnique de Paris, Palaiseau, France. [2] mirSense, Centre d'intégration NanoInnov, Palaiseau, France. [3] Technische Universität Darmstadt, Darmstadt, Germany. [4] Fang Lu Mesoscopic Optics and Quantum Electronics Laboratory, University of California Los Angeles, Los Angeles, CA, USA. [5] College of Electronic and Information Engineering, Southwest University, Chongqing, China. [6] Center for High Technology Materials, University of New-Mexico, Albuquerque, NM, USA. ✉email: olivier.spitz@telecom-paris.fr

Free-space communication has experienced a renewed interest in several optical wavelength domains where the atmosphere has high transparency. Experiments in the ultraviolet have recently achieved a transmission at 1 Gbits/s with III-nitride micro-LEDs[1]. In the mid-infrared, several strategies have emerged in order to produce high-bandwidth sources emitting in the transparency window around 4 µm. Communication up to 70 Mbits/s was demonstrated with interband cascade lasers (ICLs)[2] and transmission at several Gbits/s was achieved with wavelength down-conversion and up-conversion between 1550 nm and 3594 nm, respectively[3]. With quantum cascade lasers (QCLs), transmission at similar high speeds has been reported both at room[4] and cryogenic temperatures with a free-space television link application[5].

Despite the substantial investments into development of mid-infrared wavelengths emitters back in the seventies, these systems remained bulky, inefficient, and expensive[6]. The recent accelerated advances in QCLs[7], as well as progress in mid-infrared detectors[8,9], enable low-size, low-weight, energy-efficient, and therefore affordable optical systems operating at room temperature in the mid-infrared. The advantage of wavelengths between 3–5 µm and 8–11.5 µm compared to near-infrared wavelengths is that their transmission in the atmosphere remains high even though the presence of fog or haze[10]. Moreover, a transmission between 8 and 11.5 µm implies stealth because the thermal black-body radiation shows a strong background at these wavelengths[11]. Therefore, it would be very difficult to detect transmitted signal reliably in this mid-infrared window and for the moment, only QCLs and CO_2 lasers can output powerful beams at such wavelengths. QCLs are unipolar semiconductor lasers emitting in the mid-infrared domain[12] and they are acknowledged for various applications in this wavelength domain[13–17].

Due to the large data-carrying optical signals propagating free-space, implementation of secure cryptosystems has raised attention. Two options are currently available for those cryptosystems: ghost polarization communication[18] and quantum key distribution (QKD). The latter has been thoroughly developed during the past 20 years with a focus on visible light and free-space propagation[19]. The current challenge is to realize QKD-based ground-to-satellite communication[20] and one of the Gordian knots resides in overcoming the background noise that is detrimental during daytime[21]. Propagation conditions are more favorable during night[22] but this strongly restrains the availability of the transmission link and that is the reason why other wavelength domains are currently investigated. For instance, near-infrared light has drawn attention[23] because it is immune to parasitic visible-light perturbation and because optical sources are widely available in this wavelength domain known for telecom applications. Though very appealing because it relies on physically uncrackable photon entanglement, QKD for large-scale communication systems is still hindered by the performances of low-speed, low-yield, expensive transmission apparatus[24]. Furthermore, due to the lack of single-photon detectors, QKD technology is not yet available at mid-infrared wavelength that is one of the most relevant transmission domains.

An alternative, nearer-term pathway for free-space, high-bandwidth private optical communication relies on using chaotic waveforms from photonic oscillators[25]. In such a way, the privacy of the transmission mostly results from the fractal dimension and the complexity of the strange attractor where multiscale similarity of the density of trajectories exists[26]. Practically, several methods of encryption were studied with a particular focus on the chaos being the carrier among which the message is hidden. The main idea is to hide a message with a small amplitude within the chaotic signal of the transmitter so that the message does not disturb the larger chaotic fluctuations and remains well concealed

from a potential eavesdropper[27]. Indeed, synchronization of two very similar optoelectronic devices, in the following referred to as twins, is robust to small changes in the coupling strength[28]. Consequently, the response-twin-laser, in the following referred to as slave, will still synchronize to the chaos of a chaos-emitting driving twin-laser, in the following referred to as master, even in the presence of a perturbation that is due to message encoding. This mixed signal is then sent to the receiving twin-laser and a detector. As the receiver synchronizes only onto the chaotic fluctuations, subtracting the signal of the receiver from that of the detector allows recovering the concealed message[29]. The proof-of-concept of such configuration in the optical domain was given in 1998[30,31], followed by the extension to semiconductor lasers under optical self-feedback, which were found to exhibit high-dimensional chaos[32], leading to high bit-rate private transmission[33,34] and eventually to a real-field telecommunication system in the metropolitan fiber network of Athens[35]. It is important to underline that this type of communication link is private rather than secure. Indeed, secure would mean that the system is totally unbreakable for anybody whereas private means that it offers a decent way of encryption that is enough to defy a not very motivated eavesdropper. Other methods of communication relying on chaos have been successfully tested through an accurate control over the emitted chaotic fluctuations[36]. The control can be utilized to tune the signal emitted by the chaotic system so that it follows a prescribed symbol sequence, and this allows encoding any desired message from a chaotic oscillator. More recently, optomechanical chaos was also observed in silicon microcavities, opening the way towards synchronous-chaos secure-channel links via chip-scale oscillators[37]. As for free-space communication, only numerical modeling has proven the possibility of a private free-space communication, but for laser diodes in the near-infrared[38]. Our prior works showed that QCLs are, under certain conditions, able to exhibit mid-infrared chaotic oscillations[39,40].

In this work, we demonstrate a private communication link operating free-space in the mid-infrared window and based on chaos synchronization in QCLs. In our configuration, chaos does not originate from ray dynamics in a laser cavity[41] but from the temporal dynamics driving the evolution of both photon and carrier densities. The bandwidth of the high-dimensional chaos we generate allows for a transmission rate at 0.5 Mbits/s, and with an error ratio compatible with common telecommunication correction schemes. All in all, the proposed QCL system relying on a message embedded into chaotic waveforms provides superior privacy from hacking.

Results
Mid-infrared chaos synchronization and anti-synchronization. After having considered the principles of free-space optics communication, we now define and investigate the progress and our strategy concerning chaos synchronization and message encoding. In the following, the potential eavesdropper will be referred as "Eve" and, by extension, "she" or "her". The experimental setup that we used for the synchronization of chaos consists out of a distributed-feedback (DFB) master laser driven chaotically by optical self-feedback and a DFB slave laser and is depicted in Fig. 1. In our previous investigations about mid-infrared chaos[40], we could hardly isolate the narrow chaotic islands of the bifurcation diagram[39] under continuous operation. This issue mainly came from an imperfect setting of the mid-infrared polarizer in front of the feedback mirror and we solved this problem by placing the polarizer on a piezoelectric rotating mount. Therefore, we are now able to precisely tune the feedback strength and select the one leading to the most appropriate optical chaos. Contrary to
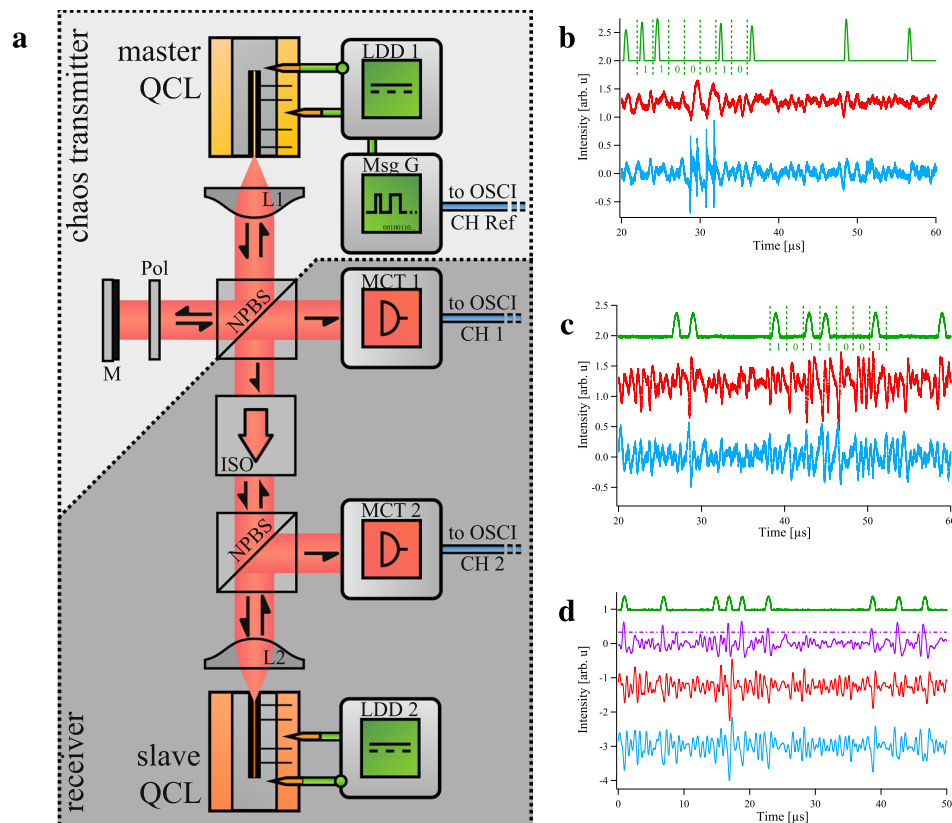
Fig. 1 Principle of operation. Left panel: experimental setup showing the transmitter unit (light gray) and receiver unit (dark gray). **a** In the transmitter part, the master laser is driven chaotically by self-optical feedback that is produced by the gold-plated mirror (M). The feedback strength is precisely tuned thanks to a mid-infrared polarizer (pol) with piezoelectric rotation. Thanks to a non-polarizing beam-splitter (NPBS), part of the signal from the master laser is sent into the slave laser through an optical isolator (ISO) to avoid back-coupling. Both the signal from the master QCL and the signal from the slave QCL are retrieved with a MCT detector and then subsequently analyzed. LDD: laser diode driver. Right panel: time series retrieved during the private communication process. **b** Synchronization case. **c** Anti-synchronization case. **d** Filtered time series during message recovery in the anti-synchronization case. The color code is as follows: time trace of the message (green), which is magnified by a factor 30 for a better visualization; time trace of the intensity of the master laser (red) with encoded message hidden within the signal; time trace of the slave laser (blue); time trace of the difference between the red and the blue signal (purple), the dashed line sets the limit between the "0"-bits and the "1"-bits during the analysis of the purple time trace.

some schemes found in laser diodes (see ref. [42] for instance), when the master and the slave laser are not coupled, the slave laser is not chaotic because there is no mirror in front of it, so we are in an open-loop configuration. The output of the master is sent towards the slave laser through an optical isolator to avoid back-reflections and the signal of the drive and the response are detected with Mercury–Cadmium–Telluride (MCT) detectors. The signal from the MCT detectors is analyzed with a fast oscilloscope and an RF spectrum analyzer. When the optical frequency of the master and the slave are matching, synchronization occurs and if the master is driven chaotically, the slave will reproduce the same chaotic pattern[43]. Modifying some of the operation conditions, such as the pump current of the master laser or the coupling conditions, can also lead to anti-synchronization[44], sometimes called reverse synchronization. Though both synchronization and anti-synchronization were achieved in our configuration, we are not able to give a precise set of parameters explaining the switching between synchronization and anti-synchronization. In other semiconductor lasers, these two states can appear for similar conditions and for instance, ref. [44] shows an example where the two types of synchronization can be achieved in the same time trace by finely tuning the pump current of the lasers.

In our case, the most relevant results in terms of mid-infrared private transmission were achieved with anti-synchronization and

consequently, we will briefly describe a synchronization case before focusing on the anti-synchronization configuration. An example of chaos synchronization with the enciphered message is given in Fig. 1b while an example of chaos anti-synchronization is displayed in Fig. 1c. In the case of anti-synchronization, the filtered time traces can be visualized in Fig. 1d. In the latter, the initial unfiltered message is displayed in green, while the filtered master signal and the filtered slave signal are displayed in red and blue, respectively. The purple time trace corresponds to the difference between the red and the blue signal and a dash-dotted purple line at the constant value 0.33 illustrates the threshold that is used to discriminate 0 and 1 in the purple time trace. One can see that most of the "1"-bits of the purple time trace correspond to the "1"-bits of the green time trace, except for the third "1"-bit of the green time trace. As the master's signal conveys both the chaotic carrier and the hidden message while the slave's signal conveys only the chaotic carrier because of the properties of synchronization, the subtraction of the filtered master's signal by the filtered slave's signal reproduces a copy of the initial message. The agreement between the original message and its copy will be evaluated hereafter.

As we shall perform communication with two QCLs, the message has to be included in the bias current, with a chaos modulation (CMo) configuration. The voltage-response amplitude of the enciphered bit code is thirty times lower than that of

the largest chaotic fluctuations. Indeed, ciphering with a CMo configuration and ensuring that a "1"-bit induces not more than a 10% increase of the average laser intensity are two key requirements for enhanced-privacy chaos transmission[26]. Besides, we observed that privacy is detrimentally affected when increasing the amplitude of the small message signal, and the current configuration with a thirty-time lower response-voltage was the optimized trade-off between privacy and decipherable message after legitimate recovery.

The frequency encoding and modulation pattern were chosen accordingly with the cut-off frequency of the modulation current source (low-pass filter below 2 MHz) and that of the mid-infrared detector (high-pass filter above 1 MHz). This is the reason why an usual non-return-to-zero format could not be selected because many frequencies included in the pattern would be cut either by the current source or by the detector. In order to comply with these constraints, a pulse-up pattern at 1 MHz was chosen because it is composed of very few frequencies outside the frequency range 1–2 MHz. Nevertheless, this was not enough to ensure that the bit is not distorted or creates an undershoot, so a blank always follows a "1"-bit. To sum up, a "1" is encoded with a half-sine and a subsequent blank, while a "0" is encoded with two consecutive blanks. This coding scheme is similar to that which is used in various configurations of high-speed private transmission[45,46], except that in our configuration, we use a return-to-zero format with 25% duty cycle[47]. It is also worth noting that the code frequency is below the cut-off bandwidth of the chaotic carrier, which is 5 MHz.

Analysis of transmission with chaos synchronization. The purpose of the private communication is to transmit a train of 50 bits among which 11 are "1"-bits. The duration of this analysis is 1582 µs, corresponding to 791 bits. Once the message is hidden and the synchronization is achieved, the quality of the transfer is evaluated with correlation diagrams (Fig. 2a), for the filtered time series. The 1D correlation diagram allows retrieving the time lag between the master's signal and the slave's signal and is given in insets for two different time scales. This 1D correlation diagram has a large output (close to 1) only for a short range of time, and that confirms the outcome unpredictability of our chaotic signal. The 2D correlation diagrams represent the output power of the slave laser as a function of the output power of the master laser. For a perfect synchronization, the correlation diagram is a straight line with a positive slope and with a Pearson's correlation coefficient of 1[48]. This line widens and the value of the correlation coefficient decreases down to 0 in case of parameters mismatch between the slave device and the master device[49]. Our synchronization exhibits a correlation coefficient of 0.70. The experimental result of the recovery can be found in Fig. 2b. The recovery chart shows the binary-converted message we want to transmit (in green) and the subsequent bits we retrieved for the master, the slave and the difference (in red, blue and purple, respectively). 212 errors are retrieved when analyzing only the signal of the slave QCL, 171 errors are retrieved when analyzing only the signal of the master QCL and 56 errors are retrieved when analyzing the difference signal between the master and the slave. As our message is made of 11 "1"-bits among 50 bits and our analysis deals with 791 bits, if Eve naively tries to decipher the full transmission only with "0"-bits, she would end with 174 errors. This value confirms that the analysis of the master's signal alone, even with an appropriate filtering, does not give any details about the transmitted bit sequence. With her bit-error-rate (BER) being 22%, we are also very close to 25% that is the lower limit commonly accepted for a non-decipherable transmission[50]. We further analyzed the previous 791-bit sequence by carrying out

the same analysis for portions of the signal. Figure 2c, d describes the correlation analysis and recovery process for bits 1–191, while Fig. 2e–f describes the correlation analysis and the recovery process for bits 401–591. In these two configurations, the correlation plots look similar to those given for the full-length sequence and the subtraction process strongly improves the message recovery. We also decided to plot the same charts when analyzing simultaneously the slave signal from Fig. 2c, d and the master signal from Fig. 2e, f. These results are gathered in Fig. 2g, h and show that the correlation is weak in that configuration and, subsequently, the message is poorly recovered. In this case, the synchronization exhibits a correlation coefficient of 0.20. This information indicates that, even if the message sequence is repeated, this does not imply a repetition of the chaotic pattern used to conceal the message. Thus, this is different from what occurs in the case of a high amplitude periodic modulation leading to synchronized bursts with external optical feedback[40].

Analysis of transmission with chaos anti-synchronization. We now investigate the configuration relying on anti-synchronization to transmit a realistic message which is made of 100 bits with 44 "1"-bits among them. As previously explained, we carry out a correlation analysis for the filtered time series (Fig. 3a), which are also reversed to allow for a better comparison with the synchronization configuration. The 1D correlation diagram allows retrieving the time lag between the master's signal and the slave's signal, which is 64 ns in this case. The quality of the correlation is increased in the anti-synchronization case because the correlation coefficient derived from the 2D correlation heatmap has a value of 0.92. The recovery process can be seen illustrated in Fig. 3b and results in 12 errors out of 191 bits. Once again, the master signal gives no clue about the hidden message because the recovery process leads to 86 errors while Eve would obtain 84 errors if she deciphered the sequence only with "0"-bits. This time, her error ratio is 45% and we perform better than in the synchronization case where her BER was 22%, both in the case she would intercept the master signal and apply relevant filtering. This means that we are now in a configuration where Eve performs worse than the limit for a non-decipherable transmission. In order to complement our study, we also display the eye diagram for each component in Fig. 3c. The eye diagram is a tool to evaluate the quality of the transmission and a successful communication is assessed by an open eye[51]. A compromise has to be found between a transmission with a low BER and an impossible recovery for an illegitimate receiver. In this configuration corresponding to a realistic private transmission, the lowest BER we were able to achieve, while ensuring a camouflaged message, is 6%, corresponding to 12 errors out of 191 bits in Fig. 3b. It was possible to achieve lower values of BER but the message started to become obvious among the eye diagram of the filtered master signal and consequently, the privacy of the transmission was threatened. Except for the initial message (green curve), all other eye diagrams are retrieved for the already filtered signals with the best fitting parameters. So this basically means that, even if she knows exactly what is the encrypted message, Eve has absolutely no chance to decipher that message by applying the most relevant filter to the master signal, as it can be visualized from Fig. 3c (red curve) where no indication about the hidden message can be derived.

Discussion

By taking support from our previous findings about optical chaos, we demonstrated a free-space private communication at mid-infrared wavelength. This achievement was combined through anti-synchronization and message enciphering, with a bit rate of
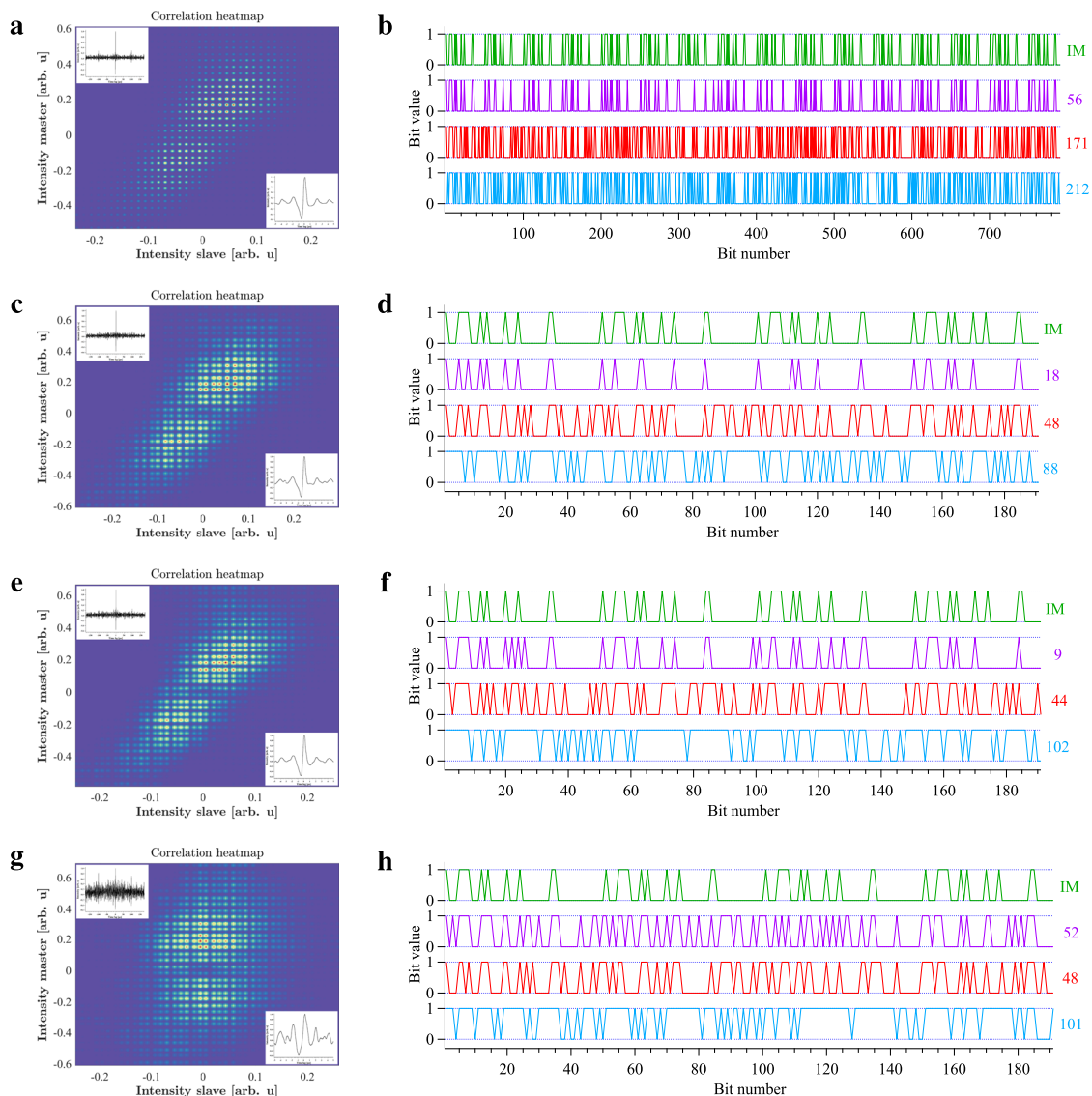
Fig. 2 Private communication with chaos synchronization. 2D and 1D (insets) correlation diagrams for the filtered intensity of the slave and the master QCL (left panels). Bit series (right panels) for the initial message (IM in green), the difference (in purple), the master's signal (in red) and the slave's signal (in blue). Except for the initial message, the number of errors is written on the right side of the bit series, with the corresponding color. **a**, **b** correspond to the global sequence with 791 bits, **c**, **d** correspond to a portion of the global sequence, between 1 and 191, **e**, **f** correspond to a portion of the global sequence, between 400 and 591, **g**, **h** correspond to a cross-analysis between the slave signal of the second row and the master signal of the third row.

0.5 Mbits/s and a BER of 6%. It is worth noting that this achievement is also possible with a synchronization scheme, but with degraded performances. Even if the mid-infrared wavelength of this transmission makes it relevant for further applications, improvements must be realized in order to comply with communication standards. Continuous progress in forward error correction (FEC)[52] allows now envisioning error-free transmission for a BER limit as high as 4%[53]. Consequently, our configuration with a BER of 6% could be used as a real-field system if we can reach a BER of 4%, which is a completely realistic improvement. The price to pay, however, is a reduction of the data rate because such correction requires additional bits during the transmission, which amounts to 27% of the initial message length in the case of a 4% BER limit. Lower values of BER decrease the number of extra correction bits and are thus desirable in our proof-of-concept experiment. It is relevant to note that FEC has a step-like efficiency, so BER below the critical value will be greatly enhanced while BER above the critical value will

remain mostly unchanged[50] and consequently, the privacy of the transmission is not threatened by this technique. Even though CMo gave better results in terms of BER with other semiconductor lasers[54], it would be interesting to compare this method with chaos masking, for instance using mid-infrared external modulators that already achieve dozens of Mbits/s[55]. Meanwhile, several opportunities can be envisioned in order to enhance the real-field performances of this experimental proof-of-concept. The first one will be to increase the distance between the master and the slave laser because it is currently only 1-m long. If a distance of several kilometers can be achieved, private communication can be well adapted for transmission between ground stations or vehicles and various aircraft. To perform such long-distance communication, it is mandatory to switch from the current 5.7 μm wavelength towards wavelengths that are more suitable for optimal transmission through the atmosphere, for instance 4 μm and 10 μm. While the latter can almost solely be achieved with QCLs, the former can be realized by other
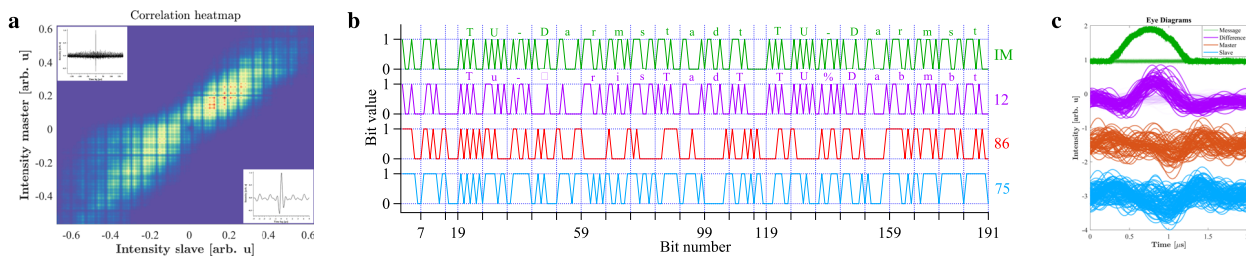
Fig. 3 Private communication with chaos anti-synchronization. a 2D and 1D (insets) correlation diagrams for the filtered intensity of the slave and the master QCL. The filtered signal of the slave laser was flipped so that the 1D correlation diagram has a maximum value of 1 and the 2D correlation diagram shows a positive correlation (instead of −1 and negative correlation, respectively). **b** Bit series for the initial message (IM in green), the difference (in purple), the master's signal (in red), and the slave's signal (in blue). Except for the initial message, the number of errors is written on the right side of the bit series, with the corresponding color. The translation of the difference bit signal is also displayed by comparison with the initial message. The private mid-infrared transmission achieves a BER of 6%, which corresponds to 12 errors out of 191 bits. **c** Experimental eye diagrams for the four time traces displayed in Fig. 1d. From these diagrams, one can see that it is impossible to recover the message only from the signal of the master QCL but it becomes possible for most of the bits from the difference signal. Bits deciphered as "0" are drawn with a light color while bits deciphered as "1" are drawn with a stressed color (particularly visible in the difference eye diagram where the "1" and "0" are well separated).

semiconductor lasers like ICLs. The most relevant option between these two lasers could be the one that is able to generate chaos with the largest bandwidth. As our private communication system is meant to be mobile, inquiries to find the semiconductor mid-infrared sources with the minimum bulkiness and energy footprint[56] will also be undertaken.

Further attention will be paid to evaluating the effect of the atmospheric turbulence on the chaos synchronization and this will guide the choice of the most appropriate wavelength. However, a transmission rate of hundreds of Gbits/s can sometimes be required and this does not seem realistic with the aforementioned semiconductor lasers. A relevant option, in this case, would be to transmit only a secret key with the chaotic scheme and then use other means to achieve a very high-speed transmission. As the key can be as small as a few dozens of kbits[57], the data rate is not an issue because we showed that it was possible to transmit a message at 0.5 Mbits/s in this work. However it is worth noting that, in the case of low-speed private communication, chaos-masking transmission is challenged by QKD. Further investigation can also consider chaos and synchronization in phased-array QCLs from Talbot-based cavity[58]. In such a case, several carrying chaotic emitters for multiple QCL transmitters could be modulated by different message signals to accommodate the larger bandwidth of the carrier. Last but not least, with the emergence of chalcogenide optical fibers[59], private transmission in the mid-infrared can also be considered in more conventional telecommunication networks, thus encouraging efforts towards higher wavelengths related to the ever-growing demand for communication services.

Methods

Synchronization conditions. Apart from the chaotic features observed with the RF spectrum analyzer and the digital oscilloscope, it is possible to confirm that the master signal is well injected into the slave by observing the behavior of the optical spectrum with a Fourier transform infrared spectrometer. Indeed, under free-running operation, the slave laser is mono-mode and it turns to be multi-mode when the synchronization is effective, as can be seen in Fig. 4. The broadening of the optical spectrum has been widely observed in semiconductor lasers generating deterministic chaos[60]. However, as already shown with the 2D correlation diagram, the synchronization between the master and the slave is not perfect and consequently, the BER remains high though sufficient for a proof-of-concept experiment. That limitation is due to the differences in the operation conditions for the two lasers in order to match their optical wavelengths, which is a mandatory condition in order to obtain a, yet imperfect, synchronization. In our configuration, the master laser is pumped in continuous mode at 750 mA and the temperature of the device is 251 K. The slave laser is pumped in continuous mode at 510 mA and kept at a temperature of 278 K. These operation conditions were achievable because the two lasers were mounted in separated Newport LDM-4872 sockets, which were further sealed and purged with gas nitrogen. It is worth noting that, apart from the
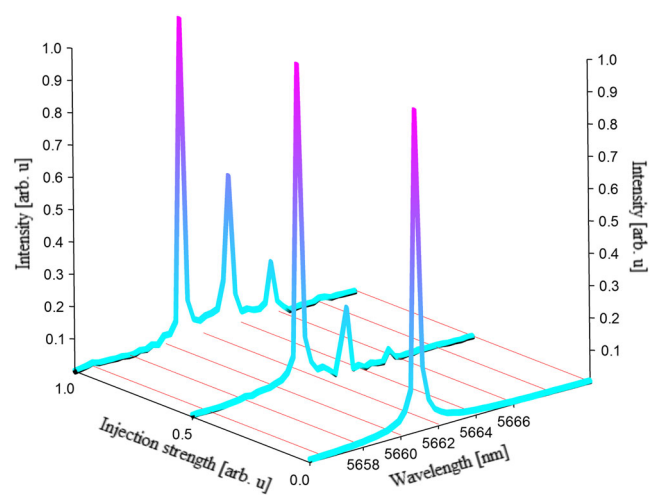

Fig. 4 Optical spectrum evolution during the coupling process. Optical spectrum of the slave laser when it is biased at 512.4 mA and for several levels of injection from the master laser. The QCL is monomode under free-running operation and when increasing the injection strength, a second mode is appearing with a subsequently following third mode. The amplitude of these side modes increases with the injection strength while the main mode remains unchanged.

case where the DFB master laser and the DFB slave laser have the same optical wavelength, it is also possible to achieve synchronization (or anti-synchronization) when the main optical frequency of the master laser is equal to that of one of the suppressed side-modes of the slave laser. Practically, this means that changing the bias current of the slave laser allows scanning the optical frequency and achieving synchronization around the aforementioned side-modes. Such current values are gathered in Table 1 and a deviation as small as 1 mA from these values hinders the synchronization because the slave QCL is no longer injection-locked to the master QCL. Indeed, the synchronization can only be possible if the master and the slave laser are in the injection-locking range. Although these multiple current values could ease the task for Eve, it is important to remember that QCLs are currently more difficult and more expensive to grow than conventional laser diodes or VCSELs. As this work is a proof-of-concept experiment, we did not analyze all the parameters which could lead to a degraded correlation between the master and the slave. In other semiconductor lasers, the key parameters to ensure a reliable synchronization are the photon lifetime, the carrier lifetime, the gain and the linewidth enhancement factor[61,62]. In our experiment, we also did not test the influence of the distance between the two lasers, which was fixed at one meter. However, we varied the injection strength and this operation did not cause any obvious degradation of performance even with an injected optical power of a few mW at the slave level. Considering that our master laser can generate up to 240 mW of optical power, this means that the beam can undergo an attenuation of roughly 20 dB, which is equivalent to a few kilometers transmission at mid-infrared wavelength. However, this does not take into account the multiple distortion and beam

Table 1 Bias currents of the slave QCL leading to synchronization when the bias current of the master QCL is fixed at 750 mA. The temperature of the master laser is fixed at 251 K while the temperature of the slave laser is fixed at 278 K.

Bias current (mA)	370	400	429	457	484	510	538	562	586	608

Table 2 Characteristics of the passband filter applied to the master's signal and the slave's signal before subtraction.

Parameter	Value
Passband low frequency	0.250 MHz
Passband high frequency	2.000 MHz
Passband ripple	0.1 dB
Stopband attenuation	60 dB
Stopband low frequency	0.137 MHz
Stopband high frequency	2.113 MHz

expansion during the transmission path. Being able to perform the synchronization even with reduced injected power in the case of QCLs is in good agreement with laser diodes experiments exhibiting a wide coupling window[63].

Optical sources. Technology of quantum devices developed by mirSense was used to fabricate DFB QCLs under study. Both their intensive (e.g., cavity length, facet coatings, etc.) and extensive parameters (e.g., carrier lifetime, gain, etc.) were matched to the best extent. The lasers emit single-mode radiation around 5.7 μm with 30 dB side-mode suppression and exhibit a wavelength shift when varying the temperature or current of operation. The order of magnitude of wavelength shift with continuous bias is 10 nm A^{-1}. The two QCLs are however different in terms of output power since the master laser is able to output up to 240 mW at 251 K, while the slave laser generates up to 15 mW at 278 K. The discrepancy in temperatures is explained by the strong requirement of wavelength matching between the master and the slave. The devices under study were grown by molecular beam epitaxy on an InP cladding and incorporates 30 periods of AlInAs/GaInAs layers[64]. The upper InP cladding is n-doped at a value of 10^{17} cm^{-3} in order to get electrical injection but without introducing any plasmonic effects. The design for the DFB laser uses index coupling and metal grating[65]. This enables single-mode emission using a top metal grating with a coupling efficiency of $\kappa \approx 4$ cm^{-1}. The slave and the master QCL come from the same batch and have the same internal cavity length, which means that their microscopic parameters such as carrier lifetime, gain and photon lifetime are almost identical. These parameters are important to ensure optimal synchronization. These lasers emit a continuous wave thanks to a standard double trench configuration without Iron doped Indium Phosphide regrowth for thermal heat sinking optimization. The back-facet of these QCLs is composed of a high-reflectivity coating and this means that the lasers only output mid-infrared light at one side that is left as-cleaved. This emitting facet has a transmission of 30% that is suitable for feedback experiments.

Recovery process. In order to achieve proper enciphering, the message concealed within the chaotic carrier has a limited bandwidth and amplitude compared to the chaotic signal[66]. Consequently, the recovery process begins with the filtering of the master (containing the message) and of the slave signal. Table 2 assembles the characteristics of our passband filter. We do not use a lowpass filter in our work because we want to get rid of both the noise at high frequency and of the low-frequency contribution because the MCT detectors we used are not able to retrieve frequency components below 0.25 MHz. Indeed, the tabulated 3 dB bandwidth value is 1 MHz but we could observe signals down to a few hundreds of kHz. After filtering, the reconstruction of the message $M(t)$ is realized by computationally evaluating the difference intensity of the chaos transmitter $I_{ct} = |E_{master}(t) + M(t)|^2$ and the intensity of the chaos-synchronized slave $I_{slave} = |E_{slave}(t)|^2 \simeq |E_{master}(t)|^2$ resulting in $I_{ct} - I_{slave} = 2\Re\left(E_{master} \cdot M(t)\right) + |M(t)|^2$.

Data availability
All relevant data are available from the authors upon reasonable request.

Code availability
Matlab code is also available from the authors upon reasonable request.

References
1. He, X. et al. 1 Gbps free-space deep-ultraviolet communications based on III-nitride micro-LEDs emitting at 262 nm. *Photonics Res.* **7**, B41–B47 (2019).
2. Soibel, A. et al. Midinfrared interband cascade laser for free space optical communication. *IEEE Photonics Technol. Lett.* **22**, 121–123 (2009).
3. Su, Y. et al. 10 Gbps DPSK transmission over free-space link in the mid-infrared. *Opt. Express* **26**, 34515–34528 (2018).
4. Pang, X. et al. Free-space communications enabled by quantum cascade lasers. *Phys. Status Solidi (A)* **218**, 2000407 (2021).
5. Martini, R. et al. High-speed modulation and free-space optical audio/video transmission using quantum cascade lasers. *Electron. Lett.* **37**, 191–193 (2001).
6. McElroy, J. H. et al. CO$_2$ laser communication systems for near-earth space applications. *Proc. IEEE* **65**, 221–251 (1977).
7. Razeghi, M. et al. Recent progress of quantum cascade laser research from 3 to 12 μm at the Center for Quantum Devices. *Appl. Opt.* **56**, H30–H44 (2017).
8. Kopytko, M. et al. High-operating temperature MWIR nBn HgCdTe detector grown by MOCVD. *Opto-Electron. Rev.* **21**, 402–405 (2013).
9. Rodriguez, E. et al. Room-temperature, wide-band, quantum well-infrared photodetector for microwave optical links at 4.9 μm wavelength. *ACS Photonics* **5**, 3689–3694 (2018).
10. Corrigan, P., Martini, R., Whittaker, E. A. & Bethea, C. Quantum cascade lasers and the Kruse model in free space optical communication. *Opt. Express* **17**, 4355–4359 (2009).
11. Puiu, A. et al. Lidar/DIAL detection of acetone at 3.3 μm by a tunable OPO laser system. *Laser Phys.* **24**, 085606 (2014).
12. Faist, J. et al. Quantum cascade laser. *Science* **264**, 553–556 (1994).
13. Lee, B. G. et al. Widely tunable single-mode quantum cascade laser source for mid-infrared spectroscopy. *Appl. Phys. Lett.* **91**, 231101 (2007).
14. Schwaighofer, A., Brandstetter, M. & Lendl, B. Quantum cascade lasers (QCLs) in biomedical spectroscopy. *Chem. Soc. Rev.* **46**, 5903–5924 (2017).
15. Hashimura, K., Ishii, K. & Awazu, K. Selective removal of atherosclerotic plaque with a quantum cascade laser in the 5.7 μm wavelength range. *Jpn. J. Appl. Phys.* **54**, 112701 (2015).
16. Faist, J. et al. Quantum cascade laser frequency combs. *Nanophotonics* **5**, 272–291 (2016).
17. Spitz, O. et al. Extreme events in quantum casacade lasers. *Adv. Photonics* **2**, 066001 (2020).
18. Rosskopf, M., Mohr, T. & Elsäßer, W. Ghost polarization communication. *Phys. Rev. Appl.* **13**, 034062 (2020).
19. Nauerth, S. et al. Air-to-ground quantum communication. *Nat. Photonics* **7**, 382 (2013).
20. Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017).
21. Miao, E.-L. et al. Background noise of satellite-to-ground quantum key distribution. *N. J. Phys.* **7**, 215 (2005).
22. Hughes, R. J., Nordholt, J. E., Derkacs, D. & Peterson, C. G. Practical free-space quantum key distribution over 10 km in daylight and at night. *N. J. Phys.* **4**, 43 (2002).
23. Liao, S.-K. et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photonics* **11**, 509 (2017).
24. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inform.* **2**, 16025 (2016).
25. Pecora, L. M. & Carroll, T. L. Driving systems with chaotic signals. *Phys. Rev. A* **44**, 2374 (1991).
26. Uchida, A. Optical communication with chaotic lasers: applications of nonlinear dynamics and synchronization (John Wiley & Sons, 2012).
27. Colet, P. & Roy, R. Digital communication with synchronized chaotic lasers. *Opt. Lett.* **19**, 2056–2058 (1994).
28. Pecora, L. M. & Carroll, T. L. Synchronization in chaotic systems. *Phys. Rev. Lett.* **64**, 821 (1990).
29. Sciamanna, M. & Shore, K. A. Physics and applications of laser diode chaos. *Nat. Photonics* **9**, 151 (2015).

30. Vanwiggeren, G. D. & Roy, R. Communication with chaotic lasers. *Science* **279**, 1198–1200 (1998).
31. Goedgebuer, J.-P., Larger, L. & Porte, H. Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode. *Phys. Rev. Lett.* **80**, 2249 (1998).
32. Fischer, I., Hess, O., Elsäßer, W. & Göbel, E. High-dimensional chaotic dynamics of an external cavity semiconductor laser. *Phys. Rev. Lett.* **73**, 2188 (1994).
33. Fischer, I., Liu, Y. & Davis, P. Synchronization of chaotic semiconductor laser dynamics on subnanosecond time scales and its potential for chaos communication. *Phys. Rev. A* **62**, 011801 (2000).
34. Peil, M., Fischer, I. & Elsäßer, W. A short external cavity semiconductor laser cryptosystem. *Comptes Rendus Phys.* **5**, 633–642 (2004).
35. Argyris, A. et al. Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature* **438**, 343 (2005).
36. Hayes, S., Grebogi, C. & Ott, E. Communicating with chaos. *Phys. Rev. Lett.* **70**, 3031 (1993).
37. Wu, J. et al. Mesoscopic chaos mediated by Drude electron-hole plasma in silicon optomechanical oscillators. *Nat. Commun.* **8**, 1–7 (2017).
38. Annovazzi-Lodi, V., Aromataris, G., Benedetti, M. & Merlo, S. Secure chaotic transmission on a free-space optics data link. *IEEE J. Quantum Electron.* **44**, 1089–1095 (2008).
39. Jumpertz, L., Schires, K., Carras, M., Sciamanna, M. & Grillot, F. Chaotic light at mid-infrared wavelength. *Light. Sci. Appl.* **5**, e16088 (2016).
40. Spitz, O. et al. Investigation of chaotic and spiking dynamics in mid-infrared quantum cascade lasers operating continuous-waves and under current modulation. *IEEE J. Sel. Top. Quantum Electron.* **25**, 1–11 (2019).
41. Podolskiy, V. A., Narimanov, E., Fang, W. & Cao, H. Chaotic microlasers based on dynamical localization. *Proc. Natl Acad. Sci.* **101**, 10498–10500 (2004).
42. Fujino, H. & Ohtsubo, J. Experimental synchronization of chaotic oscillations in external-cavity semiconductor lasers. *Opt. Lett.* **25**, 625–627 (2000).
43. Locquet, A., Masoller, C. & Mirasso, C. R. Synchronization regimes of optical-feedback-induced chaos in unidirectionally coupled semiconductor lasers. *Phys. Rev. E* **65**, 056205 (2002).
44. Wedekind, I. & Parlitz, U. Experimental observation of synchronization and anti-synchronization of chaotic low-frequency-fluctuations in external cavity semiconductor lasers. *Int. J. Bifurc. Chaos* **11**, 1141–1147 (2001).
45. Tang, S. & Liu, J. M. Message encoding–decoding at 2.5 Gbits/s through synchronization of chaotic pulsing semiconductor lasers. *Opt. Lett.* **26**, 1843–1845 (2001).
46. Lavrov, R., Jacquot, M. & Larger, L. Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications. *IEEE J. Quantum Electron.* **46**, 1430–1435 (2010).
47. Winzer, P. J. & Leuthold, J. Return-to-zero modulator using a single NRZ drive signal and an optical delay interferometer. *IEEE Photonics Technol. Lett.* **13**, 1298–1300 (2001).
48. Sedgwick, P. Pearson's correlation coefficient. *BMJ* **345**, e4483 (2012).
49. Kouomou, Y. C., Colet, P., Gastaud, N. & Larger, L. Effect of parameter mismatch on the synchronization of chaotic semiconductor lasers with electro-optical feedback. *Phys. Rev. E* **69**, 056226 (2004).
50. Bogris, A., Argyris, A. & Syvridis, D. Encryption efficiency analysis of chaotic communication systems based on photonic integrated chaotic circuits. *IEEE J. Quantum Electron.* **46**, 1421–1429 (2010).
51. Larger, L., Goedgebuer, J.-P. & Udaltsov, V. Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos. *Comptes Rendus Phys.* **5**, 669–681 (2004).
52. Chang, F., Onohara, K. & Mizuochi, T. Forward error correction for 100 G transport networks. *IEEE Commun. Mag.* **48**, S48–S55 (2010).
53. Ozolins, O. et al. 100 Gbaud PAM4 link without EDFA and post-equalization for optical interconnects. In *Proc. 45th European Conference on Optical Communication*, 1–4 (2019).
54. Liu, J.-M., Chen, H.-F. & Tang, S. Synchronized chaotic optical communications at high bit rates. *IEEE J. Quantum Electron.* **38**, 1184 (2002).
55. Li, T. et al. Ge-on-Si modulators operating at mid-infrared wavelengths up to 8 μm. *Photonics Res.* **7**, 828–836 (2019).
56. Cheng, F. et al. Ultralow power consumption of a quantum cascade laser operating in continuous-wave mode at room temperature. *Opt. Express* **28**, 36497–36504 (2020).
57. Waks, E. et al. Secure communication: quantum cryptography with a photon turnstile. *Nature* **420**, 762 (2002).
58. Gavrielides, A. & Newell, T. C. Global coupling of QCLs: inclusion of dynamics. *Opt. Express* **28**, 7746–7758 (2020).
59. Troles, J. & Brilland, L. Chalcogenide microstructured optical fibres for mid-IR applications. *Comptes Rendus Phys.* **18**, 19–23 (2017).
60. Jumpertz, L., Carras, M., Schires, K. & Grillot, F. Regimes of external optical feedback in 5.6 μm distributed feedback mid-infrared quantum cascade lasers. *Appl. Phys. Lett.* **105**, 131112 (2014).
61. Sanchez-Diaz, A., Mirasso, C. R., Colet, P. & Garcia-Fernandez, P. Encoded Gbit/s digital communications with synchronized chaotic semiconductor lasers. *IEEE J. Quantum Electron.* **35**, 292–297 (1999).
62. Murakami, A. & Ohtsubo, J. Synchronization of feedback-induced chaos in semiconductor lasers by optical injection. *Phys. Rev. A* **65**, 033826 (2002).
63. Sivaprakasam, S. & Shore, K. A. Message encoding and decoding using chaotic external-cavity diode lasers. *IEEE J. Quantum Electron.* **36**, 35–39 (2000).
64. Evans, A. et al. High-temperature, high-power, continuous-wave operation of buried heterostructure quantum-cascade lasers. *Appl. Phys. Lett.* **84**, 314–316 (2004).
65. Carras, M. et al. Room-temperature continuous-wave metal grating distributed feedback quantum cascade lasers. *Appl. Phys. Lett.* **96**, 161105 (2010).
66. Cuomo, K. M. & Oppenheim, A. V. Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett.* **71**, 65 (1993).

Author contributions
O.S. and A.H. conceived the experiments, G.M. and M.C. manufactured and characterized the lasers, O.S. conducted the experiments, O.S., A.H., and J.W. analyzed the results, O.S., A.H., J.W, C.W., W.E., and F.G. prepared the manuscript, F.G. and W.E. supervised the research work. All authors reviewed the manuscript.

Competing interests
The authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-021-23527-9.

Correspondence and requests for materials should be addressed to O.S.

Peer review information *Nature Communications* thanks Rajarshi Roy and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Supplementary information: Private communication with quantum cascade laser photonic chaos

Olivier Spitz[1,2,*], **Andreas Herdt**[3], **Jiagui Wu**[4,5], **Grégory Maisons**[2], **Mathieu Carras**[2], **Chee-Wei Wong**[4], **Wolfgang Elsäßer**[3], **and Frédéric Grillot**[1,6]

[1]LTCI, Télécom Paris, Institut Polytechnique de Paris, 19 Place Marguerite Perey, Palaiseau, 91120, France
[2]mirSense, Centre d'intégration NanoInnov, 8 avenue de la Vauve, Palaiseau, 91120, France
[3]Technische Universität Darmstadt, Schlossgartenstraße 7, D-64289 Darmstadt, Germany
[4]Fang Lu Mesoscopic Optics and Quantum Electronics Laboratory, University of California Los Angeles, Los Angeles, CA 90095, USA
[5]College of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China
[6]Center for High Technology Materials, University of New-Mexico, 1313 Goddard SE, Albuquerque, NM 87106, USA
[*]olivier.spitz@telecom-paris.fr

Supplementary discussion

Based on Shannon's theory of secrecy,[1] confusion and diffusion are two properties used to make ciphers robust against statistical analysis. Cracking a high order QCL chaotic waveform is extremely difficult due to both practical, technological, physical and mathematical limitations associated with the degree of complexity of a chaotic behavior.[2] Moreover, we would like to emphasize that our system is not intended to be primarily fiber-based, so the expected mobility of the transmitter and the receiver poses another challenge to Eve. The practical limitations to hacking the system are:

1. The QCL used by Eve must be the same as ours at the microscopic level, with the same physical parameter settings (which can be changed rapidly as part of the encryption protocol). Thus, using another QCL or other types of lasers combined with other detectors is very unlikely to succeed in recreating the initial QCL system in order to hack a transmission or in order to inject an intelligible signal into the data stream for jamming purposes.[3]

2. A transmission between 8-11.5 micron wavelengths along with chaotic waveforms would further provide stealth/masking for the signal. This is due to the random thermal blackbody background radiation,[4] hence reducing the probability of adversaries intercepting the transmission signal.

3. Quantum computers, neural networks or other computing architectures, which can potentially crack standard mathematical encryption via solving elliptical, parabolic or hyperbolic equations, are not necessarily capable of quickly cracking non-quantum dynamical chaos. This means that, in our configuration, the time to decipher the message with mathematical tools is several orders of magnitude larger than the total duration of the transmission itself: Eve may only translate the message long after its validity expired.

So, there are extreme technological and physical barriers[5] in order to attempt to predict and crack an optical chaotic system. In addition to the technological barriers, there are also mathematical barriers to cracking the QCL chaotic waveform, which are:

4. QCL chaotic waveform sources exhibit strong nonlinear dynamical topology structures and fractional dimensions of oscillation (i.e. hyperchaos), which is exactly what is needed for private optical communication links.[6] This property may strongly be reinforced by using an array of coupled QCLs.

5. Nonlinear chaotic systems with only one positive Lyapunov exponent are not robust enough to cracking (i.e. the chaotic signal can be destroyed by further arbitrarily small perturbations of the system). In other words, non-robust chaotic system dynamics enable just one variable to enslave a set of differential equations and thus, these systems will have only one positive Lyapunov exponent.[7]

Accordingly, due to these specific and intrinsic attributes of QCL chaotic systems, one insists that the message embedded in a chaotic waveform offers a decent level of privacy from hacking. This accounts for Eve actively hacking chaotic waveforms, either considering current or great advances in future technological capabilities relying on machine learning and reservoir computing, which are currently used for non-ideal chaos prediction.[8] Our current achievements make the described private-link configuration relevant in the case of operational short-message transmission, for instance between two tanks in the
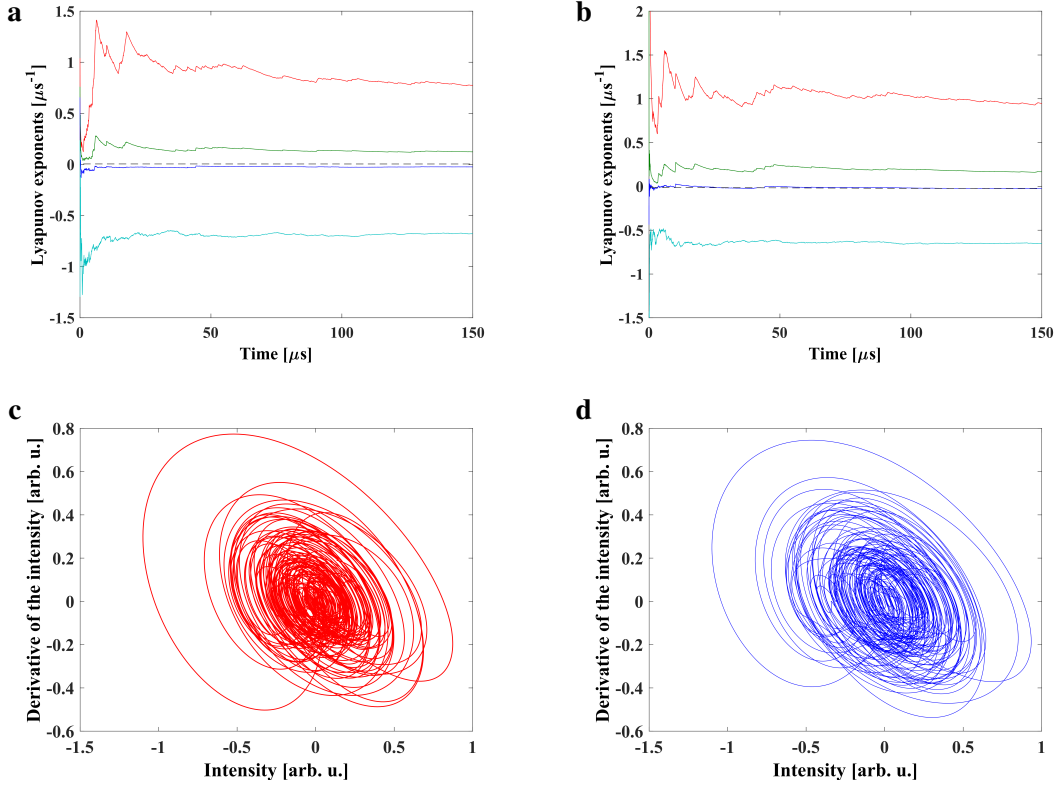
Supplementary figure 1. **Comparison of the chaos properties. a-b** System dynamics analysis through Lyapunov exponents (LEs). The four largest LEs are displayed and the chaotic behavior is confirmed by the two LEs converging towards values above zero. **c-d** Reconstructed orbital phase portraits for the filtered chaotic master laser and the filtered chaotic slave laser. The two phase portraits look similar, thus confirming the chaos synchronization between the two QCLs. The left panel is associated to the master's signal while the right panel is associated to the slave's signal.

battlefield. With our method, it is very difficult for an eavesdropper to even know that a transmission between two vehicles occurs because the wavelength of the transmission relates to the wavelength of the background environment and because the laser beam is directional. Another application is short-range communication between two rovers on Mars. These rovers have a very low speed, around 1 km/h, but they need to exchange information and free-space optics transmission raised attention. The two advantages of our private transmission scheme are a directional line-of-sight communication immune to the few nearby potential eavesdroppers (for instance other rovers or satellites) and a wavelength of operation very resistant to degraded conditions such as sandstorms.

Supplementary methods

At first, a chaotic waveform may be not distinguishable from a stochastic noisy time trace and consequently, it is mandatory to have tools such as the Lyapunov exponents (LEs) in order to characterize the observed dynamics. The basic idea of the Lyapunov exponent λ is to measure the rate at which two originally nearby trajectories diverge in time, because two close trajectories are supposed to exponentially diverge in the case of chaos.[9] As the direction of the maximum divergence or convergence locally changes on the attractor, the motion must be monitored at each point along the trajectory. On the one hand, at least one of the LEs must be positive to comply with the sensitive dependence on the initial conditions, which is an endemic property of chaotic systems. On the other hand, constant and periodic signals are linked to zero or negative LEs because this means that nearby points converge. Several methods for the calculation of the LEs from experimental time series have been developed .[10–14] In general, the number of LEs that can be retrieved corresponds to the number of system variables and only the largest exponents are derived in order to determine if the system is chaotic. We extract the largest LEs from our 1 million data points filtered time series, recorded with a sampling rate of 2.5 GSamples/s, by using the technique exposed in Ref. 15. Besides, the noise-reduced data are also relevant to reconstruct the phase space trajectories[16] because this confirms the similarities between the chaos from the master QCL and that from the slave QCL, though the latter is starting from an arbitrary condition.[17] The experimental phase diagrams can be found in Fig. 1 **c** and **d**. The analysis of the master signal shows

ASCII	binary	mistaken ASCII	mistaken binary
T	01010100		
U	01010101	u	01110101
-	00101101	%	00100101
D	01000100	□	00000100
a	01100001		00100000
r	01110010	b	01100010
m	01101101	i	01101001
s	01110011	b	01100010
t	01110100	T	01010100
a	01100001		
d	01100100		
t	01110100	T	01010100

Supplementary table 1. Binary code used to transmit the message "TU-Darmstadt" and associated errors that can be found in the recovery process.

that the four largest LEs converge towards $\lambda_1 = 0.76 \mu s^{-1}$, $\lambda_2 = 0.12 \mu s^{-1}$, $\lambda_3 = -0.02 \mu s^{-1}$ and $\lambda_4 = -0.67 \mu s^{-1}$, and the analysis of the slave signal shows that the four largest LEs converge towards $\lambda_1 = 0.94 \mu s^{-1}$, $\lambda_2 = 0.16 \mu s^{-1}$, $\lambda_3 = -0.02 \mu s^{-1}$ and $\lambda_4 = -0.65 \mu s^{-1}$, as visualized in Fig. 1 **a** and **b**, respectively. Consequently, the signal generated by the master QCL is considered as hyperchaos[18] because two LEs are positive and this confirms the potential of our setup for private transmission, contrary to systems producing chaotic outputs with only one positive LE.[19]

A key parameter is the technique used to encipher the message within the chaotic carrier. Two methods relying on the concealment of a message within a chaotic carrier have been explored in the literature and they have a tremendous influence on the lowest achievable BER.[20] The first method is called chaos masking (CMa).[21] It consists in embedding a small message $m(t)$ into a chaotic carrier $x(t)$ at the drive level and then, sending the signal $x(t) + m(t)$ to the response. Only the chaotic signal $x(t)$ is reproduced in the response system if the amplitude of the message is small enough. Then, the message $m(t)$ is deciphered by subtracting the response output $x(t)$ from the transmission signal $x(t) + m(t)$. The success of the message private concealing into a chaotic carrier and of the decoding of the message relies on a message amplitude sufficiently small compared with the averaged chaotic carrier signal. Usually, the fraction is less than 1% of the average chaotic power.
The second method is called chaos modulation (CMo).[22] In this method, a message is inserted within a chaotic carrier in the nonlinear oscillator and the two signals conform a new chaotic state different from the original one. In CMo, a delayed feedback system is usually used as a chaotic generator. This new signal together with the message is sent to the response. Since the drive and the response are the same nonlinear systems, the chaotic oscillation is exactly reproduced in the response system thanks to chaos synchronization. By subtracting the synchronized chaotic signal from the transmitted signal, it is possible to decode the message. Sometimes, the message is decoded by dividing the transmitted signal by the synchronized chaotic signal in the response. Contrary to the previous method, CMo has no restriction on the magnitude of the message, since both the chaotic carrier and the message conform new chaotic states in the nonlinear systems. However, the degree of security for data transmission becomes worse when the signal level of a message is large. Therefore, the amplitude of a message in CMo should also be small.
Several possibilities exist in order to convert alphanumeric characters into a code that is compatible with optical transmission. At least 7 bits are required to encode any ASCII character in binary. In practice, an 8th bit is added and used as a parity bit to detect transmission errors and this standard is called UTF-8. Table 1 contains the UTF-8 code we used to transfer our message. Because transmission is not flawless, the transmission errors that we possibly encountered are also gathered in that table.

Supplementary References

1. Shannon, C. E. Communication theory of secrecy systems. The Bell system technical journal 28, 656–715 (1949).

2. Anishchenko, V. Vadivasova, T. Okrokvertskhov, G. & Strelkova, G. Correlation analysis of dynamical chaos. Physica A: Statistical Mechanics and its Applications 325, 199–212 (2003).

3. Rizomiliotis, P. Bogris, A. & Syvridis, D. Message origin authentication and integrity protection in chaos-based optical communication. IEEE Journal of Quantum Electronics 46, 377–383 (2010).

4. Majumdar, A.K. & Ricklin J.C. Free-space laser communications: principles and advances, vol. 2 (Springer Science & Business Media, 2010).

5. Razeghi M. Technology of quantum devices (Springer, 2010).

6. Goedgebuer, J.-P. Levy, P. Larger, L. Chen, C.-C. & Rhodes, W.T. Optical communication with synchronized hyperchaos generated electrooptically. IEEE Journal of Quantum Electronics 38, 1178 (2002).

7. Wernecke, H. Sándor, B. & Gros, C. Chaos in time delay systems, an educational review. Physics Reports 824, 1–40 (2019).

8. Pathak, J. Lu, Z. Hunt, B.R. Girvan, M. & Ott, E. Using machine learning to replicate chaotic attractors and calculate Lyapunov exponents from data. Chaos: An Interdisciplinary Journal of Nonlinear Science 27, 121102 (2017).

9. Ohtsubo, J. Semiconductor lasers: stability, instability and chaos, vol. 111 (Springer, 2012).

10. Sano, M. & Sawada, Y. Measurement of the Lyapunov spectrum from a chaotic time series. Physical Review Letters 55, 1082 (1985).

11. Eckmann, J.-P. Kamphorst, S.O. and Ruelle, D. Ciliberto, S. Liapunov exponents from time series. Physical Review A 34, 4971 (1986).

12. Rosenstein, M.T. Collins, J.J. & De Luca, C.J. A practical method for calculating largest Lyapunov exponents from small data sets. Physica D: Nonlinear Phenomena 65, 117 (1993).

13. Wolf, A. Swift, J.B. Swinney, H.L. Vastano, J.A. Determining Lyapunov exponents from a time series. Physica D: Nonlinear Phenomena 16, 285 (1985).

14. Bryant, P. Brown, R. & Abarbanel, H.D.I. Lyapunov exponents from observed time series. Physical Review Letters 65, 1523 (1990).

15. Brown, R. Bryant, P. & Abarbanel, H.D.I. Computing the Lyapunov spectrum of a dynamical system from an observed time series. Physical Review A 43, 2787 (1991).

16. Schreiber, T. Determination of the noise level of chaotic time series. Physical Review E 48, R13 (1993).

17. Pecora, L.M. & Carroll, T.L. Synchronization in chaotic systems. Physical Review Letters 64, 821 (1990).

18. Qi, G. van Wyk, M.A. van Wyk, B.J. & Chen, G. On a new hyperchaotic system. Physics Letters A 372, 124 (2008).

19. Perez, G. & Cerdeira, H.A. Extracting messages masked by chaos. Physical Review Letters 74, 1970 (1995).

20. Liu, J.-M. Chen, H.-F. & Tang, S. Synchronized chaotic optical communications at high bit rates. IEEE Journal of Quantum Electronics 38, 1184 (2002).

21. Morgül, Ö. & Feki, M. A chaotic masking scheme by using synchronized chaotic systems. Physics Letters A 251, 169 (1999).

22. Halle, K.S. Wu, C.W. Itoh, M. & Chua, L.O. Spread spectrum communication through modulation of chaos. International Journal of Bifurcation and Chaos 3, 469 (1993).