APL Photonics

Cryptography in coherent optical information networks using dissipative metamaterial gates

Cite as: APL Photonics **4**, 046102 (2019); https://doi.org/10.1063/1.5092216
Submitted: 08 February 2019 . Accepted: 06 April 2019 . Published Online: 24 April 2019

Angelos Xomalis, Iosif Demirtzioglou, Yongmin Jung, Eric Plum, Cosimo Lacava, Periklis Petropoulos, David J. Richardson, and Nikolay I. Zheludev

COLLECTIONS

EP This paper was selected as an Editor's Pick

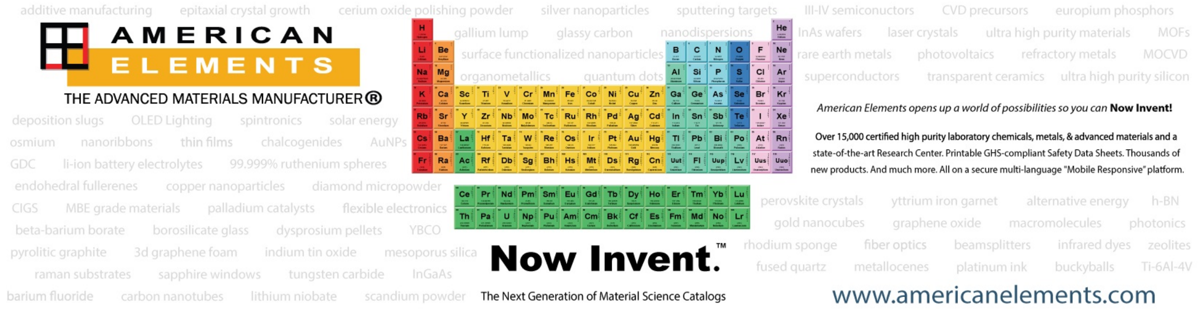
View Online Export Citation CrossMark

ARTICLES YOU MAY BE INTERESTED IN

Background-free time-resolved coherent Raman spectroscopy (CSRS and CARS): Heterodyne detection of low-energy vibrations and identification of excited-state contributions
APL Photonics **4**, 056102 (2019); https://doi.org/10.1063/1.5090585

Strong frequency conversion in heterogeneously integrated GaAs resonators
APL Photonics **4**, 036103 (2019); https://doi.org/10.1063/1.5065533

NEXAFS at nitrogen K-edge and titanium L-edge using a laser-plasma soft x-ray source based on a double-stream gas puff target
APL Photonics **4**, 030807 (2019); https://doi.org/10.1063/1.5085810



Cryptography in coherent optical information networks using dissipative metamaterial gates

Cite as: APL Photon. 4, 046102 (2019); doi: 10.1063/1.5092216
Submitted: 8 February 2019 • Accepted: 6 April 2019 •
Published Online: 24 April 2019

Angelos Xomalis,[1,2,a)] Iosif Demirtzioglou,[1] Yongmin Jung,[1] Eric Plum,[1,2] Cosimo Lacava,[1] Periklis Petropoulos,[1] David J. Richardson,[1] and Nikolay I. Zheludev[1,2,3,b)]

AFFILIATIONS

[1] Optoelectronics Research Centre, University of Southampton, Highfield, Southampton SO17 1BJ, United Kingdom
[2] Centre for Photonic Metamaterials, University of Southampton, Highfield, Southampton SO17 1BJ, United Kingdom
[3] Centre for Disruptive Photonic Technologies, SPMS, TPI, Nanyang Technological University, Singapore 637371, Singapore

[a)] **Email:** ax1c15@soton.ac.uk
[b)] **Email:** niz@orc.soton.ac.uk

ABSTRACT

All-optical encryption of information in fibre telecommunication networks offers lower complexity and far higher data rates than electronic encryption can deliver. However, existing optical layer encryption methods, which are compatible with keys of unlimited length, are based on nonlinear processes that require intense optical fields. Here, we introduce an optical layer secure communication protocol that does not rely on nonlinear optical processes but instead uses energy redistribution of coherent optical waves interacting on a plasmonic metamaterial absorber. We implement the protocol in a telecommunication optical fibre information network, where signal and key distribution lines use a common coherent information carrier. We investigate and demonstrate different encryption modes, including a scheme providing perfect secrecy. All-optical cryptography, as demonstrated here, exploits signal processing mechanisms that can satisfy optical telecom data rate requirements in any current or next-generation frequency band with bandwidth exceeding 100 THz and a switching energy of a few photons per bit. This is the first demonstration of an optical telecommunications application of metamaterial technology.

I. INTRODUCTION

Secure exchange of confidential information is essential in banking, health care, social media, the Internet of Things, government, the security forces, and many other aspects of modern life. Fully secure cryptography has been known since 1882, when Miller introduced the one-time pad technique,[1] which uses a perfectly random key that is at least as long as the message. During World War I, Vernam re-invented and patented[2,3] the technique, which was proven to be unbreakable by Shannon in 1949.[4,5] One-time pad ciphers have been used for top secret diplomatic and military communications ever since. More widely-used encryption techniques use keys of limited length, making them vulnerable to brute force attacks. Symmetric techniques, such as Data Encryption Standard (DES)[6] and Advanced Encryption Standard (AES),[7] use the same key for encryption and decryption and therefore require secure key distribution, e.g., quantum key distribution.[8–10] Asymmetric techniques, such as Rivest–Shamir–Adleman (RSA),[11] avoid the key distribution problem by using a public key for encryption and a private key for decryption but suffer from a higher computational cost. Such an encryption is normally implemented electronically, leaving the optical layer used for data transmission vulnerable to attacks. Optical layer security can be improved by all-optical encryption. However, all-optical encryption techniques that can use one-time pad ciphers in conventional networks rely on nonlinear optics,[12,13] implying high intensity and energy requirements. Moreover, the use of finite keys in all-optical encryption and related approaches to optical layer security, e.g., optical steganography[14] and code-division multiple access systems,[15–17] cannot be fully secure. Thus, efficient exchange of confidential information with perfect secrecy remains a challenge. Coherent communication, which uses the phase of optical signals, has gained attention in recent years for its potential for improving communication line capacity.[18–20] Phase stabilization techniques[21,22] and emerging networks with mutually coherent information channels[22–24] provide an opportunity to develop security solutions based on the relative phase of channels using the same wave information carrier. Within this work, we use the term "coherent information network" to refer to such networks with mutually coherent information channels.

Here we propose and experimentally demonstrate a secure encryption protocol for coherent information networks. The proposed encryption protocol is applicable to any wave information carrier in a network containing mutually coherent communication lines. It is a symmetric, one-time pad technique without significant computational cost and immediate signal recovery. We report proof-of-principle demonstrations of the encryption and decryption protocol in a coherent telecommunication optical fibre network. The underlying encryption and decryption operations occur in THz bandwidth coherent optical gates that can operate with single photons. Therefore, such optical implementations have the potential to provide perfect secrecy with THz bandwidth and low power consumption.

II. COHERENT CRYPTOGRAPHY CONCEPT

The general concept of a coherent encrypted information network based on any wave information carrier is illustrated in Fig. 1, considering transmission of secret data by a sender Alice to a receiver Bob in the presence of an eavesdropper Eve along the transmission line. A common coherent carrier is modulated to generate data and key signals. The data are encrypted by forming a coherent superposition of the data and the key in a first coherent gate. The encrypted data and the key are transmitted using separate, mutually coherent channels. Superposition of the encrypted signal with the key in a second coherent gate results in recovery of the original data.

Our optical implementation of coherent cryptography is based on analogue optical gates exploiting linear interactions of mutually coherent waves on a lossy beam splitter.[25] In recent years it has been demonstrated that a thin, lossy beam splitter illuminated from both sides can act as a four-port device for incident and reflected waves and can operate in different functional modes.[26] XOR, AND and NOT all-optical gates have been demonstrated in coherent telecommunication fiber networks[27] reaching a switching bandwidth of 1 THz.[28] Here we use such coherent optical gates for encryption and decryption of a binary optical data signal with amplitude modulation. We implement the technique in a fully-fiberized network at a bit-rate of 3 Gbit/s at the telecommunications wavelength of 1550 nm. We experimentally demonstrate partially secure modes of encryption that would require complex techniques for eavesdropping and propose a more sophisticated implementation that offers perfect secrecy.

The coherent optical gates used for encryption and decryption exploit the property that linear interactions between waves and matter may be controlled by mutually coherent waves. Counterpropagating, co-polarized, and mutually coherent light waves form an optical standing wave with alternating positions of negligible electric field (nodes) and enhanced electric field (anti-nodes). A material that is thin compared to the wavelength of the coherent waves may be placed at such a node or an anti-node, where its interaction with the optical electric field will be negligible or enhanced respectively. This allows for the absorption of light in a thin absorber to be controlled, in principle from 0% (coherent perfect transparency) to 100% (coherent perfect absorption).[29] This control over absorption of light with light without a nonlinear medium occurs on a femtosecond timescale corresponding to more than 100 THz bandwidth,[30] for single quanta of light[31] and can be used to perform all-optical signal processing functions in telecommunication frequency bands.[27] Thus, a thin absorber can act as an ultrafast, low power analogue optical gate. The gate has two inputs—the counterpropagating, mutually coherent incident waves—and two outputs formed by the superposition of transmitted and reflected waves. Here we use such gates for: (i) encryption by superposition of mutually coherent data and key signals and (ii) decryption by coherent perfect absorption of the key resulting in recovery of the original data, regardless of what the coherent key was.

Consider two coherent optical gates ($i = 1, 2$), each with counterpropagating input signals, α_i and β_i, and output signals, γ_i and δ_i. The counterpropagating, co-polarized, and mutually coherent optical input signals α_i and β_i have electric fields $E_{\alpha i}$ and $E_{\beta i}$ and interact with a linear material of negligible thickness within the gate. Linear transmission and reflection of light can be described by the generally complex Fresnel field transmission and reflection coefficients t and r, where $t = r + 1$ for planar, non-diffractive structures. Thus, the time-dependent output signals γ_i and δ_i with electric fields $E_{\gamma i}$ and $E_{\delta i}$ resulting from simultaneous reflection and transmission of the incident fields are given by

$$E_{\gamma i} = tE_{\alpha i} + rE_{\beta i} \text{ and } E_{\delta i} = rE_{\alpha i} + tE_{\beta i}. \tag{1}$$

A coherent perfect absorber of negligible thickness is described by $t = 0.5$ and $r = -0.5$, where the minus sign indicates that reflection occurs with a π phase shift. It transmits and reflects $|t|^2 = |r|^2 = 25\%$ of a single incident light beam's intensity and absorbs the

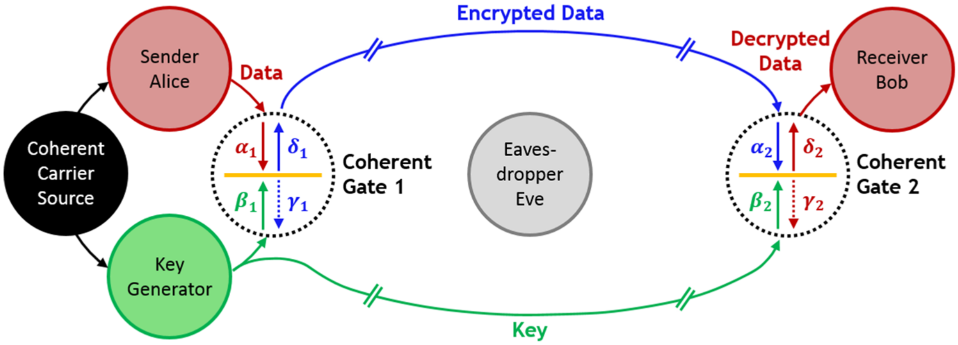


FIG. 1. Coherent encrypted information network. Alice encrypts her data by forming a coherent superposition of data and key on Coherent Gate 1. Bob decrypts the data by combining the encrypted data and the key on Coherent Gate 2. To eavesdrop the communication line, Eve would have the difficult task of detecting not only the intensity of the encrypted data and key signals, but also their mutual phase and shall also know the type of gate that has been used for encryption and decryption.

remaining 50%. Consequently, the output fields from a coherent perfect absorber will always have the same intensity and a π phase difference, $E_{\delta i} = -E_{\gamma i}$. In particular, for incident fields of the same intensity, constructive interference on the absorber ($E_{\alpha i} = E_{\beta i}$) results in coherent perfect absorption ($E_{\delta i} = E_{\gamma i} = 0$), while destructive interference ($E_{\alpha i} = -E_{\beta i}$) results in coherent perfect transparency ($E_{\gamma i} = E_{\alpha i}$ and $E_{\delta i} = E_{\beta i}$). Coherent perfect absorption results from destructive interference of the transmitted and reflected fields, which traps incident light within the thin absorber until it is dissipated. Metamaterial,[29] heavily doped silicon film,[32] 30-layer graphene,[31] and other[25] coherent perfect absorbers have been reported suitable for the microwave, terahertz, infrared, and visible spectral ranges. There are three characteristic cases of encryption for mutually coherent, binary, and intensity-modulated data and key signals, α_1, and β_1, interacting on a coherent absorber: (i) If data and key are in phase, coherent absorption of simultaneously-arriving pulses implies that a high output level (logical "1") only occurs if a single pulse is incident, corresponding to an encrypted output α_1 XOR β_1. (ii) If they have a π phase difference, a high output signal due to coherent transparency for simultaneously-arriving pulses corresponds to an encrypted output α_1 AND β_1. (iii) Other phase differences between data and key lead to partial absorption of simultaneously-arriving pulses. In particular, a $\pi/3$ phase difference yields the same output level for one or two incident pulses (e.g., $|E_{\gamma1}| = |E_{\delta1}| = 0.5|E_{\alpha1}|$ for $|E_{\alpha1}| \neq 0$, $E_{\beta1} \in \left\{0, E_{\alpha1}e^{\pm i\pi/3}\right\}$), corresponding to an encrypted output α_1 OR β_1. In all cases, the original data may be recovered (with some attenuation) by combining the encrypted signal

$$E_{\alpha2} = E_{\delta1} = E_{\beta1}/2 - E_{\alpha1}/2 \tag{2}$$

with the key $E_{\beta2} = E_{\beta1}/2$ on a second coherent absorber, where the key is removed by coherent absorption, resulting in an output

$$E_{\delta2} = E_{\alpha1}/4. \tag{3}$$

III. EXPERIMENTAL DEMONSTRATION OF COHERENT CRYPTOGRAPHY

In this paper, we focus on the characteristic cases of XOR, AND, and OR encryption and decryption using two coherent optical gates that approximate coherent perfect absorbers. Each gate contains a plasmonic metamaterial absorber fabricated on the core of an optical fibre [Fig. 2(b)] within a stainless steel enclosure with standard pigtailed FC/APC connectors ensuring compatibility with standard fibre components. The metamaterial was fabricated by thermal evaporation of a 70-nm-thick gold layer on the end face of a flat-cleaved, single-mode, PANDA-style, polarization-maintaining optical fibre, followed by focused ion beam milling of the metamaterial array. The latter is a 25 × 25 $\mu\mathrm{m}^2$ array of asymmetrically split ring apertures milled through the gold layer covering the fibre core with the metamaterial's symmetry axis aligned to the slow axis of the

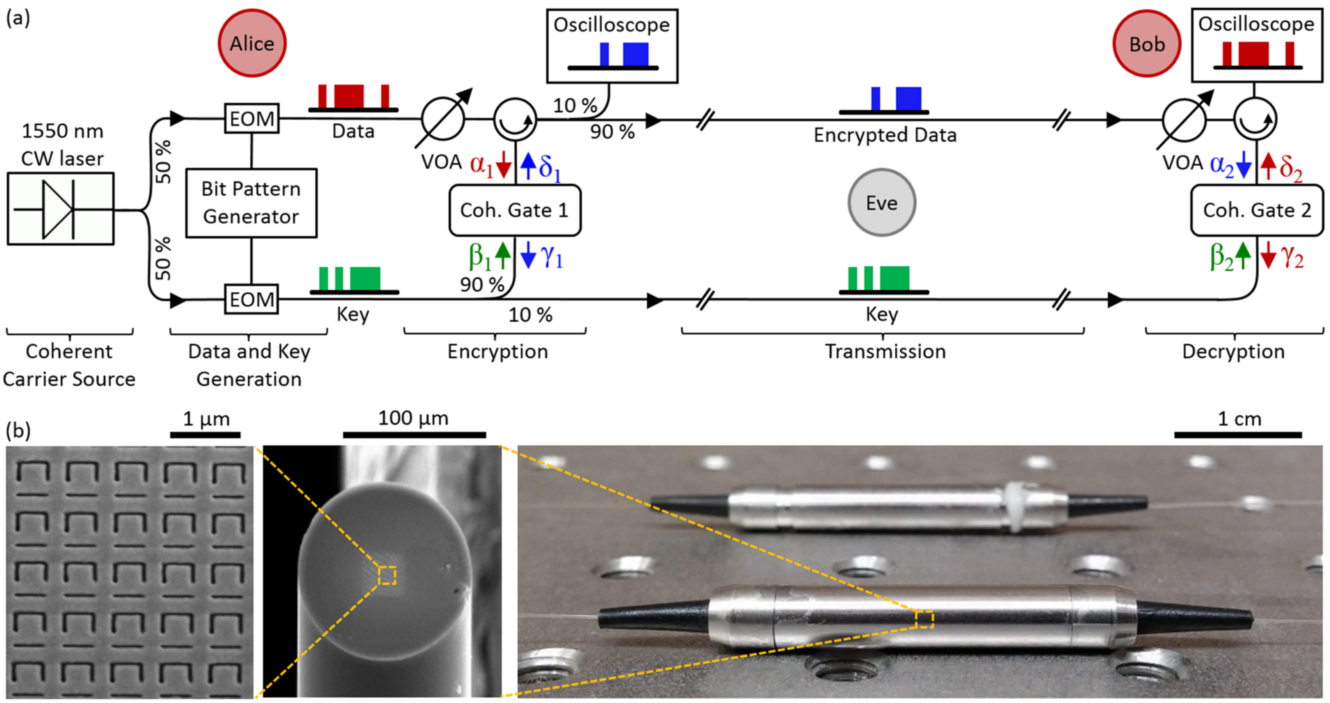


FIG. 2. Optical implementation of a coherent encrypted information network. (a) A CW diode laser operating in the telecommunications C-band was used as the coherent carrier source. Other elements in the schematic are abbreviated as follows: EOM—intensity electro-optic modulator and VOA—variable optical attenuator. (b) The coherent optical gates are based on interaction of four waves on a plasmonic metamaterial absorber. The metamaterial absorber is manufactured in a 70 nm thick gold film on the core of a single-mode, polarization-maintaining optical fibre (SEM images) and packaged in a standard fiber device housing (photo).

fibre. The metamaterial has a 700 × 700 nm^2 unit cell containing a 500 × 500 nm^2 split ring aperture with a linewidth of 50 nm. The metamaterial-covered fibre was coupled with a second cleaved optical fibre using a pair of anti-reflection-coated microcollimator lenses. The components were fixed in place with glass and metal ferrules, bonded with UV-cured adhesive and placed in a protective stainless steel package. At the measurement wavelength of 1550 nm, a single input signal entering the first coherent optical gate in channel α_1 (β_1) experiences about 15% (15%) transmission, 22% (20%) reflection and 63% (65%) losses including coupling losses. Corresponding values for the second coherent optical gate are 14% (14%) transmission, 26% (20%) reflection and 60% (66%) absorption. We note that Eq. (1) implies that, for one output of each coherent gate (e.g., δ_i), transmission and reflection coefficients with imperfect amplitude and/or phase can be fully compensated for, by adjusting the relative amplitude and phase of the coherent optical gate inputs, α_i, and β_i. This does not harm the security of the scheme, but it distorts the other coherent gate output.

We characterized the encryption and decryption functionalities of the coherent optical gates in a fibre network consisting of two polarization-maintaining fibre interferometers [Fig. 2(a)]. The output of a 1550 nm wavelength Continuous Wave (CW) laser (ID Photonics CoBrite-DX4) was split along two interferometer arms with electro-optical intensity modulators (EOSPACE AX-0K5-10-PFA-PFA-UL and FUJITSU FTM7937-AA) that were controlled by a bit pattern generator (Tektronix AWG7122C) to produce data and key bit patterns, α_1, and β_1. These were combined on the first gate to generate the encrypted data signal. Using a circulator and a splitter, the encrypted data δ_1 and the key were transmitted separately from the encryption setup (Alice) to the decryption setup (Bob), where they were combined on the second gate for decryption. A delay line was used to ensure temporal overlap of the encrypted data with the relevant part of the key on the second gate. The delay line was combined with a polarization controller and polarization beam splitter that were used to align the polarization state of the key to that of the encrypted data. A splitter, a circulator and two Erbium-doped fibre amplifiers (KEOPSYS) were used to monitor the encrypted and decrypted signals, δ_1, and δ_2, simultaneously with the aid of an oscilloscope (Agilent Infiniium DCA-J 86100C). Variable optical attenuators were used to prevent optical damage to the metamaterials within the coherent optical gates and to balance the peak power of the optical signals. In all experiments, the incident electric field was oriented parallel to the symmetry axis of the metamaterial. Our fibre interferometers are stable on sub-second timescales, which is sufficient for proof-of-principle demonstrations and allowed us to exploit the phase drift on longer timescales for switching between different types of encryption. We note that practical applications would require active stabilisation of the optical path lengths to prevent phase drift in the interferometers, as well as a fully polarization maintaining fibre network. As the coherent optical gates require mutually coherent input signals, any optical length difference between the interferometer arms must be less than the coherence length of the laser source.

Encryption and decryption were studied with binary, intensity-modulated bit patterns, where high and low intensity correspond to logical "1" and "0", respectively. While the one-time pad approach is applicable to bit patterns of any length, we demonstrate the principle with patterns of 8 bits for experimental simplicity and clarity. The data pattern in channel α_1 is 10110001 and the key pattern in channel β_1 is 10010110 at a bit rate of 3 Gbit/s throughout all experiments [Fig. 3(a)]. Depending on the optical phase difference between data and key, the output δ_1 of the first coherent optical gate corresponds to (data) XOR (key), (data) AND (key), or (data) OR (key). In the case of XOR encryption [Fig. 3(b)], where data and key input states of 1 and 1 are eliminated by coherent absorption, Eve cannot derive

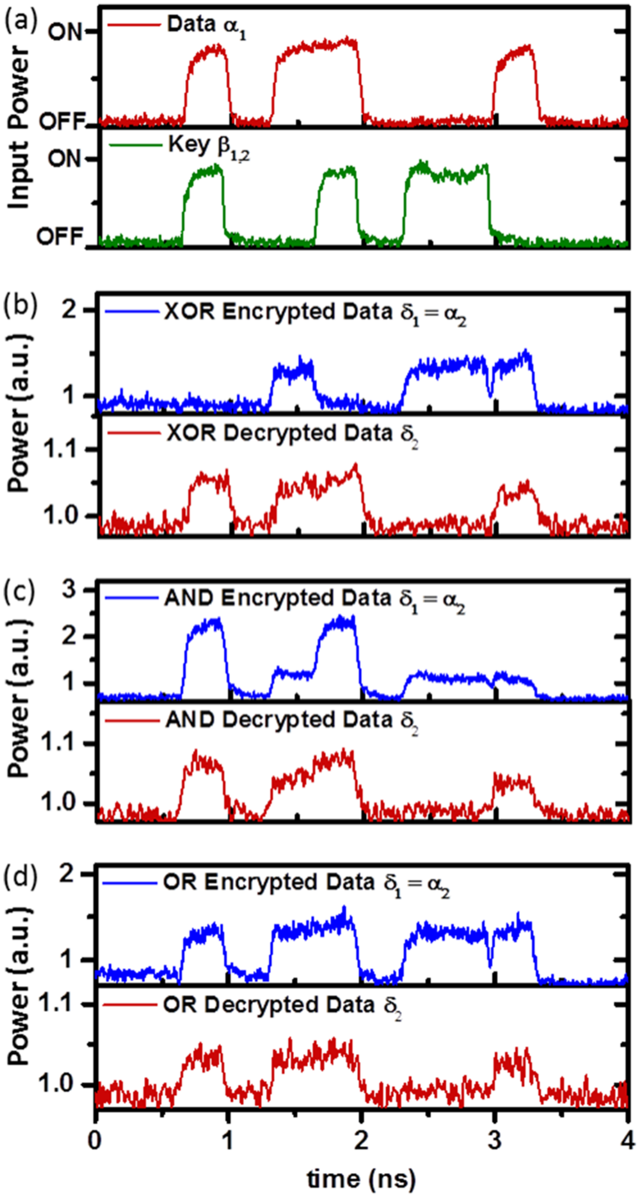


FIG. 3. Encryption and decryption in the coherent information network at 3 Gbit/s using different types of optical gates. The encryption-decryption performance is illustrated for optical signal and key sequences as presented in (a). Encrypted and decrypted sequences are illustrated for coherent optical gates operating in the following encryption modes: (b) XOR, (c) AND, (d) OR.

TABLE I. Security of coherent encryption modes. Amount of information that can be deciphered by an eavesdropper detecting the encrypted data signal.

	Information that can be deciphered from encrypted data	
Coherent encryption mode	Intensity detection (%)	Intensity and phase detection (%)
XOR	0	50
AND	50	50
OR	25[a]	100
Secrecy layer	0	0

[a] Assuming a data signal with an equal number of logical "0" and "1" states.

information about the secret message from the intensity of either the encrypted signal or the key alone: Both intensity levels in key and encrypted signal may correspond to either 1 or 0 in the data. In the case of AND encryption [Fig. 3(c)], where data and key input states of 1 and 1 are transmitted by coherent transparency, Eve can determine 50% of the data bits from the intensity of the encrypted signal, which contains 3 levels. By identifying the highest and lowest intensity levels as 1 and 0, respectively, Eve can read 10x10xxx. In the case of OR encryption [Fig. 3(d)], where any data and key input pulses are encrypted with the same intensity, Eve can read 25% of the data bits from the encrypted signal intensity. By identifying the low intensity level as 0, Eve can read x0xx0xxx and she can further assume that 2/3 of the remaining bits are likely to be 1 (assuming an equal loading between 0 and 1 bits). In all cases, Bob successfully decrypts the secret message.

Thus, if Eve can only detect intensity, then coherent XOR encryption is secure and AND and OR encryptions are partially secure as summarized in Table I. However, we examine next the case where Eve can also detect phase. Figure 4 illustrates the data, key, encrypted, and decrypted states in terms of intensity and phase, where the security of the encryption scheme depends on whether information about the secret data can be derived from the encrypted signal without the knowledge of the key (which is independent of the data and therefore cannot contain information about the data). It turns out that the high intensity states for XOR and OR encryption have different phases, allowing their decryption by phase-detection. This allows Eve to read 50%, 50% and 100% of the encrypted data in the case of XOR, AND and OR encryption respectively, without the knowledge of the key (Table I).

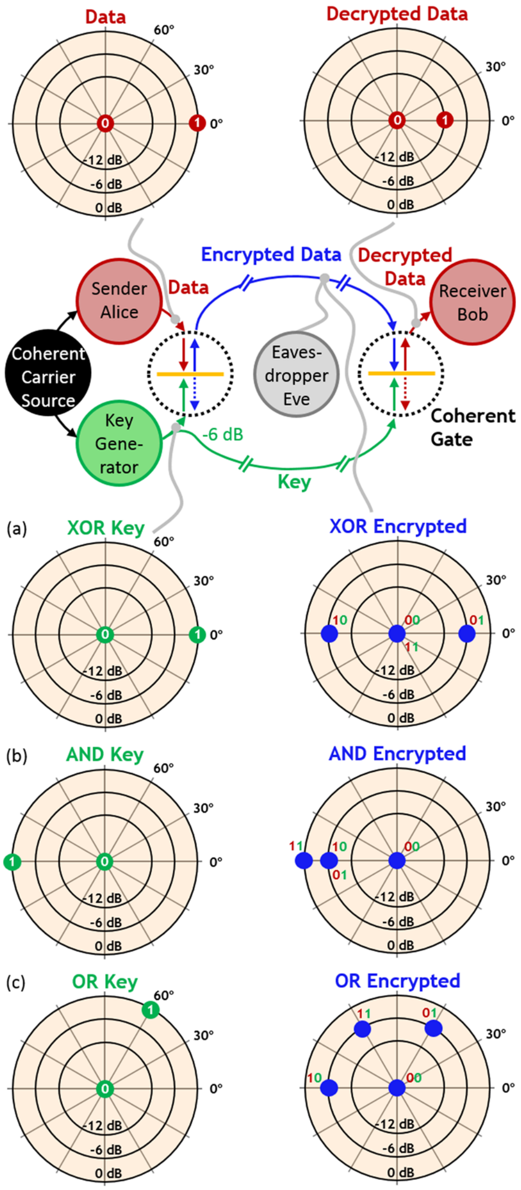


FIG. 4. Security of coherent encryption with different all-optical gates. Polar diagrams showing power and phase (as radius and angle) of data, key, encrypted, and decrypted states for the characteristic encryption modes of (a) XOR, (b) AND, and (c) OR using four-port coherent optical gates based on a thin film absorber. The binary logical states are denoted by "0" and "1". Assume eavesdropper Eve attempts to recover the data (red) by detecting the encrypted signal (blue). XOR encrypted data cannot be decrypted by detecting power alone and only partial decryption is possible with simultaneous power and phase detection. AND encrypted data can only be partially decrypted by power detection and phase detection does not provide any additional information. Full decryption of OR encrypted data is possible only by simultaneous detection of power and phase.

IV. PERFECT SECRECY SCHEME

However, we argue that the coherent encryption scheme may be adapted to become completely secure. To achieve this, the original coherent information network (Fig. 1) is modified by replacing the key generator with a "secrecy layer" (Fig. 5) that modulates the data channel in addition to generating the optical key. Alice starts with the same intensity-modulated data as before (states 0 and 1) and a CW signal from the same laser that has a phase difference of $\pi/3$ relative to the data. For randomly chosen data bits, the secrecy layer simultaneously applies a π phase shift to the data and a $\pi/3$ phase shift to the CW laser signal, generating phase-shifted data (α_1) and optical key (β_1), respectively. These are then used for encryption on Alice's coherent optical gate. Thus, the states 1 and 0 are encrypted using the key state K, while the phase-shifted data states 1′ and 0′ are encrypted with the phase-shifted key state K′ (Fig. 5). Considering Eq. (2), a perfect absorber encryption gate will generate

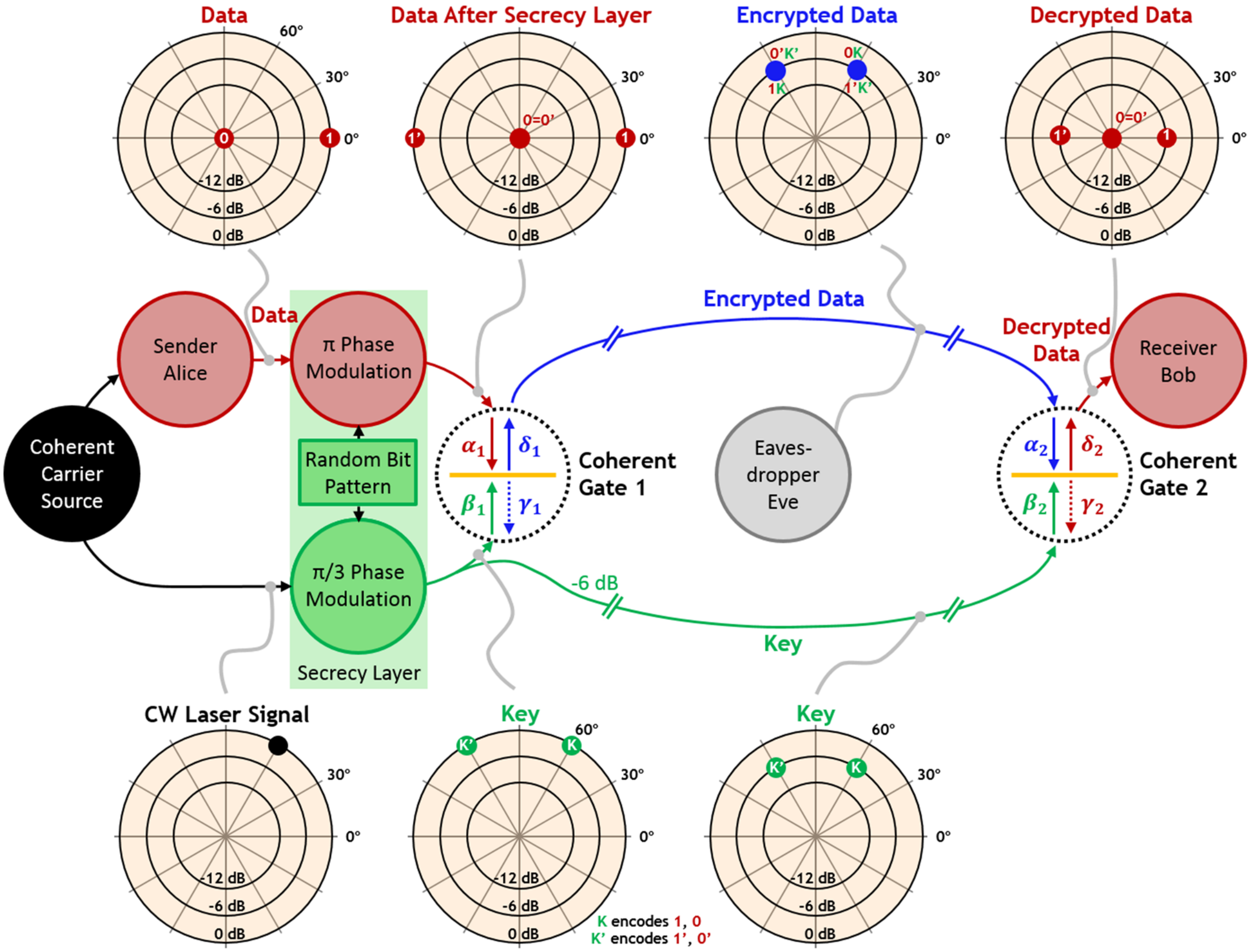


FIG. 5. Secure coherent encryption and decryption with secrecy layer. A secure encryption scheme, where neither the transmitted key nor the transmitted encrypted data alone reveals any information about the secret data. The binary logical states are represented by 0 and 1 and the key is represented by K, where ′ represents a phase shift that is applied simultaneously to data and key for randomly chosen bits.

encrypted data (δ_1) according to $E_{\delta 1} = E_{\beta 1}/2 - E_{\alpha 1}/2$. It follows from consideration of all four possible combinations of phase-shifted data and key that the encryption operation will map the original data states of 0 and 1 to only two encrypted states, with equal probability (Fig. 5). Eve cannot derive any information about the original data from the knowledge of intensity and phase of either key or encrypted data alone (perfect secrecy, Table I). In other words, encryption may translate the data into any bit sequence of the same length and all are equally likely. Nevertheless, Bob still recovers the original message by detecting only intensity after coherent absorption of the key in his coherent optical gate. We note that it does not matter that the decrypted data still contains the phase shift that was applied to random data bits, as intensity detection does not distinguish between bits without and with phase-shift (e.g., 1 and 1′). Perfect secrecy requires that the key is truly random, never reused, and at least as large as the data bit sequence. If this is satisfied, then Eve could only decrypt the data by simultaneously reading encrypted data and key including their mutual phase. This would be a complex task as these are sent along different fibres in our implementation. (As in other one-time pad encryption systems, this vulnerability could be avoided by using pre-shared keys: Bob could apply a pre-shared key bit sequence to an unmodulated CW laser signal sent by Alice.) Suitable, truly random key bit sequences can be generated at up to 300 Gbit/s based on the output of chaotic semiconductor lasers.[33] Recent measurements of coherent absorption indicate that encryption and decryption on metamaterial-based coherent optical gates can support bitrates of at least 1 Tbit/s in fibre-optic systems[28] (limited by fibre dispersion) and 100 Tbit/s in free-space implementations.[30]

V. CONCLUSIONS

We have shown how the phase of mutually coherent information carriers can be exploited for cryptography in coherent information networks. We have demonstrated encryption and decryption of intensity-modulated optical data on fibre-integrated coherent optical gates based on plasmonic metamaterial absorbers. Encryption is based on creating a superposition of mutually coherent data and key signals in a first coherent optical gate and decryption exploits coherent absorption of the key in a second coherent optical gate to recover the original data signal. We have demonstrated three characteristic modes of encryption at a bit-rate of 3 Gbit/s, identified their vulnerabilities and proposed a more advanced implementation that provides perfect secrecy (i.e., no information about the data can be derived from either encrypted data or key alone). As the underlying principle of coherent absorption is compatible with single photon signals and few femtosecond pulses, our cryptographic scheme has potential applications in quantum cryptography as well as energy-efficient and high-bandwidth cryptography and all-optical signal processing within coherent networks.

ACKNOWLEDGMENTS

This work was supported by the UK's Engineering and Physical Sciences Research Council (Grant Nos. EP/M009122/1, EP/P003990/1, and EP/N00762X/1) and the MOE Singapore (Grant No. MOE2016-T3-1-006). Following a period of embargo, the data from this paper will be available from the University of Southampton ePrints research repository: http://doi.org/10.5258/SOTON/D0873.

REFERENCES

[1] F. Miller, *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams* (C. M. Cornwell, New York, 1882).

[2] G. S. Vernam, "Secret signaling system," U.S. patent 1310719A (22 July 1919).

[3] G. S. Vernam, J. AIEE **45**(2), 109 (1926).

[4] D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, 2005).

[5] C. E. Shannon, Bell Syst. Tech. J. **28**(4), 656 (1949).

[6] W. Tuchman, in *Internet Besieged*, edited by E. Denning Dorothy and J. Denning Peter (ACM Press/Addison-Wesley Publishing Co., 1998), p. 275.

[7] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard* (Springer Science & Business Media, 2013).

[8] D. Bouwmeester, A. K. Ekert, and A. Zeilinger, *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation and Quantum Computation* (Springer Science & Business Media, 2013).

[9] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**(P1), 7 (2014).

[10] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**(2), 441 (2000).

[11] R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**(2), 120 (1978).

[12] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, IEEE Trans. Inf. Forensics Secur. **6**(3), 725 (2011).

[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, Nature **438**, 343 (2005).

[14] B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, Opt. Express **21**(2), 2065 (2013).

[15] J. A. Salehi, IEEE Trans. Commun. **37**(8), 824 (1989).

[16] P. C. Teh, P. Petropoulos, M. Ibsen, and D. J. Richardson, IEEE Photonics Technol. Lett. **13**(2), 154 (2001).

[17] P. R. Prucnal, *Optical Code Division Multiple Access: Fundamentals and Applications* (CRC Press, 2005).

[18] K. Kikuchi, J. Lightwave Technol. **34**(1), 157 (2016).

[19] F. Buchali, F. Steiner, G. Böcherer, L. Schmalen, P. Schulte, and W. Idler, J. Lightwave Technol. **34**(7), 1599 (2016).

[20] G. Rademacher, R. S. Luís, B. J. Puttnam, T. A. Eriksson, E. Agrell, R. Maruyama, K. Aikawa, H. Furukawa, Y. Awaji, and N. Wada, in Optical Fiber Communication Conference (OFC) (Postdeadline Papers), 2018, Th4C.4.

[21] L.-S. Ma, P. Jungner, J. Ye, and J. L. Hall, Opt. Lett. **19**(21), 1777 (1994).

[22] S. L. Jansen, I. Morita, T. C. W. Schenk, N. Takeda, and H. Tanaka, J. Lightwave Technol. **26**(1), 6 (2008).

[23] Y. Ma, Q. Yang, Y. Tang, S. Chen, and W. Shieh, Opt. Express **17**(11), 9421 (2009).

[24] E. Temprana, E. Myslivets, B. P. P. Kuo, L. Liu, V. Ataie, N. Alic, and S. Radic, Science **348**(6242), 1445 (2015).

[25] E. Plum, K. F. MacDonald, X. Fang, D. Faccio, and N. I. Zheludev, ACS Photonics **4**(12), 3000 (2017).

[26] X. Fang, K. F. MacDonald, and N. I. Zheludev, Light: Sci. Appl. **4**, e292 (2015).

[27] A. Xomalis, I. Demirtzioglou, E. Plum, Y. Jung, V. Nalla, C. Lacava, K. F. MacDonald, P. Petropoulos, D. J. Richardson, and N. I. Zheludev, Nat. Commun. **9**(1), 182 (2018).

[28] A. Xomalis, I. Demirtzioglou, Y. Jung, E. Plum, C. Lacava, P. Petropoulos, D. J. Richardson, and N. I. Zheludev, Appl. Phys. Lett. **113**(5), 051103 (2018).

[29] J. Zhang, K. F. MacDonald, and N. I. Zheludev, Light: Sci. Appl. **1**, e18 (2012).

[30] V. Nalla, J. Valente, H. Sun, and N. I. Zheludev, Opt. Express **25**(19), 022620 (2017).

[31] T. Roger, S. Vezzoli, E. Bolduc, J. Valente, J. J. F. Heitz, J. Jeffers, C. Soci, J. Leach, C. Couteau, N. I. Zheludev, and D. Faccio, Nat. Commun. **6**, 7031 (2015).

[32] M. Pu, Q. Feng, M. Wang, C. Hu, C. Huang, X. Ma, Z. Zhao, C. Wang, and X. Luo, Opt. Express **20**(3), 2246 (2012).

[33] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nat. Photonics **4**, 58 (2009).