Photonics based perfect secrecy cryptography: towards fully classical implementations

Valerio Mazzone,[1] Andrea Di Falco,[2] Al Cruz,[3] and Andrea Fratalocchi*[4]
[1)]*Department of Physics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland*
[2)]*School of Physics and Astronomy, University of St. Andrews, North Haugh, St. Andrews KY16 9SS, UK*
[3)]*Center for Unconventional Processes of Sciences (CUP Science), 6475 E Pacific Coast Highway, Los Angeles, California 90803, USA*
[4)]*PRIMALIGHT, Faculty of Electrical Engineering; Applied Mathematics and Computational Science, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia.*
* *Corresponding author. Email: andrea.fratalocchi@kaust.edu.sa*

(Dated: 18 June 2020)

Developing an unbreakable cryptography is a longstanding question and a global challenge in the internet era. Photonics technologies are at the frontline of research, aiming at providing the ultimate system capable of ending the cybercrime industry by changing the way information is treated and protected now and in the long run. Such perspective discusses some of the current challenges as well as opportunities that classical and quantum systems open in the field of cryptography as both a science and an engineering.

WHY PERFECT SECRECY?

In the old days of the Roman empire, Julius Caesar used a type of substitution cipher by codifying secret messages in which each character is shifted three places down the alphabet, thus reporting one of the first historical evidence of the use of cryptography to protect classified information[1]. Today, with an information society that transmits one billion Tbytes every year, securing the privacy of confidential data is a global challenge[2,3].

Currently, the majority of cryptosystems' security does not rely on unconditional proofs, but on mathematical or probable statements. The main idea centers on security margins: if a code is broken with n resources, the code is modified, e.g., by doubling the length of its key, so that the required resources increase exponentially. This model is vulnerable to technological development and does not protect users from the past: an attacker can store the information sent out today and wait for the right technology in order to crack the message tomorrow. History shows that this systematically happens on shorter timescales than what could possibly be predicted.

The most famous example is perhaps the breaking of the enigma machine, which was an encryption typewriter used during the second world war to transmit top secret military information. Because of the large number of combinations at the basis of the encrypted code, the enigma was considered unbreakable.

Notwithstanding, such security conjecture crumbled with the work of Alan Turing and his colleagues who cracked the enigma by engineering the first architectural computer, which was secretly used until the end of the war[4]. In this example, the security was broken and not publicly disclosed, allowing one party to freely break into the private information of the other, completely unnoticed. Another case is the US federal data encryption standard (DES), which was considered secure because a machine fast enough to break it was prohibitively expensive[5]. This probable argument did not predict the subsequent price revolution in integrated electronics, which after just twenty years allowed cracking the code[6]. The Advanced Encryption Standard (AES), which superseded the DES, was introduced in 2002. Within only seven years a realistic attack has been found to suggest a complete revision of its security margins[7], while several attacks have been publicly disclosed on its practical implementations[8–10]. The Rivest–Shamir–Adleman (RSA) cryptosystem, introduced in 1977, was considered unbreakable and it is currently in use for encrypting emails, internet and digital transactions. The RSA security conjecture was broken in less than 20 years by Peter Shor, who developed a quantum computing-based strategy that can also crack many other crypto-systems in use today, shifting current discussions towards post-quantum cryptography scenarios[11,12].

These few examples demonstrate that security conjectures of today are proven unreliable tomorrow, and require continuous revisions of standards that, if not addressed timely, expose the privacy of our present and past communications. To solve this problem permanently, cryptologists developed a third model of security, known as perfect secrecy. Perfect secrecy has been defined by Claude Shannon as[13]:

"...a system that after a cryptogram is intercepted by the enemy the a posteriori probabilities of this cryptogram representing various messages be identically the same as the a priori probabilities of the same messages before the interception."

In this system, an attacker cannot do better than to best guess the message without having seen it, while the secrecy of the information being communicated is unconditionally "perfect".

It might be surprising to know that a perfect secrecy cryptography has existed for a century , but it has not been adopted in practice yet. This cryptography system has been known as the Vernam cipher or the one-time pad (OTP)[14], and it is based on four conditions: i) the users share an identical random key that is as long as the message, ii) the key is kept secret, iii) the

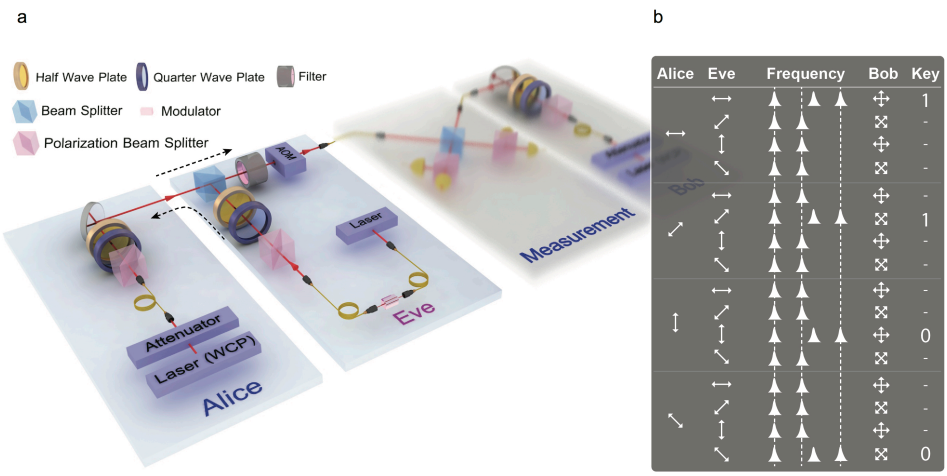

FIG. 1. Schematic algorithm Of the BB84 protocol. a) Communication setup. b) Key generation scheme. Reprinted with permission from Xiao-Ling Pang *et al.*, Physical Review Applied, 13, 034008 (2020). Copyright 2020 by the American Physical Society.

key is never reused, iv) each key is uncorrelated to the others. Shannon rigorously demonstrated that a cryptography satisfying i)-iv) can never be beaten.

Given the OTP, the crux that limited the adoption of the scheme relates to implementing the key distribution step at points i) and ii). The question is to solve the following problem: if two users have at disposal a secure channel to transmit a one time key that is as long as the message, the users would rather use the channel to send the message and not the key. In this security model the question has shifted from transmitting secure texts to distribute secure keys among different users.

LEVERAGING ON THE LAWS OF PHYSICS

As it happens in science, the solution to an apparently lockdown problem in one field is obtained by borrowing concepts from other scientific areas. In this case, a solution path towards implementing key distribution through the physics of quantum light was suggested by Bennett and Brassard in the BB84 quantum key distribution (QKD) protocol[15].

In the scheme (Fig. 1a), one user (Alice) generates bit sequences from randomly polarized single photons among four different angular directions, then she sends the sequence to the second user (Bob). After the sequence exchange, Alice and Bob compare the measures over a public classical channel, extracting a key from the sequence of correlated states (Fig. 1b). While the random nature of the data being exchanged with the BB84 does not make it possible to directly communicate a message, it allows to perform the key distribution to implement the OTP.

The security of the BB84 scheme leverages on the projection postulate of quantum mechanics: any measures performed on traveling photons will statistically change the photons polarization, introducing uncorrelated states between Alice and Bob that can be identified and discarded, leaving the attacker with zero information.

In the last forty years, the progress of QKD increased enormously, ranging from a large variety of mathematical algorithms for amplifying the privacy[16–20], to authenticating schemes[21–25] and to systems design[26–37]. However, despite significant advances, the implementation of QKD has challenges, notably lack of speed, high costs and low scalability of quantum communication networks. For distances beyond 100 km, QKD's communication bit rate is currently limited in the range of 100 bit/s[38], thus requiring expensive single-photons detectors operating at tens of degree below zero[39,40]. Other challenges involve implementation-related attacks, originating from the fact that the unbreakability of QKD is evaluated for ideal quantum communication channels, ideal quantum sources and detectors[41,42]. Practical implementations are not ideal, opening QKD schemes to different vulnerabilities[43–47].

A BLAST FROM CHAOS AND THERMODYNAMICS

If a method and system to incorporate QKD into a fully classical optical communication network became possible, Quantum network limitations would be overcome. In this sense, most of QKD development would be retained, all the while enabling the "last mile" with the benefits of classical optical communications. Classical optical networks currently enable data transfer rates up to Terabits per seconds (Tbps)[48], global transmission distance covering the entire planet with contained costs[2,49], and ultrafast switching technology for demultiplexing different users[50–52].

In the recent work[53] the authors demonstrate that such method and system indeed is feasible. They addressed the limitations of QKD and demonstrated solutions by using the theory of chaos formulated for thermodynamic irreversible systems. There is an intimate connection between quantum mechanics and chaos, which was initially explored by A. Einstein[54]. While a quantum system is in general unpredictable because any taken measure would force the system to collapse into an eigenstate chosen with random probability, a classical chaotic

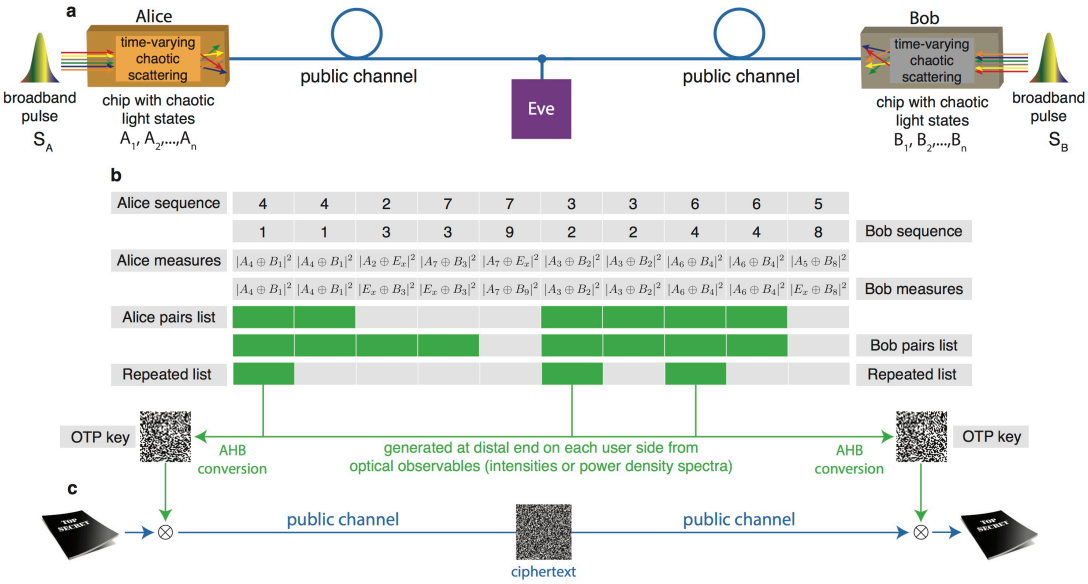

FIG. 2. A classical version of BB84. (a) Communication setup on a classical public optical channel. (b) Communication and key generation steps. (c) Encryption and decryption scheme via bitwise XOR between the text and the generated key. Adapted with permission from Di Falco, A. *et al.*, "Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips". Nat Commun 10, 5827 (2019), under license CC BY-SA 4.0.

system is equivalently unpredictable because each implementation is never identical; thus it is mathematically impossible to anticipate the system's evolution[55].

By leveraging on this property, the algorithm in[53] proposes a classical version of the BB84 QKD scheme by using chaotic correlated wavepackets generated from thermodynamic irreversible random media (Fig. 2). In this system, Alice and Bob employ two different chips (Fig. 2a) composed of time varying distribution of scatterers, which are implemented by etching holes in a silicon on insulator (SOI) platform. The chips are connected to two broadband light sources S_A and S_B, which are different for each user (Fig. 2a). The sources differences set the desired bit error rate (BER) for the communication. Each user can independently vary the input conditions A_n and B_n of light injected into the chips at every step i of the communication. Different input conditions play the role of different polarization states in the BB84 scheme. In the chaotic chips of Fig. 2, the number of input conditions is not limited to four and grows linearly with the size of the chips[53]. To couple a broadband light pulse into the chip at ultrafast speed it is possible to use directly addressable $1 \times N$ fiber bundles, which are commercially available and can also be manufactured directly in the chip.

At each communication step (Fig. 2b), Alice and Bob choose randomly a coupling waveguide, then send the spectra $A_n(i)$ and $B_n(j)$ in the public channel, detecting at each end the combined power density spectrum $|A_n(i) \oplus B_n(j)|^2$ and $|B_n(j) \oplus A_n(i)|^2$, respectively ($\oplus$ is the operator that combines the states after the propagation over the channel). If the status of the chips and that of the channel do not change during each communication step, then system is reciprocal and $|A_n(i) \oplus B_n(j)|^2 = |B_n(j) \oplus A_n(i)|^2$. In the following communication step, Alice and Bob independently decide whether to change the coupling waveguide and/or chip status or to repeat the sending and acquisition procedure. The steps are repeated as many times as required. At the end of the exchange, following the same idea of BB84, Alice and Bob communicate openly which steps have been repeated, and extract the respective signal by identifying a sequence of repeated spectra, which are digitized into an OTP key (Fig. 2c). Once the key is generated, the two chips are changed in time by an irreversible transformation. This transformation is applied independently by each user and it is not disclosed. A second irreversible transformation is applied prior to the next communication.

The above scheme implements conditions i)-iv) of the OTP: it allows the ultrafast transmission of a key that is as long as the message via classical optical communications; it generates completely uncorrelated keys in the complex scattering chips; it does not disclose the key to the attacker; it never reuses the same key. As in the BB84 QKD protocol, the security of this scheme is dictated by the laws of physics. The second law of thermodynamics does not permit to an attacker to duplicate the chips once the communication takes place, as it would require to invert an irreversible physical transformation, and the mathematical unpredictability of chaos makes it impossible for an enemy to reconstruct the correlated states $|A_n(i) \oplus B_n(j)|^2$ and $|B_n(j) \oplus A_n(i)|^2$, which can be observed only in the isolated network connecting the two users. A third person who tries to obtain the same states by measuring the data flowing in the communication line, in fact, will inevitably perturb the system. This action always results in one bit of uncertainty for every bit measured, regardless the type of attack employed or the type of instrumentation used[53].

In analogy to the BB84 scheme, active manipulation of the states generates uncorrelated sequences that can be isolated and removed with the many techniques of privacy amplifica-

tion and error reconciliation already developed for QKD. An advantage of this scheme compared to BB84 is that any non-ideal component present in the experimental realization sums up to increase the unpredictability of the system, and it does not furnish vulnerabilities[53].

It is interesting to discuss the technological requirements of the chip with respect to experimental implementations with different platforms, communication speed and scalability. In the scheme of Fig. 2, the OTP key length is proportional to the bandwidth of the spectrum, which in turn limits the maximum transmission rate B because of the fiber dispersion and the associated pulse broadening. An accepted rule of thumb is $B \leq \frac{1}{4\Delta\tau}$, where $\Delta\tau = D \cdot L \cdot \Delta\lambda$ is the pulse broadening factor with D the dispersion, L the length of the fiber and $\Delta\lambda$ the pulse bandwidth. For a single mode fiber with dispersion $D = 1$ ps$/$(km $\cdot$ nm) and length $L = 100$ km, the safe transmission of pulses with bandwidth $\Delta\lambda = 100$ nm can be as fast as $B_{max} = 25$ Mb$/$s. This value is $2 \cdot 10^5$ faster than the current best rate of QKD.

These figures give the upper boundaries for the speed required for the input waveguide switch. Current integrated waveguide arrays can be dynamically tuned using thermal, mechanical, electrical or all optical methods, with associated switching speed up to tens of fs[56], which is abundantly faster than the transmission requirements.

The state of the individual chips can be changed e.g. by coating the surface of the chip with colloidal scatterers dispersed in a solution, delivered by a microfluidic channel, allowing a material/s to be continuously deformed by external conditions such as temperature and light.

Another important factor is the number of uncorrelated channels that can be addressed at the input of the scattering section. In[53] it is demonstrated that shifting the input beam by 200 nm is enough to create uncorrelated transmission spectra. The aforementioned shows the possibility to scale up to $0.03 \cdot N_b$·Tb of different keys —with N_b the number of bits extracted from each spectrum— for every *mm* of width of the chip and prior to every irreversible transformation.

Future work includes coupling the above mentioned system to authentication schemes, addressing the security gaps that will be increasing with the evolution of society in the near future with the advent of e.g., Smart City, Internet-of-Things (IoT), Cloud Computing, Big Data, and especially the tendency that biometrics systems will be everywhere in the society.

LOOKING FORWARD

Developing unconditionally secure communications is an exciting journey that has been pursued for thousands of years, and that is not yet concluded. While there are still plenty of challenges, there are also a large number of opportunities for developing applications that could counteract a six trillion dollar cybercrime industry[57]. If perfect secrecy were to fundamentally impact society, it will need to offer ultrafast resources at a reasonable cost for users connected everywhere. *"Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it*[58]*." (Tim Cook, Apple CEO).*

DATA AVAILABILITY

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ACKNOWLEDGEMENTS

A.D.F. acknowledges support from EPSRC (EP/L017008/1).

[1] D. Luciano and G. Prichett, "Cryptology: From caesar ciphers to public-key cryptosystems," The College Mathematics Journal **18**, 2–17 (1987).

[2] E. Agrell, M. Karlsson, A. R. Chraplyvy, D. J. Richardson, P. M. Krummrich, P. Winzer, K. Roberts, J. K. Fischer, S. J. Savory, B. J. Eggleton, M. Secondini, F. R. Kschischang, A. Lord, J. Prat, I. Tomkos, J. E. Bowers, S. Srinivasan, M. Brandt-Pearce, and N. Gisin, "Roadmap of optical communications," Journal of Optics **18**, 063002 (2016).

[3] D. Adam, "Cryptography on the front line," Nature **413**, 766–767 (2001).

[4] A. Hodges, *Alan Turing: The Enigma* (Vintage, 1992).

[5] "DES (data encryption standard) review at Stanford University recording & transcript. https://web.archive.org/web/20120503083539/http://www.toad.com/des-stanford-meeting.html.".

[6] E. F. Foundation, M. Loukides, and J. Gilmore, *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design* (O'Reilly & Associates, Inc., USA, 1998).

[7] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, "Key recovery attacks of practical complexity on aes variants with up to 10 rounds," Cryptology ePrint Archive, Report 2009/374 (2009), `https://eprint.iacr.org/2009/374`.

[8] A. Biryukov, D. Khovratovich, and I. Nikolić, "Distinguisher and related-key attack on the full aes-256," in *Advances in Cryptology - CRYPTO 2009*, edited by S. Halevi (Springer Berlin Heidelberg, Berlin, Heidelberg, 2009) pp. 231–249.

[9] E. Bangerter, D. Gullasch, and S. Krennn, "Cache games – bringing access-based cache attacks on aes to practice," (2010), `http://eprint.iacr.org/2010/594.pdf`.

[10] D. A. Osvik, A. Shamir, and E. Tromer, "Cache attacks and countermeasures: the case of aes," (2005), `http://www.wisdom.weizmann.ac.il/~tromer/papers/cache.pdf`.

[11] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) pp. 124–134.

[12] R. Grimes, *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto* (Wiley, 2019).

[13] C. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, Vol 28, pp. 656–715 (1949).

[14] G. S. Vernam, "Secret signaling system," (1919), uS Patent 1,310,719.

[15] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical Computer Science **560**, 7 – 11 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[16] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Transactions on Information Theory **41**, 1915–1923 (1995).

[17] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," SIAM journal on Computing **17**, 210–229 (1988).

[18] L. Masanes, "Universally composable privacy amplification from causality constraints," Physical review letters **102**, 140501 (2009).

[19] Y. Watanabe, "Privacy amplification for quantum key distribution," Journal of physics A: Mathematical and theoretical **40**, F99 (2006).

[20]A. M. Abbas, A. Goneid, and S. El-Kassas, "Privacy amplification in quantum cryptography bb84 using combined univarsal2-truly random hashing," International Journal of Information and Network Security **3**, 98 (2014).
[21]N. Penghao, C. Yuan, and L. Chong, "Quantum authentication scheme based on entanglement swapping," International Journal of Theoretical Physics **55**, 302–312 (2016).
[22]G. Zeng and W. Zhang, "Identity verification in quantum key distribution," Physical Review A **61**, 022303 (2000).
[23]B.-S. Shi, J. Li, J.-M. Liu, X.-F. Fan, and G.-C. Guo, "Quantum key distribution and quantum authentication based on entangled state," Physics letters A **281**, 83–87 (2001).
[24]S. Lin, H. Wang, G.-D. Guo, G.-H. Ye, H.-Z. Du, and X.-F. Liu, "Authenticated multi-user quantum key distribution with single particles," International Journal of Quantum Information **14**, 1650002 (2016).
[25]C. ho Hong, J. Heo, J. G. Jang, and D. Kwon, "Quantum identity authentication with single photon," Quantum Information Processing **16**, 236 (2017).
[26]M. Leonetti, S. Karbasi, A. Mafi, E. DelRe, and C. Conti, "Secure information transport by transverse localization of light," Scientific Reports **6**, 29918 (2016).
[27]S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," Nature **564**, 225–228 (2018).
[28]S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
[29]P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, *et al.*, "Chip-based quantum key distribution," Nature communications **8**, 1–6 (2017).
[30]X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," Physical Review X **8**, 031043 (2018).
[31]N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Science advances **3**, e1701491 (2017).
[32]P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nature photonics **7**, 378–381 (2013).
[33]B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nature Photonics **9**, 163 (2015).
[34]J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," Science **356**, 1140–1144 (2017).
[35]G. Popkin, "China's quantum satellite achieves 'spooky action'at record distance," Sci Mag **15** (2017).
[36]S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, B. Liu, T. Scheidl, S. M. Dobrovolskiy, R. van der Molen, J. W. Los, V. Zwiller, *et al.*, "Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre," npj Quantum Information **6**, 1–5 (2020).
[37]D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labonté, and S. Tanzilli, "Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography," Laser & Photonics Reviews **10**, 451–457 (2016).
[38]H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Physical review letters **117**, 190501 (2016).
[39]E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Information **2**, 1–12 (2016).
[40]M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Efficient decoy-state quantum key distribution with quantified security," Optics express **21**, 24550–24565 (2013).
[41]L. O. Mailloux, M. R. Grimaila, D. D. Hodson, C. V. McLaughlin, and G. B. Baumgartner, "Quantum key distribution: Boon or bust?" Journal of Cyber Security and Information Systems **4**, 18–26 (2016).
[42]V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," Theoretical Computer Science **560**, 27–32 (2009).
[43]J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, "Hacking the bell test using classical light in energy-time entanglement–based quantum key distribution," Science advances **1**, e1500793–(7) (2015).
[44]H. P. Yuen, "Security of quantum key distribution," IEEE Access **4**, 724–749 (2016).
[45]S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, "Effect of source tampering in the security of quantum cryptography," Physical Review A **92**, 022304–(8) (2015).
[46]V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Reviews of modern physics **81**, 1301–1350 (2009).
[47]N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Physical Review A **61**, 052304–(10) (2000).
[48]M. Jinno, Y. Miyamoto, and Y. Hibino, "Networks: optical-transport networks in 2015," nature photonics **1**, 157 (2007).
[49]T. Otani, K. Goto, H. Abe, M. Tanaka, H. Yamamoto, and H. Wakabayashi, "5.3 gbit/s 11300 km data transmission using actual submarine cables and repeaters," Electronics Letters **31**, 380–381 (1995).
[50]V. Sasikala and K. Chitra, "All optical switching and associated technologies: a review," Journal of Optics **47**, 307–317 (2018).
[51]E. Stassen, C. Kim, D. Kong, H. Hu, M. Galili, L. K. Oxenløwe, K. Yvind, and M. Pu, "Ultra-low power all-optical wavelength conversion of high-speed data signals in high-confinement algaas-on-insulator microresonators," Apl Photonics **4**, 100804 (2019).
[52]D. Liang, X. Huang, G. Kurczveil, M. Fiorentino, and R. Beausoleil, "Integrated finely tunable microring laser on silicon," Nature Photonics **10**, 719 (2016).
[53]A. D. Falco, V. Mazzone, A. Cruz, and A. Fratalocchi, "Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips," Nature Communications **10**, 5827 (2019).
[54]M. Gutzwiller, *Chaos in Classical and Quantum Mechanics*, Interdisciplinary Applied Mathematics (Springer New York, 1991).
[55]E. Ott, *Chaos in Dynamical Systems*, 2nd ed. (Cambridge University Press, 2002).
[56]I. O'Connor and G. Nicolescu, *Integrated optical interconnect architectures for embedded systems* (Springer Science & Business Media, 2012).
[57]"2019 official annual cybercrime report." `https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/`.
[58]L. Kahney, *Tim Cook: The Genius Who Took Apple to the Next Level* (Penguin Books Limited, 2019).