Giant Fiber Lasers: A New Paradigm for Secure Key Distribution

Jacob Scheuer[1,*] and Amnon Yariv[2]

[1]School of Electrical Engineering, Tel-Aviv University, Ramat-Aviv, Israel

[2]Department of Applied Physics, California Institute of Technology, Pasadena, California, USA

(Received 27 April 2006; published 6 October 2006)

We propose and analyze a new concept for secure key distribution based on establishing laser oscillations between the sender and receiver. Compared to quantum mechanics based systems, our scheme allows for significantly higher key-establishing rates and longer ranges. By properly designing the laser structure, it is possible to increase the difficulty of eavesdropping almost arbitrarily, thus making our scheme an intriguing alternative and a complementary technology to quantum key-distribution systems.

DOI: 10.1103/PhysRevLett.97.140502 PACS numbers: 03.67.Dd, 42.55.Wd

The distribution of a secret key is most probably the main Achilles' heel of any secure communication system. To establish a completely secure information transfer, it is necessary for the two users to share a secret key, known only to them, before the communication can take place [1]. In many practical scenarios, especially when the two users are separated by a large distance, this requirement is difficult to realize because secure transmission of the key requires a previously shared (additional) key. This loophole was one of the main incentives behind the attempts to develop physically (as opposed to algorithmically) secure key-distribution schemes based on the fundamental properties of quantum mechanics [2–5]. Although ideally such communication protocols are perfectly secure [6], their practical implementation is not simple. Noise and attenuation in the quantum channel reduce significantly their efficiency, especially from the range and data rate aspects. Theoretical and experimental studies show that channel attenuation, noise, and detector dark counts limit the key-establishing rates and the operational ranges of quantum key-distribution (QKD) systems [3,7–11].

Recently, a classical key-distribution system (KDS) utilizing Johnson noise in resistors was suggested [12,13]. Although conceptually interesting, the suggested scheme was found to be vulnerable to an analysis of the transients of the electromagnetic waves propagating in the transmission line connecting the two parties [14]. Here we propose and analyze a new concept for key distribution, based on establishing a laser oscillation between the sender and receiver. The suggested architecture offers potential key-establishing rates which are larger by several orders of magnitude than those of the currently demonstrated QKD systems, especially at long communication ranges.

Referring to Fig. 1, the system consists of a long erbium-doped fiber laser with Alice at one end and Bob on the other. In the example depicted in Fig. 1, Bob and Alice can each choose independently a mirror from a set of three mirrors (one set at each end), labeled "T," "1," and "0" (see the inset in Fig. 1), and use it as the laser reflector at their end. Each of the three mirrors in a set has its peak at a different frequency. The T mirror is centered on ω_0, mirror 1 is centered on $\omega_0 + \delta\omega$, and mirror 0 is centered on ω_0-$\delta\omega$. The erbium-doped amplifiers (EDFA) provide the optical gain for the laser, and the inline filters IF_A and IF_B are narrow-band filters centered at ω_0. Each communication cycle (i.e., the generation of a bit for the key) starts with Alice and Bob placing their mirror at ω_0 (T). This phase resets the symmetry of the system and establishes synchronization. Next, they each randomly select a bit (i.e., 0 or 1) and switch on the appropriate mirror. The laser gain is maintained at a level such that if they pick different bits, there is sufficient gain for the laser to lase at ω_0 but at a lower amplitude compared to the T state. If they both choose 1, the lasing wavelength shifts to $\omega_0 + \delta\omega$, and if they choose 0, the lasing wavelength shifts to ω_0-$\delta\omega$ (see also Fig. 3).

The choice of mirrors determines the lasing characteristics of the laser, allowing each of the two parties to deduce which mirror was selected at the other end and, thus, to exchange a bit. To achieve security, the determination of the mirrors' choice should be simple for legiti-

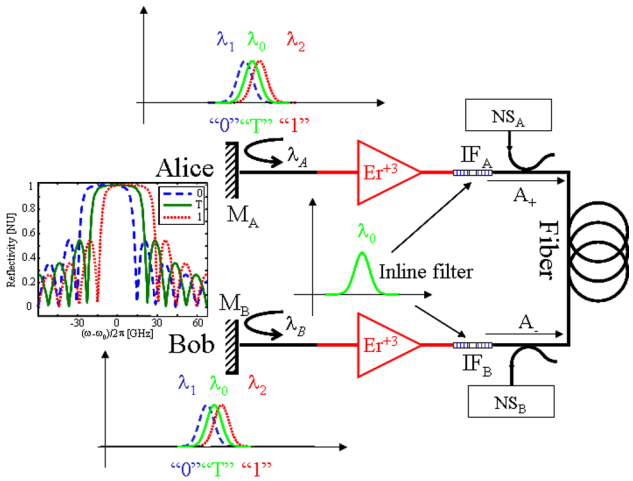

FIG. 1 (color online). GFL system for secure key distribution. M_A, M_B: Alice's and Bob's end mirrors; IF_A, IF_B: inline filters; NS_A, NS_B: broadband noise sources. Inset: Frequency response of the three mirrors at the three different states.

mate users but very difficult (ideally impossible) for an eavesdropper (Eve). Thus, the KDS should effectively serve as a "physical" one-way function. A straightforward way to accomplish that is by devising a system which indicates only the correlation (the XOR value) between the bits selected by the two parties. For Alice and Bob (who know their own bit), the correlation is sufficient to determine the values of both bits, but for Eve it is not.

The security level provided by the giant fiber laser (GFL) system is determined by the ability of Eve to extract more information than merely the correlation between the bits. To quantify this capability, a more detailed model of the scheme is considered. Referring to Fig. 1, the electromagnetic field evolving in the laser is a superposition of rightward and leftward propagating waves [$A_+(\omega)$ and $A_-(\omega)$, respectively], defined at the middle of the system ($z = L/2$). The lengths of the laser and the active region are L and d, respectively.

In each round-trip, the (complex) amplitude of, say, A_- is filtered by IF_A and amplified by Alice's EDFA, reflected from M_A, and then amplified and filtered again to generate the right propagating wave A_+. In each amplification stage, the spontaneous emission (SE) noise of the EDFA is added to the propagating field. A similar relation connects A_+ to A_-, thus yielding the following coupled equations for the evolution of the field amplitudes:

$$\begin{aligned} A_+^{l+1}(\omega) &= \{[A_-^l(\omega)\exp(\tfrac{1}{2}i\beta L)T_{\mathrm{IF}}(\omega)\exp(\gamma d/2) \\ &\quad + A_S(\omega)]r_A(\omega)\exp(\gamma d/2) \\ &\quad + A_S(\omega)\}T_{\mathrm{IF}}(\omega)\exp(\tfrac{1}{2}i\beta L) + N_A(\omega), \\ A_-^{l+1}(\omega) &= \{[A_+^l(\omega)\exp(\tfrac{1}{2}i\beta L)T_{\mathrm{IF}}(\omega)\exp(\gamma d/2) \\ &\quad + A_S(\omega)]r_B(\omega)\exp(\gamma d/2) \\ &\quad + A_S(\omega)\}T_{\mathrm{IF}}(\omega)\exp(\tfrac{1}{2}i\beta L) + N_B(\omega), \end{aligned} \tag{1}$$

where l indicates the round-trip index (or, equivalently, time), r_A and r_B are, respectively, the spectral reflectance of Alice's and Bob's mirrors, T_{IF} is the transmittance of the inline filter, β is the (complex) propagation factor, N_A and N_B are the signals generated by the optional external noise sources NS_A and NS_B, whose significance is explained further below. The overall gain in the active part is given by $\exp(\gamma d/2)$, where γ is the gain coefficient given by [15]:

$$\gamma(\omega) = \frac{\gamma_0(\omega)}{1 + I/I_{\mathrm{SAT}}}, \tag{2}$$

where $\gamma_0(\omega)$ is the small signal (i.e., unsaturated) gain of the medium as determined by the pumping level, and I is the overall intensity of the field in the active medium given by $I = \int(|A_+(\omega)|^2 + |A_-(\omega)|^2)d\omega$, where I_{SAT} is the saturation intensity. Both the gain γ and the spontaneous emission power are proportional to the population inversion ΔN, and, thus, the spontaneous emission amplitude emitted from a dz thick slice of the active medium is proportional to $\sqrt{\gamma}dz$. Taking into account the amplification of the SE in the active region, the power emitted from either side of the active medium (due to SE) is

$$A_S(\omega) = \frac{2K}{\sqrt{\gamma}}(\exp(\gamma d/2) - 1), \tag{3}$$

where K is a proportion coefficient linking the square root of the gain to the emitted amplified spontaneous emission.

To examine the security of the scheme, we need to outline the reasonable eavesdropping strategies Eve can employ. For simplicity, we initially analyze the GFL system without the external noise sources ($N_A = N_B = 0$). We assume that Eve can tap the field evolving in the laser without being detected and perform any type of measurement. In particular, Eve can introduce a beam splitter (or a fiber coupler) into the cavity, separate A_+ from A_-, and analyze them separately. Like any classical electromagnetic wave, $A_\pm$ can be completely characterized by their spectral and temporal evolution—information which is available to Eve.

Is the scheme secure? Can Eve use her measurement of $A_\pm$ to determine which mirror was selected by Bob and which by Alice? Figure 2 depicts the laser output power at ω_0 for a sequence of bit selection, found by numerically integrating (1). The parameters of the system are defined in the figure caption. The power levels clearly distinguish between correlated ($A = B$) and anticorrelated ($A \neq B$) bits. Note that, in the case of the anticorrelated bits, the intensities of $A_\pm$ are indistinguishable (although they are reflected from *different* mirrors), making it impossible for

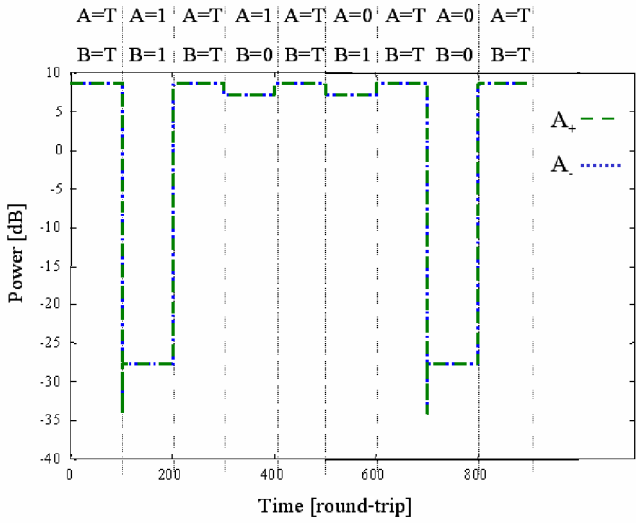

FIG. 2 (color online). Power traces of the left (dotted line) and right (dashed line) propagating waves for various bits selection by Alice and Bob. The link length is $L = 10$ km, $K\gamma_0 = 3.2 \times 10^{-4}$ $\mu\mathrm{m}^{-1}$, $d = 0.1$ m, and $I_{\mathrm{sat}} = 10$ [normalized units]. The mirrors are implemented by fiber Bragg gratings with 3 dB bandwidth of ~20 GHz and maximal reflection of ~99%. The offset between the 1 and 0 mirrors is 4 GHz. The inline filter bandwidth is ~2 GHz. The power levels are normalized to 1 mW.

Eve to learn of the choice of mirrors by monitoring the power.

Figure 3 illustrates the steady-state spectrum of the four different states of the system. The spectra of the (1, 1) and (0, 0) cases differ significantly, making it possible for Eve to distinguish between them. These bits cannot be used to attain secure communication and are, therefore, discarded. The spectra of the anticorrelated bits (1, 0) and (0, 1) are very similar though not identical—the spectra of A_+ and A_- are mirror images of each other about $\omega_0 - A_+(\omega - \omega_0) = A_-(\omega_0 - \omega)$. Nevertheless, the difference is very small, thus compelling Eve to be able to distinguish between signals which are -40 dB below the lasing power. These bits are, therefore, retained and are added to the key.

In principle, Eve can determine the exchanged bit in the anticorrelated bits case by careful examination of the spectrum of $A_\pm$. However, the difference between the two spectra can be made essentially as small as desired, and thus subvert Eve's spying, by including additional inline filtering in the laser. To demonstrate this point, we depict in Fig. 4(a) the powers of $A_\pm$ at ω_0 for the same sequence of bits as in Fig. 2 when an additional, and similar, inline filter centered at ω_0 is employed. Figures 4(b)–4(d) show the corresponding spectra of $A_\pm$ for correlated bits [Fig. 4(b)] and for the two anticorrelated bits possibilities. While the additional filtering does not significantly affect the lasing intensity, its impact on the spectra at the anticorrelated states is dramatic [see Figs. 4(c) and 4(d)]. The ratio of the spectra of A_+ and A_- is reduced to less than 0.5 dB at the -45 dB level, compared to ~ 3 dB in the case of a single inline filter (Fig. 3).

Thus, the difference between the spectra of $A_\pm$ can be reduced almost arbitrarily, making the task of determining the exchanged bit *technologically* difficult for Eve. The last property is of supreme importance, because any practical measurement performed by Eve is limited by the noise floor and the dynamic range of her apparatus. Therefore, the communicating parties can *always* reduce the signature of their bit selection (imprinted in the SE spectrum of the laser) below Eve's detection capability and achieve secure key distribution. Alternatively (or in parallel), the noise level in the system can be increased by injecting into the fiber noise from an external broadband source (see Fig. 1), thus "drowning" the faint signals Eve is trying to detect in noise, without affecting the primary laser oscillations. Thus, in contrast to QKD systems (QKDS), noise is not an "enemy" but rather an "ally" which helps concealing the exchanged bit from Eve.

Eve may also try to *actively* probe the mirrors' reflection spectrum in order to determine Alice's and Bob's choice of mirrors. In this case, Eve's injected signal would be amplified by the EDFAs and could be detected by Alice and Bob. A detailed analysis of this scenario is, however, beyond the scope of this Letter.

In addition to simplicity, the GFL-KDS also provides an enhanced key-establishing rate (compared to QKDS), especially at long ranges. The minimal time it takes a laser to establish oscillations or to shift its lasing wavelength is determined by the round-trip time $-\tau = 2Ln/c$, where c is the speed of light in vacuum. For simplicity, we assume that the state of the system can be determined after $\sim 10\tau$. Therefore, the maximal key-establishing rate is given by:

$$f_{\max} \approx \frac{c/L}{20n}. \tag{4}$$

Note that the key-establishing rate decreases as $\log(f_{\max}) \sim -\log(L)$ for the GFL system, while for QKDS this rate decreases as $\log(f_{\max}) \sim -\alpha L$, where α

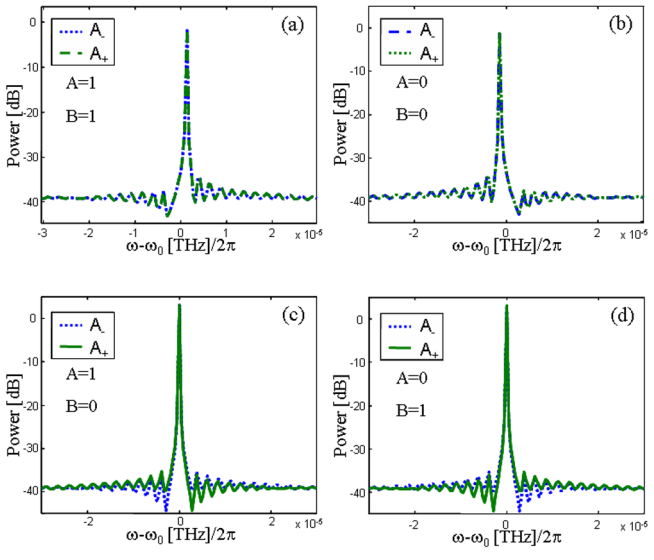

FIG. 3 (color online). Steady-state spectra of the rightward (A_+) and leftward (A_-) waves of a GFL with a single inline filter for (a) Alice = "1", Bob = "1"; (b) Alice = "0", Bob = "0"; (c) Alice = "1", Bob = "0"; and (d) Alice = "0", Bob = "1".

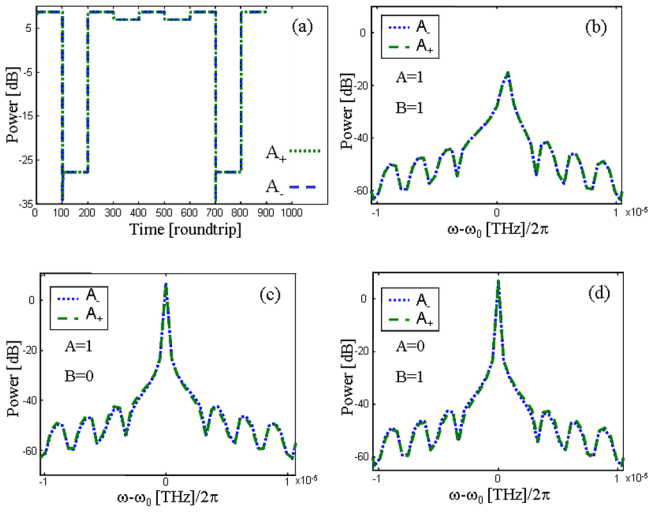

FIG. 4 (color online). Time trace intensities (a) and steady-state spectra for a GFL with additional (identical) inline filtering for (b) Alice = "1", Bob = "1"; (c) Alice = "1", Bob = "0"; and (d) Alice = "0", Bob = "1".

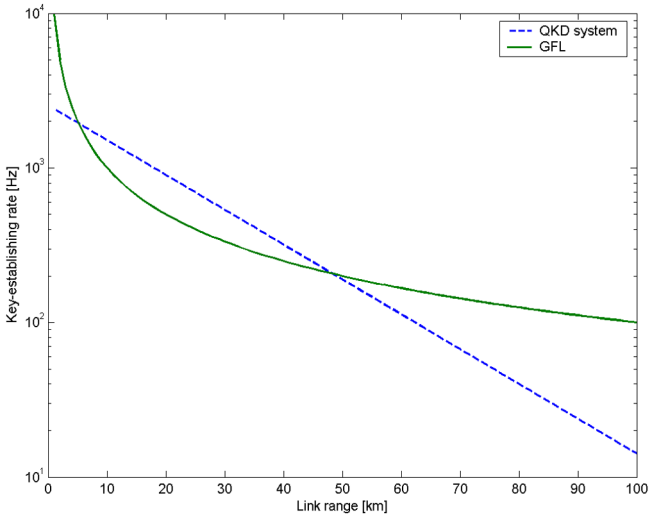

FIG. 5 (color online). Comparison between the key-establishing rates of the QKDS presented in Ref. [10] (dashed line) and the GFL system (solid line). Fiber loss is ~ 0.3 dB/km.

is the loss coefficient in the fiber (imaginary part of β). Thus, as the length of the link increases, the GFL-KDS becomes more attractive. As a concrete example, we compare $f_{\max}$ for the GFL-KDS and the measured rate of the QKDS studied in Ref. [10]. Figure 5 depicts a comparison between the key-establishing rates of the two systems. As the link length increases to more than 48 km, the GFL system wins out.

The GFL scheme offers several advantages compared to QKDS, especially from the aspects of key-establishing rates and link ranges. In addition, the realization of such a system does not require the development of sophisticated technologies such as single photon sources and detectors, quantum repeaters, etc. Analogues to classical cryptography, the GFL-KDS realizes a "one-way *technological* function" in the sense that deciphering the message is technologically difficult for an adversary but simple for legitimate users. The theoretical but not necessarily real-world disadvantage of our system is that, like any classical cryptography scheme, it does not provide unconditional security. In particular, unlike QKDS, it cannot provide an indication for eavesdropping and a bound on the information gained by the adversary. Nevertheless, such a scheme may prove to be a practical solution for secure key distribution and deserves serious consideration as a building block for secure communication solutions, especially for long haul links.

A. Y. thanks the National Science Foundation, AFSOR, and the Defence Advanced Research Projects Agency for supporting the research.

*Electronic address: kobys@eng.tau.ac.il

[1] See, e.g., D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, Boca Raton, FL, 1995).
[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[3] See N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002), and references therein.
[4] A. Ekert, Nature (London) **358**, 14 (1992).
[5] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, Nature (London) **420**, 762 (2002).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[8] M. Aspelmeyer, H. R. Bohm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. M. Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, Science **301**, 621 (2003).
[9] I. Marcikic, H. de Reidmatten, W. Tittel, H. Zbinden, M. Legre, and N. Gisin, Phys. Rev. Lett. **93**, 180502 (2004).
[10] R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47**, 533 (2000).
[11] C. Gobby, Z. L. Yual, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[12] L. B. Kish, Phys. Lett. A **352**, 178 (2006).
[13] A. Cho, Science **309**, 2148 (2005).
[14] J. Scheuer and A. Yariv, physics/0601022 [Phys. Lett. A (to be published)].
[15] See, e.g., A. Yariv, *Optical Electronics in Modern Communications* (Oxford University Press, New York, 1997), 5th ed.