100 MHz Amplitude and Polarization Modulated Optical Source for Free-Space Quantum Communications at 850 nm

M. Jofre[1,⋆], A. Gardelein[1], G. Anzolin[1], G. Molina-Terriza[1,2], J.P. Torres[1,3], M.W. Mitchell[1], and V. Pruneri[1,2]

[1] ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
marc.jofre@icfo.es
[2] ICREA-Institucio Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain
[3] Dept. Teoria del Senyal i Comunicacions, Universitat Politecnica de Catalunya, 08034 Barcelona, Spain

Abstract. We report on an 100 MHz repetition rate integrated photonic transmitter at 850 nm with arbitrary amplitude and polarization modulation. The source is suitable for free-space quantum communication links, in particular for quantum key distribution applications. The whole transmitter, with the optical and electronic components integrated, has reduced size and power consumption. In addition, the optoelectronic components forming the transmitter can be space-qualified, making it suitable for satellite and future space missions.

Keywords: Free-space optical communications, quantum communications, quantum cryptography, faint pulse source.

1 Introduction

In many applications, *free-space optical* (FSO) communications is the technology of choice to transmit information, especially when fiber optical cabling is not easily achievable or its installation is too expensive [1]. FSO communication is favorable for high data-rate, long-range point-to-point links, where the terminal size, mass, and power consumption are subjected to strong limitations, such is the case of aeronautical or space platforms.

An important issue in today's information society is the security of data transmission against potential intruders, which always put at risk the confidentiality. Current methods to increase security require that two parties wishing to transmit information securely need to exchange or share one or more keys. Quantum cryptography, or more precisely *Quantum Key Distribution* (QKD), guarantees absolutely secure key distribution based on the principles of quantum physics, since it is not since it is not possible to measure or reproduce a state (eg. polarization or phase of a photon) without being detected [2].

⋆ Corresponding author.

K. Sithamparanathan et al. (Eds.): PSATS 2010, LNICST 43, pp. 297–304, 2010.

The first QKD scheme, due to Bennett and Brassard [3], employs single photons sent through a quantum channel, plus classical communications over a public channel to generate a secure shared key. This scheme is commonly known as the BB84 protocol. Attenuated laser pulses or *faint pulse sources* (FPS), which in average emit less than one photon per pulse, are often used as signals in practical QKD devices. The introduction of the decoy-state protocol [4] made possible a much tighter bound for the key generation rate, achieving an almost linear dependency of the latter on the channel transmittance. In this way, the technologically much simpler faint pulse systems can offer comparable QKD security with respect to single photon sources. Another key feature of QKD is that the security is linked to the one-time-pad transmission, i.e. the key has to be used once and has to be equal or similar in size to the information being transmitted. It is thus evident the importance of developing faint pulse sources and systems for QKD which can generate high key bit rates. The highest Secure Key Rate reported to date over 20 Km of optical telecom fiber is of 1.02 Mb/s [5] and 14.1 b/s over 200 Km [6], while the achieved speed over 144 Km free space link is of 12.8 Kb/s [7] and 50 Kb/s over 480 m [8].

We note that previous implementations based on multiple lasers [9,8] have attempted to achieve time-frequency indistinguishability by laser pre-selection, current and temperature adjustment, and temporal and spectral measurements. Apart from being expensive and cumbersome, this kind of tuning has limited stability due to the inevitable aging of laser diodes. It is worth noting that the temporal and spectral distributions reported to date indicate indistinguishability in the time and frequency bases, but leave open the question of distinguishability based on other pulse characteristics such as chirp.

In this paper we report the development of a novel integrated pulse source which can reach rates as high as 100 Mb/s at 850nm modulated in amplitude and polarization. For QKD applications, it has been simulated that the source could achieve a Secure Key Rate of the order of 500 Kb/s at 20 Km using decoy-state protocol. The source is capable to generate pulses at around 850 nm with at least three different intensity levels (i.e. number of photons per pulse) and four different polarization states. The proposed FPS ensures indistinguishability among the different intensity and polarization pulses and ensures phase incoherence of consecutive generated states. One of the foreseen applications is its use to overcome the distance limit of QKD in optical fibers [6,10], by creating a global security network among very distant places on earth through satellite communication [11,12,13]. In particular such a source might be used in future *European Space Agency* (ESA) missions [14].

2 Integrated Faint Pulse Source

The integrated source can generate pulses at 850 nm with at least three different intensity levels (i.e. number of photons per pulse) and four different polarization states. In order to use it for space applications, the proposed integrated FPS source for FSO communication consists of commercially available space-qualified

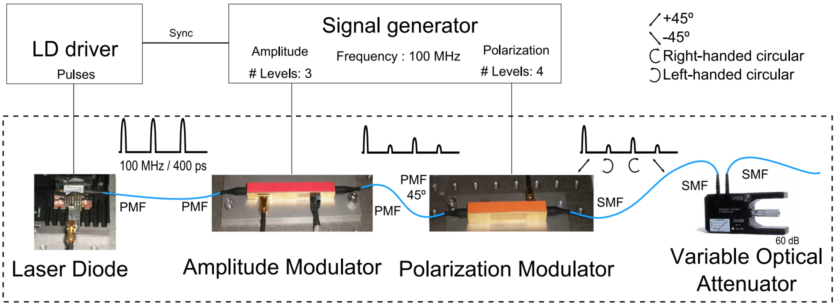


Fig. 1. Schematic of the QKD source. The source is composed of a laser diode, an amplitude modulator, a polarization modulator and a variable optical attenuator together with the driving electronics.

discrete components; single semiconductor laser diode emitting a continuous pulse train at 100 MHz followed by integrated (waveguide) amplitude and polarization lithium niobate ($LiNbO_3$) modulators (Figure 1). The wavelength, reduced power consumption, compactness and space qualifiable optoelectronic components constituting the source make it very suitable for space transmission, for free space quantum and classical communication links.

3 Side-Channel Information

In a BB84 protocol scheme implementing the decoy-state protocol different pulses should differ in polarization and amplitude while remaining indistinguishable in other characteristics, including temporal shape and frequency spectrum. If the pulses differ in spectrum, for example, an eavesdropper could use spectral measurements to infer the sent polarization without actually measuring it. Removal of this kind of *side-channel* information is thus critical to the security of the protocol. Since the information is encoded in the polarization state, the statistical similarity between pulses of different polarizations but same intensity level is more relevant than that of different intensity level but same polarization to prevent information leakage from the quantum link. Here we consider the quantum optics of side-channel information, limiting the discussion to pure states and simple measurements. A full treatment including mixed states and generalized measurements will be the subject of a future publication.

We consider a source that produces pulses with amplitudes $\mathcal{E}_l$, polarizations $\mathbf{p}_l$ and pulse shapes $\Pi_l(t)$. Without loss of generality we assume the polarizations and pulses shapes are normalized $\mathbf{p}_l^* \cdot \mathbf{p}_l = \int dt\, \Pi_l^*(t) \Pi_l(t) = 1$. In a classical description, the field envelopes are

$$\mathbf{E}_l(t) = \mathcal{E}_l \mathbf{p}_l \Pi_l(t) \tag{1}$$

The corresponding quantum state is a generalized coherent state

$$|\alpha_l\rangle \equiv D_l(\eta \mathcal{E}_l \mathbf{p}_l)\, |0\rangle \tag{2}$$

where $|0\rangle$ is the vacuum state and $D_l(\mathbf{x}) \equiv \exp[\mathbf{x} \cdot \mathbf{A}_l^\dagger - \mathbf{x}^* \cdot \mathbf{A}_l]$ is a displacement operator, defined in terms of the mode operator $\mathbf{A}_l \equiv \int dt\, \Pi_l^*(t)\mathbf{a}(t)$, $\mathbf{a} \equiv (a_x, a_y)$ is a vector of annihilation operators, with $[a_p(t), a_q^\dagger(t')] = \delta(t-t')\delta_{p,q}$ for $p, q \in \{x, y\}$. A scaling factor η is included to convert from photon units to field units, chosen such that the positive-frequency part of the quantized electric field is $\hat{\mathbf{E}}(t) = \eta^{-1}\mathbf{a}(t)$. It is easy to check that $\langle\alpha_l|\, \mathbf{a}(t)\, |\alpha_l\rangle = \eta\mathcal{E}_l\mathbf{p}_l\Pi_l(t)$, so that the average quantum field$\langle\alpha_l|\, \hat{\mathbf{E}}(t)\, |\alpha_l\rangle = \mathcal{E}_l\mathbf{p}_l\Pi_l(t)$ in agreement with Equation 1.

Quantum mechanics allows measurements on the pulse-shape Π without measurement of the polarization $\mathbf{p}$. For example, the number operator $N_l \equiv \mathbf{A}_l^\dagger \cdot \mathbf{A}_l = A_{l,x}^\dagger A_{l,x} + A_{l,y}^\dagger A_{l,y}$ counts photons in the mode Π_l independent of $\mathbf{p}_l$. If the modes $\{\Pi_l\}$ are different, an eavesdropper could use state-discrimination techniques [15,16] to determine l (and thus the secret key) *without* disturbing $\mathbf{p}$. This kind of eavesdropping would not be detected by Bob's polarization measurements. For this reason, it is critical to guarantee that this kind of *side channel* information is not present in the sent optical pulses. The similarity between the various Π_l can be quantified by an overlap integral: $[A_{l,p}, A_{m,q}^\dagger] = \int dt \Pi_l^*(t)\Pi_m(t)[a_p, a_q^\dagger] \equiv S_{lm}\delta_{p,q}$, so that for example two states with equal amplitudes $|\mathcal{E}_l| = |\mathcal{E}_m|$, $\langle\alpha_m|\, N_l\, |\alpha_m\rangle / \langle\alpha_l|\, N_l\, |\alpha_l\rangle = |S_{lm}|^2$. Finally, we note that it is possible for pulses to have the same spectra and temporal shape but still be distinguishable, for example if they have different chirp. For this reason, establishing that two (or more) distinct sources produce indistinguishable pulses is not easy.

Our strategy to eliminate side-channel information in the pulse shapes is to dissociate pulse generation from the setting of polarization and amplitude levels. As described in the previous section the FPS consists of a single laser diode emitting a continuous train of optical pulses followed by an AM, a PM and a VOA. Considering that the laser operation is the same for each pulse sent, and that both the AM and PM control voltages are held constant over the duration of the pulse, we can assume that the pulse shape does not depend on the sent amplitude and polarization. The complex expression of the pulsed electromagnetic field exiting the FPS can be written as

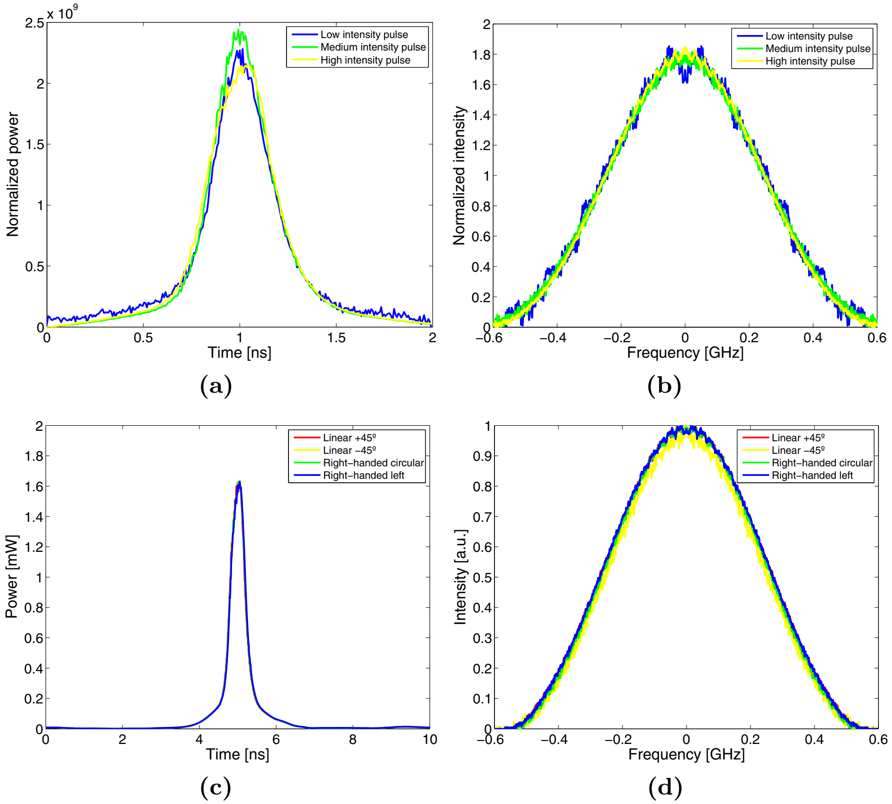
$$\mathbf{E}(t) = \sum_i A\alpha_i e^{j\phi_i} e^{j\beta_i} \frac{\hat{\mathbf{x}} + \mathbf{e}^{\mathbf{j}\gamma_\mathbf{i}}\hat{\mathbf{y}}}{\sqrt{2}} \Pi\,(t - iT) \tag{3}$$

where t is the time, T is the pulse train period and A, ϕ_i, Π are the amplitude, phase, and shape, respectively, of the optical pulse generated by the LD. α_i, β_i describe the transmission and introduced phase, respectively, of the AM. γ_i is the phase difference between $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$ introduced by the polarization modulator in order to generate the different polarization states.

Another security consideration is optical coherence between successive pulses, which could in principle be used for eavesdropping attacks [17]. As the LD is taken below threshold between pulses, each new pulse will start up from vacuum fluctuations, and will have a random overall phase ϕ_i, thus eliminating coherence between succesive pulses and thus among states. Similarly, any information contained in the AM phase β_i is washed out by the random ϕ_i.

4 Experimental Results

The resulting optical pulse duration is about 400 ps. The short optical pulse duration (small duty cycle) has the advantage to increase the signal to noise ratio since the measurement window (detection time) in the receiver can be reduced. Furthermore, the optical pulse bandwidth is small enough to enter the acceptance bandwidth of the subsequent polarization modulator. The modulator "ON" window has a duration of at least 5 ns, much larger than that of the optical pulse. Therefore, only the amplitude of the optical pulse changes, while the temporal and spectral shape remain unaltered. In addition low driving voltages are needed, half-wave voltages of 640mV and 1.56V for the amplitude and polarization modulators, respectively. Making the design suitable for electronic integration with low electrical power consumption drivers. Moreover, intensity



(a)

(b)

(c)

(d)

Fig. 2. (Top) Temporal (a) and spectral (b) profiles for pulses with three intensity levels. (Bottom) Temporal (c) and spectral (d) profiles for pulsed with four polarization states. As expected, these show a high degree of similarity, indicating minimal distortion of the pulses by the amplitude and polarization modulators.

extinction ratio and *polarization extinction ratio* (PER) higher than 25 dB have been achieved with the amplitude modulator and polarization modulator, respectively. Making the source suitable to use it to implement decoy-state QKD transmission while obtaining a low *Quantum Bit Error Rate* (QBER).

Figure 2 top subfigures (a) and (b) show pulses with the same polarization but with different intensity levels with the aim of comparing its temporal and spectral indistinguishability. A 8 GHz amplified photodiode and a 4 MHz resolution Fabry-Perot scanning interferometer where used for the temporal and spectral measurements, respectively. In order to compare pulses with different intensity levels, the different pulses are normalized to their own total intensity. Moreover, Figure 2 bottom subfigures (c) and (d) show a similar comparison, but this time pulses have the same intensity level and different polarization. As expected, there is a high degree of similarity of the pulses, independently of their polarization or intensity state, indicating minimal pulse distortion due to the AM and the PM. It has to be noticed that the small differences for the different intensity pulses are due to measurement errors. Nevertheless, as commented in section 3 polarization statistical similarity is more important than intensity statistical similarity. Furthermore, information on the absolute or relative phase between pulses is not contained in these four figures. However, by design, the phase of each pulse varies at random between pulses due to the fact that, as already mentioned, pulses are generated by taking continuously the laser diode above and below threshold, as explained in section 3.

Given the high optical performance of the proposed source, it is expected to achieve a low QBER as well as a high Secure Key Generation Rate in the order of hundreds of kHz.

5 Conclusions

We have shown that, starting from commercially available and space-qualifiable components, it is possible to build an integrated transmitter capable of generating the several intensity and polarization states required for decoy-state QKD. The experimental demonstration has been carried out at 850 nm with 100 MHz modulation rates. However, taking into consideration that the modulators bandwidth can go well beyond 10 GHz and operate also at other wavelengths (e.g. 1550 nm), the source can be easily scalable to higher bit rates, the upper limit being probably given by the laser diode itself, and other transmission systems (e.g. optical fibers).

Although we believe that the proposed source is of general use in polarization modulation optical systems, especially free-space links, we have focused our demonstration in preparation for a QKD experiment using decoy-state protocol, where the indistinguishability of the pulses, both in the frequency and time domain, is the key for the security of the link. Given the relatively low driving voltages of the modulators, the proposed transmitter is potentially low power consumption and also highly integrable.

Acknowledgments

This work was carried out with the financial support of the Ministerio de Educación y Ciencia (Spain) through grants TEC2007-60185, FIS2007-60179, FIS2008-01051 and Consolider Ingenio CSD2006-00019.

References

1. Carbonneau, T.H., Wisely, D.R.: Opportunities and challenges for optical wireless: the competitive advantage of free space telecommunications links in today's crowded marketplace. In: Wireless Technologies and Systems: Millimeter-Wave and Optical, Proc. SPIE, vol. 3232, pp. 119–128 (1998)
2. Scarani, V., Iblisdir, S., Gisin, N., Acín, A.: Quantum cloning. Rev. Mod. Phys. 77(4), 1225–1256 (2005)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179 (1984)
4. Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. 94(23), 230504 (2005)
5. Dixon, A.R., Yuan, Z.L., Dynes, J.F., Sharpe, A.W., Shields, A.J.: Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. Opt. Express 16(23), 18790–18979 (2008)
6. Chen, T.-Y., Wang, J., Liu, Y., Cai, W.-Q., Wan, X., Chen, L.-K., Wang, J.-H., Liu, S.-B., Liang, H., Yang, L., Peng, C.-Z., Chen, Z.-B., Pan, J.-W.: 200km Decoy-state quantum key distribution with photon polarization. arXiv:0908.4063v1 (2009)
7. Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, A., Zeilinger, J.G., Weinfurter, H.: Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. Phys. Rev. Lett. 98, 010504 (2007)
8. Weier, H., Schmitt-Manderbach, T., Regner, N., Kurtsiefer, C., Weinfurte, H.: Free space quantum key distribution: Towards a real life application. Fortschr. Phys. 54(8-10), 840–845 (2006)
9. Kurtsiefer, C., Zarda, P., Halder, M., Gorman, P.M., Tapster, P.R., Rarity, J.G., Weinfurter, H.: Long Distance Free Space Quantum Cryptography. In: Proc. SPIE, vol. 4917, p. 25 (2002)
10. Takesue, H., Nam, S.W., Zhang, Q., Hadfield, R.H., Honjo, T., Tamaki, K., Yamamoto, Y.: Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. Nature Photonics 1, 343–348 (2007)
11. Hwang, W.-Y.: Quantum key distribution with high loss: Toward global secure communication. Phys. Rev. Lett. 91(5), 057901 (2003)
12. Rarity, J.G., Tapster, P.R., Gorman, P.M., Knight, P.: Ground to satellite secure key exchange using quantum cryptography. New Journal of Physics 4 (2002)
13. Bonato, C., Tomaello, A., Deppo, V.D., Naletto, G., Villoresi, P.: Feasibility of satellite quantum key distribution. New Journal of Physics 11, 045017 (2009)

14. Ursin, R., Jennewein, T., Kofler, J., Perdigues, J.M., Cacciapuoti, L., de Matos, C.J., Aspelmeyer, M., Valencia, A., Scheidl, T., Fedrizzi, A., Acin, A., Barbieri, C., Bianco, G., Brukner, C., Capmany, J., Cova, S., Giggenbach, D., Leeb, W., Hadfield, R.H., Laflamme, R., Lutkenhaus, N., Milburn, G., Peev, M., Ralph, T., Rarity, J., Renner, R., Samain, E., Solomos, N., Tittel, W., Torres, J.P., Toyoshima, M., Ortigosa-Blanch, A., Pruneri, V., Villoresi, P., Walmsley, I., Weihs, G., Weinfurter, H., Zukowski, M., Zeilinger, A.: Space-quest: Experiments with quantum entanglement in space. Europhysics News 40(3), 26–29 (2009)
15. Bergou, J.A., Herzog, U., Hillery, M.: Discrimination of quantum states. Lecture Notes in Physics, vol. 649. Springer, Berlin (2004)
16. Barnett, S.M., Croke, S.: Quantum state discrimination. Adv. Opt. Photon. 1(2), 238–278 (2009)
17. Lo, H.-K., Preskill, J.: Security of quantum key distribution using weak coherent states with nonrandom phases. Quantum Information and Computation 8(5), 431–458 (2007)