MSc in Photonics

PHOTONICSBCN

Universitat Politècnica de Catalunya (UPC)
Universitat Autònoma de Barcelona (UAB)
Universitat de Barcelona (UB)
Institut de Ciències Fotòniques (ICFO)

http://www.photonicsbcn.eu

*Master in Photonics*

**MASTER THESIS WORK**

# INITIAL DESIGN OF A FAINT PULSE PHOTON SOURCE FOR QUANTUM KEY DISTRIBUTION

**Marc Jofre Cruanyes**

**Supervised by Dr. Valerio Pruneri and Dr. Arnaud Gardelein, (ICFO)**

Presented on date 9th July 2009

Registered at

Escola Tècnica Superior
d'Enginyeria de Telecomunicació de Barcelona

# Initial design of a faint pulse photon source for quantum key distribution

**Marc Jofre**

ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

E-mail: marc.jofre@icfo.es

**Abstract.** The project aims at developing new photonic transmitters for quantum cryptography applications which could be used to increase the security of communication networks. The transmitter will be designed to generate security keys at a speed up to 100 Mb/s, two orders of magnitude larger than the state-of-the-art sources. The whole transmitter, with the optical and electronic parts integrated, will have a reduced size and power consumption. In addition, space-qualified optoelectronic devices will be used, so that the final prototype will be ready for satellites and future *European Space Agency* (ESA) missions.

## 1. Introduction

The transmission, storage and processing of information is the basis of the current world and its impact on our lives is evident in almost all our daily activities. This has been possible thanks to the introduction of new technology (wireless and optical networks) with key components coming from micro-electronics and photonics. With the establishment of these means, the transmission of information is open to the possibility of the existence of intruders whose purpose is to gain undesired knowledge of the information being transmitted, thus turning the system into an insecure channel for the transmission of confidential data.

Cryptography is the art of interpreting a coded message that only desired receivers are authorized to access. Different methods of encryption, currently used, require that two parties which wish to transmit information securely need to exchange one or more keys. Once the keys have been exchanged, the information can be transferred to a known level of security. Therefore, the security in transmissions is based exclusively on the security in the key exchange. The surest way to make this key exchange is face-to-face, but this is not possible in most cases because of the multiple number of partners with whom is wished to exchange such information (banks, hospitals, on-line shopping, co working in remote locations, military,...). Quantum cryptography guarantees absolute confidentiality of the transmitted information based on the principles of quantum physics. The key is formed by quantum states of a particle (photon, electron,...), called qubits. For example, qubits can be created using properties such as the polarization or the phase of a photon. Quantum physics can guarantee that any hearing of the encrypted information (keys) can be detected immediately, due to the fundamental quantum principle that you can not measure or reproduce the state (eg. polarization or phase) of a photon without being detected [1].

Bennett and Brassard were the first to introduce a *quantum key distribution* (QKD) scheme, which uses communication over a - completely insecure - quantum channel, in addition to the classical channel. This scheme is commonly known as the BB84 protocol [2]. Although single photon sources may well be very useful for quantum computing, they are not required for QKD. Currently single photon sources are rather impractical for QKD. Instead, 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. Furthermore, the significant performance limitations of attenuated pulse systems has led to belief that single photon sources would be indispensable for building efficient QKD systems. However, the decoy state method, which is described in [3, 4], allows for 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 attenuated pulse systems are again on a level with systems based on single photon sources.

The project aims at developing new photonic transmitters for quantum cryptography applications which could be used to increase the security of communication networks. The transmitter will be designed to generate security keys at a speed up to 100 Mb/s, two orders of magnitude larger than the state-of-the-art sources. The core of the transmitter will be a photon FPS which combines an amplitude and a polarization or a phase modulation of the optic signal. The whole transmitter, with the optical and electronic parts integrated, will have a reduced size and power consumption. In addition, space-qualified optoelectronic devices will be used, so that the final prototype will be ready for satellites and future *European Space Agency* (ESA) missions. The projects also aims at developing a source which enables to combine secure networks in fiber and in free space to contribute to a global secure network based in quantum cryptography, currently limited to a 100 Km [5, 6]. The specific objective of this work is to characterize the initial design of a photon FPS which can generate, in a random operation with a 100 MHz bit rate, three energy levels which at the end will be largely attenuated (for example 1/2, 1/8 and 0 photons per pulse at the output of the source) and four polarization states (eg. lineal 45°and -45°, and circular right and left).

In Section 2, a brief description of the basic theory and state-of-the-art of FPS is reviewed. In Section 3, the general design concept of the proposed FPS is presented. In Section 4, some relevant results are shown and analyzed. In Section 5, conclusions reached in this work are drawn, as well as a description of its novelties and proposals for future work are formulated.

## 2. Theory and state-of-the-art

### *2.1. Faint pulse sources (Attenuated pulse systems)*

Alice encodes the bits to be distributed using pulses in two orthogonal states to encode a 0 and 1, respectively. To prevent the possible intrusion, the number of photons per pulse must be limited to a value much lower than unity (typically 1/2 photons per pulse). The encoding base is changed randomly between two bases (eg. linear 45°and -45°, and circular right and left) so that about half the number of pulses sent are encoded using each one of them. In the receiver (Bob) uses single photon detectors to detect light pulses converting them into electronic pulses for classical processing of the received information. The two states are separated by a splitter and 0 or 1 are received depending on the state detected. Previously, a switch is used to randomize the basis of measurement. Since at the beginning of the link the pulses are strongly attenuated and due to the attenuation loss of the link, only a very small number of pulses sent by the transmitter will be detected at the receiver. The receiver keeps in any case the record of the events generated in the detection and at the end of the transmission, or over the transmission, the two parties distill the information shared by the two entities, over a public channel. All pulses lost in transmission, as well as those detected with the incorrect base are discarded and thus are removed from the registers that keep Alice and Bob, respectively. In this way, both transmitter and receiver share the same key, in principle. The errors that appear when comparing the two is due to the presence of intruders or imperfections of the channel. Below a threshold, the errors can be corrected and any information withheld by the intruder is erased using a privacy amplification process [7].

### *2.2. Polarization encoding*

To encode the qubits in the polarization of a photon is very intuitive. In fact, the first experimental demonstration of quantum key distribution of Bennett and Brassard in 1984 (BB84) was done using this technique. The experiment consisted of a system where Alice (the sender) and Bob (the receiver) exchanged very weak pulses of light generated from a light emitting diode containing in average less than one photon per pulse, transmitted in free space over a distance of 30 cm.

Most of these systems implement a BB84 protocol type that has already been described above. In the case of free space applications it is better to encode information in the polarization of the photon. While, in fiber applications it is more suited to encode information in the phase, since optical fibers introduce an uncontrollable polarization rotation for long distances.

### *2.3. Decoy state protocol*

Quantum mechanics guarantees 100% security in the case of single-photon sources, while in the case of more practical sources such as FPS, the security is not implicitly guaranteed against an external attack, especially if the transmission line has significant losses. Recently, the introduction of the decoy state protocol has helped to keep enjoying unconditional security offered by quantum mechanics, as well as to increase the distance between the transmitter and receiver with respect to other protocols [8] using sources of weak photon pulses.

The basic idea of the decoy state protocol is as follows [3]. Assuming that Alice can prepare coherent states with random polarization or phase, and that it is possible to change the intensity of each signal independently and equally random. In this way, it is possible to introduce decoy states with a different number of average photons per pulse mixed randomly with the signal states. As the only way to distinguish a signal state from a decoy state is in the distribution of the number of photons, the attack can only be based on the photon number splitting attack (PNS) [10–12]. Computing the number of events detected, in a public way, and the error rate in each state, one can detect a possible eavesdropper (intruder). The idea is as if many events are detected for the excess number of photons pulses, while very few events for the non-excess number of photon pulses, the line is likely to suffer an attack. Thus, it becomes clear that the decoy state protocol is only designed to detect attacks and is added as a complement to other protocols (polarization or phase encoding belongs to the two bases of the BB84 protocol).

### *2.4. State-of-the-art*

Until now, basically, quantum key distribution solutions using a decoy state protocol has been based in four laser diodes, each one being independently modulated and polarized within one of the four states (0°, 45°, 90°, 135°). Then, the output of each of the four laser diodes is coupled to a common launching interface, being either a telescope for free space applications, or an optical fiber for telecommunication optical fibers applications. Such solutions imply some problems and limitations. The temporal and spectral shape of each pulse emitted by a laser diode depends on the current and temperature, changing largely from laser to laser. This variation makes it inviable to generate four pulses with the same temporal and spectral shape, lowering the security in the quantum transmission of the key. Adjusting the current and the temperature for each laser diode is one of the ways to level off the emitted pulses by the four lasers. This method does not totally guarantee a sufficient similarity, even with pre-selection of the lasers. Thus, the economical cost of the device is high. Direct modulation of lasers in order to generate the pulses limits the modulation speed down to about 10Mb/s. Due to the fact that is difficult to modulate at higher frequencies while keeping a certain degree of spectral and temporal equality of the pulses. Moreover, lasers undergo a constant process of change of their properties, known as aging, and this can reach to a point where it is not possible to compensate this differences with the control parameters (current and temperature), making it even more difficult to achieve similarity of the temporal and spectral shapes. Each laser has to generate different levels of energy per pulse (1/2, 1/8 and 0 photons per pulse at the output of the source) and this is achieved changing the current. Intrinsically, the variation of energy due to the variation of the current is a non-linear process, thus implies that the temporal and spectral shape of the generated pulses by each laser is not the same. Moreover, when the current in the laser is changed not only the optical emitted energy (intensity of the electromagnetic wave) changes but also the phase of the latter, introducing a non-controllable parameter which is going to change the temporal and spectral shape of the pulses. Newer schemes allow to overcome these limitations mentioned above, but still the key generation rate is in the order of few Mb/s [13].

## 3. Design concept

In this project it is proposed to develop a faint pulse photon source implementing the decoy state protocol. A single laser diode emitting pulses at 100MHz followed by an amplitude and a polarization modulator integrated with fiber input and output. The modulators can operate at modulations higher than 1 Gb/s with very low voltages, around 1.5 V to 3 V and 800 nm to 1550 nm. The use of a single laser diode and modulators ensures the similarity (indistinguishability) of the pulses from a temporal and spectral point of view. In Figure 1 is shown the scheme of the source.

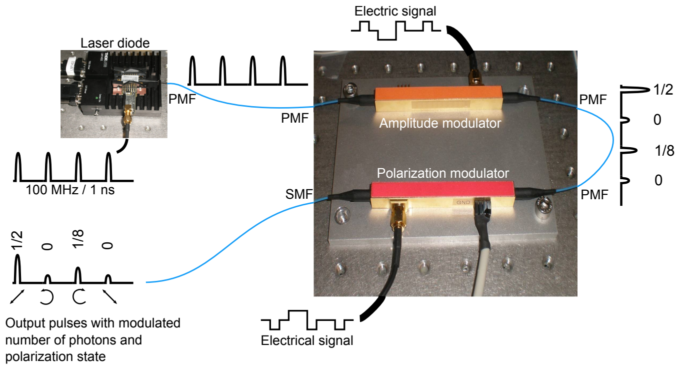


**Figure 1:** Design scheme.

The laser is directly modulated to generate a train of pulses of constant energy. This prevents the mentioned problem of differences between different pulses due to non-linearity of the electro-optical characteristic of the laser. The same train of pulses is guided through a polarization maintaining fiber (PMF) to an amplitude modulator (eg. a Mach-Zehnder modulator in $LiNbO_3$) that will generate the three different levels of energy at random. Next, these pulses will enter a polarization modulator that generates the states of polarization. Actually, the polarization modulator is a phase modulator in $LiNbO_3$ waveguide with an input of 45°with respect to the optical axis. In this way the two components of the electromagnetic field that propagates in the crystal have different refractive index, which depend on the applied electric field (proportional to the

**Table 1:** Relevant temporal and spectral parameters of the generated electrical pulses.

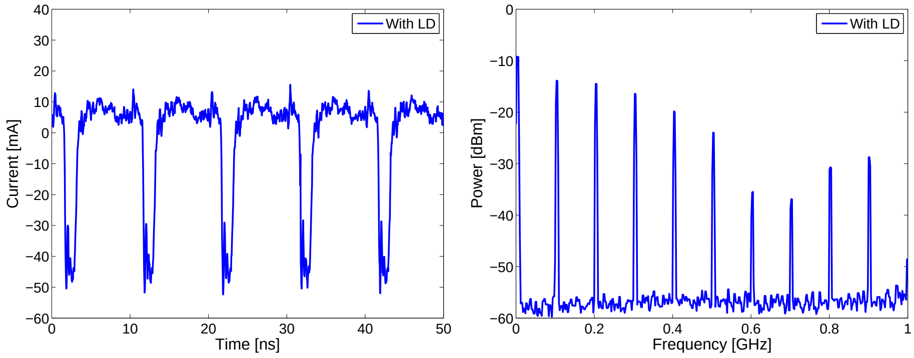
| Output | Pulse width [ns] | Max. RF current [mA] | Fall time [ps] | Rise time [ps] |
|---|---|---|---|---|
| Monitor with LD | 1.49 | $-52$ | 200 | 500 |

voltage applied to the modulator), to get the four states of polarization, linear +45°, -45°, circular right and circular left.

## 4. Results

### *4.1. Electrical pulses*

The electrical time and spectrum measurements of the laser current driver monitor output, with the laser diode loaded to the driver output, are shown in Figure 2. The parasitic inductance due to the leads of the laser diode cause some degradation of the signal, including ringing. Therefore, it is needed custom electronics with particular time and spectral characteristics to match the laser diode which is wanted to drive.



**(a)** 50ns.

**(b)** 1 GHz span.

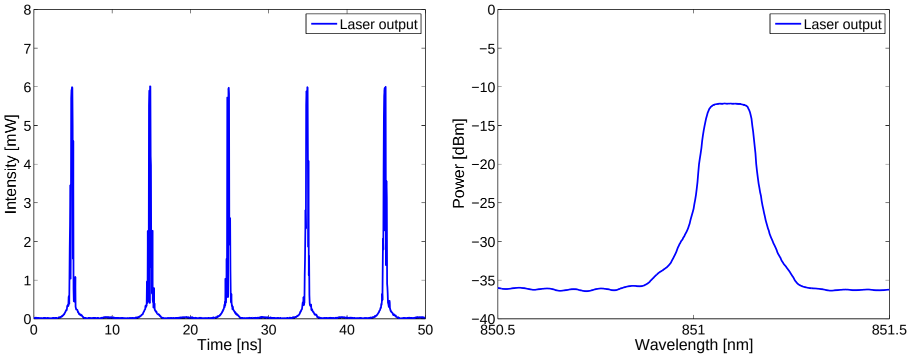
**Figure 2:** Laser diode driver pulses at 100MHz with laser diode.

Table 1 summarizes the relevant temporal and spectral parameters of the electrical driving pulses. The obtained values can be considered as acceptable for the final electronic integration of the FPS.

### *4.2. Optical pulses*

In Figure 3 is shown the generated CW train of optical pulses in time and the optical spectrum. Notice the acceptable temporal and spectral shape of the optical pulses, showing that it is possible to generate optical pulses at 100 MHz.

Table 2 summarizes the relevant temporal and spectral parameters of the optical generated pulses. The small optical pulse width is a good characteristic since the



**(a)** CW train of optical pulses.

**(b)** Spectrum of the CW train of optical pulses.

**Figure 3:** Optical time and spectrum shapes of the laser output.

**Table 2:** Relevant temporal and spectral parameters of the generated optical pulses.

| Pulse width [ps] | Max. intensity [mW] | Rise time [ps] | Fall time [ps] | Spectrum bandwidth [nm] |
|---|---|---|---|---|
| 400 | 6 | 65 | 129 | $< 0.131nm$ |

measurement window in the Bob receiver will be smaller and thus a better signal to noise ratio will be achieved. Furthermore, the optical pulse bandwidth, generated with the laser diode used for this source, is small enough to enter the acceptance bandwidth of the polarization modulator, computed to be around 0.1nm.

### *4.3. Random 3 and 4 levels driving electrical pulses*

In Figure 4 are shown the three and four different levels of electrical pulses at 100MHz, in order to drive the amplitude modulator and the polarization modulator, respectively. It is demonstrated the possibility of generating 3 and 4 different driving pulse levels at 100MHz.

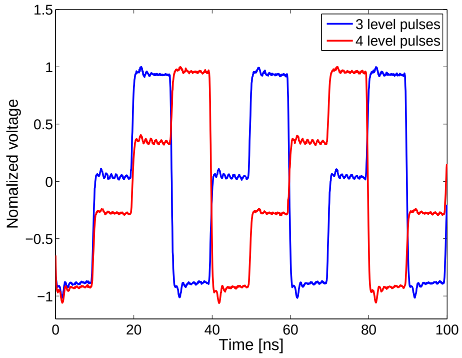


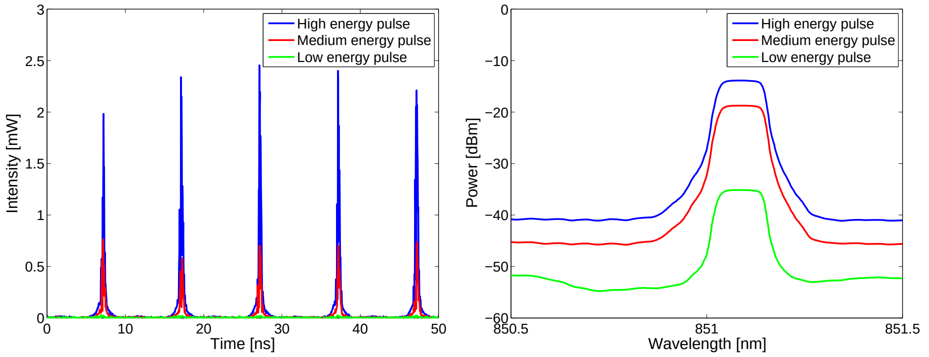
**Figure 4:** Different pulse levels at 100MHz using the modulators drivers.

**Table 3:** Relevant parameters of the AM driver's RF square pulse driving signal to the AM.

| Pulse | DC bias [V] | Square pulse amplitude (p-p) [mV] | Square pulse offset [mV] |
|---|---|---|---|
| High energy level | 0.5 | 0 | 0 |
| Medium energy level | 0.5 | 400 | 200 |
| Low energy level | 0.5 | 600 | 400 |

### *4.4. Amplitude modulator*

The three optical pulses generated with the *amplitude modulator* (AM) are shown in Figure 5. Notice that around 6dB of extinction ratio is achieved for medium energy pulse and 30dB of extinction ratio for the low energy pulse, both relative to the high energy pulse. Thus, being able to implement the different energy pulses needed for the decoy state protocol.



**(a)** CW train of optical pulses. **(b)** Spectrum of the CW train of optical pulses.

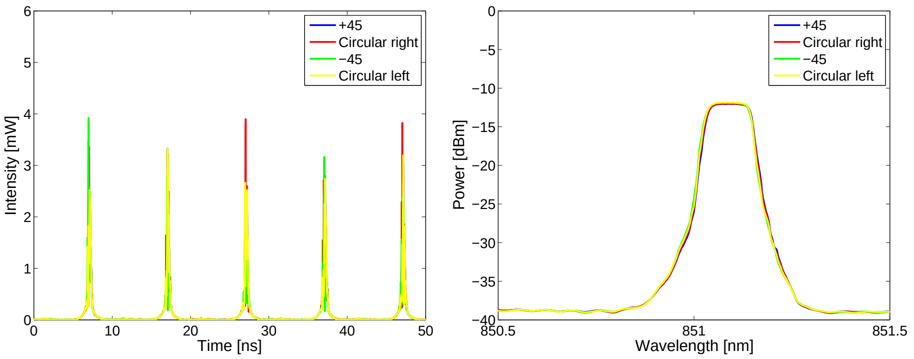
**Figure 5:** Optical time and spectrum shapes of the amplitude modulator outputs.

Table 3 summarizes the driving voltages to the AM generated with the AM driver. Notice the low driving voltages needed, which are suitable for the electronic integration of the source.

### *4.5. Polarization modulator*

The temporal and spectral shape of the four optical pulses with different polarizations are shown in Figure 6, while in Figure 7 are shown the respective four polarization states generated with the *polarization modulator* (PM).

Table 4 summarizes the driving voltages of the polarization modulator generated with the PM driver, as well as the *degree of polarization* (D.O.P.) for each polarization state. Again, notice the low driving voltages needed, which are suitable for the electronic integration of the source. While the values of the D.O.P. need to be improved, for a better *quantum bit error rate* QBER.



**(a)** CW train of optical pulses. **(b)** Spectrum of the CW train of optical pulses.

**Figure 6:** Optical time and spectrum shapes of the polarization modulator outputs.

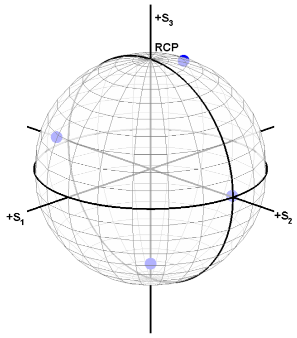


**Figure 7:** Different polarizations on the Poincare sphere, measured with a polarimeter.

**Table 4:** Relevant parameters of the PM driver's RF square pulse driving signal to the PM.

| Polarization | Square pulse amplitude (p-p) [mV] | Square pulse offset [mV] | D.O.P. |
|---|---|---|---|
| +45° | 0 | 0 | 75.125% |
| Circular right | 700 | 350 | 73.423% |
| -45° | 1400 | 700 | 79.084% |
| Circular left | −700 | −350 | 74.948% |

## 5. Conclusions

The proposed FPS implements the decoy state protocol in a BB84 scheme, using a single laser diode emitting pulses at 100MHz followed by an amplitude and a polarization modulator integrated with fiber input and output. The use of a single laser diode and two modulators ensures the similarity (indistinguishability) of the pulses from a temporal and spectral point of view. Secondly, it will be aimed at obtaining a system with low power consumption, reduced size and qualified devices for terrestrial optical fiber and free-space satellite communications. Finally, this versatile FPS design which could enable a global quantum cryptography system, combining free-space and optical fiber transmission, will overcome the current transmission limit in length (about 100 Km in optical fiber).

While performing this study, several aspects that will require further investigation have been identified, including the possibility to directly pulse the laser diode at different currents, with custom driving electronics, to reduce the complexity and power consumption of the source while keeping a reasonable indistinguishability of the different pulses. Also, it is planned to increase the key rate either by means of higher pulse generation rates or by implementing more efficient QKD protocols. At the same time, it will be pursued to reduce the cost and power consumption of the source.

## References

[1] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, “Quantum cloning,” *Rev. Mod. Phys.*, vol. 77, no. 4, pp. 1225–1256, Nov 2005.

[2] C. H. Bennett and G. Brassard, “Quantum cryptography: Public-key distribution and coin tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[3] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, Jun 2005.

[4] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Phys. Rev. A*, vol. 72, no. 1, p. 012326, Jul 2005.

[5] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, Aug 2003.

[6] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Fedrizzi, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lutkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, and A. Zeilinger, “Space-quest: Experiments with quantum entanglement in space,” 2008.

[7] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, “Generalized privacy amplification,” *Information Theory, IEEE Transactions on*, vol. 41, no. 6, pp. 1915–1923, Nov 1995.

[8] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” *Phys. Rev. Lett.*, vol. 92, no. 5, p. 057901, Feb 2004.

[9] X. Ma, C.-H.-F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, “Decoy-state quantum key distribution with two-way classical postprocessing,” *Phys. Rev. A*, vol. 74, p. 032330, 2006.

[10] M. Dusek, o. haderka, and m. Hendrych, “Generalized beam-splitting attack in quantum cryptography with dim coherent states,” *Optics communications*, vol. 169, pp. 103–108, 1999.

[11] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography,” *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, Aug 2000.

[12] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Phys. Rev. A*, vol. 61, no. 5, p. 052304, Apr 2000.

[13] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate,” *Opt. Express*, vol. 16, no. 23, pp. 18 790–18 979, 2008.