Optical fiber sensors as the primary element in the protection of critical infrastructure especially in optoelectronic transmission lines

M. Życzkowski, M. Szustakowski, W. Ciurapiński, P. Markowski, M. Karol & M. Kowalski
Institute of Optoelectronics, Military University of Technology, Poland

Abstract

The security systems of the wide area objects are dominated by fiber optic sensors, used primarily to perimeter protection as well as to the protection of vast objects such as pipelines. Critical infrastructure objects are not only industrial facilities but also the transmission lines. Authors present the sensor systems compared to sensors for extensive object security currently available on the market. The designed systems, such as double interferometer system as well as more and more popular QKD systems are sensors with distributed sensing field. These systems, described by authors in many publications, are excellent solutions for the protection of wide area infrastructural objects. Presented fiber sensors, besides sabotage detection also offer the possibility of locating the disturbance along many kilometers of the zone. The solution presented in this paper was designed to adapt well known solutions to the physical protection of the transmission line without interfering with the transmitted data. According to the knowledge of potential threats of fiber optic telecommunications, the authors present methods of protecting fiber optics telecommunication cable, and present their own solutions and describe their application possibilities.

Keywords: infrastructure protection, fiber optic sensor, interferometer sensor, quantum key distribution.

1 Introduction

Fiber optic transmission systems are becoming more widely used for replacing traditional copper telecommunications links. Optical networks offer many

WIT Transactions on The Built Environment, Vol 134, © 2013 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE130251

advantages compared to the classic copper telecommunications infrastructure, such as higher speed, throughput and network capacity with reduced error rate. Fiber optic networks are inherently resistant to external atmospheric and electromagnetic interference and do not cause such interference in their environment. For this reason, they are widely used by variety of companies and institutions which require secure and high-speed data transmission over long distances. Therefore, network infrastructure is a significant segment of interest by hackers. Although fiber optic networks seems to be secure transmission medium even from a point of view of the network administrators, the truth is that fiber optic transmission lines are also exposed to hackers attacks who are using hardware and software solutions in order to gain access to the transmitted data.

In the case of transmission of classified data, it is required to ensure full security of such networks. This is particularly important in the case of the national security services, upon which disclosure of transmitted information can have serious consequences for the security of the country. Providing a safe channel for the exchange of information makes it necessary to protect such lines and treat them as objects of critical infrastructure. There are applications of fiber optic sensors to protect wide area objects [1–7]. However specification of the attacks, their precision and characteristic of the protected object requires the new approach to the problem of protection of telecommunication lines.

Currently, the most widely used method of protecting transmitted data is the encryption, where safety depends from encryption method particularly on the length of encryption key. The weak point of encryption is the fact that the attack may be unnoticed by administrators, and security of transmission provides only secrecy of the key where the algorithm of encryption is widely known. In the currently used cryptographic systems the biggest problem is secure exchange of encryption key between the sides. The solution to this problem provides more and more popular quantum cryptography system, called quantum key distribution system.

Another way to ensure secure transmission is to monitor the telecommunication line along its entire length. The method of exchanging and encryption of the information is left on actual level, extending the optic cable with sensor fibers. This type of protection of telecommunication lines is presented in fig. 1a) and b), in fig. 1a) telecommunication line with separate sensing fibers from data fibers is presented, in fig. 1b) a solution with integration sensing fibers with data fibers is presented.

Adaptation of the known and continuously developed fiber optic sensors used in perimeter protection is the best example. Possibility of continuous monitoring of the integrity of the transmission line provides safe information transfer through supervision along the entire line with option of locating the possible disturbance in the telecommunication line. This type of protection is especially important in case of dedicated government telecommunication lines, where not only ensuring safety of data transfer is important, but also quick intervention in case of attempt of wiretapping

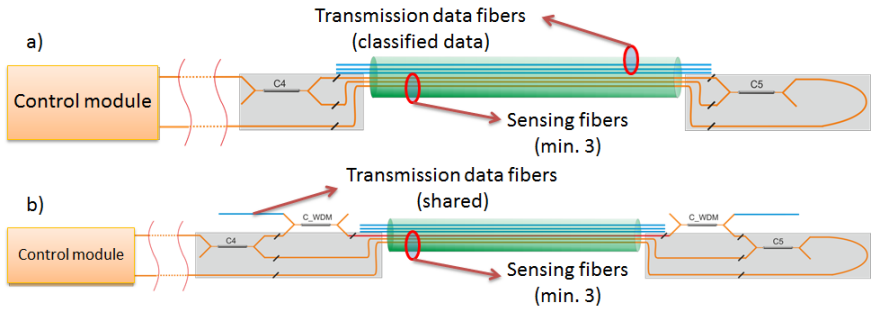

Figure 1: Methods for conducting fiber in protected lines.

2 The methods of wiretapping fiber optic networks

Optical fiber, which is the transmission data medium does not emit electromagnetic radiation outside the structure of the cable, therefore seemingly seems to be a safe way of data transmission. The condition in this case is no violation of the physical structure of an optical fiber. Therefore, to make wiretapping of the fiber optic line, it is required to physically interfere the optical fiber, decoupling and detect the radiation propagating within the fiber.

We can distinguish three methods of wiretapping fiber optic transmission [8]:

1. Direct attacks:
   - Targeted at a transmission in network: wiretapping, wiretapping and jamming occurring after signal processing, just jamming;
   - Targeted at optical amplifiers: strengthen rivalry due to local or remote attacks, crosstalk;
   - Targeted at optical transmission: cutting the fiber.
2. Indirect attacks:
   - Indirect crosstalk;
   - Unauthorized access through add/drop port;
   - Intentional crosstalk propagation from preceding blocks.
3. Pseudo attacks – irregularities which are not attacks, but can be interpreted as attacks due to the significant changes in the signal quality dependent on the physical construction of the network.

Each of these methods has different features depend on the individual network architecture and method of attack [9].

2.1 Wiretapping through plugging to the ports

The easiest way is wiretapping. It is a direct plugging into one of the ports which are built into most of optical amplifiers. These amplifiers are equipped with service connectors for maintenance and this allows easy attack. This attack would be impractical from the perspective of the intruder, if the critical points are physically well-protected.

2.2 Plexus method

The method is based on connecting (or dividing) the fiber and inserting the appropriate equipment (e.g. fiber optic coupler), which allows to reach the signal by the intruder. Performing this "optical valve" is a brief pause in data transmission. This type of attack can be detected by most network security systems. However, if the attack time is short, many operators consider it as a network fault and will continue to transport data, unaware that there was wiretap.

2.3 Splitter coupler method

This type of method is realized by bending fiber and cause leakage of the light to clad without breaking the fiber or interfering data transmission. If the fiber is bent the micro bends are formed on the surface of fiber. Part of the radiation may be lost from fiber structure. To obtain the full signal and transform it to digital form, only a few percent of radiation is needed. This type of attack is typically used as a precursor of another one and provides most of all the information about the telecommunication system.

2.4 Wiretapping of disappearance filed

Optical radiation propagating in the fiber as optical modes is not limited only to core of fiber. Part of light is propagating also in the clad as an exponentially disappearing field. This disappearing field can be used to decouple the part of radiation to the other fiber. It is performed by polishing the wiretapping fiber and by approaching two fibers to guide radiation to the wiretapping fiber. That device works particularly as an optical splitter but in a less controlled way and the fiber doesn't need to be bent as well as wiretapping does not cause a reflection of the signal.

2.5 Rayleigh scattering – wiretapping

This method is also detecting light emitted from fiber. Term Rayleigh scattering describes scattering of light in every direction, also outside of fiber. Attacker may use device which analyze scatter radiation and use simple lenses placed near the fiber to focus scattered light and direct it to other fiber. Attack with this type of device is particularly undetectable, because there is not necessary to bend or merge a fiber.

2.6 Wiretapping through crosstalk

Wiretapping through crosstalk takes advantage of the fact that most of the optical telecommunication systems transmit many signals to different users with the same link. A little part of a transmitted signal may penetrate to other channels (e.g. to another channel in WDM system).

3 Adaptation fiber optic perimeter sensors to protect telecommunication lines

One way to ensure the safety of telecommunication lines is integrity monitoring of the entire length. This type of system should have features same as perimeter protection system especially should react on mechanical disturbance which result with the attempt of physical access to transmission channel. In case of wide (many kilometers long e.g. 40km) telecommunication lines the sensor system should indicate the place of disturbance as well as should be resistant to environment factors such as changes of temperature, pressure and background vibration. Authors repeatedly present works about these types of systems in many configurations. Example of this author's system is presented in Fig. 2

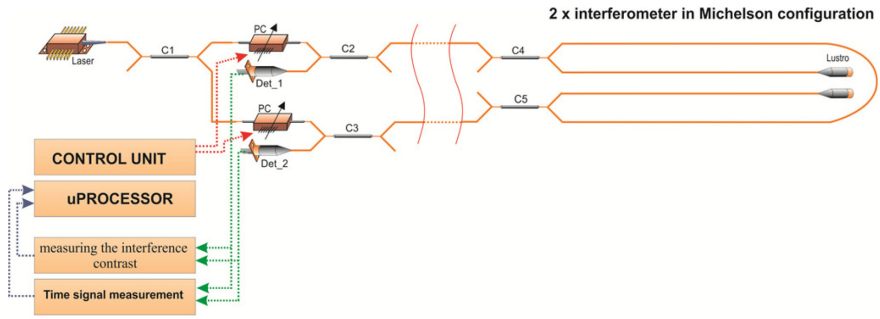

Figure 2: Mechanical disturbance sensor for protection of telecommunication lines.

Fiber sensor for monitoring of integrity of telecommunication line developed in IOE MUT is based on double Michelson fiber interferometer. The sensor system can be divided into two parts:

1. The left side is a set of optoelectronic transmitting and receiving modules with the electronic signal processing systems.
2. On the right side optical fiber sensor part is made of two couplers and two single-mode fiber sections.

The optical fiber module can be divided into two sections: sensitive and insensitive to external disturbances. The insensitive section is contained between the optoelectronic module and C4,C5 couplers. The sensitive section is fibers on the right side of C4,C5 couplers and these fibers are the arm of the interferometer. External disturbances affect both interferometers in the same way, which differ between themselves only in the direction of light propagation. For the first interferometer, the direction of light propagation is: Laser->C1->PC->C2->C4->mirror->C4->C2 (and Laser->C1->PC->C3->C5->C4->C2)->Det1. For the second interferometer, the direction of light propagation is: Laser->C1->PC->C3->C5->mirror->C5->C3 (and Laser->C1->PC->C2->C4->C5->C3)->Det1. Known relationship describing light interference in this type of system

depends on phase difference and intensity of light in both arm of interferometer. Light intensity depends on C4 and C5 coupler division.

The resulting phase difference depends on the length of optical path difference between arms of interferometer (fibers between coupler C4 and C5). The phase difference indicates type of interference (constructive or destructive). All above factors have impact to determination of the working point of interferometer. Furthermore, there is a constant phase difference caused by optical couplers and constant imbalance of optical path difference between the arms of the interferometers. The imbalance cannot be bigger than coherence of the light source. Otherwise, the interference will not occur. Practically, on the many kilometer long path, imbalance of the optical path difference can be in the level of 1 meter. It is connected with used measurement method for such long optical links. This method is OTDR measurement, by which a distance of 40km can determine the length of the fiber with a resolution of 0.25 m

To describe the principle of operation of the system, one should start from the description of the ideal state at constant external conditions affecting the system. We assume that there is not any factor that directly affect the mechanical properties of the fiber and have a direct effect on the polarization of the light in the fiber. According to the assumption of constant external conditions for an ideal system we considered the balance of optical paths for the two arms of the interferometer. However, the working point of the system is determined by following factors:

- Optical path difference;
- The introduction of the couplers constant phase shift;
- Wavelength of the radiation propagating in the system.

For ideal state of the interferometer and assuming that the laser generates constant and stable beam over time, the product of interference of each interferometer depends on the determined working point and is constant over time, providing results-constant output signal on detectors.

For such ideal system, causing the external mechanical disruption, as a result of bending, the fiber optical path length is changed. As a result, the product of interference will change formed through superposition of two waves in a coupler. Due to changes of the interference image through constructive or destructive interference on the detectors, after a certain moment of time needed for light to overcome the distance from the place of disturbance to the detector, we get interference fringes which period will depend on the external influence on the fiber.

Due to the change of the optical power illuminating the detector caused by appearance of interference fringes, electrical signal, stable to this point of time is changed. Such response indicates that some mechanical disturbance occurred. Recent research results indicate that the signals of disorders are characterized by the fact that they are involved in the transfer function of the interferometer, and they cannot be directly identified as microphone signals. To achieve the effect of acoustic monitoring, of the mechanical disorders m output signal should be demodulated. Tests results confirm that interferometers:

- Interferometric sensor is a highly sensitive microphone and can recognize human speech,
- The scope of the bandwidth of such system is particularly unlimited as to the frequency of the mechanical range (from single Hz to 25-30 kHz),
- Transmitted changes associated with acoustic/mechanical disorders of the fiber during touching are contained typically in the frequency range up to 500Hz and the duration of several – several hundred milliseconds.
- Time of light propagation in optical interferometer takes single us. (5us per 1 km of fiber).

Considering the impact of environmental factors on interferometric system as well as the fluctuation of parameters of active devices, we obtain the change in optical path of the interferometer arms and changes in polarization states propagating along the fiber due to changes in environment temperature, changes in fiber stress, vibration, and change of fiber position. Additionally, the working point may be changed due to retuning of the laser source influenced by e.g. temperature, which results in changing the terms of the sensor. As a result of such interactions, low frequency interference fringes are observed on the interferometer output. These factors have a negative impact on the operation of the system and therefore should be minimized by introducing corrections. The authors proposed, based on the solution presented in the literature [10], the introduction of a continuous and constant wavelength modulation of laser radiation to enter the fast-changing permanent changes in the system and measurement of interference contrast. The change of the measured interference contrast indicates a change in the polarization of light in the fiber. By continuous contrast measurement, changes in polarization may be observed, appeared as sudden drop in contrast.

Forcing variable frequency modulation of the system to determine the contrast may not coincide with the external disturbance signals detected by the sensor and must be within the range of the system. Expected external signals of physical interference are mostly acousto-mechanical signals in the range 0–30kHz. Therefore, introduced modulating signal must be separated from this range in order to avoid unstable system operation. It should be also introduced the system adjusting to achieve the operation at the maximum interference contrast. This can be achieved by using an automatic polarization controllers (controlled by a feedback signal from the system) introducing changes to the input polarization to achieve the highest contrast value at the output of the system. This method of determining the input polarity leads to thermal and dynamic stabilization, thus the system does not react on slow frequency environment changes. In case of sudden mechanical disorders, being a result of external physical interfering in optical link, a sudden drop of contrast detected as an alarm can occur.

Through two-way optical supply for that configuration, the places of disorders can be localized along the many kilometer transmission line. Occurrence of external disorder generates changes in the contrast detected by two detectors, but on one of them, contrast will drop sooner than in another one. This is because the light from the place of the disorder come to detectors in

different times (t1 and t2) as a result of the limited speed of light in the fiber (1km in 5us). Comparing these two times, a place of the disorder can be designated. In case of 80km line maximum differences between the detection time take 266us.

4 The quantum key distribution system (QKD)

An alternative to the physical protection of the integrity of the telecommunications lines is the improvement of methods of data encryption. Currently, widely used methods rely on the use of classical cryptography where security is assured with sufficiently long encryption key. Faster development of technology offers faster and faster computation efficiency and this requires the use of longer encryption keys. With sufficiently big computational power, hackers are able to break practically every encryption key, the only limit is the time it takes to break the encipher. The solution can be found in rapidly developed technology of quantum cryptography.

The basic principle of quantum key distribution system are the rules of quantum mechanics. According to them, it is not possible to measure two polarization states because each measurement lead to change in the measured photon polarization. Physical principles of QKD are indisputable, but in order to fully use, it is necessary to use appropriate algorithms enabling certain key exchange such as BB84. Principle of operation (Fig. 3) is based on the generation of two random sequences of bits by the sender, and then send information encoded about them with polarized photon. The value of the bit in the first sequence defines the base polarity (straight or diagonal), the value of the bit in the second sequence specifies one of the two directions of polarization in the database. On the receive side the third bits sequence is generated. Random sequence of the sender determines the polarity of the base with what polarization state will be measured. If the base of the sender and recipient are the same then

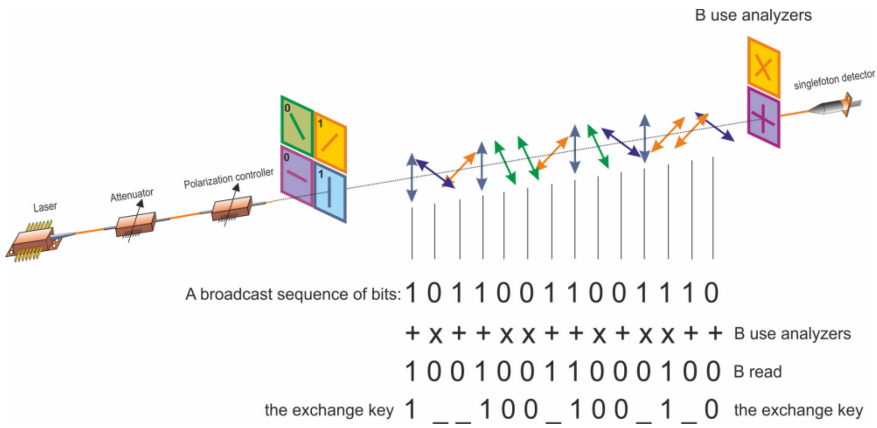

Figure 3: The principle of operation BB84 protocol used in QKD.

the correct measurement of polarization occurs, when the bases are incompatible readout of the correct value occurs with a 50% probability. Then, the information about polarization bases used to read and send the information for which the database readings value of sender and recipient are compatible is sent overtly,. Values read in the case of identical bases are a common encryption key. To validate the transmission and readings, a small part of the key is sent and compared between the parties.

Most QKD systems work according to this rule. Systems operate as two separate entities combined by classical fiber optic telecommunication link. As a result of serious difficulties in the transmission of polarization in the optical fiber, in the real systems phase shift is used. In classical systems (Figure 4a)) the light is transmitted once in one direction and systems reintroducing proper polarization state should be used. Self-compensating systems are also applied (Fig. 4b)), for which the returnable transmission compensates the influence of the optical fiber to the polarization state.

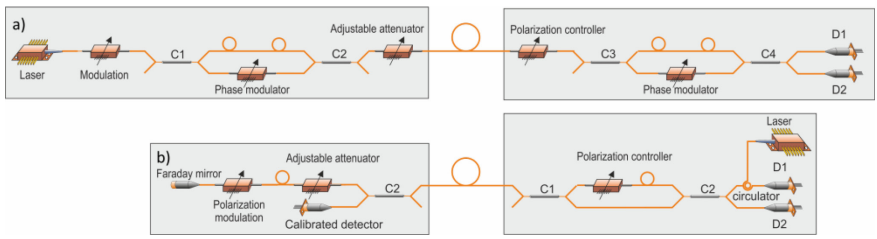

Figure 4: Configurations of currently used QKD systems a) one way impulse system, b) self-compensating system.

In QKD systems wiretapping or its lack is determined by the quantum read error rate QBER. This parameter allows us to determine the normal operating conditions of the system during operation. The disorder of the system, by attempting to wiretap causes an increase of QBER due to the fact that it is a statistics parameter of error in time, the response of the interference comes with a delay. Despite the delays, the threats detection and the possibility of taking the appropriate actions are provided. Breaking the principles of operation of QKD is impossible without violation of fundamental principles of quantum mechanics. However imperfection of the equipment used for the construction of these systems makes them vulnerable to wiretapping. This is involved with limitation of the safety and security of the data transmission, as confirmed by ongoing research [11–15].

5 Conceptions of using QKD as a sensor in a telecommunication fiber

Because of the imperfections of telecommunications systems for the transmitting of classified information or the encryption key, including QKD systems, protecting of the transmission line against possibilities of the outside interference

is required. However, the authors consider that QKD systems are the future of the exchange of classified information with simultaneous detection of potential interference in the transmission path. This resulted in the idea of using quantum key distribution systems as the security sensors and enhance the safety of transmission lines used by the system.

By introducing some simplifications in the QKD, it can be used as a sensor in telecommunication line. The principle of operation of QKD, single-photon transmission based system remains unchanged, but the same system has several simplifications. The first simplification is the possibility to omit an independent generation of the random parameter, because there is no need in this case setting and exchanging the key. This can be replaced by random or pre-determined parameters of transmitted photons, and at the same time setting up the correct analyzer compatible to transmitted parameters. Knowledge of the required analyzer at any given time facilitates proper detection, and reduces the value of QBER. This solution would eliminate the errors associated with non-compliance analyzers used during the reading. However, any attempt of wiretapping of such channel would lead to a significant increase of QBER, increasing detection speed of the interference. This can lead to increase of speed of system response to attempts of interference in lines, and reduce the risk of undisclosed wiretap.

6 Conclusions

We think that by using appropriate security measures, QKD systems will soon become the standard for the transmission of classified information. However, the entire system still needs improvements in the technology level of used components, which are critical points in transmission security. This technology has great potential for development in the near future. According to the authors, in a few years, it is possible to produce alarm components based on a certain data exchange using quantum transmission technology in fiber optic transmission line based on TCP/IP protocol. Authors indicate the possibility of using a Compressed Sensing technology in signal compression to increase the throughput of existing quantum systems.

At the present day, the only safe alternative for advanced systems based on the QKD is monitoring of link integrity. Using such systems as a physical layer of security increases safety in fiber transmission, enabling quick reaction to any attempt of physical interference in optical link which is necessary in wiretapping. One should notice that the level of absolute security is very difficult or even impossible to achieve. Therefore, the best results can be achieved using several technologies simultaneously, QKD in software layer and link integrity monitoring in physical layer.

References

[1] Zyczkowski, M., Intruder localization and identification in fiber optic systems. *Proceedings of SPIE – The International Society for Optical Engineering*, 7119, art. no. 71190L 0, 2008

[2] Zyczkowski, M., Ciurapinski, W. & Szustakowski, M., Preparation and characterization WDM technique for linear disturbance localization in fibre optical sensor. *Proceedings of SPIE – The International Society for Optical Engineering*, 6736, art. no. 67360C 0, 2007
[3] Szustakowski, M., Ciurapinski, W., Zyczkowski, M. & Palka, N., Trends in optoelectronic perimeter security sensors. *Proceedings of SPIE – The International Society for Optical Engineering*, 6736, art. no. 67360Q 1, 2007
[4] Zyczkowski, M. & Ciurapinski, W., Fibre optic sensor with disturbance localization in one optical fibre. *Proceedings of SPIE – The International Society for Optical Engineering*, 6585, art. no. 65851K 0, 2007
[5] Kondrat, M., Szustakowski, M. & Ciurapinski, W., Two-interferometer fiber optic sensor with disturbance localization. *Proceedings of SPIE – The International Society for Optical Engineering*, 6394, art. no. 63940T 1, 2006
[6] Fiber optic sensors for perimeter security with intruder localization Szustakowski, M. & Zyczkowski, M., *Proceedings of SPIE – The International Society for Optical Engineering*, 5954, art. no. 59540C, pp. 1-15 1, 2005
[7] Zyczkowski, M., Ciurapinski, W. & Kondrat, M., Two-interferometers fiber optic sensor for disturbance localization. *Proceedings of SPIE – The International Society for Optical Engineering,* 5952, art. no. 59521E, pp. 1-7 0, 2005
[8] Furdek, M. & Skorin-Kapov, N., Physical-Layer Attacks in All-Optical WDM Networks. *MIPRO 2011 Proceedings of the 34th International Convention*, ,pp. 446-451, 2011
[9] Lydersen, L. & Skaar, J., Security of quantum key distribution with bit and basis dependent detector flaws. *Quantum information & computation*, 10(1-2), pp. 60-76, 2010
[10] Patent number: US 7,952,720 B2; Future Fibre Technologies PTY LTD
[11] Banjac, V. Orlić, M. Perić, M. & Milićević, S., Securing data on fiber optic transmission lines. *20th Telecommunications forum TELFOR 2012*, , pp. 935 – 938, 2012
[12] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. & Makarov, V., Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10), pp. 686-689, 2010
[13] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. & Makarov, V., Avoiding the blinding attack in QKD reply. *Nature Photonics*, 4(12), pp. 800-801 , 2010
[14] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. & Makarov, V., Thermal blinding of gated detectors in quantum cryptography. *Optics Express*, 18(26), pp. 27938-27954, 2010
[15] Marøy, Ø., Lydersen, L. & Skaar, J., Security of quantum key distribution with arbitrary individual imperfections. *Physical Review A*, 82(3), 032337, 2010.