Side-channel Attack to Quantum Communications by Exploiting Electromagnetic Radiations of the Single Photon Detectors

A Thesis
By

Naser C. Jam

Submitted to the
Graduate School of Sciences and Engineering
In Partial Fulfilment of the Requirements for
the Degree of

Master of Science

in the
Department of Electrical and Electronics Engineering

Özyeğin University
August 2020

Copyright @ 2020 by Naser C. Jam

Approved by:

Assist. Professor Kadir Durak, Advisor
Department of Electrical and
Electronics Engineering
Özyeğin University

Assoc. Professor Saeid Karamzadeh
Department of Electrical and
Electronics Engineering
Bahçeşehir University

Assist. Professor Ahmed Akgiray
Department of Electrical and
Electronics Engineering
Özyeğin University

Date Approved: 30 August 2020

To

55 Million Fathers
Whose Children are Sleeping Hungry Tonight

ABSTRACT

In this report an unprecedented cyber-physical attack which can be a game changer in the quantum cryptosystems' security is explained. This attack is the first non-optical patented intercept in quantum field that is based on a security issue in the physical layer of the quantum communication and key distribution systems. We experimentally and theoretically showed that the bit contents of a quantum key transmission system can be intercepted from far away by exploiting the ultrawideband electromagnetic signals radiated from the hi-voltage charge acceleration in the avalanche effect inside photodiodes of the single photon detectors.

This concept was a significant hidden secret based on the physical nature of the single photon detectors that are generally used in quantum key distribution. It has been proved in this research theoretically and experimentally that any Geiger-mode avalanche photodiode that is used inside single photon detectors, systematically acts like a downconverter that converts the optical-wavelength photons to radio-wavelength photons. Our experiments also showed that the radiated waveforms captured by a suitable ultrawideband antenna can be used as a unique fingerprint to find which photodiode in the cryptosystem has absorbed a photon. These fingerprints were fed to a deep learning neural network as training data, and after training, the neural network was able to clone the bit content of quantum transmission with high accuracy without any increase in the error rate of the quantum communication link.

ACKNOWLEDGEMENTS

This work was supported by Scientific and Technological Research Council of Turkey (TUBITAK) with project number 118E156.

I am very grateful for the support of my department chairman, Prof. Murat Uysal.

I am deeply indebted to my advisor Dr. Kadir Durak of Özyeğin University for his help, not only in preparing this Thesis, but in developing the ideas that led to the thesis.

I am very grateful to Dr. Ahmed Akgiray for his excellent advice in this research.

I am very grateful to Dr. Said Karamzadeh from the Bahcesehir University which provided invaluable support for this research.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

The superexponential time scales of the solutions provided by quantum computers will likely soon break traditional public key cryptography, including the ciphers protecting most of the world's digital secrets (Furrer, 2020; Bernstein, 2009; Imre, 2013). There are many accelerating efforts in development of new quantum-resistant algorithms for post-quantum cryptography to define the public and private keys but none of them can claim to provide absolute security against future quantum algorithms. It seems that the only reliable solution on hand at this time that claim absolute security in theory is quantum cryptography.

Base on the well-known Bohm's version of the Einstein-Podolsky-Rosen experiment (Einstein et al. 1935; Bohm, 1951); the generalized Bell's theorem (Bell, 1964; Clauser et al. 1970) is used to test for eavesdropping and the ultimate benefit provided by quantum cryptography is that it is secure against all forthcoming computational and algorithmic progresses. The cryptographic security of quantum protocols never rely on any assumptions about the computing power available to the attackers.

Practically for the strict security requirements, quantum cryptography even enables the continuous generation and sharing of truly random one-time-pad keys (Ma et al. 2016).

Quantum cryptography is often claimed as being perfectly secure from cryptographic point of view. Existing fiber based and free space quantum optical links are thrusted on the confidentiality of the transmitted bits by the physical properties of single photon transmission.

The roots of the security of quantum cryptography is based on the fundamentals of quantum mechanics which says that any measurement in a quantum system disturbs the system. In theory, it is impossible for an eavesdropper to intercept a quantum encryption key without disrupting it in a noticeable way. It is based on the principle that 'a single quantum state cannot be perfectly cloned (Acin et al. 2006; Ekert, 1991; Gisin et al. 2002; Wootters, Zurek, 1982; Inamori et al. 2007; Bennett & Brassard, 1984) and one cannot make measurements of a quantum system without disturbing the system. In standard quantum cryptographic techniques like E91 and BB84 (Ekert, 1991; Bennett et al. 1992; Shor & Preskill 2000; Villar et al. 2020), the sender generates a secret key by encoding classical bit values of 0 and 1 using different quantum states of photons in different bases. The receiver, reads off these bit values using a detector that measures the quantum state of incoming photons. In theory, an eavesdropper will

disturb the properties of these photons before they reach receiver, so that if sender and receiver compare parts of their key, they will notice an increase in the error rate of the quantum link. Since practical protocols starting in the 1980's, Quantum Key Distribution (QKD) has entered into a progressive experimental field, and is rapidly becoming a solid commercial proposition. Many commercial QKD networks have been developed around the globe, and more are in progress. In addition to LEO satellite implementations (Boaron et al. 2018), recent deployments with very low background noise semiconductor single-photon detectors (SPD) with secret key rate of 350 bps which exceeded 300 km range have been reported (Merali, 2010). However, all theoretical approaches are based on this assumption that every physical element in the system is ideal and free of infirmity. The only problem that is still under debate in the quantum cryptosystems is that technologies of the implementation in quantum transceivers often enables deviations from an idealized model to be quantified. In fact, practical implementations often deviate from the theory, which leaves loopholes for eavesdropping, especially in the physical layer.

2. THEORETICAL BACKGROUND AND CONCEPTS

As described in the introduction, all quantum cryptosystems use different quantum states of single photons as a carrier for information, hence Single Photon Detectors (SPD) have prime importance in any quantum receiver.

Two common technologies for single photon detection are the Photo Multiplier Tube (PMT) and the Geiger-mode Avalanche Photo Diode (G-APD) illustrated in Fig. 1. Both devices employ a photosensitive surface that absorbs incoming photons and produces electrical signals that can be sensed and detected. In PMT detectors incoming photons impinge on a photocathode. The photocathode emits electrons that are accelerated inside an electron multiplier structure that is composed of a series of curved metal plates, known as dynodes.

On the other hand a G-APD is completely made by solid-state technology. The internal parts of a G-APD include an absorption region, and a multiplication region. The bias of G-APD produces an electric field in the absorption region that separates the electrons and the photo-generated holes, and sweeps a carrier towards the multiplication region. The multiplication region is designed to have a high electric field so as to provide internal photo-current gain by impact ionization.

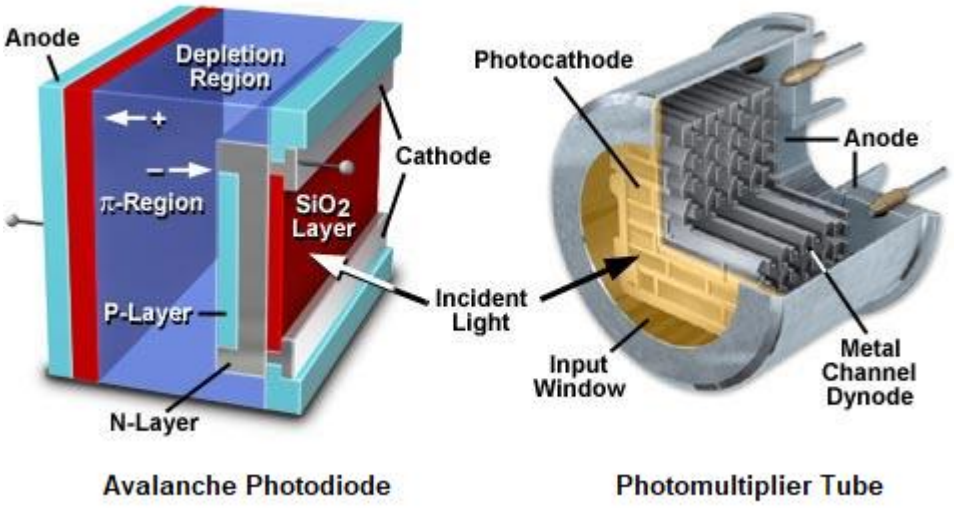

Figure 1-Internal structure of APD and photomultiplier tube (Courtesy Hamamatsu)

Generally almost all quantum cryptosystems todays are using G-APD because its sensitivity and Signal to Noise Ratio (SNR) is near to PMT while many other factors like quantum efficiency (illustrated in Fig. 2), speed, size weight, power, cost and ruggedness are better than PMT.

Table 1- PMT vs. G-APD

Parameter	**Photomultiplier Tube**	**Avalanche Photodiode**
SNR	High SNR	Similar SNR
Speed	Slow	Fast
Reliability	Fragile	Rugged
Size	Bulky	Small
Power consumption	Hi	Low
Magnetic field sensitivity	Sensitive	Insensitive
Dark count	Low	Acceptable
Quantum efficiency typical	% 30-40	%80-90
Ambient light resistance	Catastrophic	Tolerate accidental illumination
Cost	Expensive	Cheap
Operating Voltage (typical)	KV	150 V

Table 1 illustrates the benefits of G-APDs over PMT detectors. These attributes make G-APDs superior to PMTs in quantum cryptosystem applications.

G-APDs are commercially available in the wavelength ranges from 300nm to 1700nm. Silicon G-APDs have usable sensitivity between 300nm to 1100nm, germanium between 800nm and 1600nm, and InGaAs from 900nm to 1700nm.

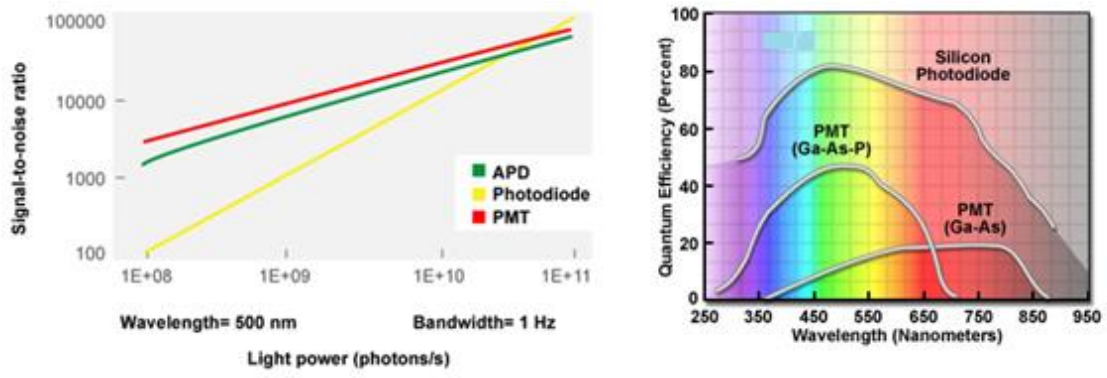

Figure 3-Signal-to-noise ratio and quantum efficiency for a PMT and APD (Herger,2014; Hamamatsu)

2.1. Operating Principle of Geiger mode avalanche photodetectors

Avalanche photodiodes operated in the Geiger mode have enough sensitivity to detect single photons. They differ from a PIN photodiode by providing internal photo-electronic signal gain. G-APDs are operating in reverse bias voltages (Point A in Fig. 3), above the breakdown voltage V_{BR} usually over 100Volts. In Geiger mode the APD is so sensitive that can absorb and detect a single incoming photon. A photon that enters the detector creates an avalanche of electrical current(Point B in Fig. 3), which results in a short digital output pulse, when the current crosses a certain threshold. The avalanche current is then quenched by decreasing the bias voltage to below the breakdown voltage of APD (Point C in Fig. 3),, this makes the APD ready for absorbing another photon.

After this process, the excess bias voltage can be restored. During this time, which is known as the pulse dead time of the G-APD, the detector is blind and insensitive to any other incoming photons. Spontaneously triggered avalanches are possible while the diode is in a metastable state. During an avalanche, some charges can be trapped inside the high field region and an avalanche can be triggered when these charges are released. These random signals are called afterpulses. The life time of the trapped charges is on the order of a few tenths of a microsecond. Hence, it is likely that an afterpulse occurs directly after a photon pulse. To exclude these after-pulses in the measurement, an additional pulse dead time can be set in measurement devices, which will cause the internal counter of the Single Photon Counting Module to ignore all pulses occurring during this pulse dead time.

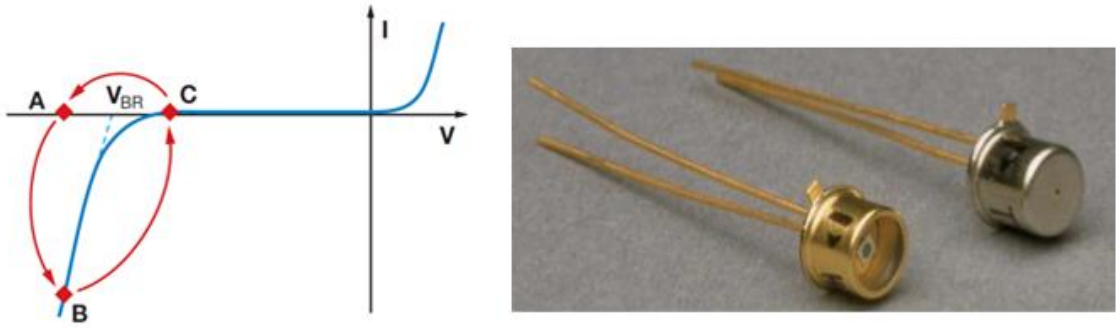

Figure 5-Current Voltage Characteristics of an Avalanche Photodiode Operated in Geiger Mode- (Courtesy Thorlabs)

There is another source of false detection events that are mostly of thermal origin and can therefore be strongly suppressed by using a cooled detector. Practically there is a factor 2 reduction of the dark counts every 8 °C.

2.2. Equivalent circuit of Geiger mode avalanche photodetectors

Pioneering work in the development of solid state single photon detectors was done in the 1960s in the RCA company and the Shockley research laboratory (Renker, 2006). A simplified version of the equivalent circuit of a G-APD was proposed by Haitz (1964). This model has a better fit to our work than more complex models that was proposed later (Zappa et al. 2009). The model is illustrated in Fig. 4. In this circuit the APD is biased by V_{BIAS} into the Geiger region, when a photon is absorbed, the switch S closes and the voltage VBR produces the avalanche pulses.

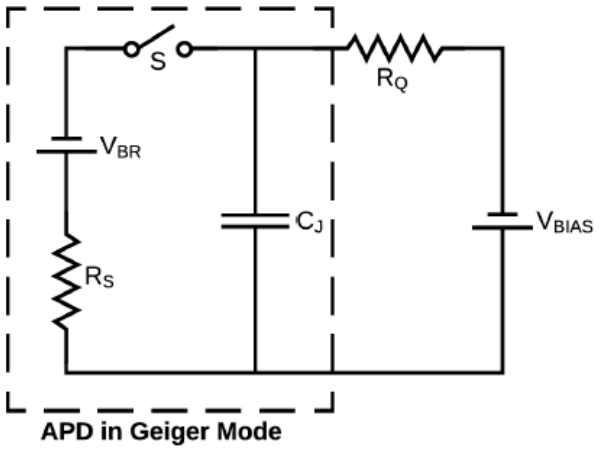

Figure 7-Equivalent circuit of G-APD RQ: quenching resistor, C_J: depletion region capacitance, R_S : combined resistance of the undepleted region (Vilà, et al. 2012)

When the ADP is in the dark, the switch S is open and C_J is charged to V_{BIAS}. The voltage on the APD is $\Delta V = V_{BIAS} - V_{BR}$ above VBR, and the APD is ready to detect a photon. When the APD absorbs a photon and the resulting charge carrier, either an electron or a hole, triggers an avalanche effect. At this state, the switch S closes and C_J discharges through R_S, which tends to lower the voltage across the APD. Since the APD is biased by a high voltage source, a current flows through the APD reaching a steady state value of $\Delta V / R_S$. This current will persist unless V_{BIAS} is reduced to V_{BR}, restoring the APD to the sensitive state. The role of the quenching resistor R_Q is to extinguish the avalanche bringing the APD back to the photo-sensitive mode.

2.3. Electronic circuits for Geiger mode avalanche photodetectors

In order to use an APD in Geiger mode there must be a quenching circuit to cease the avalanche and make the APD ready to absorb next single photon, a threshold detector that acts like a mono-bit A/D converter and a pulse shaper that conditions the output pulse to be suitable for photon counters. In most measurements a passive quenching circuit shown in Fig. 5 can be used.

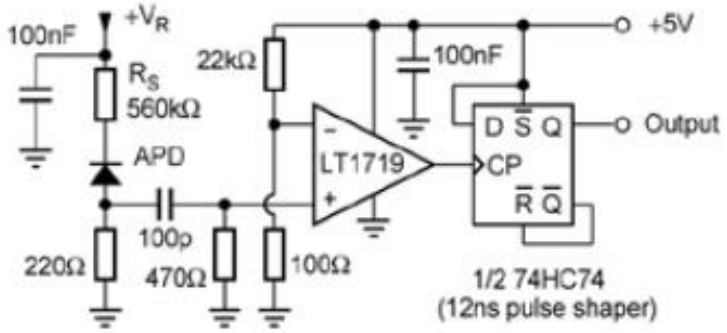

Figure 9-Passive quenching circuit followed by a threshold detector and pulse shaper (Courtesy Laser components)

When the single photon source has a high photon rate, fast recovery of the APD is required. During dead time, it is effectively blind to incoming photons. The dead time fraction, which is an inherent feature of a quenching circuit, may be defined as the ratio of missed to incident events. Fast recovery is usually done by active quenching or a combination of active and passive quenching (illustrated in Fig. 6). Active quenching works by quickly reducing the bias voltage when an avalanche occurs. After detection, the bias is then returned to a value above the breakdown voltage to detect the next photon.

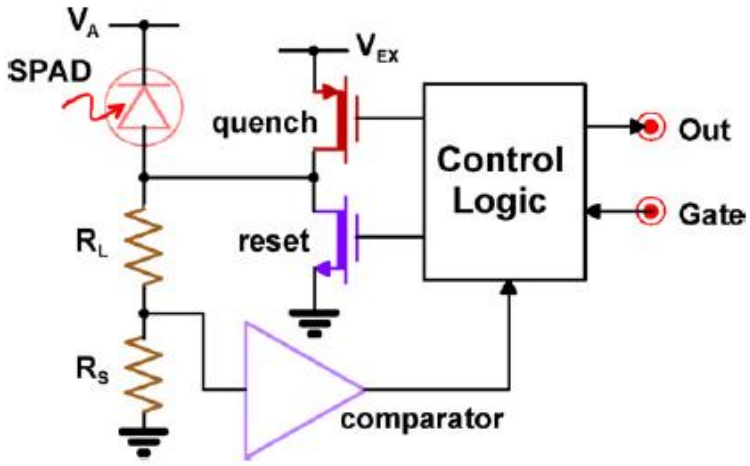

Figure 11-Mixed active-passive quenching circuit (Zappa et al. 2009)

3. EXISTING ATTACKS TO QUANTUM CRYPTOSYSTEMS

Immense experimental and theoretical researches has greatly improved our perception of the realization security of quantum cryptosystems. Methods for blocking the known exploitable loopholes have been proposed, but still when the perfect theories of quantum key transmission are implemented in real world, there are many imperfections.

There are many researches that try to reveal the imperfections of standard protocols regarding the physical limitations like multi-photon emission, weak coherent states, detectors with basis-dependent efficiency, misaligned sources and detectors, and timing jitter of SPDs (Xu, 2020; Lamas & Kurtsiefer, 2007). A summary of typical side-channel attacks against QKD systems is listed in Table 2.

Table 2- List of attacks against QKD systems - (Alléaume, 2018).

Security Issue	Description	Countermeasures
Trojan-horse attack	Intruder probes the QKD equipment with light to gain information about the device settings	privacy amplification (PA), isolators, filters
Multi-photon emission	When more than one photon is emitted in a pulse, information is redundantly encoded on multiple photons	PA, characterization, decoy states, SARG04 and other protocols
Imperfect encoding	Initial states do not conform to the protocol	PA, characterization
Phase correlation between signal pulses	Non-phase-randomized pulses leak more info to Intruder, decoy states fail	phase randomization, PA
Bright-light attack	Intruder manipulates the photon detectors by sending bright-light to them	active monitoring, measurement device independent QKD (MDI-QKD)
Efficiency mismatch and time-shift attack	Intruder can control, at least partially, which detector is to click, gaining information on the encoded bit	MDI-QKD, detector summarization
Back-flash attack	Intruder can learn which detector clicked and hence knows the bit	isolators, MDI-QKD, detector summarization
Manipulation of Local Oscillator reference	In continuous variable QKD (CV-QKD), the local oscillator (LO) can be tampered with by Intruder if it is sent on a communications channel	Generate LO at the receiver. Phase reloading, i.e. only synchronize the phase of LO
laser damage attack	creating deviations that leads to side channels by laser-damage	Continuous monitoring of channels

It is clearly shown in the table that, all attacks against quantum cryptosystems are based on optical attacks, hence our research can be considered as the first attack to quantum cryptosystems that is based on radio frequency attack.

The nearest relevant work to our research is based on the backflash of Single Photon Avalanche Detectors (SPAD) in a research published in Nature Light Journal and conducted by Meda, et al. (2017). A schematic representation of their experimental setup is shown in Fig. 7.

In this experimental setup, the quantum transmitter sends the photons of the key to the receiver in a fiber channel. When the receiver detects the photons using a SPAD, a backflash of light is emitted to the fiber channel. The eavesdropper uses a circulator to intercept this flash of light to intercept the data bits of the detector that has clicked. Needs more text

The backflash light is produced by the carrier avalanches that are triggered by an incoming photon when the SPAD is biased beyond its breakdown voltage. This backflash is quenched, together with the avalanche itself, when the SPAD operating point is lowered below the breakdown voltage.

This mechanism shows that the backflash intensity strongly depends on the settings of the quenching circuit. If we compare this approach with our research that is based on the RF radiation of the SPAD we can see an apparent advantage in our technique because when the SPAD has faster quenching it has a positive effect on RF radiation as the bandwidth increases and higher bandwidth of the pulse provides higher probability of information leakage.

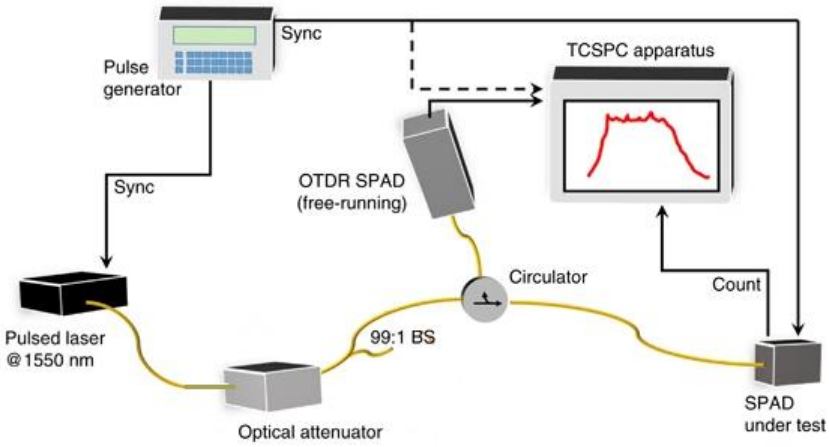

Figure 13-Backflash attack

Bit content of a quantum cryptosystem is intercepted by detecting backflash of Single Photon Avalanche Detectors. A photon-counting reflectometer receives backflash light from the single photon detector. By means of a time-correlated single-photon counter correlation of backflash and single photons are detected. Meda, A., et al. (2017)

4. RESEARCH QUESTIONS

This research is based on the theory and proof-of-concept experiments to show that this new loophole exists in the receiving side of all quantum cryptosystems. The research questions of this work can be summarized in the following items :

1- Should we expect RF radiation in the avalanche process ?
2- Is it possible to intercept RF radiations of single photon detectors from a reasonable distance ?
3- Is it possible to extract a fingerprint from the RF leakage to differentiate between signals to know which single photon detector absorbed a photon ?
4- Is it possible to capture and identify RF fingerprints of single photon detectors in an automated way ?
5- Are there any countermeasure technique to protect our own quantum cryptosystems against RF attack ?

According to the mentioned research questions, the first goal of the research is proof of presence and practical feasibility of intercepting RF leakages from single photon detectors. After positive results of feasibility study we must perform a proof-of-concept to show that we can differentiate between signals of different SPDs, otherwise the intercepted RF signal can only imply presence of single photons without any information about quantum states of photons. After positive results from proof-of-concept we should find a way to automate the identification of quantum states of the photons to clone the bit content of quantum crypto system.

This research can be considered as an ethical hack for quantum crypto systems in which the secondary but the most important goal of the research is to propose the countermeasure techniques that can decrease vulnerability of quantum cryptosystems against this new security breach.

5. METHODOLOGY AND MATERIALS

In order to answer the research questions it was first needed to evaluate the basic idea of G-APD's RF leakage in theory and practice with realistic models and devices. In the following sections both theoretical and experimental works are described.

5.1. RF Leakage of the G-APD

It have been described that the charge which is released during the breakdown in a short time produces emissions which generates a fluorescence flash of light. The main idea of this work was inspired from this assumption that in addition to light emission during avalanche, we can also expect radiation in RF wavelengths too, because we are facing an accelerating charge in the avalanche process (Fig. 8).

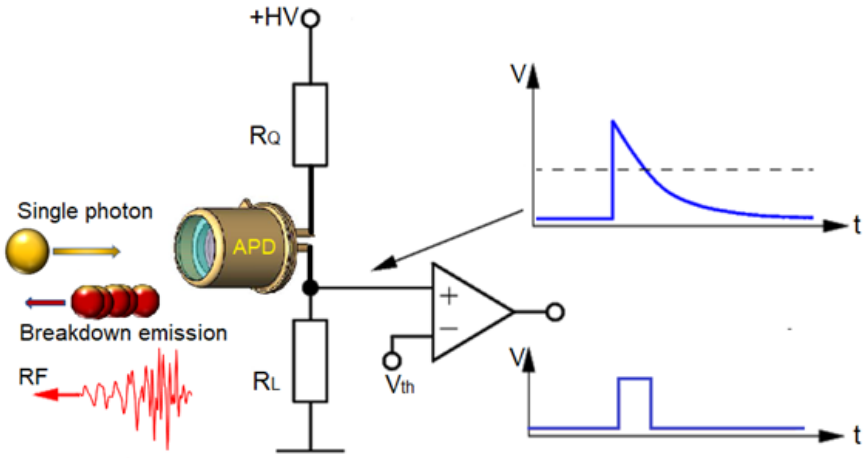

Figure 15-APD emissions

Avalanche photodiode as a single photon detector can act like a downconverter that converts optical-wavelength single photons to radio-wavelength photons. The high-voltage avalanche pulse in a typical circuit of APD produces waves that emits RF radiations when a single photon is detected.

To evaluate this idea, the time dependency of the described current flow through the APD is shown in Fig. 9. The avalanche begins at $t = t_i$. The leading edge of the current pulse increases with the time constant $R_S \times C_J$ and reaches a maximum value of I_D :

$$I_{Dmax} = \frac{V_{BIAS} - V_{BR}}{R_Q + R_S} \approx \frac{\Delta V}{R_Q} \qquad (1)$$

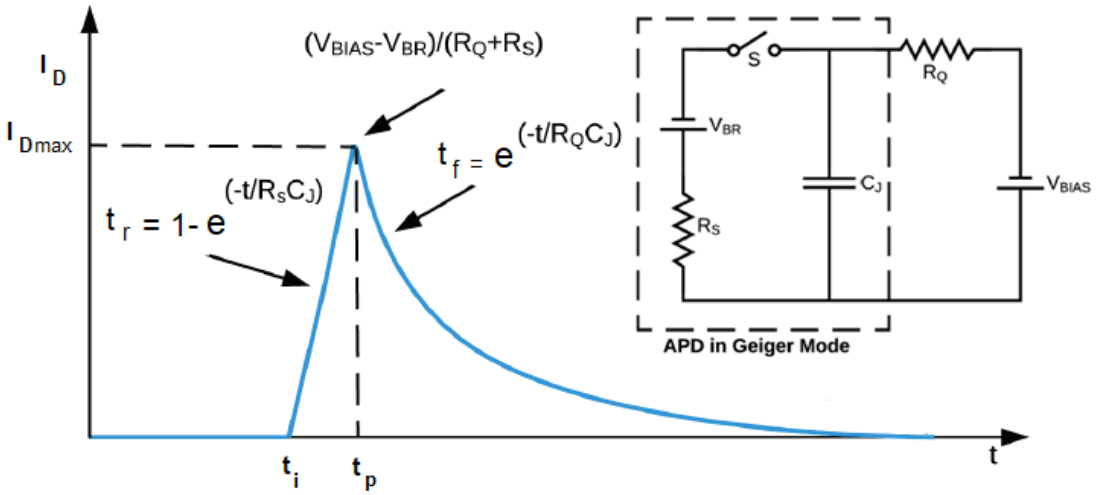

Figure 17-APD current when a photon is absorbed (D'amato, et al. 2016)

Direct measurements of discharge current of $I_D(t)$ can show that it has a typical peak current around 10 mA and pulse width of 10 ns with an exponential decay waveform convoluted with a gaussian distribution.

In the geometrical scales of an APD we can approximate the fastest accelerating charge that is expected to be in the rising part of current as a point charge, by integrating the discharge current over the pulse from rise time (t_i) to peak time (t_p) a total accelerating charge Q_D can be calculated by:

$$Q_D = \int_{t_i}^{t_p} I_D(t)dt \qquad (2)$$

By using the non-realistic electrodynamics of an accelerating point charge we can describe radiation by using *Lienard-Wiechert* potential (Schwinger et al. 1998), hence by integrating the poynting vector over a sphere the energy radiated per unit time will be :

$$P = \frac{2}{3}\frac{Q_D^2}{c^3}\left(\frac{dv}{dt}\right)^2 \quad for\ \frac{v}{c} \ll 1 \qquad (3)$$

In which ***dv/dt*** is the acceleration of charge, ***c*** speed of light and ***P*** is the total electromagnetic power radiated from the APD.

As the APD is a non-relativistic device and speed of electron avalanche ***v*** is not comparable with speed of light, analysis of this equation shows that a radiated RF power ***P*** exists around the APD and this radiation is dependent on the following factors:

1. Discharge of the avalanche pulses : Q_D

2. Rate of change in the charge of the high voltage capacitor that feeds the APD

From the viewpoint of Maxwell's equations we can consider the accelerated charge as an electric dipole shown in Fig. 10. The electric dipole is a simplified model of an antenna composed of a conductor with metal balls at its ends. It is supposed that the accelerating charges $+q(t)$ and $-q(t)$ are placed on the ends, providing a uniform distribution of current $I(t)$ along the conductor (Koshelev, et. al, 2017).

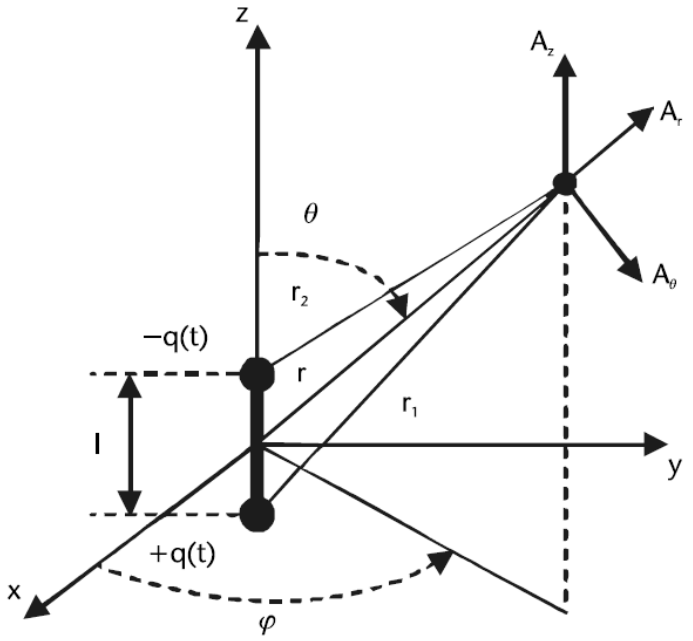

Figure 19-Radiation geometry of accelerating charge

The accelerating charge acts like an electric dipole. The high-voltage pulse produces accelerated charge that emits RF radiations like a small antenna (Koshelev, et. al, 2017)

By solving Maxwell equations for non-sinusoidal waves we can find the radiated power as (Harmuth,1983 & 1985) :

$$P = \frac{l^2}{6\pi c^2}\sqrt{\frac{\mu}{\varepsilon_0}}\left(\frac{dI_D(t)}{dt}\right)^2 \qquad (4)$$

Similar to electrodynamic equation (3) here again we can expect RF radiation around the APD when we have current acceleration. Equation 4 gives us useful information related to the APD circuit. By analyzing this equation we find that the radiated power of the APD is dependent on the length of radiating dipole ***l*** which is physically formed by the terminals of the APD and Printed Circuit Board (PCB) tracks and the rate of change (acceleration) in the current $I_D(t)$ of the avalanche pulses which depends on the detection circuitry. It means that faster detecting circuit that is needed used for high data-rate quantum communications, produces more RF radiation. From a systematic point of view we can say that this process is a kind of down conversion that is occurred in APD in a way that it converts Optical-wavelength single photons to Radio-wavelength photons. From the viewpoint of security this phenomena is expected to be a unique feature for each APD because the physical location of each APD in surrounding structure and environment is unique.

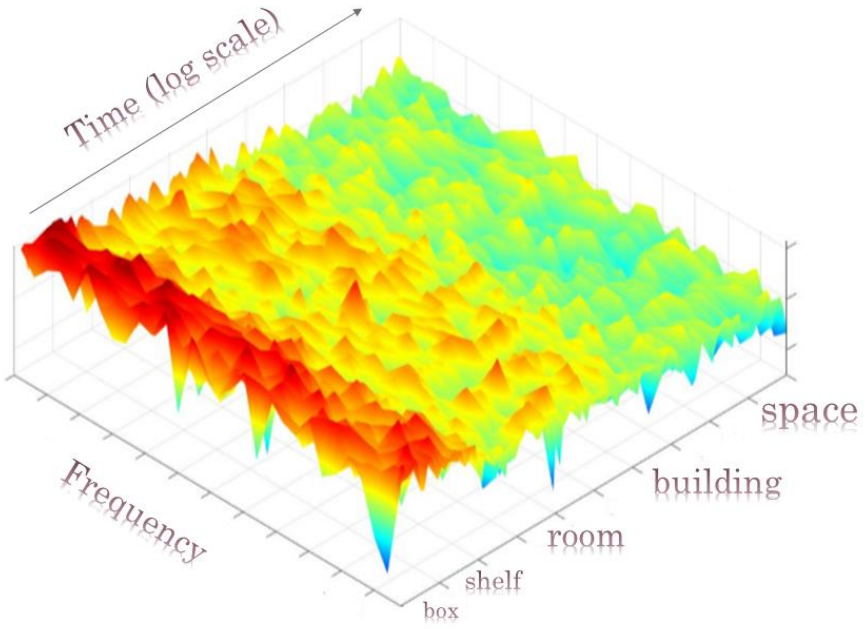

Figure 21-A qualitative outlook: formation of the fingerprint spectrum by propagation and reflections of RF pulse

5.2. RF Fingerprint

The reflection of sinusoidal waves in communication systems is a negative effect as it produces fading in the receiver by destructive combining of waves, but fortunately in our case, this is a positive effect because as shown in Fig. 11 any reflection or resonance will increase the information content of the intercepted RF wave.

In fact the radiation of APD's RF pulse in the box, shelf, rack, room, and the mechanical structure of the environment around the APD acts like a Finite Impulse Response (FIR) filter with unique weights that produces a fingerprint for each APD as illustrated in Fig. 12. This hypothetical FIR filter with unique weights is highly dependent on the location of the APD and during the experimental works we showed that it can be used to discriminate which APD was clicked and extract the data bits of the quantum cryptosystem.

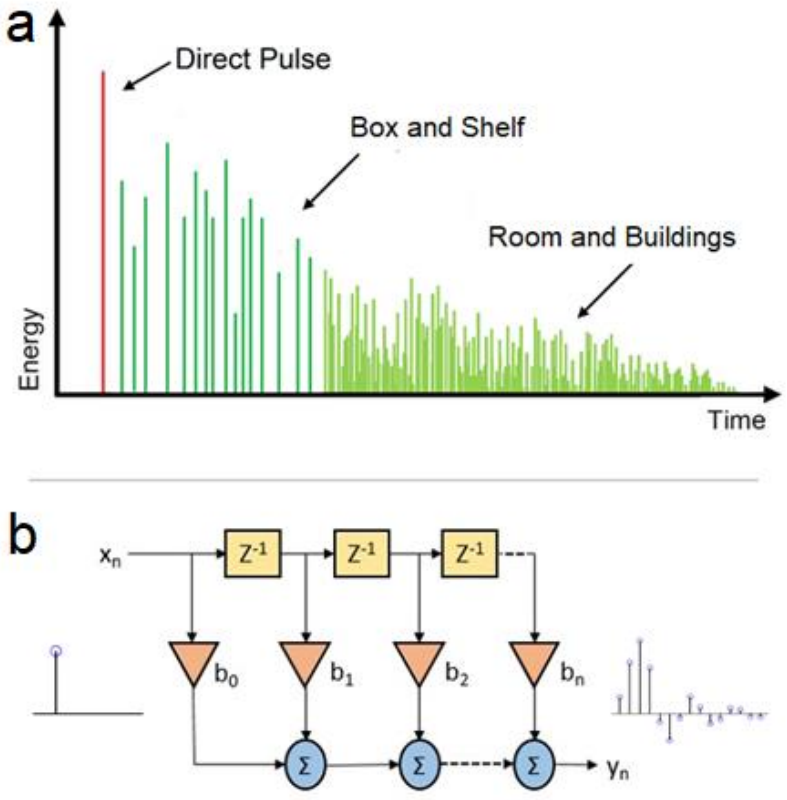

Figure 23-Fingerprint of reflections

(a) Mechanical structure of the system, room and buildings around APD acts like a filter that produces a unique response by multiple reflections for each APD as a fingerprint. (b) Structure of an FIR filter that resembles physics of reflections by delays(Z^{-1}) and reflection coefficients (b_n)

5.3. Typical penetration scenario

Based on this loophole a practical scenario for penetration to a QKD system can be proposed. The proposed penetration can be used as a practical Penetration Test (PENTEST) mechanism for ethical hack and evaluating robustness of quantum cryptography networks that are using single photon based quantum key distribution protocols. This test can be used either in free-space or fiber-optic QKD systems as long as it is at the vicinity of the detectors. Also the same concept can be used against the Entanglement-based systems.

One of the popular protocols for QKD is BB84 protocol shown in Fig. 13a. In this protocol the idea is to encode every bit of the secret key into the polarization states of a single photon. Because the polarization state of a single photon cannot be measured without destroying this photon, this information will be 'fragile' and not available to the eavesdropper. In fact it is assumed that any eavesdropper (called Eve) can tap the transmission media and detect the photons, but by absorption of the single photons she must either reveal herself or will have to re-send the photons. But if she re-sends the photons the photons will have wrong polarization states. This will lead to errors, and again the eavesdropper will reveal herself. The protocol then runs as follows:

Sender (called Alice) sends a sequence of single photons with different polarizations corresponding to secret key bits. For example Alice can encode zeroes into H-polarized(0°) photons and encode ones into V-polarized photons (90°). This sequence is only for half of the bits. The other half of bits, chosen randomly, are encoded using a diagonal polarization basis. Then, the A (45°) polarization represents zeros and the D (135°) polarization, represents ones. The receiver (called Bob), measures the polarization using a standard setup shown in Fig.5a. By this setup Bob can distinguish between V and H polarizations in half of the cases in the HV basis (denoted as '+'). But in half of the cases randomly receives photons in another AD basis (denoted as 'x'). After a certain number of bits has been transmitted, Bob announces which basis he used for each bit in a publicly available communication media. Alice then informs Bob in which cases they used similar bases. They discard the bits where they used wrong bases, and leave only those bits where they used correct bases. This procedure is called key sifting. After sifting, the length of the key is reduced twice, but what remains is random and coincides for Alice and Bob. Then, they can check if there was an eavesdropper between(Clauser et al. 1970). The test for this criteria is based on Experimental Bell's test based on S which is:

$$S \equiv \left|\langle \sigma_\alpha \sigma_\beta \rangle + \langle \sigma_\alpha \sigma_{\beta'} \rangle + \langle \sigma_{\alpha'} \sigma_\beta \rangle - \langle \sigma_{\alpha'} \sigma_{\beta'} \rangle\right| \leq 2 \qquad (5)$$

With correlators:

$$\langle \sigma a \sigma b \rangle = (1/Na,b)(N^{\uparrow\uparrow}{}_{a,b} + N^{\downarrow\downarrow}{}_{a,b} - N^{\uparrow\downarrow}{}_{a,b} - N^{\downarrow\uparrow}{}_{a,b}) \qquad (6)$$

Here $N^{AB}{}_{a,b}$ denote the number of events with the respective outcomes A, B for measurement directions a, b and Na,b is the total number of events of the respective measurement setting. Quantum mechanics predicts a violation of this inequality when measurements are performed on states.

with certain measurement settings, e.g., $\alpha=0°$, $\alpha'=90°$, $\beta=45°$, $\beta'=135°$.

To this end, Alice and Bob take a part of the key and compare it. As this procedure is public, this part of keys are then discarded. If key comparison shows errors it indicates the presence of the eavesdropper. Then the whole key is thrown out and the procedure is repeated again. The proposed penetration setup for this protocol is shown in Fig. 13b and Fig. 13c. The penetration in performed in the following two steps:

5.3.1. Learning

In the learning phase, a laser is equipped with a polarization rotator that is synchronized with a precision pulse generator that sends the test photons with random orthogonal polarizations towards the target receiver(Fig. 13b). To achieve a solid relation between received bits and the quantum system, we must insert this laser (that operates in the same wavelength of QKD system) into the link. This laser imitates the Quantum link's laser. Each single photon detector in the target system receives the test photons and generates Hi-voltage avalanche pulses that radiates Ultrawideband (UWB) Electromagnetic pulses (EMP). The EMP generated by avalanche photo-diodes will leak through electromagnetic shields because of high voltage and short pulse-width that produces high bandwidth.

The penetration system is equipped with an ultra-wideband antenna that receives the radiated electromagnetic Pulses. This antenna receives weak avalanche leakages which permits the signal processing section to extract fine differences between pulse footprints. The EMP signals are amplified with a low-noise amplifier and excessive noise caused by power lines, mobile communications, etc. is filtered by band-pass and band reject filters. The resulting pure signal is fed to a single-event Transient digitizer that is synchronized with the same precision pulse generator that triggers laser pulses.

After preparing the setup, the ultrawideband receive-only antenna with accompanying low-noise amplifier and filter must be located as close to the target photon-detectors as possible.
In this step some test photons are sent to the target. First random polarizations for transmitted single photons are selected and by receiving RF pulses a histogram of polarizations is formed which the peak of histogram shows the right polarization. After that random locations for the antenna is selected and locations are improved incrementally by a successive approximation algorithm. In the signal processor successive integration of the test pulses are performed to achieve highest possible signal-to-noise ratio (SNR).Strong and discriminated waveforms captured by the signal processor are stored in the memory as a reference for machine learning training. In this stage Alice and Bob know that eavesdropping took place because the keys would contain excessive errors. Then the whole key is thrown out and the BB84 procedure is repeated again by Alice and Bob.

5.3.2. Key Intercept

In this stage of the operation(Fig. 13c), the learning laser is removed and the target QKD system operates in its normal condition and the Eavesdropper starts to capture avalanche signals of the detectors. The signal processor and the artificial intelligence engine recognizes the received signals in a free-running form without any trigger signal. By this configuration the Eavesdropper doesn't need to make any interference in Quantum communication path and her only source of information is the classical communication path and the APD's RF backdoor, hence from the viewpoint of information theory in ideal form (which the Artificial Intelligence engine can perfectly identify different APD waveforms without error) Eve has access to the same information of Bob. It is worth mentioning that the techniques used for waveform detection in this setup are the same mature techniques that are used normally in Ultrawideband Radar and electronic warfare systems (I. T. U. 2009; Ye et al. 2011; Friedel et al. 2018; Mikki, 2020; Koshelev et al. 2017) .

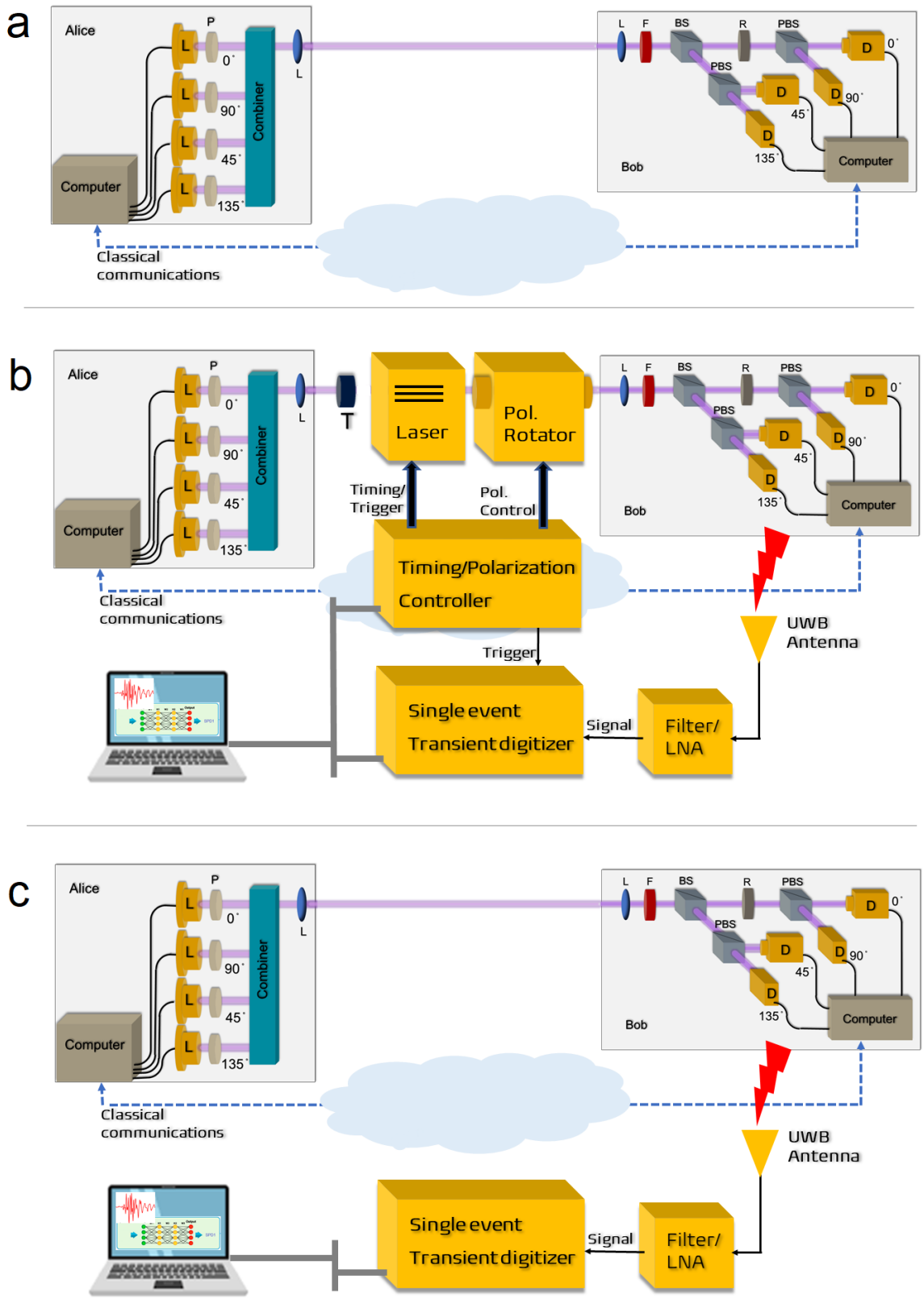

Figure 25-Penetration setup for a Quantum Key Distribution system

(a) typical BB84 QKD system, (b) penetration training phase, (c) eavesdropping and key intercept phase.

5.4. Signal intercept

We showed that the strongest radiated power of the APD is originated from rising edge of the avalanche pulse. By definition this type of signal is categorized as “short electromagnetic pulses containing no radio frequency carrier” and is classified as Ultrawideband signal (Koshelev et al. 2017).

For reception of ultrawideband RF signals, we need an ultrawideband antenna. There are several types of wideband and frequency independent antennas available for reception of such signals, but most of these antennas are designed to receive sinusoidal waves and are not suitable for reception of impulsive radio waves. The main problem with some frequency independent antennas like Log-periodic dipole arrays is dispersion effect. Classical frequency independent antennas rely on variations in geometry to obtain their broadband behavior. A smaller scale portion receives high frequency components and a larger scale portion receives lower frequency components of a signal. Because the phase center moves as a function of frequency, these antennas cause dispersion when receiving signals (Fig. 14) .

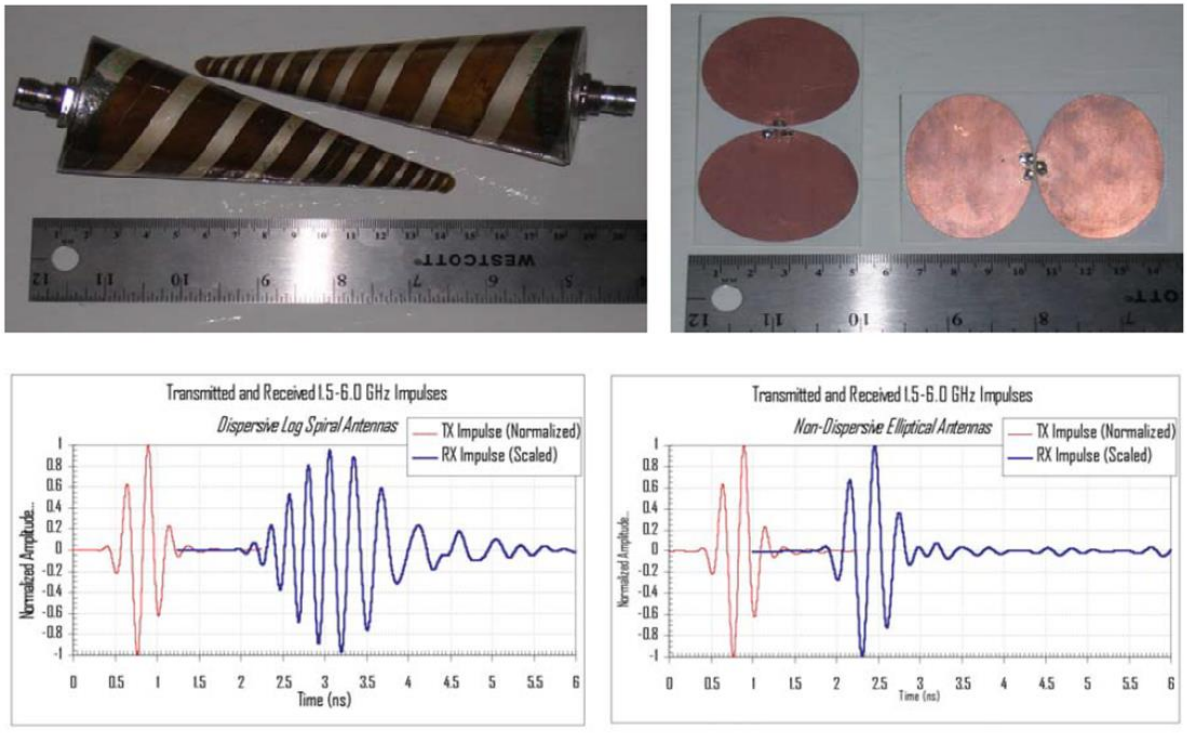

Figure 27- Ultrawideband antenna fidelity in time domain

Left : Log-conical spiral antenna has low fidelity and high dispersion in impulsive RF reception, Right : Planar elliptical dipole antenna has high fidelity with low dispersion (Schantz, 2004)

For high-fidelity reception of an impulsive RF signal a fidelity factor is defined. The cross-correlation between transmitted signal, s(t), and received signal, r(t), is calculated using the fidelity factor as follows (Mehdipour et al. 2007) :

$$F = Max \left| \frac{\int_{-\infty}^{+\infty} s(t)r(t-\tau)dt}{\sqrt{\int_{-\infty}^{+\infty} |s(t)|^2 dt \quad \int_{-\infty}^{+\infty} |r(t)|^2 \, dt}} \right| \tag{7}$$

Another factor in selection of a suitable antenna for reception of RF leakage of APD is size of the antenna. Although a large antenna has higher sensitivity in lower frequencies but in order to be able to conduct the research in the quantum optics lab with no need to a large anechoic chamber we selected an antenna with lowest possible size to measure far-field radiations.

After a survey of different types of ultrawideband antennas, we see an abundance of UWB antennas in the literature with different structures and applications; however, most UWB antennas have been designed for communication applications with sinusoidal carriers. Alternatively, the UWB Vivaldi antennas are beneficial due to directional radiation, wide bandwidth and high fidelity. According to mentioned criteria We selected the Antipodal Vivaldi antenna illustrated in Fig. 15 . This antenna is made on FR4 PCB material and uses some part of PCB as a lens to increase directivity (Karamzadeh 2020). One of the main benefits of this antenna is small size. Small size of the antenna provides short distances for far field that eases operation of the experimental setup in the limited space of the optical table.

As it is apparent in the S11 graph, despite small size this antenna may be useful for reception even in very low frequency ranges.

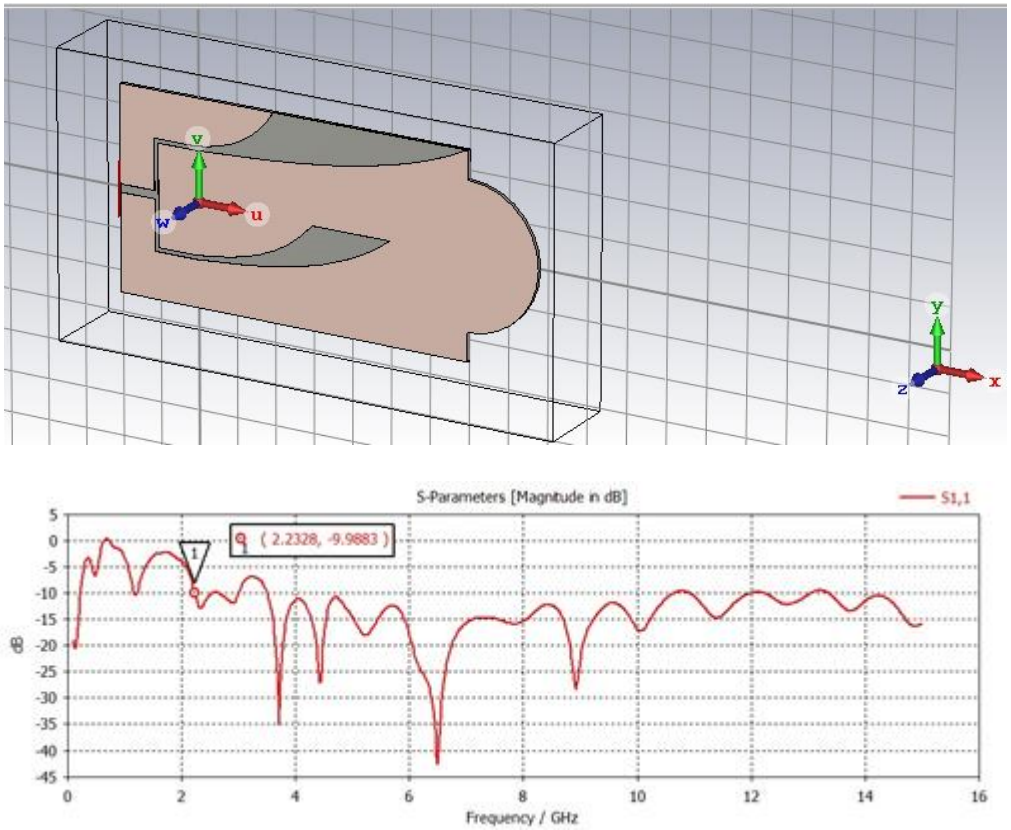

Figure 29-The Antipodal lensed Vivaldi antenna

Top: antenna structure. Down: S11 (Karamzadeh, 2020)

5.5. Signal enhancement

The real signal captured by antenna from single photon click of the APD is shown in Fig. 16a. It can be seen that the RF leakage wave of the APD is exactly synchronous with the Logic-level output pulse of the APD. The purified spectrum of the captured signal is shown in Fig. 16b. during the experiments with different type of antennas and oscilloscopes it was shown that the main energy of the APD waves are located between 30 to 300 MHz frequency range. In the signal processing procedure, the first stage removes the noises and irrelevant portions of the signal by frequency domain excision (filtering) and time domain excision. The frequency domain excision shown in Fig. 17 removes both low-frequency noises induced by sources like powerline and high frequency noises that appear in the background when no signal is present. After removing noises by frequency domain excision, the signal samples were decreased from 1200 samples to 256 samples per waveform by time domain excision, in a way that noises before and after the signals of interest were cut out from the signals. This operation not only increases the signal-to-noise ratio but also removes the effect of irrelevant parts of the signal

that contains no information from further processing. To perform a correlation analysis we made an additional processing to normalize each waveform. This normalization was performed by dividing each sample to the total power of the waveform.

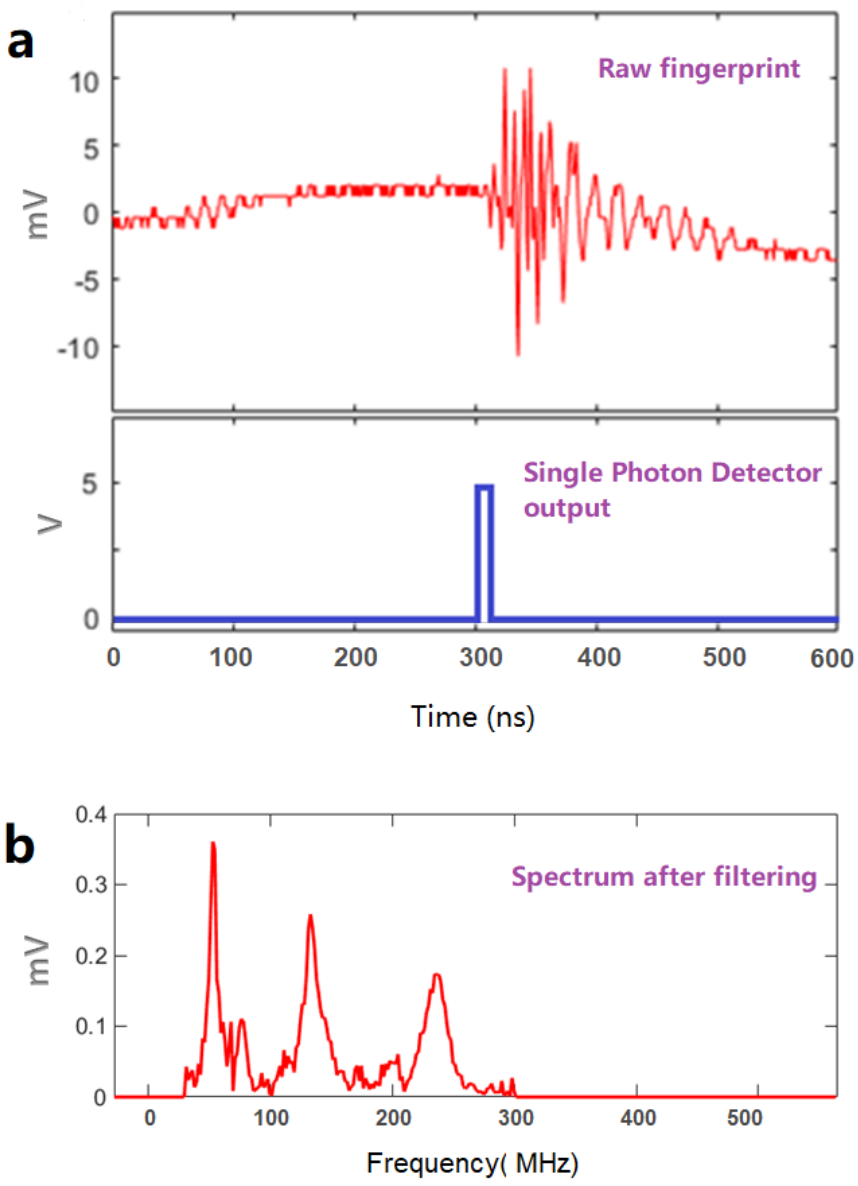

Figure 31-Electromagnetic pulse produced by Hi-voltage avalanche impulse of APD

(a) Raw fingerprint captured by the antenna and TTL output pulse of the APD used as trigger for signal acquisition. (b) Spectrum of fingerprint signal after noise removal by frequency domain excision.

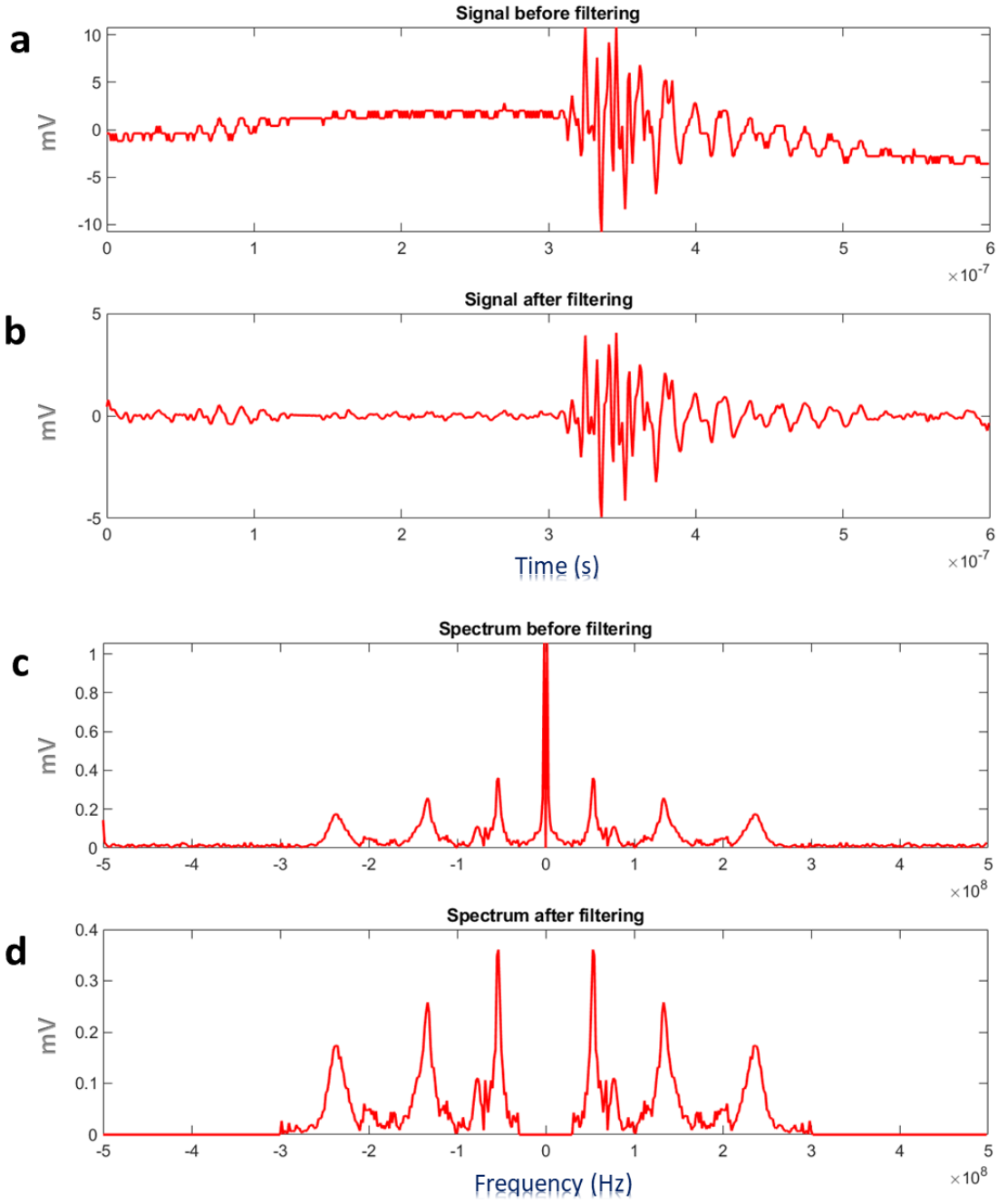

Figure 33-Noise removal by frequency domain excision

(a)Signal before filtering, (b) Signal after filtering, (c)Spectrum before filtering, (d)Spectrum after filtering

5.6. Signal correlation

Before any further processing, to obtain an overview about the amount of decorrelation of the waveforms captured from two separate SPDs, we picked a waveform from first SPD as a reference, Then we calculated the absolute value of cross-correlations of this reference with 64 waveforms of the same SPD and 64 waveforms of the second SPD, the results are shown in Fig. 18. Here we put the correlation results of the SPD1 (named co-location) and SPD2 (named cross-location) beside each other on a common scale to have an overview and physical sense about decorrelation. This decorrelation can be described as a fingerprint for each SPD by this physical property that impulses from each Avalanche photodetector experience different paths and reflections from the physical objects around (mounting boxes, shelf, rack, walls of the room, …) that act like systems having different impulse responses, let's call them $h_1[n]$ *and* $h_2[n]$ in discrete-time form. Then if we recall that the impulse produced by each Avalanche photodiode is similar to a Dirac delta function that we name it $\delta[n]$ then if we take 64 waveforms from SPD1 and 64 waveforms from SPD2 we should have the following waveforms:

$$W_1[n\,,\,i] = h_1[n] * \delta_1[n\,,\,i] + N[n\,,\,i] + Q[n\,,\,i] \quad ;\ i=1 \text{ to } 64 \qquad (8)$$

$$W_2[m\,,\,i] = h_2[m] * \delta_2[m\,,\,i] + N[m\,,\,i] + Q[m\,,\,i] \quad ;\ i=1 \text{ to } 64 \qquad (9)$$

In which, $W_1[n\,,\,i]$ is the i-th waveform received by the antenna from SPD1, $h_1[n]$ is the impulse response of the path from SPD1 to the antenna, $\delta_1[n\,,i]$ the i-th impulse of the Avalanche photodiode of SPD1 after detecting a single photon and $N[n\,,i]$ is the additive white Gaussian thermal noise of the receiving system and $Q[n,i]$ is the quantization noise of the transient digitizer which is modelled as an additive random signal.

Here $m=n+\Delta t$ in which Δt is caused by time difference of arrival of waveforms to antenna due to different distances of each SPD to antenna.

There are three sources that construct each waveform: the SPD, the radiation path, and the receiving system. The main player that has the first role in making decorrelation between SPD waveforms is the radiation path between two SPDs.

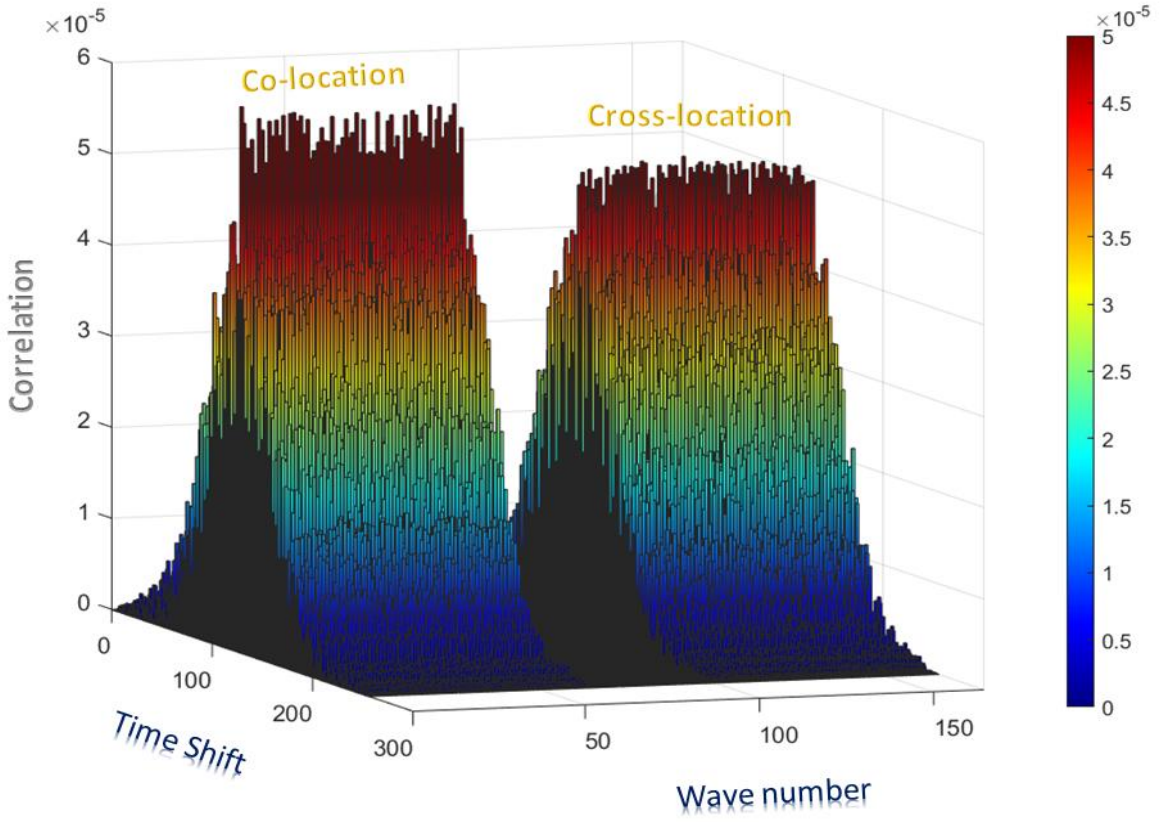

Figure 35-Correlations

Cross correlations of 64 waveforms captured from the SPDs in one place (Co-location) and two different places (Cross-location) 20 cm apart.

5.7. Feasibility study

The feasibility study of this project was first performed using a home-made, passively quenched single photon detector based on Geiger APDs (Fig.19). We used two types of commercial ADP unites with hermetically sealed metal packages, the first one was type SAP500 from 'Laser components' and the second one C30902SH-TC from "Excelitas Technologies".

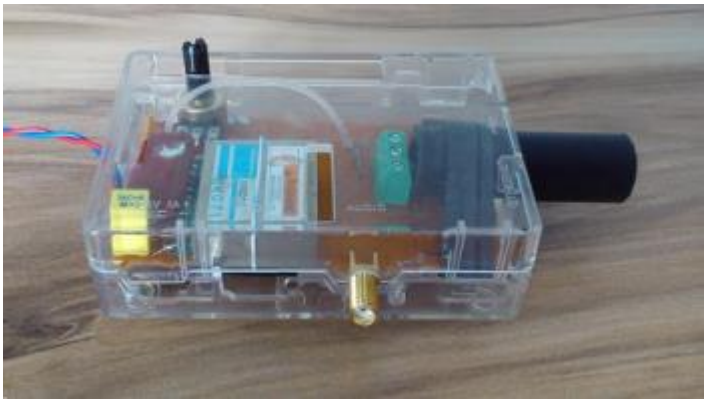

Figure 37-Home-made, passively quenched single photon detector

We captured fingerprint waveforms from both APDs with above 10 mV peak-to-peak amplitude level from 2 meter distance with zero dB antenna gain. After positive results of the feasibility study, in the next level of experiments we used two commercial single photon detector modules which was ID100 detector from "ID Quantique SA" company of Sweden and another SPD from "S-Fifteen Instruments" company of Singapore (Fig. 20). The 'ID Quantique SA' company is active in the quantum security business with mature professional QKD products. To make the proof-of-concept setup as similar to a real scenario as possible, we put the ID100 SPDs inside a 19 inch metal shelf. This made our setup analogous to CLAVIS3 QKD Platform from 'ID Quantique SA' which is 424 x 402 x 144 mm (LWH) in size.

Figure 39-Commercial Single photon detectors used in experimental setup

Right: Fiber coupled Single photon detector module from "S-Fifteen Instruments" company of Singapore
Left: ID100 detector from "ID Quantique SA" company of Sweden

Signal reception was performed using the home-made antipodal Vivaldi antenna and a wideband digital oscilloscope with 1GS/s sample rate. The distance between two SPDs were 20 cm and distance between SPD setup and receiving antenna was 2 meters. In order to eliminate any uncertainty that may occurred by moving objects, the transient recorder was remotely controlled via LAN connection. All signal processing and transforms were performed using MATLAB's signal processing toolbox. Bandpass filtering was performed by FFT excision with cut-off frequency of 30 MHz to 300 MHz . The neural network training and tests was performed using MATLAB's deep learning toolbox. We implemented a deep learning neural network with 256 inputs, each containing a time-sample of a waveform, then we made 5 layers of fully interconnected hidden neurons and two output neurons to present the bit information of the quantum transmission.

Fig. 21 shows a simplified configuration for training and operation of deep learning neural network for waveform recognition.

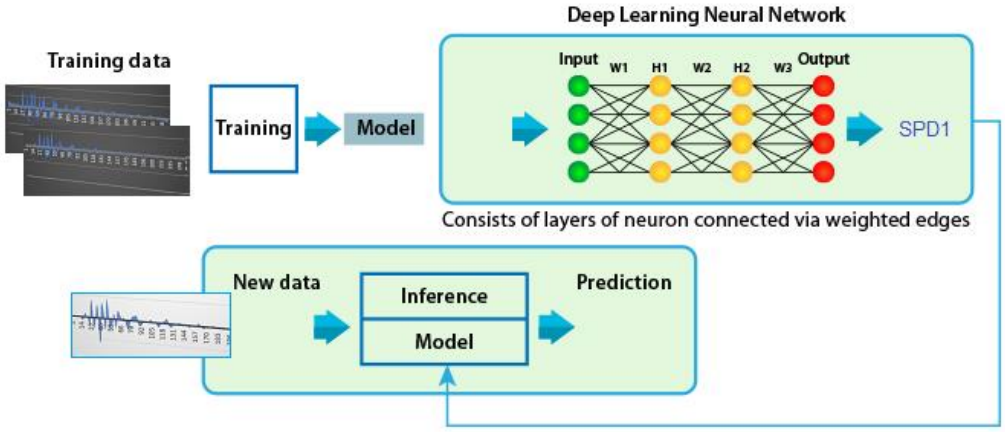

Figure 41-Deep learning process

An overview of Deep learning Neural Network for classifying fingerprint waveforms. By supplying training data, and performing learning phase, the network can differentiate between RF clicks of different polarizations in quantum cryptosystems.

6. RESULTS

To evaluate the possibility of automatic differentiation between fingerprint of radio waves that are received from different SPD locations we prepared a setup according to ITU standards (I.T.U. 2009).

6.1. Experimental results

The setup was including a digital oscilloscope as transient digitizer, an ultrawideband antenna and two commercial single photon detectors with the same model. The configuration of the experimental setup is shown in Fig. 22. The single photons received by the system are passed through a Polarizing Beam Splitter (PBS) that forwards vertically polarized photons to Detector1 and horizontally polarized photons to Detector2. Each SPD detects either vertical or horizontal polarizations and the output of detector that is a logic pulse is directly fed to the oscilloscope and the leakage waves are fed to another channel of oscilloscope through the antenna. After setting up the components, 64 waveforms were captured from each SPD with 1GS/s sampling rate and 1200 samples per waveform.

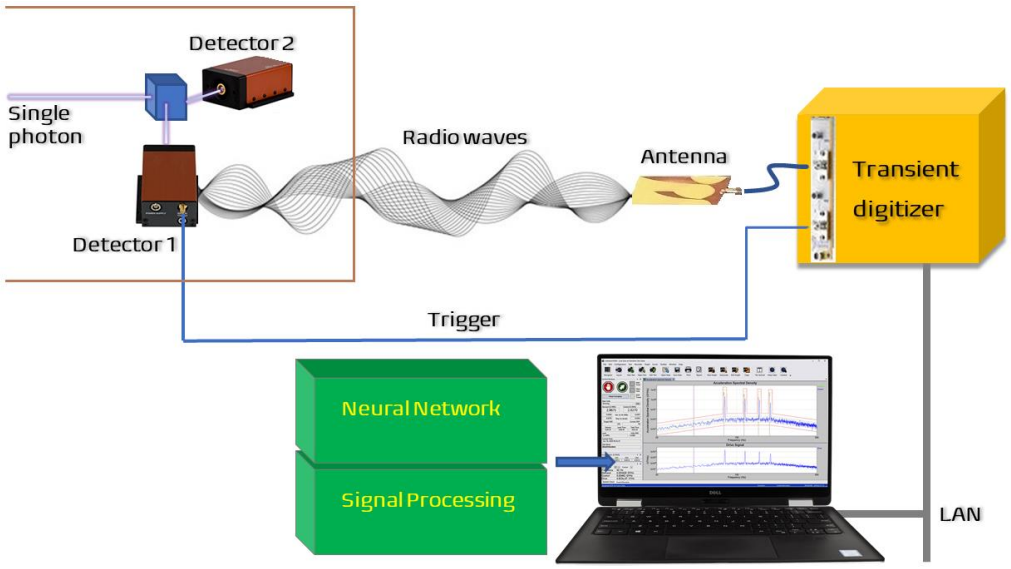

Figure 43-Experimental setup

The RF radiations caused by avalanche breakdown emissions of single photon detectors are captured by ultrawideband antenna and recognized by the Neural Network after pre-processing.

Fig. 23 shows the captured raw waveforms of two different SPDs in the experimental setup corresponding to a synchronous digital pulse created by each SPD. The Logic output pulse of the APDs is used as a synchronization pulse for precise data acquisition from the antenna.

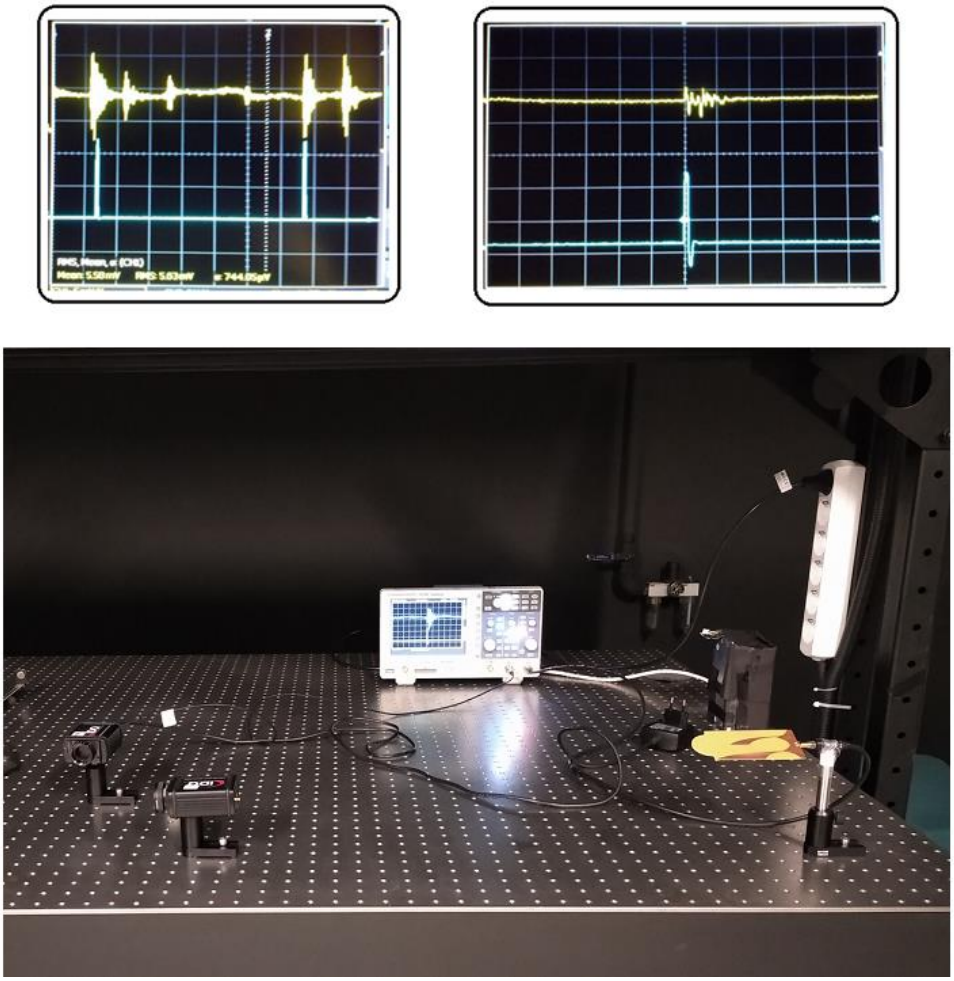

Figure 45-Real images of RF fingerprints captured by the antenna

Top-left: Raw leakage waveform of the S-Fifteen SPD. Top-right : Raw leakage waveform of the ID100 SPD
Blue pulses are the output pulse of the SPDs that presents detection of a single photon.
Down: Test setup on optical table

After obtaining an overview about the amount of decorrelation of waveforms, to make sure that there is enough decorrelation between fingerprints of two SPDs we calculated matrices of co-location peak values and cross-location correlations of waveforms. By this way we obtain two matrices as following:

$$M_{co}[i\,,j] = peak\{|Rij[\,\tau\,]|\}\ ;\ i\,,j = 1 \text{ to } 64 \qquad (10)$$

$$M_{cross}[i\,,j] = peak\{|Rij[\tau\,]|\}\ ;\ i\,,j = 1 \text{ to } 64 \qquad (11)$$

In which, $Rij[\tau]$ is cross correlation of i-th and j-th waveforms and M_{co} is co-location matrix and M_{cross} is cross-location matrix. To have a thorough view that makes sense in proof-of-concept we made two 3-dimentional heat-map graphs that shows M_{co} and M_{cross} correlation matrices in the same scale. The graphs are shown in Fig. 24.

As it can be seen in heatmap graphs, in our proof-of-concept prototype, two SPDs are mounted 20 cm apart and there is enough decorrelation between two SPD locations, hence the correlation matrixes can be separated by a flat surface as a threshold. It means that an artificial intelligence algorithm may be used to learn and differentiate between the waveforms of each APD in a fast and automated way.

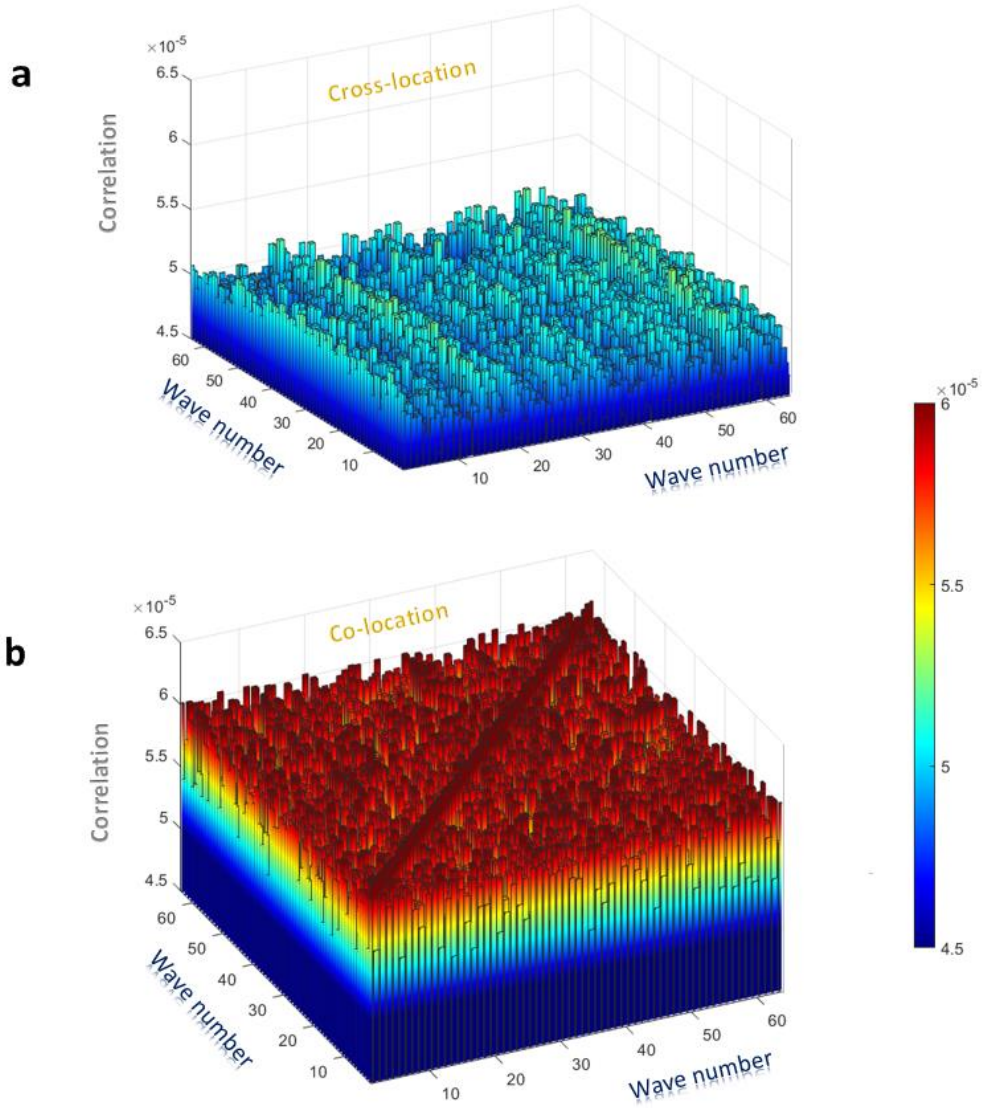

Figure 47-Correlation matrix

Cross-correlation matrices made by waveforms captured in two different places (Cross-location) and one place (Co-location): (a) Cross-correlation matrix of 64 waveforms captured from SPDs in different locations 20 cm apart. (b) Correlation matrix of 64 waveforms captured from SPDs in one location

6.2. Signal recognition by deep learning Neural Network

A survey conducted by Li et al. (2019) shows that deep learning techniques can be efficiently used in different wireless signal recognition scenarios and applying the raw signal to the neural network without any preprocessing is becoming a trend in signal recognition.

In this stage we implemented deep learning signal classification using MATLAB's Deep Learning Toolbox (Paluszek, & Thomas, 2020), among many technologies, we used simple multilayer neural network to differentiate between two SPD waveforms. In fact, this machine automates the recognition of decorrelations between waveforms after signal processing and filtering.

In our experimental setup we used half of the waveforms for training purpose and half for test. We first implemented a deep learning neural network with input neurons equal to the number of samples of input signal. After time-excision, the number of samples was reduced to 256 and each input neuron was containing a time-sample of a waveform x(t) , then we made five hidden layers of fully interconnected neurons and finally prepared one output neuron with binary output. Fig. 25 shows the schematic of the neural network that was implemented on MATLAB Toolbox. The output neurons are trained to deliver two values which represents the received waveforms of either SPD1 or SPD2. After training we applied the test waveforms to the network and the results showed that the network can classify the waveforms received from each SPD with an accuracy of better than 99.5 percent. It shows that we can clone most of the single photon bits in the quantum receiver side with very low error rate and destroy the quantum safety of the QKD link.

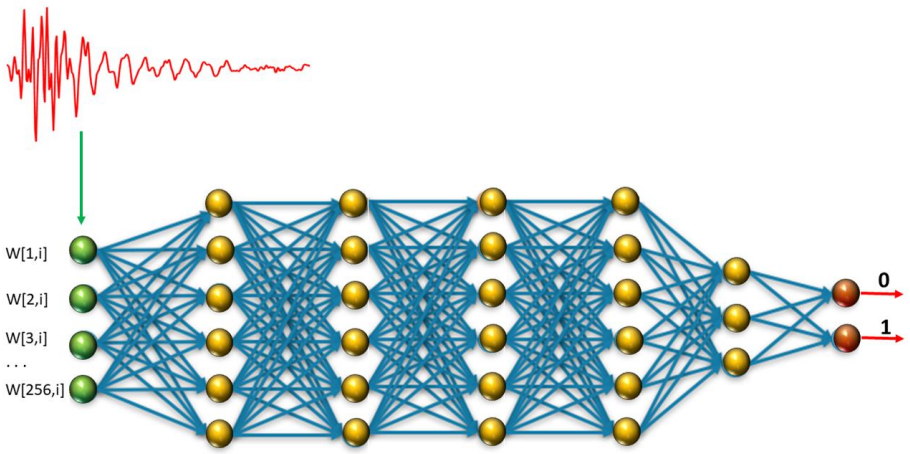

Figure 49-Fingerprint classification by neural network

Deep learning neural network classifies waveforms of each SPD. After learning it can differentiate the RF fingerprints of the radiated signals coming from SPDs in different locations.

6.3. Practical aspects

In order for this experiment to have a practical aspect, two limitations should be evaluated theoretically:

1- Distance between SPDs and eavesdropper
2- Spacing between SPDs

The Maximum distance limitation can be improved by increasing the gain of the antenna. A common way to increase the antenna gain while maintaining the bandwidth is using a dish reflector with a wideband feed. Fig. 26 shows a typical practical setup that uses two dish antennas in which one antenna is aimed toward the target SPDs and the second one is slightly deviated to a different angle to receive the ambient noise. By using this antenna configuration, a dual channel digitizer can provide spectrum subtraction to remove the ambient RF noise from RF fingerprints in the same way that professional microphones cancel the ambient acoustic noise. Increasing the antenna gain has two limitations: beam-width and antenna size.

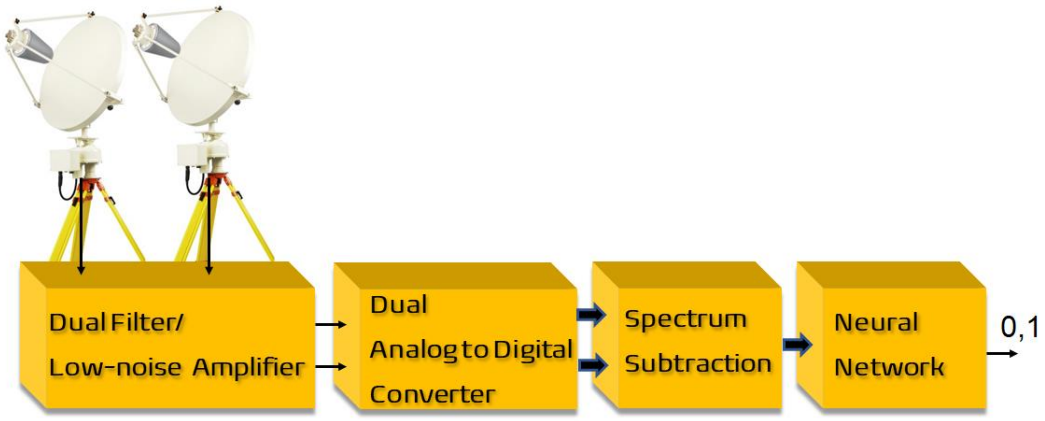

Figure 51-Range extension

Extension of range and accuracy of the experimental proof-of-concept setup is possible by using high gain antennas and high resolution A/D. A typical dual dish antenna can be used for increasing the signal acquisition range and providing spectrum subtraction to attenuate the ambient noise.

When increasing the antenna gain in this application, this fact must be taken into account that any increase in the antenna gain decreases the beam-width of the antenna which is a kind of spatial filtering that decreases the geometrical volume in which reflections of the RF fingerprints occurs hence narrower beam-width decreases the information content and decorrelation of RF fingerprints. By considering these facts we calculated the maximum achievable gain and range for two different scenarios when the antenna covers a volume with 4-meter diameter in the QKD receiver room and another scenario with 8 meter diameter. If we assume that the antenna has enough elevation and gain, then we can use single-ray (free space) propagation model, and hence we can compare achievable gains with propagation loss side-by-side in one figure. In Fig. 27 the path loss in excess of 2 meter (28 dB) is shown up to 100 meters along with the antenna gains with enough beam-widths to cover a 4-meter room and an 8-meter room using the following dish-antenna equation:

$$G = e_A\left[\frac{\pi K}{2\, tg^{-1}\left(\frac{r}{R}\right)}\right]^2 \qquad (12)$$

In which G is the antenna gain, e_A is the aperture efficiency (0.6 in typical dishes), K is the beam-width factor (typically 70), r is the radius of the coverage area in the room and R is the Range.

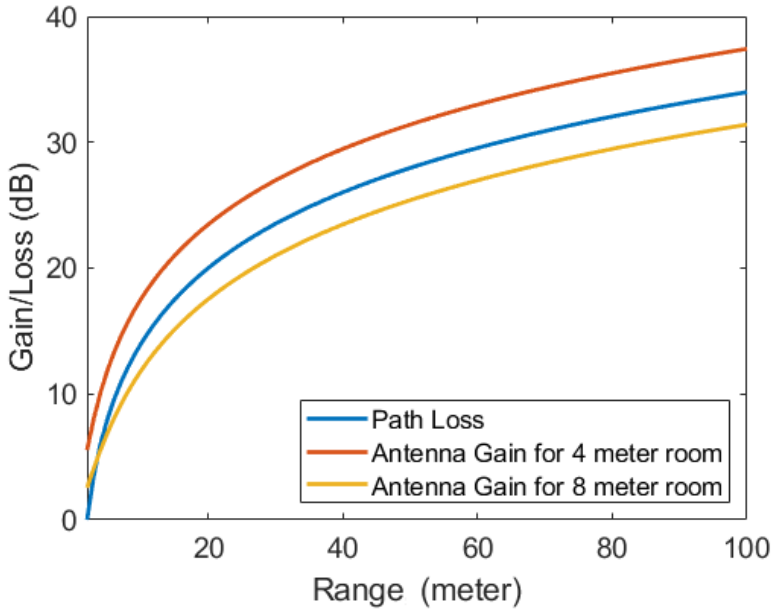

Figure 53-Path loss and antenna gain

Path loss and antenna gains for narrow-beam and wide-beam antennas as a function of range

The path loss calculations shows that to achieve enough gain to compensate the propagation loss we need to use the first version that covers a 4-meter room. Another factor that limits the gain is the antenna size that becomes too large to be practical for ranges over 100 meter.
Here we assume that in our experimental setup which has a small antenna with diameter D < 7 cm, the antenna is located in the Far-field region as the distance between antenna and APD is greater than $2D^2/\lambda$ (Johnson, R. C., & Jasik, H. 1984).
The second practical issue to consider is Minimum spacing between SPDs. During the experimental tests, it have been observed that fingerprint decorrelations are directly dependent on the spacing between two SPDs in a way that more spacing provides more decorrelation and less spacing produces more similarity in the RF fingerprints. Assuming that an eavesdropper has no limit on processing power in the neural network part using cloud computing, to attain the minimum spacing between SPDs she must be able to extract more precise details from RF fingerprint waves and to do this she must consider two factors of the digitizer:

- Receiver Bandwidth
- Receiver Noise

In our experimental setup we used 1-GSPS sample rate and 8-bit resolution to achieve 20 cm spacing between SPDs. In a practical scenario an eavesdropper can use higher bandwidth and higher resolution analog to digital (A/D) converters to achieve less SPD separation. To evaluate the amount of possible decrease in SPD spacing with the current Commercial off-the-shelf technologies, we had a review on the best state-of-the-art A/D converters available from “Texas Instruments” company. The result of this review is shown in Fig. 28. In this scenario we have two main noise sources that are Thermal noise of a typical receiving system with 3 dB Noise figure and quantization noise of the A/D.
The thermal noise power is defined by $N=KTB$ in which K is the Boltzmann constant, T is absolute temperature and B is the bandwidth of the receiving system.

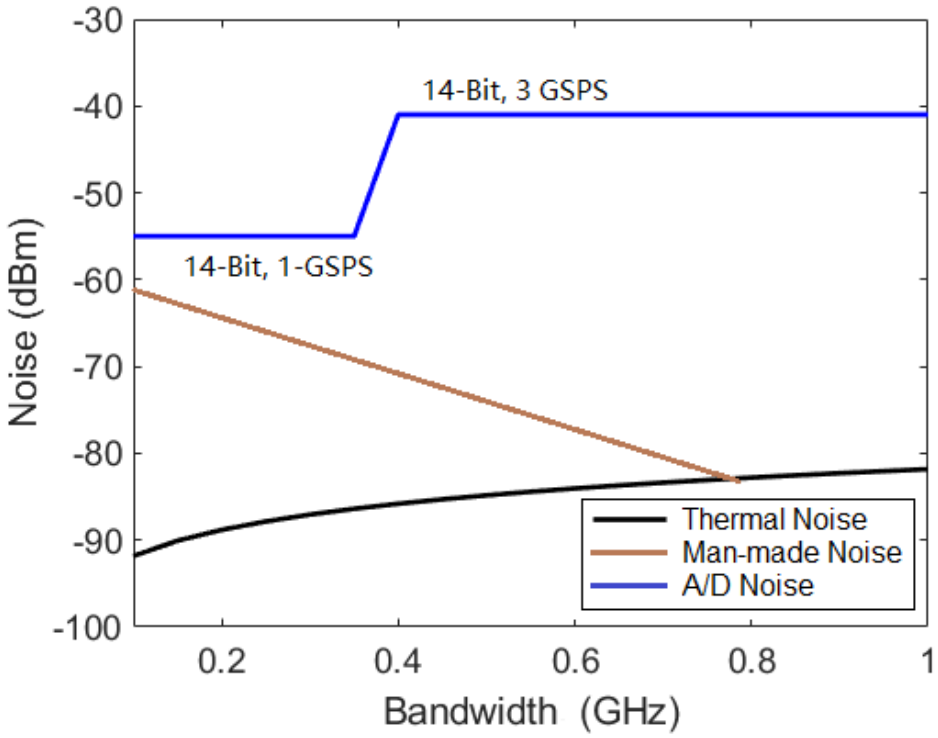

Figure 55-Internal and external noise

A/D quantization noise, man-made and thermal noise level in the receiver

In a realistic scenario we should also consider the external noises in addition to receiver's thermal noise. Fig. 29 shows that the dominant external noise that overlaps with the spectrum of APD waves is the man-made noise and other noises are negligible.

Here we can see that the thermal noise increases linearly with the bandwidth, but A/D review showed that the dominant noise in this application is A/D quantization noise rather than thermal noise. Also reviews indicates that there is a digital gap in A/D noise when we increase the sample rate to more than 1 GSPS. We compared two high-end high-resolution 14-bit A/Ds. for 1 GSPS rate the Signal to Noise Ratio (SNR) was around 69 dB which means that we have -55dB quantization noise level for a full scale signal of 14 dBm. For 3 GSPS rate the SNR was around 55 dB which means that we have -41dB quantization noise level for a full scale signal of 14 dBm, this means that if we double the receiving bandwidth the quantization noise increases to more than 20 times. Hence increasing the bandwidth to more that 350 MHz (maximum practical signal bandwidth with a 1-GSPS A/D) can not increase the performance of reception. Now as the similarity of RF fingerprints can be defined as a correlation function which is a linear operation then we can say that the minimum spacing between SPDs is linearly related with achievable quantization noise level. If we assume that our 8-bit oscilloscope (used

in experimental setup) has 7 effective number of bits then we can calculate its signal to quantization noise ratio as:

$$SQNR \approx 1.761 + 6.02\, Q_{dB} \qquad (13)$$

where Q is the number of effective quantization bits. Then for our 8-bit oscilloscope the SQNR will be around 44dB. Now if we compare this SNR with the achievable SNR of the 1-GSPS 14-bit A/D which was 69 dB SNR, then we can see a 25 dB improvement which means that the minimum spacing between SPDs can be decreased 300 times (to less than 1 mm spacing)by using a 14-bit 1-GSPS A/D.

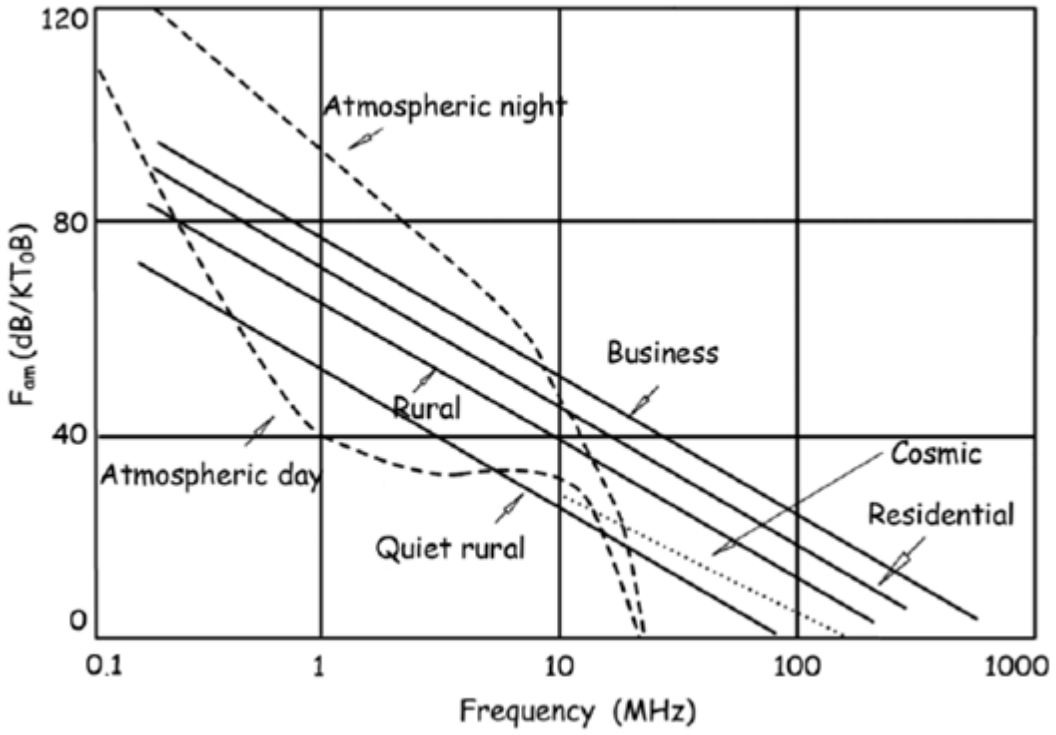

Figure 57-External noise

Median values of man-made radio noise power (solid lines) expressed in terms of Fam (dB above thermal noise at T0=288 K). Atmospheric noise (dashed lines) and cosmic background noise (dotted line) are reported for comparison with man-made noise – (Bianchi & Meloni (2007)

6.4. Countermeasures

Our experiments showed that the RF leakage is a serious loophole in all quantum cryptosystems that should not be ignored even in mature commercial systems. We showed that radiated power of this leakage is dependent on the box shielding of the SPD. We also showed that the identification of the quantum states through fingerprint is dependent on the spacing between SPDs. By using the mentioned characteristics, the following provisions should be seriously prepared for every quantum-secured communication system as a countermeasure to RF attack:

1. Assembling the SPDs as close as possible
2. Maximum Electromagnetic shielding in physical layer
3. Including a wideband jammer in the quantum receiver

7. CONCLUSION

Our theoretical discussions supported by lab. experiments with home-made and commercial SPDs proved that the RF fingerprint of the avalanche photodiodes can penetrate through the metal shielding and intercepted by an eavesdropper without affecting on the error rate of the quantum link. Another fact which have been strongly proven in the experiments, was the possibility of distinguishing between impulses received from different SPDs inside a metal shelf, by RF fingerprints of the signals which has direct relation with the quantum states of single photons. We have also proved experimentally using a deep learning neural network that the process of identification of fingerprints can be automated by machine learning. We calculated theoretically that the range of RF attack can be extended to 100 meters using commercial off-the-shelf Antenna, RF and A/D technologies.

In summary, although this experiment is not the end of the matter for QKD but it proved that any secure communication system that relies on absolute safety of quantum transmission must also include relevant cyber-physical and electronic warfare techniques (like extreme shielding and jamming), to ensure that any kind of hostile use of electromagnetic spectrum is seriously taken into consideration.

APPENDIX

MATLAB Codes

---------- FFT Filtering ----------

```
% FFT Filtering %
clear;
startfreq=30e6;  %Hz
stopfreq=300e6; %Hz
signalp11= readmatrix('C:\\Position1\\P1_1.CSV');
% signalx=signalp11(300:555,2); % Time excision
signalx=signalp11(:,2); % no Time excision
signalx=signalx-mean(signalx);
      dt = 1e-9 ; % Sampling time= 1ns
      Fs = 1/dt;  % Sampling frequency
      N = size(signalx,1); % Size of Signal in time domain
      dF = Fs/N;
      f = (-Fs/2:dF:Fs/2-dF)';
      BPF = ((startfreq < abs(f)) & (abs(f) < stopfreq)); % BP Filter
      time = dt*(0:N-1)';
      spektrum1 = fftshift(fft(signalx))/N;
      spektrum2 = BPF.*spektrum1;    % Apply Freq domain filter
      signalxBP=256*real(ifft(ifftshift(spektrum2))); %inverse ifft
      writematrix(signalxBP,'signalp11BP.csv');
%%% Figures  %%%%%%%
     figure;
     subplot(2,1,1);
     plot(f,1000*abs(spektrum1),'r', 'LineWidth',2);  % -----mV
     title('Spectrum before filtering')
     set(gca,'FontSize',14);%---------------font
     subplot(2,1,2);
     plot(f,1000*abs(spektrum2),'r', 'LineWidth',2);% -----mV
     title('Spectrum after filtering')
     xlabel('Frequency (Hz)')
     set(gca,'FontSize',14);%---------------font
     figure;
     subplot(2,1,1);
     plot(time,1000*signalx,'r', 'LineWidth',2); % -----mV
     title('Signal before filtering')
     set(gca,'FontSize',14);%---------------font
     subplot(2,1,2);
     plot(time,1000*signalxBP,'r', 'LineWidth',2);% -----mV
     xlabel('Time (s)')
     title('Signal after filtering')
     set(gca,'FontSize',14);%---------------font
```

---------- Cross-correlations of detected signals ----------

```
% Cross-correlation %
clear;
signalxcor = zeros(255, 164);
signalxcormax = zeros(64, 64);
signalmatrixP1= zeros(128, 64);
signalmatrixP2= zeros(128, 64);
for filenum=1:64
    strinP1 = sprintf('C:\\Position1b64\\filtered_%d.CSV',filenum);
    strinP2 = sprintf('C:\\Position2b64\\filtered_%d.CSV',filenum);
    signalP1= readmatrix(strinP1);
    signalP2= readmatrix(strinP2);
    signalmatrixP1(:,filenum)=signalP1;
    signalmatrixP2(:,filenum)=signalP2;
end

for counter2=1:64

signalxcor(:,counter2)=abs(xcorr(signalmatrixP1(:,1),signalmatrixP1(:,count
er2)));
end
for counter2=1:64

signalxcor(:,counter2+100)=abs(xcorr(signalmatrixP1(:,1),signalmatrixP2(:,c
ounter2)));
end

figure

b = bar3(signalxcor);
colorbar
for k = 1:length(b)
    zdata = b(k).ZData;
    b(k).CData = zdata;
    b(k).FaceColor = 'interp';
end
zlim([0, 6e-5]);
cmap = colormap(jet);
caxis([0 5e-5]);
%xtickangle(30);
set(gca,'FontSize',14);
```

---------- *Correlation Matrix* ----------

```
% Cross-correlation Matrix %
clear;
signalxcormax = zeros(64, 64);
signalmatrixP1= zeros(128, 64);
signalmatrixP2= zeros(128, 64);
for filenum=1:64
    strinP1 = sprintf('C:\\Position1b64\\filtered_%d.CSV',filenum);
    strinP2 = sprintf('C:\\Position2b64\\filtered_%d.CSV',filenum);
    signalP1= readmatrix(strinP1);
    signalP2= readmatrix(strinP2);
    signalmatrixP1(:,filenum)=signalP1;
    signalmatrixP2(:,filenum)=signalP2;
end
% Plotting max of correlations
for counter1=1:64
    for counter2=1:64

signalxcormax(counter1,counter2)=max(abs(xcorr(signalmatrixP1(:,counter1),s
ignalmatrixP2(:,counter2))));
    end
end
%signalxcormax(signalxcormax<0)=0; % no need if zlim([0,*])
figure
b = bar3(signalxcormax);
%b = bar3(signalxcor);
colorbar
for k = 1:length(b)
    zdata = b(k).ZData;
    b(k).CData = zdata;
    b(k).FaceColor = 'interp';
end
title('Same Position Correlation');
xlabel('Wave number Position 2','Rotation',22);
ylabel('Wave number Position 1','Rotation',-35);
zlabel('correlation');
xlim([1, 64]);
ylim([1, 64]);
zlim([4.5e-5, 6.5e-5]);% Z axis
caxis([4.5e-5 6.0e-5]);% Heat colors
cmap = colormap(jet);
%xtickangle(30);
set(gca,'FontSize',14);
```

---------- Maximum range and Minimum distance calculation ----------

```
% MaxRange
% Here we plot Antenna Gain and Path loss in Range
clear;
Rr1=2;     % 4 meter room , 2m radius
Rr2=4;     % 8 meter room , 4m radius
Ea=0.6;    % Antenna aperture efficiency
K=70;
Lambda=1; %wavelength
Const= 16*pi^2/(Lambda ^2);
Range=2:1:100;
Loss=10*log10(Const*(Range.^2))-28;% Path loss above 0 meter
Gain1=10*(log10((Ea*(0.5*pi*K)^2)./((atand(Rr1./Range)).^2)));
Gain2=10*(log10((Ea*(0.5*pi*K)^2)./((atand(Rr2./Range)).^2)));
plot(Range, Loss, Range, Gain1,Range, Gain2, 'LineWidth', 2)
xlim([2 100])
legend('Path Loss','Antenna Gain for 4 meter room','Antenna Gain for 8
meter room', 'Location', 'SouthEast')
xlabel('Range, (meter)')
ylabel('Gain/Loss (dB)')
%title('Antenna gain and Path Loss as a function of Range')
set(gca,'FontSize',14);%---------------font
```

```
% MinDistance
% Here we plot Antenna Gain and Path loss in Range
clear;
KT=1.38e-23 * 300 * 1e9;
B=0.1:0.05:1;
ThermalNoise=2+10*log10(KT*B)+30;% 2dB Noise figure

QN=zeros(size(B));
QN(1:6)=-55;% 100 to 350 MHz
QN(7:19)=-41;% 400 to 1000 MHz

Gain1=10;
Gain2=10;
plot(B,ThermalNoise,'black',B, QN,'blue','LineWidth',2)
xlim([0.1 1])
ylim([-100 -30])
legend('ThermalNoise','A/D Noise', 'Location', 'SouthEast')
xlabel('Bandwidth, (GHz)')
ylabel('Noise (dBm)')
%title('Thermal and Quantization Noise as a function of Bandwidth')
set(gca,'FontSize',14);%---------------font
```

BIBLIOGRAPHY

Acin, A., Gisin, N., & Masanes, L. (2006). From Bell's theorem to secure quantum key distribution. *Physical review letters*, *97*(12), 120405.

Alléaume, R. (2018). Implementation Security of Quantum Cryptography: Introduction, challenges, solutions. *ETSI White Paper*, *27*, 28.

Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, *1*(3), 195.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. *Journal of cryptology*, *5*(1), 3-28.

Bennett, C. H., & Brassard, G. (1984, August). An update on quantum cryptography. In *Workshop on the theory and application of cryptographic techniques* (pp. 475-480). Springer, Berlin, Heidelberg.

Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In *Post-quantum cryptography* (pp. 1-14). Springer, Berlin, Heidelberg.

Bianchi, C., & Meloni, A. (2007). Natural and man-made terrestrial electromagnetic noise: an outlook. Annals of geophysics.

Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., ... & Nolan, D. (2018). Secure quantum key distribution over 421 km of optical fiber. *Physical review letters*, *121*(19), 190502.

Bohm, D. (1951). Quantum Theory Prentice-Hall. *Englewood Cliffs, NJ*.

Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1970). Proposed Experiment to Test Local Hidden Variable Theories. *Physical Review Letters*, *24*(10), 549.

D'Amato, S., Baudis, L., Kish, A., & Wulf, M. S. J. (2016). Characterization of silicon photomultiplier arrays in liquid xenon and development of dedicated read-out electronics (Doctoral dissertation, Universität Zürich).

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete?. *Physical review*, *47*(10), 777.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters*, *67*(6), 661.

Friedel, J. E., Holzer, T. H., & Sarkani, S. (2018). Development, optimization, and validation of unintended radiated emissions processing system for threat identification. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*.

Furrer, F. J. (2020). Roger A. Grimes. Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics*, *74*(1), 145.

Haitz, R. H. (1964). Model for the electrical behavior of a microplasma. Journal of Applied Physics, 35(5), 1370-1376.

Harmuth, H. F., & Ding-Rong, S. (1983). Antennas for nonsinusoidal waves. I. Radiators. IEEE Transactions on Electromagnetic Compatibility, (1), 13-24.

Harmuth, H. F. (1985). Radiation of nonsinusoidal waves by a large-current radiator. IEEE transactions on electromagnetic compatibility, (2), 77-87.

Herger, E. (2014) . Guide to detector selection, tech. notes, Hamamatsu

Imre, S. (2013). Quantum communications: Explained for communication engineers. *IEEE Communications Magazine*, *51*(8), 28-35.

Inamori, H., Lütkenhaus, N., & Mayers, D. (2007). Unconditional security of practical quantum key distribution. *The European Physical Journal D*, *41*(3), 599.

I. T. U. (2009). Measurement techniques of ultra-wideband transmissions. ITU Recommendation.

Johnson, R. C., & Jasik, H. (1984). Antenna engineering handbook. mgh.

Karamzadeh, S. (2020). High Gain UWB Vivaldi Antenna for GPR Applications, MTTW'20, IEEE Microwave Theory and Techniques in Wireless Communications(under review).

Koshelev, V. I., Belichenko, V. P., & Buyanov, Y. I. (2017). Ultrawideband short-pulse radio systems. Artech House.

Lamas-Linares, A., & Kurtsiefer, C. (2007). Breaking a quantum key distribution system through a timing side channel. *Optics express*, *15*(15), 9388-9393.

Li, X., Dong, F., Zhang, S., & Guo, W. (2019). A survey on deep learning techniques in wireless signal recognition. Wireless Communications and Mobile Computing, 2019.

Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016). Quantum random number generation. *npj Quantum Information*, *2*(1), 1-9.

Meda, A., Degiovanni, I. P., Tosi, A., Yuan, Z., Brida, G., & Genovese, M. (2017). Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. Light: Science & Applications, 6(6), e16261-e16261.

Mehdipour, A., Mohammadpour-Aghdam, K., & Faraji-Dana, R.(2007). Complete dispersion analysis of Vivaldi antenna for ultra wideband applications. Progress In Electromagnetics Research, 77, 85-96.

Merali, Z. (2010). Quantum crack in cryptographic armour.

Mikki, S. (2020) Theory of Nonsinusoidal Small Antennas for Near-Field Communication System Analysis, *Progress In Electromagnetics Research B*, Vol. 86, 177-193, doi:10.2528/PIERB19121104

Paluszek, M., & Thomas, S. (2020). Practical MATLAB Deep Learning: A Project-Based Approach. Apress.

Renker, D. (2006). Geiger-mode avalanche photodiodes, history, properties and problems. Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 567(1), 48-56.

Schantz, H. G. (2004, May). Dispersion and UWB antennas. In 2004 International Workshop on Ultra Wideband Systems Joint with Conference on Ultra Wideband Systems and Technologies. Joint UWBST & IWUWBS 2004 (IEEE Cat. No. 04EX812) (pp. 161-165). IEEE.

Schwinger, J., DeRaad Jr, L. L., Milton, K., & Tsai, W. Y. (1998). Classical electrodynamics. Westview Press.

Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters*, *85*(2), 441.

Vilà, A., Arbat A., , Vilella E. and Dieguez, A. (2012). Geiger-Mode Avalanche Photodiodes in Standard CMOS Technologies, Photodetectors, Dr. Sanka Gateva (Ed.), ISBN: 978-953-51-0358-5, InTech, Available from: https://www.intechopen.com/books/photodetectors

Villar, A., Lohrmann, A., Bai, X., Vergoossen, T., Bedington, R., Perumangatt, C., ... & Chandrasekara, R. (2020). Entanglement demonstration on board a nano-satellite. *Optica*, *7*(7), 734-737.

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, *299*(5886), 802-803.

Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, *92*(2), 025002.

Ye, T., Walsh, M., Haigh, P., Barton, J., & O'Flynn, B. (2011). Experimental impulse radio IEEE 802.15. 4a UWB based wireless sensor localization technology: Characterization, reliability and ranging. In ISSC 2011, 22nd IET Irish Signals and Systems Conference, Dublin, Ireland. 23-24 Jun 2011. Institution of Engineering and Technology.

Zappa, F., Tosi, A., Dalla Mora, A. & Tisa, S. (2009). SPICE modeling of single photon avalanche diodes. Sensors and Actuators A: Physical, 153(2), 197-204.

VITA

Naser Jam received his B.Sc. Degree in Electrical Engineering from Sharif University of Technology, Tehran, Iran in 1991. After graduation he worked as engineer, chief designer and project manager in Radar and Communications projects in the Electronic Research Center of the Sharif University. From 2018 he joined Özyeğin University as a graduate student and a member of the quantum optics lab. Naser's main research areas are quantum sensing and quantum communications.