# Non-distributable key-sharing protocol with particular emphasis on the Internet of Things

Mario Mastriani

*Knight Foundation School of Computing and Information Sciences,*
*Florida International University, 11200 S.W. 8th Street, Miami, FL 33199, USA*
mmastria@fiu.edu
ORCID Id: 0000-0002-5627-3935

**Abstract** - Quantum key distribution (QKD) constitutes the most widespread family of information preservation techniques in the context of Quantum Cryptography. However, these techniques must deal with a series of technological challenges that prevent their efficient implementation, in space, as well as in exclusively terrestrial configurations. Moreover, the current smallsat constellations of Low Earth Orbit (LEO with an altitude of approx. 500 km) added to other satellites in Medium Earth Orbit (MEO), and geostationary orbits (GEO), plus a large amount of space debris present around the planet, have become a serious obstacle for Astronomy. In this work, a classic alternative to QKD is presented, also based on a symmetric key, but with low cost, and high efficiency, which dispenses with all the implementation problems present in the QKD protocols and does not require the use of satellites, and which we will call non-distributable key sharing (NDKS). Due to its low cost, simplicity of implementation, and high efficiency, NDKS is presented as an ideal solution to the problem of cybersecurity on the Internet of Things (IoT), in general, and IoT-fog-clouds, in particular.

**Keywords** – Cybersecurity, Internet of Things, IoT-fog-cloud, quantum cryptography, quantum Internet, quantum key distribution.

## 1. INTRODUCTION

The Internet of Things (IoT) is an emerging technology of technical, social, and economic importance [1]. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are now being combined with Internet connectivity and powerful data analytics capabilities, which promise to transform how everyday tasks such as work, life, and play are carried out [2]. The projections of the impact of the IoT on the Internet and the economy are remarkable. The best estimates anticipate that in the year 2025, there will be up to one hundred billion devices connected to the IoT and that its impact will be U\$S $11 \times 10^{12}$. However, IoT also poses significant challenges that could make it difficult to realize its potential benefits [3]. News about attacks on Internet-connected devices, fears of surveillance, and privacy concerns have already captured the public's attention [4]. The technical challenges are still there, but new policy, legal, and development challenges are also emerging. Definitively, its weak point is the security of the information and the preservation of the integrity of the data that travels through the network.

On the other hand, fog computing is the name of a cloud technology whereby the data generated by the devices is not uploaded directly to the cloud but is first prepared in smaller decentralized data centers [5]. The concept encompasses a network that extends from its borders, which is where the endpoints generate the data, to the central destination of the data in the public cloud or a private data center (private cloud) [6]. With the idea of a decentralized Information Technology (IT) infrastructure, cloud computing would bring data processing closer to ground level. This is done with the so-called fog nodes, processing nodes before the cloud that acts as a mediator between the cloud and the different IoT devices [7]. The objective of fog computing also called fogging, is to shorten the communication paths between the cloud and the devices and reduce the data flow in external networks [8]. The nodes would thus fulfill an intermediate layer role in the network in which it is decided which data is processed locally and which is sent to the cloud or to a data center to be analyzed or processed.

As we have mentioned before, the problem that appears as the main stumbling block for the implementation of IoT techniques in a safe way, with or without the intervention of fog computing, is precisely the security of the information and the preservation of the integrity of the data. Therefore, given that all the current Cybersecurity tools used in IT have been widely violated, new cryptographic techniques based on principles of quantum mechanics [9] and grouped under the designation of Quantum Cryptography [10] appear to be a superior option. These tools are part of the arsenal of

resources for Quantum Communications [11], whose maximum exponent is the future network of networks, i.e., the quantum Internet [12-17].

Precisely, the fundamental difference between the current Internet and the future Quantum Internet will lie in the security of information, which will be preserved in the latter through different families of techniques, among which the best known and applied is undoubtedly quantum key distribution (QKD) [10]. However, both in its purely terrestrial implementation [18, 19] as well as in space-to-ground or ground-to-space implementations [20-23], all QKD families have serious implementation problems.

These issues will be addressed in detail in the next section.

In summary, if we cannot do without QKD as far as information security is concerned, and yet its implementation problems persist in all its versions, then the only solution to ensure data integrity in IoT and the future quantum Internet is to resort to a technique that does not have the aforementioned problems. This is the central axis of this work by proposing a non-distributable key sharing (NDKS) technique to solve such an important problem.

The remainder of this paper is structured as follows. In Section 2, we describe the issues present in all QKD implementations. In Section 3, we discuss the non-distributable key-sharing technique in detail. In Section 4, we provide a discussion and outline the limitations of our work. Finally, we conclude the paper by providing future research directions in Section 5.

## 2. ISSUES WITH QKD IMPLEMENTATIONS

A typical QKD configuration requires two channels for the distribution of the key and an extra channel (public) for the transmission of the encrypted message. Figure 1 shows a generic QKD protocol, which consists of a symmetric-key system.
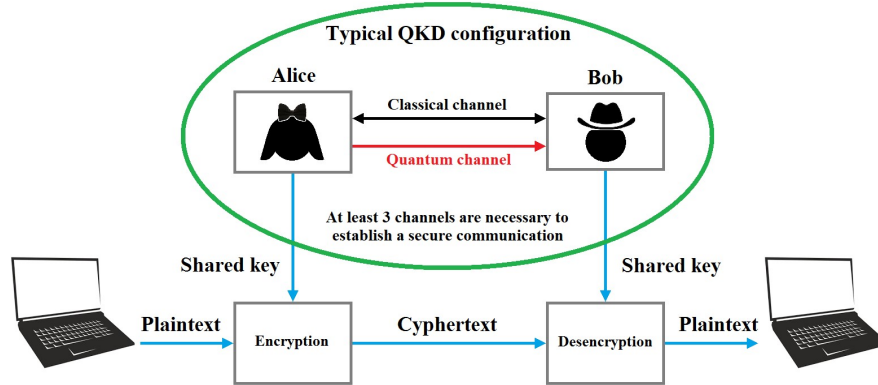


FIG. 1. Typical QKD configuration with two channels for the distribution of the key, and an extra channel (public) for the transmission of the encrypted message.

In the rest of this section, we will refer frequently to Fig. 1 as the natural environment where several of the implementation problems that this technology entails are highlighted.

Next, the different implementation problems of all QKD protocols are described according to the scope used for the distribution of the keys (land-to-land, space-to-land, land-to-space, or space-to-space), and as a consequence of this, it is evident that a new technique is required to avoid the mentioned problems and make efficient any practical implementation of this type of protocols.

### 2.1. Issues common to all QKD implementation

QKD protocols encode classical information (bits) in quantum states prepared on different discrete degrees of freedom of physical systems. The first and most important are those based on polarized

photons in orthogonal states [24], entangled photons [25], and polarized photons in non-orthogonal states [26].

The security of these protocols is determined by the careful study of the effects of the intervention of an eavesdropper. The objective of any security study is to minimize the amount of information that an eavesdropper can obtain when attacking a certain scheme, knowing the value of some conspicuous metric that allows evaluating such information exposure, e.g., the Quantum Bit Error Rate (QBER), which is estimated during the distribution of the key and the conditions in which the experiment is carried out. From this study, the proportion of maximum secure key bits that can be extracted with classical post-processing of the distilled key is estimated. Although the security of the QKD seeks to be demonstrated in the most general scenario possible, in most analyses, different restrictions on the technological capabilities of the eavesdropper are assumed. Even though this type of study only guarantees safety in a limited context, the results obtained help to understand and advance in a general demonstration of safety for different protocols. The result of these studies may yield new levels for the secure key rate, or modifications to the protocols to make them robust against different attacks. In most cases, the ultimate proof of security is an open problem.

The National Security Agency (NSA) [27] highlights the following technical limitations of the QKD protocols:

- Quantum key distribution is only a partial solution,
- Quantum key distribution requires special-purpose equipment,
- Quantum key distribution increases infrastructure costs and insider threat risks,
- Securing and validating quantum key distribution is a significant challenge, and
- Quantum key distribution increases the risk of denial of service.

Other also recent studies [28] tell us about a series of needs to take into account when working with these protocols such as privacy amplification, and information reconciliation [29].

However, the problems do not end there, in fact, they are just beginning. As we can see in Fig. 1, the key distribution uses two channels [29], one classical and one quantum. The classical channel must be authenticated, since, although quantum communication attains the ability to detect the bugging and stop the communication, the key still needs to be passed to each other in a classical communication way to ensure that the subjects do not communicate with someone else [30-32]. It is because of this apocryphal presence in the channels that configurations of several states [33] are used to create ambiguities that make it difficult for the hacker or eavesdropper to act.

The problems of attacks on the QKD protocols (e.g., man-in-the-middle attack, and some other particular cases of each type of implementation that we will see in due course) force a recurring distillation of the key to ensure that it is not shared with a hacker. However, the distillation has a consequence that the key may eventually suffer a reduction in size during said distillation process. This happens equally in terrestrial and satellite implementations of QKD. This forces the QKD protocol to be restarted again to obtain a final key, made up of the accumulation of the parts obtained in the different attempts so that at the end a key of the intended size is available.

In additionally to the aforementioned problems during a typical QKD implementation, it is needed to resort to:

- important amounts of quantum memory, to hold a state at one point while its counterpart arrives at another point,
- time synchronization so that all the operations carried out by the protocol respect the correct sequence that it requires, and
- so on.

## 2.2. Issues with terrestrial QKD implementation

As mentioned above, the unconditional security of QKD systems is based on a thorough characterization of both the theoretical protocol and its experimental implementation. The latter is one of the most complex and constantly evolving tasks in the area. Recent protocols seek to minimize the effect of the imperfections of the experimental devices used. On the other hand, shortcomings or

characteristics of the protocols and their practical implementations that can be exploited to violate their security are also sought [34-36].

Moreover, there are attacks particularly concentrated on imperfections of the single-photon detectors, where this type of action seeks either to manipulate the detection efficiency or to take advantage of some variation of this quantity in favor of the eavesdropper. On the one hand, there are attacks on detectors that work with detection windows. In general, the detection efficiency at the edges of windows does not go from 0 to the maximum value instantly. An eavesdropper can use this feature by selectively adding delays to signals intercepted in an attack [37]. Attacks that make use of a dead-time detector to manipulate measurement results have also been proposed [38]. Other attacks are carried out by damaging detectors with very powerful pulses of light. Once damaged, the eavesdropper can control the detection signals with intense light (putting the detector in photocurrent mode) and thus perform an intercept-and-forward attack without increasing the QBER [39].

Some attack proposals focus on devices used to control quantum states, both for preparation and measurement. One type of attack, known as a "Trojan horse" [40], is based on introducing intense light (generally of a different wavelength than the one used for the protocol) into Alice's (or Bob's) station to later obtain information from the primed states (or the detection basis choices) from variations in the light reflected in the quantum channel by the devices of the experimental setup or detection scheme (intensity, phase, etc. modulators). Another feature of state preparation devices that can be exploited by an eavesdropper is the wavelength dependence of their operation. For example, there are attacks based on beam splitters whose transmission factor (reflection) strongly depends on the energy of the incident photons [41]. An eavesdropper can intervene by sending signals with different wavelengths and thus force detection on a measurement or projection basis to a particular state of the protocol. In general, for each of these attacks, there is an easy-to-implement preventative countermeasure, such as measuring the intensity of light entering Alice and Bob, interference filters, or temporal filtering of the detected signals. That is to say, the real importance of this area is to study what characteristics of the systems can be attacked and to propose a simple way to avoid those vulnerabilities, keeping the requirements on practical QKD systems to a minimum.

To the aforementioned attacks, we must add those specifically aimed at a particular protocol, such as the individual attack on BB84 (intercept and resend) [42], the optimal individual attack on BB84 [43] (cloning machine [44]), and the photon number splitting attacks [45-48]. Finally, Lucamarini *et al*. provide us with a complete list of attacks [49].

On the other hand, it is not just attacks that are the problems facing any terrestrial implementation of a QKD protocol, given that an implementation of this type presents a series of challenges that are difficult to manage in practice [50-58].

These challenges are presented in the form of very high technical requirements. Among the most outstanding, we can mention:

- Every implementation of QKD demands low channel noise [59]: Unfortunately, current implementations of QKD systems show relatively low-key rates, demand low channel noise, and use *ad hoc* devices. Every QKD protocol is subject to channel noise, which strongly conditions its performance and therefore the quality of key distribution.
- These configurations require authentication [60] of the classical channel used in the protocol, i.e., the classical channel presented in Fig. 1.
- Its fiber optic installations have requirements for specific platforms and layers [61], i.e., it is not just any optical network, although this is strongly conditioned by the type of photons with which the protocol works (polarized or entangled).
- This requires synchronization [62] of both ends and recipients of the key.
- The network is too exposed to fake users, hence the previous mention of the need for classical channel authentication [63].
- All protocols need a key distillation process [64] to achieve a certain degree of security about the privacy of the distributed key, although as we have mentioned this process can reduce the size of the key so much that the protocol itself must be applied recursively until the preset key-size is reached.
- Fiber optic cabling for terrestrial implementations of QKD requires quantum repeaters every certain number of kilometers [65], which in turn requires an important amount of quantum

memory. The problem is that the key is exposed in its passage through them. There are currently two well-defined lines of research, the first has to do with the development of quantum repeaters that do not require quantum memory, at least not that much, and the second is to replace the same quantum repeaters with some type of implementation based on quantum teleportation [66].

**2.3. Issues with space-to-ground and ground-to-space QKD implementation**

To the common problems of any implementation of a QKD protocol, we must add those that arise when including a satellite that transmits photons to Earth into the equation. As a direct consequence of this, the so-called beam effects appear [67], which generate low-performance problems [68]. Consequently, the protocols are subject to transmittance problems [69], that is, the photons that are emitted by the satellite toward the Earth cannot compete with the sun when its beams reach the lens of the optical ground station (OGS) telescope. Therefore, the system can only be operational at night, as long as it is a clear night (without clouds) and preferably the OGS is located in an area with a low level of atmospheric pollution.

The atmospheric effects make it necessary to take into account the ephemeris and climatic considerations with strong seasonal and time limitations, which is essential for the modestly successful delivery of the key [67]. In addition, geographical aspects must be considered, for example, in Saudi Arabia, there are five types of dust, which means that in the event of a storm, the OGS must have positive pressure so as not to let the dust enter the delicate optical instruments, even when the OGS radome is closed.

Some of these problems were faced by the Chinese mission Quantum Experiments at Space Scale (QUESS) or Micius [70] between 2016 and 2018. In cases like the previous one, to all the difficulties mentioned, we must add the use of a double optic with an object of distributing entangled photons to two points on Earth at the same time, which forces several demanding design decisions:

- a higher orbit vs. an increase of the angle between both optics, due to the geometry of the simultaneous ground focusing, and
- a double optics vs. simple optics, although in the latter case at the cost of a heavy use of quantum memory.

This strongly conditions the type of experiments that can be carried out with the platform, because if the satellite has double optics, then it is possible to carry out teleportations between two points on Earth while the satellite is a mere distributor of entangled photons. On the other hand, if the satellite has a single optic, it is more convenient to carry out teleportations between a point on Earth and the satellite so that the quantum memory is found in the OGS. In that case, it is the OGS that emits an entangled photon of each pair to the satellite and keeps the others. Teleportation in the opposite direction would imply that the satellite would emit one photon of each entangled pair to Earth and keep the other in onboard quantum memory, implying a significant impact on the cost, size, and complexity of the platform.

On the other hand, like their terrestrial counterparts, QKD protocol implementations thanks to the use of satellites deal with the need to use classical and quantum channels [71]. Moreover, we must consider the impossibility of distributing the keys underwater [72] in the case of submerged submarines, the problems associated with different configurations of satellite repeaters [73], and severe climatic factors such as climate change and associated droughts, which involve smoke caused by fires that require the use of intermediate relays between the satellite and the OGS through the intervention of drones [74, 75]. These operational difficulties of the satellites involved in QKD protocols have given rise to a recent trend consisting of replacing the satellites directly with drones, which, by flying much closer to the OGS, avoids several of the problems mentioned above [76].

As mentioned above, all QKD satellites share many problems with strictly terrestrial setups. One of the most complicated lies in the small final size of the key after successive distillations to ensure the privacy of the key, i.e., only reserved for Alice and Bob, and no one else. To reach the pre-established key size, successive applications of the protocol are required, which in this context translates into successive orbits of the satellite, taking into account all the drawbacks mentioned above. However, a QKD satellite has serious problems of its own [54, 77, 78]. Among these problems, the need for synchronization of the protocol between both recipient points of the key distribution through the

Global Positioning System (GPS) stands out. This means that if the QKD configuration is used during a conflict by the government or the armed forces and the GPS satellite network is intervened, interrupted, or attacked by the adversary, the QKD satellite procedure is automatically out of service.

We must also take into account a serious problem that affects the link between the satellite and the OGS, or every QKD satellite itself, and that is satellite espionage, i.e., problems affecting the physical security of the satellite. In this regard we must mention:

- man-in-the-middle attacks that try to intervene in the link between the satellite and the OGS [79],
- the existence of tarantula-type satellites with prehensile extremities [80], which would allow the QKD satellite to be physically seized, thereby automatically interrupting the service, and which would lead to the acquisition by the adversary of the key history and part of the QKD protocol with its eventual innovations in that particular implementation,
- the presence of passive spy satellites [81], which are positioned in the proximity of the QKD satellite to listen to any signal coming from it, and
- the presence of active spy satellites [82], which try to stealthily modify (emulating a failure) the satellite's telemetry and orbit so that it is lost or incinerated by re-entering the atmosphere.

Finally, we must mention the damage caused by the presence of so many satellites around the Earth, some in configurations of 300 or more units, generally in Low Earth Orbit (LEO) at approximately 500 km altitude, i.e., in this context the satellites are the aggressors.

There are more than 8,000 satellites in orbit and countless pieces of space debris surround the planet [83-88]. The sky has become a veritable space dump. Therefore, it is not reasonable to continue to orbit constellations of hundreds of smallsats (CubeSats, PicoSats, and so on) in LEO, as this impedes the work of astronomers [89-93], who track asteroids, meteors, and comets on a collision course with Earth. In other words, the proliferation of the aforementioned satellite constellations conspires with the achievement of life on Earth as we know it. In addition, with this trend, one day soon Earth-based astronomy will die, so this important scientific discipline can only be carried out from orbiting platforms such as the Hubble Space Telescope, Web, and those that will inevitably have to be built soon. International Astronomical Union launched a new center to fight satellite mega-constellations threat [94]. This new center will coordinate work to mitigate the effect of satellite constellations on astronomy [95]. The main idea is the protection of the dark and quiet sky from satellite constellation interference [96]. The observatory of the Square Kilometer Array (SKA) and international partners petitioned Union Nations for the protection of Earth's dark and quiet skies [97].

Finally, given that satellites generally have a useful life, on average, of two to three years, a constant renewal of the satellite fleet of a mega-constellation is regularly required or else resort to a no less expensive method, consisting of orbiting robots, which could help fix and fuel satellites in space, i.e., machines will soon have a go at maintaining a fleet of small spacecraft orbiting Earth [98]. In other words, more satellites to assist other satellites, which would further aggravate the problem.

Although we have the vague feeling that this uncontrolled trend will one day cover the sun, one thing is certain, at this rate, it will not be long before the aforementioned constellations affect the departure of ships into space.

## 2.4. It is then required.

Based on what has been stated in this section, we conclude that to achieve a correct QBER level and overcome the difficulties of both QKD configurations (terrestrial and satellite), a system that shares keys must have the following attributes:

- It should not use satellites for QKD due to its problems, i.e., we establish a non-satellite criterion, where we avoid the use of additional satellites for QKD, even though IoT-fog-cloud is also a satellite,
- This does not require synchronization by GPS satellite constellation,
- This does not require authentication of the channels, in fact,
- This does not require quantum or classical channels,

- This does not require the distillation of keys,
- It does not require quantum memory,
- This does not require quantum repeaters,
- This does not have limitations of time, season, weather, or geographical conditions to share the key, and
- It is not subject to the action of hackers or eavesdroppers.

Therefore, if the current implementation of QKD configurations has so many complications, it is better to resort to a secure configuration, that is, one that incorporates the attributes mentioned above, and since it is about security, we consider that the technology proposed below (Non-distributable key sharing: NDKS) is the best option when it comes to sharing keys securely.

## 3. NON-DISTRIBUTABLE KEY SHARING (NDKS)

In addition to incorporating all the virtues exposed in Subsection 2.4, this technique must comply with a series of requirements when it comes to replacing the expensive, inefficient, and complicated terrestrial and space configurations of QKD. These requirements are:

- This technique must be able to be implemented in boxes, called NDKS units, which, when separated, can share a common symmetric key for encoding and decoding messages, in the sender and receiver, respectively. So that at the time of installation, both boxes start with a few common parameters and operators, which can be renewed (and which will be defined later in this section) as many times as desired, through secure transmission, where security is provided for the same boxes. NDKS units have the particularity of being able to share the same key regardless of the distance that separates them and without using any classical or quantum channel for this purpose. They can also work in a coordinated or synchronized way in configurations of more than two boxes, in fact, for any number of them.
- NDKS units act as if they are under the influence of a kind of virtual entanglement. If there were more than two NDKS units, then we would speak of a multi-virtual entanglement since it is as if the boxes shared an underlying reality, and when asking the boxes for a key (measurement), both would respond with a common result. (i.e., the collapse of a common virtual wave function). This is something similar to what happens when the Bell state $|B_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is measured for two NDKS units [99], or a Greenberger–Horne–Zeilinger state, for the case of 3 or more NDKS units virtually entangled, that is, $|GHZ_n\rangle$ [99]. In other words, the NDKS units reproduce or emulate the typical behavior of quantum mechanics [9] even though they are strictly classical entities. After all, even in QKD, the shared key to be used is ultimately digital (classical).
- A configuration based on NDKS units should create a *caveat emptor* (information asymmetry). That is, a key easily shareable by the two or more NDKS units, but impossible to acquire or deduce by the eavesdropper. This implies the existence of a significant Entropy gradient between the NDKS units and the eavesdropper, with Entropy equal to 0 between the NDKS units, and Entropy equal to 1 for the eavesdropper. After all, the important thing is not that the key is more or less random, but that the adversary does not know it and cannot deduce it. Consequently, a configuration based on NDKS units does not require a chip for quantum random number generation (QRNG) [100] for its operation.
- An NDKS unit-based configuration uses sequential synchronization instead of time synchronization. In this way, even in the event of a failure of the channel that transmits the encrypted message, all the NDKS units maintain the order while waiting for the restoration of the service, keeping an exhaustive count of the sequence, and thus the lost message can be collated with the same key. For this, buffers and a frame composed of header and data are used, the same as the frames used by Internet Protocol (IP) datagrams. In this way, the communication can be asynchronous without altering the reconstruction of the total message. This positions the NDKS technology as an ideal tool to be used in Blockchain operations [101]. Moreover, the protocol itself is the architect of synchronization and order in bidirectional communication. In this way, the

operation of a configuration based on NDKS units does not require the clock of a constellation such as GPS for its synchronization, which is extremely convenient in the event of a possible attack or hacking of that satellite network in the event of a conflict.

- Taking into account that in its simplest operation each NDKS unit is directly associated with a computer (generally through a Universal Serial Bus - USB - port), they must be able to act in two well-defined modes:

    a) the sending computer interrogates its NDKS unit, and it answers with a key. The computer can use the key to encrypt the message using Vernam's ciphered [102] based on XOR (exclusive disjunction), or another. On the other side of the channel, the receiving computer interrogates its NDKS unit, which replies with the same key as the sender, then the computer will use that key to decrypt the message, and

    b) the sending computer sends the message to be encrypted to its NDKS unit, which returns it encrypted. The computer then transmits it over the channel to the receiving computer, which sends it to its own NDKS unit for decryption.

- The NDKS unit system does not preserve the link between the sender and receiver, nor the sender's or receiver's computers, not even the original message information, but only the encrypted message information, that is, the NDKS unit system is not a firewall, neither an antivirus software, nor an intrusion monitor, but simply a technology to encapsulate Information. In this regard, the NDKS drive system is 100% responsible for the integrity and security of the encapsulated (encrypted) data. But only about it.

- The NDKS units are essentially composed of nonlinear operators (they do not comply with the superposition principle), parameters, and independent and dependent variables. These operators will reproduce the same binary sequences if the parameters and variables have the same values. That is, it is a deterministic process between the NDKS units, but of apparent absolute randomness for the eavesdropper, which only sees a non-stationary and indecipherable sequence of zeros and ones, which constitute the encrypted message. This is what we referred to in a previous requirement when we mentioned the important entropic gradient.

- The nonlinear operators mentioned above have a very high sensitivity to the parameters and variables that compose them, i.e., a small change in one decimal of the parameters or variables will give rise to a completely different binary sequence (shared key).

- A cryptographic system based on NDKS units gives rise to dynamic encryption whereby each message and each symbol of the same message can be encrypted using a different key each time. In this way, we can encrypt the message using Vernam's [102] ciphered based on XOR, or another. Even if the message always consists of the same symbol, the NDKS units will assign it a completely different encoding each time, breaking the periodicity of the message. In this way, this cryptographic system is immune from any brute force attack, statistical analysis, pattern recognition, or disambiguation processes aimed at deciphering the key and with it the message. The statistic changes with each transmission, so the Entropy is practically fixed at 1 (one) during the entire cryptographic process.

**3.1. Two contexts in which to apply NDKS units.**

The first context in which the NDKS units can be applied has to do with a pure CyberSecurity process, that is, the protection of information and data integrity in a communication such as that represented in Fig. 2. The plain text enters the Gateway, which is linked to the NDKS unit under either of the two working modes explained above, that is, the Gateway requests a key from the NDKS unit and with it encrypts the message or sends the plain-text to the NDKS unit and the cipher-text is returned to it.

As we have repeatedly mentioned before, the applied coding can be of the Vernam [102] type or any other that the configuration designer considers more convenient.

In both modes of use, the NDKS units used do not protect the plain text both at the Gateway before the encryption process (at the sender) and after the decryption process at the receiver's Gateway. For this reason, the configuration must necessarily have firewalls on both sides of the channel to protect plain text while it is present.
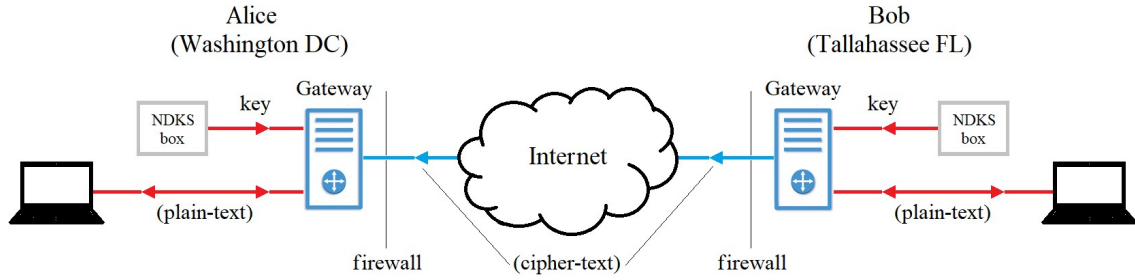
FIG. 2. NDKS units in a Cybersecurity context.

The second context alludes to the use of NDKS units in the particular case of an IoT configuration, such as the one in Fig. 3, where the Gateways are specifically linked through an IoT fog cloud. Figure 3(a) encrypts the plain signals coming from all the devices connected to this configuration and of which real-time monitoring is desired, as well as their control, while Fig. 3(b) shows they encrypt the plain commands coming from the user's computer to condition some parameter or variable of the aforementioned devices: revolutions per minute, temperature, humidity, light, and so on.
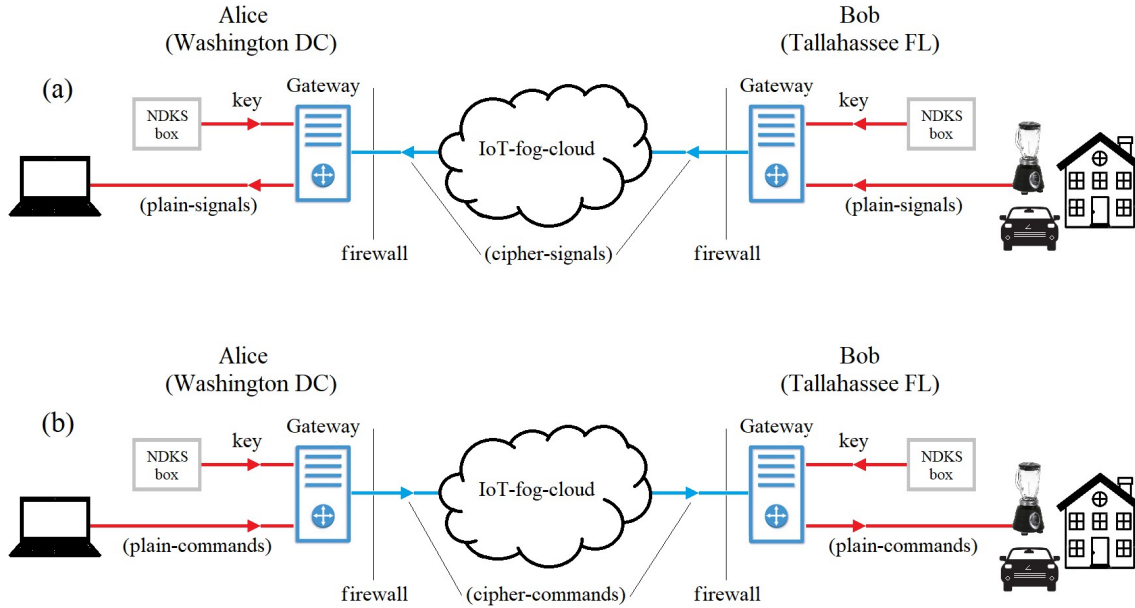


FIG. 3. NDKS units in an IoT context: a) Sensing, and b) Control.

Both monitoring and control can be carried out under the real-time, batch, and semi-batch modes, to use the IoT-fog-cloud when the connection service or the contracted rate is cheaper. In the case that concerns the physical security of tangibles, the real-time modality prevails over the other two, the same as in the case that sensed and controlled devices have to do with the field of defense and security since wrong or delayed command can trigger a conflict.

## 3.2. NDKS protocol

As we mentioned before, the NDKS units are based on a set of non-linear operators, which do not comply with the superposition principle, that is:

$$T(x+y) \neq T(x) + T(y), \text{ and} \tag{1a}$$

$$T(\alpha x) \neq \alpha T(x), \tag{1b}$$

where $T$ is the non-linear operator, $x$ and $y$ are the independent variables, while $\alpha$ is a parameter (constant). These operators are used in a composition of functions:

$$(g \circ f)(x) = g(f(x)), \tag{2}$$

where $D(g \circ f) = \{x \in D_f \ / \ f(x) \in D_g\}$, and $D(\bullet)$ means *domain of* "$\bullet$".

Then, the internal model of the NDKS units consists of a non-linear multidimensional system, which in its most generic form is:

$$y_1(k_1) = f_1\left(y_0, p_{1,1}, p_{1,2}, \ldots, p_{1,n_1}, k_1\right), \tag{3a}$$

$$y_2(k_2) = f_2\left(y_1, p_{2,1}, p_{2,2}, \ldots, p_{2,n_2}, k_2\right), \tag{3b}$$

$$\bullet \bullet \bullet$$

$$y_N(k_N) = f_N\left(y_{N-1}, p_{N,1}, p_{N,2}, \ldots, p_{N,n_N}, k_N\right). \tag{3N}$$

The composite function of this system of Eq.(3) is:

$$(f_1 \circ f_2 \circ \cdots \circ f_N)\left(k_1, k_2, \ldots, k_N, p_{1,1}, \ldots, p_{N,n_N}\right), \tag{4}$$

where $y_i$ are the dependent variables $\forall i$, with $y_0 = 0$, $p_{i,j}$ are the parameters of the system $\forall i, j$, and $k_i$ are the indices (independent variables) $\forall i$. A more practical case to be used in the NDKS units with the highest possible efficiency is:

$$y_1(k) = f_1(p_1, p_2, k), \tag{5a}$$

$$y_2(e) = f_2(y_1, e), \tag{5b}$$

$$y_3(e) = f_3(y_2, d), \tag{5c}$$

$$y_4(e) = f_4(y_3), \tag{5d}$$

where $p_1$ and $p_2$ are parameters, $k$ is the key index (independent variable), $y_1$, $y_2$, $y_3$, and $y_4$ are dependent variables, and $e$ is the index of the key element (independent variable). As we will see later, if $f_2$ is a function of the sinusoid type, then $f_1$ is its angular frequency dependent on the parameters $p_1$ and $p_2$, and the key index $k$. The composite function of this particular system is:

$$(f_1 \circ f_2 \circ f_3 \circ f_4)(k, e, d, p_1, p_2). \tag{6}$$

However, what does the independent variable $d$ represent? We will explain it with a concrete example. We generally use sinusoids in the case of the functions $f_1$ and $f_2$ because they are strongly non-linear functions with a module less than or equal to 1, therefore:

$$y_1(k) = |p_2 \ sin(p_1 \ k)|, \tag{7a}$$

$$y_2(e) = |cos(y_1(k) \ e)|, \tag{7b}$$

$$y_3(e) = numtovec\left(round\left(10^d \ y_2(e)\right)\right), \tag{7c}$$

$$y_4(e) = \left(1 + sign\left(y_3(e)/2 - floor\left(y_3(e)/2\right) - 1/4\right)\right)/2, \tag{7d}$$

where:

$y_1$ is a vector $/ k \in \mathbb{N}$ , specifically, *for k = 1 to number_of_keys* ,

$y_2$ is a vector $/ e \in \mathbb{N}^0$ , specifically, *for e = 0 to key_size-1* ,

$| \bullet |$ is the absolute value of "•",

*sin*(•) means *sine of* "•",

*cos*(•) means *cosine of* "•",

$y_3$ is a vector of *key-size* digits / each digit $\in [0,9]$,

*round*(•) means *round to the nearest integer of* "•",

*numtovec*(•) means *number* "•" *to vector,*

$y_4$ is a vector of *key-size* digits / each digit $\in [0,1]$. $y_4$ represents each key,

*floor*(•) gives as output the greatest integer less than or equal to "•", and

*sign*(•) extracts the sign of a real number "•".

Through a numerical example, that is, by giving values to the system of Eq. (7) we can better understand what *d* represents.

Suppose that $N = 10$, $e = 3$ (we must remember that $e$ can be any integer value from the interval $[0, 2^{N-1}]$), $p_1 = 0.52$, $p_2 = 25$, $k = 1$, and $d = 3$, thus:

$$y_1(1) = |25\,sin(0.52*1)| = 12.422003446093 \tag{8}$$

That is, $y_1(1)$ is the angular frequency of $y_2(3)$.

$$y_2(3) = |cos(12.422003446093*3)| = 0.907668453135977 \tag{9a}$$

$$y_3(3) = \begin{cases} 10^3 * 0.907668453135977 = 907.668453135977 \\ round(907.668453135977) = 908 \\ numtovec(908) = \begin{bmatrix} 9 & 0 & 8 \end{bmatrix} \end{cases} \tag{9b}$$

That is to say, *d* allows us to select the decimal with which to work.

$$y_4(3) = \begin{cases} lsd(908) = leo([9 \quad 0 \quad 8]) = 8 \\ (1 + sign(8/2 - floor(8/2) - 1/4))/2 = 0 \end{cases} \tag{10}$$

Where *lsd* means *less significative digit*, and *leo* means *last element of*, while the second line of $y_4(3)$ is equivalent to "*if 8 is even, then* $y_4(3) = 0$, *else* $y_4(3) = 1$".

Next, we generate some examples of keys to evaluate the high sensitivity of the system of Equation (7) with a slight variation of the parameters, which shows a great multiplier effect generating completely different keys with a small shift in the parameters.

For $N = 10$, *key-size* $= 2^{10} = 1024$, $k = 1$, $p_1 = 0.52$, $p_2 = 25$, and $d = 3$, the key is:

0010010100111110010000100111100110100010100101110100010010001100111101100111 0000
0100111010011100111111111110101000001011110010000110110001101100011011001111111111
0000000010100101111001000100011110000000110111001010101000110001001100100100010110
1001001000110111100000100010001001100100101100001000011100100111001110011001111101
0001110100011101010110010001111100110100111100001110000000100011011011110000001000
1000001100111001111001100101011110011111001001110010111010000111010110010101010010
0100000110111011000010010001011110110010111110001000110001011100111101100010010010
0101101001001111000110110100101100010110000111110000000001000100010000111100001110

0011111011110101001000100110101100010011111000100001000001110001001110101000010010
1110011001000111001100100011010111001100011101000100011010100110110000111001111000
1010000010011011001000011000011101000000011000111100011111110101111011110101100000
1101110110000001101101000000001011101111001000001000010010101010000111110000000100
0101011111100011101001010110001001001101.

For $N = 10$, $key\text{-}size = 2^{10} = 1024$, $k = 1$, $p_1 = 0.52001$, $p_2 = 25$, and $d = 3$, the key is:
0010011100110110110011010101010111011011110001010101100011100100000101000011100001
1001100100000010001000001000011000110011111101000010011001011101100011110011001001
0111111100111000100110100001111100000010010000100111011000011011000110100111011110
1110011101111100010011110001111110001011101111011100100110100111011110100100101101
0010111111001101111101110100100000111101001110111000110110110011101000010011000
1101100101110110110100010100010010101110010000011111001010000001110100000100100001
0001100101010110110100111101001100111001111111110110011100000100111100001010001111
0000011101001011011011110010000101100101001011010000110011101000101111100110111010
0111000010110001010010001101100011000101010000110010001101010000101000001111001100
0101001010100110010010110100111111010001001000001010100101111000110000101100110101
1110011000011011110110111011111100001101000011000001010001001101010001001110111000111
0111000000000110000100010111100011110000100101011011000001000011000110000011011
1110101101110000101010111000111000000011010.

For $N = 10$, $key\text{-}size = 2^{10} = 1024$, $k = 2$, $p_1 = 0.52$, $p_2 = 25$, and $d = 3$, the key is:
0110100010110011001001010001100011110111101110010110010111101111111011000100001
1111100010011100010110011110100101001010100110010011010100111111001010110001110110
0111111111100100110100011111110100100001011111111001011110011110111111111011101001
1011000000110101001100100100010100110111001010100101110101000011001101111111010100
1100101010010110010111110010000000110101001100000001000101011101001010010000001010
0101000011110001100110011111101000100011001110111010000101000111101101110011101111
1000100100100100110110011100011011111111101010101110001001010010101011111110100110100000
0000010000000100100010001000000000010111100100000110101010000010100011011000111000
1100101111100011011001111111100111110110001011111100100110100011100001010010111111
1101010001000110100111001100010110010110001100011110000000100100001100111001101000
0001000110100000111101000111010010001101000111000111100101000101100110010110010001
0011001000000100000111010010100001101000111010000000011001001011001111100001001100
0101100100110001011101000011001111100011111.

These were just a few simple examples that show the sensitivity to the parameters that the operators used have, in such a way that changing the decimals of those parameters a little completely changes the binary sequence, that is, the key.

Other nonlinear functions that can be applied as operators instead of the sinusoidal ones of the previous numerical examples can be polynomial, hyperbolic, and so on type functions.

Specifically, the nonlinearity of the operators is due to two reasons:

- the aforementioned amplification factor, and
- simple functions generate non-ergodic binary sequences.

Finally, with these examples, we have verified most of the slogans raised above.

## 4. DISCUSSION

In this section, we will develop two important topics related to this technology:

- the testing and homologation protocol, without which approval this technology cannot be commercialized, and
- the context analysis, whose purpose is to compare this technology with others of classical and quantum cryptography, in general, and QKD, in particular, and finally give it ubiquity from as many points of view as possible, i.e., economic, financial, political, manpower necessary to its implementation, and so on.

**4.1. Testing and homologation protocol**

The testing and homologation protocol of the NDKS system units consists of two main stages:

- No-Channel key sharing, and
- Encrypted communication via regular channels.

*4.1.1. No-Channel key sharing:*

With both laptops in Fig. 4 completely disconnected from Wi-Fi, Bluetooth, and any type of cable that connects them to a LAN, WAN, or Internet net, both laptops interrogate their respective NDKS unit about a key. That is, the key is exchanged instantly without any channel intervention. The Faraday's cages prevent the intervention of any external channel, such as Wi-Fi, Bluetooth, and so on. In other words, both laptops can only share the same key exclusively using the NDKS units. Then, the sending laptop encrypts the original message with the key obtained from its NDKS drive and deletes the original message, keeping only the encrypted message.
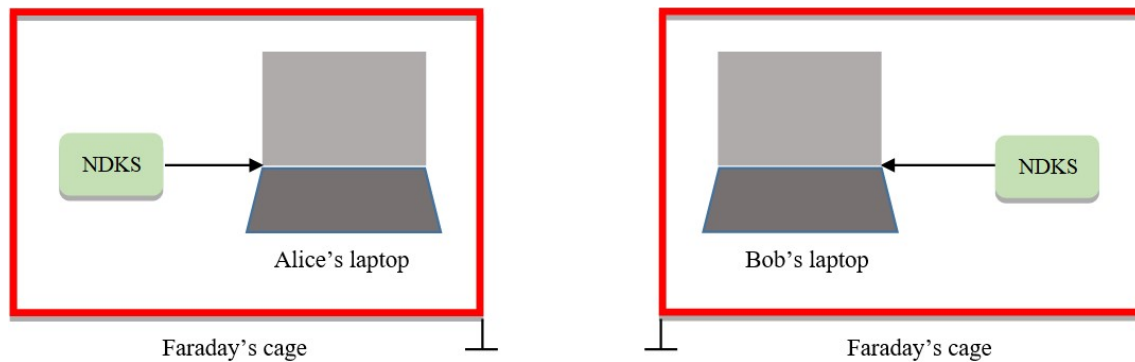


FIG. 4. No-Channel key sharing.

*4.1.2. Encrypted communication via regular channels:*

Based on Fig. 5, both laptops get rid of their respective Faraday cages and then connect to the same channel (e.g., the Wi-Fi network of the office where the test is performed). In this instance, hackers also connect to the same network, which will try to decipher the encrypted message that will be transmitted. Thus, the hackathon begins. The sending laptop transmits the encrypted message. Once the receiving laptop receives the complete encrypted message, it disconnects from the Wi-Fi network, Bluetooth, and all types of network cables that connect it to a LAN, WAN, Internet, etc. The receiving laptop then decodes the encrypted message using the key provided by its NDKS unit.

A recognized and independent expert verifies that the message originally written by the sender (Alice) from her laptop matches the one decoded by the recipient's (Bob) laptop. The expert questions the hackers about the message that they may have decoded during the transmission of the encrypted message. The expert renders his verdict.

The roles of Alice as sender and Bob as receiver are permanently swapped seamlessly and without the intervention of any special or additional switching system. The protocol is completely bidirectional. An NDKS configuration is a symmetric key technology that facilitates all operations related to bi-directionality.

These tests are of paramount importance since the NDKS protocol was originally developed to make use of a non-own (hostile) channel.

If the result of the hackathon is successful (positive verdict), the NDKS units are approved for subsequent sale. Finally, this protocol and, in consequence, the NDKS units have been designed taking into account the following considerations:
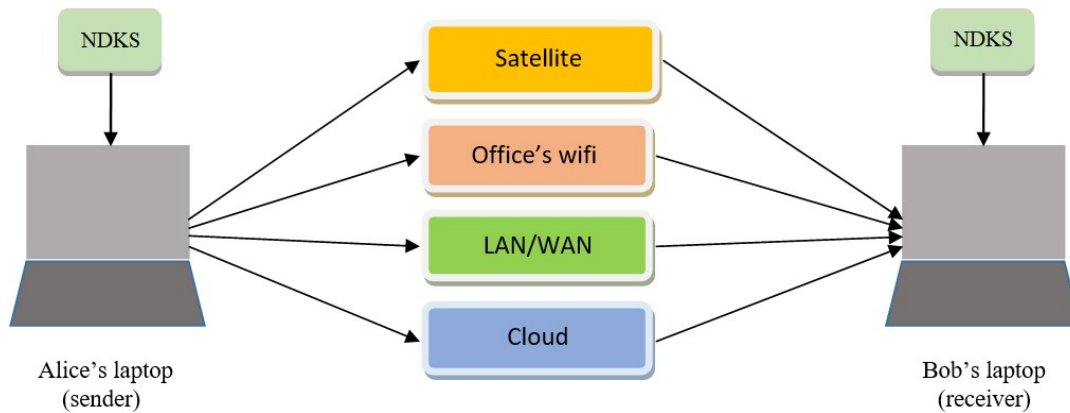
FIG. 5. Encrypted communication via regular channels.

- they can be connected to the laptop through one of its external USB ports, or internally in any slot of it, although that slot should not have any type of port that links it to the outside,
- the information that goes out and enters the NDKS units is organized in a frame structure with a header and data, which is encrypted,
- if one of the NDKS units is stolen, it will not be able to connect to a new laptop since the NDKS units share a sync word within the frame structure, which results from a recognition procedure of the physical characteristics of the laptop from which was stolen, as well as the characteristics of the network where the laptop was,
- the aforementioned synchronism word is renewed in each transmission and is encrypted within the frame,
- if an NDKS unit is opened, its contents will automatically be erased, so these units are built like a bomb,
- in any network of NDKS units, one of them will act as master and the rest as slaves, where these roles can be changed automatically at any time in a transparent way to the users if the master is stolen, opened, or destroyed,
- any new NDKS unit can be incorporated into the network at any time by simply requesting permission from the NDKS unit network administrator, privately sending through an alternative channel the physical data of the laptop and the characteristics of the network in which the latter will be connected, then the administrator will consult with the competent authority if that incorporation is scheduled. In a positive case, the master will send a synchronization signal to the entire network within the encrypted frame to put them all in an entanglement state,
- this technology should prevent the government from applying an "Internet kill switch" in case the network of networks is attacked,
- NDKS units use dynamic encryption, where the key can change even for each symbol of the same message,
- regularly it can be verified by an alternative channel if Bob decrypts what Alice encrypted, and employs a confinement procedure whereby all the units of the network are gathered in the same place, to discern if an eventual error found is due to the NDKS units or due to noise on the transmission channel,
- the keys generated by the NDKS units must not show regular patterns. This was verified by the developed examples,
- the NDKS unit that transmits is the one that generates and emits a synchronization signal inside the encrypted frame,
- the configuration can also be programmed so that the network master of the NDKS units is the unit that transmits, for which the administrator role is in a permanent relay state unless the network is used to collect data from a device with no intention of emitting any control signals, that is, a pure and exclusive monitoring state,

- NDKS units recognize three possible states at a low level: 0 (zero), 1 (one), and nothing (absence of information), so that when nothing is transmitted, pure coded zeros are not used, because in that case if the encryption is of the Vernam's type, keys that are not used to encrypt useful information would travel through the channel, that is, keys would be wasted unnecessarily,

- NDKS units can use any type of encryption technique, in such a way that if we want the key to have the same length in bits as the message to be encrypted, then we can use Vernam's ciphered (XOR). Instead, if the key is of a smaller length in bits than the message to be encrypted, a unifying file will then be used, which can be the result of a folder containing all kinds of audio, image, video, and text files, and

- as the operators used by the NDKS units are non-linear, the eavesdropper sees the keys as having random characteristics and resulting from an apparent probabilistic or stochastic source. This happens because the hacker does not understand (i.e., does not know) the underlying law behind the generation of the key, but we know that it is a 100% reproducible process (because otherwise, the network of NDKS units would not work), because we know the generating law. So, what are the keys random for? It is evident that if we do not know the laws that govern the universe, its behavior will be indecipherable to us. On the other hand, if we know them, they will be harmonic and elegant. This is what we mean when we talk about *caveat emptor* (information asymmetry).

## 4.2. Context analysis

In this subsection, two comparative tables are presented to give ubiquity in the current international context to the technology of the NDKS units. Table 1 presents a comparison between NDKS technology versus ground and space versions of QKD. The evidence contained in this table is overwhelming in favor of the technology of the NDKS units from every point of view, i.e., technological, financial, etc. Moreover, Table 2 consists of a comparison between NDKS technology and the Chinese mission QUESS/Micius [103]. In the penultimate row of Table 1, we mention an especially important item, the "legal procedures", among which we mention certain tests. Those tests are required by the launcher as a *sine-qua-non* condition to embark on the satellite unit. These tests are:

- *Vibration testing on a shaker:* This test tries to reproduce the vibrations that the satellite will suffer at the time of liftoff from the launcher.

- *Calibration and testing:* These tests refer to the evaluation of electronics and optical components, batteries, etc.

- *Vacuum and thermal cycling test:* This test studies the response of the satellite and its components against a thermal gradient in space with more than 200 ºC of thermal amplitude, which happens when the sun is absent and present at those times as a consequence of the orbit of the satellite around the Earth.

- *CubeSat attitude determination and Helmholtz cage design:* A Helmholtz cage is designed, built, and tested to provide a dynamic, 3-axis, uniform magnetic field to cancel the Earth's magnetic field and create an environment similar to the geomagnetic field a satellite would experience on-orbit.

- *Impact test:* This test concerns the mechanical response of the satellite and its components.

- *Radio-frequency (RF), electromagnetic compatibility (EMI/EMC), or anechoic chamber:* EMC tests such as Radiated Emission and Radiated Immunity are applied in a room with isolated electromagnetic signals. EMC (or anechoic) chambers are designed to create an enclosure with an extremely high level of shielding attenuation against electromagnetic interference. The idea is to study the radiation emitted by and/or radiated immunity of the satellite.

Comparisons complementary to those of the tables of an extremely heterogeneous nature are:

- *Launch cost:* Millions of dollars (due to the size and weight of the Micius satellite) vs. $0 for NDKS units,

**Table 1.** Comparison between NDKS technology and the ground and space versions of QKD.

| Attribute | Ground QKD | Space QKD | NDKS |
|---|---|---|---|
| Dynamic vs. static coding[1] | static | static | dynamic |
| Key-size in bits | small after-distillation (less than desired) | small after-distillation (less than desired) | unlimited |
| Control over final key-size | No | No | Yes |
| Number of keys generated during each operating cycle | less than one[2] | less than one | unlimited |
| Infrastructure need | Yes | Yes | No |
| Manpower | Highly qualified | Highly qualified | Low skilled |
| Maintenance need | Yes | Yes | No |
| Startup cost | Very high | Very high | Null |
| Legal procedures[3] | Too many | Too many | None |
| Contractors need | Yes | Yes | No |

Where:
1. This point refers to working with a single key or if it changes with each message or symbol of each message as the NDKS units do.
2. This is because the distillation process (to ensure that the eavesdropper does not share portions of the final key with us) of the key can leave it smaller than desired.
3. This implies building permits (channeling and fiber optic laying), tests (in the case of the space version) without which the satellite cannot be uploaded to the launcher, etc.

**Table 2.** Comparison between NDKS technology and the Chinese mission QUESS/Micius.

| Parameters | QUESS/Micius [103] | NDKS units |
|---|---|---|
| Origin | China | USA |
| Construction time | 10 years | less than an hour |
| Weight | 631 kg | 250 g |
| Useful life | 2 years | *in eternum* |
| Orbit | 488-584 km | 0 km |
| Launch year | 2016 | 2022 |
| Primal key[4] | 300,000 bits | 192,000,000 bits |
| Efficiency[5] | At night, without clouds and with low pollution (much less than 100%) | 100% |
| Final cost | $ 100 M | $ 34/unit |

Where:
4. NDKS units can generate even larger keys and deliver them complete or in single bits (as streaming of ones and zeros) in order not to saturate the internal memory of these units.
5. This refers to the impossibility of competing with the sun and the transmittance due to atmospheric and meteorological conditions.

- *Number of satellites:* Micius program has three to date, although the first one has not been in service since 2018 (two new ones are in service) vs. none by NDKS technology, and
- *Required Manpower:* Highly skilled for Micius, while in the case of NDKS units, these can be assembled by personnel without any specific specialization.

Moreover, although similar products are promoted for key delivery [104], which, however, are based on QKD technology, we must understand that, unlike the NDKS units, the aforementioned products require the typical channels of a QKD protocol to carry out the key sharing, that is, they need a classical channel and a quantum channel to be able to carry out the distribution of the aforementioned keys.

Another outstanding aspect of NDKS technology is that it is fully compatible with internationally established Cybersecurity standards, even in the most specific aspects, such as the ISO/IEC 27001 Standard: Information Security Management [105], or that of the International Association of Classification Societies (IACS), specifically regarding the recommendation on cyber resilience [106].

On the other hand, no matter how spectacular laser links are tested among satellites, airplanes, ships, and ground stations [107], these links can only be effective at night, with good weather and low pollution levels, unless the link is used only between satellites or between the same and a spacecraft leaving the Earth's atmosphere. These problems are largely overcome by the technology of the NDKS units.

Finally, as it is a dynamic encryption technology, that is, where the key changes with each message or with each symbol of the same, the NDKS units are completely immune from attacks such as those that can break an 8-character password in less than an hour [108]. Even in the case of 8-bit passwords, since it is dynamic encryption, the NDKS units make the keys change with each symbol of the message, making it impossible for a hacker to act.

## 5. CONCLUSIONS

The technology provided by the NDKS units has demonstrated to dispense with the main elements that make the implementations of the QKD protocols work, that is, the technology presented in this work has the following attributes:
- This does not require a QKD satellite with all its problems,
- this does not require synchronization via a GPS satellite network,
- this does not require authentication of the channels for the delivery of the keys, since it simply does not use them for that purpose,
- this requires no key distilling, so the key is always the expected size even on the first try,
- it does not require quantum memory,
- this does not require quantum repeaters, so the key is never exposed during its passage through them as it happens in terrestrial implementations of QKD,
- this does not require a quantum or classical channel for key distribution,
- it does not have time limitations to share the key, nor do they depend on the weather or the pollution of the environment,
- this does not force a denial of service,
- this requires minimal cost and implementation time,
- in this technology, a great multiplier effect takes place since the system of Eqs. (5) is extravagantly sensitive to the slightest change in any decimal, which will trigger a large variation in the key, without the need to resort to complex random configurations, that is, within a pure deterministic framework,
- it is not subject to the action of hackers or eavesdroppers, and,
- this does not depend on many other factors without which a cryptographic implementation based on QKD could work.

Reasons like these, and many others, make the technology of the NDKS units the chosen one when it comes to providing maximum security to sensitive communication channels (Government, Defense, Fintech, and so on) compared to their competitors, i.e., terrestrial and satellite QKD implementations.

## Declarations

## References

1. Alam M, Shakil KA, Khan S Eds. (2020) Internet of Things (IoT): Concepts and Applications. Springer Nature, Switzerland AG.
2. Greengard S (2015) The Internet of Things. The MIT Press, Boston.
3. daCosta F (2013) Rethinking the Internet of Things: A Scalable Approach to Connecting Everything. Apress Open, Santa Clara Ca.

4.  Soldatos J Eds. (2017) Building Blocks for IoT Analytics: Internet-of-Things Analytics. River Publishers, Denmark.
5.  Mahmud R, Scirama SN, Ramamohanarao K, Buyya R (2020) Profit-aware application placement for integrated Fog–Cloud computing environments. J. Parallel Distrib. Comput. 135: 177–190.
6.  Mohan N, Kangasharju J (2016) Edge-Fog Cloud: A Distributed Cloud for Internet of Things Computations. Cloudification of the Internet of Things (CIoT), pp. 1-6.
7.  Souza VBC, Ramírez W, Masip-Bruin X, Marín-Tordera E, Ren G, Tashakor G (2016) Handling Service Allocation in Combined Fog-Cloud Scenarios, In 2016 IEEE International Conference on Communications (ICC), pp. 1-5.
8.  Kallel A, Rekik M, Khemakhem MA (2021) IoT-fog-cloud based architecture for smart systems: Prototypes of autism and COVID-19 monitoring systems, Wiley, Softw: Pract Exper. 51:91–116.
9.  Phillips AC (2003) Introduction to Quantum Mechanics. Wiley, Chichester, UK.
10. Kollmitzer C, Pivk M Eds. (2010) Applied Quantum Cryptography. Springer-Verlag, Heidelberg.
11. Cariolaro G (2015) Quantum Communications: Signals and Communication Technology, Springer, Switzerland.
12. Caleffi M, Caleffi M, Chandra D, Cuomo D, Hassanpour S, Cacciapuoti AS (2020) The rise of the quantum Internet. Computer. 53(06), 67–72.
13. Cacciapuoti AS, Caleffi M, Cataliotti FS, Gherardini S, Tafuri F, Bianchi G (2020) The quantum Internet: Networking challenges in distributed quantum computing. IEEE Netw. 34(1), 137–143.
14. Cacciapuoti A S, Caleffi M, Van Meter R, Hanzo L (2020) When Entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet, IEEE Trans. on Comm. 68(6), 3808-3833.
15. Gyongyosi L, Imre S (2020) Entanglement accessibility measures for the quantum Internet. Quant. Inf. Proc. 19, 115.
16. Gyongyosi L, Imre S (2019) Entanglement access control for the quantum Internet. Quantum Inf Process. 18, 107.
17. Gyongyosi L, Imre S (2019) Opportunistic Entanglement Distribution for the Quantum Internet. Sci Rep, 9, 2219.
18. Hiskett PA, Rosenberg D, Peterson CG, Hughes RJ (2006) Long-distance quantum key distribution in optical fibre, New J. Phys. 8, 193.
19. Ruihong Q, Ying M (2019) Research progress of quantum repeaters. IOP J. Phys. Conf. Ser. 1237, 052032.
20. Polnik M, Mazzarella L, Di Carlo M, Oi DKL, Riccardi A, Arulselvan A (2020) Scheduling of space to ground quantum key distribution, EPJ Quantum Technology, 7, 3.
21. Bedington R, Arrazola JM, Ling A (2017) Progress in satellite quantum key distribution, npj Quantum Information, 3, 30.
22. Ntanos A, Lyras NK, Zavitsanos D, Giannoulis G, Panagopoulos AD, Avramopoulos H (2021) LEO Satellites Constellation-to-Ground QKD Links: Greek Quantum Communication Infrastructure Paradigm, Photonics, 8, 544.
23. Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, Yin J, Shen Q, Cao Y, Li ZP, Li FZ, Chen XW, Sun LH, Jia JJ, Wu JC, Jiang XJ, Wang JF, Huang YM, Wang Q, Zhou YL, Deng L, Xi T, Ma L, Hu T, Pan JW (2017) Satellite-to-ground quantum key distribution, Nature, 549, 43-49.
24. Bennett CH, Brassard G (1984) Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179.
25. Ekert AK (1991) Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67(6) 661–663.
26. Bennett CH (1992) Quantum cryptography using any two non-orthogonal states, Phys. Rev. Lett. 68(21), 3121-3124.
27. NSA: Quantum key distribution (QKD) and quantum cryptography QC. Available online: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (Accessed 03/05/2022)
28. Sharma, V., Padakandla, A. Quantum Error Correction and Quantum Information Theory (2020). https://ece.iisc.ac.in/~spcom/2020/Slides/TutorSPCOM2020_QECC&QCryptographyQIT_Final.pdf (Accessed 03/07/2022)
29. Mink A, Sheila F, Ray P (2019) Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration, Intern. J. Network Security & Its Applic. 1(2), 101-112.

30. Benenti G, Casati G, Strini G (2008) Principles of Quantum Computation and Information I: Volume I: Basic Concepts. World Scientific, Singapore.
31. Zhou RG, Zhang X (2021) Controlled deterministic secure semi-quantum communication. Intern. J. Theo. Phys. 60(5), 1767-1782.
32. Kravtsov KS, Radchenko IV, Kulik SP, Molotkov SN (2018) Relativistic quantum key distribution system with one-way quantum communication. Sci Rep. 8(1), 1-7.
33. Bruß D, Lütkenhaus N (2999) Quantum Key Distribution: from Principles to Practicalities: A review. arXiv preprint arXiv:9901061.
34. Makarov V, Anisimov A, Skaar J (2006) Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys. Rev. A 74(2), 022313.
35. Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V (2010) Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics. 4(10), 686.
36. Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C, Ma Z, Makarov V (2011) Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Communications. 2, 349.
37. Qi B, Fung CHF, Lo HK, Ma X (2005) Time-shift attack in practical quantum cryptosystems: A review. arXiv preprint, arXiv:0512080.
38. Weier H, Krauss H, Rau M, Fürst M, Nauerth S, Weinfurter H (2011) Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. New J. Phys. 13(7), 073024.
39. Bugge AN, Sauge S, Mardhiyah A, Ghazali M, Skaar J, Lydersen L, Makarov V (2014) Laser damage helps the eavesdropper in quantum cryptography. Phys. Rev. Lett. 112(7), 070503.
40. Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G (2006) Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A. 73(2), 022320.
41. Li HW, Wang S, Huang JZ, Chen W, Yin ZQ, Li FY, Zhou Z, Liu D, Zhang Y, Guo GC, Bao WS, Han ZF (2011) Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. Phys. Rev. A. 84(6), 062308.
42. Diamanti E (2006) Security and implementation of differential phase shift quantum key distribution systems. Ph.D. Thesis, CNRS.
43. Holevo AS (1973) Bounds for the quantity of information transmitted by a quantum communication channel, Problemy Peredachi Informatsii. 9(3), 3-11.
44. Fiurasek J (2003) Optical implementations of the optimal phase-covariant quantum cloning machine. Phys. Rev. A. 67(5), 052314.
45. Niederberger A, Scarani V, Gisin N (2005) Photon-Number-Splitting versus Cloning Attacks in Practical Implementations of the Bennett-Brassard 1984 protocol for Quantum Cryptography. arXiv preprint arXiv:0408122.
46. Reiserer A, Ritter S, Rempe G (2013) Nondestructive detection of an optical photon. Science. 1246164.
47. Nogues G, Rauschenbeutel A, Osnaghi S, Brune M, Raimond JM, Haroche S (1999) Seeing a single photon without destroying it. Nature. 400, pp. 6741, 239.
48. Hwang WY (2003) Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. 91(5), 057901.
49. Lucamarini M, Shields A, Alléaume R, Chunnilall C, Degiovanni IP, Gramegna M, Hasekioglu A, Huttner B, Lord A, Kumar R, Lütkenhaus N, Makarov V, Martin V, Mink A, Peev M, Sasaki M, Sinclair A, Spiller T, Ward M, White C, Yuan Z (2018) ETSI White Paper No. 27, Implementation Security of Quantum Cryptography: Introduction, challenges, solutions.
50. Tsai CW, Yang CW, Lin J, Chang YC, Chang RS (2021) Quantum Key Distribution Networks: Challenges and Future Research Issues in Security. Appl. Sci. 11, 3767.
51. Lo HK, Curty M, Tamaki K (2014) Secure quantum key distribution. Nature Photonics. 8, pp. 595-604.
52. Lu FY (2019) Practical issues of twin-field quantum key distribution. New J. Phys. 21, 123030.
53. Diamanti E, Lo HK, Oi B, Yuan Z (2016) Practical challenges in quantum key distribution. npj Quantum Information. 2, 16025.
54. Zhang Q, Xu F, Chen YA, Peng CZ, Pan JW (2018) Large scale quantum key distribution: challenges and solutions. Opt. Express. 26, pp. 24260-24273.
55. Lopez-Leyva JA, Talamantes-Alvarez A, Ponce-Camacho MA, Garcia-Cardenas E, Alvarez-Guzman E (2019) Quantum Cryptography in Advanced Networks, Morozov, O.G. (Eds.), Chapter: Free-Space-Optical Quantum Key Distribution Systems: Challenges and Trends, IntechOpen.

56. Fung CHF, Ma X, Chau HF (2009) Practical issues in quantum-key-distribution post-processing: A review. arXiv preprint, arXiv:0910.0312.

57. Zhao Y, Fung CHF, Qi B, Chen C, Lo HK (2011) Quantum hacking: experimental demonstration of time-shift attack against practical quantum key distribution systems: A review. arXiv preprint, arXiv:0704.3253.

58. Lovic V (2020) Quantum Key Distribution: Advantages, Challenges, and Policy. Cambridge Journal of Science & Policy. 1, 2.

59. Bacco D, Da Lio B, Cozzolino D, Da Ros F, Guo X, Ding Y, Sasaki Y, Aikawa K, Miki S, Terai H, Yamashita T, Neergaard-Nielsen JS, Galili M, Rottwitt K, Andersen K, Morioka T, Oxenløwe LK (2019) Boosting the secret key rate in a shared quantum and classical fibre communication system. Comm. Phys. 2, 140.

60. Aliro: Quantum network security: What is Quantum Key Distribution (QKD)? Available online: https://www.aliroquantum.com/blog/quantum-network-security-what-is-quantum-key-distribution-qkd?hsLang=en (Accessed on 02/25/2022).

61. Tajima A, Kondoh T, Ochi T, Fujiwara M, Yoshino K, Iizuka H, Sakamoto T, Tomita A, Shimamura E, Asami S, Sasaki M (2017) Quantum key distribution network for multiple applications. Quantum Sci. Technol. 2, 034003.

62. Agnesi C, Avesani M, Calderaro L, Stanco A, Foletto G, Zahidy M, Scriminich A, Vedovato F, Vallone G, Villoresi P (2020) Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder. Optica. 7(4), 284-290.

63. Price AB (2020) A quantum key distribution protocol for rapid denial of service detection, EPJ Quantum Technol. 7, 8.

64. Sasaki M (2018) Quantum Key Distribution and Its Applications. IEEE Security & Privacy. 16(5), 42-48.

65. Mehic M, Niemiec M, Rass S, Ma J, Peev M, Aguado A, Martin V, Schauer S, Poppe A, Pacher C, Voznak M (2020) Quantum Key Distribution: A Networking Perspective. ACM Computing Surveys. 53(5), 96.

66. Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK (1993) Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. 70(13), 1895–1899.

67. Liorni C, Kampermann H, Bruß D (2019) Satellite-based links for quantum key distribution: beam effects and weather dependence. New J. Phys. 21, 093055.

68. Zhao B, Zha X, Chen Z, Shi R, Wang R, Peng T, Yan L (2020) Performance Analysis of Quantum Key Distribution Technology for Power Business. Appl. Sci. 10, 2906.

69. Mastriani M (2023) Entanglement parallelization via quantum Fourier transform. arXiv preprint, arXiv:2302.12015.

70. Yin J, Li YH, Liao SK, Yang M, Cao Y, Zhang L, Ren JG, Cai WQ, Liu WY, Li SL, Shu R, Huang YM, Deng L, Li L, Zhang Q, Liu NL, Chen YA, Lu CY, Wang XB, Xu F, Wang JY, Peng CZ, Ekert AK, Pan JW (2020) Entanglement-based secure quantum cryptography over 1,120 kilometers. Nature. 582, pp. 501–505.

71. Sergienko AV (2006) Quantum communications and cryptography. CRC Taylor & Frances, Boca Raton.

72. Mastriani M, Iyengar SS, Latesh Kumar KJ (2021) Bidirectional teleportation for underwater quantum communications, Quantum Inf. Proce. 20, 22.

73. Mastriani M, Iyengar SS (2020) Satellite quantum repeaters for a quantum Internet. Wiley, Quantum Engineering, QUE55.

74. Liu H, Tian XH, Gu C (2020) Drone-based entanglement distribution towards mobile quantum networks. Nat. Sci. Rev. 7, pp. 921–928.

75. Mastriani M, Iyengar SS, Latesh Kumar KJ (2021) Satellite quantum communication protocol regardless of the weather. Opt. and Quantum Electronics. 53, 181.

76. Isaac S, Conrad A, Hill A, Herndon K, Wilens B, Chaffee D, Sanchez-Rosales D, Cochran R, Gauthier D, Kwiat P (2020) Drone-Based Quantum Key Distribution. In Conference on Lasers and Electro-Optics, OSA Technical Digest (Optica Publishing Group, 2020), paper JW2A.16.

77. Sharma S, Perlot N, Rödiger J, Freund R (2019) Tracking challenges of QKD over relay satellite. In International Conference on Space Optics 2018, Chania, Greece, Proc. of SPIE, 11180 1118062-1.

78. Qin H (2019) Toward large-scale quantum key distribution network and its applications. In ITU QIT4N Workshop 5-7 June, 2019 Shanghai, China.

79. Vázquez-Castro A, Rusca D, Zbinden H (2021) Quantum Keyless Private Communication Versus Quantum Key Distribution for Space Links. Phys. Rev. Applied. 16(1), 014006.

80. Deutsche Well (2020) Chinese 'space cleaner' spotted grabbing and throwing away old satellite. Available online: https://indianexpress.com/article/technology/science/chinese-space-cleaner-spotted-grabbing-and-throwing-away-old-satellite/ (Accessed on 03/03/2022).

81. Deutsche Well (2020) Modern spy satellites in an age of space wars (signal intelligence). Available online: https://www.dw.com/en/modern-spy-satellites-in-an-age-of-space-wars/a-5469-1887 (Accessed on 03/03/2022).

82. Willuhn M (2022) Satellite cyber attack paralyzes 11GW of German wind turbines. Available online: https://www.pv-magazine.com/2022/ 03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/ (Accessed on 03/03/2022).

83. Garcia M (2021) Space Debris and Human Spacecraft. Available online: https://www.nasa.gov/mission_pages/station/news/orbital_debris.html (Accessed on 02/25/ 2022).

84. National Geographics (2022) Orbital Objects: Learn more about satellites, space junk, and other objects floating in orbits. Available online: https://www.nationalgeographic.com/science/article/orbital-objects (Accessed 02/25/2022).

85. Johnson S (2022) How space debris created the world's largest garbage dump. Available online: https://bigthink.com/hard-science/space-debris-solutions/ (Accessed on 02/25/2022).

86. O'Callaghan J (2022) What is space junk and why is it a problem? Available online: https://www.nhm.ac.uk/discover/what-is-space-junk-and-why-is-it-a-problem.html (Accessed on 02/25/2022).

87. ESA (2022) About space debris. Available online: https://www.esa.int/Safety_Security/Space_Debris/About_space_debris (Accessed on 02/25/ 2022).

88. World Economic Forum (2020) Who owns our orbit: Just how many satellites are there in space? Available online: https://www.weforum.org/ agenda/ 2020/10/visualizing-easrth-satellites-sapce-spacex/ (Accessed on 02/25/2022).

89. Zhang E (2020) SpaceX's Dark Satellites Are Still Too Bright for Astronomers. Available online: https://www.scientificamerican.com/article/spacexs-dark-satellites-are-still-too-bright-for-astronomers/ (Accessed on 02/25/2022).

90. Morrison R (2022) Elon Musk's SpaceX Starlink satellites disrupt almost a FIFTH of images snapped by a crucial asteroid-spotting telescope, study warns. Available online: https://www.dailymail.co.uk/sciencetech/article-10422961/SpaceX-Starlink-satellites-disrupt-FIFTH-images-telescope.html (Accessed on 02/25/2022).

91. Morrison R (2022) Satellite mega-constellations including SpaceX's Starlink are now a WORSE threat to astronomy than light pollution, experts warn. Available online: https://www.dailymail.co.uk/sciencetech/article-10486455/SpaceXs-Starlink-WORSE-threat-astronomy-light-pollution-experts-warn.html (Accessed on 02/25/2022).

92. Morelle R (2019) Satellite constellations: Astronomers warn of threat to view of Universe. Available online: https://www.bbc.com/news/science-environment-50870117 (Accessed on 02/ 25/2022).

93. Lenta.ru (2022) Musk's satellites began to interfere with the study of dangerous asteroids. Available online: https://vpk.name/en/577811_musks-satellites-began-to-interfere-with-the-study-of-dangerous-asteroids.html (Accessed on 02/25/2022).

94. Pultarova T (2022) International Astronomical Union launches new center to fight satellite megaconstellation threat. Available online: https://www.space.com/iau-center-protect-astronomy-megaconstellation-threat (Accessed on 03/10/2022).

95. Foust J (2022) New center to coordinate work to mitigate effect of satellite constellations on astronomy. Available online: https://spacenews. com/new-center-to-coordinate-work-to-mitigate-effect-of-satellite-constellations-on-astronomy/ (Accessed on 03/10/2022).

96. CPS (2022) Protection of the Dark and Quiet Sky from Satellite Constellation Interference. Available online: https://cps.iau.org/#:~:text=The IAU Centre for the,impact of satellite constellations on (Accessed on 03/10/2022).

97. Van Wyk A (2022) SKAO and international partners petition UN for the protection of Earth's dark and quiet skies. Available online: https://www. skatelescope.org/news/skao-and-international-partners-petition-un-for-the-protection-of-earths-dark-and-quiet-skies/ (Accessed on 03/10/ 2022).

98. Kleiner K (2022) Orbiting robots could help fix and fuel satellites in space: Machines will soon have a go at maintaining fleet of small spacecraft orbiting Earth. Available online: https://arstech

nica.com/science/2022/03/orbiting-robots-could-help-fix-and-fuel-satellites-in-space/?comments=1 (Accessed on 03/10/2022).

99. Nielsen MA, Chuang IL (2004) Quantum Computation and Quantum Information. Cambridge University Press, N.Y.
100. Quantis QRNG Chip (2022) Available online: https://www.idquantique.com/random-number-generation/products/quantis-qrng-chip/ (Accessed on 03/10/2022).
101. Swan M (2015) Blockchain: Blueprint for a New Economy. O'Reilly, Sebastopol, CA.
102. Vernam GS (1926) Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. Journal of the IEEE. 55, pp. 109–115.
103. Wikipedia (2022) Quantum Experiments at Space Scale. Available online: https://en.wikipedia.org/wiki/Quantum_Experiments_at_Space_Scale (Accessed on 03/14/2022).
104. Kets (2022) Available online: https://kets-quantum.com/quantum-key-distribution/ (Accessed on 03/14/2022).
105. ISO (2022) ISO/IEC 27001: Information Security Management. Available online: https://www.iso.org/isoiec-27001-information-security.html (Accessed on 03/14/2022).
106. IACS (2022) International Association of Classification Societies (IACS). Available online: https://iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1/ (Accessed on 03/14/2022).
107. DoD Space Agency (2022) Available online: https://spacenews.com/dod-space-agency-funds-development-of-laser-terminal-that-connects-to-multiple-satellite-at-once/ (Accessed on 03/14/2022).
108. TechRepublic (2022) Available online: https://www.techrepublic.com/article/how-an-8-character-password-could-be-cracked-in-less-than-an-hour/ (Accessed on 03/14/2022).