Metrol. Meas. Syst., Vol. XX (2013), No. 1, pp. 3–16.

PAN POLSKA AKADEMIA NAUK

METROLOGY AND MEASUREMENT SYSTEMS

Index 330930, ISSN 0860-8229

www.metrology.pg.gda.pl

M&MS

UNCONDITIONAL SECURITY BY THE LAWS OF CLASSICAL PHYSICS[1]

Robert Mingesz[1)], Laszlo Bela Kish[2)], Zoltan Gingl[1)], Claes-Göran Granqvist[3)], He Wen[2,4)], Ferdinand Peper[5)], Travis Eubanks[6)], Gabor Schmera[7)]

1) University of Szeged, Department of Technical Informatics, Árpád tér 2, Szeged, H-6701, Hungary (mingesz@inf.u-szeged.hu)
2) Texas A&M University, Department of Electrical and Computer Engineering, College Station, TX 77843-3128, USA (✉ Laszlo.Kish@ece.tamu.edu, +36 979 847 9071)
3) Uppsala University, Department of Engineering Sciences, P.O. Box 534, SE-75121 Uppsala, Sweden (Claes-Goran.Granqvist@Angstrom.uu.se)
4) Hunan University, College of Electrical and Information Engineering, Changsha 410082, China (he_wen82@126.com)
5) National Institute of Information and Communication Technology, Kobe, Hyogo 651-2492, Japan (peper@nict.go.jp
6) Sandia National Laboratories, P.O. Box 5800, Albuquerque, NM 87185-1033, USA (tweuban@sandia.gov)
7) Space and Naval Warfare Systems Center, San Diego, CA 92152, USA (gabe.schmera@navy.mil)

Abstract

There is an ongoing debate about the fundamental security of existing quantum key exchange schemes. This debate indicates not only that there is a problem with security but also that the meanings of perfect, imperfect, conditional and unconditional (information theoretic) security in physically secure key exchange schemes are often misunderstood. It has been shown recently that the use of two pairs of resistors with enhanced Johnson-noise and a Kirchhoff-loop – *i.e.*, a Kirchhoff-Law-Johnson-Noise (KLJN) protocol – for secure key distribution leads to information theoretic security levels superior to those of today's quantum key distribution. This issue is becoming particularly timely because of the recent full cracks of practical quantum communicators, as shown in numerous peer-reviewed publications. The KLJN system is briefly surveyed here with discussions about the essential questions such as (*i*) perfect and imperfect security characteristics of the key distribution, and (*ii*) how these two types of securities can be unconditional (or information theoretical).

Keywords: information theoretic security, unconditional security, secure key exchange, secure key distribution, quantum encryption.

1. Introduction: Security problems with quantum key exchange

There is an ongoing debate [1–6] about the fundamental security/non-security of existing quantum key distribution (QKD) schemes. This debate was initiated by quantum security expert Horace Yuen [1, 4–6], who was later joined by Osamu Hirota [2] in claiming that the security of existing quantum key distribution schemes is questionable or poor. Recently, Renner [3] also entered the discussion and attempted to defend the old security claims. Generally speaking, the argumentation is highly technical and accessible only for experts in theoretical security analysis – and apparently even such experts disagree. According to Yuen, existing QKD schemes are either non-secure or their security is uncertain. On the other hand, he proposed [6] a new class of schemes (KCQ, keyed communication in quantum noise) that is based on multi-photonic beams and a previously shared secret key, which is free of the deficiencies of QKD and offers an extraordinarily high key generation rate.

[1] Expanded, journal version of the conference proceedings paper Mingesz, R., Kish, L.B., Gingl, Z., Granqvist, C.-G., Wen, H., Peper, F., Eubanks, T,, Schmera, G. (2013). Information theoretic security by the laws of classical physics (Plenary talk at the 5th IEEE Workshop on Soft Computing Applications, August 22–24, 2012; SOFA 2012, In: Balas VE et al. (Eds.), Soft Computing Applications, AISC 195, 11–25, (Springer).

Article history: received on Sep. 18, 2012; accepted on Dec. 15, 2012; available online on Mar. 15, 2013; DOI: 10.2478/mms-2013-0001.

While the above debate on fundamentals is currently unfolding, QKD has very recently seriously failed in a much simpler and elementary way. Thus practical quantum communicators – including several commercial ones – have been fully cracked as shown in numerous recent papers [7–21], and Vadim Makarov, who is one of the leading quantum crypto crackers, says in *Nature News* that "Our hack gave 100% knowledge of the key, with zero disturbance to the system" [7]. This claim hits at the foundations of quantum encryption schemes because the basis of the security of QKD protocols is the assumption that any eavesdropper (Eve) disturbs the system enough to be detected by the communicator parties (Alice and Bob). Furthermore, the work by Makarov proves that we were right in 2007 when claiming in our *SPIE Newsroom* article [22] that quantum security is mainly theoretical. We note, in passing, that during the period from 2007 until now there have been many research grants given to support the development of new QKD schemes – but not to the "politically incorrect" challenge to crack them.

However, the last few years have seen a radically changed picture [7–21] on the security of practical quantum communicators, and even a full-field implementation of a perfect eavesdropper on a quantum cryptography system has been carried out [8], which is a most difficult task and is an attack on an already established "secure" QKD connection. These cracking schemes are referred to as "hacking" because they utilize physical non-idealities in the building elements of QKD devices. The number of these non-idealities is large, and so is the number of hacking types. The key lessons learned are that:

i. At this moment, QKD security is only theoretical (and one should note that even this theoretical security is challenged by Yuen and Hirota; see above).

ii. The applied theory has been proven to be incorrect/incomplete for practical devices, and new defense mechanisms must be developed for each type of hacking attack.

iii. The potential for yet unexplored non-idealities/attacks is huge, and the present practical security of QKD is conditional: the condition of security is that Eve does not apply the hacking attack that breaks the key.

iv. Security analysis, taking into account the real characteristics of the devices, is essential when security matters, and novel defense mechanisms must be developed against these new types of attacks that utilize the non-ideal device features.

An important aspect of all these quantum attacks is the extraordinary (100%) success ratio (*i.e.*, information leak) of extracting the "secure" key bits by Eve, while Alice and Bob do not have a clue that efficient eavesdropping is going on.

Inspired by the interesting developments outlined above we discuss related issues in the key exchange system of the classical physical Kirchhoff-Law-Johnson-Noise (KLJN) protocol [22]. It should be noted here that there is a general misunderstanding of the KLJN scheme among people lacking the relevant expertise in statistical physics and noise-in-circuitry, as evidenced for example in the Wikipedia entry "Kish cypher" and its "talk page" where, most of the time, both the supporters and the opponents are wrong and the debate falls very short of an objective scientific exchange of views (amusingly, even the name "cypher" is incorrect). Therefore, after briefly surveying the KLJN system and its properties, we clarify the meaning of *perfect security* and *imperfect security* levels and also define the conditions of these measures: *information theoretic security* (synonym of *unconditional security*) and its limited version *computationally unconditional security*. Furthermore we mention existing prime-number-based key exchange protocols that have (computationally) *conditional security*. It will be seen that theoretical/ideal QKD and KLJN protocols have perfect information theoretic (unconditional) security. However these schemes, when realized with practical/realistic (physical/non-ideal) building elements, have imperfect security that is still information theoretic (unconditional) even though current QKD cracks [7–21] indicate that KLJN performs better.

2. The KLJN secure key exchange protocol

It is often believed that quantum physics represents modern science and that classical physics is old and outdated. Of course this is not true because the two fields rather pertain to different physical size regimes – the "small" versus the "large" where the appropriate rules of physics are different – not different periods of science history. The above claim regarding "modern" and "old" cannot be maintained even for the history of physics, though, when the point at issue concerns spontaneous random fluctuation phenomena, that are simply referred to as "noise", and it is true for even the most general and omnipresent type of classical physical noise, *viz*., thermal noise (voltage or current fluctuations in thermal equilibrium) which is a younger field of physics than quantum mechanics. Indeed two Swedish scientists, John Johnson and Harry Nyquist both working at Bell Labs, discovered/explained the thermal noise voltage of resistors [23, 24] several years after the completion of the foundations of quantum physics [25].

Similarly, quantum heat engines [26] with optional internal coherence effects [27] were proposed several years earlier than the application [28] of the thermal noise of resistors for a heat engine scheme with similar coherence effects.

Finally, the application of thermal noise for unconventional informatics, namely for noise-based logic and computing [29–36] and the KJLN secure key exchange [37–52], emerged decades later than the corresponding quantum informatics schemes such as quantum computing [53] and quantum encryption [54–56].

It is interesting to note that some "exotic" phenomena, previously thought to belong to the class of "quantum-weirdness", occur and can be utilized also in the noise schemes, for example teleportation/telecloning in KLJN networks [51] and entanglement in noise-based logic [29–36].

2.1. The Kirchhoff-Law-Johnson-Noise key distribution

The KLJN secure key exchange scheme was introduced in 2005 [37–39] and was built and demonstrated in 2007 [40]; it is founded on the robustness of classical information as well as stochasticity and the laws of classical physics. It was named by its creators the "Kirchhoff-loop-Johnson(-like)-Noise" scheme, while on the Internet – in blogs and similar sites, including Wikipedia – it has widely been nicknamed "Kish cypher" or "Kish cipher" (where both designations are wrong). The concept has often been misinterpreted and misjudged.

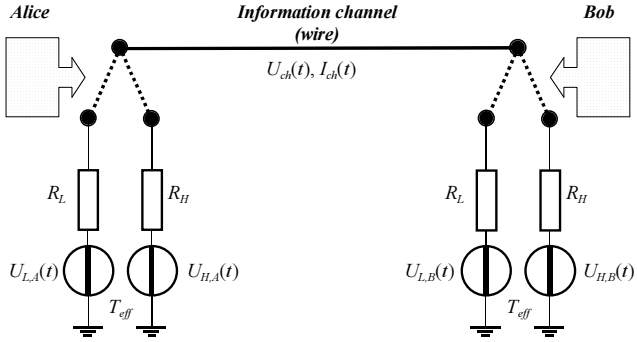

Fig. 1. Core of the KLJN secure key exchange system [37]. In the text below, the mathematical treatment is based on the power density spectra of the voltages and currents shown here.

The KLJN scheme is a statistical/physical competitor to quantum communicators and its security is based on Kirchhoff's Loop Law and the Fluctuation-Dissipation Theorem. More generally, it is founded on the Second Law of Thermodynamics, which indicates that the security of the ideal scheme is as strong as the impossibility to build a perpetual motion machine of the second kind.

We first briefly survey the foundations of the KLJN system [37, 39, 42]. Figure 1 shows a model of the idealized KLJN scheme designed for secure key exchange [37]. The resistors R_L and R_H represent the low, $L(0)$, and high, $H(1)$, bits, respectively. At each clock period, Alice and Bob randomly choose one of the resistors and connect it to the wire line. The situations LH and HL represent secure bit exchange [37], because Eve cannot distinguish between them through measurements, while LL and HH are insecure. The Gaussian voltage noise generators – delivering white noise with publicly agreed bandwidth – represent a corresponding thermal noise at a publicly agreed effective temperature T_{eff} (typically $T_{eff} \geq 10^9$ K [40]). According to the Fluctuation-Dissipation Theorem, the power density spectra $S_{u,L}(f)$ and $S_{u,H}(f)$ of the voltages $U_{L,A}(t)$ and $U_{L,B}(t)$ supplied by the voltage generators in R_L and R_H are given by:

$$S_{u,L}(f) = 4kT_{eff}R_L \quad \text{and} \quad S_{u,H}(f) = 4kT_{eff}R_H, \tag{1}$$

respectively.

In the case of secure bit exchange (*i.e.*, the LH or HL situation), the power density spectrum of channel voltage $U_{ch}(t)$ and channel current $I_{ch}(t)$ are given as:

$$S_{u,ch}(f) = 4kT_{eff}\frac{R_L R_H}{R_L + R_H} \tag{2}$$

and

$$S_{i,ch}(t) = \frac{4kT_{eff}}{R_L + R_H}, \tag{3}$$

respectively; further details are given elsewhere [37, 42]. It should be observed that during the LH and HL cases, linear superposition turns (2) into the sum of the spectra of two situations, *i.e.*, when only the generator in R_L is running one gets:

$$S_{L,u,ch}(f) = 4kT_{eff}R_L\left(\frac{R_H}{R_L + R_H}\right)^2 \tag{4}$$

and when the generator in R_H is running one has:

$$S_{H,u,ch}(f) = 4kT_{eff}R_H\left(\frac{R_L}{R_L + R_H}\right)^2. \tag{5}$$

The ultimate security of the system against passive attacks is provided by the fact that the power $P_{H\to L}$, by which the Johnson noise generator of resistor R_H is heating resistor R_L, is equal to the power $P_{L\to H}$ by which the Johnson noise generator of resistor R_L is heating resistor R_H [37, 42]. A proof of this can also be derived from (3) for a frequency bandwidth of Δf by:

$$P_{L\to H} = \frac{S_{L,u,ch}(f)\Delta f}{R_H} = 4kT_{eff}\frac{R_L R_H}{(R_L + R_H)^2}, \tag{6a}$$

and

$$P_{H\to L} = \frac{S_{H,u,ch}(f)\Delta f}{R_L} = 4kT_{eff}\frac{R_L R_H}{(R_L+R_H)^2}. \qquad (6b)$$

The equality $P_{H\to L} = P_{L\to H}$ (*cf.* (6)) is in accordance with the Second Law of Thermodynamics; violating this equality would mean not only going against basic laws of physics and the inability to build a perpetual motion machine (of the second kind) but also allow Eve to use the voltage-current cross-correlation $\langle U_{ch}(t)I_{ch}(t)\rangle$ to extract the bit [37]. However $\langle U_{ch}(t)I_{ch}(t)\rangle$ = 0, and hence Eve has an insufficient number of independent equations to determine the bit location during the *LH* and *HL* situations. The above security proof against passive (listening) attacks holds only for Gaussian noise, which has the well-known property that its power density spectrum or autocorrelation function provides the maximum information about the noise, and no higher order distribution functions or other tools are able to contribute additional information.

It should be observed [37, 39, 40, 42] that deviations from the shown circuitry – including parasitic elements, inaccuracies, non-Gaussianity of the noise, *etc.* – will cause a potential information leak toward Eve. One should note that the circuit symbol "line" in the circuitry represents an ideal wire with uniform instantaneous voltage and current along it. Thus if the wire is so long and the frequencies are so high that waves appear in it, this situation implies that the actual circuitry deviates from the ideal one [37].

To provide unconditional security against invasive attacks, including the man-in-the-middle attack, the fully armed KLJN system shown in Fig. 2 monitors the instantaneous current and voltage values at both ends (*i.e.*, for Alice as well as Bob) [39, 40, 42], and these values are compared either via broadcasting them or via an authenticated public channel. An alarm goes off whenever the circuitry is changed or tampered with or energy is injected into the channel. It is important to note that these current and voltage data contain all of the information Eve can possess. This means that Alice and Bob have full knowledge about the information Eve may have; this is a particularly important property of the KLJN system, which can be utilized in secure key exchange.

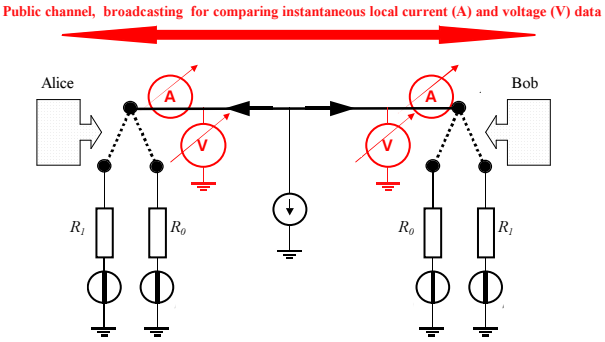

Fig. 2. Sketch of the KLJN wire communication arrangement [39, 42]. To detect the invasive eavesdropper (represented, for example, by the current generator at the middle), the instantaneous current and voltage data measured at the two ends are broadcasted and compared. The eavesdropping is detected immediately, within a small fraction of the time needed to transfer a single bit. Thus statistics of bit errors is not needed, so the exchange of even a single key bit is secure.

The situation discussed above implies the following important features of the KLJN system [37, 39, 40, 42]:

i. In a practical (non-idealized) KLJN system, Eve can utilize device non-idealities to extract some of the information by proper measurements. This is measurement information

and does not depend on Eve's computational and algorithmic ability, *i.e.*, the level of security is computationally unconditional. The maximum leak toward Eve can be designed by Alice and Bob by supposing the physically allowed best/ultimate measurement system for Eve. This designed level of security is unconditional in every sense.

ii. Even when the communication is disturbed by invasive attacks or inherent non-idealities in the KLJN arrangement, the system remains secure because no information can be eavesdropped by Eve without the full knowledge of Alice and Bob about this potential incidence and without the knowledge of the full information that Eve might have extracted (a full analysis of this aspect is provided elsewhere [42]).

iii. In other words, the KLJN system is always secure, even when it is built with non-ideal elements or designed for a non-zero information leak, in the following sense: The current and voltage data inform Alice and Bob about the exact information leak and hence, for each compromised key bit, they can decide to discard it or even to use it to mislead or manipulate Eve [42].

iv. The KLJN arrangement is naturally and fully protected against the man-in-the-middle attack [39] even during the very first run of the operation when no hidden signatures can be applied. This feature is provided by the unique property of the KLJN system that zero-bit information can only be extracted during a man-in-the-middle attack because the alarm goes off before the exchange of a single key bit has taken place [39].

v. The security of the KLJN system is not based on the error statistics of key bits, and even the exchange of single key bits is secure.

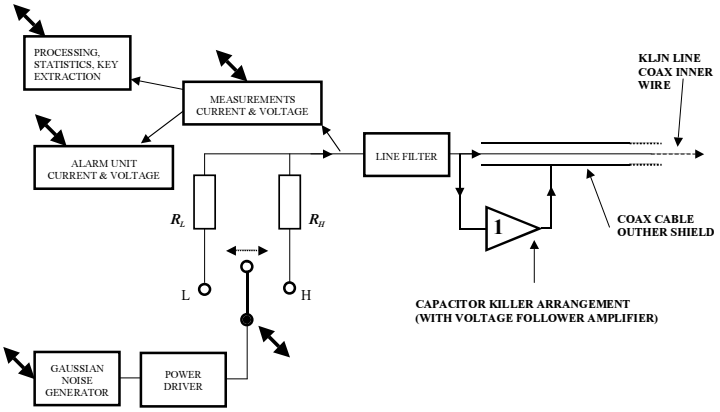

Fig. 3. A practical KLJN device set-up [40]. Double-ended arrows symbolize computer control.

Figure 3 outlines a prototype of the KLJN device [40]. The various non-idealities have been addressed by different tools with the aim that the information leak toward Eve due to non-idealities should stay below 1% of the exchanged raw key bits. For the KLJN device it was 0.19% for the most efficient attack [40]. Here we briefly address two aspects of non-idealities:

i. The role of the line filter (and of the band limitation of the noise generator) is to provide the no-wave limit in the cable, *i.e.*, to preserve the core circuitry (*cf.* Fig. 1) in the whole frequency band. This implies that the shortest wavelength component in the driving noise should be much longer than twice the cable length in order to guarantee that no active wave modes and related effects (*e.g.*, reflection, invasive attacks at high frequencies, *etc.*) take place in the cable.

ii. Another tool to fight non-idealities is the cable capacitance compensation ("capacitor killer") arrangement (*cf.* Fig. 3). With practical cable parameters and their limits, there is

a more serious threat of the security: the cable capacitance shortcuts part of the noise current, which results in a greater current at the side of the lower resistance end and thus yields an information leak. This effect can be avoided by a "capacitor-killer" [40] using the inner wire of a coax cable as KLJN line while the outer shield of the cable is driven by the same voltage as the inner wire. However, this is done via a follower voltage amplifier with zero output impedance. The outer shield will then provide all the capacitive currents toward the ground, and the inner wire will experience zero parasitic capacitance. Without "capacitor killer" arrangement and practical bare-wire line parameters, the recommended upper limit of cable length is much shorter and depends on the value of the driving resistor R_L and R_H.

2.2. Security proofs and attacks

First we define the (normalized) *information leak* mentioned above. If the key bits are uncorrelated, which is the actual situation in the KLJN system, the information leak is a reliable measure of security according to:

$$K = \frac{C_{AE}}{C_{AB}} = \frac{C_{BE}}{C_{AB}} = \frac{C_{AE}}{C_{BA}} = \frac{C_{BE}}{C_{BA}}, \tag{7}$$

where K is the (normalized) information leak and C_{AE}, C_{BE}, C_{AB}, and C_{BA} are the information channel capacity from Alice to Eve, from Bob to Eve, from Alice to Bob, and to Bob to Alice, respectively. (7) presumes a completely symmetric channel, which is appropriate for KLJN. The information channel capacity is defined by the Shannon formula for binary channel, *i.e.*,

$$C_{AE} = C_{BE} = f_c\left[1 + p_E \log_2 p_E + (1 - p_E)\log_2(1 - p_E)\right] \text{ bit/s} \tag{8}$$

and

$$C_{AB} = C_{BA} = f_c\left[1 + p_B \log_2 p_B + (1 - p_B)\log_2(1 - p_B)\right] \text{ bit/s}, \tag{9}$$

where f_c is the key bit exchange rate (clock frequency), p_E is Eve's probability of successfully guessing the key bit and p_B is the *fidelity*, *i.e.*, Bob's (and Alice's) probability of successfully guessing the key bit.

The ideal, mathematically defined KLJN system is absolutely secure, which means $K = 0$. However, real systems are rarely ideal and thus hacking attacks are possible by using non-idealities. Fortunately the KLJN system is very simple, implying that the number of such attacks is limited. Several hacking attack types, based on the non-ideality of circuit elements causing deviations from the ideal circuitry, have been published [42–48]. Each of these attacks triggered a relevant security proof that showed the efficiency of the defense mechanism (*cf.* Fig. 2). Furthermore, all known attack types were experimentally tested [40] and the theoretical security proofs were experimentally confirmed.

For practical conditions, the most effective attack employed voltage-drop-related effects on non-zero wire resistance [38, 43, 44]. It should be noted that serious calculation errors were made by Scheuer and Yariv [43], resulting in a thousand times stronger predicted value of the effect than its real magnitude. The errors were pointed out, and the calculations were corrected by Kish and Scheuer [44]. In an experimental demonstration [40], the strongest leak was indeed due to wire resistance and 0.19% of the bits leaked out to Eve, *i.e.*, $K = 0.0019$, while the fidelity of the key exchange was 99.98%, which means that a 0.02% bit-error-rate, denoted BER, for Alice and Bob. This is a very good value of K, and it can easily be made infinitesimally small by simple two-step privacy amplification, as further discussed in Section 2.3.

A general response to the mentioned and other types of small-non-ideality attacks has been presented by Kish [45], and the related information leak was shown to be miniscule as a consequence of the very poor statistics that Eve could obtain.

Other attack types, presented by Hao [46], are of less practical importance and based on differences in noise temperatures; they were proven theoretically [47] and experimentally [40] insignificant. The very high accuracy of digital simulations and digital-analog converters (at least 12-bit resolution) allows setting the effective temperature so accurately – with 0.01% or less error – that this type of inaccuracy-based information leak is not observable. In the case of 12-bit resolution one has $K = 6*10^{-11}$, *i.e.*, the leakage of one effective bit would require a 600-Megabit-long key. Therefore this effect was not visible in experiments even though extraordinarily long (74497) key bits were generated/exchanged in each run [40].

The practical inaccuracy of commercial low-cost resistors (1%) at the two ends [40, 47] is a much more serious issue; it leads to leaks up to $K \approx 10^{-4}$ (*i.e.*, about seven bits leak from the 74497-bit-long key) for a resistance inaccuracy of 1% [40]. However, its impact was still not measurable because of the statistical inaccuracies, $\sqrt{74497} \approx 270$ bits, at this key length. These inaccuracies were about forty times greater than the theoretical information leak of seven [40].

Wire capacitance would be the most serious source of information leak without the "capacitance-killer" arrangement, whereas effects of cable inductances are negligible [42].

Another attack, by Liu [48], was focused on delay effects and obtained a success rate of $p_E = 0.7$ for Eve. However, this work employed wire simulation software and used physically flawed parameters such as cable diameters being 28,000 times greater than the diameter of the known universe at two km cable length (the error in this attack was pointed out in a subsequent paper [42]). Although this attack was flawed, it is remarkable that even this non-existent, high information leak can be removed by three-step privacy amplification, as discussed below in Section 2.3.

It is important to note that the level of the allowed information leak can be chosen by Alice and Bob, and its actual value is determined only by the invested resources and also typically depends on how much speed is given up. For example, the information leak due to the wire resistance scales inversely with the fourth power of wire diameter, which means that employing a ten times thicker cable would reduce the relative information leak of 0.19% to $K = 1.9*10^{-7}$.

The best attack strategy for Eve is to observe the public data exchange about the instantaneous current and voltage amplitudes between Alice and Bob. Those data contain the highest amount of eavesdropping information because they are measured in the most ideal way, and Alice and Bob also base their decision about the bit values on those. Enhancing Eve's infrastructure beyond that ability does not improve her situation, and thus the security is information theoretic/unconditional.

2.3. Privacy amplification in non-ideal systems

Privacy amplification is a classical software-based technique which was originally developed for QKD to ensure the security of an encryption scheme with partially exposed key bits. Horvath *et al*. [49] realized simple privacy amplification by executing XOR logic operation on subsequent pairs of key bits, thereby cutting the key length in half while progressively reducing the information leak.

If the reduction of the information leak is not sufficient, the same procedure can be repeated on the new key. The resulting key length scales with 0.5^N, where N is the number of privacy amplification steps. It was found that, in contrast to quantum key distribution

schemes, the high fidelity of the raw key generated in the KLJN system allows the user to always extract a secure shorter key. The necessary conditions are sufficiently high fidelity (*i.e.*, small BER), which the KLJN provides, and an upper limit less than unity on the eavesdropper probability to correctly guess the exchanged key bits, which means the key exchange is not fully cracked (less than 100% relative information leak is present). The number of privacy amplification steps needed to achieve an information leak of $K < 10^{-8}$, when starting from the 0.19% ($K = 0.0019$) raw bit information leak, is two, thus resulting in a corresponding slowdown by a factor of four [49]. In the case of Eve's success rate of $p_E = 0.7$, obtained by the flawed simulations in earlier work [48] (see above), the necessary number of privacy amplification steps is three, thus leading to a slowdown by a factor of eight [49].

3. Security measures and their conditions

In this section we discuss some basic security measures [58, 59] and apply them to compare QKD, KLJN and software secure key exchange; see Fig. 4 for a summary.

A *perfect security* level means that the information channel capacity of the eavesdropping channel from Alice/Bob toward Eve is zero. *Imperfect security* level means that the information channel capacity of the eavesdropping channel from Alice/Bob toward Eve is non-zero. We call the encryption "cracked" if Eve can extract all of the information communicated between Alice and Bob. Thus an imperfect security level does not necessarily mean that the encryption is cracked. If the bit-error-rate is negligible then, by using privacy amplification, the effective level of imperfect security can be enhanced so that it can arbitrarily approach the perfect security level.

To characterize the situations of perfect and imperfect security levels, we must address the conditions where these levels hold. The conditions that both QKD and the KLJN protocols represent are referred to as *information theoretic security*, or *unconditional security*. We note, in passing, that these terms are often completely misunderstood by people who write into Wikipedia and to blog sites about the KLJN system, and these mistakes lead to incorrect conclusions and self-contradicting arguments.

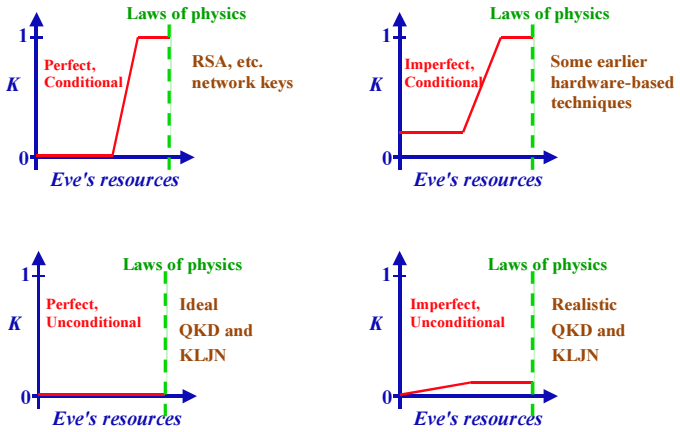

Fig. 4. Types of security levels (homogeneously distributed key is supposed thus K is a good measure): Perfect Conditional, Imperfect Conditional, Perfect Unconditional, and Imperfect Unconditional. Note that in this figures it is supposed that QKD security *does not* have fundamental security flaws, *i.e.*, these figures do not yet contain Yuen's critical assessments [1] about QKD. Moreover, it is also supposed that the weaknesses of practical QKD leading to the *major cracks* [7–21] *are all fixed* by proper defense mechanisms.

The most rigorous security condition is *information theoretic security*, which means that the information content of the data Eve can extract is limited by information theory even if Eve is using the hypothetical most powerful processing of the extracted data. *Unconditional security* is a similar term, indicating security when Eve has unlimited resources. It often means a computationally unconditional security measure, which limits the infrastructure to computers and algorithms, so it has limited validity compared to information theoretic security. Computationally unconditional security simply means that the information content of the data that Eve is able to extract is limited even if she has infinite computing power.

For example today's generally used software algorithms, utilizing prime numbers for key generation and distribution, have neither information theoretic nor computationally unconditional security. All of the information about the key exists in the data observed in the line by Eve, in a decodable form, and hence it cannot be information theoretically secure. This information can be fully decoded with a sufficiently fast computer or integer-factoring algorithm or with a normal computer running for a long enough but finite time. The security is (computationally) conditional: it is based on the assumption that Eve does not have an efficient algorithm or a fast enough computer to decode the key within a practically relevant timeframe.

It is important to note that even imperfect security can be information theoretical or (computationally) unconditional [59]. Such a situation occurs with a physically secure key distribution only, such as QKD or KLJN, because the information leak will be determined by measurement information and not by computation or algorithmic decoding.

The way in which ideal/theoretical QKD makes the key exchange secure is based on the no-cloning theorem of quantum physics [55]: photon states cannot be cloned without introducing errors. Because information bits are (theoretically) carried by single photons, Eve must clone the photon if she wants to measure one; otherwise the information is destroyed before reaching the receiving party. But cloning the photon introduces extra errors into the line, and when Alice and Bob recognize the increased BER they conclude that eavesdropping has happened and they discard the bit-package exhibiting the increased error rate.

The ideal QKD protects the system against eavesdropping, but this is strictly true only for an infinitely long key because Alice and Bob must prepare error statistics, and exacting perfect statistics requires infinite time. Otherwise, due to statistical fluctuations in the BER, Alice and Bob can never be absolutely sure that the key was not eavesdropped. To illustrate this problem, we can go to the simplest type of attack: the intercept-resend attack for the BB84 QKD protocol (see, for example, work by Xu *et al*. [57]). The probability $P(N)$ that the eavesdropping will be discovered while Eve extracts N key bits is not unity but:

$$P_h = 1 - \left(\frac{3}{4}\right)^N . \tag{10}$$

Equation (10) shows that, even though a reasonably long key will be very secure and that security can be further enhanced by privacy amplification, the security is not perfect although it can arbitrarily approach the perfect security level. However if we want to extract only a single key bit, the security is extremely poor because Eve has 25% chance to succeed.

The way by which the ideal/theoretical KLJN scheme makes the key exchange secure depends on the type of the attack: whether it is passive (listening) or invasive (introducing energy in the channel and/or modifying the channel circuitry). In the case of passive listening, information theoretic security due to zero information in the extracted data is guaranteed by the Second Law of Thermodynamics, and this is true even for single-bit attacks where QKD fails. In the case of invasive attacks, the defense mechanics is similar to that of QKD: Alice and Bob will observe deviations between instantaneous signals and they detect the presence of eavesdropping virtually immediately so that, again, even a single-bit attack has no chance.

Table 1 shows a summary/conclusion on the security levels of the various key exchange protocols.

In conclusion, the ideal KLJN protocol protects a system against invasive eavesdropping and provides zero information to passive eavesdroppers.

Table 1. Comparison of relevant security levels for existing key exchange systems.

	Perfect	**Imperfect**	**Information theoretic or unconditional**	**Conditional**
QKD theoretical	***Yes*** for the whole key ***No*** for a single bit	***No*** for the whole key ***Yes*** for a single bit	***Yes***	***No***
KLJN theoretical	***Yes*** for both the whole key and a single bit	***No***	***Yes***	***No***
QKD practical	***No***	***Yes***	***Yes***	***No***
KLJN practical	***No***	***Yes***	***Yes***	***No***
Software and prime number based	***Yes***	***No***	***No***	***Yes***

Acknowledgement

LBK is grateful to Horace Yuen for discussions on fundamental problems of current QKD schemes, on his new improved scheme, and on the general requirements for physically secure key exchange. LBK is also indebted to Vincent Poor for a discussion on unconditional (information theoretic) security of practical secure physical systems with imperfect security. RM and ZG were partially supported by grant TAMOP-4.2.1/B-09/1/KONV-2010-0005. HW was partially supported by the National Natural Science Foundation of China under grant 61002035.

References

[1] Yuen, H.P. (2012). *On the foundations of quantum key distribution – Reply to Renner and beyond.* arXiv:1210.2804.

[2] Hirota, O. (2012). *Incompleteness and limit of quantum key distribution theory*. arXiv:1208.2106v2.

[3] Renner, R. (2012). *Reply to recent scepticism about the foundations of quantum cryptography*. arXiv:1209.2423v.1.

[4] Yuen, H.P. (2012). *Security significance of the trace distance criterion in quantum key distribution.* arXiv:1109.2675v3.

[5] Yuen, H.P. (2012). *Unconditional security in quantum key distribution.* arXiv:1205.5065v2.

[6] Yuen, H.P. (2009). Key generation: Foundation and a new quantum approach. *IEEE J. Selected Topics in Quantum Electronics*, 15, 1630.

[7] Merali, Z, (2009). *Hackers blind quantum cryptographers*. Nature News, DOI:10.1038/news.2010.436.

[8] Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., Makarov, V. (2011). Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Commun*., 2, 349 DOI: 10.1038/ncomms1348.

[9] 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, 686–689, DOI: 10.1038/NPHOTON.2010.214.

[10] Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Scarani, V., Makarov, V., Kurtsiefer, C. (2011). Experimentally faking the violation of Bell's inequalities. *Phys. Rev. Lett.*, 107,170404, DOI: 10.1103/PhysRevLett.107.170404.

[11] Makarov, V., Skaar, J. (2008). Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Inf. Comp*., 8, 622–635.

[12] Wiechers, C., Lydersen, L., Wittmann, C., Elser, D., Skaar, J., Marquardt, C., Makarov, V., Leuchs, G. (2011). After-gate attack on a quantum cryptosystem. *New J. Phys*., 13, 013043, DOI: 10.1088/1367-2630/13/1/013043.

[13] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V. (2010). Thermal blinding of gated detectors in quantum cryptography. *Opt. Express*, 18, 27938–27954, DOI: 10.1364/OE.18.027938.

[14] Jain, N., Wittmann, C., Lydersen, L., Wiechers, C., Elser, D., Marquardt, C., Makarov, V., Leuchs, G. (2011). Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.,* 107, 110501, DOI: 10.1103/PhysRevLett.107.110501.

[15] Lydersen, L., Skaar, J., Makarov, V. (2011). Tailored bright illumination attack on distributed-phase-reference protocols. *J. Mod. Opt*., 58, 680–685. DOI: 10.1080/09500340.2011.565889.

[16] Lydersen, L., Akhlaghi, M.K., Majedi, A.H., Skaar, J., Makarov, V. (2011). Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New J. Phys*., 13,113042, DOI: 10.1088/1367-2630/13/11/113042.

[17] Lydersen, L., Makarov, V., Skaar, J. (2011). Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography". *Appl. Phys. Lett*., 99, 196101, DOI: 10.1063/1.3658806.

[18] Sauge, S., Lydersen, L., Anisimov, A., Skaar, J., Makarov, V. (2011). Controlling an actively-quenched single photon detector with bright light. *Opt. Express*, 19, 23590–23600.

[19] Lydersen, L., Jain, N., Wittmann, C., Maroy, O., Skaar, J., Marquardt, C., Makarov, V., Leuchs, G. (2011). Superlinear threshold detectors in quantum cryptography. *Phys. Rev. Lett*., 84, 032320, DOI: 10.1103/Phys RevA.84.032320.

[20] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V. (2010). Avoiding the blinding attack in QKD; Reply (Comment). *Nature Photonics*, 4, 801–801, DOI: 10.1038/nphoton.2010.278.

[21] Makarov, V. (2009). Controlling passively quenched single photon detectors by bright light. *New J. Phys*., 11, 065003, DOI: 10.1088/1367-2630/11/6/065003.

[22] Kish, L.B., Mingesz, R., Gingl, Z. (2007). Unconditionally secure communication via wire. *SPIE Newsroom*, DOI: 10.1117/2.1200709.0863.

[23] Johnson, J.B. (1927). Thermal agitation of electricity in conductors. *Nature*, 119, 50–51.

[24] Nyquist, H. (1928). Thermal agitation of electric charge in conductors. *Phys. Rev*., 32, 110–113.

[25] Born, M., Heisenberg, W., Jordan, P. (1926). Quantum mechanics II. *Z. Phys.*, 35, 557–615.

[26] Allahverdyan, A.E., Nieuwenhuizen, T.M . (2000). Extraction of work from a single thermal bath in the quantum regime. *Phys. Rev. Lett*., 85, 1799–1802.

[27] Scully, M.O., Zubairy, M.S., Agarwal, G.S., Walther, H. (2003). Extracting work from a single heat bath via vanishing quantum coherence. *Science*, 299, 862–864.

[28] Kish, L.B. (2011). Thermal noise engines. *Chaos Solitons Fractals*, 44, 114–121,

http://arxiv.org/abs/1009.5942

[29] Kish, L.B. (2009). Noise-based logic: Binary, multi-valued, or fuzzy, with optional superposition of logic states. *Phys. Lett*., *A*, 373, 911–918.

[30] Kish, L.B., Khatri, S., Sethuraman, S. (2009). Noise-based logic hyperspace with the superposition of 2^N states in a single wire. *Phys. Lett*., *A*, 373, 1928–1934.

[31] Bezrukov, S.M., Kish, L.B. (2009). Deterministic multivalued logic scheme for information processing and routing in the brain. *Phys. Lett*., *A*, 373, 2338–2342.

[32] Gingl, Z., Khatri, S., Kish, L.B. (2010). Towards brain-inspired computing. *Fluct. Noise Lett*., 9, 403–412.

[33] Kish, L.B., Khatri, S., Horvath, T. (2011). Computation using noise-based logic: Efficient string verification over a slow communication channel. *Eur. J. Phys*., B, 79, 85–90, *http://arxiv.org/abs/1005.1560*

[34] Peper, F., Kish, L.B. (2011). Instantaneous, non-squeezed, noise-based logic. *Fluct. Noise Lett*., 10, 231–237, *http://www.worldscinet.com/fnl/10/1002/open-access/S0219477511000521*

[35] Wen, H., Kish, L.B., Klappenecker, A., Peper, F. (June 2012). New noise-based logic representations to avoid some problems with time complexity. *Fluct. Noise Lett*., 11, 1250003.

[36] Mullins. J. (2010). Breaking the noise barrier. New Scientist, 2780, *http://www.newscientist.com/article/mg20827801.500-breaking-the-noise-barrier. html?full=true*

[37] Kish, L.B. (2006). Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law. *Phys. Lett*., *A*, 352, 178–182.

[38] Cho, A. (2005). Simple noise may stymie spies without quantum weirdness. *Science*, 309, 2148, *http://www.ece.tamu.edu/~noise/news_files/science_secure.pdf*

[39] Kish, L.B. (2006). Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson(-like)-noise cipher and expansion by voltage-based security. *Fluct. Noise Lett*., 6, L57–L63, *http://arxiv.org/abs/physics/0512177*

[40] Mingesz, R., Gingl, Z., Kish, L.B. (2008). Johnson(-like)-noise-Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line. *Phys. Lett*., *A*, 372, 978–984.

[41] Palmer, D.J. (2007). Noise encryption keeps spooks out of the loop. *New Scientist*, 2605, 32, *http://www.newscientist.com/article/mg19426055.300-noise-keeps-spooks-out-of-the-loop.html*

[42] Kish, L.B., Horvath, T. (2009). Notes on recent approaches concerning the Kirchhoff-law-Johnson-noise-based secure key exchange. *Phys. Lett*., A, 373, 901–904.

[43] Scheuer, J., Yariv, A. (2006). A classical key-distribution system based on Johnson (like) noise – How secure? *Phys. Lett*., A, 359, 737–740.

[44] Kish, L.B., Scheuer, J. (2010). Noise in the wire: The real impact of wire resistance for the Johnson(-like) noise based secure communicator. *Phys. Lett*., *A*, 374, 2140–2142.

[45] Kish, L.B. (2006). Response to Scheuer-Yariv: "A classical key-distribution system based on Johnson (like) noise – How secure?". *Phys. Lett*., *A*, 359, 741–744.

[46] Hao, F. (2006). Kish's key exchange scheme is insecure. *IEE Proc. Inform. Soc*., 153, 141–142.

[47] Kish, L.B. (2006). Response to Feng Hao's paper "Kish's key exchange scheme is insecure". *Fluct. Noise Lett*., 6, C37–C41.

[48] Liu, P.L. (2009). A new look at the classical key exchange system based on amplified Johnson noise. *Phys. Lett*., *A*, 373, 901–904.

[49] Horvath, T., Kish, L.B., Scheuer, J. (2011). Effective privacy amplification for secure classical communications. *Europhys. Lett*., 94, 28002, *http://arxiv.org/abs/1101.4264*

[50] Kish, L.B., Saidi, O. (2008). Unconditionally secure computers, algorithms and hardware. *Fluct. Noise Lett*., 8, L95–L98.

[51] Kish, L.B., Mingesz, R. (2006). Totally secure classical networks with multipoint telecloning (teleportation) of classical bits through loops with Johnson-like noise. *Fluct. Noise Lett*., 6, C9–C21.

[52] Kish, L.B,, Peper, F. (2012). Information networks secured by the laws of physics. *IEICE Trans. Commun*., E95–B, 1501–1507.

[53] *http://en.wikipedia.org/wiki/Quantum_computer*

[54] Wiesner, S. (1983). Conjugate coding. *SIGACT News*, 15, 78–88.

[55] Bennett, C.H., Brassard, G. (1983). Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing. *In Proc. IEEE Int. Symp. Inform. Theor*., St-Jovite, Canada, 91.

[56] Brassard, G., (2005). Brief history of quantum cryptography: A personal perspective. *In Proc. IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security*, Awaji Island, Japan, 19–23.

[57] Xu, F., Qi, B., Lo, H.K. (2010). Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys*., 12, 113026, *http://arxiv.org/abs/1005.2376*

[58] Liang, Y., Poor, H.V., Shamai, S. (2008). Information theoretic security. Foundations Trends Commun. *Inform. Theory*, 5, 355–580, DOI: 10.1561/0100000036.

[59] Vincent Poor, private communication.