May 19, 2013.

Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange

Yessica Saez, Laszlo B. Kish

Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843-3128, USA

Abstract

A method to quantify the error probability at the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange is introduced. The types of errors due to statistical inaccuracies in noise voltage measurements are classified and the error probability is calculated. The results are demonstrated with practical considerations.

Introduction

1.1 The KLJN secure key exchange

In today's era, network security has become one of the most important aspects in everyday life. Whether it is a large, small, private, or a government organization, it is very important to focus on security, especially when the data being sent, received, or stored contain confidential, sensitive information, such as personal information.

In private-key based secure communication, the two communicating parties (Alice and Bob) generate and share a secure key, which is typically represented by a random bit sequence. It is important to note that the security of a communication cannot be better than the security of the exchange of the key it uses. During this key exchange, the eavesdropper (often referred to as Eve) is continuously monitoring the related data. In today's Internet-based secure communications, typically a software–based key generation and distribution is utilized. However, in this method the whole information about the secure key is publicly available [1] and Eve's access to this information is limited only by her computational power. In other words, this method provides only a (*computationally*) *conditional* security level, which represents a non-future-proof-security [2-4]. It means that with a sufficiently enhanced computation power or an efficient future algorithm, Eve may be able to crack the key and all the information in the communication may become accessible.

Therefore, scientists and researchers have been working on exploring proper laws of physics to find new key exchange schemes where the information that can be measured by Eve is zero. Particularly, they have been exploring key exchange schemes where the amount of information extracted by Eve does not depend on her computational power. When the security measures are determined at Eve's maximal ability (limited only by the laws of physics and the protocols working conditions), that is referred as *unconditional security*, a term that is often interchanged with *information theoretic security* [1]. Information theoretic (unconditional) security can be *perfect* if Eve can extract no information, or *imperfect*, if Eve can extract only a small, commonly accepted amount of information. (This is allowed for practical purpose because this small information leak can further be decreased by privacy amplification, if the fidelity of the key exchange between Alice and Bob is good enough.) These terms are often misunderstood, and it is a frequent mistake in claims to misuse *unconditional security and imply perfect security* by that.

It is important to emphasize that the goal to generate/distribute a perfectly secure key is similar to approaching infinity. Perfectly secure key distribution of a key of finite length can never be reached with a real physical system within a finite duration of time. However, it is one of the goals of physical informatics to find out schemes that can arbitrarily approach (though never reach) perfect security [2].

The earliest and most famous scheme based on the laws of physics that is claiming unconditional security is the Quantum Key Distribution (QKD) [5]. The information theoretic security of this scheme is usually based on the assumption that Eve's actions will disturb the system (in accordance with the theory of quantum measurements and the no-cloning theorem) and cause errors, which uncover the eavesdropping. Note, there are some promising non-QKD initiatives that involve new types of quantum effects [6, 7].

At the fundamental side, there are ongoing debates between experts about the reachable levels of security in QKD [8-12]. At the practical side, there are some issues associated with this scheme, such as range, price, and robustness. Moreover, it is interesting to note that recently all the commercial QKD devices and many laboratory devices have been cracked by quantum-hacking [13-27]. While most of these practical weaknesses seem to be design flaws, not fundamental security problems; they still mean that current practical QKD has yet conditional security: the conditions are that Eve is not knowledgeable enough or she does not have the proper hardware to utilize the design flaws for an attack. The impressive list of papers [13-27] shows that there are enough knowledgeable Eves out with sufficient resources at the moment.

Until 2005 QKD was the only accepted scheme that was able to offer a key exchange with information theoretic security in the ideal (mathematical) situation. In 2005, the Kirchhoff-Law-Johnson-(like)-Noise (KLJN) secure key distribution was introduced [28], where the term "totally secure" was used instead of the correct "perfectly secure" expression. Later (2006), the KLJN system had been built and demonstrated [29]. KLJN is also a key exchange scheme with

information theoretic security [3] and it is based on Kirchhoff's Loop Law of quasi-static electrodynamics and the Fluctuation and Dissipation theorem of statistical physics. Its security against passive attacks is ultimately based on the Second Law of Thermodynamics [28], which means that it is as hard to crack the key exchange as to build a perpetual motion machine (of the second kind). At practical conditions it uses enhanced (electronically generated) Johnson noise with high noise temperature, where quasi-static and thermodynamic aspects must be emulated as exactly as possible in order to approach perfect security.

First, we present a brief description (based on [2-4, 28]) of the working principle of the KLJN system. The core KLJN system, without the defense circuitry against invasive attacks and vulnerabilities represented by non-ideal building elements is shown in the following figure.

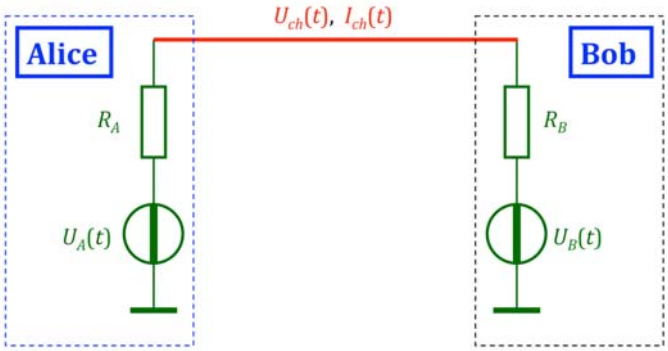

Figure 1. Outline of the core KLJN secure exchange scheme [2-4, 28] without the defense elements against active (invasive) attacks or attacks utilizing non-ideal components and conditions.

The core KLJN channel, see Fig. 1, is a wire line to which Alice and Bob connect randomly selected resistors R_A and R_B, respectively, where $R_A, R_B \in \{R_0, R_1\}$. R_0 represents the low (0) bit and R_1 the high (1) bit, respectively [28]. At the beginning of each bit exchange period, BEP, (also called KLJN clock period), Alice and Bob, who possess identical pairs of the resistors R_0 and R_1, randomly select and connect one of these resistors. The Gaussian voltage noise generators represent either the Johnson noises of the resistors or external noise generators delivering band-limited white noise with publicly known bandwidth and effective noise temperature T_{eff} [2, 3, 28, 29]. The noise voltages of Alice and Bob are $U_A(t)$ and $U_B(t)$, respectively, where $U_A(t) \in \{U_{0,A}(t), U_{1,A}(t)\}$ and $U_B(t) \in \{U_{0,B}(t), U_{1,B}(t)\}$ yield a channel noise voltage $U_{ch}(t)$ between the wire line and the ground and a channel noise current $I_{ch}(t)$ in the wire.

Alice and Bob measure the mean-square noise voltage and/or current amplitudes, that is $\langle U_{ch}^2(t) \rangle$ and/or $\langle I_{ch}^2(t) \rangle$, within the BEP in the line. Thus, by applying Johnson's noise formula

and Kirchhoff's loop law the theoretical prediction is that the mean-square noise voltage and current (i.e. the integral of the corresponding power spectral densities [2,28]) for a given channel noise bandwidth B_{KLJN} and temperature T_{eff} are given as follows:

$$\left\langle U_{ch}^2(t)\right\rangle = S_{u,ch}(f)B_{KLJN} = 4kT_{eff}R_{\|}B_{KLJN}$$
$$\left\langle I_{ch}^2(t)\right\rangle = S_{i,ch}(f)B_{KLJN} = 4kT_{eff}\frac{1}{R_{loop}}B_{KLJN} \quad , \tag{1}$$

where $\left\langle\ \right\rangle$ represents ideal (infinite-time) time average, $S_{u,ch}(f)$ is the power density spectrum of channel voltage noise, $S_{i,ch}(f)$ is the power density spectrum of channel current noise, k is the Boltzmann constant, $R_{\|} = R_A R_B/(R_A + R_B)$ and $R_{loop} = R_A + R_B$.

Ideally, by comparing the result of the accurate measurement of the mean-square channel voltage or current with the corresponding theoretical value in Eq. 1, the total loop resistance will be publicly known. Alice and Bob know their own resistor values and thus they can deduce that resistance value from the loop resistance to learn the resistance at the other end. Consequently, they can distill the actual bit value at the other side of the wire.

If Alice and Bob use the same resistance values, Eve can also recognize that bit situation because the total resistance is either the lowest or the highest value of the three possible resistance values. Thus, the resistor situations (R_0, R_0) and (R_1, R_1) represent a non-secure bit exchange since Eve can also find out the resistors values, their exact locations, and the status of the bits. On the other hand, the cases (R_0, R_1) and (R_1, R_0), which yield identical mean-square noise in the line, represent a secure bit exchange situation because Eve is unable to locate the resistors, therefore, she cannot decide if Alice (and Bob) has a bit 1 or 0. This security is provided by the Second Law of Thermodynamics, which prohibits any directional information concerning the resistors at the two sides in thermal equilibrium [2,28]. In other words, it is as difficult to extract these secure bits by Eve as to build a perpetual motion machine (of the second kind). In conclusion, on average, 50% of the bits can be kept because they are secure. The other 50% of the bits representing the non-secure situations is discarded by the protocol.

Note: the securely exchanged bits have opposite values at Alice and Bob, thus they must publicly agree which one of them will invert the exchanged bit to have identical keys at the two ends.

The fully armed KLJN system is secure even against the man-in-the-middle-attack [30]. One of the important potential applications [32] is to integrate the KLJN system on computer chips and provide unconditional security within computers and high-security instrumentations where the processors, hard drives, keyboards, etc. would secure their communications by keys shared via the KLJN protocol. Another, potential application is, at a much greater scale, to build a network

of KLJN systems utilizing already existing wire lines [4, 33, 34], particularly, realizing and unconditionally secure "smart grid" [4] (advanced electrical power distribution network).

1.2 Known attack types

Below, based on [2], we briefly survey all the published attack types. Due to the simplicity of the KLJN system, there are very few attack types available. The method of comparing the instantaneous values of voltage and current at the two ends and discarding risky 01/10 bits [28, 30, 31] (not discussed here in details) protects against all these types of attacks. But even without discarding the risky bits, passive attacks by Eve utilizing non-idealities suffer from weak signal-to-noise ratio due to poor statistics, see below.

A practically unimportant but theoretically valid type of attack was shown by Hao [36] who pointed out that the non-ideal situation of different temperatures could separate the noise levels of the 01 and 10 bit situations, thus they could give out some information to Eve. In a response by Kish [37], it was pointed out that practical problems of accuracy do not challenge the conceptual security of ideal schemes and was estimated that, even at practical situations, the information leak is negligible due to this attack. Later, it was shown in the experimental paper of Mingesz et al. [29] that a modest 14-bit accuracy of temperatures (noise generators) practically prohibit Eve to extract any useful information (with information leak less than 10^{-10}) by utilizing the Hao attack.

Scheuer and Yariv [38] analyzed the case of non-zero wire resistance where the mean-square voltages are different at the two ends in the case of the 01 and 10 bit situations. However, their calculation was incorrect including the physical units of some of the main results. Kish and Scheuer [39] carried out new, correct calculations and showed that the actual effect is about 1000 times weaker than predicted by Scheuer and Yariv. Earlier, Kish pointed out [37] in his response to [36] that at similar conditions Eve's statistic was very poor and the extracted information was practically miniscule even without the defense of discarding the risky bits. This claim was experimentally verified by Mingesz et al. [29], who showed that at clock period of 50 times of the noise correlation time, $R_0 = 2000\ \Omega$, $R_1 = 9000\ \Omega$, and wire resistance $200\ \Omega$, the information leak of exchanged raw bits to Eve was 0.19% while the fidelity between Alice and Bob was 99.98%. These results indicate that the key exchange has excellent fidelity even without error correction and that the security can be made reasonably good even without dropping the risky 01/10 bits (after current/voltage comparison at the two ends) and without privacy amplification [29].

Liu [41] used a cable simulator to evaluate the impact of delays and reflections on the security. He obtained the surprising results that, with the experimental parameters [6], Eve successfully guessed 70-80% of the key bits. In a critical study of Lui's simulations, Kish and Horvath [31]

pointed out that the chosen wave impedances of the simulated cable to reach these results were unphysical: for example, a center wire diameter of 1 millimeter implies a coaxial cable with outer diameter of 28000 times greater than the size of the known universe.

Observing transients after switching the resistors has been mentioned as a potential source of information leak; however, so far they have never been utilized. During the experimental studies, the noise was ramped up at the beginning of the clock period and ramped down at the end, thus the switching of resistors took place when the voltage and currents were zero in the line.

Note, a fully transient-free protocol is described in a recent work [48].

According to [40], one of the most efficient attack types would be utilizing capacitive currents via the cable capacitance, though it has never been tested. Mingesz et al. [29] showed a hardware based defense "capacitance killer" against this attack. Ultimately, the method of discarding the risky bits after current/voltage comparison at the two ends [28, 30, 31] and/or, in the case of negligible error probability, privacy amplification [35] are the tools to approach perfect security.

1.3 Bit errors in the KLJN key exchange

Due to the finite duration τ of the bit exchange period BEP, the measurement results of mean-square amplitudes have statistical inaccuracies. The duration τ of the BEP must be long-enough compared to the correlation time of the noise (approximately the reciprocal noise-bandwidth B_{KLJN}^{-1}) to achieve a satisfactory statistics and safely distinguish between the different resistor situations. Still, with a low probability, these uncertainties can trigger a bit error.

In the experimental demonstration Mingesz et al. [29] were able to optimize the system to have a fidelity of 99.98% (error probability 0.02%) however no mathematical analysis or design tools have been shown to address this problem. Therefore, our goal in this paper is to classify the different types of bit errors in the ideal KLJN system and analyze their impact.

Discussions and Results

2.1 KLJN Errors

In this "startup" paper about error analysis, we assume the ideal situation of the KLJN system where all the non-ideal features of real systems are neglected. The error analysis of non-ideal systems will be done in future works.

Bit errors occur when the actual value of the mean-square noise results in an incorrect bit interpretation. Figure 2 represents the mean-square channel noise voltage levels, where $\langle\ \rangle_\tau$

indicates finite (τ) time average implying random fluctuations (statistical errors) around the real mean-square value.

The 11 bit situation (when Bob's and Alice's chosen resistors are R_1 and their noise voltages are $U_{1,A}(t)$ and $U_{1,B}(t)$, respectively) results in the mean-square channel noise voltage $\left\langle u_{11}^2(t)\right\rangle_\tau$. Similarly the 01/10 situations yield $\left\langle u_{01/10}^2(t)\right\rangle_\tau$ and the 00 bit arrangement results in $\left\langle u_{00}^2(t)\right\rangle_\tau$. The threshold value Δ_1 provides the boundary between interpreting the measured mean-square values as $\left\langle u_{00}^2(t)\right\rangle$ when $\left\langle U_{ch}^2(t)\right\rangle < \left\langle u_{00}^2(t)\right\rangle + \Delta_1$; or $\left\langle u_{01/10}^2(t)\right\rangle$ when $\left\langle U_{ch}^2(t)\right\rangle \geq \left\langle u_{00}^2(t)\right\rangle + \Delta_1$. Similarly, the threshold value Δ_2 provides the boundary between interpreting the measured mean-square values as $\left\langle u_{11}^2(t)\right\rangle$ when $\left\langle U_{ch}^2(t)\right\rangle > \left\langle u_{11}^2(t)\right\rangle - \Delta_2$; and $\left\langle u_{01/10}^2(t)\right\rangle$ when $\left\langle U_{ch}^2(t)\right\rangle \leq \left\langle u_{11}^2(t)\right\rangle - \Delta_2$.

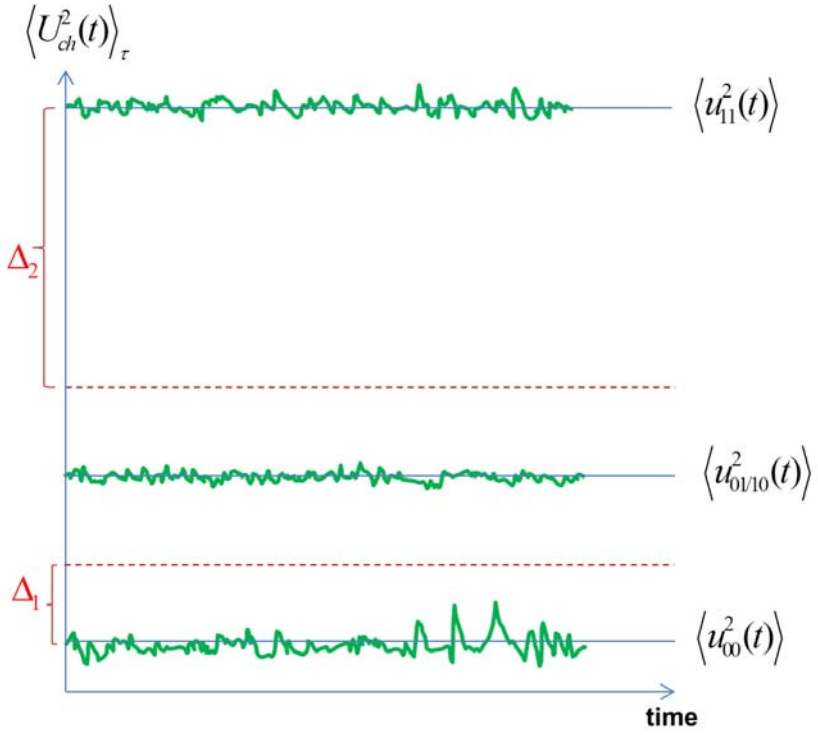

Figure 2. Illustration of the fluctuations of the finite-time mean-square voltage levels around their exact value and thresholds for interpretation (the scale is arbitrary).

An example for a bit error is the rare occurrence when the finite-time mean-square voltage of the 00 case, $\left\langle u_{00}^2(t)\right\rangle_\tau \geq \left\langle u_{00}^2(t)\right\rangle + \Delta_1$, is interpreted as the 01/10 bit situation, which is incorrect and an example of a bit error.

The different types of errors are shown in Table 1.

Table 1. Types of errors in the KLJN bit exchange.

		Actual Situation		
		00	11	01/10
Measurement Interpretation (Decision)	00	Correct (no error)	Error, Removed (automatically)	Error, Removed (automatically)
	11	Error, Removed (automatically)	Correct (no error)	Error, Removed (automatically)
	01/10	Error * (probability?)	Error * (probability?)	Correct (no error)

***The rest of the paper addresses these errors and their probability.**

Some of the errors situations, as shown in Table 1, are considered to be self-corrected by the protocol. This is because, as aforementioned, the 00 and 11 bit situations are discarded.

The rest of the paper is dealing with the analysis of errors indicated with * in Table 1.

2.2 Error probabilities in the KLJN scheme

Alice and Bob can calculate the total resistance in the system by measuring the mean-square noise voltage and/or current amplitudes, that is, $\left\langle U_{ch}^2(t)\right\rangle_\tau$ and/or $\left\langle I_{ch}^2(t)\right\rangle_\tau$. Below we evaluate the errors in the former case while the case of current-based evaluation can be done in a very similar fashion.

2.2.1 Error probability due to inaccuracies in noise voltage measurements

a) Probability of the 00 ==> 01/10 type errors

Let $R_0 = R$ and $R_1 = \alpha R$ for $\alpha > 1$. Then, the mean-square channel noise voltage for infinite-time average at the 00 bit situation is given as:

$$\left\langle u_{00}^2(t) \right\rangle = S_{00}(f) B_{KLJN}\,, \tag{2}$$

where $S_{00}(f) = S_{u,ch}(f)$ at the bit situation 00. Because $R_{\|} = R/2$, from Eq. 1, we obtain:

$$\left\langle u_{00}^2(t) \right\rangle = 2kT_{eff} R B_{KLJN} \tag{3}$$

During the BEP, only the duration τ is available for Alice, Bob and Eve to determine the mean-square channel noise because, after that, a new bit exchange begins. The block diagram of the measurement process is shown in Fig. 3.

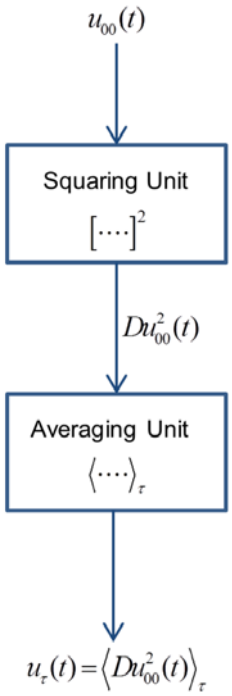

Figure 3. Illustration of the measurement process at 00.

The channel voltage enters into a squaring unit. At its output, the signal is still voltage (because it is a voltage-signal-based electronics) and the numerical value of its instantaneous amplitude is equal to the square of the instantaneous amplitude of the input voltage. This fact is

mathematically expressed by $Du_{00}^2(t)$, where $D=\frac{1}{\text{Volt}}$ is the transfer coefficient of the device to provide a Volt unit also for the square [42]. After averaging for the finite-time τ duration, the obtained measurement result is $u_\tau(t)=\left\langle Du_{00}^2(t)\right\rangle_\tau$, where the averaging can be represented by a low-pass filtering with cut-off frequency $f_B\approx 1/\tau$.

While $u_{00}^2(t)$ is not Gaussian, $u_\tau(t)$ is Gaussian with high accuracy, due to the Central Limit Theorem, because τ is much longer than the correlation time of the noise-component of $u_{00}^2(t)$, that is, $f_B << B_{KLJN}$. Thus, the 00 ==> 01/10 error probability, which is the probability of $u_\tau(t)>\Delta_1$ can exactly be given by the error function. However, the evaluation of the error function requires numerical integration, which implies that the final result is not an analytic formula.

To have an analytic formula, which is a good approximation and has the exact scaling in the small error probability limit (that is, when $\left\langle u_\tau^2(t)\right\rangle << \Delta_1$) we use Rice's formula [43, 44] of threshold crossing frequency, see similar solutions for estimating the probability of thermal noise induced switching errors [45-47]. According to Rice, the mean frequency ν of crossing the level Δ_1 by a Gaussian with power density spectrum $S_\tau(f)$ is given as:

$$\nu(\Delta_1)=\frac{2}{\hat{u}_\tau}\exp\left(\frac{-\Delta_1^2}{2\hat{u}_\tau^2}\right)\sqrt{\int_0^\infty f^2 S_\tau(f)\,df} \tag{4}$$

where $S_\tau(f)$ is the power density spectrum of u_τ while $\hat{u}_\tau$ is its RMS value, $\hat{u}_\tau=\sqrt{\left\langle u_\tau^2(t)\right\rangle}=\sqrt{\int_0^\infty S_\tau(f)\,df}$.

The estimation of error probability is based on the fact that, in the small error limit, the probability of repeated threshold crossings within the correlation time of the band-limited noise converges to zero. Moreover, the correlation time of u_τ is approximately equal to τ thus each threshold crossing (in a chosen but fixed direction) will indicate an independent error and the ratio of the mean threshold crossing frequency $\nu(\Delta_1)$ and τ yields the approximate error probability in this limit [45, 46]. Below, we proceed in this way.

Let us specify the Δ_1 threshold level as a fraction of the *measured* mean-square channel noise, where the transfer coefficient *D* of the squaring unit is also taken into the account:

$$\Delta_1=\beta\left\langle Du_{00}^2(t)\right\rangle=\beta D S_{00}(f)B_{KLJN}\ ,\quad \text{where } 0<\beta<1\ . \tag{5}$$

According to [42], the power density spectrum, $S_{2,00}(f)$, of the AC component of $u_{00}^2(t)$ is given as (note typos of missing "2" in Eqs. 6 and 7 of [42]), see Fig. 4:

$$S_{2,00}(f) = 2D^2 B_{KLJN} S_{00}^2(f)\left(1 - \frac{f}{2B_{KLJN}}\right) \quad \text{for} \quad 0 \le f \le 2B_{KLJN} \quad \text{and} \quad S_{2,00}(f) = 0 \quad \text{otherwise} \qquad (6)$$

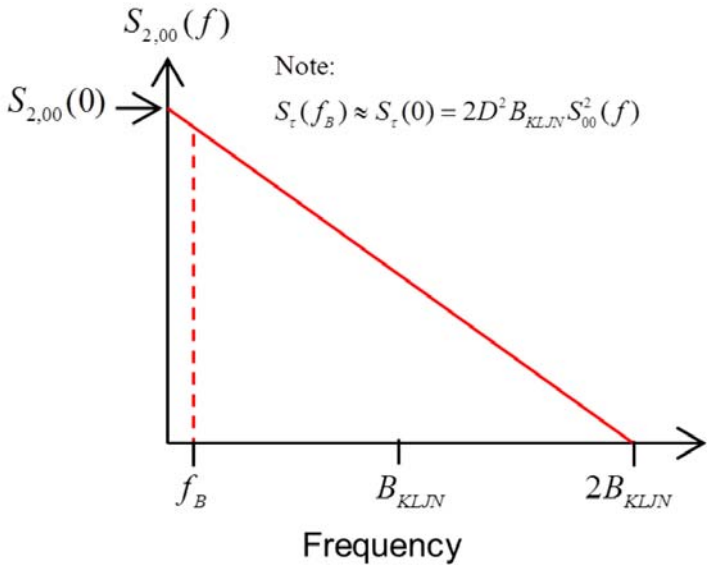

Figure 4. Power Spectral Density (PSD) of the product of two independent noises.

The low-pass filtering effect of the time averaging cuts off this spectrum for $f > f_B$ but keeps the $S_{2,00}(f)$ spectrum for $f < f_B$. Because $f_B << B_{KLJN}$, the value of $S_{2,00}(f)$ within the f_B frequency band can be approximated by its maximum, $S_\tau(f) \approx S_{2,00}(0)$. Figure 5 summarizes these findings.

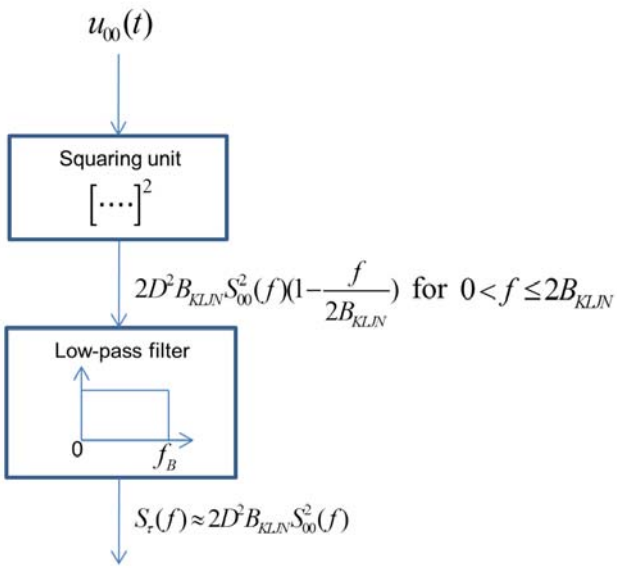

Figure 5. Spectra at the 00 bit situation.

Let us suppose that $B_{KLJN} / f_B = \gamma$. Then,

$$\hat{u}_\tau = \sqrt{\int_0^\infty S_\tau(f)df} \approx \sqrt{f_B S_{2,00}(0)} = \sqrt{2D^2\gamma f_B^2 S_{00}^2(f)} \tag{7}$$

The frequency $\nu_\uparrow(\Delta_1)$ of unidirectional level crossings is half of the level crossing frequency predicted by the Rice formula:

$$\nu_\uparrow(\Delta_1) = \frac{1}{\hat{u}_\tau}\exp\left(\frac{-\Delta_1^2}{2\hat{u}_\tau^2}\right)\sqrt{\int_0^\infty f^2 S_\tau(f)df} \quad , \tag{8}$$

where

$$\Delta_1 = \beta D S_{00}(f)\gamma f_B \tag{9}$$

From Eqs. 7 and 9, we obtain

$$\nu_\uparrow(\Delta_1) = \frac{f_B}{\sqrt{3}}\exp\left(\frac{-\beta^2 D^2 S_{00}^2(f)\gamma^2 f_B^2}{4D^2\gamma f_B^2 S_{00}^2(f)}\right) = \frac{f_B}{\sqrt{3}}\exp\left(\frac{-\beta^2\gamma}{4}\right) \tag{10}$$

In the high threshold situation the errors follow a Poisson statistics, thus the error probability during a time interval is equal to the expected numbers of errors within this interval provided this number is much less than 1.

Thus the probability ε_{00} of 00==>01/10 type of errors in the case of $\varepsilon_{00} << 1$ is:

$$\varepsilon_{00} \approx \nu_{\uparrow}(\Delta_1)\tau \approx \frac{\nu_{\uparrow}(\Delta_1)}{f_B} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\beta^2\gamma}{4}\right) \tag{11}$$

It is important to realize that the error probability is an exponential function of the parameters. The γ parameter (which is proportional to the length of time average) is particularly important because it is not limited in size.

b) Probability of the 11 ==> 01/10 type errors

We can follow the same procedure as above. Instead of β we introduce δ with similar meaning, see Fig. 2 and Eq. 5:

$$\Delta_2 = \delta\left\langle Du_{11}^2(t)\right\rangle = \delta DS_{11}(f)B_{KLJN} = \delta\gamma DS_{11}(f)f_B\ , \qquad 0 < \delta < 1 \tag{12}$$

where Δ_2 is the threshold for the 11==>01/10 type errors and $S_{11}(f)$ is the channel noise spectrum at the 11 bit situation.

The same type of calculations as given above yields the probability ε_{11} of 11==>01/10 type errors:

$$\varepsilon_{11} = \frac{\nu(\Delta_2)}{f_B} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\delta^2\gamma}{4}\right) \text{ for } 0 < \delta < 1 \tag{13}$$

The error probability is again an exponential function of the parameters.

2.3 Illustration of the results with practical parameters

To demonstrate the results, we assign possible practical values to the parameters.

For $\gamma = 100$ and $\beta = 0.5$ the bit error probability ε_{00} is:

$$\varepsilon_{00} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\beta^2\gamma}{4}\right) \approx 0.001 \tag{14}$$

This value may look too large, however, just by increasing the γ parameter (and the time average window τ) by a factor of 2, and in this way slowing down the bit exchange by the same factor, will result in the square of the above error probability value:

$$\varepsilon_{00} \approx 10^{-6} \quad , \tag{15}$$

which is satisfactory for many application. It is important to note that no error correction algorithm is used for this error reduction.

Methods and Conclusions

We have classified and analyzed the types of errors of bit exchange between Alice and Bob in the KLJN secure key exchange. Some types of errors are automatically removed by the original protocol. We mathematically analyzed the error probabilities and their dependence on the KLJN parameters of the errors that are not removed by the protocol. We identified the important parameters and the results show that the error probability decays exponentially by increasing these parameters. The most important of such parameters is the duration τ of key exchange because its value is not limited. The results indicate that it is reasonable to achieve error probabilities that are small enough to avoid the need for error correction algorithms.

Further open questions are how to combine current and voltage measurements to further reduce these errors and what is the error situation in the new advanced KLJN protocols proposed recently [48].

References

[1] Liang Y, Poor HV, Shamai S (2008) Information theoretic security. Foundations Trends Commun. Inform. Theory 5:355-580. DOI: 10.1561/0100000036.

[2] Mingesz R, Kish LB, Gingl Z, Granqvist CG, Wen H, Peper F, Eubanks T, Schmera G (2013) Unconditional Security by the laws of classical physics. Metro. & Measu. Syst. XX:3-16. DOI: 10.2478/mms-2013-0001.http://www.degruyter.com/view/j/mms.2013.20.issue-1/mms-2013-0001/mms-2013-0001.xml

[3] Mingesz R, Kish LB, Gingl Z, Granqvist CG, Wen H, Peper F, Eubanks T, Schmera G (2013) Information Theoretic Security by the laws of classical physics. Soft Computing Applications, Adv. in Int. Syst. and Comp. 195:11-25.

[4] Gonzalez E , Kish LB, Balog R, Enjeti P(2013) Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters, arXiv:1303.3262.

[5] Bennett CH, Brassard G, Breidbart S, Wiesner S (1982). Quantum cryptography, or Unforgeable subway tokens. Advances in Cryptology: Proceedings of Crypto ’82, Santa Barbara, Plenum Press, pp. 267–275.

[6] Yuen HP (2009) Key Generation: Foundation and a New Quantum Approach, IEEE J. Selec. Tops. in Quan. Elects. 15(6):1630-1645.

[7] Salih H, Li ZH, Al-Amri M, Zubairy H, (2013) Protocol for direct counterfactual quantum communication. Phys. Rev. Lett. 101 (in press). http://arxiv.org/abs/1206.2042.

[8] Yuen HP (2012) On the Foundations of Quantum Key Distribution- Reply to Renner and Beyond, arXiv:1210.2804.

[9] Yuen HP (2012) Unconditional Security in Quantum Key Distributions, arXiv: 1205.5065v2.

[10] Hirota O (2012) Incompleteness and Limit of Quantum Key Distribution Theory, arXiv:1208.2106v2.

[11] Renner R (2012) Reply to Recent Scepticism About the Foundations of Quantum Cryptography, arXiv:1209.2423v.1.

[12] Yuen HP (2012) Security Significance of the Trace distance Criterion in Quantum Key Distribution, arXiv:1109.2675v3.

[13] Merali Z (29 August 2009) Hackers blind quantum cryptographers. Nature News, DOI:10.1038/news.2010.436.

[14] 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. Nat. Comm. 2 349. DOI: 10.1038/ncomms1348.

[15] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V (2010) Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photo. 4:686-689. DOI: 10.1038/NPHOTON.2010.214.

[16] 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.

[17] Makarov V, Skaar J (2008) Faked states attack using detector efficiency mismatch on SARG04, phasetime, DPSK, and Ekert protocols. Quan. Info. and Comp. 8:622-635.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] Lydersen L, Akhlaghi MK, Majedi AH, 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.

[23] 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.

[24] 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.

[25] 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/PhysRevA.84.032320.

[26] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V (2010) Avoiding the blinding attack in QKD; REPLY (COMMENT). Nat. Photo. 4:801-801. DOI:10.1038/nphoton.2010.278.

[27] 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.

[28] Kish LB (2006) Totally secure classical communication utilizing Johnson (-like) noise and Kirchooff’s Law. Phy. Lett. A 352:178-182.

[29] Mingesz R, Gingl Z, Kish LB (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.

[30] Kish LB (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.

[31] Kish LB, Horvath T (2009) Notes on recent approaches concerning the Kirchhoff-law-Johnson-noise-based secure key exchange. Phys. Lett. A 373:901-904.

[32] Kish LB, Saidi O (2008) Unconditionally secure computers, algorithms and hardware. Fluct. Noise Lett. 8:L95-L98.

[33] Kish LB, 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.

[34] Kish LB, Peper F (2012) Information networks secured by the laws of physics. IEICE Trans. Commun. E95-B:1501-1507.

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

[36] Hao F (2006) Kish's key exchange scheme is insecure. IEE Proc. Inform. Soc. 153:141-142.

[37] Kish LB (2006) Response to Feng Hao's paper "Kish's key exchange scheme is insecure". Fluct. Noise Lett. 6:C37-C41.

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

[39] Kish LB, 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.

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

[41] Liu PL (2009) A new look at the classical key exchange system based on amplified Johnson noise. Phys. Lett. A 373:901-904.

[42] Kish LB, Mingesz R, Gingl Z, Granqvist CG (2012) Spectra for the product of Gaussian Noises. Metro. & Measu. Syst., XIX: 653-658. DOI: 10.2478/v10178-012-0057-0.

[43] Rice, SO (1944) Mathematical analysis of random noise. Bell System Tech. J. 23: 282–332.

[44] Rychlik, I (2000) On Some Reliability Applications of Rice's Formula for the Intensity of Level Crossings. Extremes (Kluwer Academic Publishers) 3 (4):331 348. doi:10.1023/A:1017942408501.

[45] Kish LB (2002) End of Moore's Law; Thermal (Noise) Death of Integration in Micro and Nano Electronics. Phys. Lett. A. 305:144–149.

[46] Kish LB, Granqvist CG (2012) Electrical Maxwell Demon and Szilard Engine Utilizing Johnson Noise, Measurement, Logic and Control. PLoS ONE 7:e46800. http://www.plosone.org/article/info:doi/10.1371/journal.pone.0046800

[47] Kish LB, Granqvist CG (2012) Energy requirement of control. EPL 98:68001; http://arxiv.org/abs/1110.0197

[48] Kish LB (2013) Enhanced secure key exchange systems based on the Johnson-noise scheme. Metrology & Measurement Systems, Volume XX (accepted for publication). http://vixra.org/abs/1302.0055; http://arxiv.org/abs/1302.3901