ERROR ELIMINATION IN THE KLJN SECURE KEY EXCHANGE AND VEHICULAR APPLICATIONS

A Dissertation

by

YESSICA LISBETH SAEZ BARRIOS

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Laszlo B. Kish
Committee Members,	Jun Zou
	Robert Balog
	Andreas Klappenecker
Head of Department,	Miroslav Begovic

August 2015

Major Subject: Electrical Engineering

ABSTRACT

The Kirchhoff-law-Johnson-noise (KLJN) system is a classical physical secure key exchange scheme based on the Kirchhoff's circuit loop law and the fluctuation-dissipation theorem of statistical physics. This dissertation contains two main studies related to this scheme: bit error analysis and removal, and applications in vehicular communication systems.

The thesis starts with a presentation of some of the challenges faced by modern communications. It also includes a description of the working principle of the KLJN system and the motivation upon which this dissertation is built. Then, a study of the errors in this scheme is carried out. In the first part, the types of errors due to statistical inaccuracies in the voltage-based and current-based measurement modes are classified and analyzed. In both measurement modes and for all types of errors, at fixed bandwidth, the error probabilities decay exponentially versus the duration of the bit sharing period. In the second part, an error removal method is proposed to improve the fidelity of the system. This method is based on the combination of the voltage-based and current-based schemes and it drastically reduces the error probabilities.

The second topic of study in the thesis explores a potential practical application for the KLJN key exchange scheme. First, we present a vehicular communication network architecture with unconditionally secure KLJN keys. Secondly, a new solution for secure KLJN key donation to vehicles is proposed and an upper limit for the lifetime of this key is given.

A summary of the work is given in the last section and the main results of the research are discussed. These contributions include: closed-form expressions for the error probabilities in the KLJN system, error removal methods without the need of implementing any error correcting technique, and a new potential vehicular application for the KLJN scheme. Some of the future research initiatives related to these topics are discussed.

To my sweet and loving parents, to my brother, and to my beloved husband

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Dr. Laszlo B. Kish, for his supervision and support throughout the course of my research at Texas A&M University and for offering his friendly advice well beyond academic matters.

Thanks also go to my committee members, Dr. Zou, Dr. Balog, and Dr. Klappenecker, with whom I shared long hours of discussions and consulted in many occasions. I thank my friends and colleagues and the department faculty and staff for making my time at Texas A&M University a great experience.

I also want to extend my gratitude to the Panamanian Government that supported me through the "Doctorate Scholarship Program" administered by SENACYT and IFARHU. Without their support, this dissertation would not have been written.

I want to give special thanks to my brother, Deeyvid, who has been a source of encouragement and inspiration to me throughout my life. I also want to thank my parents, Eida and Oscar, whose love and encouragement pushed me every day throughout the process. And last but not least, I am very grateful to my best friend and wonderful husband, Edwin, whose practical and emotional support is endless. Without him by my side, I would not have reached this goal.

NOMENCLATURE

AC	Alternating Current
BSP	Bit Sharing Period
BPSK	Binary Phase Shift Keying
CA	Certification Authority
CA2RSD	Certification Authority-to-Roadside Device
CA2RSKP	Certification Authority-to-Roadside Key Provider
CA2V	Certification Authority-to-Vehicle
DC	Direct Current
DSRC	Dedicated Short Range Communication
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
KLJN	Kirchhoff-law-Johnson-noise
MHz	Mega Hertz
NFC	Near Field Communication
OOK	ON/OFF Keying
PKI	Public Key Infrastructure
PSD	Power Spectral Density
QKD	Quantum Key Distribution
RFID	Radio Frequency Identification

RMS	Root Mean Square
RSA	Rivest, Shamir, and Adleman Public-Key Cryptosystem
RSD	Roadside Device
RSD2CA	Roadside Device-to-Certification Authority
RSD2V	Roadside Device-to-Vehicle
RSKP	Roadside Key Provider
RSKP2CA	Roadside Key Provider-to- Certification Authority
RSKP2V	Roadside Key Provider-to-Vehicle
TACKs	Temporary Anonymous Certified Keys
V2CA	Vehicle-to-Certification-Authority
V2RSD	Vehicle-to-Roadside-Device
V2V	Vehicle-to-Vehicle
WAVE	Wireless Access in a Vehicular Environment

TABLE OF CONTENTS

Page

ABSTRACT ii

DEDICATION iv

ACKNOWLEDGEMENTS v

NOMENCLATURE vii

TABLE OF CONTENTS viii

LIST OF FIGURES x

LIST OF TABLES xi

1. INTRODUCTION AND BACKGROUND 1

    1.1 Unconditionally Secure Key Exchange 1
    1.2 The Ideal Kirchhoff-law-Johnson-noise (KLJN) Secure Key Exchange Scheme 7
    1.3 Bit Errors in the KLJN Key Exchange Scheme 21
    1.4 Vehicular Application for the KLJN Key Exchange Scheme 22

2. ANALYSIS OF THE BIT ERRORS IN THE KLJN SECURE KEY EXCHANGE SCHEME 27

    2.1 Mean-square Noise Measurement Process and Bit Interpretations 27
    2.2 Type of Errors in the KLJN Key Exchange Scheme 31
    2.3 Mathematical Approach 32
    2.4 Probabilities of the Different Types of Errors 40
    2.5 A Proposed Error Removal Method 44

3. VEHICULAR APPLICATION OF THE KLJN SECURE KEY EXCHANGE SCHEME 48

    3.1 Unconditionally Secure Key Exchange for Vehicular Communication Networks 48
    3.2 Vehicular Communication Network Model with Unconditionally Secure Key Exchange 50

Page

3.3 KLJN Key Generation in Vehicular Communication Networks 53
3.4 KLJN Key Donation in Vehicular Communication Networks 54
3.5 Upper Limit of the KLJN Key Lifetime in Vehicular Communication Networks 56

4. CONCLUSIONS AND FUTURE WORK 60

4.1 Summary of the Work 60
4.2 Summary of the Contributions 62
4.3 Future Research 63

REFERENCES 65

APPENDIX 72

LIST OF FIGURES

Page

Figure 1 Thermal noise equivalent circuits for resistance R : (a)Thevenin equivalent circuit and (b) Norton equivalent circuit 7

Figure 2 Outline of the core KLJN secure key exchange scheme without defense circuitry (current/voltage monitoring/comparison) against invasive attacks or attacks utilizing non-ideal components and conditions 10

Figure 3 Outline of the core KLJN system minimally armed against invasive (active) attacks or attacks utilizing non-ideal components and conditions 18

Figure 4 A typical vehicular communication network 24

Figure 5 Mean-square channel noise voltage and current measurement process .. 28

Figure 6 Measured mean-square channel noise of voltage (a) and current (b). 30

Figure 7 Power spectral density (PSD) of the product of two independent noise voltages..... 37

Figure 8 PSD of the AC component remaining after the average time window τ in the voltage-based measurement mode 37

Figure 9 Probability of the 00==>01/10 type of errors in the voltage measurements 43

Figure 10 Probability of the 00==>01/10 type of errors in the combined voltage-current method..... 47

Figure 11 Vehicular communication network with unconditionally secure key exchange..... 51

Figure 12 Abstract illustration of roadside key providers delivering an unconditionally secure key to vehicles via near field communication.... 55

Figure 13 Key donation to vehicles with RSKP equipment embedded in the pavement..... 56

LIST OF TABLES

		Page
Table 1	Main features of the QKD and the KLJN secure key exchange schemes	5
Table 2	Types of errors in the KLJN key exchange scheme	32
Table 3	KLJN error removal method with combined voltage-current analysis	45
Table 4	Communications in the vehicular network model with unconditionally secure key exchange	52

1. INTRODUCTION AND BACKGROUND*

1.1 Unconditionally Secure Key Exchange

In today's era, security has become one of the most important issues in communication networks. Whether it is a large, small, private, or a government organization, it is very important to address security, especially when the data being sent, received, or stored contains confidential, sensitive information, such as personal information. Security aspects in communication networks include authentication, accountability and non-repudiation, data confidentiality, and integrity [1]. Authentication ensures that the receiver is able to validate the sender of the message by reading only information sent from legitimate senders. Accountability and non- repudiation guarantee that nodes cannot deny having sent/received a message. Data confidentiality ensures that the communication content remains private and protected the entire time. Integrity

*Part of this section is a modified reprinted version of: Y. Saez and L. B. Kish, Errors and their mitigation at the Kirchhoff-Law-Johnson-Noise secure key exchange, *PLoS ONE* 8 (2013) e81103 (7 pages), © 2013 Saez and Kish.

*Part of this section is reprinted with kind permission from Springer Science+Business Media: Journal of. Computational Electronics, Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law-Johnson-noise secure key exchange, 13, 2014, 271–277, Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, © Springer Science+Business Media New York 2013.

*Part of this section is reprinted with kind permission from: Y. Saez, X. Cao, L. B. Kish, and G. Pesti, Securing Vehicle Communication Systems by the KLJN key exchange protocol, *Fluctuation and Noise Letters* 13 (2014) 1450020 (14 pages), © World Scientific Publishing Company 2014.

*Part of this section is reprinted with kind permission from: X. Cao, Y. Saez, G. Pesti, and L. B. Kish, On KLJN-based secure key distribution in vehicular communication networks, *Fluctuation and Noise Letters*. 14 (2015) 1550008 (11 pages), © World Scientific Publishing Company 2015.

ensures that unauthorized observers cannot read, modify, delete, insert, and/or reorder messages.

Attacks targeting the security of communication networks fall into two categories: *passive (listening) attacks* and *active (invasive) attacks* [1]. *Passive (listening) attacks* involve those attacks in which a malicious adversary attempts to learn or to make use of the information being transmitted without modifying the information or affecting the communication system resources. An example of passive attack includes the situation where the malicious adversary continuously monitors (listens) the communication in order to recognize patterns that could be used to extract the information. In *active (invasive) attacks*, the malicious adversary attempts to gain access to the information by intentionally modifying the system, thus affecting its operation. An example of an active attack is the man in the middle (MITM) attack [1], where the attacker inserts an intermediate node in the communication path and pretends to be one of the two communicating parties in order to extract, insert, and/or modify the information being transmitted. This dissertation focuses primarily on confidentiality aspects of communication networks, and passive attacks are of primary concern in this context.

In symmetric key-based secure communication, the two communicating parties (often referred to as Alice and Bob) generate and share a secure key, which is typically represented by a random bit sequence. This key is used to encrypt and decrypt all the information transmitted between Alice and Bob. During this key exchange, a potential eavesdropper (often referred to as Eve) is continuously monitoring the communication.

Therefore, the security in the communication depends on the capability of Alice and Bob to secretly share this key while Eve is continuously monitoring/listening to the exchange. It is important to note that the security of the communication cannot be better than the security of the key exchange scheme it uses.

In today's internet-based secure communications, typically a software-based key generation and distribution method is utilized. However, Eve's information about the key is limited only by her computation power [1]. In other words, these methods provide only (*computationally*) *conditional* security level, which is not future-proof [2–5]. That is, Eve could record the communication in the present and in the future, when she has access to sufficient computation power, or to an efficient algorithm (to be developed), she could crack the key and all the communicated information becomes accessible.

Therefore, scientists and engineers have been exploring relevant laws of physics to find new secure key exchange schemes. When the communicated signal has full information about the key but Eve cannot access it even if she has unlimited computation power, that is called *unconditional* security, a term that is often interchanged with *information theoretic security* (*i.e.,* zero information about the key for Eve) [1]. In other words, the security measures are determined by information theory or, in physical systems, by measurement (information) theory. Security can theoretically be *perfect* if Eve can extract no information, or *imperfect* (the practical situation), if Eve can extract only a small amount of information. Unconditional security assumes that the practical imperfect security level can arbitrarily approach the perfect security situation provided enough resources are available, such as enough time for privacy amplification

(PA, a software-based technique used to improve the security of a partially exposed key) [6].

It is important to emphasize that the goal to generate/distribute a perfectly secure key is similar to the aim of reaching 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 unconditionally secure schemes that can arbitrarily approach (though never reach) perfect security [2, 3].

The earliest and most famous scheme based on the laws of physics that is claiming unconditional security is quantum key distribution (QKD) [7]. 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 [7]) and cause errors, uncovering the eavesdropping. Note, there are some promising non-QKD initiatives that involve other types of quantum schemes [8, 9].

At the fundamental side, there are ongoing debates between experts about the reachable levels of security in QKD [10–14]. 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 several laboratory systems have been cracked by quantum hacking [15–29]. While most of these practical weaknesses seem to be design flaws, not fundamental security problems; they still mean that before fixing theses weaknesses, QKD had only conditional security: the conditions were that Eve was not knowledgeable enough or she did not have the proper hardware to utilize the design flaws for an attack. The volume of work in [15–29] shows that there

were enough knowledgeable “Eves” out there with sufficient resources to be able to crack QKD devices.

Until 2005, QKD was the only accepted scheme that was able to offer a key exchange with information theoretic security in the ideal (mathematical) limit. In that year, the Kirchhoff-law-Johnson-noise (KLJN) secure key distribution was introduced [30], where the term "totally secure" was used instead of the technically precise "unconditionally secure" expression. Later in 2006, the KLJN system was built and demonstrated in extensive experiments [31]. KLJN is a key exchange scheme with information theoretic security [4] and it is based on Kirchhoff’s circuit loop law and the fluctuation-dissipation theorem of statistical physics. Its security against passive attacks is ultimately based on the second law of thermodynamics [4, 30–33], which means that it is as hard to crack the KLJN key exchange as to build a perpetual motion machine (of the second kind).

Table 1 compares the main features of the QKD and the KLJN key exchange schemes [34].

Table 1 Main features of the QKD and the KLJN secure key exchange schemes

	QKD	**KLJN**
Information carrier	Photons	Electrons
Medium (channel)	Optical fiber or air	Wire
Security level (ideal system)	Information theoretic (unconditional)	Information theoretic (unconditional)
Security foundation	“Non-cloning” theorem of quantum physics	Second law of thermodynamics

Table 1 Continued

	QKD	KLJN
Protection against "man in the middle attacks"?	No (for single raw bits)	Yes (even for single raw bits)
Speed	Low/High (debated)	Low
Range	Few hundred miles (exponential speed-cutoff)	Unlimited (power-law speed-cutoff)
Size	Bulky (desktop instrument size)	Chip-level-integration possible
Cost	Expensive ($100,000 a pair)	Reasonable ($20,000)

This dissertation addresses some special topics about the Kirchhoff-law-Johnson-noise (KLJN) key exchange scheme. In section 1.2, a brief background on thermal noise in resistors is presented. Then, the working principle of the ideal KLJN secure key exchange scheme is explained in detail, along with its main characteristics and features. Sections 1.3 and 1.4 introduce the motivations for our work. Section 2 classifies and analyzes the bit errors in the KLJN system. Then, error removal methods are shown to reduce the bit error probabilities. In section 3, a vehicular communication network with KLJN-based unconditionally secure key exchange is presented. The KLJN key lifetime is analyzed and the procedures for key generation and donation to vehicles are described. Section 4 presents a summary of the results; along with important research initiatives to be considered in the future.

1.2 The Ideal Kirchhoff-law-Johnson-noise (KLJN) Secure Key Exchange Scheme

1.2.1 Thermal noise in resistors

Johnson-Nyquist noise (thermal noise) is the electronic noise caused by the thermal motion of electrons within an electrical conductor. Mr. John B. Johnson, of Bell Telephone Laboratories, was the first to conduct experimental analysis and measurements of this phenomenon in 1926, followed by Dr. Harry Nyquist who was then able to develop the theory behind this phenomenon [35, 36]. Below, based on [37], we present a brief summary of some important concepts related to thermal noise.

The thermal noise equivalent circuits for the resistance R are shown in Fig. 1.

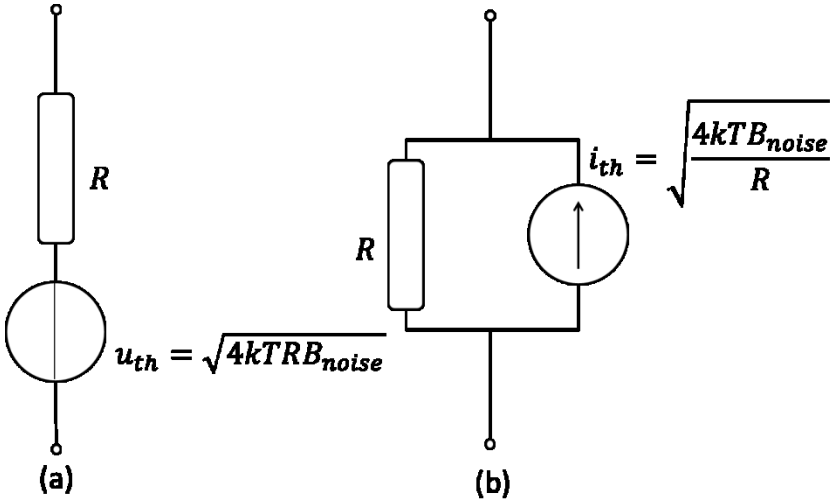

Figure 1 Thermal noise equivalent circuits for resistance R (a) Thevenin equivalent circuit and (b) Norton equivalent circuit

In thermal equilibrium at temperature T, the root-mean-square (RMS) thermal voltage u_{th} on an open-circuit resistance R is:

$$u_{th} = \sqrt{4kTRB_{noise}}, \tag{1}$$

where k is the Boltzmann's constant (1.38×10^{23} J/K), T is the absolute temperature of the resistance in kelvins (K), R is the resistance, and B_{noise} is the bandwidth of the noise of the measurement system in hertz (Hz). According to Norton's theorem, the RMS thermal noise current i_{th} of the resistance R is given by:

$$i_{th} = \sqrt{\frac{4kTB_{noise}}{R}}. \tag{2}$$

The power spectral density (PSD) of a thermal narrowband (1 Hz unit of bandwidth) noise voltage u_{th} on an open-circuit resistance R is given by:

$$S_{u,th}(f) = \frac{u_{th}^2}{B_{noise}} = 4kTR. \tag{3}$$

Due to Ohm's law, the PSD of the noise current i_{th} is:

$$S_{i,th}(f) = \frac{4kT}{R}. \tag{4}$$

From Eqs. (3) and (4), and by applying Kirchhoff's loop law, the PSD of the resultant noise voltage and current on two parallel resistors R_1 and R_2 are:

$$S_{u,th,R_{||}}(f) = 4kTR_{||} = 4kT\frac{R_1R_2}{R_1+R_2} \tag{5}$$

and

$$S_{i,th,R_{loop}}(f) = \frac{4kT}{R_{loop}} = \frac{4kT}{R_1+R_2}, \tag{6}$$

respectively, where $R_{||} = \frac{R_1R_2}{R_1+R_2}$ and $R_{loop} = R_1+R_2$.

1.2.2 The core KLJN key distribution system

Figure 2 shows the fundamental Kirchhoff-law-Johnson-noise (KLJN) key distribution system [2, 4, 30, 31, 38, 39] without defense elements against both active (invasive) attacks and attacks targeting vulnerabilities represented by non-ideal building elements. In this ideal system, all non-idealities such as wire resistance, wire

capacitance, wire inductance, transient effects, etc., are neglected. Therefore, the time-dependent voltage and current are spatially homogenous along the wire ("lumped parameter" model). Under practical conditions, this system utilizes enhanced Johnson noise with high noise temperature, obtained from Gaussian noises generated electronically so that quasi-static and thermodynamic characteristics are emulated as accurately as possible, in order to approach perfect security [40].

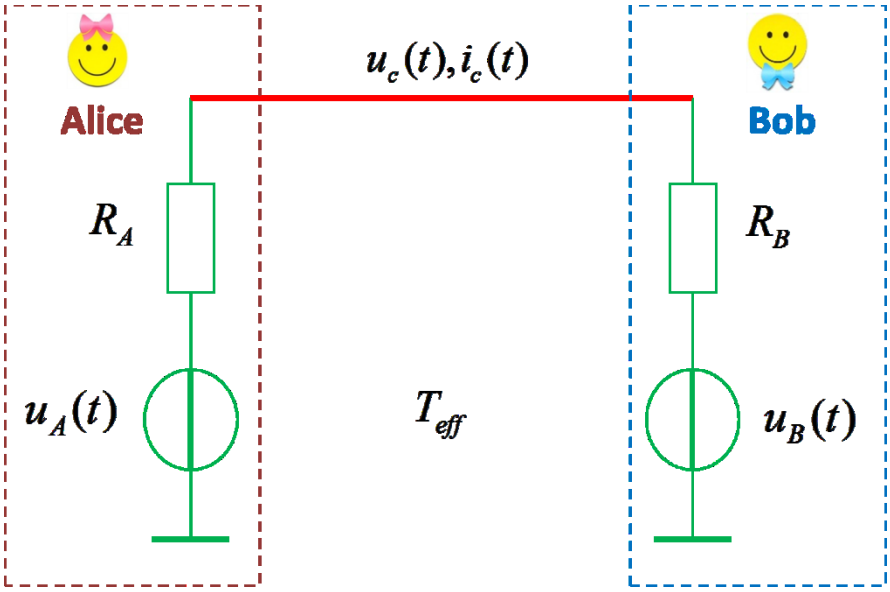

Figure 2 Outline of the core KLJN secure key exchange scheme without defense circuitry (current/voltage monitoring/comparison) against invasive attacks or attacks utilizing non-ideal components and conditions. T_{eff} is the effective noise temperature, R_A, $u_A(t)$, R_B, and $u_B(t)$ are the resistor values and noise voltages at Alice and Bob, respectively. $u_c(t)$ and $i_c(t)$ are channel noise voltage and current, respectively

The core KLJN channel is represented by a wire line. The two communicating parties, "Alice" and "Bob", have an identical closed set of finite non-zero value resistors $\{R_0, R_1\}$, with $R_0 \neq R_1$. Typically, one resistor is about 10 times bigger than the other.

The resistor R_0 indicates the low (0) bit value and the resistor R_1 indicates the high (1) bit value, respectively [30]. At the beginning of each clock period or bit sharing period (BSP), Alice and Bob, who are synchronized in time, randomly choose one resistor from the set $\{R_0, R_1\}$ and connect it to the wire line. Thus, $R_A, R_B \in \{R_0, R_1\}$, as seen in Fig. 2.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 B_{KLJN} and effective noise temperature T_{eff} [2, 30, 31]. According to the fluctuation-dissipation theorem, the enhanced Johnson noise voltages of Alice's and Bob's resistors—denoted $u_A(t)$ and $u_B(t)$ respectively, where $u_A \in \{u_{0,A}(t), u_{1,A}(t)\}$ and $u_B \in \{u_{0,B}(t), u_{1,B}(t)\}$—generate a channel noise voltage $u_c(t)$ between the wire line and ground as well as a channel noise current $i_c(t)$ in the wire.

Within the BSP, Alice and Bob (and Eve) measure the mean-square channel noise voltage and/or current amplitudes, *i.e.*, $\langle u_c^2(t) \rangle$ and/or $\langle i_c^2(t) \rangle$. By applying Johnson's noise formula and Kirchhoff's voltage loop law, it follows Eqs. (5) and (6) that the theoretical values of the mean-square noise voltage and current for a given channel noise bandwidth B_{KLJN} and temperature T_{eff} are [2, 30]:

$$\langle u_c^2(t) \rangle = S_{u,c}(f) B_{KLJN} = 4kT_{eff} R_{||} B_{KLJN} \tag{7}$$

and

$$\left\langle i_c^2(t)\right\rangle = S_{i,c}(f)B_{KLJN} = 4kT_{eff}\frac{1}{R_{loop}}B_{KLJN}, \tag{8}$$

respectively. Here, $\left\langle u_c^2(t)\right\rangle$ and $\left\langle i_c^2(t)\right\rangle$ represent ideal infinite-time averages of the square of the channel noise voltage and current, respectively; $S_{u,c}(f)$ is the power spectral density of the channel noise voltage, $S_{i,c}(f)$ is the power spectral density of the channel noise current, k is Boltzmann's constant, $R_{||} = \frac{R_A R_B}{R_A + R_B}$, and $R_{loop} = R_A + R_B$.

The resistance values $R_{||}$ and/or R_{loop} can be publicly known by comparing the result of the measurements of the mean-square channel noise voltage and/or current amplitudes with the corresponding theoretical values obtained from Eqs. (7) and (8). Alice and Bob know their own chosen resistors, and hence the total resistances $R_{||}$ and/or R_{loop} allow them to deduce the resistance value and actual bit status at the other end of the wire.

The cases when Alice and Bob choose the same resistance values—*i.e.*, the 00 and 11 situations—represent a *non-secure* bit exchange. In these situations, Eve will be able to find the resistor values, their location (*i.e.*, which end of the line has connected R_1 and which end has connected R_0), and the status of the bits, because the total resistance will be either the lowest or the highest value of the three possible magnitudes of the total resistance. The situations when Alice and Bob randomly choose different resistance values—*i.e.*, the 01 and 10 situations—signify a *secure* bit exchange event because these resistances cannot be distinguished by the *measured* mean-square values.

Alice and Bob will know that the other party has the inverse of his/her bit, which implies that a secure key exchange takes place. 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 are discarded by the protocol.

It is important to point out that since the securely exchanged bits have opposite values at Alice and Bob's sides, they must publicly and a priori agree on which one of them will invert the exchanged bit in order to have identical keys at the two ends [40].

1.2.3 Security proof against passive attacks

The ideal KLJN system provides unconditional security against passive (listening) attacks. First, during the *secure* bit exchange situations—*i.e.*, the situations when Alice and Bob have connected different resistors to the wire—the PSD of the channel noise voltage is:

$$S_{u,c}(f) = 4kT_{eff}\,\frac{R_0 R_1}{R_0 + R_1}\,. \tag{9}$$

Due to linear superposition, the PSD shown in Eq. (9) represents the sum of the spectrum of two specific situations [4, 32]. Specifically, $S_{u,c}(f) = S_{0,u,c}(f) + S_{1,u,c}(f)$, where:

$$S_{0,u,c}(f) = 4kT_{eff}R_0\left(\frac{R_1}{R_0+R_1}\right)^2, \tag{10}$$

is the PSD of the channel noise voltage when only the noise generator due to R_0 is running, and

$$S_{1,u,c}(f) = 4kT_{eff}R_1\left(\frac{R_0}{R_0+R_1}\right)^2, \tag{11}$$

is the PSD of the channel noise voltage when only the noise generator due to R_1 is running.

When evaluating unconditional security in the ideal KLJN system, the following question may arise: could Eve discover the resistance values from the mean-square noise voltage and current measurements? The answer is yes. By measuring the mean-square noise voltage and current in the wire, Eve can use the theoretical values to set up a second order equation system and the two solutions will provide the resistance values for R_0 and R_1, that is: $R_{0,1} = \dfrac{4kT_{eff}S_{u,c}(f) \pm \sqrt{\left(4kT_{eff}S_{u,c}(f)\right)^2 - 4S_{u,c}^3(f)S_{i,c}(f)}}{2S_{u,c}(f)S_{i,c}(f)}$. However, in order to extract the key bit, Eve needs to determine the exact location (Alice or Bob) of these resistances.

In order to find out the exact location of the resistors R_0 and R_1, Eve needs to measure and evaluate a physical quantity that provides directional information.

Fortunately, for the case of the ideal KLJN system, the only directional information available to Eve is the direction of the power flow [4, 32]. However, in accordance with the second law of thermodynamics and the energy conservation law, there is no net power flow in a closed system in thermal equilibrium. Consequently, the cross-correlation between voltage and current in the channel is zero—*i.e.*, $\vec{P} = \left\langle u_c(t)\, i_c(\vec{t}) \right\rangle = P_{1\to 0} - P_{0\to 1} = 0$. This is easily proven by showing that the power $P_{0\to 1}$ by which the noise generator due to resistor R_0 is heating resistor R_1 is equal to power $P_{1\to 0}$ by which the noise generator due to resistor R_1 is heating resistor R_0 [4, 32]. This fact can be shown by using Eqs. (10) and (11) for the noise with bandwidth B_{KLJN} as follows:

$$P_{0\to 1} = \frac{S_{0,u,c}(f) B_{KLJN}}{R_1} = 4kT_{eff}\, \frac{R_0 R_1}{\left(R_0 + R_1\right)^2} B_{KLJN}\,, \tag{12}$$

$$P_{1\to 0} = \frac{S_{1,u,c}(f) B_{KLJN}}{R_0} = 4kT_{eff}\, \frac{R_0 R_1}{\left(R_0 + R_1\right)^2} B_{KLJN}\,. \tag{13}$$

It is important to mention that this security proof against passive (listening) attacks holds only for the ideal cases when Gaussian noise sources are being utilized [6]. This is because Gaussian noises possess the property that its PSD or autocorrelation function already provides the maximum information about the noise [30]. Also, it has

been recently shown that no security is offered with noise of other types of distributions [41].

1.2.4 Speed and range

Speed and range are two important technical details of the KLJN key exchange that need to be discussed. First of all, the noise bandwidth B_{KLJN} is determined by the distance L between the two communicating parties. In other words, the following relationship must be satisfied: $B_{KLJN} \ll \frac{c}{L}$—*i.e.*, to satisfy the 'no-wave limit" condition (quasi-static electrodynamics) [4]—where B_{KLJN} and c are the bandwidth of the noise (*i.e.*, the highest frequency cut-off in the ideal KLJN system) and the speed of the electromagnetic waves in the wire, respectively [30]. Second of all, the duration of the bit sharing period, denoted as τ, must be long enough compared to the correlation time of the noise, denoted as τ_{KLJN}, where $\tau_{KLJN} \approx \frac{1}{B_{KLJN}}$, in order to achieve reasonable good statistics by correctly distinguishing between the different resistors situations [30]. In other words, the *secure* bit exchange rate $f_{B\_\sec}$ is much less than the noise bandwidth B_{KLJN}, that is $f_{B\_\sec} \ll B_{KLJN}$, where $f_{B\_\sec} \approx \frac{1}{2\tau}$.

According to the experimental demonstration carried out in [31], high fidelity noise statistics are achieved when $\tau = 50\tau_{KLJN}$ (*i.e.*, when $f_B = 0.02B_{KLJN}$, where f_B is the bit exchange rate). Since a secure bit exchange occurs on average 50% of the time,

the *secure* bit sharing period is around $\tau_{\text{sec}} = 100\tau_{KLJN}$. Moreover, the total time required to complete a KLJN secure key exchange depends on the length of the key. For example, if the key length is 100 bits, the total amount of time needed to complete a KLJN secure key exchange will be (on average) $10000\tau_{KLJN}$. This key stablishing rate may seem too slow. However, there is a tradeoff between the rate and the reachable level of security of this scheme. Besides, inexpensive techniques like building parallel channels by using chip technology and multi-wire cables have been proposed to improve the speed of this scheme [30]. Also, due to the small bit error probability [31], the system can afford to utilize PA algorithms to enhance the security of the system.

1.2.5 Enhancing the security in non-ideal situations

The ideal KLJN system provides unconditional security against passive (listening) attacks. As we have pointed out, this security is guaranteed by the second law of thermodynamics. However, any deviation from the ideal circuitry can cause information leak toward Eve. These practical deviations include: parasitic components, non-ideal situations with finite distance, non-zero cable resistance and capacitance, non-Gaussianity of the noise, active attacks by Eve, transient wave effects, etc. [2, 4, 30–32].

The following techniques and protocols have been proposed to enhance the security of the KLJN system.

1.2.5.1 Defense method for non-idealities and active (invasive) attacks

Invasive (active) attacks to the KLJN system require the alteration of its physical properties. In order to protect against invasive attacks—and also against passive attacks on non-ideal systems—the KLJN system can continuously monitor or measure the instantaneous current and voltage at both sides of the wireline [4, 32, 38]. These measurements are then compared via an authenticated public channel, as shown in Fig. 3. Therefore, any intruder causing changes in the circuitry and thus affecting the measurements will cause an alarm located at Alice and Bob to go off and alert the system of such intrusion.

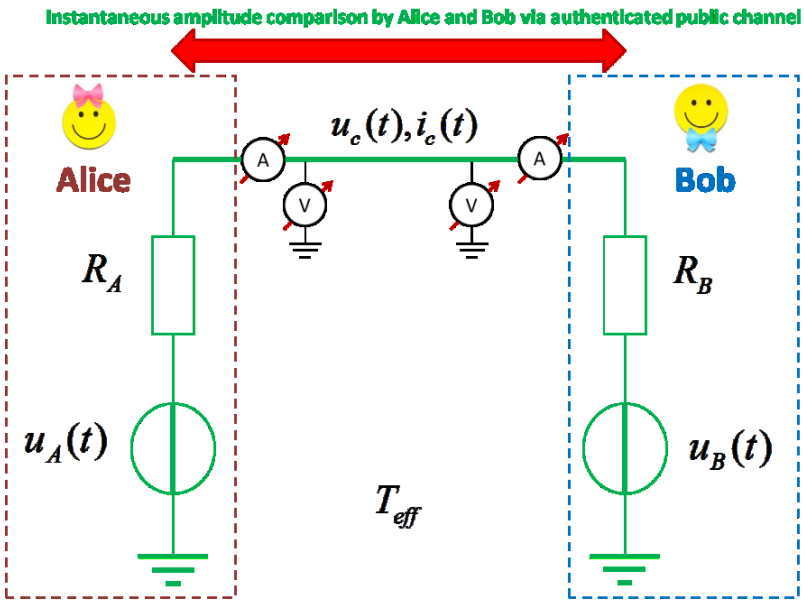

Figure 3 Outline of the core KLJN system minimally armed against invasive (active) attacks or attacks utilizing non-ideal components and conditions. To detect the active (invasive) eavesdropper the instantaneous noise current and voltage amplitudes measured at the two ends of the line are compared via an authenticated public channel

Note that the current and voltage measurement data contains all the information related to the key that Eve could have. Thus, it is impossible for Eve to extract key information without letting the communicating parties know of her activity. In consequence, Alice and Bob can decide whether or not to discard the compromised bits according to a previously agreed maximum level of information leak toward Eve [42].

1.2.5.2 Privacy amplification

To further enhance the security of the KLJN system and to try to reduce the amount of information leak that Eve can obtain about the key, a technique used in quantum communicators and called privacy amplification (PA) was analyzed [6]. PA is a software-based algorithm originally developed to improve the security in QKD systems [6]. The authors of [6] studied the effectiveness of utilizing one of the simplest PA techniques in several classical key distribution schemes, including the KLJN. This PA algorithm creates a new key by applying XOR operation between two consecutive bits of the original key. The new key has half the length of the original key and the Eavesdropper's probability of successfully guessing the key bit converges to 0.5. When this probability is 0.5, Eve's information about the key is zero since this is equivalent to obtaining her own key bits by tossing an unbiased random coin [6].

Unfortunately, while PA reduces the probability of correct guessing by Eve, it also reduces the fidelity of the system by increasing the bit error probability if it is

originally grader than zero. Thus, to use PA, the bit error probability of Alice and Bob must be as small as possible [6].

1.2.5.3 Other advanced security features and protocols

Other advanced protocols and associated basic security techniques proposed up to now to compensate for non-idealities and to enhance security in the non-ideal KLJN system include [4]:

- Selecting the values of Alice's and Bob's resistor pairs so that the wire resistance R_{wire} is negligible, that is $\{R_0, R_1\} \gg R_{wire}$ [31].
- Selecting the noise bandwidth versus the value of the wire resistance and wire capacitance in order to reduce information leak due to wire capacitance effects [2, 31].
- Low-pass line filters to provide "non-wave limit" condition in the cable and capacitor killer arrangement for cable capacitance compensation [31].
- Transient protocols such as random-walk of resistances starting at equal resistances [4, 39] or voltage ramping/timing to prevent transient effects at the beginning and at the end of the bit sharing period (BSP) [2, 31].
- Enhanced KLJN protocols, using Alice's and Bob's full knowledge of their own noise, for example the "intelligent" (iKLJN) to shorten the bit sharing period (BSP) which weakens Eve's statistics [39].

- Alice and Bob controlling the maximum information leak toward the Eavesdropper by calculating Eve's information and limiting her maximum amount of statistical information about the key by dropping high-risk bits [42].
- Protocol using the KLJN key for fully encrypting a software-based key exchange to increase the security of exchanged keys in the case of repeated usage [43].

1.3 Bit Errors in the KLJN Key Exchange Scheme

Because the working principle of the KLJN key exchange scheme is based on mean-square noise *measurements*, the study and evaluation of the uncertainties and the methods to reduce bit errors to a minimum are significantly important.

Due to the finite duration of the bit sharing period (BSP), denoted as τ, the measurement results of mean-square amplitudes have statistical inaccuracies [40]. As aforementioned, the time window τ must be long-enough so that Alice and Bob can obtain sufficiently good statistics to safely distinguish between the different mean-square channel noise levels and, therefore, make the correct bit interpretation.

In the experimental demonstration carried out in [31], the authors were able to optimize the KLJN system to have fidelity of 99.98% (error probability 0.02%). However no mathematical analysis or design tools have been shown to address the error probability issue. Besides, as we have mentioned above, error analysis in the KLJN system is crucially important when a PA algorithm is being utilized. Because PA algorithms are error amplifiers, a low error probability is a pre-requirement.

The objectives concerning errors in the ideal KLJN key exchange scheme are twofold. First, an error analysis for the ideal KLJN system is provided. An estimate of the probability of each type of error in both the voltage-based and current-based measurement modes is derived [40, 44, 45]. Second, in order to ensure that errors are as small as reasonably possible, an error mitigation method is proposed [44, 45]. This error mitigation strategy will significantly reduce the error probabilities in the KLJN system, without the need of implementing any error correction technique.

1.4 Vehicular Application for the KLJN Key Exchange Scheme

The KLJN key exchange scheme can be considered a fairly new development. A great number of improvements [4, 6, 31, 32, 38, 39, 42] and applications [5, 43, 46, 47] have been proposed and developed for this key exchange scheme. Furthermore, there are many ongoing research projects (*e.g.*, smart grid, communications in transportation systems, etc.) where security plays an important role, creating the possibility of new areas of applications for the KLJN key exchange system.

During the last years, vehicular communication networks have become an emerging research topic. The main motivation for the deployment of more intelligent vehicular systems is the need to enhance transportation safety and efficiency. In this type of network, vehicles will be equipped with advanced sensing and computing capabilities where communication protocols will enable them to share information with each other and roadside infrastructure. The incorporation of this new range of technology will

create a smart network where every vehicle is aware of its surrounding environment. In fact, a great number of applications are under development to improve traffic safety and mobility, and perform financial transactions (*e.g.*, toll collection).These new features will, at some level, improve the quality of life of people and will help to alleviate environmental issues such as pollution and the waste of non-renewable fossil energy [48].

1.4.1 Vehicular communication network architecture

A typical vehicular communication network is shown in Fig. 4 [49–54]. As summarized in previous publications [49–54], Vehicles, Roadside Devices (RSDs), and Certification Authorities (CAs) are the three basic nodes in most of vehicular communication networks. Vehicles are mobile terminal nodes in charge of collecting road and traffic information, reporting events to the CAs through the RSDs, and exchanging warning messages with nearby vehicles. The RSDs are intermediate nodes in charge of transferring messages between vehicles and CAs. The CAs are the host nodes that manage information related to vehicles. These nodes also generate secure keys and provide certifications for all vehicles in the network, control message exchanges of the whole network, and distribute information obtained outside the local vehicular communication network. Accordingly, the types of communication within vehicular communication networks include [49–54]: Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside-Device (V2RSD), and Vehicle-to-Certification-Authority (V2CA).

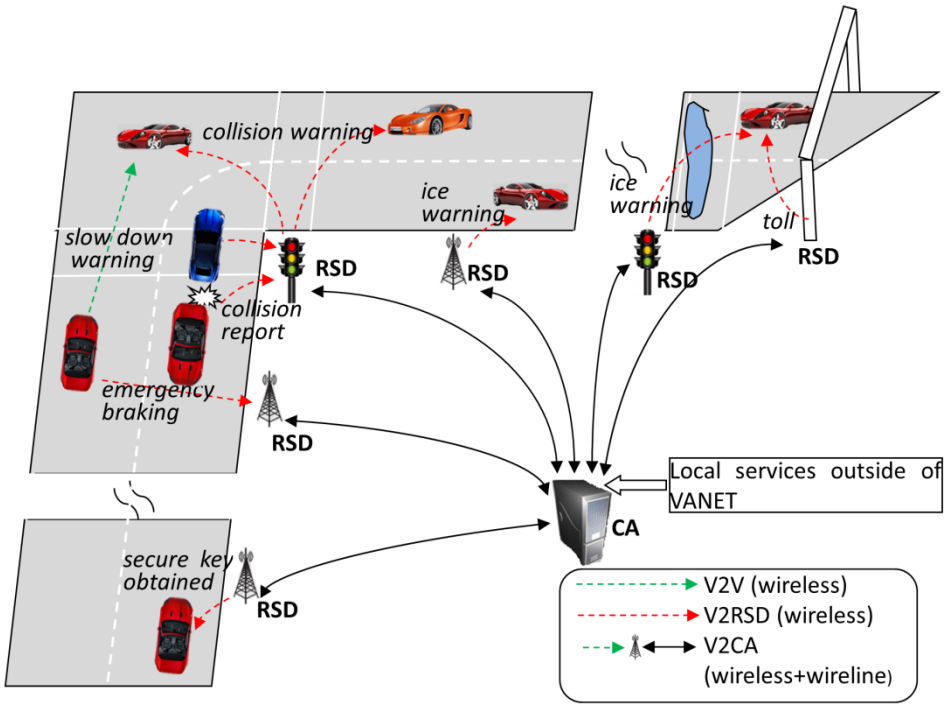

Figure 4 A typical vehicular communication network. Three basic nodes are encountered in this type of network: Vehicles, Roadside Devices (RSDs), and Certification Authorities (CAs). The types of communication within vehicular communication networks include [49–51]: Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside-Device (V2RSD), and Vehicle-to-Certification-Authority (V2CA)

The V2V and V2RSD communications use wireless technology, typically the IEEE 802.11p [55], which is an adjustment made to the IEEE 802.11 standard and it has been integrated in the 5GHz dedicated short range communication (DSRC) [55, 56] to add wireless access in a vehicular environment (WAVE) [56, 57]. V2V and V2RSD communications commonly include frequent safety-related messages (warnings) to give the drivers the necessary time to prevent and detect dangerous situations. The V2CA communication requires both wireless and wireline technology, where the RSD links to a wired network connecting the vehicles to the CA. V2CA communication normally

includes messages requesting new keys and/or signatures to establish a secure communication with other vehicles or RSDs.

1.4.2 Key exchange schemes in vehicular communication networks

Even though the integration of new technology and the levels of interconnectivity make the vehicular communication network a more reliable and efficient system, it might also create new vulnerabilities that adversaries could exploit. Since a vehicular system is a widely dispersed network, its communication infrastructure represents a potential target for malicious users. For instance, an attacker could disseminate false information that could affect the decisions of other drivers. Such attacks could lead to disastrous events such as fatal accidents. Also, a malicious user could monitor the position and/or trajectory of a specific vehicle or listen to financial transactions to steal personal and/or credit card information. Therefore, the safe and successful operation of a vehicular communication network requires the design of very robust security architecture that ensures the protection of private user information without affecting the correct operation of the entire system.

Most of the existing security mechanisms for vehicular communications use a software-based key and signature generation and distribution. This means that their performance is based on the assumption that eavesdroppers trying to gain access to security-related information possess limited computational power. Strictly speaking, these techniques offer only *computationally conditional security* [1]. Therefore, if

eavesdroppers can increase their computational power, the keys and digital signatures might be extracted. This would allow them to intercept all the communication between the transmitter and receiver.

CAs manage and store very important information associated to vehicles and RSDs, such as location information tables, node identities, and credentials. Before initiating the information exchange with another vehicle or with a RSD, a vehicle needs to obtain security-related information (*e.g.*, certificates) in order to be considered authentic. In this case, the vehicle first communicates with the RSD which then links the vehicle to the CA by using a wireline connection. If this wireline communication is intercepted on the way to/from the CA, important information could be given away. Thus, securing both the V2RSD and RSD2CA communication channels is necessary.

Though there is plenty of research on securing the V2RSD communication, very little attention has been devoted to secure the wireline RSD2CA communication. Therefore, another objective of this dissertation is to introduce a vehicular communication system with *unconditionally* secure key exchange based on the Kirchhoff-law-Johnson-noise (KLJN) key distribution scheme [52]. The secure KLJN key donation to vehicles is also addressed [58]. The lifetime of the KLJN key in vehicular communication networks is a very important technical parameter that needs to be discussed. This is because the longer the KLJN key is used; the more susceptible it is to attacks. Therefore, an upper limit for the lifetime of this key is also provided [58].

2. ANALYSIS OF THE BIT ERRORS IN THE KLJN SECURE KEY EXCHANGE SCHEME*

This section classifies and analyzes the different types of errors—due to statistical inaccuracies in noise measurements—within the voltage-based and current-based measurement modes of the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange scheme. It also presents a method to efficiently reduce these errors without the need of implementing any error correction technique. This section is a summary of recent findings presented in Saez and Kish, 2013 [40], Saez *et al.*, 2014 [44], and Saez *et al.*, 2014 [45].

2.1 Mean-square Noise Measurement Process and Bit Interpretation

Assuming ideal components/conditions, we proceed as in earlier works [40, 44, 45]. First, let us assume that Alice and Bob measure either the mean-square channel noise voltage or the mean-square channel noise current amplitude, *i.e.*, $\langle u_c^2(t)\rangle_\tau = 4kT_{eff}\frac{R_A R_B}{R_A+R_B}B_{KLJN}$ or $\langle i_c^2(t)\rangle_\tau = 4kT_{eff}\frac{1}{R_A+R_B}B_{KLJN}$, respectively, where

*Part of this section is a modified reprinted version of: Y. Saez and L. B. Kish, Errors and their mitigation at the Kirchhoff-Law-Johnson-Noise secure key exchange, *PLoS ONE* 8 (2013) e81103 (7 pages), © 2013 Saez and Kish.

*Part of this section is reprinted with kind permission from Springer Science+Business Media: Journal of. Computational Electronics, Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law-Johnson-noise secure key exchange, 13, 2014, 271–277, Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, © Springer Science+Business Media New York 2013.

$\left\langle u_c^2(t)\right\rangle_\tau$ and $\left\langle i_c^2(t)\right\rangle_\tau$ indicate finite-time average of the square of the channel noise voltage and current, respectively.

It is important to mention that during the BSP 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.

Figure 5 shows a block diagram to illustrate the measurement process in both measurement modes.

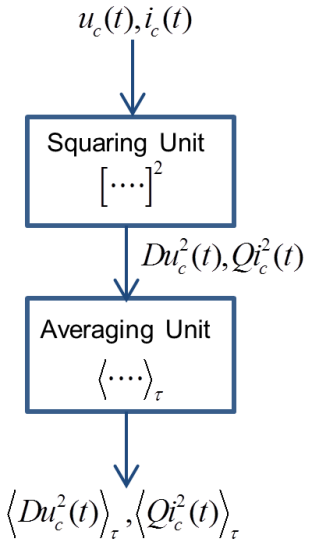

Figure 5 Mean-square channel noise voltage and current measurement process. Q and D are calibration coefficients of the squaring device to provide a Volt unit with the correct numerical value for the squaring operation

The measurement process is a follows. First, the channel noise enters into a squaring unit (analog or digital circuits). At its output, the signal is still voltage (because

the squaring unit employs voltage-signal-based electronics). Thus, for the voltage-based measurement mode, the numerical value of the instantaneous amplitude at the output of the squaring unit is equal to the square of the instantaneous amplitude of the input voltage. However, for the sake of simplicity and without losing generality, in the current-based measurement mode we assume that the numerical values of the voltage correspond to the measured current. Thus, we keep the current-based notation as if the electronics would be a current-based signal system. In other words, the voltages are calibrated so that the numerical values are the same as those of the current. These facts are mathematically expressed by the instantaneous amplitudes $Du_c^2(t)$ and $Qi_c^2(t)$, where $D = \frac{1}{\text{Volt}}$ and $Q = \frac{1}{\text{Amper}}$ are the transfer coefficients of the hypothetical multiplier device to provide a Volt/Amper unit also for the square value [59].

The instantaneous amplitudes then enter an averaging unit and after averaging for the finite-time duration τ, the obtained measurement results are $\langle Du_c^2(t)\rangle_\tau = \langle Du_c^2(t)\rangle + \mu_\tau(t)$ and $\langle Qi_c^2(t)\rangle_\tau = \langle Qi_c^2(t)\rangle + i_\tau(t)$, for the voltage-based mode and current-based mode, respectively. In other words, the *measured* mean-square channel noise voltage and current have a DC component—*i.e.*, the ideal infinite-time averages $\langle Du_c^2(t)\rangle$ and $\langle Qi_c^2(t)\rangle$, respectively—and a superimposed AC component—*i.e.*, $\mu_\tau(t)$ and $i_\tau(t)$, respectively—remaining after the finite-time average. This averaging process can be represented as a low-pass filtering with a cut-off frequency f_B inversely proportional to τ, *i.e.,* $f_B \approx \frac{1}{\tau}$.

While $\langle Du_c^2(t)\rangle$ and $\langle Qi_c^2(t)\rangle$ are not Gaussians, the AC components $\mu_\tau(t)$ and $i_\tau(t)$ are Gaussians with high accuracy [59]. This follows from central limit theorem (CLT) because the finite duration τ is much longer than the correlation time of the AC components of $Du_c^2(t)$ and $Qi_c^2(t)$ before averaging since $f_B \ll B_{KLJN}$.

Figure 6 illustrates the three possible levels of the *measured* mean-square channel noise voltage and current for the 11, 01/10, and 00 bit situations. The solid lines denote exact (infinite) time averages while the random fluctuations around them represent the finite-time averages components.

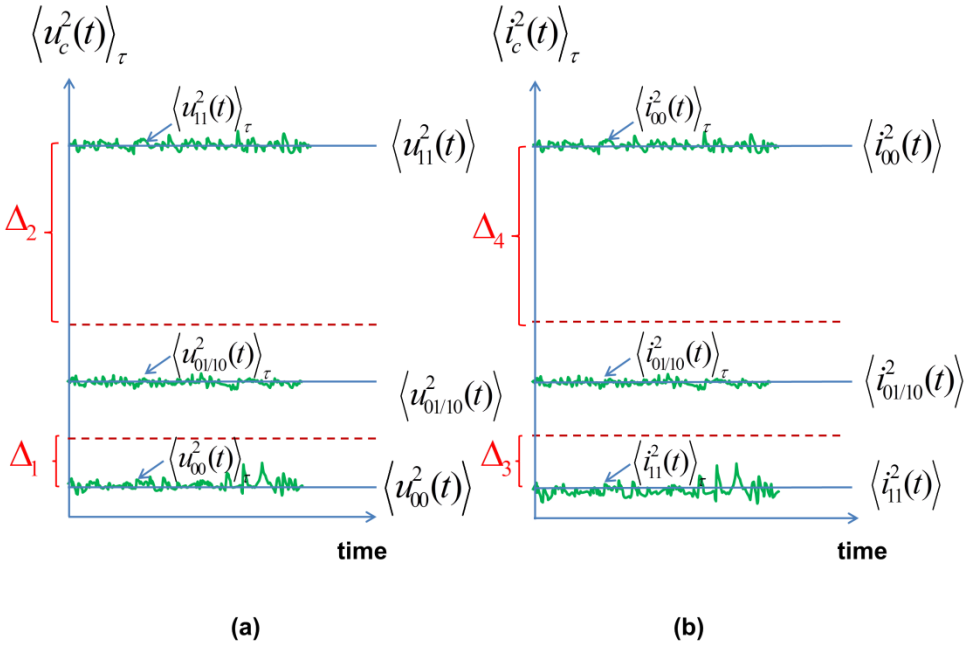

Figure 6 Measured mean-square channel noise of voltage (a) and current (b). $\langle u_{11}^2(t)\rangle_\tau$, $\langle u_{01/10}^2(t)\rangle_\tau$, $\langle u_{00}^2(t)\rangle_\tau$, and $\langle i_{11}^2(t)\rangle_\tau$, $\langle i_{01/10}^2(t)\rangle_\tau$, $\langle i_{00}^2(t)\rangle_\tau$ are the measured mean-square channel noise voltage and current at the 11, 01/10, and 00 bit situations, respectively. The scales are arbitrary. Solid lines denote exact (infinite) time average results. For the sake of simplicity we assume $R_0 = R$ and $R_1 = \alpha R$, with $\alpha \gg 1$. (Δ_1, Δ_2) and (Δ_3, Δ_4) are the thresholds for interpreting the measured mean-square voltage and current values, respectively

With a low probability, the random fluctuations in the *measured* mean-square channel noise voltage and current can cross from one mean-square noise level to another and cause Alice and Bob to make incorrect bit interpretations which will trigger a bit error.

The threshold values Δ_1, Δ_2 and Δ_3, Δ_4, are used to determine the boundaries between the different interpretations of the *measured* mean-square channel noise voltages and currents, respectively, over the time window τ. The bit interpretations of the *measured* mean-square channel noise voltage and current are 00 when $\langle u_c^2(t)\rangle_\tau < \langle u_{00}^2(t)\rangle + \Delta_1$ and $\langle i_c^2(t)\rangle_\tau > \langle i_{00}^2(t)\rangle - \Delta_4$, respectively. The interpretations are 11 when $\langle u_c^2(t)\rangle_\tau > \langle u_{11}^2(t)\rangle - \Delta_2$ and $\langle i_c^2(t)\rangle_\tau < \langle i_{11}^2(t)\rangle + \Delta_3$, respectively. The secure bit situations 01/10 are interpreted as such when $\langle u_{00}^2(t)\rangle + \Delta_1 \le \langle u_c^2(t)\rangle_\tau \le \langle u_{11}^2(t)\rangle - \Delta_2$ and $\langle i_{11}^2(t)\rangle + \Delta_3 \le \langle i_c^2(t)\rangle_\tau \le \langle i_{00}^2(t)\rangle - \Delta_4$, respectively.

2.2 Types of Errors in the KLJN Key Exchange Scheme

Bit errors occur when Alice and Bob make incorrect bit interpretations due to the statistical inaccuracies (random fluctuations) in the *measured* mean-square noise voltage and/or current. An example of a bit error is the rare occurrence when the finite-time mean-square voltage of the 00 bit situation is interpreted as the 01/10 bit situation. There are different types of errors situations, as shown in Table 2.

According to Table 2, it is apparent that two types of errors need to be addressed: the *11==>01/10 errors—i.e.*, the errors when the actual non-secure bit situation 11 is interpreted as the secure bit situation 01/10—and the *00==>01/10 errors* occurring when the actual situation 00 is interpreted as 01/10. Also, notice that some of the errors situations, as shown in Table 2, are considered to be auto-corrected by the protocol. This is because, as aforementioned, the 00 and 11 bit situations are automatically discarded by the system.

Table 2 Types of errors in the KLJN key exchange scheme

		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)

2.3 Mathematical Approach

The error probabilities in the ideal KLJN key exchange scheme can be estimated with the probability that AC components $\mu_\tau(t)$ and/or $i_\tau(t)$ are crossing specific thresholds during the time interval τ. For instance, the probability of the 00==>01/10 type errors in the voltage-based measurement mode is the probability that the AC

component *remaining* after the finite-time average of $Du_c^2(t)$ defined as $\mu_\tau(t) = \langle Du_c^2(t) \rangle_\tau - \langle Du_c^2(t) \rangle$ is beyond the threshold Δ_1, *i.e.*, $\mu_\tau(t) > \Delta_1$. Similarly, the probability of the 11==>01/10 type of errors in the current measurement mode is the probability that $i_\tau(t)$ is beyond threshold Δ_3, *i.e.*, $i_\tau(t) > \Delta_3$, (see Fig. 6). These probabilities can be evaluated from the error function; however, this approach would require numerical integration. Thus, we follow a different approach [40, 44, 45] by using Rice's formula for threshold crossings [60, 61].

To have an analytic formula, which is a good approximation and has the exact scaling in the small error probability limit, we can use the Rice formula of threshold crossing frequency [60, 61]; see similar solutions for estimating the probability of thermal noise induced switching errors [62–64]. 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. The correlation time of $\mu_\tau(t)$ and $i_\tau(t)$ is also equal to τ, thus each threshold crossing (in a chosen but fixed direction) indicates an independent error. The product of the mean threshold crossing frequency of a specific threshold Δ, where $\Delta \in \{\Delta_1, \Delta_2, \Delta_3, \Delta_4\}$, denoted as $\nu(\Delta)$, times the finite duration τ—*i.e.*, the duration of the BSP—is a good estimation of the error probabilities in this limit [62, 63].

The predictions of the Rice formula were compared with the prediction based on numerically evaluated error function and it was found that the Rice formula always gave more pessimistic error estimation. The variation of the threshold resulted in changing the

error probability predicted by the Rice formula and the error function by factors of $\sim 10^{43}$ and $\sim 10^{44}$, respectively. In the large error probability situation, the Rice formula predicted about 2 times greater error while, in the low error probability situation, about 18 times greater error. This is a negligible difference not only due to the $10^{43} - 10^{44}$ variation during the study but also because the exact error probability slightly depends on the fine details of the protocol not discussed here. To have analytic error estimation, we proceed as follows.

2.3.1 General approach

We assume that Δ is the threshold value used to determine the boundaries between the different interpretations of the AC component remaining after the average time window τ. This threshold value varies for different mean-square channel noise voltages and currents. However, for the sake of simplicity and without losing generality, in this general approach we are going use Δ for both voltage and current measurements. The AC component can be $\mu_\tau(t)$ and/or $i_\tau(t)$, depending on the quantity being measured, voltage or current, respectively. We define $S_{AC,\mu,\tau}(f)$ and $S_{AC,i,\tau}(f)$ as the power spectral densities of $\mu_\tau(t)$ and $i_\tau(t)$, respectively. Then, according to Rice [60], the mean frequency ν of crossing the level Δ by these Gaussians $\mu_\tau(t)$ and $i_\tau(t)$, with power spectral densities $S_{AC,\mu,\tau}(f)$ and $S_{AC,i,\tau}(f)$ can be given as:

$$\nu(\Delta) = \frac{2}{\hat{\mu}_\tau} \exp\left(\frac{-\Delta^2}{2\hat{\mu}_\tau^2}\right) \sqrt{\int_0^\infty f^2 S_{AC,\mu,\tau}(f) df} \tag{14}$$

and

$$\nu(\Delta) = \frac{2}{\hat{i}_\tau} \exp\left(\frac{-\Delta^2}{2\hat{i}_\tau^2}\right) \sqrt{\int_0^\infty f^2 S_{AC,i,\tau}(f) df}\ , \tag{15}$$

respectively. Where $\hat{\mu}_\tau = \sqrt{\int_0^\infty S_{AC,\mu,\tau}(f) df}$ and $\hat{i}_\tau = \sqrt{\int_0^\infty S_{AC,\mathrm{i},\tau}(f) df}$ are the RMS values of $\mu_\tau(t)$ and $i_\tau(t)$, respectively. The threshold value Δ is defined, for normalization purposes, as a fraction of the DC component of the *measured* mean-square channel noise voltage and/or current, namely:

$$\Delta = \varphi \left\langle D u_c^2(t) \right\rangle = \varphi D S_{u,c}(f) B_{KLJN} \tag{16}$$

and

$$\Delta = \zeta \left\langle Q i_c^2(t) \right\rangle = \zeta Q S_{i,c}(f) B_{KLJN}\ , \tag{17}$$

for $0 < \varphi < 1$ and $0 < \zeta < 1$, respectively. $S_{u,c}(f)$ and $S_{i,c}(f)$ are the power density spectrum of the channel voltage and current noises, respectively.

In order to compute $S_{AC,\mu,\tau}(f)$ and $S_{AC,i,\tau}(f)$, we follow the approach given in [59]. According to [59], the power spectral densities $S_{AC,\mu}(f)$ and $S_{AC,i}(f)$ of the AC components of the *non-averaged* quantities $Du_c^2(t)$ and $Qi_c^2(t)$ are:

$$S_{AC,\mu}(f) = 2D^2 B_{KLJN} S_{u,c}^2(f)\left(1-\frac{f}{2B_{KLJN}}\right) \text{ for } 0 \le f \le 2B_{KLJN} \tag{18}$$

and

$$S_{AC,i}(f) = 2Q^2 B_{KLJN} S_{i,c}^2(f)\left(1-\frac{f}{2B_{KLJN}}\right) \text{ for } 0 \le f \le 2B_{KLJN}\,. \tag{19}$$

And $S_{AC,\mu}(f) = 0$ and $S_{AC,i}(f) = 0$ otherwise, respectively.

The low-pass filtering effect of the time averaging cuts off these spectrums for $f > f_B$ but keeps them for $f < f_B$. Since $f_B \ll B_{KLJN}$, the values of $S_{AC,\mu}(f)$ and $S_{AC,i}(f)$ within the frequency band f_B can be approximated by its maximum, that is $S_{AC,\mu,\tau}(f) \approx S_{AC,\mu}(0)$ and $S_{AC,i,\tau}(f) \approx S_{AC,i}(0)$, respectively.

Figures 7 and 8 summarize these findings for the voltage-based measurement mode. Similar results can be found for the current-based measurement mode.

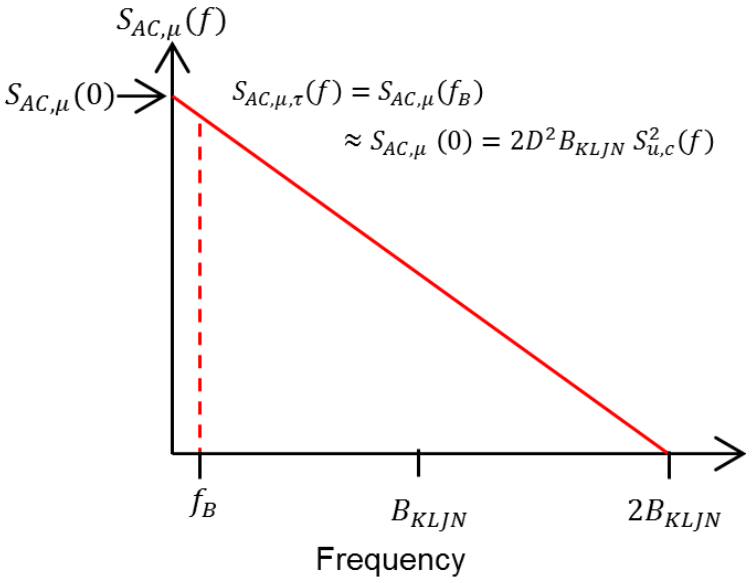

Figure 7 Power spectral density (PSD) of the product of two independent noise voltages

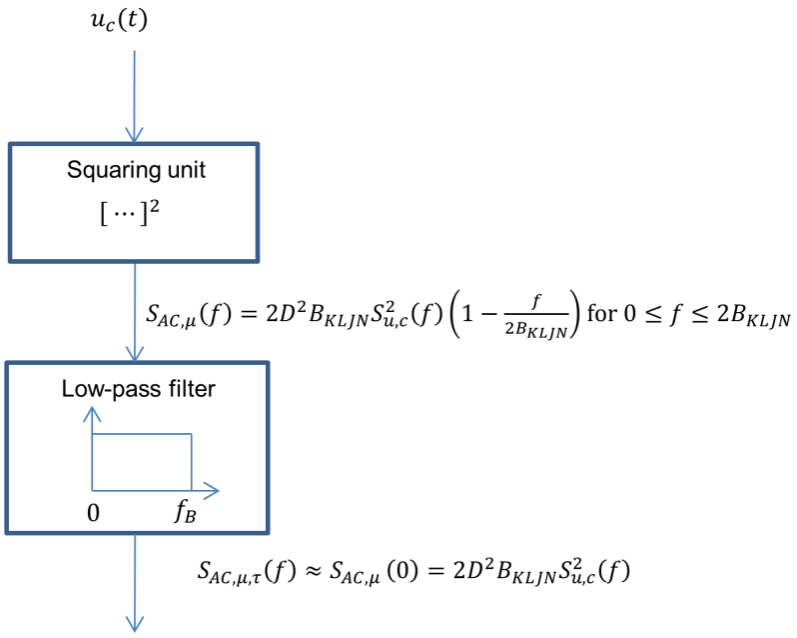

Figure 8 PSD of the AC component remaining after the average time window τ in the voltage-based measurement mode

Let us define $\gamma = \frac{B_{KLJN}}{f_B}$. Then, the RMS values $\hat{\mu}_\tau$ and $\hat{i}_\tau$ are:

$$\hat{\mu}_\tau = \sqrt{\int_0^\infty S_{AC,\mu,\tau}(f)df} \approx \sqrt{f_B S_{AC,\mu}(0)} = \sqrt{2D^2\gamma f_B^2 S_{u,c}^2(f)} \tag{20}$$

and

$$\hat{i}_\tau = \sqrt{\int_0^\infty S_{AC,i,\tau}(f)df} \approx \sqrt{f_B S_{AC,i}(0)} = \sqrt{2Q^2\gamma f_B^2 S_{i,c}^2(f)}\,, \tag{21}$$

respectively.

The frequency of unidirectional level crossings $\nu_\uparrow(\Delta)$ is half of the level crossing frequency predicted by the Rice formula. In the voltage-based measurement mode $\nu_\uparrow(\Delta)$ is given by:

$$\nu_\uparrow(\Delta) = \frac{1}{\hat{\mu}_\tau}\exp\left(\frac{-\Delta^2}{2\hat{\mu}_\tau^2}\right)\sqrt{\int_0^\infty f^2 S_{AC,\mu,\tau}(f)df}\,. \tag{22}$$

In the current-based measurement mode $\nu_\uparrow(\Delta)$ is given by:

$$\nu_\uparrow(\Delta) = \frac{1}{\hat{i}_\tau}\exp\left(\frac{-\Delta^2}{2\hat{i}_\tau^2}\right)\sqrt{\int_0^\infty f^2 S_{AC,i,\tau}(f)df}\,. \tag{23}$$

From Eqs. (14)–(23), we obtain that the frequency of unidirectional level crossings in the voltage-based and current-based measurement modes are:

$$\nu_{\uparrow}(\Delta)=\frac{f_B}{\sqrt{3}}\exp\left(\frac{-\varphi^2\gamma}{4}\right) \tag{24}$$

and

$$\nu_{\uparrow}(\Delta)=\frac{f_B}{\sqrt{3}}\exp\left(\frac{-\zeta^2\gamma}{4}\right), \tag{25}$$

respectively. In the high threshold situation the errors follow a Poisson statistics, thus the error probability during the time interval τ is equal to the expected numbers of errors within this interval provided this number is much less than 1. Thus, the probabilities in the voltage-based measurement mode and the current-based measurement mode, denoted as ε_u and ε_i, respectively, in the case of $\varepsilon_u, \varepsilon_i \ll 1$ are:

$$\varepsilon_u \approx \nu_{\uparrow}(\Delta)\tau=\frac{\nu_{\uparrow}(\Delta)}{f_B}=\frac{1}{\sqrt{3}}\exp\left(\frac{-\varphi^2\gamma}{4}\right) \tag{26}$$

and

$$\varepsilon_i \approx \nu_{\uparrow}(\Delta)\tau = \frac{\nu_{\uparrow}(\Delta)}{f_B} = \frac{1}{\sqrt{3}}\exp\left(\frac{-\zeta^2\gamma}{4}\right). \tag{27}$$

2.4 Probabilities of the Different Types of Errors

In this section, the threshold values Δ_1, Δ_2 and Δ_3, Δ_4 have meanings that are similar to the one of the threshold value Δ in the general approach presented above and are also defined as a fraction of the corresponding DC component of the *measured* mean-square channel noise voltage and current, namely: $\Delta_1 = \beta\langle Du_{00}^2(t)\rangle$ for $0<\beta<1$, $\Delta_2 = \delta\langle Du_{11}^2(t)\rangle$ for $0<\delta<1$, $\Delta_3 = \lambda\langle Qi_{11}^2(t)\rangle$ for $0<\lambda<1$, and $\Delta_4 = \rho\langle Qi_{00}^2(t)\rangle$ for $0<\rho<1$. Where $\langle Du_{00}^2(t)\rangle$, $\langle Du_{11}^2(t)\rangle$, $\langle Qi_{00}^2(t)\rangle$, and $\langle Qi_{11}^2(t)\rangle$ are the DC components of the *measured* mean-square channel noise voltage and current at the 00 and 11 bit situations, respectively.

2.4.1 Statistical errors in the voltage-based measurement mode

Substituting Δ_1 and Δ_2 in the general approach, we find that the probabilities $\varepsilon_{u,00}$ and $\varepsilon_{u,11}$ of the 00==>01/10 and 11==>01/10 types of errors in voltage measurements for $\varepsilon_{u,00}, \varepsilon_{u,11} \ll 1$ are:

$$\varepsilon_{u,00} \approx \nu_{\uparrow}(\Delta_1)\tau = \frac{\nu_{\uparrow}(\Delta_1)}{f_B} = \frac{1}{\sqrt{3}}\exp\left(\frac{-\beta^2\gamma}{4}\right) \text{for } 0<\beta<1 \tag{28}$$

and

$$\varepsilon_{u,11} \approx \nu_{\downarrow}(\Delta_2)\tau = \frac{\nu_{\downarrow}(\Delta_2)}{f_B} = \frac{1}{\sqrt{3}}\exp\left(\frac{-\delta^2\gamma}{4}\right) \text{for } 0 < \delta < 1, \tag{29}$$

respectively.

2.4.2 Statistical errors in the current-based measurement mode

Similarly, by substituting Δ_3 and Δ_4 in the general approach, we find that the error probabilities $\varepsilon_{i,00}$ and $\varepsilon_{i,11}$ of the 11==>01/10 and 00==>01/10 types of errors in the current measurements are:

$$\varepsilon_{i,00} \approx \nu_{\uparrow}(\Delta_3)\tau = \frac{\nu_{\uparrow}(\Delta_3)}{f_B} = \frac{1}{\sqrt{3}}\exp\left(\frac{-\lambda^2\gamma}{4}\right) \text{for } 0 < \lambda < 1 \tag{30}$$

and

$$\varepsilon_{i,11} \approx \nu_{\downarrow}(\Delta_4)\tau = \frac{\nu_{\downarrow}(\Delta_4)}{f_B} = \frac{1}{\sqrt{3}}\exp\left(\frac{-\rho^2\gamma}{4}\right) \text{for } 0 < \rho < 1, \tag{31}$$

respectively.

It should be noticed that—for both the voltage-based and the current-based measurement modes—the error probabilities are exponential functions of two important parameters: the parameter γ, which shows that the error probability decays exponentially with increasing magnitude of τ, and the parameter defining the value of the respective threshold, *i.e.*, β, δ and λ, ρ in the in the voltage-based and current-based methods, respectively.

2.4.3 Illustration of results with practical parameters

To demonstrate the results and to have an estimate of how large these errors are, we assign possible practical values to the parameters. We varied γ from 50 to 250, and gave β three different values between 0 and 1. The bit error probability $\varepsilon_{u,00}$ of the 00==>01/10 type of errors in voltage-based measurement mode for $\varepsilon_{u,00} \ll 1$ is shown in Fig. 9.

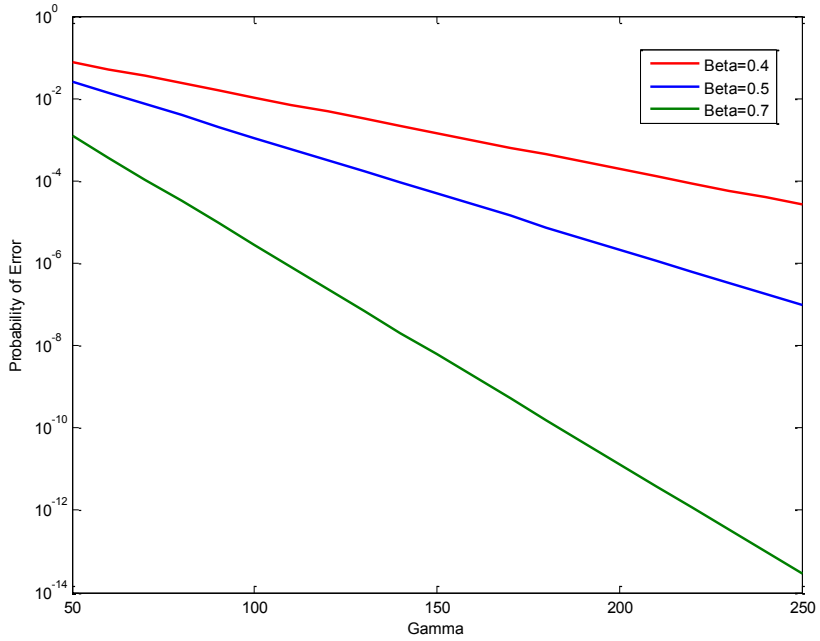

Figure 9 Probability of the 00==>01/10 type of errors in voltage measurements

Figure 9 shows that for a fixed value of γ, by increasing β (and consequently increasing the value of the threshold Δ_1 used to determine this type of error), we can significantly reduce this probability. This figure also shows how increasing the γ parameter (and thus the time average window τ) will result in a substantial reduction of this error probability. It is important to note that no error correction algorithm is used for this error reduction.

It should be mentioned that in the current-based mode, for the case of $\alpha \gg 1$, the mean-square noise level at 11 is closer to the level at 01/10 than to the level at 00 (cf., Fig. 3 as an illustration). Therefore, the bit error probability $\varepsilon_{i,00}$ for the 00==>01/10 type of errors will be significantly smaller than the bit error probability $\varepsilon_{i,11}$ for the

11==>01/10 type of errors. This situation is the opposite for the case of the voltage-based method [40]. Accordingly, the experimental test of the KLJN scheme [31] used either the voltage or the current data for decision, depending of which scheme gave the smaller bit error probability.

2.5 A Proposed Error Removal Method

In this section we examine a new error removal strategy, which utilizes both voltage and current measurements without applying any error correction algorithm.

Let us assume that Alice and Bob measure both $\langle u_c^2(t)\rangle_\tau$ and $\langle i_c^2(t)\rangle_\tau$ at the same time. In an ideal error-free situation, the same bit interpretations ensue from both mean-square channel noise amplitudes. However, the bit interpretations can differ when there are errors, because the AC components of the *measured* mean-square channel noise voltage and current are statistically independent due to the second law of thermodynamics and its Gaussian nature (when the cross-correlation between two Gaussian processes with zero mean is zero, the two processes are statistically independent).

To eliminate errors, we select the cumulative measurement output that has the smallest error associated with it; see Fig. 6 and Table 3. We make use of the fact that, in the bit situation when the current evaluation method has maximum error probability, the voltage-based method has minimum error probability, and *vice versa*.

Table 3 KLJN error removal method with combined voltage-current analysis

		Voltage measurement interpretation		
		00	**11**	**01/10**
Current measurement Interpretation	**00**	00 (Insecure/ Discard)	Discard (check attack)	00 (Insecure/ Discard)
	11	Discard (check attack)	11 (Insecure/ Discard)	11 (Insecure/ Discard)
	01/10	00 (Insecure/ Discard)	11 (Insecure/ Discard)	**01/10 (Secure)**

The only output that is kept is when *both* the current-based method and voltage-based method bit interpretations are secure, *i.e.*, when both are 01/10. For instance, suppose that the bit interpretation obtained from the current measurement is 00 and that the bit interpretation for the voltage measurement is 01/10. In this case, we assume 00 as the correct bit interpretation and hence discard the bit.

2.5.1 Error probabilities in the combined voltage-current analysis method

The AC components of the mean-square noise voltage and current mean-square noises are independent as a consequence of the second law of thermodynamics and the Gaussianity of thermal noise [4, 32, 39], and hence the probability of errors in the combined current-voltage analysis method is given by the product of the error probabilities in the current-based and voltage-based methods.

As reported in section 2.4, the probability $\varepsilon_{u,00}$ of the 00==>01/10 type of errors in the voltage-based method is $\varepsilon_{u,00} \approx \frac{1}{\sqrt{3}} \exp\left(\frac{-\beta^2\gamma}{4}\right)$ for $0 < \beta < 1$, and the probability

$\varepsilon_{i,00}$ of the 00==>01/10 type of errors in the current-based method is $\varepsilon_{i,00} \approx \frac{1}{\sqrt{3}} \exp\left(\frac{-\rho^2\gamma}{4}\right)$ for $0 < \rho < 1$. Thus, the probability $\varepsilon_{t,00}$ of the 00==>01/10 type of errors in the combined method is given by:

$$\varepsilon_{t,00} = \varepsilon_{u,00}\varepsilon_{i,00} = \frac{1}{3}\exp\left(\frac{-(\beta^2+\rho^2)\gamma}{4}\right) \text{for } 0 < \beta < 1 \text{ and } 0 < \rho < 1. \quad (32)$$

This error probability is an exponential function of the parameters γ, β, and ρ.

By following the same procedure as above, we find that the probability $\varepsilon_{t,11}$ of the 11==>01/10 type of errors in the combined voltage-current method is also exponential and is given by:

$$\varepsilon_{t,11} = \varepsilon_{u,11}\varepsilon_{i,11} = \frac{1}{3}\exp\left(\frac{-(\delta^2+\lambda^2)\gamma}{4}\right) \text{for } 0 < \delta < 1 \text{ and } 0 < \lambda < 1. \quad (33)$$

2.5.2 Illustration of the results with practical parameters

To demonstrate the results for the bit error probabilities in the error removal method, we assign practical values to the parameters γ, β, and ρ. We choose again $50 \le \gamma \le 250$, and set $\beta = 0.5$ and $\rho = 0.8$ (this is because, as aforementioned, the bit error probability $\varepsilon_{i,00}$ is significantly smaller than the bit error probabilities $\varepsilon_{u,00}$ and

$\varepsilon_{i,11}$). Figure 10 illustrates the results.

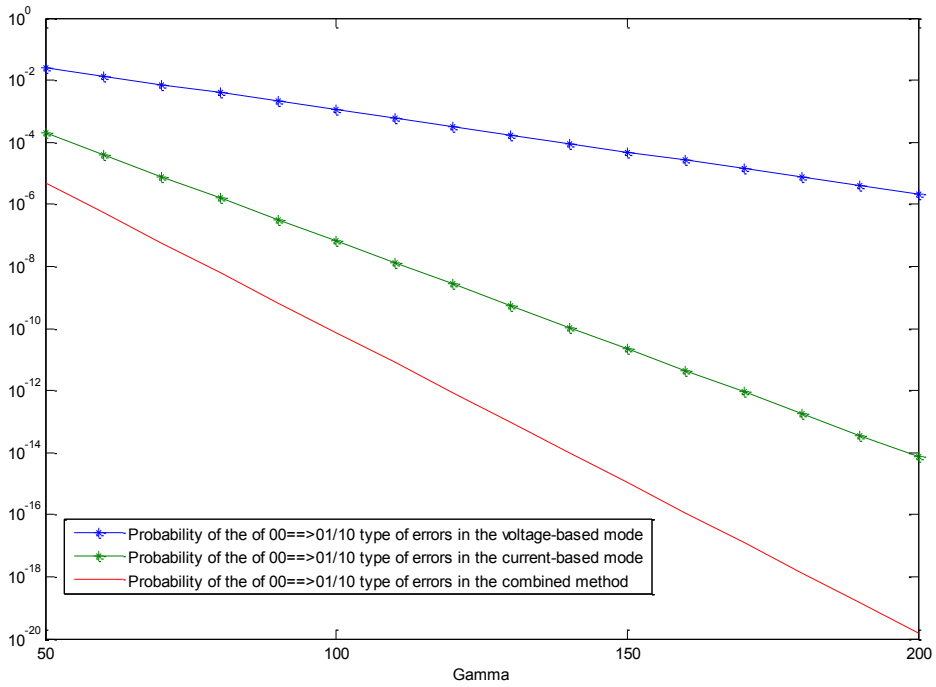

Figure 10 Probability of the 00==>01/10 type of errors in the combined voltage-current method

As notice in Fig.10, by increasing the duration of the bit exchange period, *i.e.*, τ, we can drastically decrease this error probability without the need of implementing any error correction technique/algorithm.

3. VEHICULAR APPLICATION OF THE KLJN SECURE KEY EXCHANGE SCHEME*

In this section, we propose the use of the Kirchhoff-law-Johnson-noise (KLJN) scheme to enhance the security of key exchange in vehicular communication systems. We focus primarily on providing a new network architecture with KLJN-based unconditionally secure key exchange, and describe the KLJN key generation and donation to vehicles. Also, an upper limit of the KLJN key lifetime is estimated. This section is a summary of recent findings presented in Saez *et al.*, 2014 [54] and Cao *et al.*, 2015 [58].

3.1 Unconditionally Secure Key Exchange for Vehicular Communication Networks

3.1.1 Existing key exchange techniques

In order to solve the fundamental security-related issues for promising vehicular communication network applications, several security protocols have been proposed by different researchers. In [65, 66], the authors proposed a security infrastructure that is based on public key infrastructure (PKI). Later, other solutions based on PKI were

*Part of this section is reprinted with kind permission from: Y. Saez, X. Cao, L. B. Kish, and G. Pesti, Securing Vehicle Communication Systems by the KLJN key exchange protocol, *Fluctuation and Noise Letters* 13 (2014) 1450020 (14 pages), © World Scientific Publishing Company 2014.
*Part of this section is reprinted with kind permission from: X. Cao, Y. Saez, G. Pesti, and L. B. Kish, On KLJN-based secure key distribution in vehicular communication networks, *Fluctuation and Noise Letters*. 14 (2015) 1550008 (11 pages), © World Scientific Publishing Company 2015.

proposed [67–70]. The authors of [67] provided a "lightweight" authenticated key scheme that integrates blind signature techniques for V2V and V2RSD communications. In [68], the authors presented an approach that combines the traditional PKI and identity-based public key cryptography for vehicular communication networks. In [69], a secure scheme with session keys (pairwise and group keys) used in non-safety-related applications (e.g. "chatting in platoon") was designed. In [70], temporary anonymous certified keys (TACKs) were constructed, and a key management scheme based on TACKs was proposed for vehicular communication networks. Besides PKI, group signatures are another important category of proposed security methods. Based on the strong Diffie-Hellman and linear assumptions, the authors of [71] introduced the under-200 bytes group signature scheme that has a similar security level to the RSA (Rivest, Shamir, and Adleman public-key cryptosystem) signature of the same length. A group signature-based protocol using tamper-resistance devices and a probabilistic signature verification scheme was proposed in [72]. In [73], the authors constructed an identity-based batch verification scheme for V2RSD communication in vehicular communication networks. In [74], a software-based roadside unit-aided messages authentication protocol for V2V communications was proposed. In addition, a software-based solution that uses secure and privacy enhancing communication schemes for vehicular sensor networks was provided in [75].

Most of the above security schemes or protocols are constructed based on software encryption mechanisms. The security on these software-based methods is based on the premise that the eavesdroppers have *limited computational power*. Thus, these

security schemes offer just a *computationally conditional security* [1, 2, 4, 7, 30]. Moreover, these architectures focus their attention on V2V or V2RSD communications and although there is significant information transmitted in the Roadside-Device-to-Certification-Authority (RSD2CA) communication [54], it is very rare to find works related to securing this particular communication channel.

In vehicular communication systems, where security has taken an increasingly important role, there is a need for a new key exchange scheme that can approach a perfect security level. Therefore, we outline how the KLJN system could theoretically be used to achieve unconditionally secure keys to secure vehicular communication networks.

3.2 Vehicular Communication Network Model with Unconditionally Secure Key Exchange

Before comprehending the unconditionally secure key exchange for vehicular communication systems, we should first describe our proposed network model. The main goal of this new model is to generate and distribute information theoretically secure keys that are later used to secure information prior to transmission. An abstract view of this vehicular communication architecture, with nodes and authorities, is shown in Fig. 11.

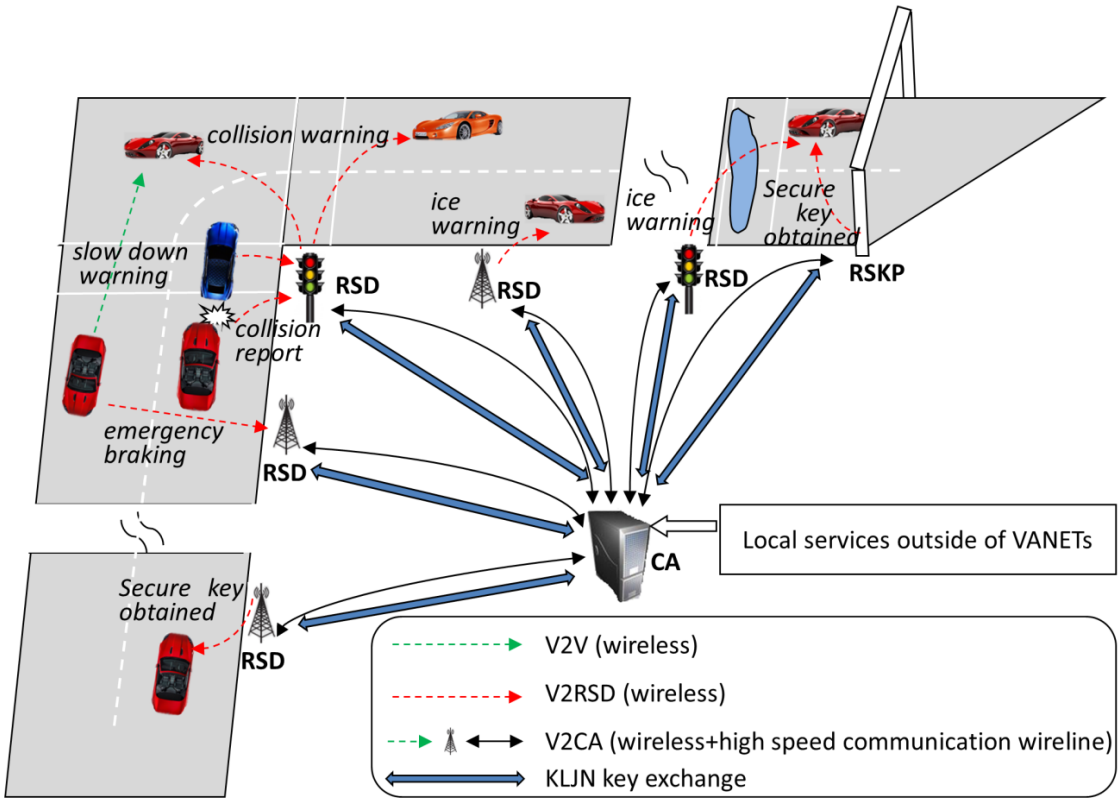

Figure 11 Vehicular communication network with unconditionally secure key exchange. The network nodes remain the same except for a new node: the roadside key provider (RSKP) and extra wires for KLJN key exchange between the CA and RSD and/or RSKP. The existing wirelines between the RSDs/RSKPs and the CA are kept for high speed communication purposes

As noticed in Fig. 11, very few changes have been made to the existing vehicular communication architecture (see Fig. 4). The network nodes remain almost the same except for a new node: the roadside key provider (RSKP). The RSKP is in charge of providing the cars with unconditionally secure keys via a near field communication technology.

Another change in the network topology is that the RSD2CA communication now utilizes an extra wire for KLJN key exchange. The existing wire line between the RSD and the CA can be kept for high speed communication purposes. Also, an extra

wire line between the RSKP and the CA has been included to transmit safety and mobility-related messages.

Table 4 shows a summary of the type of communications between the different nodes in the proposed vehicular communication network with unconditional secure key exchange. It also shows the communication technology utilized and the points at which the KLJN system will be used.

Table 4 Communications in the vehicular network model with unconditionally secure key exchange

Type of Communication	Communication Technology	KLJN system
V2V	Wireless Communication	No
V2RSD and/or RSD2V	Wireless Communication	No
V2CA and/or CA2V	Wireless Communication (V2RSD or RSD2V) and Wireline Communication (RSD2CA or CA2RSD)	Yes (wireline segment)
CA2RSKP and/orRSKP2CA	Wireline Communication	Yes
RSKP2V	Close Proximity Communication	No

Under this secure key distribution solution, each node (*i.e.*, vehicle and RSDs) will be assigned a key that does not contain any information related to the identity of a vehicle so user's privacy is preserved. This key will unconditionally secure the information that one node sends to another across the vehicular network. For instance, before a vehicle sends a message, it first signs it with its unconditionally secure key. The receiver of the message has to extract and verify the key of the sender. The protocol used

for message authentication and key verification is out of the scope of this dissertation and will be considered in future works.

3.3 KLJN Key Generation in Vehicular Communication Networks

According to the vehicular communication network model with unconditional secure key distribution proposed in [54], there is a KLJN line connecting the Certification Authority (CA) to the Roadside Devices (RSDs) and Roadside Key Providers (RSKPs) (see Fig. 11).

The KLJN key generation process is performed as follows:

- When a vehicle needs a secure key, it sends a message (via wireless communication) to the closest RSKP with the key request.
- The RSKP will use the extra wire (*i.e.,* the high speed communication line) to inform the CA in charge about the key request.
- A key generation process will take place between the RSKP and the CA.
- The RSKP will then provide the cars with the unconditional secure keys by using a near field communication wireless technology [54].
- The RSDs also use their KLJN lines that connect them to the CA to generate KLJN keys that are used to secure the communication between RSDs and the CA.

Note that the KLJN line is used only to secretly generate and share the KLJN keys that are going to be used to secure the communication between two nodes. The rest

of the communication is performed either via wireless communication or using a high speed communication wireline.

3.4 KLJN Key Donation in Vehicular Communication Networks

As pointed out in [54], the RSKP could be visualized as a gate. The communication channel used in this key distribution can be supported by a close proximity communication technology such as radio-frequency identification (RFID) [76–78], near field communication (NFC) [78], and/or near field magnetic induction communication (see Fig. 12 for an illustration)[79]. Near field magnetic induction communication utilizes an inductive coupling. The operating frequency range is centered on 13.56 MHz on ISO/IEC 18000-3 air interface and offers data transmission rates ranging from 106 kbit/s to 424 kbit/s within a distance of approximately 10 centimeters or less [80].

Since close proximity communication technologies utilize a wireless communication interface, eavesdropping is an important issue [81]. An unauthorized third party could use an antenna to listen the transmitted signals. In order to provide protection against eavesdropping and data modification attack, a secure channel can be established [81, 82]. The authors of [81] proposed a NFC specific key agreement. This key agreement does not require any asymmetric cryptography thus reducing the computational requirements significantly. In [82], a key agreement protocol between a

reader and a tag that is resistant in presence of passive adversaries in RFID communication was proposed.

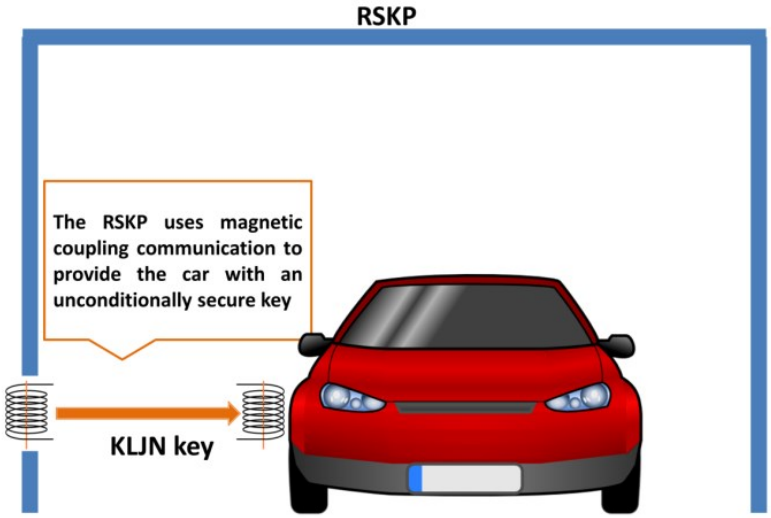

Figure 12 Abstract illustration of roadside key providers delivering an unconditionally secure key to vehicles via near field communication. Similar to the transformer principle, the magnetic near-field of two conductor coils is used to couple the initiator device (located at the RSKP) and listening device (located at the vehicle) [80]. Modulation schemes used include: amplitude on/off keying (OOK) with different modulation depth (100 % or 10 %) and Binary phase-shift keying (BPSK)[80]

It is important to mention that the aforementioned RSKP key donation, where RSKPs were visualized as gates [54], might not be as efficient as expected. This is because vehicles would have to slow down in order to get sufficiently close to the RSKPs (as proximity is needed for secure key donation). Therefore, we also propose a lane-by-lane key donation using RSKP equipment embedded in the pavement. In this way, vehicles will not have to slow down to obtain their keys. To detect vehicles in each

lane, either loop detectors [83] or high-definition digital wave radars [84] deployed on the side of the roadway can be used. Both the RSKPs and the radar units can be connected to RSDs through a high speed wireline connection. Thus, the KLJN key generation is performed between RSDs and the CA only, while the RSKP will be only in charge of providing the cars with the unconditionally secure KLJN keys. Moreover, this key donation process would be encrypted with the former key, therefore, even if an eavesdropper is listening, he/she would not be able to extract the key information unless he/she has the former key. Figure 13 illustrates this solution.

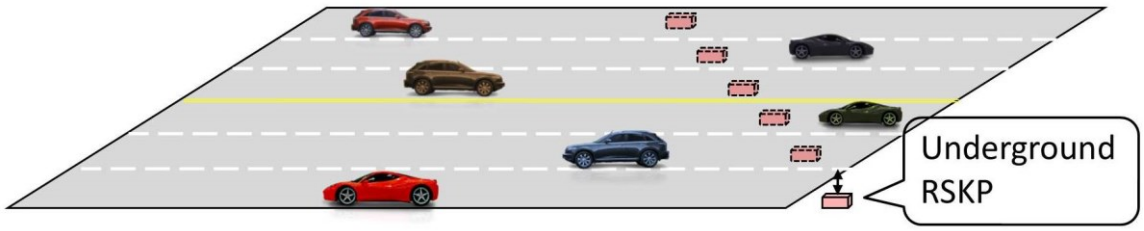

Figure 13 Key donation to vehicles with RSKP equipment embedded in the pavement. RSKPs are located underground of each lane

3.5 Upper Limit of the KLJN Key Lifetime in Vehicular Communication Networks

The lifetime of the KLJN key in vehicular communication networks is a very important technical parameter that needs to be discussed. This is because the longer the KLJN key is used, the more susceptible it is to attacks.

In order to find out the lifetime of the KLJN key in vehicular communication networks, we proceed as follows. First of all, the noise bandwidth B_{KLJN} is determined

by the distance L between the two communicating parties, which in the case of vehicular communication networks depends on the length of the KLJN line segment between RSDs and the CA. Thus, the following relationship must be satisfied [30]: $B_{KLJN} \ll \frac{c}{L}$, where c is the speed of electromagnetic waves in the wireline. Suppose that $0 < \Theta \ll 1$ and the noise bandwidth is:

$$B_{KLJN} = \Theta \frac{c}{L}. \tag{34}$$

Also, the duration of the bit sharing period τ must be long enough compared to the correlation time of the noise τ_{KLJN}, *i.e.*, $\tau_{KLJN} \approx \frac{1}{B_{KLJN}}$, in order to correctly distinguish between the different resistors situations [40, 44]. The frequency of *secure* bit exchange is:

$$f_{\text{sec}} = \frac{1}{2} \frac{B_{KLJN}}{\gamma}, \tag{35}$$

where $\gamma \gg 1$ (see [44, 45]) and the factor $\frac{1}{2}$ is due to the fact that a secure bit exchange occurs (on average) 50% of the time.

The lifetime of the KLJN key τ_k in vehicular communication networks depends on the vehicle density. For the sake of simplicity, we assume homogenous car density:

$$n_c = \frac{N_c}{N_{KLJN}}, \tag{36}$$

where N_c is the number of cars and N_{KLJN} is the number of Roadside Devices with KLJN units. Thus, a KLJN unit serves n_c cars. Consequently, the frequency of *secure* bit donation to a single car is:

$$f_c = \frac{f_{\text{sec}}}{n_c}. \tag{37}$$

If the length of the KLJN key is defined as N_k, then by combining Eqs. (34)–(37), we find that the lifetime of the KLJN key in vehicular communication networks is:

$$\tau_k = \frac{N_k}{f_c} = \frac{2N_k n_c \gamma L}{\Theta c}. \tag{38}$$

Note that this result represents a pessimistic estimation for inhomogeneous vehicular communication networks when n_c is the upper limit of the number of cars any RSD is handling. Thus, Eq. (5) gives an upper limit of the lifetime of the KLJN key in vehicular communication networks. To demonstrate the results, we assign possible practical values to the parameters. Let $L = 1000\,\text{m}$, $c = 2\times 10^8$ m/s, $\gamma = 100$ (since $\gamma = \frac{B_{KLJN}}{f_B}$, where $f_B = \frac{1}{\tau}$ should be low enough compared to B_{KLJN}, see [40, 45]),

$N_k = 100$ bits, $n_c = 1000$ vehicles, and $\Theta = 0.1$ (in order to satisfy $B_{KLJN} \ll \frac{c}{L}$, that is the "no-wave limit" condition [22]). Then the lifetime of KLJN key is $\tau_k = 10^3$ s.

Techniques such as building parallel channels by using chip and multi-wire cables can be used to enhance the speed of the KLJN scheme and to decrease τ_k [30]. There is also a possibility to increase the security of physically exchanged keys in the case of repeated usage [43].

4. CONCLUSIONS AND FUTURE RESEARCH

This section summarizes the main points presented in this dissertation and the results and contributions of this research. Also, since the KLJN key exchange scheme system possesses a wide range of possible applications and consequently new lines of work, a section on future research is also presented.

4.1 Summary of the Work

In this dissertation, the types of errors that occur in the voltage-based and current-based measurement modes of the KLJN key exchange scheme have been classified and analyzed. We also presented an important practical application of the KLJN system.

Section 1 presented an introduction to our work, describing the working principle and the main features of the KLJN key exchange scheme, which represents our focus of study. This section set the tone of this dissertation by describing how it is organized and by presenting the main objectives of our study.

In section 2, the different types of errors in both the voltage-based and the current-based measurement modes of the KLJN secure key exchange scheme were classified. The mathematical approach to estimate the error probability was presented. Close-form expressions for the probability of each type of error in both the voltage-based and current-based measurement modes were given. These error probabilities

showed an exponential dependence on the duration of the bit sharing period. Furthermore, an error mitigation method was developed. In this method, only the bits that are indicated to be secure by both the voltage-based and the current-based methods are kept. The resulting error probability of this combined error removal strategy is the product of the error probabilities of the two methods, which follows from the statistical independence of the AC components of the current and voltage mean-square measurements. This error removal method showed superior fidelity, with drastically reduced error probability compared to the former schemes.

Section 3 introduced a new practical application of the KLJN system. This section starts with a summary of some of the existing key exchange techniques proposed for vehicular communication networks. Then, special attention was given to some concerns regarding the level of security provided by these security techniques. Motivated by these concerns, we outlined how the KLJN key exchange system could theoretically be used to achieve unconditionally secure keys to secure the communication in these networks. The network model with unconditionally secure key exchange was presented. Based on this architecture, a new network node and new wire connections were described as well as the recommended communication technologies. Also, some technical considerations related to these new unconditionally secure keys such as the KLJN key generation process, the KLJN key donation to vehicles, and the KLJN key lifetime, were addressed.

4.2 Summary of the Contributions

The contributions of the work presented in this dissertation can be summarized as follows:

- This work provides a mathematical formulation of the errors in the KLJN secure key exchange scheme. A closed-form estimate of the probability of each type of error in both the voltage and current measurement modes was derived for the *first time*. These formulas are simple enough to be used as design tools for the KLJN systems. They capture the influence of the threshold values and the duration of the bit sharing period on errors.
- With the development of the combined voltage-current error mitigation strategy, it has been demonstrated that the KLJN system can operate without utilizing any error correction algorithm. This is a great advantage since adding error correction techniques cause information leak. Also, error correction algorithms might increase the data transmission overhead due to redundancy bits. It would also increase the complexity of the system due to encoding/decoding algorithm needed for error correction, which would affect the time needed for establishing the secure key.
- The KLJN key exchange scheme was proposed for enhancing the security in vehicle communication networks. The main advantage of this network model with unconditionally secure key exchange is that no computational limitations are assumed about the eavesdropper.

4.3 Future Research

After culminating this work, several future research lines related to the two main topics discussed in this dissertation have been identified. Some of them are summarized as follows:

- An experimental demonstration of the KLJN key exchange scheme was already carried out in [31]. Unfortunately, neither the values of the thresholds nor the bit exchange period was varied in this experimental paper, thus making systematic comparison with our results impossible. Thus such experiments would be interesting.
- Enhanced security protocols were proposed in [39]. These new versions of the KLJN system showed how the security of this key exchange scheme can be enhanced without discarding bits or without applying privacy amplification techniques. One of them, specifically the "Intelligent" KLJN (iKLJN) scheme, offers to improve the speed of the system and to enhance its security by reducing the bit sharing period. Therefore, a complete study regarding the effects of reducing this time window on the bit errors would be encouraged.
- Studies regarding new attack types will be helpful in guiding us to further enhance the KLJN scheme; as well it would teach us the needs of new types of countermeasures and defense strategies.
- The development of a protocol for distributing, managing, and storing the KLJN keys in the proposed unconditional secure vehicular communication model is one

of the most important subjects to take into consideration in the future. This protocol should comprise a detailed explanation on how keys are distributed and stored. It must also consider the key replacement protocol. Furthermore, a protocol used for message authentication and key verification should be developed.

REFERENCES

[1] Y. Liang, H. V. Poor, and S. Shamai, Information theoretic security, *Foundations Trends Commun. Inform. Theory* **5** (2008) 355–580.

[2] R. Mingesz, L.B. Kish, Z. Gingl, C.G. Granqvist, H. Wen, F. Peper, T. Eubanks, and G. Schmera, Unconditional security by the laws of classical physics, *Metrol. Meas. Syst.* **20** (2013) 3–16.

[3] R. Mingesz, L. B. Kish, Z. Gingl, C.G. Granqvist, H. Wen, F. Peper, T. Eubanks, and G. Schmera, Information Theoretic Security by the laws of classical physics, *Soft computing Applications: Proeedings. of the 5th International Workshop Soft Computing Applications (SOFA)*, Springer Berlin-Heidelberg, Berlin, Germany (2013), pp. 11–25.

[4] L. B. Kish, D. Abbott, and C. G. Granqvist, Critical analysis of the Bennett-Riedel attack on secure cryptographic key distributions via the Kirchhoff-law-Johnson-noise scheme, *PLoS ONE* **8** (2013) e81810 (15 pages).

[5] E. Gonzalez, L. B. Kish, and R. S. Balog, Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters, *PLoS ONE* **8** (2013) e70206 (10 pages).

[6] T. Horvath, L.B. Kish, and J. Scheuer, Effective privacy amplification for secure classical communications, *EPL* **94** (2011) 28002 (6 pages).

[7] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, Quantum cryptography, or unforgeable subway tokens, *Advances in Cryptology: Proceedings of Crypto '82*, Plenum Press, Santa Barbara, California, USA (1982), pp. 267–275.

[8] H. P. Yuen, Key Generation: Foundation and a New Quantum Approach, *IEEE J. Selected Topics in Quantum Electronics* **15** (2009) 1630–1645.

[9] H. Salih, Z. H. Li, M. Al-Amri, and H. Zubairy, Protocol for direct counterfactual quantum communication, *Phys. Rev. Lett.* **110** (2013) 170502 (5 pages).

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

[11] H. P. Yuen, Unconditional Security in Quantum Key Distributions (2012). Manuscript: arXiv:1205.5065v2.

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

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

[14] H. P. Yuen, Security Significance of the Trace distance Criterion in Quantum Key Distribution (2012). Manuscript: arXiv:1109.2675v3.

[15] Z. Merali, Hackers blind quantum cryptographers, *Nature News* (August 29, 2009).

[16] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, *Nature Commun.* **2** (2011) 349 (6 pages).

[17] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov , Hacking commercial quantum cryptography systems by tailored bright illumination, *Nature Photonics* **4** (2010) 686–689.

[18] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, Experimentally faking the violation of Bell's inequalities, *Phys. Rev. Lett.* **107** (2011) 170404 (5 pages).

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

[20] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, After-gate attack on a quantum cryptosystem, *New J. Phys.* **13** (2011) 013043 (14 pages).

[21] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Thermal blinding of gated detectors in quantum cryptography, *Opt. Express* **18** (2010) 27938–27954.

[22] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device calibration impacts security of quantum key distribution, *Phys. Rev. Lett.* **107** (2011) 110501 (5 pages).

[23] L. Lydersen, J. Skaar, and V. Makarov, Tailored bright illumination attack on distributed-phase-reference protocols, *J. Mod. Opt.* **58** (2011) 680–685.

[24] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, Controlling a superconducting nanowire single-photon detector using tailored bright illumination, *New J. Phys*. **13** (2011) 113042 (14 pages).

[25] L. Lydersen, V. Makarov, and J. Skaar, Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography", *Appl. Phys. Lett*. **99** (2011) 196101 (1 page).

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

[27] L. Lydersen, N. Jain, C. Wittmann, O. Maroy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, Superlinear threshold detectors in quantum cryptography, *Phys. Rev. Lett*. **84** (2011) 032320 (7 pages).

[28] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Avoiding the blinding attack in QKD; REPLY (COMMENT), *Nature Photonics* **4** (2010) 800–801.

[29] V. Makarov, Controlling passively quenched single photon detectors by bright light, *New J. Phys*. **11** (2009) 065003 (18 pages).

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

[31] R. Mingesz, Z. Gingl, and L. B. Kish, 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** (2008) 978–984.

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

[33] L. B. Kish and C. G. Granqvist, On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator, *Quantum Inf. Process.* **13** (2014) 2213–2219.

[34] D. Abbott and G. Schmera, Secure communications using the KLJN scheme, *Scholarpedia* **8** (2013) 31157.

[35] J. B. Johnson, Thermal Agitation of Electricity in Conductors : details of the experiment, *Phys. Rev.* **32** (1928) 97–109.

[36] H. Nyquist, Thermal Agitation of Electric Charge in Conductors: the theory, *Phys. Rev.* **32** (1928) 110–113.

[37] C. D. Motchenbacher and J.A. Connelly, Low-Noise Electronic System Design, John Wiley & Sons, New York, USA (1993), pp. 5–32.

[38] L. B. Kish, 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** (2005) L57–L63.

[39] L. B. Kish, Enhanced secure key exchange systems based on the Johnson-noise scheme, *Metrol. Meas. Syst.* **20** (2013) 3–16.

[40] Y. Saez and L. B. Kish, Errors and their mitigation at the Kirchhoff-Law-Johnson-Noise secure key exchange, *PLoS ONE* **8** (2013) e81103 (7 pages).

[41] R. Mingesz and Z. Gingl, Noise properties of the KLJN secure communication system, *PLoS ONE* **9** (2014) e96109 (4 pages).

[42] L. B. Kish and C. G. Granqvist, On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator, *Quantum Inf. Process* **13** (2014) 2213–2219.

[43] L. B. Kish, Enhanced usage of keys obtained by physical, unconditionally secure distributions (2014). Manuscript: http://arxiv.org/abs/1408.5800.

[44] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law–Johnson-noise secure key exchange, *J. Comput. Electron*. **13** (2014) 271–277.

[45] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, Bit Errors in the Kirchhoff-Law-Johnson-Noise secure key exchange, *Int. J. Mod. Phys. Conf. Ser.* **33** (2014) 1460367 (8 pages).

[46] L. B. Kish and O. Saidi, Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives, *Fluct. Noise Lett.* **8** (2008) L95–L98.

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

[48] G. Dimitrakopoulos and P. Demestichas, Intelligent Transportation Systems, *IEEE Vehicular Technol. Mag.* **5** (2010) 77–84.

[49] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. Hubaux, Secure vehicular communication system: design and architecture, *IEEE Commun.* **46** (2008) 100–109.

[50] M. Raya, P. Papadimitratos, and J. P. Hubaux, Securing vehicular communications, *IEEE Wireless Commun.* **13** (2006) 8–15.

[51] M. Raya and J. P. Hubaux, The security of vehicular Ad Hoc networks, *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc Sensor Networks*, Alexandria, VA, USA, November (2005), pp. 11–21.

[52] P. Papadimitratos, F. La, K. Evenssen, R. Bringnolo, and S. Cosenza, Vehicular communication systems: enabling technologies, applications, and future outlook on intelligent transportation, *IEEE Commun.* **47** (2009) 84–95.

[53] P. Ardelean and P. Papadimitratos, Secure and privacy-enhancing vehicular communication: Demonstration of implementation and operation, *Proceedings of the 68th IEEE Conf. on Vehicular Technology*, Calgary, CA, September (2008), pp. 1–2.

[54] Y. Saez, X. Cao, L. B. Kish, and G. Pesti, Securing vehicle communication systems by the KLJN key exchange protocol, *Fluct. Noise Lett*. **13** (2014) 1450020 (14 pages).

[55] G. Calandriello, P. Papadimitratos , J.-P . Hubaux, and A. Lioy, On the Performance of Secure Vehicular Communication Systems, *IEEE Trans. Dependable Sec. Computing* **8** (2011) 898–912.

[56] National ITS Architecture, DSRC 5GHz: Dedicated short range communication standard activities group , December (2014). http://www.iteris.com/itsarch/html/standard/dsrc5ghz.htm.

[57] IEEE P802.11p/D3.0, Draft Amendment for Wireless Access in Vehicular Environments (WAVE) , July (2007).

[58] X. Cao, Y. Saez, L. B. Kish, and G. Pesti, On KLJN-based Secure Key Distribution in Vehicular Communication Networks, *Fluct. Noise Lett*. **14** (2015) 1550008 (11 pages).

[59] L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, Spectra for the product of Gaussian noises, *Metrol. Meas. Syst.* **19** (2012) 653–658.

[60] S. O. Rice, Mathematical analysis of random noise, *Bell Syst. Tech. J*. **23** (1944) 282–332.

[61] I. Rychlik, On some reliability applications of Rice's formula for the intensity of level crossings, *Extremes* **3** (2000) 331–348.

[62] L. B. Kish, End of Moore's Law; Thermal (Noise) Death of Integration in Micro and Nano Electronics, *Phys. Lett. A.* **305** (2002) 144–149.

[63] L. B. Kish and C. G. Granqvist, Electrical Maxwell Demon and Szilard Engine Utilizing Johnson Noise, Measurement, Logic and Control, *PLoS ONE* **7** (2012) e46800 (8 pages).

[64] L. B. Kish and C. G. Granqvist, Energy requirement of control: Comments on Szilard's engine and Maxwell's demon, *EPL* **98** (2012) 68001 (6 pages).

[65] J. Blum and A. Eskandarian, The threat of intelligent collisions, *IT Professional* **6** (2004) 24–29.

[66] M. Raya and J. P. Hubaux, Securing vehicular ad hoc networks, *Journal of Computer Security* **15** (2007) 39–68.

[67] C. T. Li, M. S. Hwang, and Y. P. Chu, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, *Comput. Commun*. **31** (2008) 2803–2814.

[68] K. D. Kim and P. R. Kumar, An MPC-based approach to provable system-wide safety and liveness of autonomous ground traffic, *IEEE Trans. Autom. Control* **59** (2014) 3341–3356.

[69] N. Wang, Y. Huang, and W. Chen, A novel secure communication scheme in vehicular ad hoc networks, *Comput. Commun*. **31** (2008) 2827–2837.

[70] A. Studeret, E. Shi, F. Bai, and A. Perrig, TACKing together efficient authentication, revocation, and privacy in VANETs, *Proceedings of the 6th IEEE Annual Conf. on Sensor, Mesh and Ad Hoc Communications and Networks*, Rome, Italy (June 2009), pp. 1–9.

[71] D. Boneh, X. Boyen, and H. Shacham, Short group signatures, *Proceedings of the 24th Annual Int. Cryptology Conference*, Santa Barbara, CA, USA (August 2004), pp. 41–55.

[72] J. Guo, J. P. Baugh and S. Wang, A group signature based secure and privacy preserving vehicular communication framework, *Proceedings of the IEEE Conf. on Mob. Network. For Vehic. Environ.*, Anchorage, Alaska, United States of America (May 2007), pp. 103–108.

[73] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, *Proceedings of the 27th IEEE Conf. on Computer Communications*, Phoenix, AZ, USA (April 2008), pp. 13–18.

[74] C. Zhang, X. Lin, R. Lu, and P. Ho, RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks, *Proceedings of IEEE Int. Conf. on Communications*, Beijing, CHN (May 2008), pp. 1451–1457.

[75] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, SPECS: Secure and privacy enhancing communications schemes for VANETs, *Ad Hoc Networks* **9** (2011) 189–203.

[76] K. Domdouzis, B. Kumar, and C. Anumba, Radio-Frequency Identification (RFID) applications: A brief introduction, *Adv. Eng. Inform.* **21** (2007) 350–355.

[77] S. Weis, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, *Lect. Notes Comput. Sc.* **2802** (2004) 201–212.

[78] F. Michahelles, E. Zurich, F. Thiesse, A. Schmidt, and J.R. Williams, Pervasive RFID and Near Field Communication Technology, *IEEE Trans. Pervasive Comput.* **6** (2007) 94–96.

[79] R. Bansal, Near-field magnetic communication, *IEEE Trans. Antennas Propag.* **46** (2004) 114–115.

[80] V. Coskun, B. Ozdenizci, and K. Ok, A Survey on Near Field Communication (NFC) Technology, *Wireless Pers. Commun*. **71** (2013) 2259–2294.

[81] E. Haselsteiner and K. Breitfu, Security in near field communication: Strengths and Weaknesses, *Printed handout of Workshop on RFID security*, Graz, Austria (July 2006), pp. 151–166.

[82] C. Castelluccia and G. Avoine, Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags, *Proceedings of 7th IFIP WG 8.8/11.2 International Conference*, Tarragona, Spain (April 2006), pp. 19–21.

[83] P. Lingenfelser and P. Thilo, Loop detectors for measuring road traffic, *Siemens Rev.* **37** (1970) 332–337.

[84] D. Middleton, H. Charara, and R. Longmire, Alternative vehicle detection technologies for traffic signal systems: technical report, *Research Report FHWA/TX-09/0-5845-1*, Texas Transportation Institute, The Texas A&M University System, College Station, TX, USA (February 2009).

APPENDIX*

Published Paper 1: Errors and their Mitigation at the Kirchhoff-law-Johnson-noise (KLJN) Secure Key Exchange

This paper [40] classifies and analyzes the types of errors of bit exchange between Alice and Bob in the voltage-based measurement mode of the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange. Some types of errors are automatically removed by the original protocol. A mathematical analysis of the error probabilities and their dependence on the KLJN parameters of the errors that are not removed by the protocol is presented. Important parameters are identified, such as the duration of the bit sharing period τ and the parameters β and δ that define the threshold values for bit interpretation. The results showed that the error probability decays exponentially by increasing these parameters. The most important of such parameters is the duration of the bit sharing period τ, because its value is not limited. The results indicate that it is

*Part of this section is a modified reprinted version of: Y. Saez and L. B. Kish, Errors and their mitigation at the Kirchhoff-Law-Johnson-Noise secure key exchange, *PLoS ONE* 8 (2013) e81103 (7 pages), © 2013 Saez and Kish.

*Part of this section is reprinted with kind permission from Springer Science+Business Media: Journal of. Computational Electronics, Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law-Johnson-noise secure key exchange, 13, 2014, 271–277, Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, © Springer Science+Business Media New York 2013.

*Part of this section is reprinted with kind permission from: Y. Saez, X. Cao, L. B. Kish, and G. Pesti, Securing Vehicle Communication Systems by the KLJN key exchange protocol, *Fluctuation and Noise Letters*. 13 (2014) 1450020 (14 pages), © World Scientific Publishing Company 2014. DOI: 10.1142/S0219477514500205.

*Part of this section is reprinted with kind permission from: X. Cao, Y. Saez, G. Pesti, and L. B. Kish, On KLJN-based secure key distribution in vehicular communication networks, *Fluctuation and Noise Letters*. 14 (2015) 1550008 (11 pages), © World Scientific Publishing Company 2015. DOI: 10.1142/S021947751550008X.

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 [39].

Published Paper 2: Current and Voltage-based Bit Errors and their Combined Mitigation for the Kirchhoff-law-Johnson-noise Secure Key Exchange

This paper [44] classifies and evaluates the types of errors that occur in the current-based scheme of the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange. These error probabilities showed an exponential dependence on the duration of the bit exchange, which is analogous to the result for the corresponding voltage-based scheme as discussed in an earlier work [40].

Furthermore, we presented an error mitigation strategy based on the combination of voltage-based and current-based schemes: only those exchanged bits are kept that are indicated to be secure by both the current and voltage methods. The resulting error probability of this combined strategy is the product of the error probabilities of the two methods, which follows from the statistical independence of the current and voltage measurements. Thus, this combination method has superior fidelity, with drastically reduced error probability compared to the former schemes, and it also shows an exponential dependence on the duration of the bit sharing period. As a consequence, the

KLJN scheme can operate without error correcting algorithms, thereby preserving the independence of the exchanged bits of the secure key. Thus, the key bits remain independently and identically distributed random variables, which is an important advantage for secure communication [4].

Published Paper 3: Bit Errors in the Kirchhoff-law-Johnson-noise Secure Key Exchange

This paper [45] classifies and analyzes bit errors in the voltage and current measurement modes of the Kirchhoff-law-Johnson-noise (KLJN) secure key distribution system. In both measurement modes, the error probability decays exponentially with increasing duration of the bit sharing period (BSP) at fixed bandwidth. We also present an error mitigation strategy based on the combination of voltage-based and current-based schemes. The combination method has superior fidelity, with drastically reduced error probability compared to the former schemes, and it also shows an exponential dependence on the duration of the BSP. With this combination method is it shown that the KLJN system can operate without any error correction algorithm, which would cause information leak towards the eavesdropper.

This paper is a summary of recent findings presented in [40] and [44].

Published Paper 4: Securing Vehicle Communication Systems by the KLJN Key Exchange Protocol

In this paper [54], we assessed some concerns regarding the security in vehicular communication networks. Based on this assessment, we outlined how the KLJN could theoretically be used to achieve unconditional secure keys to secure vehicular communication networks. The points at which the KLJN system can be used are presented and the new network node in charge of delivering the secure KLJN keys to the vehicles is introduced. The main advantage of this information theoretic secure key network model is that none computational limitations are placed on the eavesdropper. This means that, with sufficient information about the channel quality and the messages, it is possible to make very accurate statements about the information that is extracted by the eavesdropper.

Published Paper 5: On KLJN-based Secure Key Distribution in Vehicular Communication Networks

In a former paper [*Fluct. Noise Lett.* **13** (2014) 1450020] we introduced a vehicular communication system with unconditionally secure key exchange based on the Kirchhoff-Law-Johnson-Noise (KLJN) key distribution scheme. In this paper [58], we address the secure KLJN key donation to vehicles. This KLJN key donation solution is

performed lane-by-lane by using roadside key provider equipment embedded in the pavement.

A method to compute the lifetime of the KLJN key is also given. This key lifetime depends on the car density and gives an upper limit of the lifetime of the KLJN key for vehicular communication networks.