THE IMPACT OF PARASITIC DC AND AC SOURCES ON THE SECURITY OF THE KLJN SECURE KEY EXCHANGE SCHEME

A Dissertation

by

MUTAZ YOUSEF MELHEM

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,	Robert S. Balog
	Jun Zou
	Andreas Klappenecker
Head of Department,	Miroslav Begovic

May 2021

Major Subject: Electrical Engineering

ABSTRACT

The Kirchhoff-Law-Johnson-Noise (KLJN) scheme is a statistical-physical secure key exchange system based on the laws of classical statistical physics to provide unconditional security. This dissertation contains four interrelated studies of the security of the KLJN system.

In the first study, a new attack against the KLJN key distribution system is explored. The attack is based on utilizing a parasitic voltage-source in the loop. Relevant situations often exist in the low-frequency limit in practical systems, especially when the communication is over a distance or between different units within an instrument, due to a ground loop and/or electromagnetic interference (EMI). The study investigates the DC ground loop situation when no AC or EMI effects are present. Surprisingly, the usual current/voltage comparison-based defense method that exposes active attacks or parasitic features (such as wire resistance based information leaks) does not work here. The attack is successfully demonstrated and we proposed defense methods against the attack as shown.

The second study investigates the security of the KLJN key distribution system with unknown parasitic DC-voltage sources at both Alice's and Bob's ends. This work is the generalization of our earlier investigation with a single-end parasitic source. Similarly to the first study, the defense method based on comparing current/voltage data at Alice's and Bob's ends is useless here since the wire currents and voltages are equal at both ends.

Under the assumption that Eve does not know the values of the parasitic sources, a new attack, utilizing the current generated by the parasitic DC-voltage sources, is introduced. The attack is mathematically analyzed and demonstrated by computer simulations. Some defense methods against the attack are shown.

The third study addresses a new question regarding the security of the KLJN scheme compromised by DC sources at Alice and Bob: What is the impact of these parasitic sources on active attacks, such as the man-in-the-middle (MITM) attack, or the current injection attack? The surprising answer is that the parasitic DC sources actually increase the security of the system because, in the case of the MITM attack, they make it easier to uncover the eavesdropping. In some of the cases Eve can fix this deficiency but then the problem gets reduced to the original MITM attack to which the KLJN scheme is immune, as it is already proven earlier.

In the last section a new attack against the KLJN secure key exchange scheme is introduced. The attack exploits a parasitic/periodic AC voltage-source at either Alice's or Bob's end. Such situations exist due to AC ground loops and electromagnetic interference (EMI). In the low-frequency limit, the procedure is the generalized form of the former DC ground loop-based attack. In the high-frequency case, the spectrum of the wire voltage is utilized. The attack is demonstrated in both the low and the high-frequency situations. Defense protocols against the attack are also discussed.

DEDICATION

To whom I pray, worship, live and die (Allah)

ACKNOWLEDGEMENTS

First of all, I would like to thank all mighty Allah for giving me this blessing and opportunity to earn my Ph.D. from this great institution.

I would like to thank my committee chair, Dr. Laszlo Kish, for his guidance and support throughout the course of this research. Also, I would like to thank my committee members, Dr. Balog, Dr. Zhou and Prof. Klappenecker.

I would like to thank my father Dr. Yousef Ayyash Melhem, and my mother Mrs. Mariam Melhem, for giving me everything they can to reach this level. Then I would like to thank my wife Dr. Sahar Ali Tawayha, and our little angels Noor, Ali, and Leen for their huge patience and support to accomplish this mission.

Also, I would specially thank my brother Dr. Ayyash Y. Melhem, for his valuable and huge support through this journey. Also, I would like to thank my other brothers and sister Maher, Bashar, and Dr. Lama for their valuable support.

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 would like to thank my valuable Jordanian friends and colleagues in the electrical and computer engineering department for their help at the beginning of the journey, Dr. Ahmad Al Bashayreh, Dr. Hussein Al Masri, Dr.

Ahmad Abu Al Rub, Dr. Munir Al Masad, Dr. Abdullah Al -Oqlah and Dr. Mustafa Al Shawaghfeh. Also I would like to thank my brother Zaid Al Btoush for his generous support at the end of my studies.

Special thanks to Prof. Stavros Kalafatis, and Dr. Chadi Geha, for giving me the opportunity to be part of the senior design team, from which I learned a lot and was financially supported during my course of study.

Special thanks to any good person I faced during this journey and offered me a valuable help.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supervised by a dissertation committee consisting of Professors Laszlo B. Kish [my graduate advisor] , Robert S. Balog and Jun Zou of Electrical and Computer Engineering and Professor Andreas Klappenecker of the Department of Computer Science and Engineering.

Mr. Shahriar Ferdous Ph.D. Student of the Department of Electrical and Computer Engineering provided the Matlab code to generate gaussian white noise for Section 5 simulations.

Also, he completely wrote Subsection 5.4.1. Ms. Christiana Chamon Ph.D. Student of the Department of Electrical and Computer Engineering contributed to Subsection 5.4.3.

Funding Sources

There are no outside funding contributions to acknowledge related to the research and compilation of this document.

NOMENCLATURE

KLJN	Kirchhoff-Law-Johnson-Noise
QKD	Quantum Key Distribution
T	Temperature
MITM	Man-in-the-Middle-Attack
MHz	Mega Hertz
IoT	Internet-of-Things
LTE	Long Term Evaluation
Eve	Eavesdropper
RMS	Root Mean Square
AC	Alternating Current
DC	Direct Current
RRRT-KLJN	Random-Resistor-Random-Temperature
EMI	Electromagnetic Interference
BEP	Bit Exchange Period
R_L	The Low Resistor
R_H	The High Resistor
$I(t)$	The Current on The Wire
$U(t)$	The Voltage on The Wire
I_{DC}	The DC Component of the Current on The Wire
$I_n(t)$	The AC (noise) Component

$U_{\mathrm{An}}(t)$	The Voltage Noise Source of the Chosen Resistor R_{A}
$U_{\mathrm{Bn}}(t)$	The Votlage Noise of the Chosen Resistor R_{B}
$S_u(f)$	The Spectral Power Density of the Voltage in The Wire
$S_i(f)$	The Spectral Power Density of the Current on The Wire
T	The Common Temperature
k	The Boltzmann's Constant
R_{A}	The Actually Connected Resistance at Alice's End
R_{B}	The Actually Connected Resistance at Bob's End
$U_{\mathrm{HAn}}(t)$	The (Thermal) Noise Voltage Generator for when R_{A} =R_{H}
$U_{\mathrm{LAn}}(t)$	The (Thermal) Noise Voltage Generator for when R_{A} =R_{L}
$U_{\mathrm{HBn}}(t)$	The (Thermal) Noise Voltage Generator for when R_{B} =R_{H}
$U_{\mathrm{LBn}}(t)$	The (Thermal) Noise Voltage Generator for when R_{B} =R_{L}
U_{LH}	The DC Component of The Wire's Voltage In the LH Situation
U_{HL}	The DC Component of The Wire's Voltage In the HL Situation
U_{th}	The Threshold Voltage
p	The Correct Guessing Probability
U_{eff}	The Effective Voltage

Some notations here and in published literature are different from standard EE notations due to the interdisciplinary nature of the work.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

1. INTRODUCTION

This section is also included in the paper "A Static-Loop-Current Attack Against the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System" *. The paper was accepted and published by the *Applied Sciences* journal in 2019.

1.1. On Secure Communications

Communications systems, standards, and technologies have been developed since ancient times. Today we have the internet, Internet-of-Things (IoT), fourth generation wireless networks (LTE), and the expected fifth generation wireless networks. An important requirement of any communication paradigm is to accomplish secure communication, i.e., to protect the privacy and integrity of users' data that is transferred over the network. To achieve the security of transferred data which can contain sensitive information (e.g., bank account credentials, social security number, etc.) it is of utmost importance to defend against attacks. These attacks might be launched by an eavesdropper (Eve) who has access to the information channel between the communicating parties A (Alice) and B (Bob).

The attack is passive if it eavesdrops without disturbing channel. The attack is active (invasive) if Eve disturbs or changes the channel, such as with a Man-in-the-Middle Attack (MITM).

1.1.1. Secure Key Exchange

Secure communication systems employ ciphers to encrypt messages (plaintext) and to decrypt encrypted messages (cyphertext). While the creation of a secure and efficient cipher is a complex problem, this problem may be solved simply. Ciphers operate with secure keys that form a momentary shared secret between Alice and Bob. Sharing (exchanging) the key securely is the difficult task. The security of the key exchange can be conditional or information-theoretic (unconditional).

1.1.2. Conditional Security

Conditionally secure key exchange systems are the most common in the existing cyber systems. They are software protocols installed at Alice and Bob. Such algorithms utilize computational complexity, achieving only conditional security (see e.g., [1,2]). The system is temporarily secure provided the adversary has limited computational resources. A major goal of quantum computer developments is to crack these types of key exchange systems (e.g., the Shor algorithm). From an information-theoretic point of view, security is non-existent because Eve has all the information to crack the encryption, but she needs

a long time to do that unless she has a quantum computer or a yet-to-be-discovered classical algorithm that can do the job in a short time. The security is not future-proof.

1.1.3. Unconditional (Information-Theoretic) Security

In order to achieve unconditional (information-theoretic) security [3,4] at the key exchange, proper laws of physics with a special hardware are utilized. Two major classes of physics-based schemes have emerged for unconditional security:

(i) Quantum key distribution (QKD) [5,6] concepts assume single photons and utilize quantum physics. The underlying laws of physics are Heisenberg's uncertainty principle and the related quantum no-cloning theorem [7]. Even though there are serious debates about the actual level of unconditional security a practical QKD can offer (see e.g., [8–43]), most scientists agree that QKD is unique in its offering information-theoretic security via (a dark) optical fiber and also through air at night, provided the visibility is good [44-47].

(ii) The second major class is the KLJN key distribution method based on the statistical physical features of the thermal noise of resistors [48–64]. The related law of physics is the fluctuation-dissipation-theorem (FDT). The scheme has a wide range of applications [65-78], and has three distinct advantages among many: It works via wire connections including power, phone, and internet lines, which can be used as information channels

[65,66] to connect homes and other establishments. It can be integrated on a chip, which implies excellent robustness, low price, and applicability in bankcards, computers, instruments, and physical unclonable function (PUF) hardware keys [67,68]. Its low price allows general applications, such as unconditional security for the control of autonomous vehicular networks [69,70].

1.2. On the KLJN Secure Key Distribution

The KLJN scheme [48–64] utilizes the thermal noise of resistors (or the emulation of that by a specific hardware). In the core scheme Alice and Bob have two identical pairs of resistors, R_L and R_H ($R_L < R_H$), respectively (see Figure 1). The key exchange protocol of a single secure bit is as follows: Alice and Bob randomly pick one of their resistors (R_L or R_H), connect it to the wire channel, and keep them there during the bit exchange period while they execute voltage and/or current measurements to learn the resistor value at the other end. The noise voltage generators shown in Figure 1 with each resistor can be the resistors' own thermal noise, or an external noise generator emulating a much higher, common noise-temperature that is publicly agreed. The power density spectra of the voltage and current in the channel are given by the Johnson-Nyquist formulas [48]:

$$S_u(f) = \frac{4kTR_AR_B}{R_A + R_B} \tag{1}$$

$$S_i(f) = \frac{4kT}{R_A + R_B} \tag{2}$$

where k is the Boltzmann's constant, T is the common temperature, and $\boldsymbol{R}_A$ and $\boldsymbol{R}_B$ are the actually connected resistances at Alice's and Bob's ends, respectively, with $R_A, R_B \in \{R_L, R_H\}$ After the measurement and spectral analysis, Equations (1) and (2) have two unknown variables, namely, the values of $\boldsymbol{R}_A$ and $\boldsymbol{R}_B$, and thus Eve can find the values of the connected resistors, but not necessarily their locations, by solving these equations. We can represent the four different situations of the connected resistors (R_L and/or R_H) at Alice's and Bob's ends by the indices of the connected resistors, LL, LH, HL, and HH, respectively. As all the resistors have the same (noise) temperature, the ideal system is in thermal equilibrium, where the second law of thermodynamics guarantees zero net power-flow. Hence, Eve cannot use the evaluation of power flow to determine the locations of the momentarily connected resistors unless they have the same resistance values. On the other hand, Alice and Bob can determine the connected resistor values by using Equations (1) or (2) since they know the value of their own connected resistors. When $R_A = R_B$, which happens at 50% of the bit exchange attempts, the results are discarded.

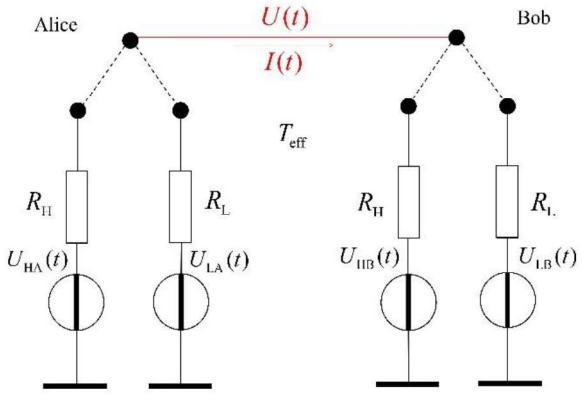

Figure 1. The core of the Kirchhoff-Law-Johnson-Noise (KLJN) system. $U_{\text{HAn}}(t)$, $U_{\text{LAn}}(t)$, $U_{\text{HBn}}(t)$, and $U_{\text{LBn}}(t)$ are the (thermal) noise voltage generators for the related resistances R_{H} and R_{L}, respectively. $U(t)$ and $I(t)$ are the measured noise voltage and the current in the wire that are used to evaluate the power density spectra $S_u(f)$ and $S_i(f)$, respectively.

1.3. On Former Attacks against the KLJN Secure Key Distribution

Several attacks [79-91] have been proposed but no attack has been able to compromise the unconditional security of the KLJN scheme because each known attack can efficiently be nullified by a corresponding defense scheme.

The attacks can be categorized into two classes:

(i) *Passive attacks* that utilize the non-ideal or parasitic features in a practical KLJN system for information leaks. Non-zero wire [resistance] (see [49,79]) poses the greatest known

threat, and the most efficient attack is power balance measurement (Second Law Attack) [80]. An efficient defense is based on a proper temperature-offset [80,81]. Temperature-inaccuracies [82] and resistance-inaccuracies [83] can also cause information leaks. On the other hand, these inaccuracies can compensate for each other [50] if used in a creative way. Non-zero cable capacitance [84] or cable inductance can also yield information leaks that can be fixed by specific designs including the proper choice of frequency range and privacy amplification. Transients can also be utilized for attack [85], but there are various means of defense against these [51,86]. The newest KLJN system, the random-resistor-random-temperature KLJN (RRRT-KLJN) scheme [52], is robust against the above vulnerabilities, or at least, no known attack exists against it yet. For other passive attacks the reader can refer to [87,88].

(ii) *Active attacks* are where Eve either modifies the information channel, or she injects an extra current into it. Current injection attacks [48,89] and MITM attacks [90] are examples which have been explored [91]. Due to the current and voltage comparison [90] feature and its more advanced cable-modeling version [89], active attacks are, so far, the least efficient attacks against the KLJN scheme.

(iii) *Flawed attacks* are some proposed attack methods that are based on misconceptions, and they do not work. For examples, see their brief summary and criticism in papers [85-86, 92–96] and the book [91].

1.4. Dissertation Focus

The research in this thesis explores new passive-attack schemes that exploit the existence of parasitic sources in a KLJN communication channel. The sources can be DC or AC, and they can be caused by ground loops, electromagnetic interference, or any imbalance between the two ends of the communication. Such sources can potentially leak information from the KLJN system.

In the first two studies, we propose attacks that exploit the existence of a parasitic DC source — or two DC sources — in a practical KLJN system. The DC source is usually a DC ground loop [97-99]. We simulated both types of attacks and proposed techniques to defend against them.

In the third study, we are studying the security of a KLJN system spoiled by two DC sources against the classical (MITM) and current-injection attacks [100].

Finally, in the fourth study, we propose a new attack that exploits the information leak resulting from an AC source located on one side of a KLJN system [101]. The attack is successfully demonstrated and shown to be easily defensible. The conclusion summarizes the key points drawn from these studies.

The importance of this research is to aid the development and design of KLJN systems against these novel passive-attack schemes. Also, it uncovers major system constraints that must be satisfied for the practical implementation of a KLJN system.

2. A LOOP-CURRENT ATTACK BASED ON HAVING A DC VOLTAGE SOURCE AT EITHER ALICE'S OR BOB'S END*

2.1. Introduction

The study in this section is also included in the paper "A Static-Loop-Current Attack Against the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System" [97]. The paper was accepted and published by the *Applied Sciences* journal in 2019.

In practical KLJN systems, in order to save a wire, the common end of the resistors (see Figure 1) is often connected to the ground. In practical situations there is often an imbalance, a voltage difference between various locations of the ground that is due, for example, to ground loop currents or electromagnetic interference (EMI) [92]. This potential information leak was pointed out in [92] as a potential source of information leaks in the case of significant cable resistance. However, it was not realized in [92] that *information leaks can exist even at zero cable resistance*. The present study is directly relevant for DC current-based ground loops (such as during secure communication between different units in instruments [67,68]).

For EMI-induced ground loops, our DC-limited study is only a first step in addressing a more general situation (which should be investigated in future works).

In this section, we explore this new information leak in the DC parasitic voltage limit. Hence, consideration was given to situations where during the bit exchange period, the relative change in the parasitic voltage is small. For the sake of simplicity but without the limitation of generality, we assume that the imperfection is represented by a positive DC voltage generator located at Alice's end (see Figure 2).

Due to Kerckhoff's principle of security, that is, the assumption that the enemy knows everything except the momentary key, we must assume that Eve knows the polarity and value of this DC voltage (If she does not know it at first, she will be able to extract it via long-time averaging). The direction of the current $I(t)$ is assumed to point from Alice to Bob. The voltage $U(t)$ and current $I(t)$ in the wire contain the sum of a DC component and a stochastic AC (that is, noise) component.

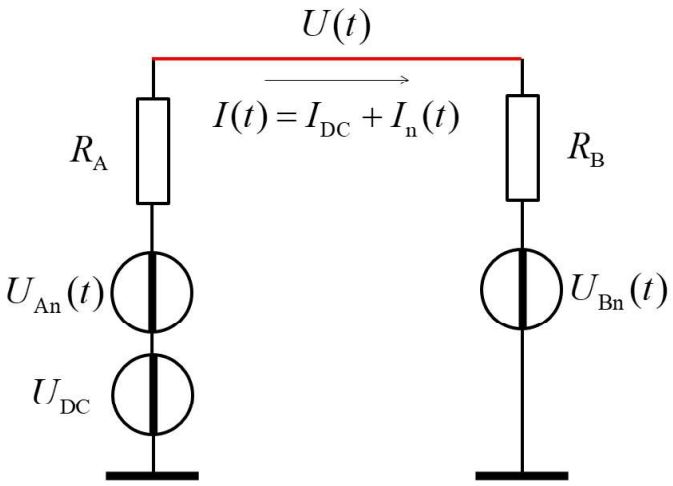

Figure 2. The KLJN system under study, where $U_{An} \lfloor \{U_{LAn};U_{HAn}\}$ and $U_{Bn} \lfloor \{U_{LBn};U_{HBn}\}$, are the noises belonging to the randomly chosen resistors, R_A and $R_B \lfloor \{R_L;R_H\}$, of Alice and Bob, respectively, U_{dc} is the DC voltage source and $U(t)$ and $I(t)$ are the voltage and current on the wire, respectively.

Let us analyze the resulting voltages and currents. The current in the wire is

$$I(t) = I_{DC} + I_n(t) \tag{3}$$

where I_{DC} is its DC component

$$I_{DC} = \frac{U_{DC}}{R_A + R_B} \tag{4}$$

and $I_n(t)$ is its AC (noise) component

$$I_{\mathrm{n}}(t)=\frac{U_{\mathrm{An}}(t)-U_{\mathrm{Bn}}(t)}{R_{\mathrm{A}}+R_{\mathrm{B}}} \tag{5}$$

in which U_{An} and U_{Bn}, with $U_{\mathrm{An}} \lfloor \{U_{\mathrm{LAn}};U_{\mathrm{HAn}}\}$ and $U_{\mathrm{Bn}} \lfloor \{U_{\mathrm{LBn}};U_{\mathrm{HBn}}\}$, are the voltage noise sources of the chosen resistors, R_{A} and R_{B}, respectively.

The voltage on the wire is

$$U(t)=I(t)R_{\mathrm{B}}+U_{\mathrm{Bn}}(t)\,. \tag{6}$$

From Equations (3) and (6) we obtain

$$U(t)=U_{\mathrm{DCw}}+U_{\mathrm{ACw}}(t)=I_{\mathrm{DC}}R_{\mathrm{B}}+I_{\mathrm{n}}(t)R_{\mathrm{B}}+U_{\mathrm{Bn}}(t) \tag{7}$$

where U_{DCw} and $U_{\mathrm{ACw}}(t)$ represent the DC and AC voltage components in the wire, respectively. The DC component can be written as

$$U_{\mathrm{DCw}}=I_{\mathrm{DC}}R_{\mathrm{B}}=\frac{U_{\mathrm{DC}}}{R_{\mathrm{A}}+R_{\mathrm{B}}}R_{\mathrm{B}}\,. \tag{8}$$

The DC component is different during Alice's and Bob's LH and HL bit situations of secure bit exchange, which yields information leaks. In the LH situation, that is, when $R_{\mathrm{A}} = R_{\mathrm{L}}$ and $R_{\mathrm{B}} = R_{\mathrm{H}}$, the DC component of the voltage on the wire is

$$U_{\mathrm{DCw}} \equiv U_{\mathrm{LH}} = U_{DC} \frac{R_{\mathrm{H}}}{R_{\mathrm{H}} + R_{\mathrm{L}}} \tag{9}$$

and, in the HL bit situation,

$$U_{\mathrm{DCw}} \equiv U_{\mathrm{HL}} = \ U_{\mathrm{DC}} \frac{R_{\mathrm{L}}}{R_{\mathrm{H}} + R_{\mathrm{L}}} \tag{10}$$

Note that as we have been assuming in the given KLJN setup that $R_{\mathrm{H}} > R_{\mathrm{L}}$, in this particular situation

$$U_{\mathrm{HL}} < U_{\mathrm{LH}} . \tag{11}$$

For later usage, we evaluate the average of U_{LH} and U_{HL} and call this quantity the *threshold voltage*, U_{th}, where

$$U_{\text{th}} = \frac{U_{\text{LH}} + U_{\text{HL}}}{2} = \frac{U_{\text{DC}}}{2}. \tag{12}$$

The effective (RMS) amplitude U_{ACw} of the noise voltage on the wire is identical in both the LH and HL cases:

$$U_{\text{ACw}} = \sqrt{4kTB_W \frac{R_{\text{L}} R_{\text{H}}}{R_{\text{L}} + R_{\text{H}}}}. \tag{13}$$

Note that the voltage and current noises in the wire follow a normal distribution since the addition of normally distributed signals results in a signal that has normal (Gaussian) distribution with a corresponding mean (see Equation 10) and variance.

For an illustration of the information leak, (see Figure 3). The DC component, that is, the mean value of the resulting (AC + DC) Gaussian depends on the bit situation during the secure key exchange. This dependence poses as a source of information for Eve about the secret key. This feature will be exploited below for the new attack scheme.

2.2. The Attack Scheme

The attack consists of three steps: measurement, evaluation, and guessing.

(i) *Measurement*: During a single secure bit exchange, Eve measures N independent samples of the wire voltage.

(ii) *Evaluation*: She evaluates the fraction γ of these N samples that are above U_{th}, which is

$$\gamma = \frac{N^+}{N} \tag{14}$$

where N^+ is the number of samples that are above U_{th}.

(iii) *Guessing* (based on Equations (9)–(14)): For $0.5 < \gamma$ and $\gamma < 0.5$, Eve's guesses are the LH and HL bit situations, respectively. For $\gamma = 0.5$, her decision is undetermined and carries no useful information.

(iv) Eve's correct guessing probability p is given as

$$p = \lim_{n_{\text{tot}} \to \infty} \frac{n_{\text{cor}}}{n_{\text{tot}}} \tag{15}$$

where n_{tot} is the total number of guess bits, and n_{cor} is the number of correctly guessed bits. The situation $p = 0.5$ indicates perfect security against Eve's attack.

In the next section, we demonstrate the attack method via computer simulation.

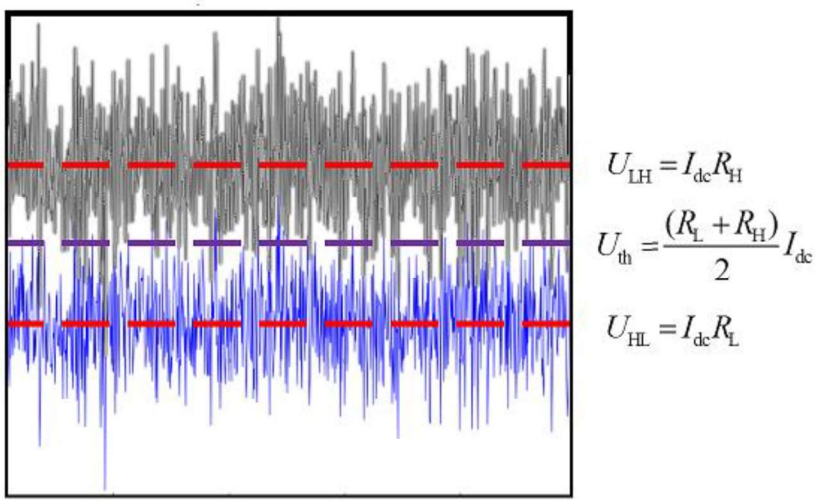

Figure 3. Eve's threshold scheme to guess the bit situation LH versus HL.

2.3. Simulation Results

To test Eve's correct guessing probability p for the LH situation, we assumed that Alice and Bob selected $R_{\text{L}} = 1\ \text{k}\Omega$ and $R_{\text{H}} = 10\ \text{k}\Omega$. During these experiments, the DC voltage was kept at a constant level of 0.1 V (see Figures 2 and 3). To generate noise, we used the

white Gaussian noise function (wgn) from the Matlab communication system toolbox to test the success statistics of the attack scheme while varying the temperature.

The effective bandwidth Δf and the range of temperatures were 1 MHz and $10^8 < T < 10^{18}$ K, respectively. At lower temperatures p was 1, within the statistical inaccuracy of simulations; at the high-temperature limit it converged to 0.5.

We tested secure key length M = 700 bits at different bit exchange durations represented by sample/bit numbers N = 1000, 500, and 200, respectively. Figure 4 shows Eve's correct guessing probability (p) of a key bit versus temperature. With temperature approaching infinity, the effective noise voltage on the wire also approaches infinity and the Gaussian density function is symmetrically distributed around the threshold voltage U_{th}. Thus, the probabilities of finding the noise amplitude above or below U_{th} are identical (0.5). Therefore, Eve's correct guessing probability represents the perfect security limit, p = 0.5.

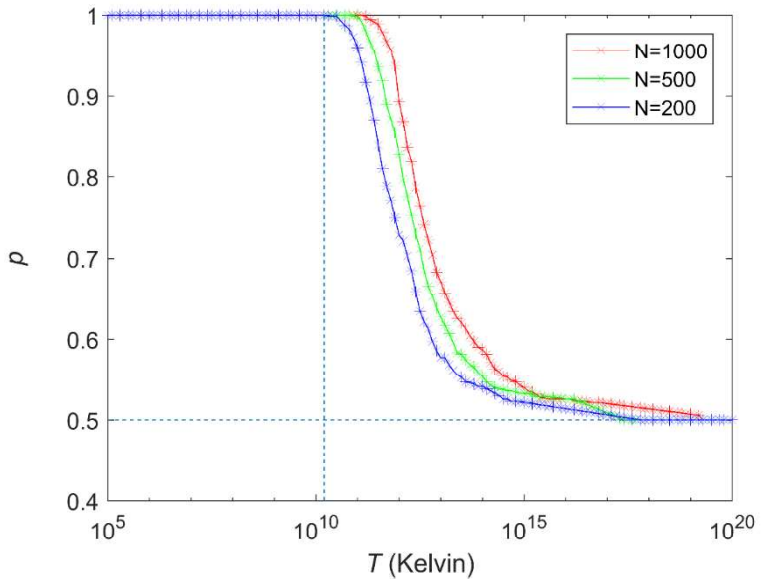

Figure 4. Eve's correct guessing probability (*p)* of key bits versus temperatures at bandwidth Δf equals 10^6 Hz, for key length 700 bits, and duration/bit (number of samples/bit) 200, 500, and 1000, respectively. The limit p = 0.5 stands for perfect security.

The observed dependence can be interpreted by the behavior of the error function (see also Equations (8) and (12))

$$p\left\{U\left(t\right)\geq U_{\text{th}}\right\}=0.5\left[1-erf\left(\frac{U_{\text{th}}-U_{\text{DCw}}}{U_{\text{eff}}\sqrt{2}}\right)\right] \tag{16}$$

where $U\left(t\right)$ is the instantaneous voltage amplitude in the wire and the error function is

(17)

$$erf(x) = \frac{1}{\sqrt{\pi}} \int_{-x}^{x} \exp\left(-y^2\right) dy .$$

The noise in the KLJN scheme is a bandlimited white noise, and thus, in accordance with the Johnson formula, the effective noise voltage scales as

$$U_{\text{eff}} \propto \sqrt{T\,\Delta f} . \tag{18}$$

Therefore, when temperature T is converging towards infinity, *p* converges to the perfect security limit of 0.5 (see Figure 4).

2.4. Some of the Possible Defense Techniques against the Attack

Based on the considerations above, the impact of the attack can be eliminated by various means. The most natural ways are:

(i) Cancelling the effect of the DC-voltage sources. For example, Bob can use a variable DC source that compensates for its effect. Similarly, eliminating ground loops is also beneficial.

(ii) Alice and Bob can increase the effective temperature, that is, the amplitudes of their noise generators (see Equation (18) and Figure 4).

(iii) Alice and Bob can increase the bandwidth to increase the effective value of the noise (see Equations (18) and (20)). However, the bandwidth must stay below the wave limit [95] to avoid information leaks due to reflection, and thus the applicability of this tool is strongly limited.

3. GENERALIZED DC LOOP CURRENT ATTACK AGAINST THE KLJN SECURE KEY EXCHANGE SCHEME*

The study in this section is also included in the paper "Generalized DC Loop Current Attack against the KLJN Secure Key Exchange" [98]. The paper was accepted and published by the journal *Metrology and Measurement Systems*.

In the present section, we study the generalized and most common practical situation of parasitic DC loop current by adding an arbitrary second generator, assuming that there was not yet enough time for Eve to utilize Kerckhoffs's principle of security [91]. We will show that Eve's job is much more complicated to attack the compromised system by two unknown DC voltage generators of arbitrary polarity that are located at Alice's and Bob's sides (see Figure 5).

* Reprinted with permission from "A Static-Loop-Current Attack against the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System." by Mutaz Melhem, and Laszlo Kish (2019). *Metrology and* Measurement Systems 26.4: 607, © [2019] by Melhem and Kish.

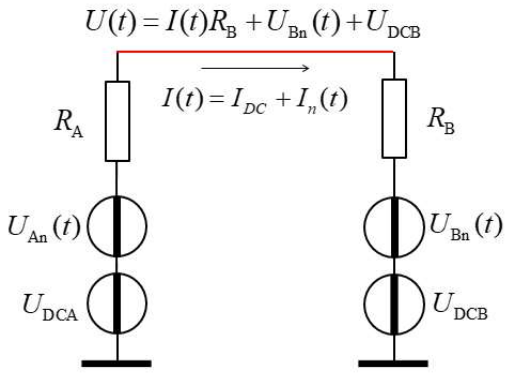

Figure 5. The KLJN system in the generalized ground loop situation $U_{Bn}(t)$ & $U_{An}(t)$ are the thermal voltage noise sources associated with R_A & R_B , respectively, where R_A & $R_B \perp \{R_L; R_H\}$. U_{DCA} & U_{DCB} are the ground loop DC voltage sources, and $U(t)$ & $I(t)$ are the wire voltage and wire current, respectively.

3.1. The Generalized DC Ground Loop Situation

As a preparation, we introduce the mathematical notations that are similar but more complex than in [97]. Both the voltage $U(t)$ and current $I(t)$ in the wire have a DC and a stochastic AC (that is, noise) components (see Figure 5). The direction of the current $I(t)$ is assumed to point from Alice to Bob. Then the current in the wire can be expressed as:

$$I(t) = I_{DC} + I_n(t), \tag{19}$$

where the DC and AC components are:

$$I_{\mathrm{DC}} = \frac{U_{\mathrm{DCA}} - U_{\mathrm{DCB}}}{R_{\mathrm{A}} + R_{\mathrm{B}}} \tag{20}$$

and

$$I_{\mathrm{n}}(t) = \frac{U_{\mathrm{An}}(t) - U_{\mathrm{Bn}}(t)}{R_{\mathrm{A}} + R_{\mathrm{B}}} \tag{21}$$

Here U_{An} and U_{Bn} are the effective (rms) values of the Johnson noise voltage sources with R_{A} and R_{B} (either physical thermal noise or external generators representing enhanced effective temperature [48,53,86,91]) with $U_{\mathrm{An}} \llcorner \{U_{\mathrm{LAn}}; U_{\mathrm{HAn}}\}$ and $U_{\mathrm{Bn}} \in \{U_{\mathrm{LBn}}; U_{\mathrm{HBn}}\}$.

The voltage on the wire can be written as:

$$U(t) = I(t)R_{\mathrm{B}} + U_{\mathrm{Bn}}(t) + U_{\mathrm{DCB}}\ . \tag{22}$$

From (3) and (6) we obtain:

$$U(t)\,..U_{\mathrm{DCw}} + U_{\mathrm{ACw}}(t) = I_{\mathrm{DC}}R_{\mathrm{B}} + U_{\mathrm{DCB}} + I_{\mathrm{n}}(t)R_{\mathrm{B}} + U_{\mathrm{Bn}}(t) \tag{23}$$

Where U_{DCw} and $U_{\mathrm{ACw}}(t)$ are the DC and AC voltage components on the wire (see Figure 5):

$$U_{\mathrm{DCw}} = I_{\mathrm{DC}} R_{\mathrm{B}} + U_{\mathrm{DCB}} = \frac{R_{\mathrm{B}} U_{\mathrm{DCA}} + R_{\mathrm{A}} U_{\mathrm{DCB}}}{R_{\mathrm{A}} + R_{\mathrm{B}}} \tag{24}$$

From Equation 24, it is obvious that a non-zero information leak occurs since the DC components are different in the LH and the HL bit case. Specifically, at the LH situation, that is, when $R_{\mathrm{A}} = R_{\mathrm{L}}$ and $R_{\mathrm{B}} = R_{\mathrm{H}}$, the DC component of the wire's voltage is:

$$U_{\mathrm{DCw}} \,..U_{\mathrm{LH}} = \frac{U_{\mathrm{DCA}} R_{\mathrm{H}} + U_{\mathrm{DCB}} R_{\mathrm{L}}}{R_{\mathrm{H}} + R_{\mathrm{L}}} \tag{25}$$

while in the HL bit situation it is:

$$U_{\mathrm{DCw}} \,..U_{\mathrm{HL}} = \frac{U_{\mathrm{DCA}} R_{\mathrm{L}} + U_{\mathrm{DCB}} R_{\mathrm{H}}}{R_{\mathrm{H}} + R_{\mathrm{L}}} \tag{26}$$

For later usage, we evaluate the average of the above-defined U_{LH} and U_{HL}, and call this quantity *threshold voltage*, U_{th}:

$$U_{\mathrm{th}} \,..\frac{U_{\mathrm{LH}} + U_{\mathrm{HL}}}{2} = \frac{U_{\mathrm{DCA}} + U_{\mathrm{DCB}}}{2} \tag{27}$$

Moreover, we compare Equations (25) and (26) to obtain the following inequality:

$$U_{\mathrm{LH}} \square U_{\mathrm{HL}} \text{ if } U_{\mathrm{DCA}} \square U_{\mathrm{DCB}} \tag{28}$$

The noise component $U_{\mathrm{ACw}}(t)$ of $U(t)$ (see Figure 5) can be written as:

$$U_{\mathrm{ACw}}(t) = I_{\mathrm{n}}(t) R_{\mathrm{B}} + U_{\mathrm{Bn}}(t) \tag{29}$$

From (21) and (29):

$$U_{\mathrm{ACw}}(t) \ldots \frac{U_{\mathrm{An}}(t) - U_{\mathrm{Bn}}(t)}{R_{\mathrm{A}} + R_{\mathrm{B}}} R_{\mathrm{B}} + U_{\mathrm{Bn}}(t) = \frac{U_{\mathrm{An}}(t) R_{\mathrm{B}} + U_{\mathrm{Bn}}(t) R_{\mathrm{A}}}{R_{\mathrm{A}} + R_{\mathrm{B}}} \tag{30}$$

Obviously, $U_{\mathrm{ACw}}(t)$ has normal distribution, since it is the linear combination of Gaussian noises and DC values, and their power spectral density is the same in both the LH and HL cases [97]. Figures 6 and 7 illustrate the different situations of the wire voltage $U(t)$ versus the threshold voltage U_{th}, when $U_{\mathrm{DCA}} > U_{\mathrm{DCB}}$ and $U_{\mathrm{DCB}} > U_{\mathrm{DCA}}$. This behavior of the wire voltage is exploited in our new attack scheme to distinguish the LH and HL bit arrangements, as it will be discussed in Sections 3 and 4.

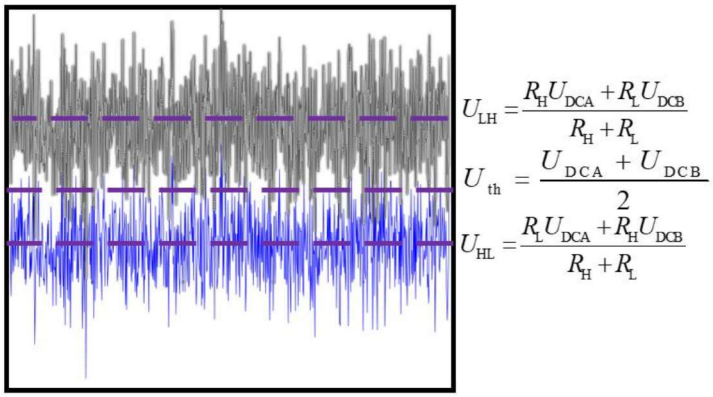

Figure 6. Eves' threshold scheme to guess the bit situation LH *vs.* HL when $U_{DCA} > U_{DCB}$, and the U_{DCA} and U_{DCB} parasitic DC voltages are assumed positive for the purpose of illustration. U_{LH} and U_{HL} are the wire's DC voltages in the LH and HL situations, respectively, and U_{th} is their mean.

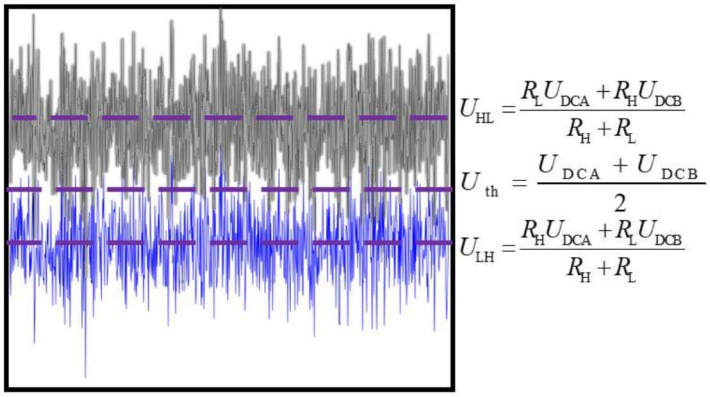

Figure 7. Eves' threshold scheme to guess the bit situation LH *vs.* HL when $U_{DCB} > U_{DCA}$, and they are assumed positive for the purpose of illustration.

3.2. Eve Estimates the Values of the Ground-Loop Voltages

The first step in our attack scheme is to compare the values of U_{DCA} and U_{DCB} . Our assumption is that Eve originally does not know the values of the parasitic voltage sources, so first we introduce a technique to measure U_{DCA} and U_{DCB} , respectively. From Equation (6), we can express U_{DCB} as:

$$U_{\mathrm{DCB}} = U(t) - I(t)R_{\mathrm{B}} - U_{\mathrm{Bn}}(t) \tag{31}$$

The above equation is useful to Eve in the LL and HH situations, where she knows the connected resistors, including R_{B} (see [97]). $U(t)$ and $I(t)$ are measurable, and even though she does not know the instantaneous signal of $U_{\mathrm{Bn}}(t)$, she can use time averaging to produce:

$$< U_{\mathrm{DCB}} >_{\tau} = < U(t) >_{\tau} - R_{\mathrm{B}} < I(t) >_{\tau} - < U_{\mathrm{Bn}}(t) >_{\tau} \tag{32}$$

Where $\langle \ \rangle_{\tau}$ represents the time average over a time period τ. If τ is long enough, the AC components will converge to zero. From (16) we get:

$$U_{\mathrm{DCB}} = \ < U(t) >_{\tau} - R_{\mathrm{B}} < I(t) >_{\tau} \tag{33}$$

For finite τ time averages, the estimation of U_{DCB} has error because the convergence to zero is incomplete. We will call this error ε_{B} . Following the same procedure for U_{DCA} :

$$U_{\mathrm{DCA}} = \ <U(t)>_{\tau} + R_{\mathrm{A}} < I(t) >_{\tau} \tag{34}$$

We call the error of this estimation ε_{A} . Knowing the resistance values in the LL and HH situations, Eve can estimate the values of U_{DCB} and U_{DCA} from (33) and (34), respectively. Equation (29) and condition $R_{\mathrm{H}} > R_{\mathrm{L}}$ imply that the noise voltage on the wire and ε_{A} and ε_{B} are higher in the HH situation than in the LL situation. Accordingly, Eve should use the LL situation to estimate U_{DCA} and U_{DCB} .

3.3. On the Attack

3.3.1. The Attack Scheme

After Eve estimates U_{DCA} and U_{DCB} , she conducts four more steps:

i) *Comparison of the DC voltages*: Eve uses the extracted U_{DCA} and U_{DCB} values to determine whether the DC voltage component in the wire is higher during the LH or the

HL bit situation (see (28)). Then Eve designs the guessing protocol discussed below.

ii) *Measurement*: During the bit exchange period (BEP), N independent samples of the wire voltage are recorded by Eve.

iii) *Evaluation*: Similarly to the procedure in [97], Eve calculates the ratio $\gamma = N^{+} / N$ where N^{+} is the number of points above U_{th} and N is the total number of samples.

iv) *Guessing* [based on (25-30)]: For $U_{\text{DCA}} > U_{\text{DCB}}$, Eve's guess is LH if $0.5 < \gamma$. Conversely, her guess is HL when $\gamma < 0.5$. For $U_{\text{DCA}} < U_{\text{DCB}}$ and $\gamma < 0.5$, her guess is LH, and it is $\text{HL}$when $0.5 < \gamma$. Regardless of the values of U_{DCA} and U_{DCB} , Eve's decision is undetermined when $\gamma = 0.5$.

Eve's probability p of correct guessing of a bit is the ratio of the number of correctly guessed bits n_{cor} to the total number of guessed bits n_{tot} , $p \,..\, n_{\text{cor}} / n_{\text{tot}}$ [97]. The $p = 0.5$ situation indicates the perfect security limit [99].

3.3.2. Can Eve Use the DC Current, Instead of the DC Voltage, in Her Scheme?

To comply with the mathematical notations used in Section 2, I_{HL} and I_{LH} denote the DC current in the wire; and $I_{\mathrm{LHn}}(t)$ and $I_{\mathrm{HLn}}(t)$ the noise (AC) components, at the HL and LH bit situations, respectively. Following the voltage-based scheme, the threshold current I_{th} is the average between I_{HL} and I_{LH}. Due to Kirchhoff's loop law, both I_{HL} and I_{LH} are equal; hence, $I_{\mathrm{LH}} \,..I_{\mathrm{HL}} = I_{\mathrm{th}}$. Also, $I_{\mathrm{LHn}}(t)$ and $I_{\mathrm{HLn}}(t)$ have the same rms values. Therefore, there is no difference in the measured values that Eve could utilize for an attack.

3.3.3. Impact of the Difference between U_{DCA} and U_{DCB} on the Attack's Success

Here we show that the efficiency of the attack depends on the difference between the parasitic DC voltages and not on their specific values. If U_{DCA} and U_{DCB} are both shifted by the same value δ then U_{LH}, U_{HL}, and U_{th} are also shifted by δ; see the illustration in Figs. 8 and 9. Thus, only the difference $U_{\mathrm{DCA}} - U_{\mathrm{DCB}}$ of these voltages determines the efficiency of the attack, not their actual values.

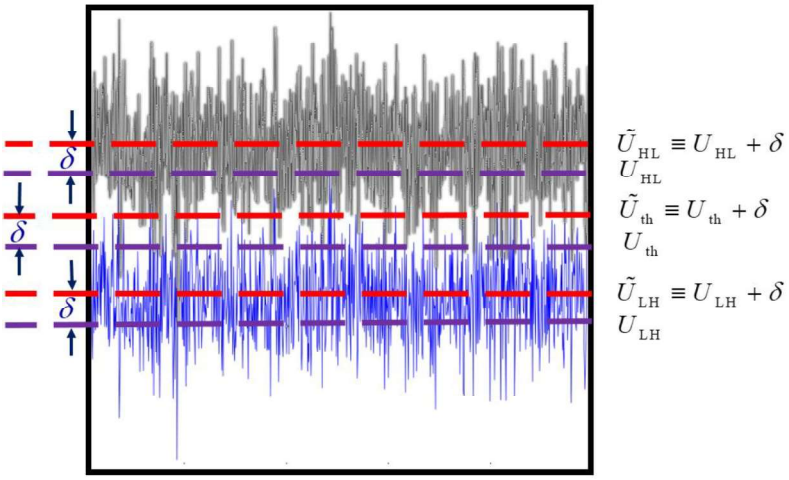

Figure 8. Illustration of the DC voltage components in the LH and HL situations before and after a δ shift in the parasitic voltages, where $\tilde{U}_{DCA} = U_{DCA} + \delta$; $\tilde{U}_{DCB} = U_{DCB} + \delta$; and $\tilde{U}_{LH}$ and $\tilde{U}_{HL}$ are the resulting DC voltages in the LH and HL situations, respectively. $\tilde{U}_{th}$ is the average of $\tilde{U}_{LH}$ and $\tilde{U}_{HL}$.

In the subsequent section, the attack method is demonstrated by computer simulations.

3.4. Demonstration

Eve's correct bit guessing probability p was evaluated analytically and tested by computer simulations (see Figure 9).

For the analytic evaluation we used the error function:

$$p\{U(t) \geq U_{th}\} = 0.5\left[1 - erf\left(\frac{U_{th} - U_{DCw}}{U_{eff}\sqrt{2}}\right)\right], \tag{35}$$

where $p\{U(t) \geq U_{\text{th}}\}$ is the probability of $U(t)$ to exceed U_{th}, and the error function is given as:

$$erf(x) = \frac{1}{\sqrt{\pi}} \int_{-x}^{x} \exp\left(-y^2\right) dy \quad . \tag{36}$$

And U_{eff} is the effective (rms) value of the noise voltage $U_{\text{ACw}}(t)$ on the wire.

In accordance to the analysis described in Section 4.3, the results were always identical when the difference $U_{\text{DCA}} - U_{\text{DCB}}$ was the fixed, regardless of the values of U_{DCA} and U_{DCB}. This fact confirms our theoretical result Section 4.3 that the success of the attack depends on the difference of parasitic DC sources only, and not on their actual values.

Computer simulations were carried out with $U_{\text{DCA}} - U_{\text{DCB}}$ = 0.1V and 0.2V. During these tests, R_{L} and R_{H} were fixed to 1 and $10\ \text{k}\Omega$, respectively. The length of the key was 700 bits. The duration of each BEP was 500 samples (time steps).

The results verify the effectiveness of the attack protocol shown in this paper.

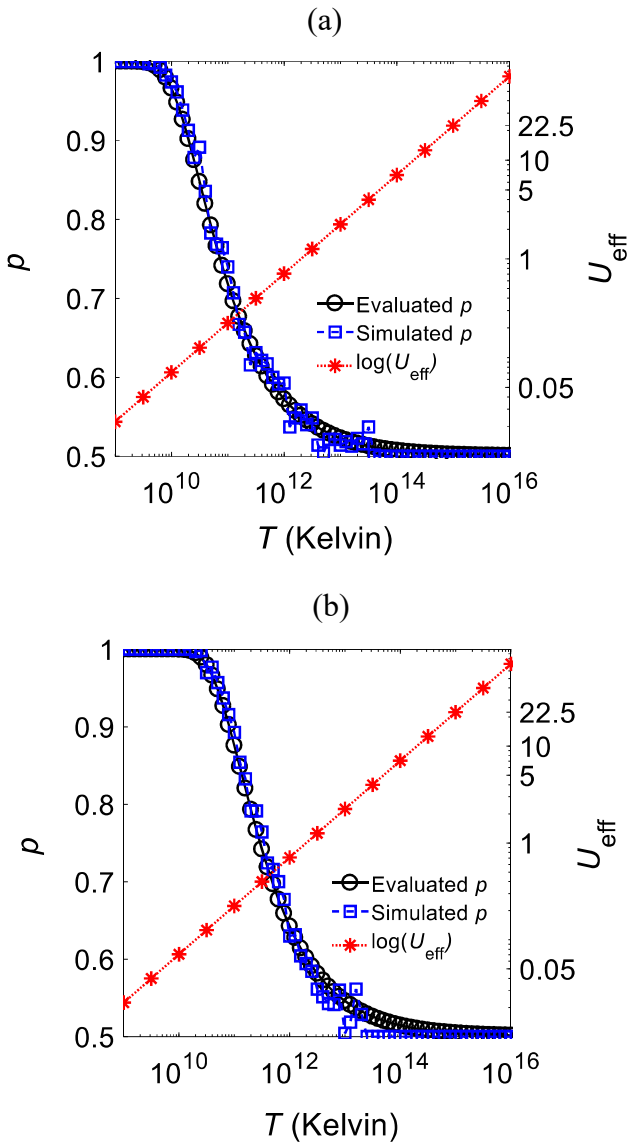

Figure 9. Eve's correct bit guessing probability (p) versus temperatures at differences of a) 0.1V and b) 0.2V, at various effective noise temperatures, with bandwidth (Δf) of 1MHz. At the computer simulations the key length was 700 bits with 500 independent time samples/bit. The asymptote, $p = 0.5$, represents perfect security. The evaluation was carried out by the error function (see Equations (35) and (36)).

3.5. Defense Methods

The attack can be countered using the same defense techniques as described in the previous section, namely, cancelling the DC voltages or by increasing the effective (rms) value of noises by increasing the noise temperature and/or the bandwidth (without exceeding the wave limit [48,91,95]). All methods are the same as those discussed in [97], except for the DC voltages cancellation techniques in which the defense can be conducted in two other ways:

i) Adding variable DC-voltage sources at each side and tuning them to compensate out the parasitic sources, or alternatively tuning them to reach $U_{\mathrm{DCB}} - U_{\mathrm{DCA}} = 0$.

ii) Naturally, a simplified version would work as well: Adding a single variable DC voltage at one side and tuning it to reach $U_{\mathrm{DCB}} - U_{\mathrm{DCA}} = 0$ yielding zero DC loop current.

iii) Attaching a capacitor in series to the cable from Alice's end, Bob's end, or from both ends to eliminate DC current in the wire. Note, this maneuver requires great precautions because of its impact on line impedance and the potential information leak.

4. MAN IN THE MIDDLE AND CURRENT INJECTION ATTACKS AGAINST THE KLJN KEY EXCHANGER COMPROMISED BY DC SOURCES*

The study in this section is also included in the paper "Man in the Middle and Current Injection Attacks against the KLJN Key Exchanger Compromised by DC Sources" [100]. The paper was accepted for publication in the journal *Fluctuation and Noise Letters*.

4.1. Introduction

In this section, we study a new situation that is combined of former attack features, which are MITM [90] and the current injection attacks [48,89] operating in the presence of parasitic voltage sources (such as ground loop) [97-99] in the wire channel. The question here is whether that the two former compromising factors synergistically help Eve to crack the system? We will see that the opposite is true in the MITM attack: The combined factors make it more difficult for Eve to keep her operation covert.

*Reprinted with permission from " Man in the Middle and Current Injection Attacks against the KLJN Key Exchanger Compromised by DC Sources," by Mutaz Melhem, and Laszlo Kish, which is accepted for publication in *Fluctuations and Noise Letters* (2020).

4.2. Man-in-the-Middle (MITM) Attacks at Parasitic DC Sources

In [90], three different versions of the MITM attack were proposed:

(i) By inserting KLJN circuitries identical to Alice's and Bob's, (see Fig. 10). The defense against this attack was the communication of measured instantaneous current values by Alice and Bob via an authenticated public channel. The noise currents at Alice and Bob become independent during the attack thus the eavesdropping is discovered instantaneously with very high probability [90].

(ii) By inserting twin noise current generators, (see Fig. 12);

(iii) By inserting twin noise voltage generators, (see Fig. 12).

Below we prove that the KLJN system compromised by parasitic DC sources [97-99] is not only secure against these attacks, but, in their original form, some of these attacks help Alice and Bob to discover Eve in much simpler ways than that was proposed earlier [90].

4.2.1. MITM Attack by Inserted KLJN Circuitries

It is obvious from the analysis of the circuitry in Fig.10 that whenever the parasitic DC sources of U_{DCA} and U_{DCB} are sufficiently different, Alice and Bob can use changes in the DC current to discover Eve. Then the DC situation will also change during the attack, and if the difference is greater than the rms value of the AC component of the wire voltage, Alice and Bob can successfully use simple time average to distinguish between the attack and no-attack situations. The original loop is broken in two separate loops thus the resultant DC loop voltage will be different in both new loops leading to different DC currents. Thus Alice and Bob can discover the attack even without comparing their instantaneous currents. The DC current they measure will change due to the attack thus *they can discover Eve without even communicating with the other party*. Hence, Alice and Bob need only to do a simple time averaging to uncover the attack.

Fig. 11 shows an *improved* MITM attack with inserted KLJN circuitries. By adding the proper DC voltage generators matching the situations at Alice's and Bob's ends, Eve's imitation of Alice and Bob is improved and Eve can stay hidden with the same probability as at the original MITM attack situation [90] because the DC current components at the two ends will remain the same. The defense against this attack is identical to the original protocol [90]. Thus, it requires the measurement and communication of measured instantaneous current values by Alice and Bob via an authenticated public channel. The noise (that is the AC) currents at Alice and Bob are statistically independent during the

attack. Thus, the eavesdropping is discovered instantaneously with very high probability. Mathematically speaking, the probability that Eve can stay hidden decays exponentially with time, and it is in the order of 10^{-20} over the bit exchange period at practical conditions [90].

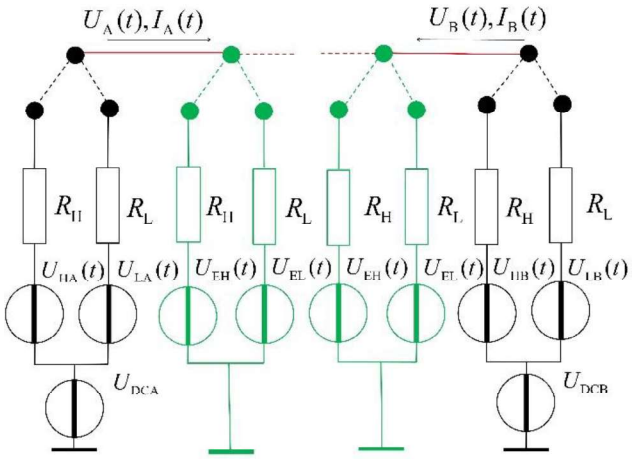

Figure 10. Using the original [90] MITM attack. Eve cuts the wire and attaches two communicators to the KLJN system; one faces Alice's end and the other faces Bob's end. Thus two independent KLJN loops are created. Both communicators are identical with the communicators of Alice and Bob (except for the parasitic voltages). Even though Eve's noise voltage generators $U_{EHn}(t)$ and $U_{ELn}(t)$ have identical spectrum as the noise generators of Alice and Bob, their time functions are statistically independent. $I_A(t)$ and $U_A(t)$ are the instantaneous current and voltage at Alice's end, while $I_B(t)$ and $U_B(t)$ are the instantaneous current and voltage at Bob's end. By comparing the instantaneous values, Alice and Bob can discover the attack quickly [90]. However, they can do that even without measuring the instantaneous currents: The DC current in their own loop will change due to the attack. They can then discover Eve without communicating with the other party and doing time averaging instead. For an improved attack, (see Fig. 11)

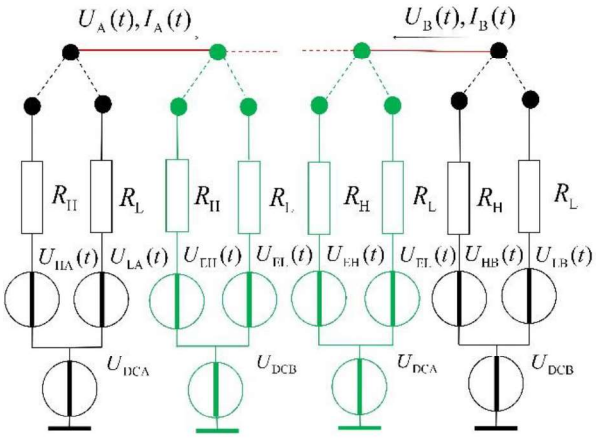

Figure 11. Improved MITM attack with inserted KLJN circuitries. By adding the proper DC voltage generators Eve's imitation of Alice and Bob is improved and Eve can stay hidden with the same probability as in the original MITM attack.

4.2.2. MITM Attack by Inserting Twin Noise Current Generators

The man-in-the-middle attack with twin noise current generators, (see Fig. 12), is the same as in the original MITM situation [90]. Even though Eve's injected currents are identical with $I_E(t)$ amplitude, due to Ohm's law, the instantaneous voltages $U_A(t)$ and $U_B(t)$ will be different most of the time because of the independence of the noise voltage generators of Alice and Bob, similar to the original situation [90]. Thus, Alice and Bob can quickly discover Eve by comparing their instantaneous voltage measurement data.

However, similar to the scheme described in Section 2.1, whenever the parasitic DC sources of U_{DCA} and U_{DCB} are sufficiently different, the DC voltage situation in the wire will also change during the attack, and if the difference is greater than the rms value of the AC component of the wire voltage, Alice and Bob can successfully use simple time

average over the bit exchange period to distinguish between the attack and no-attack situations. Here, Eve's solution (shown in Fig. 11) to fix this problem does not work because adding a voltage generator in serial to the current generators will obviously not change the voltage and current values in the loop. Thus the existence of the ground loop ultimately makes Eve's situation worse.

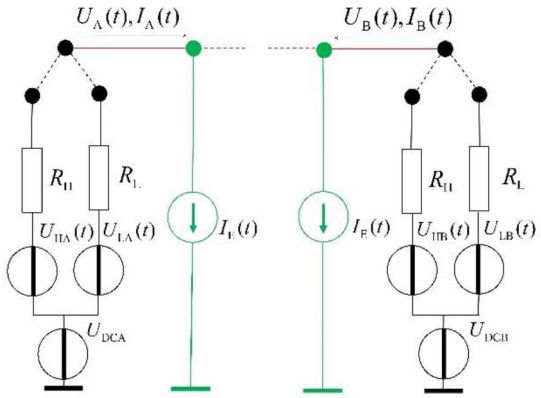

Figure 12. The man-in-the-middle attack with twin noise current generators $I_E(t)$ of identical amplitudes [90]. Alice and Bub can compare the instantaneous voltage values via an authenticated public channel or, whenever the parasitic DC voltages are sufficiently different, utilize simple time averaging to uncover the attack.

4.2.3. MITM Attack by Inserting Twin Noise Voltage Generators

The man-in-the-middle attack with twin noise voltage generators, (see Fig. 13), is the same as in the original MITM situation [90]. Even though Eve's injected currents are identical with $U_E(t)$ amplitude, due to Ohm's law, the instantaneous currents $I_A(t)$ and $I_B(t)$ will be different at most of the time due to the independence of the noise voltage generators of

Alice and Bob, similarly to the original situation [90]. Thus Alice and Bob can quickly discover Eve by comparing their instantaneous voltage measurement data [90].

However, similar to the scheme described in Section 2.1, whenever the parasitic DC sources of U_{DCA} and U_{DCB} are sufficiently different, the DC current situation in the wire will also change during the attack and, if the difference is greater than the rms value of the AC component of the wire current, Alice and Bob can successfully use simple time average of the current over the bit exchange period to distinguish between the attack and no-attack situations.

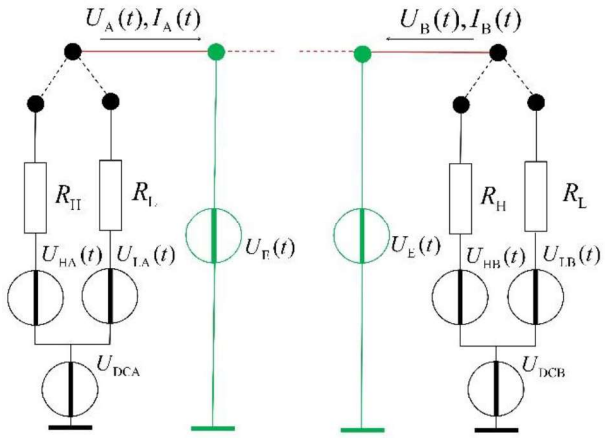

Figure 13. The man-in-the-middle attack with twin noise voltage generators $U_{\mathrm{E}}(t)$ of identical amplitudes. For other definitions, see the captions of Fig. 1 and Fig. 10. Alice and Bob can discover the attack even without comparing their instantaneous currents. The DC current in their loop will change due to the attack. Thus, they can discover Eve without communicating with the other party. For an improved attack, (see Fig. 14).

Fig. 14 shows a somewhat improved attack where Eve is attempting to compensate the DC voltage differences at the two ends by forcing a proper DC voltage component on the wire. However, she can do this deterministically only during emulating the HH or LL situation when the DC voltage on the wire is the average of the parasitic DC voltage components of the two ends. At these situations the bits are discarded. Thus, Eve does not gain any advantage.

In the secure (LH and HL) cases, Eve has only 0.5 success probability to eliminate the DC problem. For example, toward Bob, she can fix the DC voltage to imitate the DC voltage drop at the LH situation and wait until Bob randomly chooses the H resistor. The problem with this approach is that, if Bob chooses L instead, he will detect that the DC voltage is the wrong value. Thus, this attack improvement is strongly limited as works only in half of the cases. Thus, Alice and Bob can discover the attack, on the average, in two secure bit exchange periods even without public communications.

On the other hand, the original defense method [90], that is the public comparison of the instantaneous voltage measurement data of Alice and Bob, always uncovers Eve with very high probability in a very short time. Her probability to be able to stay hidden decays exponentially and reaches miniscule values [90] as mentioned above in Section 2.1.

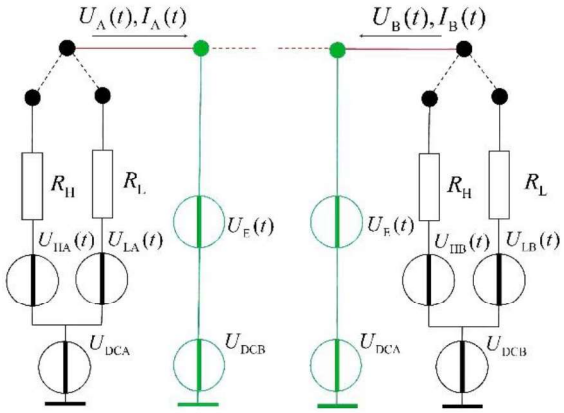

Figure 14. Improved twin voltage generator attack. By adding the proper DC voltage generators, Eve's imitation of Alice and Bob is improved, and Eve can stay hidden with the same probability as in the original situation.

4.3. Current Injection Attack at Parasitic DC Sources

During the current injection attack [48,89,93] (See Fig. 15), Eve injects a small noise current in the line and measures the cross-correlation of this current with the current in the wire. Due to Kirchhoff's node law, the cross-correlation is greater at that side of the attack point where the resistance is lower because the injected current is distributed according to the conductance of the terminations of the wire. The efficient defense against this attack is the comparison of instantaneous current amplitudes by Alice and Bob, which were formerly proposed [48], analyzed [12,93], and tested [56]. The goal of our current study is to clarify the following questions:

(a) Does Eve has any advantage or disadvantage from the parasitic DC sources and the related loop current?

(b) Does the former defense protocol [48,89,93] still work?

The answers to the above questions are straightforward:

(i) The parasitic DC current is a DC current component. Thus, it is statistically independent from the AC current components (including Eve's ones) in the wire. Thus the parasitic DC currents have zero contribution to Eve's cross-correlation measurement. Moreover, by using a current generator, Eve can conduct the same attack, without any advantage or disadvantage, as earlier.

(ii) If Alice and Bob compare the instantaneous current amplitudes of the AC components of their measurement, the detection situation (and resolution) also remains the same as earlier.

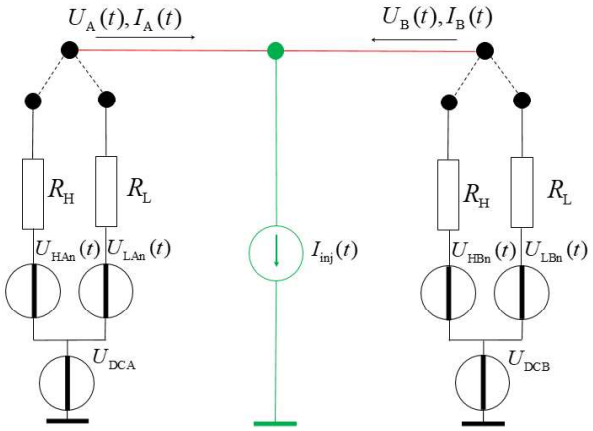

Figure 15. The current injection attack against the KLJN scheme, where $I_{inj}(t)$ is the injected current. For other definitions, see the captions of Fig.1 and Fig. 10. The existence of DC sources does not influence the distribution of injected AC currents. Thus, the setup level remains the same as without them. Alice and Bob discover the attack by comparing their instantaneous AC current amplitude.

In conclusion, the parasitic DC sources do not influence the current injection attack and its defense

5. AC LOOP CURRENT ATTACKS AGAINST THE KLJN SECURE KEY EXCHANGE SCHEME*

The study in this section is also included in the paper "AC Loop Current Attacks against the KLJN Secure Key Exchange Scheme" [101]. The paper was submitted for publication in the *Computers and Electrical Engineering* (Elsevier).

5.1. Introduction

As a significant enhancement of DC loop voltage and current attacks, in this section, we explore the situation of periodic AC voltage sources in the loop. This situation is very common at long-range secure communications. Thus, it must be taken very seriously. We show that the new attack requires different procedures in the high and low frequency limits.

*This section is a modified version of the paper, "AC Loop Current Attacks against the KLJN Secure Key Exchange Scheme," by Mutaz Melhem, Christiana Chemon, Shahriar Ferdous, and Laszlo Kish, which was submitted to *Fluctuation and Noise letters* (2020).

5.2. The AC Ground Loop Current Situation

In the next sections, the security of the KLJN is studied when a single periodic AC source $U_{\mathrm{AAC}}(t)$ is located at one of the communicating parties, see Figure 2, where $U_{\mathrm{AAC}}(t)$ is a periodic AC time function. Such situations exist due to AC ground loop and/or electromagnetic interference (EMI) from motors, power supplies, wireless networks, etc. For the sake of simplicity, we assume that the AC source is present only at Alice's terminal.

The voltage on the wire (see Figure 16) can be given as:

$$U(t) \equiv U_{\mathrm{AC}}(t) + U_{\mathrm{n}}(t) = \frac{R_{\mathrm{B}} U_{\mathrm{AAC}}(t)}{R_{\mathrm{A}} + R_{\mathrm{B}}} + \frac{R_{\mathrm{A}} U_{\mathrm{Bn}}(t) + R_{\mathrm{B}} U_{\mathrm{An}}(t)}{R_{\mathrm{A}} + R_{\mathrm{B}}} \tag{37}$$

where $U_{\mathrm{An}} \in \{U_{\mathrm{LAn}}; U_{\mathrm{HAn}}\}$ and $U_{\mathrm{Bn}} \in \{U_{\mathrm{LBn}}; U_{\mathrm{HBn}}\}$ are the standard voltage noise sources of the chosen resistors, R_{A} and R_{B}, and $U_{\mathrm{AC}}(t)$ and $U_{\mathrm{n}}(t)$ are the periodic (parasitic) and the fundamental noise (stochastic) voltage components on the wire, respectively.

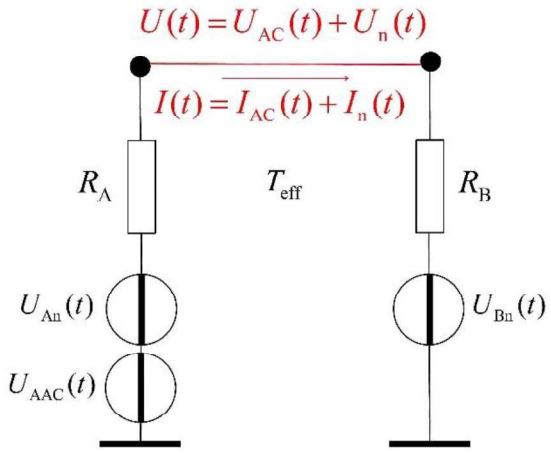

Figure 16. The KLJN system compromised by a single periodic AC source at Alice's side. $U(t)$ and $I(t)$ are the voltage and current on/in the wire, respectively. $U_{AAC}(t)$ is the AC ground loop voltage source. $R_A \,\&\, R_B \in \{R_L; R_H\}$ are the randomly chosen resistances by Alice and Bob, respectively. $U_{An} \in \{U_{LAn}; U_{HAn}\}$ and $U_{Bn} \in \{U_{LBn}; U_{HBn}\}$ are the voltage noise sources affiliated with $R_A \,\&\, R_B$, respectively. $U_{AC}(t)$ is the periodic voltage component on the wire and $I_{AC}(t)$ is the periodic current component in the wire. $U_n(t)$ and $I_n(t)$ are the fundamental noise voltage and current components in the wire, respectively.

The periodic component can be written as (see Figure 16):

$$U_{AC}(t) = \frac{R_B U_{AAC}(t)}{R_A + R_B} \quad , \tag{38}$$

See Figure 17.

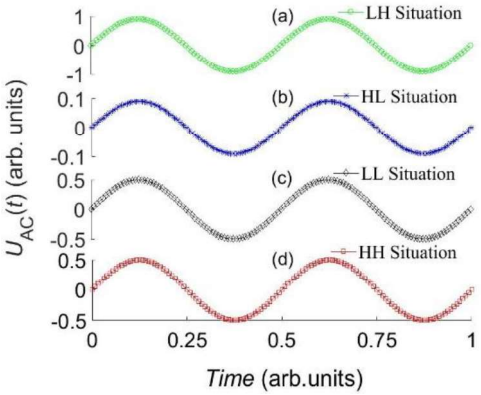

Figure 17. Illustration of the AC component of the voltage on the wire $U_{\mathrm{AC}}(t)$ in the (a) LH situation (b) HL situation (c) LL situation and (d) HH situation when $R_{\mathrm{L}} = 1\ \mathrm{k\Omega}$ and $R_{\mathrm{H}} = 10\ \mathrm{k\Omega}$ (see Equation 40).

The noise component of the voltage on the wire, as given earlier [51,91,98]:

$$U_{\mathrm{n}}(t) = \frac{R_{\mathrm{A}} U_{\mathrm{Bn}}(t) + R_{\mathrm{B}} U_{\mathrm{An}}(t)}{R_{\mathrm{A}} + R_{\mathrm{B}}} \tag{39}$$

In the next section, we introduce the new attack schemes.

5.3. The AC Loop Current Attacks

The attack protocol depends on the f_A / f_C ratio where f_A is the frequency of the periodic source and f_C is the frequency of the bit exchange. Below, we describe two protocols for different frequency limits.

5.3.1. Attack in the Low-Frequency Limit

If the frequency of the periodic source f_A is less than the bit exchange (clock) frequency f_C, Eve can attack the secure bit exchange if she knows the time function $U_{AAC}(t)$ of the periodic source. The attack has the same basic steps as the DC attack procedure described in [97,98]:

(*i*) *Measurement*: Eve measures and records *N* independent samples of the voltage *U*(*t*) on the wire during the bit exchange period, where the sampling rate is determined by the Nyquist sampling theorem and it is double the noise bandwidth.

(*ii*) *Evaluation*: Eve calculates a quantity γ_i defined as:

$$\gamma_i = \frac{N_i^+}{N}, \tag{40}$$

where N_i^+ is the number of samples that are above a *threshold* voltage $U_{\text{th},i}$ which is fixed during the *i*-th bit exchange period. The new aspect of the low-frequency AC attacks, compared to the DC attacks [97,98], is that,here, the threshold $U_{\text{th},i}$ varies between bit exchange periods. The actual threshold $U_{\text{th},i}$ is the time average of the periodic component over the *i*-th bit exchange period:

$$U_{\text{th},i} = \frac{1}{\tau} \int_{t_{\text{i-1}}}^{t_{\text{i}}} U_{\text{AAC}}(t)\, dt \quad , \tag{41}$$

where t_{i} is the end of the *i*-th bit exchange period, and $\tau = t_i - t_{i\text{-}1}$ is the duration of the bit exchange periods. Note, in this new situation, the threshold is not always positive.

(*iii*) *Guessing*:

Eve's guess of the secure resistor situation is:

- LH when $\{U_{\text{th},i} > 0 \text{ and } \gamma_i > 0.5\}$; or $\{U_{\text{th},i} < 0 \text{ and } \gamma_i < 0.5\}$, (42)
- HL when $\{U_{\text{th},i} > 0 \text{ and } \gamma_i < 0.5\}$; or $\{U_{\text{th},i} < 0 \text{ and } \gamma_i > 0.5\}$. (43)

Furthermore:

If $U_{\text{th},i} = 0$, the bit will be discarded (as undetermined). (44)

For $\gamma_i = 0.5$, the bit will be discarded (as undetermined). (45)

5.3.2. Attack in the High-Frequency Limit

In the high frequency limit, the previous attack procedure does not work. Our proposed attack is executed in the spectral domain. We assume Eve knows the frequency of the periodic source.

The attack protocol in the high frequency limit consists of three phases:

(i) Preparation phase: As preparation for the attack, Eve is running computer simulations of the KLJN system. She can do that because in accordance with the Kerckhoffs's principle [8,91] of unconditional security Eve supposedly knows all the details of protocol and hardware except the actual secure key.

(a) From the computer simulations she obtains the simulated voltages on the wire, specifically, the total voltage $U_{\text{s}}(t)$, its noise component $U_{\text{ns}}(t)$ and its AC component $U_{\text{ACs}}(t)$. Then, from these time functions she calculates the squared absolute values of their Fourier transforms over each bit exchange periods: $|U_{\text{s}}(f)|^2$ $|N_{\text{s}}(f)|^2$ and $|AC_{\text{s}}(f)|^2$,

respectively, the simulated signals are shown in Figure 18. From these spectra, she calculates:

(b) The "simulated noise-background", $\left\langle |N_s(f)|^2 \right\rangle_M$, which is the ensemble average of simulated $|N_s(f)|^2$ spectra over a large number, M, of LH and HL bit exchange periods. (Note, in accordance with the KLJN protocol (see Section 1.1) using only LH or only HL periods would result in the same values provided the KLJN system is ideal).

(c) The "AC threshold ", $\left\langle |AC_{th}(f)|^2 \right\rangle_W$, that is defined as:

$$\left\langle |AC_{th}(f)|^2 \right\rangle_W = \frac{\left\langle |AC_{s,LH}(f)|^2 \right\rangle_W + \left\langle |AC_{s,HL}(f)|^2 \right\rangle_W}{2} \qquad (46)$$

where $\left\langle |AC_{s,LH}(f)|^2 \right\rangle_W$ and $\left\langle |AC_{s,HL}(f)|^2 \right\rangle_W$ are spectral averages over the frequency: they are the average of the $|AC_s(f)|^2$ function over the noise bandwidth W, in the LH and HL situations, respectively. Note, the LH and HL cases are different for the AC component due to the voltage division factor of the different resistance values (R_L vs R_H) at the two parties.

(ii) Measurement phase: At the i-th bit exchange period, Eve measures the voltage U_i(t) on the wire and determines the actual $|U_i(f)|^2$. Then, she subtracts the simulated noise

background $\left\langle |N_s(f)|^2 \right\rangle_M$ from $|U_i(f)|^2$ to estimate the actual $|AC_i(f)|^2$, and computes its spectral average :

$$\left\langle |AC_i(f)|^2 \right\rangle_W = \left\langle |U_i(f)|^2 - \left\langle |N_s(f)|^2 \right\rangle_M \right\rangle_W , \quad (47)$$

which is scaling with the mean-square of the AC voltage component on the wire during the i-th bit exchange period.

(iii) Guessing phase: Eve compares $\left\langle |AC_i(f)|^2 \right\rangle_W$ with the AC threshold $\left\langle |AC_{th}(f)|^2 \right\rangle_W$. Based on this comparison, she guesses the actual secure resistor situation as:

-LH when $\left\langle |AC_i(f)|^2 \right\rangle_W > |AC_{th}(f)|^2$ (48)

-HL when $\left\langle |AC(f)|^2 \right\rangle_W < |AC_{th}(f)|^2$. (49)

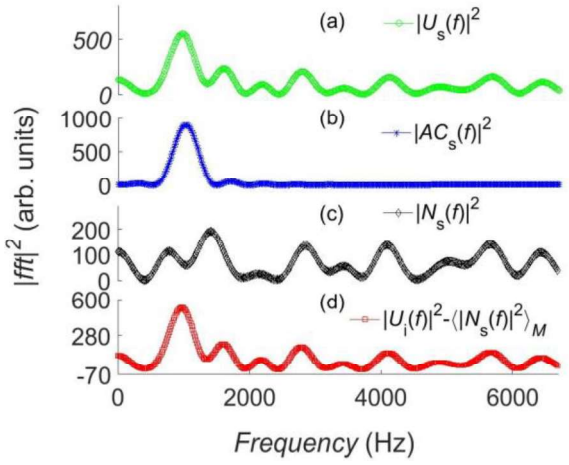

Figure 18. The square absolute value of the Fourier transform of simulated voltage components: (a) that of the voltage on the wire: $|U_s(f)|^2$; (b) that of the AC component: $|AC_s(f)|^2$; (c) that of the noise voltage component $|N_s(f)|^2$; (d) that of the estimated AC component $|U_i(f)|^2 - \left\langle |N_s(f)|^2 \right\rangle_M$. The simulation was conducted with sinusoidal periodic source of frequency f_A=1kHz, and the clock (bit exchange) frequency f_C=500 Hz. The noise bandwidth f_B=100kHz, the effective noise temperature is $9\text{x}10^{15}$ K, while R_L and R_H are 1 kΩ and 10 kΩ, respectively.

5.4. Demonstration of the Attacks

To evaluate the success of the attacks, we ran simulations in both the low and high frequency limits. The probability *p* of Eve's correct bit value guessing [8,91] is:

$$p = \lim_{n_{tot}\to\infty} \frac{n_{cor}}{n_{tot}} \tag{50}$$

where n_{cor} is the number of the successfully guesses, and n_{tot} is the total number of guesses. When $p = 0.5$, the key exchange scheme is perfectly secure [3-4,8,91].

During the simulations, R_L, R_H, f_C, and f_B were 1 $k\Omega$, 10 $k\Omega$, 1 kHz and 100 kHz, respectively. The length of the key was 1000 bits. We chose $U_{AAC}(t) = \cos(2\pi f_A t)$ [Volt] where the frequency f_A of the periodic component was varied.

The noise generation is described below.

5.4.1. Generating the Johnson Noise

MATLAB was used to generate the Gaussian Band-Limited White Noise (GBWN). Significant efforts were made to improve Gaussianity, reduce bias, and avoid any aliasing error which are typical weaknesses in computer simulations. At first, using the MATLAB randn() function, 2^{24} or 16,777,216 Gaussian random numbers were generated. Next the noise was converted from the time domain to the frequency domain using the MATLAB FFT function, and, to get rid of any aliasing error, we increased the sampled bandwidth by zero padding. The real component of the inverse FFT resulted in a GBWN noise with Nyquist sampling rate and reduced aliasing errors. The final step was to scale the noise amplitude to the physical effective value by the Johnson formula (see Equation 37) at known resistance, temperature and bandwidth.

More details about the noise generator will be available in [102].

5.4.2. Demonstration of the Attack in the Low-Frequency Limit

Tests utilizing Equations 42-47 and computer simulations were conducted at different periodic frequencies in the low-frequency limit, 1 kHz = $f_C >> f_A$ =318.3, 101.32 and 32.25 Hz, with $U_{AAC}(t) = \cos(2\pi f_A t)$ [Volt], see Figure 4. By varying the noise temperature T_{eff} (see Equation 37) the effective noise voltage U_{eff} on the wire (see Equation 37) ranged from 0.01 to 100 V_{rms}. Figure 4 shows the probability p of correct guessing of the bit versus the effective value U_{eff} the KLJN noise voltage on the wire. Similarly to the DC loop current attacks in [97,98], at low U_{eff} values compared to the amplitude of the periodic component, the system is highly vulnerable (p=1) while at high U_{eff} values the system is perfectly secure (p=0.5). See Figure 19.

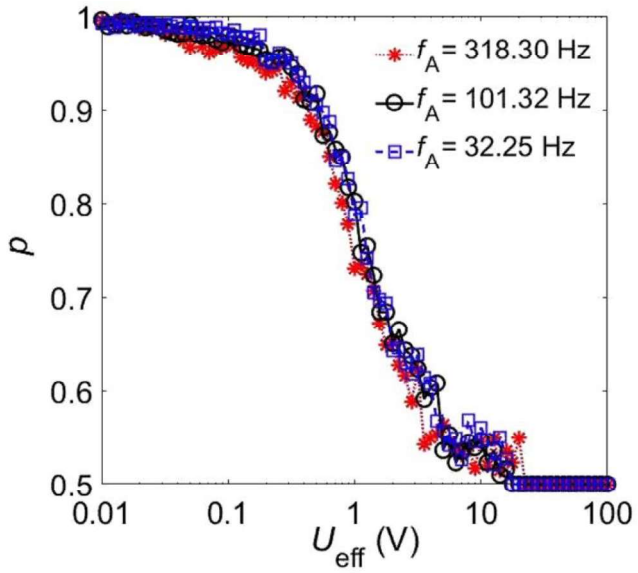

Figure 19. The correct guessing probability p vs the effective noise voltage U_{eff} on the wire. The noise bandwidth f_B is 100 kHz, the clock (bit exchange) frequency f_C is 1 kHz, the key length is 1000, and the frequency of the sinusoidal source f_A is 318.30, 101.32 and 32.25 Hz and its amplitude is $U_{AAC}(t) = \cos(2\pi f_A t)$ [Volt].

5.4.3. Demonstration of the Attack in the High-Frequency Limit

For the given periodic AC signal, the Fourier transform was obtained using fast the Fourier transform (FFT) protocol. The tests were conducted under the same conditions as in Section 4.2, except the periodic frequency f_A was set to 2, 16, and 32 kHz, and the bit exchange (clock) frequency f_C was set to 500Hz. Figure 5 shows Eve's correct-guessing probability p with respect to the KLJN noise voltage U_{eff} on the wire (controlled by the varying noise temperature T_{eff}, see Equation 37) . Similarly to the DC loop current attacks in [97, 98], at low U_{eff} values compared to the amplitude of the periodic component, the system is highly vulnerable (p=1) while at high U_{eff} values the system is perfectly secure

(p=0.5). The change from vulnerability to security takes place at a higher U_{eff} values for higher f_{A} frequencies. See Figure 20.

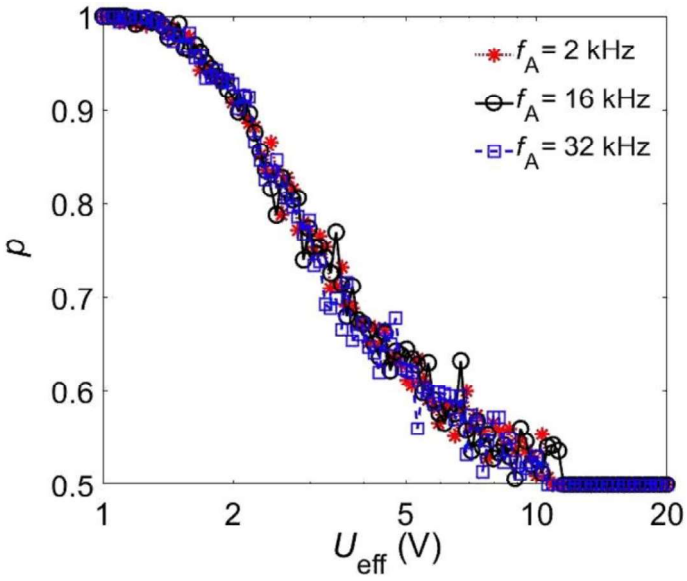

Figure 20. The probability p of correct guessing vs the effective noise voltage U_{eff} on the wire. The noise bandwidth f_{B} is 100 kHz, the clock frequency f_{C} is 500 Hz, the key length is 1000, and the frequency of the periodic sinusoidal source f_{A} is 2, 16, and 32 kHz.

5.5. Defense against the Attacks

The attack can be defended using the similar defense techniques mentioned in [97, 98]:

i) Elimination of the parasitic sources.

ii) Filtering out the parasitic component.

iii) Increasing the effective voltage of the noise on the wire (that is increasing the noise temperature T_{eff}) to approach the limit of perfect security.

iv) Various privacy amplification protocols on the exchanged secure bits [8,53,58,84,89,91,93].

6. CONCLUSION*

The KLJN secure key exchange scheme is a statistical physical system that offers unconditional (information-theoretic) security. For a detailed survey and its history, see a more detailed explanation in [91].

---

* Part of this section is reprinted with permission from "A Static-loop-current Attack Against the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System." by Mutaz Melhem, and Laszlo B. Kish (2019). *Applied Sciences* 9.4: 666, © [2019] by Melhem and Kish.
* Part of this section is a modified version of the paper "A Generalized DC Loop-Current Attack Against the (KLJN) Secure Key Exchange System." by Mutaz Melhem, and Laszlo Kish, (2020). *Metrolo. Meas. Syst* 26.4: 617, © [2019] by Melhem and Kish.
* Part of this section is a modified version of the paper "Man in the middle and current injection attacks against the KLJN key exchanger compromised by DC sources." by Mutaz Melhem., and Laszlo Kish, (2020). *arxiv*, © [2020] by Melhem and Kish.
* Part of this section is a modified version of the paper "AC Loop Current Attacks The KLJN Secure Key Exchange Scheme." by Mutaz Melhem, Christiana Chamon, Shahriar Ferdous, and Laszlo Kish, (2020). *arxiv*, © [2020] by Melhem, Chamon, Ferdous, and Kish.

In Section 2, a novel attack against the KLJN protocol was introduced using a frequently occurring parasitic feature, namely the imbalance of voltages between the ground points at the two ends. We showed that, in the DC limit, such parasite voltages and currents could cause information leaks. The present study is directly relevant for DC current-based ground loops (for example, during secure communication between different units in instruments [67,68]). The attack was demonstrated via computer simulation and proper defense protocols were shown to eliminate the information leak. Our DC-limited study is only a first step in addressing a more general situation that is investigated in section 3.

Section 3 generalizes the DC loop current attack introduced in Section 2. The generalized scheme makes Eve's work easier. We provided a mathematical analysis and verified the attacks analytically and by computer simulations. We also proposed effective defense techniques.

In conclusion, in practical KLJN key exchangers, Alice and Bob must carry out DC loop current tests before and during operation and act accordingly (see Section 3.6).

It is important to note that the general, more expensive defense method of KLJN, which is based on in-situ system simulation and comparison with measurements (see Section 4.1 in [89]), works efficiently because such a defense technique alerts for any deviation from the idealized situation, including parasitic DC voltages and currents.

In section 4, we proved that a practical KLJN system that is possibly compromised by parasitic serial DC sources remains secure against the MITM attacks and the current injection attack. In each case, Eve's probability of success to stay hidden is less or equal to the idealistic situation with no parasitic sources [90]. Thus launching these attacks against the KLJN scheme remains non-feasible.

Section 5 introduced a novel attack against the KLJN secure key exchange. The attack addressed the situation when there is a single parasitic AC source at side of Alice. Such situation could exist due to AC ground loops, and electromagnetic interference (EMI) from power motors, power supplies, wireless networks; etc.

At low-frequency disturbance, the attack follows a generalized procedure of the earlier DC attack in [98].

At high-frequency disturbance, the attack is based on frequency analysis, separating the periodic component and the utilizing the same threshold crossing statistics as in [97,98].

The vulnerability of the KLJN scheme against these attacks was successfully demonstrated by computer simulations. An important implication is that, when the KLJN system is working in the "stealth" mode, where the natural thermal noise voltages of the resistors are used and the periodic component cannot be over-powered by artificial noise generators at the resistors, a strong effort must be made to eliminate any periodic component from the loop otherwise significant information leak can be present during these attacks.

Finally, we listed available defense methods against these attacks. A practical KLJN secure key exchanger must also be armed against these new types of attacks, too.

REFERENCES

[1] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory. 1976;22(6):644-54.

[2] Delfs H, Knebl H, Knebl H. Introduction to cryptography: Springer; 2002.

[3] Pieprzyk J, Hardjono T, Seberry J. Fundamentals of computer security: Springer Science & Business Media; 2013.

[4] Shannon CE. Communication theory of secrecy systems. Bell System Technical Journal. 1949;28(4):656-715.

[5] Wiesner S. Conjugate coding. ACM Sigact News. 1983;15(1):78-88.

[6] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. arXiv preprint arXiv:200306557. 2020.

[7] Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature. 1982;299(5886):802-3.

[8] Yuen HP. Security of quantum key distribution. IEEE Access. 2016;4:724-49.

[9] Sajeed S, Huang A, Sun S, Xu F, Makarov V, Curty M. Insecurity of detector-device-independent quantum key distribution. Physical Review Letters. 2016;117(25):250505.

[10] Yuen HP, editor Essential elements lacking in security proofs for quantum key distribution. Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X; 2013: International Society for Optics and Photonics.

[11] Yuen HP. Essential lack of security proof in quantum key distribution. arXiv preprint arXiv:13100842. 2013.

[12] Hirota O. Incompleteness and limit of quantum key distribution theory. arXiv preprint arXiv:12082106. 2012.

[13] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C, Leuchs G. Trojan-horse attacks threaten the security of practical quantum cryptography. New Journal of Physics. 2014;16(12):123030.

[14] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C, Makarov V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Communications. 2011;2(1):1-6.

[15] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics. 2010;4(10):686.

[16] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Scarani V, Makarov V, et al. Experimentally faking the violation of Bell's inequalities. Physical Review Letters. 2011;107(17):170404.

[17] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. arXiv preprint quant-ph/0702262. 2007.

[18] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, et al. After-gate attack on a quantum cryptosystem. New Journal of Physics. 2011;13(1):013043.

[19] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Thermal blinding of gated detectors in quantum cryptography. Optics Express. 2010;18(26):27938-54.

[20] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, et al. Device calibration impacts security of quantum key distribution. Physical Review Letters. 2011;107(11):110501.

[21] Lydersen L, Skaar J, Makarov V. Tailored bright illumination attack on distributed-phase-reference protocols. Journal of Modern Optics. 2011;58(8):680-5.

[22] Lydersen L, Akhlaghi MK, Majedi AH, Skaar J, Makarov V. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. New Journal of Physics. 2011;13(11):113042.

[23] Yuan Z, Dynes J, Shields A. Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography. Applied Physics Letters. 2011;98(23):231104.

[24] Chaiwongkhot P, Kuntz KB, Zhang Y, Huang A, Bourgoin J-P, Sajeed S, et al. Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence. Physical Review A. 2019;99(6):062315.

[25] Gras G, Sultana N, Huang A, Jennewein T, Bussières F, Makarov V, et al. Optical control of single-photon negative-feedback avalanche diode detector. Journal of Applied Physics. 2020;127(9):094502.

[26] Huang A, Li R, Egorov V, Tchouragoulov S, Kumar K, Makarov V. Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution. Physical Review Applied. 2020;13(3):034017.

[27] Huang A, Navarrete Á, Sun S-H, Chaiwongkhot P, Curty M, Makarov V. Laser-seeding Attack in Quantum Key Distribution. Physical Review Applied. 2019;12(6):064043.

[28] Chistiakov V, Huang A, Egorov V, Makarov V. Controlling single-photon detector ID210 with bright light. Optics Express. 2019;27(22):32253-62.

[29] Fedorov A, Gerhardt I, Huang A, Jogenfors J, Kurochkin Y, Lamas-Linares A, et al. Comment on" Inherent security of phase coding quantum key distribution systems against detector blinding attacks"[Laser Phys. Lett. 15, 095203 (2018)]. arXiv preprint arXiv:180903911. 2018.

[30] Huang A, Barz S, Andersson E, Makarov V. Implementation vulnerabilities in general quantum cryptography. New Journal of Physics. 2018;20(10):103016.

[31] Pinheiro PVP, Chaiwongkhot P, Sajeed S, Horn RT, Bourgoin J-P, Jennewein T, et al. Eavesdropping and countermeasures for backflash side channel in quantum cryptography. Optics Express. 2018;26(16):21020-32.

[32] Huang A, Sun S-H, Liu Z, Makarov V. Quantum key distribution with distinguishable decoy states. Physical Review A. 2018;98(1):012330.

[33] Qin H, Kumar R, Makarov V, Alléaume R. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. Physical Review A. 2018;98(1):012312.

[34] Chaiwongkhot P, Sajeed S, Lydersen L, Makarov V. Finite-key-size effect in a commercial plug-and-play QKD system. Quantum Science and Technology. 2017;2(4):044003.

[35] Sajeed S, Minshull C, Jain N, Makarov V. Invisible Trojan-horse attack. Scientific Reports. 2017;7(1):1-7.

[36] Huang A, Sajeed S, Chaiwongkhot P, Soucarros M, Legré M, Makarov V. Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption. IEEE Journal of Quantum Electronics. 2016;52(11):1-11.

[37] Makarov V, Bourgoin J-P, Chaiwongkhot P, Gagné M, Jennewein T, Kaiser S, et al. Creation of backdoors in quantum communications via laser damage. Physical Review A. 2016;94(3):030302.

[38] Sajeed S, Chaiwongkhot P, Bourgoin J-P, Jennewein T, Lütkenhaus N, Makarov V. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. Physical Review A. 2015;91(6):062301.

[39] Sajeed S, Radchenko I, Kaiser S, Bourgoin J-P, Pappa A, Monat L, et al. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. Physical Review A. 2015;91(3):032326.

[40] Jain N, Stiller B, Khan I, Makarov V, Marquardt C, Leuchs G. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. IEEE Journal of Selected Topics in Quantum Electronics. 2014;21(3):168-77.

[41] Tanner MG, Makarov V, Hadfield RH. Optimised quantum hacking of superconducting nanowire single-photon detectors. Optics Express. 2014;22(6):6734-48.

[42] Bugge AN, Sauge S, Ghazali AMM, Skaar J, Lydersen L, Makarov V. Laser damage helps the eavesdropper in quantum cryptography. Physical Review Letters. 2014;112(7):070503.

[43] Liu Q, Lamas-Linares A, Kurtsiefer C, Skaar J, Makarov V, Gerhardt I. A universal setup for active control of a single-photon detector. Review of Scientific Instruments. 2014;85(1):349.

[44] Buttler WT, Hughes RJ, Kwiat PG, Lamoreaux SK, Luther GG, Morgan GL, et al., editors. Free-space quantum key distribution at night. Photonic Quantum Computing II; 1998: International Society for Optics and Photonics.

[45] Nauerth S, Moll F, Rau M, Fuchs C, Horwath J, Frick S, et al. Air-to-ground quantum communication. Nature Photonics. 2013;7(5):382-6.

[46] Fedrizzi A, Ursin R, Herbst T, Nespoli M, Prevedel R, Scheidl T, et al. High-fidelity transmission of entanglement over a high-loss free-space channel. Nature Physics. 2009;5(6):389-92.

[47] Weier H, Schmitt-Manderbach T, Regner N, Kurtsiefer C, Weinfurter H. Free space quantum key distribution: Towards a real life application. Fortschritte der Physik: Progress of Physics. 2006;54(8-10):840-5.

[48] Kish LB. Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law. Physics Letters A. 2006;352(3):178-82.

[49] Cho A. Simple noise may stymie spies without quantum weirdness. Science. 2005;309(5744):2148-.

[50] Vadai G, Mingesz R, Gingl Z. Generalized Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system using arbitrary resistors. Scientific Reports. 2015;5:13653.

[51] Kish LB. Enhanced secure key exchange systems based on the Johnson-noise scheme. Metrology and Measurement Systems. 2013;20(2):191-204.

[52] Kish LB, Granqvist CG. Random-resistor-random-temperature Kirchhoff-law-Johnson-noise (RRRT-KLJN) key exchange. Metrology and Measurement Systems. 2016;23(1):3-11.

[53] Kish LB, Granqvist CG. On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator. Quantum Information Processing. 2014;13(10):2213-9.

[54] Kish LB, Horvath T. Notes on recent approaches concerning the Kirchhoff-law–Johnson-noise-based secure key exchange. Physics Letters A. 2009;373(32):2858-68.

[55] Smulko J. Performance Analysis of the" Intelligent" Kirchhoff-Law–Johnson-Noise Secure Key Exchange. Fluctuation and Noise Letters. 2014;13(03):1450024.

[56] Mingesz R, Gingl Z, Kish LB. Johnson (-like)–Noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line. Physics Letters A. 2008;372(7):978-84.

[57] Mingesz R, Kish LB, Gingl Z, Granqvist C-G, Wen H, Peper F, et al. Unconditional security by the laws of classical physics. Metrology and Measurement Systems. 2013;20(1):3-16.

[58] Horváth T, Kish LB, Scheuer J. Effective privacy amplification for secure classical communications. EPL (Europhysics Letters). 2011;94(2):28002.

[59] Saez Y, Kish LB. Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange. PloS One. 2013;8(11).

[60] Mingesz R, Vadai G, Gingl Z. What kind of noise guarantees security for the Kirchhoff-law–Johnson-noise key exchange? Fluctuation and Noise Letters. 2014;13(03):1450021.

[61] Saez Y, Kish LB, Mingesz R, Gingl Z, Granqvist CG. Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law–Johnson-noise secure key exchange. Journal of Computational Electronics. 2014;13(1):271-7.

[62] Saez Y, Kish LB, Mingesz R, Gingl Z, Granqvist CG, editors. Bit errors in the Kirchhoff-Law–Johnson-Noise secure key exchange. International Journal of Modern Physics: Conference Series; 2014: World Scientific.

[63] Gingl Z, Mingesz R. Noise properties in the ideal Kirchhoff-law-Johnson-noise secure communication system. PLoS One. 2014;9(4).

[64] Liu P-L. A key agreement protocol using band-limited random signals and feedback. Journal of Lightwave Technology. 2009;27(23):5230-4.

[65] Kish LB. Methods of using existing wire lines (power lines, phone lines, internet lines) for totally secure classical communication utilizing Kirchoff's Law and Johnson-like noise. arXiv preprint physics/0610014. 2006.

[66] Gonzalez E, Kish LB, Balog RS, Enjeti P. Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters. PloS One. 2013;8(7):e70206.

[67] Kish LB, Entesari K, Granqvist C-G, Kwan C. Unconditionally secure credit/debit card chip scheme and physical unclonable function. Fluctuation and Noise Letters. 2017;16(01):1750002.

[68] Kish LB, Kwan C. Physical unclonable function hardware keys utilizing Kirchhoff-law-Johnson-noise secure key exchange and noise-based logic. Fluctuation and Noise Letters. 2013;12(03):1350018.

[69] Saez Y, Cao X, Kish LB, Pesti G. Securing vehicle communication systems by the KLJN key exchange protocol. Fluctuation and Noise Letters. 2014;13(03):1450020.

[70] Cao X, Saez Y, Pesti G, Kish LB. On KLJN-based secure key distribution in vehicular communication networks. Fluctuation and Noise Letters. 2015;14(01):1550008.

[71] Kish LB, Mingesz R. Totally secure classical networks with multipoint telecloning (teleportation) of classical bits through loops with Johnson-like noise. Fluctuation and Noise Letters. 2006;6(02):C9-C21.

[72] Kish LB, Peper F. Information networks secured by the laws of physics. IEICE Transactions on Communications. 2012;95(5):1501-7.

[73] Gonzalez EE, Kish LB, Balog RS. Encryption key distribution system and method. Google Patents; 2016. U.S. Patent # US9270448B2

[74] Gonzalez E, Balog RS, Mingesz R, Kish LB, editors. Unconditional security for the smart power grids and star networks. 2015 International Conference on Noise and Fluctuations (ICNF); 2015: IEEE.

[75] Gonzalez E, Balog RS, Kish LB. Resource requirements and speed versus geometry of unconditionally secure physical key exchanges. Entropy. 2015;17(4):2010-24.

[76] Gonzalez E, Kish LB. Key exchange trust evaluation in peer-to-peer sensor networks with unconditionally secure key exchange. Fluctuation and Noise Letters. 2016;15(01):1650008.

[77] Kish LB, Saidi O. Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives. Fluctuation and Noise Letters. 2008;8(02):L95-L8.

[78] Kish LB, Granqvist C-G. Enhanced usage of keys obtained by physical, unconditionally secure distributions. Fluctuation and Noise Letters. 2015;14(02):1550007.

[79] Kish LB, Scheuer J. Noise in the wire: The real impact of wire resistance for the Johnson (-like) noise based secure communicator. Physics Letters A. 2010;374(21):2140-2.

[80] Kish LB, Granqvist C-G. Elimination of a Second-Law-attack, and all cable-resistance-based attacks, in the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system. Entropy. 2014;16(10):5223-31.

[81] Vadai G, Gingl Z, Mingesz R. Generalized attack protection in the Kirchhoff-Law-Johnson-Noise secure key exchanger. IEEE Access. 2016;4:1141-7.

[82] Hao F. Kish's key exchange scheme is insecure. IEE Proceedings-Information Security. 2006;153(4):141-2.

[83] Kish LB. Response to Feng Hao's paper" Kish's key exchange scheme is insecure". Fluctuation and Noise Letters. 2006;6(04):C37-C41.

[84] Chen H-P, Gonzalez E, Saez Y, Kish LB. Cable capacitance attack against the KLJN secure key exchange. Information. 2015;6(4):719-32.

[85] Gunn LJ, Allison A, Abbott D. A new transient attack on the Kish key distribution system. IEEE Access. 2015;3:1640-8.

[86] Kish LB, Granqvist CG. Comments on “A New Transient Attack on the Kish Key Distribution System”. Metrology and Measurement Systems. 2016;23(3):321-31.

[87] Liu P-L. A Complete Circuit Model for the Key Distribution System Using Resistors and Noise Sources. Fluctuation and Noise Letters. 2019:2050012.

[88] Liu P-L. Re-examination of the cable capacitance in the key distribution system using resistors and noise sources. Fluctuation and Noise Letters. 2017;16(03):1750025.

[89] Chen H-P, Mohammad M, Kish LB. Current injection attack against the KLJN secure key exchange. Metrology and Measurement Systems. 2016;23(2):173-81.

[90] Kish LB. Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson (-like)-noise cipher and expansion by voltage-based security. Fluctuation and Noise Letters. 2006;6(01):L57-L63.

[91] Kish LB. The Kish Cypher: The Story of KLJN for Unconditional Security: World Scientific; 2017.

[92] Chen H-P, Kish LB, Granqvist CG. On the “cracking” scheme in the paper “A directional coupler attack against the Kish key distribution system” by Gunn, Allison and Abbott. Metrology and Measurement Systems. 2014;21(3):389-400.

[93] Kish LB, Abbott D, Granqvist CG. Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme. PloS One. 2013;8(12):e81810.

[94] Gunn LJ, Allison A, Abbott D. A directional wave measurement attack against the Kish key distribution system. Scientific Reports. 2014;4:6461.

[95] Chen H-P, Kish LB, Granqvist C-G, Schmera G. Do electromagnetic waves exist in a short cable at low frequencies? What does physics say? Fluctuation and Noise Letters. 2014;13(02):1450016.

[96] Kish LB, Gingl Z, Mingesz R, Vadai G, Smulko J, Granqvist C-G. Analysis of an attenuator artifact in an experimental attack by Gunn–Allison–Abbott against the Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system. Fluctuation and Noise Letters. 2015;14(01):1550011.

[97] Melhem MY, Kish LB. A Static-loop-current Attack Against the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System. Applied Sciences. 2019;9(4):666.

[98] Melhem MY, Kish LB. Generalized DC loop current attack against the KLJN secure key exchange scheme. arXiv preprint arXiv:191000974. 2019.

[99] Melhem MY, Kish LB. The problem of information leak due to parasitic loop currents and voltages in the KLJN secure key exchange scheme. Metrology and Measurement Systems. 2019;26(1).

[100] Melhem M, Kish L. Man in the middle and current injection attacks against the KLJN key exchanger compromised by DC sources. arXiv preprint arXiv:200403369. 2020.

[101] Melhem M, Chamon C, Ferdous S, Kish LB. AC Loop Current Attacks Against The KLJN Secure Key Exchange Scheme. arXiv preprint arXiv:200511002. 2020.

[102] Ferdous, S, et al. Defense of the KLJN secure key exchange system against transient attacks", to be published (2020).