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

Mutaz Y. Melhem, Laszlo B. Kish

Texas A&M University, Department of Electrical and Computer Engineering, College Station, TX 77843-3128, USA
(✉ *yar111@tamu.edu*, +1 979 847 907 *Laszlokish@tamu.edu*)

Abstract

A new attack against the Kirchhoff-Law-Johnson-Noise (KLJN) secure key distribution system is studied with unknown parasitic DC-voltage sources at both Alice's and Bob's ends. This paper is the generalization of our earlier investigation with a single-end parasitic source. 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. Simple defense methods against the attack are shown. The earlier defense method based solely on the comparison of current/voltage data at Alice's and Bob's terminals is useless here since the wire currents and voltages are equal at both ends. However, the more expensive version of the earlier defense method, which is based on in-situ system simulation and comparison with measurements, works efficiently.

Keywords: unconditional security, secure key exchange, parasitic loop currents and voltages, information leak.

1. Introduction

The *Kirchhoff-Law-Johnson-Noise* (KLJN) secure key distribution scheme [1–26], see Fig. 1, is based on the properties of thermal noise of the resistors. Once it was introduced in [2], it had the promise to provide robust, fast and unconditionally secure communications at low cost, and all the advantages of chip integrability. The information channel is composed of a wire. In the core of the simplest scheme, each communicator contains a switch that, at the beginning of each bit exchange cycle, randomly alternates between two resistors R_L & R_H, where we suppose $R_H > R_L$, see Fig. 1. Since, in the system, there are four different combinations of R_A & R_B, that is, $R_L R_L$ (LL), $R_H R_H$ (HH), $R_L R_H$ (LH) and $R_H R_L$ (HL), the KLJN scheme randomly alternates between four different situations. The first and second letters in the parentheses refer to the connected resistors at Alice's and Bob's ends, respectively. Note the practical scheme consists of many more elements such as noise generators, line filters, and measurement and compensation systems to

secure the privacy for arbitrary situations. The power spectral density of the voltage in the wire can be written as:

$$S_{u,w}(f) = 4kT \frac{R_A R_B}{R_A + R_B} . \tag{1}$$

While the power spectral density of the current in the wire can be written as:

$$S_{i,w\|}(f) = \frac{4kT}{R_A + R_B} . \tag{2}$$

Here T is the effective noise temperature (which can be much larger than room temperature when external voltage generators are used), k is the Boltzmann's constant, R_A and R_B are the connected resistances at Alice's and Bob's ends, respectively, where R_A, $R_B \in \{RL, RH\}$. On the other hand, each switching cycle, Alice and Bob will measure the wire's $S_{u,w}(f)$ and $S_{i,w}(f)$, and by using either (1) or (2), each party will compensate it's resistance value and the measured $S_{u,w}(f)$ or $S_{i,w}(f)$ in the left hand side of the used equation, so each equation will end with only one variable, which is the resistance of the other party. Then they will solve the resultant equation to get the other party resistant. To guarantee total security of the key, both parties will ignore any cycle where R_A & R_B are equal because Eve can know the values of the operating resistances by solving (1) and (2), while the LH and HL situations will be considered for the Key Exchange, since in these situations Eve cannot infer which resistance is operating in either side. A general proof about the unconditional security of the *Kirchhoff-Law-Johnson-Noise* (KLJN) was introduced in [2].
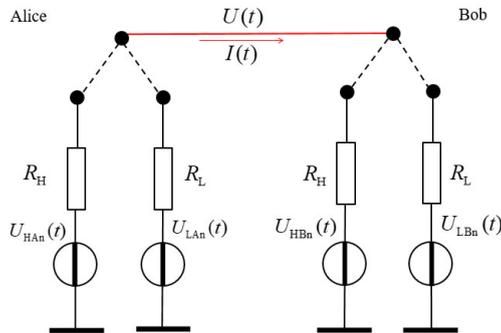

Fig. 1. The core of the KLJN system. $U_{HAn}(t)$, $U_{LAn}(t)$, $U_{HBn}(t)$ and $U_{LBn}(t)$ are either the natural (thermal) Johnsons noises sources of the related resistances or artificial noise generators with high voltages. Alice and Bob measures the voltage and the current $U(t)$ and $I(t)$ in the wire, and use them in evaluating the power density spectra $S_{u,w}(f)$ and $S_{i,w}(f)$, respectively.

Several attacks against the KLJN scheme were proposed against the KLJN scheme. None of them could impair the unconditional security of the scheme, since either there was a proper defense scheme against or attack was based on misconceptions [3–20, 27–30], including experimental errors. On the other hand, passive attacks against practical KLJN systems deviating from the ideal assumptions of the scheme [2] were discussed in several papers [4–13]. For example, parasitic or non-ideal features such as transients, wire's resistance, cable capacitance, temperature differences, delay effects and transients, etc. are such practical issues. In each case, these discussions ultimately confirmed the security of the practical KLJN with proper parameter choices, defense circuitries, compensation techniques, or privacy amplifications [1].

Recently, a new attack scheme assuming the existence of single parasitic DC source at either communicating party was introduced [14]. DC current based ground loops or similar non-idealities can yield such situation. In [14] to demonstrate the security vulnerability, the following assumptions were made:

i) The parasitic DC source was located at only one of the end of the wire channel.
ii) Eve knew the location of this parasitic DC source.
iii) Eve knew the value of the voltage of this DC source.

The above assumptions [14] were in line with Kerckhoffs's principle of security [1], that is, all the essential details of the secure communication system will eventually be known by the adversary except the momentary key [1].

In the present paper, we make Eve's job much more complicated by adding an arbitrary second generator assuming that there was not yet enough time for Eve to utilize Kerckhoffs's principle of security [1], see below.

2. The generalized DC ground loop situation

In [14], we assumed a ground loop situation with a single, known DC voltage generator located at Alice's end and demonstrated the resulting information leak. In the present paper, the generalized and most common practical situation is studied with two unknown DC voltage generators of arbitrary polarity that are located at Alice's and Bob's sides, see Fig. 2.
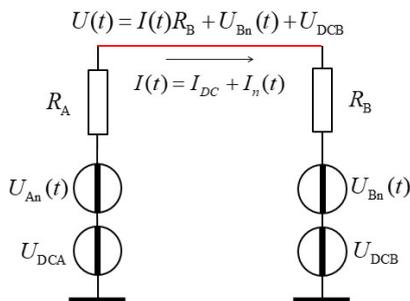
$$U(t) = I(t)R_{\mathrm{B}} + U_{\mathrm{Bn}}(t) + U_{\mathrm{DCB}}$$

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

R_{A} R_{B}

$U_{\mathrm{An}}(t)$ $U_{\mathrm{Bn}}(t)$

U_{DCA} U_{DCB}

Fig. 2. The KLJN system in the generalized ground loop situation $U_{\mathrm{Bn}}(t)$ & $U_{\mathrm{An}}(t)$ are the thermal voltage noise sources associated with R_{A} & R_{B}, respectively, where R_{A} & $R_{\mathrm{B}} \in \{R_{\mathrm{L}}; R_{\mathrm{H}}\}$. U_{DCA} & U_{DCB} are the ground loop DC voltage sources, and $U(t)$ & $I(t)$ are the wire voltage and wire current, respectively.

As a preparation, we introduce the mathematical notations that are similar but more complex than in [14]. Both the voltage $U(t)$ and current $I(t)$ in the wire have a DC and an AC (stochastic, that is, noise) components, see Fig. 2. 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:

$$I(t) = I_{\mathrm{DC}} + I_{\mathrm{n}}(t), \tag{3}$$

where the DC and AC components are:

$$I_{\mathrm{DC}} = \frac{U_{\mathrm{DCA}} - U_{\mathrm{DCB}}}{R_{\mathrm{A}} + R_{\mathrm{B}}},, \tag{4}$$

609

and

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

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 [1–4]) with $U_{\mathrm{An}} \in \{U_{\mathrm{LAn}}; U_{\mathrm{HAn}}\}$ and $U_{\mathrm{Bn}} \in \{U_{\mathrm{LBn}}; U_{\mathrm{HBn}}\}$. The voltage on the wire can be written as:

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

From (3) and (6) we obtain:

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

where U_{DCw} and $U_{\mathrm{ACw}}(t)$ are the DC and AC voltage components on the wire, see Fig. 2:

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

From (8), 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 $R_B = R_h$, the DC component of the wire's voltage is:

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

while in the HL bit situation it is:

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

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

$$U_{\mathrm{th}} \equiv \frac{U_{\mathrm{LH}} + U_{\mathrm{HL}}}{2} = \frac{U_{\mathrm{DCA}} + U_{\mathrm{DCB}}}{2} . \tag{11}$$

Moreover, we compare (9) and (10), to obtain the following inequality:

$$U_{\mathrm{LH}} \geq U_{\mathrm{HL}} \quad \text{if} \quad U_{\mathrm{DCA}} \geq U_{\mathrm{DCB}} . \tag{12}$$

The noise component $U_{\mathrm{ACw}}(t)$ of $U(t)$, see Fig. 2, can be written as:

$$U_{\mathrm{ACw}}(t) = I_{\mathrm{n}}(t)R_{\mathrm{B}} + U_{\mathrm{Bn}}(t). \tag{13}$$

From (5) and (13):

$$U_{\mathrm{ACw}}(t) \equiv \frac{U_{\mathrm{An}}(t) - U_{\mathrm{Bn}}(t)}{R_{\mathrm{A}} + R_{\mathrm{B}}}R_{\mathrm{B}} + U_{\mathrm{Bn}}(t) = \frac{U_{\mathrm{An}}(t)R_{\mathrm{B}} + U_{\mathrm{Bn}}(t)R_{\mathrm{A}}}{R_{\mathrm{A}} + R_{\mathrm{B}}} . \tag{14}$$

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 [14]. Figs. 3 and 4 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.
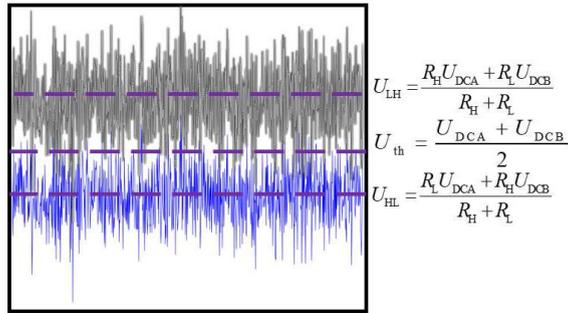
$$U_{\mathrm{LH}} = \frac{R_{\mathrm{H}} U_{\mathrm{DCA}} + R_{\mathrm{L}} U_{\mathrm{DCB}}}{R_{\mathrm{H}} + R_{\mathrm{L}}}$$

$$U_{\mathrm{th}} = \frac{U_{\mathrm{DCA}} + U_{\mathrm{DCB}}}{2}$$

$$U_{\mathrm{HL}} = \frac{R_{\mathrm{L}} U_{\mathrm{DCA}} + R_{\mathrm{H}} U_{\mathrm{DCB}}}{R_{\mathrm{H}} + R_{\mathrm{L}}}$$

Fig. 3. Eves' threshold scheme to guess the bit situation LH *vs.* HL when $U_{\mathrm{DCA}} > U_{\mathrm{DCB}}$, 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.

$$U_{\mathrm{HL}} = \frac{R_{\mathrm{L}} U_{\mathrm{DCA}} + R_{\mathrm{H}} U_{\mathrm{DCB}}}{R_{\mathrm{H}} + R_{\mathrm{L}}}$$

$$U_{\mathrm{th}} = \frac{U_{\mathrm{DCA}} + U_{\mathrm{DCB}}}{2}$$

$$U_{\mathrm{LH}} = \frac{R_{\mathrm{H}} U_{\mathrm{DCA}} + R_{\mathrm{L}} U_{\mathrm{DCB}}}{R_{\mathrm{H}} + R_{\mathrm{L}}}$$
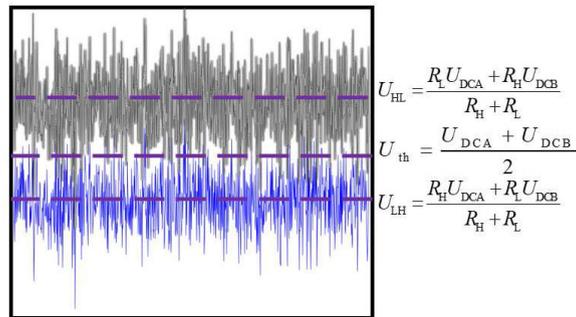
Fig. 4. Eves' threshold scheme to guess the bit situation LH *vs.* HL when $U_{\mathrm{DCB}} > U_{\mathrm{DCA}}$ and they are assumed positive for the purpose of illustration.

3. 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 (6), we can express U_{DCB} as:

$$U_{\mathrm{DCB}} = U(t) - I(t)R_{\mathrm{B}} - U_{\mathrm{Bn}}(t). \tag{15}$$

The above equation is useful to Eve in the LL and HH situations, where she knows the connected resistors, including R_{B}, see [14]. $U(t)$ 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:

$$\langle U_{\mathrm{DCB}} \rangle_\tau = \langle U(t) \rangle_\tau - R_{\mathrm{B}} \langle I(t) \rangle_\tau - \langle U_{\mathrm{Bn}}(t) \rangle_\tau, \tag{16}$$

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:

$$U_{\mathrm{DCB}} = \langle U(t) \rangle_\tau - R_{\mathrm{B}} \langle I(t) \rangle_\tau. \tag{17}$$

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}:

$$U_{\text{DCA}} = \langle U(t) \rangle_\tau + R_A \langle I(t) \rangle_\tau . \tag{18}$$

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 (17) and (18), respectively. Equation (13) and condition $R_H > R_L$ 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}.

4. On the attack

4.1. 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 (12)]. 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 [14], 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 (9)–(14)]: 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 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}, $p \equiv n_{\text{cor}}/n_{\text{tot}}$ [14]. The $p = 0.5$ situation indicates the perfect security limit [27].

4.2. Can Eve use the DC current, instead of the DC voltage, in her attack scheme?

To comply with the mathematical notations used in Section 2, I_{HL} and I_{LH} denote the DC current in the wire; and $I_{\text{LHn}}(t)$ and $I_{\text{HLn}}(t)$ 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, $I_{\text{LH}} \equiv I_{\text{HL}} = I_{\text{th}}$. Also, $I_{\text{LHn}}(t)$ and $I_{\text{HLn}}(t)$ have the same rms values. Therefore there is no difference in the measured values that Eve could utilize for an attack.

4.3. 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. 5 and 6. Thus, only the difference $U_{\text{DCA}} - U_{\text{DCB}}$ of these voltages determines the efficiency of the attack, not their actual values.

In the subsequent section, the attack method is demonstrated by computer simulations.
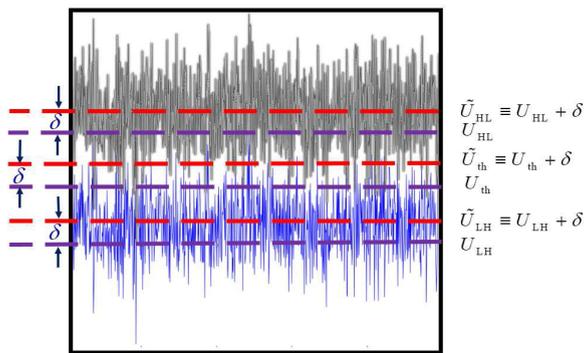
Fig. 5. Illustration of the DC voltage components in the LH and HL situations before and after a δ shift in the parasitic voltages, where $\widetilde{U}_{DCA} = U_{DCA} + \delta$; $\widetilde{U}_{DCB} = U_{DCB} + \delta$; and $\widetilde{U}_{LH}$ and $\widetilde{U}_{HL}$ are the resulting DC voltages in the LH and HL situations, respectively. $\widetilde{U}_{th}$ is the average of $\widetilde{U}_{LH}$ and $\widetilde{U}_{HL}$.
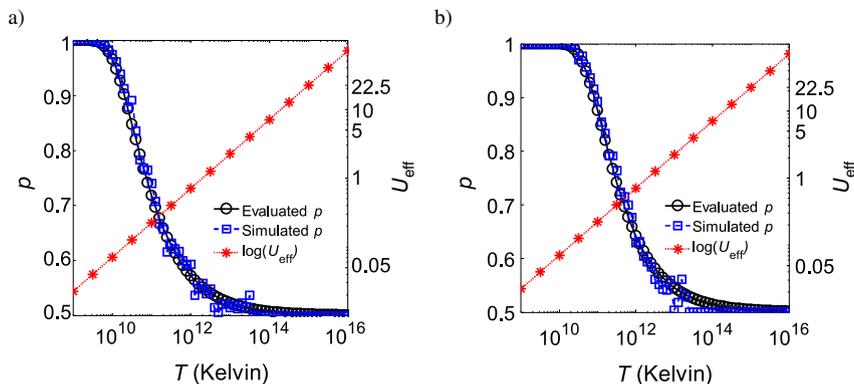

Fig. 6. Eve's correct bit guessing probability (p) versus temperatures at $U_{DCA} - U_{DCB}$ differences of a) 0.1 V and b) 0.2 V, at various effective noise temperatures, with bandwidth (Δf) of '1 MHz. At the computer simulations the key length was 700 bits with 500 independent time samples/bit. The asymptote $p = 0.5$ represents perfect security. The evaluation was carried out by the error function, see (19) and (20).

5. Demonstration

Eve's correct bit guessing probability p was evaluated analytically and tested by computer simulations, see Fig. 6.

For the analytic evaluation we used the error function:

$$p\{U(t) \geq U_{th}\} = 0.5\left[1 - erf\left(\frac{U_{th} - U_{DCw}}{U_{eff}\sqrt{2}}\right)\right], \tag{19}$$

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

$$erf(x) = \frac{1}{\sqrt{\pi}} \int\limits_{-x}^{x} \exp\left(-y^2\right) dy \tag{20}$$

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

613

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 Subsection 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 $U_{\text{DCA}} - U_{\text{DCB}} = 0.1$ V and 0.2 V. During these tests, R_{L} and R_{H} were fixed to 1 and 10 kΩ, 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.

6. Defense methods

The attack can be countered using the same defense techniques, as described in [14], 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 [1, 2, 29]). All methods are the same as those discussed in [14], 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. Alternatively tuning them to reach $U_{\text{DCB}} - U_{\text{DCA}} = 0$.

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

7. Conclusion

This paper generalizes the DC loop current attack introduced in [14]. The generalized scheme makes Eve's work easier. We provided a mathematical analysis and verified the attacks analytically and by computer simulations. We also propose effective defense techniques.

In conclusion, in practical KLJN key exchangers Alice and Bob must carry a DC loop current tests before and during operation and act accordingly (see Section 6).

It is important to note that the general, more expensive defense method of KLJN that is based on in-situ system simulation and comparison with measurements, see Subsection 4.1 in [16], works efficiently because that alarms for any deviation from the idealized situation, including parasitic DC voltages and currents.

References

[1] Kish, L.B. (2017). *The Kish Cypher: The Story of KLJN for Unconditional Security*. New Jersey: World Scientific.

[2] Kish, L.B. (2006). Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law. *Phys. Lett. A*, 352(3), 178–182.

[3] Kish, L. B., & Granqvist, C. G. (2014). On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator. *Quantum Information Processing*, 13(10), 2213-2219.

[4] Kish, L.B., Granqvist, C. G. (2016). Comments on "A New Transient Attack on the Kish Key Distribution System." *Metrol. Meas. Syst.*, 23(3), 321–331.

[5] Gunn, L.J, Andrew, A., Derek, A. (2015). A new transient attack on the kish key distribution system. *IEEE Access*, 3, 1640–1648.

[6] Cho, A. (2005). Simple noise may stymie spies without quantum weirdness. *Science*, 309(5744), 2148.

[7] Kish, L.B., Scheuer, J. (2010). Noise in the wire: The real impact of wire resistance for the Johnson (-like) noise based secure communicator. *Phys. Lett. A*, 374(21), 2140–2142.

[8] Kish, L.B., Granqvist, C.-G. (2014). Elimination of a Second-Law-attack, and all cable-resistance-based attacks, in the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system. *Entropy*, 16(10), 5223–5231.

[9] Vadai, G., Gingl, Z., Mingesz, R. (2016). Generalized attack protection in the Kirchhoff-Law-Johnson-Noise secure key exchanger. *IEEE Access*, 4, 1141–1147.

[10] Hao, F. (2006). Kish's key exchange scheme is insecure. *IEE Proceedings-Information Security*, 153(4), 141–142.

[11] Kish, L.B. (2006). Response to Feng Hao's paper Kish's key exchange scheme is insecure. *Fluct. Noise Lett.*, 6(4), C37–C41.

[12] Chen, H.-P., Gonzalez, E., Saez, Y., Kish, L.B. (2015). Cable capacitance attack against the KLJN secure key exchange. *Information*, 6(4), 719–732.

[13] Kish, L.B. (2013). Enhanced secure key exchange systems based on the Johnson-noise scheme. *Metrol. Meas. Syst.*, 20(2), 191–204.

[14] Melhem, M.Y., Kish, L.B. (2019). A static-loop-current attack against the Kirchhoff-Law-Johnson Noise (KLJN) secure key exchange system. *Applied Sciences*, 9(4), 666.

[15] Kish, L.B., Granqvist, C.G. (2016). Random-resistor-random-temperature Kirchhoff-law-Johnson-noise (RRRT-KLJN) key exchange. *Metrol. Meas. Syst.*, 23(1), 3–11.

[16] Chen, H.-P., Mohammad, M., Kish, L.B. (2016). Current injection attack against the KLJN secure key exchange. *Metrol. Meas. Syst.*, 23(2), 173–181.

[17] Kish, L.B. (2006). Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson (-like)-noise cipher and expansion by voltage-based security. *Fluct. Noise Lett.*, 6(1), L57–L63.

[18] Kish, L.B., Horvath, T. (2009). Notes on recent approaches concerning the Kirchhoff-law–Johnson-noise-based secure key exchange. *Phys. Lett. A*, 373(32), 2858–2868.

[19] Kish, L.B., Abbott, D., Granqvist, C.G. (2013). Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme. textit{PloS one}, 8(12), e81810.

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

[21] Kish, L.B. (2006). 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*.

[22] Gonzalez, E., Kish, L.B., Balog, R.S., Enjeti, P. (2013). Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters. *PLOS ONE*, 8(7), e70206.

[23] Kish, L.B., Entesari, K., Granqvist, C.-G., Kwan, C. (2017). Unconditionally secure credit/debit card chip scheme and physical unclonable function. *Fluct. Noise Lett.*, 16(1), 1750002.

[24] Kish, L.B., Kwan, C. (2013). Physical unclonable function hardware keys utilizing Kirchhoff-law-Johnson-noise secure key exchange and noise-based logic. *Fluct. Noise Lett.*, 12(3), 1350018.

[25] Saez, Y., Cao, X., Kish, L.B., Pesti, G. (2014). Securing vehicle communication systems by the KLJN key exchange protocol. *Fluct. Noise Lett.*, 13(3), 1450020.

[26] Cao, X., Saez, Y., Pesti, G., Kish, L.B. (2015). On KLJN-based secure key distribution in vehicular communication networks. *Fluct. Noise Lett.*, 14(1), 1550008.

[27] Melhem Y.M., Kish L.B. (2018). The problem of information leak due to parasitic loop currents and voltages in the KLJN secure key exchange scheme. *8th International Conference on Unsolved Problems on Noise (UPoN-2018)*, July 9–13, 2018, Gdańsk, Poland.

[28] Chen, H.-P., Kish, L.B., Granqvist, C.G. (2014). On the "cracking" scheme in the paper "A directional coupler attack against the Kish key distribution system" by Gunn, Allison and Abbott. *Metrol. Meas. Syst.*, 21(3), 389–400.

[29] Chen, H.-P., Kish, L.B., Granqvist, C.G., Schmera, G. (2014). Do electromagnetic waves exist in a short cable at low frequencies? What does physics say? *Fluct. Noise Lett.*, 13(2), 1450016.

[30] Kish, L.B., Gingl, Z., Mingesz, R., Vadai, G., Smulko, J., Granqvist, C.G. (2015). Analysis of an attenuator artifact in an experimental attack by Gunn–Allison–Abbott against the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system. *Fluct. Noise Lett.*, 14(1), 1550011.