IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 10, 2016, accepted March 13, 2016, date of publication March 21, 2016, date of current version April 1, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2544442

Generalized Attack Protection in the Kirchhoff-Law-Johnson-Noise Secure Key Exchanger

GERGELY VADAI, ZOLTAN GINGL, (Member, IEEE), AND ROBERT MINGESZ, (Member, IEEE)
Department of Technical Informatics, University of Szeged, Szeged 6720, Hungary

Corresponding author: Z. Gingl (gingl@inf.u-szeged.hu)

This work was supported by the European Union and the State of Hungary within the European Social Fund through the National Excellence Program under Grant TÁMOP 4.2.4. A/2-11-1-2012-0001.

ABSTRACT The Kirchhoff-Law-Johnson-Noise unconditionally secure key exchanger is a promising, surprisingly simple, very low cost and efficient electronic alternative to quantum key distribution. A few resistors, switches, and interconnecting cables can provide unconditionally secure data transmission in the ideal case by utilizing the thermal noise of the resistors. The key problems regarding practical realizations are related to the resistance tolerance, finite cable resistance, and other non-ideal properties that can cause information leak. In this paper, we present robust protection from cable resistance and resistance mismatch attacks against the system. Our theoretical results show that all resistive inaccuracies, parasitic resistances, cable resistance, and temperature dependence can be compensated; therefore, the practical implementation becomes much easier. The generalized method provides inherent protection against the so-called second law attack as well.

INDEX TERMS Unconditional security, secure key exchange, attack protection, KLJN secure key exchanger.

I. INTRODUCTION

Secure data transmission is without doubt among the most challenging problems today. Millions of sensitive data transfer transactions are performed in every second in various fields of economy, medicine, traffic, industry, governmental and military activities and even more. One of the most known and hopeful tool to realize unconditionally secure communication could be the quantum key distribution (QKD) [1]. However, it requires rather special and expensive hardware, electronic-to-optical signal conversion, special optical data paths. Therefore, there is a natural need for much cheaper and much less difficult alternatives that can effectively replace QKD in wide variety of high-volume practical applications. One of these is an exceptionally simple and ultralow-cost alternative based on classical physics has been introduced that can have unbeatable advantages [2]–[6]. The so-called Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme (also known as Kish Key Distribution (KKD) [7]) is an electronic system that uses only a four resistors and two switches to share a secret key fully securely. The simplest version of the KLJN system can be seen in Fig. 1.

Both communicating parties, Alice and Bob, can choose one of the two resistors to be connected to the communication line, R_L or R_H. There are four possible states depending on the choice of Alice and Bob: LL, LH, HL and HH. The thermal (Johnson) noise voltage of the selected resistor is the signal source at each end and has the effective power spectral density of $4kTR_L$ or $4kTR_H$ depending on the state of the corresponding switch, k is the Boltzmann constant, and T is the absolute temperature. The eavesdropper Eve can observe the resulting noise voltage V_E and noise current I_E in the interconnecting wire. From the eavesdropper's point of view, the two resistors are connected in parallel, therefore the power spectral density of the voltage noise is $4kTR_LR_H/(R_L+R_H)$, if different resistors are chosen at the two sides. In this case the current noise power spectral density is given by and $4kT/(R_L + R_H)$. Therefore, one can see that the LH and HL states can't be distinguished by the eavesdropper, while both Alice and Bob has the information where the lower and higher value resistors are. This can be used to exchange a single bit of information with unconditional security. There is a fundamental thermodynamical explanation of this feature: if the system is in thermal equilibrium, there is no energy

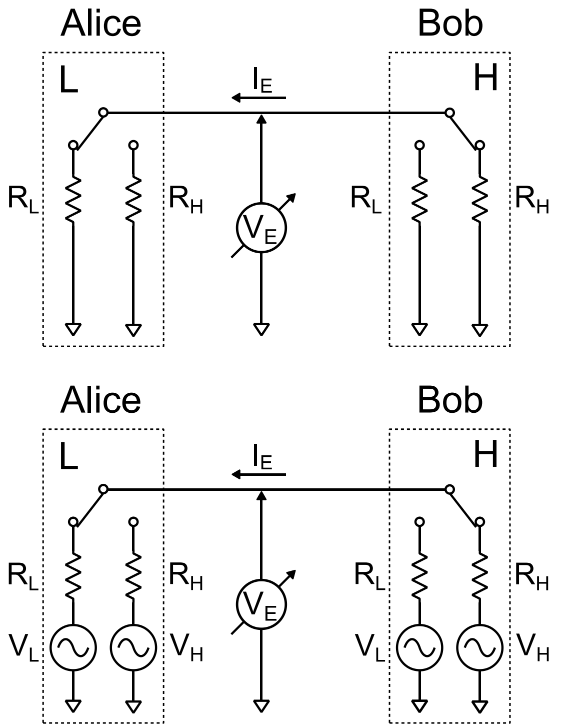

FIGURE 1. Two equivalent models of the KLJN key exchanger. At both ends lower (L) and higher (H) value resistors can be chosen using the switches. At the bottom the separate voltage generators represent the thermal noise of the corresponding resistors. The eavesdropper can measure the voltage V_E and current I_E in the cable and knows the values of R_L and R_H that are public. LH state is shown; HL state can be selected by toggling both switches.

flow between the two parties, therefore there is no way to extract information, the dynamics of the system if fully symmetric [2]. This also implies that the correlation between the voltage V_E and current I_E is zero. It is important to note that Alice, Bob and Eve must evaluate the power spectral density, therefore a certain averaging time is needed called bit transfer time. Assuming a given bandwidth, the variance is proportional to the power spectral density therefore the evaluation of this is preferred in practical applications. The instant values are meaningless due to the random nature of the signals. All system parameters are public including the values of R_L and R_H. DC or other deterministic voltage generators can't be used for secure communication.

This very smart and incredibly simple idea can be implemented in practice with the use of some additional electronic components [8] and can even be integrated on a chip easily that allows application in many modern compact electronic devices. Secret key exchange between integrated circuits on a printed circuit board, between machines in a hospital, between computers located in different buildings are all supported. Since the thermal noise amplitude is very small, artificial voltage generators typically based on digital-to-analog converters (DAC) can be used to set the voltage noise effective amplitude to the desired value [8], [9]. The effective power of the thermal noise voltage signal with bandwidth of f_{BW} is equal to $4kTRf_{BW}$, therefore the amplitude tuning can be considered as emulating different, typically very high temperatures. The system has inspired the development of a discrete time secure key exchanger [10] also. Many different kinds of attack types have been discussed: attacks based on cable resistance [4], [11]–[14], temperature difference in the channel [15], [16], finite propagation time [11], Bennett-Riedel attack [17], [18], directional coupler attack [7], [19], [20], second law attack [14], transient attack [21], and current injection attack [22]. The system is still claimed to be unconditionally secure in its ideal operating conditions [2], [3]. The phrase *unconditional security* is used in many papers about the KLJN key exchange scheme, the most detailed discussion can be found in [3], while different interpretation recently considered [21]. It is important to note that in a physical realization there is always an information leak that depends on many factors like cable length, resistance tolerance, noise bandwidth, parasitic capacitance, propagation time. However, with proper design, the information leak can be reduced to arbitrarily small level [3], [9] and, unlike in the case of conditionally secure systems, no additional restrictions are assumed on the measurement precision or computational resources available to the eavesdropper.

Many possible applications are considered including securing computer communications, hardware components, memories, processors, keyboards, mass storage devices, key distribution over the Smart Grid, ethernet cables, uncloneable hardware keys, industrial sensor networks and automotive communication [23]–[28].

The original KJLN system discussed above uses two identical resistor pairs, two switches and interconnecting cable to transfer data securely. The thermal noise of the resistors is used to hide information from the eavesdropper, while the communicating parties, Alice and Bob, can measure the noise magnitude to determine the state of the system and this way they can exchange bits of a key. Recently we have applied a different approach to guarantee unconditional security and this allowed a significant generalization of the system [29]. We have shown that it is not required to have the same lower and higher value resistors at the two ends. Our main point was that all quantities measured by the eavesdropper must be the same for the LH and HL states. This means that thermal equilibrium and zero correlation of the voltage and current fluctuations are not needed any more what was a critical point of the original arrangement to prove security and in the same time it exposed the system to rather strong attacks [14]. This generalization has already inspired new exchange schemes also [30].

In the generalized KLJN system depicted in Fig. 2 at both ends of the communication line lower (L) and higher (H) value resistors can be chosen again, but there are no other restrictions on the values of the resistors. It has been shown that the eavesdropper cannot distinguish between the states LH and HL if the voltage noise amplitudes are properly chosen [29]. In other words, if the resistor values are given, it is possible to find voltage noise amplitudes that guarantee

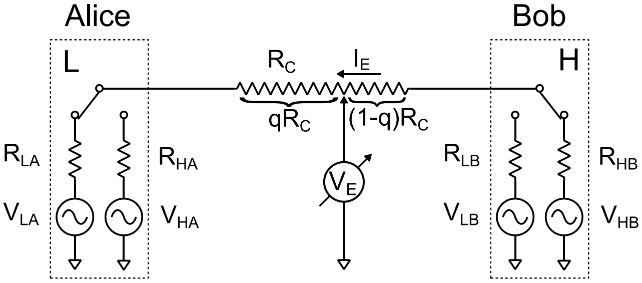

FIGURE 2. The generalized KLJN key exchanger with finite cable resistance. At both ends lower (L) and higher (H) value resistors can be chosen using the switches. The voltage generators represent the thermal noise of the corresponding resistor. The eavesdropper can measure the voltage V_E and current I_E anywhere in the cable that has resistance R_C. The observation point is indicated by q in the range of 0 to 1. LH state is shown; HL state can be selected by toggling both switches.

unconditional security. It is important to note that since in the generalized case any value for the resistors can be used, all resistor inaccuracies and parasitic resistances including the resistance of the switches can be taken into account rather easily. The voltage noise amplitudes can be tuned to fully eliminate the effect of these non-ideal components. This is a crucial feature concerning practical applications where such conditions always present. Although the application of artificial generators could allow the use of almost any kind of noise signal, we have proven that absolute security can be guaranteed if and only if Gaussian noise is used [29], [31].

In the following we consider a new, more practical case when the cable has finite resistance and the eavesdropper can measure the voltage and current anywhere in the cable.

II. RESULTS

A. GENERALIZED ATTACK PROTECTION

We prove that by proper tuning of the amplitude of the voltage noise generators can fully prevent information leak at any observation point of the cable. Instead of using thermodynamic approach [2] here we apply mathematical statistical tools following the methods used in our latest articles in the subject [29], [31], [32].

The current I_E and voltage V_E observed by the eavesdropper in the LH state (shown in Fig. 2) can be written as:

$$I_{E,LH}(t) = \frac{V_{HB}(t) - V_{LA}(t)}{R_{LA} + R_{HB} + R_C}, \tag{1}$$

$$V_{E,LH}(t) = \frac{(R_{HB}+(1-q)\cdot R_C)\cdot V_{LA}(t)+(R_{LA}+q\cdot R_C)\cdot V_{HB}(t)}{R_{LA}+R_{HB}+R_C}. \tag{2}$$

Here q specifies the observation point in the cable; it is zero at the left end of the cable and unity at the other end.

Similar equations can be obtained for the HL state, when the higher values resistor is selected at Alice's side:

$$I_{E,HL}(t) = \frac{V_{LB}(t) - V_{HA}(t)}{R_{HA} + R_{LB} + R_C}, \tag{3}$$

$$V_{E,HL}(t) = \frac{(R_{LB}+(1-q)\cdot R_C)\cdot V_{HA}(t)+(R_{HA}+q\cdot R_C)\cdot V_{LB}(t)}{R_{HA}+R_{LB}+R_C}. \tag{4}$$

The communication can only be secure, if the eavesdropper observes the same statistical properties of these signals both for the LH and HL states. The variance of the current I_E, the variance of the voltage V_E and the correlation between these signals must not depend on the actual state. Using (1) and (3) the variance of the current can be calculated for the two states, LH and HL, and these must be equal:

$$\frac{\langle V_{LA}^2(t)\rangle + \langle V_{HB}^2(t)\rangle}{(R_{LA} + R_{HB} + R_C)^2} = \frac{\langle V_{HA}^2(t)\rangle + \langle V_{LB}^2(t)\rangle}{(R_{HA} + R_{LB} + R_C)^2}. \tag{5}$$

The following equation that expresses the equality of the voltage variances in the LH and HL states can be obtained using (2) and (4):

$$\frac{(R_{HB}+(1-q)\cdot R_C)^2\cdot\langle V_{LA}^2(t)\rangle+(R_{LA}+q\cdot R_C)^2\cdot\langle V_{HB}^2(t)\rangle}{(R_{LA}+R_{HB}+R_C)^2} = \frac{(R_{LB}+(1-q)\cdot R_C)^2\cdot\langle V_{HA}^2(t)\rangle+(R_{HA}+q\cdot R_C)^2\cdot\langle V_{LB}^2(t)\rangle}{(R_{HA}+R_{LB}+R_C)^2}. \tag{6}$$

Finally, the correlation of the current and voltage must be the same in the LH and HL cases:

$$\left\langle \frac{V_{HB}(t) - V_{LA}(t)}{R_{LA} + R_{HB} + R_C} \cdot \frac{(R_{HB}+(1-q)\cdot R_C)\cdot V_{LA}(t)+(R_{LA}+q\cdot R_C)\cdot V_{HB}(t)}{R_{LA}+R_{HB}+R_C}\right\rangle = \left\langle \frac{V_{LB}(t) - V_{HA}(t)}{R_{HA} + R_{LB} + R_C} \cdot \frac{(R_{LB}+(1-q)\cdot R_C)\cdot V_{HA}(t)+(R_{HA}+q\cdot R_C)\cdot V_{LB}(t)}{R_{HA}+R_{LB}+R_C}\right\rangle. \tag{7}$$

Since all voltage noise signals are independent, the cross correlation terms, $\langle V_{HB}(t)\cdot V_{LA}(t)\rangle$, and $\langle V_{HA}(t)\cdot V_{LB}(t)\rangle$, are zero. Therefore, the left hand side of (7) can be written as

$$\begin{aligned}
&\left\langle \frac{(R_{LA}+q\cdot R_C)\cdot V_{HB}^2(t) - (R_{HB}+(1-q)\cdot R_C)\cdot V_{LA}^2(t)}{(R_{HA}+R_{LB}+R_C)^2} + \frac{R_{HB}\cdot V_{HB}(t)\cdot V_{LA}(t) - (R_{LA}+q\cdot R_C)\cdot V_{HB}(t)\cdot V_{LA}(t)}{(R_{HA}+R_{LB}+R_C)^2}\right\rangle \\
&= \frac{R_{LA}+q\cdot R_C}{(R_{LA}+R_{HB}+R_C)^2}\cdot\left\langle V_{HB}^2(t)\right\rangle - \frac{R_{HB}+(1-q)\cdot R_C}{(R_{LA}+R_{HB}+R_C)^2}\cdot\left\langle V_{LA}^2(t)\right\rangle + \frac{R_{HB}+(1-2\cdot q)\cdot R_C - R_{LA}}{(R_{LA}+R_{HB}+R_C)^2}\cdot\langle V_{HA}(t)V_{LB}(t)\rangle \\
&= \frac{R_{LA}+q\cdot R_C}{(R_{LA}+R_{HB}+R_C)^2}\left\langle V_{HB}^2(t)\right\rangle - \frac{R_{HB}+(1-q)\cdot R_C}{(R_{LA}+R_{HB}+R_C)^2}\left\langle V_{LA}^2(t)\right\rangle.
\end{aligned} \tag{8}$$

One can similarly simplify the right term of (7) to the following:

$$\frac{R_{HA}+q\cdot R_C}{(R_{HA}+R_{LB}+R_C)^2}\left\langle V_{LB}^2(t)\right\rangle - \frac{R_{LB}+(1-q)\cdot R_C}{(R_{HA}+R_{LB}+R_C)^2}\left\langle V_{HA}^2(t)\right\rangle. \quad (9)$$

Using (7), (8) and (9) we get

$$\frac{R_{LA}+q\cdot R_C}{(R_{LA}+R_{HB}+R_C)^2}\left\langle V_{HB}^2(t)\right\rangle - \frac{R_{HB}+(1-q)\cdot R_C}{(R_{LA}+R_{HB}+R_C)^2}\left\langle V_{LA}^2(t)\right\rangle = \frac{R_{HA}+q\cdot R_C}{(R_{HA}+R_{LB}+R_C)^2}\left\langle V_{LB}^2(t)\right\rangle - \frac{R_{LB}+(1-q)\cdot R_C}{(R_{HA}+R_{LB}+R_C)^2}\left\langle V_{HA}^2(t)\right\rangle. \quad (10)$$

According to (5), (6) and (10) the variances of the voltage noise signals at Alice and Bob must satisfy the following equations (11)–(13), as shown at the bottom of this page.

The variance of $V_{LA}(t)$ can be selected without restrictions that allows optimization of the signal amplitudes in real applications. We can conclude that properly chosen values of the voltage generators can be used to ensure security, therefore the information leak caused by the cable resistance can be fully eliminated even for the generalized KLJN system, when all four resistor values can have independent values. It is important to note that (11), (12) and (13) do not contain q, which means that the security is maintained over the full length of the interconnecting cable. The eavesdropper cannot determine the state of the system; it doesn't matter where the actual observation point is. Fig. 3 and Fig. 4 show examples for the dependence of the correlation between the voltage and current measured by the eavesdropper on the observation position q for different resistor values and cable resistance. The key point is that although the correlation does depend of the value of q, on the cable resistance and on the value of the resistors used in the system, it is the same for both the LH and HL cases.

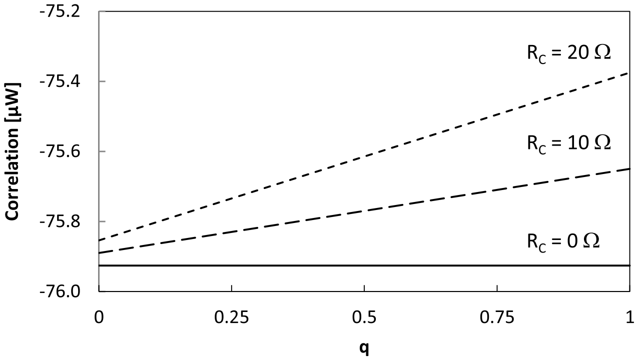

FIGURE 3. Correlation of the voltage V_E and current I_E as a function of the observation position q. Note that the correlation is the same for both the LH and HL states. In this example the following values were used in (10): R_{HA} = 10 kOhm, R_{LB} = 5 kOhm, R_{LA} = 1 kOhm, R_{HB} = 9 kOhm, V_{LA} = 1 V. The used values of R_C are indicated in the figure and V_{HB}, V_{LB} and V_{HA} were calculated using (11), (12) and (13).

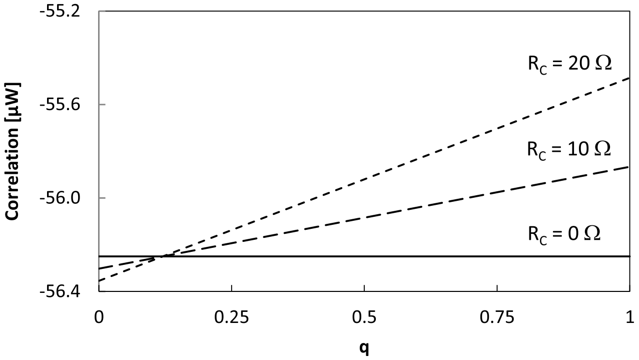

FIGURE 4. Correlation of the voltage V_E and current I_E as a function of the observation position q. Note that the correlation is the same for both the LH and HL states. In this example the following values were used in (10): R_{HA} = 9 kOhm, R_{LB} = 3 kOhm, R_{LA} = 1 kOhm, R_{HB} = 9 kOhm, V_{LA} = 1 V. The used values of R_C are indicated in the figure and V_{HB}, V_{LB} and V_{HA} were calculated using (11), (12) and (13).

B. FINITE GROUND IMPEDANCE

Fig. 1 and Fig. 2 show the most common schematic used in the articles about the KLJN system. However, the communicating parties can be far from each other, papers discussed cable lengths from a few meters to hundreds of kilometers [8], [33]. In addition, the cable resistance can matter in the case of shorter distance depending on the value of the resistors used in the system. For example, in the case of the communication between microcontrollers in a vehicle the wire resistance can be considerable. In such cases one can't assume zero impedance grounding, therefore a more practical version can be taken into account as shown in Fig. 5. Here both interconnecting wires have their own finite resistance and we assume that the eavesdropper can measure the voltage between any two points of these wires. The two wires can have similar or rather different resistance, examples can be two parallel wires and a coaxial cable. Note that a distributed RLC network analysis for high frequency signals not considered here can be found in [33].

$$\frac{\left\langle V_{HB}^2(t)\right\rangle}{\left\langle V_{LA}^2(t)\right\rangle} = \frac{R_{LB}(R_{HA}+R_{HB}+R_C)-(R_{HA}+R_C)R_{HB}-R_{HB}^2}{R_{LA}^2+R_{LB}(R_{LA}-R_{HA})+(R_C-R_{HA})R_{LA}-R_CR_{HA}} \quad (11)$$

$$\frac{\left\langle V_{LB}^2(t)\right\rangle}{\left\langle V_{LA}^2(t)\right\rangle} = \frac{R_{LB}^2+R_{LB}(R_{HA}-R_{HB}+R_C)-(R_{HA}+R_C)R_{HB}}{R_{LA}^2+R_{LA}(R_{HB}-R_{HA}+R_C)-R_{HA}R_{HB}-R_CR_{HA}} \quad (12)$$

$$\frac{\left\langle V_{HA}^2(t)\right\rangle}{\left\langle V_{LA}^2(t)\right\rangle} = \frac{R_{HA}^2+R_{LB}(R_{HB}+R_{HA}+R_C)+(R_{HA}+R_C)R_{HB}+2R_CR_{HA}+R_C^2}{R_{LA}^2+R_{LB}(R_{LA}+R_{HB}+R_C)+(R_{HB}+2R_C)R_{LA}+R_CR_{HB}+R_C^2} \quad (13)$$

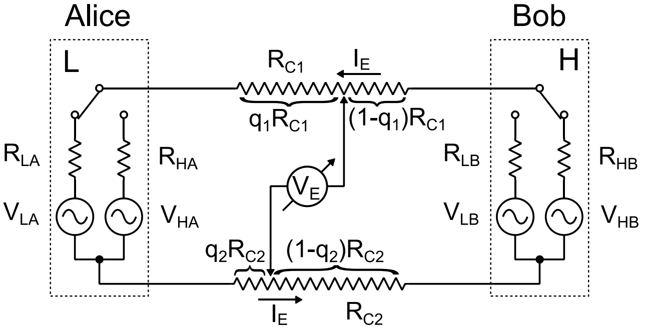

FIGURE 5. A more practical view of the generalized KLJN key exchanger with finite cable resistance that is relevant for communication between distant parties. In this case both interconnecting wires of the loop have finite resistance, no grounding with zero impedance is assumed.

Our theoretical treatment presented above is valid for this case, we only need to express the cable resistance R_C and the value of q. The same loop resistance is obtained when

$$R_C = R_{C1} + R_{C2}, \tag{14}$$

while V_E is equivalent if

$$q = \frac{q_1 R_{C1} + q_2 R_{C2}}{R_C}. \tag{15}$$

C. SPECIAL CASE, THE ORIGINAL KLJN SYSTEM

The original KLJN system can be treated as a special case, when the lower and higher value resistors are the same at the two ends: $R_{LA} = R_{LB} = R_L$ and $R_{HA} = R_{HB} = R_H$. Using this condition in (11), (12) and (13) one can obtain the voltage noise variances required for secure communication:

$$\frac{\langle V_{HB}^2(t)\rangle}{\langle V_{LA}^2(t)\rangle} = \frac{R_H + \frac{R_C}{2}}{R_L + \frac{R_C}{2}}, \tag{16}$$

$$\frac{\langle V_{HA}^2(t)\rangle}{\langle V_{LA}^2(t)\rangle} = \frac{R_H + \frac{R_C}{2}}{R_L + \frac{R_C}{2}}, \tag{17}$$

$$\left\langle V_{LB}^2(t)\right\rangle = \left\langle V_{LA}^2(t)\right\rangle. \tag{18}$$

Note that the lower and higher voltage variances are the same at both ends just like the associated resistors, regardless of the value of the cable resistance R_c. According to (16) and (17) one can see that the voltage variance must be proportional to the corresponding resistor value plus the half of the cable resistance – just as if the original system with zero resistance cable would have such resistors and the eavesdropper would listen in the middle ($q = 0.5$). Therefore, in this case the correlation between V_E and I_E is zero.

When q is different from 0.5 – i.e. the eavesdropper does not acquire voltage and current in the middle point – then the correlation between V_E and I_E is not zero, see Fig. 6.

Consequently, for non-zero cable resistance zero correlation between the voltage and current can't be required, since it can be satisfied in the middle of the cable only. On the other hand, as we have proven, the correlation is the same in the LH and HL states regardless of the value of q; therefore, the unconditional security is still provided over the full extent of the cable.

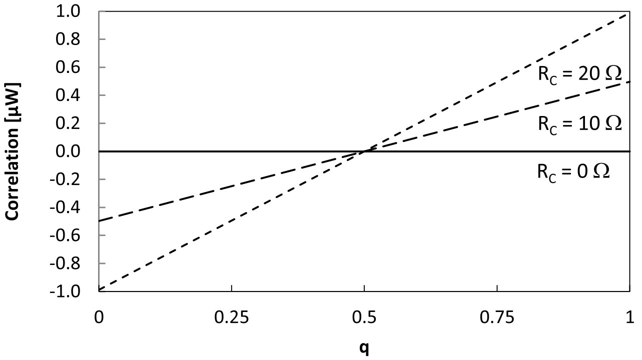

FIGURE 6. Correlation of the voltage V_E and current I_E as a function of the observation position q. Note that the correlation is the same for both the LH and HL states. The correlation is only zero at $q = 0.5$. In this example the following values were used in (10): $R_L = 1$ kΩ, $R_H = 9$ kΩ, $V_{LA} = V_{LB} = 1$ V. The used values of R_C are indicated in the figure and V_{HA} and V_{HB} were calculated using (16) and (17).

III. CONCLUSION

In this paper we have investigated the security of the KLJN secure key exchange system in its most general operating condition so far. In the original system the communicating resistor pairs must be identical at the two ends. Any deviation from this due to for example resistor inaccuracy or finite switch on-resistance causes information leak and exposes the system to attacks. Our theoretical results show that unconditional security can be maintained over the full extent of the communication line for any kind of interconnecting cables or wires and when all four resistors values can be different. In our generalized case the thermal equilibrium is not needed any more, therefore the so called second law attack [14] is inherently prevented. Note that a new version of the KLJN key exchange scheme [30] inspired by our generalization [29] is also protected against general attacks by the use of random resistors and random temperature.

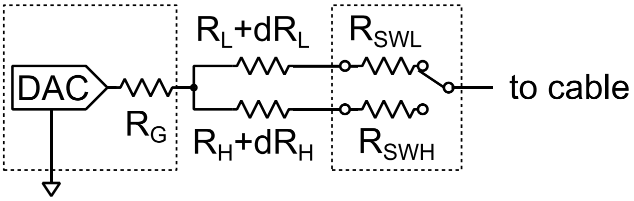

FIGURE 7. Simplified schematic of a KLJN communicator module.

One of the most important advantages of the generalized system discussed in this paper is that resistance tolerance, parasitic resistance of the switches, voltage generator source resistance and the cable resistance can all be compensated. Fig. 7 shows a simplified schematic of a possible real communicator module that utilizes a voltage output DAC to realize the artificial voltage noise generator.

Here R_G represents the output resistance of the voltage output DAC, dR_L and dR_H are the deviations from the ideal R_L

and R_H communicator resistance values and R_{SWL} and R_{SWH} are the switch on resistance values in the L and H states, respectively. This means that the equivalent lower value resistance is

$$R_{L,eq} = R_L + dR_L + R_G + R_{SWL}, \tag{19}$$

and the equivalent higher value resistance can be expressed as

$$R_{H,eq} = R_H + dR_H + R_G + R_{SWH}. \tag{20}$$

The equivalent values for both communicator modules can be used in (11), (12) and (13) to determine the required noise amplitudes that guarantee secure communication. As shown in Fig. 7 a single DAC is enough to generate the noise signal for both the L and H states, because the voltage amplitude can be programmed accordingly. Note that between state transitions (LH→HL and HL→LH) the signal must be ramped down to zero to avoid sharp changes and associated transients that can expose the system to attacks [8] and the resolution, non-linearity, limited signal range of the DAC should be considered in practical applications.

During operation the loop current and voltages at different nodes can be measured without disturbing the communication process. This means that the resistance values can be monitored in real-time, therefore even continuous compensation is possible. The temperature dependence can be considered in industrial and automotive environments, where wide range of temperature can be expected. If the communicators are used in mobile devices and different cables may be used, the cable resistance can be changed and the system's parameters can be affected. In these cases, the level of security is limited by the accuracy of the resistance measurement and the voltage amplitude tuning only.

The results presented in this paper can help to make the real world application of the KLJN protocol a lot easier in many fields [23]–[28]. Our method is based on the use of mathematical statistical tools and we did not use the original thermodynamical physical approach. Further information including open source simulation software and demonstrational videos can be found on our institutional page [34].

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Bengaluru, India, Oct. 1984, pp. 175–179.

[2] L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law," *Phys. Lett. A*, vol. 352, no. 3, pp. 178–182, 2006.

[3] L. B. Kish and C. G. Granqvist, "On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator," *Quantum Inf. Process.*, vol. 13, no. 10, pp. 2213–2219, 2014.

[4] A. Cho, "Simple noise may stymie spies without quantum weirdness," *Science*, vol. 309, no. 5744, p. 2148, 2005.

[5] D. J. Palmer, "Noise keeps spooks out of the loop," *New Sci.*, no. 2605, p. 32, May 2007. [Online]. Available: https://www.newscientist.com/article/mg19426055-300-noise-keeps-spooks-out-of-the-loop/

[6] D. Abbott and G. Schmera, "Secure communications using the KLJN scheme," *Scholarpedia*, vol. 8, no. 8, 2013, Art. no. 31157. [Online]. Available: http://www.scholarpedia.org/article/Secure_communications_using_the_KLJN_scheme

[7] L. J. Gunn, A. Allison, and D. Abbott, "A directional wave measurement attack against the Kish key distribution system," *Sci. Rep.*, vol. 4, Sep. 2014, Art. no. 6461.

[8] R. Mingesz, Z. Gingl, and L. B. Kish, "Johnson(-like)–noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line," *Phys. Lett. A*, vol. 372, no. 7, pp. 978–984, 2008.

[9] R. Mingesz, "Experimental study of the Kirchhoff-law-Johnson-noise secure key exchange," *Int. J. Mod. Phys. Conf. Ser.*, vol. 33, Sep. 2014, Art. no. 1460365.

[10] P.-L. Liu, "A key agreement protocol using band-limited random signals and feedback," *J. Lightw. Technol.*, vol. 27, no. 23, pp. 5230–5234, Dec. 1, 2009.

[11] J. Scheuer and A. Yariv, "A classical key-distribution system based on Johnson (like) noise—How secure?" *Phys. Lett. A*, vol. 359, no. 6, pp. 737–740, 2006.

[12] L. B. Kish, "Response to Scheuer–Yariv: 'A classical key-distribution system based on Johnson (like) noise—How secure?"' *Phys. Lett. A*, vol. 359, no. 6, pp. 741–744, 2006.

[13] L. B. Kish and J. Scheuer, "Noise in the wire: The real impact of wire resistance for the Johnson(-like) noise based secure communicator," *Phys. Lett. A*, vol. 374, no. 21, pp. 2140–2142, 2010.

[14] L. B. Kish and C.-G. Granqvist, "Elimination of a second-law-attack, and all cable-resistance-based attacks, in the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system," *Entropy*, vol. 16, no. 10, pp. 5223–5231, 2014.

[15] F. Hao, "Kish's key exchange scheme is insecure," *IEE Proc.-Inf. Secur.*, vol. 153, no. 4, pp. 141–142, 2006.

[16] L. B. Kish, "Response to Feng Hao's paper 'Kish's key exchange scheme is insecure,"' *Fluctuation Noise Lett.*, vol. 6, no. 4, pp. C37–C41, 2006.

[17] C. H. Bennett and C. J. Riedel. (2013). "On the security of key distribution based on Johnson–Nyquist noise." [Online]. Available: http://arxiv.org/abs/1303.7435

[18] L. B. Kish, D. Abbott, and C. G. Granqvist, "Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme," *PLoS ONE*, vol. 8, no. 12, 2013, Art. no. e81810.

[19] H.-P. Chen, L. B. Kish, C.-G. Granqvist, and G. Schmera, "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.*, vol. 21, no. 3, pp. 389–400, 2014.

[20] L. B. Kish, Z. Gingl, R. Mingesz, G. Vadai, J. Smulko, and C.-G. Granqvist, "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 Noise Lett.*, vol. 14, no. 1, 2015, Art. no. 1550011.

[21] L. J. Gunn, A. Allison, and D. Abbott, "A new transient attack on the Kish key distribution system," *IEEE Access*, vol. 3, pp. 1640–1648, Oct. 2015.

[22] H.-P. Chen, M. Mohammad, and L. B. Kish. (2015). "Current injection attack against the KLJN secure key exchange." [Online]. Available: http://arxiv.org/abs/1512.03685

[23] L. B. Kish, "Enhanced secure key exchange systems based on the Johnson-noise scheme," *Metrol. Meas. Syst.*, vol. 20, no. 2, pp. 191–204, 2013.

[24] E. Gonzalez, L. B. Kish, R. S. Balog, and P. Enjeti, "Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters," *PLoS ONE*, vol. 8, no. 7, 2013, Art. no. 70206.

[25] L. B. Kish and C. Kwan, "Physical unclonable function hardware keys utilizing Kirchhoff-law-Johnson-noise secure key exchange and noise-based logic," *Fluctuation Noise Lett.*, vol. 12, no. 2, 2013, Art. no. 1350018.

[26] L. B. Kish and O. Saidi, "Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives," *Fluctuation Noise Lett.*, vol. 8, no. 2, pp. L95–L98, 2008.

[27] Y. Saez, X. Cao, L. B. Kish, and G. Pesti, "Securing vehicle communication systems by the KLJN key exchange protocol," *Fluctuation Noise Lett.*, vol. 13, no. 3, 2014, Art. no. 14500205.

[28] E. Gonzalez and L. B. Kish. (2015). "Key exchange trust evaluation in peer-to-peer sensor networks with unconditionally secure key exchange." [Online]. Available: http://arxiv.org/abs/1511.06795v1

[29] G. Vadai, R. Mingesz, and Z. Gingl, "Generalized Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system using arbitrary resistors," *Sci. Rep.*, vol. 5, Sep. 2015, Art. no. 13653.

[30] L. B. Kish and C.-G. Granqvist, "Random-resistor-random-temperature KLJN key exchange," *Metrol. Meas. Syst.*, vol. 23, no. 1, pp. 3–11, 2016.

[31] R. Mingesz, G. Vadai, and Z. Gingl, "What kind of noise guarantees security for the Kirchhoff-law–Johnson-noise key exchange?" *Fluctuation Noise Lett.*, vol. 13, no. 3, 2014, Art. no. 1450021.

[32] Z. Gingl and R. Mingesz, "Noise properties in the ideal Kirchhoff-Law-Johnson-noise secure communication system," *PLoS ONE*, vol. 9, no. 4, 2014, Art. no. 96109.

[33] L. B. Kish and T. Horvath, "Notes on recent approaches concerning the Kirchhoff-law–Johnson-noise-based secure key exchange," *Phys. Lett. A*, vol. 373, no. 32, pp. 2858–2868, 2009.

[34] *Related Simulations*, accessed on Mar. 21, 2016. [Online]. Available: http://www.noise.inf.u-szeged.hu/Research/kljn/

GERGELY VADAI received the B.Sc. and M.Sc. degrees in physics from the University of Szeged, Hungary, in 2010 and 2012, respectively. He is currently pursuing the Ph.D. degree in computer science under the supervision of Z. Gingl. Since 2015, he has been an Assistant Lecturer with the Department of Technical Informatics, University of Szeged. He received the Fellowship granted by the Hungarian Republic in 2011.

He generalized the Kirchhoff-Law–Johnson-Noise Secure Key Exchange System with R. Mingesz and Z. Gingl in 2015. His research interests include exploitation of noise in multidisciplinary fields, such as secure communication, fluctuation enhanced sensing, or performance estimation using the fluctuations of human motion.

ZOLTAN GINGL received the M.Sc. and Ph.D. degrees in physics from the University of Szeged, and the D.Sc. degree in electrical and electronic engineering from the Hungarian Academy of Sciences. Since 1989, he has been with the University of Szeged, where he is currently a Full Professor and the Head of the Department of Technical Informatics. He has over 200 papers related to various fields, including 1/f noise, stochastic resonance, fluctuation enhanced sensing, noise-based secure communications, instrumentation and control, computer controlled measurements and analysis of heart rate, blood pressure, and blood flow fluctuations, and analysis of respiratory mechanics and education. He has edited conference proceedings and a special issue of the journal and he is a member of the Editorial Board of the journal *Fluctuation and Noise Letters*.

ROBERT MINGESZ received the Ph.D. degree from the Department of Technical Informatics, University of Szeged. He has over 12 years of experience in the fields related to instrumentation, data acquisition, data processing, and software engineering. He is currently an Assistant Professor with the Department of Technical Informatics, University of Szeged. His main research areas include the studying of properties of colored noises (stochastic resonance, 1/f noise), examining the advantages of noises and fluctuations [fluctuation enhanced sensing, Kirchhoff-Law–Johnson-Noise (KLJN)], and designing and building software defined data acquisition and data processing systems for multidisciplinary applications.

He started to work in the field of KLJN Secure Key Exchange Protocol with Laszlo Kish in 2006, and since then, several papers have been published in this field. With his colleagues, he implemented the first realization of the KLJN protocol. He is working on the implementation details of the KLJN as well as on analyzing the security and performance of the protocol.