# Generalized attack protection in the Kirchhoff-Law-Johnson-Noise secure key exchanger

Gergely Vadai, Zoltan Gingl and Robert Mingesz

Department of Technical Informatics, University of Szeged, Hungary

Corresponding author: e-mail: G. Vadai (vadaig@inf.u-szeged.hu)

## Abstract

The Kirchhoff-Law-Johnson-Noise (KLJN) unconditionally secure key exchanger is a promising, surprisingly simple and efficient electronic alternative to quantum key distribution (QKD). A few resistors, switches and interconnecting cable can provide unconditionally secure data transmission in the ideal case utilizing the thermal noise of the resistors. The key problems of 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 a robust protection from the strongest attacks against the system used in its most general operating conditions. Our theoretical results show that all resistive inaccuracies, parasitic resistances, cable resistance and temperature dependence can be compensated; therefore, the practical implementation gets a lot easier. The generalized method provides inherent protection against the so called second law attack as well.

## Introduction

Secure data transmission is without doubt one of the most challenging problem 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 unbreakable communication could be the quantum key distribution (QKD) [1], however an exceptionally simple and ultralow-cost alternative based on classical physics has been introduced that can have unbeatable advantages [2,3]. The so-called Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme (also known as Kish Key Distribution (KKD) [4]) is an electronic system that uses only a few resistors to share a secret key fully securely. This very smart and incredibly simple idea can be implemented in practice with the use of some additional electronic components [5] and can be integrated on a chip easily. The system has inspired the development of a digital key exchanger [6] and many different kind of attack types has been discussed: attacks based on cable resistance [7-11], temperature difference in the channel [12,13], finite propagation time [8], Bennett-Riedel attack [14,15], directional coupler attack [4,16,17], second law attack [11], transient attack [18], and current injection attack [19]. The system

is still believed to be unbreakable in its ideal operating conditions and 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 [20-25].

The original KJLN system uses two identical resistor pairs, two switches and interconnecting cable to transfer data securely [2]. The thermal (Johnson) noise of the resistors is used to hide information from the eavesdropper, while the communicating parties, Alice and Bob, can measure the noise properties to determine the state of the system and this way they can exchange bits of a key. Very recently we have generalized the system significantly by allowing the use of four different resistors and by relaxing the requirement of zero correlation of the voltage and current fluctuations in the cable [26]. This means that thermal equilibrium is 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 [11]. Our generalization has already inspired new exchange schemes also [27].

In the generalized KLJN system depicted in Fig. 1 at both ends of the communication line lower (L) and higher (H) value resistors can be chosen, there are no other restrictions on the values of the resistors. Accordingly, four different states are possible: LL, LH, HL, HH. It has been shown that the eavesdropper cannot distinguish between the states LH and HL if the voltage noise amplitudes are properly chosen [26]. Here we consider the case when the cable has non-zero resistance and the eavesdropper can measure the voltage and current anywhere in the cable.

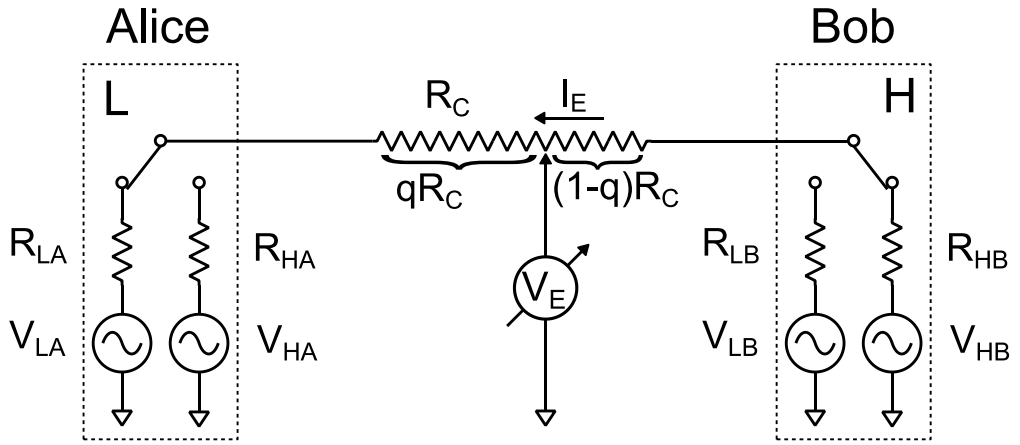


**Fig. 1** The generalized KLJN key exchanger with finite cable resistance. At both ends lower (L) and higher (H) value resistors can be chosen using the switches. The voltage generators represent the thermal noise of the corresponding resistor. The eavesdropper can measure the voltage $V_E$ and current $I_E$ 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.

It is important to note that in our generalized case the conditions $R_{LA}$=$R_{LB}$ and $R_{HA}$=$R_{HB}$ of the original system are not required [26], therefore all resistor inaccuracies and parasitic resistances including the resistance of the switches can be taken into account rather easily. This is a crucial feature concerning practical implementations. Since the thermal noise is very small, artificial voltage

generators typically based on digital-to-analog converters can be used that can emulate very high temperatures [5, 28]. This makes the effect of the cable resistance thermal noise negligible as well. 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].

## Results

In the following 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 [26,29,30].

The current $I_E$ and voltage $V_E$ observed by the eavesdropper in the LH state (shown in Fig. 1) can be written as:

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

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

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:

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

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

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:

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

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

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

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

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

Since all voltage noise signals are independent, the cross correlation terms are zero. Therefore, the left hand side of (7) can be written as

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

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

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

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

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

According to (5), (6) and (10) the variances of the voltage noise signals at Alice and Bob must satisfy the following equations:

$$\frac{\langle V_{HB}^2(t)\rangle}{\langle V_{LA}^2(t)\rangle} = \frac{R_{LB}(R_{HA}+R_{HB}+R_C)-(R_{HA}+R_C)R_{HB}-R_{HB}^2}{R_{LA}^2+R_{LB}(R_{LA}-R_{HA})+(R_C-R_{HA})R_{LA}-R_C R_{HA}}, \tag{11}$$

$$\frac{\langle V_{LB}^2(t)\rangle}{\langle V_{LA}^2(t)\rangle} = \frac{R_{LB}^2+R_{LB}(R_{HA}-R_{HB}+R_C)-(R_{HA}+R_C)R_{HB}}{R_{LA}^2+R_{LA}(R_{HB}-R_{HA}+R_C)-R_{HA}R_{HB}-R_C R_{HA}}, \tag{12}$$

$$\frac{\langle V_{HA}^2(t)\rangle}{\langle V_{LA}^2(t)\rangle} = \frac{R_{HA}^2+R_{LB}(R_{HB}+R_{HA}+R_C)+(R_{HA}+R_C)R_{HB}+2R_C R_{HA}+R_C^2}{R_{LA}^2+R_{LB}(R_{LA}+R_{HB}+R_C)+(R_{HB}+2R_C)R_{LA}+R_C R_{HB}+R_C^2}. \tag{13}$$

The variance of $V_{LA}(t)$ can be selected without restrictions. This means that proper values of the voltage generators can be used to ensure security, therefore the information leak caused by resistance inaccuracies and the cable resistance can be fully eliminated even for arbitrarily chosen resistor 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. 2 and Fig. 3 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 $q$, the cable resistance and the value of the resistors used in the system, it is the same for both the LH and HL cases.

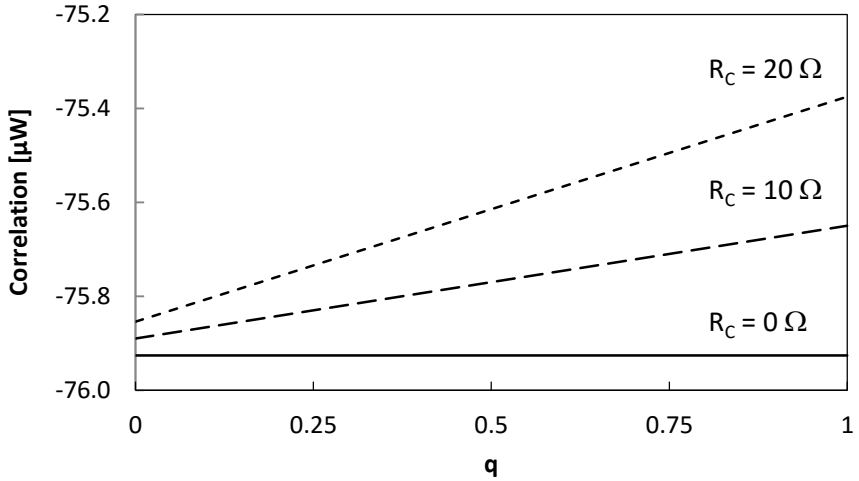


**Fig. 2** Correlation of the voltage $V_E$ and current $I_E$ as a function of the observation position $q$. Note that the correlation is the same for both the LH and HL states. In this example the following values were used in (10): $R_{HA}$=10 kOhm, $R_{LB}$=5 kOhm, $R_{LA}$=1 kOhm, $R_{HB}$=9 kOhm, $V_{LA}$=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).

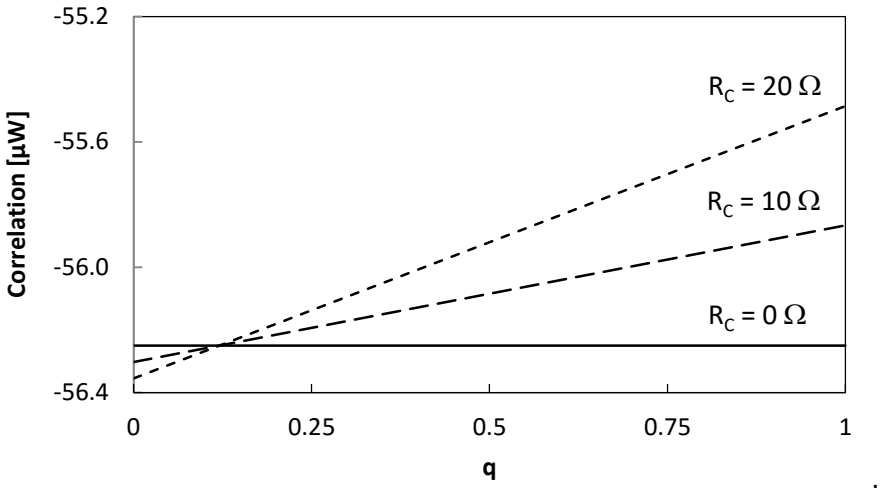


**Fig. 3** Correlation of the voltage $V_E$ and current $I_E$ as a function of the observation position $q$. Note that the correlation is the same for both the LH and HL states. In this example the following values were used in (10): $R_{HA}$=9 kOhm, $R_{LB}$=3 kOhm, $R_{LA}$=1 kOhm, $R_{HB}$=9 kOhm, $V_{LA}$=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).

In Fig. 1 we have shown the most common schematic used in the articles about the KLJN system. However, the communicating parties can be far from each other, papers discussed considerable cable lengths from a few meters to hundreds of kilometers [5, 31]. In addition, the cable resistance can matter in the case of shorter distances depending on the value of the resistors used in the system. In such cases one can't assume zero impedance grounding, therefore a more practical version can be considered shown in Fig. 4. 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. Note that a distributed RLC network analysis for high frequency signals not considered here can be found in [31].

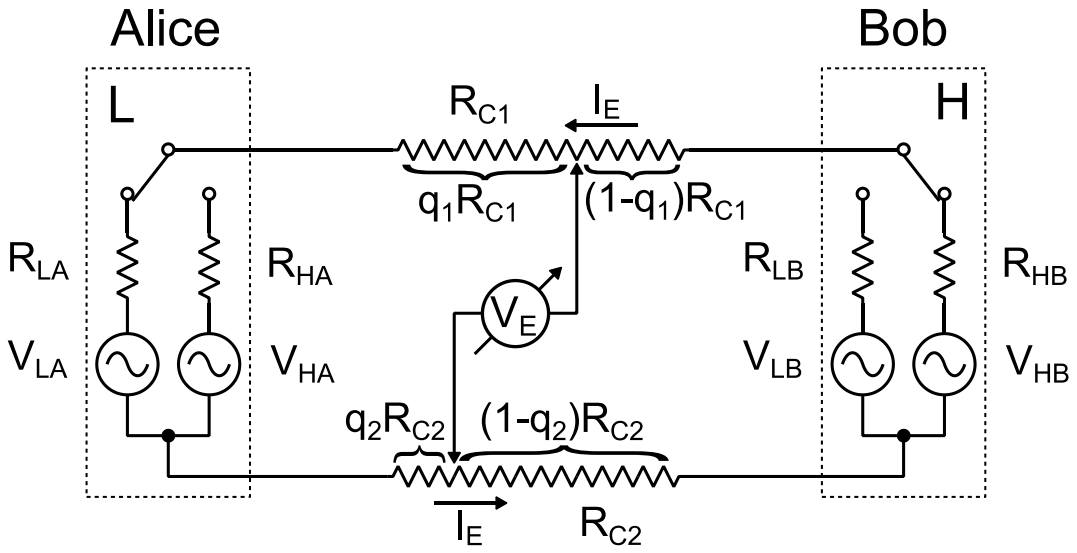

**Fig. 4** A more practical view of the generalized KLJN key exchanger with finite cable resistance that is relevant for communication between distant parties. In this case both interconnecting wires of the loop have finite resistance, no grounding with zero impedance is assumed.

Our theoretical treatment presented above is valid even for this case, we only need to express the cable resistance $R_C$ and the value of $q$ as follows:

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

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

## 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 one can obtain the voltage noise variances required for unbreakable communication:

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

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

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

Note that the lower and higher voltage variances are the same at both ends like the associated resistors. According to (16) and (17) one can see that 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. 5.

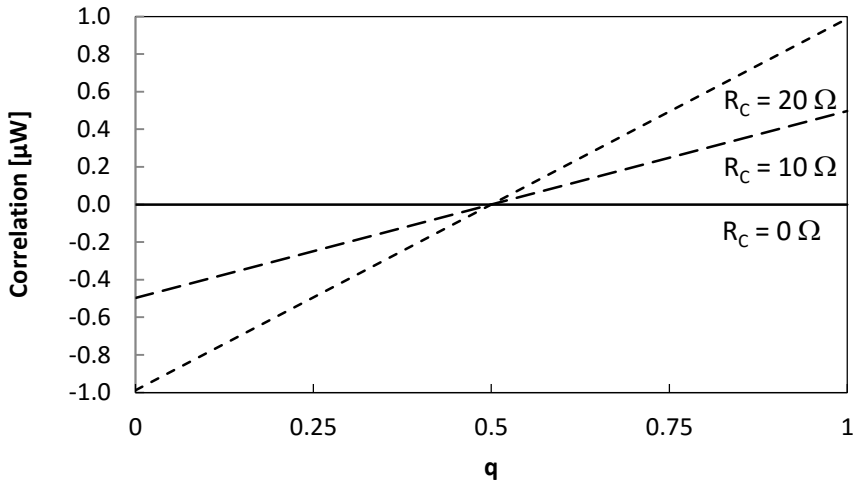


**Fig. 5** Correlation of the voltage $V_E$ and current $I_E$ as a function of the observation position $q$. Note that the correlation is the same for both the LH and HL states. The correlation is only zero at $q$=0.5. In this example the following values were used in (10): $R_L$=1 kΩ, $R_H$=9 kΩ, $V_{LA}$=$V_{LB}$=1 V. The used values of $R_C$ are indicated in the figure and $V_{HA}$ and $V_{HB}$ were calculated using (16) and (17).

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.

## Conclusion

In this paper we have investigated the security of KLJN system in its most general operating condition so far, when all four resistors can be different and the interconnecting cable can have arbitrary resistance. Our theoretical results show that the unconditional security can be maintained over the full extent of the communication line. Resistance tolerance, resistance temperature dependence, parasitic resistance of the switches, voltage generator source resistance and the cable resistance can all be compensated. Note that it is rather easy to monitor these quantities in real-time, therefore even continuous compensation can be performed. In this case the level of security is limited by the accuracy of the resistance measurement and the voltage amplitude tuning only. In our generalized case the thermal equilibrium is not needed any more, therefore the so called second law attack [11] is inherently prevented. The results can significantly advance realizations and practical applications in many fields [20-25]. Further information including open source simulation software and demonstrational videos can be found on our institutional pages [32].

## Acknowledgments

This research was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TÁMOP 4.2.4. A/2-11-1-2012-0001 'National Excellence Program'.

## References


1 C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing,* Bangalore, India, 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 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. ID 6461.

5 R. Mingesz, Z. Gingl, and L. B. Kish, “Johnson(-like)-noise–Kirchhoffloop 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.

6 P.-L. Liu, “A key agreement protocol using band-limited random signals and feedback,” *J. Lightwave Technol.*, vol. 27, no. 23, pp. 5230–5234, 2009.

7 A. Cho, “Simple noise may stymie spies without quantum weirdness,” *Science*, vol. 309, no. 5744, pp. 2148, 2005.

8 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.

9 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.

10 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.

11 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.

12 F. Hao, “Kish’s key exchange scheme is insecure,” *IEE Proc.-Inf. Secur.*, vol. 153, no. 4, pp. 141–142, 2006.

13 L. B. Kish, “Response to Feng Hao’s paper ‘‘Kish’s key exchange scheme is insecure’’,” *Fluct. Noise Lett.*, vol. 6, no. 4, pp. C37–C41, 2006.

14 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

15 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. ID e81810.

16 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.

17 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–Johnsonnoise (KLJN) secure key exchange system,” *Fluctuation Noise Lett.*, vol. 14, no. 1, 2015, Art. ID 1550011.

18 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, 2015.
19 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
20 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.
21 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. ID 70206.
22 L. B. Kish and C. Kwan, “Physical uncloneable function hardware keys utilizing Kirchhoff-Law-Johnson-Noise secure key exchange and noise-based logic,” *Fluct. Noise Lett.*, vol. **12**, no. 2, 2013, Art. ID 1350018.
23 L. B. Kish and O. Saidi, “Unconditionally secure computers, algorithms and hardware,” *Fluct. Noise Lett.*,” vol. 8, no. 2, pp. L95–L98, 2008.
24 Y. Saez, X. Cao, L. B. Kish, and G. Pesti, “Securing vehicle communication systems by the KLJN key exchange protocol,” *Fluct. Noise Lett.*, vol. 13, no. 3, 2014, Art. ID 14500205.
25 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
26 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. ID 13653.
27 L. B. Kish and C.-G. Granqvist. (2015). “Random-resistor-random-temperature KLJN key exchange.” [Online]. Available: http://arxiv.org/abs/1509.08150v2
28 R. Mingesz, “Experimental study of the Kirchhoff-Law-Johnson-Noise secure key exchange,” *Int. J. Mod. Phys. Conf. Ser.*, vol. 33, 2014, Art. ID 1460365.
29 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. ID 1450021.
30 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. ID 96109.
31 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.
32 Related simulations are available at www.noise.inf.u-szeged.hu/Research/kljn/