Type of the Paper (Article)

A Static-loop-current attack against the KLJN secure key exchange system

Mutaz Y. Melhem and Laszlo B. Kish *

Department of Electrical and Computer Engineering, Texas A & M University, 3128 TAMU, College Station, TX, 77843, USA; E-Mails: yar111@tamu.edu(MYM); Laszlo.Kish@ece.tamu.edu (L.B.K.)
* Correspondence: yar111@tamu.edu; Tel.: +1-708-776-367x6

Abstract: A new attack against the Kirchhoff-Law-Johnson-Noise (KLJN) key distribution system is introduced. The attack is based on 1) Utilizing the dc-voltage-source - which we put at Alice's end in our mathematical modeling of the attack-that could exist due to errors, imbalances, Electromagnetic interference and etc.2) On studying the number of samples per bit in the security key that the measured Alice/Bob voltages exceeds or falls below a threshold voltage, respectively. The threshold voltage is the average between dc voltages across low and high resistors- generated by a dc-voltage source. We count the number of samples the voltage at Bob's end (containing both the noise and dc components) exceeds the threshold voltage and how many times it falls below the threshold to judge whether the resistor can be guessed as low or high for every cycle. Also for a pre-specified key-length we count the number of high resistance estimations per bit –at Bob's end-according to the previous criterion and the non-successful estimations per bit to judge the final guessed resistor value at Alice's end and Bob's end, where if we have more bits with most of its measured samples are above the threshold voltage then we will predict Bob's resistance as high resistance, otherwise we predict Bob's resistance to be low resistance. The Simulation was conducted and the attack proved that it is successful unless the temperature increased dramatically to ranges more than a threshold temperature ~ 10^{10} Kelvin that increases when the number of samples per bit increases.

Keywords: Thermal-Noise; attack; sampling rate; Success Rate; simulation; Kirchoff—law-johnson-noise KLJN key distribution system; unconditional security;Measurement; evaluation ; correct guessing probability.

1. Introduction

1.1 Secure Communications

Communications systems, standards and technologies have been developed since ancient history. Today we have the internet, Internet-of-Things (IoT), the operating 4th generation wireless networks (LTE), and the expected 5th generation wireless networks. An important requirement of any communication paradigm between these devices is to accomplish the communication securely. That is, to protect the privacy of the users' data that is transferred over the network. To achieve the confidentiality of the transferred data that can contain sensitive information (e.g., bank account credentials, social security number, etc.) it is of utmost importance to defend against attacks. These

 doi:10.20944/preprints201806.0157.v1

attacks (i.e., eavesdropping, sniffing, man-in-the-middle (MitM), etc.) might be launched by malicious attackers that are located (topologically or physically) between the sender and receiver devices. Software based cryptography (SBC) emerged to assure inexpensive secure communications. SBC can be classified into two types, symmetric and asymmetric cryptography. Symmetric key exchange (that uses the same key for encrypting and decrypting data) was the most popular until W. Diffie and M.E. Hellman published their famous paper [1] with the concept of public-key cryptography (also known as asymmetric key cryptography[2]). Diffie and Hellman's publication pushed widespread scientific researches to generate a practical public-key encryption system, the goal was reached in 1978 when Ronald Rivest, Adi Shamir, and Len Adleman, introduced the RSA algorithm [3]. Such algorithms utilize computational complexity and achieve only conditional security. The system is temporarily secure if an adversary has limited computational resources. In order to achieve the unconditional security that is information-theoretic security, proper laws of physics and special hardware are utilized. Two major theorems were developed for unconditional security: 1) The Quantum key distribution (QKD) [4, 5], which is based on the Quantum no-cloning theorem. 2) The Kirchhoff's-law-Johnson-noise (KLJN) secure key distribution method, which is based on the fluctuation-distribution-theorem that satisfies the 2nd law of thermodynamics.

1.2 The KLJN Scheme:

The KLJN scheme is a statistical physical key distribution scheme [6-17]. The scheme has several advantages, for example, it can be integrated on a chip. The core model is composed of two identical pairs of resistors R_0 and R_1 at Alice's and Bob's ends, respectively, see Fig. 1. The noise generators associated with each resistor can be the thermal noise of the given resistor or an external noise generator. The power spectral density of voltage and current in the channel can be described by the following equations[11] :

$$S_u(f) = \frac{4kTR_A R_B}{R_A + R_B} \qquad (1)$$

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

Where k is Boltzmann's constant, T is temperature at thermal equilibrium, R_A and R_B are the operating resistance at Alice's and bob's ends, respectively. Equations (1) and (2) have two unknowns, so Eve can find the values of R_A & R_B but without knowing their locations. The values of R_A & R_B are either R_0 or R_1, R_0 is used to key bit 0 and R_1 is used to key bit 1 at either end. When $R_A \neq R_B$, Eve can identify the values of the resistors but without knowing which resistor is at Alice or Bob ends, which indicates the security of the system since she cannot identify the location of the resistor when 01 or 10 combinations are set in. But Eve can crack the 11 or 00 combinations. The KLJN system can be configured with an external noise generator with power spectral density $S_V(f)$=VR, where the V "temperature scaling" coefficient can be set to a large value to diminish the impact of background noise effects[11] . In the KLJN system all resistors - at both ends- have the same temperature or have the same coefficient to provide thermal equilibrium and as per the 2nd law of thermodynamics to guarantee zero net power-flow. Hence, Eve cannot use the power flow direction to crack the key. But how can Alice and Bob read the code? Using either equations (1) or

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2018 doi:10.20944/preprints201806.0157.v1

(2) they find the resistance at the other end, since each knows the value of the resistance at its end, so equations (1) and (2) are considered 1-variable equation for Alice and Bob.

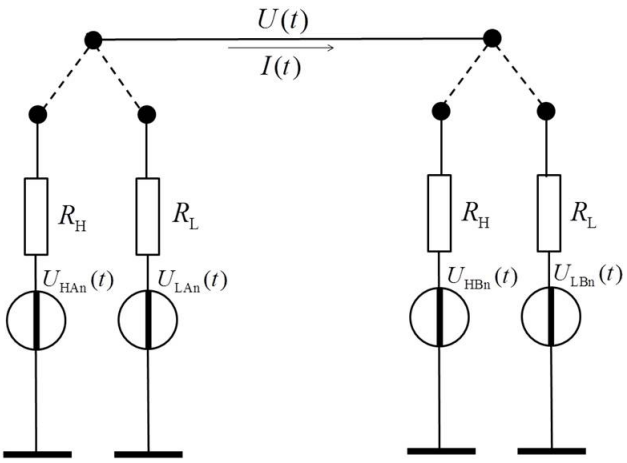

Figure 1. The KLJN System as first introduced in [18], where R_L is the low resistance that is used to key 0 and R_H is the high resistance that is used to key 1. While $U_{HAn}(t)$ & $U_{LAn}(t)$ and $U_{HBn}(t)$ & $U_{LBn}(t)$ are the noise sources generated by the high & the low resistances at either Alice's or Bob'sends, respectively. $U(t)$ and $I(t)$ are the Voltage and the current in the wire, respectively.

Since emergence of the KLJN scheme several attacking methods against the system were proposed, e.g. [8, 19], [20] which was refuted by [21], [10] which was refuted by [7, 14, 22] , and [23]. Bennet and Riedel challenged the security of KLJN and they published a paper [6] that claims that the KLJN protocols can be defeated by an adversary who is able to perfectly monitor the time-dependent fields in the region between Alice and Bob as electromagnetic theory would allow[13]. This attack neglected Nyquist's sampling theorem and it was refuted by [24]. F. Hao claimed in [25]that the temperature difference in the channel that would have exist in real communication systems will make the KLJN insecure, his argument was refuted in [26] due to the irrelevancy of the claims.
Several papers in the literature was published to prove the effectiveness and the accuracy of the KLJN system like [27]which proves the natural immunity of KLJN to man in the middle attacks, in [28] the KLJN was proved to have unconditional security against any type of non-ideality based attack..[29] Proves that the KLJN is also secure under the non-ideal situation when the wire between Alice and Bob has a resistance. The KLJN was proved to provide conditional security in ranges ten times more than the ranges of quantum communication channels [30].

Several papers was written to discuss further development of the system to enhance its security like [31],or it can be developed to count for certain types of attacks like [32], and [19] where a variable noise generator is used to eliminate second law attack. The KLJN was extended to build networks with high speed secure communications [9, 11].

2. The attack

2.1 The situation that Eve's utilizes to make the attack

The KLJN system [6, 7] assumes that each resistor is connected directly to the ground. In the real world there is often an imbalance, a DC or AC voltage difference between the end points of the resistors that are connected to the ground; for example due to ground loop or electromagnetic

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2018 doi:10.20944/preprints201806.0157.v1

interference (EMI) [7]. This potential information leak was mentioned [7] and showed to cause information leak in the case of significant cable resistance. However, the trickier situation when cable resistance is negligible has never analyzed in previous works and that situation requires a new statistical attack that is introduced in this paper.

In this paper, for the sake of simplicity, we assume that the imperfection is represented by a *positive* DC voltage generator located at Alice's end, see Fig.2. Due to Kerckhoff's principle of security, we must assume that Eve knows the polarity and value of this DC voltage. (If she does not know it at the beginning, she will be able to extract it by a long-time averaging). The direction of the current $I(t)$ is assumed to point from Alice to Bob. The voltage $U(t)$ on the wire contains the sum of a DC and an AC (stochastic) components.

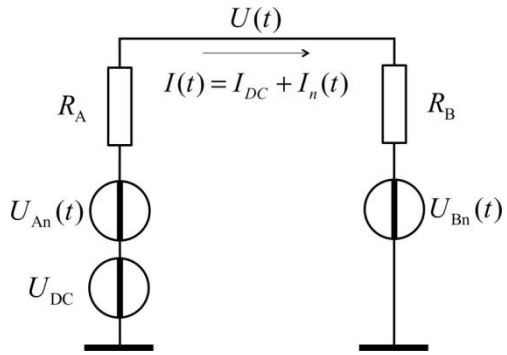

Figure 2. The KLJN system under study, where $U_{An} \in \{U_{LAn}; U_{HAn}\}$ and $U_{Bn} \in \{U_{LBn}; U_{HBn}\}$, are the noises belonging to the randomly chosen resistors, R_A and $R_B \in \{R_L; R_H\}$, of Alice and Bob, respectively, U_{dc} is the DC voltage source and $U(t)$ and $I(t)$ are the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

$$I_n(t) = \frac{U_{An}(t) - U_{Bn}(t)}{R_A + R_B}, \tag{5}$$

where U_{An} and $U_{Bn} \in \{U_{Ln}; U_{Hn}\}$, are the voltages of the noise generators are the Johnson noise sources of the randomly chosen resistors, R_A and $R_B \in \{R_L; R_H\}$, of Alice and Bob, respectively. The voltage on the wire is:

$$U(t) = I(t)R_B + U_{Bn}(t) \tag{6}$$

From Equations 5 and 8 we obtain

$$U(t) = U_{DCw} + U_{ACw}(t) = I_{DC}R_B + I_n(t)R_B + U_{Bn}(t) \tag{7}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2018 doi:10.20944/preprints201806.0157.v1

where U_{DCw} and $U_{\mathrm{ACw}}(t)$ represent the DC and AC voltage components in the wire, respectively. In general, 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 voltage and current in the wire have normal distribution since the addition of normally distributed signals result in a signal that has normal distribution with a corresponding mean (given by Equation 10) and variance.

The DC component is different during Alice's and Bob's LH and HL bit situations of secure bit exchange, which yields information leak. 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, as we have been assuming that in the given KLJN setup $R_{\mathrm{H}} > R_{\mathrm{L}}$, 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 threshold voltage, U_{th},

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

On the other hand, the corresponding AC (noise) component is the same in both the LH and HL cases:

$$U_{\mathrm{ACw}} = 4kT \frac{R_{\mathrm{L}} R_{\mathrm{H}}}{R_{\mathrm{L}} + R_{\mathrm{H}}} \tag{13}$$

where U_{ACw} means the effective noise voltage on the wire.

For an illustration, see Figure 3. The DC component, that is, the mean value of Gaussian depends on the bit situation during secure key exchange. This dependence pose as a source of information leak for Eve, and it will be exploited below for the new attack scheme.

2.2 The attack scheme

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

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2018 doi:10.20944/preprints201806.0157.v1

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}:

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

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

iii) *Guessing* (based on Equations 9-12): 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 by computer simulations.

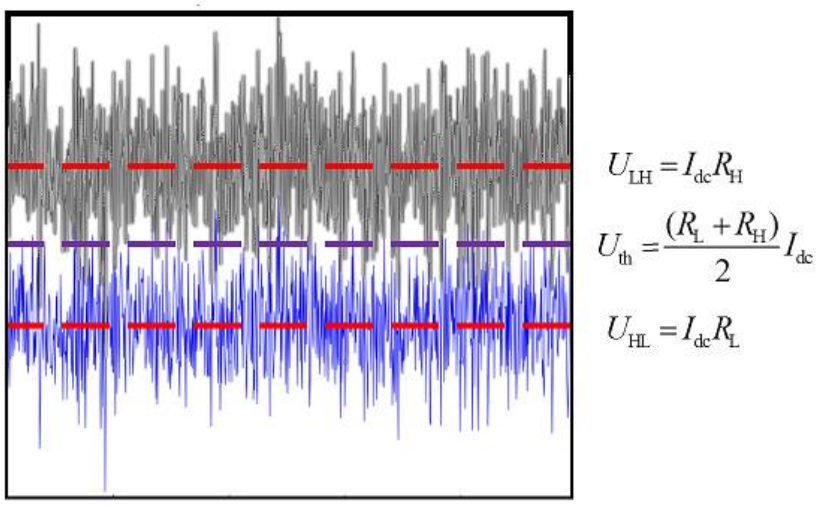

Figure 3. Eves' threshold scheme to guess the bit situation LH *vs* HL.

3. Simulation Results

We tested Eve's success probability *p* for the LH situation, see equation 9. 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 the noise, we used the white Gaussian noise function (wgn) from the communication system toolbox of Matlab [33] to test the success statistics of the attack scheme while varying the temperature. The effective bandwidth Δf and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2018 doi:10.20944/preprints201806.0157.v1

the range of temperatures were 1 MHz and $10^7 < T_{\text{eff}} < 10^{15}$ K, respectively. For lower temperatures p was 1 within the statistical inaccuracy of simulation. The duration of the *secure bit exchange period* was measured by the number N of *independent* noise samples used during the exchange of the particular bit[34] .

We carried out computer simulations with secure key length M =700 bits at different sampling rates N = 50, 100 and 200, respectively. Figure 4 shows Eve's probability p of successful guessing of a key bit vs temperature. With temperature approaching infinity, the effective noise voltage on the wire is also approaching infinity. That means, in the infinite temperature limit Gaussian density function will be symmetrically distributed around the threshold voltage U_{th} thus the probability of finding the noise amplitude above or below U_{th} is 0.5, which means Eve's probability of successful guessing of key bit represents the perfect security limit, $p = 0.5$.

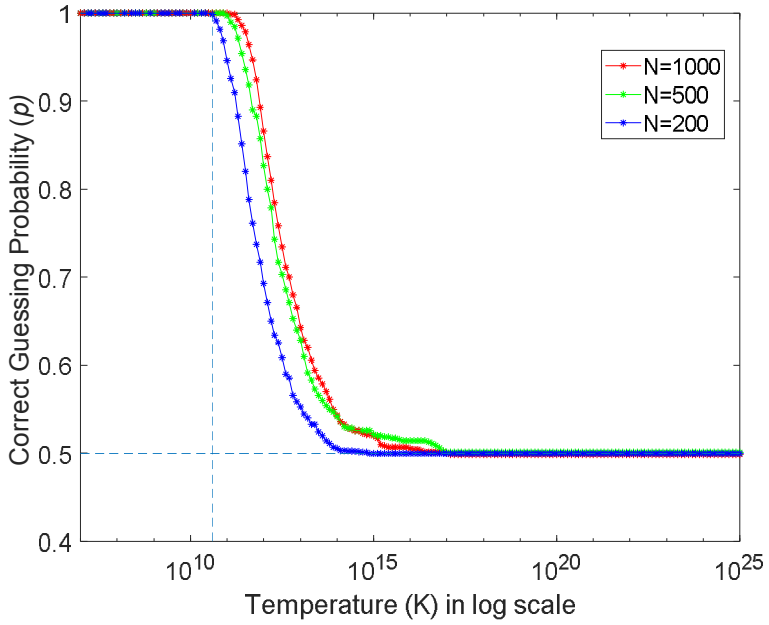

Figure 4. Eve's probability p of successful guessing of a key bit vs temperature at bandwidth Δf = 10^6 Hz, for key length 700 bits, and number of samples/bit 200, 500 and 100, respectively. p=0.5 stands for perfect security.

Of course, this dependence can simply interpreted by the behavior of the error function (see also Equations 8 and 12):

$$p\left\{U(t) \geq U_{\text{th}}\right\} = 0.5\left[1 - erf\left(\frac{U_{\text{th}} - U_{\text{DCw}}}{U_{\text{eff}}}\right)\right] \quad , \qquad (17)$$

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

 doi:10.20944/preprints201806.0157.v1

$$erf(x) = \frac{1}{\sqrt{\pi}} \int_{-x}^{x} \exp^{-y^2} dy \qquad (19)$$

The noise in the KLJN scheme is a bandlimited white noise thus, in accordance with the Johnson formula, the effective noise voltage U_{eff} is proportional to $\sqrt{T_{\text{eff}}\,\Delta f}$,

$$U_{\text{eff}} \propto \sqrt{T_{\text{eff}}\,\Delta f}\,. \qquad (20)$$

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

4. Some of the possible defense techniques against the attack

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

i) Cancelling the effect of the DC-Voltage sources. For example, Bob can put a variable DC source that compensates its effect. Also all measures for finding and eliminating ground loops should be applied to the circuit.

ii) Alice and Bob can increase the effective temperature T_{eff}, 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 [24]; this tool is strongly limited.

5. Conclusion

In this paper a novel attack against a KLJN scheme is shown that uses a practical non-ideal feature, namely the imbalance of voltages between ground points that typically occurs in connected electrical system. We showed that such parasite voltages and currents could cause information leak. Computer simulations demonstrated the attack and simple defense methods.

References

1. Diffie, Whitfield, and Martin Hellman. "New Directions in Cryptography." *IEEE transactions on Information Theory* 22, no. 6 (1976): 644-54.
2. Delfs, Hans, Helmut Knebl, and Helmut Knebl. *Introduction to Cryptography*. Vol. 2: Springer, 2002.
3. Agrawal, Vikas, Shruti Agrawal, and Rajesh Deshmukh. "Analysis and Review of Encryption and Decryption for Secure Communication." *International Journal of Scientific Engineering and Research (IJSER)* 2, no. 2 (2014).
4. Makarov, Vadim, Jean-Philippe Bourgoin, Poompong Chaiwongkhot, Mathieu Gagné, Thomas Jennewein, Sarah Kaiser, Raman Kashyap, Matthieu Legré, Carter Minshull, and Shihan Sajeed. "Laser Damage Creates Backdoors in Quantum Communications." *technology* 16 (2015): 22.
5. Renner, Renato. "Security of Quantum Key Distribution." *International Journal of Quantum Information* 6, no. 01 (2008): 1-127.
6. Bennett, Charles H, and C Jess Riedel. "On the Security of Key Distribution Based on Johnson-Nyquist Noise." *arXiv preprint arXiv:1303.7435* (2013).
7. Chen, Hsien-Pu, Laszlo B. Kish, Claes-Göran Granqvist, and Gabor Schmera. "Do Electromagnetic Waves Exist in a Short Cable at Low Frequencies? What Does Physics Say?" *Fluctuation and Noise Letters* 13, no. 02 (2014): 1450016.
8. Chen, Hsien-Pu, Muneer Mohammad, and Laszlo B. Kish. "Current Injection Attack against the KLJN Secure Key Exchange." *Metrology and Measurement Systems* 23, no. 2 (2016): 173-81.
9. Gonzalez, Elias. Information Theoretically Secure Enhanced Johnson Noise Based Key Distribution over the Smart Grid. Ph.D., 10291126, Texas A&M University, Ann Arbor, 2016.
10. Gunn, Lachlan J., Andrew Allison, and Derek Abbott. "A Directional Wave Measurement Attack against the Kish Key Distribution System." *Scientific reports* 4 (2014): 6461.
11. Kish, Laszlo B. "Totally Secure Classical Communication Utilizing Johnson (-Like) Noise and Kirchoff's Law." *Physics Letters A* 352, no. 3 (2006): 178-82.
12. Kish, Laszlo Bela. "Enhanced Secure Key Exchange Systems Based on the Johnson-Noise Scheme." *Metrology and Measurement Systems* 20, no. 2 (2013): 191-204.
13. Kish, Laszlo B. *The Kish Cypher: The Story of KLJN for Unconditional Security*: World Scientific, 2017.
14. Kish, Laszlo B., Zoltan Gingl, Robert Mingesz, Gergely Vadai, Janusz Smulko, and Claes-Göran 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 and Noise Letters* 14, no. 01 (2015): 1550011.
15. Kish, Laszlo B., and Claes G. Granqvist. "Random-Resistor-Random-Temperature Kirchhoff-Law-Johnson-Noise (Rrrt-KLJN) Key Exchange." *Metrology and Measurement Systems* 23, no. 1 (2016): 3-11.
16. Kish, Laszlo B., and Robert Mingesz. "Totally Secure Classical Networks with Multipoint Telecloning (Teleportation) of Classical Bits through Loops with Johnson-Like Noise." *Fluctuation and Noise Letters* 06, no. 02 (2006): C9-C21.
17. Mingesz, Robert. "Experimental Study of the Kirchhoff-Law-Johnson-Noise Secure Key Exchange."*International Journal of modern physics 33*, (2014):1-12.
18. Sutton, Roger J. *Secure Communications: Applications and Management*: John Wiley & Sons, 2002.

19. Kish, Laszlo B., and Claes-Göran 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* 16, no. 10 (2014): 5223-31.
20. Liu, Pao-Lo. "A New Look at the Classical Key Exchange System Based on Amplified Johnson Noise." *Physics Letters A* 373, no. 10 (2009): 901-04.
21. Kish, Laszlo B., and Tamas Horvath. "Notes on Recent Approaches Concerning the Kirchhoff-Law–Johnson-Noise-Based Secure Key Exchange." *Physics Letters A* 373, no. 32 (2009): 2858-68.
22. Chen, H.-P., Kish, L. B., Granqvist, C. G. & Schmera, G. "On the" Cracking" Experiments in Gunn, Allison, Abbott," a Directional Coupler Attack against the Kish Key Distribution System." Metrol. Meas. Syst. 21, 389–400 (2014)
23. Gunn, Lachlan J., Andrew Allison, and Derek Abbott. "A New Transient Attack on the Kish Key Distribution System." *IEEE Access* 3 (2015): 1640-48.
24. Kish, Laszlo B, Derek Abbott, and Claes G Granqvist. "Critical Analysis of the Bennett–Riedel Attack on Secure Cryptographic Key Distributions Via the Kirchhoff-Law–Johnson-Noise Scheme." *PLoS ONE* 8, no. 12 (2013): e81810.
25. Hao, Feng. "Kish's Key Exchange Scheme Is Insecure." *IEE Proceedings-Information Security* 153, no. 4 (2006): 141-42.
26. Kish, Laszlo B. "Response to Feng Hao's Paper" Kish's Key Exchange Scheme Is Insecure"." *Fluctuation and Noise Letters* 6, no. 04 (2006): C37-C41.
27. ———. "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* 6, no. 01 (2006): L57-L63.
28. Kish, Laszlo B., and Claes G. Granqvist. "On the Security of the Kirchhoff-Law–Johnson-Noise (KLJN) Communicator." *Quantum Information Processing* 13, no. 10 (2014): 2213-19.
29. Kish, Laszlo B, and Jacob Scheuer. "Noise in the Wire: The Real Impact of Wire Resistance for the Johnson (-Like) Noise Based Secure Communicator." *Physics Letters A* 374, no. 21 (2010): 2140-42.
30. Mingesz, Robert, Zoltan Gingl, and Laszlo B Kish. "Johnson (-Like)–Noise–Kirchhoff-Loop Based Secure Classical Communicator Characteristics, for Ranges of Two to Two Thousand Kilometers, Via Model-Line." *Physics Letters A* 372, no. 7 (2008): 978-84.
31. Smulko, Janusz. "Performance Analysis of the" Intelligent" Kirchhoff-Law–Johnson-Noise Secure Key Exchange." *Fluctuation and Noise Letters* 13, no. 03 (2014): 1450024.
32. Liu, Pao-Lo. "A Key Agreement Protocol Using Band-Limited Random Signals and Feedback." *Journal of Lightwave Technology* 27, no. 23 (2009): 5230-34.
33. https://www.mathworks.com/help/comm/ref/wgn.html
34. Saez, Yessica, and Laszlo B. Kish. "Errors and Their Mitigation at the Kirchhoff-Law-Johnson-Noise Secure Key Exchange." *PLoS ONE* 8, no. 11 (2013): e81103.