September 27, 2015.

RANDOM-RESISTOR-RANDOM-TEMPERATURE KLJN KEY EXCHANGE

Laszlo B. Kish [1], **Claes G. Granqvist** [2]

[1] *Texas A&M University, Department of Electrical and Computer Engineering, College Station, TX 77843-3128, USA*

[2] *Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, P.O. Box 534, SE-75121 Uppsala, Sweden*

Abstract

We introduce two new Kirchhoff-law–Johnson-noise (KLJN) secure key distribution schemes, which are the generalization of the original KLJN version. The first system, the Random-Resistor (RR-) KLJN scheme is using random resistors chosen from a quasi-continuum set of resistance values. It is well known since the creation of the KLJN concept that such system could work because Alice and Bob can calculate the unknown resistance value from measurements; however, it has not been addressed in publications as it was considered impractical. The reason for discussing it is the second scheme, the Random-Resistor-Random-Temperature (RRRT-) KLJN key exchanger inspired by a recent paper of Vadai-Mingesz-Gingl where security was maintained at non-zero power flow. In the RRRT-KLJN secure key exchanger scheme, both the resistances and their temperatures are continuum random variables. We prove that the security of the RRRT-KLJN system can be maintained at non-zero power flow thus the physical law guaranteeing the security is not the Second Law of Thermodynamics but the Fluctuation-Dissipation Theorem. Knowing their own resistance and temperature values, Alice and Bob can calculate the resistance and temperature values at the other end from the measured voltage, current and power-flow data in the wire. Eve cannot determine these values because, for her, there are 4 unknown quantities, while she can set up only 3 equations. The RRRT-KLJN scheme has several advantages and makes all the existing former attacks invalid or incomplete.

Keywords: KLJN key exchange; information theoretic security; unconditional security.

1. Introduction

The Kirchhoff-law–Johnson-noise (KLJN) secure key distribution [1-21] is a classical statistical physical alternative to the quantum key distribution. In the binary version of the scheme, see Figure 1, during a single bit exchange, the communicating parties (Alice and Bob) connect their randomly chosen resistor (including its Johnson noise generator) to a wire channel. These resistors are randomly selected from the publicly known set $\left\{R_{\mathrm{L}}, R_{\mathrm{H}}\right\}$, $R_{\mathrm{L}} \neq R_{\mathrm{H}}$, representing the low (*L*) and high (*H*) bit values. The Gaussian voltage noise generators—mimicking the Fluctuation-Dissipation Theorem and delivering band-limited white noise with publicly agreed bandwidth—produce enhanced thermal (Johnson) noise at a publicly agreed effective temperature T_{eff}, typically being $T_{\mathrm{eff}} >> 10^{10}\,\mathrm{K}$, so the temperature of the wire can be neglected. The noises are statistically independent of each other and from the noise of the former bit period.

In the case of secure bit exchange—*i.e.*, the *LH* or *HL* bit situations for Alice and Bob—an eavesdropper (Eve) cannot distinguish between these two situations by measuring the noise spectra $S_{\mathrm{u}}(f)$, $S_{\mathrm{i}}(f)$ of voltage and/or current in the cable, because the *LH* and *HL* noise levels are identical (degenerated). Thus when Alice and Bob detects the noise spectra (or noise levels) characteristic of the *LH* and *HL* situation, they know that the other party has the opposite bit and that this bit is secure. Then one of them will invert the bit (it is publicly pre-agreed who) to get the same key bit as the other party. The KLJN scheme offers unconditional (information theoretic) security at both ideal and slightly non-ideal (practical) conditions [3].

To avoid potential information leak by variations in the shape of a probability distribution, the noises are Gaussian [1], and it has been proven that other distributions cannot offer perfect security [18,19]. The security against active (invasive) attacks provided by the robustness of classical physical quantities, which guarantees that these quantities can be continuously monitored and exchanged between Alice and Bob via an authenticated communication. Therefore the system and data integrity with the known cable parameters and model can be checked *continuously* and *deterministically* without destroying the data, which is absolutely different from the case of quantum key distribution.

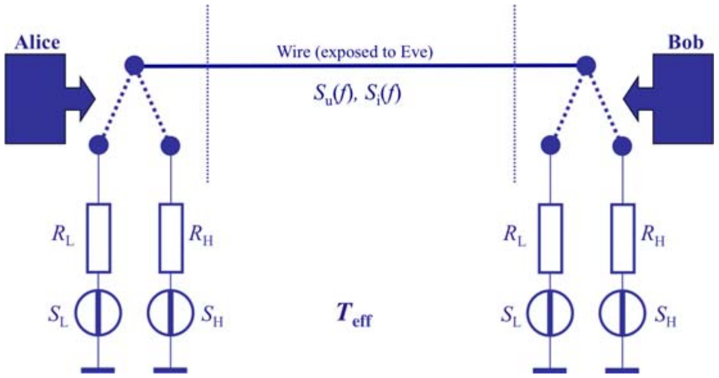

Fig. 1. The core of the KLJN scheme without the defense circuitry [2] against active (invasive) attacks and attacks utilizing non-idealities. The R_L and R_H resistors, identical pairs at Alice and Bob, represent the *Low* and *High* bit values. The corresponding noise spectra S_L and S_H also form identical pairs at the two ends however they belong to independent Gaussian stochastic processes. Both parties have the same temperature thus the net power flow is zero. The *LH* and *HL* bit situations of Alice and Bob produce identical voltage and current noise spectra, S_u and S_i, in the wire thus they represent a secure bit exchange. The *LL* and *HH* bit arrangements, which occur 50% of the cases, have singular noise levels in the wire thus they offer no security because Eve can distinguish them. Thus 50% of the bits must be discarded. This system works also with arbitrary, non-binary resistor values, too, as an analog circuitry to exchange continuum information about the distribution of random resistors, see the text below and in Sections 3,4.

We must keep in mind that the KLJN secure information exchanger is basically an analog circuitry and can work with arbitrary resistances because, even if the resistance values are not pre-agreed, Alice can calculate Bob's resistance from the measurement data [1] by using Johnson's formula and *vice versa*. For example, by using the measured current spectrum in the wire:

$$R_B = \frac{kT_{\mathrm{eff}}}{S_{\mathrm{i}}} - R_{\mathrm{A}} \tag{1}$$

It is important to note that Even Eve is able to determine an arbitrary, non-pre-agreed (non-publicly know) resistor pair connected to the line by using both the measured voltage and current spectra [1]. The two solutions of the obtained second order equation serve the two resistance values of the pair:

$$R_{1,2} = \frac{4kTS_u \pm \sqrt{\left(4kTS_u\right)^2 - 4S_u^3 S_i}}{2S_u S_i} \quad . \tag{2}$$

However, Eve cannot determine which resistor is with Alice and which is with Bob, thus the information exchange about the distribution of arbitrary, non-binary resistor values is secure in the original KLJN system, see also Section 3.

2. The Vadai-Mingesz-Gingl KLJN scheme

Resistor inaccuracies in the binary KLJN scheme can lead to remove the degeneration of the *LH* and HL noise levels in the line, leading to non-zero information leak, which was pointed out long time ago [response to Scheuer] and keeping inaccuracies at the 1 % range was recommended. Recently, Vadai-Mingesz-Gingl (VMG) published a modified KLJN scheme [20] with very interesting properties to fully eliminate such a leak. We call this the VMG-KLJN system. In a subsequent manuscript submitted for publication they also show [21] that the earlier temperature-compensation defense principle [17] against wire resistance attacks against the KLJN system can also successfully be used (with their new temperature-compensation functions) for the VMG-KLJN scheme, too.

We note by passing that the title of their paper [20] is misleading because it talks about "arbitrary" resistors indicating that as the main new result of the paper. However, the original KLJN scheme already had "arbitrary" resistors but not a random set of resistors, which the VMG-KLJN scheme cannot offer either. The really new aspect of the VMG-KLJN scheme is different, namely, that Alice and Bob can there have two *different* pairs of resistors consisting of R_{AL} , R_{AH} , R_{BL} , R_{BH} , which are Alice's and Bob's logic *Low* and *High* resistances, respectively, see Figure 2.

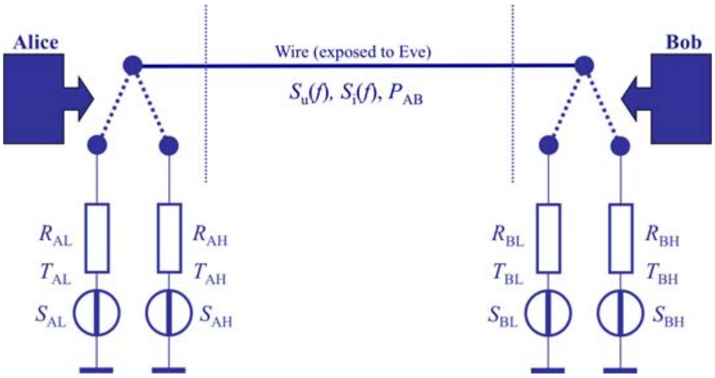

Fig. 2. The Vadai-Mingesz-Gingl KLJN scheme. The resistors pairs representing the *Low* and *High* bit values are different at Alice and Bob and their temperatures and the corresponding noise spectra are different too. Thus the net power flow is non-zero. The resistance values, R_{AL}, R_{AH}, R_{BL}, R_{BH} and their temperatures $T_{AL,}$ T_{AH}, T_{BL}, T_{BH} are pre-determined thus publicly known. This protocol is *not* desiged to work with *arbitrary*, non-binary resistor values to exchange continuum information about the distribution of random resistors because the temperatures are resistance values are interrelated and Alice and Bob cannot abruptly change them without changing the temperature(s) at the other party. For such system see the text at the end of Section 1 and in Sections 3 and 4.

Because the VMG-KLJN scheme is also binary, just like the original KLJN system, their task was to find conditions where the voltage and current noise spectra in the wire at the *HL* and *LH* bit combinations, that is for the pairs $R_{AL} - R_{BH}$ and $R_{AH} - R_{BL}$, are identical. This is not possible with uniform temperatures. From the temperature T_{AL} of Alice's R_{AL} resistor, the other temperatures, T_{AH}, T_{BL} and T_{BH}, are designed so, that the *LH* and *HL* bit situations produce identical voltage and current noise spectra and power-flow P_{AB} in the wire thus they represent a secure bit exchange. VMG found the necessary temperature values [20] in the following generic form:

$$T_{AH} = T_{AL} F\left(R_{AL}, R_{AH}, R_{BL}, R_{BH}\right) \tag{3}$$

$$T_{BL} = T_{AL} G\left(R_{AL}, R_{AH}, R_{BL}, R_{BH}\right) \tag{4}$$

$$T_{BH} = T_{AL} H\left(R_{AL}, R_{AH}, R_{BL}, R_{BH}\right), \tag{5}$$

where the *F*, *G* and *H* functions are *deterministic* (their concrete form are published in [20] and are not interesting here). Thus Alice and Bob *must know not only* their own set of resistors but also the resistance values at the other side and Bob must also know Alice's T_{AL} temperature. Thus, these resistor sets and temperatures are deterministic, which, in accordance with the Kerckhoffs's principle, implies that all these parameters are known by Eve. (Note, "keying" these parameter values by randomly generating and communicating them via secure communication by using the formerly shared key is of course possible, similarly to the Keyed-KLJN scheme [5], but such enhancements to make Eve's job more difficult are not the topic of the present paper).

The LL and HH bit arrangements, which occur 50% of the cases, have singular noise levels in the wire thus they offer no security because Eve can distinguish them, even though she knows all the temperature values and the values of resistance pairs at both ends. Thus 50% of the bits must be discarded so the VMG system does not offer a speedup of key exchange.

Concerning practical applications, in "macroscopic" circuit boards or hybrid integrated circuits of the original KLJN system, the resistors pairs can easily be chosen with sufficiently high-enough precision thus the VMG system is not needed. However, in monolith integrated circuits, if no post-processing for the trimming of the KLJN resistors is used, the VMG method can be handy to eliminate the information leak due to resistor inaccuracies [22,23].

However, in the VMG paper [20], there is a *historically important discovery*. It is the fact that they showed that *unconditional security could also be attained at non-zero power flow*, that is, at non-equilibrium conditions! That means, in their system, not the Second Law of Thermodynamics guarantees the security but the Fluctuation-Dissipation Theorem, via the Johnson-Nyquist formula (just as it was actually stated in the very first KLJN paper [1] with zero power flow; an argumentation that later switched to the more popular Second Law of Thermodynamics, which is also correct in that case).

3. The Random-Resistor (analog) KLJN scheme

Before we turn to our main results, first we outline the Random-Resistor (RR-) KLJN scheme, which is not binary but analog, see the final part of Section 1, and is still in thermal equilibrium. The RR-KLJN scheme is using random resistors chosen from a quasi-continuum set of resistance values. It is well-known since the creation of the KLJN concept that such system could work because Alice and Bob can calculate the unknown resistance value from measurements, however, it has not been addressed in publications, as it have been considered impractical.

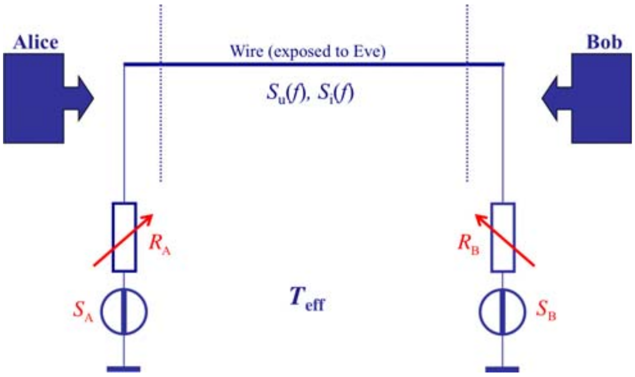

Fig. 3. The Random-Resistor KLJN scheme. The temperature at the two sides is the same and it is a pre-defined, publicly known constant value, thus the net power flow is zero. The resistors at Alice and Bob (and their corresponding voltage noise spectra) are continuum random variables with a new random choice at the beginning of each KLJN period. The *Low* and *High* bit values at Alice and Bob are determined by the relative resistance values, for example, that party has the high bit which has the higher resistance. From voltage and current measurements, Eve can also estimate the two resistance values but not their locations, unless the resistors are identical. In the hypothetical but non-practical case when the resistance distribution is ideally continuum and the inaccuracies of Alice's and Bob's estimation results are zero; 100% of the secure bit exchange is successful because the probability of choosing two identical resistances is zero. In the practical case with finite accuracy (finite bit exchange duration) and quasi-continuum discrete distribution, the secure bit exchange efficiency is less than 100%, because some of the bits must be discarded, but it is greater than 50%.

4. The Random-Resistor-Random-Temperature KLJN scheme

The important discovery by VMG [20] that unconditional perfect security exists at non-zero power flow is the very feature that inspires our new, Random-Resistor-Random-Temperature, RRRT-KLJN, see Figure 4. Yet, our new scheme is completely different from the VGA system because it is using really "arbitrary" (ad-hoc) random resistances like the RR-KLJN scheme moreover random temperatures (ad-hoc) from a continuum interval. Thus the forthcoming resistance and temperature values are unknown by even Alice and Bob (similarly to their lack of knowledge about the next secure key bit), except the ranges of values. Consequently, even the Kerckhoffs's principle does not allow information leak about them and only their continuum range is known publicly. This fact makes all formerly known attack types invalid in their original form and, without further development of them, they offer zero information gain about the key for Eve. This feature makes all formerly existing attacks invalid or, at minimum, incomplete.

3.1 Security proof of the RRRT-KLJN scheme

We analyze the protocol from Alice's point of view, which is naturally valid for Bob, too.

- Known for Alice: her own temperature, resistance, noise spectrum and the wire measurements of $S_u(f)$, $S_i(f)$ and the power P_{AB} flowing to Alice from Bob.
- Unknown for Alice: α and β.
- Known for Eve: the wire measurements of $S_u(f)$, $S_i(f)$ and P_{AB}.
- Unknown for Eve: α, β, T_A, R_A.

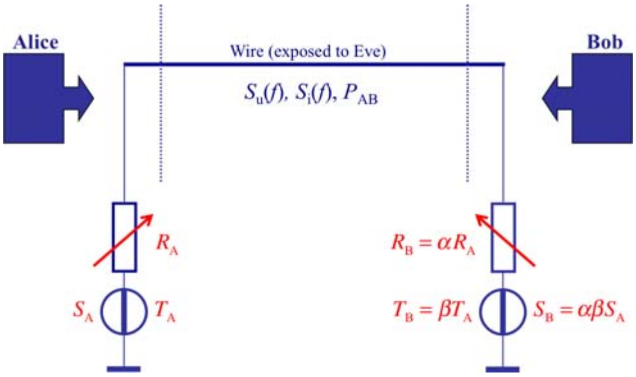
Alice
Wire (exposed to Eve)
Bob
$S_\mathrm{u}(f)$, $S_\mathrm{i}(f)$, P_AB
R_A
$R_\mathrm{B}=\alpha R_\mathrm{A}$
S_A
T_A
$T_\mathrm{B}=\beta T_\mathrm{A}$
$S_\mathrm{B}=\alpha\beta S_\mathrm{A}$

Fig. 4. The Random-Resistor-Random-Temperature KLJN scheme. The temperatures and the resistors at Alice and Bob (and their corresponding voltage noise spectra) are continuum random variables with a new random choice at the beginning of each KLJN period. The *Low* and *High* bit values at Alice and Bob are determined by the relative resistance values, for example, that party has the high bit which has the higher resistance. Known for Alice: her own temperature, resistance, noise spectrum and the wire measurements of $S_\mathrm{u}(f)$, $S_\mathrm{i}(f)$, and the power P_AB flowing to Alice from Bob. Unknown for Alice: α and β. Unknown for Eve: α, β, T_A, R_A. Known for Eve: the wire measurements of $S_\mathrm{u}(f)$, $S_\mathrm{i}(f)$ and P_AB. Eve cannot determine the two resistance values, not even their sum, like in the KLJN, VMG-KLJN and RR-KLJN cases. In the hypothetical but non-practical case when the resistance distribution is ideally continuum and the inaccuracies of Alice's and Bob's estimation results are zero; 100% of the secure bit exchange is successful. In the practical case with finite accuracy (finite bit exchange duration) and quasi-continuum discrete distribution, the secure bit exchange efficiency is less than 100%, because the bits with singular noise and power levels must be discarded, but 100% can be approached with proper design.

Alice wants to find out Bob's unknown parameters α and β. She can set up three equations by using the principles of liner operations on noise:

$$S_\mathrm{u}(f)=4kT_\mathrm{A}R_\mathrm{A}\left[\frac{\alpha R_\mathrm{A}}{R_\mathrm{A}(1+\alpha)}\right]^2+\alpha\beta 4kT_\mathrm{A}R_\mathrm{A}\left[\frac{R_\mathrm{A}}{R_\mathrm{A}(1+\alpha)}\right]^2=\frac{4kT_\mathrm{A}R_\mathrm{A}}{(1+\alpha)^2}\alpha(\alpha+\beta) \tag{6}$$

$$S_\mathrm{i}(f)=\frac{4kT_\mathrm{A}R_\mathrm{A}}{R_\mathrm{A}^2(1+\alpha)^2}+\frac{4kT_\mathrm{A}R_\mathrm{A}\alpha\beta}{R_\mathrm{A}^2(1+\alpha)^2}=\frac{4kT_\mathrm{A}}{R_\mathrm{A}}\frac{1+\alpha\beta}{(1+\alpha)^2} \tag{7}$$

and [17]:

$$P_\mathrm{AB}=\Delta f\frac{\alpha R_\mathrm{A}R_\mathrm{A}}{(R_\mathrm{A}+R_\mathrm{A}\alpha)^2}(\beta-1)4kT_\mathrm{A}=4kT_\mathrm{A}\Delta f\frac{\alpha(\beta-1)}{(1+\alpha)^2}\quad . \tag{8}$$

From Equation 6-8 we define three new quantities, which Alice can calculate from her own parameters and the measurement data:

$$\gamma=\frac{S_\mathrm{u}(f)}{4kT_\mathrm{A}R_\mathrm{A}}=\frac{\alpha(\alpha+\beta)}{(1+\alpha)^2} \tag{9}$$

$$\varphi=\frac{P_\mathrm{AB}}{4kT_\mathrm{A}\Delta f}=\frac{\alpha(\beta-1)}{(1+\alpha)^2} \tag{10}$$

$$\delta = \frac{S_{\mathrm{i}}(f)R_{\mathrm{A}}}{4kT_{\mathrm{A}}} = \frac{1+\alpha\beta}{(1+\alpha)^2} \tag{11}$$

In can be shown that Equations 9,10 lead to a second-order equation for β, which has two solutions:

$$\beta_{1,2} = \frac{-\delta(1-2\gamma)-\varphi\gamma \pm \sqrt{\left[\delta(1-2\gamma)+\varphi\gamma\right]^2 + 4(\gamma-1)(\delta-\varphi)(\varphi-\gamma\delta)}}{2(\gamma-1)} \quad , \tag{12}$$

In situations, when one solution is positive and the other one is negative, which is unphysical, the positive result gives Alice Bob's temperature value. When both solutions are positive, an alternative second order equation created from Equations 10,11 must be solved and the joint solution of that with that of Equation 12 yields the correct temperature parameter β of Bob. Finally, knowing the correct β value, anyone of Equations 9-11 yields Bob's resistance parameter α .

Eve cannot determine these values because, for her, there are 4 unknown quantities, while she can set up only 3 equations. Thus she has infinite possibilities provided the continuum system is unbounded, which is impractical.

In practical applications, the solution of the above equations will not be needed, when we consider the fact that the RRRT-KLJN system will be a digital one, similarly to the former realization. That means, the temperature and resistance data will form a quasi-continuum discrete set with resolution given by the bit resolution of the system. Thus, instead of the calculations outline above, a bottom-up version is much more feasible due to its reduced calculation need during operation: tabulation of all possibilities of temperature and resistor settings at Alice and Bob, and creating a lookup table from the $S_{\mathrm{u}}(f)$, $S_{\mathrm{i}}(f)$ and P_{AB} data.

Note: Such tabulation must be done in any case to locate possible singular $S_{\mathrm{u}}(f)$, $S_{\mathrm{i}}(f)$ and P_{AB} combinations that could uniquely tell Eve the resistance and temperature situations. The measurable set $S_{\mathrm{u}}(f)$, $S_{\mathrm{i}}(f)$ and P_{AB} for any secure bit must be degenerated thus must occur at least two opposite bit situations within the statistical inaccuracy of the KLJN operation, otherwise Eve can extract the bit by using her own model of the system, which she can build according to the Kerckhoffs's principle. Those singular shared bits are insecure and must be discarded during operation whenever they occur.

3.2 Immunity against former attacks

The RRRT-KLJN scheme has several advantages and makes all the existing formerly valid attacks invalid in their known form. For example, the key exchange speed is virtually doubled because, at proper design, almost each bit can exchange period supplies a secure key bit. Resistor or temperature inaccuracies do not matter and they cannot be utilized for Hao-type attacks [24], anymore. The Bergou-Scheuer-Yariv-Kish cable resistance attack [25,26] is also invalid in its known form, just like the new cable-capacitance attack by Chen, et al. [27]. Finally, the new transient attack [28] by Gunn-Allison-Abbott do not work either because of the unknown resistances and temperatures.

New attacks are of course possible. For example if Eve measure the voltages at the two ends of the wire, she gets a new equations thus she probably has enough equations to solve the problem. After that, information leak will exist and the real question is: how much with Eve's poor statistics due to the strongly limited bit exchange period?

3.3 Some practical considerations

A disadvantage of the RRRT-KLJN scheme is that the Kish-Granqvist temperature-compensation defense mechanism [17] cannot be used to nullify cable resistance effects against a yet unknown attack type of such kind (for an outline, see above). A perhaps more practical version of the RRRT-KLJN scheme is the generalization of the formerly proposed Multiple-KLJN (MKLJN) system [5] based on random choice of a known large set of resistors by introducing random choice of temperatures from a known large set of temperatures. As we have already mentioned above, the known sets must be properly checked because only choices with degenerated voltage/current/power values can be considered secure, not the singular values.

The bit error analysis [14,15] and error removal in the RRTT-KLJN scheme is yet and open problem.

Conclusions

We introduced two schemes with arbitrary (ad-hoc) random resistor choices and enhanced communication speed. The RRRT-KLJN scheme has also ad-hoc random temperatures, which makes this scheme unique among existing KLJN versions because even the sum of the resistances is secret. All the former attacks are invalid and, at minimum, need further developments to extract any information.

The RRRT system has some disadvantages, too, some advanced features of the enhanced KLJN schemes, such as the iKLJN improvement cannot be used and some of the defense features against active (invasive) attacks may need to be upgraded.

Only future can tell if the RRRT scheme stays as a peculiar academic interest or will became an important practical application. Both the generation of a random (analog) resistance and temperature looks technically feasible especially that accuracy and reproducibility of the resistance values is unimportant. There is no reason to use the RR-KLJN scheme because the RRRT system needs only a minor expansion form there.

It is yet an open question if the original KLJN system and its enhanced versions (iKLJN, KKLJN, VMG, etc.) or the RRRT-KLJN scheme are more feasible for practical applications, while they all offer unconditional (information theoretic) security.

Acknowledgements

Discussions with Zoltan Gingl are appreciated.

References

1. Kish LB (2006) Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law. Phys. Lett. A 352:178-182.
2. Kish LB (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:L57-L63
3. Kish LB, Granqvist CG (2014) On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator. Quantum Information Processing 13:2213-2219.
4. Mingesz R, Kish LB, Gingl Z (2008) Johnson(-like)-noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line. Phys. Lett. A 372:978–984.
5. Kish LB (2013) Enhanced secure key exchange systems based on the Johnson-noise scheme. Metrology & Measurement Systems 20:191–204.
6. Smulko J (2014) Performance analysis of the "intelligent" Kirchhoff's-law–Johnson-noise secure key exchange. Fluct. Noise Lett. 13:1450024.
7. Kish LB, Abbott D, Granqvist CG (2013) Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme. PLoS ONE 8:e81810/1–e81810/15.
8. Kish LB, Horvath T (2009) Notes on recent approaches concerning the Kirchhoff-law–Johnson-noise-based secure key exchange. Phys. Lett. A 373:2858–2868.
9. Mingesz, R, Kish, LB, Gingl Z, Granqvist CG, Wen H, Peper F, Eubanks T, Schmera G (2013) Unconditional security by the laws of classical physics. Metrology & Measurement Systems, 20:3–16
10. Kish LB, Gingl Z, Mingesz R, Vadai G, Smulko J, Granqvist CG (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. 14:1550011, DOI: 10.1142/S021947751550011X.
11. Chen HP, Kish LB, Granqvist CG, Schmera G. On the "cracking" scheme in the paper "A directional coupler attack against the Kish key distribution system" by Gunn, Allison and Abbott. Metrology and Measurement Systems 21:389–400, DOI:10.2478/mms-2014-0033.
12. Chen, H.P., Kish, L.B., Granqvist, C.G., Schmera, G. Do electromagnetic waves exist in a short cable at low frequencies? What does physics say? Fluctuation and Noise Letters 13 (2014) 1450016, DOI 10.1142/S0219477514500163.
13. Chen H-P, Kish LB, Granqvist CG, Schmera G (2014) Do electromagnetic waves exist in a short cable at low frequencies? What does physics say? Fluct. Noise Lett. 13:1450016 (1-13), http://arxiv.org/abs/1404.4664 , http://vixra.org/abs/1403.0964.
14. Saez Y, Kish LB (2013) Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange, PLoS ONE 8:e81103. DOI: 10.1371/journal.pone.0081103
15. Saez Y, Kish LB, Mingesz R, Gingl Z, Granqvist CG (2014) Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law-Johnson-noise secure key exchange. Journal of Computational Electronics 13:271–277.

16. Mingesz, R (2014) Experimental study of the Kirchhoff-Law-Johnson- Noise secure key exchange. Int. J. Mod. Phys. Conf. Ser. 33:1460365, DOI: 10.1142/S2010194514603652
17. Kish LB, Granqvist CG (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 16:5223-5231.
18. Gingl Z, Mingesz R (2014) Noise properties in the ideal Kirchhoff-law–Johnson-noise secure communication system. PLoS ONE 9:e96109/1–e96109/4. doi:10.1371/journal.pone.0096109.
19. Mingesz R, Vadai G, Gingl Z (2014) What kind of noise guarantees security for the Kirchhoff-loop–Johnson-noise key exchange? Fluct. Noise Lett., in press. http://arxiv.org/abs/1405.1196.
20. Vadai G, Mingesz R, Gingl Z (2015) Generalized Kirchhoff-Law- Johnson-Noise (KLJN) secure key exchange system using arbitrary resistors. Sci. Rep. 2015:13653, doi:10.1038/srep13653.
21. Vadai G, Gingl Z, Mingesz R (2015) Generalized attack protection in the Kirchhoff-Law-Johnson-Noise secure key exchanger. Submitted for publication.
22. Kish LB (2006) Response to Scheuer–Yariv: "A classical key-distribution system based on Johnson (like) noise—how secure?". Phys. Lett. A 359:741–744.
23. Kish LB (2006) Response to Feng Hao’s paper "Kish’s key exchange scheme is insecure". Fluct. Noise Lett. 6:C37-C41.
24. Hao F (2006) Kish’s key exchange scheme is insecure. IEE Proc. Inform. Soc. 153:141-142.
25. Kish LB, Scheuer J (2010) Noise in the wire: The real impact of wire resistance for the Johnson (-like) noise based secure communicator. Phys. Lett. A 374:2140–2142.
26. Scheuer J, Yariv A (2006) A classical key-distribution system based on Johnson (like) noise–How secure? Phys. Lett. A 359:737-740.
27. Chen HP, Gonzalez E, Saez J, Kish LB (2015) Cable Capacitance Attack against the KLJN Secure Key Exchange. Submitted for publication. http://vixra.org/abs/1508.0079 , http://arxiv.org/abs/1508.02984
28. Gunn LJ, Allison A, Abbott D (2014) A new transient attack on the Kish key distribution system. IEEE Access, in press, DOI: 10.1109/ACCESS.2015.2480422.