ON THE "CRACKING" SCHEME IN THE PAPER "A DIRECTIONAL COUPLER ATTACK AGAINST THE KISH KEY DISTRIBUTION SYSTEM" BY GUNN, ALLISON AND ABBOTT

Hsien-Pu Chen [1), Laszlo B. Kish [1), Claes-Göran Granqvist [2), G. Schmera [3)

[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*

[3) *Space and Naval Warfare Systems Center, San Diego, CA 92152, USA*

1. Introduction

Recently Gunn, Allison and Abbott (GAA) [1] proposed a new scheme to utilize electromagnetic waves for eavesdropping on the Kirchhoff-law–Johnson-noise (KLJN) secure key distribution. In a former paper [2], we proved that the wave claims in the GAA's attack are heavily unphysical, since the quasi-static limit holds for the KLJN scheme, implying that physical waves do not exist in the wire channel. The assumption of existing wave modes in the short cable at the low frequency limits violates a number of laws of physics including the Second Law of Thermodynamics. One aspect of the mistakes is that in electrical engineer jargon all oscillating and propagating time functions are called waves while in physics the corresponding retarded potentials can be wave-type of non-wave type. Physical waves involve two dual energy forms that are regenerating each other during the propagation, such as the electrical and magnetic fields are doing (similarly kinetic and potential energy in elastic waves); while non-wave-type retarded potential effects in the quasi-static regime, such as in KLJN, have negligible crosstalk between these energy forms and the energy exchange takes place between them and the generators [2].

We note in passing that, while there are no physical waves in the system, the propagation delay of the non-wave-type retarded potentials may still serve with information for Eve thus a correct analysis of the situation is essential.

The correct analysis based on impedances in the quasi static limit shows [2] that the starting (d'Alambert) equation

$$U(t,x) = U_+\left(t - \frac{x}{v}\right) + U_-\left(t + \frac{x}{v}\right) \qquad , \qquad (1)$$

which is the foundation of GAA's scheme is invalid because the system cannot be described with a single phase velocity [2] as these velocities depends on the directions during secure key exchange. Here U_+ and U_- are voltage components of waves propagating to the right and left along the *x*-axis and originating at the other end, and v is a *single* propagation velocity. From Eq. 1, GAA deduced the following equations as base of their "directional coupler" attack:

$$\frac{dU}{dt}+v\frac{dU}{dx}=2\frac{dU_+}{dt} \tag{2}$$

and

$$\frac{dU}{dt}-v\frac{dU}{dx}=2\frac{dU_-}{dt} \quad . \tag{3}$$

Their claim [1] is that the quantities at the left hand side of Eqs. 2,3 are measurable therefore the time derivatives at the right-hand side of the equations can be calculated and utilized for eavesdropping.

Before we analyze the experimental claims and potential artifacts, we take a closer look at the mathematics of Eqs. 1-3 by using the correct approach.

2. Mathematical analysis of the GAA scheme

In this section, we present the correct analysis of the GAA scheme and show that Eve's eavesdropped information is always less with the GAA scheme than with the old mean-square attack of comparing the two end-voltages [4] unless there are flaws in the realization of the KLJN key exchanger.

We assume in the rest of the paper that the bit value arrangement between Alice and Bob is mixed, that is, one of them connects the large resistance to the cable and the other one uses a small resistance. This situation indicates not only a secure key exchange event but also that different phase velocities must be used for the two directions in Eq. 1 during steady-state, see the related theory and verifications by simulation in our former paper [2].

2.1 General considerations

Even for waves, Eq.1 is not suitable for steady-state excitations [3] and the second term violates causality. However, there is a way to modify this equation under the steady-state KLJN conditions by using direction-dependent phase velocities [2] of these retarded potentials; and also the causality is fixed in the following way:

$$U(t,x)=U_+\left(t-\frac{x}{v_+}\right)+U_-\left(t-\frac{D-x}{v_-}\right) \quad , \tag{4}$$

where at the left end of the cable *x*=0 and at the right end *x*=*D* (thus *D* is the cable length). The phase velocities are

$$v_+=\frac{DR_B}{L_c} \quad \text{and} \quad v_-=\frac{DR_A}{L_c} \quad , \tag{5}$$

where R_A and R_B are the resistances of Alice and Bob and it is assumed that Alice is at the *x*=0 end while Bob is at the *x*=*D* end.

It is important to realize that, in accordance with Eqs. 4,5, to have the correct input for the GAA experiments, Eve must know the resistor values of Alice and Bob, consequently Eve's 1-bit uncertainty persist, which is the *indication* of security. For the *proof* of security, see Eq. 21 below.

Our earlier work [2] proved that, in the quasi-static frequency limit pertinent to the KLJN scheme, the exact distributed-impedance rendition of the cable shown in Figure 1 leads to the simplified serial impedance models in Figures 2a and 2b, because the capacitive currents converge to zero in the limit of low frequencies. Figure 2a is the first-order approximation of the real situation, while Figure 2b models a situation wherein the cable is lossless or the voltage drop on the resistive component is negligible compared to that of the inductive component (in the dominant frequency range of the quasi-static regime).

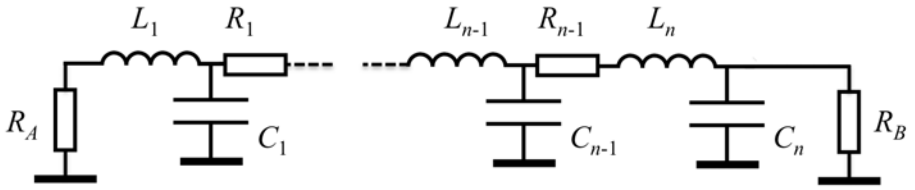

Figure 1. Outline of the pertinent part of the KLJN scheme with a distributed LCR model of a long and leakage-free cable [2]. When the cable losses can be neglected, one may omit the R_i resistors representing the distributed resistance of the cable. Alice's and Bob's resistors, denoted R_A and R_B, respectively, are randomly selected from the set $\{R_L, R_H\}$ with $(R_L \neq R_H)$ at the beginning of each bit-exchange period. These resistors, with associated serial generators (not shown), emulate thermal noise with high noise temperature and strongly limited bandwidth.

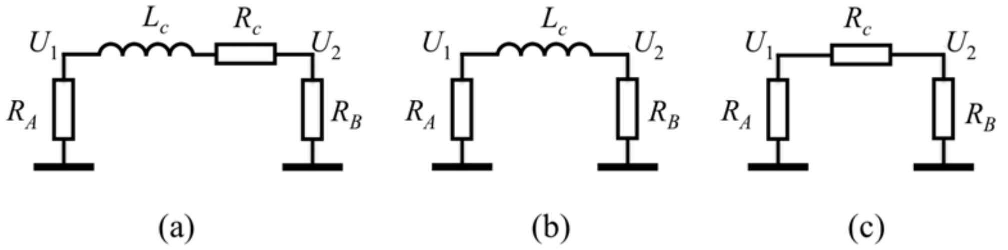

Figure 2. Lumped impedance-components-based model of the short cable [2] at low frequencies for analyzing voltage drop along the cable and phase shift in the quasi static limit. Part (a) represents a cable with loss (cable inductance and resistance are designated L_c and R_c, respectively), and part (b) represents a lossless cable. Part (c) is used to determine the voltage drop in the asymptotic case where loss dominates the cable impedance (this case is not practical and used only for the sake of analysis).

For the security analysis of the KLJN scheme, see Figure 3. U_A and U_B are the voltages of the noise voltage generators, and R_A and R_B are the resistors of Alice and Bob, respectively. U_1 and U_2 are the voltages at the two ends of the cable; U_{12}=U_1-U_2 (not shown); and Z_c is the cable impedance.

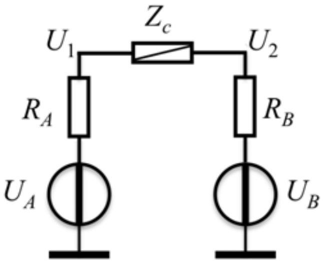

Figure 3. For the impedance-based analysis of the GAA attack. U_A and U_B are the voltages of the noise voltage generators, and R_A and R_B are the resistors of Alice and Bob, respectively. U_1 and U_2 are the voltages at the two ends of the cable; U_{12}=U_1-U_2; and Z_c is the cable impedance.

For the sake of security the voltage drop on the cable must be kept small compered to the other voltages [4] thus:

$$U_1 \cong U_2 \equiv U \quad . \tag{6}$$

However, in the former, wire resistance based attack [4], the miniscule differences between the mean-square voltages $\left\langle U_1^2 \right\rangle$ and $\left\langle U_2^2 \right\rangle$ served as information leak toward Eve. When the numbers of observed correlation times during bit exchange was N_{oc}=50, the wire resistance was 200 Ohm, R_A and R_B 2kOhm and 9kOhm, Eve's successful guessing probability p was p=0.525, which meant that the relative information leak was 0.19% of the exchanged key bits thus a 2-stage privacy amplification was needed [6] to reduce this leak below the desired 10^{-8} level. For this type of attack, at fixed N_{oc}, p scales as [7]:

$$p = 0.5 + \theta \frac{\left|Z_c\right|^2}{R_A R_B} \tag{7}$$

where θ is a constant (function only of N_{oc}). During the GAA experiments, $\left|Z_c\right|^2$ is about 10^5 times less while R_A and R_B have similar values (1kOhm and 10kOhm).

With the same N_{oc} and using the old method [4], Eve's probability of successful bit guessing would have been [6]:

$$p \approx 0.5000002 \quad , \tag{8}$$

which is better than even the p value (p=0.5006 [6]) needed to secure the 10^{-8} upper limit for the relative information leak.

Instead of that, GAA is claiming that by using their standard statistical method, they measure:

$$p \approx 1 \tag{9}$$

at these conditions. This is an extraordinarily strong claim, which basically means that, if it is true, GAA's method revolutionize mathematical statistics, moreover at these conditions Eve can do a nearly deterministic guess not only about the bit states but also the exact time dependence of the noise voltages of Alice and Bob.

2.2 Lossless short cable with very small impedance

Due to this situation, we assume that Eq. 6 holds however U_{12} is still measurable. Suppose, Eve is using Eq. 2 to extract the information. Then, by using the proper velocity, and the measurable quantities at the left-hand side of Eq. 2a, we get:

$$\frac{dU}{dt}+v_+\frac{dU}{dx}=2\frac{dU_x}{dt} \qquad (10)$$

where we want to clarify the meaning of the resulting $U_x(t)$ voltage in the right-hand side of Eq. 2a. After Fourier transforming Eq. 6, we obtain:

$$j\omega U(\omega)+v_+\frac{dU(\omega)}{dx}=2j\omega U_x(\omega) \qquad (11)$$

$$2U_x(\omega)=U(\omega)+\frac{v_+}{j\omega}\frac{dU(\omega)}{dx} \qquad (12)$$

$$2U_x(\omega)=U(\omega)+\frac{DR_B}{j\omega L_c}\frac{dU(\omega)}{dx}=U(\omega)+\frac{DR_B}{j\omega L_c}\frac{U_{12}(\omega)}{D} \quad , \qquad (13)$$

where $U_{12}(\omega)=U_1(\omega)-U_2(\omega)$.

Using Ohm's law for impedances, we obtain:

$$2U_x(\omega)=U(\omega)+R_B\frac{U_{1,2}(\omega)}{j\omega L_c}=U(\omega)+R_BI(\omega) \qquad (14)$$

The following relation, which is the Fourier transform of Eq 6, holds for the very small cable impedance case:

$$U(\omega)\cong U_1(\omega)\cong U_2(\omega) \qquad (15)$$

(c.f. Figure 3). Thus

$$2U_x(\omega)=U_2(\omega)+R_BI(\omega)=U_B(\omega) \qquad (16)$$

After inverse Fourier transformation and substituting the voltages back into Eq. 6, we obtain that the corrected Eq. 2a reads as:

$$\frac{dU}{dt}+v_+\frac{dU}{dx}=\frac{dU_B(t)}{dt} \qquad (17)$$

Similar considerations for GAA's other equation with the opposite sign of the second term lead to

$$\frac{dU}{dt} - v_{-}\frac{dU}{dx} = \frac{dU_A(t)}{dt} \tag{18}$$

The right hand side of Eqs. 17 and 18 give the voltages of Alice's and Bob's generators provided Eve uses the *correct guess* and consequently substitutes the *correct resistances* in these equations. This result proves that GAA does not have a directional coupler but something else, which can be called a “separator”, which is able to extract the voltage amplitudes of Alice's and Bob's voltage generators (without the voltage-division caused by the resistor at the other end). This situation would be even better for Eve however this works only if the correct phase velocity is assumed. Because the phase velocity in the steady state is determined by the unknown resistor terminating the cable toward the propagation direction [2], Eve must correctly guess the value of the resistor at that end in order to obtain the correct voltage.

What happens if Eve *assumes the wrong* value of resistor at Bob's side, that is, when Eve assumes the resistor value of Alice? Obviously, the resulting voltage $U_x(t)$ will be the weighted superposition of the voltages seen by Alice and Bob. However, the real question is: what will be its statistical properties? Can Eve utilize these to extract information? The answer is simple:

a) The voltage $U_x(t)$ will also be a Gaussian noise [12-14] because a linear combination of Gaussians results in a Gaussian due to the Central Limit Theorem. Thus the real question is its variance.

b) The variance calculation is also straightforward. Eq. 16 becomes:

$$2U_x(\omega) = U_2(\omega) + R_A I(\omega) \cong U_1(\omega) + R_A I(\omega) \tag{19}$$

It is important to realize that the cable voltage and current are orthogonal (uncorrelated) to ensure zero net power flow and satisfy the Second Law of Thermodynamics [7-11]:

$$\langle U(t)I(t)\rangle = 0 \tag{20}$$

. Thus in accordance with Pythagoras's rule, for the variance (mean-square) of the sum at the right-hand side of Eq. (19) is invariant to changing the plus sign to minus (see also Figure 4 for an illustration):

$$\langle U_x^2(t)\rangle = \langle U_1^2(t)\rangle + R_A^2\langle I^2(t)\rangle = \langle U_1^2(t)\rangle - R_A^2\langle I^2(t)\rangle \ \ , \tag{21}$$

which is exactly the variance of Alice's noise voltage in accordance with Kirchhoff's law (cf. Fig 3). Note, GAA is using the time derivatives however that does not change the situation of orthogonality.

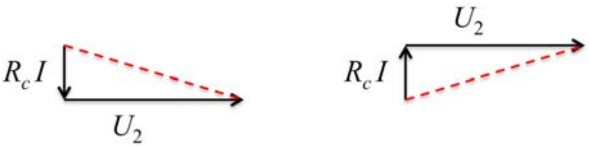

Figure 4. The added orthogonal noise voltages produce the same RMS voltage (and mean-square voltage) even if the sign of the current is flipped to the opposite value. The resulting time-dependent voltages will be completely different however their mean-square (and RMS) amplitude remains the same.

Thus the mean square voltages always correspond to that of the noise source of the assumed resistor: Eve gets what she expects instead of learning about the true bit situation. *It is important to realize that the only role of the inductance of the lossless cable is to detect the current in the wire. It should also be noted that "separators" of the same kind can be easily realized by directly measuring the current and using Ohm's law with guessed resistance values to determine the voltages at Alice's and Bob's ends*, see in [7] where we described such separators and called them "impedance-based directional couplers" and we pointed out that they are useless for Eve. The obtained mean-square voltages *satisfy* the *supposed* resistance value, and Eve cannot extract any information by using this system.

2.3 Short cable dominated by loss

For a *lossy cable*, the voltage drop on the resistor makes even the modified D'alambert-equation-approach (Eq. 4) invalid even if the correct phase velocity is used. Eqs. 12,13 become:

$$2U_x(\omega) = U(\omega) + \frac{v_+}{j\omega}\frac{U_{12}(\omega)}{D} = U(\omega) + \frac{DR_B}{j\omega L_c}\frac{U_{12}(\omega)}{D} = U(\omega) + \frac{R_B}{L_c}\frac{U_{12}(\omega)}{j\omega} \tag{22}$$

After inverse Fourier transformation it becomes:

$$2U_x(t) = U(t) + \frac{R_B}{L_c}\int U_{12}(t)dt \quad . \tag{23}$$

The obtained U_x does not have any meaning or information for Eve because $U(t)$ and the integral of the U_{12}(t) (which is proportional to the time integral of the current) are orthogonal even if the current and $U(t)$ have some small correlation due to the loss.

2.4 Conclusion of sections 2.2 and 2.3

As we have shown, Eve can extract no information either in the lossless cable or in the lossy cable provided Rel. 6 holds. However, Rel. 6 is only approximate because there is a non-zero difference (U_{12}) between U_1 and U_2. This small difference sets in a small offset into the related results and that is indeed and information for Eve.

However, this offset is the very same one, which have been utilized directly in the old wire resistance attack method [4] without the extra noise components shown above. The conclusion is straightforward: the GAA method provides always less information than the old wire resistance attack [4].

3. Experiments: What could go wrong?

Many things. Here we try to identify the most probable difficulties scientists not experienced with generating, manipulating and analysis noises may face. However, as an honor to the authors of [1] we suppose that elementary conceptual errors concerning the experiments, such as we have found with their theory in [1], are not present. From the many possibilities, we select only the few and only those that are related to the realization of KLJN, not to the measurement setup, which also offers plenty.

3.1 The experimental claim

GAA [1] used a standard statistical method to compare the distributions of the extracted voltage components and to identify the bit (resistor) arrangement at the two ends of the wire. They stated that they were able to identify the resistor arrangement within a very short time in the case of lossy cables.

Let us now estimate the observable relative difference of the mean-square voltages at the two ends in GAA’s experiment. The resistors were 1 kΩ and 10 kΩ and the cable length was 2 m. GAA did not specify their cable parameters, but at the 1.5 meter length assuming 1 mm^2 copper wire (a reasonable estimation) yields a corresponding cable resistance of 0.07 Ω.

As we have seen above, the old wire resistance attack [4] is an upper limit for the extracted information. Note, because the mean-square operation is an efficient estimator for Gaussian processes [12], other statistical method cannot offer much advantage. Using the result in [4] for the measurable relative mean-square voltage difference we get:

$$\Delta_{rel}^2 \approx \frac{\left|\left\langle U_1^2(t)\right\rangle - \left\langle U_2^2(t)\right\rangle\right|}{\left\langle U_1^2(t)\right\rangle} \approx \frac{\left|\left\langle U_1^2(t)\right\rangle - \left\langle U_2^2(t)\right\rangle\right|}{\left\langle U_2^2(t)\right\rangle} \approx \frac{R_c^2}{R_A R_B} = \frac{0.07}{10^3 10^4} = 7\text{x}10^{-9}$$

Thus the imbalance of the mean-square voltages of the two Gaussian noises is less than 10^{-8}. GAA’s claim to identify which one of these distributions is the narrower by sampling a few correlation times is untenable and normally hundreds of millions of correlation times would be required for a reasonably low error probability.

The question then arises as to what was GAA did measure and how they obtained their surprising results?

3.2 Non-Gaussianity: a potential for poor KLJN design

According to the security proofs in [13,14], it is a strict mathematical requirement for the KLJN security to have Gaussian processes, which means that the time derivatives must also be Gaussians. GAA does not provide the specifications of their waveform generator thus it is unclear how Gaussian the noise is. Most importantly commercial noise generators use algorithms and filtering to approach Gaussian. Due to the Central Limit Theorem, time-integration is shifting the statistics of noises toward Gaussian. Time derivatives, which GAA is using, strongly amplify non-Gaussian components.

Thus one of the strong candidate for the poor performance of GAA's KLJN system is non-Gaussianity of the time derivatives.

3.3 Aliasing effects, non-linearity, spurious noise components

Aliasing effects (which cause high-frequency non-Gaussian noises), non-linearity, and other type of spurious signals in the generator are strong candidates to destroy the Gaussianity. Again, the time derivative will again strongly emphasize these weakness.

3.3 Deterministic currents in the loop

Related by slightly different error if low-frequency or DC current component exist in the cable, such as one caused by a ground loop or DC offset. The voltage drop originating from such parasitic currents will introduce a location-dependent bias into the distributions and quickly uncover the natures of the resistors at the two ends of the wire, see Fig 5.

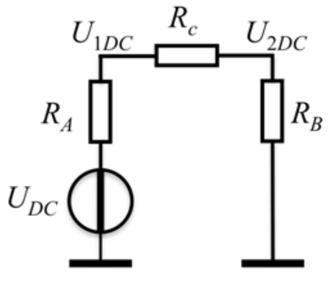

Figure 5. Illustration of parasite DC and low-frequency ground loop artifacts. For the sake of simplicity we assume that the parasite source exists only at Alice's side. We show only the parasite voltage generator because its impact is additive to the voltages obtained in the above analysis. The parasite (DC or low-frequency) components U_{1DC} and $U_{2\mathrm{DC}}$ of U_1 and U_2, respectively, is sensitive for the location of the low/high resistor choice at Alice's and Bob's side. See Fig. 5 for its impact.

However, Eve does not need to use GAA’s method [1] to elucidate the resistor values. She can simply measure and compare the DC or 50/60 Hz voltage components of the strongly correlated voltage noises at the two ends of the wire and extract the key or its inverse. Figure 6 shows computer simulations of two strongly correlated noises with a small DC shift, as an example. In this particular case, a single-time measurement is able to identify the DC voltage shift and uncover the key (or its inverse). If the DC shift is greater than the stochastic difference between the time functions then a single-time measurement is enough to distinguish the two noises and the bit situations in KLJN.

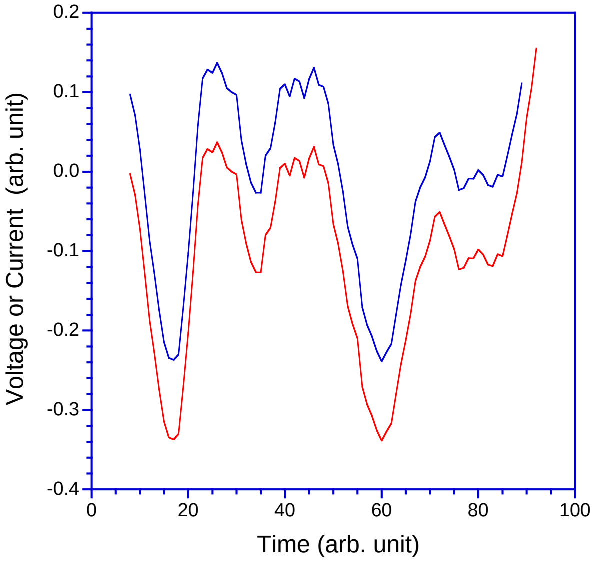

Figure 5. Computer generated illustration how a DC shift can distinguish two strongly correlated noises by using a comparison at a single moment of time.

For such situation GAA's finding that Eve's successful guessing probability is progressively increasing by increasing cable loss is also obvious. A lossless cable is represented by an inductance (see Figure 2b), which produces a voltage drop proportional to the time derivative of the current. That means zero DC voltage and zero shift between the distribution functions due to a parasitic DC current in the loop. This situation changes with cable loss where the a DC voltage shift will be present in accordance with Ohm's law due to the cable resistance R_c.

This effect will also strongly be enhanced by the time derivation of the channel voltage in GAA's scheme because the voltage drop on the cable is not time-derivated.

3.4 Conclusion about the experiments

It is important to note that—while GAA's approach [1] is invalid and their experimental results are caused by artifacts—a correct interpretation of their results is very enlightening because it shows that parasitic currents constitute very dangerous potential non-idealities in a practical KLJN system. The removal of such currents is straightforward, however, and can be accomplished by careful design, filters etc, while ignoring them can lead to the cracking of the key. To assure safe results, a well-defended KLJN system can execute spectral and statistical analysis on the noise in the cable to ascertain that these effects are not present.

Acknowledgements

Discussions with Janusz Smulko and Robert Nevels are appreciated.

References

1. Gunn LJ, Allison A, Abbott D (2014) A directional coupler attack against the Kish key distribution system. manuscript http://arxiv.org/abs/1402.2709 (2014) versions 1 and 2.
2. Chen HP, Kish LB, Granqvist CG, Schmera G (2014) Do electromagnetic waves exist in a short cable at low frequencies? What does physics say? Fluctuation and Noise Lett. accepted for publication (April 7, 2014), http://arxiv.org/abs/1404.4664 , http://vixra.org/abs/1403.0964.
3. Nevels RD. This flaw of GAA's [1] by misusing Eq. 1, which is valid only for pulses (instead of steady-state signals) was first pointed out by Dr. Nevels in private communications (3/2014).
4. 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.
5. 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.
6. Horvath T, Kish LB, Scheuer J (2011) Effective Privacy Amplification for Secure Classical Communications", EPL (formerly Europhys. Lett.) 94:28002-p1-p6.
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.
8. 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 XX:3–16. http://www.degruyter.com/view/j/mms.2013.20.issue-1/mms-2013-0001/mms-2013-0001.xml
9. Kish LB (2013) Enhanced secure key exchange systems based on the Johnson-noise scheme. Metrology & Measurement Systems XX:191–204. http://www.degruyter.com/view/j/mms.2013.20.issue-2/mms-2013-0017/mms-2013-0017.xml
10. 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.
11. Kish LB (2006) Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law. Phys. Lett. A 352:178-182.
12. Smulko J (2014) Performance analysis of the "intelligent" Kirchhoff's-law-Johnson-noise secure key exchange. Fluctuation and Noise Lett., in press.
13. Gingl Z, Mingesz R (2014) Noise properties in the ideal Kirchhoff-Law-Johnson-Noise secure communication system. PLoS ONE 9:e96109. doi:10.1371/journal.pone.0096109
14. Mingesz R, Vadai G, Gingl Z (2014) What kind of noise guarantees security for the Kirchhoff-loop-Johnson-noise key exchange? Fluctuation and Noise Lett. in press. http://arxiv.org/abs/1405.1196