Second version, submitted for publication, June 27, 2014. http://vixra.org/abs/1406.0124

Elimination of a Second-Law-attack, and all cable-resistance-based attacks, in the Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system

LASZLO B. KISH [1(a)] and CLAES G. GRANQVIST [2(b)]

[1] *Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843-3128, USA*
[2] *Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, P. O. Box 534, SE-75121 Uppsala, Sweden*

received and accepted dates provided by the publisher
other relevant dates provided by the publisher

PACS 72.70.+m – Noise processes and phenomena
PACS 89.20.Ff – Computer science and technology
PACS 89.90.+n – Other topics in areas of applied and interdisciplinary physics

Abstract – We introduce the so far most efficient attack against the Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system. This attack utilizes the lack of exact thermal equilibrium in practical applications and is based on cable resistance losses and the fact that the Second Law of Thermodynamics cannot provide full security when such losses are present. The new attack does not challenge the unconditional security of the KLJN scheme, but it puts more stringent demands on the security/privacy enhancing protocol than for any earlier attack. In this paper we present a simple defense protocol to fully eliminate this new attack by increasing the noise-temperature at the side of the smaller resistance value over the noise-temperature at the at the side with the greater resistance. It is shown that this simple protocol totally removes Eve's information not only for the new attack but also for the old Bergou-Scheuer-Yariv attack. The presently most efficient attacks against the KLJN scheme are thereby completely nullified.

Introduction. – The Kirchhoff-law–Johnson-noise (KLJN) scheme [1,2], shown in Figure 1, is a classical statistical physical competitor to a quantum key distribution for secure communication. For the duration of a single bit exchange, the communicating parties (Alice and Bob) connect their randomly chosen resistor and corresponding noise-voltage generator to a wire line (cable). These resistors are randomly selected from the publicly known set $\{R_\mathrm{L}, R_\mathrm{H}\}$, $R_\mathrm{L} \neq R_\mathrm{H}$, where the elements represent 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 $T_\mathrm{eff} \geq 10^9\,\mathrm{K}$ [3], 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 mean-square value of the voltage $U_c(t)$ and/or current $I_c(t)$ in the cable, because both arrangements lead to the same result. In the rest of the paper we assume that one of these secure bit exchange situations (either LH or HL) apply.

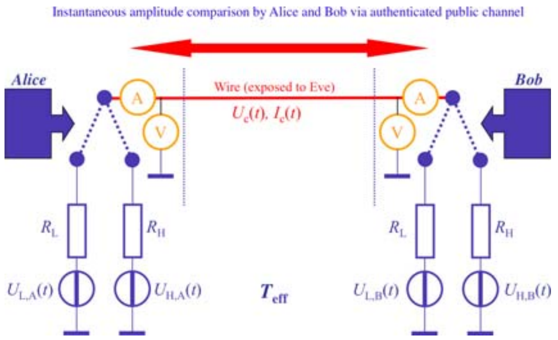

Figure 1. Schematic of the Kirchhoff-law–Johnson-noise secure key exchange system. To defend against active and hacking attacks, the cable parameters and integrity are randomly monitored; the instantaneous voltage $U_c(t)$ and current $I_c(t)$ amplitudes in the cable are measured and compared via public authenticated data exchange; and full spectral and statistical analysis/checking is carried out by Alice and Bob. R, t and T_eff denote resistance, time and effective temperature, respectively. Line filters, etc., are not shown.

To avoid potential information leak by variations in the

[(a)] E-mail: Laszlokish@tamu.edu
[(b)] E-mail: Claes-Goran.Granqvist@Angstrom.uu.se

shape of a probability distribution, the noises are Gaussian [1], and it has been proven that other distributions are not secure [4,5]. From a physics perspective, the security is provided by the Second Law of Thermodynamics because directional information, due to the direction of power flow, does not exist since the mean power flow is zero even though the LH and HL situations have asymmetric resistance arrangements [1]. In other words, the security of the *ideal* KLJN scheme against passive (non-invasive listening/measuring) attacks is as strong as the impossibility to build a perpetual motion machine of the second kind. The security against active (invasive) attacks is—perhaps surprisingly—provided by the robustness of classical physical quantities, which guarantees that these quantities can be monitored (and their integrity with the cable parameters and model can be checked) *continuously* without destroying their values. We observe, in passing, that the situation is totally different for the case of quantum physics.

The most famous and explored, and so far the most effective, attack against the *non-ideal* KLJN scheme is the Bergou-Scheuer-Yariv (BSY) cable resistance attack [6,7] which utilizes the fact that, due to the non-zero cable resistance, the mean-square voltage will be slightly less at the cable end with the smaller resistance value than at the other end with the greater resistance. It should be noted that the results (including their physical units) are wrong in Ref. [7], but a correct evaluation of the BSY effect was carried out later by Kish and Scheuer (KS) [8]. Eve's measured absolute difference between the mean-square voltages $\langle U_{\mathrm{cH}}^2(t)\rangle$ and $\langle U_{\mathrm{cL}}^2(t)\rangle$ of the "H" and "L" ends (*cf.* Figure 2) is given by [8]

$$\Delta_{\mathrm{KS}} = \left|\langle U_{\mathrm{cH}}^2(t)\rangle - \langle U_{\mathrm{cL}}^2(t)\rangle\right| = 4kT_{\mathrm{eff}}\Delta f \left|\frac{R_{\mathrm{c}}^2 (R_{\mathrm{H}} - R_{\mathrm{L}})}{(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}})^2}\right| , \quad (1)$$

where k is Boltzmann's constant, Δf is noise bandwidth and R_c is cable resistance. Clearly Δ_{KS} scales with the square of the cable resistance, *i.e.*, $\Delta_{\mathrm{KS}} \propto R_{\mathrm{c}}^2$.

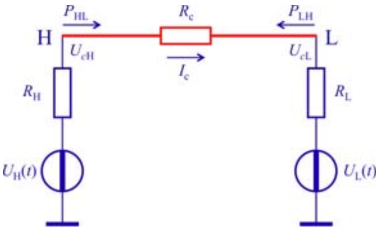

Figure 2. Scheme devised to illustrate the Bergou-Scheuer-Yariv attack and the Second-Law-attack. Alice's and Bob's locations are arbitrary in the figure. During the Second-Law-attack, the powers flowing out from the "H" and "L" ends of the cable are calculated and compared. The temperature of the cable resistor R_c can be neglected because of the high noise temperature of the generators. The notation is consistent with that in Figure 1.

The Second-Law-attack – In the rest of the paper we use the rules about transformations of noise spectra in linear systems, along with Johnson's formula for thermal noise, and write [1]

$$\langle U_{\mathrm{R}}^2(t)\rangle = 4kT_{\mathrm{eff}} R\Delta f \quad . \quad (2)$$

Here $\langle U_{\mathrm{R}}^2(t)\rangle$ denotes mean-square voltage fluctuations on the resistor, with resistance R, within the bandwidth Δf .

The cable resistance has a non-zero value, and therefore the resistors and their noise generators are not in thermal equilibrium in practical versions of the KLJN system (with T_{eff} much greater than the cable temperature). Consequently the Second Law of Thermodynamics cannot provide full security. The cable-heating powers by the generators at the "H" and "L" ends are different and are given by

$$P_{\mathrm{Hc}} = \langle I_{\mathrm{A}}^2(t)\rangle R_{\mathrm{c}} = \frac{4kT_{\mathrm{eff}} R_{\mathrm{H}} \Delta f}{(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}})^2} R_{\mathrm{c}} \quad , \quad (3)$$

and

$$P_{\mathrm{Lc}} = \langle I_{\mathrm{B}}^2(t)\rangle R_{\mathrm{w}} = \frac{4kT_{\mathrm{eff}} R_{\mathrm{L}} \Delta f}{(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}})^2} R_{\mathrm{c}} = P_{\mathrm{Hc}} \frac{R_{\mathrm{L}}}{R_{\mathrm{H}}} \quad . \quad (4)$$

The difference between P_{Hc} and P_{Lc} can be utilized for the Second-Law-attack, because the resistor values R_{H} and R_{L} are publicly known. The implementation of this attack is to measure and compare the net power flows at the two ends of the cable, as illustrated in Figure 2. The mean power flow P_{HL} from the "H" end toward the "L" end of the cable, and the mean power flow P_{LH} from the "L" end toward the "H" end are, respectively,

$$\begin{aligned} P_{\mathrm{HL}} &= \langle U_{\mathrm{H}}^2(t)\rangle \left(\frac{R_{\mathrm{c}} + R_{\mathrm{L}}}{R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}}}\right)^2 \frac{1}{R_{\mathrm{c}} + R_{\mathrm{L}}} \\ &\quad - \langle U_{\mathrm{L}}^2(t)\rangle \left(\frac{R_{\mathrm{H}}}{R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}}}\right)^2 \frac{1}{R_{\mathrm{H}}} \qquad (5) \\ &= 4kT_{\mathrm{eff}}\Delta f \frac{R_{\mathrm{H}}(R_{\mathrm{c}} + R_{\mathrm{L}}) - R_{\mathrm{L}} R_{\mathrm{H}}}{(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}})^2} = 4kT_{\mathrm{eff}}\Delta f \frac{R_{\mathrm{H}} R_{\mathrm{c}}}{(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}})^2} \end{aligned}$$

and

$$\begin{aligned} P_{\mathrm{LH}} &= \langle U_{\mathrm{L}}^2(t)\rangle \left(\frac{R_{\mathrm{c}} + R_{\mathrm{H}}}{R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}}}\right)^2 \frac{1}{R_{\mathrm{c}} + R_{\mathrm{H}}} \\ &\quad - \langle U_{\mathrm{H}}^2(t)\rangle \left(\frac{R_{\mathrm{L}}}{R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}}}\right)^2 \frac{1}{R_{\mathrm{L}}} \qquad (6) \\ &= 4kT_{\mathrm{eff}}\Delta f \frac{R_{\mathrm{L}}(R_{\mathrm{c}} + R_{\mathrm{H}}) - R_{\mathrm{H}} R_{\mathrm{L}}}{(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}})^2} = 4kT_{\mathrm{eff}}\Delta f \frac{R_{\mathrm{L}} R_{\mathrm{c}}}{(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}})^2} \end{aligned}$$

The power flows P_{HL} and P_{LH} are directly measurable by Eve, and their difference,

$$\Delta P_{\mathrm{HL}} = P_{\mathrm{HL}} - P_{\mathrm{LH}} = 4kT_{\mathrm{eff}}\Delta f \frac{R_{\mathrm{c}}(R_{\mathrm{H}} + R_{\mathrm{L}})}{(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}})^2} \quad , \quad (7)$$

gives the difference between the powers supplied by the two cable ends; with the measured cable voltages and current (see Figure 2) it is

$$\Delta P_{\mathrm{HL}} = P_{\mathrm{HL}} - P_{\mathrm{LH}} = \left\langle I_{\mathrm{c}}(t) U_{\mathrm{cH}}(t) \right\rangle - \left\langle -I_{\mathrm{c}}(t) U_{\mathrm{cL}}(t) \right\rangle \\ = \left\langle \left[U_{\mathrm{cH}}(t) + U_{\mathrm{cL}}(t) \right] I_{\mathrm{c}}(t) \right\rangle \quad . \qquad (8)$$

It should be observed that the opposite current sign at the “L” end expresses the fact that the current flowing *out* from the “H” end is flowing *into* the “L” end (using the same current sign would instead provide the power dissipated in the cable resistance, which is always positive and gives no directional information).

Suppose now that Eve measures the above current–voltage cross-correlations at the two ends and evaluates the pertinent quantities. With the notation introduced in Figure 3, one finds that

$$\Delta P_{\mathrm{AB}} = P_{\mathrm{AB}} - P_{\mathrm{BA}} = \left\langle \left[U_{\mathrm{cA}}(t) + U_{\mathrm{cB}}(t) \right] I_{\mathrm{c}}(t) \right\rangle \quad . \qquad (9)$$

As an example, suppose that R_{H} has the greater resistance value and R_{L} the smaller one, *i.e.*, $R_{\mathrm{L}} < R_{\mathrm{H}}$. In the *ideal* case, when $R_{\mathrm{c}} = 0$, one obtains $\Delta P_{\mathrm{AB}} = 0$ in accordance with the Second Law of Thermodynamics, which yields $\left\langle U_{\mathrm{c}}(t) I_{\mathrm{c}}(t) \right\rangle = 0$. However, in the *practical* case, with $R_{\mathrm{c}} > 0$, one finds

(*i*) if $\Delta P_{\mathrm{AB}} > 0$, then Alice has R_{H} and Bob has R_{L} ,

(*ii*) if $\Delta P_{\mathrm{AB}} < 0$, then Alice has R_{L} and Bob has R_{H} .

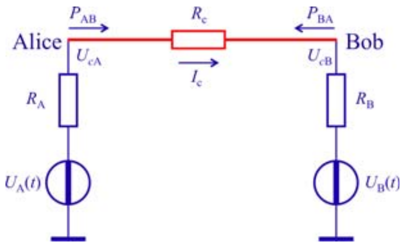

Figure 3. Eve’s measurements during the Second-Law-attack. The powers flowing out from the two ends of the cable are measured and compared. The notation is consistent with that in Figure 1.

The signal inherent in the Second-Law-attack scales linearly with R_{c} , which provides a much better situation for Eve—especially in the case of vanishing cable resistance—than the square-law scaling of the BSY attack. Moreover, it is also obvious that in a practical case [3,9,10], where $R_{\mathrm{c}} << R_{\mathrm{L}} << R_{\mathrm{H}}$, Eve’s signal-to-noise ratio is always greater in the Second-Law-attack than in the BSY attack. This is so because the BSY attack evaluates the dc fraction of $\approx R_{\mathrm{c}}^2 / \left(R_{\mathrm{L}} R_{\mathrm{H}} \right)$ in the measured (empirical) mean-square channel noise voltage, while the Second-Law-attack evaluates the dc fraction of $R_{\mathrm{c}} / R_{\mathrm{H}}$ in the measured mean power flow. It should be noted that the measured mean-square channel noise voltage, and the measured mean power flow, follow similar statistics because they are the time average of the products of Gaussian processes [11].

The Second-Law-attack is an elegant and efficient one, but it *does not challenge the unconditional security of the KLJN scheme* [2]. Eve’s probability *p* of successful guessing can arbitrarily approach the limit $p = 0.5$ by proper tuning of the parameters inherent in the KLJN scheme, such as resistances and bandwidth, and privacy amplification can be implemented if needed; this was evaluated in detail elsewhere [2], where relationships were reported between security level, cable parameters and communication speed. Nevertheless the new Second-Law-attack is important and may significantly increase the demands on parameter tuning and/or necessitate elaborate privacy amplification [12], which of course come at a cost.

In the rest of this paper we demonstrate two methods capable of fully eliminating the Second-Law attack. The advanced method nullifies the BSY attack as well.

Natural/“Simple” defense – Suppose it is possible to keep the cable and the resistors at the same temperature. This temperature-equilibration method virtually eliminates any Second-Law-attack information for Eve (but not the information in the BSY-attack, albeit its formula for the information leak is changed).

Temperature equilibration constitutes a very simple defense, but the cable temperature and its possible variations cannot be neglected any longer. If the cable temperature is different from that of the resistors, then the KLJN scheme is vulnerable to the Hao-type attack [13]. In principle, with cables of homogeneous temperatures, this attack can be avoided if Alice and Bob are able to monitor the temperature value of the cable by resistance and Johnson noise measurements, since they can then choose T_{eff} to be the same as the cable temperature. While these steps can be taken, the KLJN scheme is no longer simple. Moreover, the mentioned defense method may be unpractical because of the requirement of a homogeneous cable temperature, small noise levels, and since it prohibits the adoption of enhanced KLJN methods wherein Alice and Bob eliminate their own contributions in order to accomplish higher speed and security [9,14].

Advanced defense, also eliminating all cable resistance attacks – As we have seen, the cable end with the smaller resistance value emits less power toward the other end, and this is the foundation of the Second-Law-attack. This effect, as well as Eve’s related signal, can be completely eliminated by properly changing the *ratio* of the noise-temperatures of the generators for the resistors with the smaller and the greater resistance values (see Figure 4).

Suppose now that we introduce an offset in the noise-temperatures of the generators for the R_{H} and the R_{L} resistors so that the equation

$$\Delta P_{\mathrm{HL}} = P_{\mathrm{HL}}\left(T_{\mathrm{eff}}\right) - P_{\mathrm{LH}}\left(\beta T_{\mathrm{eff}}\right) = 0 \qquad (10)$$

holds, where T_{eff} is the noise temperature at the R_{H} resistors and βT_{eff} is the noise temperature of the R_{L} resistors. The solution of the equation is

$$\beta = \frac{1 + \frac{R_{\mathrm{c}}}{R_{\mathrm{L}}}}{1 + \frac{R_{\mathrm{c}}}{R_{\mathrm{H}}}} \quad . \qquad (11)$$

This value of β for the temperature-offset consequently eliminates Eve's opportunity to use the Second-Law-attack. One finds $\beta > 1$ for $R_{\mathrm{L}} < R_{\mathrm{H}}$ and $\beta < 1$ for $R_{\mathrm{H}} < R_{\mathrm{L}}$.

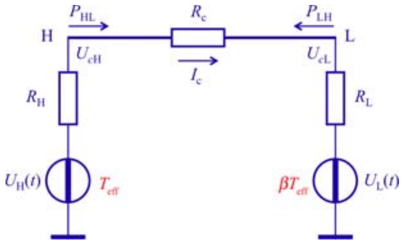

Figure 4. Schematic for illustrating the elimination of the Second-Law-attack and the BSY-attack by introduction of a proper temperature offset. The notation is consistent with that in Figure 1.

The remaining, essential question is whether the defense method delineated above introduces a higher signal for Eve's BSY-attack or not. Reevaluating the analysis of the BSY [8] with the a temperature offset given by Eq. 11, one obtains

$$\begin{aligned}\Delta_{\mathrm{KS}}\left(T_{\mathrm{eff}}, \beta T_{\mathrm{eff}}\right) &= \left|\left\langle U_{\mathrm{cH}}^2(t)\right\rangle - \left\langle U_{\mathrm{cL}}^2(t)\right\rangle\right| \\ &= 4kT_{\mathrm{eff}}\Delta f R_{\mathrm{H}}\left|\frac{R_{\mathrm{c}}^2\left(1-\alpha\beta\right) - \alpha R_{\mathrm{H}} R_{\mathrm{c}}\left(\beta - 1\right)}{\left(R_{\mathrm{H}} + R_{\mathrm{c}} + R_{\mathrm{L}}\right)^2}\right| \quad , \qquad (12)\end{aligned}$$

where $\alpha = \frac{R_{\mathrm{L}}}{R_{\mathrm{H}}}$. By substituting the above value for β , the nominator becomes zero so that

$$\Delta_{\mathrm{KS}}\left(T_{\mathrm{eff}}, \beta T_{\mathrm{eff}}\right) = \left|\left\langle U_{\mathrm{cH}}^2(t, T_{\mathrm{eff}})\right\rangle - \left\langle U_{\mathrm{cL}}^2(t, \beta T_{\mathrm{eff}})\right\rangle\right| = 0 \qquad (13)$$

Hence a modification of the noise temperature of the generators supplying the noise of the R_{L} resistors by the factor β yields a complete elimination the strongest attacks against the KLJN key exchange scheme, namely the Second-Law-attack and the BSY-attack [6–8].

Conclusions – We introduced the so far most efficient attack against the Kirchhoff-law–Johnson-noise (KLJN) secure key exchanger, *i.e.*, the Second-Law-attack. This attack utilizes the lack of exact thermal equilibrium in practical applications involving cables with non-zero resistance and results in more advantageous scaling and signal-to-noise ratio for Eve.

An advanced defense against this attack, involving a proper increase of the noise-temperature of the noise generator for the smaller resistances compared to that of the generators for the greater resistances surprisingly eliminated not only the Second-Law-attack but also the old Bergou-Scheuer-Yariv attack [6–8]. Removing these attacks can radically reduce Eve's fidelity while increasing Alice's and Bob's ones as a result of the potentially allowed longer bit-exchange periods or higher bandwidths [15].

Finally it should be emphasized that, in order to reduce the risk for hacking attacks or attacks due to possible malfunction, it is important not only to monitor and compare the voltage and current amplitudes at the two cable ends but also to run Gaussianity, spectral and other proper statistical checks on the signals, and to monitor the cable transfer function and signal integrity against hacking.

REFERENCES

[1] KISH L. B., *Phys. Lett. A* **352** (2006) 178–182.

[2] KISH L. B. and GRANQVIST C. G., *Quantum Inf. Process.*, (2014), in press, DOI: 10.1007/s11128-014-0729-7.

[3] MINGESZ R., GINGL Z. and KISH L. B., *Phys. Lett. A*, **372** (2008) 978–984.

[4] GINGL Z. and MINGESZ R., *PLoS ONE*, **9** (2014) e96109.

[5] MINGESZ R., VADAI G. and GINGL Z., *Fluct. Noise Lett.* (2014), in press, *arXiv*:1405.1196.

[6] BERGOU J., interviewed in: CHO A., *Science* **309** (2005) 2148.

[7] SCHEUER J. and YARIV A., *Phys. Lett. A*, **359** (2006) 737–740.

[8] KISH L. B. and SCHEUER J., *Phys. Lett. A*, **374** (2010) 2140–2142.

[9] KISH L. B., *Metrol. Meas. Syst.*, **20** (2013) 191–204. DOI: 10.2478/mms-2013-0017.

[10] MINGESZ R., KISH L. B., GINGL Z., GRANQVIST C. G., WEN H., PEPER F., EUBANKS T. and SCHMERA G., *Metrol. Meas. Syst.* **20** (2013) 3–16. DOI: 10.2478/mms-2013-0001 .

[11] KISH L. B., MINGESZ R., GINGL Z. and GRANQVIST C. G., *Metrol. Meas. Syst.* **19** (2012) 653–658.

[12] HORVATH T., KISH L. B. and SCHEUER J., *EPL* **94** (2011) 28002.

[13] HAO F., *IEE Proc. Inform. Soc.* **153** (2006) 141–142.

[14] SMULKO J., *Fluct. Noise Lett.* (2014), in press.

[15] SAEZ Y., KISH L. B., MINGESZ R., GINGL Z. and GRANQVIST C. G., *J. Comput. Electron.* **13** (2014) 271–277.