First version, June 19, 2014. http://vixra.org/abs/1406.0124

Second-law-attack, and eliminating all cable resistance attacks in the Johnson noise based secure scheme

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, SE-75121 Uppsala, Sweden*

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 exchanger. The attack utilizes the lack of exact thermal equilibrium at practical applications due to the cable resistance loss. Thus the Second Law of Thermodynamics cannot provide full security. While the new attack does not challenge the unconditional security of the KLJN scheme, due to its more favorable properties for Eve, it requires higher requirements for the security/privacy enhancing protocol than any earlier versions. We create a simple defense protocol to fully eliminate this attack by increasing the noise-temperature at the side of the lower resistance value. We show that, this simple defense protocol totally eliminates Eve's information not only in this but also in the old (Bergou)-Scheuer-Yariv attack. Thus the so far most efficient attack methods become useless against the KLJN scheme.

Introduction. – The Kirchhoff-law-Johnson-noise (KLJN) scheme [1,2], see Figure 1, is a classical statistical physical competitor of quantum key distribution. For the duration of a single bit exchange, Alice and Bob connect their randomly chosen resistor and the corresponding noise voltage generator to the wire line (cable). These resistors are randomly selected from the publicly known set $\{R_L, R_H\}$, $R_L \neq R_H$, where the elements represent the "Low" and "High" bit values. The Gaussian voltage noise generators—imitating the Fluctuation-Dissipation Theorem and delivering band-limited white noise with publicly agreed bandwidth—represent enhanced thermal (Johnson) noise at a publicly agreed effective temperature T_{eff} (typically $T_{eff} \geq 10^9\,\mathrm{K}$ [3] so the temperature of the wire can be neglected). Their noises are statistically independent from 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 situation of Alice/Bob), the eavesdropper (Eve) cannot distinguish between the LH and HL 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. During the rest of the paper we assume the presence of one of these secure bit exchange (LH or HL) situations.

To avoid potential information leak by variations of the shape of probability distribution, the noises are Gaussian [1] and it has been proven that other distributions are not secure [4,5]. The security at the physics side is physically provided by the Second Law of Thermodynamics because the directional information due to the direction of power flow is nonexistent as the mean power flow is zero even though the LH and HL situations have asymmetric resistance arrangement [1].

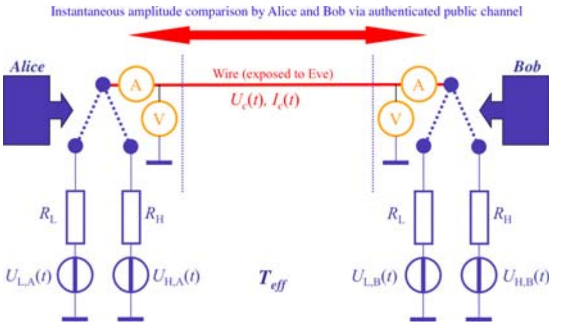

Figure 1. Schematic of the Kirchhoff-law–Johnson-noise secure key exchange system. To defend against active and hacking attacks, the cable parameters and integrity are randomly monitored; the instantaneous voltage $U_c(t)$ and current $I_c(t)$ amplitudes in the cable are measured and compared via a public 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., the

In other words, the security of the *ideal* scheme against passive (non-invasive listening/measuring) attacks is as strong as

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

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* (see Figure 1) without destroying their values (which is totally different for the case of quantum physics).

The most famous/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 lower resistor value ("High" end) than at the other end ("Low" end) of the cable. Note, the results (including their physical units) in [7] are incorrect and the correct evaluation of the BSY effect was carried out later by Kish and Scheuer (KS) [8]. Eve's measured difference between the mean-square voltages $\left\langle U_{\mathrm{cH}}^2(t)\right\rangle$ and $\left\langle U_{\mathrm{cL}}^2(t)\right\rangle$ of the "High" and "Low" ends is [8] given as:

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

where k is the Boltzmann constant and Δf is the noise bandwidth. Observe that Δ_{KS} scales with the square of the cable resistance, $\Delta_{\mathrm{KS}} \propto R_{\mathrm{c}}^2$.

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

$$\left\langle U_{\mathrm{R}}^2(t)\right\rangle = 4kT_{\mathrm{eff}}R\Delta f \ , \qquad (2)$$

where $\left\langle U_{\mathrm{R}}^2(t)\right\rangle$ and $\left\langle I_{\mathrm{R}}^2(t)\right\rangle$ are the mean-square voltage and current fluctuations on the resistor of resistance R within the Δf bandwidth.

Due to the non-zero cable resistance, the resistors and their noise generators in the practical/advanced versions of the KLJN system (with T_{eff} much greater than the cable temperature) are not in thermal equilibrium with each other thus the Second Law cannot provide full security. The cable-heating powers by the generators at "High" and "Low" ends are different, see Figure 2:

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

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

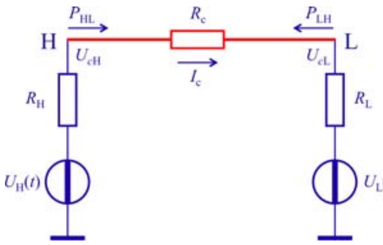

Figure 2. For the derivation of the Second-Law-attack. The powers flowing out from the "H" and "L" ends of the cable are calculated and compared. The temperature of the cable resistance can be neglected due to the high noise temperature of the generators.

This fact can be utilized for the Second-Law-attack because the resistor values R_{H} and R_{L} are publicly known. The simplest method is to measure and compare the measured mean power at the two ends of the cable. The mean power flow P_{HL} from the "High" end toward the "Low" end of the cable and the mean power flow P_{LH} from the "Low" end toward the "High" end are:

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

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

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

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

shows the difference between the powers supplied by the two cable ends. With the measured cable voltages and current, it is:

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

Observe: the opposite current sign at the L end is expressing 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, with no directional information).

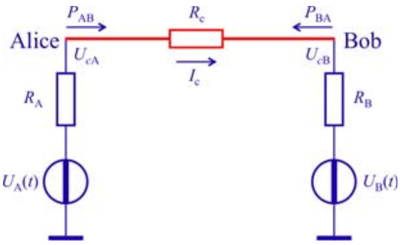

Figure 3. Eve's measurements during the Second-Law-attack. The powers flowing out from the "H" and "L" ends of the cable are measured and compared.

Suppose that $R_{\mathrm{H}} > R_{\mathrm{L}}$ and Eve is measuring the above current-voltage crosscorrelations at Alice's and Bob's end and evaluates the quantity, see Figure 3:

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

In the ideal case, when $R_{\mathrm{c}} = 0$, also $\Delta P_{\mathrm{AB}} = 0$, in accordance with the Second Law. However, in the practical case, $R_{\mathrm{c}} > 0$. Then,

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} .

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

While the Second-Law-attack is the existing most efficient scheme based on the non-zero wire resistance, it does not challenge the unconditional security of the KLJN scheme [2]. Eve's probability p of successful guessing can arbitrarily approach the $p = 0.5$ limit with the proper tuning of the KLJN parameters (resistances, bandwidth, privacy amplification), see [2] for details and for the related costs such as cable and speed). However this new attack may significantly increase the related costs and/or privacy amplification requirements [12] thus efficient defense methods are important. In the rest of the paper we show two such methods where the advanced version fully eliminates the BSY attack, too.

Natural/"Simple" defense – Suppose, the cable and the resistors have the same temperature. This method virtually eliminates any Second-Law-attack information for Eve (but not the BSY-attack information, though its evaluation formula changes). This is a very simple defense however the cable temperature and its possible variations cannot be neglected anymore. In such case, if the cable temperature is different, the KLJN system is vulnerable to the Hao-attack [13]. To avoid that, Alice and Bob can monitor the temperature value of the cable by resistance and Johnson noise measurements on the cable. Then they can choose T_{eff} to be the same as the cable temperature. While these steps are doable, this is not a simple method anymore. Moreover, this defense method is not too practical because of the small noise levels and because it prohibits using the enhanced KLJN methods where Alice and Bob eliminate their own contribution for higher speed and security [9,14].

Advanced: Eliminating all cable resistance attacks – As we have seen, the "Low" cable end with lower resistance value emits less power toward the other end and this is the foundation of the Second-Law-attack. This effect and Eve's related signal can fully be eliminated by properly increasing the noise temperature of the generators of the R_{L} resistors of Alice and Bob. The solution of the equation

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

where T_{eff} is the noise temperature at the "High" end and βT_{eff} is the noise temperature at the "Low" end, is:

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

Thus the above β value eliminates Eve's opportunity to use the Second-Law-attack. For $R_\mathrm{L} < R_\mathrm{H}$, $1 < \beta$.

The remaining but essential question is whether, by using this defense method, we introduce a higher signal for Eve's BSY attack, or not. Reevaluating Eqs. (6-9) in [8] results in the following equation instead of their Eq. 10:

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

where $\alpha = \dfrac{R_\mathrm{L}}{R_\mathrm{H}}$. Substituting the above value for β, the nominator becomes zero thus:

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

In conclusion, increasing the noise temperature of the generators supplying the noise of the R_L resistors by the factor of β completely eliminates the strongest attacks against the KLJN key exchange: the Second-Law-attack and the BSY-attack [6-8].

Conclusions – We have introduced the so far most efficient attack against the Kirchhoff-law-Johnson-noise (KLJN) secure key exchanger: the Second-Law-attack. The attack utilizes the lack of exact thermal equilibrium at practical applications due to the cable resistance loss and results in more advantageous scaling and signal-to-ratio for Eve.

The advanced defense against this attack, that is the proper increase of the temperature at the lower resistance end, surprisingly eliminated not only the Second-Law-attack but also the old Bergou-Scheuer-Yariv attack [6-8]. Eliminating these attacks can radically reduce Eve's fidelity while increase Alice's and Bobs' ones due to the potentially allowed longer bit exchange periods or higher bandwidths [15].

The remaining passive (listening) attack types in the steady-state mode with a potential impact is the cable capacitance attack, which requires capacitance killer or bandwidth reduction for elimination [2,3].

Finally, it is important to emphasize that, in order to reduce the chance 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 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., 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**, 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.