# Impedance and Temperature attacks against the VMG-KLJN Secure Key Exchange Protocol

Shahriar Ferdous, Christiana Chamon, and Laszlo B. Kish
Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX

**The KLJN Scheme:** The Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchanger [1-2], which is the classical physical competitor of Quantum Key Distribution (QKD) [1], offers unconditional, hardware-based security.

- At each clock period, Alice and Bob randomly select one of the $R_L$ or $R_H$ resistors and connect it to the wire line.
- The situation LH (Alice $R_L$, Bob $R_H$) or HL (Alice $R_H$, Bob $R_L$) represents the two values of the secure bit.
- This is a secure bit exchange; because the eavesdropper (Eve) knows that the situation is either HL or LH, but she is uncertain which one.
- The net power flow between Alice and Bob is zero because their resistors have the same temperature (backed by Second Law of Thermodynamics).

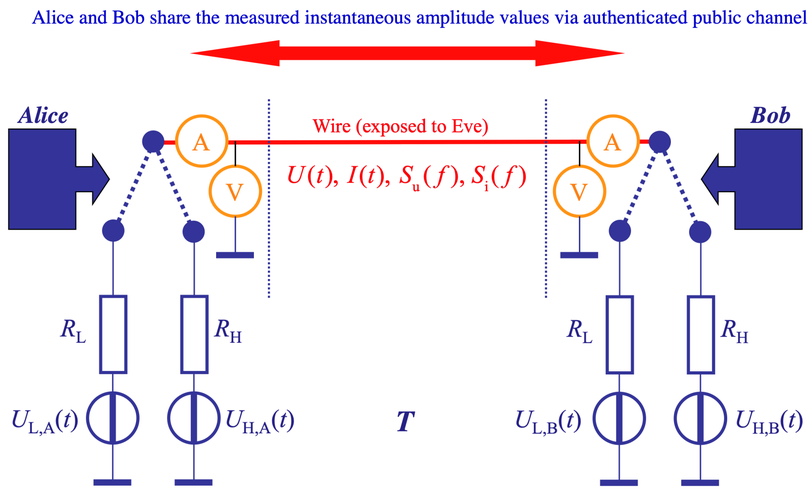


**Fig. 1.** The core of the KLJN secure key exchanger scheme [1]

**The VMG-KLJN Scheme:** Vadai et al. [3] introduced the VMG-KLJN protocol that can operate with 4 arbitrary resistance values and claimed to provide the same perfect security level. This system requires different temperatures for the resistors to guarantee the non-distinguishability of the LH and HL levels, thus it is out of equilibrium. ***But how secure is it?*** We show simple attacks against the VMG-KLJN system. The original KLJN scheme is resistant against these attacks.

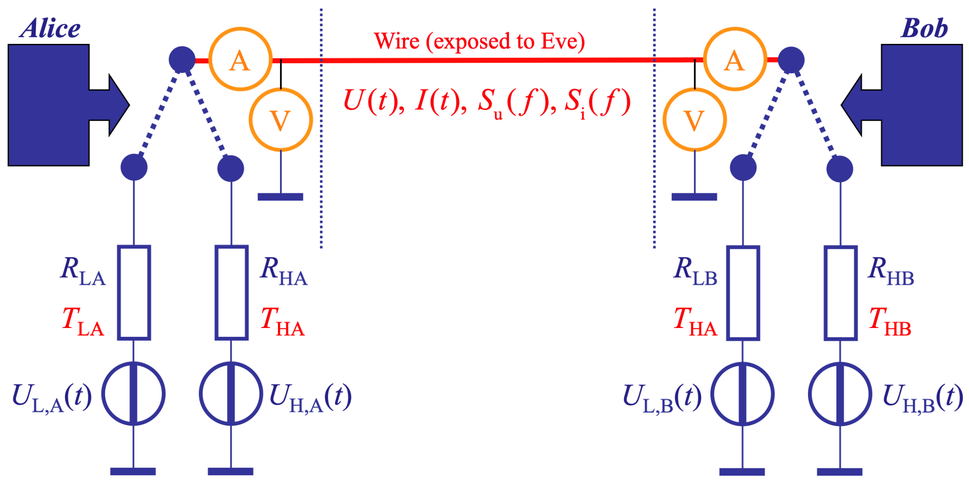


**Fig. 2.** The core of the VMG-KLJN secure key exchanger scheme [3]

**Information leak in the practical VMG protocol:**

- Different resultant resistances and different temperatures during LH and HL situation
- Parasitic cable capacitance and parasitic cable inductance.

**Security vulnerability due to bit-dependent impedances:**

- VMG assumed cable capacitance ($C_c$) and inductance ($L_c$) to be zero. However in practical case: $C_c > 0$ and $L_c > 0$
- The VMG-KLJN protocol does not guarantee that the LH and HL crossover frequencies are equal, therefore allowing a non-zero-information leak.

$$f_{U\mathrm{crHL}} = \frac{R_{\mathrm{HA}} + R_{\mathrm{LB}}}{2\pi R_{\mathrm{HA}} R_{\mathrm{LB}} C_c} \qquad f_{U\mathrm{crLH}} = \frac{R_{\mathrm{LA}} + R_{\mathrm{HB}}}{2\pi R_{\mathrm{LA}} R_{\mathrm{HB}} C_c}$$

Where, $R_{\mathrm{HA}}$ and $R_{\mathrm{LB}}$ are resistors at Alice and Bob in the HL case, respectively.
And, $R_{\mathrm{LA}}$ and $R_{\mathrm{HB}}$ are resistors at Alice and Bob in the LH case, respectively.

| HL | | LH | | Bit resistance (Parallel) [kOhm] | | Crossover frequencies of voltage noise spectra | |
|---|---|---|---|---|---|---|---|
| $R_{HA}$ [kOhm] | $R_{LB}$ [kOhm] | $R_{LA}$ [kOhm] | $R_{HB}$ [kOhm] | $R_{pHL}$ | $R_{pLH}$ | $f_{UcrHL}$ [Hz] | $f_{UcrLH}$ [Hz] |
| 9 | 1 | 1 | 9 | 0.9 | 0.9 | 884 | 884 |
| 10 | 5 | 1 | 9 | 3.33 | 0.9 | 239 | 884 |
| 5 | 5 | 1 | 9 | 2.5 | 0.9 | 318 | 884 |

**Table 1.** $U_{\mathrm{LA}}$ = 1 V, noise bandwidth $B$ = 1 kHz, cable length 2 km, 100 picoFarad/meter specific capacitance and 0.7 microHenry/meter specific inductance [4]. The first row shows a classical KLJN situation, thus the HL and LH crossover frequencies are naturally identical. The HL and LH crossover frequencies are different in the second and the third cases, indicating a non-zero information leak about the exchanged bit, in each case.

**Security vulnerability due to bit-dependent noise temperature:**

- Depending on the choice of the 4 arbitrary resistors, there are situations which can lead to unequal effective line temperature for HL and LH case. And, this will also lead to non-zero information leak.

$$T_{U\mathrm{HL}} = \frac{U^2_{\mathrm{HL}}}{4kBR_{\mathrm{pHL}}} = \frac{U^2_{\mathrm{HL}}\left(R_{\mathrm{HA}} + R_{\mathrm{LB}}\right)}{4kBR_{\mathrm{HA}}R_{\mathrm{LB}}} \quad \text{and} \quad T_{U\mathrm{LH}} = \frac{U^2_{\mathrm{LH}}}{4kBR_{\mathrm{pLH}}} = \frac{U^2_{\mathrm{HL}}\left(R_{\mathrm{LA}} + R_{\mathrm{HB}}\right)}{4kBR_{\mathrm{LA}}R_{\mathrm{HB}}}$$

Where, $k$ is the Boltzmann constant, $B$ is the noise bandwidth, $U^2_{\mathrm{HL}}$ & $U^2_{\mathrm{LH}}$ are the mean square line voltage at HL and LH situation, respectively.

| HL | | LH | | Bit resistance (Parallel) [kOhm] | | Channel noise voltage temperature | |
|---|---|---|---|---|---|---|---|
| $R_{HA}$ [kOhm] | $R_{LB}$ [kOhm] | $R_{LA}$ [kOhm] | $R_{HB}$ [kOhm] | $R_{pHL}$ | $R_{pLH}$ | $T_{UHL}$ [K] | $T_{ULH}$ [K] |
| 9 | 1 | 1 | 9 | 0.9 | 0.9 | $1.81 \times 10^{16}$ | $1.81 \times 10^{16}$ |
| 10 | 5 | 1 | 9 | 3.33 | 0.9 | $4.48 \times 10^{15}$ | $1.66 \times 10^{16}$ |
| 5 | 5 | 1 | 9 | 2.5 | 0.9 | $6.04 \times 10^{15}$ | $1.65 \times 10^{16}$ |

**Table 2.** Same circuit parameters were used as in Table-1. The first case is a classical KLJN situation, thus the HL and LH voltage noise temperatures are naturally identical. However the HL and LH voltage noise temperatures are different in the second and the third cases, indicating a non-zero information leak about the exchanged bit, in each case.

**Defense methods to reduce the extra information leak of the VMG-KLJN system:**

**Reducing the noise bandwidth ($B$) of noise generators:**

- The information leak converges to zero, if noise bandwidth approaches zero. One thing to keep in mind, decreasing the noise-bandwidth will result in the reduction of key exchange speed.

$$U^2_{\mathrm{C}}(B) = \int_0^B \frac{S_U(0)}{1 + f^2 / f^2_{U\mathrm{cr}}} = S_U(0) f_{U\mathrm{cr}} \tan^{-1}\left(\frac{B}{f_{U\mathrm{cr}}}\right)$$

Where, $U^2_{\mathrm{C}}$ is the mean-square noise voltage on $C_c$; $S_{\mathrm{U}}(0)$ is the power density spectrum of the channel voltage at zero frequency, $f_{\mathrm{Ucr}}$ is the crossover frequency of the voltage noise spectra.

**Selecting a resistor set with identical bit-impedances and identical bit-temperatures:**

- We can select identical parallel HL and LH resistances ($R_{\mathrm{pHL}} = R_{\mathrm{pLH}}$). This will confirm that the bit temperature due to cable capacitance will be same between HL and LH condition.

- Where $R_{\mathrm{pHL}} = \dfrac{R_{\mathrm{HA}}R_{\mathrm{LB}}}{R_{\mathrm{HA}} + R_{\mathrm{LB}}}$ $\qquad$ $R_{\mathrm{pLH}} = \dfrac{R_{\mathrm{LA}}R_{\mathrm{HB}}}{R_{\mathrm{LA}} + R_{\mathrm{HB}}}$

- Solving $R_{\mathrm{pHL}} = R_{\mathrm{pLH}}$ for $R_{\mathrm{LB}}$ results in

$$R_{\mathrm{LB}} = \frac{R_{\mathrm{HA}}R_{\mathrm{LA}}R_{\mathrm{LB}}}{R_{\mathrm{HA}}R_{\mathrm{HB}} + R_{\mathrm{HA}}R_{\mathrm{LA}} - R_{\mathrm{HB}}R_{\mathrm{LA}}}$$

- An analogous (dual) security vulnerability exists also for the current and cable inductance; moreover the impedance compensation method cannot work to eliminate both vulnerabilities simultaneously [5].

**Conclusion:** The VMG-KLJN system is less secure than the original KLJN protocol because the attacks shown above work against the VMG-KLJN scheme while the classical KLJN system is immune against them.

**References:**

1. L. B. Kish and C. G. Granqvist, "On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator", *Quantum Information Processing*, **13** (2014) 2213-2219.
2. L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchhoff's law", *Physics Letters A*, **352** (2006) 178-182.
3. G. Vadai, R. Mingesz, and Z. Gingl, "Generalized Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system using arbitrary resistors", Scientific Reports, **5** (2015) 13653.
4. H.-P. Chen, L. B. Kish, C.-G. Granqvist, and G. Schmera, "Do electromagnetic waves exist in a short cable at low frequencies? What does physics say?", *Fluctuation and Noise Letters*, **13** (2014) 1450016.
5. S. Ferdous, C. Chamon, L. B. Kish, "Comments on the Generalized KJLN Key Exchanger with Arbitrary Resistors: Power, Impedances, Security", to be published (2020).