Hot Topics in Physical Information (HoTPI-2013)
International Journal of Modern Physics: Conference Series
Vol. 33 (2014) 1460367 (8 pages)

DOI: 10.1142/S2010194514603676

World Scientific
www.worldscientific.com

Bit errors in the Kirchhoff-Law–Johnson-Noise secure key exchange

Yessica Saez, Laszlo B. Kish

Department of Electrical and Computer Engineering, Texas A&M University, College Station, Texas 77843-2128, USA
yessica.saez@neo.tamu.edu; laszlo.kish@ece.tamu.edu

Robert Mingesz, Zoltan Gingl

Department of Technical Informatics, University of Szeged, Árpád tér 2, Szeged, H-6701, Hungary
mingesz@inf.u-szeged.hu; gingl@inf.u-szeged.hu

Claes G. Granqvist

Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, P.O. Box 534, SE-75121 Uppsala, Sweden
claes-goran.granqvist@angstrom.uu.se

Published 17 September 2014

We classify and analyze bit errors in the voltage and current measurement modes of the Kirchhoff-law–Johnson-noise (KLJN) secure key distribution system. In both measurement modes, the error probability decays exponentially with increasing duration of the bit sharing period (BSP) at fixed bandwidth. We also present an error mitigation strategy based on the combination of voltage-based and current-based schemes. The combination method has superior fidelity, with drastically reduced error probability compared to the former schemes, and it also shows an exponential dependence on the duration of the BSP.

Keywords: Information theoretic security; secure key distribution via wire KLJN; bit errors.

1. Introduction

This paper classifies and analyzes different types of errors, due to statistical inaccuracies in noise measurements, within the Kirchhoff-law–Johnson-noise (KLJN) system[1,2] and demonstrates a new and efficient way of removing these errors.[3,4] It is a summary of recent findings presented in Refs. 3 and 4.

We first present a brief description of the working principle of the KLJN system.[1-4]

1.1 The Kirchhoff-law–Johnson-noise secure key distribution

The KLJN secure key exchange has been proven to give information-theoretic security.[5,6] This key distribution scheme is based on Kirchhoff's loop law of quasi-static electrodynamics and the fluctuation-dissipation theorem of statistical physics.[1-9] Figure 1 shows the ideal KLJN scheme.[1-4] The core channel is a wire line to which the two communicating parties, denoted "Alice" and "Bob", connect their resistors R_A and R_B, respectively. These resistors are randomly chosen from the set $\{R_0, R_1\}$, with $R_0 \neq R_1$, where R_0 and R_1 represent the different bit values. At the beginning of each bit sharing period (BSP), Alice and Bob—who have identical pairs of resistors—randomly select and connect one of these resistors to the wire line. Therefore there are four possible bit situations in which these two pairs of resistors can be connected to the wire line: 00, 01, 10 and 11.

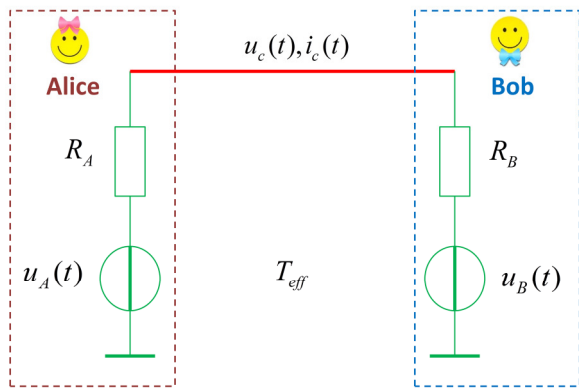

Fig. 1. Outline of the core KLJN secure key exchange scheme without defense circuitry (current/voltage monitoring/comparison) against invasive (active) attacks or attacks utilizing non-ideal components and conditions. T_{eff} is the effective noise temperature of the Gaussian noise voltage generators, R_A, $u_A(t)$, R_B, and $u_B(t)$ are the resistor values and noise voltages at Alice and Bob, respectively. $u_c(t)$ and $i_c(t)$ are channel noise voltage and current, respectively.

The cases when Alice and Bob use the same resistance values—*i.e.*, the 00 and 11 situations—represent a non-secure bit exchange. The situations when Alice and Bob use different resistance values—*i.e.*, the 01 and 10 bit situations—signify a secure bit exchange event because, according to the Second Law of Thermodynamics,[3-6] Eve cannot distinguish between them through measurements, and whenever Alice and Bob see the 01/10 situation they know that the other party has the complementary bit value, which means that they can infer the full bit arrangement. Thus a secure bit has been generated and shared.

1.2. KLJN bit interpretations

Assuming ideal components/conditions, we proceed as in earlier works.[3,4] Let us assume that Alice and Bob measure the mean-square channel noise voltage and/or current amplitudes, *i.e.*, $\left\langle u_c^2(t)\right\rangle_\tau = 4kT_{eff}R_{||}B_{KLJN}$ and/or $\left\langle i_c^2(t)\right\rangle_\tau = 4kT_{eff}\dfrac{1}{R_{loop}}B_{KLJN}$, respectively, where k is Boltzmann's constant, B_{KLJN} is channel noise bandwidth, $R_{||} = R_A R_B/(R_A+R_B)$, $R_{loop} = R_A + R_B$, and $\langle\ \rangle_\tau$ indicates finite-time average. Statistical errors (random fluctuations) appear due to the finite duration time τ of the BSP.[3,4]

Figure 2[3,4] illustrates the three possible levels of the measured mean-square channel noise voltage and current for the 11, 01/10, and 00 bit situations. The threshold values Δ_1, Δ_2 and Δ_3, Δ_4 are used to determine the boundaries between the different interpretations of the measured mean-square channel noise voltages and currents, respectively, over the time window τ.

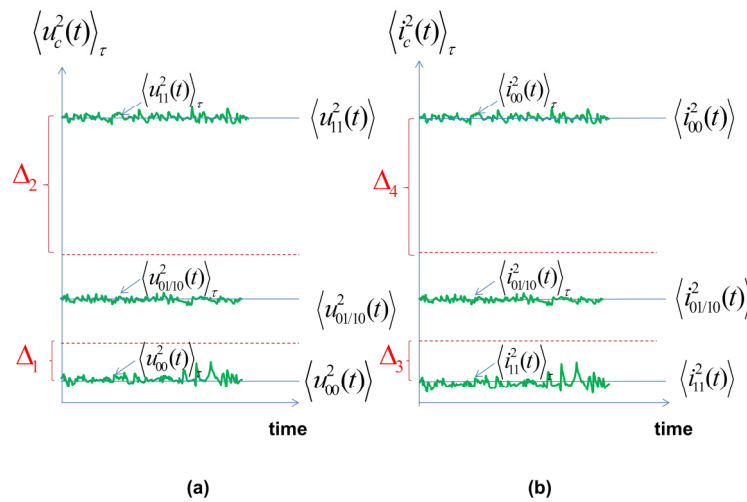

Fig. 2. Measured mean-square channel noise of voltage (a) and current (b). $\left\langle u_{11}^2(t)\right\rangle_\tau$, $\left\langle u_{01/10}^2(t)\right\rangle_\tau$, $\left\langle u_{00}^2(t)\right\rangle_\tau$ and $\left\langle i_{11}^2(t)\right\rangle_\tau$, $\left\langle i_{01/10}^2(t)\right\rangle_\tau$, $\left\langle i_{00}^2(t)\right\rangle_\tau$ are measured mean-square channel noise voltage and current at the 11, 01/10 and 00 bit situations, respectively. The solid lines with the quantities in $\langle\ \rangle$ represent ideal (infinite-time) averages. For the sake of simplicity we assume $R_0 = R$ and $R_1 = \alpha R$, with $\alpha >> 1$.

The bit interpretations of the measured mean-square channel noise voltage[3] and current[4] are 00 when $\left\langle u_{ch}^2(t)\right\rangle_\tau < \left\langle u_{00}^2(t)\right\rangle + \Delta_1$ and $\left\langle i_c^2(t)\right\rangle_\tau > \left\langle i_{00}^2(t)\right\rangle - \Delta_4$, respectively. The interpretations are 11 when $\left\langle u_{ch}^2(t)\right\rangle_\tau > \left\langle u_{11}^2(t)\right\rangle - \Delta_2$ and $\left\langle i_c^2(t)\right\rangle_\tau < \left\langle i_{11}^2(t)\right\rangle + \Delta_3$, respectively. The secure bit situations 01/10 are interpreted as such when

$\left\langle u_{00}^2(t)\right\rangle + \Delta_1 \le \left\langle u_{ch}^2(t)\right\rangle_\tau \le \left\langle u_{11}^2(t)\right\rangle - \Delta_2$ and $\left\langle i_{11}^2(t)\right\rangle + \Delta_3 \le \left\langle i_c^2(t)\right\rangle_\tau \le \left\langle i_{00}^2(t)\right\rangle - \Delta_4$,

respectively.

2. Error analysis in the KLJN system

Bit errors occur when the protocol makes incorrect bit interpretations due to statistical inaccuracies in the measured mean-square noise voltage and/or current. There are different types of errors situations, as shown in Table 1.[3,4]

Table 1. Types of errors in the KLJN bit exchange scheme.

		Actual Situation		
		00	11	01/10
Measurement Interpretation (Decision)	00	Correct (no error)	Error, removed (automatically)	Error, removed (automatically)
	11	Error, removed (automatically)	Correct (no error)	Error, removed (automatically)
	01/10	Error (probability?)	Error (probability?)	Correct (no error)

It is apparent that two types of errors need to be addressed: the 11==>01/10 errors—*i.e*., the errors when the actual situation 11 is interpreted as the secure noise level 01/10—and the 00==>01/10 errors occurring when the actual situation 00 is interpreted as 01/10.

Figure 3 shows a block diagram for the measurement process. The channel voltage and/or current first enter a squaring unit. For typical practical applications, the output signal is a voltage, because the squaring unit employs voltage-signal-based electronics. Thus when measuring the current, for the sake of simplicity and without losing generality, we assume that the numerical values of the voltage correspond to the measured current.

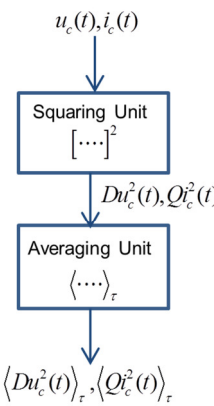

Fig. 3 Mean-square channel noise voltage and/or current measurement process. Q and D are calibration coefficients of the squaring device to provide a Volt unit with the correct numerical value for the squaring operation.

The measured mean-square channel noise voltage and/or current for the finite-time average τ have a DC and a superimposed AC component $\mu(t)$ remaining after the finite-time average.[3,4] This averaging process can be represented as low-pass filtering with a cut-off frequency $f_B \approx 1/\tau$. The AC component $\mu(t)$ of the finite-time average is Gaussian with high accuracy,[3,4,10] which follows from the Central Limit Theorem because τ is much larger than the correlation time for the AC component before averaging ($f_B << B_{KLJN}$). We estimate the error probability with the probability that $\mu(t)$ is crossing a threshold during the time interval τ. To compute this probability, we follow a procedure that is analogous to the one in Refs. 3 and 4, specifically by using Rice's formula[11,12] for threshold crossings.

2.1. General approach

We suppose that Δ is the threshold value used to determine the boundaries between the different interpretations of $\mu(t)$ over the time window τ. If we define $S_{AC,\tau}(f)$ as the power density spectrum of $\mu(t)$, the mean frequency of level crossing can be given as

$$\nu(\Delta) = \frac{2}{\hat{\mu}} \exp\left(\frac{-\Delta^2}{2\hat{\mu}^2}\right) \sqrt{\int_0^\infty f^2 S_{AC,\tau}(f)df} \ , \tag{1}$$

where $\hat{\mu} = \sqrt{\int_0^\infty S_{AC,\tau}(f)df}$ is the RMS value of $\mu(t)$ and the threshold value Δ is defined, for normalization purposes, as a fraction of the measured mean-square channel noise voltage and/or current, namely $\Delta = \varphi\left\langle Du_c^2(t)\right\rangle$ and/or $\Delta = \varphi\left\langle Qi_c^2(t)\right\rangle$ for $0 < \varphi < 1$, respectively. According to Ref. 10, the power density spectrum $S_{AC}(f)$ for the AC component of the non-averaged quantity $u_c^2(t)$ and/or $i_c^2(t)$ is

$$S_{AC}(f) = 2D^2 B_{KLJN} S_c^2(f)\left(1 - \frac{f}{2B_{KLJN}}\right), \text{ for } 0 \le f \le 2B_{KLJN}, \tag{2}$$

and $S_{AC}(f) = 0$ otherwise, where $S_c(f)$ is the power density spectrum of the mean-square channel noise voltage and/or current.

The low-pass filtering effect of the time averaging cuts off this spectrum for $f > f_B$ but keeps the $S_{AC}(f)$ spectrum for $f < f_B$. Since $f_B << B_{KLJN}$, the value of $S_{AC}(f)$ within the frequency band f_B can be approximated by its maximum, so that $S_{AC,\tau}(f) \approx S_{AC}(0)$. Therefore, by setting $\gamma = B_{KLJN}/f_B$ one obtains that the frequency $\nu_\uparrow(\Delta)$ of unidirectional level crossings (half of the level crossing frequency predicted by Rice's formula) is

$$\nu_\uparrow(\Delta) = \frac{f_B}{\sqrt{3}} \exp\left(\frac{-\varphi^2\gamma}{4}\right). \tag{3}$$

In the high-threshold situation, the errors follow Poisson statistics and thus the error probability during a time interval is equal to the expected number of errors within this interval provided this number is much less than one. Thus the probability ε in the case of $\varepsilon << 1$ is

$$\varepsilon \approx \nu_{\uparrow}(\Delta)\tau \approx \frac{\nu_{\uparrow}(\Delta)}{f_B} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\varphi^2 \gamma}{4}\right). \tag{4}$$

2.2. Statistical errors in the voltage and current measurement modes

In this section, the threshold values Δ_1, Δ_2 and Δ_3, Δ_4 have meanings that are similar to the one of the threshold value Δ in the general approach presented above and are also defined as a fraction of the corresponding measured mean-square channel noise voltage and current, namely: $\Delta_1 = \beta\left\langle Du_{00}^2(t)\right\rangle$ for $0 < \beta < 1$, $\Delta_2 = \delta\left\langle Du_{11}^2(t)\right\rangle$ for $0 < \delta < 1$, $\Delta_3 = \lambda\left\langle Qi_{11}^2(t)\right\rangle$ for $0 < \lambda < 1$, and $\Delta_4 = \rho\left\langle Qi_{00}^2(t)\right\rangle$ for $0 < \rho < 1$.

Substituting Δ_1 or Δ_2 in Eq. (4), we find that the probabilities ε_{00} and ε_{11} of the 00==>01/10 and 11==>01/10 types of errors in *voltage* measurements[3] for $\varepsilon_{00} << 1$ are

$$\varepsilon_{00} \approx \frac{\nu_{\uparrow}(\Delta_1)}{f_B} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\beta^2 \gamma}{4}\right), \text{ for } 0 < \beta < 1, \tag{5}$$

$$\varepsilon_{11} \approx \frac{\nu_{\downarrow}(\Delta_2)}{f_B} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\delta^2 \gamma}{4}\right), \text{ for } 0 < \delta < 1, \tag{6}$$

respectively.

Similarly, by substituting Δ_3 and Δ_4 in Eq. (4) we find that the error probabilities $\varepsilon_{i,11}$ and $\varepsilon_{i,00}$ of the 11==>01/10 and 00==>01/10 types of errors in *current* measurements[4] are

$$\varepsilon_{i,11} \approx \frac{\nu_{\uparrow}(\Delta_3)}{f_B} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\lambda^2 \gamma}{4}\right), \text{ for } 0 < \lambda < 1, \tag{7}$$

$$\varepsilon_{i,00} \approx \frac{\nu_{\downarrow}(\Delta_4)}{f_B} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\rho^2 \gamma}{4}\right), \text{ for } 0 < \rho < 1, \tag{8}$$

respectively.

It should be noticed that—for both the voltage-based and the current-based methods—the error probabilities are exponential functions of the parameter γ, which shows that the error probability decays exponentially with increasing magnitude of τ.

2.3. Illustration of the results with practical parameters

To demonstrate the results, we assign practical values to the parameters in Eq. (4). For $\gamma = 100$ and $\varphi = 0.5$, the bit error probability is $\varepsilon = 0.001$. Increasing γ by a factor of two (and analogously the time average window τ) results in $\varepsilon \approx 10^{-6}$, which is satisfactory for many applications.

In our case of $\alpha >> 1$ the mean square noise current level at 11 is much closer to the value at 01/10 than to the value at 00 (*cf.* Fig. 2), and hence $\varepsilon_{i,00} << \varepsilon_{i,11}$. This situation is reversed for the case of the voltage-based method, where $\varepsilon_{00} >> \varepsilon_{11}$.

2.4. A combined current–voltage error removal strategy

We assume that Alice and Bob measure both $\left\langle u_c^{\,2} \right\rangle_\tau$ and $\left\langle i_c^{\,2} \right\rangle_\tau$ at the same time. In an ideal error-free situation, the same bit interpretations ensue from both mean-square channel noise amplitudes. However the bit interpretations can differ when there are errors, because the current and voltage amplitudes are statistically independent due to Gaussianity and the Second Law of Thermodynamics.[1-6] To eliminate errors, we keep only those cases where both the current and voltage methods interpret 01/10 bit values. Table 2 illustrates this situation.[4]

Table 2 KLJN error removal method with combined current and voltage analysis.

		Voltage measurement interpretation		
		00	11	01/10
Current measurement interpretation	00	00 (Insecure/Discard)	Discard (check attack)	00 (Insecure/Discard)
	11	Discard (check attack)	11 (Insecure/ Discard)	11 (Insecure/ Discard)
	01/10	00 (Insecure/ Discard)	11 (Insecure/ Discard)	01/10 (Secure)

Due to their independence, the error probabilities in the combined current-voltage method are the product of the error probabilities of the current-based and voltage-based schemes.[4] The resultant probabilities $\varepsilon_{t,00}$ and $\varepsilon_{t,11}$ of 00==>01/10 and 11==>01/10 types of errors are[4]

$$\varepsilon_{t,00} = \varepsilon_{00}\varepsilon_{i,00} = \frac{1}{3}\exp\left(\frac{-\gamma(\beta^2+\rho^2)}{4}\right), \text{ for } 0<\beta<1 \text{ and } 0<\rho<1, \tag{9}$$

$$\varepsilon_{t,11} = \varepsilon_{11}\varepsilon_{i,11} = \frac{1}{3}\exp\left(\frac{-\gamma(\delta^2+\lambda^2)}{4}\right), \text{ for } 0<\delta<1 \text{ and } 0<\lambda<1, \tag{10}$$

respectively.

These error probabilities are again exponential functions of the parameter γ. For the practical parameters $\gamma = 100$ and $\beta = \rho = 0.5$ we find that $\varepsilon_{t,00} = 1.24\times10^{-6}$, which is drastically less than with the former methods. If the duration of the bit exchange period, *i.e.*, γ, is increased by a factor of two, the total bit error probability $\varepsilon_{t,00}$ is decreased to $\varepsilon_{t,00} \approx 4.6\times10^{-12}$. Similar improvements can be found for $\varepsilon_{t,11}$.

Although in the experimental setup presented in Ref. 9 we used a slightly modified decision table, the joint use of voltage and current detection had already been found suitable for decreasing error ratios. In addition, the results presented in current article are in good agreement with the experimental results.

3. Conclusion

This paper has classified and analyzed the types of errors in the KLJN key exchange for both voltage-based and current-based schemes. These error probabilities showed an exponential dependence on the duration of the bit exchange. Furthermore, we presented an enhanced error mitigation method, based on the combination of the voltage-based and current-based schemes, which operates without any error correction algorithm.

Acknowledgments

Y. Saez is grateful to IFARHU/SENACYT for supporting her PhD studies at Texas A&M. R. Mingesz's contribution is supported by the European Union and the European Social Fund. Project #TÁMOP-4.2.2.A-11/1/KONV-2012-0073.

References

1. D. Abbott, G. Schmera, *Scholarpedia* **8** (8), 31157 (2013).
2. L.B. Kish, *Physics Letters A* **352**, 178 (2006).
3. Y. Saez, L.B. Kish, *PLoS ONE* **8**(11): e81103 (2013).
4. Y. Saez, L.B. Kish, R. Mingesz, Z. Gingl, C.G. Granqvist, *Journal of Computational Electronics,* DOI: 10.1007/s10825-013-0515-2 (2013).
5. R. Mingesz, L.B. Kish, Z. Gingl, C.G. Granqvist, H. Wen, F. Peper, T. Eubanks, G. Schmera, *Metrology and Measurement Systems* **20**, 3 (2013).
6. L.B. Kish, D. Abbott, C.G. Granqvist. Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme. viXra preprint viXra:1306.0058; arXiv preprint arXiv:1306.653 (2013).
7. L.B. Kish, Fluctuations and Noise Letters **6**, L57 (2005).
8. L.B. Kish, Metrology and Measurement Systems **20**, 191 (2013).
9. R. Mingesz, L.B. Kish, Z. Gingl, *Physics Letters A* **372**, 978 (2008).
10. L.B. Kish, R. Mingesz, Z. Gingl, C.G. Granqvist, *Metrology and Measurement Systems* **19**, 653 (2012).
11. S.O. Rice, Bell System Technical Journal **23**, 282 (1944).
12. I. Rychlik, *Extremes* **3**, 331 (2000).