Fluctuation and Noise Letters
Vol. 0, No. 0 (0000) 000–000

PERFORMANCE ANALYSIS OF THE "INTELLIGENT" KIRCHHOFF-LAW-JOHNSON-NOISE SECURE KEY EXCHANGE

JANUSZ SMULKO

Faculty of Electronics, Telecommunications and Informatics, Department of Metrology and Optoelectronics, Gdansk University of Technology,
80-233 Gdansk, G. Narutowicza 11/12, Poland
jsmulko@eti.pg.gda.pl

Received (received date)
Revised (revised date)
Accepted (accepted date)

The Kirchhoff-Law-Johnson-Noise (KLJN) secure key distribution system provides a way of exchanging theoretically secure keys by measuring random voltage and current through the wire connecting two different resistors at Alice's and Bob's ends. Recently new advanced protocols for the KLJN method have been proposed with enhanced performance. In this paper we analyze the KLJN system and compare with the "intelligent" KLJN (iKLJN) scheme. That task requires determination of the applied resistors and identification of various superpositions of known and unknown noise components. Some statistical tools will be explored to determine how the duration of the bit exchange window (averaging time) influences the performance of the secure bit exchange.

Keywords: Johnson-Noise; secure communication; statistical hypothesis.

1. Introduction

Secure communication is a topical subject in modern society due to increasing importance of data transfer, internet banking and digital rights management in electronic media. Therefore the introduction of key exchange protocol which requires ordinary resistors and thermal noise analysis only is very promising for such applications [1]. The KLJN scheme is founded on the Second Law of Thermodynamics, which makes the scheme as secure as it is impossible to build a perpetual motion machine of the second kind. Additionally, an enhanced secure key exchange system (e.g. "intelligent" KLJN – iKLJN) based on this scheme was proposed to assure practically-perfect security [2] by means of classical physics, without using quantum encryption and bulky systems [3]. The KLJN scheme is a challenging proposal and requires in-depth analysis to establish how the KLJN protocols are resistant against eavesdropping at the settled noise bandwidth, averaging time and resistances. Moreover, it is another interesting application of noise in

information processing, in the development phase, together with other examples of noise use in signal processing and sensing [4–7].

In this theoretical study some selected statistical tests are applied as a new tool to determine time of averaging which is necessary for correct bits detection at a given significance level. The same analysis method was applied to compare the efficiency of two protocols: the classical KLJN [1] and the recently introduced iKLJN [2]. Effectiveness of the secure data transfer is analyzed to establish statistical errors of incorrect detection of the transferred bits (type I and type II errors). The influence of the distance between the observed noise intensities responding to the transferred bit combinations and averaging time on errors of the transmitted data was considered. Finally, some conclusions achieved for the introduced iKLJN scheme were presented to highlight its new quality in secure key exchange, requiring shorter averaging time than the classical KLJN scheme. We derived the formula for the number of averaged noise samples necessary to assure the assumed error levels.

1.1. *The Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme*

The idealistic KLJN scheme comprises two sets of resistors of low R_L and high R_H resistance at both communicating parties Alice (A) and Bob (B) which are randomly chosen and connected to the transmission line (Fig. 1). The resistances $R_H = a \cdot R_L$ are of significantly different values ($a >> 1$). Noise is introduced into the system by the Gaussian voltage noise generators, connected in series with the resistors. The generators deliver white noise at a publicly established bandwidth and at effective temperature T_{eff}, typically many orders of amplitude higher than the system temperature [4]. The noise sources are statistically independent and have a voltage power spectral density $S_u(f) = 4kT_{eff}R$, where R equals R_L or R_H respectively. Noise in the transmission line (current $I_C(t)$ or voltage $U_C(t)$) can be observed within a clock period which responds to a single bit exchange rate. For simplicity in this paper only voltage fluctuations $U_C(t)$ on the transmission line will be analyzed to determine which bits are exchanged. The same results can be received when the current $I_C(t)$ is considered.

A secure bit transfer occurs only in the case when the resistors on both sides (A) and (B) have different values R_H and R_L or R_L and R_H which is adequate to the case of 01 or 10 bits exchange. Such a case will result according to the Second Law of Thermodynamics in the same intensity of noise at the transmission line but information about the adjusted resistors will be secure because only Alice and Bob will know their resistors positions. Otherwise (11 or 00 bits transmission) an eavesdropper would be able to extract the data.

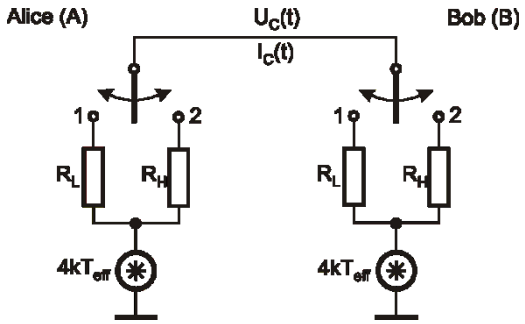

Fig. 1. Schematic circuit of the Kirchhoff-Law-Johnson-Noise (KLJN) secure key distribution system.

The variance of voltage fluctuations for these cases at the normalized bandwidth Δf is derived by [2]:

$$\sigma_{01}^2 = \sigma_{10}^2 = 4kT_{eff}R_{loop}\Delta f \,, \tag{1}$$

where R_{loop} is the substitute resistance of the transmission loop. Thus, we can expect that according to three various combinations of R_{L} and R_{H} at both ends of the loop, three different variances in the transmission line can be observed:

$$\sigma_{00}^2 = 4kT_{eff}\frac{R_L R_L}{R_L + R_L}\Delta f = 4kT_{eff}\frac{R_L}{2}\Delta f \,, \tag{2}$$

$$\sigma_{01}^2 = \sigma_{10}^2 = 4kT_{eff}\frac{R_L R_H}{R_L + R_H}\Delta f = 4kT_{eff}\frac{R_L R_H}{R_L + R_H}\Delta f = 4kT_{eff}R_L\frac{a}{1+a}\Delta f \,, \tag{3}$$

$$\sigma_{11}^2 = 4kT_{eff}\frac{R_H R_H}{R_H + R_H}\Delta f = 4kT_{eff}\frac{R_H}{2}\Delta f = 4kT_{eff}R_L\frac{a}{2}\Delta f \,. \tag{4}$$

The values of σ_{00}, σ_{01} and σ_{10}, or σ_{11} observed in the transition line are unevenly distributed because distances between them depend on the parameter a ($R_{\text{H}} = a \cdot R_{\text{L}}$) and at $a = 10$ are close to the ratios 1:1.81:10. Voltage variance σ^2 at the transmission line will be estimated over a limited observation time and therefore the random error of its value has to be considered to evaluate the probability of false detection of the transmitted bits. Especially, a relatively smaller difference between variances σ_{00} and σ_{01} or σ_{10} can influence strongly the correctness of the transmitted data in the established averaging time.

This problem was addressed in literature by utilizing Rice's formula for the level crossing statistics [8, 9]. Error probability due to inaccuracies in noise voltage measurements was established for a case when the actual situation of the transmitted 00 bits was interpreted as a secure noise level 01 or 10. In the literature, to the best knowledge of the author of this article, no advanced statistical analysis has been presented how the distances between the estimated variances influence the accuracy of the transmitted bits detection and how to establish the averaging time to assure the assumed accuracy. Thus, a more in-depth analysis of that problem has to be conducted. To solve this issue an approach of testing statistical hypothesis can be utilized. The tests consider random errors when the accepted hypothesis of the transferred bits was not true.

1.2. *The "intelligent" Kirchhoff-Law-Johnson-Noise (iKLJN) secure key exchange scheme*

The secure data exchange KLJN scheme of 01 and 10 bits transmission relies on noise intensity measurements in the line and secret knowledge of Alice and Bob of which of their sides resistors R_L or R_H are attached. A new KLJN scheme has been proposed recently where Alice and Bob utilize as well the knowledge of the stochastic time function of their own noise generator [2]. Thus, this new "intelligent" iKLJN scheme gives additional privilege to Alice and Bob when compared to Eve who can observe channel noise only. Therefore, the iKLJN scheme will reduce the averaging time at the same correctness of bits transmission rate when compared with the KLJN scheme introduced earlier.

To reduce the averaging time Alice and Bob have to observe line noise (e.g., voltage $U_C(t)$) and their noise generator stochastic time function (e.g., $U_B(t)$ for Bob and $U_A(t)$ for Alice). The observed channel noise $U_C(t)$ can be reduced by subtracting the scaled noise component of noise $U_B(t)$ for Bob and $U_A(t)$ for Alice according to the assumed positions of the resistors at Alice and Bob ends. If the assumption was true, the line noise component after subtraction is uncorrelated with Bob or Alice noise sequence. This fact can be investigated by estimating the cross-correlation function which is an independent source of information about the transferred bits. A detailed way of determining the cross-correlation function can be found elsewhere [2]. For simplicity let us consider an exemplary situation when Bob having resistance R_L assumed correctly that Alice has a different resistance $R_H = a \cdot R_L$. Thus, Bob knows the time sequence $U_B(t)$ of his noise generator and can subtract from the observed line noise $U_C(t)$ the part coming from his generator and attenuated by the existing voltage divider of the resistances R_L and R_H[2]:

$$U_{C*}(t) = U_C(t) - U_B(t)\frac{a}{1+a} = \frac{U_A(t) + aU_B(t)}{1+a} - U_B(t)\frac{a}{1+a} = \frac{U_A(t)}{1+a}. \tag{5}$$

The correctness of Bob's assumption can be proved by estimating the cross-correlation function:

$$E\left[U_{C*}(t) \cdot U_B(t)\right] = \frac{E\left[U_A(t) \cdot U_B(t)\right]}{1+a} = 0 \tag{6}$$

if the assumption is true. Operator E means averaging. To sum up, we conclude that the iKLJN scheme can comprise two independent procedures:

- estimation of noise variance in the transmission line,
- determination if the cross-correlation function between the generator stochastic time function and the line noise after subtracting the respectively scaled generator stochastic time function is different from zero according to the statistical test result.

Both functions will assure 01 or 10 secure bit exchange. Thus, a combination of these two procedures will strengthen data exchange by shortening the averaging time or decreasing the transmission error rate when compared with the firstly proposed KLJN scheme.

We can consider the cross-correlation between $U_{C*}(t)$ and $U_B(t)$ or voltage variance σ^2 in the channel line as independent probabilistic quantities. It means that using both independent procedures, the probability of erroneous bit detection is a product of the

probabilities of these two procedures. Thus, keeping the same error of bits rate exchange we can substantially decrease the averaging time. This conclusion is very substantial when a practical system is considered because the iKLJN scheme will make the bits exchange more robust against plausible attacks when compared with the KLJN scheme. This conclusion is valid even when the cross-correlation will not be absolutely independent from noise variance in the line in a non-ideal system. It should be underlined that some preliminary tests of secure bits transmission have been performed to shed light on its limitations in practical applications [10].

Introduction of the iKLJN scheme means that we have to test if the selected quantities $U_{C*}(t)$ and $U_B(t)$ are correlated or not. This fact can be explored using statistical tools, like testing correlation by the statistical test of non-zero linear correlation coefficient or testing if the mean value of the cross-correlation function defined by (6) is different from zero.

2. Discussions and results

In this paragraph a new approach to the KLJN secure scheme will be considered by utilizing statistical hypothesis tests. The tests will take into account the averaging time necessary to establish a statistical hypothesis about transmitted bits at a given error rate. The number of averaged noise samples will be considered which responds to the averaging time at the given sampling rate. Firstly, problems of determining variance σ^2 of noise in the transmission line at given error of false detection (detection of the bits 01 or 10 transmission instead of 00 and vice versa) will be considered. Secondly, methods of cross-correlation detection will be discussed according to their potential application in the iKLJN scheme for more efficient detection of the transmitted bytes.

2.1. *Inaccuracy interval in the KLJN secure key exchange scheme*

The estimation of noise variance in the line requires averaging over a limited number of voltage samples. The estimator s^2 of variance σ^2 by using N samples of $U_C(t)$ in the transmission line is derived from the formula:

$$s^2 = \frac{1}{N-1}\sum_{i=1}^{N}\left(U_C(t) - \mu_{U_C}\right)^2, \tag{7}$$

where μ_{Uc} is the estimated mean value derived by using the same voltage samples $U_C(t)$ as to estimate s^2. It is [10] that the product

$$\sum_{i=1}^{N}\left(U_C(t) - \mu_{U_C}\right)^2 = \sigma^2 \chi_n^2, \tag{8}$$

where χ^2_n has a Chi-square distribution with $n = N - 1$ degrees of freedom. By applying information about the distribution of the estimated variance we can determine the confidence intervals at the given level of significance α – the probability that the variance σ^2 belongs to this interval determined by variance estimator s^2:

$$\text{Prob}\left[\frac{ns^2}{\chi^2_{n,\alpha/2}} \le \sigma^2 < \frac{ns^2}{\chi^2_{n,1-\alpha/2}}\right] = \alpha\,, \tag{9}$$

where $\chi^2_{n,\alpha/2}$ and $\chi^2_{n,1-\alpha/2}$ are Chi-square distribution values which can be read out from the distribution table at the given level of significance α and which determines the probability that the estimated variance exceeds the interval defined by (9).

In secure bits transmission using the KLJN scheme the estimator s^2 of variance σ^2 is used to detect the transmitted bits. A fixed number, usually $\alpha = 0.05$, is referred as a level of significance and determines the probability of incorrect rejection of the true statistical hypothesis (s^2 is equal to σ^2 which is called the null hypothesis) in favor of the second alternative hypothesis (s^2 is not equal to σ^2). Such incorrect assumption is called the Type I Error and its rate is equal α (false positive rate). At the given level of significance α it is possible by using (9) to determine the number of averaged voltage samples $N = n + 1$ which is necessary to detect the transmitted bits at the given probability.

Another error type happens when the hypothesis may be accepted when in fact it is false. Such case is called a Type II Error and can be established when the true value of the estimated parameter is different by a fixed constant from the hypothesized value. The type II error is equal β which can be different in general from the type I error equal α. The probability $1 - \beta$ is called power of the test. For any given number N of averaged samples a Type I Error can be reduced by reducing the level of significance α. At the same time the probability β of the Type II Error will be increased (reducing the power of the test). The only way to reduce both errors is to increase the number N of the averaged samples.

When the KLJN scheme is taken into account, the case of detecting bits transmission 00 or 01 and 10 will respond to the same situation as presented before when the estimated variance has to be assigned to one of two values σ_{00}^2 and σ_{10}^2 or σ_{01}^2, which are shifted by $\Delta\sigma^2$ (Fig. 2). The third observable variance σ_{11}^2 at the transmitted bits 11 can be omitted because its distance from other variances responding to the transmissions of other bits is a few times greater than between σ_{00}^2 and σ_{10}^2 or σ_{01}^2 according to the selected parameter $a \ge 10$ (see. the eq. (3), (4) and (5)).

To optimize selection of the averaged samples $N = n + 1$ by assuring the same value of Type I Error and Type II Error it is necessary to write equations for lower and upper limit of variance estimator s^2 for both errors, when the distributions cross each other (Fig. 2). The difference between the variances according to (2) and (3) is equal to:

$$\Delta\sigma^2 = \sigma_{10}^2 - \sigma_{00}^2 = \sigma_{01}^2 - \sigma_{00}^2 = 4kT_{eff}\Delta f R_L \frac{a-1}{2(a+1)}\,. \tag{10}$$

Hence, the equations for the lower limit of s^2 can be delivered from (9):

$$s^2 = \frac{\sigma_{01}^2 \chi^2_{n,\alpha/2}}{n}\,, \tag{11}$$

and at the same time the higher limit for the Type II Error is given by:

$$s^2 = \frac{\sigma_{01}^2 \chi^2_{n,1-\beta}}{n} - \Delta\sigma^2\,. \tag{12}$$

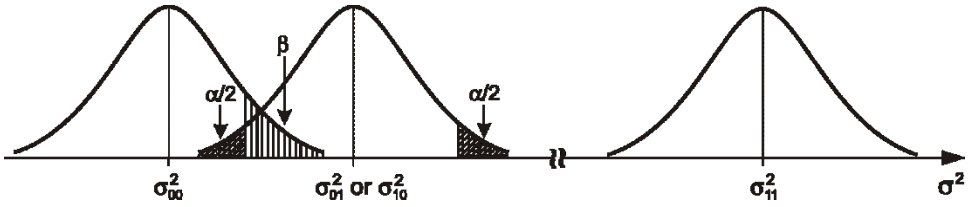

Fig. 2. Illustration of noise variance σ^2 at their given probability distributions (solid lines) observed in the transmission line at different combination of resistances R_L, R_H at the ends of the KLJN secure key distribution system; the low index of variance responds to the combination of the resistances: R_L means 0 and R_H means 1; probability α of the Type I Error (crossed area) and probability β of the Type II Error (striped area) were marked; in order to provide the best results, one may choose an asymmetric confidence interval, since it is easier to distinguish between 10 and 11 state than between 10 and 00 state.

Chi-square distribution tends to Gaussian distribution, represented by normalized variable z (having zero mean value and variance equal to 1), at sufficiently high n, which usually exceeds at least a few tens of samples:

$$\chi_n^2 \approx \sqrt{2n}z + n\,. \tag{13}$$

Thus, by comparing (11) with (12) and using simplification to Gaussian distribution due to (13) we can get:

$$\frac{a\left(\sqrt{2n}z_{\alpha/2}+n\right)}{(1-a)n} = \frac{a\left(\sqrt{2n}z_{1-\beta}+n\right)}{(1-a)n} - \frac{a-1}{2(a+1)}\,. \tag{14}$$

Equation (14) after necessary rearrangements can be reduced to the statement describing how the number of noise samples $N = n + 1$ depends on both assumed error levels α, β and parameter a:

$$N = 8\left(z_{\alpha/2} - z_{1-\beta}\right)^2 \cdot \frac{a^2(a+1)^2}{(a-1)^4} + 1\,. \tag{15}$$

Some interesting conclusions can be drawn from the resulting eq. (15). When a tends to 1 (the applied resistors R_H and R_L tend to have the same value), the time necessary for averaging tends to infinity. Additionally, the function (15) is a continuous function of the parameter a without local extremes and tends to zero when a closes to infinity. This means that noise averaging time decreases when the distance between R_H and R_L becomes bigger. That fact corresponds to the general occurrence of the continuous character of classical physics laws applied in the KLJN scheme.

The number N of the averaged noise samples depends on the difference between $z_{\alpha/2}$ and $z_{1-\beta}$. Assuming a typical value for $\alpha/2 = 2.5\%$ we can decrease N even to one ($z_{\alpha/2} = z_{1-\beta}$) when $1 - \beta = 2.5\%$ as well. Then the Type II Error is equal to $\beta = 97.5\%$ which means that this error is close to certainty and such case does not have any practical meaning. Independently from the considered borderline cases, eq. (15) can estimate the necessary number of averaged noise samples N at given transmission conditions (assumed Type I and Type II Errors by the selected levels of significance α and β).

2.2. *Benefits of the iKLJN secure key exchange scheme*

When the iKLJN scheme is applied the presented statistical approach for determination of noise variance in the transmission line can be used as well. Additionally, the condition of independence between the considered noise time series (given by eq. 6) can be tested using another statistical test which is independent in the ideal case from the variance test applied to the KLJN scheme. The correlation between the selected noise time series $U_{C*}(t)$ and $U_B(t)$ can be investigated using a linear correlation coefficient [11] or another measure of correlation between two variables [12]. A statistical test of linear correlation coefficient can establish at a given level of significance α if the hypothesis about non-zero correlation between $U_{C*}(t)$ and $U_B(t)$ exists or should be rejected. Another possible and equivalent analysis to that mentioned above is to test whether the cross-correlation given by eq. (6) is equal to zero. This can be done by testing if the mean value of (6) is zero using an acceptance interval similar to that given by eq. (9) and determined for variance estimator s^2. Then, the statistical approach proposed above can establish the number N of the samples necessary for averaging.

3. Conclusions

In this theoretical study the problem of secure bits detection using the KLJN scheme was considered by applying a statistical approach to noise parameters estimation. It has been proved that the presented method can determine the number N of noise samples necessary for averaging at the assumed level of statistical errors of Type I and Type II.

When the iKLJN scheme is applied an additional statistical test of cross-correlation or simple linear correlation between the noise time series can be utilized to reduce bits detection error at the same averaging time. Another possibility when using the iKLJN scheme is to reduce averaging time at the same error rate of bits detection. This case requires additional analysis how to estimate the averaging time by keeping the same error rate. It should be underlined that the KLJN scheme is intensively investigated subject and some statistical analysis begun to be published, to determine the probability density needed for secure key distribution [13]. The present paper addresses other statistical properties of the secure key exchange, responsible for statistical errors during transmission. Further studies to provide appropriate examples and error rates at given measurement lengths are planned.

Acknowledgments

This research was partially supported by a statutory project (Dzialalnosc Statutowa), Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Poland. The paper is an updated and enriched version of the presentation given at the conference Hot Topics in Physical Informatics HotPI – 2013, Changsha, Hunan, China.

References

[1] L. B. Kish, *Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law, Physics Letters A* **352** (2006) 178–182.

[2] L. B. Kish, *Enhanced secure key exchange systems based on the Johnson-noise scheme, Metrology and Measurement Systems* **20** (2013) 191–204.

[3] C. H. Bennett, G. Brassard, S. Breidbart, S. Wiesner, *Quantum cryptography, or Unforgeable subway tokens. Advances in Cryptology, Springer US* (1982) 267–275.

[4] A. Kwiatkowski, M. Gnyba, J. Smulko, P. Wierzba, *Algorithms of chemicals detection using Raman spectra, Metrology and Measurement Systems*, **17** (2010) 549–559.

[5] J. Mroczka, D. Szczuczyński, *Inverse problems formulated in terms of first-kind Fredholm integral equations in indirect measurements, Metrology and Measurement Systems*, **16** (2009) 333–357.

[6] C. Kwan, G. Schmera, J. Smulko, L. B. Kish, P. Heszler, C. G. Granqvist, *Advanced agent identification with fluctuation-enhanced sensing, IEEE Sensors Journal* **8** (2008) 706–713.

[7] J. Smulko, *Methods of electrochemical noise analysis for investigation of corrosion processes, Fluctuation and Noise Letters*, **6** (2006) R1–R9.

[8] Y. Saez, L. B. Kish, *Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange, PloS one*, **8** (2013) e81103.

[9] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, C. G. Granqvist, *Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law–Johnson-noise secure key exchange, Journal of Computational Electronics*. 13 (2014) 271–277.

[10] R. Mingesz, Z. Gingl Z, L. B. Kish, *Johnson (-like)–Noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via modelline, Physics Letters A* **372** (2008) 978–984.

[11] J. S. Bendat, A. G. Piersol, *Random data analysis and measurement procedures*, John Wiley and Sons, New York (2011).

[12] J. L. Rodgers, W. A. Nicewander, *Thirteen ways to look at the correlation coefficient, The American Statistician*, **42** (1988) 59–66.

[13] Z. Gingl, R. Mingesz, *Noise properties in the ideal Kirchhoff-Law-Johnson-Noise secure communication system, PloS one*, **9** (2014) e96109.