www.czasopisma.pan.pl PAN POLSKA AKADEMIA NAUK www.journals.pan.pl

Metrol. Meas. Syst., Vol. 23 (2016), No. 3, pp. 321–331.

PAN POLSKA AKADEMIA NAUK

METROLOGY AND MEASUREMENT SYSTEMS

Index 330930, ISSN 0860-8229

www.metrology.pg.gda.pl

M&MS

COMMENTS ON "A NEW TRANSIENT ATTACK ON THE KISH KEY DISTRIBUTION SYSTEM"

Laszlo B. Kish[1)], Claes G. Granqvist[2)]

1) Texas A&M University, Department of Electrical and Computer Engineering, College Station, TX 77843-3128, USA (✉ Laszlo.Kish@ece.tamu.edu, +1 979 847 9071)

2) Uppsala University, Department of Engineering Sciences, P.O. Box 534, SE-75121 Uppsala, Sweden (Claes-Goran.Granqvist@Angstrom.uu.se)

Abstract

A recent IEEE Access Paper by *Gunn, Allison and Abbott* (GAA) proposed a new transient attack against the *Kirchhoff-law-Johnson-noise* (KLJN) secure key exchange system. The attack is valid, but it is easy to build a defense for the KLJN system. Here we note that GAA's paper contains several invalid statements regarding security measures and the continuity of functions in classical physics. These deficiencies are clarified in our present paper, wherein we also emphasize that a new version of the KLJN system is immune against all existing attacks, including the one by GAA.

Keywords: measurement theory, information security, foundations of physics, engineering over-simplifications.

1. Introduction

Research on and development of unconditionally secure communication and key exchange have a history of progress via attacks and debates and, for example, this type of evolution has taken place for *Quantum Key Distributions* (QKDs) [1, 2, and references therein]. The present paper concerns the classical statistical-physics-based *Kirchhoff-law-Johnson-noise* (KLJN) key distribution system, delineated in Fig. 1, which is no exception to the tradition of the research area, and the creation of the KLJN schemes [3, 4] immediately triggered attacks [5–7]. The various attacks [5–16] have led to useful discussions [17–23], including corrections of flaws in the attacks [19–23] and developments of new defense protocols [5, 10, 11, 13, 24, 25] as well as protocols that have increased immunity against attacks in general [24–27]. Furthermore, KLJN schemes that are totally immune to a certain attack have been presented [13, 28–30] as has a new system that is immune to *all* existing attacks [31]. Responses to the attacks have included plain denials of their validity [18, 21–23], and in some cases experimental results that purportedly supported an attack have been found flawed [23]. The debates sometimes represent a standoff between opposing parties with different scientific backgrounds, which is a typical feature of science debates on breakthrough results in physics, as observed already by Max Planck [32].

Recently, *Gunn, Allison and Abbott* (GAA) published an interesting paper [15] with the first attack utilizing transients at the beginning of the bit-exchange. Their idea is impressively simple and involves monitoring the mean-square voltage before the front of the transient reaches the other end of the communication cable. We note that this approach requires a very short sampling time – less than 10% of the correlation time for the noise [14] – and the relative change of the voltage is typically small during this period.

In a simple illustration of the key effect of GAA's approach, we assume that Eve monitors the voltage on the cable while its capacitance C is charged up by a DC voltage via a resistor R.

Article history: received on Apr. 19, 2016; accepted on May 12, 2016; available online on Jul. 18, 2016; DOI: 10.1515/mms-2016-0039.

According to the Johnson-Nyquist formula [3], the voltage noise spectrum can be written as $S(f) = 4\,kTR$ – where f is frequency, k is Boltzmann's constant and T is temperature – which means that a larger resistance has a higher mean-square voltage. Thus the DC voltage scales with $\sqrt{R}$, whereas the RC time constant scales linearly with the resistance and the rate scales inversely with this time constant. If Alice and Bob use no precaution and abruptly switch the resistors (with their generators) to the line, then the mean absolute value of the rate-of-change for cable voltage at the entry point will scale as $\sim 1/\sqrt{R}$. It is also obvious from the above considerations that a linear ramping-up of the noise amplitude is not helpful, at least not if the communicating parties perform the ramping in a symmetrical fashion as in the first experimental demonstration [11] of the KLJN scheme.

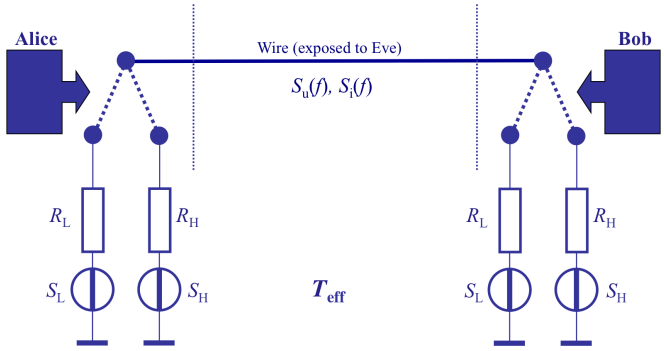

Fig. 1. An outline of the KLJN scheme without defense circuitry [3] against active (invasive) attacks and attacks utilizing non-idealities. The R_L and R_H resistors, identical pairs at Alice and Bob, represent the Low (L) and High (H) bit-values. The corresponding (band-limited) white noise spectra S_L and S_H form identical pairs at the two ends, but they belong to independent Gaussian stochastic processes. Both parties are at the same temperature T_{eff}, so the net power flow is zero. The LH and HL bit-situations of Alice and Bob produce identical voltage and current noise spectra, S_u and S_i, in the wire, implying that they represent a secure bit exchange. The total loop resistance R_{loop} is publicly known and can be calculated by the measured voltage noise or current noise spectrum and the Johnson formula, for example as $R_{loop} = 4\,kT/S_i$. In the LH and HL case, Alice and Bob can calculate the resistance at the other end of the cable by subtracting their own resistance value from R_{loop}. The LL and HH bit arrangements, which occur in 50% of the cases, do not offer security. Consequently, 50% of the bits must be discarded. This system works also with arbitrary, continuum resistor values to securely generate and share continuum random numbers.

We have confirmed GAA's conclusion [15] that their attack works with about $p = 0.7 - 0.8$, where p is Eve's probability of successfully guessing the key-bits. These values of p require four stages of the simplest XOR-based privacy amplification in order to reduce p to its ideal range of $0.5 < p < 0.5006$ [33], which implies a corresponding 16-fold slowdown of the key exchange. Then, the corresponding relative information leak toward Eve is less than 10^{-8} [33].

2. A KLJN scheme that is immune against the attack

There are many easily executable ways to reduce the efficiency of GAA's attack [15], and some of them were outlined in their paper. Here, we emphasize that the new *Random-Resistor-Random-Temperature* (RRRT) KLJN scheme [31], see Fig. 2, is *totally immune* against not only GAA's recent attack but against *all* presently known attacks.

Metrol. Meas. Syst., Vol. 23 (2016), No. 3, pp. 321–331.

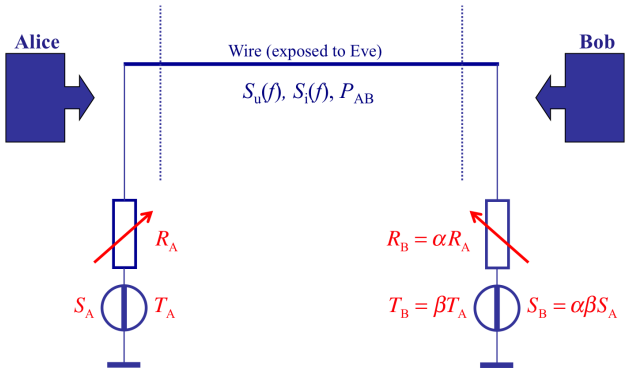

Fig. 2. An outline of the RRRT-KLJN scheme [31]. The temperatures and resistors at Alice (A) and Bob (B), and their corresponding voltage noise spectra, are continuum random variables with a new random choice made at the beginning of each KLJN period. The Low (*L*) and High (*H*) bit values at Alice and Bob are determined by relative resistance values; for example, the party with the higher resistance has the high bit. Eve cannot determine even the sum of the resistance values, because there is no public knowledge about the temperatures, and the mean-square noise voltages and the resistances fluctuate independently.
(Various symbols are defined in Fig. 1 and elsewhere [31]).

The mean-square generator voltages and the resistance values are independent random variables, and hence Eve cannot relate the measured transient mean-square voltage to the resistance value. Thus, GAA's transient attack [15] yields zero information leak about the key ($p = 0.5$).

3. Deficiencies in the GAA paper

The main reason for writing our present article is that, although GAA's attack works, there are important deficiencies in their paper [15], which we want to correct. A general comment is that GAA's paper is poorly documented and void of details regarding simulations: for example, what cable model or software was used, how were the noise generated, what simplifications were assumed, *etc*. All of these questions point at essential information needed for assessing the validity of, and potential flaws in, GAA's simulations [14, 22–24].

We confirmed GAA's results [15] by use of the LTSPICE industrial cable simulator (details of these types of simulations, and their underlying assumptions, are described elsewhere [14]), and in this section we focus on remaining problems inherent in GAA's work [15]. First, in subsections A and B, we address two minor mistakes, the second one possibly emanating from an inadequacy in our former paper [24], which we also correct here. Finally, in subsection C, we deal with major flaws in GAA's paper [15] regarding physics and security claims based on incomplete circuit theory.

A. Secrecy rate as a measure of unconditional security

GAA [15] use the term "secrecy rate" to characterize security. We note that GAA cite several old papers concerning the secrecy rate [4, 17, 34, 35], but this term does not exist in the mentioned papers. For a modern discussion of "secrecy rate", we refer to work by Chorti and Poor [36].

When using the secrecy rate to characterize security, the bit-error probability q of Alice and Bob enters into the result: the higher the q, the lower the secrecy rate. Under certain special conditions, but not for KLJN in general, one can relate the secrecy rate to the maximum rate of secure bit-exchange after privacy amplification. However, security (secrecy) and secrecy rate are like apple and orange: both are fruits but are completely different. The secrecy rate is not

an ultimate measure of security but is only a practically useful performance parameter in some special situations of secure communication [36]. The basic condition of (perfect unconditional) secrecy of key exchange is that the probability of Eve's successful guessing the key-bit is not improved by her monitoring the key exchange [37, 38].

When Eve's knowledge of a uniformly generated key is zero, then her probability of successfully guessing the bits is 0.5. In the case of perfect secrecy (security), p remains at this value even when Eve is eavesdropping, and the bit-error probability of key exchange between Alice and Bob is irrelevant. We offer the following illustrative example to show the inadequacy in using the secrecy rate to judge the security of the KLJN system [39, 40]. By manipulating wire resistance, frequency bandwidth and bit-detection thresholds, it is possible to design two different KLJN systems with the identical secrecy rate; one of the systems has very poor security ($p \approx 1$) while the other has very strong security ($p \approx 0.5$).

One should note that, in the case of the KLJN system, the bit-error probability can be so low that it is not even measurable, such as 10^{-20}, and therefore the use of secrecy rates may lead to the same conclusions as when p is employed. However, it is incorrect to use the secrecy rate in order to characterize the level of unconditional security of key exchange, and such an error can produce misleading results.

B. Parameter tuning to approach perfect security

The Appendix of GAA's work [15] contains some incorrect comments about our general security proof [24] for the KLJN key exchange. Here we discuss a minor issue: how to reach a desired security level by properly tuning the parameters of the KLJN system to be sufficiently close to their ideal values. For a mathematical proof of unconditional security, it is not necessary that this tuning is economical or practical – the tuning merely has to be physically achievable.

We first note that GAA cites the classical Diffie-Hellman paper [41] (their reference [2]) about unconditional security. This paper is from the times when physical unconditionally secure key exchange did not yet exist and the key was supposed to be perfectly unconditionally secure (such as by delivery via courier) or only conditionally secure by using one-way-functions. Unconditional security of physical key exchangers, on the other hand, was introduced [1] 25 years later by Mayers [42]. An unconditionally secure physical key-exchanger is never perfectly secure, but perfect security can be approached arbitrarily at least conceptually.

GAA argue [15] correctly that, when parameters are tuned towards their ideal values to match security requirements, there are some parameters that may have limits for doing that. GAA use the example of cable length, which can rarely be close to zero (except in intra-instrument chip-to-chip communication). This limitation is true, but the goal of a proof for unconditional security is to show that there is a set of practical parameter values for which the required security level is reached. This was proved by us [24] via the continuity of functions in stable classical-physical systems, which implies that the parameters approach their ideal values when p converges towards 0.5 representing perfect security. However, *all* parameters are not required to approach their ideal values for convergence to perfect security. For example, the influence of a large cable-length can be evaded by privacy amplification [33] at the cost of a sufficiently small bandwidth (the more privacy amplification steps, the smaller the bandwidth), and thus one can reach the required security level even when the cable-length is significant. Clearly, invested time is the ultimate price to pay in order to approach perfect security, which is the same as in QKD [1].

We now illustrate the case of a finite cable-length with the hypothetical function $p = 0.5 + xy$, where x represents the cable-length and y the reduced bandwidth (reciprocal of the duration of bit-exchange). Perfect security is approached when $x \to 0$ and/or $y \to 0$. Consequently, it is not necessary that both x and y approach their ideal values; one parameter can stay significant

Metrol. Meas. Syst., Vol. 23 (2016), No. 3, pp. 321–331.

and the system still converges to perfect security. Practical situations are of course more complex and less ideal than in this example.

Finally, we note that our previous paper [15] contains an inadequacy in (5), where the Taylor polynomial is shown only up to the first order. However, most effects in the KLJN system require an expansion at least up to the second order and that is so for the example above. However, the inadequacy does not alter the main conclusion about the existence of unconditional security and the fact that the fundamental base of unconditional security of the KLJN system lies in the continuity of functions in stable classical-physical systems and in the existence of a parameter set, belonging to perfect security, which can be approached in a continuum fashion.

C. Continuity of functions in stable classical-physical systems

The last and most important point of concern about GAA's paper [15] deals with security versus physics. As an objection to our earlier argument [24] that p can be tuned in a continuous fashion in KLJN, GAA claim in the Appendix of their article [15], by using a circuit example, that functions in stable classical-physical systems are not always continuous.

This is an assertion with very far-reaching consequences! However, it must be incorrect since otherwise the whole theoretical framework, as well as the education, of classical physics – including mechanics, elasticity, electrodynamics, fluid dynamics, statistical physics, condensed matter physics, *etc*. [43–50] – are flawed. We therefore investigate GAA's claim [15] and argue that there are three different types of errors in their argumentation; they are related to electrical circuit theory, security and physics.

We first note that the system examined by GAA [15] is *not* the KLJN system. The circuit underlying their demonstration is shown in Figure 3, which represents a situation wherein it is publicly known that Alice and Bob have 1 Ω resistors whereas their DC voltages U_A and U_B are secret. For the sake of simplicity, we assume that the arbitrary voltages U_A and U_B represent bit-values in a pre-agreed, realistic fashion. Eve measures the voltages U_{AE} and U_{BE}. If $R_E > 0$, she can exactly determine the voltages U_A and U_B from the measured quantities, and thus Eve has perfect eavesdropping of the bit-values ($p = 1$). In the case of $R_E = 0$, see Fig. 4, Eve cannot determine the secret voltages from U_{AE} and U_{BE} because the related matrix is not invertible, and then GAA [15] argue that Eve has zero information about the bits ($p = 0.5$). From this fact, GAA conclude that the transition from complete information with $p = 1$ (at $R_E > 0$) to zero information with $p = 0.5$ (at $R_E = 0$) proves the existence of a non-continuous $p(R_E)$ function because of the singularity of p at $R_E = 0$. Thus, GAA profess that a function related to security is non-continuous in a classical-physical system.

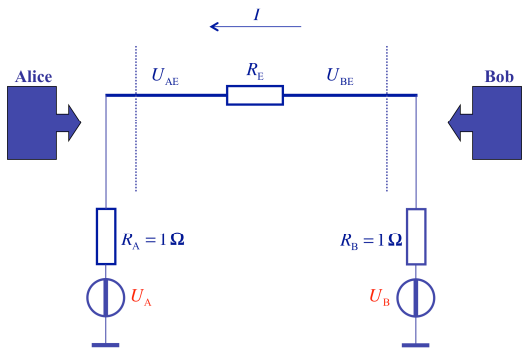

Fig. 3. An outline of the situation wherein Eve knows the resistor values and measures the voltages U_{AE} and U_{BE}. If $R_E > 0$, she can determine the voltages U_A and U_B.

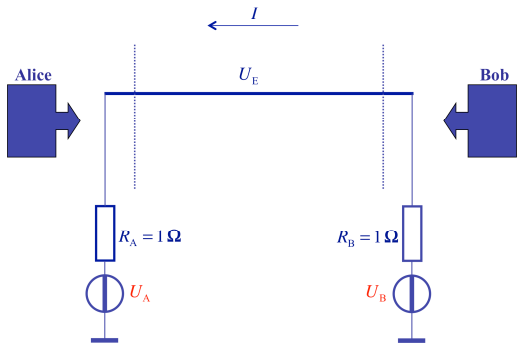

Fig. 4. An outline of the situation wherein Eve measures voltage and knows the resistor values but still cannot find out the voltages. However, this is an absurdly limited Eve because she does not measure current, which contradicts the rules of security that Eve must utilize all of the information she has access to. If she measures also the current, she can determine the voltages.

The following questions emerge as a result of GAA's claims:

(i) When GAA [15] discuss security and eavesdropping, do they follow the elementary rules of attacks against unconditional security, in particular, do they exploit all of Eve's available circuit measurement tools in the attack?

(ii) Is GAA's approach physical or is it only an unphysical engineering-type simplification from which one cannot draw safe conclusions about underlying physics?

(iii) If GAA's approach is indeed unphysical, does their conclusion hold if their approach is modified so as to make it physical?

4. Discussion

We now scrutinize the questions (*i*)–(*iii*). The answer to question (*i*) is that by ignoring the possibility of current measurement one makes a circuit-theoretical mistake that leads to an absurdly limited Eve. This contradicts the basic rules of security analysis that Eve must utilize all of the information she has access to. If she measures also the current I, as can be done in various ways, she can determine the voltages exactly by $U_A = U_E - I*1\Omega$ and $U_B = U_E + I*1\Omega$. Clearly, the role of a non-zero R_E is to enable current to be used in order to provide extra information via the voltage drop over R_E and, equally obviously, this information is lost at $R_E = 0$. Consequently, there is no discontinuity within GAA's approach [15]. In fact, Eve's eavesdropping ability is constant and maximum ($p = 1$), and hence the situation explored by GAA does not offer security.

The reply to question (*ii*) is that the system GAA investigate [15] in order to challenge a fundamental rule of classical physics is unphysical because their circuit model does not contain the Johnson noise voltage sources of the resistances. This deficiency implies an underlying assumption about the physical system, *i.e.* its being at zero absolute temperature. However, zero absolute temperature cannot be reached as a consequence of the laws of thermodynamics and statistical physics, and assuming its existence renders GAA's model unphysical.

To answer question (*iii*), finally, we make GAA's system physical by adding Johnson noise generators $U_{An}(t)$, $U_{Bn}(t)$ and $U_{En}(t)$ to the corresponding resistors; see Fig. 5. The impact of the non-zero noise is pervasive, and the Gaussian distribution of Johnson noise voltage guarantees non-perfect eavesdropping and a continuous transition of p towards $R_E = 0$. The amplitude density of a Gaussian process will never reach zero and thus, mathematically, noise can cause bit-flips at any finite value of U_A and U_B. For $R_E \to 0$, the DC voltage drop and noise on R_E scale

Metrol. Meas. Syst., Vol. 23 (2016), No. 3, pp. 321–331.

with R_E and $\sqrt{R_E}$, respectively, which implies that the relative inaccuracy of the measured voltage on R_E scales with $1/\sqrt{R_E}$ and is divergent when approaching the limit of $R_E = 0$; this divergence takes place in a continuum fashion. Perfect eavesdropping at non-zero R_E can be achieved only via infinitely long time-averaging, which is an unphysical situation. Consequently, p is a continuous function of R_E at finite-time averaging and non-zero temperature.

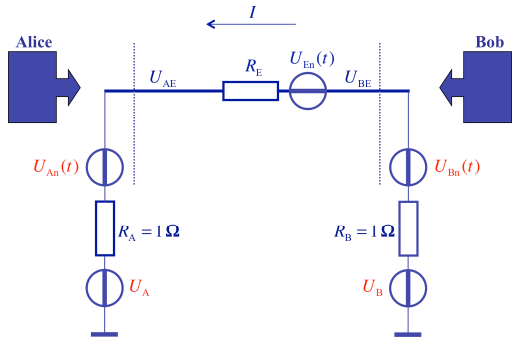

Fig. 5. An outline of the situation encompassing correct physics represented by non-zero Johnson noise voltages of the resistors. The impacts of U_{An} and U_{Bn} are significant: for GAA's absurdly limited Eve it provides non-perfect eavesdropping and a continuous change of the information leak when R_E converges to zero. Perfect eavesdropping can be achieved only after infinitely long time-averaging, which is unphysical.

5. Conclusions

We have analysed a recent paper entitled "A New Transient Attack on the Kish Distribution System" by Gunn, Allison and Abbott [15]. Their attack is valid, but countermeasures are readily found. Our present paper discusses the arguments behind the attack, and we show a number of found that are sufficiently general to warrant a detailed treatment, as presented above. In particular, GAA's "proof" of the existence of a discontinuous function in a stable, linear, classical-physical system is invalid. Continuous functions prevail as soon as the system is made physical by including unavoidable thermal fluctuations. Our analysis shows, once again, that *over-simplified engineering models are unable to prove or disprove the Laws of Physics*.

Appendix

This manuscript, in its various versions, has been criticized by reviewers and others on issues of a fundamental character. Some of these issues, we believe, are connected with traditions and lines of thought entrenched in different disciplines, such as in Engineering and in Physics. Here we give a brief discussion of some of the contentious items that may be of general relevance and where, as we perceive the situation, the engineering tradition leads to over-simplified, or even erroneous, results. We underscore that the present exposition is preliminary and awaiting a more in-depth treatment.

Our presentation in this paper rests on the existence of *continuous functions*. It has been questioned that such functions are important for the present purpose, and it has been argued that we are guilty of having invented an "imaginary law" without giving any reference. However, it is an elementary issue that, in classical physics, functions describing linear systems and stable non-linear systems must be continuous. This is the very reason why differential calculus

can be applied throughout classical physics [43–50]! The reliance on continuous functions is usually not stated explicitly, but it is as basic as the assumption that calculations in physics follow the rules of algebra.

As a history aside, we note that the realization that continuous functions describe physics is underlying Newton's formulation of differential and integral calculus. Discontinuities simply do not exist in classical physics, and if a model says so it is over-simplified.

We illustrate our view with an example: High-school physics says that, when we heat ice, after reaching the melting point the temperature remains constant during continuous energy influx until the energy representing the latent heat of the ice is exceeded. At first sight this represents a discontinuity. But of course this is not so and statistical thermodynamics tells that the temperature and the latent heat are continuous functions associated with thermal fluctuations at the phase change. In fact, the same effect constitutes a vigorous research field in superconductivity, *viz*., fluctuation-conductance. Other examples could be given.

An asserted counterexample to the continuity of functions in physics, which was put forward by a reviewer, is related to the *special case of Euler's disc*, which is a well-known system in classical physics. A practical example of Euler's disc is a coin spinning on a flat surface. This object oscillates with increasing frequency and then suddenly stops, seemingly via a discontinuous process.

But what does "suddenly stops" mean here? According to Newton's Second Law, the abrupt cessation of non-zero motion of non-zero mass requires an infinitely strong and infinitely narrow pulse of force – *i.e*., a Dirac pulse – which is unphysical although commonly employed in simplified calculations in electrical engineering in order to estimate the behaviour of circuits. However, such simplified engineering-type estimations are insufficient to address fundamental questions in physics.

A deeper investigation of the physics related to Euler's disc shows that it never really stops. Its centre-of-mass and all of its molecules will continue to oscillate randomly to satisfy Boltzmann's Equipartition Theorem, which states that there is $kT/2$ mean energy per thermal degree of motion, where k is Boltzmann's constant and T is absolute temperature. Thus thermal noise guarantees that continuity prevails even when a simplified model may predict a discontinuity.

Another bone of contention regards the fact that GAA's paper, discussed by us above, purportedly highlights *discontinuities in a probability function*. As an example, it was argued that a stochastic physical system subjected to some limiter or threshold would have a truncated distribution (*i.e*., a discontinuity), and therefore GAA's paper would be perfectly valid.

But this assertion is flawed. Probability functions are always continuous in any physical system, and this includes not only classical physics but also quantum physics. Freshman quantum physics of quantum tunnelling serves as a good example: This treatment uses the fact that wave functions and their squared absolute values, which are the probability density of the particle under consideration, are always continuous whenever the height of the potential barrier is finite, *i.e*., for any physical system. The underpinning reason for this can be found in Schrödinger's Equation. There are certainly discontinuous energy solutions in solid-state quantum systems, but they represent different states and continuity persists within any single state. The only discontinuities of probability in quantum physics happen during quantum measurements.

Finally, a reviewer claimed that "a stochastic physical system that is subjected to some limiter or threshold will have a truncated distribution". But this is obviously unphysical, and no physical limiter or threshold can be mathematically abrupt. There is always a continuous transition at the level of the limitation, which is evident since an abrupt limit would require not only infinite power but also infinitely fast response – and both requirements are unphysical. The analogy to Euler's disc is evident.

Metrol. Meas. Syst., Vol. 23 (2016), No. 3, pp. 321–331.

Acknowledgements

Valuable discussions with Horace Yuen, Vincent Poor, Tamas Erdelyi and Laszlo Leindler are appreciated.

References

[1] Yuen, H. (2016). Security of quantum key distribution. *IEEE Access*, 4, 724–749.

[2] Makarov, V., Bourgoin, J.P., Chaiwongkhot, P., Gagne, M., Jennewein, T., Kaiser, S., Kashyap, R., Legre, M., Minshull, C., Sajeed, S. (2015). Laser damage creates backdoors in quantum communications. *ArXiv*, 1510.03148, (submitted for publication).

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

[4] Cho, A. (2005). Simple noise may stymie spies without quantum weirdness. *Science*, 309, 2148.

[5] Kish, L.B. (2006). Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson(-like)-noise cipher and expansion by voltage-based security. *Fluctuation and Noise Letters*, 6, L57–L63.

[6] Scheuer, J., Yariv, A. (2006). A classical key-distribution system based on Johnson (like) noise-how secure? *Physics Letters A*, 359, 737–740.

[7] Hao, F. (2006). Kish's key exchange scheme is insecure. *IEE Proceedings – Information Security*, 153, 141–142.

[8] Liu, P.L. (2009). A new look at the classical key exchange system based on amplified Johnson noise. *Physics Letters A*, 373, 901–904.

[9] Bennett, C.H., Riedel, C.J. (2013). On the security of key distribution based on Johnson-Nyquist noise. *ArXiv*, 1303.7435.

[10] Kish, L.B., Mingesz, R. (2006). Totally secure classical networks with multipoint telecloning (teleporation) of classical bits through loops with Johnson-like noise. *Fluctuation and Noise Letters*, 6, C9–C21.

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

[12] Gunn, L.J., Allison, A., Abbott, D. (2014). A directional wave measurement attack against the Kish key distribution system. *Scientific Reports*, 4, 6461.

[13] Kish, L.B., Granqvist, C.G. (2014). Elimination of a second-law-attack, and all cable-resistance-based attacks, in the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system. *Entropy*, 16, 5223–5231.

[14] Chen, H.P., Gonzalez, E., Saez, Y., Kish, L.B. (2015). Cable capacitance attack against the KLJN secure key exchange. *Information*, 6, 719–732.

[15] Gunn, L.J., Allison, A., Abbott, D. (2015). A new transient attack on the Kish key distribution system. *IEEE Access*, 3, 1640–1648.

[16] Chen, H.P., Mohammad, M., Kish, L.B. (2016). Current injection attack against the KLJN secure key exchange, accepted for publication. *Metrol. Meas. Syst.*, 23(2), 173–181.

[17] Kish, L.B. (2006). Response to Feng Hao's paper "Kish's key exchange scheme is insecure". *Fluctuation and Noise Letters*, 6, C37–C41.

[18] Kish, L.B. (2006). Response to Scheuer-Yariv: "A classical key-distribution system based on Johnson (like) noise-how secure?" *Physics Letters A*, 359, 741–744.

[19] Kish, L.B., Scheuer, J. (2010). Noise in the wire: The real impact of wire resistance for the Johnson (-like) noise based secure communicator. *Physics Letters A*, 374, 2140–2144.

[20] Kish, L.B., Abbott, D., Granqvist, C.G. (2013). Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law-Johnson-noise scheme. *PloS One*, *8*, e81810. Open access.

[21] Chen, H.P., Kish, L.B., Granqvist, C.G. (2014). On the "cracking" scheme in the paper "A directional coupler attack against the Kish key distribution system" by Gunn, Allison and Abbott. *Metrol. Meas. Syst.*, 21(3), 389–400.

[22] Kish, L.B., Gingl, Z., Mingesz, R., Vadai, G., Smulko, J., Granqvist, C.G. (2015). Analysis of an attenuator artifact in an experimental attack by Gunn-Allison-Abbott against the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system. *Fluctuation and Noise Letters*, 14, 1550011.

[23] Chen, H.P., Kish, L.B., Granqvist, C.G., Smulko J. (2015), Waves in a short cable at low frequencies, or just hand-waving? What does physics say? *23rd International Conference on Noise and Fluctuations (ICNF 2015)*, Xi'an, China, Jun. 2–5, 2015, DOI: 10.1109/ICNF.2015.7288604; *ArXiv*, 1505.02749.

[24] Kish, L.B., Granqvist, C.G. (2014). On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator. *Quantum Information Processing*, 13, 2213−2219.

[25] Mingesz, R. (2013). Experimental study of the Kirchhoff-law-Johnson-noise secure key exchange. *International Journal of Modern Physics: Conference*, 33, 1460365, DOI: 10.1142/S2010194 514603652.

[26] Kish, L.B. (2013). Enhanced secure key exchange systems based on the Johnson-noise scheme. *Metrol. Meas. Syst.*, 20(2), 191–204.

[27] Smulko, J. (2014). Performance analysis of the "intelligent" Kirchhoff-law-Johnson-noise secure key exchange. *Fluctuation and Noise Letters*, 13, 1450024.

[28] Liu, P.L. (2009). A key agreement protocol using band-limited random signals and feedback. *Journal of Lightwave Technol*ogy, 27, 5230–5234.

[29] Kish, L.B., Horvath, T. (2009). Notes on recent approaches concerning the Kirchhoff-law-Johnson-noise-based secure key exchange. *Physics Letters A*, 373, 2858–2868.

[30] Vadai, G., Mingesz, R., Gingl, Z. (2015). Generalized Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system using arbitrary resistors. *Scientific Reports*, 5, 13653.

[31] Kish, L.B., Granqvist, C.G. (2016). Random-resistor-random-temperature KLJN key exchange. *Metrol. Meas. Syst.*, 23(1), 3–11.

[32] Planck, M. (1949). *Scientific Autobiography and Other Papers.* New York: Philosophical Library.

[33] Horváth, T., Kish, L.B., Scheuer, J. (2011). Effective privacy amplification for secure classical communications. *EPL (Europhysics Letters)*, 94, 28002.

[34] Maurer, U.M. (1993). Secret key agreement by public discussion from common information. *IEEE Transaction on Information Theory*, 39, 733–742.

[35] Wyner, A.D. (1975). The wire-tap channel. *Bell Systems Technology Journal*, 54, 1355–1387.

[36] Chorti, A., Poor, H.V. (2012). Achievable secrecy rates in physical layer secure systems with a helping interferer. *International Conference on Computing, Networking and Communications (ICNC)*, Maui, Hawaii, 18–22, DOI: 10.1109/ICCNC.2012.6167408.

[37] Shannon, C.E. (1949). Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28, 656–715.

[38] Gilbert, G., Hamrick, M. (2002). Secrecy, computational loads and rates in practical quantum cryptography. *Algorithmica*, 34, 314–339.

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

[40] Saez, Y., Kish, L.B., Mingesz, R., Gingl, Z., Granqvist, C.G. (2014). Bit errors in the Kirchhoff-law-Johnson-noise secure key exchange. *International Journal of Modern Physics: Conference Series*, 33, 1460367.

[41] Diffie, W., Hellman, M.E. (1976). New directions in cryptography. *IEEE Transaction on Information Theory*, 22, 644–654.

[42] Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM*, 48, 351–406.

[43] Landau, L.D., Lifshitz, E.M. (1969). *Mechanics*. Pergamon, Oxford.

[44] Landau, L.D., Lifshitz, E.M. (1971). *The Classical Theory of Fields*. Pergamon, Oxford.

Metrol. Meas. Syst., Vol. 23 (2016), No. 3, pp. 321–331.

[45] Landau, L.D., Lifshitz, E.M., Pitaevskiĭ, L.P. (1984). *Electrodynamics of Continuous Media. Butterworth-Heinemann.* Oxford.

[46] Landau, L.D., Lifshitz, E.M. (1980). *Statistical Physics. Butterworth-Heinemann*. Oxford.

[47] Lifshitz, E.M., Pitaevskiĭ, L.P. (1980). *Statistical Physics, Part 2, Theory of the Condensed State. Butterworth-Heinemann*. Oxford.

[48] Lifshitz, E.M., Pitaevskiĭ, L.P. (1981). *Physical Kinetics*. Pergamon, Oxford.

[49] Landau, L.D., Lifshitz, E.M. (1986). *Theory of Elasticity. Butterworth-Heinemann*. Oxford.

[50] Landau, L.D., Lifshitz, E.M. (1987). *Fluid Mechanics*. Butterworth-Heinemann, Oxford.