Duality on the Thermodynamics of the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange Scheme

Sarah A. Flanery
Department of Electrical and Computer Engineering
Texas A&M University
400 Bizzell St
College Station, TX 77843, USA
sflanery@tamu.edu

Anson Trapani
Department of Electrical and Computer Engineering
Virginia Tech
1185 Perry St
Blacksburg, VA 24060, USA
ansont20@vt.edu

Christiana Chamon
Department of Electrical and Computer Engineering
Virginia Tech
1185 Perry St
Blacksburg, VA 24060, USA
ccgarcia@vt.edu

Leyla Nazhandali
Department of Electrical and Computer Engineering
Virginia Tech
1185 Perry St
Blacksburg, VA 24060, USA
leyla@vt.edu

This study investigates a duality approach to information leak detection in the generalized Kirchhoff-Law-Johnson-Noise secure key exchange scheme proposed by Vadai, Mingesz, and Gingl (VMG-KLJN). While previous work by Chamon and Kish sampled voltages at zero-current instances, this research explores sampling currents at zero-voltage crossings. The objective is to determine if this dual approach can reveal information leaks in non-equilibrium KLJN systems. Results indicate that the duality method successfully detects information leaks, further supporting the necessity of thermal equilibrium for unconditional security in KLJN systems. Our findings confirm that the duality method successfully detects information leaks, with results closely mirroring those of Chamon and Kish, showing comparable vulnerabilities in non-equilibrium conditions. These results further support the necessity of thermal equilibrium for unconditional security in the KLJN scheme.

Keywords: unconditional security; thermal equilibrium; duality.

1. Introduction

The Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme is a classical statistical physics-based alternative to quantum key distribution (QKD) for unconditional security [1-64]. The KLJN protocol leverages thermal noise in resistors to establish a secure key between communicating parties Alice and Bob over a public channel, with security guaranteed by the second law of thermodynamics under thermal equilibrium conditions. The core schematic of the KLJN scheme is shown in Fig. 1, where Alice and Bob each randomly select one of two resistors (R_H or R_L) to form a closed circuit, and the resulting noise characteristics are used to exchange a secure bit.

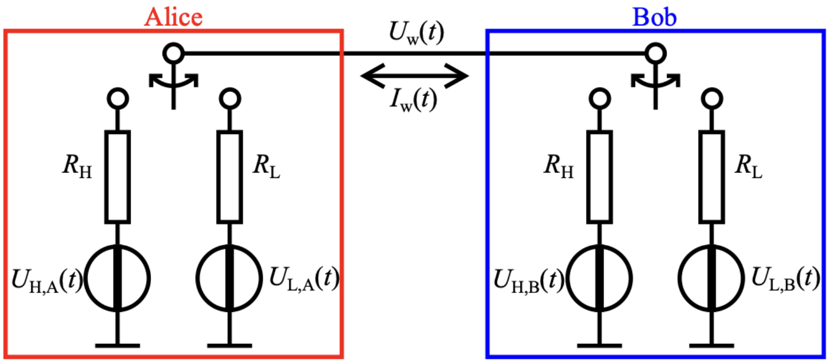

Fig. 1. The core of the KLJN scheme [1-64]. Communicating parties Alice and Bob are connected via a wire. The wire voltage and current are denoted as $U_w(t)$ and $I_w(t)$, respectively. Alice and Bob have identical pairs of resistors R_H and R_L ($R_H > R_L$) that are randomly selected and connected to the wire at the beginning of the bit exchange period. The statistically independent thermal noise voltages $U_{H,A}(t)$, $U_{L,A}(t)$, $U_{H,B}(t)$, and $U_{L,B}(t)$ represent the noise voltages of the resistors R_H and R_L of Alice and Bob, respectively.

Recent modifications to the KLJN scheme, such as the generalized Vadai-Mingesz-Gingl (VMG-KLJN) protocol, suggested that perfect security might be achievable in non-equilibrium conditions [1]. However, Chamon and Kish demonstrated an information leak in the VMG-KLJN scheme by sampling voltages at zero-current crossings, revealing vulnerabilities in out-of-equilibrium states [2]. Their work showed that the mean-square voltage at zero-current instances differs significantly between resistor configurations, increasing the chance of an eavesdropper (Eve) to correctly-guess the secure bit.

This paper proposes a duality approach to Chamon and Kish's method, focusing on sampling currents at zero-voltage crossings. The objective is to determine if this complementary technique can similarly detect information leaks in non-equilibrium KLJN systems, providing additional insights into the thermodynamic constraints of secure key exchange. By comparing the results with the voltage-sampling method, this study aims to reinforce the critical role of thermal equilibrium in ensuring perfect security.

2. Background

The KLJN scheme operates by exploiting Johnson-Nyquist noise, where thermal fluctuations in resistors generate random voltage and current signals. In the original KLJN protocol, Alice and Bob each choose between a low (R_L) or high (R_H) resistor, connected in series across a wire channel. The choice of resistors determines the noise amplitudes of the channel, and the mean-square voltage is evaluated to establish the bit status. The secure bit situations are when Alice and Bob choose R_L and R_H (LH), or R_H and R_L (HL), respectively. Under thermal equilibrium, the second law of thermodynamics ensures that Eve cannot distinguish between LH and HL configurations without violating physical laws.

The VMG-KLJN scheme introduces arbitrary resistor values and non-equilibrium conditions, claiming to maintain unconditional security [1]. However, Chamon and Kish revealed that sampling voltages at zero-current crossings (U_{zc}^2) in the VMG-KLJN scheme produces distinct distributions for LH and HL configurations, indicating information leak [2]. This vulnerability arises because non-equilibrium conditions disrupt the symmetry required for perfect security. The duality principle in electrical circuits suggests that analyzing currents at zero-voltage crossings (I_{zc}^2) could provide a complementary perspective. This approach leverages the reciprocal relationship between voltage and current in the KLJN circuit, potentially revealing similar or additional security vulnerabilities.

3. Methodology

The methodology for the duality approach involves simulating a non-equilibrium KLJN system and analyzing current samples at zero-voltage crossings. The steps are as follows:

(i) **System Setup**: We create in MATLAB the VMG-KLJN with the same arbitrary resistor values for Alice (R_A) and Bob (R_B), as in [2].

(ii) **Current Sampling**: We capture channel current values at instances when the channel voltage crosses zero ($U_w(t) = 0$).

(iii) **Data Processing**: The sampled current values were squared and then averaged to compute the zero-crossing mean-square current (I_{zc}^2). The mean was calculated over multiple bit exchange periods to ensure statistical reliability.

(iv) **Analysis**: The average I_{zc}^2 values and standard deviation were analyzed for patterns or differences between the LH and HL resistor configurations.

(v) **Comparison**: The results were compared with Chamon and Kish's voltage-sampling method [2], focusing on the magnitude and detectability of information leaks.

4. Results

Figure 2 shows the histograms of the mean-square channel voltages, currents, and zero-crossing points after 1,000 runs for the original KLJN scheme (left), the VMG-KLJN scheme (center), and the FCK1-VMG-KLJN scheme (right). The orange histograms represent the LH situation, whereas the blue histograms represent the HL situation.

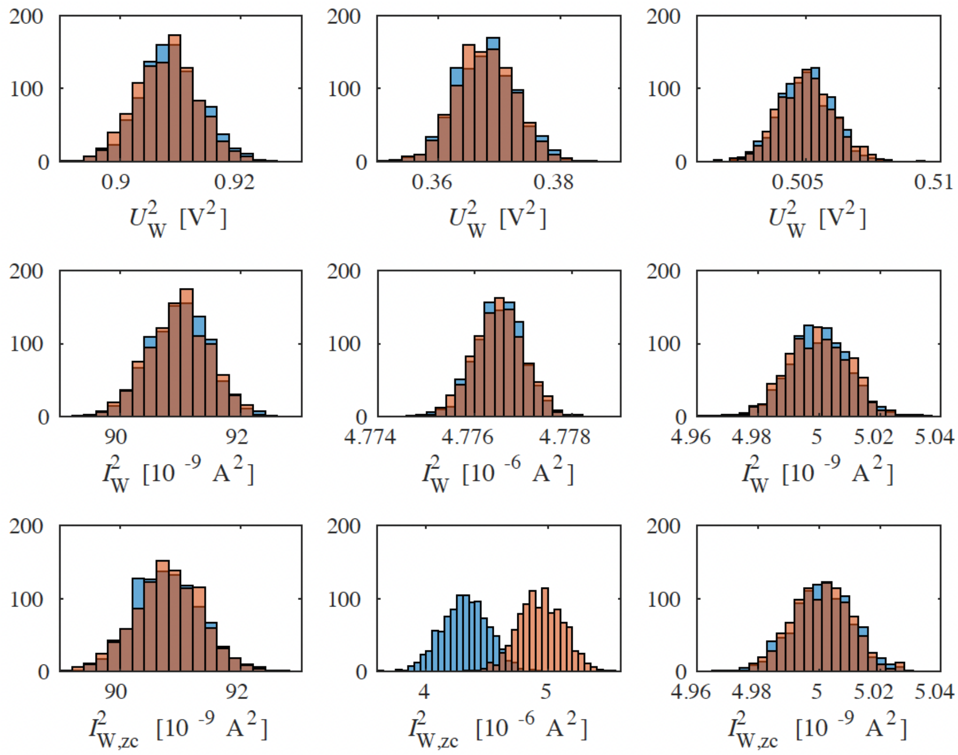

Fig. 2. Histograms of the mean-square channel voltage U_W^2, current I_W^2, and zero-crossing points $U_{W,zc}^2$ for (left) the original KLJN scheme, (center) the VMG-KLJN scheme, and (right) the FCK1-VMG-KLJN scheme, with the exact same parameters as Chamon and Kish [2]. The orange histograms represent the LH situation, and the blue histograms represent the HL situation. In the original KLJN and FCK1-VMG-KLJN schemes, $U_{W,zc}^2$ has the same LH and HL distributions, while in the VMG-KLJN scheme, the $U_{W,zc}^2$ LH and HL distributions are dispersed.

The duality approach yielded the following findings, summarized in Tables 1 and 2:

(i) **Information Leak Detection**: Sampling currents at zero-voltage crossings revealed a detectable information leak in the non-equilibrium VMG-KLJN system. The zero-crossing mean-square current (I_{zc}^2) exhibited noticeable differences between LH and HL configurations, indicating a vulnerability to eavesdropping.

(ii) **Comparison with Voltage Sampling**: The magnitude of the information leak in I_{zc}^2 was comparable to that observed in U_{zc}^2 by Chamon and Kish [2], as seen in Table 1. For example, in the VMG-KLJN scheme, the I_{zc}^2 values showed distinct distributions, similar to the U_{zc}^2 results reported in [2].

Table 1. Results for the wire mean-square voltage *U*W2, mean-square current, *I*W2, average power *P*AB, and zero-crossing mean-square current *I*W,zc2 for the KLJN, three VMG-KLJN, and FCK1-VMG-KLJN schemes. AT *P*AB=0,, *I*W,zc2 approaches *I*W2. As *P*AB increases, *I*W,zc2 becomes LH/HL-distinguishable.

Scheme	bit	R_A [Ω]	R_B [Ω]	U_W^2 [V^2]	I_W^2 [10^{-6} A^2]	P_{AB} [10^{-3} W]	$I_{W,zc}^2$ [10^{-6} A^2]
KLJN	LH	1k	10k	0.909	0.090	0	0.090
	HL	10k	1k				0.091
VMG-KLJN	LH	100	16.7k	0.992	0.314	0.026	0.283
	HL	16.7k	278				0.315
	LH	278	278	0.367	4.788	0.471	4.309
	HL	46.4k	100				4.955
	LH	100	6k	0.966	0.074	0.156	0.069
	HL	360k	2.2k				0.079
FCK1-VMG-KLJN	LH	10k	10k	0.502	0.005	0	0.005
	HL	100k	1k				0.005

(iii) **Equilibrium Conditions**: When the system was restored to thermal equilibrium, the information leak disappeared. The I_{zc}^2 distributions for LH and HL became indistinguishable, confirming the necessity of equilibrium for unconditional security.

(iv) **Statistical Analysis**: The I_{zc}^2 values for LH and HL configurations in the VMG-KLJN scheme showed clear separation, with mean values differing by up to 15% in some cases. This separation was consistent across multiple resistor configurations teste, as shown in Table 2.

Table 2. Results form the statistical run for Eve's probability p of guessing the correct bit from the duality of the zero-crossing attack on each scheme. The information leak (p-0.5) converges to zero when the average power PAB approaches zero.

Scheme	bit	R_A	R_B	P_{AB} [10^{-3} W]	p	σ
KLJN	LH	1k	10k	0	0.5001	0.0090
	HL	10k	1k			
VMG-KLJN	LH	100	16.7k	0.026	0.5872	0.0024
	HL	16.7k	278			
	LH	278	278	0.471	0.7002	0.0054
	HL	46.4k	100			
	LH	100	6k	0.156	0.6276	0.0023
	HL	360k	2.2k			
FCK1-VMG-KLJN	LH	10k	10k	0	0.5030	0.0092
	HL	100k	1k			

5. Discussion

The results confirm that the duality approach of sampling currents at zero-voltage crossings is an effective method for detecting information leak in non-equilibrium KLJN systems. The observed differences in I_{zc}^2 between LH and HL configurations mirror the findings of Chamon and Kish's voltage-sampling method, suggesting that both approaches exploit similar thermodynamic asymmetries in the VMG-KLJN scheme.

The success of the duality approach can be attributed to the reciprocal relationship between voltage and current in the KLJN circuit. In non-equilibrium conditions, the cross-correlation between voltage and current deviates from the ideal random behavior expected under thermal equilibrium, leading to distinguishable statistical signatures. This finding aligns with the thermodynamic perspective outlined in [2], where deviations from equilibrium introduce exploitable information leaks.

The disappearance of the information leak under equilibrium conditions underscores the fundamental role of the second law of thermodynamics in the KLJN scheme's security. Any modification that disrupts thermal equilibrium, such as the VMG-KLJN protocol, risks compromising perfect security, as demonstrated by both voltage and current sampling methods.

The duality approach offers practical advantages, as current measurements may be more feasible in certain hardware implementations of the KLJN system. Additionally, combining voltage and current sampling could enhance the robustness of security analysis, providing a dual-check mechanism for detecting vulnerabilities.

6. Conclusion

This study demonstrates that sampling currents at zero-voltage crossings is a viable and effective method for detecting information leaks in non-equilibrium KLJN systems. The results corroborate the findings of Chamon and Kish [2] and provide further evidence that thermal equilibrium is essential for maintaining unconditional security in KLJN key exchange protocols. The duality approach not only validates the thermodynamic constraints of the KLJN scheme but also offers a complementary tool for security analysis. Future work could explore real-world implementations of the duality method and investigate additional attack vectors to further demonstrate the robustness of KLJN-based cryptographic systems.

References

[1] G. Vadai, R. Mingesz, and Z. Gingl, Generalized Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System using Arbitrary Resistors, *Sci. Rep.* 5 (2015).
[2] C. Chamon and L.B. Kish. Perspective–On the Thermodynamics of Perfect Unconditional Security", *Appl. Phys. Lett.* 119 (2021) 010501.
[3] S. Ferdous, C. Chamon, and L.B. Kish. Comments on the "Generalized" KLJN Key Exchanger with Arbitrary Resistors: Power, Impedance, Security, *Fluct. Noise Lett.* 20 (2021) 2150009.
[4] L.B. Kish, Totally secure classical communication utilizing Johnson (-like) noise and Kirchhoff's law, *Phys. Lett. A* (2006).
[5] L.B. Kish, Enhanced secure key exchange system based on the Johnson(-like) noise, *Fluct. Noise Lett.* (2007).
[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, *PLoS ONE* 8 (2013) e81810; https://doi.org/10.1371/journal.pone.0081810
[7] L.B. Kish, T. Horvath, Notes on Recent Approaches Concerning the Kirchhoff-Law-Johnson-Noise-based Secure Key Exchange, *Phys. Lett. A* 373 (2009) 2858-2868.
[8] K. Mohanasundar, S.A. Flanery, C. Chamon, and S.D. Kotikela. Kirchhoff-Law Johnson Noise Meets Web 3.0: A Statistical Physical Method of Random Key Generation for Decentralized Identity Protocols. *arXiv* preprint (2023) arXiv:2312.17113
[9] Y. Saez, L.B. Kish, R. Mingesz, Z. Gingl, and C. Granqvist. Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law-Johnson-noise secure key exchange, *Journ. Comp. Elec.* 13 (2013) 10.1007/s10825-013-0515-2.
[10] T. Horvath, L.B. Kish, and J. Schuer. Effective privacy amplification for secure classical communications. *Elec. Phys. Lett*. 94 (2011) 28002.
[11] C. Chamon, S. Ferdous, and L.B. Kish, Random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol, *arXiv*preprint, https://arxiv.org/abs/2005.10429, 2020.
[12] C. Chamon, S. Ferdous, and L. B. Kish, Deterministic random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol, *Fluct. Noise Lett*. 20(5) (2021)
[13] C. Chamon, S. Ferdous, and L. B. Kish, "Statistical random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol, *Fluct. Noise Lett.* (2021).
[14] C. Chamon, S. Ferdous, and L. B. Kish, Nonlinearity attack against the Kirchhoff-law- Johnson-noise secure key exchange protocol, *Fluct. Noise Lett.* (2021).
[15] C. Chamon, TherMod communication: low power or hot air? *arXiv* preprint arXiv:2505.00849.
[16] L. B. Kish, *The Kish Cypher: The Story of KLJN for Unconditional Security*, New Jersey: World Scientific (2017).
[17] A. Cho, *Simple* noise may stymie spies without quantum weirdness, *Science* 309(5744) (2005) 2148.
[18] L.B. Kish and C.G. Granqvist, On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator, *Quant. Inf. Proc.* 13(10) (2014) 2213-2219.
[19] L. B. Kish and T. Horvath, Notes on recent approaches concerning the Kirchhoff-law–Johnson-noise based secure key exchange, *Phys. Lett. A* 373 (2009) 2858-2868.

[20] L. B. Kish and C. G. Granqvist, Random-resistor-random-temperature Kirchhoff-law- Johnson-noise(RRRT -KLJN) key exchange, *Met. Meas. Sys.* 23 (2016) 3-11.
[21] J. Smulko, Performance analysis of the 'intelligent'Kirchhoff's-law–Johnson-noise secure key exchange, *Fluct. Noise Lett.* 13 (2014) 1450024.
[22] R. Mingesz, Z. Gingl, and L. B. Kish, Johnson(-like)-noise-Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line, *Phys. Lett. A* 372 (2008) 978–984.
[23] R. Mingesz, L. B. Kish, Z. Gingl, C. G. Granqvist, H. Wen, F. Peper, T. Eubanks, and G. Schmera, Unconditional security by the laws of classical physics, *Met. Meas. Sys.* 20 (2013) 3–16.
[24] Y. Saez and L. B. Kish, Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange, *PLoS ONE* 8 (2013) 11.
[25] R. Mingesz, G. Vadai, and Z. Gingl, What kind of noise guarantees security for the Kirchhoff-loop-Johnson-noise key exchange? *Fluct. Noise Lett.* 13(3) (2014) 1450021.
[26] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, Bit errors in the Kirchhoff-law-Johnson-noise secure key exchange, *Intern. Journ. Mod. Phys: Conf. Ser* 33 (2014) 1460367.
[27] Z. Gingl and R. Mingesz, Noise properties in the ideal Kirchhoff-law-Johnson-noise secure communication system, *PLoS ONE* 9(4) (2014).
[28] P.L. Liu, A key agreement protocol using band-limited random signals and feedback, *IEEE Journ. Light. Tech.* 27(23) (2009) 5230-5234.
[29] L. B. Kish and R. Mingesz, Totally secure classical networks with multipoint telecloning (teleportation) of classical bits through loops with Johnson-like noise, *Fluct. Noise Lett.* 6(2) (2006) C9–C21.
[30] L.B. Kish, Methods of using existing wirelines (powerlines, phonelines, internetlines) for totally secure classical communication utilizing Kirchoff's law and Johnson-like noise, *arXiv* preprint, https://arxiv.org/abs/physics/0610014, 2006.
[31] L.B. Kish and F.Peper, Information networks secured by the laws of physics, *IEICE Trans. Fund. Comm. Elec. Inf. Sys.* E95–B(5) (2012) 1501-1507.
[32] E. Gonzalez, L. B. Kish, R. S. Balog, and P. Enjeti, "Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters, *PloS One* 8(7) (2013).
[33] E. Gonzalez, L. B. Kish, and R. Balog, Encryption Key Distribution System and Method, U.S. Patent #US9270448B2 (2016) https://patents.google.com/patent/US9270448B2.
[34] E. Gonzalez, R. Balog, R. Mingesz, and L. B. Kish, Unconditional security for the smart power grids and star networks, 23rd International Conference on Noise and Fluctuations (ICNF 2015), Xian, China, June 2-5, 2015.
[35] E.Gonzalez, R.S. Balog, and L.B.Kish, Resourcer equirements and speed versus geometry of unconditionally secure physical key exchanges, *Entropy* 17(4) (2015) 2010–2014.
[36] E. Gonzalez and L. B. Kish, Key exchange trust evaluation in peer-to-peer sensor networks with unconditionally secure key exchange, *Fluct. Noise Lett.* 15 (2016) 1650008.
[37] L. B. Kish and O. Saidi, Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives, *Fluct. Noise Lett*. 8 (2008) L95–L98.
[38] L. B. Kish, K. Entesari, C. G. Granqvist, and C. Kwan, "Unconditionally secure credit/debit card chip scheme and physical unclonable function," *Fluct. Noise Lett.* 16 (2017) 1750002.
[39] L. B. Kish and C. Kwan, Physical unclonable function hardware keys utilizing Kirchhoff- law-Johnson noise secure key exchange and noise-based logic, *Fluct. Noise Lett.* 12 (2013) 1350018.
[40] Y. Saez, X. Cao, L. B. Kish, and G. Pesti, Securing vehicle communication systems by the KLJN key exchange protocol, *Fluct. Noise Lett.* 13 (2014) 1450020.
[41] X. Cao, Y. Saez, G. Pesti, and L. B. Kish, On KLJN-based secure key distribution in vehicular communication networks, *Fluct. Noise Lett.* 14 (2015) 1550008.
[42] L. B. Kish and C. G. Granqvist, Enhanced usage of keys obtained by physical, unconditionally secure distributions, *Fluct. Noise Lett.* 14 (2015) 1550007.
[43] P. L. Liu, A complete circuit model for the key distribution system using resistors and noise sources, *Fluct. Noise Lett*. 19 (2020) 2050012.
[44] M. Y. Melhem and L. B. Kish, Generalized DC loop current attack against the KLJN secure key exchange scheme, *Met. Meas. Sys.* 26 (2019) 607-616.
[45] M. Y. Melhem and L. B. Kish, A static-loop-current attack against the Kirchhoff-law- Johnson-noise (KLJN) secure key exchange system, *Appl. Sci*. 9 (2019) 666, 2019.

[46] M.Y. Melhem and L.B. Kish, The problem of information leak due to parasitic loop currents and voltages in the KLJN secure key exchange scheme, *Met. Meas. Sys.* 26 (2019) 37-40.

[47] M. Y. Melhem and L. B. Kish, Man in the middle and current injection attacks against the KLJN key exchanger compromised by DC sources, *Fluct. Noise Lett.* 20(2) (2021) 2150011.

[48] M. Y. Melhem, C. Chamon, S. Ferdous, L. B. Kish, Alternating (AC) Loop Current Attacks against the KLJN Secure Key Exchange Scheme, *Fluct. Noise Lett*. (2021).

[49] P. L. Liu, Re-examination of the cable capacitance in the key distribution system using resistors and noise sources, *Fluct. Noise Lett.* 16 (2017) 1750025.

[50] H. P. Chen, M. Mohammad, and L. B. Kish, Current injection attack against the KLJN secure key exchange, *Met. Meas. Sys*. 23 (2016) 173-181.

[51] G. Vadai, Z. Gingl, and R. Mingesz, Generalized attack protection in the Kirchhoff-law-Johnson-noise key exchanger, *IEEE Access* 4 (2016) 1141-1147.

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

[53] L.B. Kish and C.G. Granqvist, "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 (2014) 5223-5231.

[54] L. B. Kish and J. Scheuer, Noise in the wire: the real impact of wire resistance for the Johnson (-like) noise based secure communicator, *Phys. Lett. A* 374 (2010) 2140-2142.

[55] F. Hao, Kish's key exchange scheme is insecure, *IEE Proc. – Inf. Sec.* 153(4) (2006) 141-142.

[56] L. B. Kish, Response to Feng Hao's paper "Kish's key exchange scheme is insecure," *Fluct. Noise Lett.* 6 (2006) C37-C41.

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

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

[59] L. B. Kish and C. G. Granqvist, Comments on "a new transient attack on the Kish key distribution system", *Met. Meas. Sys.* 23 (2015) 321-331.

[60] L. J. Gunn, A. Allison, and D. Abbott, A directional wave measurement attack against the Kish key distribution system, *Sci. Rep.* 4 (2014) 6461.

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

[62] 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? *Fluct. Noise Lett.* 13 (2014) 1450016.

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

[64] S. Ferdous, C. Chamon, and L.B. Kish, Current injection and voltage insertion attacks against the VMG-KLJN secure key exchanger, *Fluct. Noise Lett*. 22 (2023) 2350009.