applied sciences

MDPI

Article

A Static-loop-current Attack Against the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System

Mutaz Y. Melhem * and Laszlo B. Kish

Department of Electrical and Computer Engineering, Texas A & M University, 3128 TAMU, College Station, TX 77843, USA; laszlokish@tamu.edu

* Correspondence: yar111@tamu.edu; Tel.: +1-979-847-9071

Received: 10 October 2018; Accepted: 12 February 2019; Published: 15 February 2019

Abstract: In this study, a new attack against the Kirchhoff-Law-Johnson-Noise (KLJN) key distribution system is explored. The attack is based on utilizing a parasitic voltage-source in the loop. Relevant situations often exist in the low-frequency limit in practical systems, especially when the communication is over a distance, or between different units within an instrument, due to a ground loop and/or electromagnetic interference (EMI). Our present study investigates the DC ground loop situation when no AC or EMI effects are present. Surprisingly, the usual current/voltage comparison-based defense method that exposes active attacks or parasitic features (such as wire resistance allowing information leaks) does not function here. The attack is successfully demonstrated and proposed defense methods against the attack are shown.

Keywords: KLJN key exchange; unconditional security; ground loop vulnerability; passive attack

1. Introduction

1.1. On Secure Communications

Communications systems, standards, and technologies have been developed since ancient times. Today we have the internet, Internet-of-Things (IoT), operating fourth generation wireless networks (LTE), and the expected fifth generation wireless networks. An important requirement of any communication paradigm between these devices is to accomplish secure communication, i.e., to protect the privacy and integrity of users' data that is transferred over the network. To achieve the security of transferred data which can contain sensitive information (e.g., bank account credentials, social security number, etc.) it is of utmost importance to defend against attacks. These attacks might be launched by an eavesdropper (Eve) who has access to the information channel between the communicating parties A (Alice) and B (Bob). The attack is passive if it eavesdrops without disturbing the channel. The attack is active (invasive) if Eve disturbs or changes the channel, such as with a man-in-the-middle attack. In the present paper, we introduce a new passive attack against the Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme.

1.1.1. Secure Key Exchange

Secure communication systems employ ciphers to encrypt messages (plaintext) and to decrypt encrypted messages (cyphertext). While the creation of a secure and efficient cipher is a complex problem, this problem may be solved simply. Ciphers operate with secure keys that form a momentary shared secret between Alice and Bob. Sharing (exchanging) the key securely is the difficult task. A communicator system cannot be more secure than its key. The security of the key exchange can be conditional or information-theoretic (unconditional).

1.1.2. Conditional Security

Conditionally secure key exchange systems are the ones used generally nowadays. They are software protocols installed at Alice and Bob. Such algorithms utilize computational complexity and achieve only (computationally) conditional security (see e.g., [1,2]). The system is temporarily secure provided the adversary has limited computational resources. A major goal of quantum computer developments is to crack these types of key exchange systems (e.g., the Shor algorithm). From an information-theoretic point of view, security is non-existent because Eve has all the information to crack the encryption, but she needs a long time to do that unless she has a quantum computer or a yet-to-be-discovered classical algorithm that can do the job in a short time. The security is not future-proof.

1.1.3. Unconditional (Information-Theoretic) Security

In order to achieve unconditional (information-theoretic) security at the key exchange, proper laws of physics with a special hardware are utilized. Two major classes of physics-based schemes have emerged for unconditional security:

(i) Quantum key distribution (QKD) [3,4] concepts assume single photons and utilize quantum physics. The underlying laws of physics are Heisenberg's uncertainty principle and the related quantum no-cloning theorem [5]. Even though there are serious debates about the actual level of unconditional security a practical QKD can offer (see e.g., [6–29]), most scientists agree that QKD is unique in its offering information-theoretic security via (a dark) optical fiber and also through air at night, provided the visibility is good.

(ii) The Kirchhoff-Law-Johnson-Noise key distribution method that is based on the statistical physical features of the thermal noise of resistors [30–56]. The related law of physics is the fluctuation-dissipation-theorem (FDT). Some of its advantages are: It works via wire connections including power, phone, and internet lines, which can be used as information channels [31,32] to connect all homes and other establishments. It can be integrated on a chip, which implies excellent robustness, low price, and applicability in bankcards, computers, instruments, and physical unclonable function (PUF) hardware keys [33,34]. Its low price allows general applications such as unconditional security for the control of autonomous vehicular networks [35,36].

1.2. On the KLJN Secure Key Distribution

The KLJN scheme [30–52] utilizes the thermal noise of resistors (or the emulation of that by a specific hardware). In the core scheme Alice and Bob have two identical pairs of resistors, R_{L} and R_{H} ($R_{\mathrm{L}} < R_{\mathrm{H}}$), respectively (see Figure 1).

The key exchange protocol of a single secure bit is as follows: Alice and Bob randomly pick one of their resistors (R_{L} or R_{H}), connect it to the wire channel, and keep them there during the bit exchange period while they execute voltage and/or current measurements to learn the resistor value at the other end (see below).

The noise voltage generators shown in Figure 1 with each resistor can be the resistors' own thermal noise, or an external noise generator emulating a much higher, common *noise-temperature* that is publicly agreed. The power density spectra of the voltage and current in the channel are given by the Johnson-Nyquist formulas [11]

$$S_u(f) = \frac{4kTR_{\mathrm{A}}R_{\mathrm{B}}}{R_{\mathrm{A}} + R_{\mathrm{B}}}, \tag{1}$$

$$S_i(f) = \frac{4kT}{R_{\mathrm{A}} + R_{\mathrm{B}}} \tag{2}$$

where k is the Boltzmann's constant, T is the common temperature, and R_{A} and R_{B} are the actually connected resistances at Alice's and Bob's ends, respectively, with $R_{\mathrm{A}}, R_{\mathrm{B}} \in \{R_{\mathrm{L}}, R_{\mathrm{H}}\}$. After the measurement and spectral analysis, Equations (1) and (2) have two unknown variables, namely,

the values of R_A and R_B, and thus Eve can find the values of the connected resistors, but not necessarily their locations, by solving these equations.

We can represent the four different situations of the connected resistors (R_L and/or R_H) at Alice's and Bob's ends by the indices of the connected resistors, LL, LH, HL, and HH, respectively. As all the resistors have the same (noise) temperature, the ideal system is in thermal equilibrium, where the second law of thermodynamics guarantees zero net power-flow. Hence, Eve cannot use the evaluation of power flow to determine the locations of the momentarily connected resistors unless they have the same resistance values. On the other hand, Alice and Bob can determine the connected resistor values by using Equations (1) or (2) since they know the value of their own connected resistors. When $R_A = R_B$, which happens at 50% of the bit exchange attempts, the results are discarded.

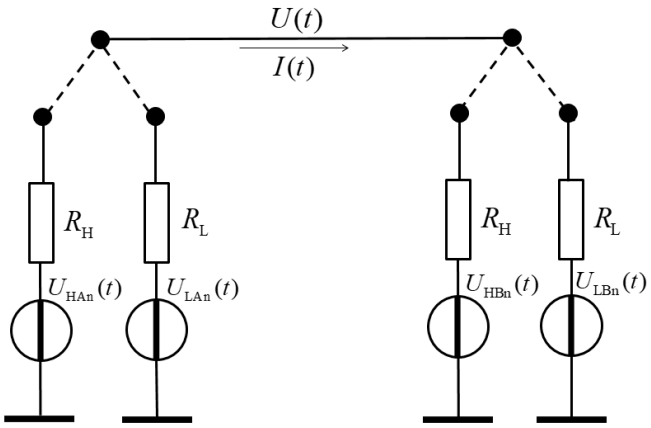

Figure 1. The core of the Kirchhoff-Law-Johnson-Noise (KLJN) system. $U_{HAn}(t)$, $U_{LAn}(t)$, $U_{HBn}(t)$, and $U_{LBn}(t)$ are the (thermal) noise voltage generators for the related resistances R_H and R_L, respectively. $U(t)$ and $I(t)$ are the measured noise voltage and the current in the wire that are used to evaluate the power density spectra $S_u(f)$ and $S_i(f)$, respectively.

On Former Attacks Against the KLJN Secure Key Distribution

Several attacks have been proposed but no attack has been able to compromise the unconditional security of the KLJN scheme because each known attack can efficiently be nullified by a corresponding defense scheme.

The attacks can be categorized into two classes:

(i) Passive attacks that utilize the non-ideal or parasitic features in a practical KLJN system for information leaks. Non-zero wire resistance (see [37,38]) poses the greatest known threat, and the most efficient attack is power balance measurement (Second Law Attack) [39]. An efficient defense is based on a proper temperature-offset [39,40]. Temperature-inaccuracies [41] and resistance-inaccuracies [42] can also cause information leaks. On the other hand, these inaccuracies can compensate for each other [43] if used in a creative way. Non-zero cable capacitance [44] or cable inductance can also yield information leaks that can be fixed by specific designs including the proper choice of frequency range and privacy amplification. Transients can also be utilized for attack [45] but there are various means of defense against these [46,47]. The newest KLJN system, the random-resistor-random-temperature KLJN (RRRT-KLJN) scheme [48], is robust against the above vulnerabilities, or at least, no known attack exists against it yet.

(ii) Active attacks, where Eve either modifies the information channel or she injects an extra current into it. Current injection attacks [30,49] and man-in-the-middle attacks [50] are examples which have been explored [56]. Due to the current and voltage comparison [50] feature and its more advanced cable-modeling version [49], active attacks are, so far, the least efficient attacks against the KLJN scheme.

(iii) Flawed attacks. There are some proposed attack methods that are based on misconceptions and they do not work. See their brief summary and criticism in, for example, papers [51–55] and the book [56].

2. The New Attack Scheme Utilizing Deterministic Loop Currents

2.1. The Situation that Eve Utilizes for the Attack

In practical KLJN systems, in order to save a wire, the common end of the resistors (see Figure 1) is often connected to the ground. In practical situations there is often an imbalance, a voltage difference between various locations of the ground that is due, for example, to ground loop currents or electromagnetic interference (EMI) [53]. This potential information leak was pointed out in [53] as a potential source of information leaks in the case of significant cable resistance. However, it was not realized in [53] that information leaks can exist even at zero cable resistance. The present study is directly relevant for DC current-based ground loops (such as during secure communication between different units in instruments [33,34]). For EMI-induced ground loops, our DC-limited study is only a first step in addressing a more general situation (which should be investigated in future works).

In this paper, we explore this new information leak in the DC parasitic voltage limit. Hence, consideration was given to situations where during the bit exchange period, the relative change in the parasitic voltage is small. For the sake of simplicity but without the limitation of generality, we assume that the imperfection is represented by a positive DC voltage generator located at Alice's end (see Figure 2).

Due to Kerckhoffs's principle of security, that is, the assumption that the enemy knows everything except the momentary key, we must assume that Eve knows the polarity and value of this DC voltage (if she does not know it at first, she will be able to extract it via long-time averaging). The direction of the current $I(t)$ is assumed to point from Alice to Bob. The voltage $U(t)$ and current I(t) in the wire contain the sum of a DC component and an AC (stochastic, that is, noise) component.

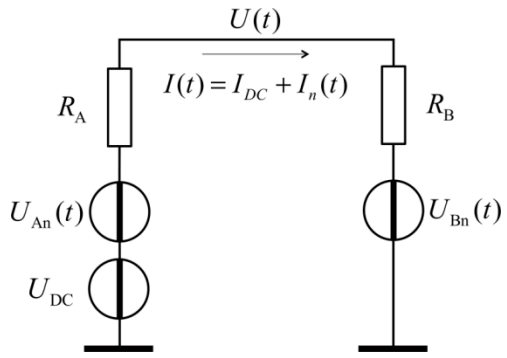

Figure 2. The KLJN system with ground loop voltage. Here $U_{An} \in \{U_{LAn}; U_{HAn}\}$ and $U_{Bn} \in \{U_{LBn}; U_{HBn}\}$ are the voltage noises belonging to the randomly chosen resistors, $R_A \& R_B \in \{R_L; R_H\}$, belonging to Alice and Bob, respectively. U_{DC} is the ground loop DC voltage source and $U(t)$ and $I(t)$ are the voltage and current on the wire, respectively.

Let us analyze the resulting voltages and currents. The current in the wire is

$$I(t) = I_{DC} + I_n(t) \tag{3}$$

where I_{DC} is its DC component

$$I_{DC} = \frac{U_{DC}}{R_A + R_B} \tag{4}$$

and $I_n(t)$ is its AC (noise) component

$$I_{\mathrm{n}}(t) = \frac{U_{\mathrm{An}}(t) - U_{\mathrm{Bn}}(t)}{R_{\mathrm{A}} + R_{\mathrm{B}}} \tag{5}$$

in which U_{An} and U_{Bn}, with $U_{\mathrm{An}} \in \{U_{\mathrm{LAn}}; U_{\mathrm{HAn}}\}$ and $U_{\mathrm{Bn}} \in \{U_{\mathrm{LBn}}; U_{\mathrm{HBn}}\}$, are the voltage noise sources of the chosen resistors, R_{A} and R_{B}, respectively.

The voltage on the wire is

$$U(t) = I(t)R_{\mathrm{B}} + U_{\mathrm{Bn}}(t). \tag{6}$$

From Equations (3) and (6) we obtain

$$U(t) = U_{\mathrm{DCw}} + U_{\mathrm{ACw}}(t) = I_{\mathrm{DC}}R_{\mathrm{B}} + I_{\mathrm{n}}(t)R_{\mathrm{B}} + U_{\mathrm{Bn}}(t) \tag{7}$$

where U_{DCw} and $U_{\mathrm{ACw}}(t)$ represent the DC and AC voltage components in the wire, respectively. The DC component can be written as

$$U_{\mathrm{DCw}} = I_{\mathrm{DC}}R_{\mathrm{B}} = \frac{U_{\mathrm{DC}}}{R_{\mathrm{A}} + R_{\mathrm{B}}}R_{\mathrm{B}}. \tag{8}$$

The DC component is different during Alice's and Bob's LH and HL bit situations of secure bit exchange, which yields information leaks. In the LH situation, that is, when $R_{\mathrm{A}} = R_{\mathrm{L}}$ and $R_{\mathrm{B}} = R_{\mathrm{H}}$, the DC component of the voltage on the wire is

$$U_{\mathrm{DCw}} \equiv U_{\mathrm{LH}} = U_{DC}\frac{R_{\mathrm{H}}}{R_{\mathrm{H}} + R_{\mathrm{L}}} \tag{9}$$

and, in the HL bit situation,

$$U_{\mathrm{DCw}} \equiv U_{\mathrm{HL}} = U_{\mathrm{DC}}\frac{R_{\mathrm{L}}}{R_{\mathrm{H}} + R_{\mathrm{L}}}. \tag{10}$$

Note that as we have been assuming that in the given KLJN setup $R_{\mathrm{H}} > R_{\mathrm{L}}$, in this particular situation

$$U_{\mathrm{HL}} < U_{\mathrm{LH}}. \tag{11}$$

For later usage, we evaluate the average of U_{LH} and U_{HL} and call this quantity the threshold voltage, U_{th}, where

$$U_{\mathrm{th}} = \frac{U_{\mathrm{LH}} + U_{\mathrm{HL}}}{2} = \frac{U_{\mathrm{DC}}}{2}. \tag{12}$$

The effective (RMS) amplitude U_{ACw} of the noise voltage on the wire is identical in both the LH and HL cases:

$$U_{\mathrm{ACw}} = \sqrt{4kTB_W\frac{R_{\mathrm{L}}R_{\mathrm{H}}}{R_{\mathrm{L}} + R_{\mathrm{H}}}}. \tag{13}$$

Note that the voltage and current noises in the wire follow a normal distribution since the addition of normally distributed signals results in a signal that has normal (Gaussian) distribution with a corresponding mean (see Equation (10)) and variance.

For an illustration of the information leak, see Figure 3. The DC component, that is, the mean value of the resulting (AC + DC) Gaussian depends on the bit situation during the secure key exchange. This dependence poses as a source of information for Eve about the secret key. This feature will be exploited below for the new attack scheme.

2.2. The Attack Scheme

The attack consists of three steps: measurement, evaluation, and guessing.

(*i*) Measurement: During a single secure bit exchange, Eve measures N independent samples of the wire voltage.

(*ii*) Evaluation: She evaluates the fraction γ of these N samples that are above U_{th}, which is

$$\gamma = \frac{N^+}{N} \tag{14}$$

where N^+ is the number of samples that are above U_{th}.

(*iii*) Guessing (based on Equations (9)–(14)): For $0.5 < \gamma$ and $\gamma < 0.5$, Eve's guesses are the LH and HL bit situations, respectively. For $\gamma = 0.5$ her decision is undetermined and carries no useful information.

(*iv*) Eve's correct guessing probability p is given as

$$p = \lim_{n_{\text{tot}} \to \infty} \frac{n_{\text{cor}}}{n_{\text{tot}}} \tag{15}$$

where n_{tot} is the total number of guess bits and n_{cor} is the number of correctly guessed bits. The situation $p = 0.5$ indicates perfect security against Eve's attack.

In the next section, we demonstrate the attack method via computer simulation.

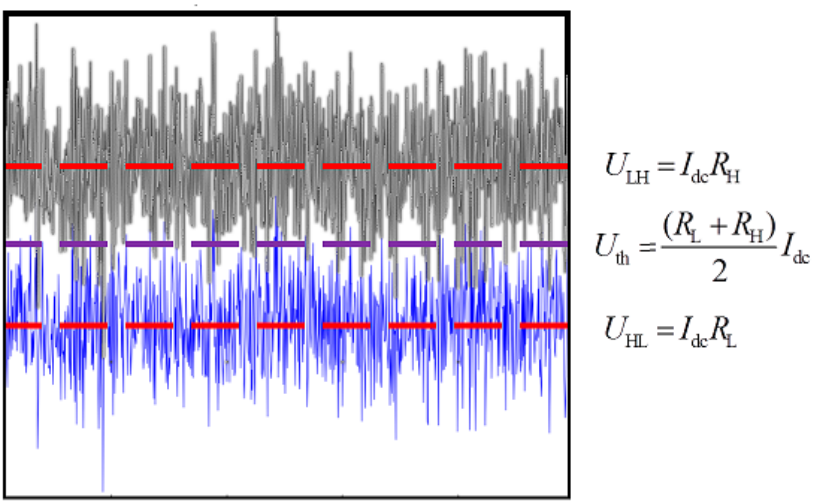

Figure 3. Eve's threshold scheme to guess the bit situation LH versus HL.

3. Simulation Results

To test Eve's correct guessing probability p for the LH situation, we assumed that Alice and Bob selected $R_{\text{L}} = 1$ kΩ and $R_{\text{H}} = 10$ kΩ. During these experiments, the DC voltage was kept at a constant level of 0.1 V (see Figures 2 and 3). To generate noise, we used the white Gaussian noise function (wgn) from the Matlab communication system toolbox to test the success statistics of the attack scheme while varying the temperature. The effective bandwidth Δf and the range of temperatures were 1 MHz and $10^8 < T < 10^{18}$ K, respectively. At lower temperatures p was 1, within the statistical inaccuracy of simulations; at the high-temperature limit it converged to 0.5. The duration of the secure bit exchange period was characterized by the number N of *independent* noise samples used during the exchange of the particular bit.

We tested secure key length M = 700 bits at different bit exchange durations represented by sample/bit numbers N = 1000, 500, and 200, respectively. Figure 4 shows Eve's correct guessing probability (p) of a key bit versus temperature. With temperature approaching infinity, the effective noise voltage on the wire also approaches infinity and the Gaussian density function is symmetrically distributed around the threshold voltage U_{th}. Thus, the probabilities of finding the noise amplitude above or below U_{th} are identical (0.5) Therefore, Eve's correct guessing probability represents the perfect security limit, p = 0.5.

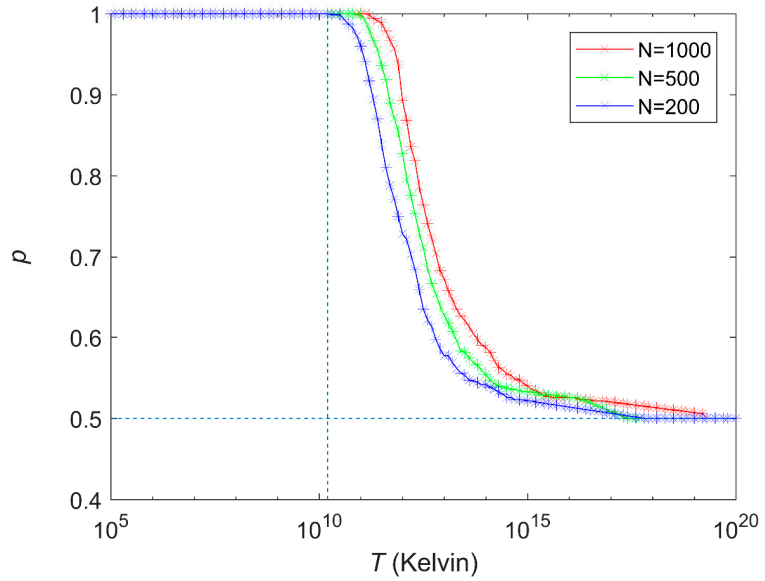

Figure 4. Eve's correct guessing probability (p) of key bits versus temperatures at bandwidth Δf equals 10^6 Hz, for key length 700 bits, and duration/bit (number of samples/bit) 200, 500, and 1000, respectively. The limit $p = 0.5$ stands for perfect security.

The observed dependence can be interpreted by the behavior of the error function (see also Equations (8) and (12))

$$p\{U(t) \geq U_{\text{th}}\} = 0.5\left[1 - erf\left(\frac{U_{\text{th}} - U_{\text{DCw}}}{U_{\text{eff}}\sqrt{2}}\right)\right] \tag{16}$$

where $U(t)$ is the instantaneous voltage amplitude in the wire and the error function is

$$erf(x) = \frac{1}{\sqrt{\pi}}\int_{-x}^{x} \exp\left(-y^2\right) dy. \tag{17}$$

The noise in the KLJN scheme is a bandlimited white noise, and thus, in accordance with the Johnson formula, the effective noise voltage scales as

$$U_{\text{eff}} \propto \sqrt{T\,\Delta f} \tag{18}$$

Therefore, when temperature T is converging towards infinity, p converges to the perfect security limit of 0.5 (see Figure 4).

4. Some of the Possible Defense Techniques Against the Attack

Based on the considerations above, the impact of the attack can be eliminated by various means. The most natural ways are:

(i) Cancelling the effect of the DC-voltage sources. For example, Bob can use a variable DC source that compensates for its effect. Similarly, eliminating ground loops is also beneficial.

(ii) Alice and Bob can increase the effective temperature, that is, the amplitudes of their noise generators (see Equation (18) and Figure 4).

(iii) Alice and Bob can increase the bandwidth to increase the effective value of the noise (see Equations (18) and (20)). However, the bandwidth must stay below the wave limit [54] to avoid information leaks due to reflection, and thus the applicability of this tool is strongly limited.

5. Conclusions

The KLJN secure key exchange scheme is a statistical physical system that offers unconditional (information-theoretic) security. For a detailed survey and its history, see the recent book [56].

In this paper a novel attack against the KLJN protocol is shown which has revealed that uses a frequently occurring parasitic feature, namely the imbalance of voltages between the ground points at the two ends. We showed that, in the DC limit, such parasite voltages and currents could cause information leaks. The present study is directly relevant for DC current-based ground loops (for example, during secure communication between different units in instruments [33,34]). The attack was demonstrated via computer simulation and proper defense protocols were shown to eliminate the information leak. For AC-type ground loops, our DC-limited study is only a first step in addressing a more general situation (which should be investigated in future works).

Author Contributions: M.Y.M. and L.B.K. conceived and designed the studies; M.Y.M. performed the computer simulations; M.Y.M. and L.B.K. analyzed the data; M.Y.M. and L.B.K. wrote the paper.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
2. Delfs, H.; Knebl, H. *Introduction to Cryptography*; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2.
3. Wiesner, S.J. Conjugate Coding. *Sigact News* **1983**, *1*, 78–88. [CrossRef]
4. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* **1984**, *175*, 8. [CrossRef]
5. Wootters, W.; Zurek, W. A Single Quantum Cannot be Cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
6. Yuen, H. Security of quantum key distribution. *IEEE Access* **2016**, *4*, 724–749. [CrossRef]
7. Makarov, V.; Bourgoin, J.P.; Chaiwongkhot, P.; Gagné, M.; Jennewein, T.; Kaiser, S.; Kashyap, R.; Legré, M.; Minshull, C.; Sajeed, S. Laser Damage Creates Backdoors in Quantum Communications. *Technology* **2015**, *16*, 22.
8. Renner, R. Security of Quantum Key Distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1–127. [CrossRef]
9. Yuen, H.P. On the foundations of quantum key distribution—Reply to Renner and beyond. *arXiv* **2012**, arXiv:1210.2804.
10. Hirota, O. Incompleteness and limit of quantum key distribution theory. *arXiv* **2012**, arXiv:1208.2106v2.
11. Renner, R. Reply to recent scepticism about the foundations of quantum cryptography. *arXiv* **2012**, arXiv:1209.2423v.1.
12. Yuen, H.P. Security significance of the trace distance criterion in quantum key distribution. *arXiv* **2012**, arXiv:1109.2675v3.
13. Yuen, H.P. Unconditional security in quantum key distribution. *arXiv* **2012**, arXiv:1205.5065v2.
14. Yuen, H.P. Key generation: Foundation and a new quantum approach. *IEEE J. Sel. Top. Quantum Electron.* **2009**, *15*, 1630–1645. [CrossRef]
15. Merali, Z. Hackers blind quantum cryptographers. *Nat. News* **2009**. [CrossRef]
16. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2011**, *2*, 349. [CrossRef] [PubMed]
17. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. [CrossRef]
18. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Scarani, V.; Makarov, V.; Kurtsiefer, C. Experimentally faking the violation of Bell's inequalities. *Phys. Rev. Lett.* **2011**, *107*, 170404. [CrossRef]
19. Makarov, V.; Skaar, J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Inf. Comp.* **2008**, *8*, 622–635.
20. Wiechers, C.; Lydersen, L.; Wittmann, C.; Elser, D.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. After-gate attack on a quantum cryptosystem. *New J. Phys.* **2011**, *13*, 013043. [CrossRef]

21. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Thermal blinding of gated detectors in quantum cryptography. *Opt. Express* **2010**, *18*, 27938–27954. [CrossRef]
22. Jain, N.; Wittmann, C.; Lydersen, L.; Wiechers, C.; Elser, D.; Marquardt, C.; Makarov, V.; Leuchs, G. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **2011**, *107*, 110501. [CrossRef] [PubMed]
23. Lydersen, L.; Skaar, J.; Makarov, V. Tailored bright illumination attack on distributed-phase-reference protocols. *J. Mod. Opt.* **2011**, *58*, 680–685. [CrossRef]
24. Lydersen, L.; Akhlaghi, M.K.; Majedi, A.H.; Skaar, J.; Makarov, V. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New J. Phys.* **2011**, *13*, 113042. [CrossRef]
25. Lydersen, L.; Makarov, V.; Skaar, J. Comment on Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography. *Appl. Phys. Lett.* **2011**, *99*, 196101. [CrossRef]
26. Sauge, S.; Lydersen, L.; Anisimov, A.; Skaar, J.; Makarov, V. Controlling an actively-quenched single photon detector with bright light. *Opt. Express* **2011**, *19*, 23590–23600. [CrossRef] [PubMed]
27. Lydersen, L.; Jain, N.; Wittmann, C.; Maroy, O.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. Superlinear threshold detectors in quantum cryptography. *Phys. Rev. Lett.* **2011**, *84*, 032320. [CrossRef]
28. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Avoiding the blinding attack in QKD; Reply (Comment). *Nat. Photonics* **2010**, *4*, 801. [CrossRef]
29. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New J. Phys.* **2009**, *11*, 065003. [CrossRef]
30. Kish Laszlo, B. Totally Secure Classical Communication Utilizing Johnson (-Like) Noise and Kirchhoff's Law. *Phys. Lett. A* **2006**, *352*, 178–182. [CrossRef]
31. Kish, L.B. Methods of Using Existing Wire Lines (power lines, phone lines, internet lines) for Totally Secure Classical Communication Utilizing Kirchhoff's Law and Johnson-like Noise. *arXiv* **2006**, arXiv:physics/0610014.
32. Gonzalez, E.; Kish, L.B.; Balog, R.; Enjeti, P. Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters. *PLoS ONE* **2013**, *8*, e70206. [CrossRef]
33. Kish, L.B.; Entesari, K.; Granqvist, C.G.; Kwan, C. Unconditionally secure credit/debit card chip scheme and physical unclonable function. *Fluct. Noise. Lett.* **2017**, *16*, 1750002. [CrossRef]
34. Kish, L.B.; Kwan, C. Physical Uncloneable Function Hardware Keys Utilizing Kirchhoff-Law-Johnson-Noise Secure Key Exchange and Noise-Based Logic. *Fluct. Noise Lett.* **2013**, *12*, 1350018. [CrossRef]
35. Saez, Y.; Cao, X.; Kish, L.B.; Pesti, G. Securing Vehicle Communication Systems by the KLJN Key Exchange Protocol. *Fluct. Noise Lett.* **2014**, *13*, 1450020. [CrossRef]
36. Cao, X.; Saez, Y.; Pesti, G.; Kish, L.B. On KLJN-based secure key distribution in vehicular communication networks. *Fluct. Noise Lett.* **2015**, *14*, 1550008. [CrossRef]
37. Cho, A. Simple noise may stymie spies without quantum weirdness. *Science* **2005**, *309*, 2148. [CrossRef] [PubMed]
38. Kish, L.B.; Scheuer, J. Noise in the Wire: The Real Impact of Wire Resistance for the Johnson (-Like) Noise Based Secure Communicator. *Phys. Lett. A* **2010**, *374*, 2140–2142. [CrossRef]
39. Kish, L.B.; Granqvist, C.G. Elimination of a Second-Law-attack, and all cable-resistance-based attacks, in the Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system. *Entropy* **2014**, *16*, 5223–5231. [CrossRef]
40. Vadai, G.; Gingl, Z.; Mingesz, R. Generalized attack protection in the Kirchhoff-law–Johnson-noise secure key exchanger. *IEEE Access* **2016**, *4*, 1141–1147. [CrossRef]
41. Hao, F. Kish's key exchange scheme is insecure. *IEEE Proc. Inf. Soc.* **2006**, *153*, 141–142. [CrossRef]
42. Kish, L.B. Response to Feng Hao's paper Kish's key exchange scheme is insecure. *Fluct. Noise Lett.* **2006**, *6*, C37–C41. [CrossRef]
43. Vadai, G.; Gingl, Z.; Mingesz, R. Generalized Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system using arbitrary resistors. *Sci. Rep.* **2015**, *2015*, 13653. [CrossRef] [PubMed]
44. Chen, H.P.; Gonzalez, E.; Saez, Y.; Kish, L.B. Cable Capacitance Attack against the KLJN Secure Key Exchange. *Information* **2015**, *6*, 719–732. [CrossRef]
45. Gunn, L.J.; Allison, A.; Abbott, D. A new transient attack on the Kish key distribution system. *IEEE Access* **2015**, *3*, 1640–1648. [CrossRef]
46. Kish, L.B.; Granqvist, C.G. Comments on A New Transient Attack on the Kish Key Distribution System. *Metrol. Meas. Syst.* **2016**, *23*, 321–331. [CrossRef]

47. Kish, L.B. Enhanced secure key exchange systems based on the Johnson-noise scheme. *Metrol. Meas. Syst.* **2013**, *20*, 191–204. [CrossRef]
48. Kish, L.B.; Granqvist, C.G. Random-resistor–random-temperature Kirchhoff-law-Johnson-noise (RRRT-KLJN) key exchange. *Metrol. Meas. Syst.* **2016**, *23*, 3–11. [CrossRef]
49. Chen, H.P.; Mohammad, M.; Kish, L.B. Current Injection Attack against the KLJN Secure Key Exchange. *Metrol. Meas. Syst.* **2016**, *23*, 173–181. [CrossRef]
50. Kish, L.B. 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.* **2006**, *6*, L57–L63. [CrossRef]
51. Kish, L.B.; Horvath, T. Notes on Recent Approaches Concerning the Kirchhoff-Law-Johnson-Noise-based Secure Key Exchange. *Phys. Lett. A* **2009**, *373*, 2858–2868. [CrossRef]
52. Kish, L.B.; Abbott, D.; Granqvist, C.G. Critical analysis of the Bennett-Riedel attack on secure cryptographic key distributions via the Kirchhoff-law-Johnson-noise scheme. *PLoS ONE* **2013**, *8*, e81810. [CrossRef]
53. Chen, H.P.; Kish, L.B.; Granqvist, C.G. 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.* **2014**, *21*, 389–400. [CrossRef]
54. Chen, H.P.; Kish, L.B.; Granqvist, C.G.; Schmera, G. Do Electromagnetic Waves Exist in a Short Cable at Low Frequencies? What Does Physics Say? *Fluct. Noise Lett.* **2014**, *13*, 1450016. [CrossRef]
55. Kish, L.B.; Gingl, Z.; Mingesz, R.; Vadai, G.; Smulko, J.; Granqvist, C.G. 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.* **2015**, *14*, 1550011. [CrossRef]
56. Kish, L.B. The Kish Cypher. The Story of KLJN for Unconditional Security. *World Sci.* **2017**. [CrossRef]