Information **2015**, *6*, 719-732; doi:10.3390/info6040719

OPEN ACCESS

information

ISSN 2078-2489

www.mdpi.com/journal/information

Article

Cable Capacitance Attack against the KLJN Secure Key Exchange

Hsien-Pu Chen *, Elias Gonzalez †, Yessica Saez † and Laszlo B. Kish

Department of Electrical and Computer Engineering, Texas A & M University, 3128 TAMU, College Station, TX 77843, USA; E-Mails: eliasg23@tamu.edu (E.G.); yessica.saez@tamu.edu (Y.S.); Laszlo.Kish@ece.tamu.edu (L.B.K.)

† These authors contributed equally to this work.

* Author to whom correspondence should be addressed; E-Mail: barrychen@tamu.edu; Tel.:+1-979-6334850.

Academic Editors: Qiong Huang and Guomin Yang

Received: 11 August 2015 / Accepted: 26 October 2015 / Published: 30 October 2015

Abstract: The security of the Kirchhoff-law-Johnson-(like)-noise (KLJN) key exchange system is based on the fluctuation-dissipation theorem of classical statistical physics. Similarly to quantum key distribution, in practical situations, due to the non-idealities of the building elements, there is a small information leak, which can be mitigated by privacy amplification or other techniques so that unconditional (information-theoretic) security is preserved. In this paper, the industrial cable and circuit simulator LTSPICE is used to validate the information leak due to one of the non-idealities in KLJN, the parasitic (cable) capacitance. Simulation results show that privacy amplification and/or capacitor killer (capacitance compensation) arrangements can effectively eliminate the leak.

Keywords: KLJN; cable capacitance attack; capacitor killer; secure key exchange; unconditional security; privacy amplification

1. Introduction

The Kirchhoff-law-Johnson-(like)-noise (KLJN) key exchange system [1–4] was first introduced in 2005. Earlier, it was claimed that only quantum key distribution (QKD) [5] could offer unconditional (that is, information-theoretic) security. In due course, QKD's fundamental security

claims have been debated by experts in the field [6–12]. Furthermore, its practical realizations, including all commercial quantum communicators, have been fully cracked by hacking, that is, by utilizing non-ideal features of the hardware components [13–26]. While counter-measures were later proposed to overcome these attacks, when the idea of a new attack is unknown by the communicating parties and no counter-measures have been implemented yet, the eavesdropper can fully utilize such an attack [27–30].

Naturally, there have also been efforts to challenge KLJN's security [31–43]. Studies have consistently shown that both the ideal and the practical KLJN versions remain unconditionally secure [4,34–43] despite facing various attacks and related information leaks associated with the non-idealities of components in the system. The impacts of the attacks against practical KLJN systems have been weak. With proper protocols, the eavesdropper's (Eve's) probability of successful guessing of a bit can always be reduced to a value that is sufficiently close to 0.5 [3,34–38] to preserve unconditional security [4].

We will show that one of the most effective attacks against the practical KLJN system is the cable capacitance attack. It was first mentioned in 2006 [36], but it has never been tested. Subsequently, in 2008, a solution was suggested to eliminate this attack by adding a capacitor killer (capacitance compensation) arrangement [39].

In this paper, we use the industrial cable and circuit simulator LTSPICE by Linear Technology to simulate practical realizations of the KLJN system and to evaluate the cable capacitance attack. Solutions to mitigate this attack, such as the capacitor killer arrangement [39] and privacy amplification [44], are also tested.

2. The KLJN Secure Key Exchange System

2.1. The KLJN Protocol

The KLJN secure key exchange system [1–4,38–60] is based on Kirchhoff's Loop Law and the Fluctuation-Dissipation Theorem. The core KLJN system is illustrated in Figure 1 [2]. It consists of a cable as an information channel, switches, and two identical pairs of resistors, R_L and R_H, ($R_L \neq R_H$), where R_L represents the low key bit (0) and R_H represents the high key bit (1).

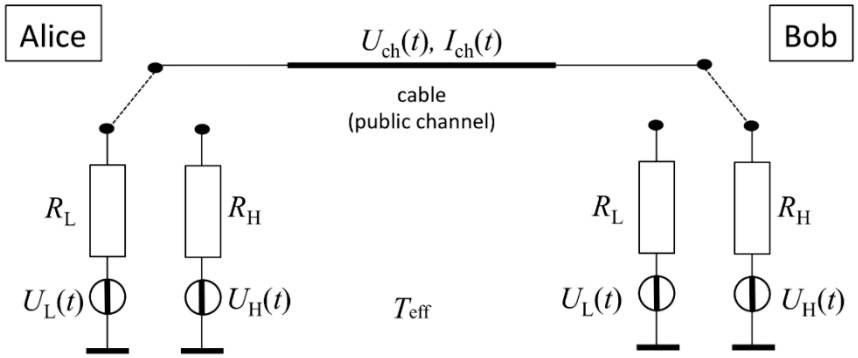

Figure 1. The core of the KLJN secure key exchange system [2]. The resistor values are R_L and R_H. The thermal noise voltages, $U_L(t)$ and $U_H(t)$, are generated at an effective temperature T_{eff} (typically $T_{eff} \geq 10^{14}$ K) [40]. The channel noise voltage and current are $U_{ch}(t)$ and $I_{ch}(t)$, respectively.

At the beginning of each bit exchange period (BEP), Alice and Bob randomly select R_L or R_H and connect the corresponding resistor to the cable. The Gaussian voltage noise generators in the figure represent either the Johnson noise sources of the resistors or external voltage noise generators emulating Johnson noise (filters are not shown). The noise is band-limited white noise with publicly agreed common bandwidth B_{noise} and a publicly agreed common noise-temperature T_{eff} [40]. The noises are statistically independent from each other and from the noise samples in the previous BEP [4]. Note that there are many advanced KLJN versions [41,42,56,60] with a greater number of resistor values, some with different temperatures [56,60].

Within each BEP, Alice and Bob measure the mean-square channel noise voltage $\left\langle U_{ch}^2(t)\right\rangle$ and/or the channel noise currents $\left\langle I_{ch}^2(t)\right\rangle$ in the cable. The BEP has to be properly chosen to provide sufficient time for good statistics on the mean-square noise voltages and currents but not enough time for Eve to effectively utilize possible information leaks due to hardware non-idealities. According to Johnson's noise formula:

$$\left\langle U_{ch}^2(t)\right\rangle = 4kT_{eff}\frac{R_A R_B}{R_A + R_B}B_{noise} \tag{1}$$

$$\left\langle I_{ch}^2(t)\right\rangle = 4kT_{eff}\frac{1}{R_A + R_B}B_{noise} \tag{2}$$

where k is the Boltzmann's constant (1.38×10^{-23} J/K), R_A and R_B are the actual resistance values selected by Alice and Bob, respectively.

Based on Equation (1) or (2), by measuring $\left\langle U_{ch}^2(t)\right\rangle$ and/or $\left\langle I_{ch}^2(t)\right\rangle$, and by knowing their own resistance value, Alice and Bob can determine [2] the resistor value at the other end and hence they can learn the bit value (0 or 1) there.

With the cable being public, an eavesdropper (Eve) can also measure the channel noise voltages and currents. If Alice and Bob use the same resistance values, so the arrangement is $R_L R_L$ or $R_H R_H$, the resulting noise levels are singular, (see Equations (1) and (2)) thus the exchanged bit is non-secure and is discarded [2]. Conversely, the combinations $R_L R_H$ and $R_H R_L$ are degenerated because they produce the same noise levels. Thus the bit exchange is secure because Eve cannot differentiate between the two bit alternatives. From the noise levels (see Equations (1) and (2)) Eve knows that Alice and Bob have exchanged a secure bit, but she does not know the location of R_L and R_H.

In reality, the cable is non-ideal. Thus Eve can exploit the non-idealities of the cable, such as parasitic resistance, parasitic inductance and parasitic capacitance, to attack the KLJN system.

2.2. Cable Capacitance Attack

In this paper, we assume coaxial cables because, in this case, the cable capacitance attack [36] can effectively be eliminated without the usage of privacy amplification. However, the attack works with any cable. Coaxial cables include two conductors: the inner wire, which is used as the KLJN channel, and the outer shield, which is grounded (for the ground, see also Figure 1). There is a non-zero capacitance between these two conductors that leads to capacitive currents. Part of the channel noise current is diverted by the parasitic capacitance, which causes a greater current at the end

of the lower resistance. This gives Eve a chance to guess the value of the resistors with probability of success greater than 0.5.

Figure 2 shows the distributed elements model of coaxial cables. According to Kirchhoff's current law, at position x, the channel noise current $I_x(t)$ is the sum of the capacitive current $I_{c,x}(t)$ through the parasitic capacitor element C_x, and the channel noise current $I_{x+1}(t)$. This is written as

$$I_x(t) = I_{c,x}(t) + I_{x+1}(t) \tag{3}$$

The capacitive current $I_{c,x}(t)$ is proportional to the time derivative of the channel noise voltage $U_x(t)$ and it is given by

$$I_{c,x}(t) = C_x \cdot \frac{dU_x(t)}{dt} \tag{4}$$

We define the cross-correlation $\rho(x)$ [34] at position x as the product of the channel noise current and the time derivative of the channel noise voltage:

$$\rho(x) = \left\langle I_x(t) \cdot \frac{dU_x(t)}{dt} \right\rangle_\tau \tag{5}$$

where $\langle\ \rangle_\tau$ means finite time (τ) average. The location-dependence of $\rho(x)$ represents information leak [34].

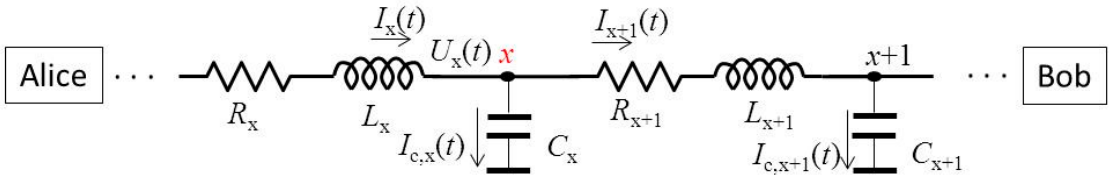

Figure 2. Cable model and cable capacitive currents.

3. Realization of the Attack

The cable and a circuit simulator LTSPICE by Linear Technology was used to emulate the practical KLJN system with the RG58 coaxial cable from its library. Throughout the simulations, we assumed that Alice selected R_L = 1 kohm and Bob R_H = 9 kohm; see Figure 3.

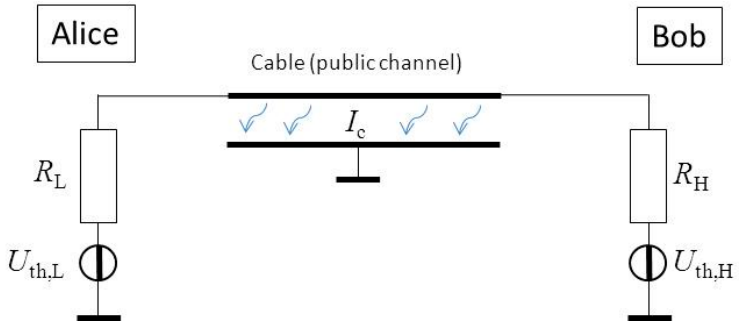

Figure 3. The simulated KLJN system with capacitive current I_c. The generator voltages $U_{th,L}$ and $U_{th,H}$ are the Johnson noise voltages of R_L and R_H, respectively.

3.1. Generating the Noise

For the simulations, we generated Gaussian band-limited white noises. According to Johnson's noise formula, the required rms noise voltage U_{th} is

$$U_{\text{th}} = \sqrt{4kT_{\text{eff}}RB_{\text{noise}}} \tag{6}$$

As the mean value is zero, the rms noise voltages are the same as their standard deviations (denoted as σ_{L} and σ_{H} for $U_{\text{th,L}}$ and $U_{\text{th,H}}$, respectively). Thus

$$U_{\text{th,L}}/U_{\text{th,H}} = \sigma_{\text{L}}/\sigma_{\text{H}} = \sqrt{R_{\text{L}}/R_{\text{H}}} \tag{7}$$

where $\sqrt{R_{\text{L}}/R_{\text{H}}} = \sqrt{1/9}$, thus $\sigma_{\text{L}}/\sigma_{\text{H}} = 1/3$. For the simulations, the rms thermal noise voltages of R_{L} and R_{H} were chosen as 1 V and 3 V, respectively, corresponding to $T_{\text{eff}} \approx 7\times10^{16}$ K.

Figure 4a shows the probability density function (histogram) of the noise voltage of R_{L}. In Figure 4b the cumulative distribution as normal probability plot can be seen where a straight line indicates exact normal distribution.

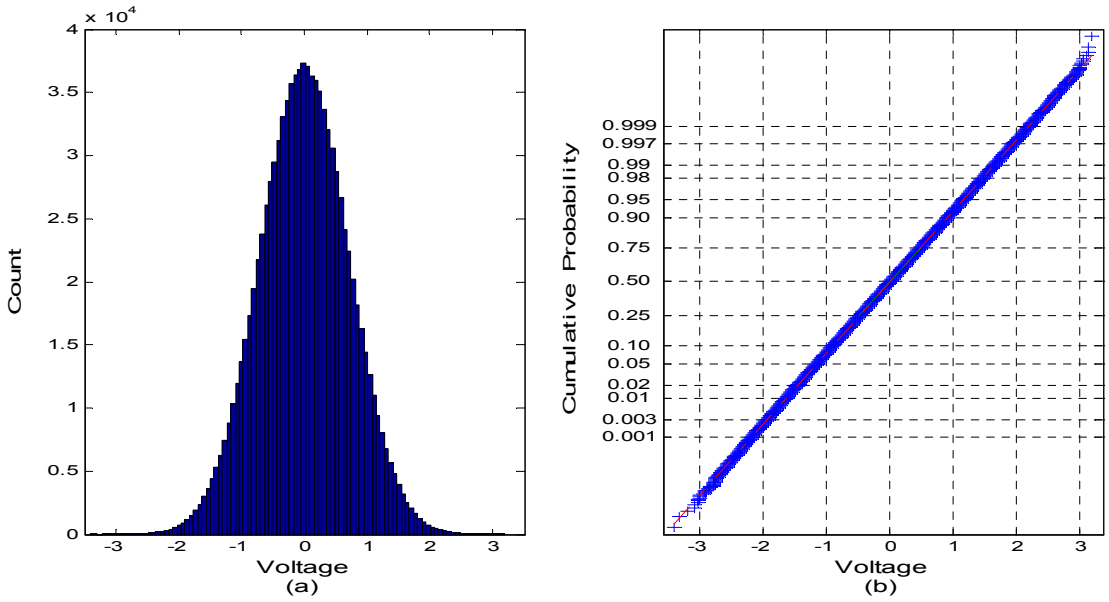

Figure 4. Statistics of the Johnson noise voltage of R_{L} with 10^6 samples. (**a**) Probability density function (histogram); (**b**) Cumulative distribution as normal probability plot.

3.2. Comparing the Lumped and Distributed Element Models at Different Wavelengths

First, for enhanced computational speed, we explored the possibility of using a lumped element cable model for the simulations because the continuum model simulations are at least 1000 times slower. Our data below proves that lumped elements can be used for high-accuracy simulations at the operational conditions of KLJN.

The quasi-static condition is required for the security of the KLJN system [2,34]. That means

$$L_{\text{ch}} \ll \lambda = c/B_{\text{noise}} \text{ or } \gamma = \lambda/L_{\text{ch}} \gg 1 \tag{8}$$

where L_{ch} is the cable length, λ is the shortest wavelength at the highest frequency component of the noise bandwidth B_{noise}, c is the propagation velocity in the cable, and γ is the ratio of the wavelength to the cable length. It has been assumed that γ must be at least around 10 to fulfill the KLJN conditions [34,49,50,57,58] (*i.e.*, approximate quasi-static electrodynamics; see [49,50] concernig the proof that there are no waves in this limit).

Figure 5a,b shows the simple lumped element model and the distributed model of the RG58 coaxial cable. Based on the specific inductance and capacitance, the propagation velocity c in the RG58 coaxial cable is 2×10^8 m/s. Three simulations were run to compare the resultant voltage waveforms at Alice's side, at three different noise bandwidths B_{noise} (250 kHz, 25 kHz, 0.25 kHz) on these 2 models. The cable length was set at 1000 m, and based on Equation (8), the three corresponding wavelengths (λ) were 800 m, 8 km, and 800 km, while the corresponding γ ratios were 0.8, 8 and 800. Other parameters such as the component values of the models used in the simulations are also shown in Figure 5.

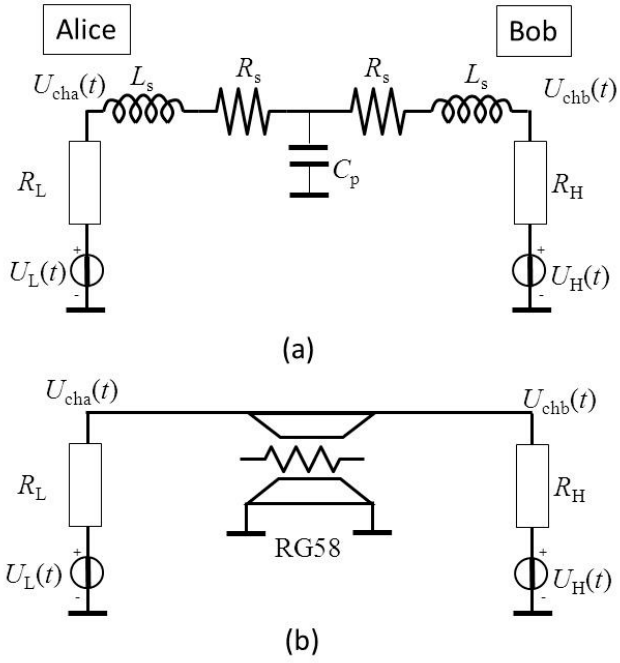

Figure 5. The RG58 coaxial cable models (1000 m length) with R_L (1 kohm) and R_H (9 kohm). The lumped element model: component values $R_S = 10.5$ ohm, $L_S = 125$ μH, $C_P = 100$ nF. The distributed model had the following parameters: $R = 0.021$ ohm/meter, $L = 250$ nH/meter, $C = 100$ pF/meter. The characteristic impedance of the cable is 50 ohms.

Figure 6 shows the simulation results, where $U_{cha,lump}$ and $U_{cha,dist}$ are the voltage time functions of the lumped and distributed element models, respectively. In Figure 6a, the two waveforms are significantly different for the shortest wavelength with $\gamma = 0.8$. In such a case, the waves can only be simulated with the distributed model. However, this situation is irrelevant for the operation of KLJN, as mentioned above.

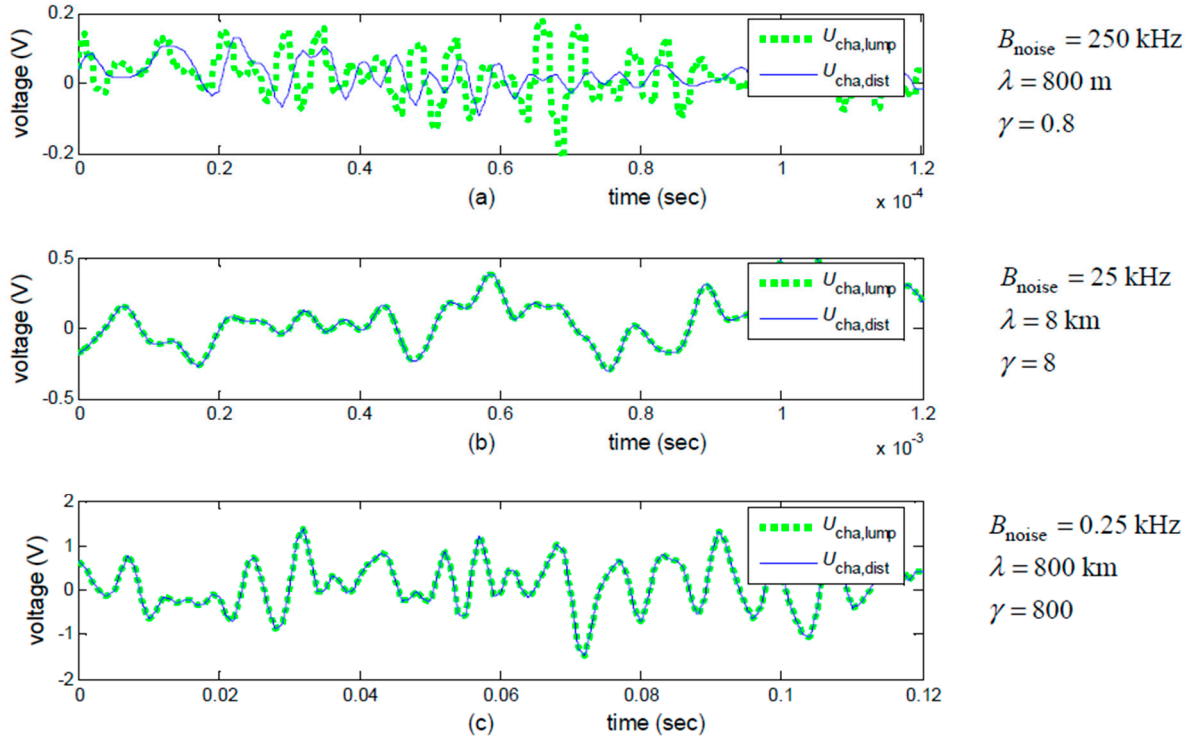

Figure 6. The voltage waveforms at Alice's side, $U_{\text{cha,lump}}$ and $U_{\text{cha,dist}}$, for the lumped and distributed element models, respectively, for a 1000 m cable, at (**a**) γ = 0.8; (**b**) γ = 8; (**c**) γ = 800.

In Figure 6b, with γ = 8, the two waveforms are very similar whereas in Figure 6c, at $\gamma = 800$, the two waveforms are indistinguishable. Thus we can conclude that for situations $\gamma \geq 8$, the lumped element simulations are satisfactory. Both cases are fine for the KLJN operation and we will use the $\gamma \geq 800$ condition in the rest of the paper.

For our resistor values R_{L} = 1 kohm and R_{H} = 9 kohm, the cut-off frequency by the cable capacitance is 1.76 kHz and 17.6 kHz for a 1000 and a 100 m cable, respectively. To avoid having the cable capacitance truncate the effective bandwidth of the noise, we used noise bandwidth $B_{\text{noise}} = 0.25$ kHz for the noise generators ($\gamma = 800$ at 1000 m and $\gamma = 8000$ at 100 m).

3.3. The Attack Protocol

In this section, we discuss the information leak caused by the cable capacitance and evaluate Eve's success probability in terms of guessing the key bits. The fixed bit arrangement is used between Alice and Bob.

During the exchange of the *i*-th bit, Eve measures the cross-correlations:

$$\rho_{\text{ia}} = \left\langle I_{\text{cha}}(t) \cdot \frac{dU_{\text{cha}}(t)}{dt} \right\rangle_{\tau} \tag{9}$$

$$\rho_{\text{ib}} = \left\langle I_{\text{chb}}(t) \cdot \frac{dU_{\text{chb}}(t)}{dt} \right\rangle_{\tau} \tag{10}$$

where $U_{\text{cha}}(t)$, $I_{\text{cha}}(t)$, $U_{\text{chb}}(t)$ and $I_{\text{chb}}(t)$ are the channel voltages and currents at Alice's and Bob's ends, respectively, see Figure 7. The time average $\langle\ \rangle_\tau$ is taken over the bit exchange period τ. Eve calculates $\rho_i = \rho_{ia} - \rho_{ib}$ $(i = 1,...,N)$ and decides as follows:

$$\begin{aligned} &\text{If} \quad \rho_i > 0 \quad \text{then} \ \ q_i = 1 \quad (\textit{Eve guessed the bit correctly}) \\ &\text{If} \quad \rho_i < 0 \quad \text{then} \ \ q_i = 0 \quad (\textit{Eve guessed the bit wrongly}) \end{aligned} \tag{11}$$

When N approaches infinity, the probability of Eve's successful guessing of the bits is equal to the expected value of q and

$$\langle q_i \rangle_N = p_E = 0.5 + \varepsilon \text{, where } 0 \le \varepsilon < 0.5 \tag{12}$$

where non-zero ε represents an information leak. When $\varepsilon = 0$, the KLJN key exchange system is perfectly secure. We found that the higher the difference between the resistances, the higher the bandwidth, or the higher the parasitic capacitance (the longer the cable), the greater the leak.

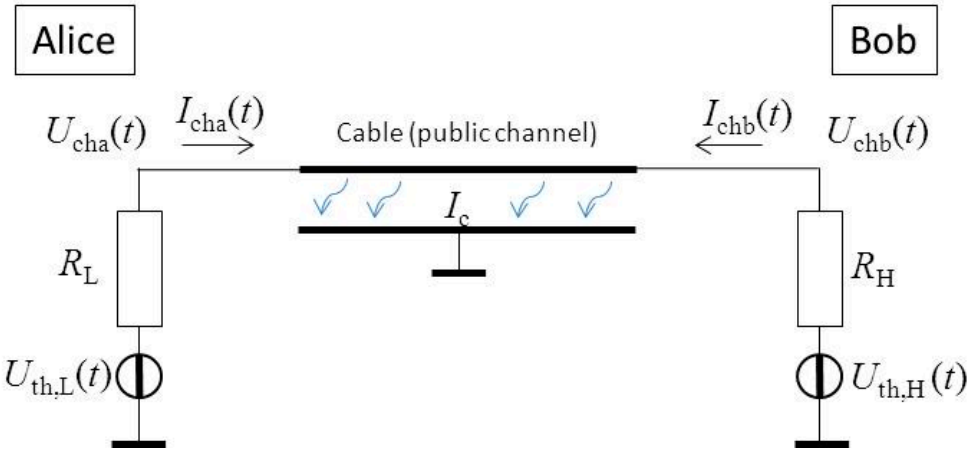

Figure 7. The simulated model with LH bit arrangement (R_L = 1 kohm and R_H = 9 kohm). $U_{\text{cha}}(t)$, $I_{\text{cha}}(t)$, $U_{\text{chb}}(t)$ and $I_{\text{chb}}(t)$ are the voltages and currents at Alice's and Bob's ends, respectively.

3.4. Simulation Results of the Cable Capacitance Attack

We simulated 6 different attack scenarios with these parameters: R_L = 1 kohm, R_H = 9 kohm, noise bandwidth B_{noise} = 0.25 kHz, sampling period t_s = 1 msec; for 3 different single-bit exchange durations (measured by the unit of the autocorrelation time of the noise), 20, 50, and 100; at 2 different cable lengths, 100 and 1000 m. At each scenario, the key was 1000 bits long.

The simulation results are shown in Table 1. At bit exchange duration = 20 (50 bits per second), with a 100 m cable, Eve's success rate was 50.9%. However, when the cable length was increased to 1000 m with the other parameters unchanged, Eve's success rate increased to 62.2%.

Table 1. Attack simulation results—Eve's success rate p_E (%) with 1000 bits key length.

Bit Exchange Duration	Bits Per Second	100 m Cable	1000 m Cable
20	50	50.9%	62.2%
50	20	52.1%	69.7%
100	10	52.6%	76.9%

When the bit exchange duration was increased to 50 and 100, Eve's success rate increased accordingly as shown in Table 1. In the most effective attack case, Eve success rate was 76.9%.

4. Defense against the Attack

4.1. Capacitor Killer

The parasitic capacitance of the RG58 coaxial cable can be eliminated by the well-known capacitance compensation technique, called capacitor killer arrangement [39], providing the same voltage on the outer shield of the cable as on the inner wire. This can be done by an ideal voltage follower, see Figure 8. There is no capacitive current from the inner wire to the outer shield, so the attack is nullified.

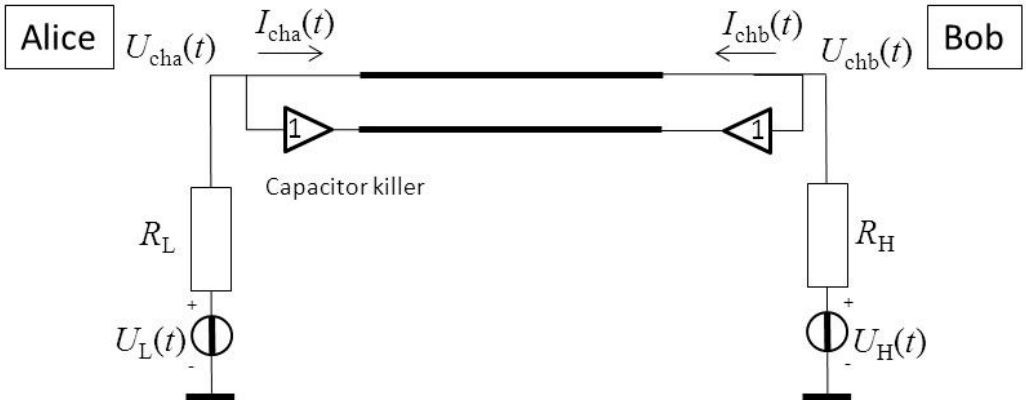

Figure 8. The KLJN system with the capacitor killer. An ideal voltage follower is driving the outer shield, which is not grounded at this time.

We simulated the capacitor killer arrangement in the most effective attack scenario (*i.e.*, when Eve success rate was 76.9%). The simulation results showed that Eve's success rate was reduced from 76.9% to 50.1%. This indicated that the capacitor killer is very effective in eliminating the leak due to the parasitic capacitance under the practical cable conditions we tested.

4.2. Privacy Amplification

Another method to secure the key exchange and to reduce information leak is by utilizing privacy amplification [44]. Due to the extraordinarily low bit error probability of the KLJN system [51–53], privacy amplification (which is basically an error enhancer) can be used to effectively reduce any information leak. The simplest and most secure concept [44] is that Alice and Bob XOR the subsequent pairs of the key bits (*i.e.*, XOR the first and the second bits to get the first bit of the new

key, XOR the third and the fourth bits to get the next one, *etc.*). In this way, the length of the new key will be half of the original one but Eve's success probability will get closer to 0.5; that is, it moves toward the limit of zero information. We simulated the effect of this technique by utilizing the most effective attack scenario (see Table 1). The simulation results showed that by XOR-ing once, Eve's success probability was reduced from 76.9% to 64.2%, which was further reduced to 54.4% by XOR-ing a second time to produce a cleaner key with the corresponding significantly higher security and one quarter of its original length.

5. Conclusions

By utilizing the LTSPICE simulator we have validated the cable capacitance attack. Both the capacitor killer method and privacy amplification have been able to eliminate the attack. The unconditional security of a practical KLJN key exchange system [4] has been preserved against this attack, too.

Note that the temperature compensation method [59] based on the non-equilibrium thermodynamical aspects of KLJN to eliminate the information leak in a wire resistance attack does not reduce the efficiency of the cable capacitance attack.

Finally, note that there is a new, advanced protocol, the random-resistor-random-temperature (RRRT) KLJN scheme [60], where all the former attacks become invalid or incomplete, and currently no known attack works against it. This is also true for the cable capacitance attack presented above; it is invalid against the RRRT-KLJN scheme. Further studies will be needed to find ways for all the former attack schemes to successfully extract information from the RRRT-KLJN system [60] at non-ideal conditions where they may leak information.

Author Contributions

Theory: Hsien-Pu Chen and Laszlo B. Kish; Math analysis: Hsien-Pu Chen and Laszlo B. Kish; Simulations: Hsien-Pu Chen; Interpretation: Hsien-Pu Chen and Laszlo B. Kish; Writing: Hsien-Pu Chen, Elias Gonzalez, Yessica Saez and Laszlo B. Kish. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Cho, A. Simple Noise May Stymie Spies Without Quantum Weirdness. *Science* **2005**, *309*, 2148, doi:10.1126/science.309.5744.2148b.
2. Kish, L.B. Totally secure classical communication utilizing Johnson(-like) noise and Kirchoff's law. *Phys. Lett. A* **2006**, *352*, 178–182.
3. 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.
4. Kish, L.B.; Granqvist, C.G. On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator. *Quantum Inf. Process.* **2014**, *13*, 2213–2219.

5. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Banglore, India, 10–12 December 1984; pp. 175–179.
6. Yuen, H.P. Essential lack of security proof in quantum key distribution. **2013**, arXiv:1310.0842.
7. Hirota, O. Incompleteness and Limit of Quantum Key Distribution Theory. **2012**, arXiv:1208.2106.
8. Renner, R. Reply to recent scepticism about the foundations of quantum cryptography. **2012**, arXiv*:*1209.2423.
9. Yuen, H.P. Unconditional Security In Quantum Key Distribution. **2012**, arXiv:1205.5065.
10. Yuen, H.P. On the Foundations of Quantum Key Distribution—Reply to Renner and Beyond. **2012**, arXiv:1210.2804.
11. Yuen, H.P. Security Significance of the Trace Distance Criterion in Quantum Key Distribution. **2011**, arXiv:1109.2675.
12. Yuen, H.P. Key Generation: Foundations and a New Quantum Approach. **2009**, arXiv:906.5241.
13. Merali, Z. Hackers blind quantum cryptographers. *Nat. News* **2009**, doi:10.1038/news.2010.436.
14. 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, doi:10.1038/ncomms1348.
15. 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*, doi:10.1103/PhysRevLett.107.170404.
16. 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.
17. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Avoiding the blinding attack in QKD. *Nat. Photonics* **2010**, *4*, doi:10.1038/nphoton.2010.278.
18. 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.
19. 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*, doi:10.1103/PhysRevLett.107.110501.
20. Lydersen, L.; Jain, N.; Wittmann, C.; Marøy, Ø.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. Superlinear threshold detectors in quantum cryptography. *Phys. Rev. A* **2011**, *84*, doi:10.1103/PhysRevA.84.032320.
21. Lydersen, L.; Skaar, J.; Makarov, V. Tailored bright illumination attack on distributed-phase-reference protocols. *J. Mod. Opt.* **2011**, *58*, 680–685.
22. 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*, doi:10.1088/1367-2630/13/1/013043.
23. Lydersen, L.; Akhlaghi, M.K.; Hamed Majedi, A.; Skaar, J.; Makarov, V. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New J. Phys.* **2011**, *13*, doi:10.1088/1367-2630/13/11/113042.

24. Sauge, S.; Lydersen, L.; Anisimov, A.; Skaar, J.; Makarov, V. Controlling an actively-quenched single photon detector with bright light. *Opt. Express* **2011**, *19*, doi:10.1364/OE.19.023590.
25. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New J. Phys.* **2009**, *11*, doi:10.1088/1367-2630/11/6/065003.
26. Makarov, V.; Skaar, J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Inf. Comput.* **2008**, *8*, 622–635.
27. Lim, C.C.W.; Walenta, N.; Legré, M.; Gisin, N.; Zbinden, H. Random Variation of Detector Efficiency: A Countermeasure Against Detector Blinding Attacks for Quantum Key Distribution. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 1–5.
28. Xu, F.; Curty, M.; Qi, B.; Lo, H.K. Measurement-device-independent quantum cryptography. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 1–11.
29. Jain, N.; Stiller, B.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 1–10.
30. Sajeed, S.; Chaiwongkhot, P.; Bourgoin, J.P.; Jennewein, T.; Lütkenhaus, N.; Makarov, V. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A* **2015**, *91*, doi:10.1103/PhysRevA.91.062301.
31. Bennett, C.H.; Jess Riedel, C. On the security of key distribution based on Johnson-Nyquist noise. **2013**, arXiv:1303.7435.
32. Hao, F. Kish's key exchange scheme is insecure. *IEEE Proc. Inf. Secur.* **2006**, *153*, 141–142.
33. Scheuer, J.; Yariv, A. A classical key-distribution system based on Johnson (like) noise—How secure? *Phys. Lett. A* **2006**, *359*, 737–740.
34. 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.
35. Kish, L.B. Response to Feng Hao's paper "Kish's key exchange scheme is insecure". *Fluct. Noise Lett.* **2006**, *6*, C37–C41.
36. Kish, L.B. Response to Scheuer-Yariv: "A classical key-distribution system based on Johnson (like) noise—How secure?" *Phys. Lett. A* **2006**, *359*, 741–744.
37. 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.
38. 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.
39. Mingesz, R.; Gingl, Z.; Kish, L.B. Johnson(-like) Noise Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line. *Phys. Lett. A* **2008**, *372*, 978–984.
40. Mingesz, R.; Bela Kish, L.; Gingl, Z.; Granqvist, C.G.; Wen, H.; Peper, F.; Eubanks, T.; Schmera, G. Unconditional security by the laws of classical physics. *Metrol. Meas. Syst.* **2013**, *20*, 3–16.
41. Kish L.B. Enhanced Secure Key Exchange Systems Based on the Johnson-Noise Scheme. *Metrol. Meas. Syst.* **2013**, *20*, 191–204.
42. Smulko, J. Performance Analysis of the "Intelligent" Kirchhoff-Law-Johnson-Noise Secure Key Exchange. *Fluct. Noise Lett.* **2014**, *13*, doi:10.1142/S0219477514500242.

43. Kish, L.B.; Mingesz, R. Totally secure classical networks with multipoint telecloning (teleporation) of classical bits through loops with Johnson-like noise. *Fluct. Noise Lett.* **2006**, *6*, C9–C21.
44. Horváth, T.; Kish, L.B.; Scheuer, J. Effective privacy amplification for secure classical communications. *EPL (Europhys. Lett.)* **2011**, *94*, doi:10.1209/0295-5075/94/28002.
45. Kish, L.B.; Peper, F. Information Networks Secured by the Laws of Physics. *IEICE Trans. Commun.* **2012**, *95*, 1501–1507.
46. Gonzalez, E.; Kish, L.B.; Balog, R.S.; Enjeti, P. Information Theoretically Secure, Enhanced Johnson Noise Based Key Distribution over the Smart Grid with Switched Filters. *PLoS ONE* **2013**, *8*, e70206.
47. Kish, L.B.; Kwan, C. Physical unclonable function hardware keys utilizing Kirchhoff-law-Johnson-noise secure key exchange and noise-based logic. *Fluct. Noise Lett.* **2013**, *12*, doi:10.1142/S0219477513500181.
48. Kish, L.B.; Saidi, O. Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives. *Fluct. Noise Lett.* **2008**, *8*, L95–L98.
49. 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*, doi:10.1142/S0219477514500163.
50. Kish, L.; Chen, S.; Granqvist, C.; Smulko, J. Waves in a short cable at low frequencies, or just hand-waving? In Proceedings of the 2015 International Conference on Noise and Fluctuations (ICNF), Xi'an, China, 2–6 June 2015; pp. 1–5.
51. Saez, Y.; Kish, L.B.; Mingesz, R.; Gingl, Z.; Granqvist, C.G. Bit errors in the Kirchhoff-Law-Johnson-Noise secure key exchange. *Int. J. Mod. Phys. Conf. Ser.* **2014**, *33*, doi:10.1142/S2010194514603676.
52. Saez, Y.; Kish, L.; Mingesz, R.; Gingl, Z.; Granqvist, C. Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law-Johnson-noise secure key exchange. *J. Comput. Electron.* **2014**, *13*, 271–277.
53. Saez, Y.; Kish, L.B. Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange. *PLoS ONE* **2013**, *8*, e81103.
54. Saez, Y.; Cao, X.; Kish, L.B.; Pesti, G. Securing vehicle communication systems by the kljn key exchange protocol. *Fluct. Noise Lett.* **2014**, *13*, doi:10.1142/S0219477514500205.
55. Gonzalez, E.; Balog, R.S.; Kish, L.B. Resource requirements and speed *versus* geometry of unconditionally secure physical key exchanges. *Entropy* **2015**, *17*, 2010–2024.
56. Vadai, G.; Mingesz, R.; Gingl, Z. Generalized Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system using arbitrary resistors. *Sci. Rep.* **2015**, *5*, doi:10.1038/srep13653.
57. 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*, doi:10.1142/S021947751550011X.
58. Chen, H.P.; Laszlo, B.K.; Claes, G.G.; Claes, G.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.

59. 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.
60. Kish, L.B.; Granqvist, C.G. Random-resistor-random-temperature Kirchhoff-law-Johnson-noise (RRRT-KLJN) key exchange. **2015**, arXiv:1509.08150.