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; yessica.saez@tamu.edu; Laszlo.Kish@ece.tamu.edu

† These authors contributed equally to this work.

* Author to whom correspondence should be addressed; E-Mail: barrychen@tamu.edu

Abstract: The Kirchhoff-law-Johnson-(like)-noise (KLJN) is a secure key exchange system based on the laws 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 technique so that the 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) unconditional secure key exchange system [1-4] was first introduced in 2005. Before KLJN, it was assumed that only Quantum Key Distribution (QKD) [5] could offer this level of security. QKD's fundamental security has 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 utilizing non-ideal features of the hardware building elements [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 on the practical KLJN system have been weak with the Eavesdropper's (Eve) probability of successful guessing of bits approaching zero [3,34-38] and thus preserving the unconditional (information theoretic) 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 realized. 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*

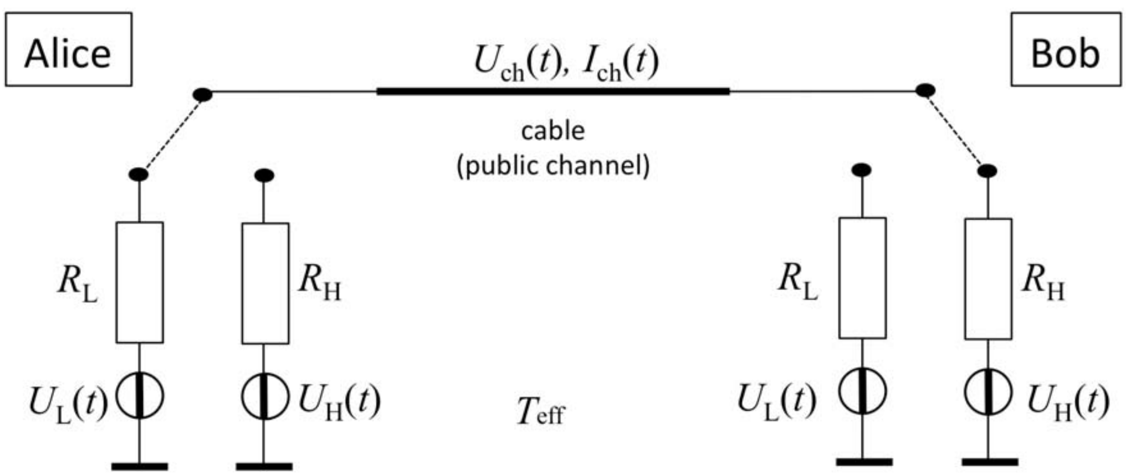

Figure 1. The core of the KLJN secure key exchange system [2]. The resistors values are denoted as R_L and R_H, respectively. The thermal noise voltages of R_L and R_H (denoted as $U_L(t)$ and $U_H(t)$, respectively) are generated at an effective temperature T_{eff} (typically $T_{eff} \geq 10^9$ K) [40]. The channel noise voltage and current are denoted as $U_{ch}(t)$ and $I_{ch}(t)$, respectively.

The KLJN secure key exchange system [1-4,38-56] is based on Kirchhoff's Loop Law and the Fluctuation-Dissipation Theorem. The core KLJN system is illustrated in Fig. 1 [2]. It is composed of a cable as an information channel, and two identical pairs of resistors (R_L and R_H) possessed by a sender (Alice) and a receiver (Bob), respectively, where R_L represents the Low key bit (0) and R_H

represents the High key bit (1) at Alice's side (at Bob's side the opposite), with $R_{\mathrm{L}} \neq R_{\mathrm{H}}$ and $R_{\mathrm{L}} < R_{\mathrm{H}}$, and two switches at each end connecting the selected resistors to the cable. (Note, there are many advanced KLJN versions [41,42,56] with greater number of resistor values, and even with non-zero power flow [56], which we cannot discuss in the present paper and the cracking scheme in this paper works against most of them).

At the beginning of each bit exchange period (BEP), Alice and Bob randomly select R_{L} or R_{H} at their ends and connect the corresponding resistor to the cable. The Gaussian voltage noise generators represent either the Johnson noise sources of the resistors (denoted as $U_{\mathrm{L}}(t)$ and $U_{\mathrm{H}}(t)$ for R_{L} and R_{H}, respectively) or external noise generators, which deliver band-limited white noise with publicly agreed bandwidth B_{noise} and a publicly agreed effective temperature T_{eff} [40]. The noises are statistically independent from each other and from the noise sources in the previous BEP [4].

Within each of the BEP, Alice and Bob measure the mean-square channel noise voltages $\left\langle U_{\mathrm{ch}}^2(t) \right\rangle$ and/or the channel noise currents $\left\langle I_{\mathrm{ch}}^2(t) \right\rangle$ in the cable. The BEP has to be properly chosen to provide sufficient time for obtaining a good statistics of 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 and Kirchhoff's Loop Law, it is given that:

$$\left\langle U_{\mathrm{ch}}^2(t) \right\rangle = 4kT_{\mathrm{eff}} \frac{R_{\mathrm{A}} R_{\mathrm{B}}}{R_{\mathrm{A}} + R_{\mathrm{B}}} B_{\mathrm{noise}} , \tag{1}$$

$$\left\langle I_{\mathrm{ch}}^2(t) \right\rangle = 4kT_{\mathrm{eff}} \frac{1}{R_{\mathrm{A}} + R_{\mathrm{B}}} B_{\mathrm{noise}} , \tag{2}$$

where k represents the Boltzmann's constant (1.38×10^{23} J/K), T_{eff} is the effective temperature , R_{A} and R_{B} are the resistors selected by Alice and Bob, respectively, and B_{noise} is the noise bandwidth.

Based on equation 1 or 2, by measuring $\left\langle U_{\mathrm{ch}}^2(t) \right\rangle$ and/or $\left\langle I_{\mathrm{ch}}^2(t) \right\rangle$, and by having their own resistors' value, Alice and Bob can figure out which of the resistors is used by the other party and hence they can identify the bit (0 or 1) at the other end.

With the cable being public, an eavesdropper (Eve) can also measure the channel noise voltages and currents to obtain the total loop resistance in the cable. If Alice and Bob use the same resistance values, $R_{\mathrm{L}} R_{\mathrm{L}}$ or $R_{\mathrm{H}} R_{\mathrm{H}}$, the exchanged bit is non-secure and is discarded [2]. Conversely the combinations $R_{\mathrm{L}} R_{\mathrm{H}}$ and $R_{\mathrm{H}} R_{\mathrm{L}}$ are secure, and Eve cannot differentiate between the two alternatives. This is because the mean-square resultant noises are identical for $R_{\mathrm{L}} R_{\mathrm{H}}$ and $R_{\mathrm{H}} R_{\mathrm{L}}$ provided that the cable is ideal and short. Eve knows that Alice and Bob have exchanged a secure bit, but she does not know who is using R_{L} and who is using 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 Fig. 1). There is a non-zero capacitance between these two conductors that leads to capacitive currents causing information leak. 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.

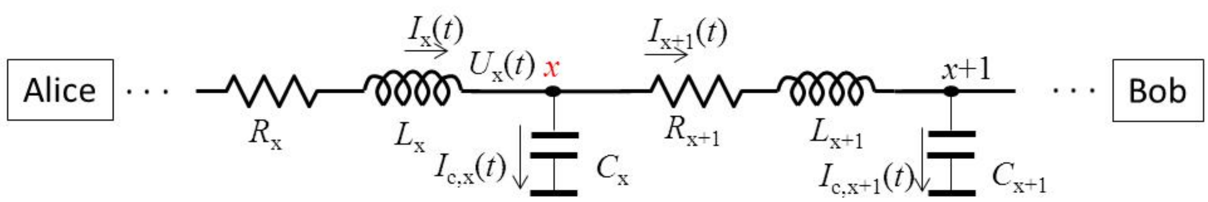

Figure 2. Cable model and cable capacitance attack

Fig. 2, shows the distributed elements model of coaxial cables. According to the 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].

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, respectively, see Fig. 3.

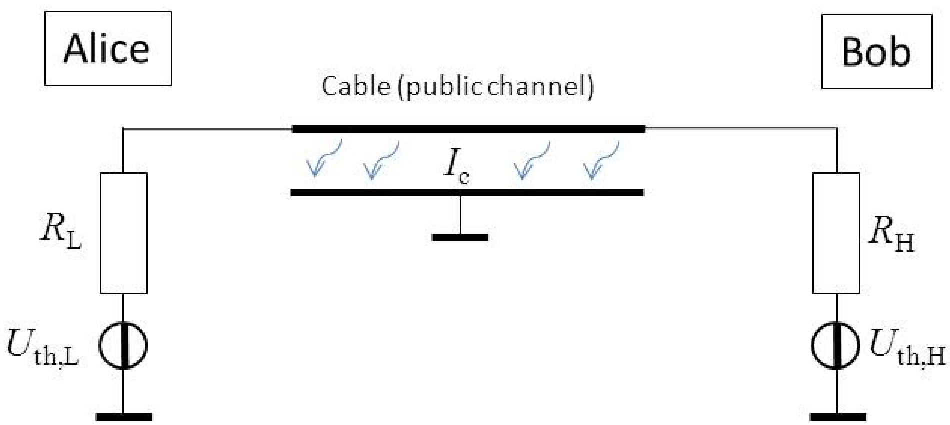

Figure 3. The simulated KLJN secure key exchange system with the capacitive current I_c. The generator voltages $U_{th,L}$ and $U_{th,H}$ are the Johnson noise voltages of R_L and R_H, respectively.

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

$$U_{th} = \sqrt{4kT_{eff} R B_{noise}} . \tag{6}$$

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 $U_{th,L}$ and $U_{th,H}$, respectively). Thus

$$U_{th,L} / U_{th,H} = \sigma_L / \sigma_H = \sqrt{R_L / R_H} , \tag{7}$$

where $\sqrt{R_L/R_H} = \sqrt{1/9}$, thus $\sigma_L/\sigma_H = 1/3$. For the simulations, the rms thermal noise voltages of R_L and R_H were chosen as 1V and 3V, respectively, corresponding to $T_{eff} \approx 7\times 10^{16}$ K.

Fig. 4(a) shows the amplitude density function (histogram) of the noise voltage of R_L and Fig. 4(b) shows the cumulative distribution as normal probability plot where a straight line indicates exact normal distribution.

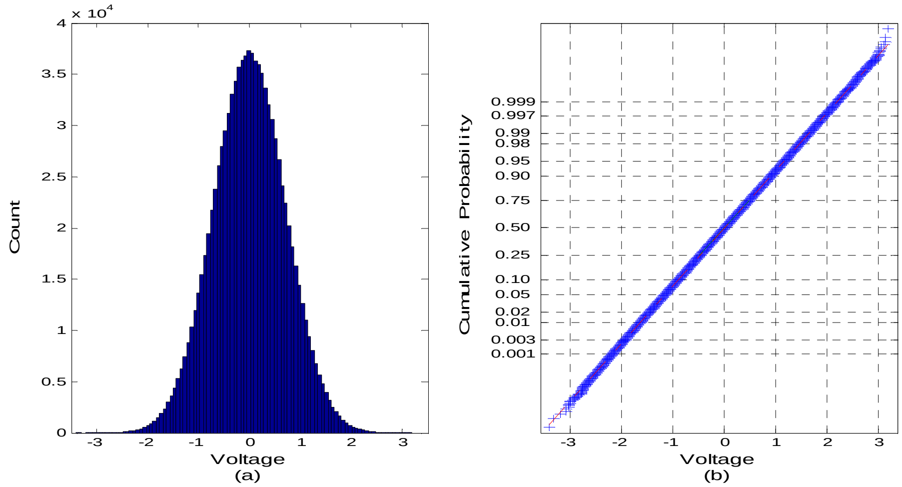

Figure 4. Statistics of the Johnson noise voltage of R_L with 10^6 samples. (**a**) amplitude density function (histogram); (**b**) cumulative distribution as normal probability plot.

3.2 Comparing a lumped and the distributed element models at different wavelengths

First, for enhanced computational speed, we explored the possibility of using lumped element cable model for the simulations because the continuum model simulations are at least 1000 times slower. Our investigation 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

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

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] about the proof that there are no waves in this limit).

Fig. 5(a) and 5(b) shows the simple lumped element model and the distributed model of the RG58 coaxial cable, respectively. Based on the specific inductance and capacitance, the propagation velocity c in the RG58 coaxial cable is 2×10^8 meter/sec. 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 meters, 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 at Fig. 5.

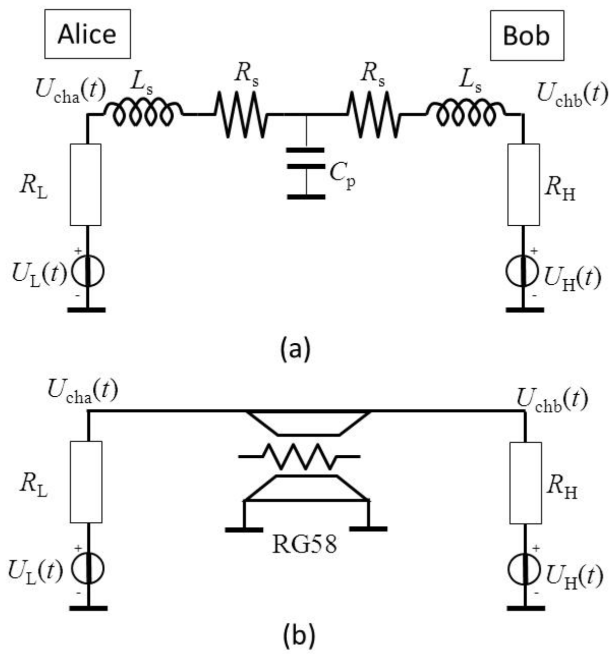

Figure 5. The RG58 coaxial cable models (1000 m length) with R_L (1 kOhm) and R_H (9 kOhm).

(a) The lumped element model: the component values: $R_S = 10.5\text{ Ohm}$, $L_S = 125\ \mu\text{H}$, $C_P = 100\text{ nF}$.

(b) The distributed model had the following parameters: $R = 0.021\text{ Ohm/meter}$, $L = 250\text{ nH/meter}$, $C = 100\text{ pF/meter}$. The characteristic impedance of the cable is 50 Ohm.

Fig. 6 shows the simulation results in which $U_{\text{cha,lump}}$ and $U_{\text{cha,dist}}$ denoted the voltage timefunctions of the lumped and distributed element models, respectively. In Fig. 6(a), the two waveforms were 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, too, as mentioned above.

In Fig. 6(b), with γ=8, the two waveforms are very similar whereas in Fig 6(c), 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 meters cable, respectively. To avoid that the cable capacitance truncates the effective bandwidth of the noise, we used noise bandwidth $B_{noise} = 0.25$ kHz for the noise generators ($\gamma = 800$ at 1000 meters and $\gamma = 8000$ at 100 meters).

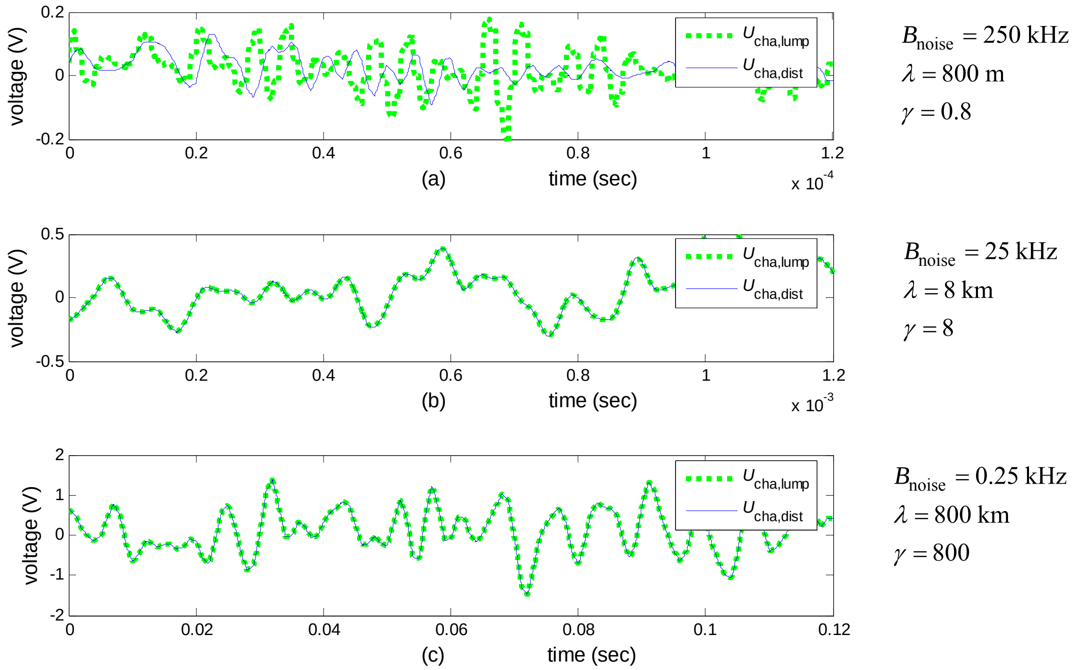

Figure 6. The voltage waveforms at Alice's side, $U_{cha,lump}$ and $U_{cha,dist}$, for the lumped and distributed element models, respectively, for a 1000 meters cable, at **(a)** γ=0.8; **(b)** γ=8; **(c)** γ =800.

3.3 The attack protocol

In this section, we discuss the information leak caused by the cable capacitance and evaluate Eve's success probability of guessing the key bits.

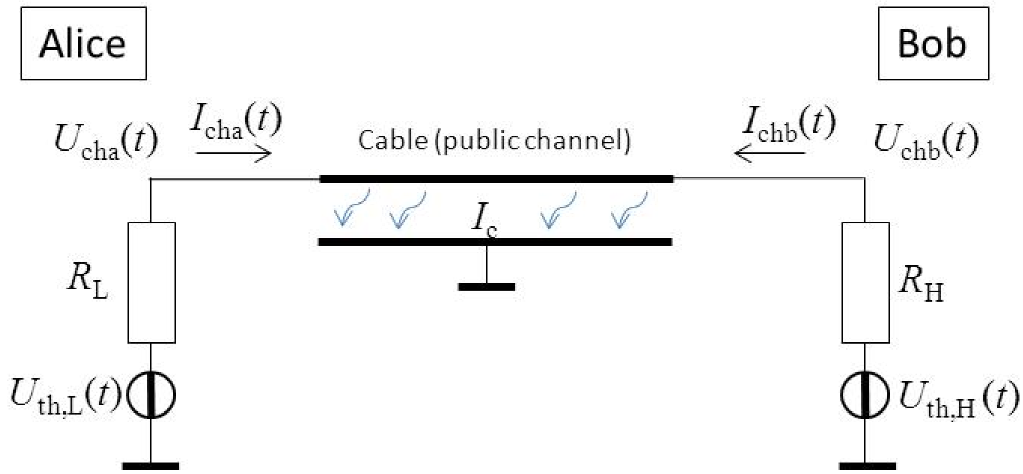

Figure 7. The simulated model with $R_L = 1$ kOhm and $R_H = 9$ kOhm. $U_{cha}(t)$, $I_{cha}(t)$, $U_{chb}(t)$ and $I_{chb}(t)$ are the voltages and currents at Alice's and Bob's ends, respectively.

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

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

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

where $U_{cha}(t)$, $I_{cha}(t)$, $U_{chb}(t)$ and $I_{chb}(t)$ are the channel voltages and currents at Alice's and Bob's ends, respectively, see Fig. 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:

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

When *N* approaches infinity, then 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 bandwidth, or the parasitic capacitance (longer the cable), the higher the leak.

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, 100; at 2 different cable lengths, 100 and 1000 meters. 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 meters cable, Eve's success rate was 50.9%. However, when the cable length was increased to 1000 meters with the other parameters unchanged, Eve's success rate became 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 meters cable**	**1000 meters 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, providing the same voltage on the outer shield of the cable as on the inner wire [39]. This can be done by an ideal voltage follower, see Fig. 8. There is no capacitive current from the inner wire to the outer shield thus, the attack is nullified.

We simulated the capacitor killer arrangement at the most effective attack scenario (i.e., when Eve success rate was 76.9%). The simulation results showed that Eve 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 at the practical cable conditions we tested.

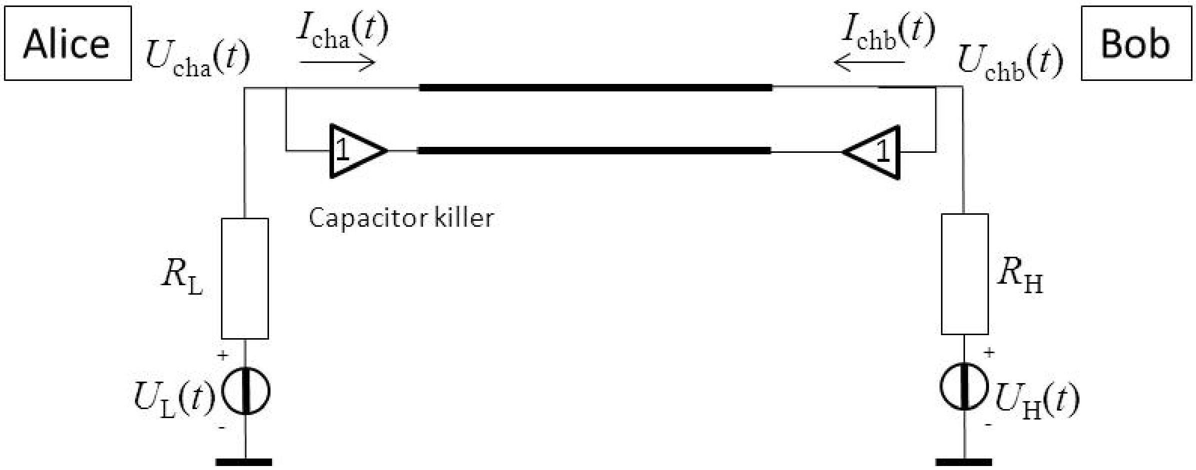

Figure 8. The KLJN system with the capacitor killer. An ideal voltage follower is driving the outer shield, which is not grounded at this time.

4.2 Privacy Amplification

Another method to secure the key exchange and to reduce information leak is by utilizing privacy amplification [44]. The simplest and most secure concept 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 resulting a cleaner key with much higher security and one quarter of its original length. This type of privacy amplification can be used by the KLJN scheme to effectively reduce any information leak due to the extraordinarily low bit error probability of the KLJN system [51-53].

Conclusions

By utilizing the LTSPICE simulator we have validated the cable capacitance attack. The results have shown that Eve success rate was 76.9% for a 1000 meters RG58 coaxial cable, with 100 samples per bit, at 10 bits/sec. To reduce the information leak due to the cable capacitance attack, capacitor killer and privacy amplification techniques have been utilized and simulated. The capacitor killer reduced Eve’s success rate from 76.9% to 50.1%, while the privacy amplification technique was also effective at the price of slowing down. The unconditional security of a practical KLJN key exchange system [4] has been preserved against this attack, too.

References

1. Cho, A. Simple Noise May Stymie Spies Without Quantum Weirdness. *Science* **2005**, *309*, 2148.
2. Kish, L.B. Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law. *Physics Letters 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. *Fluctuation and Noise Letters* **2006**, *6*, L57-L63.
4. Kish, L.B.; Granqvist, C.G. On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator. *Quantum Information Processing* **2014**, *13*, 2213-2219.
5. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* **1984**, 175-179.
6. Yuen, H.P. Essential lack of security proof in quantum key distribution. In *ArXiv e-prints*, 2013; Vol. 1310, p 842.
7. Hirota, O. Incompleteness and Limit of Quantum Key Distribution Theory. In *ArXiv e-prints*, 2012; Vol. 1208, p 2106.
8. Renner, R. Reply to recent scepticism about the foundations of quantum cryptography. In *ArXiv e-prints*, 2012; Vol. 1209, p 2423.
9. Yuen, H.P. Unconditional Security In Quantum Key Distribution. In *ArXiv e-prints*, 2012; Vol. 1205, p 5065.
10. Yuen, H.P. On the Foundations of Quantum Key Distribution - Reply to Renner and Beyond. In *ArXiv e-prints*, 2012; Vol. 1210, p 2804.
11. Yuen, H.P. Security Significance of the Trace Distance Criterion in Quantum Key Distribution. In *ArXiv e-prints*, 2011; Vol. 1109, p 2675.
12. Yuen, H.P. Key Generation: Foundations and a New Quantum Approach. In *ArXiv e-prints*, 2009; Vol. 0906, p 5241.
13. Merali, Z. Hackers blind quantum cryptographers. In *Natures News*, 2009.
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. *Nature Communications* **2011**, *2*, 349.
15. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Scarani, V.; Makarov, V.; Kurtsiefer, C. Experimentally Faking the Violation of Bell's Inequalities. *Physical Review Letters* **2011**, *107*, 170404.
16. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **2010**, *4*, 686-689.
17. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Avoiding the blinding attack in QKD. *Nature Photonics* **2010**, *4*, 801.
18. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Thermal blinding of gated detectors in quantum cryptography. *Optics 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. *Physical Review Letters* **2011**, *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. *Physical Review A* **2011**, *84*, 32320.
21. Lydersen, L.; Skaar, J.; Makarov, V. Tailored bright illumination attack on distributed-phase-reference protocols. *Journal of Modern Optics* **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 Journal of Physics* **2011**, *13*, 3043.
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 Journal of Physics* **2011**, *13*, 3042.
24. Sauge, S.; Lydersen, L.; Anisimov, A.; Skaar, J.; Makarov, V. Controlling an actively-quenched single photon detector with bright light. *Optics Express* **2011**, *19*, 23590.
25. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics* **2009**, *11*, 5003.
26. Makarov, V.; Skaar, J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Info. 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. *Selected Topics in Quantum Electronics, IEEE Journal of* **2015**, *21*, 1-5.
28. Xu, F.; Curty, M.; Qi, B.; Lo, H.-K. Measurement-device-independent quantum cryptography. *Selected Topics in Quantum Electronics, IEEE Journal of* **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. *Selected Topics in Quantum Electronics, IEEE Journal of* **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. *Physical Review A* **2015**, *91*, 062301.
31. Bennett, C.H.; Jess Riedel, C. On the security of key distribution based on Johnson-Nyquist noise. In *ArXiv e-prints*, 2013; Vol. 1303, p 7435.
32. Hao, F. Kish's key exchange scheme is insecure. *IEE Proceedings-Information Security* **2006**, *153*, 141-142.
33. Scheuer, J.; Yariv, A. A classical key-distribution system based on Johnson (like) noise---How secure? *Physics Letters 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" *Fluctuation and Noise Letters* **2006**, *06*, C37-C41.
36. Kish, L.B. Response to Scheuer–Yariv: "A classical key-distribution system based on Johnson (like) noise—how secure?". *Physics Letters 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. *Physics Letters 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. *Physics Letters 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. *Physics Letters 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. *Metrology and Measurement Systems* **2013**, *20*, 3-16.
41. Kish Laszlo, B. Enhanced Secure Key Exchange Systems Based on the Johnson- Noise Scheme. In *Metrology and Measurement Systems*, 2013; Vol. 20, p 191.
42. Smulko, J. Performance Analysis of the" Intelligent" Kirchhoff-Law–Johnson-Noise Secure Key Exchange. *Fluctuation and Noise Letters* **2014**, *13*, 1450024.

43. Kish, L.B.; Mingesz, R. Totally secure classical networks with multipoint telecloning (teleporation) of classical bits through loops with Johnson-like noise1. *Fluctuation and Noise Letters* **2006**, *06*, C9-C21.
44. Horváth, T.; Kish, L.B.; Scheuer, J. Effective privacy amplification for secure classical communications. *EPL (Europhysics Letters)* **2011**, *94*, 28002.
45. Kish, L.B.; Peper, F. Information Networks Secured by the Laws of Physics. *IEICE Transactions on Communications* **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. *Fluctuation and Noise Letters* **2013**, *12*, 1350018.
48. Kish, L.B.; Saidi, O. Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives. *Fluctuation and Noise Letters* **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? *Fluctuation and Noise Letters* **2014**, *13*, 1450016.
50. Kish, L.; Chen, S.; Granqvist, C.; Smulko, J. Waves in a short cable at low frequencies, or just hand-waving?, invited paper at the International Conference on Noise and Fluctuations (2015), Xi'an, China, in press. . *arXiv preprint arXiv:1505.02749* **2015**.
51. Saez, Y.; Kish, L.B.; Mingesz, R.; Gingl, Z.; Granqvist, C.G. Bit errors in the Kirchhoff-Law–Johnson-Noise secure key exchange. *International Journal of Modern Physics: Conference Series* **2014**, *33*, 1460367.
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. *Fluctuation and Noise Letters* **2014**, *13*, 1450020.
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. *Scientific Reports* **2015**, *5*, 13653.
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. *Fluctuation and Noise Letters* **2015**, *14*, 1550011.
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. In *Metrology and Measurement Systems*, 2014; Vol. 21, p 389.