TherMod Communication: Low Power or Hot Air?

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

Received Day Month Year
Revised Day Month Year
Accepted Day Month Year
Published Day Month Year

Communicated by

The Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme leverages statistical physics to enable secure communication with zero average power flow in a wired channel. While the original KLJN scheme requires significant power for operation, a recent wireless modification, TherMod, proposed by Basar claims a “low power” implementation. This paper critically examines this claim. We explain that the additional components inherent in Basar’s wireless adaptation substantially increase power consumption, rendering the “low power” assertion inappropriate. Furthermore, we clarify that the security claims of the original KLJN scheme do not directly translate to this wireless adaptation, implying significant security breach. Finally, the scheme looks identical one of the stealth communicators from 2005, which was shown not to be secure.

Keywords: unconditional security; wireless modification; power consumption.

1. Introduction

The Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme, introduced by Kish in 2005 [1-3], represents a novel approach to secure communication by exploiting the principles of statistical physics. Unlike traditional cryptographic methods that rely on computational complexity, KLJN uses thermal noise generated by resistors to establish a secure key exchange over a wired channel with zero average power flow in the information channel. The core of the KLJN scheme, illustrated in Fig. 1, consists of resistors, switches, and noise generators that create an unconditionally secure system primarily based on the 2nd law of thermodynamics.

Recently, Basar proposed a wireless modification of the KLJN scheme, referred to as the TherMod scheme [4], claiming it achieves “low power” communication. This claim has significant implications for applications where energy efficiency is critical, such as IoT devices and wireless sensor networks. However, the practical realization of the KLJN system introduces complexities that challenge the validity of the “low power” assertion, which the wireless expansion further enhances. This paper critically evaluates Basar’s claim, analyzing the power consumption of both the original KLJN scheme and its wireless adaptation. Additionally, we investigate whether the security guarantees of the wired KLJN scheme are upheld in the wireless context, identifying "killer" vulnerabilities, because it

has been well known that the KLJN scheme can offer security only in the no-wave limit (quasi static limit) [5-7]. Furthermore, the scheme in [4] is itself essentially unsecure because Alice and Bob do not form parallel resistor pairs to manifest a secure key exchange. The Basar scheme looks like one of the stealth communicators from 2005, which were shown not to be secure [8].

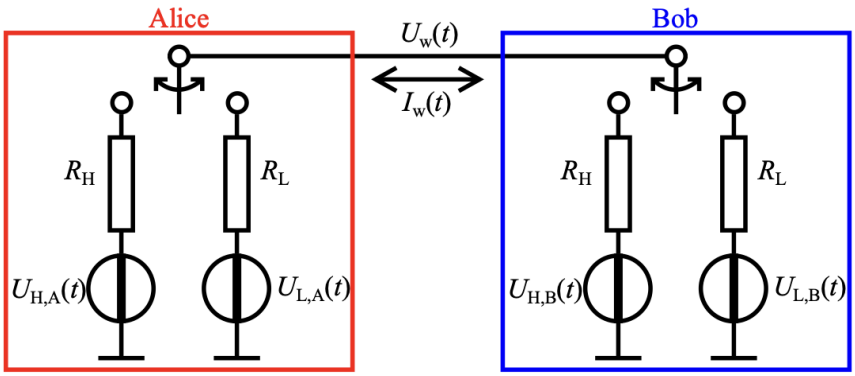

Fig. 1. The core of the KLJN scheme [1-3]. Communicating parties Alice and Bob are connected via a wire. The wire voltage and current are denoted as $U_w(t)$ and $I_w(t)$, respectively. Alice and Bob have identical pairs of resistors R_H and R_L ($R_H > R_L$) that are randomly selected and connected to the wire at the beginning of the bit exchange period. The statistically independent thermal noise voltages $U_{H,A}(t)$, $U_{L,A}(t)$, $U_{H,B}(t)$, and $U_{L,B}(t)$ represent the noise voltages of the resistors R_H and R_L of Alice and Bob, respectively.

2. Background and Methodology

2.1. *The KLJN Scheme*

The KLJN scheme operates by leveraging Johnson-Nyquist noise, which arises from the thermal agitation of charge carriers in resistors. In the KLJN setup, the two communicating parties (Alice and Bob) each randomly select one of two resistors (R_H or R_L) and connect them to the shared wire. The thermal noise generated by these resistors is measured as voltage and current fluctuations across the channel. By comparing the noise characteristics, Alice and Bob establish a shared secret key. The security of the scheme relies on the indistinguishability of the noise profiles to an eavesdropper (Eve), ensuring unconditional security [1].

The power efficiency of the KLJN scheme is often highlighted due to the zero average power flow in the information channel. However, this does not account for the power consumed by absolutely necessary auxiliary components, such as random number generators, switches, and measurement devices.

2.2. *Basar's Wireless Adaptation (TherMod)*

Basar's TherMod scheme [4] is trying adapt the KLJN principles to a wireless medium, as depicted in Fig. 2. This modification replaces the wired channel with a wireless link, using antennas to transmit and receive noise signals. The TherMod scheme aims to retain the

security and power efficiency of the original KLJN system while enabling wireless communication. Basar claims that this adaptation achieves "low power" operation, making it suitable for energy-constrained applications. This mistake is probably due to error of neglecting the power requirements of the devices that run the KLJN system. This power is significant, particularly if one compares it with the very slow data transport of the KLJN scheme that involves amplification and statistical signal processing to extract just a single exchanged bit.

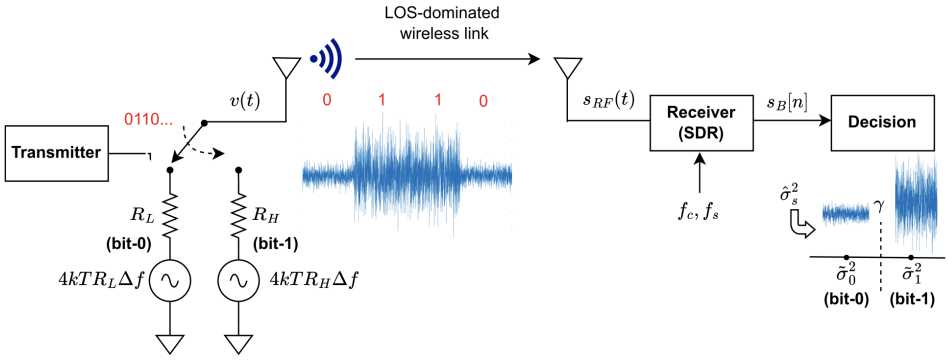

Fig. 2. The core of the proposed TherMod scheme, illustrating the wireless transmission of thermal noise signals using antennas and additional signal processing components [4].

2.3. *Methodology*

To evaluate Basar's claim, we analyze the power consumption of both the KLJN and TherMod schemes. We consider the energy requirements of all components, including those not directly involved in the information channel. For the TherMod scheme, we examine the additional components introduced by the wireless medium, such as amplifiers and signal processing units. We also assess the security implications of the wireless adaptation by identifying potential vulnerabilities not present in the wired KLJN scheme.

3. Analysis and Refutation of the "Low Power" Claim

3.1. *Power Consumption in the KLJN Scheme*

While the KLJN scheme achieves zero average power flow in the information channel, this metric does not apply when assessing the system's overall energy efficiency. The KLJN setup requires several power-consuming components:

- **Random Number Generators**: These produce the noise signals necessary for key exchange, consuming significant energy to ensure high entropy.
- **Switches**: These alternate between resistor values (R_H or R_L), requiring power for actuation and control.
- **Measurement Devices**: These amplify voltage and current fluctuations, necessitating sensitive electronics with non-negligible power demands.

- Statistical evaluation of the mean-square voltages and differentiation between secure and non-secure levels.

These components operate continuously during key exchange, resulting in substantial power consumption despite the zero net energy transfer in the channel and thus undermining any claims of inherent energy efficiency.

3.2. *Power Consumption in the TherMod Scheme*

Basar's TherMod scheme introduces additional components to enable wireless communication, further increasing power consumption. Key differences include:

- **Signal Amplification**: Wireless transmission requires amplifiers to boost the noise signals to levels suitable for propagation over a wireless medium. These amplifiers consume significant power, especially in environments with high noise or interference.
- **Sophisticated Measurement Techniques**: The wireless medium introduces signal degradation due to path loss, fading, and interference. To accurately measure noise characteristics, the TherMod scheme requires advanced signal processing and error correction, both of which are power-intensive.
- **Antenna Systems**: The use of antennas for transmission and reception adds to the energy budget, particularly for maintaining signal integrity over varying distances.

Our analysis indicates that the power consumption of the TherMod scheme is substantially higher than that of the wired KLJN scheme. For example, a typical RF amplifier used in wireless communication can consume tens to hundreds of milliwatts, compared to the microwatt-level power requirements of wired measurement circuits. This discrepancy directly contradicts Basar's "low power" claim.

3.3. *Quantitative Comparison*

To quantify the power difference, consider a simplified model. In the KLJN scheme, assume the auxiliary components (random number generators, switches, and measurement devices) consume a total of 10 mW during operation. In the TherMod scheme, the addition of an RF amplifier (50 mW) and advanced signal processing (20 mW) increases the total power consumption to approximately 80 mW. This represents an eightfold increase, rendering the "low power" label inaccurate.

4. Security Considerations

The security of the original KLJN scheme relies on the physical properties of thermal noise and the wired channel's controlled environment. An eavesdropper attempting to intercept the key must distinguish between noise profiles generated by different resistor combinations, and this is impossible [2].

In the wireless TherMod scheme, the security landscape changes significantly:

- **Environmental Noise**: The wireless medium is susceptible to external noise and interference, which can mask or alter the thermal noise signals, potentially compromising the indistinguishability of noise profiles.
- **Signal Interception**: Wireless signals are inherently broadcast, making it easier for an eavesdropper to capture the transmitted noise without physical access to the channel.
- **Amplification Artifacts**: The amplification process may introduce artifacts that an eavesdropper could exploit to infer information about the resistor states.

These vulnerabilities suggest that the unconditional security of the wired KLJN scheme does not directly translate to the TherMod scheme. Further research is needed to quantify these risks and develop mitigation strategies.

5. Conclusion

The Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme offers an innovative approach to secure communication by leveraging thermal noise. However, claims of "low power" operation, particularly in Basar's wireless TherMod adaptation, are misleading. Our analysis demonstrates that the TherMod scheme's additional components, such as amplifiers and advanced signal processing units, significantly increase power consumption compared to the wired KLJN scheme. Furthermore, the security guarantees of the original KLJN system are not assured in the wireless context due to environmental noise, signal interception risks, and amplification artifacts.

These findings highlight the challenges of achieving low-power, secure communication in wireless environments using KLJN-based schemes. Researchers and practitioners should approach such claims with skepticism and prioritize comprehensive power and security analyses in future proposals. While the KLJN scheme remains a promising concept, its practical implementation, requires careful consideration of energy and security trade-offs. Finally, security in the KLJN scheme exists only in the no-wave limit. Any waves reflections, interference, delays beyond the autocorrelation time eliminate the security. The scheme in [4] is rather imitating the "stealth" thermal noise communicator of Kish [8] which has wireless version, too, and was shown not to be secure.

References

[1] C. Chamon and L.B. Kish, Perspective–On the Thermodynamics of Perfect Unconditional Security, *Appl. Phys. Lett.* **119** (2021) 010501.
[2] L.B. Kish, Totally secure classical communication utilizing Johnson (-like) noise and Kirchhoff's law, *Phys. Lett. A* (2006).
[3] L.B. Kish, Enhanced secure key exchange system based on the Johnson(-like) noise, *Fluct. Noise Lett.* (2007).
[4] E. Basar, Communication by Means of Thermal Noise: Toward Networks With Extremely Low Power Consumption, *IEEE Comm*. (2022).
[5] L.B. Kish, D. Abbott, C.G. Granqvist, "Critical analysis of the Bennett-Riedel attack on secure cryptographic key distributions via the Kirchhoff-law-Johnson-noise scheme", PLoS ONE 8 (2013) e81810; https://doi.org/10.1371/journal.pone.0081810
[6] L.B. Kish, T. Horvath, "Notes on Recent Approaches Concerning the Kirchhoff-Law-Johnson-Noise-based Secure Key Exchange", Physics Letters A 373 (2009) 2858-2868.

[7] L.B. Kish, S.P. Chen, C.G. Granqvist, J. Smulko, "Waves in a short cable at low frequencies, or just hand- waving? What does physics say?", invited talk at the 23rd International Conference on Noise and Fluctuations (ICNF 2015), Xian, China, June 2-5, 2015. DOI: 10.1109/ICNF.2015.7288604

[8] L.B. Kish, "Stealth communication: Zero-power classical communication, zero-quantum quantum communication and environmental-noise communication", Applied Physics Lett. 87 (2005), Art. No. 234109.