RANDOM NUMBER GENERATOR, ZERO-CROSSING, AND NONLINEARITY ATTACKS AGAINST THE KIRCHHOFF-LAW-JOHNSON-NOISE (KLJN) SECURE KEY EXCHANGE PROTOCOL

A Dissertation

by

CHRISTIANA SÖKELAND FREITAS CHAMON

Submitted to the Graduate and Professional School of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Laszlo Kish
Committee Members,	Jun Zou
	Chanan Singh
	Andreas Klappenecker
Head of Department,	Miroslav Begovic

May 2022

Major Subject: Electrical Engineering

ABSTRACT

This dissertation demonstrates three new types of attacks against the Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchanger.

The first attack type is based on compromised random number generators.

The first RNG attacks are deterministic. In the first attack, Eve knows both noises. We show that Eve can quickly crack the bit via Ohm's Law and one-bit powers, within a fraction of the bit exchange period. In the second attack, Eve knows only Bob's noise, so she can learn Bob's resistance value via Ohm's Law and Alice's resistance at the end of the bit exchange period. She can also use a process of elimination.

The second RNG attacks are statistical. In the first attack, Eve has partial knowledge of Alice's and Bob's noises. We show that Eve can crack the bit by taking the highest cross-correlation between her noises and the measured noise in the wire, and by taking the highest cross-correlation between her noises and her evaluation of Alice's/Bob's noises. In the second attack, Eve has partial knowledge of only Alice's noise. In this situation, Eve can still crack the bit, but after the bit exchange period.

The second attack type is based on thermodynamics. Previously, the KLJN scheme required thermal equilibrium. However, Vadai, et al, in (Nature) Science Reports shows a modified scheme, where there is a non-zero thermal noise, yet the system resists all the known attacks. We introduce a new attack against their system, which utilizes coincidence events between the line current and voltage. We show that there is non-zero information leak toward the Eavesdropper. As soon as the thermal equilibrium is restored, the system becomes perfectly secure again.

The final attack type is based on the nonlinearity of the noise generators. We explore the effect of total distortion at the second order, third order, and a combination of the second and third orders on the security of the KLJN scheme. It is demonstrated that a distortion as little as 1% results in a notable power flow, which leads to a significant information leak. We also show that decreasing the effective temperature results in the KLJN scheme approaching perfect security.

DEDICATION

To Theo, my heart, my sunshine.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor Dr. Laszlo Bela Kish for taking me in as a "refugee" Ph.D. student and for his continual friendship, mentorship, guidance, humor, and support throughout the remainder of my time here at Texas A&M University and for providing me the training wheels needed to live up to my potential as a scientist. Switching to his research group is literally the best decision I've ever made as a graduate student. I would also like to thank my committee members Dr. Jun Zou, Dr. Chanan Singh, and Dr. Andreas Klappenecker for being here for me and for their friendly encounters.

I would also like to thank Dr. Jose Silva-Martinez, Dr. Edgar Sanchez-Sinencio, and Dr. Kamran Entesari for being such great professors and for the friendly encounters, conversations, and laughs, as well as those from Ms. Ella Gallagher. I always enjoyed their company, and I would especially like to thank Dr. Sanchez for keeping the coffee machine constantly running! The graduate office crew Melissa Sheldon, Katie Bryan, and Dr. Scott Miller also have my thanks for their academic advising and for the aforementioned.

My main collaborator Shahriar Ferdous has my thanks for actively working with me and for his never-ending friendship. My thanks also extends to my friends in the ECEN department for their friendship, mentorship, and keeping me happy, as well as my friends outside of ECEN and Texas A&M University. A special thanks goes to my friend and former professor Dr. Gülin Tulunay Aksu from the University of Houston for being here for me, keeping me grounded in reality, and continually providing evaluations and suggestions in and out of school from the perspective of a former graduate student.

My gratitude further extends to my AggieWesties family who makes me look like a good West Coast Swing dancer every Wednesday night as I escape from reality. It was truly an honor to serve as the treasurer and vice president of the greatest organization in the world. The same thanks also extends to my Westie friends outside of AggieWesties. My Dance Barre family also holds a special place in my heart, and I cannot thank them enough for helping me improve my solo

technique, continually pushing me to be the best dancer I can be, providing me a safe space, and for being here for me throughout the COVID-19 pandemic when the dance floor was forcibly taken away from me.

I am grateful for my parents Jorge and Ana Chamon, my siblings Julia and Gabriel Chamon, my parents-in-law Lusi and Doroteo Garcia, and my siblings-in-law Michael and Bianca Ortega and Juan and Jasmine Garcia for their constant care and support, even though I am 100 miles away. This thanks also extends to my prickle, for continually including me in their lives and cheering for me no matter how far away they are or how busy their lives got.

Penultimately but far from least, I am forever indebted to my wonderful loving husband, biggest fan, and best friend in the world Doroteo "Theo" Garcia for moving to College Station to be with me, for his exceeding patience, for constantly supporting and cheering for me, and for believing in me even when I didn't believe in myself. Being married to a graduate student is hard. However, he pulled it off so amazingly. It is to him that I dedicate this dissertation to.

My Ph.D. studies would not have been possible without these people, for which I stand eternally grateful. Finally, my eternal gratitude extends to God, for it is He who has ultimately provided me with this opportunity ("Jesus looked at them and said, 'With man this is impossible, but with God all things are possible.'" ~Matthew 19:26).

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supported by a dissertation committee consisting of Dr. Laszlo Kish [advisor], Dr. Jun Zou, and Dr. Chanan Singh of the Department of Electrical Engineering and Dr. Andreas Klappenecker of the Department of Computer Science.

The Gaussian band-limited white noise was provided by Shahriar Ferdous.

All other work conducted for the dissertation was completed by the student independently.

Funding Sources

Graduate study was supported by a Teaching Assistantship, the Ebensberger Fellowship, and grader positions, all from Texas A&M University.

NOMENCLATURE

BEP	Bit Exchange Period
D	Distortion
FCK	Ferdous, Chamon, and Kish
FFT	Fast Fourier Transform
GBLWN	Gaussian Band-Limited White Noise
IFFT	Inverse Fast Fourier Transform
KLJN	Kirchhoff-Law-Johnson-Noise
NSA	National Security Agency
NSS	National Security Systems
QKD	Quantum Key Distribution
RMS	Root Mean Square
RNG	Random Number Generator
TD	Total Distortion
VMG	Vadai, Mingesz, and Gingl

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

LIST OF TABLES

TABLE Page

1. INTRODUCTION[1,2]

1.1 On Secure Communications

One way to establish the security of a communication is through encryption, that is, the conversion of plaintext into ciphertext via a cipher [1]. Figure 1.1 provides the general scope of symmetric-key cryptography [1]. The key is a string of random bits and both communicating parties Alice and Bob use the same key and ciphers to encrypt and decrypt their plaintext.

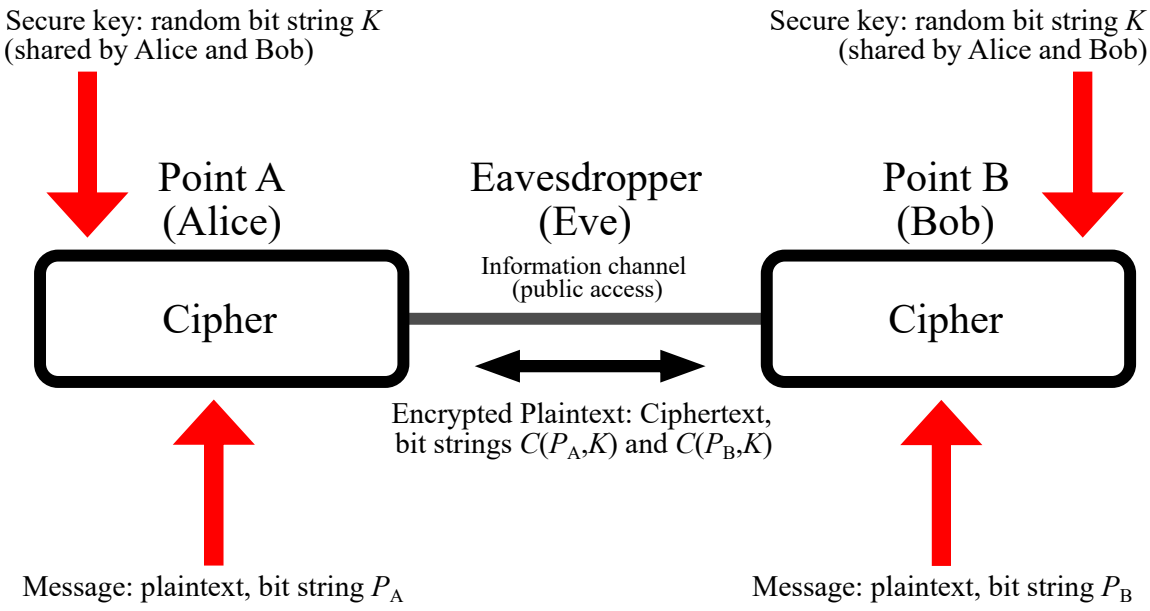


Figure 1.1: Symmetric-key cryptography [1]. Alice and Bob securely exchange a key (a string of random bits) through an information channel. The ciphers encrypt plaintext into the ciphertext C. The secure key is K, the plaintext messages of Alice and Bob are denoted by P_A and P_B, respectively, and the ciphertext is a function $C(P,K)$.

[1]Part of this chapter is reprinted with permission from C. Chamon, S. Ferdous, and L. B. Kish, "Deterministic random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, vol. 20, no. 5, 2021. Copyright 2021 by World Scientific Publishing Company.

[2]Part of this chapter is reprinted with permission from C. Chamon, S. Ferdous, and L. B. Kish, "Statistical random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, accepted for publication, 2021. Copyright 2021 by World Scientific Publishing Company.

For a plaintext message P and a secure key K, the encrypted message, or the ciphertext C, is a function of P and K, that is,

$$C = C(P, K). \tag{1.1}$$

In symmetric-key cryptography, for decryption, the inverse operation is used:

$$P = C^{-1}[C(P, K), K]. \tag{1.2}$$

Because the secure keys must be the same at the two sides (shared secret), another type of secure data exchange is needed before the encryption can begin: the secure key exchange, which is the generation and distribution of the secure key over the communication channel. Usually, this is the most demanding process in the secure communication because the communication channel is accessible by Eve, thus the secure key exchange is itself a secure communication where the cipher scheme shown in Figure 1.1 cannot be used. Eve records the whole communication during the key exchange, too. She knows every detail of the devices, protocols, and algorithms in the permanent communication system (as stated by Kerckhoffs's[3] principle/Shannon's maxim [2]), except for the key. In the ideal case of perfect security, the key is securely generated/shared, immediately used by a One Time Pad [3], and discarded after the usage. In practical cases, usually there are deviations from these strict conditions, yet the general rule holds: a secure system cannot be more secure than its key.

Our focus topic is the unconditionally secure Kirchhoff-law-Johnson-noise (KLJN) symmetric-key exchanger.

1.2 The KLJN Scheme

The KLJN system [40–99] is a statistical physical scheme based on the Second Law of Thermodynamics. It is a classical (statistical) physical alternative of Quantum Key Distribution (QKD),

[3] Auguste Kerckhoffs, not to be confused with Gustav Kirchhoff.

the base of quantum cryptography, which utilizes quantum physical photonic features.

As an illustration of the difficulties and depth of the issues of security, in papers [3–39], important criticisms and attacks are presented about QKD indicating some of the most important aspects of unconditionally secure quantum hardware and their theory. Very recently, National Security Agency (NSA) has made a public statement: "NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS)...". While we have reservations about this NSA statement, it inherently brings KLJN up for further considerations. Both the QKD and KLJN schemes count as "Post-Quantum" hardware solutions because they are resilient against any (past and future) computing schemes, including quantum computers, but only the KLJN scheme can be integrated on chips with currently available technology to offer unconditional security of communication within computers and instruments.

Figure 1.2 illustrates the core of the KLJN scheme. The two communicating parties Alice and Bob are connected via a wire. They have identical pairs of resistors $R_{\rm A}$ and $R_{\rm B}$. The statistically independent thermal noise voltages $U_{\rm H,A}(t)$, $U_{\rm L,A}(t)$, and $U_{\rm H,B}(t)$, $U_{\rm L,B}(t)$ represent the noise voltages of the resistors $R_{\rm H}$ and $R_{\rm L}$ ($R_{\rm H} > R_{\rm L}$) of Alice and Bob, respectively, which are generated from random number generators (RNGs) and must have a Gaussian amplitude distribution [59,62].

At the beginning of each bit exchange period (BEP), Alice and Bob randomly choose one of their resistors to connect to the wire. The wire voltage $U_{\rm w}(t)$ and current $I_{\rm w}(t)$ are as follows:

$$U_{\rm w}(t) = I_{\rm w}(t)R_{\rm B} + U_{\rm B}(t), \tag{1.3}$$

$$I_{\rm w}(t) = \frac{U_{\rm A}(t) - U_{\rm B}(t)}{R_{\rm A} + R_{\rm B}} \tag{1.4}$$

where $U_{\rm A}(t)$ and $U_{\rm B}(t)$ denote the instantaneous noise voltage of the resistor chosen by Alice and Bob, respectively. Alice and Bob (as well as Eve) use the mean-square voltage of the wire to assess the situation. According to the Johnson formula,

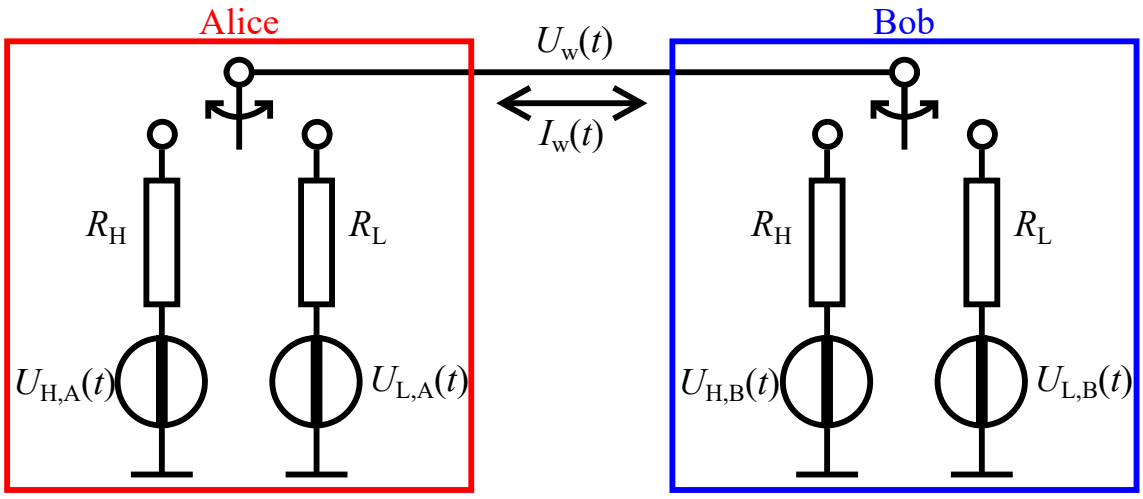


Figure 1.2: The core of the KLJN scheme. The two communicating parties Alice and Bob are connected via a wire. The wire voltage and current are denoted as $U_{\rm w}(t)$ and $I_{\rm w}(t)$, respectively. The parties have identical pairs of resistors $R_{\rm H}$ and $R_{\rm L}$ ($R_{\rm H} > R_{\rm L}$) that are randomly selected and connected to the wire at the beginning of the bit exchange period. The statistically independent thermal noise voltages $U_{\rm H,A}(t)$, $U_{\rm L,A}(t)$, and $U_{\rm H,B}(t)$, $U_{\rm L,B}(t)$ represent the noise voltages of the resistors $R_{\rm H}$ and $R_{\rm L}$ of Alice and Bob, respectively.

$$U^2_{\rm w,eff} = 4kT_{\rm eff}R_{\rm p}\Delta f_{\rm B}, \tag{1.5}$$

where k is the Boltzmann constant (1.38 x 10^{-23} J/K), $T_{\rm eff}$ is the publicly agreed effective temperature, $R_{\rm P}$ is the parallel combination of Alice and Bob's chosen resistors, given by

$$R_{\rm P} = \frac{R_{\rm A}R_{\rm B}}{R_{\rm A} + R_{\rm B}}, \tag{1.6}$$

and $\Delta f_{\rm B}$ is the noise bandwidth of the generators.

Four possible resistance situations can be formed by Alice and Bob: HH, LL, LH, and HL. Using the Johnson formula, these correspond to three mean-square voltage levels, as shown in Figure 1.3.

The HH and LL cases represent insecure situations because they form distinct mean-square voltages. The HL and LH cases represent secure bit exchange because Eve cannot distinguish between the corresponding two resistance situations (HL and LH). On the other hand, Alice and

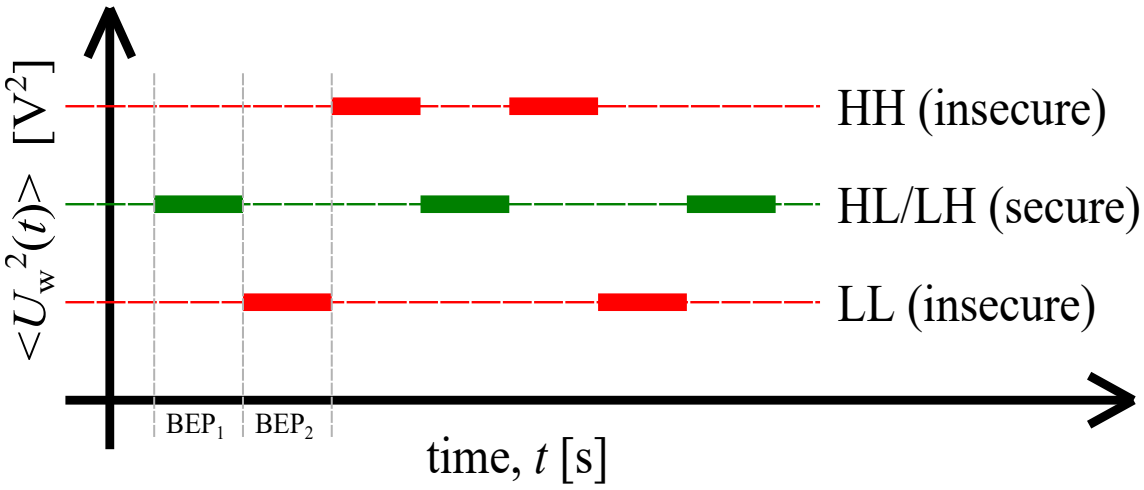


Figure 1.3: The three mean-square voltage levels. The HH and LL cases represent insecure situations because they form distinct mean-square voltages. The HL and LH cases represent secure bit exchange because Eve cannot distinguish between the corresponding two resistance situations (HL and LH). On the other hand, Alice and Bob can determine the resistance at the other end because they know their own connected resistance values.

Bob can determine the resistance at the other end because they know their own connected resistance values.

Several attacks against the KLJN system have been proposed [40–44, 79–99], but no attack has been able to compromise its information-theoretic (unconditional) security because each known attack is either invalid (conceptually incorrect errors in theory and/or experiments) or can be nullified by a corresponding defense scheme such that Eve's information entropy about the key approaches the bit length of the key, while Alice's and Bob's information entropy about the key approaches zero.

The rest of this dissertation is as follows. Chapter 2 introduces four deterministic and four statistical attacks based on the assumption that the random number generators Alice and Bob use to generate their noises are compromised. Chapter 3 introduces an attack based on coincidence events between the wire voltage and current. Chapter 4 introduces an attack based on the nonlinearity of Alice's and Bob's noise generators. Finally, Chapter 5 summarizes and concludes this dissertation.

2. RANDOM NUMBER GENERATOR ATTACK AGAINST THE KIRCHHOFF-LAW-JOHNSON-NOISE SECURE KEY EXCHANGER[1,2]

2.1 Random Number Generator Attacks

There are two classes of practical random number generators: true (physical) and computational. The nature of computational RNGs is that they collect randomness from various low-entropy input streams and try to generate outputs that are in practice indistinguishable from truly random streams [100–105]. The randomness of an RNG relies on the uncertainty of the random seed, or initialization vector, and a long sequence with uniform distribution. The moment an adversary learns the seed, the outputs are known, and the RNG is compromised.

Various RNG attacks exist against conditionally secure communications [100–105]. Unconditionally secure communications also require true random numbers for perfect security. That is also true for the noises of Alice and Bob, and for the randomness of their switch driving. Yet, it is unclear how Eve can utilize compromised RNGs to attack the KLJN scheme. Here, we demonstrate with simple attack examples that compromised noises lead to information leak.

The rest of this chapter is organized as follows. Section 2.2.1 describes the new deterministic attack protocols, Section 2.2.2 demonstrates their results, and Section 2.2.3 closes this part of the chapter. Then, Section 2.3 describes the new statistical attack protocols, Section 2.3.2 demonstrates their results, and Section 2.3.3 closes this chapter.

[1]Part of this chapter is reprinted with permission from C. Chamon, S. Ferdous, and L. B. Kish, “Deterministic random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, vol. 20, no. 5, 2021. Copyright 2021 by World Scientific Publishing Company.

[2]Part of this chapter is reprinted with permission from C. Chamon, S. Ferdous, and L. B. Kish, “Statistical random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, accepted for publication, 2021. Copyright 2021 by World Scientific Publishing Company.

2.2 Deterministic RNG Attack against the KLJN Scheme

2.2.1 Attack Methodology

Two theoretical situations are introduced where Eve can use compromised RNGs to crack the KLJN scheme: one where Eve knows the roots of both Alice's and Bob's generators (bilateral parameter knowledge), and another where Eve knows the root of only Bob's generator (unilateral parameter knowledge). A scenario is also introduced where the only statistical evaluation needed is in the rarely-occurring event of a negligible waiting/verification (no-response) time.

2.2.1.1 Bilateral Parameter Knowledge

2.2.1.1.1 *Ohm's Law*

Eve knows the roots of both Alice's and Bob's RNGs, thus she knows the instantaneous amplitudes of the noise voltage generators for each of their resistors (see Figure 1.2). With $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$ known, Eve measures the wire voltage $U_{\mathrm{w}}(t)$ and the wire current $I_{\mathrm{w}}(t)$ to determine R_{B} (see Equation (1.3)) and determines that the correct waveform for R_{B} is a flat line at the expected resistor value, while the incorrect waveform is a noise with divergent spikes. This is because the difference between $U_{\mathrm{w}}(t)$ and $U_{\mathrm{B}}(t)$ is directly proportional to $I_{\mathrm{w}}(t)$, with R_{B} as the scaling factor, and the incorrect noise voltage for $U_{\mathrm{B}}(t)$ would not render a constant value for R_{B}.

A realization of the waveforms for R_{B} is shown in Figure 2.1 at $R_{\mathrm{H}} = 100$ kΩ, $R_{\mathrm{L}} = 10$ kΩ, $T_{\mathrm{eff}} = 10^{18}$ K, and $\Delta f_{\mathrm{B}} = 500$ Hz. At the present situation, the flat line corresponds to R_{H}, thus Eve determines that Bob has chosen R_{H}. With $U_{\mathrm{A}}(t)$, $U_{\mathrm{B}}(t)$, R_{B}, and $I_{\mathrm{w}}(t)$ known, Eve uses Equation (1.4) to solve for R_{A}.

2.2.1.1.2 *One-Bit Powers*

Eve knows the roots of both Alice's and Bob's RNGs, thus she knows the instantaneous amplitudes of the noise voltage generators for each of their resistors (see Figure 1.2). With $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$ known, Eve uses Equations (1.3) and (1.4) to come up with the four possible waveforms for $U_{\mathrm{w}}(t)$ and $I_{\mathrm{w}}(t)$ and therefore the four possible waveforms for the instantaneous power flow from Alice to Bob, given by

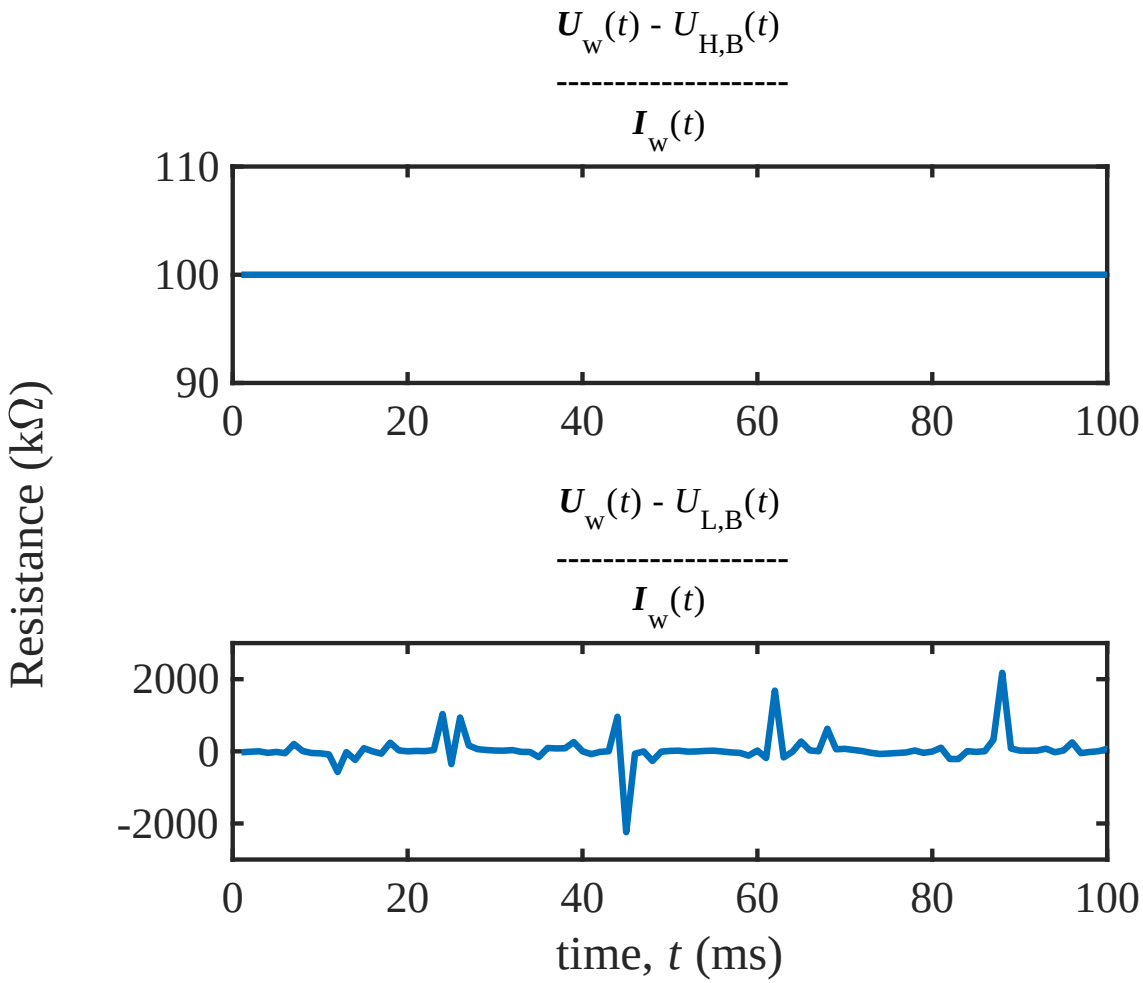


Figure 2.1: A realization of the waveforms for $R_{\rm B}$ (see Equation (1.3)) at $R_{\rm H} = 100$ kΩ, $R_{\rm L} = 10$ kΩ, $T_{\rm eff} = 10^{18}$ K, and $\Delta f_{\rm B} = 500$ Hz. The flat line corresponds to $R_{\rm H}$, thus Eve determines that Bob has chosen $R_{\rm H}$. The incorrect waveform is a noise with divergent spikes.

$$P_{\rm w}(t) = U_{\rm w}(t) I_{\rm w}(t). \tag{2.1}$$

Eve measures $U_{\rm w}(t)$ and $I_{\rm w}(t)$ and determines the actual $P_{\rm w}(t)$, which will be identical to one of her four hypothetical waveforms.

Note, the protocol shown above can be simplified to the extreme: Eve's instruments may have just one bit resolution, which is suitable to determine solely the instantaneous direction of the power flow.

2.2.1.2 Unilateral Parameter Knowledge

2.2.1.2.1 *Ohm's Law*

Eve knows only the root of Bob's generator RNG, thus she knows merely the noise generator outputs of Bob's resistors, $U_{\mathrm{L,B}}(t)$ and $U_{\mathrm{H,B}}(t)$. Alice's generator voltages are unknown to her. Eve uses the same protocol as mentioned in the bilateral case (see Section 2.2.1.1) to determine R_{B}, but because Alice's generator voltages are unknown to her, she cannot use Equation (1.4) to solve for R_{A}. Instead, she uses the KLJN protocol as Bob does: use the entire bit exchange period to evaluate the measured mean-squared voltage on the wire. From that value, by using Equation (1.5), she evaluates the parallel resultant R_{P} of the resistances of Alice and Bob. From R_{P} and R_{B}, she can calculate R_{A}. This method can still be applied in case Eve is not sure of her result from the bilateral case (see Section 2.2.1.1).

2.2.1.2.2 *Process of Elimination*

Eve knows the root of Alice's RNG. Thus, she knows merely the noise generator outputs of Alice's resistors, $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$. Bob's generator voltages are unknown to her. Eve measures the wire voltage $U_{\mathrm{w}}(t)$ and wire current $I_{\mathrm{w}}(t)$. Then, she calculates the hypothetical voltage drops on Alice's possible choice of resistances R_{H} and R_{L}. With these data, she tests two hypotheses:

Hypothesis (i): Alice has chosen R_{L}.

Hypothesis (ii): Alice has chosen R_{H}.

With Hypothesis (i), Eve takes the sum

$$U^{*}_{\mathrm{R_L}}(t) = U_{\mathrm{w}}(t) + I_{\mathrm{w}}(t)R_{\mathrm{L}}. \tag{2.2}$$

To test Hypothesis (i) she compares the $U_{\mathrm{A}}(t)$ determined by Equation (2.2) to $U_{\mathrm{L,A}}(t)$. If they are identical, then Hypothesis (i) is correct, otherwise Hypothesis (ii) is valid.

Finally, Eve evaluates the measured mean-square voltage on the wire over the bit exchange period. From that value, by using Equation (1.5), she evaluates the parallel resultant R_{P} of the

resistances of Alice and Bob. From R_{P} and R_{A}, she calculates R_{B}, thus she has cracked the KLJN scheme.

2.2.1.3 Timing

In each attack, Eve may or may not know which noise belongs to which resistor, or the noises may provide a voltage-to-current ratio that results in either R_{H} or R_{L}. In these scenarios, there will be a negligible waiting/verification (no-response) time before Eve can differentiate between the noises. The probability of the two independent noises being equal at any given point is

$$p_0 = \frac{1}{2^{\Delta}}, \tag{2.3}$$

where Δ is the number of resolution bits.

We can consider the event that the noises run identically for n subsequent steps to be a geometric distribution, with a probability of

$$p = p_0^n, \tag{2.4}$$

where $n = t/\tau$ and τ is the autocorrelation time, given by the Nyquist Sampling Theorem

$$\tau \approx \frac{1}{2\Delta f_{\mathrm{B}}}. \tag{2.5}$$

The approximation sign is due to the quantized nature of the noises, as they are constant throughout the bit exchange periods.

While such an identical match between the two noises is taking place, Eve cannot distinguish between the two noises, thus the actual resistance situation (see Figure 1.3) remains secure. However, the exponential decay in Equation (2.4) yields an efficient cracking scheme of the secure key bit value within a short amount of time. In accordance with Equation (2.4), the probability of the two independent seeds running identically is

$$p \approx p_0^{t/\tau} \approx \left(\frac{1}{2^{\Delta}}\right)^{t/\tau}. \tag{2.6}$$

2.2.2 Demonstration

2.2.2.1 Johnson Noise Emulation

First, we generated Gaussian band-limited white noise (GBLWN). Precautions were used to avoid aliasing errors, improve Gaussianity, and reduce bias:

(i) At first, using the MATLAB randn() function, 2^{24} or 16,777,216 Gaussian random numbers were generated.

(ii) This process was repeated 10 times to generate 10 independent raw noise series, and then an ensemble average was taken out of those 10 series to create one single noise time function with improved Gaussianity and decreased short-term bias.

(iii) Then this time series was converted to the frequency domain by Fast Fourier Transformation (FFT). To get rid of any aliasing error, we opened the real and imaginary portions of the FFT spectrum and doubled their frequency bandwidths by zero padding.

(iv) Finally, we performed an inverse FFT (IFFT) of the zero-padded spectrum to get the time function of the anti-aliased noise.

The real portion of the IFFT result is the band-limited, anti-aliased noise with improved Gaussianity and decreased bias.

The histogram and probability plot for the generated noise are shown in Figures 2.2 and 2.3, respectively, showing that the noise is Gaussian. Figure 2.4 demonstrates that the noise has band-limited, white power density spectrum and it is anti-aliased.

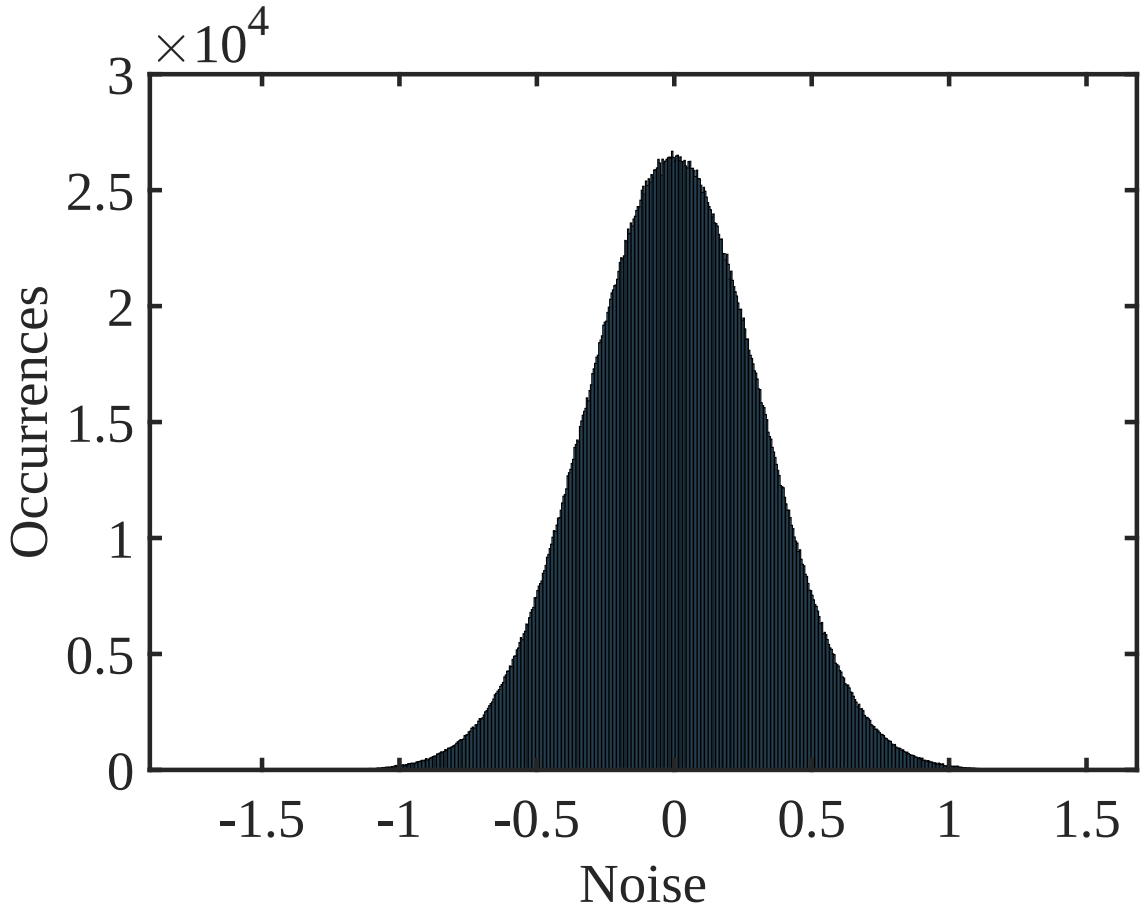


Figure 2.2: Histogram of the noise. A mean of zero and a standard deviation of 1 indicates a standard normal distribution.

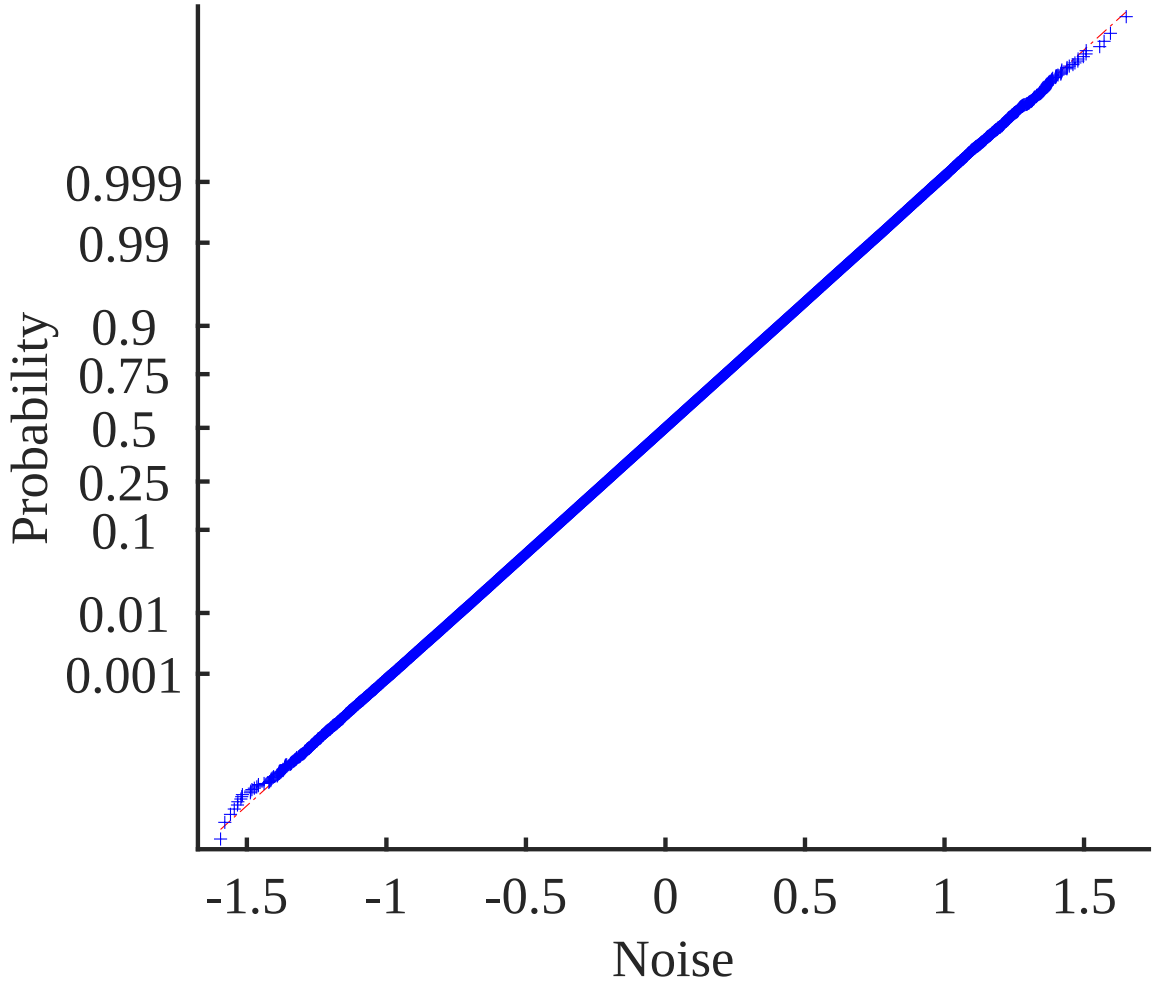


Figure 2.3: Normal-probability plot of the noise. A straight line indicates a pure Gaussian distribution.

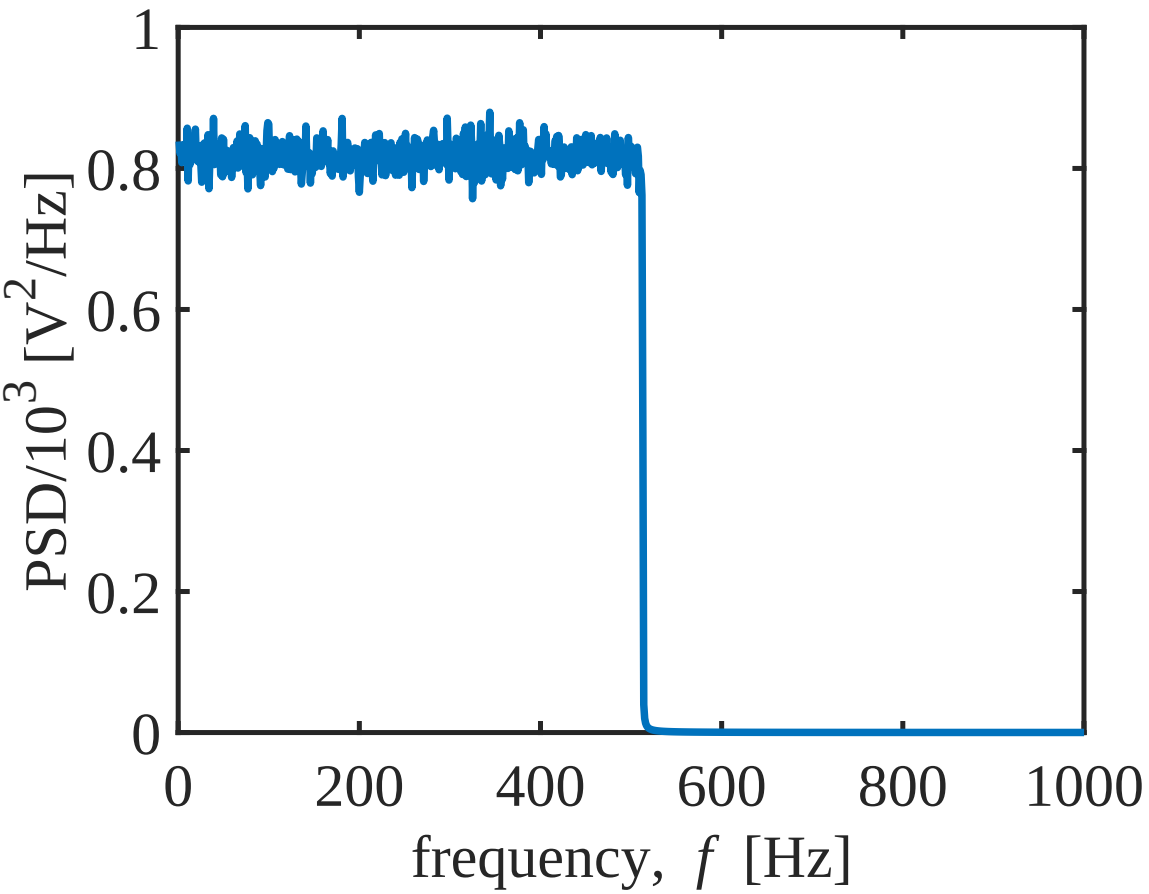


Figure 2.4: Power spectral density of the noise. The bandwidth of the noise is 500 Hz, see Equation (1.5).

The final step was to scale this normalized Gaussian nosie (see Equation (1.5)) to the required level of Johnson noise for the given resistance, temperature, and bandwidth values (R_{L}, R_{H}, T_{eff}, and Δf_{B}, respectively). We chose R_{L}=10 kΩ, R_{H}=100 kΩ, T_{eff}=10^{18} K, and Δf_{B}=500 Hz. A realization of the Johnson noise of $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$, where $U_{\mathrm{H,A}}(t)$ is the noise voltage of Alice's R_{H}, $U_{\mathrm{L,A}}(t)$ is the noise voltage of Alice's R_{L}, $U_{\mathrm{H,B}}(t)$ is the noise voltage of Bob's R_{H}, and $U_{\mathrm{L,B}}(t)$ is the noise voltage of Bob's R_{L} (see Figure 1.2), over 100 milliseconds is displayed in Figure 2.5. The histogram, probability plot, and power spectral density for those noise voltages are shown in Figures 2.6, 2.7, and 2.8, respectively.

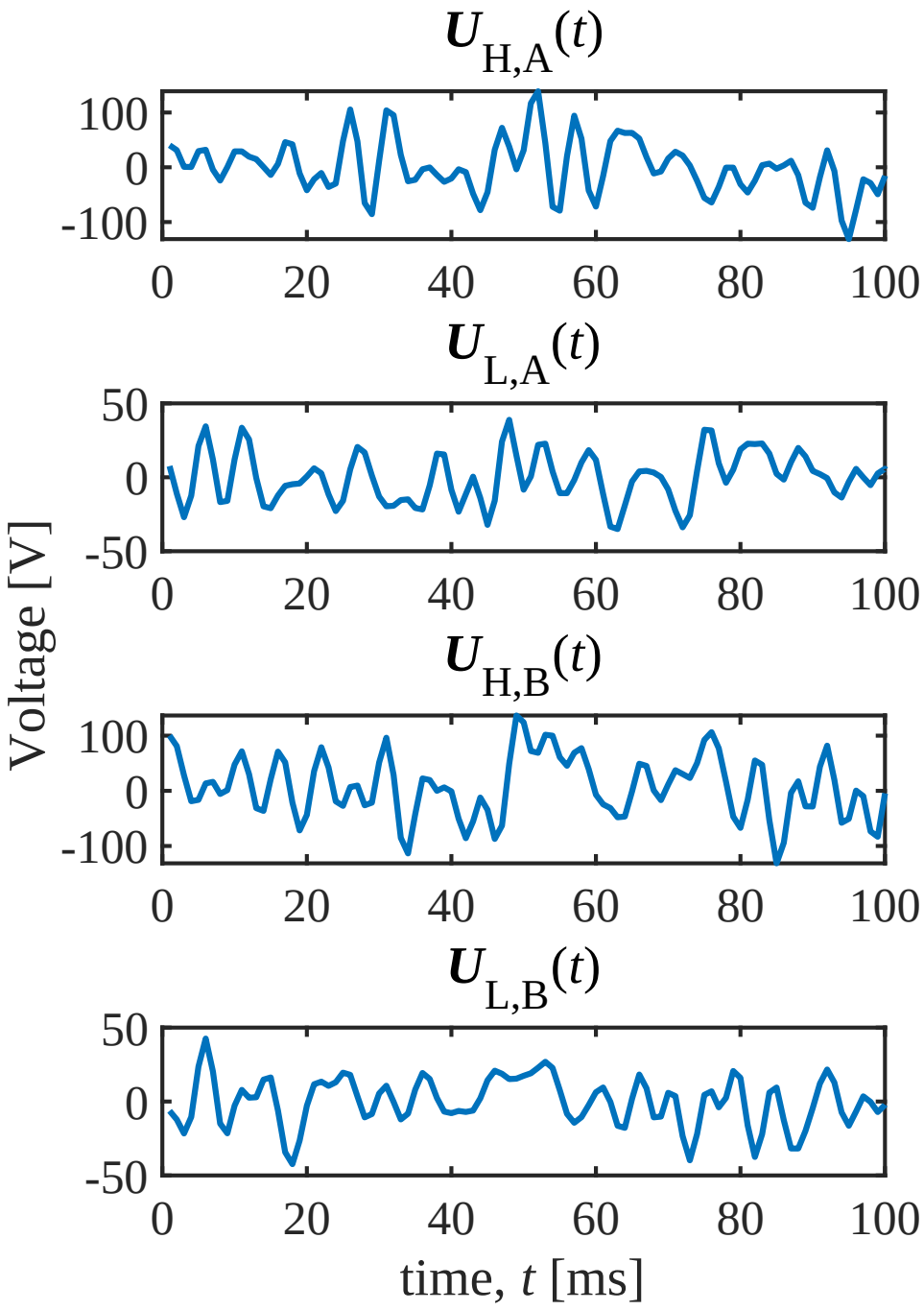


Figure 2.5: A realization of $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$ (see Figure 1.2) displayed over 100 milliseconds. $U_{\mathrm{H,A}}(t)$ is the noise voltage of Alice's R_{H}, $U_{\mathrm{L,A}}(t)$ is the noise voltage of Alice's R_{L}, $U_{\mathrm{H,B}}(t)$ is the noise voltage of Bob's R_{H}, and $U_{\mathrm{L,B}}(t)$ is the noise voltage of Bob's R_{L}. Each time step is one millisecond.

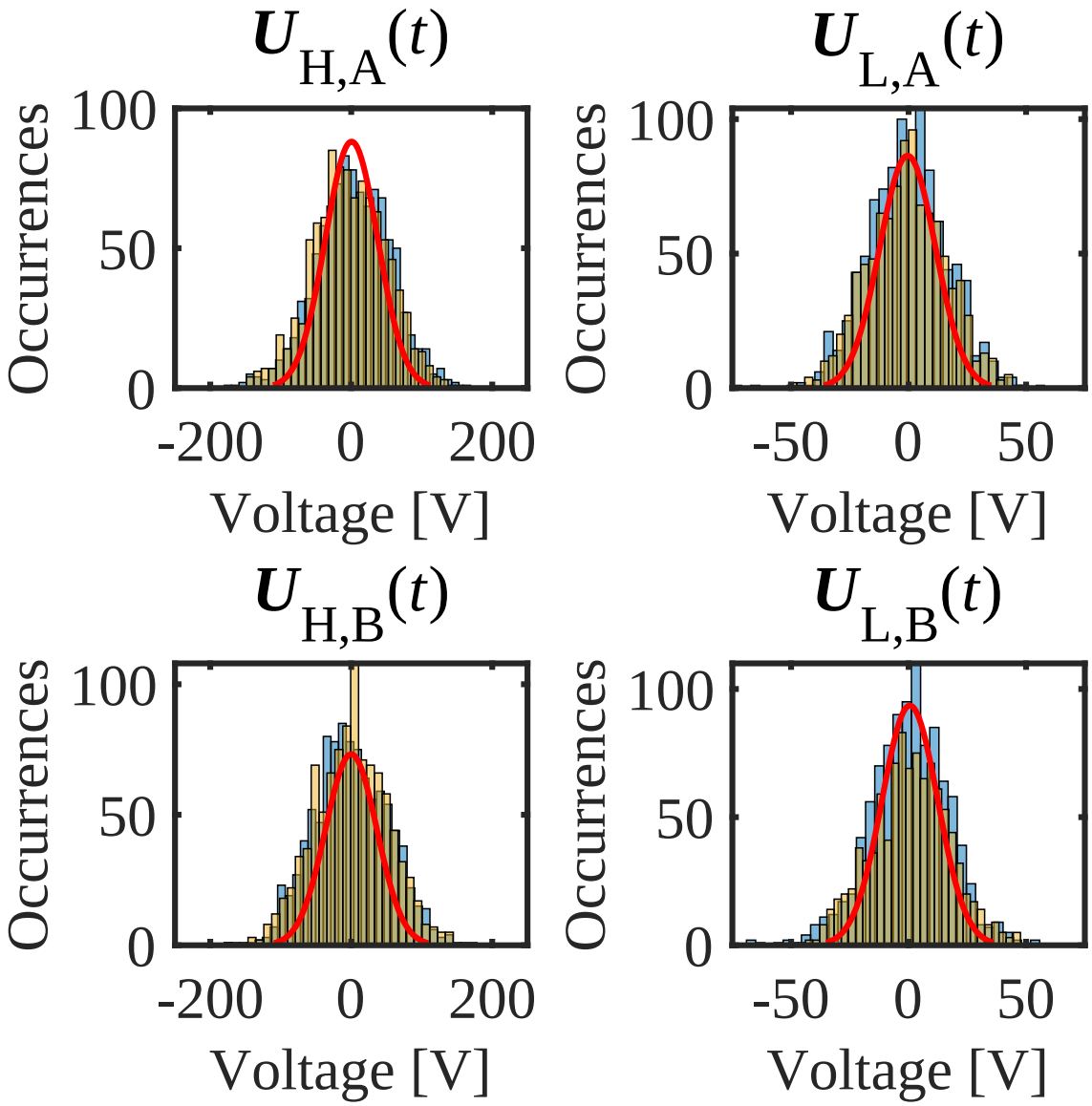


Figure 2.6: Histogram of the Johnson noise of $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$, where $U_{\mathrm{H,A}}(t)$ is the noise voltage of Alice's R_{H}, $U_{\mathrm{L,A}}(t)$ is the noise voltage of Alice's R_{L}, $U_{\mathrm{H,B}}(t)$ is the noise voltage of Bob's R_{H}, and $U_{\mathrm{L,B}}(t)$ is the noise voltage of Bob's R_{L} (see Figure 1.2). The blue histograms represent the occurrences of the noise voltages over time, and the yellow histograms represent the occurrences of the noise voltages sampled 1000 times at a specific time point. The green area represents the overlap between the blue and yellow histograms. The red line represents the best-fitting normal probability density function (PDF) for both histograms, serving to demonstrate that the noise voltages in all four cases (HH, LL, HL, and LH) are Gaussian and ergodic.

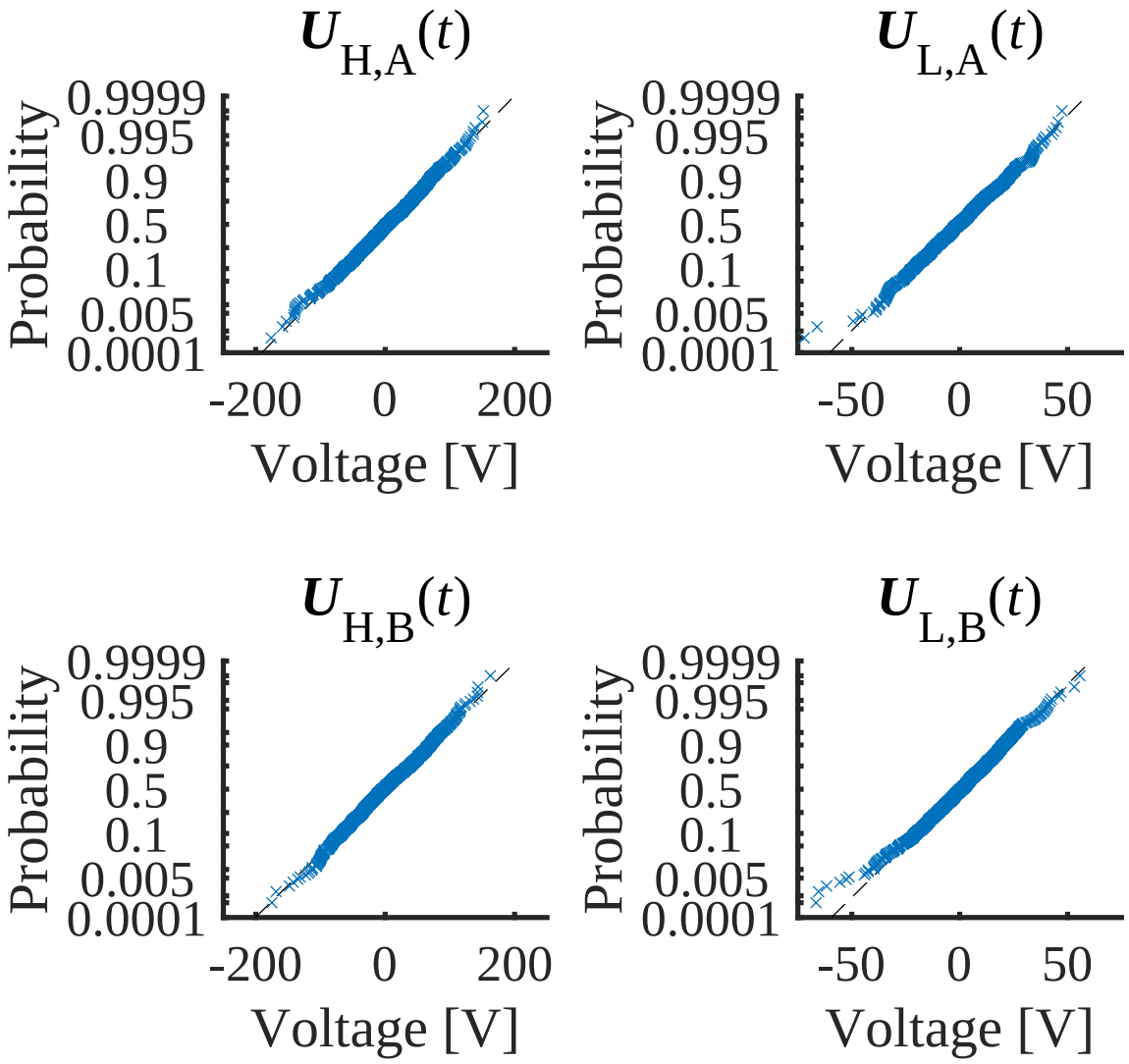


Figure 2.7: Normal-probability plot of the Johnson noise of $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$. A straight line indicates a pure Gaussian distribution.

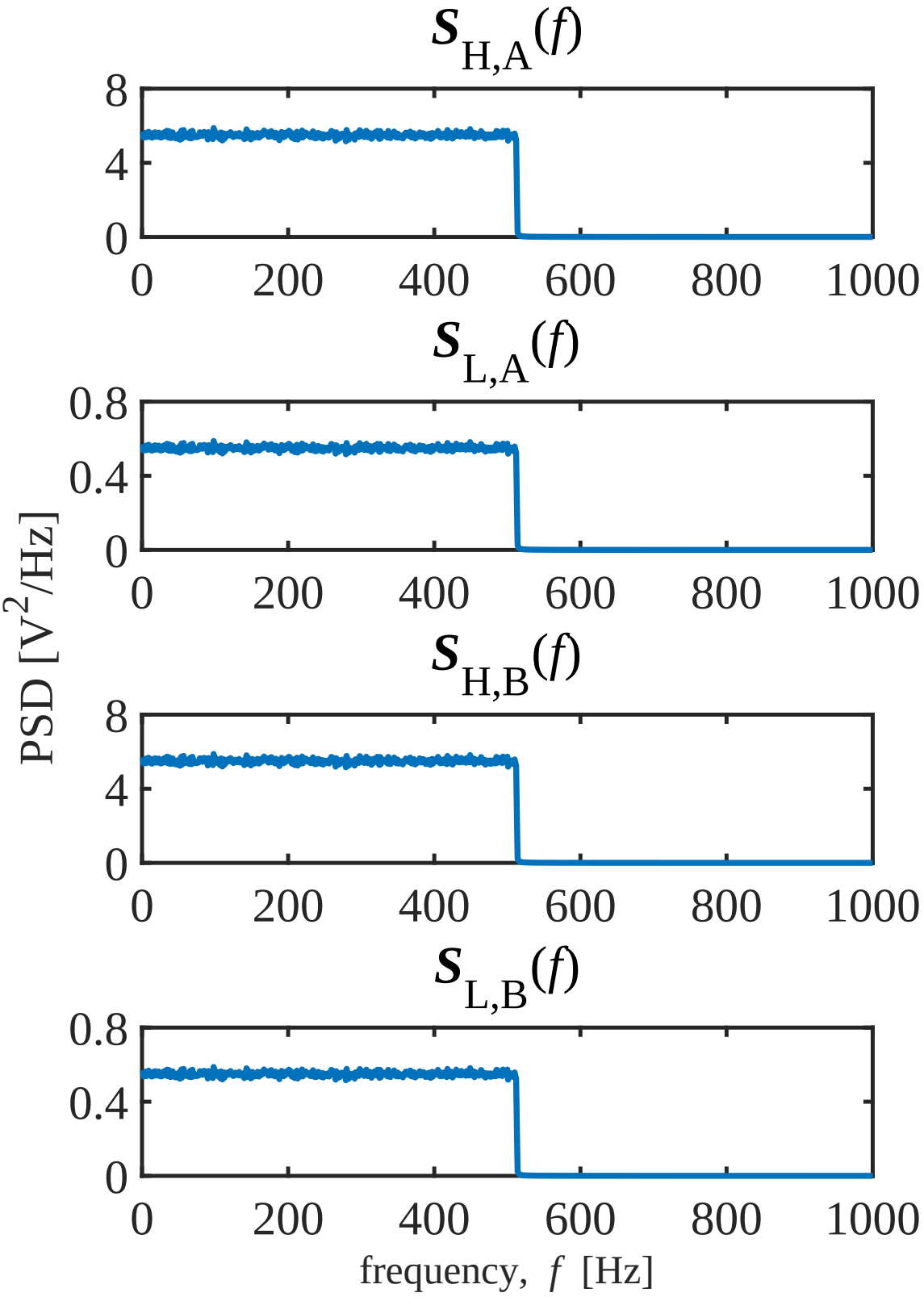


Figure 2.8: Power spectral density of the Johnson noise of $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$. The bandwidth of the noise is 500 Hz, see Equation (1.5).

From the Nyquist Sampling Theorem,

$$\tau = \frac{1}{2\Delta f_{\mathrm{B}}} \tag{2.7}$$

where τ represents the time step, a Δf_{B} of 500 Hz renders a time step of 10^{-3} seconds. Because this is ideal band-limited white noise, the Nyquist samples are statistically independent.

2.2.2.2 Setup of Eve's Noises

To generate Eve's noises that are correlated with the noises in the KLJN system, independent "thermal" noises (see Section 2.2.2.1) are added to the noises of Alice and Bob, and the resulting noises are normalized to have the same effective value as the original noises.

For example, the new correlated noise of Eve corresponding to Alice's thermal noise $U_{\mathrm{L,A}}(t)$ is

$$U_{\mathrm{EL,A}}(t) = U_{\mathrm{L,A}}(t) + MU^{*}_{\mathrm{EL,A}}(t), \tag{2.8}$$

where $U_{\mathrm{EL,A}}(t)$ is the new correlated noise, $U^{*}_{\mathrm{EL,A}}(t)$ is an independently generated "thermal" noise for resistance value R_{L}, and the M coefficient controls the cross-correlation between Eve's and Alice's noises, CCC_{LA} (see Section 2.3.1.1.2). The direct relationship between M and CCC_{LA} is demonstrated in Tables 2.2 and 2.4, respectively located in Sections 2.3.2.1.2 and 2.3.2.2.2.

Note, $U_{\mathrm{EL,A}}(t)$ and $U^{*}_{\mathrm{EL,A}}(t)$ have the same effective value. Accordingly,

$$U^{*}_{\mathrm{EL,A}}(t) = x(t)\sqrt{4kT_{\mathrm{eff}}R_{\mathrm{L}}\Delta f_{\mathrm{B}}}, \tag{2.9}$$

where $x(t)$ represents a new noise with 1 Volt effective value.

However, the effective value of $U_{\mathrm{EL,A}}(t)$ does not satisfy the Johnson formula anymore, so in order to call it a thermal noise, it must be scaled to the proper level [41]:

$$U_{\mathrm{L,A}}(t) = \frac{U_{\mathrm{EL,A}}(t)}{\sqrt{\left\langle \left[U_{\mathrm{EL,A}}(t)\right]^2 \right\rangle}}\sqrt{4kT_{\mathrm{eff}}R_{\mathrm{L}}\Delta f_{\mathrm{B}}}. \tag{2.10}$$

In this way, the same M used for the different resistance choices of Alice and Bob results in

the same cross-correlation coefficient between Eve's noises and the corresponding noises of the communicating parties. Thus, four new sets of independent additive noises have been generated using the same method as in Section 2.2.2.1.

A realization of Eve's noise voltages in comparison to Alice's and Bob's noise voltages over 100 milliseconds is displayed in Figure 2.9. $U_{\mathrm{H,A}}(t)$ is the noise voltage of Alice's R_{H}, $U_{\mathrm{L,A}}(t)$ is the noise voltage of Alice's R_{L}, $U_{\mathrm{H,B}}(t)$ is the noise voltage of Bob's R_{H}, and $U_{\mathrm{L,B}}(t)$ is the noise voltage of Bob's R_{L} (see Figure 1.2). Each time step is one millisecond.

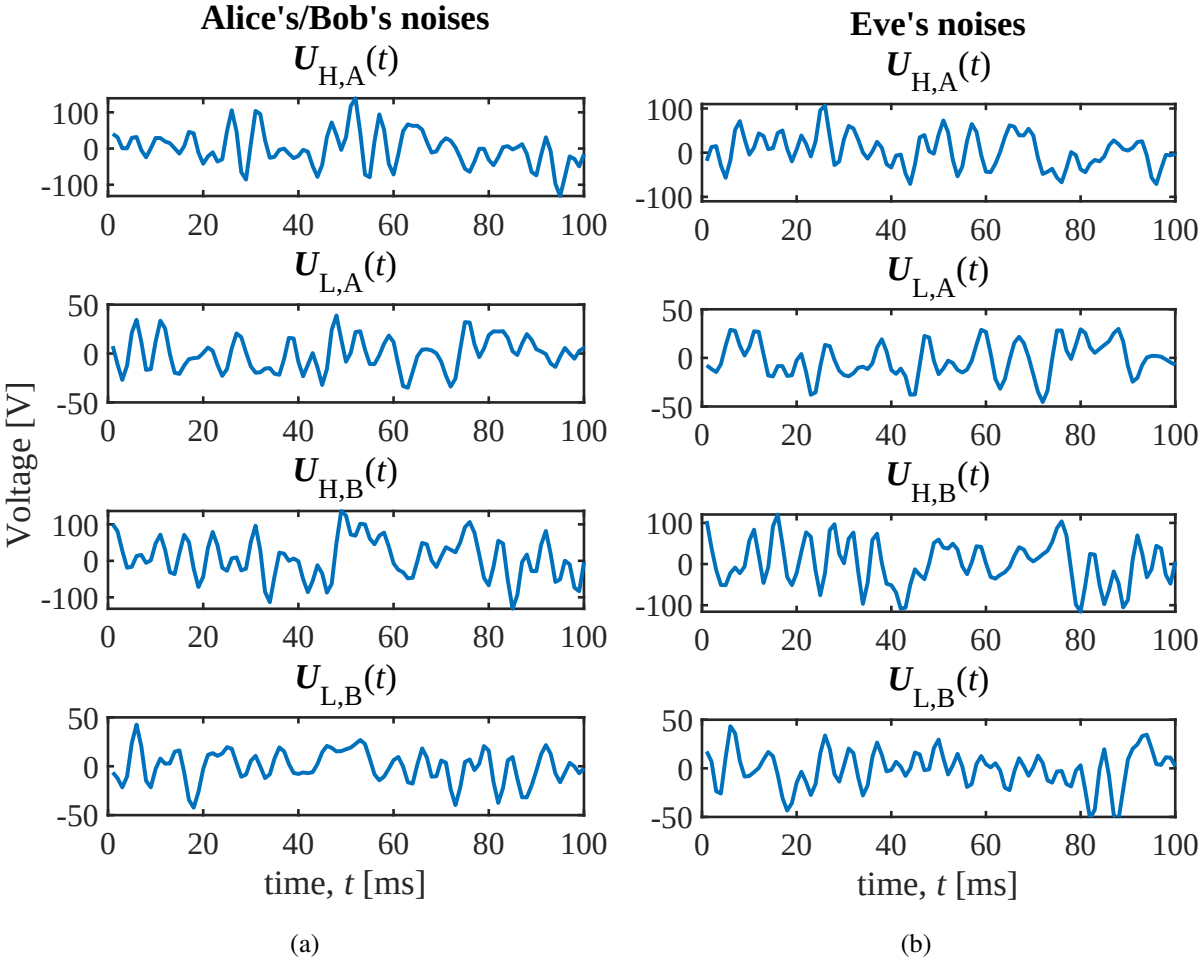


Figure 2.9: A realization of $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$ (see Figure 1.2) for Alice and Bob (a), and for Eve (b), at $M = 1$, displayed over 100 milliseconds.

For the deterministic attack demonstration (see Section 2.2.2), we keep M at 0, while in the statistical attack (see Section 2.3.2), we vary M.

2.2.2.3 Attack Demonstration when Eve Knows Both Noises

At the bilateral parameter knowledge (see Section 2.2.1.1), Figure 2.10 shows the hypothetical power flow waveforms generated by Eve (top four graphs). The single-bit plot of her measurement of the actual power flow $P_{\mathrm{w}}(t)$ is shown by the bottom graph. If the power is delivered from Alice to Bob, the single-bit value is +1, while in the opposite case the result is -1. The orange dashed lines in the upper plots indicate the power flow in the 1-bit resolution limit. At the present situation, Eve's measured single-bit data are identical to the dashed lines in the LH scenario only, thus Eve decides that the LH is the secure resistance situation.

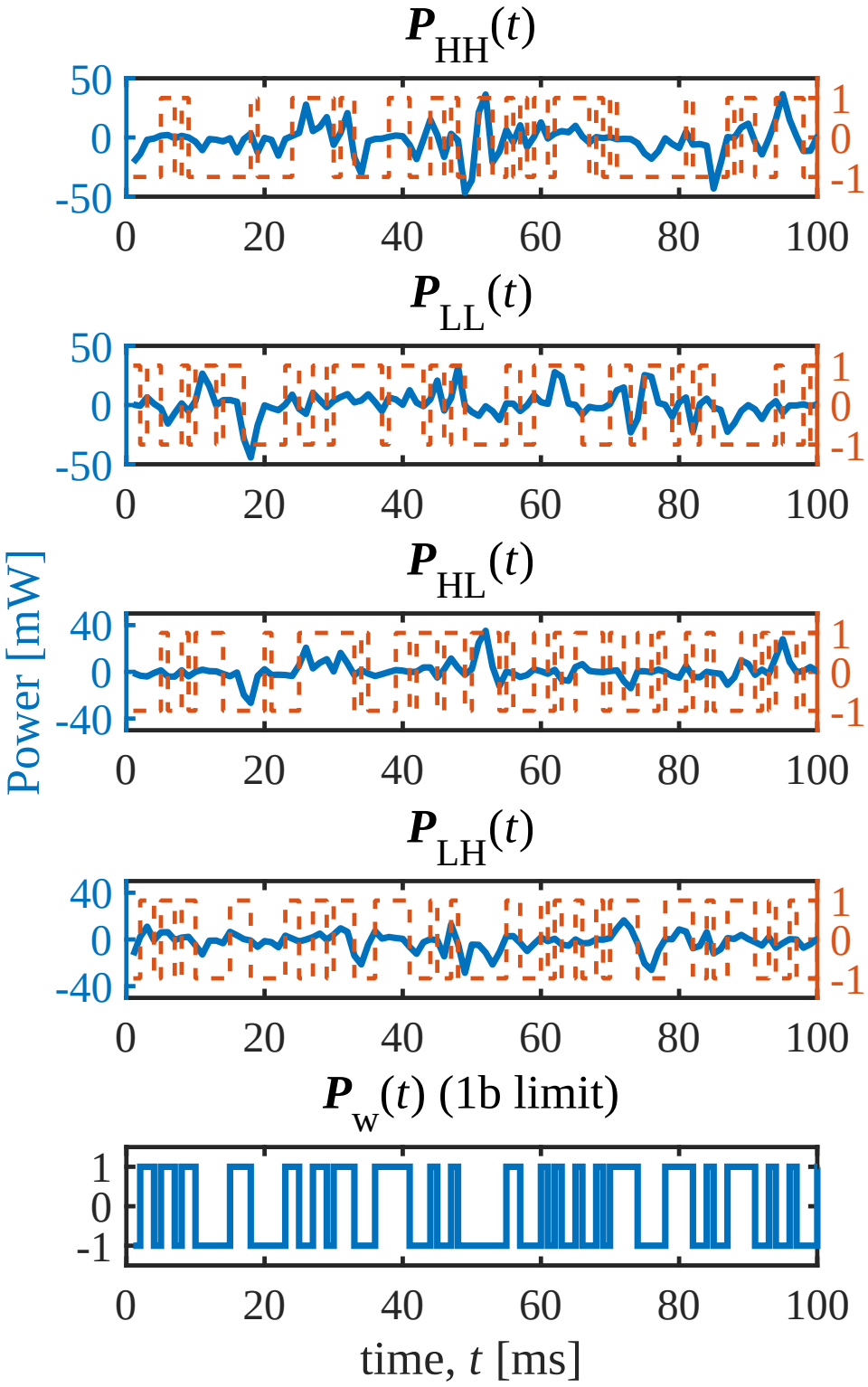


Figure 2.10: The hypothetical and their 1-bit limit waveforms for $P_{\mathrm{w}}(t)$ generated by Eve. $P_{\mathrm{HH}}(t)$ is the hypothetical power flow in the HH case, $P_{\mathrm{LL}}(t)$ is the hypothetical power flow in the LL case, $P_{\mathrm{HL}}(t)$ is the hypothetical power flow in the HL case, and $P_{\mathrm{LH}}(t)$ is the hypothetical power flow in the LH case. $P_{\mathrm{w}}(t)$ is the single-bit measurement of the actual power flow.

However, similarly to the case of string verification with noise-based logic [106], two independent random bit sequences, such as two different binary sequences in Figure 2.10, may run identically for n subsequent steps with probability

$$p = \frac{1}{2^n} \tag{2.11}$$

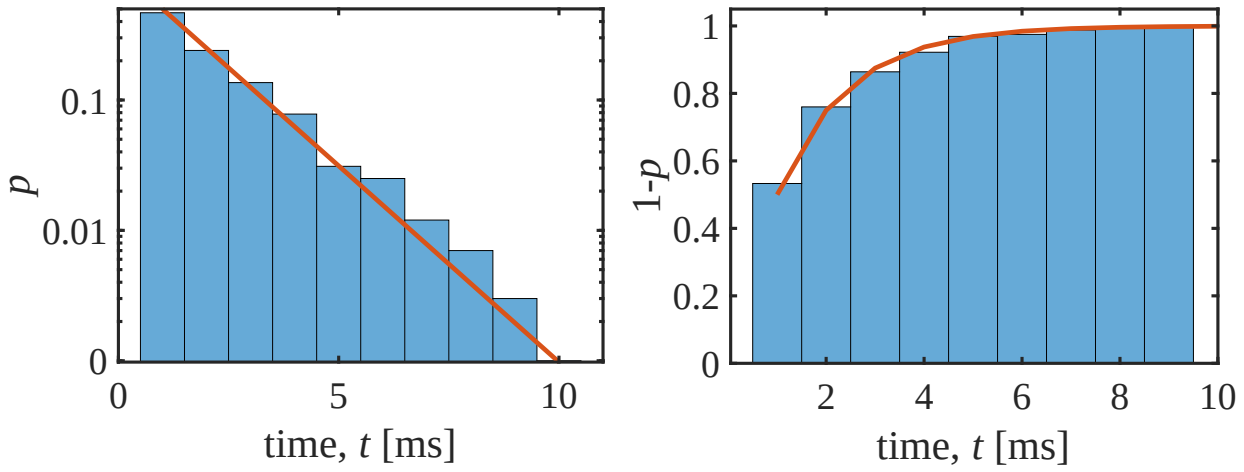
where the independence of the subsequent samples within a given binary sequence is also essential, and $n = t/\tau$.

While such an identical match between two of the 4 noises is taking place, Eve cannot decide which one of the hypothetical sequences is valid thus the actual resistor situation (see Figure 1.3) remains secure. However, the exponential decay of the probability of the duration of this phenomenon in Equation (2.11) yields an efficient cracking of the secure key bit value within a short time. In accordance with (2.11), the probability of two independent ones of our binary sequences (Figure 2.10) running identically is

$$p(t) \approx \frac{1}{2^{t/\tau}} = \frac{1}{2^{1000t}} \tag{2.12}$$

The approximation sign is due to the quantized nature of $p(t)$ because it is staying constant during the bit exchange periods.

This simulation was run 1000 times. Figure 2.11a shows the probability that the exchange of the current key bit is still secure. Figure 2.11b shows the probability that Eve has already cracked the bit. The red lines follow the scaling given by Equation (2.12).



(a) (b)

Figure 2.11: Probabilities during the attack with single-bit resolution of Eve's measurements. (a) Probability that the exchange of the current key bit is still secure; (b) and probability that Eve has already cracked it. The histograms represent the simulation results, and the red lines represent the scaling given by Equation (2.12).

2.2.2.4 Attack Demonstration when Eve Knows Only One of the Sources

At the unilateral parameter knowledge (see Section 2.2.1.2), Eve knows the root of Alice's RNG, while the root of Bob's RNG is unknown to her. Thus, we suppose she knows $U_{\mathrm{A}}(t)$ (like at the bilateral case), but not $U_{\mathrm{B}}(t)$. A realization of the wire voltage and current, $U_{\mathrm{w}}(t)$ and $I_{\mathrm{w}}(t)$, under the LH condition over 100 milliseconds, is displayed in Figure 2.12. Figure 2.13 shows the hypothetical noise voltages generated by Eve's simulations across R_{L} and R_{H} via Ohm's Law.

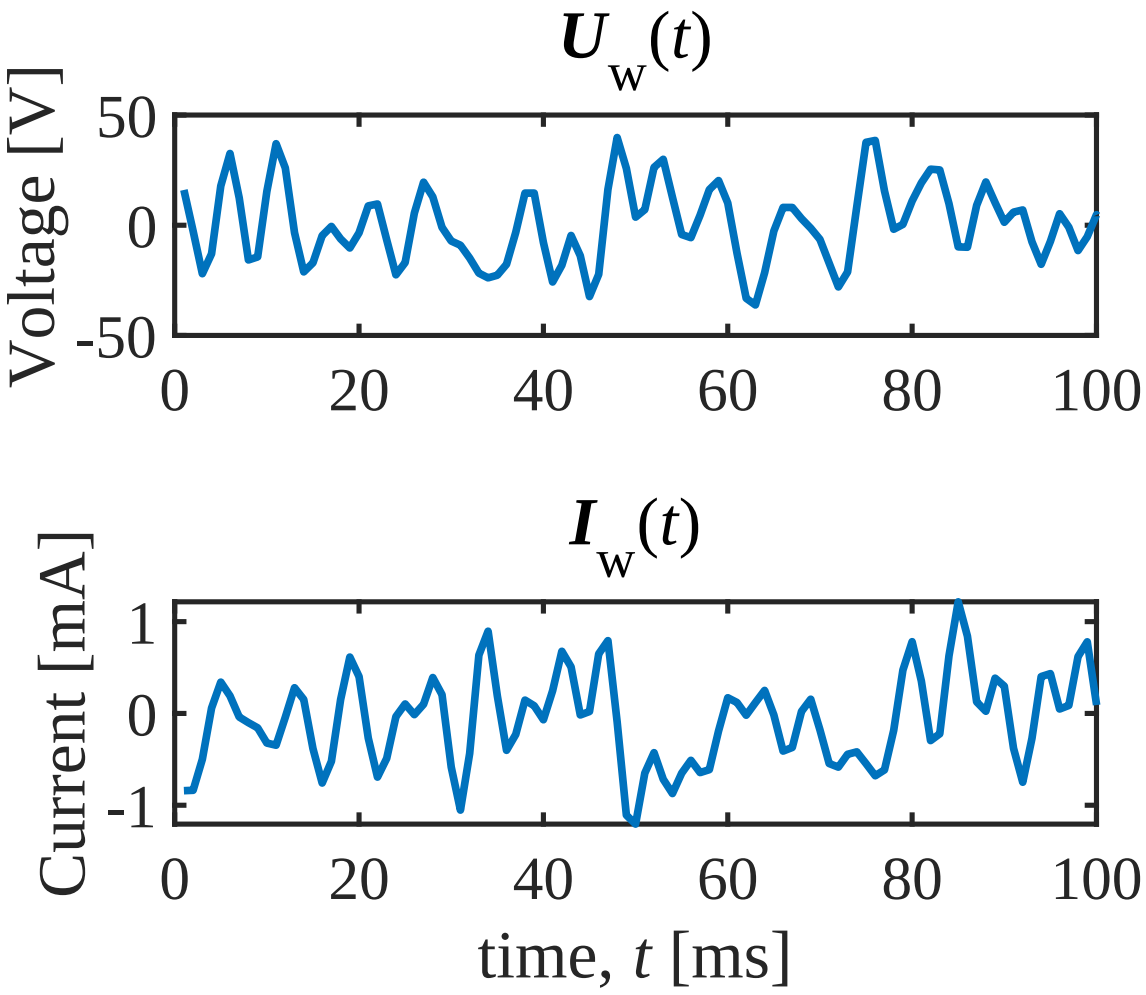


Figure 2.12: A realization of $U_{\mathrm{w}}(t)$ and $I_{\mathrm{w}}(t)$ (see Figure 1.2) displayed over 100 milliseconds. Eve measures and records these data.

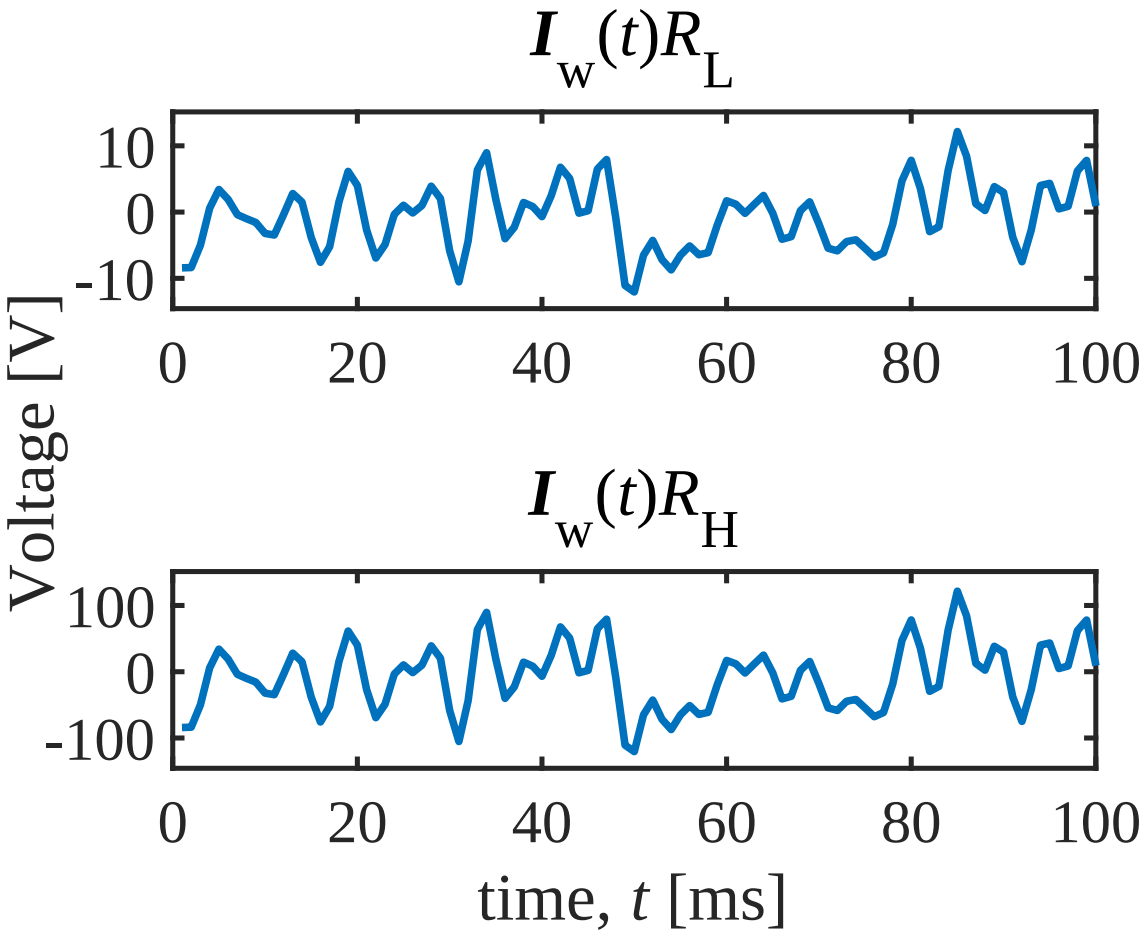


Figure 2.13: Hypothetical noise voltage drops across R_{L} and R_{H} by Eve's current measurements and Ohm's law. These results are used in Equation (2.2) to calculate the hypothetical waveforms for $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$.

Figure 2.14 shows Eve's hypothetical waveforms for $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$, which we denote as $U^*_{\mathrm{R_L}}(t)$ and $U^*_{\mathrm{R_H}}(t)$ (see Equation (2.2)), in comparison to her known $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$. In this case, the waveform for $U^*_{\mathrm{R_L}}(t)$ is identical to that of $U_{\mathrm{L,A}}(t)$, thus Eve decides that Alice has chosen R_{L}. A correlation plot is also shown in Figure 2.15, between (a) $U^*_{\mathrm{R_L}}(t)$ vs. $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$, and (b) $U^*_{\mathrm{R_H}}(t)$ vs. $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$. A one-to-one correlation between $U^*_{\mathrm{R_L}}(t)$ and $U_{\mathrm{L,A}}(t)$ indicates that Alice has chosen R_{L}.

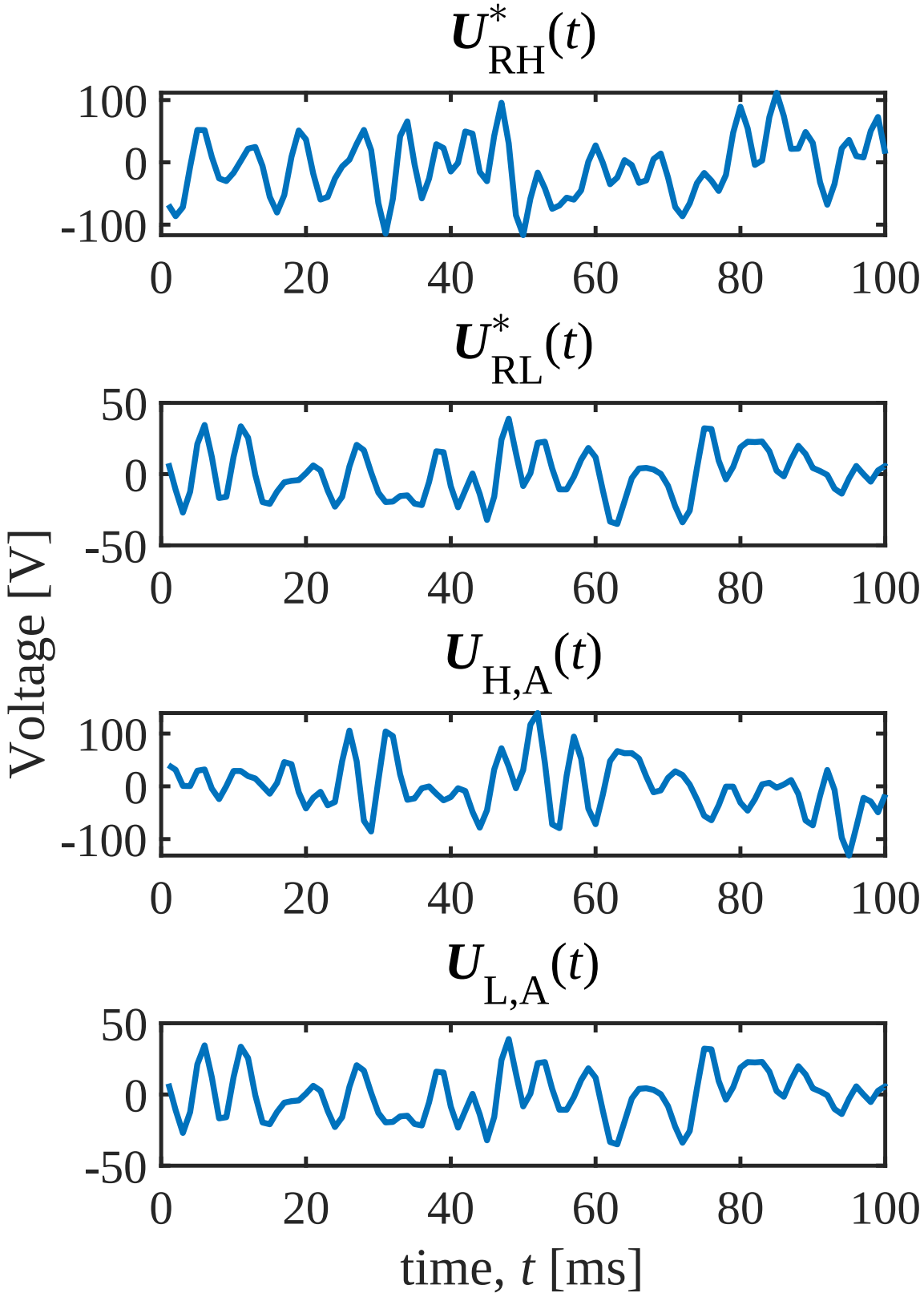
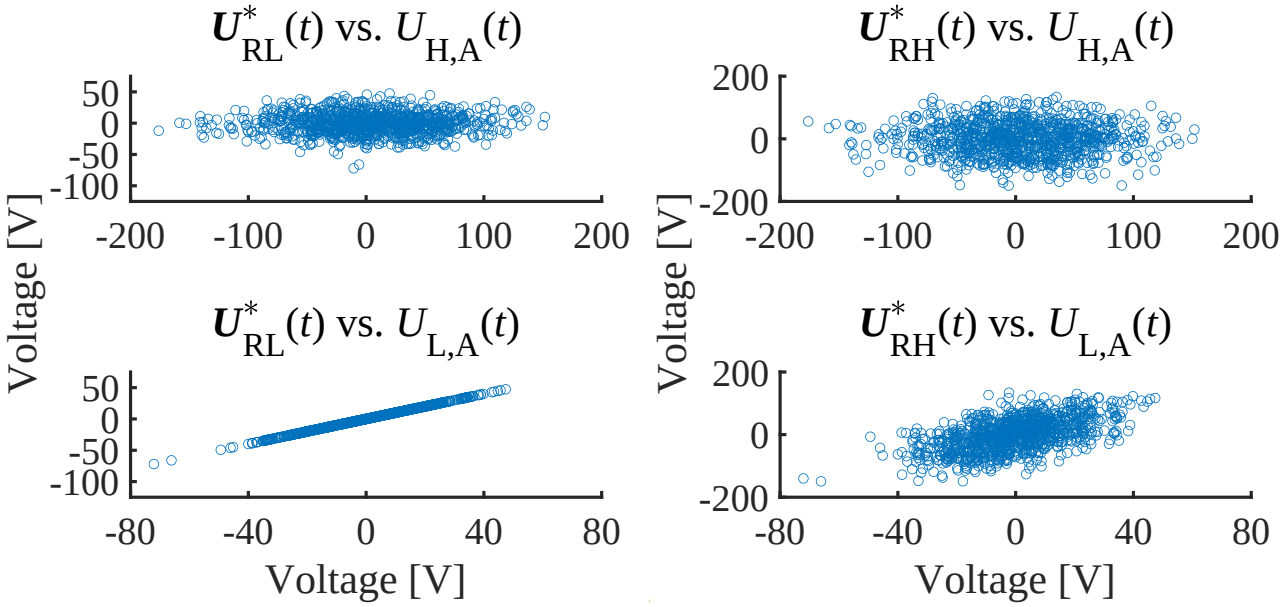


Figure 2.14: Eve's hypothetical waveforms for $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$, which we denote as $U^*_{\mathrm{R_L}}(t)$ and $U^*_{\mathrm{R_H}}(t)$ (see Equation (2.2)), in comparison to her known $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$.



(a) (b)

Figure 2.15: Correlation between (a) $U^*_{\mathrm{R_L}}(t)$ vs. $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$, and (b) $U^*_{\mathrm{R_H}}(t)$ vs. $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$. A one-to-one correlation between Eve's known $U_{\mathrm{A}}(t)$ and the hypothetical waveform for $U_{\mathrm{L,A}}(t)$ indicates that Alice has chosen R_{L}.

Finally, Eve evaluates the measured mean-square voltage on the wire over the bit exchange period, shown in Figure 2.16. From that value, by using Equation (1.5), she evaluates the parallel resultant R_{P} of the resistances of Alice and Bob. From R_{P} and R_{A}, she can calculate R_{B}. In this particular case, Bob has chosen R_{H}, thus Eve has cracked the LH situation and the related secure bit value.

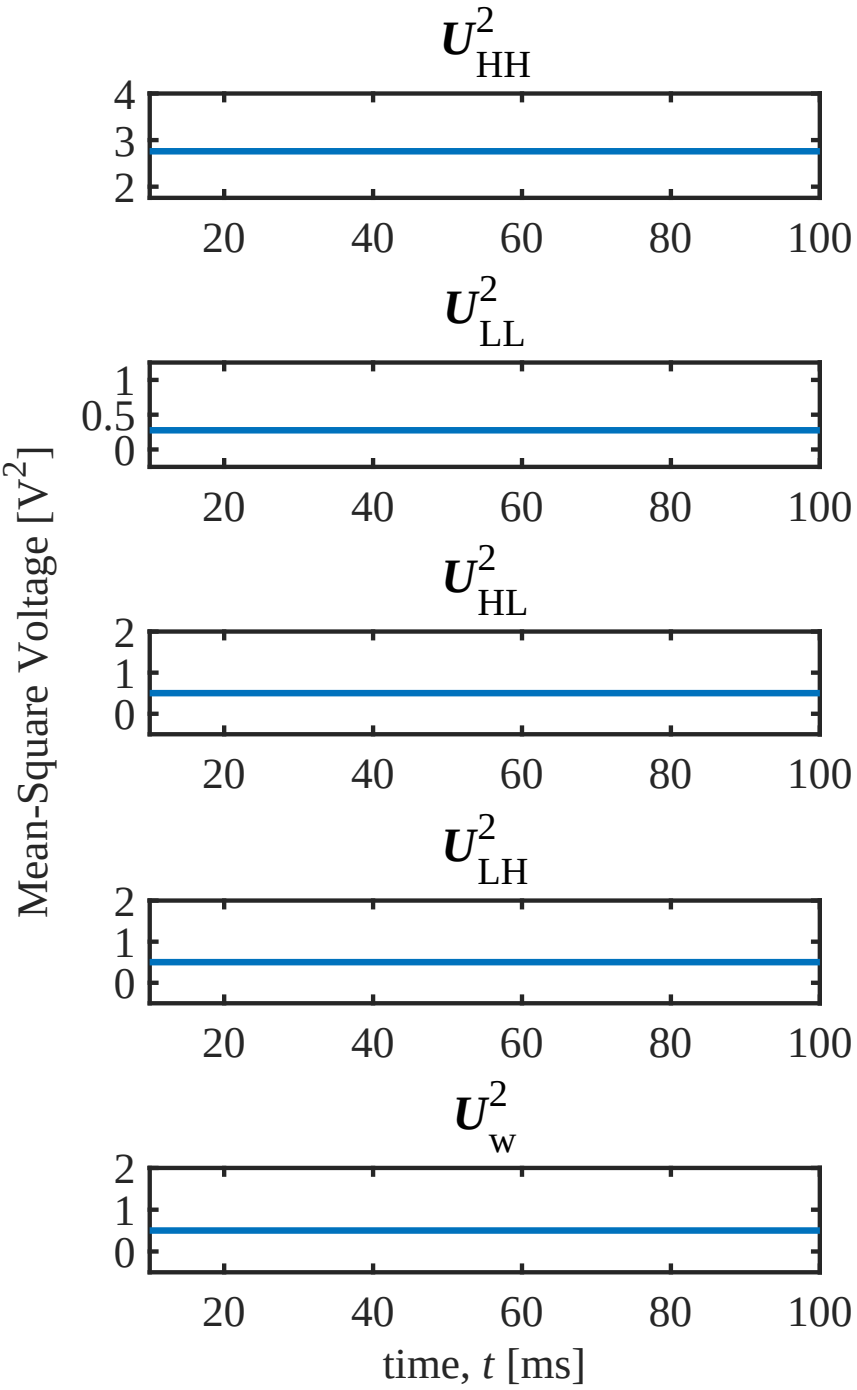


Figure 2.16: The hypothetical and measured mean-square voltage generated by Eve. $U^2_{\mathrm{HH,eff}}$ is the hypothetical mean-square voltage in the HH case, $U^2_{\mathrm{LL,eff}}$ is the hypothetical mean-square voltage in the LL case, $U^2_{\mathrm{HL,eff}}$ is the hypothetical mean-square voltage in the HL case, and $U^2_{\mathrm{LH,eff}}$ is the hypothetical mean-square voltage in the LH case. $U^2_{\mathrm{w,eff}}$ is the measurement of the actual mean-square voltage.

2.2.3 Transition

This concludes the deterministic RNG attacks presented in this dissertation. Now, we move onto the statistical RNG attacks.

2.3 Statistical RNG Attack against the KLJN Scheme

2.3.1 Statistical Attack Protocol

Two situations are introduced where Eve can use compromised RNGs to crack the KLJN scheme: one where Eve has partial knowledge of both Alice's and Bob's generators (bilateral knowledge), and another where Eve has partial knowledge of only Alice's generator (unilateral knowledge).

2.3.1.1 Bilateral Knowledge

Eve has statistical knowledge of the amplitudes of the noise voltage generators $U_{\mathrm{H,A}}(t)$, $U_{\mathrm{L,A}}(t)$, $U_{\mathrm{H,B}}(t)$, and $U_{\mathrm{L,B}}(t)$ for each of Alice's and Bob's resistors, see Figure 1.2. These noises are correlated with Alice's and Bob's corresponding noises. Eve then uses Equations (1.3), (1.4), and (2.1) for the cross-correlation attacks shown below.

2.3.1.1.1 *Cross-correlation attack utilizing Alice's/Bob's and Eve's channel voltages, currents and power*

For the four possible resistor combinations, HL, LH, LL and HH, Eve sets up a simulator utilizing her noises (that are correlated with Alice's Bob's corresponding noises), and she records the resulting wire voltages $U_{\mathrm{HH}}(t)$, $U_{\mathrm{LL}}(t)$, $U_{\mathrm{HL}}(t)$, and $U_{\mathrm{LH}}(t)$. Then she evaluates the cross-correlation between the measured wire voltage $U_{\mathrm{w}}(t)$ of Alice and Bob, and the simulated ones. For example, in the HH simulated resistor situation, this is given by

$$CCC_{\mathrm{HH,U}} = \frac{\langle U_{\mathrm{w}}(t)U_{\mathrm{HH}}(t)\rangle}{U_{\mathrm{w}}U_{\mathrm{HH}}}, \tag{2.13}$$

where $CCC_{\mathrm{HH,U}}$ is the cross-correlation coefficient between her simulated wire voltage $U_{\mathrm{HH}}(t)$ in the HH case and the *measured* channel voltage $U_{\mathrm{w}}(t)$.

Finally, Eve guesses that the actual resistor situation is the one with the highest cross-correlation between the voltage on the wire and in Eve's probing system.

Note, this protocol of cross-correlating the simulated and real wire data can also be repeated for the channel current $I_{\mathrm{w}}(t)$ and channel power $P_{\mathrm{w}}(t)$.

For the channel current protocol, she measures $I_{\mathrm{w}}(t)$ and evaluates the cross-correlation between the measured $I_{\mathrm{w}}(t)$ and her four simulated wire currents $I_{\mathrm{HH}}(t)$, $I_{\mathrm{LL}}(t)$, $I_{\mathrm{HL}}(t)$, and $I_{\mathrm{LH}}(t)$. In the HH example, this is given by

$$CCC_{\mathrm{HH,I}} = \frac{\langle I_{\mathrm{w}}(t) I_{\mathrm{HH}}(t) \rangle}{I_{\mathrm{w}} I_{\mathrm{HH}}}, \tag{2.14}$$

where $CCC_{\mathrm{HH,I}}$ is the cross-correlation coefficient between her simulated wire voltage $I_{\mathrm{HH}}(t)$ in the HH case and the *measured* channel current $I_{\mathrm{w}}(t)$.

Finally, similarly to the above voltage correlation attack, Eve guesses that the bit situation is the one with the highest cross-correlation between the current in the wire and in Eve's probing system.

For the channel power protocol, Eve has the measured $U_{\mathrm{w}}(t)$ and $I_{\mathrm{w}}(t)$ at her disposal. She uses her noises to simulate the four possible waveforms, $P_{\mathrm{HH}}(t)$, $P_{\mathrm{LL}}(t)$, $P_{\mathrm{HL}}(t)$, and $P_{\mathrm{LH}}(t)$, for the instantaneous power flow from Alice to Bob, and cross-correlates the with the actual measured $P_{\mathrm{w}}(t)$. In the HH example:

$$CCC_{\mathrm{HH,P}} = \frac{\langle P_{\mathrm{w}}(t) P_{\mathrm{HH}}(t) \rangle}{P_{\mathrm{w}} P_{\mathrm{HH}}}, \tag{2.15}$$

where $P_{\mathrm{HH}}(t)$ is the simulated channel power in the HH case, and the measured power is given by Equation (2.1).

Finally, Eve guesses that the bit situation is the one with the highest cross-correlation between the power flows in the wire and in Eve's probing system.

2.3.1.1.2 *Cross-correlation attack directly utilizing Alice's/Bob's and Eve's voltage sources*

There is an alternative way for correlation attacks. Eve measures the wire voltage $U_{\mathrm{w}}(t)$ and wire

current $I_{\mathrm{w}}(t)$ [41, 42]. Then, from $I_{\mathrm{w}}(t)$, she uses Ohm's law to calculate the hypothetical voltage drops on Alice's/Bob's possible choices of resistances R_{H} and R_{L}. From that voltage drop, by using Kirchhoff's loop law, Eve calculates Alice's/Bob's hypothetical noise voltage amplitudes. With these data, she tests four hypotheses:

Hypothesis (i): Alice has chosen R_{L}

Hypothesis (ii): Alice has chosen R_{H}

Hypothesis (iii): Bob has chosen R_{L}

Hypothesis (iv): Bob has chosen R_{H}

With Hypothesis (i), to utilize Kirchhoff's loop law, using the same current direction (Alice $\rightarrow$ Bob) as with the power calculation in Equation (2.1), Eve takes the sum

$$U^{*}_{\mathrm{L,A}}(t) = U_{\mathrm{w}}(t) + I_{\mathrm{w}}(t)R_{\mathrm{L}} \tag{2.16}$$

to calculate the hypothetical value $U^{*}_{\mathrm{L,A}}(t)$ of Alice's noise $U_{\mathrm{L,A}}(t)$.

To test Hypothesis (i) she finds the cross-correlation between $U_{\mathrm{L,A}}(t)$ (see Figure 1.2) and the $U^{*}_{\mathrm{L,A}}(t)$ determined by (Equation (2.16)), given by

$$CCC_{\mathrm{LA}} = \frac{\langle U^{*}_{\mathrm{L,A}}(t)U_{\mathrm{L,A}}(t)\rangle}{U^{*}_{\mathrm{L,A}}U_{\mathrm{L,A}}}. \tag{2.17}$$

Then, with the same equation, she finds the cross-correlation coefficient between $U^{*}_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$. If the former result yields the higher cross-correlation, then Eve has determined that Hypothesis (i) is correct; otherwise, Hypothesis (ii) is valid.

Similarly, at Bob's side, with Hypothesis (iii), Eve takes the difference

$$U^{*}_{\mathrm{L,B}}(t) = U_{\mathrm{w}}(t) - I_{\mathrm{w}}(t)R_{\mathrm{L}} \tag{2.18}$$

to calculate the hypothetical value $U^{*}_{\mathrm{L,B}}(t)$ of Bob's noise $U_{\mathrm{L,B}}(t)$.

To test Hypothesis (iii) she finds the cross-correlation between $U_{\mathrm{L,B}}(t)$ (see Figure 1.2) and the $U^*_{\mathrm{L,B}}(t)$ determined by Equation (2.18), given by

$$CCC_{\mathrm{LB}} = \frac{\langle U^*_{\mathrm{L,B}}(t) U_{\mathrm{L,B}}(t) \rangle}{U^*_{\mathrm{L,B}} U_{\mathrm{L,B}}}. \tag{2.19}$$

Then, with the same equation, she finds the cross-correlation coefficient between $U^*_{\mathrm{L,B}}(t)$ and $U_{\mathrm{H,B}}(t)$. If the former result yields the higher cross-correlation, then Eve has determined that Hypothesis (iii) is correct; otherwise, Hypothesis (iv) is valid.

2.3.1.2 Unilateral Knowledge

Eve has partial knowledge of only Alice's noises, that is, the noise generator outputs of Alice's resistors, $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$. Bob's generator voltages are completely unknown to her. The attack methods described in Section 2.3.1.1 work even here with a minor modification as described below.

2.3.1.2.1 *Cross-correlations between Alice's/Bob's and Eve's channel voltages, currents and power*

Eve generates two independent "dummy" thermal noises to substitute for Bob's unknown noise voltages $U_{\mathrm{H,B}}(t)$ and $U_{\mathrm{L,B}}(t)$. Then, she uses the same protocol as the bilateral case (see Section 2.3.1.1): she measures $U_{\mathrm{w}}(t)$ and $I_{\mathrm{w}}(t)$, determines $P_{\mathrm{w}}(t)$ from Equation (2.1), and uses Equations (2.13)-(2.15) to find the cross-correlation between her four simulated $U_{\mathrm{w}}(t)$, $I_{\mathrm{w}}(t)$, and $P_{\mathrm{w}}(t)$, and the measured $U_{\mathrm{w}}(t)$, $I_{\mathrm{w}}(t)$, and $P_{\mathrm{w}}(t)$.

2.3.1.2.2 *Cross-correlations between Alice's and Eve's voltage sources*

With $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$ partially known, Eve uses a protocol corresponding to the bilateral case (see Section 2.3.1.1): she measures $U_{\mathrm{w}}(t)$ and $I_{\mathrm{w}}(t)$ [41, 42]. Then, from $I_{\mathrm{w}}(t)$, she calculates the hypothetical voltage drops on Alice's possible choice of resistances R_{H} and R_{L}. With these data, she tests two hypotheses:

Hypothesis (i): Alice has chosen R_{L}

Hypothesis (ii): Alice has chosen R_{H}.

Note that, in the bilateral case, she had knowledge of Bob's noises, thus she could form four hypotheses. In the unilateral case, she has knowledge of only Alice's generator voltages, therefore she can form only two hypotheses.

With Hypothesis (i), Eve uses Equation (2.16) to find $U^*_{\mathrm{L,A}}(t)$. Then, she uses Equation (2.17) to find the cross-correlation between $U_{\mathrm{L,A}}(t)$ and $U^*_{\mathrm{L,A}}(t)$, and then the cross-correlation between $U^*_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$. If the former result yields the higher cross-correlation, then Eve has determined that Hypothesis (i) is correct; otherwise, Hypothesis (ii) is valid.

The extra step that is needed to add to the protocol described in Section 2.3.1.1.2 is as follows: with Alice's chosen resistance known, Eve does the same exact KLJN protocol as Alice see Section 1.2): she evaluates the measured mean-square voltage on the wire over the whole bit exchange period. From that value, by using Equation (1.5), she evaluates the bit situation (see Figure 1.3). Thus she has cracked the KLJN scheme [41].

2.3.2 Demonstration

The noise generation is the same as in Sections 2.2.2.1 and 2.2.2.2.

2.3.2.1 Attack demonstration when Eve knows both noises (bilateral attacks)

2.3.2.1.1 *Bilateral attack demonstration utilizing cross-correlations between Alice's/Bob's and Eve's wire voltages, currents and powers*

Computer simulations were executed with MATLAB, and each simulation was averaged over 1000 runs, see Tables 2.1-2.4. During the attacks, the sample size (number of time steps) is 1000, and the KLJN system is kept in the LH state. A realization of the wire voltage, current, and power, $U_{\mathrm{w}}(t)$, $I_{\mathrm{w}}(t)$, and $P_{\mathrm{w}}(t)$, under the LH condition over 100 milliseconds is displayed in Figure 2.17.

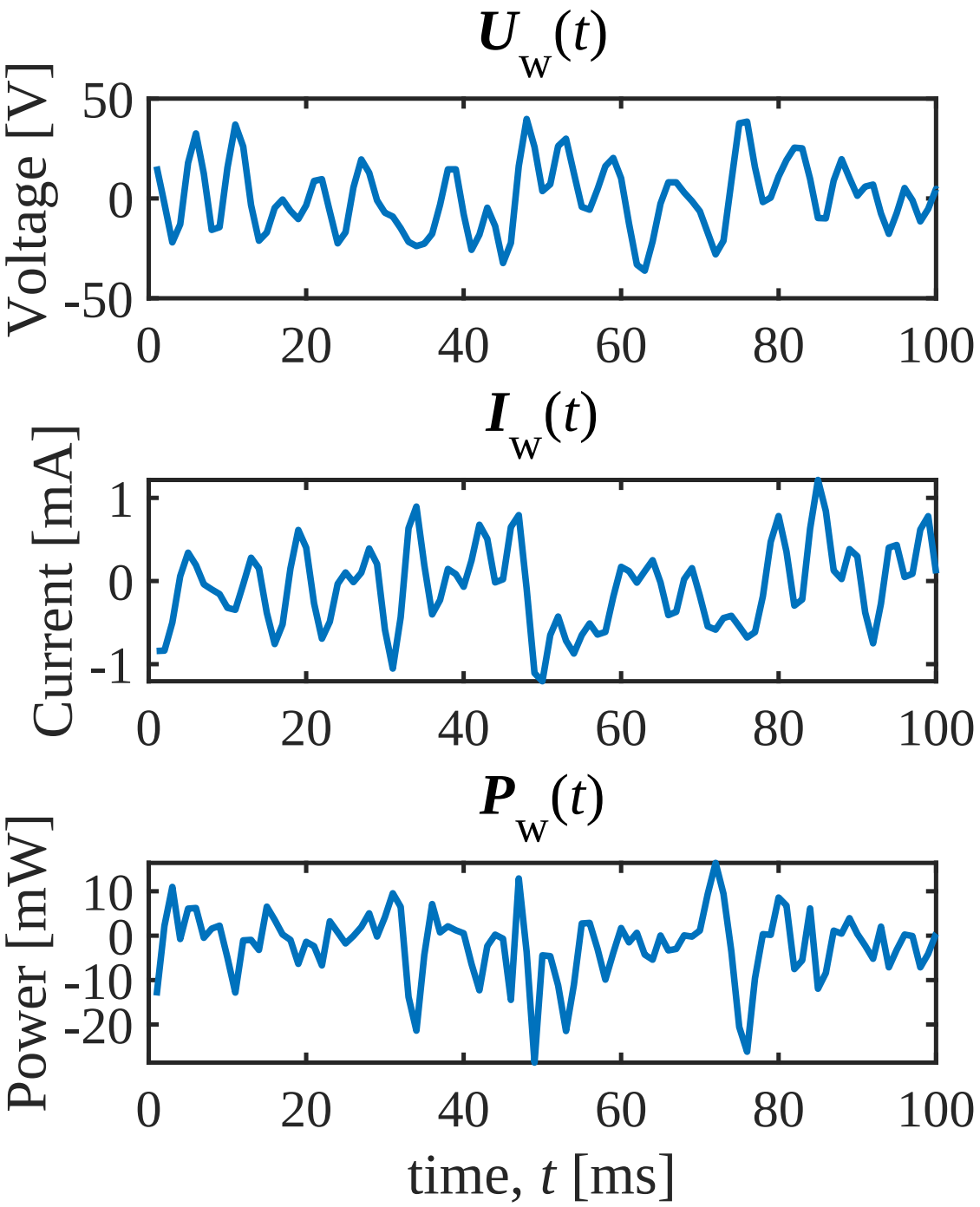


Figure 2.17: A realization of $U_{\mathrm{w}}(t)$, $I_{\mathrm{w}}(t)$, (see Figure 1.2) and $P_{\mathrm{w}}(t)$ (see Equation (2.1)) for the LH situation displayed over 100 milliseconds [41]. Eve measures and records these data.

A visual example of the correlations between Eve's *measured* channel voltage, $U_{\mathrm{w}}(t)$, and

her four *simulated* channel voltages, $U_{\mathrm{HH}}(t)$, $U_{\mathrm{LL}}(t)$, $U_{\mathrm{HL}}(t)$, and $U_{\mathrm{LH}}(t)$, at $M = 1$ (see Section 2.2.2.2), is shown in Figure 2.18. The highest correlation is the LH case, thus Eve guesses that the secure resistance situation is LH.

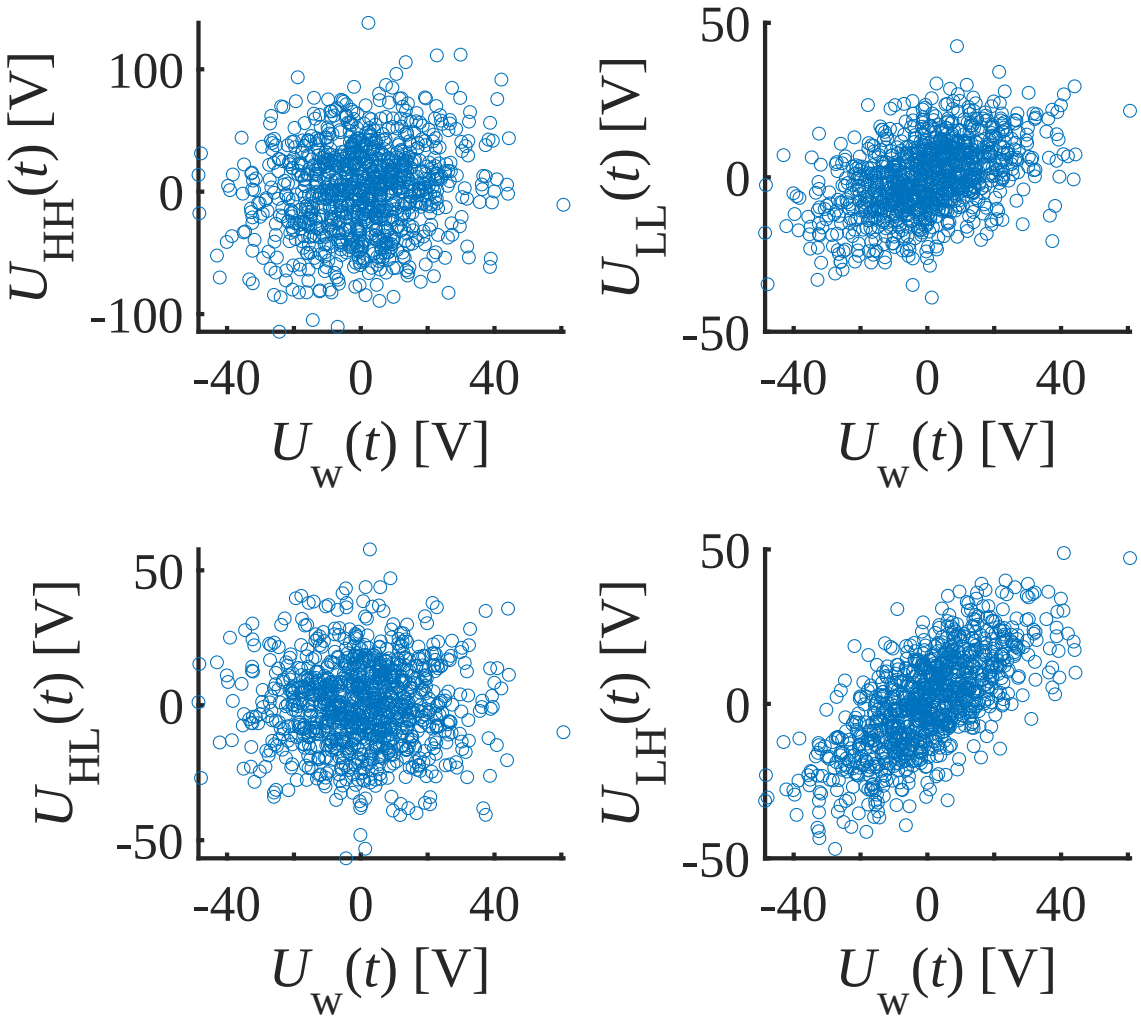


Figure 2.18: Correlation between Eve's *measured* channel voltage, $U_{\mathrm{w}}(t)$, and her four *simulated* channel voltages, $U_{\mathrm{HH}}(t)$, $U_{\mathrm{LL}}(t)$, $U_{\mathrm{HL}}(t)$, and $U_{\mathrm{LH}}(t)$ at $M = 1$.

The results of the attack are shown in Table 2.1. The HL situation of Eve has zero cross-correlation with Eve's probe signals because, in this case, Alice/Bob and Eve do not have a common noise. In all the other cases, they have at least one mutual noise. In the LH attack situation,

both noises are common, thus they yield the highest cross-correlation with Eve's LH probe, therefore Eve guesses that the secure resistance situation is LH.

Using the correlations between the voltages for the attack yielded the highest probability p of successful guessing, and the correlations between the powers yielded the lowest one. This is because power is the product of voltage and current (see Equation (2.1)), and the inaccuracies in both the voltage and current correlations affect the power correlations.

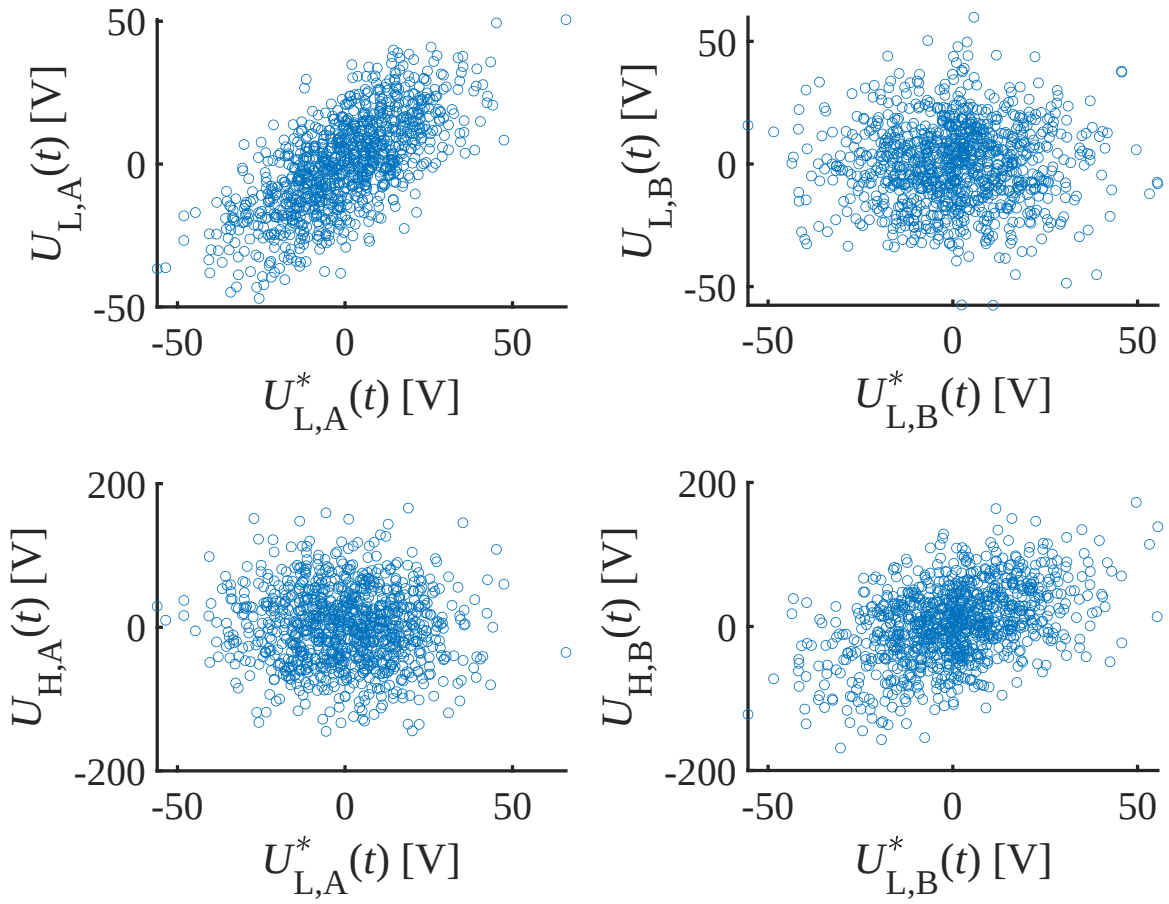
2.3.2.1.2 *Bilateral attack demonstration utilizing cross-correlations among the voltage sources*

Eve uses Equation (2.16) to find $U^*_{\mathrm{L,A}}(t)$, Equation (2.17) to find the cross-correlation between $U^*_{\mathrm{L,A}}(t)$ and $U_{\mathrm{L,A}}(t)$, Equation (2.18) to find $U^*_{\mathrm{L,B}}(t)$, and Equation (2.19) to find the cross-correlation between $U^*_{\mathrm{L,B}}(t)$ and $U_{\mathrm{L,B}}(t)$.

A visual example of the correlations between (a) $U^*_{\mathrm{L,A}}(t)$ and $U_{\mathrm{L,A}}(t)$, $U^*_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$, and (b) $U^*_{\mathrm{L,B}}(t)$ and $U_{\mathrm{L,B}}(t)$, $U^*_{\mathrm{L,B}}(t)$ and $U_{\mathrm{H,B}}(t)$, is shown in Figure 2.19. The highest correlation on Alice's side is with $U^*_{\mathrm{L,A}}(t)$, and the highest correlation on Bob's side is with $U_{\mathrm{H,B}}(t)$, thus Eve guesses that Alice has R_{L} and Bob has R_{H}.

Table 2.1: Simulation of the average cross-correlation coefficient, CCC (see Equations (2.13)-(2.15)), Eve's average p of correctly guessing the LH bit situations, and standard deviation σ at varying multipliers M (see Section 2.2.2.2). As M increases, which implies increasing differences between the noises of Alice/Bob and Eve's probing noises, the cross-correlation decreases. Yet, in each case of the present situation, the LH case yields the highest correlation. Thus, Eve guesses that LH is the secure bit situation. The correlations CCC_{u} between the voltages yielded p_{u}, which had the highest probability p of successful guessing, and the correlations CCC_{p} between the powers yielded the lowest p. This is because power is the product of voltage and current (see Equation (2.1)), and the inaccuracies in both the voltage and current correlations affect the power correlations.

Eve's probing bit	M	CCC_{u}	p_{u}	σ_{u}	CCC_{i}	p_{i}	σ_{i}	CCC_{p}	p_{p}	σ_{p}
HH	0	0.21314			0.67455			0.28482		
LL		0.67377			0.21317			0.28502		
HL		-0.00118			0.00128			-0.00126		
LH		1	1	0	1	1	0	1	1	0
HH	0.1	0.21087			0.67048			0.28198		
LL		0.67090			0.21326			0.28573		
HL		-0.00030			-0.00007			0.00095		
LH		0.99504	1	0	0.99505	1	0	0.99005	1	0
HH	0.5	0.18975			0.60201			0.23101		
LL		0.60349			0.19047			0.23089		
HL		-0.00023			-0.00090			-0.00114		
LH		0.89457	1	0	0.89441	1	0	0.79926	1	0
HH	1	0.15004			0.47631			0.14297		
LL		0.47705			0.15241			0.14315		
HL		0.00082			0.00074			0.00061		
LH		0.70664	1	0	0.70667	1	0	0.49926	1	0
HH	1.5	0.11814			0.37380			0.08931		
LL		0.37390			0.11798			0.08669		
HL		0.00022			-0.00024			-0.00141		
LH		0.55434	1	0	0.55473	1	0	0.30762	1	0
HH	5	0.04021			0.13280			0.01158		
LL		0.13142			0.03961			0.01000		
HL		-0.00069			0.00087			-0.00052		
LH		0.19490	1	0	0.19525	0.996	0.0144	0.03830	0.756	0.0144
HH	10	0.02200			0.06581			0.00266		
LL		0.06692			0.02130			0.00525		
HL		0.00064			-0.00102			0.00090		
LH		0.09905	0.977	0.0034	0.09878	0.907	0.0111	0.01244	0.613	0.0209



(a) (b)

Figure 2.19: Correlation between (a) $U^*_{\mathrm{L,A}}(t)$ vs. $U_{\mathrm{L,A}}(t)$ and $U_{\mathrm{H,A}}(t)$, and (b) $U^*_{\mathrm{L,B}}(t)$ vs. $U_{\mathrm{L,B}}(t)$ and $U_{\mathrm{H,B}}(t)$. The highest correlation on Alice's side is with $U^*_{\mathrm{L,A}}(t)$, and the highest correlation on Bob's side is with $U_{\mathrm{H,B}}(t)$, thus Eve guesses that Alice has R_{L} and Bob has R_{H}.

A simulation results of the cross correlation for each bit case is displayed in Table 2.2. As the multiplier M in the superposition increases (see Section 2.2.2.2), the correlations decrease. Yet, in each case at the present (LH) situation, the highest correlation ended up being the LH case, thus Eve has decided that LH is the secure resistance situation.

Table 2.2: Simulation of the cross-correlation coefficients CCC at the attack described in Section 2.3.1.1.2 (see Equations (2.17) and (2.19)), Eve's average correct-guessing probability p, and standard deviation σ at varying multipliers M (see Section 2.2.2.2). As M increases, which implies increasing differences between the noises of Alice/Bob and Eve's probing noises, the cross-correlation decreases. Yet, in each case of the present situation, the R_{L} hypothesis yields the highest cross-correlation with Alice's noise. Thus, Eve guesses that Alice has R_{L}. The same procedure done for Bob's noise results in the highest cross-correlation for the R_{H} hypothesis at Bob's side.

M	$CCC_{\mathrm{LA}}(R_{\mathrm{L}})$	$CCC_{\mathrm{LA}}(R_{\mathrm{H}})$	$CCC_{\mathrm{LB}}(R_{\mathrm{L}})$	$CCC_{\mathrm{LB}}(R_{\mathrm{H}})$	p	σ
0	1	-0.03331	-0.00092	0.57727	1	0
0.1	0.99504	0.00948	0.00031	0.55856	1	0
0.5	0.89451	0.01440	0.00063	0.51939	1	0
1	0.70682	-0.05075	0.00140	0.40084	1	0
1.5	0.55430	-0.02511	0.00004	0.31684	1	0
5	0.19496	-0.03176	-0.00088	0.14445	0.995	0.0022
10	0.09949	-0.02127	-0.00009	0.01611	0.894	0.0095

2.3.2.2 Attack demonstration when Eve knows only one of the sources (unilateral attacks)

2.3.2.2.1 *Unilateral attack demonstration utilizing cross-correlations between Alice's/Bob's and Eve's wire voltages, currents and powers*

Like the bilateral results (see Section 2.3.2.1.1), the HL situation of Eve has zero cross-correlation with Eve's probe signals because, in this case, Alice/Bob, and Eve do not have a common noise. In all the other cases, they have at least one mutual noise. In the LH probe attack, both noises are common, thus they yield the highest cross-correlation with Eve's LH probe, therefore Eve guesses that the secure resistance situation is LH, see Table 2.2.

Using the correlations between the voltages for the attack yielded the highest probability p of successful guessing, and the correlations between the powers yielded the lowest one. This is because power is the product of voltage and current (see Equation (2.1)), and the inaccuracies in both the voltage and current correlations affect the power correlations.

Finally, Eve evaluates the measured mean-square voltage on the wire over the bit exchange period. From that value, by using Equation (1.5), she evaluates the parallel resultant R_{P} of the

Table 2.3: Simulation of the cross-correlation coefficient, CCC (see Equations (2.13)-(2.15)), Eve's average p of correctly guessing the LH bit situations, and standard deviation σ at varying multipliers M (see Section 2.2.2.2). As M increases, which implies increasing differences between the noises of Alice/Bob and Eve's probing noises, the cross-correlation decreases. Yet, in each case of the present situation, the LH case yields the highest correlation. Thus, Eve guesses that LH is the secure bit situation. The correlations CCC_{u} between the voltages yielded p_{u}, which had the highest probability p of successful guessing, and the correlations CCC_{p} between the powers yielded the lowest p. This is because power is the product of voltage and current (see Equation (2.1)), and the inaccuracies in both the voltage and current correlations affect the power correlations.

Eve's probing bit	M	CCC_{u}	p_{u}	σ_{u}	CCC_{i}	p_{i}	σ_{i}	CCC_{p}	p_{p}	σ_{p}
HH	0	-0.00166			0.00018			-0.00055		
LL		0.67432			0.08975			0.16311		
HL		0.00055			0.00084			-0.00193		
LH		0.90898	1	0	0.21237	0.995	0.0016	0.28506	0.982	0.0042
HH	0.1	-0.00027			-0.00048			0.00198		
LL		0.67119			0.09030			0.16500		
HL		0.00051			-0.00006			0.00048		
LH		0.90462	1	0	0.21337	0.995	0.0026	0.28580	0.980	0.0044
HH	0.5	0.00022			0.00049			0.00224		
LL		0.60249			0.08149			0.13370		
HL		-0.00168			-0.00165			0.00062		
LH		0.81357	1	0	0.18865	0.983	0.0034	0.23146	0.962	0.0049
HH	1	-0.00081			0.00079			-0.0000		
LL		0.47610			0.06526			0.08290		
HL		-0.00029			0.00009			0.00092		
LH		0.64237	1	0	0.15093	0.929	0.0132	0.14373	0.926	0.0062
HH	1.5	-0.00046			-0.00097			0.00001		
LL		0.37480			0.04921			0.04924		
HL		0.00159			0.00003			-0.00016		
LH		0.50383	1	0	0.11863	0.859	0.0133	0.08675	0.827	0.0116
HH	5	-0.00018			0.00094			0.00088		
LL		0.13188			0.01730			0.00728		
HL		0.00010			0.00168			-0.00036		
LH		0.17768	1	0	0.04152	0.637	0.0157	0.01052	0.561	0.0143
HH	10	0.00058			-0.00017			-0.00088		
LL		0.06566			0.00989			0.00180		
HL		-0.00108			0.00121			-0.00096		
LH		0.08992	0.978	0.0055	0.02084	0.604	0.0134	0.00307	0.523	0.0170

resistances of Alice and Bob. From $R_{\rm P}$ and $R_{\rm A}$, she can calculate $R_{\rm B}$. In this particular case, from the mean-square voltage Eve will learn that the actual situation is LH thus Bob has chosen $R_{\rm H}$ because Alice has $R_{\rm L}$ [41].

Alternatively, since she knows Alice's resistance, she can use the mean-square voltage to determine the secure bit situation and thus crack the KLJN scheme.

2.3.2.2.2 *Unilateral attack demonstration utilizing cross-correlations among the voltage sources*

Eve uses (Equation (2.16)) to find $U^*_{\rm L,A}(t)$ and (Equation (2.17)) to find the cross-correlation between $U^*_{\rm L,A}(t)$ and $U_{\rm L,A}(t)$. A simulation results of the cross correlation for each bit case is displayed in Table 2.4. As the multiplier M increases (see Section 2.2.2.2), the correlation decreases, yet the highest correlation always ended up being the LH case, thus Eve has decided that LH is the secure resistance situation.

Table 2.4: A realization of the cross-correlation coefficient, CCC (see Equation (2.17)), Eve's average correct-guessing probability p, and standard deviation σ at varying multipliers M (see Section 2.2.2.2). As M increases, which implies increasing differences between the noises of Alice/Bob and Eve's probing noises, the cross-correlation decreases. Yet, the $R_{\rm L}$ case yields the highest correlation. Thus, Eve guesses that Alice has $R_{\rm L}$.

M	$CCC_{\rm LA}(R_{\rm L})$	$CCC_{\rm LA}(R_{\rm H})$	p	σ
0	1	-0.03331	1	0
0.1	0.99504	0.00948	1	0
0.5	0.89451	0.01440	1	0
1	0.70682	-0.05075	1	0
1.5	0.55430	-0.02511	1	0
5	0.19496	-0.03176	1	0
10	0.09949	-0.02127	0.989	0.0022

Finally, Eve evaluates the measured mean-square voltage on the wire over the bit exchange period. From that value, by using Equation (1.5), she evaluates the parallel resultant $R_{\rm P}$ of the

resistances of Alice and Bob. From R_{P} and R_{A}, she can calculate R_{B}. In this particular case, from the mean-square voltage, Eve will learn that the actual situation is LH, thus Bob has chosen R_{H} because Alice has R_{L} [41].

2.3.3 Transition

This concludes the RNG attacks presented in this dissertation. As a take-home message, the security of the KLJN scheme requires the RNG outputs to appear truly random for Eve. Now, we move onto the zero-crossing attack.

3. ZERO-CROSSING ATTACK AGAINST THE KIRCHHOFF-LAW-JOHNSON-NOISE SECURE KEY EXCHANGER[4]

3.1 Security in Thermal Equilibrium

In the KLJN protocol, the net power flow $\langle P_{\rm w}(t)\rangle$ between Alice and Bob (see Equation (2.1)) is zero because their resistors have the same (noise) temperature. The noise spectra of the voltage $U_{\rm w}(t)$ and current $I_{\rm w}(t)$ in the wire (see Figure 1.2), $S_{\rm u}$ and $S_{\rm i}$, respectively, are given by the Johnson formulas of thermal noise:

$$S_{\rm u}(f) = 4kTR_{\rm P}, \tag{3.1}$$

$$S_{\rm i}(f) = \frac{4kT}{R_{\rm S}}, \tag{3.2}$$

where *k* is the Boltzmann constant, and $R_{\rm P}$ and $R_{\rm S}$ are the parallel and serial resultants of the connected resistors, respectively. In the HL and LH cases the resultants are:

$$R_{\rm P_{LH}} = R_{\rm P_{HL}} = \frac{R_{\rm L}R_{\rm H}}{R_{\rm L}+R_{\rm H}}, \tag{3.3}$$

$$R_{\rm S_{LH}} = R_{\rm S_{HL}} = R_{\rm L}+R_{\rm H}, \tag{3.4}$$

Equations (3.1)-(3.4) guarantee that the noise spectra and effective voltage and current values in the wire are identical in the LH and HL cases, in accordance with the perfect security requirement. In conclusion, the quantities that Eve can access with passive measurements satisfy the following equations that, together with Equations (3.3) and (3.4), form the pillars of security against passive

[4]Part of this chapter is reprinted with permission from C. Chamon, L. B. Kish, "Perspective–on the thermodynamics of perfect unconditional security," *Applied Physics Letters*, vol. 119, pp. 010501, 2021. Copyright 2021 by AIP Publishing.

attacks against the KLJN system:

$$U_{\mathrm{LH}} = U_{\mathrm{HL}}, \tag{3.5}$$

$$I_{\mathrm{LH}} = I_{\mathrm{HL}}, \tag{3.6}$$

$$P_{\mathrm{LH}} = P_{\mathrm{HL}} = 0 \tag{3.7}$$

where U_{LH}, I_{LH}, and P_{LH} denote the RMS wire voltage, RMS wire current, and net power flow from Alice to Bob in the LH case, and U_{HL}, I_{HL}, and P_{HL} denote the RMS wire voltage, RMS wire current, and net power flow from Alice to Bob in the HL case.

3.2 Security out of Equilibrium? The VMG-KLJN System

Vadai, Mingesz, and Gingl (VMG) have made an impressive generalization attempt [51], see Figure 3.1. They assumed that the four resistors are different and arbitrarily chosen (with some limitations [51]) and asked the question if the security can be maintained by a proper choice of different temperatures of these resistors.

In search for their solution, they used Equations (3.5) and (3.6) and removed Equation (3.7), the zero power flow condition.

VMG obtained the following solutions for the required mean-square thermal noise voltages of the thermal noise generators of the resistors, where the rms voltage $U_{\mathrm{L,A}}$ of the resistor $R_{\mathrm{L,A}}$ (see Figure 3.1) is freely chosen:

$$U_{\mathrm{H,B}}^2 = U_{\mathrm{L,A}}^2 \frac{R_{\mathrm{L,B}}(R_{\mathrm{H,A}} + R_{\mathrm{H,B}}) - R_{\mathrm{H,A}}R_{\mathrm{H,B}} + R_{\mathrm{H,B}}^2}{R_{\mathrm{L,A}}^2 + R_{\mathrm{L,B}}(R_{\mathrm{L,A}} - R_{\mathrm{H,A}}) - R_{\mathrm{H,A}}R_{\mathrm{L,A}}} = 4kT_{\mathrm{H,B}}R_{\mathrm{H,B}}\Delta f_{\mathrm{B}}, \tag{3.8}$$

$$U_{\mathrm{H,A}}^2 = U_{\mathrm{L,A}}^2 \frac{R_{\mathrm{L,B}}(R_{\mathrm{H,A}} + R_{\mathrm{H,B}}) + R_{\mathrm{H,A}}R_{\mathrm{H,B}} + R_{\mathrm{H,A}}^2}{R_{\mathrm{L,A}}^2 + R_{\mathrm{L,B}}(R_{\mathrm{L,A}} + R_{\mathrm{H,B}}) + R_{\mathrm{H,B}}R_{\mathrm{L,A}}} = 4kT_{\mathrm{H,A}}R_{\mathrm{H,A}}\Delta f_{\mathrm{B}}, \tag{3.9}$$

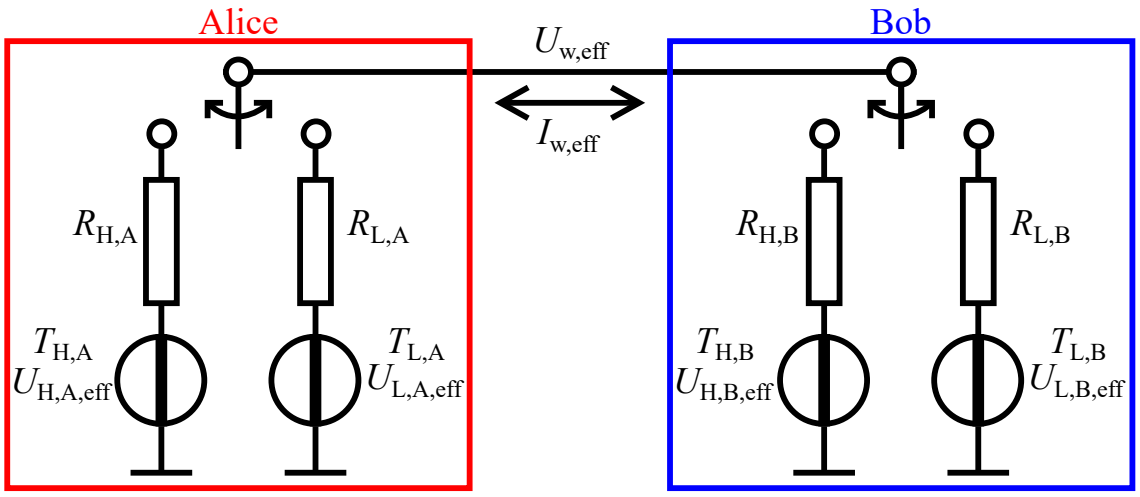


Figure 3.1: The core of the Vadai-Mingesz-Gingl (VMG-KLJN) secure key exchanger scheme. The four resistors are different and they can be freely chosen (though with some limitations because of certain unphysical solutions). One temperature is freely chosen. The other 3 temperatures depend on the resistor values and can be deducted by the VMG-equations (3.8)-(3.10), see Equations (3.11)-(3.13) below.

$$U_{\mathrm{L,B}}^2 = U_{\mathrm{L,A}}^2 \frac{R_{\mathrm{L,B}}(R_{\mathrm{H,A}} - R_{\mathrm{H,B}}) - R_{\mathrm{H,A}}R_{\mathrm{H,B}} + R_{\mathrm{L,B}}^2}{R_{\mathrm{L,A}}^2 + R_{\mathrm{L,A}}(R_{\mathrm{H,B}} - R_{\mathrm{H,A}}) - R_{\mathrm{H,A}}R_{\mathrm{H,B}}} = 4kT_{\mathrm{L,B}}R_{\mathrm{L,B}}\Delta f_{\mathrm{B}}, \tag{3.10}$$

For more direct statistical physical comparison, we expanded [51] the VMG equations by introducing (on the right hand side) the temperatures of the resistors, where Δf_{B} is the noise bandwidth of the generators, which is identical for all resistors, and the required temperatures of the resistors shown above are determined by the Johnson-Nyquist formula, see Equation (1.5). Thus, from Equations (3.8)-(3.10) and Equation (1.5), the temperatures are:

$$T_{\mathrm{H,B}} = \frac{R_{\mathrm{L,A}}}{R_{\mathrm{H,B}}} T_{\mathrm{L,A}} \frac{R_{\mathrm{L,B}}(R_{\mathrm{H,A}} + R_{\mathrm{H,B}}) - R_{\mathrm{H,A}}R_{\mathrm{H,B}} + R_{\mathrm{H,B}}^2}{R_{\mathrm{L,A}}^2 + R_{\mathrm{L,B}}(R_{\mathrm{L,A}} - R_{\mathrm{H,A}}) - R_{\mathrm{H,A}}R_{\mathrm{L,A}}}, \tag{3.11}$$

$$T_{\mathrm{H,A}} = \frac{R_{\mathrm{L,A}}}{R_{\mathrm{H,A}}} T_{\mathrm{L,A}} \frac{R_{\mathrm{L,B}}(R_{\mathrm{H,A}} + R_{\mathrm{H,B}}) + R_{\mathrm{H,A}}R_{\mathrm{H,B}} + R_{\mathrm{H,A}}^2}{R_{\mathrm{L,A}}^2 + R_{\mathrm{L,B}}(R_{\mathrm{L,A}} + R_{\mathrm{H,B}}) + R_{\mathrm{H,B}}R_{\mathrm{L,A}}}, \tag{3.12}$$

$$T_{\mathrm{L,B}} = \frac{R_{\mathrm{L,A}}}{R_{\mathrm{L,B}}} T_{\mathrm{L,A}} \frac{R_{\mathrm{L,B}}(R_{\mathrm{H,A}} - R_{\mathrm{H,B}}) - R_{\mathrm{H,A}}R_{\mathrm{H,B}} + R_{\mathrm{L,B}}^2}{R_{\mathrm{L,A}}^2 + R_{\mathrm{L,A}}(R_{\mathrm{H,B}} - R_{\mathrm{H,A}}) - R_{\mathrm{H,A}}R_{\mathrm{H,B}}}, \tag{3.13}$$

where $T_{\mathrm{L,A}}$ is the temperature of resistor $R_{\mathrm{L,A}}$.

The practical advantage of the VMG-KLJN scheme would appear with inexpensive versions of chip technology where resistance accuracy and its temperature stability are poor. However, concerning the fundamental physics aspects for security, there is a much more important question: What law of physics that guarantees the perfect security of the ideal system? In the case of the standard KLJN system, that is the *Second Law of Thermodynamics* (see Section 1.2). However, due to VMG's security claim at nonzero power flow, this explanation is seemingly irrelevant in the VMG-KLJN system.

3.2.1 The FCK1-VMG-KLJN System: Different Resistors but Still in Equilibrium

Recently, Ferdous, Chamon and Kish (FCK) [51] pointed out some excess information leak (compared to classical KLJN protocols) in the VMG-KLJN system under practical conditions. Among others, they proposed three modified VMG-KLJN versions for improvements. One of these schemes, the FCK1-VMG-KLJN scheme [51], is able to operate with four different resistors so that during each secure bit exchange period *the connected* resistor pair (one resistor at each side) is in thermal equilibrium, that is, the resistors in the pair have the same temperature. However, the two "secure-choice" resistor arrangements $R_{\mathrm{H,A}}||R_{\mathrm{L,B}}$ and $R_{\mathrm{L,A}}||R_{\mathrm{H,B}}$ must be at a different temperature, except in the original KLJN scheme where the two resistor pairs (of the HL and LH situations) are identical. (This is a minor security risk but is out of the topic of our present dissertation.)

The condition of zero power is that the geometrical means of the connected resistors in the LH and HL situations are equal [51]. In other words, when we choose three resistors freely, the fourth one is determined by the condition of zero power flow. For example, with $R_{\mathrm{H,B}}$, $R_{\mathrm{L,A}}$, and $R_{\mathrm{H,A}}$ chosen, we get:

$$R_{\mathrm{L,B}} = \frac{R_{\mathrm{H,B}} R_{\mathrm{L,A}}}{R_{\mathrm{H,A}}}. \tag{3.14}$$

Due to the thermal equilibrium during a single bit exchange, the FCK1-VMG-KLJN system has a special role in the study of the non-equilibrium VMG-KLJN protocol in the following section.

In the next section, we answer the following question: Is it possible that there is a new, unknown attack that can extract information from the VMG-KLJN system while it is unable to do that with the standard KLJN scheme? If so, the VMG-KLJN arrangement would be just a modified KLJN scheme that is *distorted* for a special purpose (free resistor choice) while, as a compromise, its perfect security is given up. It would still have the same foundation of security, the Second Law, but in an imperfect way due to the nonideality introduced by the nonzero power flow. In the next two sections, we show that this is indeed the case.

3.3 ZERO-CROSSING ATTACK AGAINST THE VMG-KLJN SCHEME

The VMG-KLJN scheme seems to be perfectly secure at nonzero power flow because the voltage and the current are Gaussian processes and their mean-square values are identical in the LH and HL bit situations, even though the resistor and related mean-square voltage pairs are different. Therefore, even the power, which is the mean of their product (see Equation (2.1)), seems to carry no useful information for Eve. Gaussian processes are perfect information hiders.

Thus, we are exploring here a yet uncharted area: the statistics of the coincidence properties of the voltages at the two ends. Whenever the current is zero in the wire, the voltages at the two ends are equal. Let us *sample* the voltages on the wire at these coincidence points: then the voltage in the wire has the same value as that of the generators of Alice and Bob because the current is zero. For an intuitive start, imagine the situation when in the HL case the VMG voltage is very high at the H side and small at the L side, while in the LH case the voltages are similar (see Equations (3.8)-(3.10)). The Gaussian process is statistically confined to the order of the RMS value, thus these samples will be mostly confined to a fraction of the RMS value of the large noise at the H side of the HL situation, which is very different from what we have in the LH situation outlined above.

In this way, we have a heuristic hope that the mean-square values of these voltage samples will depend on the bit situations (HL or LH). Note, such an attack would not work against the original KLJN scheme, as there the HL and LH voltage and resistor pairs are identical.

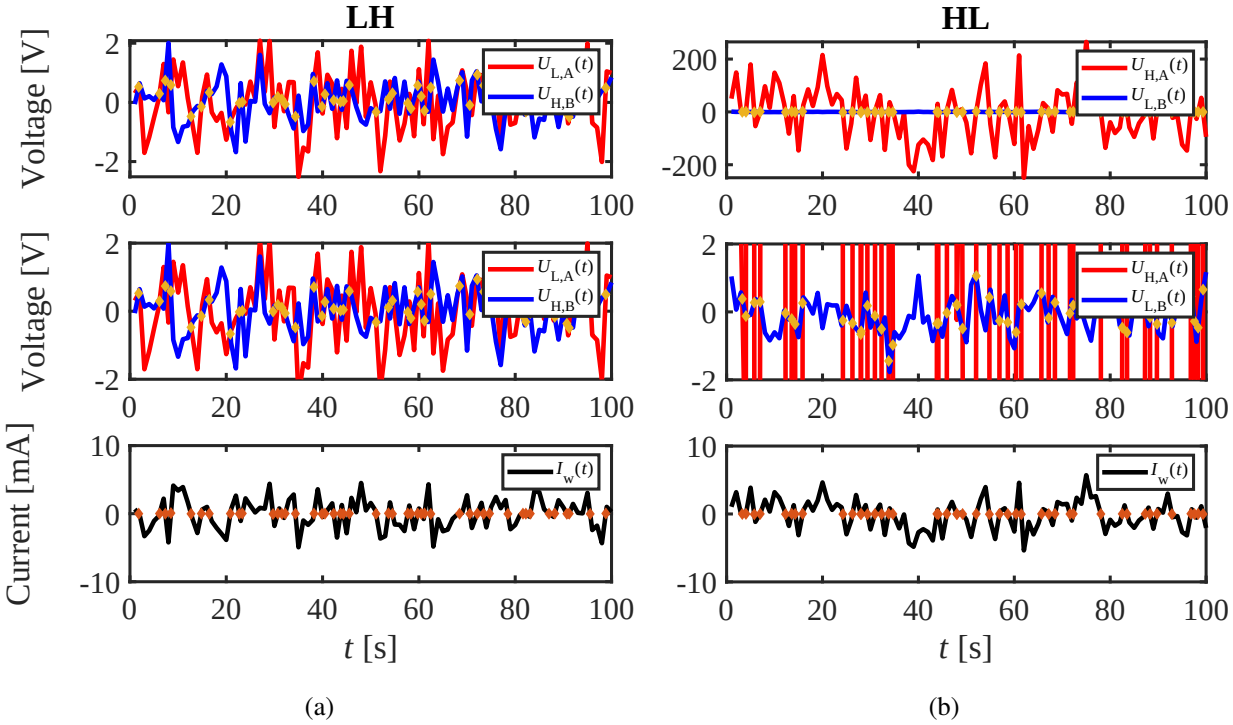
Moreover, whenever the net power flow is zero due to thermal equilibrium, such as in the original KLJN scheme, the wire voltage and current are uncorrelated. Then their Gaussianity implies that sampling the voltage at the zero-crossing times of the current represents an independent sampling of the voltage. That means the mean-square wire voltage will be the nominal value for the HL/LH situation, thus there is no information there for Eve. This is another reason why the original KLJN scheme would be immune against such a zero-crossing attack. Moreover, it is an indication that the FCK1-VMG-KLJN system, where the power flow is also zero, is also immune against this new attack.

Below, we demonstrate by computer simulations that the intuitive expectation turns out to be valid, and the VMG-KLJN scheme is leaking information at nonzero power flow. In the next section, we also show that there is a new KLJN scheme that is secure against the attack even though the four resistors are different.

3.3.1 Computer Simulations/Verification of the Zero-Crossing Attack

During the noise generation, we used oversampling and interpolation to produce sufficiently smooth noises to emulate physical noise sources and to detect the zero-crossing current events with sufficient accuracy, see Figure 3.2.

An example for Alice's and Bob's noise voltages and channel current in the VMG-KLJN scheme, at $R_{\mathrm{H,A}} = 46,416\ \Omega$, $R_{\mathrm{L,A}} = 278\ \Omega$, $R_{\mathrm{H,B}} = 278\ \Omega$, $R_{\mathrm{L,B}} = 100\ \Omega$, $T_{\mathrm{H,A}} = 8.0671 \times 10^{18}$ K, $T_{\mathrm{L,A}} = 1.3033 \times 10^{17}$ K, $T_{\mathrm{H,B}} = 6.2112 \times 10^{16}$ K, $T_{\mathrm{L,B}} = 1.1694 \times 10^{17}$ K, and $\Delta f_{\mathrm{B}} = 500$ Hz, is shown in Figure 3.2. The zero-crossing points of the channel current are the points where Alice's and Bob's noise voltages are equal. At the particular choice of resistances, in the LH case, Alice and Bob have similar noise voltage amplitudes, while in the HL case, Alice's noise voltage amplitudes are much larger than Bob's, thus the zero-crossing points are ultimately determined by Bob's noise voltage.



(a) (b)

Figure 3.2: A realization of the instantaneous noise voltages of Alice (red) and Bob (blue) and the channel current (black) in the LH (a) and HL (b) cases for the VMG-KLJN scheme, at $R_{\mathrm{H,A}} = 46,416\ \Omega$, $R_{\mathrm{L,A}} = 278\ \Omega$, $R_{\mathrm{H,B}} = 278\ \Omega$, $R_{\mathrm{L,B}} = 100\ \Omega$, $T_{\mathrm{H,A}} = 8.0671 \times 10^{18}$ K, $T_{\mathrm{L,A}} = 1.3033 \times 10^{17}$ K, $T_{\mathrm{H,B}} = 6.2112 \times 10^{16}$ K, $T_{\mathrm{L,B}} = 1.1694 \times 10^{17}$ K, and $\Delta f_{\mathrm{B}} = 500$ Hz. $U^2_{\mathrm{L,A}} = 1\ \mathrm{V}^2$, $U^2_{\mathrm{H,B}} = 0.477\ \mathrm{V}^2$, $U^2_{\mathrm{H,A}} = 1.03 \times 10^4\ \mathrm{V}^2$, and $U^2_{\mathrm{L,B}} = 0.323\ \mathrm{V}^2$. The points where the channel current $I_{\mathrm{w}}(t)$ is zero, represented in orange, are the points where Alice's and Bob's noise voltages are equivalent, represented in yellow. In the LH case, Alice's noise voltage $U_{\mathrm{L,A}}(t)$ is comparable to Bob's noise voltage $U_{\mathrm{H,B}}(t)$, while in the HL case, Alice's noise voltage $U_{\mathrm{L,A}}(t)$ is significantly larger than Bob's noise voltage $U_{\mathrm{H,B}}(t)$, thus the points where Alice's and Bob's noise voltages are equal to each other are ultimately determined by the smaller noise amplitude. $U_{\mathrm{H,A}} \gg U_{\mathrm{L,B}}$, thus $U_{\mathrm{L,B}}(t)$ looks like a straight line because of limited resolution in the figure. The middle subplot in (b) shows an enlarged scale to visualize crossing events while figure on the left is the same as above for comparison purposes.

The histograms of the mean-square channel voltages, currents, and zero-crossing points after 1,000 runs are shown in Figure 3.3 for the original KLJN scheme (a), the VMG-KLJN scheme (b), and the FCK1-VMG-KLJN scheme (c). The orange histograms represent the LH situation, whereas the blue histograms represent the HL situation. The red lines represent the expected (mean) value. The secure bit (LH and HL) mean-square voltages and currents are the same in all

schemes, as it has been expected by the VMG-KLJN creators. However, in the LH and HL cases, the zero-crossing sampled mean-square voltages $U^2_{\mathrm{w,zc}}$ are the same only in the original KLJN and FCK1-VMG-KLJN schemes, but markedly different in the VMG-KLJN scheme, indicating its cracked security.

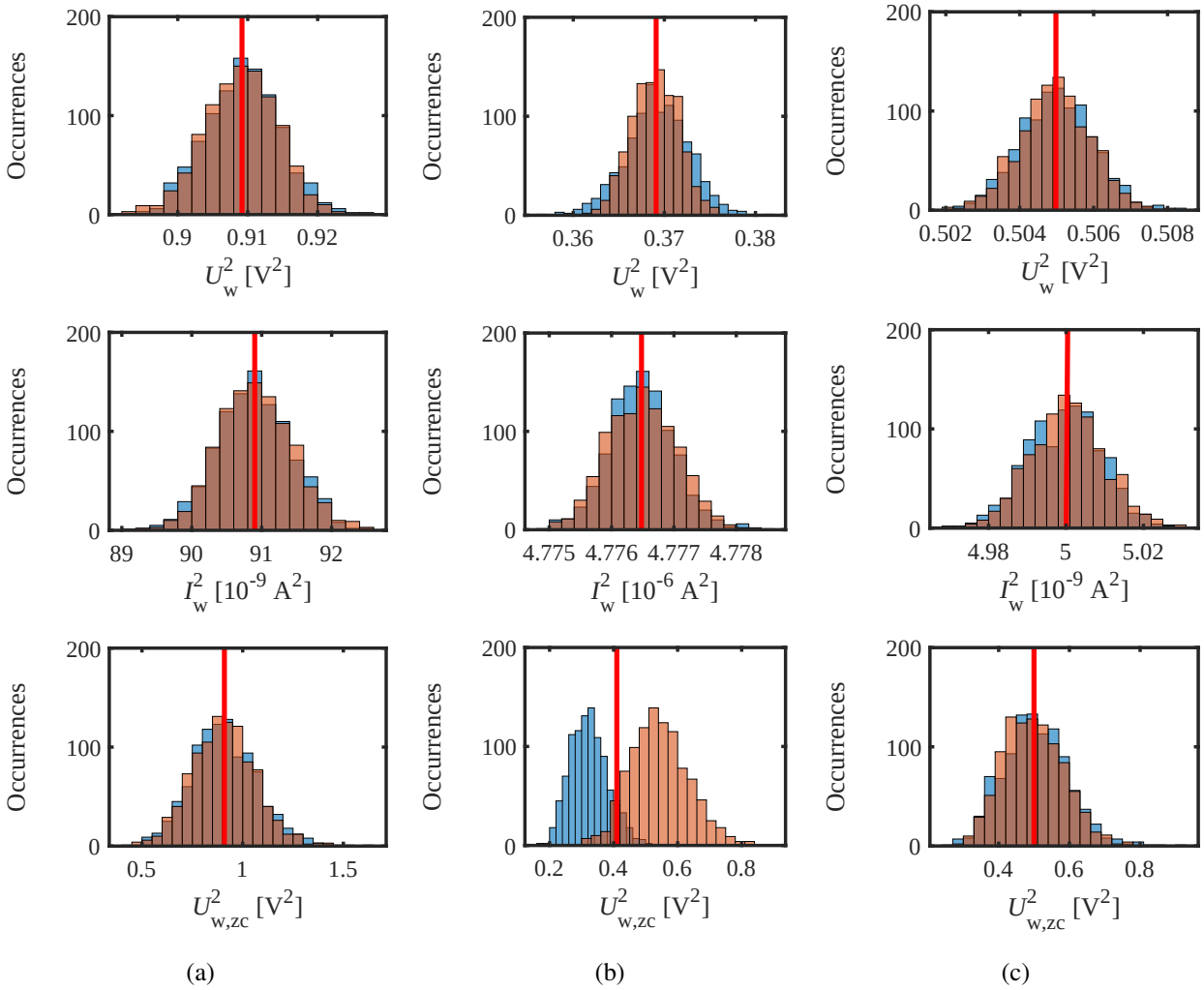


Figure 3.3: Histograms of the mean-square channel voltage $U_{\rm w}^2$ (first row), current $I_{\rm w}^2$ (second row), and zero-crossing points $U_{\rm w,zc}^2$ (third row) for:
Column-(a) the original KLJN scheme at $R_{\rm H,A} = R_{\rm H,B} = 10$ kΩ and $R_{\rm L,A} = R_{\rm L,B} = 1$ kΩ,
Column-(b) the VMG-KLJN scheme at $R_{\rm H,A} = 46.4$ kΩ, $R_{\rm L,A} = 278\ \Omega$, $R_{\rm H,B} = 278\ \Omega$, and $R_{\rm L,B} = 100\ \Omega$, and
Column-(c) the FCK1-VMG-KLJN scheme at $R_{\rm H,A} = 100$ kΩ, $R_{\rm L,A} = 10$ kΩ, $R_{\rm H,B} = 10$ kΩ, and $R_{\rm L,B} = 1$ kΩ. The orange histograms represent the LH situation, and the blue histograms represent the HL situation. The red vertical lines represent the expected (mean) value. In all three schemes, $U_{\rm w}^2$ and $I_{\rm w}^2$ have the same LH and HL distributions (within statistical inaccuracy). In the original KLJN and FCK1-VMG-KLJN schemes, $U_{\rm w,zc}^2$ has the same LH and HL distributions, in accordance with their perfect security. In the VMG-KLJN scheme, the distributions of the $U_{\rm w,zc}^2$ values at the LH and HL cases are split, which indicates significant information leak.

Table 3.1 shows the mean-square voltage $U_{\rm w}^2$, mean-square current, $I_{\rm w}^2$, average power $\langle P_{\rm w}(t)\rangle$,

and zero-crossing mean-square voltage $U^2_{\mathrm{w,zc}}$ values for the original KLJN, three VMG-KLJN, and FCK1-VMG-KLJN representations.

In the original KLJN and FCK1-VMG-KLJN representations, the mean-square zero-crossing voltage approaches the channel voltage indicating a random, current-independent sampling. In the VMG-KLJN scheme, as the cross-correlation between the voltage and current increases (indicated also by the nonzero power flow), the mean-square zero-crossing voltage becomes more dispersed in the LH and HL cases.

Table 3.2 shows the statistical run for Eve's probability p and its standard deviation σ_p of guessing the correct bit. When the average power $\langle P_{\mathrm{w}}(t)\rangle$ approaches zero, the p value approaches 0.5 (thus the information leak converges zero) because the cross-correlation coefficient between the current and voltage also converges to zero.

Table 3.1: Results for the wire mean-square voltage U^2_{w}, mean-square current, I^2_{w}, average power $\langle P_{\mathrm{w}}(t)\rangle$, and zero-crossing mean-square voltage $U^2_{\mathrm{w,zc}}$ for the KLJN, three VMG-KLJN, and FCK1-VMG-KLJN schemes, where R_{A} and R_{B} represent Alice's and Bob's resistor choices, respectively. In the classical KLJN and FCK1-VMG-KLJN schemes, $U^2_{\mathrm{w,zc}}$ approaches U^2_{w}. In the VMG-KLJN scheme, as $\langle P_{\mathrm{w}}(t)\rangle$ increases, $U^2_{\mathrm{w,zc}}$ becomes split in the LH and HL situations.

Scheme	bit	R_{A} [Ω]	R_{B} [Ω]	U^2_{w} [V]	I^2_{w} [10^{-6} A^2]	$\langle P_{\mathrm{w}}(t)\rangle$ [10^{-3} W]	$U^2_{\mathrm{w,zc}}$ [V^2]
KLJN	LH	1k	10k	0.908	0.091	0	0.907
	HL	10k	1k				0.908
VMG-KLJN	LH	100	16.7k	0.991	0.314	0.026	0.989
	HL	16.7k	278				1.009
	LH	278	278	0.368	4.786	0.471	0.301
	HL	46.4k	100				0.576
	LH	100	6k	0.967	0.073	0.156	0.675
	HL	360k	2.2k				0.845
FCK-VMG-KLJN	LH	10k	10k	0.500	0.005	0	0.498
	HL	100k	1k				0.502

In conclusion, the computer simulations confirmed that the zero-crossing attack is an efficient passive attack against the general VMG scheme whenever the net power flow is not zero. The FCK1-VMG-KLJN protocol, which is the zero-power version of the scheme, is robust against this

Table 3.2: Statistical run for Eve's probability p of guessing the correct bit from the zero-crossing attack on each scheme. When the average power $\langle P_{\rm w}(t)\rangle$ approaches zero, the p value approaches 0.5 (thus the information leak converges zero) because the cross-correlation coefficient between the current and voltage also converges to zero.

Scheme	bit	$R_{\rm A}$ [Ω]	$R_{\rm B}$ [Ω]	$\langle P_{\rm w}(t)\rangle$ [10^{-3} W]	p	σ_p
KLJN	LH	1k	10k	0	0.5002	0.0091
	HL	10k	1k			
VMG-KLJN	LH	100	16.7k	0.026	0.5885	0.0022
	HL	16.7k	278			
	LH	278	278	0.471	0.7006	0.0053
	HL	46.4k	100			
	LH	100	6k	0.156	0.6281	0.0021
	HL	360k	2.2k			
FCK1-VMG-KLJN	LH	10k	10k	0	0.5028	0.0091
	HL	100k	1k			

attack similarly to the original KLJN scheme.

3.3.2 Transition

This concludes the zero-crossing attack presented in this dissertation. As a take-home message, thermal equilibrium is a requirement in the KLJN scheme. Now, we move onto the nonlinearity attack.

4. NONLINEARITY ATTACK AGAINST THE KIRCHHOFF-LAW-JOHNSON-NOISE (KLJN) SECURE KEY EXCHANGE PROTOCOL[5]

4.1 Nonlinearity

The noise generators of Alice and Bob have analog amplifiers as drivers. These have nonlinear characteristics [107]. We can model their output voltage by taking the Taylor Series approximation

$$U^*(t) = A\left[U(t) + BU^2(t) + CU^3(t) + ...\right], \tag{4.1}$$

where $U^*(t)$ is the output voltage of the generator, A is the linear amplification, $U(t)$ is the input noise voltage, and B and C are the second and third order nonlinearity coefficients, respectively.

Nonlinearity obviously distorts the amplitude distribution function and the Gaussianity of the noise sources. Vadai, Mingesz, and Gingl mathematically proved [59] that the KLJN scheme is secure only if the distribution of the noise voltages is Gaussian. Thus, nonlinearity is expected to cause information leak in these systems. It is an open question how much is this leak at practical conditions.

In this dissertation, we explore the effect of nonlinearity at the second order, third order, and a combination of the two orders. We also show that, as we decrease T_{eff}, the KLJN scheme approaches perfect security because the nonlinear components get negligibly small due to the reduced noise voltage.

4.2 The Nonlinearity Attack

The overview of the nonlinearity attack is shown in Figure 4.1. Alice's and Bob's key exchangers have a nonlinearity component to them, and Eve measures the power flow from Alice to Bob to guess the secure key bit situation.

[5]Part of this chapter is reprinted with permission from C. Chamon, S. Ferdous, and L. B. Kish, "Nonlinearity attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol" *Fluctuation and Noise Letters*, in press, 2021.

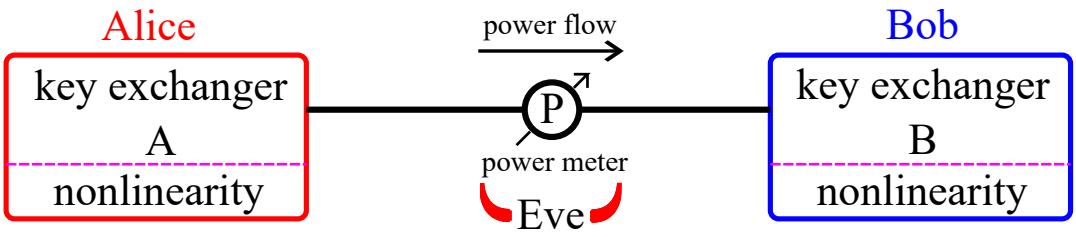


Figure 4.1: Overview of the nonlinearity attack. Alice's and Bob's key exchangers have a nonlinearity component to them, and Eve measures the power flow from Alice to Bob to guess the secure key bit situation.

For illustrative purposes, we use only the second and third order nonlinearities to account for the effects of the even and odd order nonlinearities. To quantify the nonlinearity, we use the total distortion, given by the sum of the normalized mean-square components:

$$\mathrm{TD} = \frac{\sqrt{\left\langle [BU^2(t)]^2 \right\rangle + \left\langle [CU^3(t)]^2 \right\rangle}}{\left\langle [U(t)]^2 \right\rangle}. \tag{4.2}$$

Eve measures the channel voltage and current, $U_{\mathrm{w}}(t)$ and $I_{\mathrm{w}}(t)$ (see Figure 1.2) and calculates the net power flow from Alice to Bob (see Equation (2.1)),

$$\langle P_{\mathrm{w}}(t) \rangle = \langle I_{\mathrm{w}}(t) U_{\mathrm{w}}(t) \rangle, \tag{4.3}$$

where the interpretation of voltage and current polarities are properly chosen for the direction of the power flow. Suppose the following protocol is publicly shared between Alice and Bob:

(i) If the net power flow is greater than zero, Eve surmises that HL is the secure bit situation;

(ii) If the net power flow is less than zero, Eve surmises that LH is the secure bit situation.

For example, in accordance with Equations (1.5) and (4.1) we conclude: In the case of positive nonlinear coefficients in Equation (4.1), the HL case means a higher mean-square voltage and a higher temperature at Alice's end, thus a positive power flow from Alice to Bob. If Eve extracts a

key, she can test that key or its inverse. One of them will be the true key. (For example, with proper negative coefficients, HL can imply a negative power flow, which would lead to the inverse key. If Eve, in accordance with Kerckhoffs's principle, knows the nonlinear coefficient in Equation (4.1), the inverse operation with the key is not needed.)

4.3 Demonstration

Computer simulations with Matlab measure the information leak with practical nonlinearity parameters in Equation (4.1). The tests show a significant amount of information leak, even with small nonlinearity.

The protocol is as follows:

- For each bit exchange, Eve measures and evaluates the average power at the information channel $\langle P_{\rm w}(t)\rangle$ (see Equation (4.3)).
- If the result is greater than zero, she guesses that HL is the secure bit situation;
- If the result is less than zero, she guesses that LH is the secure bit situation (see Section 4.2).
- The process above is independently repeated 1,000 times to obtain the statistics shown.

Out of the linear (Ideal) case, the investigated nonlinear situations are:

(a) case D_2 with second-order nonlinearity;

(b) case D_3 with third-order nonlinearity;

(c) case $\mathrm{D}_{2,3}$ with third-order nonlinearity;

Figure 4.2 illustrates the IU scatterplots between the wire voltage and current for the Ideal (a), D_2 (b), D_3 (c), and $\mathrm{D}_{2,3}$ (d) situations. The chosen parameters are $R_{\rm H} = 100$ kΩ, $R_{\rm L} = 10$ kΩ, $T_{\rm eff} = 10^{18}$ K, and $\Delta f_{\rm B} = 500$ Hz. At D_2, $B = 6 \times 10^{-3}$ and $C = 0$. At D_3, $B = 0$ and $C = 5 \times 10^{-5}$. At $\mathrm{D}_{2,3}$, $B = 1 \times 10^{-6}$ and $C = 5 \times 10^{-5}$. The blue circles represent the HL case, whereas the orange crosses represent the LH case.

The HL and LH situations are statistically indistinguishable in the Ideal (linear) situation, indicating perfect security.

In the D_2 case, the HL arrangement has an upward dominance, while the LH has a downward tendency. In the D_3 and $\mathrm{D}_{2,3}$ cases, the HL situation has a right-diagonal footprint, while the LH situation has a left-diagonal footprint. In conclusion, the nonlinear IU scatterplots indicate lack of security at the given conditions.

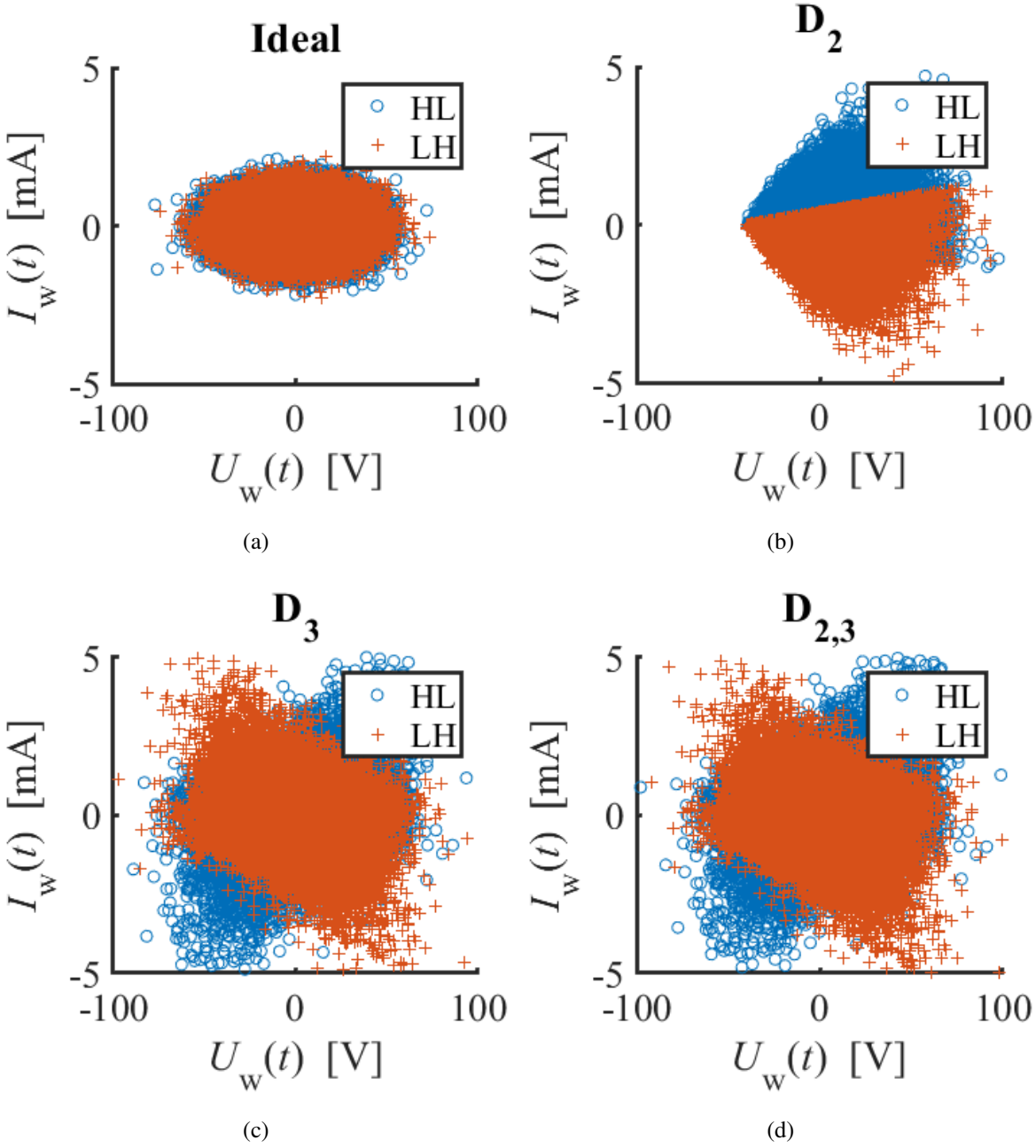


Figure 4.2: The IU scatterplots between the wire voltage and current for the ideal (a), D_2 (b), D_3 (c), and $\mathrm{D}_{2,3}$ (d) situations. The parameters chosen are $R_{\mathrm{H}} = 100$ kΩ, $R_{\mathrm{L}} = 10$ kΩ, $T_{\mathrm{eff}} = 10^{18}$ K, and $\Delta f_{\mathrm{B}} = 500$ Hz. At D_2, $B = 6 \times 10^{-3}$ and $C = 0$. At D_3, $B = 0$ and $C = 5 \times 10^{-5}$. At $\mathrm{D}_{2,3}$, $B = 1 \times 10^{-6}$ and $C = 5 \times 10^{-5}$. The blue circles represent the HL case, whereas the orange crosses represent the LH case. The HL and LH situations are statistically indistinguishable in the ideal situation. In the D_2 case, the HL arrangement has an upward dominance, while the LH has a downward tendency. In the D_3 and $\mathrm{D}_{2,3}$ cases, the HL situation has a right-diagonal trajectory, while the LH has a left-diagonal trajectory.

Table 4.1 shows the statistical run for Eve's probability p of correctly guessing the bit situations, and its standard deviation σ, for four different sample sizes (time steps) γ. For each nonlinearity situation, the p value increases as γ increases, as expected, due to the increasing accuracy of Eve's statistics.

Table 4.1: The statistical run for Eve's correct-guessing probability p and its standard deviation σ for four different sample sizes γ. For each nonlinearity situation, the p value increases as γ increases

D	γ	p	σ
2	10	0.5502	0.0135
	20	0.6172	0.0203
	100	0.7498	0.0149
	1000	0.9869	0.0042
3	10	0.5632	0.0159
	20	0.5982	0.0140
	100	0.7383	0.0126
	1000	0.9831	0.0047
2,3	10	0.5761	0.0114
	20	0.6106	0.0166
	100	0.7434	0.0137
	1000	0.9855	0.0037

Varying the effective temperature T_{eff} resulted in varying the effective voltage on the wire U_{w} (see Equation (1.5)). The statistical protocol with results shown in Table 4.1 was repeated for various effective temperatures.

Figure 4.3 illustrates Eve's correct-guessing probability p (top) and Eve's bit error ϵ (bottom), given by

$$\epsilon = 1 - p, \tag{4.4}$$

with respect to the effective wire voltage U_{w} for D_2 (a), D_3 (b), and $\mathrm{D}_{2,3}$ (c) for all sample sizes γ. As γ and U_{w} (that is, the effective temperature) decrease, p approaches perfect security.

Figure 4.4 shows p and ϵ vs. U_{w} at $\gamma = 1000$ for all the distortions. With the given parameters, convergence toward perfect security happened at D_2 before D_3 and $\mathrm{D}_{2,3}$.

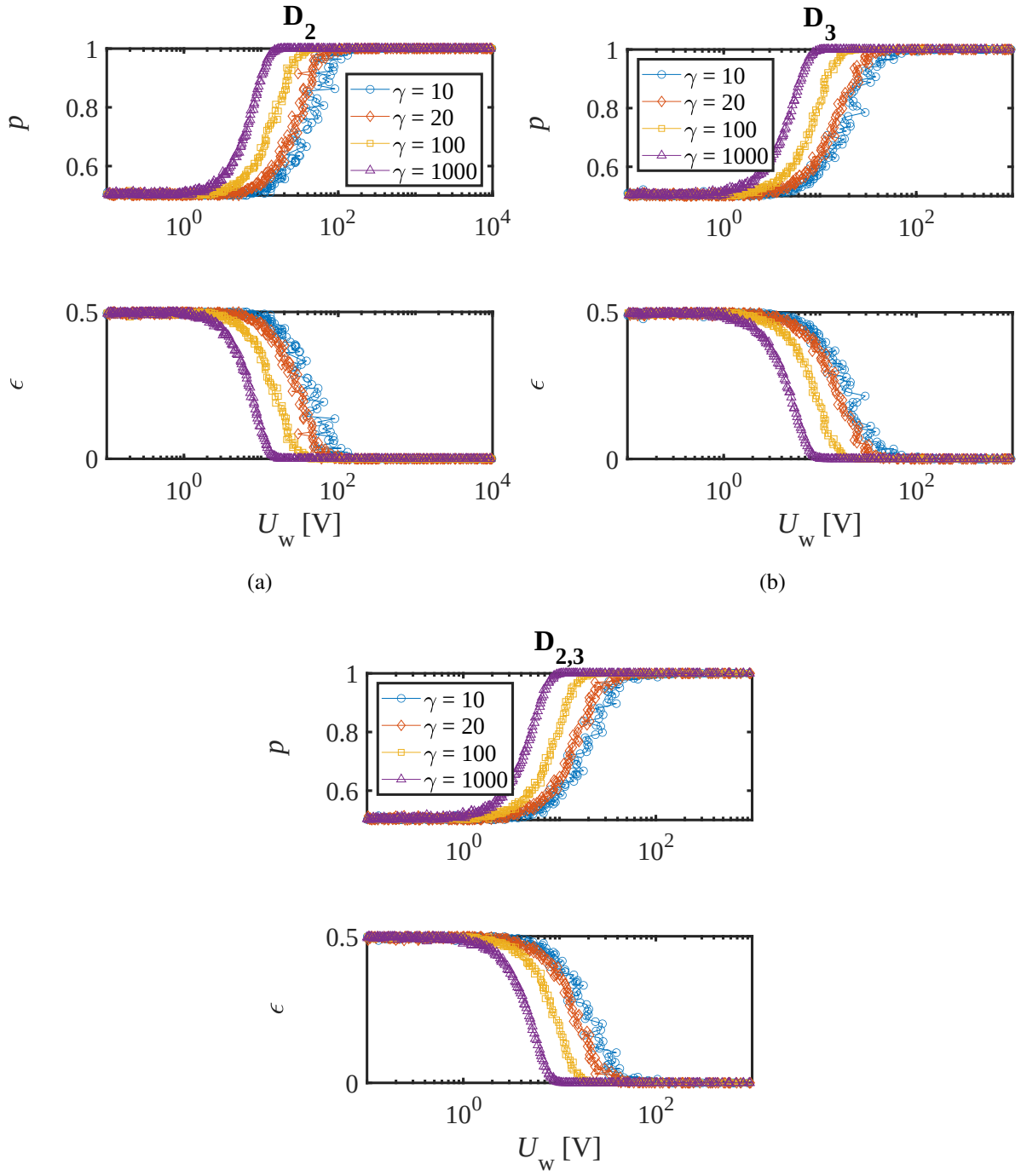


Figure 4.3: Eve's correct-bit-guessing probability p (top) and Eve's bit error ϵ (bottom) with respect to the effective voltage U_{w} for: D_2 (a), D_3 (b), and $\mathrm{D}_{2,3}$ at $\gamma = 10$ (blue), $\gamma = 20$ (orange), $\gamma = 100$ (yellow), and $\gamma = 1000$ (purple). As γ and U_{w} (driven by the effective temperature) decrease, p approaches perfect security.

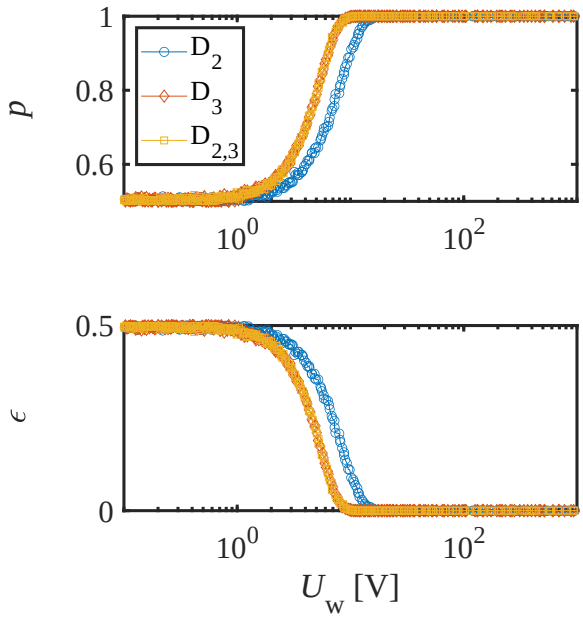


Figure 4.4: Eve's correct-bit-guessing probability p (top) and Eve's bit error ϵ (bottom) with respect to the effective voltage U_{w} at $\gamma = 1000$ for D_2, D_3, and $\mathrm{D}_{2,3}$. p increases and ϵ decreases as U_{w} (driven by the effective temperature) increases. Convergence to perfect security happens at D_2 before D_3 and $\mathrm{D}_{2,3}$.

Varying the effective temperature T_{eff} also resulted in varying the effective current on the wire I_{w}. Figure 4.5 illustrates Eve's correct-guessing probability p (top) and Eve's bit error ϵ (bottom, see Equation (4.4)), with respect to the effective wire current I_{w} for D_2 (a), D_3 (b), and $\mathrm{D}_{2,3}$ (c) for all sample sizes γ. As γ and I_{w} (that is the effective temperature) decrease, p approaches perfect security.

Figure 4.6 shows p and ϵ vs. I_{w} at $\gamma = 1000$ for all the distortions. With the given parameters, convergence toward perfect security happened at D_2 before D_3 and $\mathrm{D}_{2,3}$.

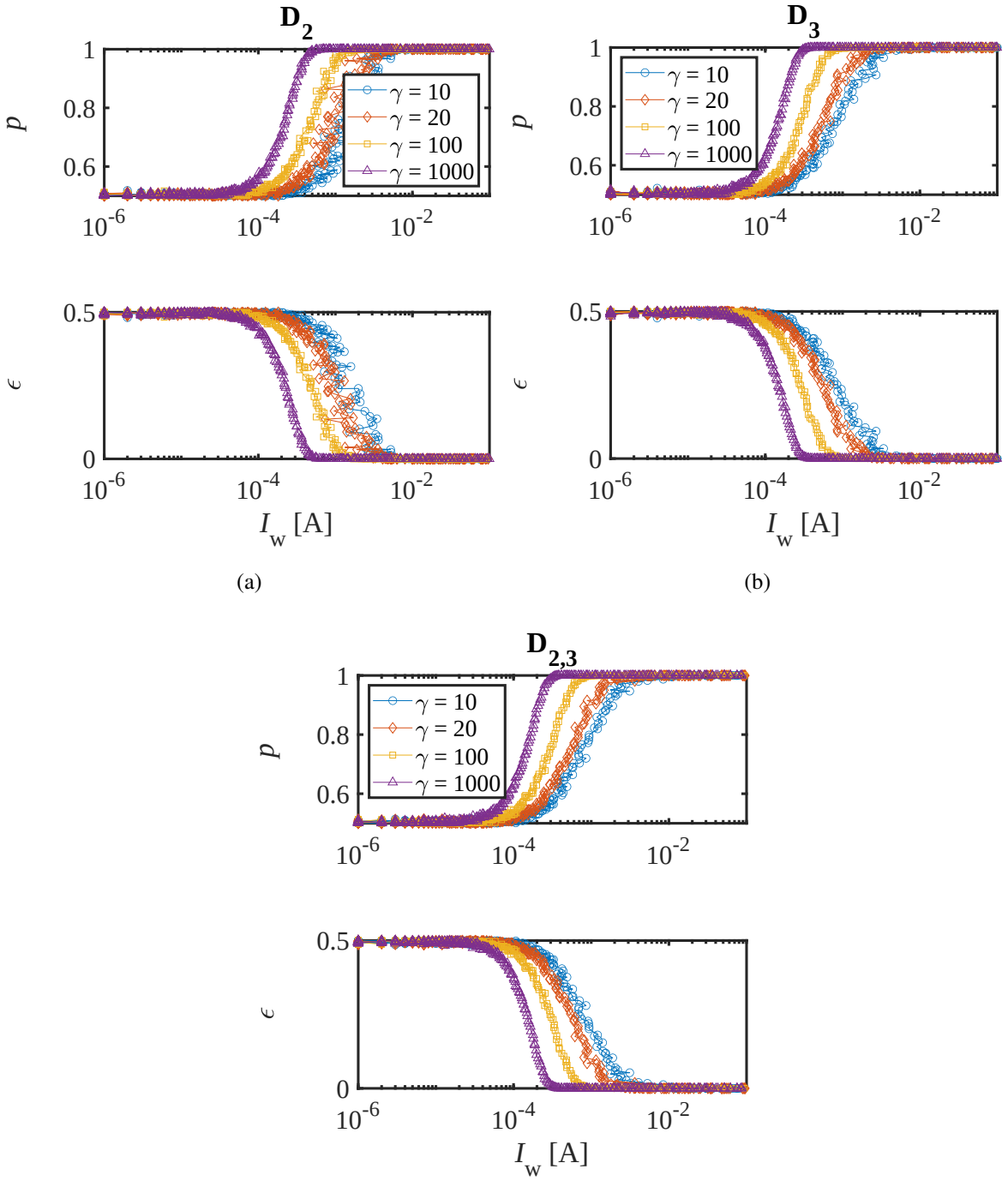


Figure 4.5: Eve's correct-bit-guessing probability p (top) and Eve's bit error ϵ (bottom) with respect to the effective current I_{w} for: D_2 (a), D_3 (b), and $\mathrm{D}_{2,3}$ at $\gamma = 10$ (blue), $\gamma = 20$ (orange), $\gamma = 100$ (yellow), and $\gamma = 1000$ (purple). As γ and I_{w} (driven by the effective temperature) decrease, p approaches perfect security.

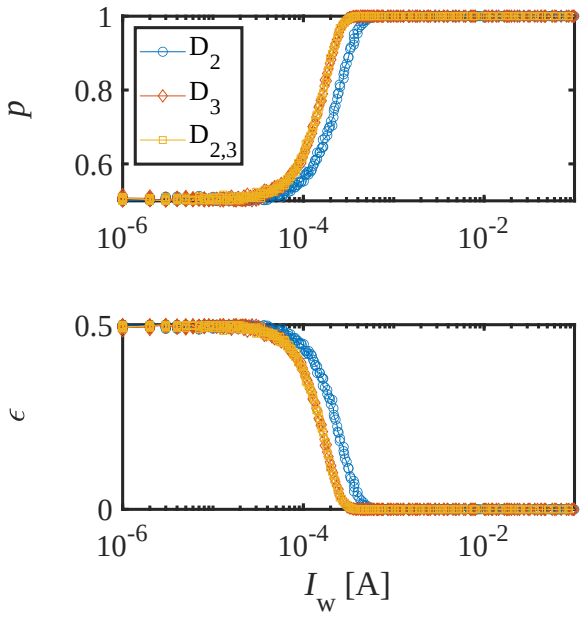


Figure 4.6: Eve's correct-bit-guessing probability p (top) and Eve's bit error ϵ (bottom) with respect to the effective current I_{w} at $\gamma = 1000$ for D_2, D_3, and $\mathrm{D}_{2,3}$. p increases and ϵ decreases as I_{w} (driven by the effective temperature) increases. Convergence to perfect security happened at D_2 before D_3 and $\mathrm{D}_{2,3}$.

4.3.1 Transition

This concludes the nonlinearity attack presented in this dissertation. As a take-home message, nonlinearity causes a nonzero power flow that leads to information leak. Now, we move onto our overall summary and conclusions.

5. SUMMARY AND CONCLUSIONS[1,2,4,5]

Secure key exchange protocols utilize random numbers, and compromised random numbers lead to information leak. So far, it had been unknown how Eve can utilize full or partial knowledge about the random number generators to attack the KLJN protocol. To demonstrate how compromised RNGs can be utilized by Eve, we have introduced four deterministic RNG attacks and four statistical RNG attacks on the KLJN scheme.

For the deterministic attacks, we showed that if Eve knows the root of both Alice's and Bob's RNGs, that is, when she exactly knows the random numbers, she can use Ohm's Law to crack the bit exchange. Eve can extract the bit very quickly, and she will learn the exchanged bit faster than Alice and Bob who know only their own random numbers. We showed that if Eve knows the seed of both Alice's and Bob's RNGs, that is, when she exactly knows the random numbers, she can crack the bit exchange even if her measurements have only one bit of resolution. The situation is similar to string verification in the noise-based logic systems. The cracking of the exchanged bit is exponentially fast; Eve can extract the bit within a fraction of the bit exchange period. Thus, Eve will learn the exchanged bit faster than Alice and Bob who know only their own random numbers.

We have also shown that if Eve knows the seed of only Alice's RNG, she can still crack the secure bit by using Ohm's Law or a process of elimination. However, she is required to utilize the whole bit exchange period.

---

[1]Part of this chapter is reprinted with permission from C. Chamon, S. Ferdous, and L. B. Kish, "Deterministic random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, vol. 20, no. 5, 2021. Copyright 2021 by World Scientific Publishing Company.

[2]Part of this chapter is reprinted with permission from C. Chamon, S. Ferdous, and L. B. Kish, "Statistical random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, accepted for publication, 2021. Copyright 2021 by World Scientific Publishing Company.

[4]Part of this chapter is reprinted with permission from C. Chamon, L. B. Kish, "Perspective–on the thermodynamics of perfect unconditional security," *Applied Physics Letters*, vol. 119, pp. 010501, 2021. Copyright 2021 by AIP Publishing.

[5]Part of this chapter is reprinted with permission from C. Chamon, S. Ferdous, and L. B. Kish, "Nonlinearity attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol" *Fluctuation and Noise Letters*, in press, 2021. Copyright 2021 by World Scientific Publishing Company.

No statistical evaluation is needed, except for in the rarely-occurring event that Eve does not know which RNG belongs to which resistor, which will render in a waiting/verification (no-response) time that has a negligible effect on Eve's cracking scheme.

For the statistical attacks, we explored various situations how RNGs compromised by statistical knowledge can be utilized by Eve. We have introduced four new attacks against the KLJN scheme. The defense against these attacks is the usage of true random number generators (with proper tamper resistance) at Alice's and Bob's sides.

It is important to note that:

- To utilize these attacks, we implicitly used Kerckhoffs's principle/Shannon's maxim [2], which means Eve knows all the fine details of the protocol, including how the seeds are utilized and the RNG outputs timed.

- This exploration was done assuming an ideal KLJN scheme. Future work would involve a practical circuit implementation or a cable simulator and related delays and transients.

- Deterministic and statistical knowledge of the random number(s) by Eve is a strong security vulnerability. However, it is an illustrative way how such attacks can be developed.

We introduced a new passive attack that extracts information from the VMG-KLJN system and successfully compromises its security. On the other hand, the standard KLJN and the FCK1-VMG-KLJN schemes are immune against this attack because their net power flow is zero due to their thermal equilibrium feature. Our results prove that thermal equilibrium is essential for the perfect security of KLJN schemes, including their VMG-KLJN variations. Therefore, the Second Law of Thermodynamics is the fundamental component of the security of the VMG-KLJN system, too.

Nevertheless, we believe that, with careful design and proper compromises, the VMG-KLJN scheme [51] has strong potential for applications in chip technology even if its security level is reduced compared to the features of original KLJN protocol. It is a security level that is sufficient for many practical applications but is reduced due to the deviation from the original KLJN.

Its FCK1-VMG-KLN version [52] virtually eliminates the information leak, but then only three resistors can be freely chosen.

Finally, we introduced a new passive attack against the KLJN secure key exchange scheme when nonlinearity is present in the transfer function of the amplifier stage of noise generators. We demonstrated the effect of a 1% total distortion at the second order (D_2), third order (D_3), and a combination of the two orders ($\mathrm{D}_{2,3}$) on the KLJN scheme.

We also demonstrated that, at a given nonlinear transfer characteristic, decreasing the effective voltage and, in this way reducing the nonlinearity, is a viable defense against the effect of nonlinearity in the KLJN scheme.

Our results showed that nonlinearity causes a notable power flow that leads to a significant information leak, so a careful design must be implemented such that the total distortion is kept at a minimum.

Alternatively, privacy amplification protocols [48, 50, 57, 99] can also be used. For example, as an active privacy amplification, Alice and Bob can also measure and compare the power flow and discard a proper fraction of high-risk bits [48, 50].

REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy systems," *Bell Systems Technical Journal* pp. 656-715, 1949.

[2] Y. Liang, H. V. Poor, S. Shamai, “Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, pp. 355-380, 2008.

[3] H.P Yuen, “Security of Quantum Key Distribution," *IEEE Access*, vol. 4, pp. 7403842, 2016.

[4] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, “Insecurity of detector-device-independent quantum key distribution," *Physical Review Letters*, vol. 117, no. 25, 2016.

[5] H. P. Yuen, “Essential elements lacking in security proofs for quantum key distribution," *Proc. SPIE*, vol. 8899, pp. 88990J–88990J-13, 2013.

[6] H. P. Yuen, “Essential lack of security proof in quantum key distribution," arXiv preprint, https://arxiv.org/abs/1310.0842, 2013.

[7] O. Hirota, “Incompleteness and limit of quantum key distribution theory," arXiv preprint, https://arxiv.org/abs/1208.2106, 2012.

[8] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, *New Journal of Physics*, vol. 16, 2014.

[9] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, *Nature Communications*, vol. 2, no. 349, pp. 1-6, 2011.

[10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[11] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurt-Siefer, “Experimentally faking the violation of Bell’s inequalities," *Physical Review Letters*, vol. 107, 2011.

[12] V. Makarov and J. Skaar, “Fakes states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert Protocols," *Quantum Information & Computation*, vol. 8, no. 6, pp. 622–635, 2008.

[13] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, “After-gate attack on a quantum cryptosystem," *New Journal of Physics*, vol. 13, 2011.

[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Thermal blinding of gated detectors in quantum cryptography, *Optics Express*, vol. 18, no. 26, pp. 27938–27954, 2010.

[15] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, “Device calibration impacts security of quantum key distribution," *Physical Review Letters*, vol. 107, 2011.

[16] L. Lydersen, J. Skaar, and V. Makarov, “Tailored bright illumination attack on distributed-phase-reference protocols," *Journal of Modern Optics*, vol. 58, no. 8, pp. 680–685, 2011.

[17] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, “Controlling a superconducting nanowire single-photon detector using tailored bright illumination," *New Journal of Physics*, vol. 13, 2011.

[18] L. Lydersen, V. Makarov, and J. Skaar, “Comment on “resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography"," *Applied Physics Letters*, vol. 98, 2011.

[19] P. Chaiwongkhot, K. B. Kuntz, Y. Zhang, A. Huang, J. P. Bourgoin, S. Sajeed, N. Lütkenhaus, T. Jennewein, and V. Makarov, “Eavesdropper’s ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence," *Physical Review A*, vol. 99, no. 6, 2019.

[20] G. Gras, N. Sultana, A. Huang, T. Jennewein, F. Bussières, V. Makarov, and H. Zbinden, “Optical control of single-photon negative-feedback avalanche diode detector," *Journal of Applied Physics*, vol. 127, 2020.

[21] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, “Laser-damage attack against optical attenuators in quantum key distribution," *Physical Review Applied*, vol. 13, 2020.

[22] A. Huang, Á. Navarrete, S. H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, “Laser-seeding attack in quantum key distribution," *Physical Review Applied*, vol. 12, 2019.

[23] V. Chistiakov, A. Huang, V. Egorov, and V. Makarov, “Controlling single-photon detector ID210 with bright light," *Optics Express*, vol. 27, no. 22, pp. 32253-32262 2019.

[24] A. Fedorov, I. Gerhardt, A. Huang, J. Jogenfors, Y. Kurochkin, A. Lamas-Linares, J. Å. Larsson, G. Leuchs, L. Lydersen, V. Makarov, and J. Skaar, “Comment on “inherent security of phase coding quantum key distribution systems against detector blinding attacks"," *Laser Physics Letters*, vol. 15, pp. 095203, 2018.

[25] A. Huang, S. Barz, E. Andersson, and V. Makarov, “Implementation vulnerabilities in general quantum cryptography," *New Journal of Physics*, vol. 20, pp. 103016, 2018.

[26] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J. P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, “Eavesdropping and countermeasures for backflash side channel in quantum cryptography," *Optics Express*, vol. 26, pp. 21020, 2018.

[27] A. Huang, S. H. Sun, Z. Liu, and V. Makarov, “Quantum key distribution with distinguishable decoy states," *Physical Review A*, vol. 98, pp. 012330, 2018.

[28] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, “Homodyne-detector-blinding attack in continuous-variable quantum key distribution," *Physical Review A*, vol. 98, pp. 012312, 2018.

[29] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Invisible Trojan-horse attack, *Scientific Reports*, vol. 7, 2017.

[30] P. Chaiwongkhot, S. Sajeed, L. Lydersen, and V. Makarov, “Finite-key-size effect in commercial plug-and-play QKD system," *Quantum Science and Technology*, vol. 2, no. 4, pp. 044003, 2017.

[31] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, “Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption," *IEEE Journal of Quantum Electronics*, vol. 52, no. 11, 2016.

[32] V. Makarov, J. P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, “Creation of backdoors in quantum communications via laser damage," *Physical Review A*, vol. 94, no. 3, 2016.

[33] S. Sajeed, P. Chaiwongkhot, J. P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, “Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch," *Physical Review A*, vol. 91, 2015.

[34] S. Sajeed, I. Radchenko, S. Kaiser, J. P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, “Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing," *Physical Review A*, vol. 91, 2015.

[35] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, “Risk analysis of Trojan-horse attacks on practical quantum key distribution systems," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 168-177, 2015.

[36] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, “Trojan-horse attacks threaten the security of practical quantum cryptography," *New Journal of Physics*, vol. 16, 2014.

[37] M. G. Tanner, V. Makarov, and R. H. Hadfield, “Optimised quantum hacking of superconducting nanowire single-photon detectors," *Optics Express*, vol. 22, pp. 6734, 2014.

[38] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, “Laser damage helps the eavesdropper in quantum cryptography," *Physical Review Letters*, vol. 112, no. 7, 2014.

[39] Q. Liu, A. Lamas-Linares, C. Kurtsiefer, J. Skaar, V. Makarov, and I. Gerhardt, “A universal setup for active control of a single-photon detector," *The Review of Scientific Instruments*, vol. 85, pp. 013108, 2014.

[40] C. Chamon, L. B. Kish, “Perspective–on the thermodynamics of perfect unconditional security," *Applied Physics Letters*, vol. 119, pp. 010501, 2021.

[41] C. Chamon, S. Ferdous, and L.B. Kish, “Random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," arXiv preprint, https://arxiv.org/abs/2005.10429, 2020.

[42] C. Chamon, S. Ferdous, and L. B. Kish, “Deterministic random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, vol. 20, no. 5, 2021.

[43] C. Chamon, S. Ferdous, and L. B. Kish, “Statistical random number generator attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, accepted for publication, 2021.

[44] C. Chamon, S. Ferdous, and L. B. Kish, “Nonlinearity attack against the Kirchhoff-law-Johnson-noise secure key exchange protocol," *Fluctuation and Noise Letters*, in press, 2021.

[45] L. B. Kish, The Kish Cypher: The Story of KLJN for Unconditional Security, New Jersey: World Scientific, 2017.

[46] L. B. Kish, “Totally secure classical communication utilizing Johnson (-like) noise and Kirchhoff’s law," *Physics Letters A*, vol. 352, no. 3, pp. 178-182, 2006.

[47] A. Cho, “Simple noise may stymie spies without quantum weirdness," *Science*, vol. 309, no. 5744, pp. 2148, 2005.

[48] L. B. Kish and C. G. Granqvist, “On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator," *Quantum Information Processing*, vol. 13, no. 10, pp. 2213-2219, 2014.

[49] L. B. Kish, “Enhanced secure key exchange systems based on the Johnson-noise scheme," *Metrology and Measurement Systems*, vol. 20, no. 10, pp. 191-204, 2013.

[50] L. B. Kish and T. Horvath, “Notes on recent approaches concerning the Kirchhoff-law–Johnson-noise based secure key exchange," *Physics Letters A*, vol. 373, pp. 2858-2868, 2009.

[51] G. Vadai, R. Mingesz, and Z. Gingl, “Generalized Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system using arbitrary resistors," *Scientific Reports*, vol. 5, 2015.

[52] S. Ferdous, C. Chamon, and L. B. Kish, “Comments on the “generalized" KJLN key exchanger with arbitrary resistors: power, impedance, security," *Fluctuation and Noise Letters*, vol. 20, pp. 2130002, 2020.

[53] L. B. Kish and C. G. Granqvist, “Random-resistor-random-temperature Kirchhoff-law-Johnson-noise(RRRT -KLJN) key exchange," *Metrology and Measurement Systems*, vol. 23, pp. 3-11, 2016.

[54] J. Smulko, “Performance analysis of the ‘intelligent’Kirchhoff’s-law–Johnson-noise secure key exchange," *Fluctuations and Noise Letters*, vol. 13, pp. 1450024, 2014.

[55] R. Mingesz, Z. Gingl, and L. B. Kish, “Johnson(-like)-noise-Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line," *Physics Letters A*, vol. 372, pp. 978–984, 2008.

[56] R. Mingesz, L. B. Kish, Z. Gingl, C. G. Granqvist, H. Wen, F. Peper, T. Eubanks, and G. Schmera, “Unconditional security by the laws of classical physics," *Metrology and Measurement Systems*, vol. 20, pp. 3–16, 2013.

[57] T. Horvath, L. B. Kish, and J. Scheuer, “Effective privacy amplification for secure classical communications," *EPL*, vol. 94, pp. 28002, 2011.

[58] Y. Saez and L. B. Kish, “Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange," *PLoS ONE*, vol. 8, no. 11, 2013.

[59] R. Mingesz, G. Vadai, and Z. Gingl, “What kind of noise guarantees security for the Kirchhoff-loop-Johnson-noise key exchange?" *Fluctuation and Noise Letters*, vol. 13, no. 3, pp. 1450021, 2014.

[60] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, “Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law-Johnson-noise secure key exchange," *Journal of Computational Electronics*, vol. 13, pp. 271–277, 2014.

[61] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, “Bit errors in the Kirchhoff-law-Johnson-noise secure key exchange," *International Journal of Modern Physics: Conference Series*, vol. 33, pp. 1460367, 2014.

[62] Z. Gingl and R. Mingesz, “Noise properties in the ideal Kirchhoff-law-Johnson-noise secure communication system," *PLoS ONE*, vol. 9, no. 4, 2014.

[63] P. L. Liu, “A key agreement protocol using band-limited random signals and feedback," *IEEE Journal of Lightwave Technology*, vol. 27, no. 23, pp. 5230-5234, 2009.

[64] L. B. Kish and R. Mingesz, “Totally secure classical networks with multipoint telecloning (teleportation) of classical bits through loops with Johnson-like noise," *Fluctuation and Noise Letters*, vol. 6, no. 2, pp. C9–C21, 2006.

[65] L. B. Kish, “Methods of using existing wire lines (power lines, phone lines, internet lines) for totally secure classical communication utilizing Kirchoff’s law and Johnson-like noise," arXiv preprint, https://arxiv.org/abs/physics/0610014, 2006.

[66] L. B. Kish and F. Peper, “Information networks secured by the laws of physics," *IEICE Transactions on the Fundamentals of Communications, Electronics, Information, and Systems*, vol. E95–B, no. 5, pp. 1501-1507, 2012.

[67] E. Gonzalez, L. B. Kish, R. S. Balog, and P. Enjeti, “Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters," *PloS One*, vol. 8, no. 7, 2013.

[68] E. Gonzalez, L. B. Kish, and R. Balog, “Encryption Key Distribution System and Method," U.S. Patent #US9270448B2 , https://patents.google.com/patent/US9270448B2, 2016.

[69] E. Gonzalez, R. Balog, R. Mingesz, and L. B. Kish, “Unconditional security for the smart power grids and star networks," *23rd International Conference on Noise and Fluctuations (ICNF 2015)*, Xian, China, June 2-5, 2015.

[70] E. Gonzalez, R. S. Balog, and L. B. Kish, “Resource requirements and speed versus geometry of unconditionally secure physical key exchanges," *Entropy*, vol. 17, no. 4, pp. 2010–2014, 2015.

[71] E. Gonzalez and L. B. Kish, “Key exchange trust evaluation in peer-to-peer sensor networks with unconditionally secure key exchange," *Fluctuation and Noise Letters*, vol. 15, pp. 1650008, 2016.

[72] L. B. Kish and O. Saidi, “Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives," *Fluctuation and Noise Letters*, vol. 8, pp. L95–L98, 2008.

[73] L. B. Kish, K. Entesari, C. G. Granqvist, and C. Kwan, “Unconditionally secure credit/debit card chip scheme and physical unclonable function," *Fluctuation and Noise Letters*, vol. 16, pp. 1750002, 2017.

[74] L. B. Kish and C. Kwan, “Physical unclonable function hardware keys utilizing Kirchhoff-law-Johnson noise secure key exchange and noise-based logic," *Fluctuation and Noise Letters*, vol. 12, pp. 1350018, 2013.

[75] Y. Saez, X. Cao, L. B. Kish, and G. Pesti, “Securing vehicle communication systems by the KLJN key exchange protocol," *Fluctuation and Noise Letters*, vol. 13, pp. 1450020, 2014.

[76] X. Cao, Y. Saez, G. Pesti, and L. B. Kish, “On KLJN-based secure key distribution in vehicular communication networks," *Fluctuation and Noise Letters*, vol. 14, pp. 1550008, 2015.

[77] L. B. Kish and C. G. Granqvist, “Enhanced usage of keys obtained by physical, unconditionally secure distributions," *Fluctuation and Noise Letters*, vol. 14, pp. 1550007, 2015.

[78] P. L. Liu, “A complete circuit model for the key distribution system using resistors and noise sources," *Fluctuation and Noise Letters*, vol. 19, pp. 2050012, 2020.

[79] M. Y. Melhem and L. B. Kish, “Generalized DC loop current attack against the KLJN secure key exchange scheme," *Metrology and Measurement Systems*, vol. 26, pp. 607-616, 2019.

[80] M. Y. Melhem and L. B. Kish, “A static-loop-current attack against the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system," *Applied Sciences*, vol. 9, pp. 666, 2019.

[81] M. Y. Melhem and L. B. Kish, “The problem of information leak due to parasitic loop currents and voltages in the KLJN secure key exchange scheme," *Metrology and Measurement Systems*, vol. 26, pp. 37-40, 2019.

[82] M. Y. Melhem and L. B. Kish, “Man in the middle and current injection attacks against the KLJN key exchanger compromised by DC sources," *Fluctuation and Noise Letters*, vol. 20, no. 2, pp. 2150011, 2021.

[83] M. Y. Melhem, C. Chamon, S. Ferdous, L. B. Kish, “Alternating (AC) Loop Current Attacks against the KLJN Secure Key Exchange Scheme," *Fluctuation and Noise Letters*, 2021.

[84] P. L. Liu, “Re-examination of the cable capacitance in the key distribution system using resistors and noise sources," *Fluctuation and Noise Letters*, vol. 16, pp. 1750025, 2017.

[85] H. P. Chen, M. Mohammad, and L. B. Kish, “Current injection attack against the KLJN secure key exchange," *Metrology and Measurement Systems*, vol. 23, pp. 173-181, 2016.

[86] G. Vadai, Z. Gingl, and R. Mingesz, “Generalized attack protection in the Kirchhoff-law-Johnson-noise key exchanger," *IEEE Access*, vol. 4, pp. 1141-1147, 2016.

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

[88] L. B. Kish and C. G. Granqvist, “Elimination of a second-law-attack, and all cable-resistance-based attacks, in the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system," *Entropy*, vol. 16, pp. 5223-5231, 2014.

[89] L. B. Kish and J. Scheuer, “Noise in the wire: the real impact of wire resistance for the Johnson (-like) noise based secure communicator," *Physics Letters A*, vol. 374, pp. 2140-2142, 2010.

[90] F. Hao, “Kish’s key exchange scheme is insecure," *IEE Proceedings - Information Security*, vol. 153, no. 4, pp. 141-142, 2006.

[91] L. B. Kish, Response to Feng Hao’s paper “Kish’s key exchange scheme is insecure," *Fluctuation and Noise Letters*, vol. 6, pp. C37-C41, 2006.

[92] L. B. Kish, “Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson (-like)-noise cipher and expansion by voltage-based security," *Fluctuation and Noise Letters*, vol. 6, pp. L57-L63, 2006.

[93] L. J. Gunn, A. Allison, and D. Abbott, “A new transient attack on the Kish key distribution system," *IEEE Access*, vol. 3, pp. 1640-1648, 2015.

[94] L. B. Kish and C. G. Granqvist, “Comments on “a new transient attack on the Kish key distribution system"," *Metrology and Measurement Systems*, vol. 23, pp. 321-331, 2015.

[95] L. J. Gunn, A. Allison, and D. Abbott, “A directional wave measurement attack against the Kish key distribution system," *Scientific Reports*, vol. 4, pp. 6461, 2014.

[96] H. P. Chen, L. B. Kish, and C. G. Granqvist, “On the “cracking" scheme in the paper “a directional coupler attack against the Kish key distribution system" by Gunn, Allison and Abbott," *Metrology and Measurement Systems*, vol. 21, pp. 389-400, 2014.

[97] H. P. Chen, L. B. Kish, C. G. Granqvist, and G. Schmera, “Do electromagnetic waves exist in a short cable at low frequencies? What does physics say?" *Fluctuation and Noise Letters*, vol. 13, pp. 1450016, 2014.

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

[99] L. B. Kish, D. Abbott, and C. G. Granqvist, “Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme," *PloS One*, vol. 8, no. 12, 2013.

[100] R. Halprin and M. Naor, Games for extracting randomness, *Proc. SOUPS*, New York, NY, USA, 2009.

[101] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Cryptanalytic attacks on pseudorandom number generators," *Fast Software Encryption*, Springer-Verlag Berlin Heidelberg, vol. 1372, pp. 168–188, 1998.

[102] I. Goldberg and D. Wagner, “Randomness and netscape browser," *Dr. Dobb’s Journal*, 1996.

[103] L. Dorrendorf, Z. Gutterman, and B. Pinkas, “Cryptanalysis of the Windows random number generator," *Proc. CCS*, New York, NY, USA, 2007.

[104] E. Barker and J. Kelsey, *Recommendation for random number generation using deterministic random bit generators*, Gaithersburg, MD, USA: NIST (2012).

[105] K. Nohl, D. Evans, S. Starbug, and H. Plötz, “Reverse-engineering a cryptographic RFID tag," *Proc. SS*, San Jose, CA, USA, 2008.

[106] L. Kish, S. Khatri, and T. Horvath, “Computation using noise-based logic: efficient string verification over a slow communication channel," *The European Physical Journal B*, vol. 79, pp. 85–90, 2011.

[107] B. Razavi, RF Microelectronics, Prentice Hall, 2011.