Analog Cancellation of a Known Remote Interference: Hardware Realization and Analysis

James M. Doty, Robert W. Jackson, *Fellow, IEEE,* and Dennis L. Goeckel, *Fellow, IEEE*

***Abstract*—The onset of quantum computing calls for secrecy schemes that can provide everlasting secrecy resistant to increased computational power of an adversary. One novel physical layer scheme proposes that an intended receiver capable of performing analog cancellation of a known key-based interference would hold a significant advantage in recovering small underlying messages versus an eavesdropper performing cancellation after analog-to-digital conversion. This advantage holds even if an eavesdropper later obtains the key and employs it in their digital cancellation. Inspired by this scheme, a flexible software-defined radio receiver design capable of maintaining analog cancellation ratios over 40 dB, reaching up to and over 50 dB, is implemented. Using analog cancellation levels from the hardware testbed, practical everlasting secrecy rates up to 2.0 bits/symbol are shown to be gained by receivers performing interference cancellation in analog rather than on a digital signal processor.**

***Index Terms*—Interference rejection techniques; Security, privacy, and authentication; Software radio**

I. Introduction

SECURITY is a key challenge in wireless communication systems. In the standard model, there are three entities: Alice - the transmitter; Bob - the intended recipient; and Eve - an adversary eavesdropper. Most security is obtained by encryption, where Alice's information is encrypted at a data level based on a key such that the transformation can be easily undone by a key-informed Bob, but a key-uninformed Eve would need to perform computational processing well beyond current capabilities to recover the information. However, Alice cannot guarantee her information is protected indefinitely via encryption: an adversary who records the ciphertext and then either: (i) obtains the key at some point after message transmission; or, (ii) is able to employ significant advances in computation (e.g., quantum computation), can readily obtain the message text. Hence, if a user desires everlasting secrecy, cryptography is insufficient [1] [2].

Information-theoretic secrecy considers adversaries with unlimited computation and has been extensively studied since Wyner's work on wiretap coding [3]. Unfortunately, the secrecy obtained through wiretap coding only holds when the intended receiver, Bob, has some advantage, such as a higher received power, over the eavesdropper, Eve. This cannot generally be guaranteed, as the position of Eve is often unknown and could be near the transmitter (a "near Eve" scenario).

Physical-layer techniques have been introduced to address the "near Eve" scenario [4]. Cooperative jamming, which employs the transmission of a large interference that is based on a shared key known by the jammer and Bob, allows Bob to exploit his knowledge to employ interference cancellation on their received signal [5]. The powerful uncanceled interferer acts as an additional noise source in Eve's reception, masking the much lower power information signal that they are attempting to recover. Performing cancellation of the interferer at the intended receiver is a critical requirement of the approach.

Interference cancellation encapsulates two distinct methodologies which can be used in isolation or conjunction. Analog cancellation often takes place at radio-frequency (RF) before downconversion and digitization by an analog-to-digital converter (ADC). Digital cancellation occurs in the discrete domain following conversion by an ADC. Work in known-interference cancellation for cooperative jamming has focused on architectures that employ digital cancellation, but full-duplex receiver research has demonstrated effective analog and hybrid analog/digital cancellation methods [6]. Analog cancellation requires the additional step of interpolating and upconverting the generated cancellation signal for RF cancellation, increasing complexity of the receiver design and adding another source of synchronization error.

However, implementing analog cancellation before an ADC has significant advantages. It has been shown that the nonlinearity and finite resolution of an ADC - strict hardware limitations - can be exploited by transmitting a message signal of interest (SoI) in the presence of a much larger interference that is capable of saturating an eavesdropper's ADC. Forcing the eavesdropping ADC to operate at its full dynamic range leads to loss and distortion of the lower energy SoI. This non-invertible and thus permanent deformation of signal provides everlasting secrecy even under the scenario in which an eavesdropper is able to obtain the key at a later time and utilize it to attempt to decode the message from their digitized copy of the original transmission [2].

Utilizing software-defined radios (SDRs), we implement a hardware testbed demonstrating analog interference cancellation of a known remote interferer received across an unknown wireless communication channel. Using this system, empirical results for cancellation ratios have been found for a binary phase-shift keying (BPSK) modulated interference and are used to calculate everlasting secrecy rates [2].

This work has been supported by the National Science Foundation under grant ECCS-2029323.

J. Doty was with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, USA. He is now with The MITRE Corporation, Bedford, MA, USA. The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author. Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-2811.

R. Jackson and D. Goeckel are with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, USA.

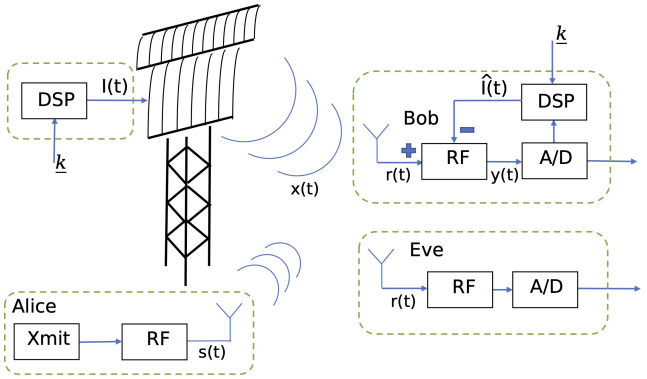


Fig. 1: The message signal transmitted from Alice, $s(t)$, is hidden by the much larger interference, $I(t)$. Having knowledge of the shared key used to generate the interference, $\underline{k}$, Bob is capable of estimating the interference, $\hat{I}(t)$, to perform analog cancellation before their ADC. Conversely, Eve's ADC is not protected from saturation by cancellation, resulting in a compressed reception of the message.

Contributions of this work:

1) *Analog cancellation of a remote interferer:* We demonstrate analog cancellation of a remote interferer and determine the degree of cancellation. Analog cancellation has previously been demonstrated for full-duplex transceivers; in that scenario, the canceller has the advantage of a known reference oscillator and a more stable interference level. In this work, the interference is generated by a separate transmitter that has its own reference oscillator and arrives at the receiver through an unknown wireless channel.
2) *Extension and evaluation of the security algorithm in [1], [2]*: We put forward a radar "jammer" for [2]. More importantly, by considering how well receiver Bob can cancel a known remote interferer, we are able to evaluate the potential performance of the scheme of [2].

II. System Overview

Figure 1 shows the system operation during transmission of the SoI. Unlike prior works in cooperative jamming, during message transmission the interference cancellation takes place prior to digitization by the intended receiver's ADC. The cooperative jammer and intended receiver must generate their interference and cancellation signals, $I(t)$ and $\hat{I}(t)$, simultaneously based on the shared key, $\underline{k}$. Bob and Eve will receive a combination of the SoI, $s(t)$, from Alice and separately transmitted interference distorted by channel effects. This combination of signals in the air is:

$$x(t) = s(t) + I(t). \tag{1}$$

We consider a BPSK-modulated signal generated from the shared key as the interference $I(t)$. The bandwidth is assumed small enough to yield a frequency-nonselective channel; hence,

$$r(t) = h_s s(t-\tau_s)e^{j2\pi(t-\tau_s)f_s} + h_i I(t-\tau_i)e^{j2\pi(t-\tau_i)f_i} + n(t), \tag{2}$$

where $r(t)$ is the RF signal at the receiver assuming AWGN $n(t)$. The parameters h_s and τ_s as well as h_i and τ_i are the complex gains and real time delays of the SoI and interference channels, respectively. The carrier frequencies f_s and f_i of the two transmitters may be offset by a small amount from what the receiver assumed.

A synchronization and channel estimation period is adopted prior to transmission of the interference and SoI. This will be referred to as the "learning period," during which the transmitter sends a cyclic transmitted learning sequence, $I_l(t)$, while no SoI is present. The intended receiver iterates over the learning sequence to model the channel parameters. The received signal $r_l(t)$ during this period is:

$$r_l(t) = h_i I_l(t-\tau_i)e^{j2\pi(t-\tau_i)f_i} + n(t). \tag{3}$$

Then, at a predetermined time, both the interference transmitter and receiver switch over from the learning sequence to the key-based interference sequence. Simultaneously, the message transmitter will begin transmitting a low-power SoI, $s(t)$, alongside the interference. With the learned channel model, the receiver is able to maintain cancellation of the interference and receive the uncompressed SoI.

Eavesdropper Eve is just as capable as the receiver Bob but lacks knowledge of the single-use key-based large interferer and hence is unable to perform real-time analog cancellation. In particular, the interference is generated from the shared ephemeral cryptographic key in the same manner that the jamming sequence is generated in [2] (e.g., via a stream cipher). Even if Eve were able to perfectly observe the interference sequence, it is no easier to obtain the shared key and predict the interference than to break a standard cryptographic algorithm. Given the short duration of message transmission, this is well beyond any reasonable Eve's capabilities. Since Eve's receiver is saturated by the interference, even perfect digital cancellation can only operate on a signal that has been significantly degraded by the quantization noise of the ADC.

We further note that it is not the power of the interferer that is important; it is the dynamic range of the combined jammer and signal. Even if a weak combined signal reached both Eve and Bob, Bob would cancel the jammer and increase the receiver gain enough to decode the signal. Eve cannot cancel the jammer, and thus cannot increase gain as much without saturating the system. The lower gain leaves the relatively small signal of interest contaminated by quantization noise.

III. Hardware Testbed

The testbed is shown in Figure 2. It features two USRP B210 SDRs. The B210 employs two pairs of 12-bit ADCs and DACs. Each of the four channels have individually tunable gain and frequency settings. The USRP B210 must be connected to a host PC, where most of the digital sample processing occurs. The transmitter and receiver (see Figure 2) each use a Mini-Circuits ZFSC-2-11+ RF splitter/combiner to combine signals and utilize reference output signal of seperate Keysight N9000B signal analyzers. Stable references are required to minimize carrier frequency drift, the effects of which will be discussed later. Sample generation, processing, and radio control is handled via GNURadio, an open source radio environment that can be implemented via GNURadio companion, C++, or Python programming languages.

The repeated learning pattern is a 16-bit BPSK sequence modulated and upconverted to the carrier frequency. Results for 100 MHz and 1 GHz carriers are presented. Data for the 1 GHz carrier is for a wireless channel with radios about 10 feet apart. Results using a 100 MHz carrier employ a coaxial cable channel due to cancellation ratios being limited by propagation rather than estimation error. The interference signal has a 94 kHz bandwidth at a 3 MHz baseband sample rate. The oversampling allowed for improved time domain resolution and for the system to operate assuming a frequency non-selective (flat) fading channel in wireless testing.

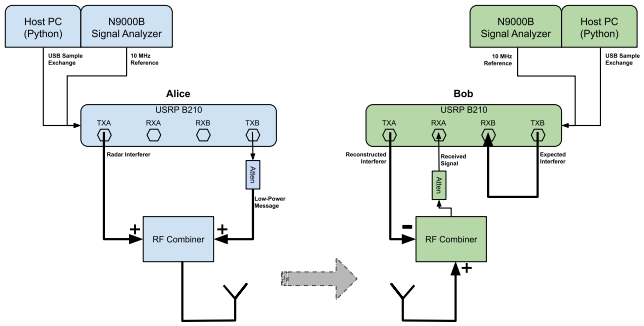


Fig. 2: Testbed hardware diagram: Each B210 SDR uses its own host PC and reference source, hence yielding isolation from one another. Intended receiver, Bob, loops an analog copy of the expected interference out and back into one of their receivers to solve an indeterminate sample timing delay issue introduced by the single-stream USB interface.

In order for Bob to create an effective cancellation signal, Alice must send an interference signal that accurately resembles what Bob assumes. The Alice B210 settings are crucial for this. The transmitter SNR must be large and the transmit power must be backed off from saturation to maintain linearity. In these experiments, the transmitter has been backed off by roughly 20 dB. In a more realistic situation, an radar transmitter would be operated closer to saturation, but with power amplifier pre-distortion [7] to ensure signal integrity.

IV. Receiver Design and Implementation

Fine synchronization of carrier frequency offset and channel parameters is accomplished by digital signal processing of the learning sequence. The signal used for cancellation is an estimate of the last term in (2):

$$\hat{I}(t) = \hat{h}I(t-\hat{d})e^{j2\pi(t-\hat{d})(f_r+f_o)}, \tag{4}$$

where f_r is the receiver local oscillator frequency and the terms f_o, $\hat{d}$, and $\hat{h}$ are determined as described below.

The transmitter and receiver oscillators will have an innate offset that must be compensated. The offset is estimated using a Costas Loop, a second order phase locked loop (PLL) [8]. The offset estimate, f_o, is employed by the receiver to frequency shift the baseband signals before and after upconversion and downconversion, respectively.

The channel effects on the interference can be described by a time delay d_i and a complex channel gain h_i. The time delay of the channel is largely dependent on the physical distance between transmitter and receiver and thus will not change

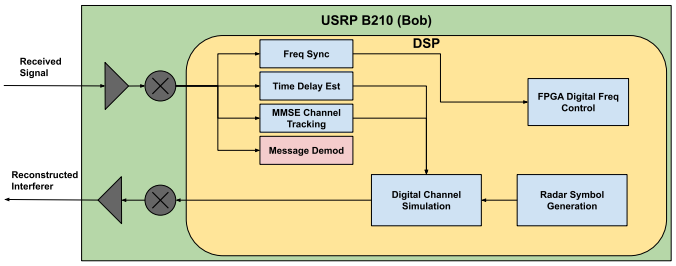


Fig. 3: Flow graph of the intended receiver's signal processing.

rapidly over time; hence, a single estimate is sufficient. The channel time delay estimate, $\hat{d}$, is calculated by maximizing the correlation function of the digitized learning sequence before cancellation and the digital signal expected to be received:

$$\hat{d} = \arg\max_{d} \frac{1}{M} \sum_{n=1}^{M*N} r_l[n] * I_l[n-d], \tag{5}$$

where $r_l[n] = r_l(nT_s/M)$, $I_l[n] = I_l(nT_s/M)$, T_s is the radio sample period, M is an interpolation factor greater than one, and N is the period of the cyclic learning sequence in samples before interpolation. Interpolating the signals allows the estimator to measure a sub-sample period delay.

The channel time delay is not an exact multiple of the sampling period, which results in a floating point estimate $\hat{d}$. To implement sub-sample period time delays, a band-limited digital fractional-delay filter (FDF) is used. This design utilizes a finite impulse response approximation of the Nyquist-Shannon ideal FDF for a fractional delay, $d_f = \hat{d} - \lfloor \hat{d} \rfloor$, between 0 and 1. The FDF impulse response is [9] [10]:

$$h_f[n, d_f] = \text{sinc}[n - d_f] = \frac{\sin[(n-d_f)\pi]}{(n-d_f)\pi}. \tag{6}$$

There is no perfect digital implementation for non-bandlimited filters, and the approximation introduces inter-symbol interference (ISI). ISI results in a reduction in cancellation capability based on the fractional delay that is required [11].

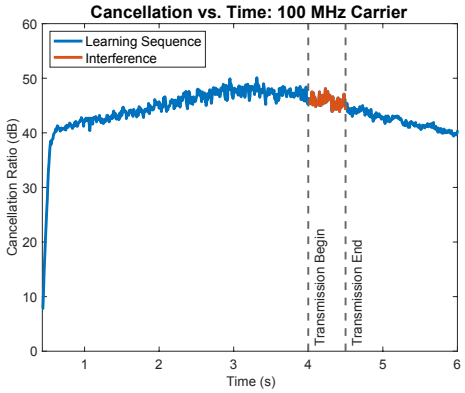
The attenuation and phase delay of the received signal are influenced by environmental changes due to multipath and thus vary more rapidly than the time delay. The complex gain of the fading channel is iteratively estimated as $\hat{h}$ from the residual signal by the learning rule:

$$\hat{h}_{N+1} = \hat{h}_N + \alpha[y(nT_s t) * I_l(nT_s t)^*]. \tag{7}$$

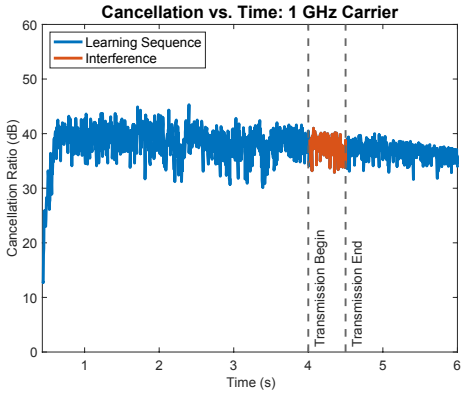
The learning rate α, bounded on [0,1], controls how quickly the gain estimate can track a changing channel [12] [13].

V. Cancellation Capability and Limitations

As shown in Figure 4, peak cancellation ratios for the 100 MHz and 1 GHz carriers of 52 dB and 42 dB were observed, respectively. Cancellation for either frequency varied over time, but could be maintained over 40 dB and 30 dB, respectively, for a few seconds. Highlighted by the orange sections of Figure 4, cancellation is maintained across the predetermined transmitter switch between the cyclic learning sequence and key-based interference, which protects the transmitted message for the short duration needed for messages



(a)



(b)

Fig. 4: Cancellation ratio versus time plotted for (a) the 100 MHz carrier and (b) the 1 GHz carrier. The time axis begins at the start of delay and channel estimation, but follows the carrier frequency estimation period. The window of time highlighted from 4 to 4.5 seconds shows where the both transmitter and receiver simultaneously switch from the learning sequence to the shared-key based interference masking the SoI.

requiring this extreme level of security. This is crucial. If Eve is able to learn the key as the pattern is repeatedly transmitted, then the advantage Bob and Alice hold over Eve is lost. While we are unaware of other analog remote interference cancellation schemes, analog cancellation schemes for self interference cancellation achieved cancellation levels of 25 dB [14] and, in a more complex multi-tap scheme, 35 dB [15]. Signals levels in those cases were output from saturated power amplifiers and thus had more nonlinear behavior than the cases we consider in our configurations.

Figure 5 compares the power spectral density of the received signal before (blue) and after (black) cancellation for the 1 GHz carrier during peak cancellation. Without cancellation, the SoI can be hidden from Eve by the more powerful interference (blue). A receiver capable of performing analog cancellation can reduce the interference down to a much smaller residual (black) that allows the SoI to be received.

Our architecture will provide the advantages of analog cancellation while achieving peak cancellation values comparable to recent digital systems [5] despite a prominent challenge in analog cancellation systems: frequency stability. In this

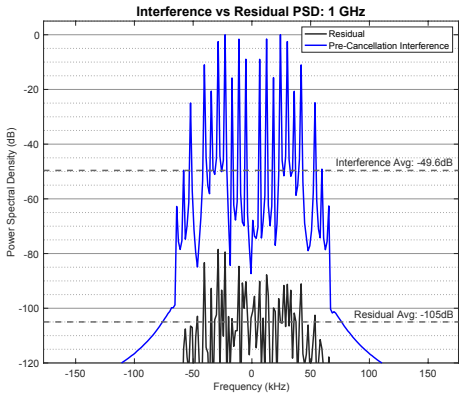


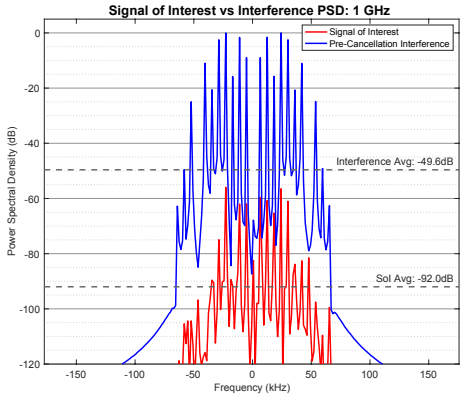
Fig. 5: A frequency domain view of the receiver's analog cancellation capability at 1 Ghz. In blue is the pre-cancellation interference received by Bob. The black trace shows the remaining residual received by Bob's ADC post-cancellation.

testbed, the carrier frequency offset estimation takes place while cancellation is off and the receiver sees high interference SNR. After estimation, the cancellation is turned on and the carrier frequency is assumed fixed. In practice, however, some frequency drift occurs and eventually causes the cancellation to degrade. Based on the frequency sensitivity of interference cancellation shown by Guo et al. in [9], to achieve a 50+ dB cancellation ratio, the frequency error must be on the order of 10^{-6} of the interference bandwidth, which would be less than 0.1 Hz here. Since frequency drift is proportional to carrier frequency, lower carrier frequencies will produce reduced drift and therefore reduced carrier frequency error, as shown by increased peak cancellation and cancellation stability in the 100 MHz carrier results. Fractional time error is also impactful, and a limitation of SDRs and digital signal processing for this application is time delay resolution. If the channel time delay is estimated to be between multiples of the SDR sample period, the receiver is unable to synchronize to that time delay without introducing ISI to the cancellation signal, as described in the previous section.

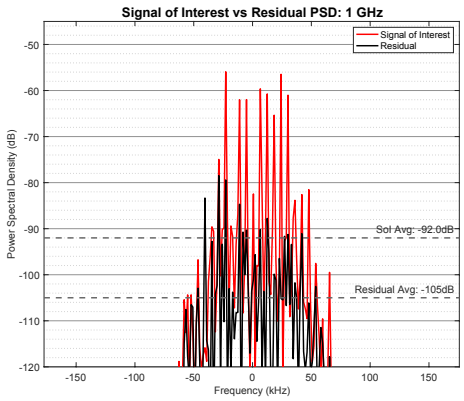
VI. Secrecy Advantage Due to Limited Adversary Analog to Digital Converter

Figure 6 demonstrates how secrecy is obtained using the results for the 1 GHz carrier. Eve, without an analog cancellation stage, must recover the red SoI from underneath the more powerful blue interference (Figure 6a). Bob's receiver sees the red message signal that is more powerful than the black residual interference (Figure 6b), hence allowing information recovery.

Next, we quantify the secrecy performance when the analog interference cancellation results obtained here replace the perfect cancellation assumptions of [2]. By assuming that the SoI follows a Gaussian distribution with power spectral density characterized by the results using the testbed and that the jamming is uniformly distributed with similarly characterized power spectral density, rough estimates for the secrecy capacity can be calculated. Using the interference and SoI power levels, P_I and P_S, results generated using the testbed



(a)



(b)

Fig. 6: Frequency domain representations of the signals received by the eavesdropper, Eve (a), and intended receiver, Bob (b).

described in Section IV and shown by Figure 6b, the necessary parameters to find the secrecy rate can be calculated. The power of a uniform interference spanning from $-c$ to c can be found as the second moment of its distribution, $P_I = \int_{-c}^{c} \frac{1}{2c} x^2 \, dx = \frac{c^2}{3}$. From here, the interference amplitude can be calculated from the known P_I as $c = \sqrt{3P_I}$. The mutual information between the signal and Eve's reception is maximized when their ADC span is $2l\sigma$, where sigma is the standard deviation of the SoI, with $l = 2.5$ [2]. This gives $2l\sigma = 5\sqrt{P_S}$. These values are used to determine k, the number of key-bits per interference symbol that can be successfully cancelled. Using $(2^k - 1) \times 2l\sigma = 2c$, the ADC-attacking secrecy architecture is capable of supporting cancellation of about $k = 6.5$ key-bits per jamming symbol for an interference-to-SoI ratio of 42.3 dB. From results in [2], this corresponds to a secrecy rate of approximately 2.0 bits/symbol over an eavesdropper performing perfect digital cancellation with the same number of ADC bits as the intended receiver, or an enhancement of the secrecy rate in standard cooperative jamming schemes by the same amount. We view this as a promising rate for a communication signal requiring such a high level of security and under the very pessimistic assumption that the adversary obtains the key after message transmission.

VII. Conclusion

A hardware testbed was built to characterize a scheme for everlasting secrecy that requires analog interference cancellation of a known remote interferer. The testbed was capable of maintaining an interference power reduction over 40 dB or 30 dB (with peaks up to 52 dB or 42 dB) at the intended receiver for a 100 MHz or 1 GHz carrier frequency, respectively. Increased carrier frequencies showed reduced interference cancellation ratios due to carrier frequency drift.

Next, the cancellation capability was related to achievable secrecy rates. The testbed performance suggests everlasting secrecy rates of up to 2.0 bits/symbol in the presence of an eavesdropper with the same number of ADC bits as the intended receiver. Analog known interference cancellation also has use for reducing intended receiver compression in jamming or other interference cancellation scenarios due to nonlinear amplifier operation. This is further explored in [16].

References

[1] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Everlasting secrecy by exploiting non-idealities of the eavesdropper's receiver," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1828–1839, September 2013.

[2] ——, "Jamming based on an ephemeral key to obtain everlasting security in wireless environments," *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6072–6081, November 2015.

[3] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[4] E. R. Alotaibi and K. A. Hamdi, "Optimal cooperative relaying and jamming for secure communication," *IEEE Wireless Communications Letters*, vol. 4, no. 6, pp. 689–692, December 2015.

[5] W. Guo, H. Zhao, and Y. Tang, "Testbed for cooperative jamming cancellation in physical layer security," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 240–243, February 2020.

[6] J. W. Kwak, M. S. Sim, J. S. P. I. W Kang, J. Park, and C. B. Chae, "A comparative study of analog/digital self-interference cancellation for full duplex radios," in *53rd Asilomar Conference on Signals, Systems, and Computers*, 2019, pp. 1114–1119.

[7] S. J. Frasier, F. Argenti, and L. Facheris, "Predistortion for very low pulse-compression sidelobes in solid-state meteorological radar," *IEEE Geoscience and Remote Sensing Letters*, vol. 20, pp. 1–5, 2023.

[8] C. R. Johnson, W. A. Sethares, and A. G. Klein, *Carrier Recovery*. Cambridge University Press, 2011, ch. 10, pp. 192–225.

[9] W. Guo, C. Li, H. Zhao, R. Wen, and Y. Tang, "Comprehensive effects of imperfect synchronization and channel estimation on known interference cancellation," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 457–470, 2020.

[10] T. Laakso, V. Valimaki, M. Karjalainen, and U. Laine, "Splitting the unit delay [fir/all pass filters design]," *IEEE Signal Processing Magazine*, vol. 13, no. 1, pp. 30–60, 1996.

[11] C. Li, H. Zhao, F. Wu, and Y. Tang, "Digital self-interference cancellation with variable fractional delay fir filter for full-duplex radios," *IEEE Communications Letters*, vol. 22, no. 5, pp. 1082–1085, 2018.

[12] T. Huusari, Y.-S. Choi, P. Liikkanen, D. Korpi, S. Talwar, and M. Valkama, "Wideband self-adaptive rf cancellation circuit for full-duplex radio: Operating principle and measurements," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, 2015, pp. 1–7.

[13] H. Arslan and G. E. Bottomley, "Channel estimation in narrowband wireless communication systems," *Wireless Communications and Mobile Computing*, vol. 1, no. 2, pp. 201–219.

[14] X. Quan, Y. Liu, W. Pan, Y. Tang, and K. Kang, "A two-stage analog cancellation architecture for self-interference suppression in full-duplex communications," in *2017 IEEE MTT-S International Microwave Symposium (IMS)*, 2017, pp. 1169–1172.

[15] K. E. Kolodziej, J. G. McMichael, and B. T. Perry, "Multitap rf canceller for in-band full-duplex wireless communications," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4321–4334, 2016.

[16] J. Doty, "Analog cancellation of a known remote interference: Hardware realization and analysis," Master's thesis, University of Massachusetts Amherst, Amherst MA, 2023.