

Artificial Intersymbol Interference (ISI) to Exploit Receiver Imperfections for Secrecy

Azadeh Sheikholeslami, Dennis Goeckel and Hossein Pishro-nik
Electrical and Computer Engineering Department, University of Massachusetts, Amherst
{sheikholesla,goeckel,pishro}@ecs.umass.edu

Abstract—Secure communication over a wireless channel in the presence of a passive eavesdropper is considered. We present a method to exploit the eavesdropper’s inherent receiver vulnerabilities to obtain everlasting secrecy. An ephemeral cryptographic key is pre-shared between the transmitter and the legitimate receiver and is utilized to induce intentional intersymbol interference (ISI). The legitimate receiver uses the key to cancel the ISI while the eavesdropper, since it does not have the key, cannot do such. It is shown that although ISI reduces the capacity of the main channel, it can lead to a net gain in secrecy rate. The achievable secrecy rates for different ISI filter settings are evaluated and the proposed method is compared with other information-theoretic security schemes.

I. INTRODUCTION

The messages sent over a wireless network are vulnerable to being overheard by any malicious party in the coverage range of the transmitter. The traditional way to prevent an eavesdropper from obtaining a secret message is to encrypt the message such that decoding the cypher without having the key is beyond the eavesdropper’s computational capability [1]. However, the vulnerability shown by many implemented cryptographic schemes, the lack of a fundamental proof establishing the difficulty of the scheme, and the potential for transformative changes in computing motivate forms of security that are provably everlasting. In particular, when a cryptographic scheme is employed, the adversary can record the clean cypher and recover it later when the cryptographic algorithm is broken [2] or when the eavesdropper obtains the key, which is not acceptable in sensitive applications requiring everlasting secrecy.

The desire for such everlasting security motivates considering information-theoretic approaches, where the eavesdropper is unable to extract any information about the secret message from the received signal. The feasibility of information-theoretic security was demonstrated by the seminal work of Wyner [3], where he showed for discrete memoryless wiretap channel, that, if the eavesdropper’s channel is degraded with respect to the main channel, adding randomness to the codebook allows perfect secrecy to be achieved. Later, the idea was extended to the more general case where the eavesdropper’s channel is not necessarily degraded, but “more noisy” or “less capable” with respect to the main channel [4]. Thus, the desirable situation for achieving information theoretic

secrecy is to have a better channel from the transmitter to the intended receiver than that from the transmitter to the eavesdropper. However, this is not always guaranteed, as the eavesdropper can be very close to the transmitter or can use a directional antenna to improve its received signal, while the eavesdropper’s location and its channel state information is not known to the legitimate nodes. When such an advantage does not exist, approaches based on “public discussion” [5], [6] can be employed. However, these approaches, while they could be used to generate an information-theoretically secure one-time pad, are basically designed for secret key agreement by performing multiple two-way transmissions and utilizing a public authenticated channel [7, Chapter 7.4] rather than efficient one-way secret communication. Recently, approaches based on the cooperative jamming approach of [8] have been considered. However, all of these approaches require either multiple antennas, helper nodes, and/or fading, and many are susceptible to attacks such as pointing directive antennas.

For a one-way scenario with a single antenna, Cachin and Maurer [9] exploited hardware limitations to obtain everlasting security, as is our interest. In particular, they introduced the “bounded memory model” in such a way that the eavesdropper is not able to store the information it would need to eventually break the cypher. This novel approach suffers from two shortcomings: (1) by Moore’s Law (see NAND scaling plot at [10]), the density of memories increases at an exponential rate; (2) memories can be stacked arbitrarily subject only to (very) large space limitations. Hence, although the bounded memory model is a viable approach to everlasting security, it is difficult to pick a memory size beyond which it will be effective and thus it is difficult to employ in wireless communication.

Our approach to provide everlasting security is that, instead of attacking the memory in the receiver back-end, we attack the receiver front-end. In particular, the technology of analog-to-digital (A/D) converters progresses slowly and unlike memory, they cannot be stacked arbitrarily (in fact, high-quality A/Ds already employ parallelization to the limit of the jitter). Also, importantly from a long-term perspective, there is a fundamental bound on the ability to perform A/D conversion [11], [12]. Hence, our goal is to exploit the receiver analog-to-digital conversion processing effect for security. The transmitter (Alice) and the intended receiver (Bob) pre-share a cryptographic key that only needs to be kept secret for the duration of the transmission (i.e. it can be given to the

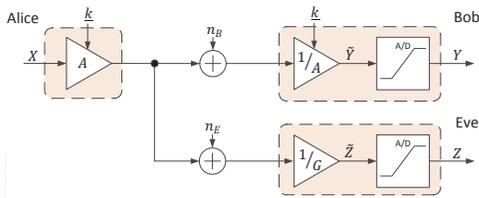


Fig. 1. The transmitter perform fast power modulation to obtain secrecy by utilizing a cryptographic key pre-shared between Alice and Bob.

eavesdropper immediately afterward). By using this key, we consider inserting intentional distortion on the transmitted signal. Since Bob knows the distortion, he can undo its effect before his A/D, whereas Eve must store the signal and try to compensate for the distortion after her A/D; however, she already lost the information she need to recover the message. We considered a rapid power modulation instance of this approach in [13] and [14], where the transmitted signal is modulated by two vastly different power levels at the transmitter (Figure 1). Since Bob knows the key, he can cancel the effect of power modulator before his A/D, putting his signal in the appropriate range for A/D conversion. On the other hand, Eve must compromise between larger quantization noise and more A/D overflows. Consequently, she will lose information she needs to recover the message and information-theoretic security is obtained. However, a clear risk of this approach is an eavesdropper with multiple A/Ds.

Motivated by the fact that an additive white Gaussian noise (AWGN) channel will have a higher capacity than an intersymbol interference channel under the same output power constraint, we seek to induce an ISI channel for Eve while preserving an AWGN channel at Bob. The transmitter is equipped with a linear filter with random coefficients that are taken based on a pre-shared key between Alice and Bob. The secret message is broken into chunks of data with a guard interval between every two chunks and is transmitted over the channel after going through the ISI filter. Bob, since he knows the key, places a filter before his A/D in concert with the ISI filter to cancel the ISI. In order to prevent Eve from performing any kind of adaptive equalization to cancel the ISI, the coefficients of the ISI filter are changed based on the key during each chunk. By exploiting the resulting distortion, information-theoretic secrecy can be obtained, even if Eve is given the key immediately after message transmission.

The rest of paper is as follows. Section II describes the system model, metrics, and the proposed idea in detail. In Section III, the achievable secrecy rates for the proposed method are characterized. In Section IV, the results of numerical examples for various realizations of the system and comparison of the proposed method to the public discussion approaches of [5], [6] are presented. Conclusions and ideas for future work are discussed in Section V.

II. SYSTEM MODEL AND APPROACH

A. System Model

A simple wiretap channel is considered, which consists of a transmitter, Alice, an intended receiver, Bob, and an eavesdropper, Eve. The eavesdropper is assumed to be passive, i.e. it does not attempt to actively thwart (i.e. via jamming, signal insertion) the legitimate nodes. Thus, the location and channel state information of the eavesdropper is assumed to be unknown to the legitimate nodes.

Alice and Bob either pre-share a cryptographic key or use a standard key agreement scheme (e.g. Diffie-Hellman [15]) to generate a shared key. Then, the number of key bits can be expanded aggressively using a linear feedback shift register (LFSR) to make a long key sequence. Generally, the output of an LFSR, even when the initial state is unknown, is easily predictable, thus making it inappropriate for cryptography. However, here the key is employed only ephemerally and it is assumed (pessimistically) that Eve is handed the full key once transmission is complete. Since Eve only views the transmitted signal through a very noisy process (using the method described in Section II.B), and the key is changed by the legitimate nodes periodically, she cannot hope to recover the key during the transmission period. We consider a one-way communication system, and assume that both Bob and Eve are at a unit distance from the transmitter by including variations of the path-loss in the noise variance; thus, the channel gain of both channels is unity. Both channels experience additive white Gaussian noise (AWGN). Let n_B and n_E denote the zero-mean noise processes at Bob's and Eve's receivers with flat power spectrum $N_B(f) = N_B/2$ and $N_E(f) = N_E/2$, respectively. Let \hat{X} denote the input of both channels, \hat{Y} denote the received signal at Bob's receiver, and \hat{Z} denote the received signal at Eve's receiver (Figure 2).

Both Bob and Eve employ high precision uniform analog-to-digital converters and the effect of the A/D on the received signal (quantization noise) is modeled by an additive Gaussian noise with variance $\delta^2/12$, where δ is the length of one quantization level. The assumption that quantization noise follows a Gaussian distribution is not accurate; however, it enables us to use results of Gaussian channels to obtain some insight about the actual system. The equivalent continuous-time power spectrum of the quantization noise of Bob's A/D, n_{QB} , and quantization noise of Eve's A/D, n_{QE} , are assumed to be flat, i.e. $N_{QB}(f) = N_{QB}/2$ and $N_{QE}(f) = N_{QE}/2$, respectively. Let X denote the current code symbol. Since all noises are assumed to be Gaussian processes, we assume that X is taken from a standard Gaussian codebook where each entry has variance P , i.e. $X \sim \mathcal{N}(0, P)$.

B. Artificial ISI for secrecy

Our goal is to study how Alice and Bob can employ bits of the shared cryptographic key to modify their radios to gain an information theoretic advantage. Assume that Alice applies a linear filter after her D/A with spectral density $G_k(f)$ (as shown in Figure 2). The spectral density of this filter is chosen

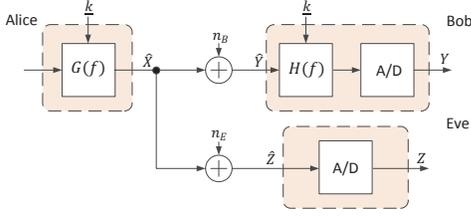


Fig. 2. Alice sends the message through an ISI filter that is determined by the key sequence, pre-shared between Alice and Bob. Bob uses the key sequence to cancel the effect of ISI on his signal before the analog-to-digital conversion process.

based on the pre-shared key between Alice and Bob. Since Bob shares the (long) key with Alice, he easily cancels the effect of this filter before his A/D properly, whereas Eve will struggle with such. In essence, we are inducing an ISI channel that Bob is able to equalize before his A/D, while Eve cannot. Thus, Eve will suffer from the channel degradation due to ISI and information-theoretic security is obtained. Further, Alice changes the weights of ISI filter taps frequently (based on the shared key) to ensure that Eve is not able to perform any kind of adaptive ISI cancellation.

Here we use a filter similar to a n -tap ISI channel,

$$\hat{x}(j) = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} g_{\underline{k}}(i)x(j-i)$$

where $x(j)$ is the channel input, $\hat{x}(j)$ is the channel output, and $g_{\underline{k}}(i)$, $i = 0, \dots, n-1$ are filter coefficients. Hence, the spectrum of the ISI filter is,

$$G_{\underline{k}}(f) = \begin{cases} \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} g_{\underline{k}}(i)e^{-j\pi f i/W}, & -W \leq f \leq W \\ 0, & \text{else} \end{cases} \quad (1)$$

In order to confuse Eve, the coefficient vector $g_{\underline{k}} = [g_{\underline{k}}(0)g_{\underline{k}}(1) \dots g_{\underline{k}}(n-1)]$ is chosen randomly from an i.i.d ensemble that follows $\mathcal{N}(\mu, \sigma^2)$ according to the key sequence, \underline{k} , pre-shared between Alice and Bob. These coefficients are chosen such that the ISI filter does not change the average output transmit power, i.e. $E[g_{\underline{k}}(i)^2] = 1$, $i = 0, \dots, n-1$. To cancel the ISI at Bob's receiver, we put a filter with power spectrum $H_{\underline{k}}(f) = 1/G_{\underline{k}}(f)$ at the input of Bob's receiver. Note that the assumption that Bob applies a $H_{\underline{k}}(f) = 1/G_{\underline{k}}(f)$ is for ease of proof of Theorem 1 and establishes an achievable secrecy rate of the proposed approach. The optimization of $H_{\underline{k}}(f)$ to maximize the provable secrecy rate is a topic of ongoing work. In the sequel, the average secrecy rates that can be obtained using the proposed method will be investigated.

III. ARTIFICIAL ISI FOR SECRECY

To the best of our knowledge the secrecy capacity of the wiretap ISI channel is not established yet. Therefore we represent a theorem for the achievable secrecy rates of the Gaussian band-limited wiretap channel that is shown in Figure 2.

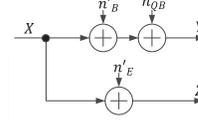


Fig. 3. Equivalent wiretap channel.

Theorem 1. The average secrecy rate of the wiretap channel shown in Figure 2 without CSI of both the main and eavesdropper channels for a given key sequence, \underline{k} , is:

$$R_s = \int_{-W}^W \frac{1}{2} \log \left(1 + \frac{P|G_{\underline{k}}(f)|^2}{W(N_{QB}|G_{\underline{k}}(f)|^2 + N_B)} \right) - \frac{1}{2} \log \left(1 + \frac{P|G_{\underline{k}}(f)|^2}{W(N_{QE} + N_E)} \right) df. \quad (2)$$

Proof: The equivalent wiretap channel is shown in Figure 3. The channel noise of the main channel can be substituted by n'_B with spectrum $N'_B(f) = N_B(f)/|G_{\underline{k}}(f)|^2$ at the input of the main channel. Since $H_{\underline{k}}(f)G_{\underline{k}}(f) = 1$, the spectrum of quantization noise of Bob's receiver will be $N_{QB}(f)H_{\underline{k}}(f)G_{\underline{k}}(f) = N_{QB}(f)$ and thus n_{QB} remains unchanged. Similarly, the total noise of the eavesdropper channel can be substituted by n'_E with spectrum $N'_E(f) = (N_E(f) + N_{EB}(f))/|G_{\underline{k}}(f)|^2$. Since we want to induce ISI and the transmitter does not have knowledge of the main channel, the transmitter does not perform spectral-loading (e.g. water-filling) at the transmitter and thus the power spectral density of the input of the wiretap channel, $P/2W$, is fixed. In a finite time interval of length T , by expanding the auto-correlation function of the equivalent noise of the main channel, $n'_B(t)$, using the Karhunen-Loeve expansion,

$$n'_B(t) = \sum_{l=1}^{\infty} n'_{Bl} \phi_l(t),$$

where $\phi_l(t)$ are the orthonormal eigenfunctions and the coefficients n'_{Bl} are independent Gaussian random variables of variance $\lambda_{Bl} = \lambda_l N_B/2$. The λ_l s are the eigenvalues corresponding to the spectrum $1/|G_{\underline{k}}(f)|^2$. We can represent the other noises and the input signal in terms of $\phi_l(t)$ s, $n'_E(t) = \sum_{l=1}^{\infty} n'_{El} \phi_l(t)$, $n_{BQ}(t) = \sum_{l=1}^{\infty} n_{BQl} \phi_l(t)$, and $x(t) = \sum_{l=1}^{\infty} x_l \phi_l(t)$, where n'_{El} , n_{BQl} , and x_l are independent Gaussian random variables with variances $\lambda_l(N_E + N_{QE})/2$, $N_{QB}/2$, and $P/2W$, respectively. Thus, our wiretap channel is decomposed into an infinite number of independent parallel wiretap channels. Thus,

$$R_s = \lim_{T \rightarrow \infty} \frac{1}{T} R_s(T) = \lim_{T \rightarrow \infty} \sum_{l=0}^{\infty} \frac{1}{2} \log \left(1 + \frac{P/2W}{(N_{QB}/2 + \lambda_l N_B/2)} \right) - \frac{1}{2} \log \left(1 + \frac{P/2W}{\lambda_l (N_{QE} + N_E)/2} \right).$$

By applying the Toeplitz distribution theorem for continuous random variables [16] and since the spectrum of output filter

is limited to $[-W, W]$, R_s in (2) is obtained. \blacksquare

The secrecy rate averaged over all key sequences is,

$$R_s = E_{\underline{k}} \left[\int_{-W}^W \frac{1}{2} \log \left(1 + \frac{P|G_{\underline{k}}(f)|^2}{W(N_{QB}|G_{\underline{k}}(f)|^2 + N_B)} \right) - \frac{1}{2} \log \left(1 + \frac{P|G_{\underline{k}}(f)|^2}{W(N_{QE} + N_E)} \right) df \right]. \quad (3)$$

Equation (1) for a given $G_{\underline{k}}(f)$ is complicated, and thus it is not possible to obtain a closed form for the average achievable secrecy rates. However, in the high SNR regime, it can be shown that R_s in (3) is always greater than the secrecy capacity of the corresponding wiretap channel without applying the ISI filter, which is,

$$C_s^{WTC} = W \left\{ \log \left(1 + \frac{P}{W(N_B + N_{QB})} \right) - \log \left(1 + \frac{P}{W(N_E + N_{QE})} \right) \right\}$$

Suppose that $C_s^{WTC} > 0$. Since we are working in high SNR regime,

$$\begin{aligned} C_s^{WTC} &\approx W \log \left(\frac{P}{W(N_E + N_{QE})} \right) - W \log \left(\frac{P}{W(N_E + N_{QE})} \right) \\ &= W \log(N_E + N_{QE}) - W \log(N_B + N_{QB}) \\ &= \frac{1}{2} \int_{-W}^W \log(N_E + N_{QE}) - \log(N_B E_{\underline{k}}[|G_{\underline{k}}(f)|^2] + N_{QB}) df \\ &\leq \frac{1}{2} \int_{-W}^W \log(N_E + N_{QE}) - E_{\underline{k}} \left[\log(N_B |G_{\underline{k}}(f)|^2 + N_{QB}) \right] df \\ &= E_{\underline{k}} \left[\int_{-W}^W \frac{1}{2} \log \left(\frac{P|G_{\underline{k}}(f)|^2}{W(N_B |G_{\underline{k}}(f)|^2 + N_{QB})} \right) - \frac{1}{2} \log \left(\frac{P|G_{\underline{k}}(f)|^2}{W(N_E + N_{QE})} \right) df \right] \\ &\approx E_{\underline{k}} \left[\int_{-W}^W \frac{1}{2} \log \left(1 + \frac{P|G_{\underline{k}}(f)|^2}{W(N_B |G_{\underline{k}}(f)|^2 + N_{QB})} \right) - \frac{1}{2} \log \left(1 + \frac{P|G_{\underline{k}}(f)|^2}{W(N_E + N_{QE})} \right) df \right] \leq R_s \end{aligned}$$

where the second equality is from the fact that $E_{\underline{k}}[|G_{\underline{k}}(f)|^2] = 1$, the first inequality is Jensen's inequality, and in the last equality we use the fact that the probability of $|G_{\underline{k}}(f)| = 0$ at uncountably infinite number of points over the interval $[-W, W]$ is zero. This shows that inducing the ISI, which lowers the capacity of the main channel, provides a net gain in secrecy capacity.

Numerical results are presented in the next section.

IV. NUMERICAL RESULTS AND COMPARISON TO OTHER METHODS

In this section we study the achievable secrecy rates of the proposed method for various scenarios. Also, we compare the proposed method to the conventional Gaussian wiretap channel (WTC) [17] and public discussion (PD) [5]. Public discussion, in contrast to the wiretap channel which is limited to one-way rate-limited communication, may take advantage of two-way communication over a noiseless and public authenticated

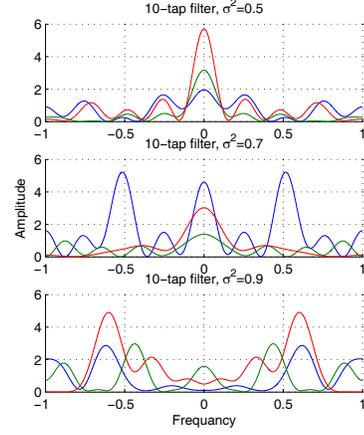


Fig. 4. Frequency spectrum of 10-tap ISI filters for various values of variance, $\sigma^2 = 0.5, 0.7, \text{ and } 0.9$, and three realizations of filter coefficients in each case.

channel. Hence, the legitimate parties can agree on a secret key by extracting information from realizations of correlated random variables. This secret key can be used in a one-time-pad for secret communication between Alice and Bob. A closed form for the general secret-key capacity is not available; however, in the case of a Gaussian source model in which $X \sim \mathcal{N}(0, P)$ and a Gaussian wiretap channel, i.e. when the channel between Alice and Bob and the channel between Alice and Eve are AWGN channels, the secrecy capacity of the public discussion method has a simple form [7, Chapter 5]:

$$C_s^{SM} = \log \left(1 + \frac{PN_E^t}{(P + N_E^t)N_B^t} \right) \quad (4)$$

where here $N_B^t = N_B + N_{QB}$ and $N_E^t = N_E + N_{QE}$.

In the proposed method, suppose that the bandwidth of the transmit filter is normalized as $[-W, W] = [-1, 1]$ and its coefficients are taken from an ensemble with normal distribution such that the ISI filter does not change the average transmit power, i.e. $g_{\underline{k}}(i) \sim \mathcal{N}(\mu, \sigma^2)$, $i = 0, \dots, n-1$ such that $E[g_{\underline{k}}(i)^2] = \mu^2 + \sigma^2 = 1$. The frequency spectrum of 10-tap ISI filter for various values of σ^2 for three realizations of the filter coefficients are shown in Figure 4. observe that as the variance of the filter coefficients becomes smaller, the uncertainty of the shape of the frequency response of the ISI filter lessens and the eavesdropper might be able to increase the information leakage by using this information. However, by applying a random phase shift to the transmitted signal based on the key, we can prevent the eavesdropper from doing such while the achievable secrecy rates remain unchanged.

First we look at the extreme case that Eve is able to receive exactly what Alice transmits and receives (e.g. the adversary is able to pick up the transmitter's radio and hook directly to the antenna), but the channel between Alice and Bob is noisy and hence the conventional wiretap channel does not work. In other words, the channel between Alice and Bob experiences an additive white Gaussian noise, while Eve's

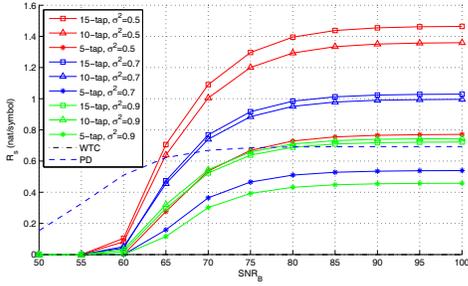


Fig. 5. Achievable secure rate of the proposed method, conventional wiretap channel (WTC), and public discussion (PD) vs. SNR of channel between Alice and Bob while the channel between Alice and Eve is noiseless (Eve has perfect access to the transmitted signal). σ^2 is the variance of the ISI filter coefficients. Because Eve has perfect access to the signal, note that the secrecy rate of the wiretap channel is zero.

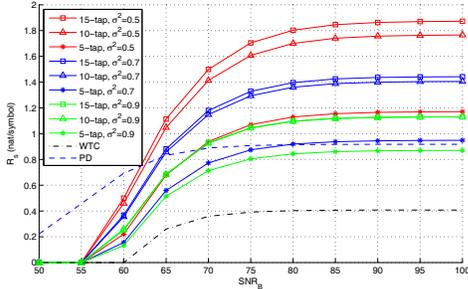


Fig. 6. Achievable secure rate of the proposed method, conventional wiretap channel (WTC), and public discussion (PD) vs. SNR of channel between Alice and Bob when SNR of channel between Alice and Eve is 60 dB. σ^2 is the variance of the ISI filter coefficients.

channel is noiseless ($n_E = 0$). Figure 5 shows the achievable secrecy rate versus signal-to-noise ratio at Bob's receiver when Eve's receiver is noiseless. The average transmit power $P = 1$ and both Bob and Eve use 10-bit A/Ds. It can be seen that, although the eavesdropper's channel is much better than the main channel, when the SNR at Bob's receiver is greater than 55 dB, which is quite common in short-range communication, positive secrecy rates are obtained. Public discussion, although it provides better secrecy rates in low SNRs, needs two-way communication and a public authenticated channel which are not always possible. If a public authenticated channel exists and users can perform two-way communication, the proposed method still has utility: it can enhance the underlying channel and thus improve the secrecy rate of the public discussion.

Another observation is that as the ISI channel gets further from the flat channel, higher secrecy rates are achievable due to greater variation of the channel. In the current construction of the ISI filter, this occurs when σ^2 gets smaller.

In Figure 6, the achievable secrecy rate versus SNR at Bob's receiver is shown. Again, the average transmit power $P = 1$ and both Bob and Eve use 10-bit A/Ds. Similar to the previous case, as expected, channels with greater variations lead to higher secrecy rates. For our model here, those correspond

to channels with larger numbers of taps and smaller σ^2 .

V. CONCLUSION

In this paper, a new method that utilizes an ephemeral cryptographic key to achieve secrecy is introduced. The secret message goes through a time-varying ISI filter with filter coefficients determined by the shared key. The intended receiver uses the key sequence to cancel the effect of ISI on its signal, while the eavesdropper cannot. The coefficients of the filter are changed frequently and thus the eavesdropper is not able to perform adaptive ISI cancellation. It is shown that this method can substantially improve the achievable secrecy rate of the corresponding wiretap channel and provide secrecy even in the case that the eavesdropper has perfect access to the output of the transmitter's radio. At high SNRs, the secrecy rates are better than public discussion, which takes advantage of additional resources in the form of two-way communication and a public authenticated channel. Nevertheless, in the case that two-way communication is possible and a public channel is available, our scheme can be used in conjunction with public discussion and improve its performance by adding more uncertainty to the adversary's channel.

REFERENCES

- [1] D. Stinson, *Cryptography: theory and practice*. CRC press, 2006.
- [2] R. Benson, "The verona story," *National Security Agency Central Security Service, Historical Publications (available via WWW)*.
- [3] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [5] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.
- [6] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- [7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
- [8] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference, 2005*, vol. 62, p. 1906.
- [9] C. Cachin and U. Maurer, "Unconditional security against memory-bounded adversaries," *Advances in Cryptology*, pp. 292–306, 1997.
- [10] R. Kuchibhatla, "Imft 25-nm mlc nand: technology scaling barriers broken," *EE Times News and Analysis*, 2010.
- [11] S. Krone and G. Fettweis, "Fundamental limits to communications with analog-to-digital conversion at the receiver," in *IEEE 10th Workshop on Signal Processing Advances in Wireless Communications*, pp. 464–468, 2009.
- [12] S. Krone and G. Fettweis, "A fundamental physical limit to data transmission and processing," *Signal Processing Letters, IEEE*, vol. 17, no. 3, pp. 305–307, 2010.
- [13] A. Sheikholeslami, D. Goeckel, and H. Pishro-nik, "Exploiting the non-commutativity of nonlinear operators for information-theoretic security in disadvantaged wireless environments," *50th Annual Allerton Conference*, 2012.
- [14] A. Sheikholeslami, D. Goeckel, and H. Pishro-nik, "Everlasting secrecy by exploiting non-idealities of the eavesdroppers receiver," *arXiv:1210.1790*, 2012.
- [15] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [16] R. E. Blahut, *Principles and Practice of Information Theory*. Addison-Wesley, 1987.
- [17] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.