Artificially Noise-Injected Low-Density Parity-Check Codes for the Gaussian Wiretap Channel

ARTIFICIALLY NOISE-INJECTED LOW-DENSITY PARITY-CHECK CODES FOR THE GAUSSIAN WIRETAP CHANNEL

Md Munibun Billah
Department of Electrical and Computer Engineering, Brigham Young University
Brigham Young University
Provo, UT, USA
billahm@byu.edu

Faculty Advisor:
Willie K. Harrison

ABSTRACT

Wireless telemetry communication systems may be vulnerable to eavesdroppers due to their broadcasting nature, which is a risk to confidential information transmission. This paper explores the feasibility of low-density parity-check (LDPC) codes for wiretap coding over a Gaussian channel for standard telemetry links. By introducing a wiretap LDPC coding method, we aim to mitigate the risk of eavesdropping. We further explore the notion of fine-tuning the trade-off in these codes between secrecy and reliability through artificial noise injection. Simulation results demonstrate the effectiveness of employing an LDPC-based wiretap code over telemetry links to provide secrecy. The analysis of the code shows that a neural network-based mutual information estimator can be utilized to calculate information leakage over telemetry links.

INTRODUCTION

With the advent of the information age, the rapid advancement and deployment of telemetry systems in various industries, including aerospace, telecommunication, and remote sensing, necessitates error-free secure communication more than ever. The noise in the channel introduces errors in the received data. To detect and correct those errors, intensive studies have been done in error correction coding techniques which have led to the development of some capacity-achieving codes: LDPC codes, turbo codes, polar codes, and Reed-Muller codes [1, 2, 3, 4]. Due to capacity-achieving capabilities and low implementation complexity, LDPC codes have been adopted into the IRIG 106-17 standard [5]. However, the security aspect for telemetry systems is not addressed by these codes [6, 7]. Much of the secrecy aspects for telemetry focus on cryptography, which is employed at the upper layers of the Open System Interconnection (OSI) model [8]. Due to the confidential nature of telemetry data, it is only natural to desire additional security for the system. Recent progress in physical-layer security has emerged as a viable candidate for providing additional security against an eavesdropper for telemetry links [9]. Physical-layer security can provide

an additional layer of security beyond cryptographic efforts already in place. Error control codes have been studied extensively for physical-layer security applications since they are ubiquitous in digital communication systems [10, 11].

LDPC codes, first introduced by Robert Gallager in 1962, are widely used due to their near-optimum performance and ease of implementation [1]. The IRIG 106 standard has adopted systematic and quasi-cyclic LDPC codes with three different coding rates ($1/2, 2/3, 4/5$) and two information block sizes (1024 and 4096 bits). Readers are referred to [5] for detailed descriptions of the construction of the generator matrices and parity check matrices specified in the standard. Since LDPC codes can provide reliability and are used in telemetry standards, the study of LDPC codes as wiretap codes in the domain of telemetry systems is the next logical step.

The usage of error correction codes for achieving physical-layer security has gained much attention recently. The existence of LDPC wiretap codes was shown in [12]. LDPC wiretap codes have been studied for different wiretap channels in [13, 14, 15]. However, the Gaussian channel is of practical interest since telemetry channels are mostly modeled as additive white Gaussian noise (AWGN) channels, sometimes in tandem with a fading effect [16]. Most of the above-mentioned work considers asymptotic regimes for codes analyzed as blocklength tends to infinity. To employ LDPC wiretap codes in practical telemetry links, finite blocklength codes need to be considered. This paper aims to develop an LDPC wiretap code based on artificial noise injection called artificially noise-injected low-density parity-check (ANI-LDPC) codes and studies the feasibility of such codes for achieving confidentiality over the Gaussian wiretap channel.

In this paper, we measure the physical-layer security using an information-theoretic approach. We define the term leakage as the amount of mutual information between the confidential message and the eavesdropper's received signal. No closed-form solution exists to calculate the information leakage to the eavesdropper for a finite blocklength code over a Gaussian channel [17]. There exist several data-driven mutual information estimators based on discretization, kernel density estimation, and k-nearest neighbor estimation [18, 19, 20, 21, 22, 23]. Due to a lack of proper scalability with data or dimension, these estimators have failed to be general-purpose. In [24], Donsker-Varadhan's Kullback-Leibler divergence representation has been used to archive a general-purpose mutual estimator that is linearly scalable and trainable, called the mutual information neural estimator (MINE). In this paper, MINE has been used to calculate leakage over the Gaussian wiretap channel due to MINE's ability to learn the channel for high dimensional data. Due to limitations of computing power to calculate leakage using MINE for LDPC codes with block size 1024 and 4096 bits defined in the IRIG 106 standard, this paper uses a much simpler and smaller code of blocklength eight. Future advances in computing will surely allow the analysis of larger codes using MINE.

THE WIRETAP CHANNEL AND LDPC WIRETAP CODES

The wiretap channel was introduced by Wyner in his seminal paper [25] and a version of it is shown in Figure 1. Here Alice is sending a confidential message M to Bob by encoding it to X^n and transmitting it over the main channel. Bob sees the main channel output Y^n and estimates the confidential message $\hat{M}$. There is an eavesdropper Eve who also receives a version of the

transmission Z^n over the wiretap channel. Here all the capital letters denote random variables and lowercase letters are the realization of corresponding random variables. It is assumed that Eve has perfect knowledge of the encoder and decoder employed by Alice and Bob. One of the consequences of Wyner's result is that to achieve secrecy the wiretap channel has to be noisier than the main channel [26]. To maintain an information-theoretic security argument, secrecy is

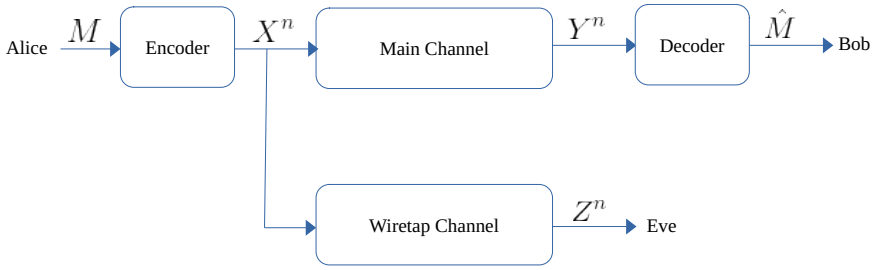

Figure 1: The wiretap channel.

measured by the mutual information between confidential message M and wiretap channel output Z^n, given by $I(M; Z^n)$.

Several criteria of information theoretic secrecy have been defined in the literature, notable among them are strong secrecy [27] and weak secrecy [25]. Strong secrecy is achieved when

$$\lim_{n\to\infty} I(M; Z^n) = 0, \tag{1}$$

and weak secrecy is achieved when

$$\lim_{n\to\infty} \frac{1}{n} I(M; Z^n) = 0. \tag{2}$$

Both of these definitions require some sense of statistical independence between M and Z^n as n approaches infinity and a means to calculate the information leakage $I(M; Z^n)$. Weak secrecy requires that $I(M; Z^n)$ grows sublinearly with n, and strong secrecy requires the total information to go to zero with n approaching infinity. While strong secrecy is preferred, weak secrecy is easier to achieve. Several LDPC codes have been constructed to achieve weak secrecy [28, 29, 30]. In [15], Klinc used punctured LDPC codes to achieve secrecy but he was unable to analyze his scheme using information theoretic techniques. Inspired by the puncturing technique, this work aims to implement a similar technique that uses an artificial noise injection method to the LDPC codewords and calculates leakage as the secrecy metric.

LDPC codes can be specified by bipartite graphs, consisting of variable nodes and check nodes. The degree distribution of the code is given by two polynomials

$$\lambda(x) = \sum_{i=1}^{n} \lambda_i x^{i-1}, \tag{3}$$

and

$$\rho(x) = \sum_{i=1}^{n} \rho_i x^{i-1}. \tag{4}$$

The coefficient λ_i represents the fraction of edges connected to variable nodes of degree i and ρ_i represents the fraction of edges connected to check nodes of degree i. Let us define a noise injection polynomial

$$p(x) = \sum_{i=1}^{n} p_i x^{i-1}, \tag{5}$$

where the coefficient p_i is the probability of injecting noise at the ith variable node. If artificial noise is injected to a variable node i, then the bit is flipped. The ANI-LDPC encoding method is described precisely as follows: Alice generates k bits of a confidential message $m = [m_1\, m_2\, \cdots\, m_k]$. The message m is then converted to a codeword c given by $c = mG$ where G is an LDPC generator matrix and $c = [c_1\, c_2\, \cdots\, c_n]$. Now, for each c_i in c there exists a coefficient p_i with the same subscript in the noise injection polynomial $p(x)$ which determines if c_i is flipped with a Bernoulli trial of probability p_i. After the noise injection, the ANI-LDPC codeword is X^n. Provided here are the specifications of the ANI-LDPC code used for simulation in this work:

$$\begin{aligned} n &= 8, \\ k &= 4, \\ \lambda(x) &= 0.307 + 0.461x + 0.23x^2, \\ \rho(x) &= 0.153x + 0.23x^2 + 0.615x^3, \\ p(x) &= 0.14 + 0.14x + 0.14x^2 + 0.14x^7. \end{aligned}$$

Thus, in this work, $p(x) = 0.14+0.14x+0.14x^2+0.14x^7$ indicates that the first, second, third, and eighth bits of every codeword will be subject to noise injection, each with probability 0.14. Those bits will simply be flipped in this paper, although additional methods of noise injection could be considered in future works.

MINE

To calculate the leakage $I(M; Z^n)$, this work uses the mutual information neural estimator (MINE). MINE uses the Donsker-Varadhan representation of the Kullback-Leibler divergence

$$D_{KL}(P||Q) = \sup_{F:\Omega\to\mathbb{R}} \mathbb{E}_P[f(X,Y)] - \log(\mathbb{E}_Q[e^{f(X,Y)}]), \tag{6}$$

where the supremum is taken over all functions f such that the expectations are finite for random variables X and Y. The relation between mutual information and Kullback-Leibler divergence is given by

$$I(X;Y) = D_{KL}(P_{XY}||P_X P_Y). \tag{7}$$

In [24], the authors proposed to choose $\mathcal{F}$ to be a set of functions $T_\theta : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$ parameterized by deep neural network $\theta \in \Theta$. Since (6) is a lower bound for Kullback-Leibler divergence with equality with an optimal function choice,

$$I(X;Y) \geq I_\Theta(X;Y), \tag{8}$$

where

$$I_\Theta(X;Y) = \sup_{\theta\in\Theta} \mathbb{E}_{p(x,y)}[T_\theta(X,Y)] - \log(\mathbb{E}_{p(x)p(y)}[e^{T_\theta(X,Y)}]). \tag{9}$$

Now, if we identify X as a confidential message M and Y as the wiretap channel output Z^n, then $p(M, Z^n)$ is the joint probability distribution, and p_M, p_{Z^n} are the respective marginals of (M, Z^n). Then (9), can be written as

$$I_\Theta(M; Z^n) = \sup_{\theta \in \Theta} \mathbb{E}_{p(M,Z^n)}[T_\theta(M, Z^n)] - \log(\mathbb{E}_{p(M)p(Z^n)}[e^{T_\theta(M,Z^n)}]). \tag{10}$$

Since in practice, the true distribution $p(M, Z^n)$ is unknown, we can't use $I_\Theta(M; Z^n)$ to estimate $I(M; Z^n)$. Rather we can estimate expectations presented in the equation (10) using the samples of joint and marginal distributions, by rewriting $I_\Theta(M; Z^n)$

$$\hat{I}(M; Z^n) := \frac{1}{l} \sum_{i=1}^{l} [T_\theta(m_i, z_i^n)] - \log \frac{1}{l} \sum_{i=1}^{l} [e^{T_\theta(\overline{m}_i, \overline{z}_i^n)}], \tag{11}$$

where l is the number of samples. In (11), l samples of the joint distribution are generated by producing uniformly distributed confidential messages m, and from wiretap channel outputs z^n. The term $(\overline{m}_i, \overline{z}_i^n)$ represents samples generated from marginal distributions. The network used in this work has five fully connected hidden layers with each layer consisting of 500 nodes and Relu activation functions. The input layer has $k+n$ neurons. During the training, ten thousand messages with a batch size of 1000 were used. We also used the Adam optimizer [31] with a learning rate of 10^{-7} and 2.5×10^5 epochs.

COMMUNICATION MODEL

The communication model is designed as follows. Alice generates k bits of a confidential message M and encodes them to form a codeword X^n using ANI-LDPC described above. Then a BPSK modulated version of the codeword is transmitted over the AWGN channel as

$$Y^n = X^n + N_B^n, \tag{12}$$

$$Z^n = X^n + N_E^n, \tag{13}$$

where Y^n and Z^n are received signal outputs of the main channel and wiretap channel respectively, and X^n has been mapped to $\{\pm 1\}^n$. N_B^n and N_E^n are zero-mean Gaussian random vectors with variances σ_B and σ_E respectively, where each random variable in the vector is independent. Since the wiretap channel has to be noisier than the main channel, $\sigma_E > \sigma_B$. The confidential message M and wiretap channel output Z^n are then used as inputs to the neural estimator to calculate the leakage. To compare the leakage of ANI-LDPC codes with LDPC codes, the confidential message M has been encoded using the LDPC code described by $\lambda(x)$ and $\rho(x)$ without any kind of addition of artificial noise, and the codewords are transmitted over the AWGN channel and the leakage between confidential message and AWGN output for LDPC codes have been calculated. Since the ANI-LDPC code can also be used to correct errors introduced by the noisy channel, the bit error rate (BER) for both ANI-LDPC and LDPC codes have been calculated and compared.

RESULTS

The output of MINE for an SNR of 15 dB for the case using ANI-LDPC codes is shown in Figure 2. The overall trend of the output gradually converges to the maximum amount of information, four

bits, but the output contains a large variance. Therefore, the output of MINE has been processed by applying a moving average filter with a window size of 10^4 points. After the application of the filter, the mutual information converges to four bits with roughly 1.5×10^5 epochs. The moving average filter is used to process the MINE outputs for all results following.

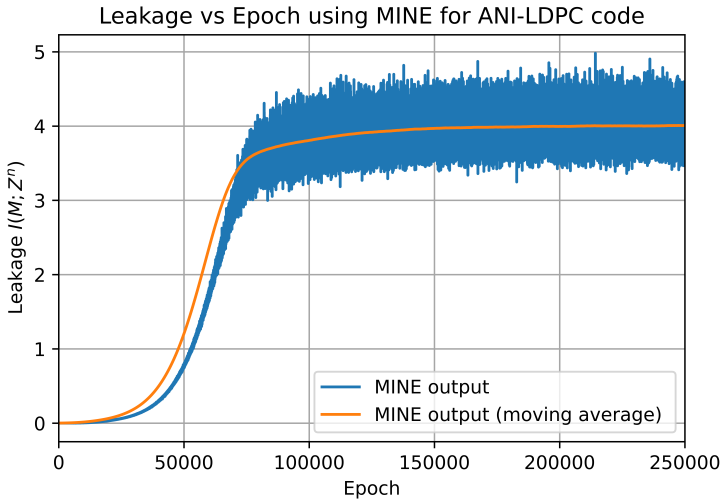

Figure 2: The output of MINE at SNR 15 dB.

For the AWGN channel, the leakage $I(M;Z^n)$ for different signal-to-noise ratio (SNR) values is shown in Figure 3. From this figure, we can see that at high and low SNR, the LDPC code leaks almost the same amount of information as the ANI-LDPC code. At high SNR, both the LDPC code and the ANI-LDPC code leak all of the information because the channel is almost noise free. Even with the artificial noise injection, the eavesdropper can utilize a state-of-the-art LDPC decoder to extract all the information. Similarly, at low SNR the received signal contains almost no information, and therefore cannot leak any information. By comparing both codes, it can be seen that ANI-LDPC can mitigate leakage between -10 dB and 10 dB. Since many radios operate in this region, this technique can aid security efforts at higher layers in the protocol stack (e.g., cryptography) in keeping telemetry data secure during wireless transmission.

ANI-LDPC codes can also be used to correct errors introduced by the channel. To compare the BER between LDPC codes and ANI-LDPC codes, the output of the wiretap channel for both the LDPC code and the ANI-LDPC code used in this work were decoded using the standard belief propagation (BP) decoder [32]. The tradeoff between BER for the LDPC code and the ANI-LDPC code under test is shown in Figure 4. Though the ANI-LDPC code used in this work provides error correction capabilities up to the probability of bit error 10^{-2}, it fails to match the performance of the LDPC code for correcting errors due to the artificial noise injected in the ANI-LDPC code. Due to the high probability of noise injection used in this work, the BER curve of ANI-LDPC reaches something akin to an error floor at 10^{-2} for an SNR of 7 dB. This is because at high SNR the AWGN channel noise is very low and can be corrected by the BP decoder while the noise injected by the noise injection polynomial $p(x)$ remains in the received codeword. The BER performance coupled with the leakage performance indicates a trade-off between reliability and secrecy. More

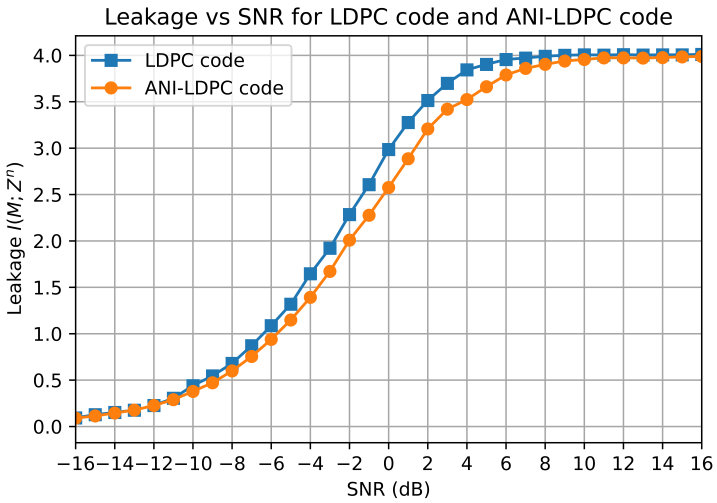

Figure 3: The leakage for AWGN channel.

work is required to fully explore parameter optimization for desired performance levels in both areas.

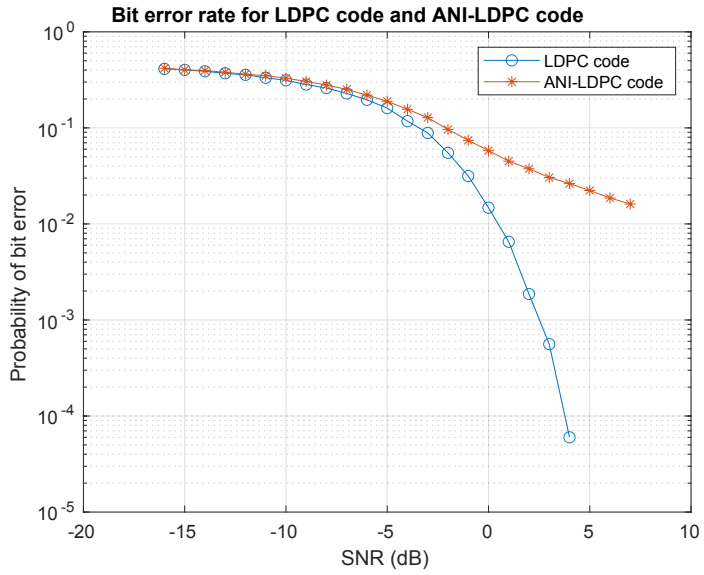

Figure 4: Comparison of BER for LDPC codes and ANI-LDPC codes.

CONCLUSIONS

In conclusion, an example of wiretap coding is provided to demonstrate the wiretap code's capability to mitigate leakage in the practical operating SNR regions of wireless telemetry. The results show that the ANI-LDPC codes can be utilized over AWGN telemetry links to achieve secrecy, but at the expense of some reliability. The employed code in this paper can mitigate leakage up to 0.3 bits from the eavesdropper. This work also shows the application of MINE to estimate leakage over the AWGN channel. MINE's general-purpose analysis technique can be applied to other more advanced wiretap codes as well, which may pave the way for wiretap coding in telemetry links.

REFERENCES

[1] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[2] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," in *Proc. IEEE Int. Conf. Communications (ICC)*, vol. 2, pp. 1064–1070, 1993.

[3] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[4] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşoğlu, and R. L. Urbanke, "Reed–Muller codes achieve capacity on erasure channels," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4298–4316, 2017.

[5] R. T. Group, "IRIG-106-17: Digital telemetry recorder standards," 2019.

[6] S. O'Neal, J. Lukins, and D. Hodack, "Integrated network enhanced telemetry (iNET) - information security in a multi-service program," *2009. [Online]. Available: http://hdl.handle.net/10150/606002*.

[7] R. Dukes, "Proposed iNET network security architecture," *2009. [Online]. Available: http://hdl.handle.net/10150/605971*.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[9] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. USA: Cambridge University Press, 2011.

[10] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41–50, 2013.

[11] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, 2015.

[12] J. Muramatsu, "Secret key agreement from correlated source outputs using low-density parity check matrices," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 89-A, pp. 2036–2046, 2006.

[13] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[14] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 585–594, 2011.

[15] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, 2011.

[16] M. Rice and D. H. Friend, "Antenna gain pattern effects on multipath interference in aeronautical telemetering," *1997. [Online]. Available: http://hdl.handle.net/10150/607555*, 1997.

[17] W. K. Harrison, K. Nelson, and S. Dye, "Physical-layer security for aeronautical telemetry," *2018. [Online]. Available: http://hdl.handle.net/10150/631657*, 2018.

[18] G. Darbellay and I. Vajda, "Estimation of the information by an adaptive partitioning of the observation space," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1315–1321, 1999.

[19] M. Koeman and T. Heskes, "Mutual information estimation with random forests," in *Proc. Neural Information Processing*, pp. 524–531, Springer International Publishing, 2014.

[20] A. Marx, L. Yang, and M. van Leeuwen, "Estimating conditional mutual information for discrete-continuous mixtures using multi-dimensional adaptive histograms," in *Proc. SIAM International Conference on Data Mining (SDM)*, pp. 387–395, 2021.

[21] W. Gao, S. Oh, and P. Viswanath, "Density functional estimators with k-nearest neighbor bandwidths," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 1351–1355, 2017.

[22] L. Paninski and M. Yajima, "Undersmoothed kernel entropy estimators," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4384–4388, 2008.

[23] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Phys. Rev. E*, vol. 69, p. 066138, June 2004.

[24] M. I. Belghazi, A. Baratin, S. Rajeshwar, S. Ozair, Y. Bengio, A. Courville, and D. Hjelm, "Mutual information neural estimation," in *Proc. International Conference on Machine Learning*, vol. 80, pp. 531–540, 2018.

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

[26] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 2152–2155, 2005.

[27] U. Maurer and S. Wolf, "From weak to strong information-theoretic key agreement," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, p. 18, 2000.

[28] C. W. Wong, T. F. Wong, and J. M. Shea, "LDPC code design for the BPSK-constrained gaussian wiretap channel," in *Proc. IEEE GLOBECOM Workshops*, pp. 898–902, 2011.

[29] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Two edge type LDPC codes for the wiretap channel," in *Proc. Asilomar Conference on Signals, Systems and Computers*, pp. 834–838, 2009.

[30] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type LDPC codes for the BEC wiretap channel," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1048–1064, 2013.

[31] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv:1412.6980*, 2017.

[32] T. K. Moon, *Error correction coding: Mathematical Methods and algorithms*. John Wiley & Sons, 2005.