Secrecy using Compressive Sensing

Shweta Agrawal and Sriram Vishwanath
Department of Electrical and Computer Engineering
University of Texas at Austin, TX, USA
Email: shweta.a@gmail.com, sriram@ece.utexas.edu

***Abstract*—This paper uses the compressive sensing framework to establish secure physical layer communication over a Wyner wiretap channel. The idea, at its core, is simple - the paper shows that compressive sensing can exploit channel asymmetry so that a message, encoded as a sparse vector, is decodable with high probability at the legitimate receiver while it is impossible to decode it with high probability at the eavesdropper.**

I. Introduction

The area of compressive sensing has seen an explosion of interest in the last few years, finding wide ranging applications from data mining to computer vision. In compressive sensing, sparse vectors are compressed using a linear transformation, and reconstruction is possible in polynomial time using an optimization or algorithmic framework [1], [2]. There are multiple algorithms for sparse signal recovery in presence or absence of additive noise corrupting the sensing process [3], [4], [5], [6], [7]. An algorithm of particular importance is Lasso [8], which has been widely applied and analyzed for signal recovery in presence of noise. Regardless of the particular algorithm used, an important underlying principle of compressive sensing is *incoherence*, which is essential for accurate signal retrieval [9], [10]. From the analysis perspective, there is a large and growing body of literature on the necessary and sufficient conditions for sparse signal recovery [6], [10], [11], [12]. In this paper, we utilize and build upon this analytical framework to use compressive sensing for secure communication over the Wyner wiretap channel.

Secure communication over wiretap channels is a well-established and growing area of research. A classical problem in this domain is the Wyner wiretap channel [13] (see Figure 1), where communication between a legitimate transmit-receive pair is eavesdropped. Secure communication over such channels can be studied based on multiple notions of secrecy. The most common formulation studied from an information-theoretic perspective is that of perfect secrecy, where one places no computational bounds on the adversary and requires that the adversary gain no knowledge of the message being communicated. The other extreme case is one of computational secrecy, most commonly studied from a cryptographic perspective. In this setting, a computationally unbounded adversary can, in theory, determine the message exactly, but such recovery is not possible due to the imposed computational limits. In this paper, we consider an intermediate notion of secrecy we call *Wolfowitz secrecy*, which captures elements of both domains. In line with information theoretic formulations, we assume a computationally unbounded adversary. In addition, we require that the legitimate receiver be able to decode the codeword in polynomial time, similar to computational secrecy. Our secrecy notion is as follows: we require that the transmission codebook be chosen so that the average probability of error of decoding at the eavesdropper be arbitrarily close to unity regardless of the decoding strategy.

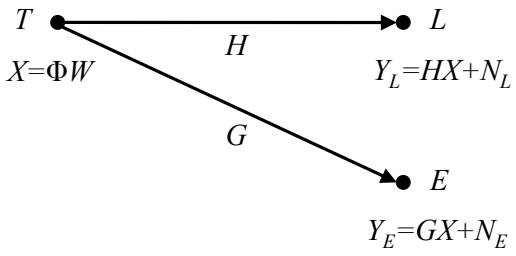

Fig. 1. The Wyner wiretap channel with a single transmitter T, one legitimate receiver L and one eavesdropper E.

Our main result is: given the Wyner wiretap channel with time-varying channel gains known to the transmitter, we find sufficient conditions under which Wolfowitz secret communication is possible on the channel via compressive sensing.

We view our work as a step towards providing *constructive* codes with *efficient* decoding for the legitimate receiver and *provably strong secrecy* guarantees with respect to the eavesdropper.

The rest of this paper is organized as follows. Section II gives a description of the system model. Section III presents the main results and Section IV concludes the paper.

Notation: The notation used in this paper is as follows. I_n denotes the identity matrix of size $n \times n$. For a square matrix A, $Tr(A)$ and $det(A)$ represents its trace and determinant. For a vector V, $||V||_1$ and $||V||_2$ denotes its ℓ_1 and ℓ_2 norm.

II. System Model

The system model is depicted in Figure 1, and corresponds to a (potentially) time-varying additive Gaussian noise (AGN) channel. Over n channel uses, the channel model is given by the following relations:

$$Y_L = HX + N_L,$$
$$Y_E = GX + N_E.$$

X is the $n \times 1$ real-valued vector output of transmitter T. Y_L and Y_E are $n \times 1$ vectors seen by legitimate receiver L

and eavesdropper E respectively. N_L and N_E are $n \times 1$ noise vectors with i.i.d. entries from $\mathcal{N}(0, \sigma^2)$ distribution. H and G are $n \times n$ real-valued matrices representing the legitimate receiver's channel and eavesdropper's channel respectively. For simplicity, we assume that H and G are diagonal matrices (potentially time-varying) and have the following forms:

$$H = \begin{pmatrix} h_1 & 0 & \cdots & 0 \\ 0 & h_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_n \end{pmatrix}, G = \begin{pmatrix} g_1 & 0 & \cdots & 0 \\ 0 & g_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_n \end{pmatrix}.$$

We assume in this paper that the diagonal values of H and G are independently generated from some continuous distribution, fixed, and known to all parties (legitimate pair and eavesdropper). Thus, H and G are distinct matrices with probability one, and our scheme exploits this difference to achieve Wolfowitz secret communication.

a) Prior Work and Our Results: For achieving perfect secrecy, [13] shows that the capacity of this wiretap channel, with average power constraint P, is

$$\max_{\Sigma_n : Tr(\Sigma_n) \leq nP} (C_L(\Sigma_n) - C_E(\Sigma_n)),$$

whenever the quantity is a positive number, and where

$$\begin{aligned} C_L(\Sigma_n) &= \frac{1}{n} \log |\sigma^2 I_n + H \Sigma_n H^T|, \\ C_E(\Sigma_n) &= \frac{1}{n} \log |\sigma^2 I_n + G \Sigma_n G^T|. \end{aligned}$$

Although perfect secrecy is highly desirable, achieving rate close to this capacity requires the use of nested lattices or structured binning for codebook generation, for which there are no known polynomial-time decoding algorithms. We also note that these codes are not constructive; probabilistic arguments are used to establish the existence of one good code from an ensemble of codes. Thus, such codes cannot be deployed in practice.

On the practical side, there certainly exist codes that achieve good rate for a given channel, but for such codes, there are no guarantees of secrecy from an eavesdropper. The probability of the eavesdropper recovering the message cannot be made arbitrarily small in such codes, and there are no satisfying theoretical guarantees for secrecy.

Thus, existing approaches addressing the issue of efficient, secret communication either have strong secrecy but are not polynomial time (and are non-constructive in addition) or are constructive and efficient but do not have provable security in an information-theoretic sense.

Ideally, for this problem, we would like a constructive, polynomial time code achieving rate greater than the capacity of the eavesdropper's channel. This would imply Wolfowitz secrecy by the strong converse theorem in addition to efficiency and good rate. Specifically, we know from Wolfowitz's strong converse theorem for the discrete memoryless channel, that if

$$\max_{\Sigma_n : Tr(\Sigma_n) \leq nP} C_L(\Sigma_n) > \max_{\Sigma_n : Tr(\Sigma_n) \leq nP} C_E(\Sigma_n)$$

then a rate of $\max_{\Sigma_n : Tr(\Sigma_n) \leq nP} C_L(\Sigma_n)$ can be achieved by the legitimate transmit-receive pair while the eavesdropper's probability of error in decoding grows exponentially with the coding block size (number of channel uses) to unity. However, this requires a near-capacity achieving code to be employed between the legitimate transmitter receiver pair. Capacity achieving codes that have polynomial-time encoding/decoding algorithms exist for the binary symmetric and certain other classes of channels [14]. However, for the time-varying additive Gaussian noise channel as studied in this paper, a deterministic construction of a low-complexity code is yet to be determined.[1]

Note that, in practice, a near-capacity achieving low-density parity check (LDPC) code or another practical code can be employed that operates at a rate above the capacity of the eavesdropper channel. However, it is hard to provide theoretical guarantees in this setting for Wolfowitz secrecy. Our construction provides an unusual code, based on compressive sensing, which is constructive, provably efficiently encodable and decodable, and comes with a fairly strong secrecy guarantee namely - the probability that the eavesdropper decodes the message correctly can be made arbitrarily small. Unfortunately, the rate achievable using our scheme is hard to determine analytically, and we are performing simulations to determine the maximum rates at which such a compressive sensing based scheme can be utilized in the Wyner wiretap channel.

b) Wolfowitz Secrecy: We consider a new notion of secrecy, which we term as *Wolfowitz secrecy* – the eavesdropper must be unable to decode the message intended for legitimate receiver with high probability (equivalently, the eavesdropper's probability of successful message recovery can be made arbitrarily small). We argue that this is a natural notion of secrecy, one that lies between perfect information theoretic secrecy and computational secrecy. We propose that perfect secrecy is too strong a notion for most applications. Note that perfect secrecy implies that the eavesdropper does not gain *any* information about the message; in particular, from its viewpoint, every other message from the message space seems *equally likely*. For Wolfowitz secrecy, the claim is somewhat weaker, but we argue that the secrecy notion is sufficiently strong nevertheless. Wolfowitz secrecy implies that the probability of error of decoding at the eavesdropper tends to unity. In other words, the eavesdropper can *narrow* its guess of the message somewhat; instead of every point in the message space being an equally likely candidate for the sent message, now, it knows that the message falls in a large fraction (exponential size) of the message space.

[1]Note that multiple polar code constructions for non-time varying AGNs have been proposed [15] based on discretization and/or the central limit theorem, but these are not directly applicable to our case as these schemes can have an extremely high complexity of encoding and decoding depending on number of layers/level of quantization.

However, it still cannot determine the transmitted message with anything but negligible probability, and we believe that this is sufficiently strong for most applications.

c) Efficient Endong/Decoding: In this paper, we desire both Wolfowitz secrecy and polynomial-time encoding/decoding algorithms. There may be multiple ways in which this can potentially be achieved. We choose a compressive sensing framework, and (as we show in the remainder of this paper) this approach yields tractable and non-trivial conditions for possibility of Wolfowitz secret communication over the channel.

For the transmitter, we choose linear encoding, $X = \Phi W$, where W denotes the transmitted message – a vector uniformly chosen from the set of $p \times 1$ k-sparse vectors with non-zero entries coming from the set $\{-1, 1\}$ (k, p are functions of n). Φ is the real-valued $n \times p$ precoding matrix, whose choice depends on H and G.

For the legitimate receiver, decoding based on the popular, efficient LASSO algorithm will suffice (as we show in Section III). We draw the attention of the reader to the fact that the eavesdropper cannot recover the message using LASSO, because our asymmetric linear coding (which depends on matrices H and G) ensures that the effective matrix seen by the eavesdropper will not satisfy the incoherence properties that are required for decoding (while the effective matrix seen by the legitimate receiver will). This is formalized in the next section.

III. Main Results

The wiretap channel model relations can be rewritten as:

$$\begin{aligned} Y_L &= H\Phi W + N_L, \\ Y_E &= G\Phi W + N_E. \end{aligned} \tag{1}$$

The intuition for achieving Wolfowitz secrecy over the channel is as follows: we pick the precoding matrix Φ so that $H\Phi$, the effective channel matrix for legitimate receiver, allows for error-free retrieval (w.h.p.) of sparse vector W from Y_L, while $G\Phi$, the effective channel matrix for eavesdropper, is such that the probability of error in correctly retrieving W from Y_E via any decoding algorithm is arbitrarily close to unity. Note that the structure of the message set makes it sufficient for the decoder at the legitimate receiver to recover only the signed support[2] of W in order to recover W. This motivates the use of a Lasso-based decoder at the legitimate receiver.

A. Accurate Recovery by Legitimate Receiver:

Since the legitimate receiver has knowledge of channel matrix H, it recovers W from the following equivalent system:

$$Y_L' = \Phi W + N_L', \tag{2}$$

where

$$Y_L' = H^{-1} Y_L$$

and

$$N_L' = H^{-1} N_L.$$

This system resembles the compressive sensing setup with noisy observations/measurements. The sufficient conditions required for accurate recovery of signed support of sparse vector in presence of i.i.d. gaussian noise using Lasso have been described in [10]. However, unlike in [10], in our case the noise vector N_L' does not consist of i.i.d. entries (the noise variances can potentially vary with channel uses). Hence, we need to re-derive the sufficient conditions under which accurate signed support recovery is possible, to enable error-free message recovery at the legitimate receiver using the Lasso-based decoder:

$$\hat{W} = \underset{V \in \mathbb{R}^p}{\operatorname{argmin}} \left\{ \frac{1}{2n} ||Y_L' - \Phi V||_2^2 + \lambda_n ||V||_1 \right\},$$

where λ_n is the regularizing parameter (function of n).

We choose Φ to be a random matrix with i.i.d. entries coming from the distribution $\mathcal{N}(0, \tau)$, where τ is suitably chosen depending on channel matrices H and G. The following theorem (modified version of Theorem 3 in [10]) states the sufficient conditions on n, p, k and τ for accurate signed support recovery of W using Lasso at the legitimate receiver:

Theorem 1. *Consider the system model described by Equation (2) and the following family of regularizing parameters:*

$$\lambda_n := \sqrt{\frac{\sigma^2 \tau}{\nu h_{min}^2 k}}$$

where ν is some constant and $h_{min} = \min(|h_1|, \ldots, |h_n|)$. Then, if for some fixed $\epsilon > 0$, the sequence $\{n, p, k\}$ satisfies

$$n > 2(1+\epsilon)(1+\nu) k \log(p-k), \tag{3}$$

with probability greater than

$$1 - c_1 \exp(-c_2 \min(k, \log(p-k))),$$

we have that:

- *Lasso returns a unique solution $\hat{W}$ whose support is contained in the support of W ($supp(\hat{W}) \subset supp(W)$).*
- *Lasso further recovers the signed support uniquely if*

$$\tau > \left(c_3 \sqrt{\frac{\sigma^2}{\nu h_{min}^2 k}} + c_4 \sqrt{\frac{\sigma^2 \log k}{h_{min}^2 n}} \right)^2. \tag{4}$$

Here, c_1, c_2, c_3, c_4 are some positive constants.

Proof: Our proof follows the lines of the proof of achievability for Lasso (Theorem 3) in [10]. The covariance matrix of our choice, Φ, satisfies the incoherence conditions specified in [10], which implies applicability of Theorem 3 in [10]. The only change in our analysis is that the noise vector N'_L does not contain i.i.d entries. However, the entries of N'_L are still independent random variables, and their variance does not exceed σ^2/h_{min}^2. This gives

$$||N_L'||_2^2 \leq ||N_L||_2^2 / h_{min}^2$$

[2]Signed support of a sparse vector refers to its support (indices of non-zero entries) as well as signs (+/-) of the non-zero entries.

and rest of the analysis follows from the achievability proof. ∎

We define $k = \mu n/\log n$, and $p = n^{\alpha+1}$ for some $\alpha, \mu > 0$. Then, the bound on τ as in Equation (4) can be reduced to

$$\tau \geq \tau_{min} := \frac{\sigma^2}{h_{min}^2} \underbrace{\left(\frac{c_3}{\sqrt{\mu\nu}} + c_4\right)^2}_{c_5(\mu,\nu)} \frac{\log n}{n}. \tag{5}$$

Also note that the transmitted signal is subject to an average power constraint P, i.e., $E(X^T X) \leq nP$. We statistically approximate message vector W as follows: for $i = 1, \ldots, p$, we let $W_i = 1$ w.p. $k/2p$, -1 w.p. $k/2p$ and 0 otherwise. This approximation yields the following additional constraint on τ:

$$\tau \leq \frac{P}{k} = \frac{P}{\mu}\frac{\log n}{n}. \tag{6}$$

Equations (5) and (6) impose a condition on the SNR of the system as

$$\text{SNR} := P/\sigma^2 \geq \gamma := \mu c_5(\mu,\nu)/h_{min}^2.$$

Therefore, we have determined the sufficient conditions for accurate recovery of message by the legitimate receiver.

B. Infeasible Recovery by Eavesdropper:

In this section, we examine the conditions necessary for decoding failure (with high probability) at the eavesdropper. We let R_E be the rate of the eavesdropper's channel. Then, we have by information theoretic analysis:

$$\begin{aligned} nR_E &:= I(Y_E; W) \\ &= E_p\left[\log \frac{p(Y_E|W)}{p(Y_E)}\right] \quad (p := p(W, Y_E)) \\ &\leq E_p\left[\log \frac{p(Y_E|W)}{q(Y_E)}\right] \quad (\text{any dist. } q(Y_E)) \\ &\leq -h(N_E) + E_p\left[\log \frac{1}{q(Y_E)}\right]. \end{aligned} \tag{7}$$

Let $q(Y_E) \sim \mathcal{N}(0, \Delta)$, $\Delta = \Gamma^2$ and $det(\Delta) = \beta$. Then,

$$\begin{aligned} E_p\left[\log \frac{1}{q(Y_E)}\right] &= \frac{1}{2}\log(2\pi)^n\beta + \frac{1}{2}E_p\left[Y_E^T \Delta^{-1} Y_E\right] \\ &= \frac{1}{2}\log(2\pi)^n\beta + \frac{1}{2}E_p\left[\widehat{Y_E}^T \widehat{Y_E}\right], \end{aligned}$$

where we set $\widehat{Y_E} := \Gamma^{-1} Y_E$. Using Equation (1), we get

$$\begin{aligned} E_p\left[\widehat{Y_E}^T \widehat{Y_E}\right] &= Tr\left(E_p\left[\widehat{Y_E}\widehat{Y_E}^T\right]\right) \\ &= Tr\left(\Gamma^{-1} E_p\left[(G\Phi W W^T \Phi^T G^T) + \sigma^2 I_n)\right]\Gamma^{-1}\right) \\ &= Tr\left(\Gamma^{-1}\left(\frac{k}{p} G E_p[\Phi\Phi^T] G^T + \sigma^2 I_n\right)\Gamma^{-1}\right) \\ &= Tr\left(\Gamma^{-1}\left(k\tau GG^\top + \sigma^2 I_n\right)\Gamma^{-1}\right). \end{aligned}$$

Assume $\Delta = \theta I_n$, $\theta > 0$, so that $\Gamma^{-1} = \theta^{-1/2} I_n$. Then,

$$E_p\left[\widehat{Y_E}^T \widehat{Y_E}\right] = \frac{1}{\theta} Tr(k\tau GG^T + \sigma^2 I_n).$$

This relation, along with the fact $det(\Delta) = \beta = \alpha^n$, gives

$$E_p\left[\log \frac{1}{q(Y_E)}\right] = \frac{1}{2}\log(2\pi)^n\alpha^n + \frac{1}{2\theta} Tr(k\tau GG^T + \sigma^2 I_n).$$

Substituting the above expression in Equation (7) gives

$$R_E \leq \frac{-1}{2} - \frac{1}{2}\log\sigma^2 + \frac{1}{2}\log\theta + \frac{1}{2\theta}\left(\frac{k\tau}{n} Tr(GG^T) + \sigma^2\right).$$

The RHS of the above expression is minimized for

$$\theta = \frac{k\tau}{n} Tr(GG^\top) + \sigma^2.$$

Substituting this value of θ yields

$$R_E \leq \frac{1}{2}\log\left(1 + \frac{k\tau}{\sigma^2}\frac{Tr(GG^T)}{n}\right).$$

Next, note that

$$Tr(GG^T) = \sum_{i=1}^{n} |g_i|^2 := n\bar{g}^2.$$

This gives

$$R_E \leq \frac{1}{2}\log\left(1 + \frac{k\tau}{\sigma^2}\bar{g}^2\right). \tag{8}$$

Also, from construction of the message space, we have

$$R_E = \frac{1}{n}\log\left[\binom{p}{k} 2^k\right], \tag{9}$$

if accurate message recovery is possible for the eavesdropper. Hence, by Equations (8) and (9), we get a sufficient condition, for infeasibility of message recovery by eavesdropper, as:

$$n < \frac{2(\log\binom{p}{k} + k\log 2)}{\log(1 + \frac{k\tau}{\sigma^2}\bar{g}^2)}. \tag{10}$$

Thus, if the above inequality is satisfied, by Wolfowitz's strong converse theorem, the probability of decoding error at the eavesdropper tends to unity as code block size increases. Note that all the parameters in the equation- n, p, k are tending to infinity, and we desire that this inequality always be satisfied for secret communication.

C. Putting it all together: Accurate Recovery by Legitimate Receiver as well as Infeasible Recovery by Eavesdropper:

We desire to find n such that the legitimate receiver can recover the message efficiently using Lasso while the eavesdropper cannot recover the message. For this, we put together the derived conditions as given by Equations (3), (4), (10):

$$2(1+\epsilon)(1+\nu)k\log(p-k) < n < \frac{2(\log\binom{p}{k} + k\log 2)}{\log(1 + \frac{k\tau}{\sigma^2}\bar{g}^2)},$$

subject to $\tau > \tau_{min}$. We set $\tau = \tau_{min}$, since it maximizes the range of n, as observed in the above expression. Substituting $k = \mu n/\log n$, $p = n^{\alpha+1}$ and simplification gives the following sufficient condition for existence of n, μ and α:

$$\frac{1}{2}\log\left(1 + \mu c_5(\mu,\nu)\frac{\bar{g}^2}{h_{min}^2}\right) < \frac{1}{2(1+\epsilon)(1+\nu)} - \mu. \tag{11}$$

Note that the LHS of the above expression is an increasing function of μ, while the RHS is a decreasing function of μ. Therefore, suitable μ, α exist if for $\mu \to 0$, the inequality is still preserved. Letting $\mu \to 0$ in Equation (11) gives

$$\log\left(1 + \frac{c_3^2}{\nu}\frac{\bar{g}^2}{h_{min}^2}\right) < \frac{1}{(1+\epsilon)(1+\nu)}.$$

After rearranging, we get the following sufficient condition:

$$\bar{g}^2 < \delta(\epsilon,\nu)h_{min}^2,$$

where

$$\delta(\epsilon,\nu) := (\nu/c_3^2)(\exp([(1+\epsilon)(1+\nu)]^{-1}) - 1).$$

Thus, if the average singular value of G is less than a constant multiple of the minimum singular value of H then there exists values for n, μ and α that enables Wolfowitz secret communication over the Wyner wiretap channel.

D. A Word about the Rate of Legitimate Receiver:

For $k = \mu n/\log n$ and $p = n^{\alpha+1}$ and from construction of the message space, the rate of legitimate receiver is given by

$$R_L = \frac{1}{n}\left[\log\binom{p}{k}2^k\right] \xrightarrow{n\to\infty} \alpha\mu,$$

subject to constraints given by Equations (3) and (10). There is an upper bound on R_L imposed by the maximum achievable rate on the legitimate channel subjected to the codebook architecture (k-sparse p-length message vectors in our case), as well as because of Equations (3) and (10). It is difficult, analytically, to obtain a closed form expression for the above-mentioned bound on R_L. Hence, to understand the rate achieved by our specific codebook architecture, we are performing some simulations. The simulations are work in progress, and its results are deferred to the full version of this work.

IV. Conclusions

We have seen how compressive sensing can be used to construct an unusual code that helps obtain secrecy benefits in a wiretap channel. We view this work as a step in the direction of constructing explicit, efficient codes with provable secrecy.

The rates achieved by such a scheme is non-trivial to characterize, and we are simulating the system to better understand this. Even though we are currently unable to provide guarantees on the rate of the legitimate receiver, we believe the techniques in the paper (of using compressive sensing for secret communication) are of independent interest.

References

[1] David Donoho, "Compressed sensing," *IEEE Trans. on Information Theory*, Vol. 52, No. 4, pp. 1289–1306, April 2006.

[2] Emmanuel Candes and Terence Tao, "Near optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Trans. on Information Theory*, Vol. 52, No. 12, pp. 5406–5425, December 2006.

[3] Joel Tropp and Anna Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. on Information Theory*, Vol. 53, No. 12, pp. 4655–4666, December 2007.

[4] Shriram Sarvotham, Dror Baron, and Richard Baraniuk, "Sudocodes - Fast measurement and reconstruction of sparse signals," *IEEE Int. Symposium on Information Theory (ISIT)*, Seattle, Washington, July 2006.

[5] David Donoho and Yaakov Tsaig, "Fast solution of ℓ_1-norm minimization problems when the solution may be sparse," *Stanford University Department of Statistics Technical Report*, 2006.

[6] David Donoho, "For most large underdetermined systems of linear equations, the minimal ℓ_1 norm solution is also the sparsest solution," *Communications on Pure and Applied Mathematics*, Vol. 59, pp. 797–829, June 2006.

[7] E. J. Candes and T. Tao, "The Dantzig selector: statistical estimation when p is much larger than n," *Annals of Statistics*, Vol. 35, pp. 2392–2404.

[8] R. Tibshirani, "Regression shrinkage and selection via the lasso," *Royal Statistical Society, Ser. B*, Vol. 58, No. 1, pp. 267–288, 1996.

[9] Emmanuel Candes and Justin Romberg, "Sparsity and incoherence in compressive sampling," *Inverse Problems*, Vol. 23, pp. 969–985, 2007.

[10] M. J. Wainwright, "Sharp thresholds for noisy and high-dimensional recovery of sparsity using ℓ_1-constrained quadratic programming (Lasso)", *IEEE Transactions on Information Theory*, 2009.

[11] J. J. Fuchs, "Recovery of exact sparse representations in the presence of noise," *IEEE Transactions on Information Theory*, Vo. 51, No. 10, pp. 3601–3608, October 2005.

[12] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, Vol. 52, No. 2, pp. 489-509, February 2004.

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

[14] S. Korada, "Polar codes for channel and source coding", PhD disseration, EPFL, 2009.

[15] E. Abbe and A. Barron, "Polar coding schemes for the AWGN channel", preprint.