Compressed Sensing Encryption: Compressive Sensing Meets Detection Theory

Mahmoud Ramezani-Mayiami,[1] Hamid G. Bafghi[2], and Babak Seyfe[3]
[1] WISENET Lab, University of Agder, Grimstad, Norway.
[2] Wireless Research Lab., Sharif University of Technology, Tehran, Iran.
[3] ITLS Lab, Shahed University, Tehran, Iran.
Email: mahmoud.ramezani@uia.no; h.bafghi@staff.sharif.edu; seyfe@shahed.ac.ir

Abstract—Since compressive sensing utilizes a random matrix to map the sparse signal space to a lower dimensional transform domain, it may be possible to apply this matrix at the same time for encrypting the signal opportunistically. In this paper, a compressed sensing based encryption method is considered and the secrecy of the measurement matrix of compressive sensing analyzed from the detection theory perspective. Here the detection probabilities of the intended and unintended receivers are compared by applying the Neyman-Pearson test. We prove that the detection probability of the eavesdropper will be reduced significantly because he does not know the transform domain sub-space. Furthermore, in some situations, the unintended receiver's probability of detection may be decreased to 0.5, which makes the eavesdropped data useless, i.e., perfect secrecy will be achieved theoretically. On the other hand, from an information theoretic point of view, since the signal to noise ratio are different for the main and wiretapper channels, we showed that it is possible to design a measurement matrix for secure transmission even when the wiretapper knows the measurement matrix.

Index Terms—Compressive sensing, detection, perfect secrecy, secret communication, probability of detection, measurement rate, secrecy rate region.

I. Introduction

The theory of compressed sensing (CS) or compressive sampling introduced and expanded in [1] and [2] proposes that it is possible to sense and compress the signal simultaneously. Although it is the exact concept of CS, a number of applications have used CS to implement wide range of applications, such as image processing [3] and channel estimation [4].

Also, several research studies have used compressive sensing to decide between two hypotheses, which is the main contribution of the signal detection framework. For example, Duarte and his colleagues [5] proposed an approach to solve a signal detection problem from the incoherent projections without reconstructing the exact signal. Davenport and his colleagues [6] used compressive measurements to detect signals contaminated with Gaussian noise instead of recovering the signal first and making the decision consequently. They calculated sufficient statistics based on the compressive measurements and proposed a method to decide which hypothesis is correct when the receiver knows the underlying measurement matrix.

On the other hand, Orsdemir *et al*. [7] unified the sensing, compression and encryption of the signal in a simple linear measurement step using a pseudo-random generated sampling matrix to offer a method for encrypting the signal via CS without requiring extra computational cost. What is more, the security and robustness of this method were investigated and the results showed that the CS-based encryption method makes attacking more difficult in practice and since it is fairly robust against additive noise, it can be used as an encryption approach for multimedia signals. Also, from an information theoretic perspective, Rachlin and Baron [8] proved that it is impossible to achieve perfect secrecy through compressive measurements. However, in our previous work [9], we found two conditions in which Shannon definition of perfect secrecy was held.

In this paper, the secrecy of a CS measurement matrix was evaluated from a detection theory viewpoint where a Neyman-Pearson test was applied to find the relationship between a false alarm and the probability of detection. When the receiver is unintended and does not know the underlying compression/encryption matrix, it has to try several measurement matrices to detect the correct hypothesis. Herein, we will show that the detection probability of the eavesdropper was reduced to 0.5 for a specific set of measurement matrices. The remainder of the paper is organized as follows: In section II, we review the concept of CS and the basics of signal detection. Our main idea is proposed in Section III. We will discuss more results and conclude in Sections IV and VI, respectively.

II. Background

A. Compressive Sensing

Suppose $\boldsymbol{x}\epsilon\mathcal{R}^N$ to be a K-sparse signal, i.e., K elements of $\boldsymbol{x}$ are non-zero for $K \ll N$ or the coefficient vector of $\boldsymbol{x}$ in some orthonormal basis has K non-zero elements. For example, suppose $\boldsymbol{x} = \boldsymbol{\Psi\alpha}$, where $\boldsymbol{\Psi}\epsilon\mathcal{R}^{N\times N}$ is a transform basis and $\boldsymbol{\alpha}\epsilon\mathcal{R}^N$ is a weighting coefficient

Manuscript received August 30, 2017; revised January 31, 2018.
Mahmoud Ramezani-Mayiami was with the ECE department of Shahed University, Tehran, Iran. He is now working towards a Ph.D. degree at the Department of Information and Communication Technology, University of Agder, Grimstad, Norway.
Corresponding author email: Mahmoud.ramezani@uia.no
doi:10.12720/jcm.13.2.82-87

vector, which has K non-zero entries. The compressed sensing or compressive sampling (CS) framework proposed is not essential to sense and compress the sparse signal in two separate consequent stages, since we can apply the compressing and sensing process simultaneously by implementing $\boldsymbol{y} = \boldsymbol{\Phi x}$, where $\boldsymbol{y}$ and $\boldsymbol{\Phi}$ are the $M \times 1$ measurement vector and $M \times N$ measurement matrix, respectively. Since this system of linear equations is underdetermined ($M \ll N$), $\boldsymbol{x}$ cannot be recovered by conventional mathematics. Then designing a measurement matrix for a specific application is directly related to the inverse problem and signal reconstructions.

In [1] and [2], it was stated that we can recover $\boldsymbol{x}$ from the measurement vector $\boldsymbol{y} = \boldsymbol{\Phi x}$, where $\boldsymbol{\Phi}$ is incoherent with $\boldsymbol{\Psi}$. Incoherency means that no columns of $\boldsymbol{\Psi}$ have a sparse representation relative to any rows of $\boldsymbol{\Phi}$ and vice versa. Candes and Tao [11] proved that if $\boldsymbol{\Phi}$ is generated by sampling from an independent and identically distributed Gaussian random variable with zero mean and variance $\frac{1}{M}$, it is incoherent with high probability with respect to any transform basis $\boldsymbol{\Psi}$.

Assume $\boldsymbol{A} = \boldsymbol{\Phi\Psi}$ is the holographic dictionary. Then the following general optimization problem was applied for signal reconstruction [12]:

$$P_0: \min_{\boldsymbol{\alpha}} \|\boldsymbol{\alpha}\|_0 \text{ subject to } \boldsymbol{y} = \boldsymbol{A\alpha}. \tag{1}$$

Here and below, $\|\boldsymbol{\alpha}\|_p$ indicates l_p-norm defined as $\|\boldsymbol{\alpha}\|_p = \sqrt[p]{\sum_{i=1}^{N} |\alpha_i|^p}$ and α_i are the entries of vector α_i for $1 < i < N$. In the special case for $p = 0$, $\|\boldsymbol{\alpha}\|_0$ is computed as the limit of l_p-norm for $p \to 0$. Roughly speaking, $\|\boldsymbol{\alpha}\|_{\boldsymbol{0}}$ counts the non-zero elements in $\boldsymbol{\alpha}$.

The optimization problem (1) can be solved by several methods such as matching pursuit (MP), orthogonal matching pursuit (OMP) [13], [14] and stagewise orthogonal matching pursuit (StOMP) [15]. Since P_0 is a non-convex optimization problem, it needs an exhaustive search over all possible solutions, which is computationally expensive. Another solution for reconstructing x from y was proposed through P_1 as follows [12]:

$$P_1: \min_{\boldsymbol{\alpha}} \|\boldsymbol{\alpha}\|_1 \text{ subject to } \boldsymbol{y} = \boldsymbol{A\alpha} \tag{2}$$

Candes and Tao [11] proved that if the measurement matrix satisfies the restricted isometry property (RIP), P_1 proposes a solution using linear programming, which is identical to the solution of P_0.

Definition 1: $\boldsymbol{\Phi}$ respects RIP of order K whenever a $\varepsilon_k \epsilon (0,1)$ exists such that

$$(1 - \varepsilon_k)\|\boldsymbol{x}\|_2 \leq \|\boldsymbol{\Phi x}\|_2 \leq (1 + \varepsilon_k)\|\boldsymbol{x}\|_2 \tag{3}$$

holds for all K-sparse vector $\boldsymbol{x}$.

B. Nayman-Pearson Test

In the binary hypothesis testing of detection theory, the main problem is choosing one of the two existing hypotheses, the null hypothesis H_0 and the alternative hypothesis H_1 defined as follows:

$$\begin{aligned} H_0: &\quad \boldsymbol{r} = \boldsymbol{n} \\ H_1: &\quad \boldsymbol{r} = \boldsymbol{s} + \boldsymbol{n} \end{aligned} \tag{4}$$

where $\boldsymbol{s} \epsilon \mathcal{R}^N$ and $\boldsymbol{r} \epsilon \mathcal{R}^N$ are the transmitted and received signal, respectively and $\boldsymbol{n} \sim \mathcal{N}(0, \sigma^2 I_N)$ is an independent and identically distributed (i.i.d) additive white Gaussian noise with zero mean and variance σ^2. Herein, we use the Neyman-Pearson (NP) rule to distinguish between H_0 and H_1 [10]. The NP detector maximizes the probability of detection P_D while the false alarm probability P_F is fixed, where P_D and P_F are defined as follows:

$$\begin{aligned} P_F &= Pr(H_1 | H_0 \; is \; correct) \\ P_D &= Pr(H_1 | H_1 is \; correct) \end{aligned} \tag{5}$$

Also, it is proved that for Gaussian noise the sufficientstatistic t and the decision threshold ζ are as follows:

$$\begin{aligned} t &= < \boldsymbol{r}, \boldsymbol{s} > = \boldsymbol{r}^T \boldsymbol{s} \\ \zeta &= Q^{-1}(\alpha)\sigma \parallel \boldsymbol{s} \parallel_2 \end{aligned} \tag{6}$$

where α is the constant level of the false alarm probability and $Q(\tau) = (2\pi)^{-0.5} \int_{\tau}^{\infty} e^{\frac{-u^2}{2}} du$. Also, $(.)^T$ and $< \boldsymbol{r}, \boldsymbol{s} >$ denote to the transpose of the vector and inner product, respectively.

III. Main Idea

In the conventional method of digital communication, the data samples should be firstly collected from the source and then compressed based on the underlying signal features. Finally, we should apply an encryption method to transmit it securely via a wireless channel. This approach not only wastes time, but also includes additional computational complexity since three separate steps must be implemented. On the other hand, CS-based encryption unifies these three stages of sensing, compressing, and encrypting with a low computational cost. Here, in the same way, suppose we have compressive measurements instead of entire Nyquist samples of the signal and are interested in sending them to the intended receiver via a noisy channel. Then, the hypotheses are as follows:

$$\begin{aligned} H_0: &\quad \boldsymbol{r} = \boldsymbol{n} \\ H_1: &\quad \boldsymbol{r} = \boldsymbol{\Phi s} + \boldsymbol{n} \end{aligned} \tag{7}$$

Since the intended receiver knows the measurement matrix $\boldsymbol{\Phi}$, by multiplying the received signal by $\boldsymbol{\Phi'} = (\boldsymbol{\Phi^T \Phi})^{-1} \boldsymbol{\Phi^T}$, the above hypotheses are rewritten as follows:

$$\begin{aligned} H_0: &\quad \boldsymbol{\Phi' r} = \boldsymbol{\Phi' n} \\ H_1: &\quad \boldsymbol{\Phi' r} = \boldsymbol{\Phi' \Phi s} + \boldsymbol{\Phi' n} \end{aligned} \tag{8}$$

Here and below, $(.)'$ and $(.)^{"}$ denote to the intended and unintended receivers, respectively. Hence, the hypotheses of intended receiver are as follows:

$$\begin{aligned} H_0&: \quad \boldsymbol{r}' = \boldsymbol{n}' \\ H_1&: \quad \boldsymbol{r}' = \boldsymbol{s} + \boldsymbol{n}' \end{aligned} \tag{9}$$

where we use the estimate $\boldsymbol{s} \cong \boldsymbol{\Phi}'\boldsymbol{\Phi}\boldsymbol{s}$ [6] for the alternative hypothesis. Because n is a Gaussian random variable, its linear inner products with the measurement matrix elements have a Gaussian probability density function (pdf). Then, we have $\boldsymbol{n}' \sim \mathcal{N}(\mu, \eta)$ with the following mean and variance,

$$\begin{aligned} \mu &= E[\boldsymbol{n}'] = E[\boldsymbol{\Phi}'\boldsymbol{n}] = E[(\boldsymbol{\Phi}^{\boldsymbol{T}}\boldsymbol{\Phi})^{-1}\boldsymbol{\Phi}^{\boldsymbol{T}}\boldsymbol{n} = 0 \\ \eta &= E[\boldsymbol{n}'\boldsymbol{n}'^{T}] = E[\boldsymbol{\Phi}'\boldsymbol{n}\boldsymbol{n}^{T}\boldsymbol{\Phi}'^{T} = \sigma^2(\boldsymbol{\Phi}^{T}\boldsymbol{\Phi})^{-1} \end{aligned} \tag{10}$$

Under the hypotheses H_0 and H_1, the probability density functions of the received signal are as follows:

$$\begin{aligned} f_0(\boldsymbol{r}') &= \frac{\exp(-\boldsymbol{r}'^{T}(\boldsymbol{\Phi}^{\boldsymbol{T}}\boldsymbol{\Phi})\boldsymbol{r}'/2\sigma^2)}{|\sigma^2(\boldsymbol{\Phi}^{\boldsymbol{T}}\boldsymbol{\Phi})^{-1}|(2\pi)^{N/2}} \\ f_1(\boldsymbol{r}') &= \frac{\exp(-\{\boldsymbol{r}'^{T}(\boldsymbol{\Phi}^{\boldsymbol{T}}\boldsymbol{\Phi})\boldsymbol{r}' - 2\boldsymbol{r}'^{T}(\boldsymbol{\Phi}^{\boldsymbol{T}}\boldsymbol{\Phi})\boldsymbol{s} + \| \boldsymbol{\Phi}\boldsymbol{s} \|_2^2\}/2\sigma^2)}{|\sigma^2(\boldsymbol{\Phi}^{\boldsymbol{T}}\boldsymbol{\Phi})^{-1}|(2\pi)^{N/2}} \end{aligned} \tag{11}$$

By using the likelihood ratio test for the hypotheses of (9), the sufficient test statistic t is as follows:

$$t' = \boldsymbol{r}'^{T}\boldsymbol{s} = \boldsymbol{r}^{T}\boldsymbol{\Phi}(\boldsymbol{\Phi}^{T}\boldsymbol{\Phi})^{-1}\boldsymbol{s} \tag{12}$$

If we use the orthoprojector matrix ($\boldsymbol{\Phi}$ is orthoprojector matrix if $\boldsymbol{\Phi}\boldsymbol{\Phi}^{T}$ is an identity matrix), the test statistic is reduced to $t' = < \boldsymbol{r}, \boldsymbol{\Phi}\boldsymbol{s} >$ [6]. After some manipulations, the pdf of t' under the two hypotheses is as follows:

$$\begin{aligned} &if\ H_0\ is\ correct: t' \sim \mathcal{N}(0, \sigma^2 \| \boldsymbol{\Phi}\boldsymbol{s} \|_2^2) \\ &if\ H_1\ is\ correct: t' \sim \mathcal{N}(\| \boldsymbol{\Phi}\boldsymbol{s} \|_2^2, \sigma^2 \| \boldsymbol{\Phi}\boldsymbol{s} \|_2^2) \end{aligned} \tag{13}$$

Suppose $P_F' = \alpha$, then we have the threshold $\zeta' = Q^{-1}(\alpha)\sigma \| \boldsymbol{\Phi}\boldsymbol{s} \|_2$ and the probability of detection can be calculated as follows:

$$\begin{aligned} P_D'(\alpha) = \Pr(t' > \zeta' | H_1) &= Q\left(\frac{\zeta' - \| \boldsymbol{\Phi}\boldsymbol{s} \|_2^2}{\sigma \| \boldsymbol{\Phi}\boldsymbol{s} \|_2}\right) \\ &= Q(Q^{-1}(\alpha) - \frac{\| \boldsymbol{\Phi}\boldsymbol{s} \|_2}{\sigma}) \end{aligned} \tag{14}$$

The probability of detection for the intended user is achieved like the one for the compressive detector [6] as shown below when an orthoprojector matrix is applied.

$$P_D(\alpha) = Q\left[Q^{-1}(\alpha) - \sqrt{M/N}\sqrt{\frac{\| \boldsymbol{s} \|_2^2}{\eta}}\right] \tag{15}$$

The probability of detection is reduced regarding the fact that $\sqrt{M/N} < 1$, which denotes the CS effect. However, this reduction is the cost of unified compressing, sensing, and encryption for secret transmission with low computational complexity.

Now, we are interested in finding the probability of detection for the eavesdropper who has no a priori information in regard the sensing matrix's elements except its dimension $M \times N$. Suppose that the eavesdropper generates the sampling matrix erroneously namely $\boldsymbol{\Gamma}$. Hence, his test statistic and threshold are as follows:

$$\begin{aligned} t^{"} &= \boldsymbol{r}'^{T}\boldsymbol{\Gamma}\boldsymbol{s}, \\ \zeta^{"} &= Q^{-1}(\alpha)\sigma \| \boldsymbol{\Gamma}\boldsymbol{s} \|_2. \end{aligned} \tag{16}$$

The pdf for the above sufficient statistic and the probability of detection are as (17) and (18), respectively

$$\begin{aligned} &if\ H_0\ is\ correct: t^{"} \sim \mathcal{N}(0, \sigma^2 \| \boldsymbol{\Gamma}\boldsymbol{s} \|_2^2) \\ &if\ H_1\ is\ correct: t^{"} \sim \mathcal{N}(\boldsymbol{s}^{T}\boldsymbol{\Phi}^{T}\boldsymbol{\Gamma}\boldsymbol{s}, \sigma^2 \| \boldsymbol{\Phi}\boldsymbol{s} \|_2^2) \end{aligned} \tag{17}$$

$$\begin{aligned} P_D^{"}(\alpha) = Pr(t^{"} > \zeta^{"} | H_1) &= Q\left(\frac{\zeta^{"} - \boldsymbol{s}^{T}\boldsymbol{\Phi}^{T}\boldsymbol{\Gamma}\boldsymbol{s}}{\sigma \| \boldsymbol{\Gamma}\boldsymbol{s} \|_2}\right) \\ &= Q\left(Q^{-1}(\alpha) - \sqrt{\frac{\boldsymbol{s}^{T}\boldsymbol{\Phi}^{T}\boldsymbol{\Gamma}\boldsymbol{s}}{\sigma \| \boldsymbol{\Gamma}\boldsymbol{s} \|_2^2}}\right) \end{aligned} \tag{18}$$

or equivalently we can rewrite it in the inner product form as follows:

$$P_D^{"}(\alpha) = Q\left(Q^{-1}(\alpha) - \frac{\| \boldsymbol{\Phi}\boldsymbol{s} \|_2}{\sigma}\frac{< \boldsymbol{\Phi}\boldsymbol{s}, \boldsymbol{\Gamma}\boldsymbol{s} >}{\| \boldsymbol{\Phi}\boldsymbol{s} \|_2 \| \boldsymbol{\Gamma}\boldsymbol{s} \|_2}\right) \tag{19}$$

IV. Discussion

From a mathematical viewpoint, $< \boldsymbol{\Phi}\boldsymbol{s}, \boldsymbol{\Gamma}\boldsymbol{s} > = \| \boldsymbol{\Phi}\boldsymbol{s} \|_2 \| \boldsymbol{\Gamma}\boldsymbol{s} \|_2 \cos(\theta)$, where $0 < \cos(\theta) < 1$ and θ can be assumed as the angle between the sub-spaces of $\boldsymbol{\Phi}\boldsymbol{s}$ and $\boldsymbol{\Gamma}\boldsymbol{s}$. To analyze the boundary situations, first suppose $\cos(\theta) = 1$; i.e., $P_D^{"} = P_D'$ when the eavesdropper can find the same amount of information from transmitted signal as the intended receiver. On the other hand, if $\cos(\theta) = 0$, i.e., the compressed measurement's sub-space is orthogonal to the unintended receiver's one, the eavesdropped signal is completely useless, since eavesdropper's probability of detection is 0.5 or $P_D^{"} = P_F^{"}$. From the information theoretic perspective this situation happens when perfect secrecy is held. As we proved in our previous work [9], when the measurement matrix holds the RIP and $M \geq 2K$, the Shannon perfect secrecy condition is held either if the message set's cardinality tends to infinity or the message set has no zero message, which are practical assumptions. It is useful to note that generally we have $0 < \cos(\theta) < 1$, which confirms the fact that there are some situations in which the compressive sensing based encryption cannot provide perfect secrecy, which has been previously proven by Rachlin and Baron in [8]. They calculated the mutual information between the cryptogram $\boldsymbol{r} = \boldsymbol{\Phi}\boldsymbol{s}$ and plain text $\boldsymbol{s}$, and showed that for general cases $(\boldsymbol{s}; \boldsymbol{r}) > 0$.

On the other hand, according to (14), the probability of detection for the intended receiver is directly proportional

to the signal to noise ratio (SNR). Then if $SNR = \frac{\|\boldsymbol{\Phi s}\|_2^2}{\sigma^2}$ is increased, P_D' also increases for the intended receiver while the detection probability of the eavesdropper does not follow this increase since it is a function of $\frac{<\boldsymbol{\Phi s}, \boldsymbol{\Gamma s}>}{\sigma\|\boldsymbol{\Gamma s}\|_2}$ in (19). Moreover, it is necessary to note that all the above analyses are based on a worst-case scenario in which the unintended receiver has a priori knowledge of the measurement matrix dimensions. Otherwise, the detection probability for the unintended receiver gets worse than the one presented here and the compressive sensing based encryption has better performance.

V. Secrecy Constraint

As mentioned above, the transmitter uses the measurement matrix for mapping the signal space into a new space, which is known for the intended receiver. Also, the intended receiver uses the same sampling matrix to decrypt the received signal after detection. The eavesdropper tries to find an estimation of matrix $\boldsymbol{\Phi}$ to decode/decrypt the received signal without any a-prior information via some methods, such as blind source separation (BSS) [1] and [16]–[18]. Moreover, there are some approaches to decode a sparse signal from the received mixture signal based on the scarcity property of the primal signal and have some limitations on the number of measurement coefficients used for compressing the primal signal [16]. Some of these methods like sparse component analysis (SCA) sparsifies the received signal and estimates the measurement matrix from the scatter plot of the received signal using independent component analysis (ICA) or clustering techniques with a variant of weighted K-means. Using these methods under some constraints shows that the eavesdropper, which does not know the measurement matrix, can still extract the primal signal with a few trial and errors. Besides the constraints forced by the BSS method to extract the message from the received signal, there are some constraints on the number of measurements needed for reconstruction. As we assumed before, the received signal is a noisy version of the compressed primal signal. This measurement and transmission noise is the crucial factor that dictates the number of measurements needed for reconstruction [19].

The CS reconstruction can be performed via l_1 minimization by applying linear programming techniques, which requires approximately $K\,log(N/K)$ measurements [1]. Moreover, it is proved that we cannot reconstruct a K -sparse signal using fewer than $M = K + 1$ measurements [20]. However, the only approach for CS reconstruction using only $M = K + 1$ measurements is via l_0 -minimization, known to be NP-complete and therefore impractical [21].

Proposing Lemma 1, Sarvotham *et al.* [19] lower bounded the rate-distortion performance of a CS system.

Lemma 1: For a signal source with rate-distortion function $R(.)$, the lower bound on the CS measurement rate required to obtain a normalized reconstruction error $\mathcal{E}(\mathcal{D}_s)$ subject to a fixed SNR is given by:

$$\delta \geq \frac{2R\big(\mathcal{E}(\mathcal{D}_s)\big)}{log(1+\mathrm{SNR})} \tag{20}$$

where $\delta = \frac{M}{N}$ and the SNR measurement is defined as follows:

$$SNR = \frac{E[\|\boldsymbol{\Phi s}\|_2^2]}{E[\|\boldsymbol{n}\|_2^2]} = \frac{E[\|\boldsymbol{\Phi s}\|_2^2]}{M\sigma^2} \tag{21}$$

and the normalized reconstruction error, which is a metric to evaluate the reconstruction quality is defined as follows:

$$\mathcal{E}(\mathcal{D}_s) = \frac{E[\|\boldsymbol{s} - \hat{\boldsymbol{s}}\|_2^2]}{E[\|\boldsymbol{s}\|_2^2]} \tag{22}$$

where $\hat{\boldsymbol{s}}$ denotes the estimation of the primal signal $\boldsymbol{s}$ at the receiver. We should notice that the lower bound (20) attained with the assumption of knowing $\boldsymbol{\Phi}$ at the receiver and is valid when $N \to \infty$. The following theorem devices the secrecy rate region of the measurement rate where we assume one intended receiver and a wiretapper, which knows the measurement matrix $\boldsymbol{\Phi}$. Furthermore, we assume that SNR_1 and SNR_2 are the SNRs of the main and the wiretap channels, respectively (both channels are shown in Fig. 1).

Theorem 1: For the wiretap channel shown in Fig. 1 with a signal source with a rate-distortion function $R(.)$ and measurement matrix $\boldsymbol{\Phi}$, the utter bound of the CS measurement rate required to prevent the wiretapper to obtain a normalized reconstruction error $\mathcal{E}(Dx)$ is given by

$$\delta \leq \frac{2R\big(\mathcal{E}(\mathcal{D}_s)\big)}{log(1+\mathrm{SNR}_2)} \tag{23}$$

Proof: Follows the proof of Theorem 1 in [19].

Herein, we assumed that the SNR of the main channel is more than the one in the wiretap channel. So, the received signal in the wiretapper is a degraded version of the one received in the intended receiver. This utter bound satisfies that the sent message is not decoded in the wiretapper despite of knowing the measurement matrix. Thus, we have the following limitations on the measurement rate:

$$\frac{2R\big(\mathcal{E}(\mathcal{D}_s)\big)}{log(1+\mathrm{SNR}_1)} \leq \delta \leq \frac{2R\big(\mathcal{E}(\mathcal{D}_s)\big)}{log(1+\mathrm{SNR}_2)} \tag{24}$$

In Fig. 2, we simulate these bounds for $SNR_1 = 5$ and $SNR_2 = 1$. Therefore, the transmitter preserves the primal signal by choosing the measurement rate in the secure bound, which is also limited by the condition of $M/N \leq 1$, coming from the nature of the compressive sensing measurement matrix dimensions. So, the primal signal could be decoded by the intended receiver in a way that the unintended receiver cannot eavesdrop it. This

ability is based on the high SNR in the main channel and lower SNR in the wiretap channel.

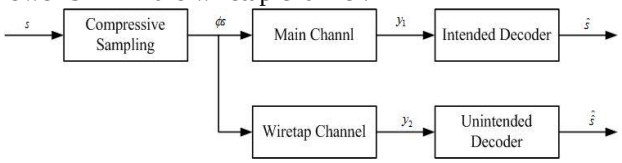

Fig. 1. The block diagram of the wiretap channel with compressive sampling as an encryption in its input.

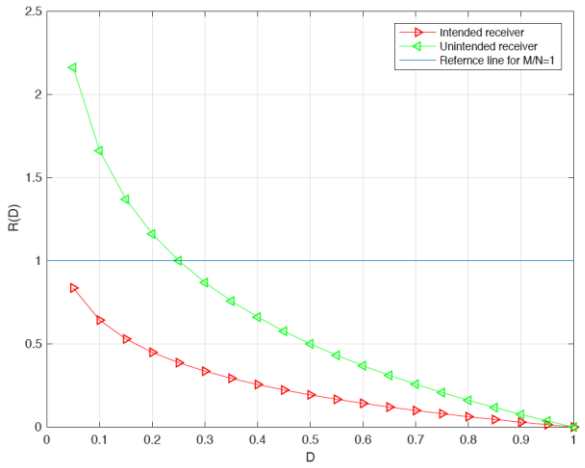

Fig. 2. The utter and lower bounds of δ when $SNR_1 = 5$ and $SNR_2 = 1$. The signal $\boldsymbol{s}$ has a Gaussian probability with zero mean and unit variance.

VI. Conclusions

In this paper, we applied the unified scheme of sensing, compression, and encryption for signal transmission contaminated with Gaussian noise. We showed that an unintended receiver who does not know the exact elements of the measurement matrix, experiences less detection probability than that of intended receiver, even if we assume that he has a priori information in regard the measurement matrix dimensions. Also, we analyzed this scenario from an information theoretic perspective. From this point of view, since the main and the wiretap channels have different SNRs, we can choose a specific measurement matrix for the encryption of the transmitted signal. This measurement scheme causes that the received signal at the intended receiver to be recoverable but not at the unintended one. Moreover, has been shown that when eavesdropper's signal space is orthogonal to the intended user's signal space, the detection probability and false alarm probability for the eavesdropper will be equal and ideal secret communication is achieved based on Shannon's definition of perfect secrecy.

References

[1] E. J. Cand`es, 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, 2006.

[2] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[3] J. Romberg, "Imaging via compressive sampling [introduction to compressive sampling and recovery via convex programming]," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 14–20, 2008.

[4] J. L. Paredes, G. R. Arce, and Z. Wang, "Ultra-wideband compressed sensing: channel estimation," *IEEE Journal of Selected Topics in Signal Processing*, , vol. 1, no. 3, pp. 383–395, 2007.

[5] M. F. Duarte, M. A. Davenport, M. B. Wakin, and R. G. Baraniuk, "Sparse signal detection from incoherent projections," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 3. IEEE, 2006, pp. III–305–III–308.

[6] M. A. Davenport, M. B. Wakin, and R. G. Baraniuk, "Detection and estimation with compressive measurements," Dept. of ECE, Rice University, *Tech. Rep*, 2006.

[7] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *Proc. Military Communications Conference*, 2008, pp. 1–7.

[8] Y. Rachlin and D. Baron, "The Secrecy of Compressed Sensing Measurements," in *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, 2008, pp. 813–817.

[9] M. R. Mayiami, B. Seyfe, and H. G. Bafghi, "Perfect Secrecy via Compressed Sensing," in *Proc. Iran Workshop on Communication and Information Theory*, 2013, pp. 1–5.

[10] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, Prentice-Hall, 1998.

[11] E. J. Candes and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Transactions on Information Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.

[12] A. M. Bruckstein, D. L. Donoho, and M. Elad, "From sparse solutions of systems of equations to sparse modeling of signals and images," *SIAM Review*, vol. 51, no. 1, pp. 34–81, 2009.

[13] Y. C. Pati, R. Rezaiifar, and P. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition," in *Proc. Conference Record of The Twenty-Seventh Asilomar Conference on Signals, Systems and Computers*, 1993, pp. 40–44.

[14] S. Chen, S. A. Billings, and W. Luo, "Orthogonal least squares methods and their application to non-linear system identification," *International Journal of Control*, vol. 50, no. 5, pp. 1873–1896, 1989.

[15] D. L. Donoho, Y. Tsaig, I. Drori, and J. L. Starck, "Sparse solution of underdetermined systems of linear equations by stagewise orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1094–1121, 2012.

[16] R. Gribonval and S. Lesage, "A survey of sparse component analysis for blind source separation: Principles, perspectives, and new challenges," in *Proc. 14th European Symposium on Artificial Neural Networks*, 2006, pp. 323–330.
[17] A. Gilbert and P. Indyk, "Sparse recovery using sparse matrices," *Proceedings of the IEEE*, vol. 98, no. 6, pp. 937–947, 2010.
[18] P. Tune, S. R. Bhaskaran, and S. Hanly, "Number of measurements in sparse signal recovery," in *Proc. IEEE International Symposium on Information Theory*, 2009, pp. 16–20.
[19] S. Sarvotham, D. Baron, and R. G. Baraniuk, "Measurements vs. bits: Compurssed sensing meets information theory" in *Proc. Allerton Conference on Communication, Control and Computing*, 2006.
[20] D. Baron, M. B. Wakin, M. F. Duarte, S. Sarvotham, and R. G. Baraniuk, "Distributed compressed sensing," 2005.
[21] E. Candes, M. Rudelson, T. Tao, and R. Vershynin, "Error correction via linear programming," in *Proc. 46th Annual IEEE Symposium on Foundations of Computer Science*, 2005, pp. 668–681.

Mahmoud Ramezani-Mayiami received his B.Sc. and M.Sc. degrees in 2008 and 2011, respectively from Shahed University, Tehran, Iran. From 2016, he has been a Ph.D. student in the Department of Information and Communication Technology, University of Agder, Grimstad, Norway. His research interests include statistical signal processing, machine learning sparse representation, signal detection and estimation, graph signal processing, and wireless sensor networks.

Hamid G. Bafghi received his B.Sc. degree from Shahid Beheshti University, Tehran, Iran, and M.Sc. and PhD degrees in 2010 and 2016, respectively from Shahed University, Tehran, Iran. Moreover, he was a Research Fellow at Sharif University of Technology from 2008. Now, he is with the Wireless Research Lab. (WRL) at Sharif University as a postdoctoral research fellow. His research interests include information theory (IT) and its applications in security, privacy, and signal processing, IT learning, sparse signal processing, and molecular communications.

Babak Seyfe received his B.Sc. degree from the University of Tehran, Tehran, Iran, and M.Sc. and Ph.D. degrees from Tarbiat Modares University, Tehran, Iran in electrical and computer engineering in 1991, 1995, and 2004, respectively. He is with the Department of Electrical Engineering, Shahed University, Tehran, Iran. Prior to this, he was with the Centre for Digital Signal Processing Research at King's College, London, UK. He was with the Department of Electrical and Computer Engineering at Tarbiat Modares University from 2004 to 2005 and with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, Canada as a Visiting Researcher in 2002. His research interests are detection and estimation theory, statistical signal processing, communication systems, and non-parametric and robust statistics.