Security Aspects of Compressed Sensing

Tiziano Bianchi and Enrico Magli

Politecnico di Torino, tiziano.bianchi@polito.it

I. Introduction and Problem Statement

Compressed sensing (CS) has recently been proposed as an efficient framework for acquiring sparse signals represented by few nonzero coefficients in a suitable basis [1]. CS relies on the fact that linear measurements of a sparse signal enable signal recovery with high probability when the measurements satisfy certain incoherence properties with respect to the signal basis. Interestingly, measurements acquired using linear projections generated according to a random sensing matrix have such properties [2].

Right from the introduction of CS, researchers have suggested that the randomness in the signal acquisition process may provide some notion of security. In this sense, the security of CS has been analyzed following two main paradigms. A first approach is to argue that CS provides computational secrecy if viewed as a cryptosystem, since looking for the correct sensing matrix over the key space is a computationally intractable problem [3], [4]. However, this approach does not provide any formal security proof regarding CS. The second approach is to consider the security of random linear measurements according to an information theoretic framework [5]. As correctly pointed out in [3], CS does not provide information theoretic secrecy, meaning that the mutual information between the measurements and the sensed signal is always greater than zero. However, it is possible to prove that CS measurements asymptotically reveal only the energy of the signal [6] and that normalizing the measurements can provide a perfectly secure channel in the case of Gaussian sensing matrices [7].

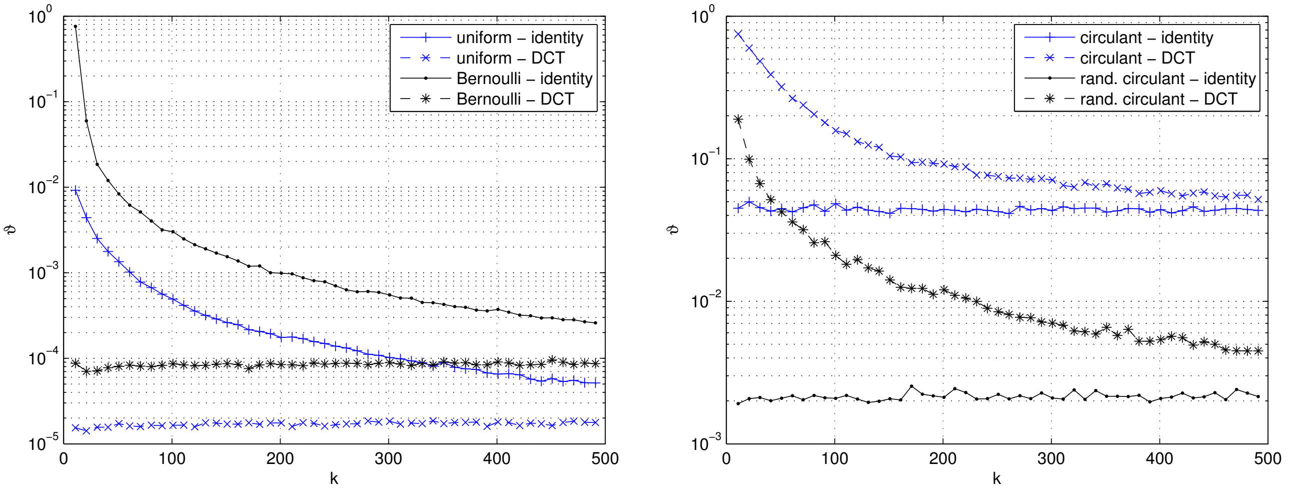
The results in the previous works are based on the central limit theorem and the properties of the Gaussian distribution and are valid when the elements of the sensing matrix are i.i.d. random variables. Moreover, they consider a scenario in which the sensing matrix is continually updated, implementing a sort of one time pad. Such requirements are usually too demanding for practical CS systems. Using fully random matrices requires either storing or generating on the fly a great amount of random values. Moreover, the generation of Gaussian distributed values may be difficult in low complexity systems.

The above problems can be solved in practice by resorting to structured matrices [8], [9] and generating the sensing matrix according to simpler distributions, like the Bernoulli one. However, even if such constructions guarantee similar recovery properties as fully random matrices made of Gaussian i.i.d. values, their security properties are still not fully understood. In this paper, we will analyze the security of such matrices according to an alternative security definition based on the performance of a detector which tries to distinguish different signals from their measurements. We will also provide useful bounds to characterize the security of CS according to this definition and validate such bounds in simple scenarios through simulations.

II. Security Analysis

The proposed security notion is based on the problem of distinguishing whether the measurements y comes from one of two known given signals x_1 and x_2. Let us consider a signal x that belongs to a two-elements set $\{x_1, x_2\}$ and a detector $\mathcal{D}$ that given the measurements y outputs either x_1 or x_2. Given a certain detector, we define the probability of detection as $P_d = \Pr\{\mathcal{D}(y) = x_i | x = x_i\}$ and the probability of false alarm as $P_f = \Pr\{\mathcal{D}(y) = x_i | x \neq x_i\}$. We will say that a CS system is *ϑ-indistinguishable* with respect to two signals x_1 and x_2 if for every possible detector $\mathcal{D}(y)$ we have

$$P_d - P_f \leq \vartheta. \tag{1}$$



(a) (b)

Fig. 1. Distinguishability of k-sparse unit energy signals under different sparsity bases, for $n = 1000$: (a) different distributions of the sensing matrix; (b) different kinds of structured matrices.

Given a particular distribution of the sensing matrix, the ϑ-indistinguishability of the resulting CS system can be directly evaluated by computing the total variation (TV) distance between the probability distributions $\mathbb{P}(y|x_1)$ and $\mathbb{P}(y|x_2)$ [10] or upper bounded by computing the Kullback-Leibler (KL) divergence between the same distributions and applying Pinsker's inequality [11]. In the paper, we will provide expressions for the value of ϑ in a number of different cases, including non-Gaussian matrices and partially circulant matrices [8]. Moreover, the theoretical ϑ will be compared to the performance of both practical detectors and optimal detectors defined according to the Neyman-Pearson (NP) lemma.

In Fig. 1, we show some preliminary results regarding the ϑ-indistinguishability of practical CS sensing matrices based on different distributions (uniform and Bernoulli) and different structures (partially circulant and circulant with randomly chosen rows). The results give interesting insights regarding the security of CS measurements, indicating that the level of confidentiality depends on the sparsity of the signal and on the sparsity basis. Moreover, even if different distributions/constructions provide different security levels, the asymptotic behavior of ϑ appears to be the same. Finally, the results suggest that CS based on practical sensing matrices, even though it does not provide strong secrecy, can still be used to provide some form of data confidentiality similar to perceptual encryption.

References

[1] D. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

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

[3] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *2008 46th Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 2008, pp. 813–817.

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

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell. Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[6] V. Cambareri, J. Haboba, F. Pareschi, H. Rovatti, G. Setti, and K.-W. Wong, "A two-class information concealing system based on compressed sensing," in *ISCAS'13*, 2013, pp. 1356–1359.

[7] T. Bianchi, V. Bioglio, and E. Magli, "On the security of random linear measurements," in *ICASSP'14*, 2014, pp. 4020–4024.

[8] J. Haupt, W. Bajwa, G. Raz, and R. Nowak, "Toeplitz compressed sensing matrices with applications to sparse channel estimation," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5862–5875, 2010.

[9] T. Do, L. Gan, N. Nguyen, and T. Tran, "Fast and efficient compressive sensing using structurally random matrices," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 139–154, Jan 2012.

[10] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses*, 3rd ed. New York: Springer, 2005.

[11] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.