ON THE SECURITY OF RANDOM LINEAR MEASUREMENTS

Tiziano Bianchi, Valerio Bioglio, Enrico Magli

Dept. of Electronics and Telecommunications, Politecnico di Torino, Italy

ABSTRACT

In this paper, we analyze the security of compressed sensing (CS) as a cryptosystem. We demonstrate that random linear measurements acquired using a Gaussian i.i.d. matrix reveal only the energy of the sensed signal, and that only the energy of the measurements leaks information about the signal. We provide useful bounds for assessing the information leakage about the energy, linking those bounds to the minimum mean square error achievable by practical estimators. Moreover, we propose a simple strategy based on the normalization of the measurements which achieves, at least in theory, perfect secrecy, enabling the use of CS-based encryption in practical cryptosystems.

Index Terms— Compressed sensing, encryption, random matrices, security.

1. INTRODUCTION

Compressed sensing (CS) has recently emerged as an efficient framework for acquiring signals at a rate well below that predicted by the classical Shannon-Nyquist theory [1, 2, 3]. The key intuition behind CS is that linear measurements of a sparse or compressible signal enable signal recovery with high probability, provided that the measurements satisfy certain incoherence properties. Interestingly, several results confirm that linear measurements acquired using random matrices have indeed such properties [4, 5].

Right from the introduction of the CS paradigm, researcher have hinted the possibility that acquiring signals via random linear projection may provide some notion of security. In [6], the authors argue that CS does not provide information theoretic secrecy [7], while it can be viewed as a cryptosystem offering computational secrecy. The security of CS is also investigated in [8], where the authors conclude that CS is computationally secure against a systematic search of the sensing matrix, even if the degree of sparsity is known. Other authors have found that CS can be employed to achieve security in the wiretap channel model, i.e., if an eavesdropper has access to a secret communication through a different channel with respect to the intended receiver [9, 10].

This work is supported by the European Research Council under the European Community's Seventh Framework Programme (FP7/2007-2013) / ERC Grant agreement n. 279848.

In this paper, following the approach of [6], we analyze the security of CS as a cryptosystem. Differently from [6], we demonstrate that random linear measurements acquired using a Gaussian i.i.d. matrix can achieve secrecy in an information theoretic sense under specific distributions of the sensed signal. Namely, we prove that a Gaussian sensing matrix reveals only the energy of the sensed signal, and that only the energy of the measurements leaks information about the signal. The result is that CS using Gaussian random matrices is, at least in theory, perfectly secure when sensing constant energy signals. Moreover, we propose a simple strategy based on the normalization of the measurements which achieves, at least in theory, perfect secrecy irrespective of the distribution of the sensed signal. In the case of generic signals, we also provide useful bounds for assessing the information leakage regarding the energy of the sensed signals and we link such bounds to the minimum mean square error achievable by practical estimators. Simulation results are also included to validate such bounds in a simple scenario.

2. BACKGROUND

2.1. Compressed Sensing

A signal $x \in \mathbb{R}^n$ is called k-sparse if there exists a basis Φ such that $x = \Phi\theta$ and θ has at most k nonzero entries, i.e., $||\theta||_0 \leq k$. According to the compressed sensing framework, a k-sparse signal can be exactly recovered from $m < n$ linear measurements

$$y = Ax \tag{1}$$

by solving the minimization problem

$$\hat{\theta} = \arg\min_{\theta} ||\theta||_0, \text{ subject to } A\Phi\theta = y \tag{2}$$

as long as $m \geq 2k$ and the $m \times n$ sensing matrix A satisfies certain properties [1, 2].

Recovering x from only $m = 2k$ measurements is in general a combinatorial problem. In practice, if the entries of A are i.i.d. variables from a sub-Gaussian distribution, then exact recovery of k-sparse signals can be achieved with very high probability by solving the convex minimization problem

$$\hat{\theta} = \arg\min_{\theta} ||\theta||_1, \text{ subject to } A\Phi\theta = y \tag{3}$$

as long as $m = O(k \log(n/k))$ [4]. In the following, we will focus on random sensing matrices A with i.i.d. entries.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

2.2. Security definitions

Let us call the set of possible plain texts $\mathcal{P}$, the set of cipher texts $\mathcal{C}$ and a key K. A private key cryptosystem is a pair of functions $e_K : \mathcal{P} \to \mathcal{C}, d_K : \mathcal{C} \to \mathcal{P}$ such that, given a plain text $p \in \mathcal{P}$, $d_K(e_K(p)) = p$ and such that, given a cipher text $c \in \mathcal{C}$, it is unfeasible to determine p such that $e_K(p) = c$, without knowing the key K.

A cryptosystem is perfectly secure [7] if the posterior probability of the cipher text given the plain text p is independent of p, i.e.,

$$\mathbb{P}(c|p) = \mathbb{P}(c). \tag{4}$$

For a perfectly secure cryptosystem, any attack can not be more successful than guessing the plain text at random.

Practical cryptosystems are usually computationally secure, meaning that breaking the cryptosystem is equivalent to solve a computationally hard problem, that is, a problem whose solution can not be computed in polynomial time with respect to the size of the key.

Given the CS model $y = Ax$, we can define the following equivalences between CS and a private key cryptosystem: the signal x is the plain text, the sensing matrix A is the secret key and the measurement vector y is the cipher text. The encryption function is matrix multiplication, whereas decryption is achieved by solving the problem in (3). The notions of perfect security and computational security can be extended also to the cryptosystem defined by the CS framework.

2.3. Security Scenarios and Attack Models

The security of the CS-based cryptosystem will be affected by the policies regarding the generation of the sensing matrix in the case of multiple measurements. On the one hand, using the same sensing matrix for multiple signals limits the overhead due to the transmission of the sensing matrix. On the other hand, generating a different and independent sensing matrix for each measurement is somewhat analogous to a one-time pad cryptosystem and may offer greater security.

In this paper, we will focus on the one-time sensing matrix (OTS) scenario. We will assume that each sensing matrix is used only once, and that different sensing matrices are statistically independent. Under this scenario, it is sufficient to consider the security of $y = Ax$, since measurements of multiple signals will be statistically independent.

The security of a cryptosystem depends also on the resources of the adversary. In this paper, we will focus on a ciphertext-only attack (COA) scenario where the adversary has only knowledge of the measurements y.

3. SECURITY OF THE MEASUREMENTS

In this section, we summarize the main results of the paper. Proofs are omitted due to space limitations. Let us consider the OTS cryptosystem defined by $y = Ax$. Let us denote with $I(x, y)$ the mutual information between x and y [11], with $[A]_{i,j}$ the (i, j) element of matrix A, and define $\mathcal{E}_x = ||x||_2^2$. We have the following important result:

Proposition 1. If $[A]_{i,j}$ are i.i.d. zero-mean Gaussian variables, then the OTS cryptosystem satisfies $I(x; y) = I(\mathcal{E}_x; y)$.

As a proof sketch, we note that for a given x, y has a multivariate Gaussian distribution whose covariance matrix depends only on $\mathcal{E}_x$, hence $\mathbb{P}(y|x) = \mathbb{P}(y|\mathcal{E}_x)$. The above result says that an OTS cryptosystem using an i.i.d. Gaussian sensing matrix does not reveal anything more about x than what can be inferred by the knowledge of its energy. It is worth noting that this is true irrespective of the sparsity degree of x, that is, x does not have to be necessarily sparse. In the following, we will denote such a cryptosystem as Gaussian-OTS (G-OTS) cryptosystem. An immediate consequence of the above proposition is that the G-OTS cryptosystem does not reveal anything about a family of signals with a constant energy.

Corollary 1. If $\forall x$, $\mathcal{E}_x = \beta > 0$, then the G-OTS cryptosystem is perfectly secure.

Moreover, let $U_x = x/\sqrt{\mathcal{E}_x}$. Then we have that under some conditions U_x is perfectly hidden.

Corollary 2. If U_x and $\mathcal{E}_x$ are statistically independent, then the G-OTS cryptosystem satisfies $I(U_x; y) = 0$.

Since for most signals of interest the constant energy requirement is usually not verified, it is interesting to evaluate the information leakage due to the observation of y. For the case of i.i.d. Gaussian sensing matrices, we have the following two results:

Proposition 2. Let $\mathcal{E}_y = ||y||_2^2$. If $[A]_{i,j}$ are i.i.d. zero-mean Gaussian variables, then we have $I(x; y) = I(\mathcal{E}_x; \mathcal{E}_y)$. Moreover, $I(x; y)$ can be upper bounded as

$$I(x; y) \leq \xi(\kappa^*) - \xi\left(\frac{m}{2}\right) - \psi(\kappa^*) + \psi\left(\frac{m}{2}\right) \tag{5}$$

where $\xi(\kappa) \triangleq \kappa + \log(\Gamma(\kappa)) + (1 - \kappa)\psi(\kappa)$, $\Gamma(\kappa) = \int_0^\infty t^{\kappa-1}e^{-t}dt$ is the Gamma function, $\psi(\kappa) = \frac{d\log(\Gamma(\kappa))}{d\kappa}$ is the digamma function, and κ^* is the solution to the non-linear equation $\log(\kappa^*) - \psi(\kappa^*) = \log(m/2) - \psi(m/2) + \log(E[\mathcal{E}_x]) - E[\log(\mathcal{E}_x)]$.

As a proof sketch for the first part, we note that y follows a spherically symmetric distribution around $y = 0$, hence $\mathcal{E}_y$ is independent of $y/\mathcal{E}_y$. The first result says that $\mathcal{E}_y$ is a sufficient statistic for estimating x, irrespective of the distribution of x. The second part gives an upper bound on the amount of information that y leaks about x. It is worth noting that the upper bound in (5) does not depend on the variance of $[A]_{i,j}$.

An interesting consequence of the above result is that it can be exploited to obtain a perfectly "securized" version of

the G-OTS cryptosystem. Let us modify the G-OTS cryptosystem so that only normalized measurements are transmitted, i.e, the ciphertext is given by $U_y = y/\sqrt{\mathcal{E}_y}$, and denote it as SG-OTS.

Lemma 1. The SG-OTS cryptosystem is perfectly secure, i.e., $\mathbb{P}(U_y|x) = \mathbb{P}(U_y)$.

4. SECURITY BOUNDS

The standard cryptographic definition of security fails to capture the fact that an attacker may try to estimate x up to a certain precision instead of recovering its exact value. Hence, it may have sense to introduce an alternative notion of security linked to the mean squared error (MSE) between x and an estimate $\hat{x}$ obtained by observing only the measurements y. In the following, we will say that a cryptosystem is η-MSE secure with respect to x, if, for every possible estimator $\hat{x}(y)$ of x, we have

$$\frac{E[||x - \hat{x}(y)||_2^2]}{\text{tr}(C_x)} \triangleq \eta_{\hat{x}} \geq \eta \tag{6}$$

where C_x is the covariance matrix of x and tr() denotes the trace operator. Note that a Bayesian estimator is always at least 1-MSE secure, since in the absence of any a posteriori information the minimum MSE (MMSE) estimator of x is $\hat{x}(y) = E[x]$, yielding $E[||x - \hat{x}(y)||_2] = \text{tr}(C_x)$.

Let us consider an estimator $\hat{x}(y)$ of x which relies on the measurement y. By using rate-distortion theory [11], we can link the mutual information between y and x to the MSE of the estimator through the following lower bound

$$\frac{E[||x - \hat{x}(y)||_2^2}{n} \geq \frac{1}{2\pi} e^{\frac{2h(x|y)}{n} - 1} = \frac{1}{2\pi} e^{\frac{2h(x)}{n} - \frac{2I(x;y)}{n} - 1}. \tag{7}$$

Since we know that a G-OTS cryptosystem reveals only $\mathcal{E}_x$, we can apply the definition of η-MSE security to the estimation of $\mathcal{E}_x$. Let us assume that x can be modeled as an exactly k-sparse signal, whose nonzero entries are i.i.d. Gaussian variables with zero mean and variance σ_x^2. In this case, $\mathcal{E}_x$ is distributed as a chi-square variable with k degrees of freedom scaled by σ_x^2. The above fact, together with (7), leads immediately to the following

Lemma 2. If x is an exactly k-sparse signal with i.i.d. Gaussian nonzero entries, a G-OTS cryptosystem is at least η-MSE secure with respect to $\mathcal{E}_x$, where

$$\eta = \frac{e^{2\xi\left(\frac{k}{2}\right) + 2\xi'\left(\frac{m}{2}\right) - 2\xi'(\kappa^*) - 1}}{k\pi} \tag{8}$$

where $\xi'(\kappa) = \xi(\kappa) - \psi(\kappa)$ and κ^* satisfies $\log(\kappa^*) - \psi(\kappa^*) = \log(m/2) - \psi(m/2) + \log(k/2) - \psi(k/2)$.

4.1. Estimation Attacks

Lemma 2 gives a lower bound for the MSE of any possible estimator of $\mathcal{E}_x$ in the case of i.i.d. Gaussian sparse signals. Such a bound can be compared with the performance of practical estimators.

The maximum likelihood (ML) estimator of $\mathcal{E}_x$ in the case of a Gaussian sensing matrix is given by

$$\hat{\mathcal{E}}_{x,ML} = \max_{\mathcal{E}_x} \log(\mathbb{P}(y|\mathcal{E}_x)) = \frac{\mathcal{E}_y}{m\sigma_A^2}. \tag{9}$$

The performance of the ML estimator can be derived as $\sigma^2_{\hat{\mathcal{E}}_{x,ML}} = \frac{2\mathcal{E}_x^2}{m}$. By taking the expectation over $\mathcal{E}_x$, we readily obtain $E[(\mathcal{E}_x - \hat{\mathcal{E}}_{x,ML})^2] = \frac{2k(k+2)\sigma_x^4}{m}$ from which

$$\eta_{\hat{\mathcal{E}}_x,ML} = \frac{k+2}{m}. \tag{10}$$

For a Gaussian k-sparse signal, a closed form of the MMSE estimator can be derived as

$$\hat{\mathcal{E}}_{x,ML} = \frac{\sigma_x\sqrt{\mathcal{E}_y}}{\sigma_A} \frac{K_{\frac{k}{2}-\frac{m}{2}+1}\left(2\sqrt{\frac{\mathcal{E}_y}{4\sigma_A^2\sigma_x^2}}\right)}{K_{\frac{k}{2}-\frac{m}{2}}\left(2\sqrt{\frac{\mathcal{E}_y}{4\sigma_A^2\sigma_x^2}}\right)} \tag{11}$$

where $K_\nu(x)$ denotes the modified Bessel function of the second kind of order ν. Unfortunately, there is no closed form for the MSE of the above estimator. A simpler estimator can be obtained by searching for the estimator minimizing the MSE among all estimators which can be expressed as a linear function of $\mathcal{E}_y$. For a Gaussian k-sparse signal, this linear MMSE (LMMSE) estimator is

$$\hat{\mathcal{E}}_{x,LMMSE} = \frac{\mathcal{E}_y}{\sigma_A^2(m+k+2)} + \frac{k(k+2)\sigma_x^2}{m+k+2}. \tag{12}$$

The MSE can be evaluated as $E[(\mathcal{E}_x - \hat{\mathcal{E}}_{x,LMMSE})^2] = \frac{2k(k+2)\sigma_x^4}{m+k+2}$ from which we obtain

$$\eta_{\hat{\mathcal{E}}_x,LMMSE} = \frac{k+2}{m+k+2}. \tag{13}$$

The performance of the above estimators will be compared to the theoretical bound in Section 6.

5. PRACTICAL IMPLEMENTATION

The implementation of either the G-OTS or the SG-OTS cryptosystem will require to transmit a sequence of i.i.d. Gaussian sensing matrices. A solution is to use a secure random number generator (SRNG) [12] and assume that sender and receiver synchronize their generators by sharing a secret seed. The resulting cryptosystem is not perfectly secure, since a brute force search of the key space will surely break the cryptosystem [6]. Moreover, the attacker may exploit some weaknesses

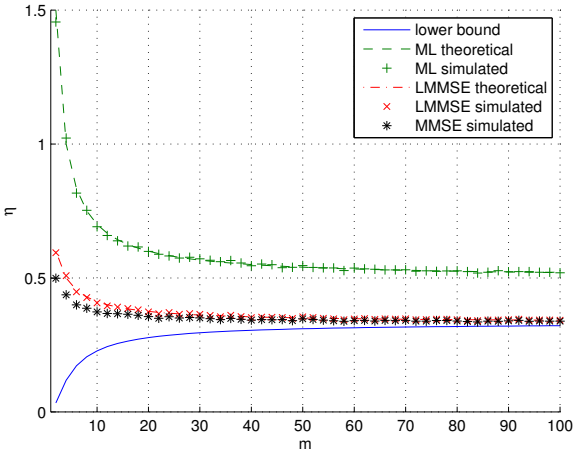

Fig. 1. MSE security of the G-OTS cryptosystem for different number of measurements at $\rho = k/m = 0.5$.

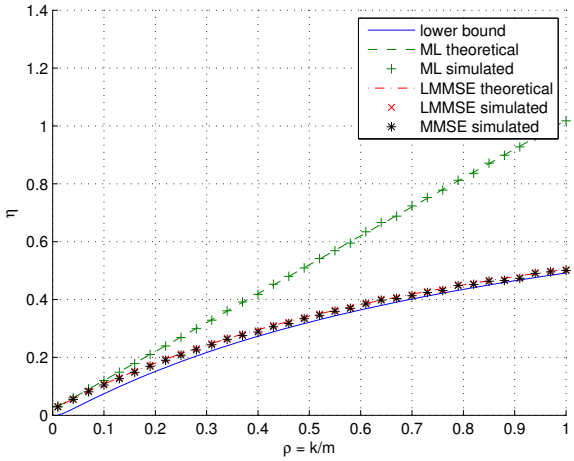

Fig. 2. MSE security of the G-OTS cryptosystem for different overmeasuring rates: $m = 100$, k ranges form 1 to m.

of the SNRG in order to try to estimate the key, or the distribution of the SRNG may slightly deviate from i.i.d. Gaussian.

As to the SG-OTS cryptosystem, an auxiliary secure channel to transmit the value of $\mathcal{E}_y$ is required in order to exactly recover x at the intended receiver. Such a secure channel can be implemented by relying on conventional cryptographic techniques. As a consequence, the combination of SG-OTS cryptosystem and auxiliary channel will not be perfectly secure, since practical cryptosystem, like AES, offer only computational security. Nevertheless, we can conclude that a practical implementation of the SG-OTS cryptosystem is at least as secure as the standard cryptographic tools used to encrypt the auxiliary channel and generate the sensing matrices. This can offer a significant advantage with respect to full encryption of the measurements, since we obtain basically the same security level by performing only one encryption every m measurements.

6. SIMULATION RESULTS

In this section, we evaluate the security of the G-OTS cryptosystem for Gaussian k-sparse signals. For each experiment, empirical MSE values for the ML, LMMSE, and MMSE estimators are obtained by averaging over 10^5 independent realizations of the measurements for each choice of k and m.

In a first experiment, we consider a fixed overmeasuring rate $\rho = k/m = 0.5$ and we vary k in the interval $[1, 100]$. The obtained empirical η values versus the number of measurements m are shown in Fig. 1, together with the theoretical performance of the ML and LMMSE estimator given in (10) and (13), respectively, and the theoretical lower bound given in (8). For a fixed ρ, the G-OTS cryptosystem tends to have a constant MSE security as m grows, with the η value that does not decrease significantly for $m > 50$. It is also worth noting that the theoretical lower bound is quite loose for $m < 50$, but becomes relatively tight when m increases.

In a second experiment, we consider a fixed number of measurements $m = 100$ and we vary k in the interval $[1, 100]$, obtaining different overmeasuring rates ρ in the interval $[0, 1]$. The obtained empirical η versus ρ are shown in Fig. 2, together with the theoretical performance of the estimators and the theoretical lower bound. It is evident that the security of the G-OTS cryptosystem decreases with ρ. It is also evident that for values of ρ that are relevant to practical CS systems all the estimators can estimate the energy of x with an MSE lower than $\sigma^2_{\mathcal{E}_x}/10$, which means that the measurements permit to obtain a reasonable guess of $\mathcal{E}_x$ even if the sensing matrix is unknown.

7. CONCLUSIONS

The results obtained in this paper give interesting insights regarding the security of CS measurements. The first important result is that a sensing matrix with zero mean i.i.d. Gaussian entries reveals only the energy of the sensed signal. As a consequence, the spherical angle of the signal is perfectly hidden by the measurements if the energy and the angle are statistically independent. Moreover, it is possible to upper bound the information leakage about the energy and predict the precision with which the energy can be estimated.

The second important result in the paper is that for a sensing matrix with zero mean i.i.d. Gaussian entries the information leakage is confined to the energy of the measurements. Based on the above property, a simple normalization of the measurements yields a perfectly secure cryptosystem, that can be used as a building block of a practical CS-based cryptosystem offering the same security of standard cryptographic tools at a reduced complexity.

8. REFERENCES

[1] E.J. 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, 2006.

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

[3] E.J. Candes and M.B. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 21–30, 2008.

[4] 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.

[5] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constructive Approximation*, vol. 28, no. 3, pp. 253–263, 2008.

[6] 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.

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

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

[9] S. Agrawal and S. Vishwanath, "Secrecy using compressive sensing," in *2011 IEEE Information Theory Workshop (ITW)*, 2011, pp. 563–567.

[10] G. Reeves, N. Goela, N. Milosavljevic, and M. Gastpar, "A compressed sensing wire-tap channel," in *2011 IEEE Information Theory Workshop (ITW)*, 2011, pp. 548–552.

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

[12] P. C. van Oorschot A. J. Menezes and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.