Analysis of the Security of Compressed Sensing with Circulant Matrices

Analysis of the Security of Compressed Sensing with Circulant Matrices

T. Bianchi, E. Magli
Dept. of Electronics and Telecommunications, Politecnico di Torino, Italy

***Abstract*—Recent results have shown that the compressed sensing (CS) framework can provide a form of data confidentiality when the signals are sensed by a fully random matrix. In this paper, we extend those results by considering the security achievable by partially circulant sensing matrices generated from a vector of random variables. Circulant matrices, having similar CS recovery performance as fully random matrices and admitting a fast implementation by means of a fast Fourier transform, are more suitable for practical CS systems. Compared to fully random Gaussian matrices, which leak only the energy of the sensed signal, we show that circulant matrices leak also some information on the autocorrelation of the sensed signal. In order to characterize the above information leakage, we propose an operational definition of security linked to the difficulty of distinguishing equal energy signals and we propose practical attacks to test this definition. The results provide interesting insights on the security of such matrices, showing that a properly randomized partially circulant matrix can provide a weak encryption layer if the signal is sparse in the sensing domain.**

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

I. Introduction

Compressed sensing (CS) has recently been proposed as an efficient framework for acquiring sparse signals, i.e., signal that can be represented by few nonzero coefficients in a suitable basis [1], [2]. CS relies on the fact that linear measurements of a sparse signal enable signal recovery with high probability, provided that the measurements satisfy certain incoherence properties with respect to the signal basis. An interesting result is that linear measurements acquired using random matrices have indeed such properties [3].

The randomness in the signal acquisition process suggests that CS may provide some notion of security. In [4] the authors conclude that CS does not provide information theoretic secrecy [5], while it offers computational secrecy if viewed as a cryptosystem. In [6] the authors show that CS is computationally secure against a systematic search of the sensing matrix. Recently, the security of a practical CS system based on Bernoulli sensing matrices has been considered in [7], showing that CS measurements asymptotically reveal only the energy of the signal. More formal results in this sense were proved in [8], where it was also shown that normalizing the measurements can provide a perfectly secure channel in the case of Gaussian sensing matrices.

The results in the previous works are valid when the elements of the sensing matrix can be considered as i.i.d. random variables, i.e, for fully random sensing matrices. Despite their inherent security, using fully random matrices is difficult in practice, since it requires either storing or generating on the fly a great amount of random values. Also, the matrix product involving a fully random matrix is usually expensive. In order to solve the above problems, some researchers have proposed the use of partially circulant sensing matrices based on a random vector that is circularly shifted to generate every row [9], [10]. As to recovery properties, such matrices usually prove to be almost as good as fully random matrices [11]. Moreover, they only require managing a single row of random values and matrix product can be efficiently implemented by relying on a fast Fourier transform (FFT). Circulant sensing matrices can also allow to perform linear filtering directly on the measurements, which enables direct processing in the measurement domain without costly recovery procedures [12].

In this paper, we analyze the security properties of random circulant matrices generated from a row of i.i.d. Gaussian variables. Unlike the case of fully random Gaussian matrices [8], we demonstrate that, due to their additional structure, random circulant matrices do not leak only the energy of the sensed signal, but also some partial information on the signal autocorrelation. This information can be partly obfuscated by randomly selecting the rows of the partially circulant sensing matrix [10], however the above dependence can not be eliminated. In order to characterize the additional security leakage of circulant matrices, we propose an operational definition of security linked to the performance of a detector trying to distinguish equal-energy signals with different autocorrelation structures and we provide useful bounds to evaluate the security of CS according to the above definition. Finally, we present simulation results to validate such bounds in simple scenarios and we provide some empirical relationships between the security of the system, the signal length, the signal sparsity, and the number of measurements.

II. Background

A. Compressed Sensing with Circulant Matrices

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 CS framework, a k-sparse signal can be exactly recovered from $m < n$ linear measurements

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

by solving a minimization problem [1], [2]. In practice, if the entries of A are i.i.d. variables drawn 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

$$\hat{\theta} = \arg\min_{\theta} ||\theta||_1, \quad \text{subject to } A\Phi\theta = y \tag{2}$$

as long as $m = O(k \log(n/k))$ [3].

Due to the complexity of performing the product Ax when A is a fully random matrix, some authors have suggested to use partially circulant matrices generated from a row of i.i.d. variables [9]–[11]. Such matrices have the following form

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ \vdots & & & & \vdots \\ a_{n-m+2} & a_{n-m+3} & a_{n-m+4} & \dots & a_{n-m+1} \end{bmatrix} \tag{3}$$

where the first row $a^T = [a_1, a_2, \dots, a_n]$ is a vector of i.i.d. variables from a Gaussian or sub-Gaussian (e.g., Bernoulli) distribution. Partially circulant matrices have similar recovery performance as fully random matrices [10]. Moreover, they can be diagonalized using a discrete Fourier transform (DFT) as

$$A = PW^H \Lambda W \tag{4}$$

where W is the unitary DFT matrix, Λ is a diagonal matrix whose nonzero elements are the DFT of the sequence $[a_1, a_n, a_{n-1}, \dots, a_2]$, i.e., the first column of the $n \times n$ fully circulant matrix generated from a^T, and P is a $m \times n$ matrix that selects the first m entries of a vector of n elements. Thanks to the above decomposition, the product Ax can be efficiently implemented using a fast Fourier transform (FFT). Moreover, the cost of transmitting or generating the sensing matrix is also sensibly reduced, since only n random values are required. The randomness of partially circulant matrices can be improved by letting P choose a random subset of m indexes instead of the first m entries [10].

B. Security definitions

Let us call the set of possible plaintexts $\mathcal{P}$, 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 $p \in \mathcal{P}$, and a ciphertext $c \in \mathcal{C}$, we have that $d_K(e_K(p)) = p$ and that it is unfeasible, without knowing the key K, to determine p such that $e_K(p) = c$.

A cryptosystem is said to be perfectly secure [5] if the posterior probability of the ciphertext given the plaintext p is independent of p, i.e., if

$$\mathbb{P}(c|p) = \mathbb{P}(c). \tag{5}$$

Given a perfectly secure cryptosystem, an attack can not be more successful than guessing the plaintext at random.

Following the approach in [8], we define a CS-based cryptosystem where the signal x is the plain text p, the sensing matrix A is the secret key K and the measurement vector y is the cipher text c. The encryption function e_A is the matrix multiplication between the sensing matrix A and the signal x; the decryption is achieved by solving the problem in (2). We assume that each sensing matrix is used only once (one-time sensing matrix (OTS) scenario), and that different sensing matrices are statistically independent. Under this scenario, we can assume that the adversary has only knowledge of the measurements y (ciphertext-only attack (COA) scenario), since the knowledge of plaintext/ciphertext pairs (x, y) does not reveal anything about the unknown plaintexts.

CS-based cryptosystems can not achieve in general perfect secrecy [4], [8]. However, some application scenarios may be interested in a weaker security notion with respect to standard cryptographic definitions. For example, in multimedia encryption it is sometimes required that an attacker is not able to recover a copy of the plaintext with a sufficiently high quality, which is referred to as perceptual/transparent encryption [13]. Since this is usually an application-dependent notion, in this case there are no formal and universally agreed security definitions. In the next sections, we will define an ad-hoc security measure in order to characterize the security of CS as a weak encryption layer.

III. Security of Circulant Matrices

Let us consider the OTS cryptosystem defined by $y = Ax$, where A can be expressed as in (4) and the matrix P is public. We will denote such a cryptosystem as OTS-circulant (OTS-C). Let us define C_x as the circular autocorrelation matrix of x, that is, $[C_x]_{ij} = \sum_{r=1}^{n} x_r x_{r+i-j \mod n}$, for $i, j = 1, \dots, n$. It is easy to verify that C_x is a Toeplitz matrix and that its diagonal elements are equal to $\mathcal{E}_x = x^T x$. We have the following result:

Proposition 1. If a_i, $i = 1, \dots, n$, are i.i.d. zero-mean Gaussian variables, then the OTS-C cryptosystem satisfies $\mathbb{P}(y|x) = \mathbb{P}(y|PC_xP^T)$.

Proof. Let us consider the probability distribution function $\mathbb{P}(y|x)$ for a given x. Since a_i are Gaussian, we have that $\mathbb{P}(y|x)$ is a multivariate Gaussian distribution with mean $\mu_{y|x}$ and covariance matrix $C_{y|x}$. It is immediate to find $\mu_{y|x} = E[y|x] = E[A]x = 0$, whereas we have

$$\begin{aligned} C_{y|x} =& E[Axx^TA^T] = E[PW^H\Lambda(Wx)(Wx)^H\Lambda^H WP^T] \\ =& nPW^H \mathrm{diag}\{Wx\} E[(W^Ha)(W^Ha)^H] \\ & \times \mathrm{diag}\{Wx\}^H WP^T \\ =& nPW^H \mathrm{diag}\{Wx\} W^H E[aa^T] W \mathrm{diag}\{Wx\}^H WP^T \\ =& n\sigma_A^2 PW^H |\mathrm{diag}\{Wx\}|^2 WP^T = \sigma_A^2 PC_xP^T \end{aligned} \tag{6}$$

where $\mathrm{diag}\{v\}$ denotes a diagonal matrix defined by vector v, we use $\Lambda = \sqrt{n} \cdot \mathrm{diag}\{W^Ha\}$ and the fact that $\mathrm{diag}\{u\}v = \mathrm{diag}\{v\}u$, and we assume that a_i have variance σ_A^2. It follows that y depends on x only through the autocorrelation PC_xP^T, i.e. $\mathbb{P}(y|x) = \mathbb{P}(y|PC_xP^T)$. □

The above result says that an OTS-C cryptosystem using i.i.d. Gaussian variables reveals only some elements of the circular autocorrelation matrix of x, according to the particular

selection matrix P. It is worth noting that this is true irrespective of the sparsity degree of x, that is, x does not necessarily have to be sparse. In the following, we will denote such a cryptosystem as Gaussian-OTS-C (G-OTS-C) cryptosystem.

Let us now consider a similar OTS cryptosystem in which the selection matrix P is randomly drawn, with uniform distribution, over all the possible choices of m indexes out of n (we have $N_P = n!/(n-m)!$ possible sequences) and kept secret. We will denote such a cryptosystem as Gaussian-OTS-randomized circulant (G-OTS-R). In this case, it is easy to derive the following result:

Corollary 1. The G-OTS-R cryptosystem satisfies

$$\mathbb{P}(y|x) = \frac{1}{N_P}\sum_{r=1}^{N_P}\mathcal{N}(0, \sigma_A^2 P_r C_x P_r^T)$$

where P_r denotes the rth possible selection matrix and $\mathcal{N}(\mu, C)$ denotes a multivariate Gaussian distribution with mean μ and covariance matrix C.

When the choice of the rows of a Gaussian circulant sensing matrix is randomized, the distribution of the measurements given a particular x follows a mixture of multivariate Gaussian distributions, whose covariance matrix is given by all the possible principle minors of size m of the matrix C_x.

The previous results indicate that the measurements taken with a circulant matrix in general are not distributed according to a spherically symmetric distribution. As a result, circulant sensing matrices provide a weaker security than Gaussian sensing matrices, since their information leakage is not limited to the energy of x [8]. In order to characterize this additional leakage, we introduce a security notion based on the problem of distinguishing whether the measurements y comes from one of two known signals x_1 and x_2. Let us consider a signal x that belongs to a two-element set $\{x_1, x_2\}$; a detector is a function that given the measurements y outputs one of two possible signals x_1, x_2. Formally, this can be defined as $\mathcal{D} : \mathbb{R}^m \to \{x_1, x_2\}$. 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 $P_f = \Pr\{\mathcal{D}(y) = x_i | x \neq x_i\}$. In the following, we will say that a cryptosystem is ϑ-indistinguishable with respect to two signals x_1 and x_2 if for every possible detector $\mathcal{D}(y)$ we have

$$P_d - P_f \leq \vartheta. \tag{7}$$

According to the above definition, lower values of ϑ correspond to higher security, with $\vartheta = 0$ being equivalent to perfect secrecy. Given an OTS cryptosystem defined by a sensing matrix A with a certain distribution, we can link the ϑ-indistinguishability of the cryptosystem to $\mathbb{P}(y|x_1)$ and $\mathbb{P}(y|x_2)$. Let us define the total variation (TV) distance between the probability distributions $\mathbb{P}_A(a)$ and $\mathbb{P}_B(b)$ as $\delta(\mathbb{P}_A(a), \mathbb{P}_B(b)) = \frac{1}{2}\int |\mathbb{P}_A(t) - \mathbb{P}_B(t)| dt$. Let us also denote in short $\delta(\mathbb{P}(y|x_1), \mathbb{P}(y|x_2)) = \delta(\mathbb{P}_1, \mathbb{P}_2)$. We have the following:

Lemma 1. An OTS cryptosystem is at least $\delta(\mathbb{P}_1, \mathbb{P}_2)$-indistinguishable with respect to two signals x_1 and x_2.

Proof. The sum of error probabilities in a statistical hypothesis test can be lower bounded as [14]

$$\begin{aligned}\Pr\{\mathcal{D}(y) = x_2|x_1\} + \Pr\{\mathcal{D}(y) = x_1|x_2\} &= 1 - P_d + P_f \\ &\geq 1 - \delta(\mathbb{P}(y|x_1), \mathbb{P}(y|x_2))\end{aligned} \tag{8}$$

from which it is immediate to derive $P_d - P_f \leq \delta(\mathbb{P}_1, \mathbb{P}_2)$. □

The above result can be used to characterize the security of G-OTS-C and G-OTS-R cryptosystems. Given any two different signals x_1 and x_2, we have the following result:

Proposition 2. A G-OTS-C cryptosystem is at least $\vartheta_C(x_1, x_2)$-indistinguishable w.r.t. x_1, x_2, where

$$\vartheta_C(x_1, x_2) = \frac{1}{2}\sqrt{\log\frac{|C_2|}{|C_1|} + \mathrm{Tr}(C_2^{-1}C_1) - m} \tag{9}$$

and $C_h = P C_{x_h} P^T$, for $h = 1, 2$.

Proof. Thanks to Proposition 1, we have that $\mathbb{P}(y|x_h) = \mathcal{N}(0, \sigma_A^2 C_h)$. Hence, the Kullback-Leibler (KL) divergence between $\mathbb{P}(y|x_1)$ and $\mathbb{P}(y|x_2)$ can be expressed as [15]

$$D(\mathbb{P}_1||\mathbb{P}_2) = \frac{1}{2}\left[\log\frac{|C_2|}{|C_1|} + \mathrm{Tr}(C_2^{-1}C_1) - m\right]. \tag{10}$$

The result then follows from Pinsker's inequality between TV distance and KL divergence [16], which states $\delta(\mathbb{P}_1, \mathbb{P}_2) \leq \sqrt{D(\mathbb{P}_1||\mathbb{P}_2)/2}$. □

Proposition 3. A G-OTS-R cryptosystem is at least $\vartheta_R(x_1, x_2)$-indistinguishable w.r.t. x_1, x_2, where

$$\vartheta_R(x_1, x_2) = \sqrt{\frac{1}{4N_P}\sum_{r=1}^{N_P}\left[\log\frac{|C_{2,r}|}{|C_{1,r}|} + \mathrm{Tr}(C_{2,r}^{-1}C_{1,r})\right] - \frac{m}{4}} \tag{11}$$

and $C_{h,r} = P_r C_{x_h} P_r^T$, for $h = 1, 2$.

Proof. Thanks to Corollary 1, we have that $\mathbb{P}(y|x_h) = \frac{1}{N_P}\sum_{r=1}^{N_P}\mathcal{N}(0, \sigma_A^2 C_{h,r})$. The KL divergence between two mixture distributions with the same number of components $\mathbb{P}_i = \sum_r w_{h,r}\mathbb{P}_{h,r}$, $h = 1, 2$, can be upper bounded as [15]

$$D(\mathbb{P}_1||\mathbb{P}_2) \leq D(w_1||w_2) + \sum_r w_{1,r} D(\mathbb{P}_{1,r}||\mathbb{P}_{2,r}). \tag{12}$$

The result can be easily obtained by considering that $w_{1,r} = w_{2,r} = \frac{1}{N_P}$, from which $D(w_1||w_2) = 0$, $D(\mathbb{P}_{1,r}||\mathbb{P}_{2,r})$ can be computed as in (10), and then applying Pinsker's inequality to the upper bound on the KL divergence. □

For relatively small values of n and m, the computation of the bound in (11) can be become prohibitively expensive. Following the suggestion in [17], we can approximate the KL divergence between the two mixture distributions using the KL divergence of two multivariate Gaussian distributions having the same mean and covariance matrix. Interestingly, the

covariance matrix of the involved mixture distributions has a very peculiar form, since

$$[C_h]_{ij} = \sum_{r=1}^{N_P} \frac{1}{N_P}[C_{h,r}]_{ij} = \begin{cases} \sigma_A^2 \mathcal{E}_{x_h} & i = j \\ \sigma_A^2 \sum_{s \neq t} x_{h,s} x_{h,t} & i \neq j \end{cases} \tag{13}$$

for $h = 1, 2$. The above covariance matrix can be expressed in a compact form as $C_h = \alpha_h I_m + \beta_h \mathbb{1}\mathbb{1}^T$, where we define $\alpha_h = \frac{\sigma_A^2}{n-1}(n\mathcal{E}_{x_h} - (\mathbb{1}^T x_h)^2)$ and $\beta_h = \frac{\sigma_A^2}{n-1}((\mathbb{1}^T x_h)^2 - \mathcal{E}_{x_h})$. Thanks to the above representation, the KL divergence between $\mathbb{P}(y|x_1)$ and $\mathbb{P}(y|x_2)$ can be approximated as

$$\begin{aligned} D(\mathbb{P}_1||\mathbb{P}_2) \approx & \frac{1}{2}\left[\log \frac{\alpha_2^{m-1}(\alpha_2 + m\beta_2)}{\alpha_1^{m-1}(\alpha_1 + m\beta_1)} \right. \\ & \left. + \frac{m\alpha_2(\alpha_1 + \beta_1) + m(m-1)\alpha_1\beta_2}{\alpha_2(\alpha_2 + m\beta_2)} - m\right] \\ \triangleq & \tilde{D}(x_1, x_2). \end{aligned} \tag{14}$$

The above equation can be used together with Pinsker's inequality to provide an approximation of the TV between the two mixture distribution. However, since (14) is not an upper bound on KL divergence, we can not use it to provide a strict security bound for the G-OTS-R cryptosystem.

In [8], the authors proposed to create a sort of secure channel by normalizing the measurements to unit norm vectors. Such a normalization does not provide a perfectly secure channel in the case of circulant sensing matrices. However, we can provide an upper bound on the security of normalized G-OTS-C and G-OTS-R cryptosystems by using the above propositions. Let us define $u_{x_h} = x_h/\sqrt{\mathcal{E}_{x_h}}$ and $u_{y_h} = y_h/\sqrt{\mathcal{E}_{y_h}}$, where $y_h = Ax_h$, $h = 1, 2$. Then we have the following

Corollary 2. If a G-OTS cryptosystem based on circulant matrices is $\vartheta(u_{x_1}, u_{x_2})$-indistinguishable w.r.t. equal-energy signals u_{x_1}, u_{x_2}, then the normalized version of the same cryptosystem is at least $\vartheta(u_{x_1}, u_{x_2})$-indistinguishable w.r.t. generic signals x_1, x_2.

Proof. Let us define $y_i' = Au_{x_i}$. It is easy to verify that $u_{y_i'} = y_i'/\sqrt{\mathcal{E}_{y_i'}} = u_{y_i}$. Then, we have the following inequalities involving the KL divergence

$$\begin{aligned} D(y_1'||y_2') =& D(\mathbb{P}(u_{y_1}, \mathcal{E}_{y_1'})||\mathbb{P}(u_{y_2}, \mathcal{E}_{y_2'})) \\ =& D(u_{y_1}||u_{y_2}) + D(\mathbb{P}(\mathcal{E}_{y_1'}|u_{y_1})||\mathbb{P}(\mathcal{E}_{y_1'}|u_{y_1})) \\ \geq& D(u_{y_1}||u_{y_2}) \end{aligned} \tag{15}$$

where we exploited the chain rule for KL divergence [16] and the fact that KL divergence is always nonnegative. Hence, the proof follows from the following chain of inequalities

$$\delta(\mathbb{P}(u_{y_1}), \mathbb{P}(u_{y_2})) \leq \sqrt{\frac{1}{2}D(u_{y_1}||u_{y_2})} \leq \sqrt{\frac{1}{2}D(y_1'||y_2')}. \tag{16}$$

It is easy to verify that in the case of G-OTS-C and G-OTS-R cryptosystems the right hand side of (16) evaluates to $\vartheta_C(u_{x_1}, u_{x_2})$ and $\vartheta_R(u_{x_1}, u_{x_2})$, respectively. □

IV. Attacks to CS Cryptosystems based on Circulant Matrices

The bounds introduced in the previous Section hold for any possible attack under the COA scenario. However, it is interesting to evaluate the performance of practical attacks with respect to those bounds. In this section, we will introduce two attacks to G-OTS-C and G-OTS-R cryptosystems. The aim of the attacks is to distinguish two different equal-energy signals by exploiting their different autocorrelation functions. Since these attacks are derived as the solution of a detection problem, they will be referred to as *detection attacks*.

We consider a scenario in which an OTS cryptosystem is used to sense two distinct signals x_1 and x_2 having equal energy. Without loss of generality, we can assume that $\mathcal{E}_{x_1} = \mathcal{E}_{x_2} = 1$. The aim of the attacker is to guess whether the measurements conceal the signal x_1 or the signal x_2. This is a classical detection problem, where the aim is to distinguish whether the measurements y come from the probability distribution $\mathbb{P}(y|x_1)$ or from the probability distribution $\mathbb{P}(y|x_2)$.

Let us consider a detector $\mathcal{D}$. The Neyman-Pearson (NP) lemma states that for a given probability of false alarm P_f, the probability of detection is maximized by letting $\mathcal{D}(y) = x_1$ whenever

$$\Lambda(y) = \frac{\mathbb{P}(y|x_1)}{\mathbb{P}(y|x_2)} \geq \tau \tag{17}$$

where τ satisfies $\Pr\{\Lambda(y) \geq \tau | x_2\} = P_f$.

In the case of the G-OTS-C cryptosystem, the optimal NP test can be easily obtained as

$$\Lambda_C(y) = y^T(C_2^{-1} - C_1^{-1})y \geq \tau'. \tag{18}$$

where $\tau' = \log\tau + \frac{1}{2}\log|2\pi C_1| - \frac{1}{2}\log|2\pi C_2|$.

In the case of the G-OTS-R cryptosystem, the optimal NP test would be obtained as the ratio of two mixture distributions. Even with relatively small values of n and m, the number of components of such mixture distributions becomes prohibitively high, so that it is not practical to evaluate the NP test. As done for the approximation of the KL divergence, a suboptimal yet practical test can be obtained by approximating the two mixture distributions using two multivariate Gaussian distributions with the same mean and covariance matrix. By using the expressions of the covariance matrices found in Section III, after simple computations the test can be expressed as

$$\begin{aligned} \Lambda_R(y) = & \left(\frac{1}{\alpha_2} - \frac{1}{\alpha_1}\right) y^T y \\ & - \left(\frac{\beta_2}{\alpha_2(\alpha_2 + m\beta_2)} - \frac{\beta_1}{\alpha_1(\alpha_1 + m\beta_1)}\right)(\mathbb{1}^T y)^2 \\ \geq & \tau'' \end{aligned} \tag{19}$$

where τ'' satisfies $\Pr\{\Lambda_R(y) \geq \tau'' | x_2\} = P_f$. It is worth noting that the above test is not able to distinguish equal-energy signals whose components sum up to the same value in magnitude, i.e., such that $|\mathbb{1}^T x_1| = |\mathbb{1}^T x_2|$, since in this case we have $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$.

V. Simulation Results

In this section, we evaluate the security of G-OTS-C and G-OTS-R cryptosystems in different scenarios. For the G-OTS-C cryptosystem, we consider the matrix P that selects the first m rows of the $n \times n$ circulant matrix $W^H \Lambda W$: an advantage of this construction is that the resulting sensing matrix enables several processing tasks directly on the measurements [12]. In a first experiment, we compared the theoretical upper bounds ϑ_C and ϑ_R with the performance obtained by the optimal test Λ_C and the suboptimal test Λ_R, respectively. Since the upper bound ϑ_R can be efficiently computed only for small values of N_P, we also considered the approximation $\vartheta'_R = \sqrt{\tilde{D}(x_1, x_2)/2}$ computed according to (14). We consider only unit energy signals: thanks to Cor. 2, similar results also apply to arbitrary signals if we consider normalized measurements. The signals have been defined as $x_1 = [1, 0, \ldots, 0]$ and $[x_2]_i = Z(\alpha) e^{-4\alpha(i-1)}$, for $i = 1, \ldots, n$, where $Z(\alpha)$ is a suitable normalizing constant such that $\mathcal{E}_{x_2} = 1$. The above signals have a common autocorrelation function. Moreover, x_2 tends to become similar to x_1 as α increases.

In Fig. 1 we show the theoretical upper bounds for $\alpha \in [0, 1]$, $m = 2$, and $n = 100$. In the same plot, we also show the maximum value of $P_d - P_f$ achieved by the two tests in (18) and (19), evaluated over 10^7 independent realizations. The performance of the detection attack Λ_C is predicted quite well by the theoretical upper bound ϑ_C, whereas the upper bound ϑ_R appears quite loose. Interestingly, the approximation ϑ'_R is quite close to the simulated performance of the detection attack Λ_R, especially for higher values of ϑ. In Fig. 2, we show the same performance metrics for $\alpha = 1$ and $m \in [2, 100]$. The bound ϑ_R is not computed here since its complexity becomes exceedingly high when m increases. From both figures, it is evident that the G-OTS-R cryptosystem has a greater security than the G-OTS-C one. However, the security of both cryptosystems appears to have the same asymptotic behavior: namely, both curves in Fig. 2 suggest that the performance of the detection attack increases as $O(\sqrt{m})$.

In a second experiment, we computed the numerical upper bound $\vartheta_C(x_1, x_2)$ and the approximated bound $\vartheta'_R(x_1, x_2)$ for different realizations of equal-energy signals x_1 and x_2 and different scenarios. The exact upper bound $\vartheta_R(x_1, x_2)$ is not considered here because its computation would become impractical. We considered 1000 pairs θ_1, θ_2 of independent vectors of length k with values uniformly distributed on a unit norm k-sphere: the respective k-sparse signals were obtained by multiplying those vectors by a $n \times k$ matrix obtained by taking k columns from a $n \times n$ unitary matrix Φ. The first scenario considered as Φ the identity matrix, i.e., the signals were sparse in the sensing domain, where the k columns were randomly chosen. The second scenario considered the first k columns of the discrete cosine transform (DCT) matrix. In both scenarios we computed the bounds for $m = 2$.

In Fig. 3, we show the 0.95 percentile of $\vartheta_C(x_1, x_2)$ and $\vartheta'_R(x_1, x_2)$ when $n = 1000$ and k varies in the interval $[1, 500]$. The results show that for the two considered classes

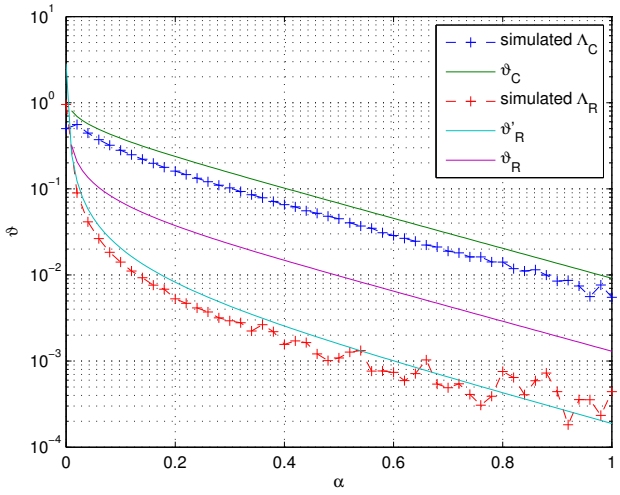

Figure 1. Distinguishability of unit energy vectors for $m = 2$, $n = 100$.

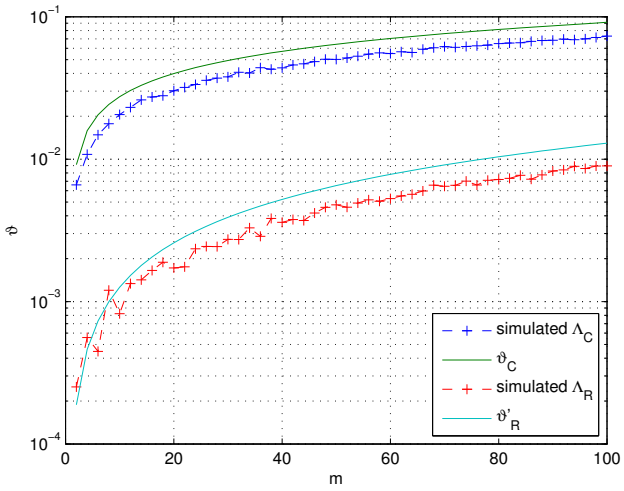

Figure 2. Distinguishability of unit energy vectors for $\alpha = 1$, $n = 100$.

of sparse signals the security of G-OTS-C and G-OTS-R has a similar behavior: the security of both cryptosystems is independent of k when the signal is sparse in the sensing domain, whereas there is a strong dependence on the signal sparsity when the signal is sparse in the DCT domain, since sparser signals are more difficult to conceal. An intuitive explanation is that a very sparse signal in the DCT domain is heavily correlated in the sensing domain and a circulant matrix leaks a lot of information on this correlation.

In Fig. 4, we show the 0.95 percentile of $\vartheta_C(x_1, x_2)$ and $\vartheta'_R(x_1, x_2)$ when $k = 10$ and n varies in the interval $[20, 1000]$. The security of the G-OTS-C cryptosystem increases for large values of n when the signal is sparse in the sensing domain, whereas it surprisingly decreases for large values of n when the signal is sparse in the DCT domain. In the case of the G-OTS-R cryptosystem, the security is independent of n when the signal is sparse in the DCT domain, whereas it significantly increases for large values of n when

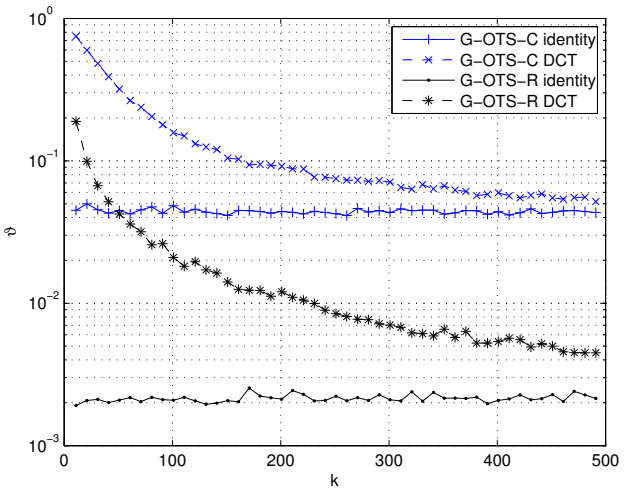

Figure 3. Distinguishability of k-sparse unit energy signals, for $n = 1000$.

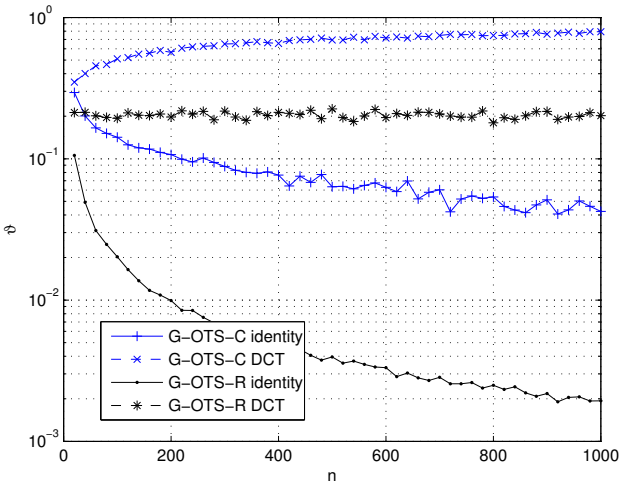

Figure 4. Distinguishability of k-sparse unit energy signals, for $k = 10$.

the signal is sparse in the sensing domain.

VI. Conclusions

In this paper, we have analyzed the security of CS measurements when the sensing matrix is a partially circulant random matrix. Unlike the case of fully random Gaussian matrices, which reveal only the energy of the sensed signal, we find that circulant matrices reveal also some partial information on the autocorrelation of the signal. This fact implies that normalizing the measurements can not achieve a perfectly secure channel for this kind of matrices. In order to measure this loss of security, we introduce an operational definition of security based on the problem of distinguishing different signals and we provide useful bounds for evaluating the security of circulant sensing matrices according to this definition.

The above definition has been applied to two different types of partially circulant matrices, considering two classes of sparse signals. The results indicate that partially circulant matrices obtained by taking the first rows of a circulant matrix, which are interesting in practical settings since they enable processing directly on the measurements, are in general less secure than matrices obtained by randomly selecting the rows. Moreover, the results also show that randomized circulant matrices can provide a weak encryption layer if the signals are sparse in the sensing domain, but are not very secure if the signal is sparse in a DFT-like domain. Since the security of circulant matrices is linked to the autocorrelation of the sensed signal, an interesting direction for future research is investigating whether a scrambling applied before sensing [18] can actually improve the security of this kind of matrices when applied to signals that are sparse in generic domains.

Acknowledgment

The research leading to these results has received funding from the European Research Council under the European Community's Seventh Framework Programme (FP7/2007-2013) / ERC Grant agreement n. 279848.

References

[1] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, 2006.

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

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] T. Bianchi, V. Bioglio, and E. Magli, "On the security of random linear measurements," in *ICASSP'14*, 2014, pp. 3992–3996.

[9] H. Rauhut, "Circulant and Toeplitz Matrices in Compressed Sensing," in *SPARS'09 - Signal Processing with Adaptive Sparse Structured Representations*, 2009.

[10] W. Yin, S. Morgan, J. Yang, and Y. Zhang, "Practical compressive sensing with Toeplitz and circulant matrices," in *Proc. SPIE*, vol. 7744, 2010, pp. 77 440K–77 440K–10.

[11] 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.

[12] D. Valsesia and E. Magli, "Compressive signal processing with circulant sensing matrices," in *IEEE ICASSP'14*, 2014, pp. 1015–1019.

[13] T. Stütz and A. Uhl, "A survey of H.264 AVC/SVC encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 325 –339, Mar. 2012.

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

[15] M. Do, "Fast approximation of Kullback-Leibler distance for dependence trees and hidden Markov models," *IEEE Signal Process. Lett.*, vol. 10, no. 4, pp. 115–118, April 2003.

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

[17] J. Hershey and P. Olsen, "Approximating the Kullback Leibler divergence between Gaussian mixture models," in *ICASSP'07*, vol. 4, April 2007, pp. IV–317–IV–320.

[18] 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.