Information Processing Letters 116 (2016) 279–283

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Introducing the counter mode of operation to Compressed Sensing based encryption

Robin Fay

Chair for Data Communications Systems, University of Siegen, Hoelderlinstr. 3, 57068 Siegen, Germany

ARTICLE INFO

Article history:
Received 13 July 2015
Received in revised form 2 November 2015
Accepted 13 November 2015
Available online 19 November 2015
Communicated by L. Viganò

Keywords:
Compressed Sensing
Cryptography
Modes of operation

ABSTRACT

Compressed Sensing based encryption is computationally secure in a one time key scenario, but it does not resist chosen-plaintext attacks (CPA) due to the deterministic encryption process. This paper introduces the counter mode of operation to Compressed Sensing based encryption in order to achieve probabilistic encryption with security against chosen-plaintext attacks. In particular, the proposed scheme addresses the case where multiple signals are encrypted under one master key. The security of the proposed scheme is solely based on the inherent secrecy of the compressed measurements, meaning that no additional ciphers are utilized to ensure CPA-security. To achieve this objective, a method for updating the secret sensing matrix on every signal is presented, such that each signal is encrypted under a fresh pseudorandom matrix.

1. Introduction

In the Compressed Sensing (CS) framework confidentiality is achieved by treating the coefficients of the underlying underdetermined system of linear equations as a shared secret between sender and recipient. By this means, compression and encryption can be performed in a single operation where the additional costs are limited to key management only. Prior studies showed that breaking this kind of encryption is computationally hard for an eavesdropping adversary in the case where just one signal is encrypted under a particular matrix [1]. Conversely, it is clear that the adversary learns useful information if a matrix is used to encrypt multiple signals, since encryption is performed in Electronic Codebook (ECB) mode. This circumstance is a primary motivation to develop and investigate methods towards protecting Compressed Sensing based encryption against chosen-plaintext attacks (CPA).

Huang et al. [2] proposed an image encryption scheme, where CPA-security is achieved through Compressed Sensing followed by additional substitution and permutation layers. While this approach is application specific, it presents a general concept to achieve CPA-security in the framework of Compressed Sensing that may be called *compress-then-encrypt*, because resistance against CPA is achieved by supplementary block cipher components. Indeed, these components introduce further costs, although the secrecy of the compressed measurements may be exploited directly to ensure CPA-security. Apart from that, Zhang et al. [3] suggested to use a bi-level protection where a distinct key is used in order to generate a key-related sparsifying basis besides the secret sensing matrix. This approach is more general than the compress-then-encrypt concept but it might prove hard to find suitable sparsifying bases for each particular application.

In modern cryptography, security against an active attacker is achieved by running the block cipher in some mode of operation, which turns the deterministic behavior of the block cipher after fixing the key into a probabilistic encryption scheme. This paper introduces a mode of operation to Compressed Sensing based encryption in order to ensure confidentiality when one shared master key is used to encrypt multiple messages. More precisely, this paper

E-mail address: robin.fay@uni-siegen.de.

http://dx.doi.org/10.1016/j.ipl.2015.11.010
0020-0190/

describes a general model in order to alter the secret sensing matrix on every new signal.

The rest of this paper is organized as follows: Section 2 presents related works that deal with general properties and requirements of Compressed Sensing and the secrecy of Compressed Sensing based encryption. The overall challenges with CPA-security in Compressed Sensing are discussed and the core idea of the proposed method is explained. Section 3 presents the design of the so called *Compressed Sensing Counter Mode of operation* (CS-CTR) as well as its properties and some implementation details followed by a short experimental proof of concept. Section 3.5 discusses the security of the proposed mode. The final section draws a conclusion and states the future work.

2. Related work

The main challenge with CPA-security in Compressed Sensing is the linearity of the encryption process. Let $\vec{x} \in \mathbb{R}^N$ be the plaintext signal, which is assumed to be s-sparse or compressible in some domain Ψ meaning that there exists some $\vec{s}$ with

$$\vec{s} = \Psi\vec{x} \tag{1}$$

where only s entries in $\vec{s}$ are nonzero. If $\vec{x}$ is s-sparse, we may set $\Psi = I_N$.

Further let $A \in \mathbb{R}^{m\times N}(N \gg m)$ be the secret sensing matrix and let $\vec{y} \in \mathbb{R}^m$ be the ciphertext vector. Then, the sensing process respectively encryption function is defined as:

$$\vec{y} = A\vec{x} \tag{2}$$

The randomness which allows reconstruction of the sparse signal [4,5], is also necessary for the purpose of encryption and is introduced by the sensing matrix A whose entries are chosen at random from a (sub) Gaussian distribution.

The common sensing matrices for practical applications are binary sometimes called Bernoulli sensing matrices, meaning that their entries are drawn uniformly at random from the set $\{-1, 1\}$. The bit sequences used in Compressed Sensing are assumed to be from the set $\{-1, 1\}^*$ instead of $\{0, 1\}^*$, as long as not mentioned otherwise. From a cryptographic point of view, the matrix generation can be modeled using a shared secret key k as a seed for a secure pseudorandom number generator. The key needs to be random and sufficient large, say $|k| \geq 128$-Bit. Rachlin and Baron showed in [1], that it is computationally hard for an adversary to reconstruct the original signal from eavesdropped measurements without knowing the sensing matrix. An exhaustive search of all binary sensing matrices of size $m \times N$ would have complexity $2^{m\cdot N}$. In practical scenarios it can be assumed that $N \cdot m > |k|$ holds. Hence, if a pseudorandom number generator is used for matrix generation, the computational complexity of a brute force attack is reduced to the size of the shared secret key.

As described independently by Bianchi et al. [6] and Cambareri et al. [7], the encryption process preserves the signals energy so that an adversary is able to distinguish between the encryption of two signals with different energy. Cambareri et al. proved that, for large enough N, Compressed Sensing based encryption with sub Gaussian matrices leaks no information about the signal but its energy and they named this *asymptotic spherical secrecy*. Furthermore, Bianchi et al. claimed, that information theoretic secrecy can be obtained if Gaussian random matrices are used when the measurements are normalized to the same energy. Since the measurements energy needs to be known to the recipient it must be transmitted over a secure channel, which is protected using classical cryptography.

However, this strategy does not protect against an active attacker performing a chosen-plaintext attack as long as multiple signals are encrypted under the same matrix. In the CPA scenario, the adversary has access to an encryption oracle which encrypts arbitrary plaintexts of his/her choice. In order to break Compressed Sensing based encryption in ECB mode, an adversary would ask his/her encryption oracle for the encryption of all unit vectors of the standard basis and he/she would obtain the columns of the secret sensing matrix. Even if the measurements are normalized to the same energy, the attacker would gain enough useful information to break the system. For example, assume that binary random matrices are used. In this case, the adversary is just interested in the measurements sign, which does not change due to normalization. With Gaussian random matrices, the captured sensing matrix is equal to the original matrix up to a scaling factor, thus still useful for reconstruction [8, chap. 3]. Based on the fact that Compressed Sensing based encryption is deterministic for a fixed A, a general solution to achieve a probabilistic encryption scheme is to use a different random A on every new signal. This will render the previously mentioned attack useless, since an adversary would only obtain the columns of independent sensing matrices.

The main contribution of this letter is to lift the theoretical results from [6] and [7] to a more practical level, by exploiting the inherent secrecy of Compressive Sensing in order to achieve security against CPAs in a multiple encryption scenario.

3. The compressed sensing counter mode

The proposed solution is based upon the fact that encryption by Compressed Sensing leaks no information about the plaintext but its energy. It is stressed that the proposed encryption scheme does not leak additional information to an attacker even if he/she has access to an encryption oracle. The general design of the proposed *CS-CTR* mode of operation is shown in Fig. 1.

3.1. Algorithm description

At first, assume that the sender and recipient are honest parties sharing a secret key k. Both sides agree publicly on a function *rec* from the family of suitable Compressed Sensing reconstruction algorithms and an optional sparsifying basis Ψ. Further details about the reconstruction function are omitted here for the sake of adaptability, since there are many suitable candidate functions depending on the application (see [8, chap. 4/5]). If the total number of plaintexts is denoted by l, let $A_i \in \{-1, 1\}^{m\times N}$ be the sens-