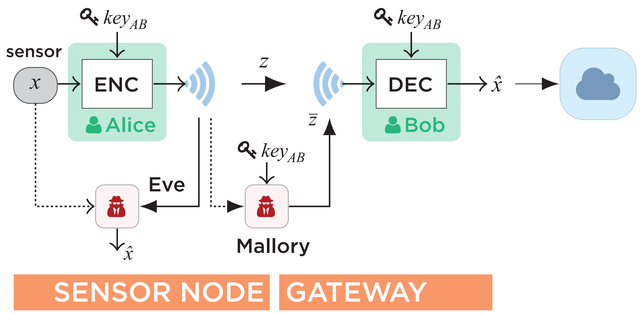
Mauro Mangia[1,3], Alex Marchioni[1], Fabio Pareschi[2,3], Riccardo Rovatti[1,3], Gianluca Setti[2,3]

CHAINED COMPRESSED SENSING FOR IOT NODE SECURITY

[1,3] DEI / ARCES - Università di Bologna - Bologna - ITALY [2] DET - Politecnico di Torino - Torino - ITALY

ABSTRACT Compressed sensing can be used to yield both compression and a limited form of security to the readings of sensors. This can be most useful when designing the low-resources sensor nodes that are the backbone of IoT applications. Here, we propose to use chaining of subsequent plaintexts to improve the robustness of CS-based encryption against ciphertext-only attacks, known-plaintext attacks and man-in-the-middle attacks.

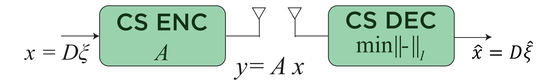


Ciphertext-Only Attacks COAs. The eavesdropper (Eve) observes the statistics of the ciphertext and tries to guess the plaintext. The attacker has some knowledge of the plaintext. For instance, the attacker might know the class of signals and the statistical distribution of the plaintext.

Know Plaintext Attacks KPAs. Eve captures some plaintext-ciphertext pairs from which she tries to identify the key key_{AB} so that, she is able to decrypt future transmissions. KPAs are easy on sensor nodes, Eve may deploy another node close to the attacked one, with the aim of acquiring the same physical signal and thus knowing the plaintext.

Man in the Middle Attacks MMAs. The attacker (Mallory), sends messages to Bob pretending to be Alice. To do so, Mallory knows the upstream key_{AB}. If an MMA is successful, Bob receives a counterfeited version of potentially critical information.

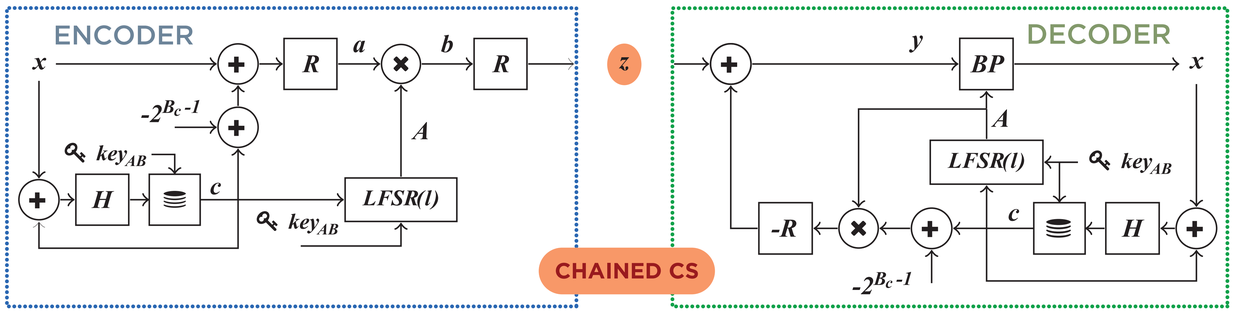
Compressed Sensing (CS) aims to merge acquisition and compression. Under the assumption that x is sparse, CS is able to acquire all the information content using fewer samples with respect to the limit imposed by the Shannon-Nyquist theorem. We say that a class of signals is sparse if slices in time of the input signals x, expressed in a proper basis D (an $n \times n$ matrix), are associated to n-dim. vectors ξ with at most k non-null coefficients with $k << n$. In these cases x is k-sparse.



Encoder. The signal is acquired by projections on proper set of m different sampling sequences a_j collected row by row in the sensing matrix A (note that $m < n$). As guideline for the sampling sequences generation, the CS theory suggests to use i.i.d. random vectors.

Decoder. x can be reconstructed by solving the following optimization problem which looks at the sparsest vector mapped in the collected measurements. Classical CS theory guarantees reconstruction for $m > m_{\min} = 4k \log(n/k)$

$$\hat{\xi} = \arg\left\{\min_{\zeta} \|\zeta\|_1 \ \text{ s.t. } \ AD\zeta = y\right\} \quad \textbf{BP}$$



ENCODER

$$z = R\left(A\,R(x + c - 2^{B_c-1})\right)$$

DECODER

$$y = R\left(z - R\left(AR(c - 2^{B_c-1})\right)\right)$$

LFSR generates antipodal sensing matrices A
B_ξ number of bits to code ξ

signed modulus

$$R(\xi) = (\xi \bmod 2^{B_c}) - 2^{B_c-1} \in \mathbb{Z}(B_c)$$

LFSR state

$$l = \left(l_{prev} + \sum_{j=0}^{n-1} c_j\right) \bmod 2^{B_{LSFR}}$$

$$y = R\left(R\left(AR(x + c - 2^{B_c-1})\right) - R\left(AR(c - 2^{B_c-1})\right)\right) = R\left(A\,R(x + c - 2^{B_c-1} - c + 2^{B_c-1})\right) = Ax$$

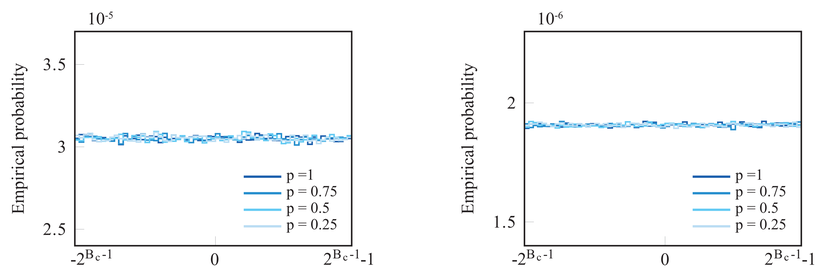
c as function of the previous state c_{prev} and the previous signal x_{prev}

$$c = H(c_{prev} + x_{prev}) = \left((2^{B_c} - 3)(c_{prev} + x_{prev}) + 1\right) \bmod 2^{B_c}$$

COA

CS $z = y = Ax$, with n high enough, x is completely hidden but, since y is obtained by mean of linear transformations, info about signal energy leaks.

Chained CS makes the statistics of z independent from the energy of x so that no info about the plaintext leaks. Each chainer state component c_j is uniformly distributed due to the hash function H. Thus, $a = R(x + c - 2^{B_c-1})$ is uniformly distributed as well as $b = Aa$.



Empirical probabilities of different values of the ciphertext z (k=3,12) and for different average energy of the plaintext.

n	k	m	B_x	B_c	$KPA >>$
128	3	27	8	15	5.3×10^{889}
128	6	41	10	17	2.4×10^{1326}
128	12	57	12	19	4.7×10^{1809}

k	m	p	KS[10^{-4}]	$\overline{\text{KS}}$[10^{-4}]	Γ[10^{-2}]	$\overline{\Gamma}$[10^{-2}]
3	27	1.00	6.7	3.8	0.85	1.16
3	27	0.75	3.5		1.04	1.05
3	27	0.50	3.0		0.76	1.08
3	27	0.25	4.0		0.88	1.09
6	41	1.00	4.8	3.4	1.10	1.22
6	41	0.75	4.3		1.20	1.06
6	41	0.50	3.4		1.07	1.04
6	41	0.25	2.6		1.09	0.98
12	57	1.00	4.1	2.5	1.07	1.04
12	57	0.75	5.3		1.43	1.14
12	57	0.50	4.7		1.15	1.10
12	57	0.25	4.5		1.14	1.09

KPA

CS A can be computed by inverting $y = A\,x$, therefore, by solving a set of underdetermined diophantine equations, where for each antipodal row of A, a_j, the attacker is not able to detect wich one is the right solution along a huge amount af indistinguishable candidates.

$$2^{n-B_x}\sqrt{3/\pi n}$$

Chained CS The attacker has access to x and z but she does not know y and c. In addiotion to above task, Eve must invert the signed modulus R by solving $z + 2^{B_c} d = A\,a$ for a, A, and d unknown. Here d is an integer and a is a function of the chainer state.

MMA

CS No immunity

Chained CS If Mallory steps in after the communication has been established between Alice and Bob, she does not know the history of ciphertextes and she can reconstruct neither the state of the chain nor the state of the LFSR that, instead is known to both Alice and Bob.

Valerio Cambareri, Mauro Mangia, Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, "Low-complexity multiclass encryption by compressed sensing," IEEE Transactions on Signal Processing, vol. 63, no. 9, pp. 2183–2195, May 2015.

Valerio Cambareri, Mauro Mangia, Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, "On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis," IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2182–2195, Oct. 2015.

Tiziano Bianchi, Valerio Bioglio, and Enrico Magli, "Analysis of one-time random projections for privacy preserving compressed sensing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 313–327, Feb. 2016.