CHAINED COMPRESSED SENSING FOR IOT NODE SECURITY

Mauro Mangia[†+], *Alex Marchioni*[+], *Fabio Pareschi*[†*], *Riccardo Rovatti*[†+], *Gianluca Setti*[†*]

[†] ARCES - Università di Bologna - via Toffano 2/2 - Bologna - ITALY
[*] DET - Politecnico di Torino - c.so Duca degli Abruzzi 24 - Torino - ITALY
[+] DEI - Università di Bologna - viale Risorgimento 2 - Bologna - 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.

Index Terms— compressed sensing, criptography, internet of things

1. INTRODUCTION

The real-world deployment of systems inspired by the Internet of Things (IoT) paradigm (see, e.g., [1], [2], and [3]) requires the collection of data from a multitude of sensing nodes with minimal energy footprint. This has increased the attention to the need of guaranteeing the privacy of data gathered and distributed by low-complexity networked devices in which every resource, including those spent for security, must be tailored to the actual requirements of each application.

Compressed Sensing (CS) is a signal acquisition technique embedding implicit compression that has been investigated as a way of implementing low-resources sensing nodes (see, e.g., [4][5]) and has been proposed to also introduce security directly into the acquisition process at the analog-to-information interface or jointly with digital signal compression [6, 7, 8, 9, 10, 11, 12, 13].

In rough terms, what happens in CS is that chunks of an input waveform are represented with fewer scalars than the number of samples indicated by the Nyquist-Shannon theorem, which makes CS very appealing for low-resources IoT nodes. Such a lower-resource acquisition is possible assuming that the signal to process is *sparse*, i.e. a proper basis exists such that the projection of any input waveform over that basis has only few terms significantly different from zero. Acquisition (encoding) is practically achieved by multiplication by a random matrix, whose knowledge is needed to reconstruct the original signal via a non-linear decoding algorithm [14]. Such a matrix can therefore be considered as a key which, once shared between the IoT node and the corresponding gateway, guarantees a certain degree of secrecy *without the need of any additional cryptographic stage*.

The main contribution of this paper is the application of chaining techniques (i.e., the idea that every piece of encoded information incorporates a summary of previous pieces of information, as happens in the block-chain technology already proposed in the IoT context [15, 16, 17]) to improve the privacy level of CS acquisition, thus obtaining a solution for secure data transmission between an IoT node and the gateway.

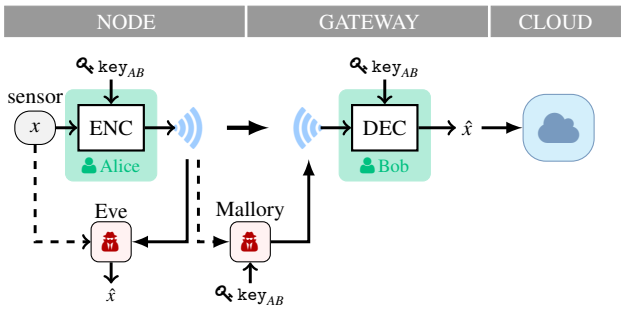

Fig. 1. The upstream link and possible attacks in a distributed sensing environment.

The paper is organized as follows. Section 2 describes the essential steps in CS encoding and decoding. Section 3 frames CS in the context of secure communication between sensor nodes and gateways. Section 4 introduces chaining and its properties that are exploited in Section 5 to show that the link has been hardened against typical attacks. Due to space limitations proofs are only sketched. Section 6 reports some empirical evidence and conclusions are drawn at the end.

2. COMPRESSED SENSING AND BLOCK CIPHERS

The signal waveform is acquired as a sequence of time windows, the t-th of which starts at discrete instant t. Within each window n samples are collected that we arrange in the vector $x[t] = (x[t]_0, \dots, x[t]_{n-1})$. If, given a number B of bits, we define $\mathbb{Z}(B) = \{-2^{B-1}, \dots, 2^{B-1} - 1\}$ and $\mathbb{N}(B) = \{0, \dots, 2^B - 1\}$ then we have $x[t] \in \mathbb{Z}(B_x)^n$ for some B_x.

CS assumes that at most $\kappa \ll n$ entries of $x[t]$ are non-zero [18]. Then, it multiplies $x[t]$ by an $m \times n$ matrix $A[t]$ to obtain a so-called measurement vector $y[t] = A[t]x[t]$. We will assume that $A[t]$ is a random choice of ± 1 symbols generated by a Pseudo-Random Number Generator (PRNG) [19].

Despite the fact the $y[t]$ is only m-dimensional, one may recover the original signal $x[t]$ exploiting the sparsity prior to solve the otherwise undetermined system of equations $y[t] = A[t]x[t]$. In fact, it can be proved [18] that this may be done, under suitable assumptions, by estimating $\hat{x}[t]$ as

$$\hat{x}[t] = \arg\min_x \|x\|_1 \quad \text{s.t. } A[t]x = y[t] \tag{1}$$

where $\|\cdot\|_1$ is the ℓ_1-norm, i.e., $\|x\|_1 = \sum_{j=0}^{n-1} |x_j|$. This method is called Basis Pursuit (BP) and gives ground to most non-greedy

recovery algorithms commonly employed in CS (see, f.i., [20] and references therein).

Since (1) is convex it admits a unique solution and since $x[t]$ has integer entries, then $y[t] = A[t]x[t]$ also has integer entries and recovery can yield $\hat{x}[t] = x[t]$, i.e. and errorless reconstruction.

Theory ensures that this happens when m is $O\left(\kappa \log\left({}^{n}/_{\kappa}\right)\right)$ [18, 14]. In practical cases $m \ll n$ and thus, since the data representing the signal must be transmitted or stored, CS provides acquisition with implicit compression.

Further to that, note that to recover the original signal, the decoder needs $A[t]$, i.e., the seed of the PRNG used to generate it which implicitly plays the role of a private key in a block cipher scheme encrypting the *plaintext* $x[t]$ into the *ciphertext* $y[t]$. The corresponding decoded is (1) that uses the same key to recover the plaintext.

3. A PROTECTED COMMUNICATION SCHEME BETWEEN SENSORS AND GATEWAYS

In a classical abstract framework, a legitimate transmitter (Alice) produces a ciphertext from a plaintext and transmits it to a receiver (Bob). For us, Alice may represent the sensing subsystem of any IoT device and Bob is the gateway collecting readings and feeding them to the cloud. Figure 1 reports a schematic view of the link and of the attackers.

Alice and Bob have agreed on the private key $\texttt{key}_{AB}$ that should ensure privacy of the upstream link from sensor to hub. The classical way of exploiting CS as a block cipher is to make $\texttt{key}_{AB}$ control the PRNG that generates $A[t]$ [6, 7, 8, 13].

In Ciphertex-Only Attacks (COAs) the eavesdropper (Eve) observes the statistics of the ciphertext and tries to guess the plaintext. It is known (see, e.g., [6, 8]) that when n is large, straightforward implementation of CS almost completely hide the ciphertext since the components in $y[t]$ are distributed as identical Gaussian whose variance is proportional to the average energy of $x[t]$, which is therefore the only leaking information.

Known-Plaintext Attacks (KPAs) are even more threatening as they rely on side-information. Eve captures some plaintext-ciphertext pairs from which she tries to identify the corresponding encoding matrices and thus $\texttt{key}_{AB}$ to be able decrypt future transmissions. Regrettably, KPAs are easy on sensor nodes. In fact, Eve may deploy another node close to the attacked one, with the aim of acquiring the same physical signal and thus knowing the plaintext.

Rejection of KPAs is not complete. Given $x[t]$ and $y[t]$, finding a matrix $A[t]$ made of ± 1 that is compatible with $y[t] = A[t]x[t]$ is quite easy. Security stems from the fact that the number of candidate solutions $A[t]$ can be made so large that pinpointing the true matrix can be made very hard [7].

In MMAs, the attacker (Mallory), sends messages to Bob pretending to be Alice. To do so, Mallory knows the upstream key $\texttt{key}_{AB}$. If an MMA is successful, Bob receives a counterfeited version of potentially critical information.

In this paper, we embed chaining into encryption by CS to increase robustness against COAs and KPAs and help countering MMA attempts.

4. CS WITH CHAINING

Chaining is a common way of increasing the security of sequences of block ciphers. Here we use it both as a signal masking technique and to affect the reproducible PRNG. Figure 2 reports a block scheme of the encoding and decoding stages.

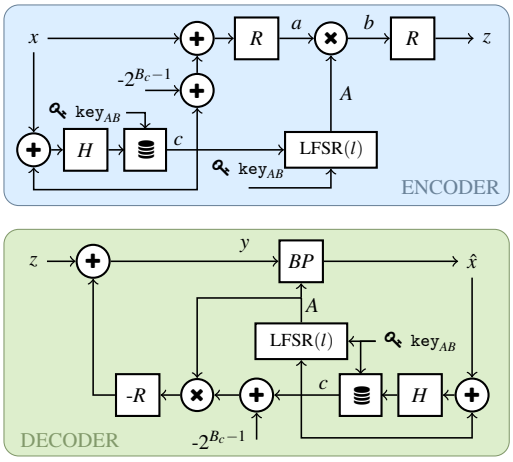

Fig. 2. Block scheme of an encoder and a decoder based on chained CS.

Chaining is made on each component of the signal window by defining a vector of B_c-bits digital words $c[t] \in \mathbb{N}(B_c)^n$ that is initialized by with $c[0] = \texttt{key}_{AB}$ and updated as

$$c[t+1] = H\left(c[t] + x[t]\right) = \left(\alpha\left(c[t] + x[t]\right) + \beta\right) \bmod 2^{B_c} \quad (2)$$

where we set $\beta = 1$ and $\alpha = 2^{B_c} - 3$ to guarantee that the congruential mapping in the update preserves maximum length cycles [21] and the hashing function H that remains implicitly defined is applied component-by-component. The number of bits devoted to each chain state is $B_c = B_x + \lceil \log_2 n \rceil$ and is equal to the number of bits needed to encode each of the measurements in $y[t] = A[t]x[t]$ that results from the signed sum of n terms each encoded in B_x bits.

Before entering the linear encoding, the signal $x[t]$ is mixed with the chain state and the ciphertext is computed as

$$z[t] = R\left(A[t]R\left(x[t] + c[t] - 2^{B_c-1}\right)\right) \quad (3)$$

where the *signed-modulus* $R(\xi) = \left(\xi \mod 2^{B_c}\right) - 2^{B_c-1} \in \mathbb{Z}(B_c)$ is applied component-by-component.

As far as the generation of $A[t]$ is concerned, though more sophisticated non-white PRNG may find applications in CS (see, e.g., [22] for rakeness-based CS[1]), to limit system complexity we here adopt a simple Linear-Feedback-Shift-Register (LFSR) with B_{LFSR} bits. With this, if $l'[t] \in \mathbb{N}(B_{\mathrm{LFSR}})$ is the integer encoding the state from which the LFSR is run to produce the antipodal entries of the matrix $A[t]$, then

$$l'[t] = \left(l''[t-1] + \sum_{j=0}^{n-1} c[t]_j\right) \mod 2^{B_{\mathrm{LFSR}}}$$

where $l''[t]$ is the state of the LFSR at the end of the generation of $A[t]$,with $l''[-1] = \texttt{key}_{AB} \mod 2^{B_{\mathrm{LFSR}}}$.

[1] a technique [23] to adapt $A[t]$ to the features of the input signals not unlikely to what is done in (chaos-based) DS-CDMA where chip waveforms, spreading sequence statistics and rake receivers taps can be jointly selected to *rake* as much energy as possible at the received side [24][25].

At each time instant the decoder receives $z[t]$ and knows the chain state $c[t]$, since it knows the key and has decoded previous transmissions reconstructing $x[\tau]$ for $\tau = 0, \ldots, t-1$. Hence it may compute

$$y[t] = z[t] - R\left(A[t]\left(c[t] - 2^{B_c - 1}\right)\right) = R\left(A[t]x[t]\right) = A[t]x[t]$$

where the last equality holds since B_c is the number of bits needed to represent each entry of $A[t]x[t]$. The current $x[t]$ can therefore be obtained by BP.

5. HARDENING BY CHAINING

Chaining is a valuable tool in hardening CS-based encryption mainly due to its fundamental property: under mild conditions on the statistics of $x[t]$ the entries of $c[t]$ tends to be uniformly distributed in $\mathbb{N}(B_c)$ for $t \to \infty$. The proof of such a property can be sketched as follows.

Focus on a single entry of $c[t]$ (indicated as $s[t] \in \mathbb{N}(B_c)$) and on the corresponding entry of $x[t]$ (indicated as $w[t] \in \mathbb{Z}(B_x)$). The evolution of $s[t]$ can be seen as a trajectory of the discrete-time, finite-state dynamic

$$s[t+1] = H\left(s[t] + w[t]\right) \tag{4}$$

in which $s[t]$ is the state and $w[t]$ is a perturbation applied at each time-step. We know that our choice of parameters $\alpha = 2^{B_c} - 3$ and $\beta = 1$ make the unperturbed system periodic [21] with a period going through all the 2^{B_c} states. Due to the random nature of the incoming signal, and thus of $w[t]$, the evolution of (4) is no longer deterministic but can modeled in statistical terms. To do so, define $p[t]$ as the vector of probabilities such that $p[t]_j = \Pr\{s[t] = j\}$ and note that

$$p[t+1]_j = \sum_{k=0}^{2^{B_c}-1} \Pr\{s[t+1] = j | s[t] = k\} p[t]_k$$

where the transition probabilities $\Pr\{s[t+1] = j | s[t] = k\}$ depend on the statistics of $w[t]$ and, if the latter is stationary, can be collected in a time-invariant transition matrix P such that $p[t+1] = Pp[t]$. Under very mild assumptions on the input, we have that P is a primitive matrix, i.e., that P^τ has no null entry for τ large enough. This guarantees that there is an asymptotic $p[\infty]$ that is the unique vector of probabilities such is invariant with respect to P, i.e., $p[\infty] = Pp[\infty]$ [26, chap I and II].

To see that $p[\infty]$ is uniform, assume that $s[t]$ is distributed according to $p[\infty]$ and consider $s[t+1] = H\left(s[t] + w[t]\right) = H\left(\left(s[t] + w[t]\right) \mod 2^{B_c}\right)$. Since $s[t]$ is uniformly distributed in $\mathbb{N}(B_c)$, also $\left(s[t] + w[t]\right) \mod 2^{B_c}$ is uniformly distributed in $\mathbb{N}(B_c)$. Moreover, since the application of H would produce a maximal cycle, H itself is a bijection from $\mathbb{N}(B_c)$ to $\mathbb{N}(B_c)$ and this preserves uniformity.

Hence, for large t, components of $c[t]$ distribute uniformly over $\mathbb{N}(B_c)$. This has favorable security implications that may be distinguished depending on the attack we are trying to resist.

5.1. Robustness to COAs

We may recall (3) and decompose it by defining the intermediate vectors $a[t] = R\left(x[t] + c[t] - 2^{B_c - 1}\right)$, $b[t] = A[t]a[t]$, and $z[t] = R(b[t])$.

With this, we may first observe that if the components of $c[t]$ are uniformly distributed in $\mathbb{N}(B_c)$ then $a[t]$ has components uniformly distributed in $\mathbb{Z}(B_c)$ independently of the statistics of $x[t]$.

Hence, independently of $x[t]$, $b[t] = A[t]a[t]$ is a linear mapping of a vector of fixed statistics. Moreover the average of the components of $b[t]$ is $\mathbf{E}[b[t]] = \mathbf{E}[A[t]]a[t] = 0$ and the correlations between the component of $b[t]$ are in the matrix $\mathbf{E}\left[b[t]b[t]^\top\right] = a[t]\mathbf{E}\left[A[t]A[t]^\top\right]a[t]^\top = 0$, where the last equalities depend on the fact that $A[t]$ is made of independent antipodal symbols and thus $\mathbf{E}[A[t]] = 0$ and $\mathbf{E}\left[A[t]A[t]^\top\right] = 0$.

These are the same conditions that allow to prove (e.g., [6, 8]) that for large n the normalized result of the linear mapping, $n^{-1/2}b[t]$ distributes as a vector of Gaussian, zero-mean, independent entries with a variance equal to $1/n \sum_{j=0}^{n-1} a[t]^2$. In conventional configurations, the average of such a variance is the information that $b[t]$ leaks about $a[t]$. Yet, in our case, since the statistics of $a[t]$ is independent of $x[t]$, nothing about the plaintext can be detected by a statistical analysis of the ciphertext.

5.2. Robustness to KPAs

In the conventional configuration, the vulnerability to KPAs stems from the fact that at a certain τ, the plaintext is $x[\tau]$ and the ciphertext is $y[\tau] = A[\tau]x[\tau]$. In that case $A[\tau]$ can be computed by solving a set of underdetermined diophantine equations. Our scheme exposes $z[\tau]$ as the ciphertext. Hence, given $z[\tau]$ and $x[\tau]$, Eve must solve (3) for $A[\tau]$ and $c[\tau]$. Then, from $A[\tau]$ would like to infer the state $l'[\tau]$ of the LFSR that, along with $c[\tau]$ and $x[\tau]$, allows to compute the subsequent $A[t]$ for $t > \tau$ and thus break the cipher. The first step would be to solve

$$z[\tau] + 2^{B_c} d = A[\tau]a[\tau] \tag{5}$$

for $a[\tau]$ unknown in $\mathbb{Z}(B_c)^n$, for $A[\tau]$ made of antipodal symbols and for $d \in \{-n+1, \ldots, n-1\}^n$ to model the effect of the signed-modulus operation. Could $a[\tau]$ be guessed, $c[\tau]$ would be computed by inverting $a[\tau] = R\left(x[\tau] + c[\tau] - 2^{B_c - 1}\right)$.

Since the entries of $a[\tau]$ are uniformly distributed in their range, we may apply the results in [7] and say that for any candidate d and $a[\tau]$, the number of instances of $A[\tau]$ compatible with (5) is $\left(2^{n - B_c}\sqrt{3/\pi n}\right)^m$ for large n.

Due to the fact that neither d nor $a[\tau]$ are known and must be simultaneously identified, the number of solutions to (5) among which Eve is not able to discriminate will be much larger than that, thus making KPAs even less threatening.

5.3. Robustness to MMAs

Mallory may try to impersonate Alice as she knows $\texttt{key}_{AB}$. Yet, the state of the LFSR generating $A[t]$ depends on both $\texttt{key}_{AB}$ and $c[t]$.

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

More specifically, Mallory knows both $c[0]$ and the initialization of the LFSR since they both depend on $\texttt{key}_{AB}$. Hence, by solving (3), she would be able to compute $x[0]$ from the ciphertext $z[0]$ and thus $c[1]$ and so on, computing each $c[t]$ and $l'[t]$ from the corresponding $z[t]$. Each $c[t]$ and $l'[t]$ can then used to encode a counterfeited plaintext into a message that Bob believes to be authentic.

Yet, if she misses a certain $z[\tau]$, then the corresponding $x[\tau]$ would be unknown and since (2) needs $x[\tau]$ to compute $c[\tau+1]$ also

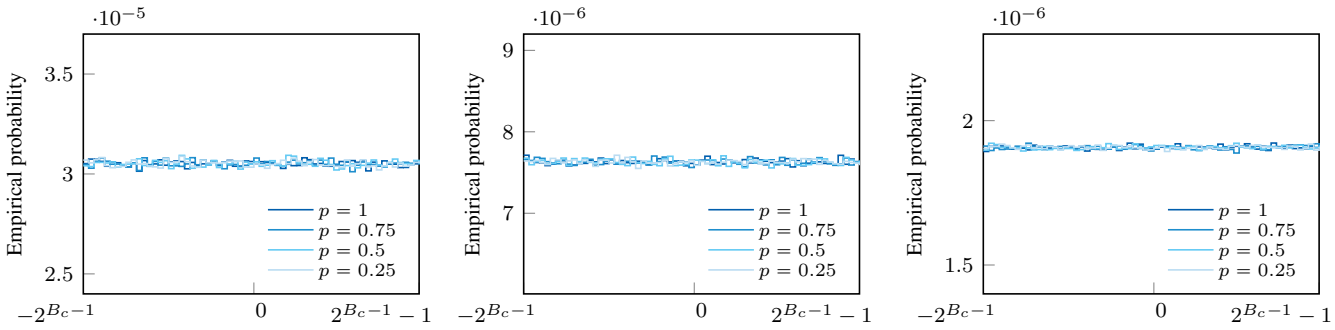

Fig. 3. Empirical probabilities of different values of the ciphertext in the three configurations (left-to-right $k = 3$, $k = 6$, and $k = 12$) and for different average energy of the plaintext.

Table 1. Tested configurations

n	k	m	B_x	B_c	KPA$\gg$
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}

the latter will be unknown preventing Mallory from reconstructing $l'[\tau]$ and thus $A[\tau + 1]$. Hence, for $t > \tau$, $c[t]$ and $l'[t]$ will be unknown, thus making impossible for Mallory to forge messages accepted by Bob.

6. NUMERICAL EVIDENCE

We adopt a common setting in which the k non-zero components of the signal vectors are selected at random among the n possible and filled with integers uniformly distributed in a range $\{-X, \dots, X - 1\}$ where $X \leqslant 2^{B_x - 1}$ can be chosen to set the average energy of the whole vector x.

We adopt $n = 128$, $B_{\text{LFSR}} = 32$ and test different settings that are summarized in Table 1. The value of m is found as the minimum for which the decoder produces an errorless reconstruction for not less than 4000 subsequent acquisitions. The last column of Table 1 contains a lower bound on the average number of indistinguishable solutions that Eve would find in a KPA to quantify the intrinsic robustness to such attack.

For each configuration, we consider signals with different average energy, expressed as a fraction p of the maximum possible average energy corresponding to $X = 2^{B_c - 1}$. From the 10^5 Montecarlo trials of each simulation we estimate the distribution of the entries of the ciphertext $z[t]$ on which all the security features substantially hinge.

We match such an empirical distribution against the uniform one by computing its Kolmogorov-Smirnov (KS) statistic [27, Chapter 15]. The results are reported in the fourth column of Table 2 in which smaller values mean a more uniform distributions. As a comparison, the value of the Kolmogorov-Smirnov statistic ($\overline{KS}$) of an equal number of samples generated in the same range by a truly uniform distribution is reported in the fifth column. The sixth column reports the maximum Γ of the estimated correlation coefficients between components of $z[t]$, while the seventh column reports the same value $\overline{\Gamma}$ for an equal number of samples generated in the same range by an algorithmic PRNG.

Table 2. Statistical analysis of the components of the ciphertext: Kolmogorov-Smirnov statistics for the distribution of its components matched against ideal uniform distribution and maximum of the correlation between pairs of its components. In both cases values of the same feature for an equal number of samples drawn in the same range by an algorithmic PRNG are given as a reference.

k	m	p	$KS \times 10^4$	$\overline{KS} \times 10^4$	$\Gamma \times 10^2$	$\overline{\Gamma} \times 10^2$
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

The fact that chaining allows to prevent any substantial leakage of information can also be intuitively assessed by looking at the empirical probability distributions in Figure 3 in which profiles do not change when the average energy of the plaintext changes.

7. CONCLUSION

By introducing chaining of plaintextes before CS-based encryption we are able to increase robustness with respect to attacks that may threaten the secure transmission of information between IoT sensor nodes and gateways.

8. REFERENCES

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb 2014.

[2] P. A. Catherwood, D. Steele, M. Little, S. Mccomb, and J. Mclaughlin, "A community-based iot personalized wireless healthcare solution trial," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 6, pp. 1–13, 2018.

[3] S. Feng, P. Setoodeh, and S. Haykin, "Smart home: Cognitive interactive people-centric internet of things," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 34–39, February 2017.

[4] Fabio Pareschi, Pierluigi Albertini, Giovanni Frattini, Mauro Mangia, Riccardo Rovatti, and Gianluca Setti, "Hardware-Algorithms Co-Design and Implementation of an Analog-to-Information Converter for Biosignals Based on Compressed Sensing," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 10, no. 1, pp. 149–162, Feb. 2016.

[5] David Bellasi, Riccardo Rovatti, Luca Benini, and Gianluca Setti, "A Low-Power Architecture for Punctured Compressed Sensing and Estimation in Wireless Sensor-Nodes," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 5, pp. 1296–1305, May 2015.

[6] 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.

[7] 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.

[8] 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.

[9] Robin Fay, "Introducing the counter mode of operation to compressed sensing based encryption," *Information Processing Letters*, vol. 116, no. 4, pp. 279–283, Apr. 2016.

[10] N. Y. Yu, "Indistinguishability of compressed encryption with circulant matrices for wireless security," *IEEE Signal Processing Letters*, vol. 24, no. 2, pp. 181–185, Feb 2017.

[11] Yushu Zhang, Jiantao Zhou, Fei Chen, Leo Yu Zhang, Kwok-Wo Wong, Xing He, and Di Xiao, "Embedding cryptographic features in compressive sensing," *Neurocomputing*, vol. 205, pp. 472 – 480, 2016.

[12] C. Chou, E. Chang, H. Li, and A. Wu, "Low-complexity privacy-preserving compressive analysis using subspace-based dictionary for ecg telemonitoring system," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 12, no. 4, pp. 801–811, Aug 2018.

[13] Mauro Mangia, Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, "Low-cost security of iot sensor nodes with rakeness-based compressed sensing: Statistical and known-plaintext attacks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 327 – 340, Sept. 2018.

[14] Emmanuel J Candès and Michael B Wakin, "An introduction to compressive sampling," *Signal Processing Magazine, IEEE*, vol. 25, no. 2, pp. 21–30, 2008.

[15] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Feb 2017, pp. 464–467.

[16] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov 2016, pp. 1–6.

[17] Ali Dorri, Salil S. Kanhere, and Raja Jurdak, "Towards an optimized blockchain for iot," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, New York, NY, USA, 2017, IoTDI '17, pp. 173–178, ACM.

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

[19] J. Haboba, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "A pragmatic look at some compressive sensing architectures with saturation and quantization," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 2, no. 3, pp. 443–459, Sept 2012.

[20] F. Pareschi, M. Mangia, D. Bortolotti, A. Bartolini, L. Benini, R. Rovatti, and G. Setti, "Energy analysis of decoders for rakeness-based compressed sensing of ecg signals," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 11, no. 6, pp. 1278–1289, Dec 2017.

[21] T.E. Hull and A.R. Dobell, "Random number generators," *SIAM Review*, vol. 4, no. 3, pp. 230–254, Jul. 1962.

[22] Riccardo Rovatti, Gianluca Mazzini, and Gianluca Setti, "Memory-m antipodal processes: spectral analysis and synthesis," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 56, no. 1, Jan. 2009.

[23] Mauro Mangia, Riccardo Rovatti, and Gianluca Setti, "Rakeness in the design of analog-to-information conversion of sparse and localized signals," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 59, no. 5, pp. 1001–1014, May 2012.

[24] R. Rovatti, G. Mazzini, and G. Setti, "Enhanced rake receivers for chaos-based ds-cdma," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 7, pp. 818–829, July 2001.

[25] G. Setti, R. Rovatti, and G. Mazzini, "Performance of chaos-based asynchronous ds-cdma with different pulse shapes," *IEEE Communications Letters*, vol. 8, no. 7, pp. 416–418, July 2004.

[26] Henryk Mink, *Nonnegative matrices*, John Wiley & Sons, 1987.

[27] Albert Nikolaevich Shiryayev, *Selected Works of A. N. Kolmogorov*, Mathematics and Its Application (Soviet Series). Springer, 1992.