Secure Wireless Communications Based on Compressive Sensing: A Survey

Yushu Zhang, *Member, IEEE*, Yong Xiang, *Senior Member, IEEE*, Leo Yu Zhang, *Member, IEEE*, Yue Rong, *Senior Member, IEEE*, and Song Guo, *Senior Member, IEEE*

***Abstract*—Compressive sensing (CS) has become a popular signal processing technique and has extensive applications in numerous fields such as wireless communications, image processing, magnetic resonance imaging, remote sensing imaging, and anology to information conversion, since it can realize simultaneous sampling and compression. In the information security field, secure CS has received much attention due to the fact that CS can be regarded as a cryptosystem to attain simultaneous sampling, compression and encryption when maintaining the secret measurement matrix. Considering that there are increasing works focusing on secure wireless communications based on CS in recent years, we produce a detailed review for the state-of-the-art in this paper. To be specific, the survey proceeds with two phases. The first phase reviews the security aspects of CS according to different types of random measurement matrices such as Gaussian matrix, circulant matrix, and other special random matrices, which establishes theoretical foundations for applications in secure wireless communications. The second phase reviews the applications of secure CS depending on communication scenarios such as wireless wiretap channel, wireless sensor network, Internet of Things, crowdsensing, smart grid, and wireless body area networks. Finally, some concluding remarks are given.**

***Index Terms*—Wireless communications, compressive sensing, secure compressive sensing, compressive sensing cryptosystem.**

I. Introduction

COMPRESSIVE sensing (CS) theory was proposed by Donoho *et al.* in 2004, which is a new signal sampling theory of being able to efficiently capture and recover a signal through settling underdetermined linear systems [1]–[3]. Sparsity and incoherence are two crucial conditions to attain this purpose. On the one hand, the sparsity condition requires the signal of interest to be sparse under some sparse basis or have the compressibility. On the other hand, the incoherence condition imposes a requirement for the sparse basis and the measurement matrix. In comparison with the traditional Shannon-Nyquist sampling theorem, CS exploits far fewer samples to achieve the same recovery accuracy of the signal. This is understandable, since, taking the sampling of electrocardiography signals for an example, an electrocardiography signal typically acquires 256 samples per second in the traditional sampling paradigm [4]. When expressed under appropriate basis or dictionary, such as wavelet or Gabor, most of the coefficients will be zero and only the nonzero ones carry information. These nonzero coefficients, rather than the original dimension 256, control the number of measurements to encode the signal and perform recovery. In this sense, the CS theory is built on a workaround to directly record the nonzero coefficients.

The CS technique has widespread applications in various fields since its inception [5]. In particular, in wireless communications, it is a promising technique for 5G [6], since the inherent characteristics of CS are more suitable for the sparse channel impulse response than the Shannon-Nyquist sampling theory. The CS was claimed in [6] to well address the key technical directions in 5G including increased spectral efficiency [7], [8] and larger transmission bandwidth [9]–[12]. So far, there have been a great number of CS-based applications in wireless communications such as data gathering [13]–[17], data collection [18], [19], data aggregation [20]–[22], data recovery [23]–[26], spectrum sensing [27]–[32], distribution networks [33]–[37], channel estimation [38]–[41], and other applications [42]–[49].

In a pioneer work of the fundamental CS theory [50], the security of CS was highlighted in the sense that measurements projected into random subspace can be viewed as a way of information protection. A weak form of encryption offered by a pseudorandom basis was mentioned in [51]. It has also been discussed that the encryption matrix is involved in a one-time pad [52]. However, for the first time, a formal investigation of CS as a cryptosystem was stated by Rachlin and Baron [53] who considered the measurement matrix as a key. After a signal is sampled by a Gaussian measurement matrix, the obtained measurements can provide the secrecy, since the adversary has no knowledge of the measurement matrix and cannot figure out the original signal. Though a certain level of secrecy can be provided, the Shannon's perfect secrecy [54] cannot be achievable. Moreover, it was

Manuscript received April 19, 2018; revised August 5, 2018 and September 22, 2018; accepted October 16, 2018. Date of publication October 31, 2018; date of current version May 31, 2019. This work was supported in part by the Australian Research Council under Grant LP170100458, in part by the National Natural Science Foundation of China under Grant 61702221 and Grant 61502399, and in part by the NVIDIA Corporation. *(Corresponding author: Yong Xiang.)*

Y. Zhang is with the School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China, and also with the School of Information Technology, Deakin University, Victoria, BC 3125, Australia (e-mail: yushuboshi@163.com).

Y. Xiang is with the School of Information Technology, Deakin University, Victoria, BC 3125, Australia (e-mail: yxiang@deakin.edu.au).

L. Y. Zhang is with the School of Information Technology, Deakin University, Geelong, VIC 3216, Australia (e-mail: leo.zhang@deakin.edu.au).

Y. Rong is with the Department of Electrical and Computer Engineering, Curtin University, Perth, WA 6845, Australia (e-mail: y.rong@curtin.edu.au).

S. Guo is with the Department of Computing, Hong Kong Polytechnic University, Hong Kong (e-mail: song.guo@polyu.edu.hk).

Digital Object Identifier 10.1109/COMST.2018.2878943

demonstrated that when the Gaussian measurement matrix is used, a weak secrecy notion called asymptotic perfect secrecy can be realized [55]. Based on this notion, the perfect secrecy can be attained by imposing more constraint on the signal to be sampled. Bianchi *et al.* [56], further proved that only the signal energy is exposed to the adversary who observes the measurements. This means that CS-based encryption satisfies the perfect secrecy if the sensed signal keeps a constant energy. In other words, normalizing the measurements before transmission can guarantee the perfect secrecy regardless of the statistical features.

However, Gaussian measurement matrix is a completely random matrix and therefore occupies a great amount of storage and computing resources. In consideration of this, circulant matrix was introduced in [57], which outperforms the Gaussian measurement matrix in terms of cost savings, since it adopts a fast Fourier transform implementation and has a similar reconstruction performance as the Gaussian matrix. When circulant measurement matrix is used, security analysis discloses that the adversary only reveals the information on the autocorrelation of the signal.

Besides using existing measurement matrices [53], [55]–[57] as the encryption keys, some special secret measurement matrices have been designed [58]–[61]. The perturbation-type measurement matrix aims at partially corrupting measurement matrix with low-cost [58], which is applied to the scenario that the same signal shows different levels of recovery quality for the receivers. With the partially corrupted measurement matrix, the quality of the recovered signal is inevitably reduced. Therefore, adjusting the number of corrupted entries can optionally control the signal quality for each receiver. This multiclass encryption possesses the asymptotic spherical secrecy. Generally speaking, the measurement matrix needs to be updated once to be against common attacks. For the purpose of using a fixed measurement matrix repeatedly, a bi-level protected CS scheme was suggested in [59], whose basic idea is to transfer the sparsifying basis from the sensing matrix to the measurement matrix and then set it a key. The transfer was verified in the sense that the reconstruction performance will not be affected. Moreover, double protection using two matrices can resist plaintext attacks.

Fang *et al.* [62] proposed parallel CS to address the problem of data size expansion for the measurement matrix when sampling a multi-dimensional signal and further exploited the zig-zag permutation operation to promote the reconstruction performance of sampling two-dimensional discrete cosine transformation signal. Embedding cryptographic features in parallel CS was discussed in [60], which demonstrated that random permutation based encryption can make the restricted isometry constant of parallel CS relaxed efficiently at a high probability, i.e., enhance the quality of the reconstructed signal. It has the asymptotic spherical secrecy as the multiclass encryption scheme [58]. Djeujo and Ruland ensured the secrecy by embedding some cryptographically secure matrix transformations in structured CS [61]. These transformations are invertible matrices and do not compromise the reconstruction performance.

For CS applications in wireless communications, a great number of security and privacy issues have been studied. Since secure communication was formally proposed by Shannon from the view point of information theory [54], many research works have been emerging to guarantee secure message sharing between communication nodes based on cryptographic tools at the application layer [63] and ensure secure communications over wireless channels [64]. In particular, the wiretap channel proposed by Wyner [65] is one of the classic channels and has attracted widespread attention [66]–[68]. Secure communication over wiretap channel is always a research focus in wireless communications. For example, a widely used system model involves a transmitter and two receivers including a legitimate receiver and an eavesdropper. The transmitter connects the legitimate receiver through the main channel while connecting the eavesdropper through the wiretap channel. The investigations on the wiretap channel focus mainly on how much information can be leaked to the eavesdropper and how the transmission of perfect secrecy can be accomplished when the channel is eavesdropped. Note that, secure communication over wiretap channel differs from traditional sampling, compression and encryption, since it occurs after traditional sampling, compression and encryption. The infrastructure of CS was exploited for constructing a secure communication channel. For example, based on channel asymmetry, a message is transformed into a sparse sequence, which cannot be decoded by the eavesdropper with overwhelming probability while the legitimate receiver can decode it with high probability [69].

There are some important theoretical foundations of secure wireless communications based on CS. Reeves *et al.* [70] proposed a multiplicative Gaussian channel based on CS and calculated the secrecy capacity bounds including lower bound and upper bound, where the introduced security hardly affects the capacity based on the condition that the attacker's channel is strictly worse than the legal user's. The distributed CS was used for the design of physical layer secrecy solution resulting from the fact that it occupies less amount of channel uses and consumes less power [71]. The reconstruction framework of CS was utilized in the system of multiple-input multiple-output (MIMO) precoding and postcoding to reconstruct the transmitted signals [72], which can optimize the signal-to-noise ratio (SNR) when full channel state information is available and can compensate the loss of SNR when full channel state information is unavailable. Yu [73] considered the circulant matrices for wireless security and demonstrated the indistinguishability depending on the measure of relative entropy.

Moreover, there exist many applications of secure wireless communication based on CS in terms of different wireless communication scenarios such as multicarrier system [74]–[76], cooperative networks [77], wireless sensor network (WSN) [78]–[87], Internet of things (IoT) [88]–[92], crowdsensing [93]–[95], smart grid [96]–[98], and wireless body area networks [99]–[101]. In multicarrier systems, Choi proposed a CS based encryption scheme by selectively transmitting artificial noise with a sparse signal in the frequency domain [74]. Chang *et al.* [77] investigated the secrecy capacity of a cooperative amplify-and-forward wireless network

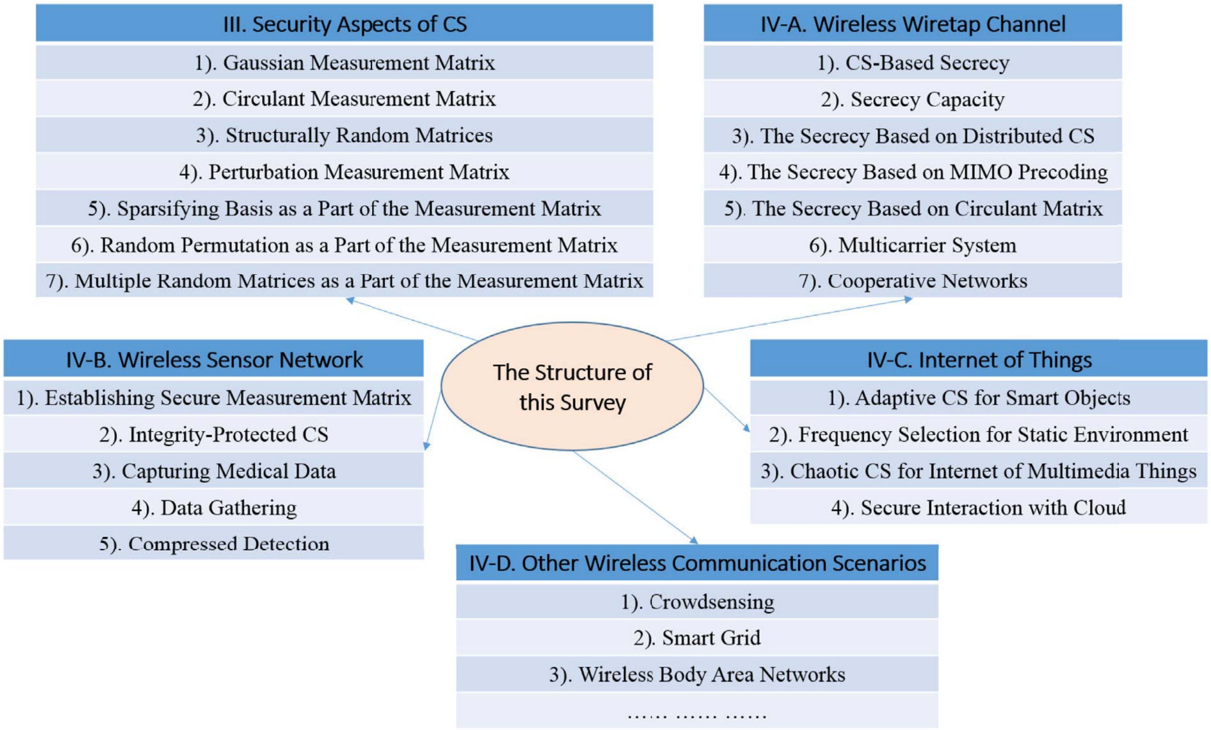

III. Security Aspects of CS
1). Gaussian Measurement Matrix
2). Circulant Measurement Matrix
3). Structurally Random Matrices
4). Perturbation Measurement Matrix
5). Sparsifying Basis as a Part of the Measurement Matrix
6). Random Permutation as a Part of the Measurement Matrix
7). Multiple Random Matrices as a Part of the Measurement Matrix
IV-A. Wireless Wiretap Channel
1). CS-Based Secrecy
2). Secrecy Capacity
3). The Secrecy Based on Distributed CS
4). The Secrecy Based on MIMO Precoding
5). The Secrecy Based on Circulant Matrix
6). Multicarrier System
7). Cooperative Networks
IV-B. Wireless Sensor Network
1). Establishing Secure Measurement Matrix
2). Integrity-Protected CS
3). Capturing Medical Data
4). Data Gathering
5). Compressed Detection
The Structure of this Survey
IV-C. Internet of Things
1). Adaptive CS for Smart Objects
2). Frequency Selection for Static Environment
3). Chaotic CS for Internet of Multimedia Things
4). Secure Interaction with Cloud
IV-D. Other Wireless Communication Scenarios
1). Crowdsensing
2). Smart Grid
3). Wireless Body Area Networks
…… …… ……

Fig. 1. The intuitional structure of this survey.

using a CS and energy harvesting protocol designed for cooperative networks. Dautov and Tsouri [78] exploited the sensing matrix for an encryption framework based on wireless physical layer security and linear feedback shift register used in WSN. In IoT applications, Fragkiadakis *et al.* [88] presented an adaptive CS framework for energy-efficient smart objects. Built upon CS, Wu *et al.* [93] sampled and compressed received signal strength values along each road segment to preserve the privacy in crowdsensing network. In smart grid, Gao *et al.* [96] guaranteed secure data transmission and enhanced transmission efficiency based on CS. In wireless body area networks, Peng *et al.* [99] designed a low-cost and confidentiality-assured data transmission scheme with the help of chaotic CS.

In this survey, we make a systematic investigation for applications of CS in secure wireless communications. In order to better discuss the applications of CS in secure wireless communications, we first review security aspects of CS based on the type of measurement matrix such as Gaussian measurement matrix, circulant measurement matrix, etc, which will be potential for applications to secure wireless communication scenarios. According to the security aspects of CS, we then review different forms of wireless communication scenarios including wireless wiretap channel, WSN, IoT, crowdsensing, smart grid, and wireless body area networks. Table I gives a overall perception for the readers and the corresponding details are shown later. A graphical presentation of the structure of this survey is shown in Fig. 1.

There are some existing relevant survey and tutorial papers involving CS. A comprehensive overview in terms of CS theories and applications was shown in [102]. Because of the extensive applications of CS, some survey papers focusing on application-specific scenarios have also been presented. For example, the survey papers [103] and [104] overviewed the applications of CS in cognitive radio communications. The survey papers [31], [105], and [106] contain the review of CS applications in terms of spectrum sensing for cognitive radio networks, machine learning for WSN, and robust carrier tracking techniques, respectively. Nevertheless, these works did not involve the security issues of CS. Meanwhile, a tutorial paper [107] discussed image and video encoding modes and wireless transmission based on CS, which apparently differs from the present survey. The survey paper [108] involves some privacy protection and security problems of CS, but it only simply reviewed several kinds of CS encryption schemes and did not consider the secure wireless communication problems based on CS. The most similar paper to the present survey is [109], which reviews the security aspects of CS in information security field. However, it focuses mainly on CS-based image security rather than wireless communications. Table II gives a conclusive comparison for better comprehension.

This survey proceeds as follows. In Section II, the basic theory of CS is overviewed. Section III reviews the security aspects of CS. Section IV reviews the applications of CS in secure wireless communication scenarios including wireless wiretap channel, WSN, IoT, crowdsensing, smart grid, and wireless body area networks. Some concluding remarks and future research in this area are shown in the last section.

II. Compressive Sensing Basics

A signal $\mathbf{x} \in \mathbb{R}^N$ is called S-sparse if there exists a basis $\mathbf{B} \in \mathbb{R}^{N \times N}$ satisfying

$$\mathbf{x} = \mathbf{B}\mathbf{s}, \tag{1}$$

TABLE I
OVERALL FRAMEWORK

Security Aspects of CS		Gaussian Measurement Matrix
		Circulant Measurement Matrix
		Structurally Random Matrices
		Perturbation Measurement Matrix
		Sparsifying Basis as a Part of the Measurement Matrix
		Random Permutation as a Part of the Measurement Matrix
		Multiple Random Matrices as a Part of the Measurement Matrix
Application Scenarios	Wireless Wiretap Channel	CS-Based Secrecy
		Secrecy Capacity
		The Secrecy Based on Distributed CS
		The Secrecy Based on MIMO Precoding
		The Secrecy Based on Circulant Matrix
		Multicarrier System
		Cooperative Networks
	Wireless Sensor Network	Establishing Secure Measurement Matrix
		Integrity-Protected CS
		Capturing Medical Data
		Data Gathering
		Compressed Detection
	Internet of Things	Adaptive CS for Smart Objects
		Frequency Selection for Static Environment
		Chaotic CS for Internet of Multimedia Things
		Secure Interaction with Cloud
	Crowdsensing	Crowdsensing
	Smart Grid	Smart Grid
	Wireless Body Area Networks	Wireless Body Area Networks

TABLE II
COMPARISONS OF RELEVANT SURVEY & TUTORIAL PAPERS INVOLVING CS

Paper Type	Scope and Contributions	Difference with This Survey
Review Paper [102]	Theories and applications of CS	Not involve security aspects of CS
Survey Paper [103]	Applications of CS in cognitive radio communications	Not involve security aspects of CS
Survey Paper [104]	Applications of CS in cognitive radio communications	Not involve security aspects of CS
Survey Paper [31]	Applications of CS in cognitive radio networks	Not involve security aspects of CS
Survey Paper [105]	Applications of CS in machine learning for WSN	Not involve security aspects of CS
Survey Paper [106]	Applications of CS in robust carrier tracking techniques	Not involve security aspects of CS
Tutorial Paper [107]	CS-based multimedia encoding and wireless transmission	Not consider secure wireless communication problems based on CS
Survey Paper [108]	Several kinds of CS encryption schemes	Not consider secure wireless communication problems based on CS
Review Paper [109]	Image security based on CS	Not consider secure wireless communication problems based on CS

where $\mathbf{s}$ is an N-dimensional vector with at most S nonzero coefficients. It is called S-compressible if the S significant coefficients are much larger than zero and the $N{-}S$ insignificant coefficients approach to zero. The sparsity (compressibility) of the signal ensures the exact (approximate) recovery of $\mathbf{s}$ (and $\mathbf{x}$ since $\mathbf{x} = \mathbf{Bs}$ given $\mathbf{B}$ and $\mathbf{s}$) from linear projections

$$\mathbf{y} = \mathbf{Ax}, \tag{2}$$

where $\mathbf{A} \in \mathbb{R}^{M \times N}$ $(M < N)$ denotes the measurement matrix. The recovery can be done through settling an l_0 optimization problem expressed as

$$\min \|\mathbf{s}\|_0 \ s.t. \ \mathbf{y} = \mathbf{Hs}, \tag{3}$$

where $\mathbf{H} = \mathbf{AB}$ denotes the sensing matrix [3], [50]. However, solving this optimization problem requires an exhaustive search over all subsets of columns of $\mathbf{H}$, which is NP-hard, as indicated in [3]. It can be further relaxed into the convex optimization form as follows

$$\min \|\mathbf{s}\|_1 \ s.t. \ \mathbf{y} = \mathbf{Hs}. \tag{4}$$

The solution of this convex problem can be identical to that of the l_0 form with overwhelming probability when $\mathbf{H}$ follows the Restricted Isometry Property (RIP) [50]. The sensing matrix $\mathbf{H}$ possesses the RIP of order S when the following inequality holds [1], [2]

$$(1-\delta)\|\mathbf{v}\|_2^2 \leq \|\mathbf{Hv}\|_2^2 \leq (1+\delta)\|\mathbf{v}\|_2^2, \tag{5}$$

where $\mathbf{v}$ is an arbitrary sparse signal that has S nonzero entries at most and $\delta \in (0, 1)$. One can define the smallest value of δ satisfying the above inequality as the restricted isometry constant δ_S. In addition, another criterion, the mutual coherence, is also used to evaluate the performance of the sensing matrix. It is defined as [110]

$$\mu(\mathbf{H}) = \max_{1<i\neq j<N} \frac{\left|\mathbf{h}_i^T \mathbf{h}_j\right|}{\|\mathbf{h}_i\|_2 \|\mathbf{h}_j\|_2}, \tag{6}$$

where $\mathbf{h}_i$ represents the ith column of $\mathbf{H}$. It was demonstrated that there exists at most an S-sparse signal $\mathbf{s}$ satisfying $\mathbf{y} = \mathbf{Hs}$ provided that $\mu(\mathbf{H}) < 1/(2S-1)$ for any $\mathbf{y}$ [110]. So far, there have been a number of algorithms used for the reconstruction such as orthogonal matching pursuit [111], gradient projection [112], and nonconvex minimization [113].

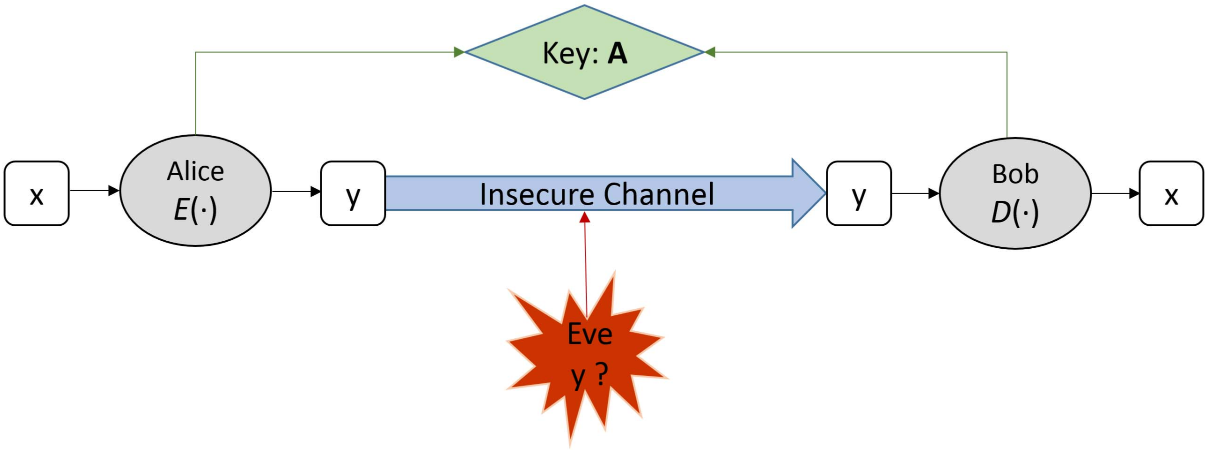


Fig. 2. Compressive sensing as a cryptosystem.

TABLE III
COMPARISONS OF CSC AND GENERAL SYMMETRIC-KEY CIPHERS

Type	CSC	General Symmetric-Key Ciphers
Relationship with the Nyquist Sampling	Require fewer samples for the same recovery accuracy	Not possess the sampling capacity
Relationship with the quantization	Require quantizing the result	Not require quantizing the result
Relationship with the compression	Possess the compression capacity	Not possess the compression capacity
Relationship with the universal encryption	Cannot be applied to universal encryption	Can be applied to universal encryption

III. SECURITY ASPECTS OF COMPRESSIVE SENSING

In this section, we firstly describe the main idea of compressive sensing as a cryptosystem, which is marked as CSC for short hereinafter. Then, we review the security aspects of CS from two sides, i.e., various random measurement matrices and some security analyses.

A. The Main Idea of CSC

Compressive sensing can be regarded as a symmetric-key cryptosystem when the measurement matrix acts a key, as shown in Fig. 2, in which $\mathsf{E}(\cdot)$ and $\mathsf{D}(\cdot)$ represent the encryption and decryption functions, respectively. The cryptosystem contains five objectives, i.e., input signal $\mathbf{x}$ as plaintext, measurement matrix $\mathbf{A}$ as key, sampled result $\mathbf{y}$ as ciphertext, measurement process in (2) as encryption function $\mathsf{E}(\cdot)$, and reconstruction process in (4) as decryption function $\mathsf{D}(\cdot)$. Let X and Y be the sets of plaintexts and ciphertexts, respectively, and K be the key set. Alice encrypts the plaintext $\mathbf{x} \in X$ with the encryption function $\mathsf{E}_K(\cdot) : X \to Y$ and the measurement matrix $\mathbf{A} \in K$ shared between Alice and Bob, and the corresponding ciphertext $\mathbf{y} \in Y$ is sent to Bob over insecure channel in which an evil attacker called Eve tries to intercept message $\mathbf{y}$. Upon receiving $\mathbf{y}$, Bob decrypts it with the decryption function $\mathsf{D}_K(\cdot) : Y \to X$ and $\mathbf{A}$ to obtain the original $\mathbf{x}$. Note that, the $\mathbf{y}$ that Bob receives may have a tiny change due to the channel noise. Moreover, the recovered $\mathbf{x}$ may be a little different from the exact $\mathbf{x}$, since it is often an approximate version after being recovered by some reconstruction algorithms. Therefore, we have $\mathsf{D}_{\mathbf{A}}(\mathbf{y}) = \mathsf{D}_{\mathbf{A}}(\mathsf{E}(\mathbf{x})) = \mathbf{x}$ while neglecting the subtle influence of the channel noise and the reconstruction operation.

Note that, in comparison with the general symmetric-key cipher that is not based on CS, the CSC has the extra advantage of compression capacity. The compression capacity also brings a new issue that the decrypted result is often an approximated version of the original plaintext to facilitate the computation, although the original plaintext can be exactly obtained without loss of information in theory. Another difference between them is that the CSC is not suitable for multiple rounds of encryption for security enhancement, since, after one-time sampling, the measurements tend to be random and would not possess the sparsity. The design of CSC focuses mainly on the security guarantee while taking CS for signal sampling. As a result, the CSC cannot be applied to universal encryption. In addition, the encryption result for CSC can be further quantized while the general ciphers cannot perform quantization, since the robustness of CS can still guarantee a feasible reconstruction for the signal. Table III summarizes their comparison results in terms of the relationships with the Nyquist sampling, the quantization, the compression capacity, and the universal encryption.

B. Various Random Measurement Matrices

As mentioned above, the reason that CS can be regarded as a cryptosystem depends mainly on treating the measurement matrix as a key. Thus, we want to investigate which measurement matrices actually play the keys of the CSC, what properties these CSC systems possess, and what level of secrecy they have. To play a role of key, the measurement matrix should have the property of "randomness"; otherwise, it cannot provide the secrecy. Fox example, the deterministic measurement matrices apparently cannot offer any kind of secrecy. Correspondingly, we turn to random measurement matrices including Gaussian matrix, circulant matrix, and other special random matrices, which can be potentially applied in secure wireless communications.

1) Gaussian Measurement Matrix: Gaussian matrix consisting of independent and identically distributed (i.i.d.) Gaussian random variables was considered as a key in CSC for the first time [50] and we denote it as Gaussian-CSC. Which level of secrecy the Gaussian-CSC can achieve will be elaborated in the followings. Shannon, the founder of information theory, pioneered the prefect secrecy from a statistical sense when considering an eavesdropper with unbounded computation [54].

Definition 1: Perfect Secrecy. A cryptosystem is said to have a perfect secrecy if for any plaintext x and corresponding ciphertext y,

$$p(x|y) = p(x). \tag{7}$$

The above formula means that a plaintext's posterior probability conditioned on the ciphertext equals its priori probability. Alternatively, it is interpreted as $I(x;y) = 0$ from the information theory perspective, in which $I(x;y)$ represents the mutual information of plaintext and ciphertext [114]. Moreover, the above formula can be also equivalently interpreted as $p(y|x) = p(y)$ by using Bayes' theorem.

The Gaussian-CSC in terms of perfect secrecy was first investigated in [53], where the adversary, Eve, is assumed to lunch a ciphertext-only attack (COA) through leveraging y, the sparsity of x, and K to recover x. The key is defaulted to one-time, meaning that each $\mathbf{A}$ is used only once.

Theorem 1: Gaussian-CSC is not perfectly secure.

It was proved in [53, Lemma 1]. In fact, due to the RIP property of Gaussian measurement matrix, the energy of ciphertext reveals energy information of the plaintext, thus violating the definition of perfect secrecy. It was demonstrated in [56] that after sampling using an i.i.d. Gaussian matrix consisting of Gaussian variables with zero mean as a key, the generated random linear measurements intercepted by Eve will not reveal anything about the plaintext other than its energy.

Theorem 2: Gaussian-CSC yields

$$p(\mathbf{y}|\mathbf{x}) = p(\mathbf{y}|\varepsilon_{\mathbf{x}}). \tag{8}$$

The above equation is equivalent to $I(\mathbf{x};\mathbf{y}) = I(\varepsilon_{\mathbf{x}};\mathbf{y})$ [56], where $\varepsilon_{\mathbf{x}}$ is used for characterizing the energy of the plaintext, i.e., $\varepsilon_{\mathbf{x}} = \|\mathbf{x}\|_2^2$. This result says that Eve only infers the knowledge of $\varepsilon_{\mathbf{x}}$, which holds regardless of the sparse degree of x. According to this theorem, the prefect secrecy of Gaussian-CSC is achievable under some assumptions.

Theorem 3: Gaussian-CSC is said to be perfectly secure while $\varepsilon_{\mathbf{x}}$ keeps a constant.

$\varepsilon_{\mathbf{x}}$ keeping a constant indicates the energy of the signal maintains unchanged, thus Eve cannot dig out any information from the ciphertext. In general, the assumption of the constant energy signal is far-fetched and then we can exert some processing on the ciphertext to easily deduce another prefect secrecy.

Theorem 4: Gaussian-CSC is said to be perfectly secure when transmitting the normalized ciphertext

$$\mathbf{y}_{norm} = \mathbf{y}/\varepsilon_{\mathbf{y}}, \tag{9}$$

where $\varepsilon_{\mathbf{y}} = \|\mathbf{y}\|_2^2$ represents the energy of the ciphertext.

Apparently, after the normalization, the energy of the plaintext is hided such that Eve is not able to know $\varepsilon_{\mathbf{x}}$ any more. Now that $\mathbf{y}$ results in the energy of $\mathbf{x}$ if not normalized, it is required to be aware of how much information is exactly leaked through observing $\mathbf{y}$. Bianchi *et al.* quantified this kind of information leakage using the mean square error and gave some useful bounds and estimators for the generic signals, and the relevant details are referred to [56].

2) Circulant Measurement Matrix: Circulant matrix is also capable of offering the randomness, which has lower complexity in contrast to Gaussian matrix when generated, transmitted and used for measuring the signal [115]. It consists of a sequence of i.i.d. Gaussian or sub-Gaussian variables expressed as

$$\mathbf{A} = \begin{bmatrix} a_1 & a_2 & \cdots & a_N \\ a_N & a_1 & \cdots & a_{N-1} \\ a_{N-1} & a_N & \cdots & a_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N-M+2} & a_{N-M+3} & \cdots & a_{N-M+1} \end{bmatrix}_{M\times N}, \tag{10}$$

where the N-dimensional row vector $\mathbf{a} = [a_i]$, $i = 1, 2, \ldots, N$, spanning the whole matrix $\mathbf{A}$. It was demonstrated that this kind of matrix, when acting as a measurement matrix used for measuring and reconstruction, has similar performance as the full Gaussian matrix [115]. Thus, it can act as an alternative for reducing the complexity. Interestingly, it can be quickly realized using a fast Fourier transform by

$$\mathbf{A} = \mathbf{\Delta}\mathbf{F}^H\mathbf{\Lambda}\mathbf{F}, \tag{11}$$

in which $\mathbf{F}$ stands for the unitary discrete Fourier transform (DFT) matrix, $\mathbf{F}^H$ is the Hermitian transpose of $\mathbf{F}$, $\mathbf{\Lambda}$ represents a diagonal matrix in which diagonal entries are the values generated by the DFT of $\mathbf{a}$, and $\mathbf{\Delta}$ is a subsampling operator of randomly extracting M entries from N ones.

The secrecy of circulant matrix as a key was inspected in [57], which introduces a generic permutation matrix $\mathbf{P}$ that has only one "1" in both each row and each column before measuring. In other words, the measurement matrix is changed into

$$\mathbf{A} = \mathbf{\Delta}\mathbf{F}^H\mathbf{\Lambda}\mathbf{F}\mathbf{P}. \tag{12}$$

The corresponding cryptosystem is denoted as Circulant-CSC. Let $\mathbf{C}^{\mathbf{v}}$ stand for the circular autocorrelation matrix of vector $\mathbf{v}$, i.e.,

$$\left[C_{i,j}^{v}\right] = \sum\nolimits_{l=1}^{N} v_l v_{(l+i-j) \bmod N}, \; i, j = 1, 2, \ldots, N, \tag{13}$$

where mod is the modulo operator. Maintaining $\mathbf{\Delta}$ and $\mathbf{P}$ public, one has the following result.

Theorem 5: Circulant-CSC only leaks $\mathbf{C}^{\mathbf{Px}}$.

Here, *leak* refers to the fact that the eavesdropper could only learn $\mathbf{C}^{\mathbf{Px}}$ in theory when observing the ciphertext. In fact, it was proved that Circulant-CSC satisfies $p(\mathbf{y}|\mathbf{x}) = p(\mathbf{y}|\mathbf{\Delta}\mathbf{C}^{\mathbf{Px}}\mathbf{\Delta}^T)$ [57], meaning that Eve only reveals some entries of the circular autocorrelation matrix of vector $\mathbf{Px}$. Which entries are revealed depends on the subsampling operator $\mathbf{\Delta}$. The detailed analysis of the autocorrelation of the plaintext can be found in [57].

3) Structurally Random Matrices: A kind of fast and efficient structurally random matrices was designed for the measurement matrix [116], which is generated by multiplying three matrices as follows:

$$\mathbf{A} = \sqrt{N/M}\mathbf{\Delta}\mathbf{F}'\mathbf{R}, \tag{14}$$

where $\mathbf{R} \in \mathbb{R}^{N\times N}$ can be a diagonal matrix in which diagonal entries can be i.i.d. Bernoulli variables. $\mathbf{R}$ can also be a permutation matrix. It focuses on scrambling the signal's sample locations globally or flipping the signals sample signs locally, respectively. $\mathbf{F}' \in \mathbb{R}^{N\times N}$ is an orthonormal matrix such as Walsh-Hadamard Transform (WHT) and discrete cosine transform (DCT). $\mathbf{\Delta} \in \mathbb{R}^{M\times N}$ is operator used for subsampling. The purpose of $\sqrt{N/M}$ is to balance the energy of the measurement vector and that of the input signal by normalizing the transform. In this measurement matrix, $\mathbf{\Delta}$ and $\mathbf{R}$ are random matrices, which can be set as the secret keys. From the viewpoint of the reconstruction performance, it has theoretical sensing performance as that of Gaussian measurement matrix but lower complexity due to fast computation transform, supporting block-based processing, and friendly hardware implementation. Thus, $\mathbf{\Delta}$ and $\mathbf{R}$ maintaining as the keys can make this kind of structurally random matrices suitable for privacy-preserving, large-scale, and real-time signal acquisition applications. Apparently, it cannot attain the perfect secrecy but more stronger secrecy if normalizing the ciphertext.

4) Perturbation Measurement Matrix: Perturbation-type measurement matrix was presented in [58], which is used for building scalable encryption methods. Assume that two receivers have the same ciphertext $\mathbf{y}$ but different decoding matrices, then they yield different quality of plaintexts after decryption. In order to build different decoding matrices, the initial measurement matrix $\mathbf{A}^{(0)}$ is a Bernoulli random matrix and then perturbed by flipping the sign of some entries in a random pattern as the following formula:

$$\mathbf{A}^{(1)}_{i,j} = \begin{cases} \mathbf{A}^{(0)}_{i,j}, & (i,j) \notin \Gamma^{(0)} \\ -\mathbf{A}^{(0)}_{i,j}, & (i,j) \in \Gamma^{(0)}, \end{cases} \tag{15}$$

where $\Gamma^{(0)}$ denotes a subset consisting of index pairs of the perturbed entries. Let $|\Gamma^{(0)}|$ represent the number of entries in $\Gamma^{(0)}$, then the relation between $\mathbf{A}^{(0)}$ and $\mathbf{A}^{(1)}$ is determined by a $|\Gamma^{(0)}|$-sparse random perturbation matrix $\mathbf{A}^{(\Delta)}$

$$\mathbf{A}^{(1)} = \mathbf{A}^{(0)} + \mathbf{A}^{(\Delta)}, \tag{16}$$

where

$$\mathbf{A}^{(\Delta)}_{(i,j)} = \begin{cases} 0, & (i,j) \notin \Gamma^{(0)} \\ -2\mathbf{A}^{(0)}_{i,j}, & (i,j) \in \Gamma^{(0)}. \end{cases} \tag{17}$$

When the sampling mode is $\mathbf{y} = \mathbf{A}^{(1)}\mathbf{x} = \mathbf{A}^{(0)}\mathbf{x} + \mathbf{A}^{(\Delta)}\mathbf{x}$, the receiver with the knowledge of $\mathbf{A}^{(1)}$ could exactly reconstruct the sparse solution while the receiver only knowing $\mathbf{A}^{(0)}$ is only able to reconstruct a noisy version of x due to the term $\mathbf{A}^{(\Delta)}\mathbf{x}$. Based on this kind of two-class perturbation mode, Cambareri *et al.* [58] also suggested an improved version for multiple receivers and the corresponding performance bounds about the recovery quality are theoretically analysed. Although not perfectly secure, it can attain a notion called asymptotic spherical secrecy at almost zero cost.

Definition 2: Asymptotic spherical secrecy [58]. Assume that X and Y are random processes, which correspond to plaintexts and ciphertexts, respectively. The plaintexts have bounded energy $\bar{\varepsilon}_{\mathbf{x}} = \lim\limits_{N\to\infty} \frac{1}{N}\sum_{j=1}^{N} x_j^2$. A encryption scheme satisfies asymptotic spherical secrecy provided that for any plaintext $\mathbf{x}$, ciphertext $\mathbf{y}$, the following formula holds

$$f_{Y|X}(\mathbf{y}|\mathbf{x}) \underset{D}{\to} f_{Y|\bar{\varepsilon}_{\mathbf{x}}}(\mathbf{y}), \tag{18}$$

in which $\underset{D}{\to}$ denotes the distribution convergence.

Theorem 6: The CSC with perturbation measurement matrix has the asymptotic spherical secrecy [58].

It indicates that only the energy of plaintext will be leaked, which, in fact, is similar to the above Theorems 2-4. They characterize the almost same meaning.

Generally speaking, known-plaintext attack possesses more threat than ciphertext-only attack, since Eve can leverage some pairs of plaintext and ciphertext rather than solely the ciphertext. Cambareri *et al.* [117] performed a quantitative analysis for the CSC of perturbation measurement matrix as a key against a special form of known-plaintext attack, in which the problem of attacking the key is transformed into a subset-sum problem [118] and how much Eve can reveal the measurement is quantitatively investigated.

Definition 3: Let $\mathbf{u}$ be a positive integer vector of size N and v be a positive integer. The subset-sum problem is to assign a binary vector $\mathbf{b}$ of size N such that

$$v = \sum\nolimits_{l=1}^{N} b_l u_l, \tag{19}$$

where $\mathbf{b}$ is referred to as the solution.

Consider the CSC of perturbation measurement matrix, the sampling method is expressed as $\mathbf{y} = \mathbf{A}^{(1)}\mathbf{x}$, then Eve attempts to reveal $\mathbf{A}^{(1)}_j$ with a set of antipodal symbols $\hat{\mathbf{A}}^{(1)}_j$ such that $\mathbf{y} = \hat{\mathbf{A}}^{(1)}_j\mathbf{x}$.

Theorem 7: The known-plaintext attack to $\mathbf{A}^{(1)}$ is equivalent to the subset-sum problem, where $u_l = |x_l|$, $b_l = \frac{1}{2}(\mathrm{sign}(x_l)\hat{\mathbf{A}}^{(1)}_{j,l} + 1)$, and $v = \frac{1}{2}(y_j + \sum_{l=1}^{N} |x_l|)$.

Based on the above theorem, a solution $\bar{\mathbf{b}}$ in the subset-sum problem corresponds to the row $\mathbf{A}^{(1)}_j$ while the remaining candidate solutions correspond to the rows $\hat{\mathbf{A}}^{(1)}_j \neq \mathbf{A}^{(1)}_j$. Therefore, when Eve performs an attack to $\mathbf{A}^{(1)}$, the expected number of finding out rows in $\mathbf{A}^{(1)}$ can be estimated by using the expected number of solutions as follows.

Theorem 8: The expected number of candidate solutions for large N, asymptotically equals $\frac{2^N}{L}\sqrt{\frac{3}{\pi N}}$, in which all the coefficients u_l from $\{1, 2, \ldots, L\}$ are i.i.d. and uniform, and

TABLE IV
THE LEVEL OF SECRECY FOR DIFFERENT TYPES OF CSCS FROM VIEW OF KEY

The Type of CSC	The Level of Secrecy
Gaussian measurement matrix [50], [53], [56]	Have perfect secrecy under the condition of normalizing the ciphertext
Circulant measurement matrix [57]	Leak some information of the autocorrelation of the plaintext
Structurally random matrices [116]	Not having perfect secrecy
Perturbation measurement matrix [58]	Have asymptotic spherical secrecy
Sparsifying basis as a part of the measurement matrix [59]	Not have perfect secrecy but being against plaintext attacks
Random permutation as a part of the measurement matrix [60]	Have asymptotic spherical secrecy
Multiple random matrices as a part of the measurement matrix [61]	Not have perfect secrecy but being against plaintext attacks

the true solution $\bar{\mathbf{b}}$ yields equiprobable and independent binary values.

In addition, for the recovery performance of this kind of CSC, a detailed analysis can be referred to [119].

5) Sparsifying Basis as a Part of the Measurement Matrix: In general, the measurement matrix needs to be updated once to ensure the security of CSC, since the attacker can launch a plaintext attack to reveal the measurement matrix by possibly contrasting several plaintext and ciphertext pairs. However, a key reuse circumstance of utilizing a fixed measurement matrix with multiple times was devised in [59]. Except the secret protection of the measurement matrix, a secret sparsifying basis $\mathbf{B}$ can be added in the signal sampling, thus it becomes a bi-level protection sampling model:

$$\mathbf{y} = \mathbf{A}'\mathbf{x} = \mathbf{A}\mathbf{B}^{-1}\mathbf{x}, \tag{20}$$

in which $\mathbf{A}' = \mathbf{A}\mathbf{B}^{-1}$ is the new measurement matrix. However, with respect to the RIP property of this new measurement matrix, it may not stand up any more, thus possibly leading to an incorrect reconstruction. Interestingly, Candes and Plan [120] demonstrated an efficient reconstruction in virtue of RIPless theory. It is mainly because given a secret basis $\mathbf{B}$, the new sensing matrix used for reconstruction becomes $\mathbf{H}' = \mathbf{A}'\mathbf{B} = \mathbf{A}\mathbf{B}^{-1}\mathbf{B} = \mathbf{A}$, which is exactly the original measurement matrix. That is to say, the sensing matrix still follows the RIP theory. For an attacker, only revealing $\mathbf{A}'$ through launching plaintext attacks is far from enough, since $\mathbf{B}$ is still unknown and then $\mathbf{A}$ is also unknown. In fact, the difficulty of attacking lies in how to decompose $\mathbf{A}'$ into $\mathbf{A}$ and $\mathbf{B}$. It is verified that this bi-level protection sampling model supports reusing the measurement matrix and can thwart plaintext attacks.

6) Random Permutation as a Part of the Measurement Matrix: The permutation technique has been found to be able to relax the RIP requirement in parallel CS theory [62]. In other words, prior to sampling, the 2D sparse signal is possibly permuted to make each sub-signal have almost equal number of nonzero entries, therefore the recovery performance can be improved. Fang *et al.* suggested that zig-zag permutation can makes the RIP efficiently relaxed at a high probability in parallel CS [62]. Different from the general permutation technique, random permutation is a common technique widely used in cryptography and is considered to be embedded in CSC in [60], where random permutation is demonstrated to be an efficient RIP relaxation technique. Let $P(\cdot)$ denote a random permutation matrix or a random permutation operation, then the sampling method is represented as

$$\mathbf{y} = \mathbf{A} \cdot P(\mathbf{x}). \tag{21}$$

The new measurement matrix can be regarded as $\mathbf{A}' = \mathbf{A} \cdot P(\cdot)$. If $P(\cdot)$ is a matrix, $\mathbf{A}'$ will be a matrix. If $P(\cdot)$ is an operation, $\mathbf{A}'$ will also be a measurement operation. As the case of sparsifying basis as a part of the measurement matrix, random permutation as a part of the measurement matrix possesses double layer protection mechanism thanks to $P(\cdot)$ acting as a new key. Nevertheless, the former can be against plaintext attacks but the latter does not necessarily.

Theorem 9: The CSC with random permutation as a part of the measurement matrix has the asymptotic spherical secrecy [60].

7) Multiple Random Matrices as a Part of the Measurement Matrix: Besides random permutation matrix playing a part of the measurement matrix, some other matrices can also be embedded in the measurement matrix. Djeujo and Ruland [61] came up with the following matrix transform:

$$T(\mathbf{A}) = \mathbf{R}_p\mathbf{R}_r\mathbf{P}_r\mathbf{A}\mathbf{P}_c\mathbf{R}_c, \tag{22}$$

where $\mathbf{R}_p$ is an $M \times M$ binary matrix, which is generated by doing p times the operation of adding one row of an identity matrix to another. $\mathbf{R}_r$ and $\mathbf{R}_c$ are diagonal matrices, whose sizes are $M \times M$ and $N \times N$, respectively. $\mathbf{P}_r$ and $\mathbf{P}_c$ are random permutation matrices with single "1" per row and column, whose sizes are $M \times M$ and $N \times N$, respectively. With this new measurement matrix, the sampling scheme is

$$\mathbf{y} = \mathbf{A}' = T(\mathbf{A})\mathbf{x} = \mathbf{R}_p\mathbf{R}_r\mathbf{P}_r\mathbf{A}\mathbf{P}_c\mathbf{R}_c\mathbf{x}. \tag{23}$$

It can be easily proved that the newly added five random matrices can maintain the invariance of RIP for the new measurement matrix. They shall be secretly altered for each signal sampling to be against plaintext attacks.

A summary result is shown in Table IV. We can find a CSC scheme does not attain the perfect secrecy in general, which can be easily understood due to the linearity of the encryption algorithm. A CSC scheme must leak the information more or less, for example, for the cases of Gaussian measurement matrix, circulant measurement matrix, and structurally random matrices. In other terms, in order for reaching the perfect secrecy, some additional conditions need to be appended. The asymptotic spherical secrecy is an ad hoc definition for the CSC and a CSC scheme satisfying this definition can be thought as an excellent cryptosystem like the cases of perturbation measurement matrix and random permutation as a part of the measurement matrix. For the cases of sparsifying basis as a part of the measurement matrix and multiple random matrices as a part of the measurement matrix, being able to resist plaintext attacks will make themselves have wider applications than other CSC schemes.

C. Some Security Analyses

1) General Security Analysis: For the general random measurement matrices such as Gaussian and Bernoulli matrices, whose corresponding CSC is marked as General-CSC, the security analysis is evaluated by Hossein *et al.* [55], in which the mutual information between plaintext and ciphertext is analysed with regard to whether the distribution of the plaintext is known. Let χ denote a discrete source alphabet set.

Theorem 10: $I(\mathbf{x};\mathbf{y}) = \log(|\chi|)/|\chi|$ if the plaintext yields a uniform distribution for alphabet set χ in a CSC system.

It can be observed from the above result of the mutual information that the perfect secrecy is unachievable, but the asymptotically perfect secrecy is accessible when the number $|\chi|$ tends to the infinity in a countable domain. This kind of secrecy is referred to as Maurer-sense perfect secrecy [121], which apparently is not stronger than the perfect secrecy.

Definition 4: A cryptosystem is said to have a Maurer-sense perfect secrecy if $\lim\limits_{N\to\infty} I(X, Y) = 0$, in which *X* and *Y* respectively correspond to plaintext and ciphertext sets and *N* represents the number of plaintexts generated from χ.

The case of the uniform distribution is generalized into that of the unknown distribution [55], and the mutual information is shown in the following theorem. In other words, Eve is able to reveal the mutual information based on ciphertext-only attack.

Theorem 11: When the statistical distribution of the plaintext set is unknown in a CSC system, we have the following result

$$I(\mathbf{x};\mathbf{y}) = \frac{1 - f_X(0)^2 + I_1(\mathbf{x};\mathbf{y})}{2M \ln 2}, \tag{24}$$

where $f_X(\mathbf{x})$ represents the density function of plaintexts and $I_1(\mathbf{x};\mathbf{y})$ follows a gamma distribution approximately.

In the above security analyses, the key is assumed to be without any privacy leakage. Nevertheless, it was claimed that for sparse plaintext, the key may be partly retrieved by use of the prior sparsity knowledge of the plaintext and thus the security analysis is further exploited from two newly defined criteria including the extended Shannon-sense perfect secrecy (ESSPS) and the extended Wyner-sense perfect secrecy (EWSPS) [122].

Definition 5: A cryptosystem is said to have ESSPS if

$$I\big(X'; Y'\big) + I\big(K'; Y'\big) = 0, \tag{25}$$

in which X' represents plaintext, Y' represents ciphertext, and K' represents key.

Definition 6: A cryptosystem is said to have EWSPS if

$$\lim_{N'\to\infty} \frac{I\big(X'; Y'\big) + I\big(K'; Y'\big)}{N'} = 0, \tag{26}$$

in which N' represents the plaintext length.

Theorem 12: The General-CSC cannot achieve ESSPS when changing the measurement matrix for each sampling.

Theorem 13: The General-CSC can achieve EWSPS when changing the measurement matrix for each sampling.

Theorem 14: The General-CSC cannot achieve EWSPS when utilizing the measurement matrix for multiple samplings.

Theorem 15: Eve can partly assess the measurement matrix and the plaintext with probability 1 with the increase of repeated times of utilizing the same measurement matrix, if the plaintexts are mutually independent.

The above theorem indicates the General-CSC is not immune against plaintext attacks, as shown in the next section.

2) Security Enhancement: Chosen-plaintext attack is able to arbitrarily select plaintexts and obtain the corresponding ciphertext. Therefore, if a cryptosystem is secure against chosen-plaintext attack, it also resists known-plaintext attack and ciphertext-only attack. For a CSC, the linearity of the sampling structure determines the difficult of being against chosen-plaintext attack. Fay introduced the counter mode [123] in the CSC for the sake of resisting chosen-plaintext attack [124]. A series of plaintexts $\mathbf{x}^i$, $i = 1, 2, \ldots, l$, is encrypted as follows

$$\mathbf{y}^i = \mathbf{A}^i \mathbf{x}^i, \tag{27}$$

where $\mathbf{A}^i$ is a Bernoulli random matrix. Let $\mathbf{A}^i_j$ be the *j*-th row vector of $\mathbf{A}^i$, where *j* represents the positive integer no larger than *M*, then

$$\mathbf{A}^i = \left(\left(\mathbf{A}^i_1\right)^T, \left(\mathbf{A}^i_2\right)^T, \ldots, \left(\mathbf{A}^i_M\right)^T\right)^T, \tag{28}$$

where $\mathbf{A}^i_j$ is generated by using a keyed hash function with the input ctr_i and *j*. The counter mode requires an initialization vector *IV*, and ctr_i is calculated as

$$\mathsf{ctr}_{i+1} = (\mathsf{ctr}_i + 1) \bmod 2^n,\ \mathsf{ctr}_1 = IV. \tag{29}$$

The decryption process is described as

$$\hat{\mathbf{x}}^i = \mathsf{Rec}\Big(\mathbf{y}^i, \mathbf{A}^i\Big), \tag{30}$$

where *Rec*$(\cdot)$ represents a reconstruction algorithm. The introduced counter mode in the CSC that is secure against chosen-plaintext attack means that one key can be used to encrypt multiple messages. In addition, an advantage of this mode is the parallelizability, i.e., the sampling and reconstruction can be implemented in parallel.

Fay and Ruland further improved the CSC with the counter mode [124] by developing modes of operation to encrypt multiple plaintexts with different energy while not leaking the signal energy to Eve [125]. As indicated in [56] and [58], the signal energy can be normalized prior to transmission to achieve ciphertext indistinguishability or asymptotic ciphertext indistinguishability, i.e., the encryption algorithm is

$$\bar{\mathbf{y}}^i = \frac{1}{\varepsilon_{\mathbf{x}_i}} \mathbf{A}^i \mathbf{x}^i, \tag{31}$$

where the signal energy $\varepsilon_{\mathbf{x}_i} = \|\mathbf{x}_i\|_2^2$. For the purpose of learning about the signal energy, a separate sensor needs to be loaded in the sensing system. Yet, it gives rise to a problem

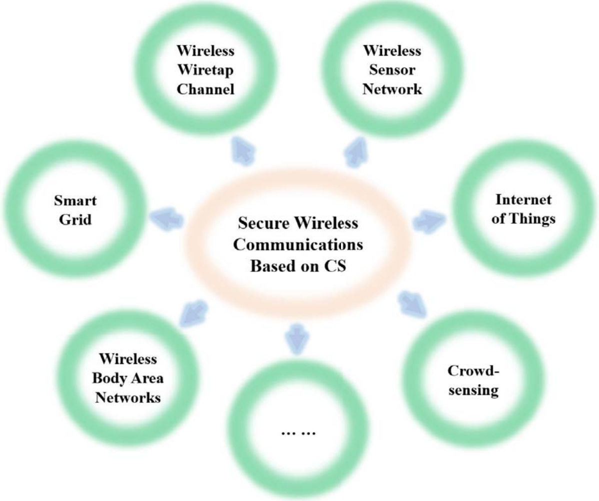


Fig. 3. Various scenarios of secure wireless communications based on CS.

of how to secretly delivery the signal energy used for Bob's decryption. Fay and Ruland [125] decorated two encryption modes for the signal energy including the counter mode and the cipher block chaining [126]. Both two modes have different properties and applications. The former allows precomputation of matrices and parallel processing, thus being able to offer high performance while the latter is self-synchronizing, suitable for some connection-less protocols where the ciphertext order is allowed to be changed to some extent.

IV. Secure Wireless Communications Based on CS

Based on the secret measurement matrices, Alice can secretly sample the signal of interest and then transmit the sampled measurements over some wireless communication channels to Bob. Moreover, the CS framework can be applied to some channels to bring benefits. Different forms of channel characteristics in wireless communications imply different scenarios of CSC, which are discussed in the following subsections in detail in terms of wireless wiretap channel, wireless sensor network, Internet of things, crowdsensing, smart grid, and wireless body area networks, as graphically shown in Fig. 3.

A. Wireless Wiretap Channel

In the wireless wiretap channel, Eve as an eavesdropper intercepts the message over a wiretap channel except a main channel between Alice and Bob.

1) CS-Based Secrecy: Based on the CS framework, Agrawal and Vishwanath built up a secure communication way over a wiretap physical layer channel by leveraging the channel asymmetry [69]. The channel model, as depicted in Fig. 4, is as follows

$$\begin{cases} \mathbf{y}_{Bob} = \mathbf{J}_{Bob}\mathbf{A}\mathbf{x} + \mathbf{e}_{Bob} \\ \mathbf{y}_{Eve} = \mathbf{J}_{Eve}\mathbf{A}\mathbf{x} + \mathbf{e}_{Eve}, \end{cases} \tag{32}$$

in which $\mathbf{x}$ represents an $N \times 1$ vector to be transmitted, and $\mathbf{y}_{Bob}$ and $\mathbf{y}_{Eve}$ are the output vectors that are transmitted over Bob's channel $\mathbf{J}_{Bob}$ and Eve's channel $\mathbf{J}_{Eve}$, respectively. $\mathbf{e}_{Bob}$ and $\mathbf{e}_{Eve}$ are the Gaussian noise vectors with zero-mean and variance σ^2. The precoding $\mathbf{Ax}$ is the framework of CS, which encodes the original message into low-dimensional measurements. Analyses pointed out that Bob can exploit accurate recovery and Eve only obtains an infeasible recovery.

2) Secrecy Capacity: With respect to a multiplicative Gaussian wiretap channel based on CS, the secrecy capacity was quantitatively studied in [70]. The channel model is described as

$$\begin{cases} \mathbf{y}_{Bob} = \mathbf{J}_{Bob}\mathbf{A}\mathbf{x} \\ \mathbf{y}_{Eve} = \mathbf{J}_{Eve}\mathbf{A}\mathbf{x}, \end{cases} \tag{33}$$

where $\mathbf{x}$ is assumed to be the input binary vector with length N, and $\mathbf{J}_{Bob}$ and $\mathbf{J}_{Eve}$ are fixed and known to all parties, whose lengths are N_{Bob} and N_{Eve}, respectively, satisfying $0 \leq N_{Eve} < N_{Bob} < N/2$. The secrecy capacity bounds are reflected as the following two theorems.

Theorem 16: The lower bound is

$$\frac{1}{N}\log N' - \frac{1}{2N}\log J' + \sum\nolimits_{\mathbf{x}} \frac{1}{2NN'}\log J'',$$

where $N' = \begin{pmatrix} N \\ N_{Bob} - 1 \end{pmatrix}$, $J' = \det(\frac{1}{N}\mathbf{J}_{Eve}\mathbf{J}_{Eve}^T)$, $J'' = \det\left(\frac{1}{N'_{Bob}}\mathbf{J}_{Eve}(\mathbf{x})\mathbf{J}_{Eve}(\mathbf{x})^T\right)$, and $\mathbf{x}$ is from the set of all binary vectors with $N_{Bob} - 1$ ones.

Theorem 17: The upper bound is

$$\frac{1}{N}\max\left(\log N', \max_{N_{Bob} \leq j \leq N}(\tilde{c}_1(i) - \tilde{c}_2(j))\right) + \frac{\log N}{N},$$

where $\tilde{c}_1(i) = \max\limits_{1 \leq i \leq N} \frac{N_{Bob}}{2}\log(\frac{1}{N_{Bob}}\|\mathbf{J}_{Bob}(i)\|^2)$ and $\tilde{c}_2(j) = \max\limits_{\mathbf{x}} \frac{1}{2}\log(\det(\frac{1}{j}\mathbf{J}_{Bob}(\mathbf{x})\mathbf{J}_{Bob}(\mathbf{x})^T))$, $\mathbf{x}$ is from the set of all binary vectors with j ones.

Following the secrecy capacity bounds, the expectation of the secrecy capacity and the asymptotic secrecy capacity are further analysed in [70].

3) The Secrecy Based on Distributed CS: Different from the CS-based physical layer secrecy schemes that involve only a point-to-point communication [69], [70], an amplify and forward scheme based on distributed CS was proposed to well cater the distributed nature of WSN [127]. It offers the physical layer secrecy underlying the distributed scheme [128] that can consume less power and occupy less amount of channel uses. For offering the physical layer secrecy, the measurement matrix as the channel matrix is used to encode the signal and Eve cannot reveal the true signal without its information. This scheme was demonstrated to be able to attain the perfect secrecy when facing a group of coordinated eavesdroppers. It is worth noting that this scheme has the advantage of key-based secrecy [53] as well as keyless-based physical layer secrecy [69], [70].

4) The Secrecy Based on MIMO Precoding: The secrecy capacity can be maximized provided that the information of full channel state of Bob and Eve can be acquired [129]. However, some applications make it impractical that a transmitter knows the information of channel state of Eve. Aiming at the transmitter with the knowledge of only the channel state information, Lin *et al.* [72] put forward a secure transmission paradigm based on an MIMO technique, which can

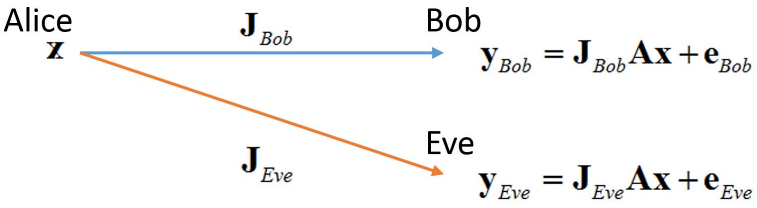

Alice
$\mathbf{x}$
$\mathbf{J}_{Bob}$
Bob
$\mathbf{y}_{Bob} = \mathbf{J}_{Bob}\mathbf{A}\mathbf{x} + \mathbf{e}_{Bob}$
$\mathbf{J}_{Eve}$
Eve
$\mathbf{y}_{Eve} = \mathbf{J}_{Eve}\mathbf{A}\mathbf{x} + \mathbf{e}_{Eve}$

Fig. 4. Wiretap channel mode based on CS.

simultaneously maximize the secrecy and SNR. The CS technique can be embedded in the proposed paradigm and makes it become an underdetermined linear system, therefore some CS reconstruction algorithms can be directly used to recover the transmitted signals. If only knowing partial information of channel state, the transmitter could exploit a new Lloyd algorithm to quantize the precoder based on the newly constructed codebooks while not cutting down the secrecy. Even if the full information is unknown, a low-cost postcoder can still be adopted to make up for the loss of SNR. To sum up, the full recovery rate and the perfect secrecy are both achievable. In addition, for the general channel coding problem of CS in the wiretap channel, some relevant results can be found in [130].

5) The Secrecy Based on Circulant Matrix: As previously mentioned, the CSC with circulant matrix as a key leaks only the autocorrelation of the plaintext [115]. Likewise, this CSC based on circulant matrix can ensure wireless indistinguishability security when maintaining the plaintext-to-noise ratio of Eve and the low channel gains for a short ciphertext and a long keystream [73]. The security measure is conducted by the relative entropy [114].

Definition 7: The relative entropy is described as the total variation distance of two cases $p(y|x_1)$, $p(y|x_2)$, where y is from one of two plaintexts x_1 and x_2.

Theorem 18: For the CSC with the circulant matrix in (11) and the channel model (32), the relative entropy is bounded by

$$\frac{M}{2}\left(\frac{\eta_\nu \varepsilon_{\mathbf{x}}}{V_{noise}\sqrt{N}} - \log\left(\frac{\eta_\nu \varepsilon_{\mathbf{x}}}{V_{noise}\sqrt{N}} + 1\right)\right)$$

with probability $1-\nu$, where for the noise, its variance is represented by V_{noise}, $\frac{\varepsilon_{\mathbf{x}}}{V_{noise}M}$ represents the plaintext-to-noise ratio, and η_ν, which has an directly proportional relationship with the channel gains, is a constant related to ν.

From this theorem, it can be found that with the growth of the keystream length N and the ciphertext length M, and the decrease of channel gain and the plaintext-to-noise ratio, the relative entropy becomes smaller and then the indistinguishability becomes stronger.

6) Multicarrier System: For a multicarrier system [131], CS was considered to provide secret communication [74], in which, to enhance the difficult of Eve's attack, the transmitter can transmit artificial noise and a sparse signal over the frequency domain. Meanwhile, the channel state information can be exploited to selectively transmit artificial noise to reduce its impact on Bob. The specific way is to partition subcarriers into two subsets, which are separately used for secure transmission from Alice to Bob and artificial noise transmission to degrade Eve's channel. Due to the impact of noise, it is difficult for Eve to get the knowledge of the received signals and estimate the measurement matrix, thus not being able to recover the original sparse signal. Finally, an upper bound on Eve's successful probability was derived. Besides of adding the artificial noise to increase the secret rate [131], a channel-aware randomization approach is induced in the encryption process to provide the secrecy against Eve while a feasible recovery at Bob [75]. In comparison with [131], both the secret signal and the original signal have the same statistical properties, and the probability of successful attack rather than the secret rate is the performance measure, as the perfect secrecy is not achievable.

Cho and Yu [76] studied a particular measurement matrix for secure communication in the multicarrier system. The measurement matrix is given as

$$\mathbf{A} = \frac{1}{\sqrt{MN}}\mathbf{R}_{Ber}\mathbf{F}, \tag{34}$$

where $\mathbf{R}_{Ber}$ is a random Bernoulli matrix and $\mathbf{F}$ represents the DFT matrix. The number field is complex-valued. With this measurement matrix and a constraint on plaintexts, each corresponding ciphertext is represented by a circularly symmetric complex Gaussian random vector when transmitted over spectral domain of multicarrier communications. To further figure out the energy sensitivity and indistinguishability, two distance measure tools including total variation and Hellinger distance are adopted to examine the probability distributions of ciphertexts. This cryptosystem was verified to have the indistinguishability against Eve's attack when keeping the plaintext a constant energy, which is a similar to the result of [56].

7) Cooperative Networks: Along with the amplify and forward CS scheme [127], a secure communication scheme based on CS and energy harvesting was designed for cooperative networks [77]. The superiority of energy harvesting lies in its capability of transferring energy from sources and relays, thus the relays can exploit energy harvesting on the received signals from sources by use of the power splitting relaying protocol and then the harvested energy can help to amplify the information and then forward it to the destination. The analyses showed that the secrecy capacity of this scheme is high enough.

B. Wireless Sensor Network

The CS can perform simultaneous sampling and compression with low complexity and has a wide application in resource-limited WSN. Embedding the security into the process of CS can bring simultaneous sampling, compression, and encryption without affecting the CS performance.

1) Establishing Secure Measurement Matrix: Dautov and Tsouri [78] constructed a secure measurement matrix for wireless security. To generate this matrix, the received signal strength indicator values are performed by the reciprocal quantization and then utilized for secret bit extraction and these bits are considered as the initial seeds of a linear feedback shift register. Iterating this register forms the final measurement matrix. This matrix was evaluated in the Rician fading model [132], which can ensure the physical layer security. Similar to [78], a lightweight encryption scheme was reported [79], in which the information of channel measurements controls the generation of the measurement matrix and thus no key distribution agreement exists.

2) Integrity-Protected CS: Instead of establishing a secure measurement matrix [78], the advanced encryption standard (AES) affords the encryption on the measurements after CS and meanwhile, a hash algorithm is added over transmission channel for integrity checking [80]. The proposed architecture was evaluated by a hardware implementation platform, where a 65-nm CMOS technology is employed for realizing the CS, AES, and integrity checking algorithms. The evaluation results showed that this architecture is energy-efficient and highly secure.

3) Capturing Medical Data: Aiming at medical WSN, Othman *et al.* [81] presented a secure data transmission scheme, which has a resemblance with [80], i.e., the data are captured and then encrypted rather than embedding the security into the CS process. It consists of the medical data samples based on CS, XOR encryption, patient's personal aggregator, and room controller's aggregator. Note that, the scheme differs from the CS-based aggregation schemes [20], [21], [105], [133], since the CS and aggregation are separate procedures in the present scheme.

4) Data Gathering: The CS is an efficient technique of data gathering in WSN [134]–[138]. This is due to the fact that each node can send multiple projected results rather than only a message to the sink with the help of the CS and it can obtain a high-quality result recovered from a handful of received messages [139]–[141]. Nevertheless, the privacy is overlooked, since the environment used for deploying the sensor nodes is often open and the sensing data are very likely sensitive. A privacy-protected version for CS-based data gathering with the help of two cryptographic schemes was suggested in [82]. One cryptographic scheme is to integrate pseudorandom permutations and symmetric encryption, and the other one is based on pseudorandom permutations and additively homomorphic encryption. The first one relies on the nature of CS to some extent without introducing much computational complexity while the additively homomorphic encryption consumes too much computation overhead in the second one. In contrast to the first one, however, the second one does not worry about a more malicious Eve, as it has a strict cryptography guarantee.

Two statistical inference attacks [83] were analysed for the general CS data gathering framework. The analysis showed that the information leakage can be easy and highly probable with only a sensor compromised by Eve who could reveal the sensor readings effectively. The leakage error is quantitatively estimated through extensive statistical analyses. According to these analyses, Hu *et al.* [83] came up with a secure scheme to prevent the inference attacks. To increase the security, chaos system was considered to be applied to CS data gathering framework [84], in which the security and performance of the multimedia data gathering were promoted by a block encryption mode and a message authentication code based on a chaotic system. While one can exert the security protection on the measurements for each sensor, it is not treated as a privacy-preserving version due to no security guarantee during the CS process. For this purpose, Xie *et al.* [85] brought forth such a compressive data gathering scheme based on homomorphic cryptosystem. The homomorphic encryption benefits the intermediate sensor nodes recode the message over encrypted domain without the knowledge of the decryption key and thereby the privacy does not leak.

5) Compressed Detection: To directly detect the compressive measurements without reconstruction is a promising signal processing application, which has been investigated in many references [142]–[146]. In particular, there exist some works focusing on secrecy guarantees [86], [87]. In [86], collaborative compressed detection is performed at distributed nodes by elaborately designing measurement matrices. On one hand, to deceive Eve, some artificial noise is injected in cooperated trustworthy nodes to help the fusion centre. On the other hand, some measurement matrices optimized with the injection of artificial noise ensure the maximized detection performance of the network without compromising the secrecy. The collaborative compressed detection [86] was extended to the work [87] from two aspects. One aspect is that the performance loss caused by the compression with a single sensor can be compensated and the other is to characterize the trade-off between dimensionality reduction and the achievable performance. Cognitive radio networks [147]–[149] are chosen for experiment test to verify theoretical findings.

C. Internet of Things

The IoT is becoming increasingly popular now and the existing privacy issues in it are also non-negligible [150]–[153]. The CS can be a candidate tool for IoT security [154], [155].

1) Adaptive CS for Smart Objects: Smart objects are the fundamental blocks in IoT system and are resource-constrained, and the adaptive CS can offer lightweight compression and encryption [88]. The framework is simply formulated by

$$\min M \ s.t. \ e_{recon} < e_{thre}, \tag{35}$$

for a given quality-of-service. M represents the number of packets after CS sampling. e_{recon}, e_{thre} represent the reconstruction error and corresponding threshold error, respectively. The above expression means to find out the optimal compression performance without affecting the service equality. The adaptive CS is to rely mainly on the information of some smart objects and adapt the CS measurement conditions for the rest of smart objects.

2) Frequency Selection for Static Environment: The static environment may result in the information leakage when the CS is applied to physical layer security model, thus a physical layer security model based on CS and frequency in IoT was proposed in [89]. The circulant matrix was exploited to play a role of the measurement matrix for high efficiency, as indicated in [115], and a binary resilient function was utilized for strong security. To cope with the static application scenario, the authors put the frequency-selective feature of the wireless channel [90] into use to increase the entropy of the measured channel and accelerate the rate of generating keys from physical layer.

3) Chaotic CS for Internet of Multimedia Things: The multimedia IoT [156] becomes pervasive with the era of multimedia data and social networks. It faces two challenges including low-cost sampling and confidentiality preservation. Accordingly, a mechanism presented in [91] can overcome these two challenges based on chaotic CS. The encryption algorithm is comprised by several key steps as follows.

- Sampling multiple images based on the measurement matrix generated by chaos,

$$\mathbf{y}_i = \mathbf{A}\mathbf{x}_i. \tag{36}$$

- Rearrange the multiple measurements $\mathbf{y}_i$ into a master image $\mathbf{y}_{master}$.
- Permute the master image $\mathbf{y}_{master}$ to obtain $\mathbf{y'}_{master}$ based on Arnold transform.
- Diffuse the permuted result $\mathbf{y'}_{master}$ to obtain the final result $\mathbf{y''}_{master}$.

Observing the above steps can find that the encryption is allowed to perform batch image processing, catering to the multimedia big data. Meanwhile, the encryption is with the architecture of two-layer, i.e., chaotic measurement matrix and permutation-diffusion, thus the confidentiality can be preserved well.

4) Secure Interaction With Cloud: When the IoT data are straightforwardly placed at the cloud server, the privacy will be exposed. A secure interaction between IoT and the cloud based on CS was investigated in [92]. The raw data are acquired by random compressed encryption and then uploaded to the cloud server. Because the random compressed encryption is a kind of multiplicative coefficient perturbation, the accessor can calculate some statistical values over encrypted domain without performing the decryption to obtain the raw data, which brings great query convenience. This kind of encryption brings two additional advantages including statistical decryption and decryption on demand. In addition to efficient statistics computation, this encryption supports secure data insertion and accurate raw decryption in cloud-enabled IoT scenarios.

D. Other Wireless Communication Scenarios

1) Crowdsensing: The strength of low-complexity data acquisition makes CS a promising tool for crowdsensing systems with high burden on each participant [157], [158], in which privacy issues are missing. Privacy issues based on CS in crowdsensing were discussed in [93]–[95]. In mobile crowdsensing, large-scale received signal strength maps often expose participants' sensitivity information, therefore a privacy-preserving scheme was projected by Wu *et al.* [93]. To maximize the geographic map coverage while protecting the participants' trace privacy, the goal of generating a received signal strength map can boils down to an objective function

$$\begin{aligned}\bigcup\nolimits_{i=1}^{l'} \Im_i^* &= \underset{\Im_i \subseteq \wp_i, \forall i}{\arg\max} \bigcup\nolimits_{i=1}^{l'} \Im_i, \\ s.t.\ \mathsf{PE}(\Im_i) &\geq \bar{C}\ or\ \mathsf{PE}(\Im_i) = 0,\end{aligned} \tag{37}$$

in which l' reflects the participant number, $\Im_i$ represents the trace of road segments of participant *i*, and $\wp_i$ is the reported road segments of participant *i*. $\mathsf{PE}(\cdot)$ indicates the privacy exposure function that reflects the minimum number of connections between two road segments. There are several steps to realize the objective function. First, one can sample the values of the received signal strength with CS so as to remove the concrete and temporal location information in every road segment. Then, after choosing some road segments, each participant deliveries a third party the sampled data. Then the third party removes more road segments for better privacy protection. Finally, an expected map is generated in the central server.

The work [94] was aimed at the data loss with a trajectory because of hardware and energy constraints and proposed a privacy-assured CS to collectively optimize the user privacy protection and the data recovery accuracy in crowdsensing. To tackle the privacy issue, a vector perturbation method was established to perturb a user's trajectory with other trajectories and therefore attain a privacy-preserving CS. Specifically, harnessing the vector perturbation method encrypts each user's incomplete location data. Then, the encrypted data are transmitted to the crowdsensing server, which reconstructs the encrypted data for all users straightforwardly without need of decrypting the data. At last, the reconstructed data are sent to each user who decrypts the data to obtain the trajectory of his own with the inverse vector perturbation. The user's privacy can be preserved, since the data keep the encrypted form while not affecting the CS reconstruction performance. The work [95] has a similar idea to [94], i.e., a privacy-preserving CS protocol without comprising its performance. The perturbed CS in [95] embeds the cryptographic feature in CS, which saves the sensor energy and is secure against chosen-plaintext attack.

2) Smart Grid: In smart grid, the data privacy is a critical concern due to the consumer information that smart meters collect is often sensitive [159]–[162]. Gao *et al.* [96] applied the CS to smart grid for secure data transmission, whose basic idea is to construct a secret measurement matrix for simultaneous encryption, sampling, and compression. It bears an analogy to the previous works like [53], whereas there is a novel data preprocessing step, which is simply summarized as follows.

- At time *t*, an access point acquires *N* readings

$$\mathbf{R}^{read,t} = \left(R_1^{read,t}, \ldots, R_N^{read,t}\right)$$

from *N* smart meters.

- At time $t + 1$, the access point calculates the difference vector

$$\begin{aligned}&\mathbf{R}^{read,t+1} - \mathbf{R}^{read,t} \\ &\quad = \left(R_1^{read,t+1} - R_1^{read,t}, \ldots, R_N^{read,t+1} - R_N^{read,t}\right).\end{aligned}$$

TABLE V
PERFORMANCE FOR DIFFERENT SECURITY MODELS

Security Model	Performance
CS-Based Secrecy [69]	Build up a secure wireless wiretap channel by leveraging the channel asymmetry
Secrecy Capacity [70]	Quantitatively investigate the lower and upper bounds of the secrecy capacity
The Secrecy Based on Distributed CS [127]	Design an amplify-forward scheme to cater the distribute nature of wireless sensor network
The Secrecy Based on MIMO Precoding [72]	Simultaneously maximize the secrecy and the signal-to-noise ratio
The Secrecy Based on Circulant Matrix [73]	Guarantee the wireless indistinguishability security with some conditions
Multicarrier System [74]–[76]	Induce artificial noise/channel randomization/particular measurement matrix for the security
Cooperative Networks [77]	Own the superiority of energy harvesting and high secrecy capacity
Establishing Secure Measurement Matrix [78], [79]	Design measurement matrix with reciprocal quantization/channel measurements
Integrity-Protected CS [80]	AES for the encryption of measurements and hash algorithm for integrity checking
Capturing Medical Data [81]	Capture data firstly and then encrypt them
Data Gathering [82]–[85]	Combine pseudorandom permutations and symmetric/additively homomorphic encryption
Compressed Detection [86], [87]	Perform collaborative compressed detection at distributed nodes
Adaptive CS for Smart Objects [88]	Utilize the information of smart objects to adapt the CS measurement condition
Frequency Selection for Static Environment [89], [90]	Enlarge the entropy of measured channel and accelerate the rate of generating keys
Chaotic CS for Internet of Multimedia Things [91]	Realize low-cost sampling and confidentiality preservation
Secure Interaction with Cloud [92]	Random compressed encryption for the raw data
Crowdsensing [93]–[95]	Maximize the geographic map coverage and protect the participants' trace privacy
Smart Grid [96]–[98]	Construct a secret measurement matrix for joint encryption, sampling, and compression
Wireless Body Area Networks [99]–[101]	Exploit chaotic CS for energy saving and data security

The above data processing is ingenious, because, in general, only a small number of readings will change between adjoining moment and the difference vector is sparse. To keep a long delay off over fading channels [163], multi-antenna access point was suggested to improve the reliability [164]. At the same time, the security can be enhanced by frequently updating keys and the physical layer security is achievable. In addition, for wireless energy auditing networks, metering data fidelity and secrecy are simultaneously ensure based on CS [97], [98], which still make full use of the advantage of CS with joint compression and encryption.

3) Wireless Body Area Networks: It consists of tiny sensor nodes deployed around human body [165]–[167], which involve some problems including the battery energy, storage, communication, privacy, etc. In the case of privacy, the CS-based monitoring was studied in [99]–[101]. In [99], chaotic CS was designed to tackle two crucial problems including energy saving and data security. The sampling equation based on chaotic CS is

$$\mathbf{y} = \beta_1 \mathbf{A}\mathbf{x} + \beta_2 \mathbf{A}_{mask}, \tag{38}$$

where $\mathbf{A}_{mask}$ is mask matrix, and β_1, β_2 are the adjustment parameters. The function of the mask matrix is to enhance the security by masking the compressive measurements. Adjusting the parameters can make the encrypted data reach a uniform distribution approximately. The sampling equation can be reformulated as

$$\mathbf{y}' = \frac{\mathbf{y} - \beta_2 \mathbf{A}_m}{\beta_1} = \mathbf{A}\mathbf{x}, \tag{39}$$

which indicates that the original measurements $\mathbf{y}$ are further encrypted into $\mathbf{y}'$ with three keys $\mathbf{A}_{mask}$, β_1, and β_2. The chaotic CS behaves that the sampling process is controlled by a chaotic system. In other words, given the initial values and parameters, the chaotic system can generate a series of pseudo-random values, which is mapped into the measurement matrix $\mathbf{A}$ and mask matrix $\mathbf{A}_{mask}$ according to some mapping rule. As a result, the whole sampling process can be manipulated by the chaotic system's initial values and parameters as the keys, which bring great convenience for key sharing. Furthermore, the sensitivity of the initial value of chaotic system can furnish strong security.

Following the encryption framework in [78], the reference [100] exploited the CS for electrocardiography. They have consistent results of the physical layer security and the energy consumption, although facing different application scenarios. However, they did not consider long-range consecutive health monitoring. In order for this, Nia *et al.* quantified some requirements with eight biomedical sensors including heart rate, body temperature, accelerometer, blood glucose, electrocardiogram, electroencephalogram, etc. and systematically analysed the energy and storage requirements [101]. On account of this, the authors proposed the corresponding solutions, one of which is to cut down the consumption for data transmission, storage, and encryption. However, the encryption is not designed in the CS but beyond the sampling, i.e., encrypting the measurements with the existing classic encryption schemes, similar to [80] and [81].

V. CONCLUDING REMARKS AND FUTURE RESEARCH

We have provided a comprehensive survey for the state-of-the-art involved in the security aspects of CS and applications of wireless communications. Aiming at how to design secure CS, we have reviewed different CSC schemes through investigating different types of measurement matrix. Subsequently, aiming at classifying extensive applications of CS, various kinds of secure communication schemes for different communication scenarios are examined. A summary result is listed in Table V for an overall understanding, in which each security model based on CS has the corresponding particular performance. Moreover, a statistical result for the number of works is shown in Fig. 5, in which the horizontal axis represents the year from 2006 to now and the vertical axis stands for the number of references in terms of the security aspects of CS and the applications of CS in secure wireless communications. It can be observed from Fig. 5 that secure wireless

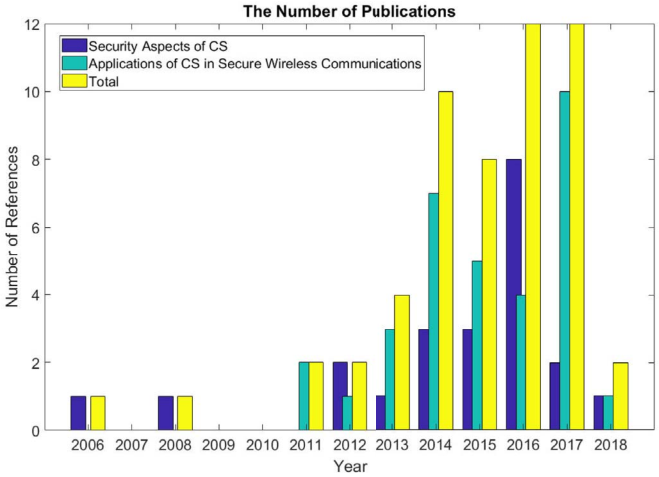


Fig. 5. The number of publications.

communications based on CS is an increasingly hot research area, especially in recent years.

As can be seen from this survey, there has been substantial progress on the theoretical research of secure wireless communications based on CS, but the application performance in practical scenarios still needs to be further investigated. The benefits that the CS can bring to wireless communications are apparent. The complexity can be reduced and the reliability can be improved. It can be easily incorporated into the current software systems and the security can be guaranteed. Thus, it has great potential in practical applications and is expected to be able to work in the design of future wireless communications. However, several critical techniques remain to be developed before put in use:

- Developing adaptive sampling rate techniques, since the sparsity of the signal to be processed is often unknown and the bandwidth of the signal is not constant in time-varying wireless environments;
- Constructing appropriate sparsity bases, which can well match with the present variable signals in compressive detection/estimation;
- Building up low-cost measurement matrix generation techniques, because random measurement matrices require high-complexity realizations and occupy large memory;
- Designing low-complexity reconstruction algorithms as high-complexity reconstruction is not suitable for real-time communication processing;
- Exploiting robust CS mechanisms against unforeseen circumstances such as noise, channel uncertainty, channel correlation, synchronization errors, multicarrier distortion, etc.;
- Establishing hardware platforms for CS realization compatible with practical wireless communication environments.

REFERENCES

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

[2] E. J. 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, Feb. 2006.

[3] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[4] A. L. Goldberger *et al.*, "Physiobank, physiotoolkit, and physionet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. E215–E220, 2000.

[5] Y. Zhang, Y. Xiang, and L. Y. Zhang, *Secure Compressive Sensing in Multimedia Data, Cloud Computing and IoT*. Singapore: Springer, 2018.

[6] Z. Gao *et al.*, "Compressive sensing techniques for next-generation wireless communications," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 144–153, Jun. 2018.

[7] Z. Gao, L. Dai, W. Dai, B. Shim, and Z. Wang, "Structured compressive sensing-based spatio-temporal joint channel estimation for FDD massive MIMO," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 601–617, Feb. 2016.

[8] L. Dai *et al.*, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sep. 2015.

[9] Z. Qin, Y. Gao, and C. G. Parini, "Data-assisted low complexity compressive spectrum sensing on real-time signals under sub-Nyquist rate," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1174–1185, Feb. 2016.

[10] S. Gishkori, V. Lottici, and G. Leus, "Compressive sampling-based multiple symbol differential detection for UWB communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 3778–3790, Jul. 2014.

[11] Z. Zhou *et al.*, "Low-rank tensor decomposition-aided channel estimation for millimeter wave MIMO-OFDM systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1524–1538, Jul. 2017.

[12] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[13] C. Luo, F. Wu, J. Sun, and C. W. Chen, "Efficient measurement generation and pervasive sparsity for compressive data gathering," *IEEE Trans. Wireless Commun.*, vol. 9, no. 12, pp. 3728–3738, Dec. 2010.

[14] G. Chen, X.-Y. Liu, L. Kong, J.-L. Lu, and M.-Y. Wu, "Multi-attribute compressive data gathering," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2014, pp. 2178–2183.

[15] C. Luo, J. Sun, and F. Wu, "Compressive network coding for approximate sensor data gathering," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2011, pp. 1–6.

[16] D. Ebrahimi and C. Assi, "On the interaction between scheduling and compressive data gathering in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2845–2858, Apr. 2016.

[17] J. Cheng, Q. Ye, H. Jiang, D. Wang, and C. Wang, "STCDG: An efficient data gathering algorithm based on matrix completion for wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 850–861, Feb. 2013.

[18] C. Liu, C. Chigan, and C. Gao, "Compressive sensing based data collection in VANETs," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2013, pp. 1756–1761.

[19] Y. Yao, Q. Cao, and A. V. Vasilakos, "EDAL: An energy-efficient, delay-aware, and lifetime-balancing data collection protocol for heterogeneous wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 23, no. 3, pp. 810–823, Jun. 2015.

[20] X. Xu, R. Ansari, and A. Khokhar, "Power-efficient hierarchical data aggregation using compressive sensing in WSNs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2013, pp. 1769–1773.

[21] C. Zhao, W. Zhang, X. Yang, Y. Yang, and Y.-Q. Song, "A novel compressive sensing based data aggregation scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 18–23.

[22] F. Zhu, A. Liu, and V. K. N. Lau, "Joint interference mitigation and data recovery for massive carrier aggregation via non-linear compressive sensing," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 1389–1404, Feb. 2018.

[23] N. Deligiannis, J. F. C. Mota, E. Zimos, and M. R. D. Rodrigues, "Heterogeneous networked data recovery from compressive measurements using a copula prior," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5333–5347, Dec. 2017.

[24] G. Quer, R. Masiero, G. Pillonetto, M. Rossi, and M. Zorzi, "Sensing, compression, and recovery for WSNs: Sparse signal modeling and monitoring framework," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3447–3461, Oct. 2012.

[25] B. Khalfi, B. Hamdaoui, M. Guizani, and N. Zorba, "Efficient spectrum availability information recovery for wideband DSA networks: A weighted compressive sampling approach," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2162–2172, Apr. 2018.

[26] S. Jin and X. Zhang, "Exact recoverability analysis for joint sparse optimization with missing measurements," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2015, pp. 1660–1665.

[27] X. Zhang, Y. Ma, H. Qi, and Y. Gao, "Low-complexity compressive spectrum sensing for large-scale real-time processing," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 674–677, Aug. 2018.

[28] Z. Tian, "Cyclic feature based wideband spectrum sensing using compressive sampling," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–5.

[29] S. Mistry and V. Sharma, "New algorithms for wideband spectrum sensing via compressive sensing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2013, pp. 2595–2600.

[30] Y. Wang, Z. Tian, and C. Feng, "Sparsity order estimation and its application in compressive spectrum sensing for cognitive radios," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2116–2125, Jun. 2012.

[31] A. Ali and W. Hamouda, "Advances on spectrum sensing for cognitive radio networks: Theory and applications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1277–1304, 2nd Quart., 2017.

[32] H. Sun, A. Nallanathan, J. Jiang, and H. V. Poor, "Compressive autonomous sensing (CASe) for wideband spectrum sensing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2012, pp. 4442–4446.

[33] R. Du, L. Gkatzikis, C. Fischione, and M. Xiao, "Energy efficient sensor activation for water distribution networks based on compressive sensing," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2997–3010, Dec. 2015.

[34] W. Chen, M. R. D. Rodrigues, and I. J. Wassell, "Distributed compressive sensing reconstruction via common support discovery," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–5.

[35] W. Chen and I. J. Wassell, "A decentralized Bayesian algorithm for distributed compressive sensing in networked sensing systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1282–1292, Feb. 2016.

[36] A. Talari and N. Rahnavard, "CStorage: Distributed data storage in wireless sensor networks employing compressive sensing," in *Proc. Glob. Telecommun. Conf. (GLOBECOM)*, 2011, pp. 1–5.

[37] Z. Chen, J. Ranieri, R. Zhang, and M. Vetterli, "DASS: Distributed adaptive sparse sensing," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2571–2583, May 2015.

[38] R. Mohammadian, A. Amini, and B. H. Khalaj, "Compressive sensing-based pilot design for sparse channel estimation in OFDM systems," *IEEE Commun. Lett.*, vol. 21, no. 1, pp. 4–7, Jan. 2017.

[39] X. Ma, F. Yang, S. Liu, J. Song, and Z. Han, "Design and optimization on training sequence for mmWave communications: A new approach for sparse channel estimation in massive MIMO," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1486–1497, Jul. 2017.

[40] P. Chen, Y. Rong, S. Nordholm, Z. He, and A. J. Duncan, "Joint channel estimation and impulsive noise mitigation in underwater acoustic OFDM communication systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6165–6178, Sep. 2017.

[41] Y. Du *et al.*, "Joint channel estimation and multiuser detection for uplink grant-free NOMA," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 682–685, Aug. 2018.

[42] D. C. Dhanapala, V. W. Bandara, A. Pezeshki, and A. P. Jayasumana, "Phenomena discovery in WSNs: A compressive sensing based approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2013, pp. 1851–1856.

[43] L. Kong *et al.*, "Autonomous relay for millimeter-wave wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 9, pp. 2127–2136, Sep. 2017.

[44] B. Sun, Y. Guo, N. Li, and D. Fang, "Multiple target counting and localization using variational Bayesian EM algorithm in wireless sensor networks," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2985–2998, Jul. 2017.

[45] H. Cui, C. Luo, J. Wu, C. W. Chen, and F. Wu, "Compressive coded modulation for seamless rate adaptation," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 4892–4904, Oct. 2013.

[46] G. Yang, V. Y. F. Tan, C. K. Ho, S. H. Ting, and Y. L. Guan, "Wireless compressive sensing for energy harvesting sensor nodes over fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2013, pp. 4962–4967.

[47] S. Xiang and L. Cai, "Transmission control for compressive sensing video over wireless channel," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1429–1437, Mar. 2013.

[48] Z. Liu, Z. Li, M. Li, W. Xing, and D. Lu, "Path reconstruction in dynamic wireless sensor networks using compressive sensing," *IEEE/ACM Trans. Netw.*, vol. 24, no. 4, pp. 1948–1960, Aug. 2016.

[49] F. Wu, D. Liu, Z. Wu, Y. Zhang, and G. Chen, "Cost-efficient indoor white space exploration through compressive sensing," *IEEE/ACM Trans. Netw.*, vol. 25, no. 3, pp. 1686–1702, Jun. 2017.

[50] E. J. 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, Dec. 2006.

[51] M. F. Duarte, S. Sarvotham, M. B. Wakin, D. Baron, and R. G. Baraniuk, "Joint sparsity models for distributed compressed sensing," in *Proc. IEEE Workshop Signal Process. Adapt. Sparse Struct. Represent.*, 2005, pp. 1–4.

[52] I. Drori, "Compressed video sensing," in *Proc. BMVA Symp. 3D Video Anal. Display Appl.*, 2008, pp. 1–2.

[53] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. IEEE 46th Annu. Allerton Conf. Commun. Control Comput.*, 2008, pp. 813–817.

[54] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[55] S. A. Hossein, A. E. Tabatabaei, and N. Zivic, "Security analysis of the joint encryption and compressed sensing," in *Proc. IEEE 20th Telecommun. Forum (TELFOR)*, 2012, pp. 799–802.

[56] T. Bianchi, V. Bioglio, and E. Magli, "Analysis of one-time random projections for privacy preserving compressed sensing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 313–327, Feb. 2016.

[57] T. Bianchi and E. Magli, "Analysis of the security of compressed sensing with circulant matrices," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, 2014, pp. 173–178.

[58] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-complexity multiclass encryption by compressed sensing," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2183–2195, May 2015.

[59] L. Y. Zhang, K.-W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Trans. Multimedia*, vol. 18, no. 9, pp. 1720–1732, Sep. 2016.

[60] Y. Zhang *et al.*, "Embedding cryptographic features in compressive sensing," *Neurocomputing*, vol. 205, pp. 472–480, Sep. 2016.

[61] R. A. Djeujo and C. Ruland, "Embedding cryptographically secure matrix transformation in structured compressive sensing," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, 2017, pp. 1–7.

[62] H. Fang, S. A. Vorobyov, H. Jiang, and O. Taheri, "Permutation meets parallel compressed sensing: How to relax restricted isometry property for 2D sparse signals," *IEEE Trans. Signal Process.*, vol. 62, no. 1, pp. 196–210, Jan. 2014.

[63] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[64] Z. Li, R. Yates, and W. Trappe, "Secure communication over wireless channels," in *Proc. Inf. Theory Appl. Workshop*, 2007, pp. 1–5.

[65] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[66] B. Dai, Z. Ma, M. Xiao, X. Tang, and P. Fan, "Secure communication over finite state multiple-access wiretap channel with delayed feedback," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 723–736, Apr. 2018.

[67] M. Chraiti, A. Ghrayeb, and C. Assi, "Achieving full secure degrees-of-freedom for the MISO wiretap channel with an unknown eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7066–7079, Nov. 2017.

[68] A. Nooraiepour and T. M. Duman, "Randomized convolutional codes for the wiretap channel," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3442–3452, Aug. 2017.

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

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

[71] J. E. Barceló-Lladó, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a PHY-layer secrecy solution in wireless sensor networks," in *Proc. 7th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Hoboken, NJ, USA, 2012, pp. 113–116.

[72] C.-H. Lin, S.-H. Tsai, and Y.-P. Lin, "Secure transmission using MIMO precoding," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 801–813, May 2014.

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

[74] J. Choi, "Secure transmissions via compressive sensing in multicarrier systems," *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1315–1319, Oct. 2016.

[75] J. Choi, "Channel-aware randomized encryption and channel estimation attack," *IEEE Access*, vol. 5, pp. 25046–25054, 2017.

[76] W. Cho and N. Y. Yu, "Secure communications with asymptotically Gaussian compressed encryption," *IEEE Signal Process. Lett.*, vol. 25, no. 1, pp. 80–84, Jan. 2018.

[77] S. Chang, J. Li, X. Fu, and L. Zhang, "Energy harvesting for physical layer security in cooperative networks based on compressed sensing," *Entropy*, vol. 19, no. 9, p. 462, 2017.

[78] R. Dautov and G. R. Tsouri, "Establishing secure measurement matrix for compressed sensing using wireless physical layer security," in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (ICNC)*, San Diego, CA, USA, 2013, pp. 354–358.

[79] A. Fragkiadakis, E. Tragos, and A. Traganitis, "Lightweight and secure encryption using channel measurements," in *Proc. IEEE 4th Int. Conf. Wireless Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. (VITAE)*, Aalborg, Denmark, 2014, pp. 1–5.

[80] M. Zhang, M. M. Kermani, A. Raghunathan, and N. K. Jha, "Energy-efficient and secure sensor data transmission using encompression," in *Proc. 26th Int. Conf. LSI Design/12th Int. Conf. Embedded Syst. (VLSID)*, Pune, India, 2013, pp. 31–36.

[81] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Secure data transmission protocol for medical wireless sensor networks," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Victoria, BC, Canada, 2014, pp. 649–656.

[82] S. Qi, Z. Li, and Y. Liu, "Achieving private, scalable, and precise data collection in wireless sensor networks," in *Proc. IEEE 18th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Singapore, 2012, pp. 14–21.

[83] P. Hu, K. Xing, X. Cheng, H. Wei, and H. Zhu, "Information leaks out: Attacks and countermeasures on compressive data gathering in wireless sensor networks," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, 2014, pp. 1258–1266.

[84] J. Qi, X. Hu, Y. Ma, and Y. Sun, "A hybrid security and compressive sensing-based sensor data gathering scheme," *IEEE Access*, vol. 3, pp. 718–724, 2015.

[85] K. Xie *et al.*, "An efficient privacy-preserving compressive data gathering scheme in WSNs," *Inf. Sci.*, vol. 390, pp. 82–94, Jun. 2017.

[86] B. Kailkhura, S. Liu, T. Wimalajeewa, and P. K. Varshney, "Measurement matrix design for compressed detection with secrecy guarantees," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 420–423, Aug. 2016.

[87] B. Kailkhura, T. Wimalajeewa, and P. K. Varshney, "Collaborative compressive detection with physical layer secrecy constraints," *IEEE Trans. Signal Process.*, vol. 65, no. 4, pp. 1013–1025, Feb. 2017.

[88] A. Fragkiadakis, P. Charalampidis, and E. Tragos, "Adaptive compressive sensing for energy efficient smart objects in IoT applications," in *Proc. 4th Int. Conf. Wireless Commun. Veh. Techn. Inf. Theory Aerosp. Electron. Syst. (VITAE)*, Aalborg, Denmark, 2014, pp. 1–5.

[89] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in Internet of Things based on compressed sensing and frequency selection," *IET Commun.*, vol. 11, no. 9, pp. 1431–1437, Jul. 2017.

[90] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1779–1790, Sep. 2013.

[91] Y. Zhang *et al.*, "Low-cost and confidentiality-preserving data acquisition for Internet of multimedia things," *IEEE Internet Things J.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8171723, doi: 10.1109/JIOT.2017.2781737.

[92] W. Xue *et al.*, "Kryptein: A compressive-sensing-based encryption scheme for the Internet of Things," in *Proc. 16th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Pittsburgh, PA, USA, 2017, pp. 169–180.

[93] X. Wu, P. Yang, S. Tang, X. Zheng, and Y. Xiong, "Privacy preserving RSS map generation for a crowdsensing network," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 42–48, Aug. 2015.

[94] L. Kong *et al.*, "Privacy-preserving compressive sensing for crowdsensing based trajectory recovery," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Columbus, OH, USA, 2015, pp. 31–40.

[95] Z. Zhang, C. Jin, M. Li, and L. Zhu, "A perturbed compressed sensing protocol for crowd sensing," *Mobile Inf. Syst.*, vol. 2016, May 2016, Art. no. 1763416.

[96] J. Gao, X. Zhang, H. Liang, and X. S. Shen, "Joint encryption and compressed sensing in smart grid data transmission," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Austin, TX, USA, 2014, pp. 662–667.

[97] S.-Y. Chiu, H. H. Nguyen, R. Tan, D. K. Yau, and D. Jung, "JICE: Joint data compression and encryption for wireless energy auditing networks," in *Proc. 12th Annu. IEEE Int. Conf. Sens. Commun. Netw. (SECON)*, Seattle, WA, USA, 2015, pp. 453–461.

[98] R. Tan, S.-Y. Chiu, H. H. Nguyen, D. K. Yau, and D. Jung, "A joint data compression and encryption approach for wireless energy auditing networks," *ACM Trans. Sensor Netw.*, vol. 13, no. 2, p. 9, 2017.

[99] H. Peng *et al.*, "Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks," *IEEE Trans. Biomed. Circuit Syst.*, vol. 11, no. 3, pp. 558–573, Jun. 2017.

[100] R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," *IEEE J. Biomed. Health Inf.*, vol. 20, no. 1, pp. 135–142, Jan. 2016.

[101] A. M. Nia, M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Energy-efficient long-term continuous personal health monitoring," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 1, no. 2, pp. 85–98, Apr./Jun. 2015.

[102] M. F. Duarte and Y. C. Eldar, "Structured compressed sensing: From theory to applications," *IEEE Trans. Signal Process.*, vol. 59, no. 9, pp. 4053–4085, Sep. 2011.

[103] S. K. Sharma, E. Lagunas, S. Chatzinotas, and B. Ottersten, "Application of compressive sensing in cognitive radio communications: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1838–1860, 3rd Quart., 2016.

[104] F. Salahdine, N. Kaabouch, and H. El Ghazi, "A survey on compressive sensing techniques for cognitive radio networks," *Phys. Commun.*, vol. 20, pp. 61–73, Sep. 2016.

[105] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018, 4th Quart., 2014.

[106] J. A. López-Salcedo, J. A. Del Peral-Rosado, and G. Seco-Granados, "Survey on robust carrier tracking techniques," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 670–688, 2nd Quart., 2014.

[107] S. Pudlewski and T. Melodia, "A tutorial on encoding and wireless transmission of compressively sampled videos," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 754–767, 2nd Quart., 2013.

[108] J. Guo, B. Song, Y. He, F. R. Yu, and M. Sookhak, "A survey on compressed sensing in vehicular infotainment systems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2662–2680, 4th Quart., 2017.

[109] Y. Zhang *et al.*, "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, pp. 2507–2519, 2016.

[110] D. L. Donoho and X. Huo, "Uncertainty principles and ideal atomic decomposition," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2845–2862, Nov. 2001.

[111] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.

[112] M. A. Figueiredo, R. D. Nowak, and S. J. Wright, "Gradient projection for sparse reconstruction: Application to compressed sensing and other inverse problems," *IEEE J. Sel. Top. Signal Process.*, vol. 1, no. 4, pp. 586–597, Dec. 2007.

[113] R. Chartrand, "Exact reconstruction of sparse signals via nonconvex minimization," *IEEE Signal Process. Lett.*, vol. 14, no. 10, pp. 707–710, Oct. 2007.

[114] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Somerset, U.K.: Wiley, 2012.

[115] W. Yin, S. Morgan, J. Yang, and Y. Zhang, "Practical compressive sensing with Toeplitz and circulant matrices," in *Proc. SPIE*, 2010, Art. no. 77440K.

[116] T. T. Do, L. Gan, N. H. Nguyen, and T. D. Tran, "Fast and efficient compressive sensing using structurally random matrices," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 139–154, Jan. 2012.

[117] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2182–2195, Oct. 2015.

[118] M. Silvano and T. Paolo, *Knapsack Problems: Algorithms and Computer Implementations*. New York, NY, USA: Wiley, 1990.

[119] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Average recovery performances of non-perfectly informed compressed sensing: With applications to multiclass encryption," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2015, pp. 3651–3655.

[120] E. J. Candes and Y. Plan, "A probabilistic and RIPless theory of compressed sensing," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7235–7254, Nov. 2011.

[121] B. Goebel, Z. Dawy, J. Hagenauer, and J. C. Mueller, "An approximation to the distribution of finite sample size mutual information estimates," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 2, 2005, pp. 1102–1106.

[122] Z. Yang, W. Yan, and Y. Xiang, "On the security of compressed sensing-based signal cryptosystem," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 3, pp. 363–371, Sep. 2015.

[123] P. Rogaway, *Evaluation of Some Blockcipher Modes of Operation*, Cryptography Res. Eval. Committees (CRYPTREC) Govt. Japan, Los Gatos, CA, USA, 2011.

[124] R. Fay, "Introducing the counter mode of operation to compressed sensing based encryption," *Inf. Process. Lett.*, vol. 116, no. 4, pp. 279–283, 2016.

[125] R. Fay and C. Ruland, "Compressive sensing encryption modes and their security," in *Proc. 11th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, 2016, pp. 119–126.

[126] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," in *Proc. 38th Annu. Symp. Found. Comput. Sci.*, 1997, pp. 394–403.

[127] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 839–850, May 2014.

[128] J. E. Barceló-Lladó, A. Morell, and G. Seco-Granados, "Optimization of the amplify-and-forward in a wireless sensor network using compressed sensing," in *Proc. IEEE 19th Eur. Signal Process. Conf.*, 2011, pp. 363–367.

[129] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[130] W. Huleihel, N. Merhav, and S. S. Shitz, "On compressive sensing in coding problems: A rigorous approach," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5727–5744, Oct. 2015.

[131] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. Chichester, U.K.: Wiley, 2010.

[132] C. Xiao, Y. R. Zheng, and N. C. Beaulieu, "Novel sum-of-sinusoids simulation models for Rayleigh and Rician fading channels," *IEEE Trans. Wireless Commun.*, vol. 5, no. 12, pp. 3667–3679, Dec. 2006.

[133] X. Xu, R. Ansari, and A. Khokhar, "Adaptive hierarchical data aggregation using compressive sensing (A-HDACS) for non-smooth data field," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 65–70.

[134] H. Zheng, S. Xiao, X. Wang, X. Tian, and M. Guizani, "Capacity and delay analysis for data gathering with compressive sensing in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 917–927, Feb. 2013.

[135] H. Zheng, S. Xiao, X. Wang, and X. Tian, "On the capacity and delay of data gathering with compressive sensing in wireless sensor networks," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2011, pp. 1–5.

[136] Y. Li, J. Zou, and H. Xiong, "Global correlated data gathering in wireless sensor networks with compressive sensing and randomized gossiping," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2011, pp. 1–5.

[137] R. Xie and X. Jia, "Minimum transmission data gathering trees for compressive sensing in wireless sensor networks," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2011, pp. 1–5.

[138] X. Wu, Y. Xiong, P. Yang, S. Wan, and W. Huang, "Sparsest random scheduling for compressive data gathering in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5867–5877, Oct. 2014.

[139] Y. Tang, B. Zhang, T. Jing, D. Wu, and X. Cheng, "Robust compressive data gathering in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2754–2761, Jun. 2013.

[140] L. Xu, Y. Wang, and Y. Wang, "Major coefficients recovery: A compressed data gathering scheme for wireless sensor network," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2011, pp. 1–5.

[141] L. Xiang, J. Luo, and C. Rosenberg, "Compressed data aggregation: Energy-efficient and high-fidelity data collection," *IEEE/ACM Trans. Netw.*, vol. 21, no. 6, pp. 1722–1735, Dec. 2013.

[142] H. Zheng, S. Xiao, and X. Wang, "Sequential compressive target detection in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–5.

[143] B. Wang, L. Dai, Y. Zhang, T. Mir, and J. Li, "Dynamic compressive sensing-based multi-user detection for uplink grant-free NOMA," *IEEE Commun. Lett.*, vol. 20, no. 11, pp. 2320–2323, Nov. 2016.

[144] A. Garcia-Rodriguez and C. Masouros, "Low-complexity compressive sensing detection for spatial modulation in large-scale multiple access channels," *IEEE Trans. Commun.*, vol. 63, no. 7, pp. 2565–2579, Jul. 2015.

[145] E. Lagunas and M. Nájar, "Spectral feature detection with sub-Nyquist sampling for wideband spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3978–3990, Jul. 2015.

[146] Y. Wang, Z. Tian, and C. Feng, "Collecting detection diversity and complexity gains in cooperative spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 11, no. 8, pp. 2876–2883, Aug. 2012.

[147] Z. Qin, Y. Liu, Y. Gao, M. Elkashlan, and A. Nallanathan, "Wireless powered cognitive radio networks with compressive sensing and matrix completion," *IEEE Trans. Commun.*, vol. 65, no. 4, pp. 1464–1476, Aug. 2017.

[148] A. El Shafie, N. Al-Dhahir, and R. Hamila, "Exploiting sparsity of relay-assisted cognitive radio networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2015, pp. 1153–1158.

[149] H. Qi and Y. Gao, "Two-dimensional compressive spectrum sensing in collaborative cognitive radio networks," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2017, pp. 1–6.

[150] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[151] J. Lin *et al.*, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[152] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[153] W. Chen, M. R. Rodrigues, and I. J. Wassell, "A Fréchet mean approach for compressive sensing date acquisition and reconstruction in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3598–3606, Oct. 2012.

[154] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[155] A. Fragkiadakis *et al.*, "Signal processing techniques for energy efficiency, security, and reliability in the IoT domain," in *Internet of Things (IoT) in 5G Mobile Technologies*. Cham, Switzerland: Springer, 2016, pp. 419–447.

[156] S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood, "Internet of multimedia things: Vision and challenges," *Ad Hoc Netw.*, vol. 33, pp. 87–111, Oct. 2015.

[157] T. Liu, Y. Zhu, Y. Yang, and F. Ye, "Incentive design for air pollution monitoring based on compressive crowdsensing," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.

[158] D. Wu *et al.*, "Adaptive lookup of open WiFi using crowdsensing," *IEEE/ACM Trans. Netw.*, vol. 24, no. 6, pp. 3634–3647, Dec. 2016.

[159] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2820–2835, 4th Quart., 2017.

[160] F. G. Marmol, C. Sorge, O. Ugus, and G. M. Pérez, "Do not snoop my habits: Preserving privacy in the smart grid," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 166–172, May 2012.

[161] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, 4th Quart., 2012.

[162] T. W. Chim, S.-M. Yiu, L. C. K. Hui, and V. O. K. Li, "Privacy-preserving advance power reservation," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 18–23, Aug. 2012.

[163] B. M. Hochwald and S. Ten Brink, "Achieving near-capacity on a multiple-antenna channel," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 389–399, Mar. 2003.

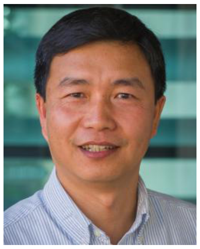
[164] J. Choi, K. Lee, Y. Lee, and N. Y. Yu, "Secure compressive random access for meter reading in smart grid using multi-antenna access point," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Sydney, NSW, Australia, 2016, pp. 116–121.

[165] H. Cao, V. Leung, C. Chow, and H. Chan, "Enabling technologies for wireless body area networks: A survey and outlook," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 84–93, Dec. 2009.

[166] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and *m*-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

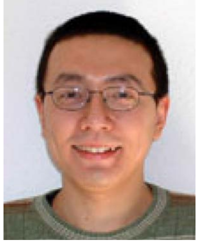
[167] G. A. Conway, S. L. Cotton, and W. G. Scanlon, "An antennas and propagation approach to improving physical layer performance in wireless body area networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 1, pp. 27–36, Jan. 2009.

Yushu Zhang (M'17) received the Ph.D. degree from the College of Computer Science, Chongqing University, Chongqing, China, in 2014. He is an Associate Professor with the School of Electronics and Information Engineering, Southwest University, Chongqing, since 2015. He held various research positions with the City University of Hong Kong and the University of Macau. He is currently an Alfred Deakin Post-Doctoral Research Fellow with the School of Information Technology, Deakin University, Australia. His research interests include multimedia security, compressive sensing security, cloud computing, and big data security. He has published over 70 refereed journal articles and conference papers in the above areas.



Yong Xiang (SM'12) received the Ph.D. degree in electrical and electronic engineering from the University of Melbourne, Australia. He is a Professor and the Director of the Artificial Intelligence and Image Processing Research Cluster, School of Information Technology, Deakin University, Australia. His research interests include information security and privacy, signal and image processing, data analytics and machine intelligence, Internet of Things, and blockchain. He has published four monographs, over 100 refereed journal articles, and numerous conference papers in the above areas. He is an Associate Editor of IEEE SIGNAL PROCESSING LETTERS and IEEE ACCESS. He has served as the program chair, the TPC chair, the symposium chair, and the session chair for a number of international conferences.

Leo Yu Zhang (S'14–M'17) received the Ph.D. degree from the Department of Electronic Engineering, City University of Hong Kong, in 2016. He was a Post Doctoral Fellow with the Department of Computer Science, City University of Hong Kong. He is currently a Lecturer with the School of Information Technology, Deakin University, Australia. He held various research positions with the City University of Hong Kong, the University of Macau, Macau, China, the University of Ferrara, Ferrara, Italy, and the University of Bologna, Bologna, Italy. His current research interests include cloud security, multimedia security, and compressed sensing.



Yue Rong (S'03–M'06–SM'11) received the Ph.D. degree *(summa cum laude)* in electrical engineering from the Darmstadt University of Technology, Darmstadt, Germany, in 2005. He was a Post-Doctoral Researcher with the Department of Electrical Engineering, University of California at Riverside from 2006 to 2007. Since 2007, he has been with the Department of Electrical and Computer Engineering, Curtin University, Bentley, Australia, where he is currently a Professor. His research interests include signal processing for communications, wireless communications, underwater acoustic communications, applications of linear algebra and optimization methods, and statistical and array signal processing. He has published over 150 journal and conference papers in the above areas. He was a recipient of the Best Paper Award at the 2011 International Conference on Wireless Communications and Signal Processing, the Best Paper Award at the 2010 Asia–Pacific Conference on Communications, and the Young Researcher of the Year Award of the Faculty of Science and Engineering at Curtin University in 2010. He is an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He was an Editor of the IEEE WIRELESS COMMUNICATIONS LETTERS from 2012 to 2014, a Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS special issue on theories and methods for advanced wireless relays, and was a TPC Member for the IEEE ICC, WCSP, IWCMC, EUSIPCO, and ChinaCom.

Song Guo (M'02–SM'11) received the Ph.D. degree in computer science from the University of Ottawa. He is a Full Professor with the Department of Computing, Hong Kong Polytechnic University. He was a Professor with the University of Aizu from 2007 to 2016. His research has been sponsored by JSPS, JST, MIC, NSF, NSFC, and industrial companies. His research interests are mainly in the areas of big data, cloud computing and networking, and distributed systems with over 400 papers published in major conferences and journals. His work was recognized by the 2016 Annual Best of Computing: Notable Books and Articles in Computing in *ACM Computing Reviews*. He was a recipient of the 2017 IEEE Systems Journal Annual Best Paper Award and other five best paper awards from IEEE/ACM conferences. He was an Associate Editor of IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS from 2011 to 2015 and an IEEE Communications Society Distinguished Lecturer from 2016 to 2017. He is currently on the editorial boards of IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and IEEE COMMUNICATIONS. He also served as the general, TPC, and symposium Chair for numerous IEEE conferences. He is currently the Member of Board of Governors and the Director of Membership Services of IEEE Communications Society.