

PAPER

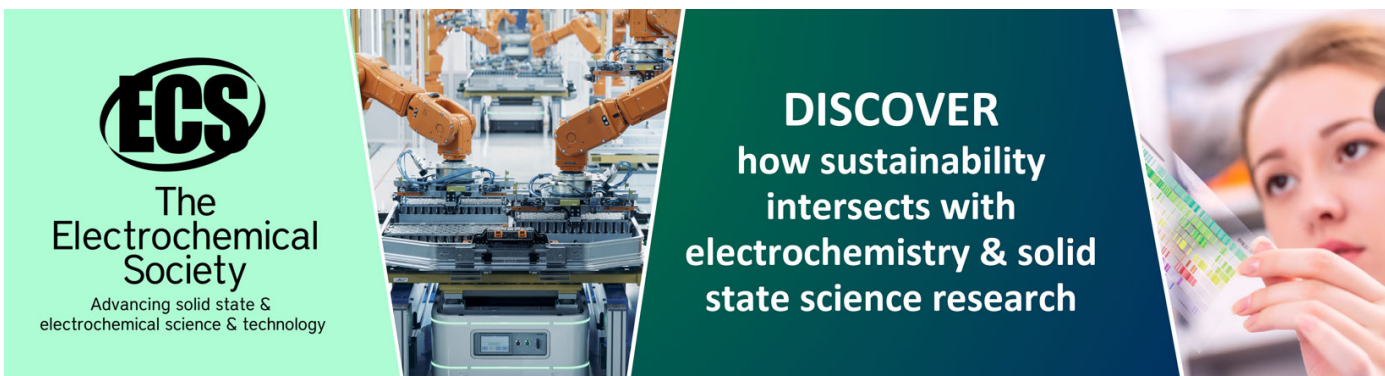
A graphite oxide (GO)-based remote readable tamper evident seal

To cite this article: A Cattaneo *et al* 2015 *Smart Mater. Struct.* **24** 105014

View the [article online](#) for updates and enhancements.

You may also like

- [Optical security based on near-field processes at the nanoscale](#)
Makoto Naruse, Naoya Tate and Motoichi Ohtsu
- [Power system topological node tamper detection method based on fuzzy graph theory](#)
Huijuan Tan, Wenxin Guo, Shiming Li et al.
- [Design and concept proof of an inductive impulse self-destructer in sense-and-react countermeasure against physical attacks](#)
Sho Tada, Yuki Yamashita, Kohei Matsuda et al.



ECS
The
Electrochemical
Society
Advancing solid state &
electrochemical science & technology

DISCOVER
how sustainability
intersects with
electrochemistry & solid
state science research

A graphite oxide (GO)-based remote readable tamper evident seal

A Cattaneo¹, J A Bossert², C Guzman³, A Haaker⁴, G Gupta², A Mohite², J H Dumont², G M Purdy², K A Miller⁵, A N Marchi¹, C R Farrar¹ and D D L Mascareñas¹

¹ Los Alamos National Laboratory, Engineering Institute, PO Box 1663, MS T001, Los Alamos, NM 87544, USA

² Los Alamos National Laboratory, Center for Integrated Nanotechnologies, MS-K763, PO Box 1663, Los Alamos, NM 87545, USA

³ Prairie View A&M University, Thermal Science Research Center, MS-2525, PO Box 519, Prairie View, TX 77446, USA

⁴ University of New Mexico, Mechanical Engineering Department, MSC01 1150, Albuquerque, NM 87131, USA

⁵ Los Alamos National Laboratory, Safeguards Science and Technology, MS-E540, PO Box 1663, Los Alamos, NM 87545, USA

E-mail: cattaneo@lanl.gov

Received 25 March 2015, revised 8 July 2015

Accepted for publication 20 July 2015

Published 8 September 2015



Abstract

This paper presents a prototype of a remotely readable graphite oxide (GO) paper-based tamper evident seal. The proposed device combines the tunable electrical properties offered by reduced graphite oxide (RGO) with a compressive sampling scheme. The benefit of using RGO as a tamper evident seal material is the sensitivity of its electrical properties to the common mechanisms adopted to defeat tamper-evident seals. RGO's electrical properties vary upon local stress or cracks induced by mechanical action (e.g., produced by shimming or lifting attacks). Further, modification of the seal's electrical properties can result from the incidence of other defeat mechanisms, such as temperature changes, solvent treatment and steam application. The electrical tunability of RGO enables the engraving of a circuit on the area of the tamper evident seal intended to be exposed to malicious attacks. The operation of the tamper evident seal, as well as its remote communication functionality, is supervised by a microcontroller unit (MCU). The MCU uses the RGO-engraved circuitry to physically implement a compressive sampling acquisition procedure. The compressive sampling scheme provides the seal with self-authentication and self-state-of-health awareness capabilities. The prototype shows potential for use in low-power, embedded, remote-operation non-proliferation security related applications.

Keywords: tamper evident seal, graphite oxide, compressive sensing, damage detection and classification, sensing skin

(Some figures may appear in colour only in the online journal)

1. Introduction

Tamper evident seals are devices conceived to easily recognize unauthorized access to a protected article. A seal is not designed to offer physical security; instead, its mission consists of providing irreversible traces as proof of penetration [1]. Tamper evident seals are routinely used by the

government and industry to reveal access to secure sites (e.g., hazardous substance storage areas and weapon and ammo depots), certified instruments (e.g., electricity and gas meters and concentration detectors) and, sensitive items (e.g., medicine and bio-specimen containers, certified tools and equipment, such as fire-extinguishers and first-aid kits). Tamper evident seals also play a crucial role in supporting nuclear

safeguards and non-proliferation [2]. In particular, the objective of the International Atomic Energy Agency's (IAEA) safeguards mandate is timely detection of the diversion of a significant quantity of nuclear materials [2]. The IAEA uses seals and containment verification techniques to maintain continuity of knowledge of nuclear material in containers and IAEA facility equipment [2]. The traditional approach adopted by the IAEA consists of sending inspectors to verify the integrity of seals at predefined time intervals. However, current tamper evident seal designs require specialized teams to be onsite for installation and removal. Furthermore, after removal, the seals may need to be processed by multiple labs to ensure accuracy of the seal's assessment [2]. In addition to the unquestionable difficulties related to inspecting thousands of IAEA seals spread across multiple countries, it is worth noting that a Los Alamos National Laboratory (LANL) vulnerability assessment team found that a well-practiced attacker could trivially defeat most tamper evident seals [3].

The tamper evident seal presented in this work aims to offer advantages over conventional seals in terms of the required breach-inspection resources and the potential difficulty associated with their defeat. The novelty of the proposed device lies in combining the strengths of the signal processing technique known as compressive sensing (CS) [4–7] and the tamper-sensitive electrical properties of a graphite oxide (GO) thin-film [8–10] into a highly versatile and reconfigurable architecture controlled and supervised by a microcontroller unit (MCU) [11]. The circuit manufactured on the GO film acts as a sensitive element to detect tampering and, simultaneously, implements a compressive sampling procedure. Specifically, as detailed in the following sections, the reduced graphite oxide (RGO) circuitry is used to build a physical encryption key. CS equips the seal with a low-power means for self-authentication and self-state-of-health awareness. The device expressly takes advantage of the non-bit sensitive encryption capability provided by CS, which is of paramount importance for ensuring correct operation of the seal. Moreover, the non-bit sensitive encryption mechanism, featured by CS, enables the seal to accommodate perturbations to the GO physical encryption key when it is exposed to environmental changes (e.g., temperature and humidity modifications). Therefore, small variations in the parameters used to construct the encryption key will not prevent the seal from correctly detecting if tampering has occurred.

The paper is organized as follows. Section 2 offers a theoretical background on CS and its encryption features. Section 3 describes the architecture behind the seal prototype, explains how the seal works and provides further details about seal manufacturing and testing. Section 4 presents the results from the tests performed on the working seal prototype. Section 5 makes use of simulations to provide insight on the seal's response to perturbations of the physical encryption key. Section 6 offers some more insights on the seal developed by the authors and sketches out possible ways to improve over the current seal's version. Conclusions in section 7 point out how the seal's architecture proposed in

this paper lends itself to applications in the discipline of structural health monitoring (SHM).

2. Theoretical background

As briefed in section 1, the designed tamper evident seal implements a compressive sampling scheme by leveraging the tunable electrical properties of a GO film, which is inherently sensitive to the common tampering attacks discussed in the literature [1–3]. Section 2 offers essential theoretical background information about CS, GO and RGO.

2.1. Compressive sensing

CS, also called compressive sampling, is a signal acquisition protocol that allows one with knowledge of the underlying structure of a general signal to simultaneously sample, compress and encrypt the signal prior to storage or transmission [5, 6]. By leveraging the principles of sparsity and incoherence, one can use CS to recover signals sampled below the Nyquist rate [4, 12, 13]. A signal is considered sparse with respect to some basis if it has a concise representation in that basis, e.g., if there are few non-zero expansion coefficients relative to the dimension of the signal [4, 7, 12, 13]. A signal is sparse if the information it carries is predominantly redundant. Conversely, a signal is said to be incoherent if it has few vanishing expansion coefficients relative to its dimension [4, 12]. For a much more detailed discussion of the protocol, the reader is directed to the literature [4, 7, 12, 13].

To outline the CS protocol, starting with discrete signal $\mathbf{x} \in \mathbb{R}^N$ and sparsifying basis $\Psi \in \mathbb{C}^{N \times N}$, or more generally a dictionary, then the expansion coefficients $s_i \in \mathbb{C}^N$ are given by the decomposition $\mathbf{x} = \Psi \mathbf{s}$. The compressed signal $\mathbf{y} \in \mathbb{R}^M$ is acquired in the linear measurement step $\mathbf{y} = \Phi \mathbf{x}$, where $\Phi \in \mathbb{R}^{M \times N}$ is known as the measurement or sensing matrix. The columns of Φ are populated by waveforms that are incoherent with respect to Ψ , i.e., waveforms that do not have sparse representations in Ψ . As shown previously, matrices populated with Gaussian and Bernoulli random variables make good choices for Φ given any fixed Ψ [4, 12]. The property of sparsity is leveraged by CS in order to solve the ill-posed signal recovery problem by seeking the solution that is most sparse, among the infinite set of candidate signals $\tilde{\mathbf{x}}$ satisfying $\Phi \tilde{\mathbf{x}} = \mathbf{y}$ [14]. The problem is solved by taking advantage of a particular algorithm called basis-pursuit [15]. This algorithm finds the sparsest decomposition of a signal within a dictionary by solving the following convex optimization problem [13]:

$$P_1: \min_{\mathbf{s}} \|\mathbf{s}\|_1 \text{ s. t. } \mathbf{y} = \Phi \Psi \mathbf{s}. \quad (1)$$

The l_1 norm function $\|\cdot\|_1$, defined for a general vector \mathbf{x} occupying \mathbb{R}^N as $\|\mathbf{x}\|_1 = \sum_{i=1}^N |x_i|$, acts as a sparsity-promoting function, i.e., among all the possible decompositions, it leads to the one whose sorted coefficients decay quickly [4, 13, 16]. To solve (1) the YALL1 MATLAB package for l_1 minimization is used [17]. As anticipated, CS also functions

as a shared, or secret, key encryption algorithm. In this manner, the shared key is the measurement matrix Φ , the plaintext is the sampled signal x and the ciphertext is the compressed signal y [18–21].

As it is customary in security analyses of cryptosystems, one can assume that the key is shared across a secure channel between two friends, Alice and Bob, and that an eavesdropper, Eve, cannot access it [5]. It has been shown that CS is computationally secure in response to ciphertext-only attacks, i.e., no practical means is currently known by which Eve can recover the plaintext from only the ciphertext [5, 6]. Furthermore, CS is computationally secure with regard to known plaintext attacks provided one refrains from reusing measurement matrices Φ [6]. Conventional encryption systems may suffer the loss of information in the presence of a noisy channel [6]. Conversely, CS is considered to be robust such that small perturbations of the encryption key manifest as small changes in the ciphertext [6]. This property is unusual for a cryptosystem; indeed, most popular systems are bit-sensitive, and consequently, the integrity of the transmitted information is very much dependent on the integrity of the key [6]. In this sense, CS is said to be non-bit-sensitive. The CS capabilities to simultaneously sample, compress and encrypt, in a non-bit-sensitive fashion, a signal are advantageously exploited to shape the architecture of the developed seal, as presented in section 3.

2.2. GO and RGO

GO is used as a precursor for the inexpensive production of graphene-based materials on a large scale [22–25]. Graphene [8], which was discovered in 2004 [26] and earned its creators the Nobel Prize for physics in 2010, has been studied in tens of thousands of scientific publications. Graphene's excellent mechanical and electrical properties [25, 27, 28] have been exploited to improve performance in a variety of applications [29], among which it is worth mentioning batteries, supercapacitors, broadband communications, solar cells and gas barriers. This paper takes advantage of the techniques developed to prepare graphene starting from GO. GO is rich in oxygen species, creating defects in its electronic structure and nearing an electrically insulating material [9, 30]. A number of reducing methods have been developed to remove these oxygen species and re-establish the carbon network of graphene, which consists of a flat monolayer of carbon atoms tightly packed into a two-dimensional (2D) honeycomb lattice [8]. Among these methods, laser reduction of GO lends itself as an inexpensive process for both reduction and patterning [31–35]. According to [33], laser excitation of GO with different laser sources (e.g., 663 nm continuous-wave laser or 790 nm femtosecond laser) as well as dissimilar atmospheres during the reduction process (e.g., ambient air or N_2) may lead to completely different results [33]. Additionally, definitive evidence of graphene production using some laser techniques is questionable based on the results presented in the literature. Specifically, the evidence for the effectiveness of producing graphene by a laser reduction technique is the presence of a distinct 2D band in the Raman spectra [33]. The

present work does not address this issue. As described in more detail in section 3.2, a CO_2 laser is used to engrave patterns of increased conductivity (i.e., RGO patterns) on a GO film. This work does not provide evidence of graphene production through the analysis of Raman spectra. In this work, the technique of laser irradiating a thin GO film to produce RGO patterns is exploited to engrave circuitry, which is inherently sensitive to humidity [9], high temperatures (e.g., 100 °C [36, 37] or 130 °C [38], above which reduction starts), solvents [22, 25] and mechanical action [39]. The architecture that enables the exploitation of these properties to manufacture a tamper evident seal is addressed in section 3.

3. Seal concept

A tamper evident seal must meet three necessary requirements. It must be susceptible to the common mechanisms used by an attacker to defeat it (see section 2.2), while simultaneously it must be robust to normal environmental variations. It must also be uniquely identifiable. Stated in other words, the seal must undergo an irreversible damage process whenever an attacker tries to temporarily remove the seal and then restore it back to the original configuration. Likewise the seal must guarantee unicity in order to prevent any attempt to replace it with a counterfeit copy.

The authors developed a seal architecture that can arguably meet these three requirements based on the results reported in this paper. The GO film, which is inherently sensitive to common tampering attacks, acts as the support to laser engrave a resistive circuitry. The resistive circuitry is used in combination with a re-programmable MCU in order to equip the seal with the capability to mimic a CS acquisition scheme. As anticipated in section 2.1, CS functions as a shared encryption key which uniquely identifies a particular seal and enables it to encrypt the messages sent back to the remote reader. Tampering with the seal will create a mismatch between the two copies of the encryption key, one embedded into the seal and the other one shared with the remote reader.

This work performs a series of tests on a seal prototype in order to assess the false positive and false negative rate of the seal when the seal is tampered with. The results are discussed in section 4.

Further, a series of numerical simulations are performed in order to quantify at what extent the non-bit-sensitive feature of CS (see section 2.1) enables the remote reader to keep deciphering the messages received from the seal when environmental perturbations (e.g. temperature and humidity changes) affect the electrical properties of the circuitry engraved on the GO seal. The details about the simulation framework developed in this work and the results obtained are collected in section 5.

Although not directly explored in this work, it is worth mentioning that the MCU can be programmed in order to provide a means to securely change the measurement matrix used to perform the compressive sampling procedure (i.e., the encryption key) and the plaintext message encrypted by the seal. Some examples, though not exhaustive, from literature

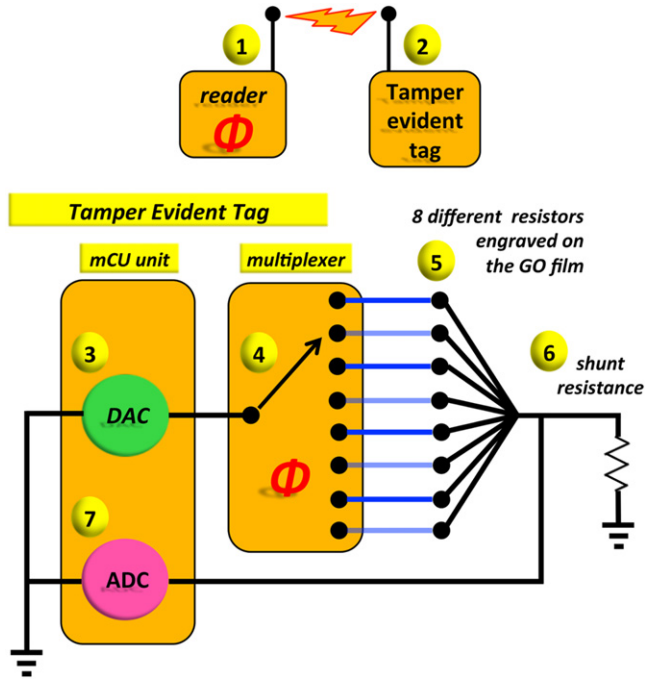


Figure 1. Seal architecture: the communication between the reader (1) and the seal (2) takes place over an unsecure channel. A plaintext message saved in the memory of the microcontroller is converted into an analog voltage via the DAC (3). The DAC sends the signal to the multiplexer (4), which duplicates the switching sequence, Φ , by switching to the appropriate resistor (5) at the correct time. The voltage drop across the resistor is measured across the shunt resistor (6) and converted to a digital sample at the ADC (7). The microcontroller emulates the compressive sensing procedure by keeping a running sum of the digital samples collected for the analog signal generated from the DAC and sent through the multiplexer. The compressed samples are sent back from the tamper evident tag (2) to the reader (1).

[18–21] suggest some approaches that can be adopted to reconfigure the seal for increased security.

3.1. Seal architecture

The seal architecture represented in figure 1 shows the query method used to obtain the status of the seal (element #2, figure 1). For a status query, the signal temporarily saved on the tamper evident seal was parsed by the MCU, after which a voltage signal, corresponding to the signal saved in the memory of the microcontroller, was sent out by the digital to analog converter (DAC) unit (element #3, figure 1) to the multiplexer (MUX) (element #4, figure 1). The MUX specified the particular resistor (element #5, figure 1) to which the voltage was applied across. The MUX used a switching sequence corresponding to particular resistors to determine where to route the voltage. The voltage drop across the shunt resistance (element #6, figure 1) was then measured by the analog to digital converter (ADC) unit (element #7, figure 1).

The voltage across the shunt resistance was used to deduce the voltage across the seal resistor using the voltage divider shown in figure 2. In particular, the relationship between the voltage drop V_{ADC} measured by the ADC unit

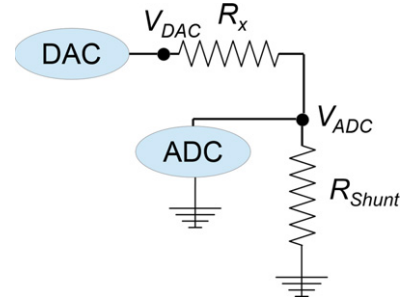


Figure 2. Voltage divider circuit: the voltage in, represented as V_{DAC} , is dropped across both the seal resistor (R_x) and the shunt resistance (R_{shunt}). The voltage out, representing one multiplication in the inner product of the signal and one row of the Φ matrix, is measured by the ADC between the two resistors.

across the shunt resistance R_{shunt} and the voltage V_{DAC} generated by the DAC unit for a given signal sample and sent through a specific resistor R_x can be expressed by the following equation:

$$V_{ADC} = \frac{R_{shunt}}{R_x + R_{shunt}} V_{DAC}. \quad (2)$$

Following complete measurement of the voltage drop, the process was repeated for every sample n among the N available in the signal saved in the memory of the microcontroller. The MCU kept a running sum of the N measured voltage drops until M compressed samples were collected. This process emulated the matrix multiplication between the sparse signal and the $M \times N$ measurement matrix, resulting in a compressed signal. Specifically, the generic element ϕ_{ij} of the equivalent measurement matrix $\Phi_{M \times N}$ associated with the linear projections performed by the seal is equal to

$$\phi_{ij} = \frac{R_{shunt}}{R_{x,ij} + R_{shunt}}, \quad (3)$$

where $R_{x,ij}$ is the value of one (labeled with x) of the eight resistors connected to the multiplexer drawn at random from a uniform distribution for the generic ij element of the measurement matrix Φ , with $i \in [1, M]$ and $j \in [1, N]$. This compressed signal was then sent back to the remote reader (element #1, figure 1) for reconstruction. Tampering with the seal will result in a change in the seal resistances, which will change the effective measurement matrix that is being applied to compress the signal. Therefore, a particular measurement matrix was associated with a unique switching sequence. Additionally, the seal architecture provided flexibility and variability in the components' characteristics. The architecture offered the ability to dynamically select a particular measurement matrix by setting a unique switching sequence. A new switching sequence may be selected at every query if desired. The seal architecture was not constrained to a predetermined sparse signal. The remote reader may use a new sparse signal at every query. The tunable properties of GO provided an additional layer of flexibility within the architecture. These possible variations allowed for a large range of feasible measurement matrices available for

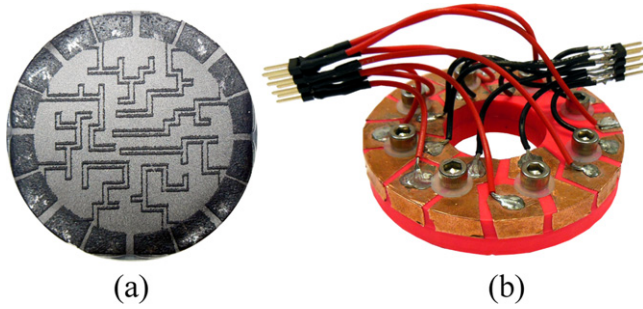


Figure 3. (a) The printed GO seal. The contact pads rim the outside, while the resistive paths meander on the inside. The light gray is indicative of insulating GO, while the darker gray and more textured parts are conductive RGO. (b) The seal container. The GO seal is placed in the central hole, and in the space (not visible) between the two layers of ABS plastic. The copper tape wraps over the outer edge of the upper ABS piece, and down to its underside where it makes contact with the GO seal.

selection. Further details about the actual implementation of the seal are provided in section 3.2.

3.2. Seal implementation details

A solution of GO, prepared according to Hoffmann's method [40], was used to make a 36 mm diameter by 22 μm thick GO film through a vacuum filtration process. This film was then reduced using a 40 W CO₂ Hobby Laser 5th gen manufactured by Full Spectrum Laser. The reduction of the GO film produced RGO, which is electrically conductive, while GO is highly insulating. Using a space-filling, self-avoiding random walk algorithm [41] with eight starting points, eight resistors were designed and printed onto the seal, as shown in figure 3(a). This algorithm created a random path for each resistor, allowing unique seals to be easily fabricated. The random path was space filling; therefore, it was sensitive to cracks or other mechanical damage across the entire surface of the seal exposed to tampering attacks. The algorithm was implemented in MATLAB, and a bitmap image file (.bmp) was generated as output. The picture was then processed using the RetinaEngrave 3D software, which enabled control over the laser raster power (set to 23%) and engraving speed (set to 20%). The path of each resistor was assigned to a different layer. By controlling the number of repeats of each layer, it was possible to generate different resistance values for each RGO path. The RGO path resistance values as measured by the MCU unit connected to the seal are collected in table 1.

The GO seal was held in an acrylonitrile butadiene styrene (ABS) plastic container, fabricated using an additive manufacturing process, as shown in figure 3(b). The plastic container consisted of two identical rings, each 70 mm in diameter with a 28 mm diameter hole in the center, and eight evenly spaced holes around the perimeter, that allow it to be secured together with bolts. The upper container element had copper tape that extends from the underside, where it made contact with the GO seal, to the top, where it was soldered to wires that connected it to the rest of the seal system. The GO

seal was placed between the two container halves, where its outer 4 mm was compressed between the two halves by the securing bolts. This kept the seal in place and ensured proper contact between the seal and the copper tape.

Once the seal was designed and printed, the shunt resistance must be chosen to match the resistance values of the seal. The shunt resistance acted as the second resistance in the voltage divider depicted in figure 2, and as such, it controlled the voltage drop over the measurement resistor. Shunt resistance values too high or too small, compared to the resistors engraved on the GO film, were avoided. If the combination of the RGO and shunt resistor resistances yielded a very small voltage change at the measurement resistor, then seal tampering would result in inappreciable modification of the compressed samples collected by the MCU. In practice, a shunt resistance selected to be between the highest resistance and twice the highest resistance proved to work for this seal. For the seal depicted in figure 3, a calibrated shunt resistance of 159.440 k Ω was selected.

The MCU specifically used for this project was an Atmel ATxmega128A1 unit programmed in C++ using object-oriented techniques to produce a modular code that is extensible and reusable for future implementations. The seal was connected to a computer running MATLAB via a serial port to collect the compressed samples sent back from the seal and perform signal reconstruction. The results of the preliminary tests performed on the seal are reported in section 4.

4. Preliminary test results

A preliminary test series was performed on the seal aiming to demonstrate the effectiveness of the proposed architecture. The tests were performed by having the MCU DAC unit generate a three-period sine wave. The Atmel ATxmega128A1 DAC unit was set to use the accurate internal 1.00 V voltage V_{ref} as reference. Also, the output voltage V_{DAC} from a generic DAC channel is given as

$$V_{\text{DAC}} = \frac{\text{Channel_Data}}{4095} \times V_{\text{ref}}, \quad (4)$$

where Channel_Data is the digital signal ranging in the closed interval [0; 4095]. The microcontroller was compiled to output a full wave rectified sine wave with amplitude ranging from 0 to 0.9 V, such that the DAC does not saturate. During acquisition of the compressed samples, the measured voltage drop across the shunt resistance was added to the running sum with an inverted sign for all those samples that originally belonged to the negative half of the sine wave. Section 4.1 describes how the preliminary tests were carried out and presents upfront the obtained results. Section 4.2 provides further details about seal operation.

4.1. Test description and recovered signal

Preliminary tests of the seal were performed as follow. The acquisition of M compressed samples from the same three-period sine wave described above were repeated 100 times

Table 1. GO seal resistance values.

R_1 (k Ω)	R_2 (k Ω)	R_3 (k Ω)	R_4 (k Ω)	R_5 (k Ω)	R_6 (k Ω)	R_7 (k Ω)	R_8 (k Ω)
95.362	49.558	84.819	44.854	14.029	41.096	30.074	60.020

with all of the resistors connected to the MCU (see figure 4—case #01). Next, the wires leading into the enclosure (see figure 3) were disconnected one at a time to prevent the signal from reaching each resistor on the GO film; therefore, cutting of the resistors was simulated without inflicting damage to the seal. Again, 100 runs were carried out for each case. Figure 4—case #02 shows the results obtained by disconnecting the RGO resistor path #08; figure 4—case #03 shows the measurement collected with RGO resistor path #07 disconnected; and accordingly, cases #04 through #09 report the results obtained after disconnecting the RGO resistor paths from #06 to #01, respectively. Finally, all of the resistors were simultaneously disconnected (see figure 4—case #10), and the seal was kept running 100 times more, simulating a total destruction condition. For each case the reconstruction error was computed according to the following formula:

$$\varepsilon = \frac{\|\mathbf{x}_{\text{recovered}} - \bar{\mathbf{x}}\|_2}{\|\bar{\mathbf{x}}\|_2}, \quad (5)$$

where $\bar{\mathbf{x}}$ is the vector representing the original signal and $\|\cdot\|_2$ is the l_2 norm operator.

As seen in figure 4—case #01, the test case representing an intact seal showed 100 recovered signals with an error approximately ranging from 6% to 18%. The other cases from case #02 to case #09 were affected by a reconstruction error that was consistently above 125% when disconnecting one resistor at a time. For each case, the recovered signals were consistent. Finally, figure 4—case #10 reports the results for disconnection of all RGO paths from the MCU. Case #10 recovered signals exhibited a reconstruction error around 100% with the recovered samples lacking any underlying structure. From these results, important conclusions may be drawn about the implementation of the seal prototype. By setting a reconstruction error threshold to a value lower than that observed in any of the cases where a resistor path was disrupted, it was always possible to correctly distinguish the intact seal condition from the tampered conditions (i.e., with one or all RGO paths disconnected). According to the experimental results, both the false positive and false negative rates were equal to zero. Future work will include a complete assessment of the seal performance, which will require extensive testing including comprehensive documentation of the effect of temperature and humidity by putting the seal both in an oven and in a moisture chamber. Also, long term testing will be required to assess the stability of the electrical properties of the RGO circuitry over time. Such a large-scale testing campaign will require the production of several seals from currently unobtainable necessary resources. Nevertheless, numerical simulation was carried out to quantify both the bit-non-sensitive feature of CS and the seal performance

as a function of perturbations inflicted onto the nominal RGO resistor values. The description and results of the numerical simulations are reported in section 5.

4.2. GO seal implementation details

In accordance with the seal architecture description provided in section 3.1, reconstruction of the original signal starting from the CS samples was performed by running the YALL1 algorithm in MATLAB. Details about the recovery process are provided hereafter. The signal $\bar{\mathbf{x}}$, saved on the MCU memory and generated by the MCU DAC unit, was a three period sine wave defined as

$$\bar{\mathbf{x}} = 0.9 \cdot \sin(3t), \quad (6)$$

where $t = 2\pi(\frac{n}{N})$, with $n \in [0;127]$ and $N = 128$. This type of signal has a naturally sparse representation over a Fourier basis. For this reason, this basis was used as dictionary Ψ to solve equation (1). The resulting Ψ was an $N \times N$ orthonormal basis with the generic k th column given by

$$\psi_k(n) = \frac{1}{\sqrt{N}} e^{-2\pi i k n / N}, \quad 0 \leq n, k \leq N-1, \quad (7)$$

where N is the length of the vector \mathbf{n} .

The measurement matrix used to collect the compressed samples was implemented according to the procedure described in section 3.1. The specific switching sequence, drawn at random from a random uniform distribution in the closed interval $[1; 8]$ and used to obtain the results presented in section 4.1, resulted in sensing matrix $\bar{\Phi}$ (see equation (3)). The YALL1 algorithm became problematic when working with the sensing matrix $\bar{\Phi}$ defined as described above. Specifically, the algorithm was yielding null recoveries (i.e., the expansion coefficients of vector \mathbf{s} , see equation (1), were exhibiting a magnitude in the ball park of 10^{-21}) for nearly 50 recoveries over 100 runs. The null recovery problem was present for all of the cases shown in section 4.1. At the time the authors submitted this paper, they were currently investigating the reason for the difficulty obtaining successful reconstructions. The authors suspect the recovery problem was caused either by the numerical scaling inherent to the nature of their prototype, or the implementation of the measurement matrix was results in measurement matrices that are on the edge of satisfying the restricted isometry property [4]. However, the authors have found a mathematical artifice that has significantly helped circumvent the null recovery problem. First, the columns of the measurement matrix $\bar{\Phi}$ were normalized as follows. Letting $\bar{\Phi}_{\text{norm}}$ be the matrix resulting from normalization, then the $\bar{\Phi}_{\text{norm}}$ matrix was obtained by

$$\bar{\Phi}_{\text{norm}} = \bar{\Phi} / \|\bar{\Phi}_1\|, \quad (8)$$

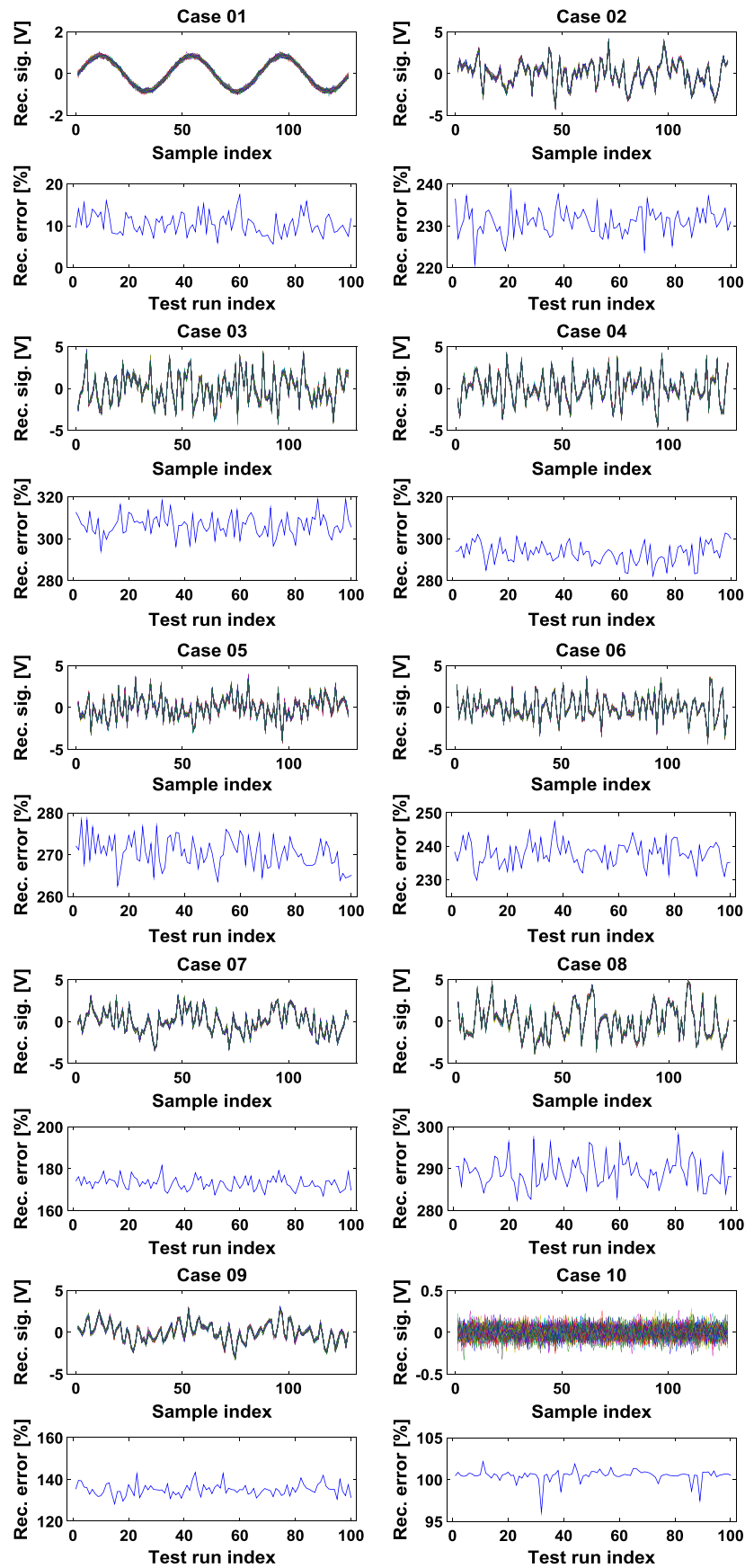


Figure 4. Results obtained from the preliminary tests performed on the seal. Reconstructed signal and reconstruction error are displayed. Case 01: all of the resistors connected; cases 02 through 09: resistors from #8 to #1 respectively disconnected; case 10: all of the resistors simultaneously disconnected.

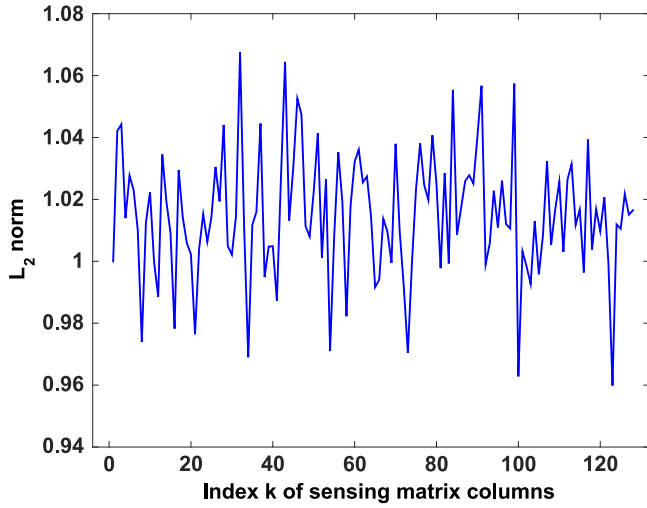


Figure 5. l_2 norm computed for the columns of the normalized sensing matrix $\bar{\Phi}_{\text{norm}}$.

where $\|\bar{\Phi}_1\| \approx 4.2731$ is the l_2 norm of the first column of matrix $\bar{\Phi}$. As observed in figure 5, the operation performed according to equation (8) enabled the formation of a new measurement matrix $\bar{\Phi}_{\text{norm}}$ whose columns had an approximately unitary norm.

Second, the l_1 norm minimization problem of equation (1) has been slightly changed to

$$P_1: \min_s \|s\|_1 \text{ s. t. } \hat{y} = \bar{\Phi}_{\text{norm}} \Psi s, \quad (9)$$

where \hat{y} is a modified version of the compressed samples vector y (see section 2.1), obtained as

$$\hat{y} = \bar{\Phi}_{\text{norm}}(\bar{x} + \bar{c}), \quad (10)$$

where \bar{c} , with dimensions $N \times 1$, is an arbitrary constant vector and $\bar{\Phi}_{\text{norm}}$ is the normalized sensing matrix as defined in equation (8). Third, the first data set from the compressed measurements y_1 collected for case #01 (see section 4.1) was selected to repeatedly solve the minimization problem of equation (9) for

$$\hat{y} = \frac{y_1 + \bar{\Phi}_1 \bar{c}}{\|\bar{\Phi}_1\|}, \quad (11)$$

where the elements of the constant vector \bar{c} have been increased at each iteration from an initial value of 0.01 to a final value of 10.00 by steps of 0.01. Once the expansion coefficients s were retrieved from solving equation (9) the recovered signal was finally obtained as

$$x_{\text{recovered}} = \Psi s - \bar{c}. \quad (12)$$

For the 1000 simulations performed, the reconstruction error was computed according to equation (5). The reconstructed signals are collected in figure 6(a), and the reconstruction error is presented in figure 6(b). As observed in figure 6(a), null recoveries could be avoided by adding the arbitrary constant vector \bar{c} . Further, for arbitrary constants in

the interval $[0.01; 1.50]$, the reconstruction error remained approximately between 9% and 10%. According to these results, a constant vector \bar{c} populated with elements equal to 0.6 was used to perform all of the reconstructions presented in section 4.1 and successive sections.

The results presented thus far show how the seal prototype can correctly detect a tampered state corresponding to a seal damaged by disconnecting one RGO resistor at a time or by disconnecting all of the RGO resistors. Section 5 will introduce a simulation framework used to quantify how the bit non-sensitive feature of CS can accommodate perturbations of the encryption key.

5. Numerical simulations

This section presents a simulation framework that enables the study of how perturbations of the RGO resistor values modified the compressed samples collected by the seal and how the perturbations affected the reconstruction quality of the original signal. The architecture depicted in figure 1 shows that both the ADC and DAC units are exploited to implement the CS scheme on the seal. Therefore, the noise affecting the samples generated by the DAC and acquired by the ADC entered the entire process. Figure 7 shows the voltage measured from the ADC unit for an increasing voltage output generated from the DAC unit; the insert provides a zoomed view which enables to appreciate the DAC to ADC loop noise. According to the data, the noise affecting the DAC to ADC loop is estimated to be 10 times the resolution of the ADC/DAC units.

A simulation framework was created to reproduce the compressive sampling scheme implemented on the seal and depicted in figure 1. Specifically, simulations were performed using the same measurement matrix $\bar{\Phi}$ used on the seal, and the DAC to ADC loop noise exhibited by the MCU was introduced. Validation of the simulation framework is presented in section 5.1.

5.1. Simulation framework validation

For validation purposes, the simulation framework was used to reproduce the results presented in section 4.1. Specifically, 100 simulation runs were performed for each case presented in section 4.1. For every simulation run, random noise with a standard deviation equal to 10 times the resolution of the ADC/DAC units was added to the samples to build up the running sum and obtain the compressed samples y_{sim} . For the purpose of clarity the compressed samples obtained from the operating seal and presented in section 4.1 are addressed in this section as y_{op} . In order to synthetically compare the results obtained from the simulation framework with those obtained by the operating seal a correlation statistic parameter, namely the sample covariance cov, was computed. Specifically, the sample covariance cov was computed between the compressed samples $y_{\text{base}} = \bar{\Phi} \bar{x}$ computed for the intact seal—with $\bar{\Phi}$ and \bar{x} respectively defined in

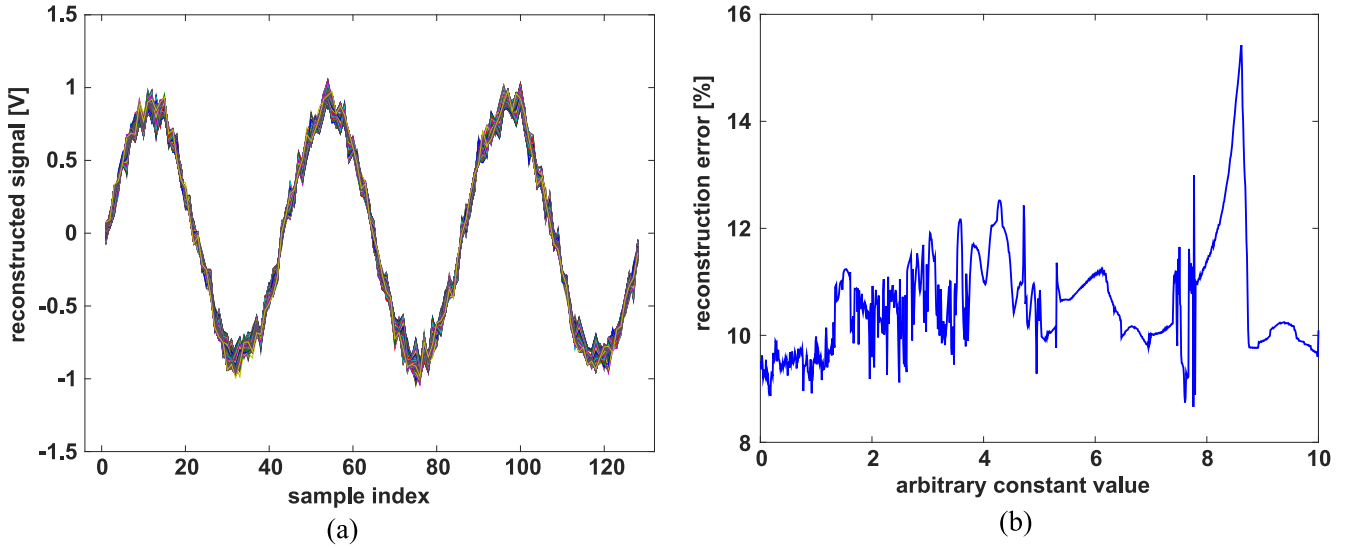


Figure 6. (a) Reconstructed signal and (b) reconstruction error obtained by solving the problem P_1 of equation (9) with the arbitrary constant \bar{c} ranging in the interval $[0.01; 10.00]$ using a step size of 0.01.

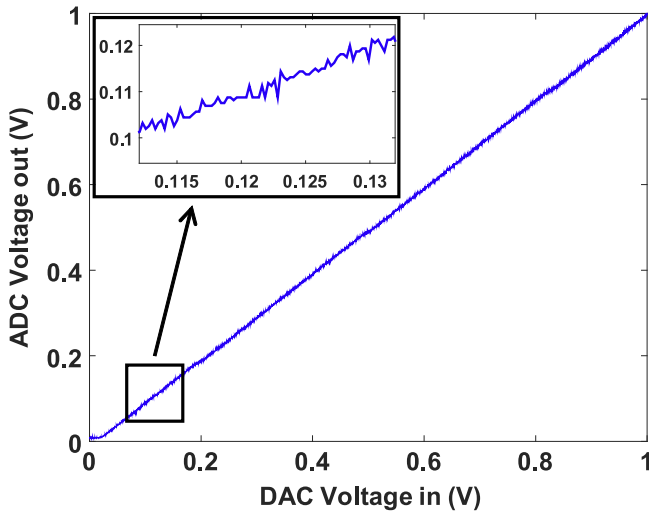


Figure 7. Noise affecting the DAC to ADC loop.

equations (3) and (6)—and the compressed samples y according to the following formula:

$$\text{cov} = \frac{1}{M-1} \sum_{i=1}^M \left[(y_{\text{base},i} - \bar{y}_{\text{base}}) \cdot (y_i - \bar{y}) \right], \quad (13)$$

where M is the number of compressed samples, \bar{y}_{base} and \bar{y} respectively are the mean values of the compressed samples y_{base} and y . The covariance cov is computed using $y = y_{\text{sim}}$ for the compressed samples obtained from the simulation framework and using $y = y_{\text{op}}$ for the compressed samples obtained from the operating seal. Figure 8 shows and compares the convex hulls computed for the set of points defined by the coordinates $[\text{cov}, (1 - \rho)^3]$, where ρ is the correlation coefficient defined as $\rho = \text{cov} / (\sigma_{y_{\text{base}}} \cdot \sigma_y)$ with $\sigma_{y_{\text{base}}}$ and σ_y representing the standard deviations of y_{base} and y . The x -axis in figure 8 represents the correlation statistic cov , while the y -axis represents $(1 - \rho)^3$. The convex hulls encompassing the compressed samples acquired from the

operating seal and those obtained through the simulation framework are shown in figures 8(a) and (b), respectively. Both of the plots show that the convex hulls representative of a damaged condition (i.e., with one or all the resistors disconnected) are located in positions distinct from the one occupied by the convex hull associated with the intact seal. Figure 8(c) facilitates better comparison of the results presented in figures 8(a) and (b). The positions of the convex hulls and their extensions are comparable for both the experimental and numerical cases. Based on the results shown in figure 8, the simulation framework developed by the authors can be considered validated. It follows that the simulation framework is deemed to possess an acceptable level of accuracy to numerically generate compressed samples that can be used to study the behavior of the real seal.

The simulation framework developed thus far was used to better understand what happens to the seal when perturbations are applied to its resistors' values; simulations and results are discussed in section 5.2.

5.2. How perturbations affect the seal's resistor impact on reconstruction quality

The simulation framework, validated in section 5.1, enabled quantification of the bit non-sensitive feature of the CS scheme implemented on the GO seal. 100 simulation runs were performed by introducing the perturbations listed in table 2 to all RGO resistors simultaneously.

The results of the simulations are collected in figure 9 (positive perturbations and unperturbed cases) and figure 10 (negative perturbations cases). After doubling all of the resistor values concurrently (see case 101, figure 9), the reconstruction error never exceeds 40%. For smaller positive perturbations the reconstruction error decreases (see case 102 through 106, figure 9). The reconstruction error approximately oscillates around 20% for case 102

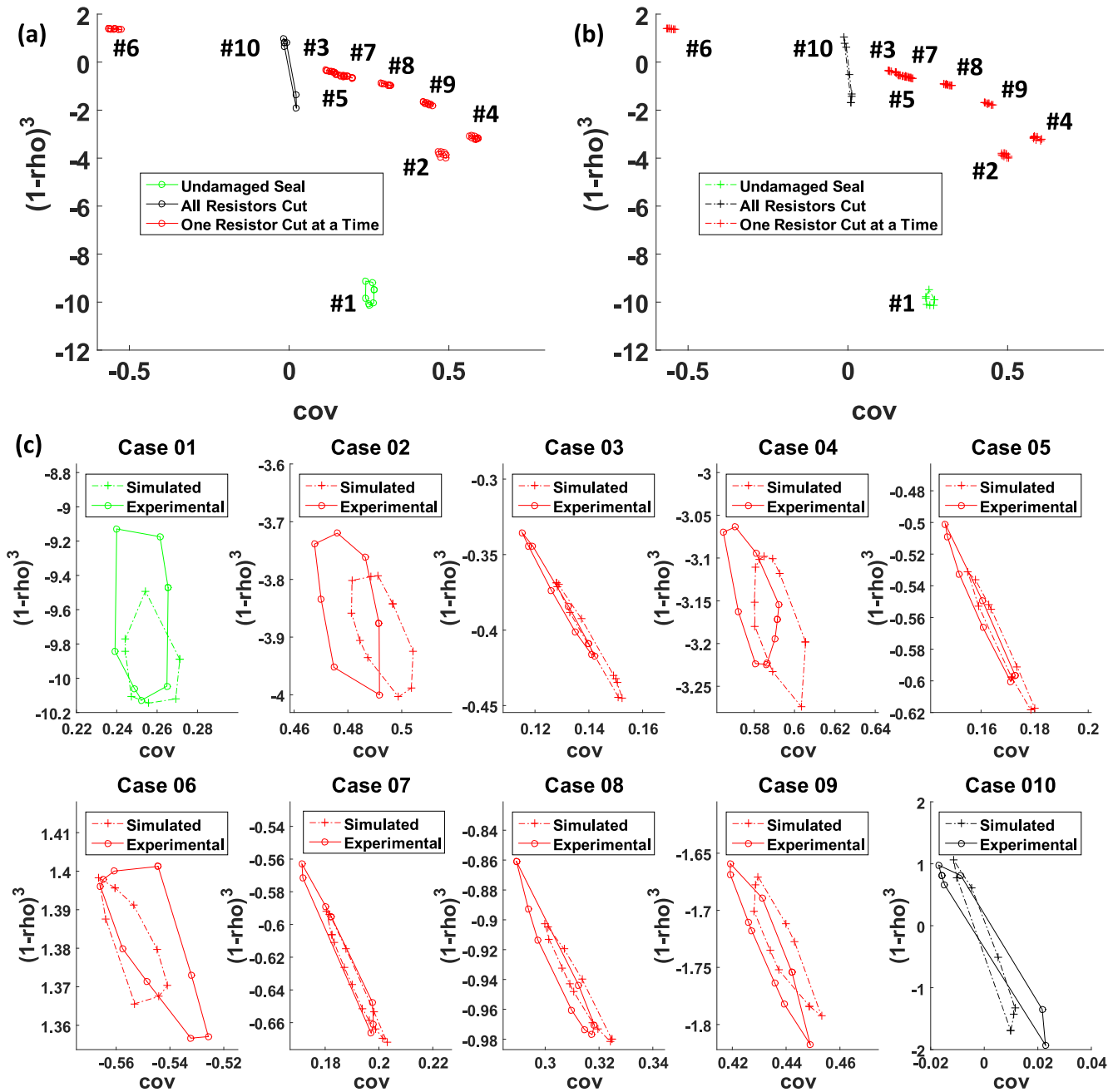


Figure 8. Convex hulls encompass the data for cases from #01 to #10, relative to (a) data acquired on the GO seal, (b) data simulated and (c) comparison between the two.

Table 2. Small and large perturbations applied to the RGO resistors.

Case	Perturbation	Case	Perturbation
101	+100%	108	-1%
102	+50%	109	-2.5%
103	+10%	110	-5%
104	+5%	111	-10%
105	+2.5%	112	-50%
106	+1%	113	-99%
107	0%		

(i.e. resistors' perturbation of +50%) and around 10% for all the other positive perturbation cases considered.

Further, the unperturbed case (see case 107, figure 9) compares favorably with the reconstruction error obtained for the real GO seal tested when it was intact (see case 01, figure 4). This correlation further proved that the simulation framework developed in section 5 was effective.

As far as the negative perturbations are concerned, for small perturbations (below 10%), the reconstruction error never exceeds 30% (see cases 108 through 111, figure 10). For very large perturbations (-50% and -99%, see cases 112

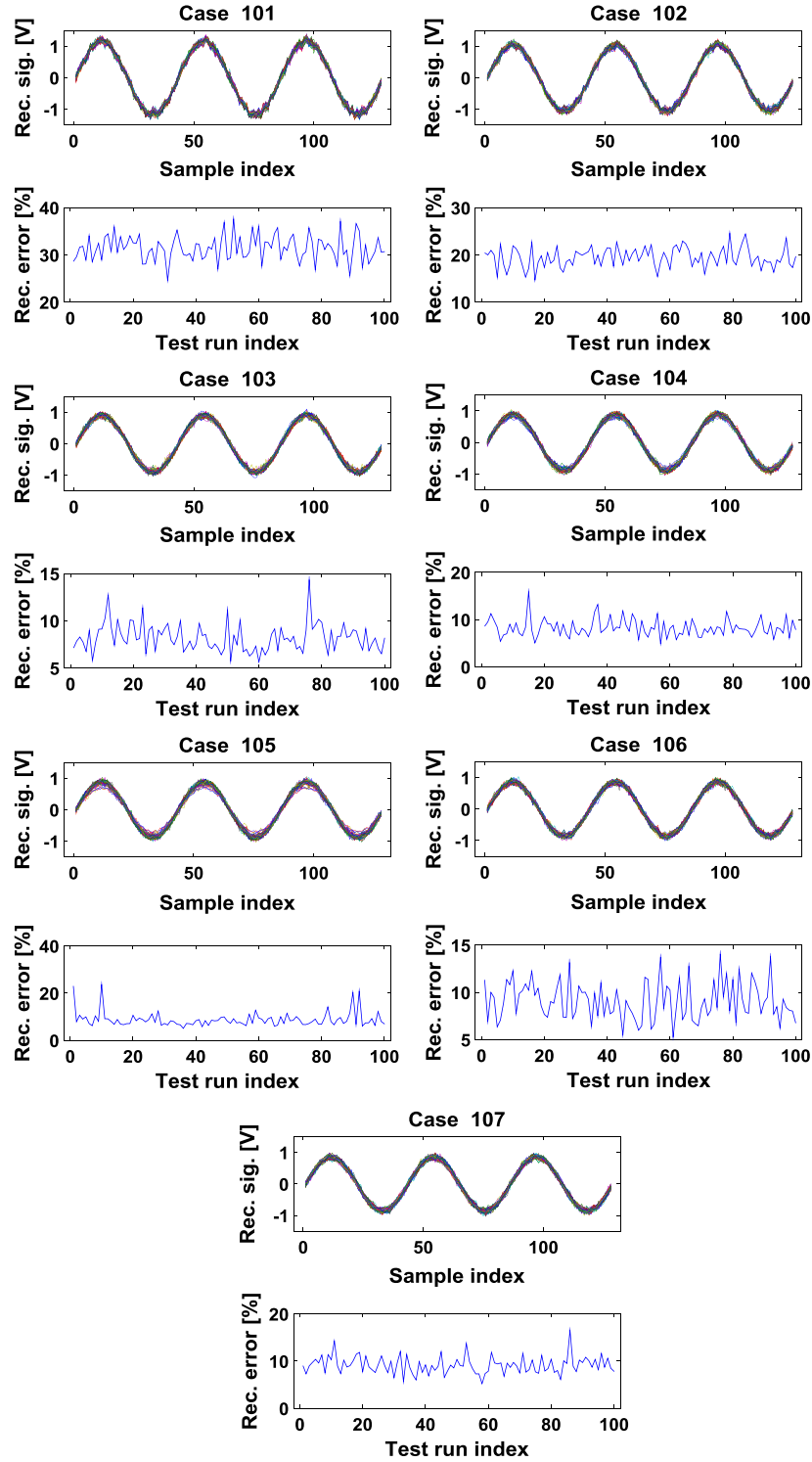


Figure 9. Results for the positive perturbations and the unperturbed cases listed in table 2. Reconstructed signal and reconstruction error are displayed.

and 113, figure 10), the reconstruction error ramps up to almost 50% and 100%, respectively. For case 113, the reconstructed signal no longer matches the original sinusoid.

The results presented in the current section proved that the CS non-bit-sensitive feature made the seal particularly

robust to percentage variations affecting all seal resistors simultaneously. These applied perturbations are believed to be representative of variations induced by environmental changes (e.g., temperature and humidity). Further experiments are required to validate this hypothesis.

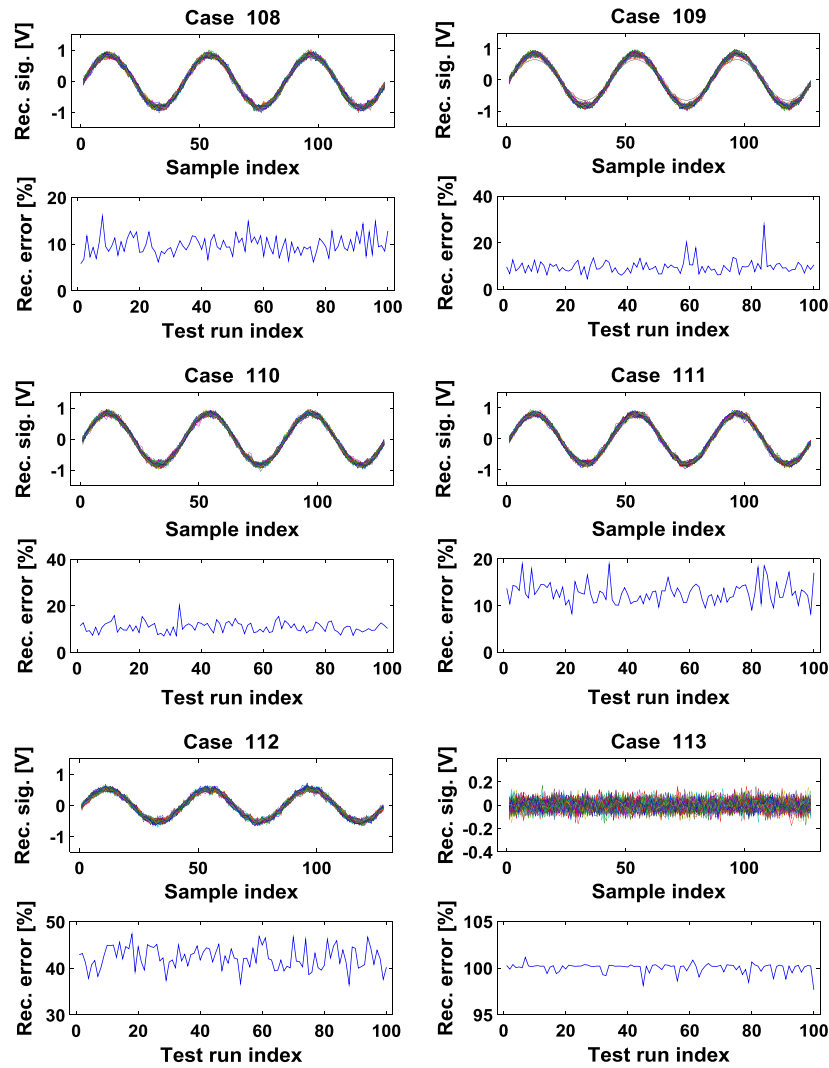


Figure 10. Results for the negative perturbations listed in table 2. Reconstructed signal and reconstruction error are displayed.

6. Further considerations about the seal

The authors are aware that the design and implementation of a tamper evident seal involves many nuances. As already deliberated in section 3, a tamper evident seal must be capable of remaining intact while experiencing ordinary environmental conditions expected to occur over the seal's service life. Concurrently, a seal must become irreversibly damaged when exposed to a malicious attack. Considering these essential factors, additional properties exclusive to this seal are worth mentioning. This seal's architecture relies on a compressive sampling scheme that makes use of resistive patterns engraved on GO paper. One possible mechanism an attacker could use to defeat the GO paper-based tamper evident seal may consist of gaining access to the resistor values of the GO pattern and replacing the original GO pattern with an array of resistors whose values are close to the original ones. Furthermore, an exact estimation of the original GO resistor values may not be necessary due to the non-bit sensitive feature inherent to CS. An interesting property that makes GO a material suitable for the tamper evident seal



Figure 11. Damage induced by a multimeter probe on GO paper during an attempt to measure its resistive value.

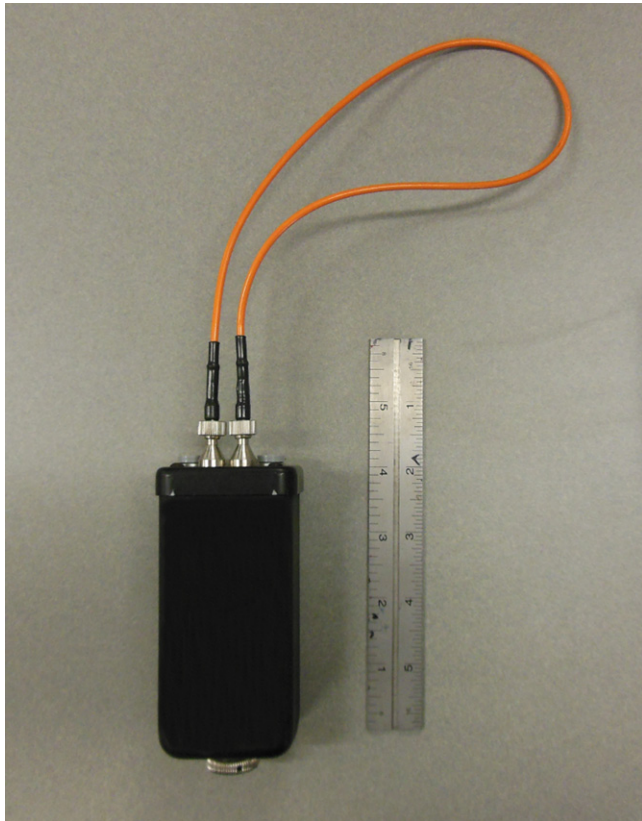


Figure 12. Example of electronic seal loop on the market.

developed in the current work is that GO paper is irreversibly altered by simply positioning a multimeter probe on top of it. Figure 11 shows an example of the damage generated on GO paper when it is probed with a multimeter. In the author's experience with GO paper material, the damage induced by the multimeter probe tip has the potential to produce a change in the resistance reading. Consequently, an attack aiming at disassembling the seal to measure the GO pattern resistance values is unlikely to be effective. To increase the potential of damaging the seal during an attempt to measure the GO paper resistance values, a simple solution may consist of covering the GO paper with a layer of epoxy. This additional coverage would make it almost impossible for an attacker to gain access to the GO paper (e.g., drilling the seal) without inducing severe damage.

The authors explored the possibility of replacing traditional paper-based tamper evident seals with a new architecture that combines the unique properties of CS with GO. The novelty of the current work consists of using the resistive elements engraved on a GO-based tamper evident seal to physically implement the random linear measurement process, which is the basis of CS. A specifically engineered solution will be needed to address the differing currently available seal technologies; however, virtually any of these technologies can benefit from the proposed architecture. For example, without being exhaustive, electronic seal loops on the market (see figure 12) can be improved using the architecture developed by the authors. Multiple GO conductive elements, with different resistance values, can be embedded

into the seal loop and connected to a MCU. Any attempt to cut through the loop or gain access to the GO conductive elements in order to read their resistive values is likely to fail.

The inherent sensitivity of GO's tunable electrical properties to tampering attacks has made such a material an ideal candidate for the development of an innovative paper-based tamper evident seal. The GO paper used to build the prototype described in the current work was produced at a relatively low cost due to the authors' affiliation with the Center for Integrated Nanotechnologies at LANL. A couple of considerations are worth noting with regards to cost efficiency. First, the fabrication and electrical tuning process of GO-paper may be adapted to large-scale production in order to further reduce costs. Second, the ongoing research in the field of tunable electrical materials sensitive to tampering/electrical probing attacks may help improve the prototype's current version.

Finally, some further remarks about CS are worth mentioning. Following the seminal works of Donoho and Candès [4, 12], huge efforts have been made to explore this field both in terms of applications and theorems capable of bounding the performance of CS. Many of these performance-bounding theorems are based on the assumption that Gaussian or other random matrices are used to accomplish the linear measurement process. Implementing such sensing matrices on real circuits may be impractical. Therefore, different approaches have been developed, such as using CS matrices consisting of Toeplitz and circulant structures [42, 43], deterministic matrices [44–46], sampling matrices that can be applied to binary sparse signals, and algorithms that show promise in recovering signals from 1-bit measurements. The aforementioned approaches may help to improve the results presented in this paper. A more thorough study of these approaches is required in order to understand how they behave with respect to the non-bit sensitivity and encryption properties explored in the current work. Of particular interest is using sampling matrices that can be applied to binary sparse signals [47] and the 1-bit CS technique [48, 49]. The former may enable the use of binary signals, eliminating the use of DAC and ADC units; the latter should still enable measurement of analog signals by simply requiring an inexpensive comparator.

7. Conclusions

This work proved that a tamper evident seal made from a thin GO film could be successfully realized. The GO seal physically implemented the secret encryption key of a compressive sampling acquisition scheme in order to achieve self-state awareness and self-authentication capabilities. The tests performed on the working prototype showed that tampering attempts resulting in the total destruction of one RGO resistor path at a time and of all RGO resistor paths simultaneously could always be correctly detected. Both the false positive and false negative rates of the seal were equal to 0. A simulation framework was developed to better understand the behavior of the seal, specifically, the effect of perturbations on the resistive properties of the RGO paths engraved on the

seal. According to the results, the seal showed the capability to maintain a reconstruction error within 30% for perturbations inflicted on the RGO resistor paths ranging from -10% to $+50\%$. These results showed the potential for the seal to correctly operate when exposed to operational conditions that it may encounter when used in real applications, permitted by the bit non-sensitive feature of the compressive sampling acquisition scheme.

From a broader viewpoint, this work demonstrated how material science and signal processing techniques could be successfully fused to create devices capable of detecting a damaged state. Using appropriate materials, the proposed architecture could virtually open a new field for SHM related applications.

Acknowledgments

The authors would like to acknowledge the support of the Los Alamos National Laboratory—Laboratory Directed Research and Development program. Grant number 20130527ER. The authors acknowledge also the United States Department of State. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the particular funding agency.

References

- [1] Johnston R G 2001 Tamper detection for safeguards and treaty monitoring: fantasies, realities, and potentials *Nonproliferation Rev.* **8** 102–15
- [2] Doyle J E 2008 *Nuclear Safeguards, Security, and Nonproliferation: Achieving Security With Technology and Policy* (Amsterdam: Elsevier/Butterworth-Heinemann)
- [3] Johnston R G 2003 Tamper-indicating seals: practices, problems, and standards *Los Alamos National Laboratory Report* LA-UR-03-0269
- [4] Candes E J and Wakin M B 2008 An introduction to compressive sampling *IEEE Signal Process. Mag.* **25** 21–30
- [5] Rachlin Y and Baron D 2008 The secrecy of compressed sensing measurements, *Proc. 46th Annual Allerton Conf. on Communication, Control, and Computing (IEEE)* pp 813–7
- [6] Orsdemir A, Altun H O, Sharma G and Bocko M F 2008 On the security and robustness of encryption via compressed sensing *Proc. MILCOM 2008—2008 IEEE Military Communications Conf.* pp 1–7
- [7] Candès E J, Eldar Y C, Needell D and Randall P 2011 Compressed sensing with coherent and redundant dictionaries *Appl. Comput. Harmon. Anal.* **31** 59–73
- [8] Geim A K and Novoselov K S 2007 The rise of graphene *Nat. Mater.* **6** 183–91
- [9] Gao W, Singh N, Song L, Liu Z, Reddy A L M, Ci L, Vajtai R, Zhang Q, Wei B and Ajayan P M 2011 Direct laser writing of micro-supercapacitors on hydrated graphite oxide films *Nat. Nanotechnol.* **6** 496–500
- [10] Marcano D C, Kosynkin D V, Berlin J M, Sinitskii A, Sun Z, Slesarev A, Alemany L B, Lu W and Tour J M 2010 Improved synthesis of graphene oxide *ACS Nano* **4** 4806–14
- [11] Atmel Corporation 2012 AVR XMEGA A Manual, revision I (www.atmel.com/devices/atxmega128a1.aspx)
- [12] Donoho D L 2006 Compressed sensing *IEEE Trans. Inf. Theory* **52** 1289–306
- [13] Eldar Y C and Kutyniok G 2012 *Compressed Sensing: Theory and Applications* (New York: Cambridge University Press) p 555
- [14] Elad M 2007 Optimized projections for compressed sensing *IEEE Trans. Signal Process.* **55** 5695–702
- [15] Chen S S, Donoho D L and Saunders M A 1998 Atomic decomposition by basis pursuit *SIAM J. Sci. Comput.* **20** 33–61
- [16] Rubinstein R, Bruckstein A M and Elad M 2010 Dictionaries for sparse representation modeling *Proc. IEEE* **98** 1045–57
- [17] Yang J and Zhang Y 2009 Alternating direction algorithms for ℓ_1 -problems in compressive sensing *SIAM J. Sci. Comput.* **33** 250–78
- [18] Dautov R and Tsouri G R 2013 Establishing secure measurement matrix for compressed sensing using wireless physical layer security *ICNC: Int. Conf. on Computing, Networking and Communications (IEEE)* pp 354–8
- [19] Lin G-S, Chang H T, Lie W-N and Chuang C-H 2003 Public-key-based optical image cryptosystem based on data embedding techniques *Opt. Eng.* **42** 2331
- [20] Sreedhanya A V and Soman K P 2013 Ensuring security to the compressed sensing data using a steganographic approach *Bonfring Int. J. Adv. Image Process.* **3** 01–07
- [21] George S N and Deepthi P P 2013 PWLCM based image encryption through compressive sensing 2013 *IEEE Recent Advances in Intelligent Computational Systems* pp 48–52
- [22] Compton O C and Nguyen S T 2010 Graphene oxide, highly reduced graphene oxide, and graphene: versatile building blocks for carbon-based materials *Small* **6** 711–23
- [23] Dikin D A, Stankovich S, Zimney E J, Piner R D, Dommett G H B, Evmenenko G, Nguyen S T and Ruoff R S 2007 Preparation and characterization of graphene oxide paper *Nature* **448** 457–60
- [24] De S, King P J, Lotya M, O'Neill A, Doherty E M, Hernandez Y, Duesberg G S and Coleman J N 2010 Flexible, transparent, conducting films of randomly stacked graphene from surfactant-stabilized, oxide-free graphene dispersions *Small* **6** 458–64
- [25] Dreyer D R, Todd A D and Bielawski C W 2014 Harnessing the chemistry of graphene oxide *Chem. Soc. Rev.* **43** 5288–301
- [26] Novoselov K S, Geim A K, Morozov S V, Jiang D, Zhang Y, Dubonos S V, Grigorieva I V and Firsov A A 2004 Electric field effect in atomically thin carbon films *Science* **306** 666–9
- [27] Zhang Y, Tan Y-W, Stormer H L and Kim P 2005 Experimental observation of the quantum Hall effect and Berry's phase in graphene *Nature* **438** 201–4
- [28] Lee C, Wei X, Kysar J W and Hone J 2008 Measurement of the elastic properties and intrinsic strength of monolayer graphene *Science* **321** 385–8
- [29] Brumfiel G 2009 Graphene gets ready for the big time *Nature* **458** 390–1
- [30] Jung I, Dikin D A, Piner R D and Ruoff R S 2008 Tunable electrical conductivity of individual graphene oxide sheets reduced at 'low' temperatures *Nano Lett.* **8** 4283–7
- [31] Abdelsayed V, Moussa S, Hassan H M, Aluri H S, Collinson M M and El-Shall M S 2010 Photothermal deoxygenation of graphite oxide with laser excitation in solution and graphene-aided increase in water temperature *J. Phys. Chem. Lett.* **1** 2804–9
- [32] Huang L, Liu Y, Ji L-C, Xie Y-Q, Wang T and Shi W-Z 2011 Pulsed laser assisted reduction of graphene oxide *Carbon* **49** 2431–6
- [33] Sokolov D A, Shepperd K R and Orlando T M 2010 Formation of graphene features from direct laser-induced reduction of graphite oxide *J. Phys. Chem. Lett.* **1** 2633–6

- [34] Zhang Y, Guo L, Wei S, He Y, Xia H, Chen Q, Sun H-B and Xiao F-S 2010 Direct imprinting of microcircuits on graphene oxides film by femtosecond laser reduction *Nano Today* **5** 15–20
- [35] Zhou Y, Bao Q, Varghese B, Tang L A L, Tan C K, Sow C-H and Loh K P 2010 Microstructuring of graphene oxide nanosheets using direct laser writing *Adv. Mater.* **22** 67–71
- [36] Wu X, Sprinkle M, Li X, Ming F, Berger C and de Heer W 2008 Epitaxial-graphene/graphene–oxide junction: an essential step towards epitaxial graphene electronics *Phys. Rev. Lett.* **101** 026801
- [37] Mattevi C, Eda G, Agnoli S, Miller S, Mkhoyan K A, Celik O, Mastrogiorganni D, Granozzi G, Garfunkel E and Chhowalla M 2009 Evolution of electrical, chemical, and structural properties of transparent and conducting chemically derived graphene thin films *Adv. Funct. Mater.* **19** 2577–83
- [38] Wei Z et al 2010 Nanoscale tunable reduction of graphene oxide for graphene electronics *Science* **328** 1373–6
- [39] Sharp N, Kuntz A, Brubaker C, Amos S, Gao W, Gupta G, Mohite A, Farrar C and Mascareñas D 2014 A bio-inspired asynchronous skin system for crack detection applications *Smart Mater. Struct.* **23** 055020
- [40] Poh H L, Šaněk F, Ambrosi A, Zhao G, Sofer Z and Pumera M 2012 Graphenes prepared by Staudenmaier, Hofmann and Hummers methods with consequent thermal exfoliation exhibit very different electrochemical properties *Nanoscale* **4** 3515–22
- [41] Madras N and Slade G 2013 *The Self-Avoiding Walk* (New York: Springer)
- [42] Haupt J, Bajwa W U, Raz G and Nowak R 2010 Toeplitz compressed sensing matrices with applications to sparse channel estimation *IEEE Trans. Inf. Theory* **56** 5862–75
- [43] Rauhut H, Romberg J and Tropp J A 2012 Restricted isometries for partial random circulant matrices *Appl. Comput. Harmon. Anal.* **32** 242–54
- [44] Li S, Gao F, Ge G and Zhang S 2012 Deterministic construction of compressed sensing matrices via algebraic curves *IEEE Trans. Inf. Theory* **58** 5035–41
- [45] DeVore R A 2007 Deterministic constructions of compressed sensing matrices *J. Complex* **23** 918–25
- [46] Duarte M F and Eldar Y C 2011 Structured compressed sensing: from theory to applications *IEEE Trans. Signal Process.* **59** 4053–85
- [47] Nakarmi U and Rahnavard N 2012 BCS: Compressive sensing for binary sparse signals *Proc. MILCOM 2012–2012 IEEE Military Communications Conf.* pp 1–5
- [48] Boufounos P T and Baraniuk R G 2008 1-bit compressive sensing *Proc. 42nd Annual Conf. on Information Sciences and Systems (IEEE)* pp 16–21
- [49] Jacques L, Laska J N, Boufounos P T and Baraniuk R G 2013 Robust 1-Bit compressive sensing via binary stable embeddings of sparse vectors *IEEE Trans. Inf. Theory* **59** 2082–102