This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JETCAS.2021.3074938, IEEE Journal on Emerging and Selected Topics in Circuits and Systems

An Energy-efficient Compressed Sensing Based Encryption Scheme for Wireless Neural Recording

Xilin Liu, *Member, IEEE,* Andrew G. Richardson, *Senior Member, IEEE* and Jan Van der Spiegel, *Life Fellow, IEEE*

***Abstract*—This paper presents a compressed sensing (CS) based encryption scheme for wireless neural recording. An ultra-high efficiency was achieved by leveraging CS for simultaneous data compression and encryption. CS enables sub-Nyquist sampling of neural signals by taking advantage of their intrinsic sparsity, while the CS process simultaneously encrypts the data with the sampling matrix being the cryptographic key. To share the key over an insecure wireless channel, we implemented an elliptic-curve cryptography (ECC) based key exchanging protocol. Local key shuffle and updating were adopted to eliminate the risks of potential information leakage. CS was executed in an application-specific integrated circuits (ASIC) fabricated in 180nm CMOS technology. Mixed-signal circuits were designed to optimize the power efficiency of the matrix-vector multiplication (MVM) of the CS operation. The ECC was implemented in a low-power Cortex-M0 based microcontroller (MCU). To be protected from timing attacks, the implementation avoided possible data-dependent branches. A wireless neural recorder prototype has been developed to demonstrate the proposed scheme. The prototype achieved an 8x data rate reduction and a 35x power saving compared with conventional implementation. The overall power consumption of ASIC and MCU was 442μW during the encrypted wireless transmission. The average correlated coefficient between the reconstructed signals and the uncompressed signals was 0.973, while the ciphertext-only attacks (CoA) achieved no better than 0.054 over 200,000 attacks. This work demonstrates a promising data compression and encryption scheme that can be used in a wide range of low-power signal recording systems with security requirements.**

***Index Terms*—Hardware security, compressed sensing, cryptographic circuits, low power, mixed-signal IC, wireless, neural recording.**

I. Introduction

Large-scale neural recording with high energy efficiency and safety is crucial to the growing number of therapies employing closed-loop neurostimulation [1] and neuroprosthetics [2] to treat brain injury and disease. Although the circuits and system community has devoted a considerable amount of effort to improve the performance and power efficiency of neural recording systems, few investigations have been done to mitigate the security risks. In fact, cybersecurity issues have already emerged in FDA-approved medical devices [3]. Medical devices, including neural interfacing devices, pose serious risks from malicious attacks. Compromised neural interfacing devices may not only disclose critical health-related information, but also leave the users vulnerable to life-threatening attacks. Thus, it is urgent to investigate secure neurotechnologies.

Battery-powered wireless neural recording devices are especially vulnerable to malicious attacks, and their restrained energy budget imposes a significant challenge to implementing data encryption. A typical wireless neural recorder consists of the following key blocks: low-noise amplifiers and filters, analog-to-digital converters (ADCs), wireless transmitters, and optional digital signal processing units. Energy-efficient circuit design techniques of each block have been extensively discussed in the literature. For a low-power neural amplifier design with a noise efficiency factor (NEF) of 3, the energy cost is around 0.1nJ/bit [4]. For a low-power ADC design with a Walden figure-of-merit (FoM) of 100fJ/conv-step, the energy cost is around 0.01nJ/bit [5]. For a low-power wireless transceiver design for biomedical applications, an energy cost of 1nJ/bit is typical, while ultra-low power designs with energy costs below 1nJ/bit have also been reported [6–8]. However, the hardware implementation of data encryption standards by application-specific integrated circuits (ASICs) and general-purpose processors typically takes 1nJ/bit and 10nJ/bit, respectively [9–11]. As a result, standard encryption algorithms may not meet the power requirement for direct integration into low-power neural recorders without optimization.

In this work, we proposed a novel encryption scheme for neural recording that achieves ultra-high energy efficiency by leveraging compressed sensing (CS) technique, as illustrated in Fig. 1. The key concept of CS is that a sparse signal can

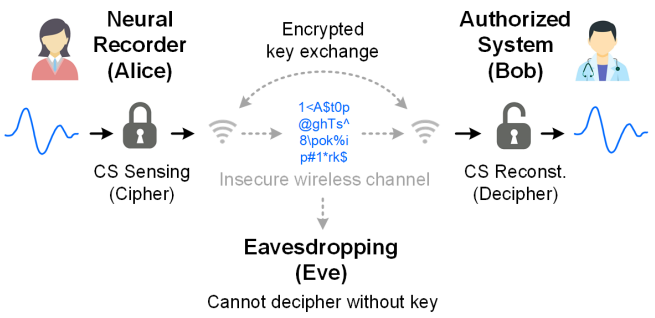

Fig. 1. Illustration of the proposed neural recording system with CS based encryption. The conventional character Alice represents the neural recorder, Bob represents the authorized external system, and Eve represents the illegitimate parties that tend to steal private information by eavesdropping.

Xilin Liu and Jan Van der Spiegel are with the Department of Electrical and Systems Engineering (ESE), University of Pennsylvania, Philadelphia, PA, 19104 USA. E-mail: xilinliu@seas.upenn.edu.

Andrew G. Richardson is with the Department of Neurosurgery, University of Pennsylvania, Philadelphia, PA, 19104 USA.

Digital Object Identifier

be sampled at a reduced rate (below Nyquist frequency) based on the actual amount of information it contains [12]. Neural signals are proven to be sparse in certain domains and pre-learned dictionaries [13–15]. Recent studies have successfully demonstrated highly efficient CS based neural recorder designs [14–20]. Moreover, the CS theory also permits its application in data encryption [21]. It has been proven that CS can provide a computational guarantee of secrecy, provided that an adversary doesn't know the sampling matrix [22]. Recently, several works have explored this property in image processing [23, 24] and internet of things (IoT) applications [25, 26]. We presented in this paper, to the best of our knowledge, the first implementation in neural recording systems.

For CS based encryption to be successfully implemented in a neural recording system, several challenges must be addressed. First, the sampling matrix (i.e. the cryptographic key) must be safely exchanged between the neural recorder and authorized external system. Second, CS sampling is a linear projection process, where the energy features of the signal may be revealed without an accurate decipher [27]. Interception of energy features could be used to disclose age, gender, and potentially other information about the subject, thus, additional mechanisms must be introduced to protect these features. Third, the hardware implementation must be protected from side-channel attacks, such as timing attacks [28, 29]. Last but not least, the overall encryption cannot lead to a significant power penalty. To overcome these challenges, we proposed a novel system that combines an optimized integration of an ASIC and a general-purpose microcontroller (MCU). The ASIC performs mixed-signal CS operations at ultra-low power consumption, while the MCU handles the low duty-cycle key sharing, shuffling, and updating. An elliptic-curve cryptography (ECC) based protocol was implemented in the MCU with time-constant executions. A prototype design using the proposed scheme achieved an 8x data rate reduction and a 35x power saving compared with traditional implementation.

The rest of this paper is organized as follows. Section II describes the operating principles of the proposed system. Section III presents the implementation details. Section IV shows the experimental results. Section V discusses the limitations and future directions. Finally, Section VI concludes the paper.

II. Operating Principles

A. CS for Joint Signal Compression & Encryption

We first briefly review the fundamentals of CS. Suppose the input signal $\mathbf{x}$ has a sparse representation $\mathbf{s}$ on a certain basis $\mathbf{\Psi}$. CS theory predicts that $\mathbf{x}$ can be sampled at a reduced rate (depending on its sparsity) with nearly no information loss. The compressed measurement $\mathbf{y}$ can be expressed as:

$$\mathbf{y} = \mathbf{\Phi x} \tag{1}$$

where $\mathbf{x} \in \mathbb{R}^{N\times 1}$, $\mathbf{y} \in \mathbb{R}^{M\times 1}$, and $\mathbf{\Phi} \in \mathbb{R}^{M\times N}$. Note that $N>M$, and the term N/M is referred to as compression ratio (CR). Although $\mathbf{y}$ cannot be solved directly from Eq. (1), if the sampling matrix $\mathbf{\Phi}$ is incoherent with $\mathbf{\Psi}$ (obeying the restricted isometry property (RIP) [30–32]), the sparse representation $\mathbf{s}$, thus the original signal $\mathbf{x}$, can be solved as a convex optimization problem [31]:

$$\min ||\mathbf{s}||_{0\ (or\ 1)},\ \text{ s.t. } \mathbf{y} = \mathbf{\Phi x} = \mathbf{\Phi \Psi^{-1} s} \tag{2}$$

In this work, we used a $l1$-norm based reconstruction algorithm [12]. It has been proven that a binary random matrix $\mathbf{\Phi}$ consisting of 0 and 1 meets the minimum requirements in fulfilling the incoherent requirement [31]. Prior works showed improved reconstruction performance and resistance to noises by having additional resolution [15, 20]. Here, we adopted a 4-bit $\mathbf{\Phi}$ consisting of elements of {0, ±1/8, ±2/8, ±3/8, ±4/8, ±5/8, ±6/8, ±7/8} following a Gaussian distribution. The hardware implementation will be discussed in Section III-A.

Since the introduction of CS in 2006 [12], many algorithms and techniques have been proposed for improving the reconstruction performance. In addition to the convex optimization based approaches (under different norm regularizations), greedy strategy approximation based algorithms (e.g. orthogonal matching pursuit [33]), dictionary learning [36], adaptive CS [34], as well as deep learning [35] have been proposed to speed up the process of finding the optimal solution. Our objective in this work was not to achieve record-breaking reconstruction performance. Rather, we focused on the hardware design and optimization of the sampling end (i.e. the neural recorder).

The secrecy property of CS has also been rigorously discussed in the literature [21, 22, 37, 38]. Although achieving Shannon's perfect secrecy is conditional [38], computational secrecy can be guaranteed [21]. Encryption algorithms with computational secrecy are commonly adopted in cryptography standards, given that extracting information without the key is a nondeterministic polynomial time problem (NP-problem) [22, 37]. However, since CS sampling is a linear projection process, the energy of $\mathbf{x}$ can be revealed in $\mathbf{y}$ without accurately deciphering the measurement [27]. The energy features of neural signals can contain biometrics and private information of the subject. The information may be leaked to over-the-air eavesdroppers if no additional protection is used.

To mitigate this risk, Chen and colleagues proposed a method of inserting watermarks to mask the energy features [26]. Cambareri and colleagues proposed a multiclass encrypting scheme [39]. In our application of neural recording, we hope not to degrade the reconstructed signal quality or significantly increase the hardware complexity. Thus, we proposed a pseudo-random key shuffle as well as a synchronized key updating for disturbing the energy features. The power penalty of this scheme was negligible in the overall system due to its low active duty cycle.

B. Elliptic-Curve Cryptography and Key Exchanging

There are two types of encryption schemes, known as symmetric encryption and asymmetric encryption [40]. Symmetric encryption uses one key to cipher and decipher the messages. Asymmetric encryption uses a pair of keys: a public key to cipher the messages, and a private key to decipher them. In symmetric encryption, the key must be kept secret once shared

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JETCAS.2021.3074938, IEEE Journal on Emerging and Selected Topics in Circuits and Systems

between the sender and receiver. Conversely, in asymmetric encryption, the public keys are available to all, and the private keys are never shared. Asymmetric encryption avoids sharing private keys at the expense of computation. To reduce the computational cost, we adopted a scheme where the asymmetric encryption algorithm was only used for establishing the secret keys, which were used for CS based symmetric encryption.

Rivest-Shamir-Adleman (RSA) algorithm has been widely used for asymmetric encryption, however, ECC based encryption can achieve the same level of security as RSA with a shorter key length, a lower computation cost, and a lower latency [9]. For example, a 224-bit ECC achieves an equivalent security level of a 2048-bit RSA, which was a security level recommended by the National Institute of Standards and Technology (NIST) in 2015 [41]. In this work, we adopted a 256-bit ECC based key exchanging protocol, namely Elliptic-curve Diffie-Hellman (ECDH) [42]. ECDH is an ECC variant of the classic Diffie-Hellman protocol [43]. ECDH allows two parties to establish a shared secret key independently. The shared secret key can then be used directly or for deriving other keys, which in our case are the CS sampling matrices. The detailed implementation is described in Section III-B.

C. Framework of the Proposed Hybrid Encryption

In a typical scenario of neural signal transmission, the neural recorder (the conventional character Alice) sends the sampled data to the authorized external system (Bob) via a low-power insecure wireless channel. Illegitimate parties (Eve) may steal the messages by eavesdropping. In this work, we adopted a commonly used threat model that Eve knows the encryption algorithms (including the parameters of elliptic curves, field, etc.), the communication protocol, as well as the public keys, but doesn't have access to the unciphered plaintext and the private key (the CS sampling matrices $\mathbf{\Phi_S}$). This is also known as a ciphertex-only attack (CoA) model [26]. Considering the practical use scenarios of wearable or implantable neural recording devices, we assumed that the adversary won't gain physical ownership of the device during its signal transmission, but may non-invasively detect the power profile of the devices (e.g. using electromagnetic approaches) and deduce timing characteristics from power analysis [45]. Finally, the attack range we considered in this work is within a personal area network (PAN), not telecommunication networks.

Fig. 2 illustrates the basic operation principles of the proposed cryptographic neural recording system. The operation procedure is as follows.

1) Alice and Bob first agree on a set of domain parameters (public) for the cryptography, including the parameters of the elliptic curve, the generator point $\mathbf{G}$, etc.;
2) Alice picks a private key $\mathbf{K}_\alpha$ and generates a public key $\mathbf{K_A} = \mathbf{K}_\alpha \circledast \mathbf{G}$, where $\circledast$ is a multiplication defined by ECC; Similarly, Bob picks a private key $\mathbf{K}_\beta$ and generates a public key $\mathbf{K_B} = \mathbf{K}_\beta \circledast \mathbf{G}$;
3) Alice and Bob exchange their public keys $\mathbf{K_A}$ and $\mathbf{K_B}$;
4) Alice and Bob generate a shared secret key $\mathbf{K_s}$ using their own private keys and the public keys provided by the other party:

$$\mathbf{K_s} = \mathbf{K_A} \circledast \mathbf{K}_\beta = (\mathbf{K}_\alpha \circledast \mathbf{G}) \circledast \mathbf{K}_\beta \quad (\leftarrow Bob) \tag{3}$$
$$= \mathbf{K}_\alpha \circledast (\mathbf{G} \circledast \mathbf{K}_\beta) = \mathbf{K}_\alpha \circledast \mathbf{K_B} \quad (\leftarrow Alice) \tag{4}$$

so that Alice and Bob have the same secret key, but Eve cannot get it;
5) Alice and Bob individually generate a set of sampling matrices $\mathbf{\Phi_S}$ using the secret key $\mathbf{K_s}$;
6) Alice performs CS on acquired neural signal $\mathbf{x}$, and sends the lower-dimensional measurement $\mathbf{y}$ to Bob;
7) Bob recovers the neural signal $\mathbf{x}$ from $\mathbf{y}$ by solving optimization problem using $\mathbf{\Phi_S}$;
8) Alice and Bob shuffle the $\mathbf{\Phi_S}$ according to a pre-agreed protocol, and then repeat the CS encryption;
9) To prevent from using the same set of $\mathbf{\Phi_S}$ repeatedly, Alice and Bob would update the $\mathbf{K_S}$ (thus the sampling matrix $\mathbf{\Phi_S}$) periodically on a synchronized manner.

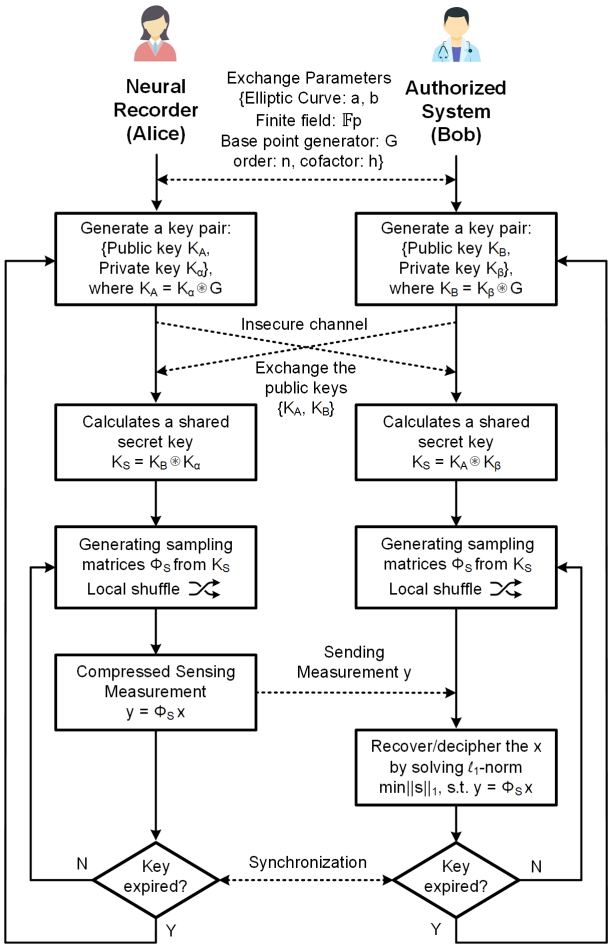

Fig. 2. The operation of the proposed neural recording system. Dashed lines indicate the communication is via an insecure wireless communication channel.

It should be noticed that the encryption scheme implemented in this work doesn't verify identities during the public key exchanging process. The authentication process can be established in various ways, such as implementing the digital signature algorithm [44].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JETCAS.2021.3074938, IEEE Journal on Emerging and Selected Topics in Circuits and Systems

III. System Implementation

The high-level block diagram of the proposed neural recording system (Alice) is shown in Fig. 3. The system mainly consists of an ultra-low power ASIC and a general-purpose MCU. The ASIC executes CS measurements of neural signals using mixed-signal circuits and sends out the measurements using an on-chip wireless transmitter (Tx). The MCU executes the ECC based key exchanging and handshakes with external receivers via a 2.4GHz duplex wireless transceiver (Tx + Rx) for PAN communication. The ASIC design and MCU implementation are discussed in the subsequent sections.

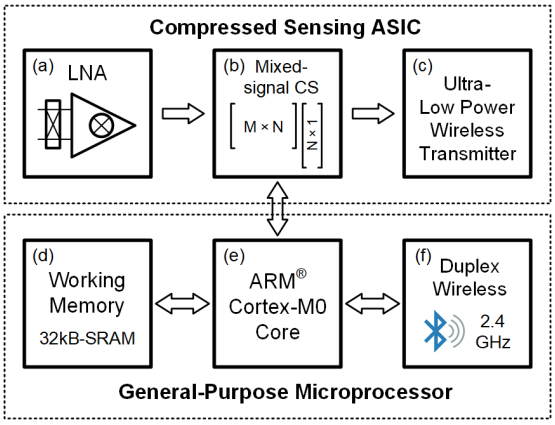

Fig. 3. The high-level block diagram of the proposed system. The system mainly consists of an ultra-low power ASIC for CS (always ON), and a general-purpose Cortex-M0 MCU for ECC based key sharing (low duty cycle).

On the other hand, a computer interfacing device (Bob) has been designed. This device integrates a MCU and corresponding wireless transceivers for pairing with the neural recorder (Alice). A standard USB 2.0 port is integrated for high-speed communication with the computer system. A MATLAB based user interface has been developed for device configuration and data logging [46, 47].

A. ASIC Design for Mixed-Signal CS

The block diagram of the ASIC design is shown in Fig. 4. The ASIC integrates low-noise instrumentation amplifiers (IA) and filters, a programmable gain amplifier (PGA), a successive-approximation register (SAR) ADC, a CS processor, an ultra-low power wireless transmitter, and peripheral circuits including power management units (not shown in the figure). 16-channel IA and filters were integrated for pairing with microelectrode array (MEA), but only one recording channel is used in this work. The IA and wireless transmitter design reuses aspects of our previous work [48–50].

The ASIC design focused on improving the energy efficiency of the CS operation. In particular, the repeated matrix-vector multiplication (MVM) between the input signal $\mathbf{x}$ and the $\mathbf{\Phi}$ dominates the system's power consumption. In this work, we avoided the power and silicon area consuming digital multiplication by using a combination of analog processing and simple digital logic. As discussed in the Section II-A, we adopted $\mathbf{\Phi}$ with a resolution of 4-bit. The common factor of 1/8 among $\{0, \pm 1/8, \pm 2/8, \pm 3/8, \pm 4/8, \pm 5/8, \pm 6/8, \pm 7/8\}$

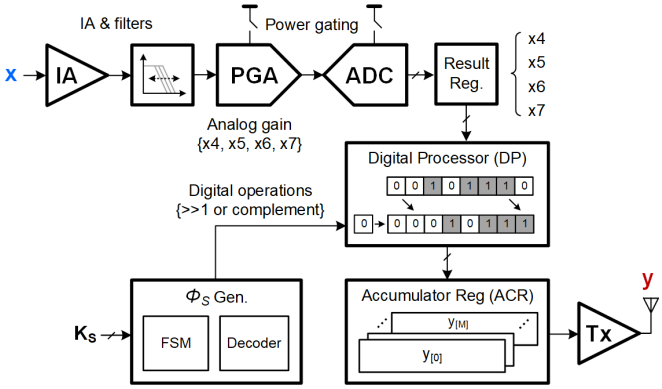

Fig. 4. The block diagram of the mixed-signal ASIC for CS operation.

is combined with the IA gain. Analog gain values of $\{\times 4, \times 5, \times 6, \times 7\}$ are provided by a programmable gain amplifier (PGA) before digitization. Results of $\times 2$ and $\times 3$ are generated by shifting the samples of $\times 4$ and $\times 6$ after digitization by 1-bit to the right ($>>1$), respectively. In this way, power hungry digital multiplication is replaced by simple logic operations. Negative numbers are generated by digital complementation. Table I summarizes the operations. It should be noticed that $\times 1$ was sampled directly bypassing the PGA by default, but it can also be generated by shifting the samples of $\times 4$ by 2 bits.

TABLE I
MIXED-SIGNAL MULTIPLICATION OF $\mathbf{x}$ AND $\mathbf{\Phi}$

	Analog	Digitial	
	PGA gain	Bit shift	Complement
0	- †	-	-
± 1/8 *	-	-	- or (-1)
± 2/8	× 4	>> 1	- or (-1)
± 3/8	× 6	>> 1	- or (-1)
± 4/8	× 4	-	- or (-1)
± 5/8	× 5	-	- or (-1)
± 6/8	× 6	-	- or (-1)
± 7/8	× 7	-	- or (-1)

† '-' indicates no operation required.
* The common factor of 1/8 is combined with the IA gain.

The signal processing flow of the CS measurement is as follows. The neural signal is first amplified and conditioned by the low-noise IA and filters. During an input period of t_i (Fig. 5), the signal x_i is sampled four times in a sequence with PGA gain values of $\{\times 4, \times 5, \times 6, \times 7\}$. The four samples are digitized by the SAR ADC and saved in corresponding registers. The digital processor (DP) processes the samples based on the $\Phi_{i,j}$, where $j \in (1, M)$. The M results are sent to the accumulator registers (ACR) in 16 bits. The ACR adds N samples during one CS measurement (eq. 1).

The input data rate f_x is determined by the bandwidth of the target neural signal. The output data rate f_y is 1/CR of f_x. Given the frequency nature of intracranial EEG signals, the f_x is typically less than 500 Hz [51]. The PGA consists of an operational amplifier with an open-loop gain of 75dB over PVT in simulation. The closed-loop gain of the PGA is set by programmable feedback resistors. The layout of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JETCAS.2021.3074938, IEEE Journal on Emerging and Selected Topics in Circuits and Systems

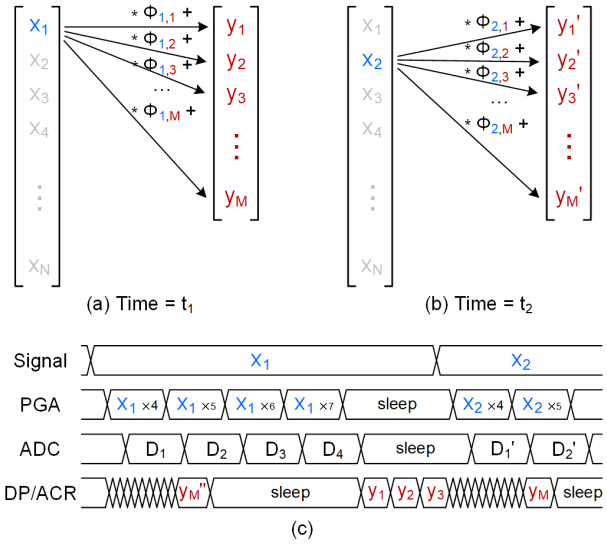

Fig. 5. Illustration of the mixed-signal MVM operation and the timing of the CS measurement. (a) and (b) show the arithmetical operation at time point t_1 and t_2, respectively. (c) shows the timing diagram of the analog sampling, digitization, and the digital processing.

resistors was carefully placed for good unit matching. Post-layout Monte-Carlo simulation results showed that the PGA achieved the required linearity for the 9-bit digitization. The SAR ADC was designed with a 10-bit resolution with an effective number of bits (ENoB) better than 9-bit. The PGA and SAR ADC were designed with a bandwidth of at least $4f_x$ for the proposed CS operation, and the DP processes the data in Mf_x. In practice, the bandwidth of the analog blocks was designed with margin, and these blocks were gated when not activated for power saving. N and M are programmable on-chip for a CR of 2x to 16x. M is programmable to be 64, 96, or 128. The 16-bit CS measurement **y** is sent off-chip serially. All CS operations are in real-time.

B. MCU Implementation of Key Exchanging

As discussed in Section II-B, ECC based algorithms have advantages over conventional asymmetric cryptography algorithms in terms of speed, security level (given a key length), as well as the corresponding computational costs. These features make it attractive for both security-critical applications (e.g. virtual currency [52]) and resource-constrained applications, including wireless neural recording.

Among established elliptic curves, we chose Curve25519 for our application, because of its low requirements in memory and computational resources. Curve25519 and the corresponding Diffie-Hellman functions were originally proposed by Daniel Bernstein in 2006 [42]. The function is a field-restricted scalar multiplication on an elliptic curve E:

$$y^2 = x^3 + 486662x^2 + x \quad (x, y) \in \mathbb{F}_p^2 \tag{5}$$

where p is $2^{255} - 19$. When a point P (on the curve E) multiplies a scalar S, it adds to itself (S-1) times to a point Q, which remains on the curve E (the set forms an abelian group). The computation only uses the x-coordinate, thus is also called x-coordinate scalar multiplication. The x-coordinate scalar multiplication is repeated twice (on each party) in the ECDH protocol for generating the public key and the shared secret key (as illustrated in Fig. 2), respectively.

In this work, we adopted a 256-bit key using a radix 2^{32} representation for the code implementation. The x-coordinate scalar multiplication can be efficiently computed using the classic Montgomery ladder [53]. Algorithm 1 describes the operation in pseudo-codes. Each $Ladderstep$ performs one differential addition and one doubling [54].

Algorithm 1 Scalar Multiplication (Original)

Inputs: P (a point on the curve E), S (a scalar)
Output: Q (a point on the curve E)
$Q \Leftarrow Initial\ point$
for *each bit* b *of* S (254 *downto* 0) **do**
  if b *is* 1 **then**
    swap the values of P *and* Q
  end if
  $(P, Q) \Leftarrow Ladderstep(P, Q)$
  if b *is* 1 **then**
    swap the values of P *and* Q
  end if
end for

Algorithm 2 Scalar Multiplication (Time-Constant Implementation)

Inputs: P (a point on the curve E), S (a scalar)
Output: Q (a point on the curve E)
$Q \Leftarrow Initial\ point$
for *each bit* b *of* S (254 *downto* 0) **do**
  if b *is* 0 **then**
    $(P, Q) \Leftarrow Ladderstep0(P, Q)$
  else
    $(P, Q) \Leftarrow Ladderstep1(P, Q)$
  end if
end for

In order to make the implementation immune to timing attacks, all input-dependent branches or operations, such as the conditional swap in the original algorithm, should be avoided. In this work, we modified the $Ladderstep$ function into two functions $Ladderstep0$ and $Ladderstep1$, as described in Algorithm 2. These two functions have identical timing. The execution of either function depends on the loop's variable bit b; thus, the timing dependence of the input data is eliminated. In addition, the initial coordinates were randomly projected in each execution according to [28] for resistance to differential power attacks (DPA).

The 256-bit multiplication and squaring are the most computationally intensive operations. The 32-bit Cortex-M0 executes 32-bit multiplication in a single clock cycle, however, the returned results are in 32-bit instead of a full 64-bit. The 256-bit multiplication was implemented as a three-level Karatsuba multiplication with time-constant implementation [55, 56]. Squaring operations use the same Karatsuba algorithm, but at a faster computing speed, thanks to the arithmetic simplification and memory access reduction [57].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JETCAS.2021.3074938, IEEE Journal on Emerging and Selected Topics in Circuits and Systems

IV. Experimental Results

The ASIC was fabricated in standard 180nm CMOS technology, occupying a silicon area of 2.5mm×0.6mm excluding the IO pads (Fig. 6 (a)). The system was assembled on a 4-layer printed circuit board (PCB) (Fig. 6 (b)). The main PCB

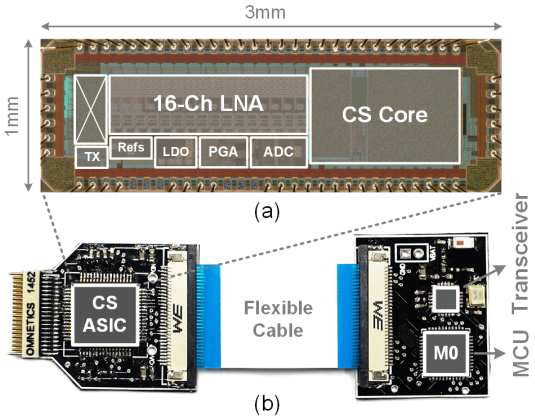

Fig. 6. (a) A micrograph of the fabricated CS ASIC. (b) A photo of the assembled neural recording device. The device consists of a main PCB integrating the ASIC and an extension PCB integrating the MCU and a wireless transceiver.

contained the ASIC and a micro-connector for pairing with MEA. The MCU and the 2.4GHz wireless transceiver were assembled on an extension PCB, which was connected to the main PCB via a flexible cable. The device was powered by 3.7V lithium batteries. On-chip low-dropout regulators (LDOs) provide 1.8V analog and digital supplies to the ASIC, while the MCU and wireless transceiver use a 3.3V supply provided by an external LDO on board. The weight of the assembled device was 4.7g including a 46mAh battery.

The device was fully tested for functionality and performance. The measured noise of the IA was 2.31μV with an integral bandwidth of 0.5 to 250Hz. The IA gain was programmable from 40 to 54dB. The measured distortion at 100Hz was below -60dB, and the common-mode rejection ratio was above 73dB. The bandwidth of the PGA was 20kHz. The measured ENoB of the SAR ADC was 9.3 bit.

The CS function was tested using pre-recorded intracranial EEGs of epilepsy patients [58]. The signal was carefully reviewed and the seizure onset times were annotated by experts. In our experiment, we used a subset of the database that contains the recordings of two patients. The recorded EEG was replayed by an arbitrary signal generator in a resolution of 16-bit, followed by a 5th order low-pass filter with a cut-off frequency of 250Hz. A $l1$-norm based reconstruction algorithm was implemented in MATLAB [12, 15]. Fig. 7 shows the experimental results using one of the patients' data. The reconstructed signals from a CR of 4x and 8x are plotted in comparison with the original signal without compression. M was fixed at 128 in this experiment. The time-domain waveforms are shown in Fig. 7 (a). The spectrograms of a continuous recording of 7.5 hours are shown in Fig. 7 (b). The computed PSNR is 32.75dB at a CR of 8x. The resulting loss due to compression is below the thermal noise

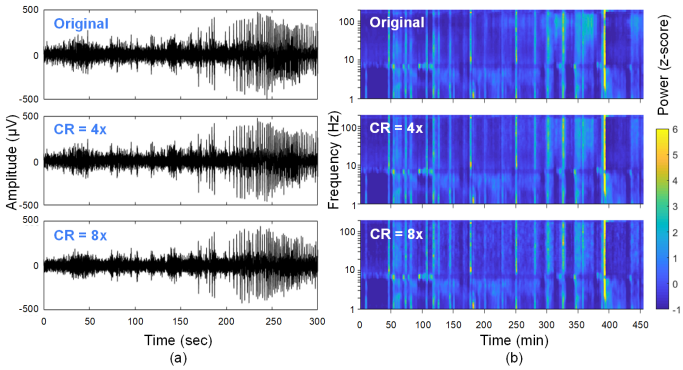

Fig. 7. Experimental results of CS and signal reconstruction with different compression ratio (CR). (a) A 10-min segment of signal during the onset of a seizure event. (b) A 7.5-hour segment of spectrogram showing multiple seizure events. The three rows show the uncompressed signal, CR = 4x, and CR = 8x, respectively.

floor of intracranial EEG recording [51], indicating a sufficient performance for research and clinical use.

We tested the neural recording system under mock attacks using the CoA model. Fig. 8 shows the results of a total of 200,000 CoA attacks to 200 data segments randomly selected from the two patients' recordings. For each data segment, Bob had one reconstruction using the genuine key, while Eve made 1000 reconstruction attempts using randomly generated keys. Here we assumed Eve had prior knowledge of the targeting signals' characteristics, thus Eve used the same basis Ψ as Bob for the signal reconstruction. Fig. 8 (a) shows the correlation coefficients ρ (the higher the better) between Bob's and Eve's reconstructed signals and the original signals. The ρ as defined by Pearson was calculated as:

$$\rho = \frac{N\sum_{i=1}^{N} x_i\hat{x}_i - \sum_{i=1}^{N} x_i \sum_{i=1}^{N} \hat{x}_i}{\sqrt{N\sum_{i=1}^{N} x_i^2 - (\sum_{i=1}^{N} x_i)^2}\sqrt{N\sum_{i=1}^{N} \hat{x}_i{}^2 - (\sum_{i=1}^{N} \hat{x}_i)^2}} \quad (6)$$

where $\hat{\mathbf{x}}$ is the reconstructed signal, N is the dimension of the data segment. The ρ of Eve's reconstructions are within a random noise level. Fig. 8 (b) is the scatter graph of the results from the 200 data segments with x-coordinate being the ρ of Bob's reconstruction and y-coordinate being the ρ of Eve's best shot. It should be noted that Eve doesn't know which one is the best shot since Eve doesn't possess the original signal as the ground truth. The highlighted red dots in (a) and (b) show the trails where the performance of Eve's best attack was closest to Bob's reconstruction. The corresponding time-domain waveforms are plotted Fig. 8 (c). Eve's reconstruction didn't reveal meaningful information about the neural signals. Fig. 8 (d) shows the distribution of Bob's reconstructions and Eve's attacks. The results suggest that the CS neural recorder is safe from CoA attacks.

As discussed in Section II-A, the CS based encryption cannot prevent the energy of the signal $\mathbf{x}$ from being revealed, and the energy features of neural signals often contain valuable

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JETCAS.2021.3074938, IEEE Journal on Emerging and Selected Topics in Circuits and Systems

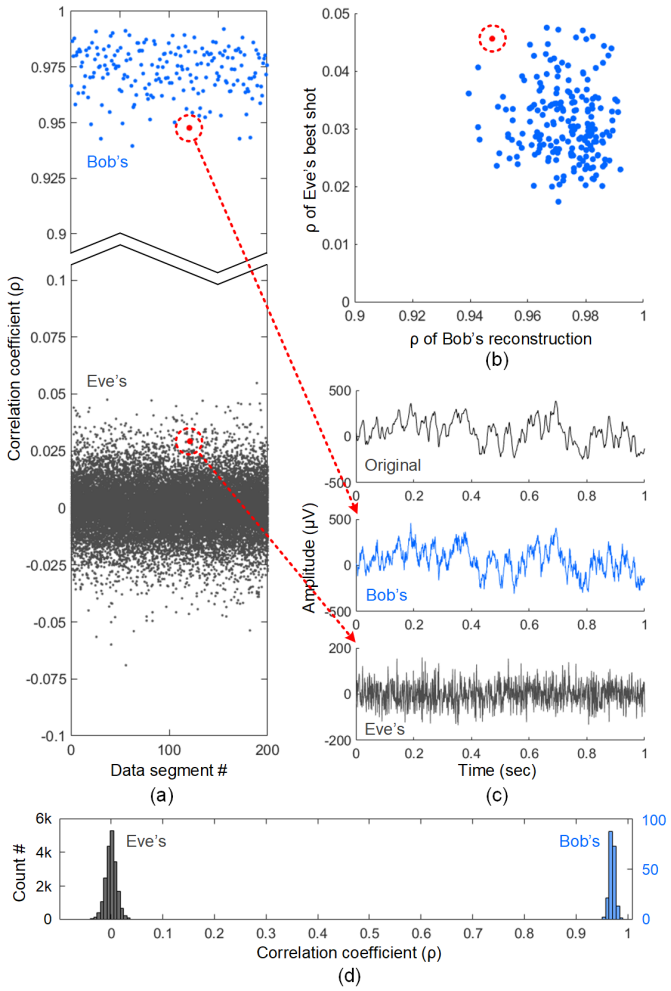

Fig. 8. Experiment of 200,000 mock attacks using the CoA model. (a) The correlation coefficients (ρ) between Bob's and Eve's reconstructed signals and the original signals. (b) The scatter graph of Bob's reconstruction vs. Eve's best shot. (c) The time-domain waveforms of the trails where the $\Delta\rho$ between Bob's and Eve's reconstruction was minimum. (d) Histograms of the ρ of Bob's and Eve's reconstructions.

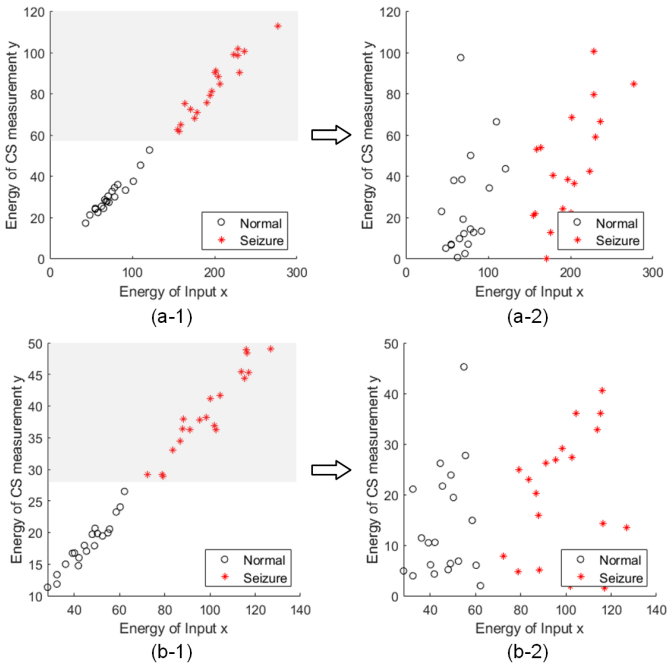

Fig. 9. Experimental results of pseudo-random key shuffle. (a-1,2) and (b-1,2) show analysis of EEGs from two patients, with x-coordinate being the energy of the signal **x** and y-coordinate being the energy of the CS measurement **y**. Black circle markers show segments containing neural signals with normal activities, and red star markers show segments containing neural signals with seizure onset. The left column (a-1) and (b-1) use the same key for all CS measurements, and the right column (a-2) and (b-2) use the pseudo-randomly scrambled keys for the measurements of the same dataset.

information. It should be noticed that the energy features of the neural signals are not the same as the energy of the wireless signals. To evaluate potential information leakage, we used the two patients' recordings with seizures. Long periods of interictal data segments were removed to speed up the experiment. Each marker in Fig. 9 indicates a data segment with x-coordinate being the energy of the signal **x** and y-coordinate being the energy of the CS measurement **y** (without decipher). In addition, a circle marker (black) indicates the segment contains neural signals with normal activities, while a star marker (red) indicates the segment contains neural signals with seizure onset. The plots in the left column ((a-1) and (b-1)) use the same key for CS all measurements. The results show that seizure events can be classified using only the feature along the y-axis. In comparison, the plots in the right column ((a-2) and (b-2)) use the proposed key shuffle for the CS measurement of the same dataset. As expected, seizure classification is not possible using only the features in **y**. This experiment shows that the proposed scheme successfully places an additional layer of protection on the conventional CS based encryption.

As discussed in Section II.C, an adversary may non-invasively detect the power profile of the neural recording device and deduce timing characteristics of the encryption system from power analysis. Although we assumed that an adversary may acquire the timing information indirectly, we directly measured it during the experiments to evaluate the risk. Specifically, timing measurements were obtained using randomly generated key vectors. The measurement results confirmed that the execution of the ECC and ECDH protocols are time constant. No input-dependent branches were observed in 100,000 test runs. The results suggested that the scheme is safe against timing-based attacks.

The power consumption of the developed prototype was measured and compared with conventional implementations. Fig. 10 shows the measurement results with a detailed power breakdown. To compare the result with conventional encryption schemes, we implemented a 256-bit AES on the MCU without data compression. The power consumption was measured to be 15.8mW including wireless transmission. Then we implemented the proposed ECC and CS hybrid scheme both on the MCU. The resulting power consumption was 2.77mW, corresponding to a 5.7x power saving. At last, the power consumption of the proposed device using the ASIC based CS and the MCU based key handling was 442μW. This was measured at a data rate of 500S/s and a CR of 8x.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JETCAS.2021.3074938, IEEE Journal on Emerging and Selected Topics in Circuits and Systems

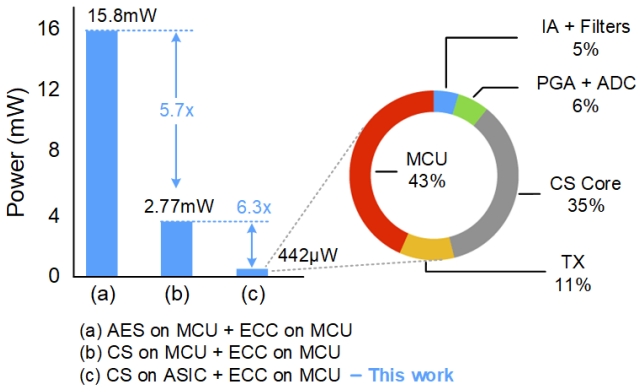

Fig. 10. The measured power consumption of the developed wireless neural recording system in comparison with conventional implementations. The proposed encryption scheme achieved a 5.7x power saving for implementation all in MCUs, while the ASIC design further reduced the power by 6.3x. A 442μW was measured during a sampling rate of 500S/s and a CR of 8x. The detailed power breakdown is shown on the right.

The results suggest that the developed prototype achieved an over 35x power saving compared with conventional encryption schemes.

The specifications and measured performance of the system are summarized in Table II. In addition, the energy efficiency for encryption is compared with prior low-power hardware encryption studies in Table III. By taking advantage of the sparsity of neural signals, energy efficient ASIC design and MCU implementation, the proposed CS based encryption achieved a high energy efficiency.

TABLE II
MEASURED SPECIFICATIONS SUMMARY

Feature	Value	Feature	Value
ASIC Technology	180nm	CS Sampling	500S/s
Supplies	3.3V/1.8V	CS Ratio	2x - 16x
IA gain	40 - 54dB	ASIC clock	up to 4MHz
IA Noise	2.31μVrms	MCU clock	32MHz
IA Bandwidth	0.5 - 250Hz	PSNR*	32.75dB
PGA Gain	4x - 7x	ρ*	0.973
PGA Bandwidth	20kHz	CS power	155μW
ADC Rate	up to 40kSps	Overall power	442μW
ADC ENoB	9.3 bit	Weight	4.7g

* Reconstruction results from a CR of 8x.

V. DISCUSSION

There are several limitations of this work that could be addressed with future research. First, authentication is important for exchanging public keys. Although the initial authentication of medical devices can often be conducted in a secure environment, such as during clinical visits, an integrated digital signature algorithm would improve the robustness and flexibility of the device. Established algorithms, such as the elliptic curve digital signature algorithm (ECDSA), can be implemented in the MCU [44]. Since the authentication process happens at a low frequency, it would not significantly impact the overall system power consumption.

Second, the dimension and resolution of the sampling matrices are important for achieving the optimal performance in terms of the reconstructed signal quality, maximum CR, security level, as well as hardware costs. The design trade-offs also include the targeted signal characteristics and the signal-to-noise ratio. It would be worth studying these trade-offs and implementing a configurable design in the future.

TABLE III
COMPARISON WITH PRIOR LOW-POWER HARDWARE ENCRYPTION STUDIES

	2014 [60]	2014 [61]	2018 [62]	2018 [63]	This work
Hardware	ASIC	Cortex M0	ASIC	ASIC	ASIC + Cortex M0
Data compression	No	No	No	No	8x CS
Wireless channel	No	No	No	No	Yes
Encryption method	AES	ECC	SHA-2	SHA-3	CS + ECC
Energy (norm.)	124 nJ	45.9 nJ	24.3 nJ	48.7 nJ	36.2 nJ*

* IA, filters and wireless power is excluded for comparison.

Third, differential power analysis (DPA) was not conducted in this work. DPA based attacks try to obtain the private keys by statistically analyzing the power consumption of the device [28]. A thorough analysis and an IC level design that eliminates the risks from DPA would be an important step forward.

Finally, the MCU core can be integrated on-chip to further reduce the device form-factor and the power overhead (at an additional cost of silicon area). This is possible by integrating the Cortex-M0 core (freely available for research purpose [64]) or other open-source RISC-V processors. A wireless receiver (Rx) can be integrated on-chip for duplex wireless handshaking, so that the 2.4GHz transceiver can be removed from the system.

VI. CONCLUSION

In this paper, we developed an energy-efficient wireless neural recording system with simultaneous data compression and encryption. The system integrated an ultra-low power CS ASIC and a general-purpose MCU. Novel techniques have been proposed to eliminate the risks from malicious attacks while maintaining an ultra-low power consumption. Experimental results showed that the developed system achieves a secure, reliable, energy-efficient neural recording over time. Data encryption technology will be needed as therapies involving wireless neural interfaces become more prevalent in the treatment of neurological disorders [65]. Moreover, the scheme and circuit techniques introduced in this paper can be applied to a wide range of applications where high energy-efficiency and security are required.

REFERENCES

[1] F. Sun and M. Morrell, “Closed-loop neurostimulation: the clinical experience", *Neurotherapeutics*, vol. 11, no. 3, 2014.
[2] C. Bouton, A. Shaikhouni, N. Annetta, M. Bockbrader, D. Friedenberg, *et al.*, “Restoring cortical control of functional movement in a human with quadriplegia", *Nature*, vol. 533, 2016.

[3] FDA Cybersecurity Safety Communications. [Online]. Available: https://www.fda.gov/medical-devices/digital-health/cybersecurity. [Accessed: July 2020].

[4] R. Harrison, and C. Charles, "*A low-power low-noise CMOS amplifier for neural recording applications*", *IEEE J. Solid-State Circuits*, vol. 38, no. 6, 2013.

[5] B. Murmann, "The race for the extra decibel: A brief review of current ADC performance trajectories", *IEEE Solid-State Circuits Magazine*, vol. 7, no. 3, 2015.

[6] K. Teng, T. Wu, X. Liu, Z. Yang, and C. Heng, "A 400MHz wireless neural signal processing IC with 625x on-chip data reduction and reconfigurable BFSK/QPSK transmitter based on sequential injection locking", *IEEE Trans. Biomed. Circuits Syst.*, vol. 11, no. 3, 2017.

[7] J. Rosenthal, A. Sharma, E. Kampianakis, and M. S. Reynolds, "A 25Mbps 12.4 pJ/bit DQPSK Backscatter Data Uplink for the NeuroDisc Brain Computer Interface", *IEEE Trans. Biomed. Circuits Syst.*, vol. 13, no. 5, 2019.

[8] S. Lee, P Cheng, C. Tsou, C. Lin, and G. Shieh, "A 2.4GHz ISM Band OOK Transceiver with High Energy Efficiency for Biomedical Implantable Applications", *IEEE Trans. Biomed. Circuits Syst.*, vol. 14, no. 1, 2020.

[9] M. Alioto, "Trends in Hardware Security - From Basics to ASICs", *IEEE Solid-State Circuits Magazine*, vol. 11, no. 3, 2019.

[10] J. Han, R. Dou, L. Zeng, S. Wang, Z. Yu, and X. Zeng, "A Heterogeneous Multicore Crypto-Processor With Flexible Long-Word-Length Computation", *IEEE Trans. Circuits Syst. - I*, vol. 62, no. 5, 2015.

[11] B. Devlin, M. Ikeda, H. Ueki, and K. Fukushima, "Completely Self-Synchronous 1024-bit RSA Crypt-engine in 40nm CMOS", *IEEE Asian Solid-State Circuits Conf.*, 2013.

[12] D. Donoho, "Compressed sensing", *IEEE Trans. Inf. Theory*, vol. 52, no. 4, 2006.

[13] S. Aviyente, "Compressed sensing framework for EEG compression", *IEEE Statistical Signal Process.*, 2007.

[14] T. Xiong, J. Zhang, C. Martinez-Rubio, C. S. Thakur, E. N. Eskandar, S. P. Chin, R. Etienne-Cummings, and T. D. Tran, "An Unsupervised Compressed Sensing Algorithm for Multi-Channel Neural Recording and Spike Sorting", *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 26, no. 6, 2018

[15] X. Liu, M. Zhang, T. Xiong, A. G. Richardson, T. H. Lucas, P. S. Chin, R. Etienne-Cummings, T. D. Tran, and J. Van der Spiegel, "A Fully Integrated Wireless Compressed Sensing Neural Signal Acquisition System for Chronic Recording and Brain-Machine Interface", *IEEE Trans. Biomed. Circuits Syst.*, vol. 10, no. 4, 2016.

[16] M. Shoaran, M. H. Kamal, C. Pollo, P. Vandergheynst, A. Schmid, "Compact Low-power Cortical Recording Architecture For Compressive Multi-channel Data Acquisition", *IEEE Trans. Biomed. Circuits Syst.*, vol. 8, no. 6, 2014.

[17] M. Mangia, L. Prono, A. Marchioni, F. Pareschi, R. Rovatti, and G. Setti, "Deep Neural Oracles for Short-Window Optimized Compressed Sensing of Biosignals", *IEEE Trans. Biomed. Circuits Syst.*, vol. 14, no. 3, 2020.

[18] W. Zhao, B. Sun, T. Wu, and Z. Yang, "On-Chip Neural Data Compression Based on Compressed Sensing With Sparse Sensing Matrices", *IEEE Trans. Biomed. Circuits Syst.*, vol. 12, no. 1, 2018.

[19] C. Aprile, K. Ture, L. Baldassarre, M. Shoaran, G. Yilmaz, F. Maloberti, C. Deollain, Y. Leblebici, and V. Cevher, "Adaptive Learning-Based Compressive Sampling for Low-Power Wireless Implants", *IEEE Trans. Circuits Syst. - I*, vol. 65, no. 11, 2018.

[20] X. Liu, H. Zhu, M. Zhang, A. G. Richardson, T. H. Lucas, and J. Van der Spiegel, "Design of a Low-Noise, High Power Efficiency Neural Recording Front-end With an Integrated Real-Time Compressed Sensing Unit", *IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2015.

[21] Y. Rachlin, and D. Baron, "The secrecy of compressed sensing measurements", *Annual Allerton Conf. Commun., Control, Computing*, 2008.

[22] Y. Zhang, L. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, "A Review of Compressive Sensing in Information Security Field", *IEEE Access*, vol. 4, 2016.

[23] L. Zhang, Y, Liu, F. Pareschi, Y. Zhang, K. Wong, R. Rovatti, and G. Setti, "On the Security of a Class of Diffusion Mechanisms for Image Encryption", *IEEE Trans. on Cybernetics*, vol. 48, no. 4, 2018.

[24] W. Cho, and N. Yu, "Secure and Efficient Compressed Sensing-Based Encryption With Sparse Matrices", *IEEE Trans. Inf. Forensics Security*, vol. 15, 2020.

[25] M. Mangia, A. Marchioni, F. Pareschi, R. Rovatti, and G. Setti, "Chained Compressed Sensing: A Blockchain-Inspired Approach for Low-Cost Security in IoT Sensing", *IEEE Internet Things J.*, vol. 6, no. 4, 2019.

[26] T. Chen, K. Hou, W. Beh, and A. Wu, "Low-Complexity Compressed-Sensing-Based Watermark Cryptosystem and Circuits Implementation for Wireless Sensor Networks", *IEEE Trans. Very Large Scale Integration (VLSI) Syst.*, vol. 27, no. 11, 2019.

[27] P. Kaushik, A. Gupta, P. Roy, and D. Dogra, "EEG-Based Age and Gender Prediction Using Deep BLSTM-LSTM Network Model", *IEEE Sensors Journal*, vol. 19, no. 7, 2019.

[28] J. Coron, "Resistance Against Differential Power Analysis For Elliptic Curve CryptoSyst", *Int. Workshop Cryptographic Hardware and Embedded Syst.*, 1999.

[29] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", *Annual International Cryptology Conference*, 1996.

[30] R. Baraniuk, "Compressive Sensing", *IEEE Signal Process. Magazine*, 2007.

[31] M. Wakin, "An Introduction to Compressive Sensing", *IEEE Signal Process. Magazine*, 2008.

[32] E. Candes, and T. Tao, "Decoding by Linear Programming", *IEEE Trans. Inf. Theory*, vol. 51, no. 12, 2005.

[33] T. Zhang, "Sparse Recovery With Orthogonal Matching Pursuit Under RIP", *IEEE Trans. Inf. Theory*, vol. 57, no. 9, 2011.

[34] M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Adapted Compressed Sensing: A Game Worth Playing", *IEEE Circuits Syst. Magazine*, vol. 20, no. 1, 2020.

[35] B. Sun, and H. Feng, "Efficient Compressed Sensing for Wireless Neural Recording: A Deep Learning Approach", *IEEE Signal Process. Letters*, vol. 24, no. 6, 2017.

[36] Z. Zhang, Y. Xu, J. Yang, X. Li, and D. Zhang, "A Survey of Sparse Representation: Algorithms and Applications", *IEEE Access*, vol. 3, 2015.

[37] Z. Yang, W. Yan, and Y. Xiang, "On the Security of Compressed Sensing-Based Signal Cryptosystem", *IEEE Trans. Emerging Topics in Computing*, vol. 3, no. 3, 2015.

[38] M. R. Mayiami, B. Seyfe, and H. G. Bafghi, "Perfect Secrecy via Compressed Sensing", *Iran Workshop Commun. Inf. Theory*, 2013.

[39] 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, 2015.

[40] G. J. Simmons, "Symmetric and Asymmetric Encryption", *ACM Computing Surveys*, vol. 11, no. 4, 1979.

[41] E. Barker, and Q. Dang, "Recommendation for key management part 3: Application-specific key management guidance", *NIST special publication*, 2015. doi:10.6028/NIST.SP.800-57pt3r1

[42] D. Bernstein, "Curve25519: new Diffie-Hellman speed records", *Int. Workshop Public Key Cryptography*, pp. 207-228, 2006.

[43] W. Diffie, and M. E. Hellman, "New Directions in Cryptography", *IEEE Trans. Inf. Theory*, vol. 22, no. 6, 1976.

[44] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)", *International journal of information security*, 2001.

[45] E. De Mulder et al., "Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem," The International Conference on "Computer as a Tool", pp. 1879-1882, 2005.

[46] X. Liu, M. Zhang, B. Subei, A. G. Richardson, T. H. Lucas, and J. Van der Spiegel, "The PennBMBI: Design of a General Purpose Wireless Brain-Machine-Brain Interface System", *IEEE Trans. Biomed. Circuits Syst.*, vol. 9, no. 2, 2015.

[47] X. Liu, B. Subei, M. Zhang, A. G. Richardson, T. H. Lucas, and J. Van der Spiegel, "The PennBMBI: A general purpose wireless Brain-Machine-Brain Interface system for unrestrained animals", *IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2014.

[48] X. Liu, H. Zhu, M. Zhang, X. Wu, A. G. Richardson, S. Y. Sritharan, D. Ge, Y. Shu, T. H. Lucas, and J. Van der Spiegel, "A Fully Integrated Wireless Sensor-Brain Interface System to Restore Finger Sensation", Circuits and Systems, IEEE International Symposium on (ISCAS), May 2017.

[49] X. Liu, H. Zhu, T. Qiu, S. Y. Sritharan, D. Ge, S. Yang, M. Zhang, A. G. Richardson, T. H. Lucas, N. Engheta, and J. Van der Spiegel, "A Fully Integrated Sensor-Brain-Machine Interface System for Restoring Somatosensation", IEEE Sensors Journal, Oct. 2020.

[50] X. Liu, M. Zhang, A. G. Richardson, T. H. Lucas, and J. Van der Spiegel, "Design of a Closed-Loop, Bidirectional Brain Machine Interface System With Energy Efficient Neural Feature Extraction and PID Control", *IEEE Trans. Biomed. Circuits Syst.*, vol. 11, no. 4, 2016.

[51] E. Niedermeyer, and F. L. da Silva, "Electroencephalography: basic principles, clinical applications, and related fields." *Lippincott Williams*

& Wilkins., 2004.
[52] F. Turan, and I. Verbauwhegh, "Compact and flexible FPGA implementation of ED25519 and X25519", *ACM Trans. Embedded Computing Syst.*, vol. 18, no. 3, 2019.
[53] P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization", *Mathematics of Computation*, vol. 48, no. 177, 1987.
[54] P. Sasdrich, T. Guneysu, "Efficient elliptic-curve cryptography using curve25519 on reconfigurable Devices", *Int. Symp. Applied Reconfigurable Computing*, 2014.
[55] A. Karatsuba, Y. Ofman, "Multiplication of Multidigit Numbers on Automata", *Soviet Physics Doklady*, vol. 7, 1963.
[56] M. Dull, B. Haase, G. Hinterwalder, M. Hutter, C. Paar, A. H. Sanchez, and P. Schwabe, "High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers", *Designs Codes and Cryptography*, vol. 77, no. 2, 2015.
[57] E. Nascimento, J. Lopez, and R. Dahab, "Efficient and secure elliptic curve cryptography for 8-bit AVR microcontrollers", *Int. Conf. Security, Privacy, and Applied Cryptography Engineering*, 2015.
[58] J. Wagenaar, "Collaborating and sharing data in Epilepsy Research", *J. Clin. Neurophyiol.*, vol. 32, no. 3, 2015.
[59] M. Hellman, "A cryptanalytic time-memory trade-off". *IEEE trans. on Inf. Theory*. vol. 26, no. 4, Jul 1980.
[60] G. Sayilar and D. Chiou, "Cryptoraptor: High throughput reconfigurable cryptographic processor," *in Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2014.
[61] R. de Clercq, L. Uhsadel, A. Van Herrewege, and I. Verbauwhede, "Ultra low-power implementation of ECC on the ARM cortex-M0+," in *Proc. 51st ACM/EDAC/IEEE Design Autom. Conf. (DAC),* Jun. 2014.
[62] U. Banerjee, C. Juvekar, A. Wright, Arvind, A. P. Chandrakasan, "An energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in iot applications", *ISSCC Dig. Tech. Papers*, Feb. 2018.
[63] Y. Zhang, L. Xu, K. Yang, Q. Dong, S. Jeloka, D. Blaauw, and D. Sylvester, "Recryptor: A reconfigurable in-memory cryptographic Cortex-M0 processor for IoT". *IEEE Symposium on VLSI Circuits, Digest of Technical Papers*, 2017.
[64] ARM Technologies, "ARM Offers Free Access to Cortex-M0 Processor IP to Streamline Embedded SoC Design", 2015. [Online]. Available: https://www.arm.com/company/news/2015/10/arm-offers-free-access-to-cortex-m0-processor-ip-to-streamline-embedded-soc-design. [Accessed: July 2020].
[65] S. Naufel, G. L. Knaack, R. Miranda, T. K. Best, K. Fitzpatrick, A. A. Emondi, E. Van Gieson, and T. McClure-Begley, "DARPA investment in peripheral nerve interfaces for prosthetics, prescriptions, and plasticity", *Journal of Neuroscience Methods*, vol. 332, 2020.

Xilin Liu (S'13-M'17) received the Ph.D. degree at the University of Pennsylvania, Philadelphia, PA in 2016. He is currently with Qualcomm Inc., San Diego, CA. His research interests include mixed-signal IC and system design with edge machine learning for emerging applications, especially brain-machine interfaces.

Dr. Liu received the IEEE Solid-State Circuits Society (SSCS) 2015-16 predoctoral achievement award, the Best Student Paper Award on the 2017 International Symposium on Circuits and Systems (ISCAS), the Best Paper Award (1st place) on the 2015 Biomedical Circuits and Systems Conference (BioCAS), and the Best Paper Award of the biomedical track on the 2014 ISCAS. He is also the recipient of the Student-Research Preview Award of the 2014 IEEE International Solid-State Circuits Conference (ISSCC). His industrial experience includes contributions to a series of premium IC products including the worldâĂŹs first commercial 5G chipset.

Andrew G. Richardson (M'14-SM'19) received the B.S.E degree in biomedical engineering from Case Western Reserve University, Cleveland, OH, USA in 2000 and the S.M. degree in mechanical engineering and Ph.D. degree in biomedical engineering from the Massachusetts Institute of Technology, Cambridge, MA, USA in 2003 and 2007, respectively.

He was a Senior Fellow at the University of Washington, Seattle, WA, USA from 2008 to 2012 and a Senior Research Investigator at the University of Pennsylvania, Philadelphia, PA, USA from 2012 to 2015. He is currently a Research Assistant Professor of Neurosurgery at the University of Pennsylvania. He has coauthored over 100 journal and conference papers and abstracts. His primary research interest is in brain-machine interfaces.

Dr. Richardson coauthored papers selected for Best Paper Awards at the IEEE International Symposium on Circuits and Systems in 2014 and 2017, at the IEEE Biomedical Circuits and Systems Conference in 2015, and at the IEEE Radio Frequency Integrated Circuits Symposium in 2020. His work was a finalist for the Brain-Computer Interface Award in 2018. He currently serves on the editorial board of *Artificial Organs*.

Jan Van der Spiegel (S'73-M'79-SM'90-F'02) is a Professor of Electrical and Systems Engineering at the University of Pennsylvania. He is former Department Chair of Electrical Engineering, and Associate Dean of Education and Professional Programs of the School of Engineering. He was a Senior Visiting Professor at the Institute of Microelectronics and the Department of Electronics Engineering at Tsinghua University (Sept. 2017 till Feb. 2018).

Dr. Van der Spiegel received his Master's degree in Electro-Mechanical Engineering and his Ph.D. degree in Electrical Engineering from the University of Leuven, Belgium. His primary research interests are in mixed-mode microelectronics circuits, smart CMOS vision sensors for polarization imaging, bio-inspired image sensors and brain-machine interfaces. He is the author of over 250 journal and conference papers and holds 8 patents. He is also the Founding Director of the Rachleff Scholars Program at the Engineering School of the University of Pennsylvania, and Director of the SUNFEST program that offers summer research opportunities to talented students. The SUNFEST program is sponsored by the National Science Foundation.

He is a Life Fellow of the IEEE, a Distinguished Lecturer of the Solid-State Circuit Society, and is the recipient of the IEEE Major Educational Innovation Award in recognition of his groundbreaking work with the SUNFEST program. He received the IEEE Third Millennium Medal, the UPS Foundation Distinguished Education Chair and the Bicentennial Class of 1940 Term Chair. He received the IBM Young Faculty Development Award and the Presidential Young Investigator Award.

He has served on several IEEE program committees (IEDM, ICCD, ISCAS, ISSCC, ASICON) and was the technical program chair of the 2007 International Solid-State Circuit Conference (IEEE ISSCC). He is an Associate Editor of the Transaction of BioCAS, a member of the Editorial Board of the IEEE Proceedings and Section Editor of the Journal of Engineering of Institute of Engineering and Technology (IET). He was the president of the IEEE Solid-State-Circuits Society (2016-2017). He is the Past Conference Chair of the IEEE International Solid-State Circuits Conference (ISSCC).