Randomized Switching Successive Approximation Register (RS-SAR) ADC Protections for Power and Electromagnetic Side Channel Security................................................................. 21
A 140-GHz FMCW TX/RX-Antenna-Sharing Transceiver with Low-Inherent-Loss Duplexing and Adaptive Self-Interference Cancellation................................................................. 22
A Bit-level Sparsity-aware SAR ADC with Direct Hybrid Encoding for Signed Expressions Leveraging Algorithm-circuit Co-design ........................................................................ 23
Physical Tags: Fingerprints and Markers Embedded in Objects for Ubiquitous Sensing and Seamless Interactions........ 24
A Low-power THz Wakeup Receiver for an Ultra-miniaturized Platform............................................................. 25
A Dual-antenna, 263-GHz Energy Harvester in CMOS with 13.6% RF-to-DC Conversion Efficiency at -8dBm Input Power ......................................................................................... 26
Stability Improvement of CMOS Molecular Clocks Using an Auxiliary Loop Based on High-order Detection and Digital Integration.................................................................................. 27
Time Series Anomaly Detection Applied to Switched Reluctance Motor System ...................................................... 28
A Sampling Jitter Tolerant Continuous-time Pipelined ADC in 16-nm FinFET ................................................................................................. 29
Energy-efficient System for Bladder Volume Monitoring with Conformable Ultrasound Patches ................. 30
Hardware Design for Efficient Video Understanding on the Edge.......................................................................... 31
Modeling and Design of High-power RF Power Combiners Based on Transmission-lines ................................. 32
Randomized Switching Successive Approximation Register (RS-SAR) ADC Protections for Power and Electromagnetic Side Channel Security

M. Ashok, E. V. Levine, A. P. Chandrakasan
Sponsorship: MITRE Innovation Program, NSF Graduate Research Fellowship Program, MathWorks Engineering Fellowship

Analog to digital converters (ADCs) are necessary in most Internet of Things (IoT) devices, to link the physical analog world to digital computation. In many of these applications, the ADC is processing sensitive data such as biomedical signals or private conversations, which should not be accessible to an attacker. Physical side channel attacks (SCAs) have been used to reconstruct information processed within digital integrated circuits in a variety of applications, through power or electromagnetic (EM) traces. These attacks correlate unintentional leakage of information in the current consumption to the operations and data processed by a circuit, allowing for complete reconstruction of private data, as seen in Figure 1a. Specifically, EM SCAs allow fully non-invasive and localized attacks, by simply placing a probe above a packaged chip, eliminating the effectiveness of some global protections.

In this work, we propose the RS-SAR ADC, which decorrelates the data processed by the ADC from the power and EM side channel leakage. In the capacitive DAC, the parallel unit capacitors corresponding to the more significant bits are independently controlled with random bits, as shown in Figure 1b. This control randomization leads to variable timing of the binary search conversion, eliminating the attacker's ability to determine which of the digital data bits the various measured current spikes correspond to. When tested on a chip fabricated in TSMC 65-nm complementary metal-oxide-semiconductor (CMOS) (Figure 1c, provided through TSMC University Shuttle), the protected ADC has 82x the attack error of the unprotected ADC for power SCA and 32x the attack error for EM SCA.

FURTHER READING

A 140-GHz FMCW TX/RX-Antenna-Sharing Transceiver with Low-Inherent-Loss Duplexing and Adaptive Self-Interference Cancellation

X. Chen, M. I. W. Khan, X. Yi, X. Li, W. Chen, J. Zhu, Y. Yang, K. E. Kolodziej, N. M. Monroe, R. Han

High-resolution integrated radars are crucial in today’s automotive, vital sign, and security-sensing applications. Compared to radars operating in the microwave/low-millimeter-wave and optical regimes, the sub-terahertz/sub-THz (sub-THz/THz) spectrum shows great opportunities in both high-resolution and all-weather radar imaging capabilities. For isolation between the radar transmitter (TX) and receiver (RX), a bistatic configuration with separate TX and RX antenna positions is commonly adopted. However, in non-MIMO high-angular resolution systems, the radar transceiver should pair with a large lens/reflector for beam collimation. The bistatic arrangement then causes severe misalignment between the peaks of TX and RX beam patterns, as in Figure 1. Radar transceivers with a shared TX and RX antenna interface, or monostatic configuration, are therefore required in this scenario. Prior monostatic radars adopt hybrid/directional couplers for passive TX-RX duplexing, but at the cost of 3dB + 3dB insertion loss inherent to couplers.

As demonstrated in Figure 2, we present a 140-GHz frequency-modulated continuous-wave (FMCW) radar transceiver in 65-nm CMOS, featuring TX/RX antenna sharing that solves the TX/RX beam misalignment problem. A full-duplexing technique based on circular polarization and geometrical symmetry is applied to mitigate that 6dB inherent insertion loss, while maintaining high TX-to-RX isolation. In addition, a self-adaptive self-interference cancellation is implemented to suppress extra leakage due to antenna mismatch from a desired frontside radiation scheme. The TX/RX antenna sharing enables the pairing with a large 3D-printed planar lens and boosts the measured EIRP to 25.2dBm. The measured total radiated power and minimum single-sideband noise figure including antenna and duplexer losses are 6.2dBm and 20.2dB, respectively. The measured total TX-RX isolation is 33.3dB under 14-GHz wide FMCW chirps. Among all reported sub-THz transceivers with TX/RX antenna sharing, our work demonstrates the highest total radiated power and is the only work that has >30dB of TX-RX isolation while mitigating the inherent 6dB coupler loss.

![Figure 1: Architecture of cryptographic core and chip micrograph.](image1.png)

![Figure 2: Demo of the 140-GHz FMCW radar transceiver in 65-nm CMOS. The TX/RX antenna sharing enables the pairing with a large 3D-printed planar lens and accurate TX/RX beam alignment.](image2.png)

**FURTHER READING**

A Bit-level Sparsity-aware SAR ADC with Direct Hybrid Encoding for Signed Expressions Leveraging Algorithm-circuit Co-design

R.-C. Chen, H.-T. Kung, A. P. Chandrakasan, H.-S. Lee
Sponsorship: CICS, DARPA

Machine learning is promising for many applications including image recognition and natural language processing. Machine learning accelerators are needed for these computation-intensive tasks. Analog neural networks are promising for breaking the memory wall for conventional machine learning accelerators. In this work, we propose the first sparsity-aware successive approximation register analog-to-digital converter (SAR ADC) with direct hybrid encoding for signed expressions (HESE) leveraging encoding algorithm-circuit co-design. ADCs are typically a bottleneck of analog neural networks. For a pre-trained convolutional neural network (CNN) inference, ANN with HESE SAR minimizes the non-zero terms and enables a reduction in energy along with the term quantization (TQ). The proposed SAR ADC directly produces the HESE signed-digit representation (SDR) using two thresholds per cycle as a 2-bit look-ahead. A proof-of-concept direct HESE SAR ADC is being fabricated by 65-nm technology. Measurements show that it provides the novel sparsity encoding with a Walden figure-of-merit of 15.2fJ/conv-step at a 45-MHz sampling rate. The core area is 0.072 mm^2. This opens the direction of direct sparsity encoding ADCs.

**FURTHER READING**

Physical tags, i.e., metadata attached to objects for identification, are an essential component of manufactured goods and raw materials. Conventional means of tagging these without electronics involve sticking separate labels (barcodes) to objects. However, such tags do not subtly blend into the objects and are often visually distracting or prone to damage. We propose to replace this synthetic “tagging” process with improved and robust approaches that use unobtrusive physical features of objects and materials as tags.

We focus on two types of unobtrusive tags: natural tags and engineered tags. The former allows us to leverage objects’ natural properties as an ID, e.g., their micron-scale surface texture. For SensiCut (ACM UIST ’21), we used laser speckle imaging to sense material sheets in laser cutters without any pre-labeled stickers. Differences in surface structure result in unique speckle patterns for each material, which we use to classify its type with a convolutional neural network. We trained the network with more than 38k images, resulting in an accuracy rate of 97.97%.

Second, engineered tags enable us to define the type of information or pattern we want to embed on an object during the fabrication process. By manipulating a 3D printer’s path, we create unique and subtle surface textures for each copy of the same 3D model, which can be distinguished from a single photograph (ACM CHI’20). For this approach, called G-ID, we evaluated how finely these texture-related parameter differences can be differentiated between and built a mobile application that uses image processing techniques to retrieve these parameters from photos. Together, these approaches represent an important first step towards enabling digitally readable tags in objects without disrupting their integrity, look, or feel.

FURTHER READING

A Low-power THz Wakeup Receiver for an Ultra-miniaturized Platform

E. Lee, M. I. Ibrahim, U. Banerjee, R. T. Yazicigil, A. P. Chandrakasan, R. Han
Sponsorship: NSF, Korea Foundation for Advanced Studies

With the increasing demand for wirelessly connected devices, extending the lifetime of the communication nodes has become essential. As wireless communication is often one of the most power-hungry parts of an overall system, it is necessary to use devices with low-power wireless communication capabilities. A wakeup receiver (WuRX) is a circuit block that listens to the predefined token and turns on the node. The WuRX keeps the node in standby mode until a valid request, which helps to reduce unnecessary power consumption and, thus, lengthen the battery lifetime. Among various metrics of WuRXs, sensitivity and power consumption are two major axes that have led the progress of WuRXs in past decades. Several sub gigahertz/gigahertz works have achieved sensitivity-power tradeoff by co-designing off-chip components such as a high-Q antenna. While these have improved sensitivity and power performance, they are not suitable for ultra-miniaturized platforms due to the external components.

Pushing the carrier frequency to terahertz (THz) is key to reducing the form factor near the mm2- scale. Thanks to the small antenna aperture size requirement of the THz electromagnetic waves, antennas can be fabricated on a chip and integrated with the receiver’s front-end without any external off-chip components. In this work, we aim at developing a sub-microwatt THz WuRX, operating at 261 GHz. We use an envelope detector first receiver architecture to avoid large power consumption of THz demodulation. To increase the sensitivity of the WuRX, we investigate a method to improve the noise equivalent power of the THz detector. The THz detector output is amplified, filtered, and recovered to the original data. The duty-cycling technique is also applied to reduce power consumption. In addition, we propose a secure wakeup protocol to prevent the battery-drainage attack, which is especially critical to battery size-limited miniaturized platforms. While this project is still in progress, this system will facilitate the use of THz for the ultra-miniaturized platform.

FURTHER READING


▲ Figure 1: Conceptual application scenario for the THz wakeup receiver.
A Dual-antenna, 263-GHz Energy Harvester in CMOS with 13.6% RF-to-DC Conversion Efficiency at -8dBm Input Power

M. I. W. Khan, E. Lee, N. M. Monroe, A. P. Chandrakasan, R. Han
Sponsorship: NSF (Grant No. SpecEES ECCS-1824360)

Pushing the wave frequency of far-field wireless power transfer (WPT) to the terahertz regime is essential for ultra-miniaturized, battery-less platforms, which currently can only be powered through light or ultra-sound. As an example, the mm²-size THz identification tag (THz-ID) in [1] relies on integrated photo-diodes, and THz WPT will allow embedding the tags into optically-opaque packages of small-size goods (e.g., semiconductor chips). In this work, a 263-GHz energy harvester using Intel’s 22nm FinFET process is reported, increasing the highest frequency of CMOS harvester by ~3x. The antenna-integrated harvester is ultra-compact (~0.5mm²) and does not rely on any external component. In Fig.1, a self-biased N-FinFET is simulated with various (V_{ds}, V_{gs}) combinations while keeping input power equal to -8dBm. An \eta_{max} of 25.8% is obtained, when phase difference V_{ds}-V_{gs} is \Delta \phi = 45° and the amplitude ratio |V_{ds}|/|V_{gs}| is A_{opt} = 3.75. The schematic meeting these conditions is shown in Fig.2, where the additional phase tuning is provided by TL\textsubscript{7}. Lastly, connecting the central AC ground nodes of the patch antennas together enables self-biasing of the transistor without interfering with antenna operations. The same connection is also used to extract DC output power. The measured load line performance of the harvester at 5cm distance, shown in Fig.3a, results in an optimum load of ~1kΩ. Fig. 3b shows that -8dBm input power the measured \eta_{max} is 13.6% and 22µW of DC power is harvested.

FURTHER READING

Stability Improvement of CMOS Molecular Clocks Using an Auxiliary Loop Based on High-order Detection and Digital Integration

M. Kim, H.-S. Lee, R. Han
Sponsorship: JPL, NSF

An ultra-stable frequency reference is a key element for a wide variety of applications, ranging from sensing to navigation. Recently, chip-scaled molecular clocks (CSMC) have achieved high frequency stability with low power and compact size by using a rotational-mode transition of carbonyl sulfide (OCS) centered around 231.061 GHz as a frequency reference (f₀). In the molecular clock, the probing signal generated from the transmitter is frequency-modulated at fm around the center frequency (fc). Since fc is locked to f₀ in a feedback loop, the output frequency inherits the excellent stability of the OCS transition frequency. Due to its fully electronic implementation, CSMC provided a solution to significantly reduce the cost of high-stability miniaturized clocks. However, the frequency stability is still limited by a finite loop gain of the frequency locked loop and detection non-idealities coming from baseline variations that are susceptible to environmental disturbance even though an invariant physical constant is used as the frequency reference.

In this work, we propose a new dual loop CSMC architecture based on both fundamental and high-order transition probing as well as digital integration. While the fundamental harmonic detection forms the main loop, the higher-order probing is used in an auxiliary loop. The main loop enables the fast correction of the frequency, and the auxiliary loop responds against long-term frequency variation. As a result, the dual-loop architecture combines the advantages of both fundamental locking and high-order locking: high signal-to-noise ratio (SNR) and robustness against the environmental variations. The proposed CSMC was implemented in 65-nm complementary metal-oxide-semiconductor (CMOS) and achieved 20-ppt Allan Deviation at 104 s averaging time with 71-mW power consumption. This demonstrates the feasibility of miniaturization, as well as the low power and low cost of the clock.
We explore methods to enable motor systems to utilize sensor data to assess installation and detect or predict anomalous events before possible breakdown. Here, we use an autoencoder neural network model for unsupervised anomaly detection on an air-handling system driven by a switched-reluctance motor (Figure 1). The motor system consists of a belt-driven blower-motor unit with a 6/10 stator/rotor pole configuration.

Our model (Figure 2) takes the Fourier transform of recorded sensor time signals and trains one autoencoder per feature. The sum of the reconstruction errors is used as an anomaly score for prediction. The autoencoder has been effective on time series datasets in multiple fields. We generate datasets with differences in various parameters (e.g., belt tightness, motor speed, blower output valve condition) and label the data according to the anomalous scenarios. For instance, if a dataset is used for anomaly detection of belt tightness, we label the time series generated with normal belt tightness “normal” and an over tight/loose belt “anomalous.” We choose three kinds of sensor data (line current, motor current, vibration) as the time series for anomaly detection. We assume that the system operates normally during training and that sensor data used for training purposes contain few, if any, anomalies.

The base frequencies of motor current and vibration are identical and consistent with the 6:10 pole ratio. Characteristic curves are found in randomly ordered runs for transient sensor data during activation (Figure 3). Results of stable sensor data show 100% area under curve (AUC) / 98% accuracy for anomaly detection of belt tightness, and 95% AUC / 82% accuracy for speed; 52% AUC / 34% accuracy for valve condition indicates that this condition remains difficult to detect. Combining the labels for the three parameters achieves 94% AUC / 87% accuracy. Our model detects anomalies on motor systems for one or several aggregated failure modes.

**FURTHER READING**

Almost all real-world signals are analog. Yet most of the data is stored and processed digitally due to advances in the integrated circuit technology. Therefore, analog-to-digital converters (ADCs) are an essential part of any electronic system. The advances in modern communication systems including 5G mobile networks and baseband processors require the ADCs to have a large dynamic range and bandwidth. Although there have been steady improvements in the performance of ADCs, the improvements in conversion speed have been less significant because the speed-resolution product is limited by the sampling clock jitter (Figure 1). The effect of sampling clock jitter has been considered fundamental. However, it has been shown that continuous-time delta-sigma modulators may reduce the effect of sampling jitter. But since delta-sigma modulators rely on relatively high oversampling, they are unsuitable for high-frequency applications. Therefore, ADCs with low oversampling ratio are desirable for high-speed data conversion.

In conventional Nyquist-rate ADCs, the input is sampled upfront. Any jitter in the sampling clock directly affects the sampled input and degrades the signal-to-noise ratio (SNR). It is well known that for a given root-mean-square (RMS) sampling jitter $\sigma_t$, the maximum achievable SNR is limited to $1/(2\pi f_{in} \sigma_t)$, where $f_{in}$ is the input signal frequency. In a silicon-on-chip environment, it is difficult to reduce the RMS jitter below 100 fs. This limits the maximum SNR to just 44 dB for a 10-GHz input signal. Therefore, unless the effect of sampling jitter is reduced, the performance of an ADC would be greatly limited for high-frequency input signals.

We propose a continuous-time pipelined ADC having reduced sensitivity to sampling jitter (Figure 2). The analog input is processed in continuous time in the first stage. The residue is sampled by the backend ADC after amplification and low-pass filtering. This results in a much smaller derivative for the residue signal compared to the analog input. Since the error voltage due to clock jitter is proportional to the derivative of the sampled signal, the effect of sampling jitter is greatly reduced. We are designing this ADC in 16-nm FinFET technology to give a proof-of-concept for improved sensitivity to the sampling clock jitter.
Energy-efficient System for Bladder Volume Monitoring with Conformable Ultrasound Patches

V. Mittal, Z. Song, C. Marcus, L. Zhang, S. J. Schoen, V. Kumar, Y. Eldar, C. Dagdeviren, A. E. Samir, H.-S. Lee, A. P. Chandrakasan
Sponsorship: Texas Instruments

Continuous monitoring of bladder volume aids the management of many common conditions such as post-operative urinary retention and benign prostatic hyperplasia. Despite the success of ultrasound technology, there is a lack of wearable ultrasound probes capable of imaging curved body parts with high spatio-temporal resolution and making diagnostic decisions. Current systems are not sufficiently energy-efficient to permit continuous wearable device deployment for more than 1-2 days, as their power budget is several mW. We aim to develop a conformable, energy-efficient, battery-operated, wearable ultrasound patch capable of real-time organ monitoring. The wearable patch will be fully integrated with the transceiver electronics for energy-efficient processing of the ultrasonic signals and an efficient inference engine for bladder volume estimation. This system will incorporate several key innovations, including (1) deep neural network- (DNN) based segmentation algorithms employed to generate accurate bladder volume estimates; (2) low voltage ultrasound transceivers to enable low power, portable integrated system; and (3) signal processing algorithms capable of working with low signal-to-noise ratio (SNR) environments.

We aim to integrate the transducers with the analog front-end and DNN accelerator while ensuring that heat dissipation is within FDA specified limits. The power-efficient patch will operate at low voltage, thus posing the challenge of working with a low SNR signal. The transmitter consists of energy-efficient pulsers, appropriately beam-formed and multiplexed for different sub-apertures of the transducer array. On the receiver end, low-voltage, energy-efficient techniques are used to optimize the active power of the analog front end.

An on-chip DNN will extract the segmented mask from the beamformed image. The network is trained on bladder ultrasound images from MGH. The network is mostly binarized with the remaining operations quantized to minimize the memory requirement and eliminate the need for on-chip floating-point operation support. A DNN accelerator is designed for optimal binary DNN performance but also supports low bit-width computation. Lastly, the bladder volume is extracted from the segmented images and given as the system output using the double area method.

FURTHER READING

Hardware Design for Efficient Video Understanding on the Edge

M. Wang, Y. Lin, Z. Zhang, J. Lin, S. Han, A. P. Chandrakasan
Sponsorship: Qualcomm Incorporated

With the rise of various applications including autonomous driving, object tracking for unmanned aerial vehicles, etc., there is an increasing need for accurate and energy-efficient video understanding on the edge. Although there are many deep learning chips designed for images, little work has been done for videos. Video understanding on the edge has three major challenges. First, video understanding requires temporal modeling. For example, it identifies the difference between opening and closing a box, which is distinguishable only with temporal information considered. Second, many applications are delay-critical, such as self-driving cars. Third, high energy efficiency is important for edge devices with a tight power budget. Due to temporal continuity, consecutive frames might share a lot of common information, providing the potential to improve processing efficiency. However, an image-based processing system cannot utilize that since each frame is processed individually.

In this project, we co-design algorithms and hardware for energy-efficient video processing on delay-critical applications. We design architecture to natively support temporal shift module on the backbone of 2D convolutional neural networks for temporal modeling. Moreover, we propose a Real-Time DiffFrame method to utilize temporal redundancy and reduce on-chip energy and dynamic random-access memory (DRAM) traffic for delay critical applications. Compared to an ordinary convolution baseline, our method achieves around 2x reduction in both DRAM and static RAM (SRAM) accesses and 2x improvement in throughput with temporal modeling capability and no accuracy loss. The system has been fabricated in TSMC 28-nm complementary metal-oxide-semiconductor (CMOS) process. Figure 1 shows the chip photograph and specifications. We are evaluating our proposed system and measuring the performance of the chip.

---

FURTHER READING

Modeling and Design of High-power RF Power Combiners Based on Transmission-lines

H. Zhang, G. Cassidy, A. Jurkov, K. Luu, A. Radomske, D. J. Perreault
Sponsorship: MKS Instruments, Inc.

Industrial plasma generation for semiconductor processing applications are usually characterized by high power levels (e.g., kWs), wide power ranges (e.g., 30dB dynamic range), narrow-frequency-band operations (e.g., 13.56MHz ± <5%), and the need to combine power from multiple sources. Power combiners based on transmission lines are attractive due to their small form factor and high efficiency. However, most existing literature focuses on frequency response, with little consideration regarding losses or co-design with magnetic components. Here we introduce a lumped-element circuit model better suited for this application space and further propose a tuning technique that, by adding two capacitors, minimizes impedance distortion while preserving high efficiency. A 13.56-MHz, 1-kW prototype is designed and built, validating the model and tuning technique with both small-signal measurements and high-power tests. The study would help in realizing radio frequency power generation systems that maintain high efficiency over a very wide power range.

FURTHER READING