A Secure Multimodal Electrochemical Sensor for Sustainable Biomanufacturing

Alperen Yasar[1], Dilara Caygara[1], Yash H. Patel[1], Ananya Pemaraj[1], Leo Boisvert[1], Andrew Magyar[2], Tao Yu[3], Benoit Dufort[3], Tze-Lei Poo[3], Rabia Tugce Yazicigil[1]

(1) Department of Electrical and Computer Engineering, Boston University, Boston, MA, US

(2) Capra Biosciences, Sterling, VA, US

(3) Analog Devices Inc., Boston, MA, US

***Abstract*—This work introduces a secure multimodal sensor capable of performing cyclic voltammetry, amperometry, and electrochemical impedance spectroscopy to monitor glucose concentrations and bacterial cell density in real time as indicators of bioreactor health. The sensor achieves a dynamic range (DR) of 140.55 dB and an integrated noise of 9.48 pA$_{RMS}$ over 100 kHz bandwidth. Low-power physical-layer security is embedded within a delta-sigma modulator by utilizing quantization noise and dithering. This enables 2.67x lower wireless system energy consumption compared to a traditional stream cipher.**

Keywords—physical-layer security, delta-sigma modulator, bioreactor, biomanufacturing, analog front end, potentiostat

I. Introduction

Biomanufacturing is essential for synthesizing various products, such as plastic components, food ingredients, and active pharmaceutical substances. These processes are conducted in large-scale bioreactors, which provide a controlled environment for cultivating microorganisms that produce specific ingredients. Precise control of bioreactor conditions enhances manufacturing accuracy, efficiency, and yield [1]. This can be achieved using a closed-loop system with a multimodal sensing platform to monitor bacterial concentrations (e.g., *Escherichia coli (E. coli)*) or target molecules. Current sensing methods require extracting samples for offline analysis, or the use of large probes, risking contamination and limiting data to specific locations and times. In contrast, floating wireless sensors can provide robust, high-precision, real-time data for a comprehensive assessment of the bioreactor's state.

This work, illustrated in Fig. 1, presents a low-power electrochemical sensor designed for spatially distributed monitoring by floating inside bioreactors. The system supports: 1) cyclic voltammetry (CV) for measuring redox potentials, 2) amperometry for glucose concentration detection, and 3) electrochemical impedance spectroscopy (EIS) for determining *E. coli* cell concentrations.

Due to the widespread use of bioreactors across various industries, maintaining data security and integrity is essential. An attack, such as spoofing, could cause classified data leakage, or evolve into altering the manufacturing, potentially causing financial losses or a health hazard. However, the resource constraints of these sensors render cryptographic methods impractical to implement [2-5]. To address these challenges, we present a secure multimodal sensor designed for sustainable biomanufacturing featuring a physical-layer security solution embedded within the analog-to-digital converter (ADC).

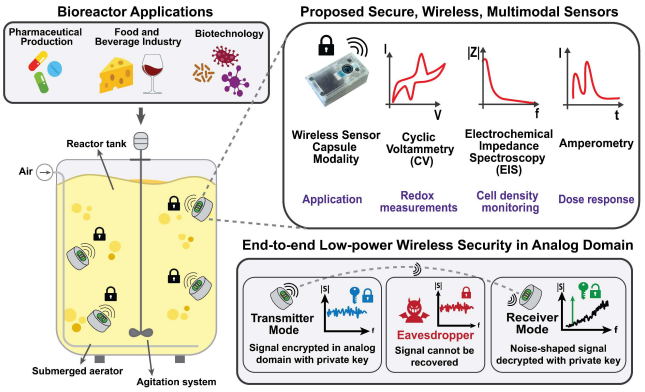

Fig. 1. Multimodal biosensor for bioreactor applications, with embedded security in analog sensor against eavesdroppers.

II. Chip Architecture

A. Sensor Front End

The sensor architecture, shown in Fig. 2, includes a potentiostat front end suitable for both two-electrode and three-electrode electrochemical measurements. DC bias and arbitrary excitation through the counter electrode induce a current over the load, flowing into the working electrode. The reference electrode maintains a stable potential without drawing current, ensuring precise measurements. The circuit features a 12-bit digital-to-analog converter (DAC) for setting the DC bias of the counter electrode. The counter electrode is driven by a class-AB amplifier, for high current source/sink capabilities.

Electrochemical reaction currents in the bioreactor can vary by several orders of magnitude, influenced by measurement conditions, such as temperature and pH, as well as the specific electrochemical processes involved [6]. Furthermore, electrode geometry also impacts the current levels, adding to the variability of electrochemical signals [7], necessitating a high DR for the front-end circuitry. Additionally, EIS-based bacterial growth monitoring typically operates within a frequency range extending up to 100kHz to capture changes in cellular impedance characteristics [8].

To address these requirements, the front-end circuit was designed with a low-noise transimpedance amplifier (TIA) in two-stage Miller topology, providing four levels of adjustable gains (3.30, 31.81, 321.88, and 3,055.22 kΩ), allowing precise control over the amplification of electrochemical signals. The system achieves a dynamic range of 140.55 dB and supports a maximum current input of 101.6 µA at the lowest gain setting. The low-noise front-end design ensures high measurement accuracy, with a measured input-referred noise of 9.48 pArms integrated over a 100 kHz bandwidth.

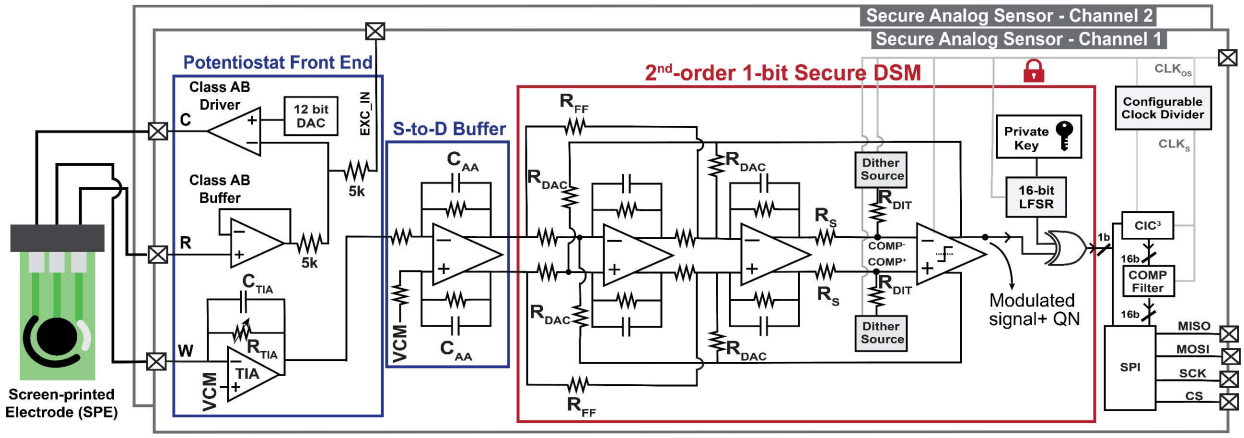

Fig. 2. Top-level secure electrochemical sensor front-end architecture.

B. *Sampling Back End*

The front end is followed by a Delta-Sigma Modulator (DSM) that is commonly used in low-frequency sensors for their oversampling and noise-shaping capabilities. A single-ended-to-differential (S-to-D) buffer connects the TIA output to the fully-differential DSM, acting as an anti-aliasing filter. Considering the needed resolution and power constraints of the application, a second-order, 1-bit, continuous-time architecture is chosen for the DSM implementation. Utilizing two integrators and a strong-arm latch comparator operating at 10MHz, the proposed DSM achieves an oversampling ratio (OSR) of 50 for 100kHz, the highest frequency within the TIA bandwidth. A 1-bit architecture enhances linearity by the usage of resistors as feedback (R_{DAC}) without requiring a DAC or switches, which are among the main sources of nonlinearity. This also further reduces the power consumption and complexity of the modulator. For a V_{DD} of 1.2 V, R_{DAC} values are chosen to effectively provide feedback of 0.75 V_{DD} (V_{REF+}) or 0.25 V_{DD} (V_{REF-}) at the integrator summing node based on the comparator output.

An XOR gate encrypts the modulator's output stream with a random bit output from a 16-bit linear feedback shift register (LFSR) pseudo-random number generator (PRNG). Details of the security scheme will be discussed in Section III. A third-order cascaded integrator-comb (CIC) filter is used for low-pass filtering and decimating the signal, with a compensation filter flattening the filter response. Combined with the DSM, this filter forms a 16-bit DSM ADC, resulting in an analog-in digital-out full-chain system. Additionally, an on-chip voltage-divider-based dithering structure is used to decorrelate the quantization noise (QN) from the input signal, removing idle tones due to limit cycles within the noise-shaped spectrum and enhancing the security through additional randomness. Two 16-bit LFSR PRNGs generate bit sequences to control NMOS switches, adjusting the resistive ladder's relative voltage division ratio between 0.978 and 1.022. This adds a slight chance for a bit flip at each sampling output without disrupting the underlying signal. Since the QN is dependent on factors including the previous decision of the sampler, this slight probability will accumulate over time, sustaining hard-to-predict flipping sequences. The receiver chain includes a data synchronizer, decryptor, CIC, and compensation filters for outputting digital data. All the communication for data transmission, control, and status flags is done over standard serial peripheral interface (SPI) protocol.

III. Secure Delta-Sigma Modulator

A. *Threat Model*

Biomanufacturing requires frequent collection of data (e.g., feedstock, pH, temperature) for monitoring the bioreactor state. This information is crucial to sustain a healthy bioreactor environment and high-yield manufacturing. However, a breach in security could cause leakage of confidential information about the product, such as the manufacturing process of a certain product. Additionally, the adversary could place themselves into the middle of the communication link from the sensor to the server, forming a man-in-the-middle (MITM) attack model. In a bioreactor setting, an MITM attack can be used to capture the data packets, change the information, and send it to the server to misinform the biomanufacturing control loop. This could result in a lower yield in the production, or health hazards in the biopharmaceutical industry such as, drug production.

For an adversary to leak information by sniffing on the data packets, or to spoof the server by identifying themselves as the sensor to form MITM, they need to eavesdrop on the sensor. The packet should be reverse-engineered to continue the attack without getting detected. Our work considers an eavesdropping threat model, aiming to mitigate the threat from its starting point. We assume that the adversary has full knowledge about the chip architecture, working principles, security scheme, PRNGs, and their polynomials, and has access to a replica of the device as a black box, able to provide any known input to perform cryptanalysis without using invasive attacks through physical access. Additionally, we do not consider any denial-of-service attacks, such as jamming. These assumptions are reasonable given the controlled bioreactor environment which could detect those active attacks. The symmetric private key is unknown to the adversary and is assumed to be shared securely between the transmitter and receiver ahead of time.

B. *Security Scheme*

Secure Delta-Sigma Modulator (S-DSM) offers a practical scheme that effectively balances security requirements with the constraints of resource-limited sensors, delivering a security strength that aligns with their performance metrics and cost considerations. Similar to a stream cipher, the S-DSM uses an XOR operation to encrypt the 1-bit modulated signal with the LFSR PRNG output, serving as a trapdoor function.

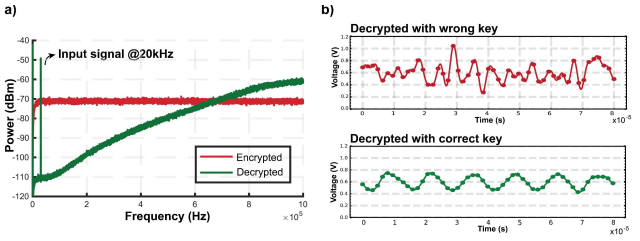

Fig 3. Measured results for (a) encrypted and decrypted frequency spectrums, and (b) decryption with wrong and correct key in the time domain.

This scrambles the bit sequence but also redistributes the noise-shaped spectrum of DSM, hiding the information under the white-noise-like spectrum. A known key can revert the process by generating the same PRNG sequence. However, a wrong key will result in a white-noise-like sequence, hiding the information from adversaries as depicted in Fig. 3.

In a conventional stream cipher, an attacker conducting cryptanalysis using the same key across multiple encryptions could potentially gain information or discover key leaks. In S-DSM, this is mitigated by using the QN as a secondary source of randomness source. To enhance randomization, we utilize dithering for security purposes for the first time, which is already a commonly used technique in DSM implementations for ADC performance. This creates a one-to-many relationship between the analog input and S-DSM output, where the same key and message can result in different cipher streams. However, the authorized receiver can recover the message without knowing the QN sequence, as the decryption will revert to the noise-shaped spectrum where QN is noise-shaped towards the higher frequencies.

The working principle of the S-DSM can be modeled as the following. Let $DSM_n(M)$ be the output of the nth DSM when the input message is M. Given the QN sequences will be different, two different modulators will output different sequences for the same input, D_1, and D_2, although when passed through the CIC filter, both would give the sampled information of M.

$$DSM_1(\mathrm{M}) = D_1 \neq D_2 = DSM_2(\mathrm{M}) \quad (1)$$

$$\mathrm{CIC}(D_1) = \mathrm{M}' = \mathrm{CIC}(D_1) \quad (2)$$

Where M' is the sampled ADC output of M. To derive the effect of the QN on D_1 relative to D_2, D_1 can be written as

$$D_1 = D_1 \oplus D_2 \oplus D_2 = K_{QN} \oplus D_2 \quad (3)$$

K_{QN} is defined as the bitwise randomization from the QN, i.e., the difference between the modulated sequences for the same input, and $\oplus$ denotes the XOR operator. Similarly, the cipher output of the S-DSM scheme can be modeled as

$$S\text{-}DSM_1(\mathrm{M}) = \mathrm{D}_1 \oplus K_{LFSR} = C_1 \quad (4)$$

K_{LFSR} is the key sequence generated by the LFSR PRNG, and C_1 is the cipher output of S-DSM$_1$. Using (3) and (4)

$$C_1 = D_2 \oplus K_{QN} \oplus K_{LFSR} = D_2 \oplus K_{S\text{-}DSM} \quad (5)$$

$K_{S\text{-}DSM}$ can be defined as the effective key of the S-DSM scheme, which involves the effect of the random bit flips caused by the QN.

IV. Measurement Results

The proposed chip was fabricated in 65nm CMOS technology. All measurements were taken with a 1.2 V supply.

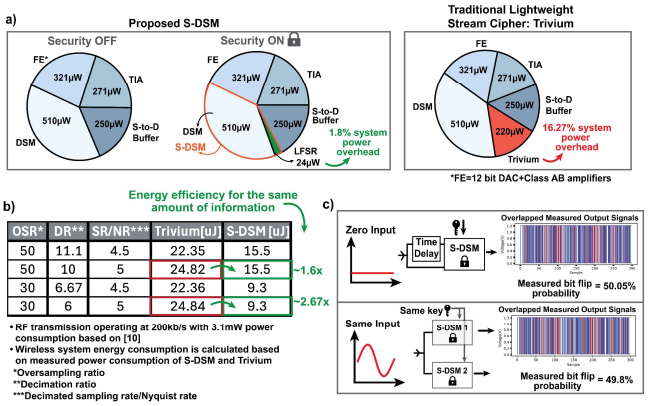

Fig. 4. (a) Measurement results for power breakdown of the chip, S-DSM overhead, and comparison with Trivium, (b) energy calculations for wireless capsule board including the RF front-end, and (c) measured bit flip probability and output signals under zero and same input attack threat models.

A. Security Measurements

A low-power stream cipher, Trivium [9], was designed on chip for benchmarking purposes. S-DSM only introduces a system power overhead of 1.8%, which is 9 times lower compared to Trivium (Fig. 4(a)). Although S-DSM requires transmission of undecimated sequence, the overall energy consumption of the capsule including the wireless communication [10], is reduced by up to 2.67 times (Fig. 4(b)).

A security evaluation measurement testbench was set up based on (1) to (3), using two channels of the same chip to encrypt the same message, using the same key. Channels are designed identically; the only deliberate difference is the dithering sequence. Using (3), the relative QN can be calculated from the outputs of the two channels. This was performed under two attack scenarios, zero-input and same key attacks.

In a conventional stream cipher, providing a DC input would reveal the output pattern of the PRNG. However, S-DSM continuously scrambles the output bits, hiding the PRNG output independent from the input. This was tested by providing the same DC input to both channels and comparing the output sequences. A bit-flip probability of 50.05% is measured, where 50% indicates complete randomness. Similarly, encrypting the same message with the same key is measured to maintain a bit-flip probability of 49.8% on average, as shown in Fig. 4(c). Additionally, over 120 megabytes of collected data, S-DSM achieved a Shannon entropy of 0.9999978907 bits and a min-entropy of 0.907679 bits, as evaluated using non-IID NIST SP800-90B RNG tests [11,12].

B. Electrical and Biological Measurements

The measured electrical front-end performance of the sensor chip is presented in Fig. 5. The low-noise TIA achieves an input-referred noise of 9.48 pA_{rms} integrated over a 100 kHz bandwidth. The TIA's 1-dB compression point at a gain setting of 3.30 kΩ is measured at 101.6 µA, providing a DR of 140.55 dB.

Fig. 6 demonstrates the biological performance measurement of the sensor chip. Glucose concentrations and *E. coli* cell density measurements are characterized as indicators of bioreactor health. Amperometry is demonstrated by applying a -0.1 V DC bias, which corresponds to the redox potential of H_2O_2 (a product of the glucose oxidase + glucose reaction) determined from CV measurements. This bias is

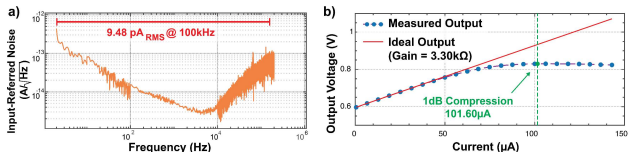

Fig. 5. Electrical performance measurements of the sensor front end. (a) 9.48 pA_{RMS} integrated noise over 100 kHz bandwidth, and (b) 1 dB compression at 101.6 μA input current.

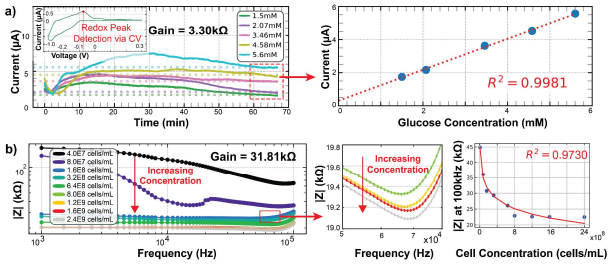

Fig. 6. Biological demonstrations of the chip for (a) redox peak detection via CV and glucose concentration measurement via amperometry, and (b) *E. coli* cell density measurement via EIS.

applied to measure glucose concentrations between 1.5 and 5.6 mM, as shown in Fig. 6, with a fitting accuracy of R^2 = 0.9981.

EIS was demonstrated by measuring cell concentrations of *E. coli* between 4.0x107 cells/mL and 2.4x109 cells/mL, with an excitation frequency of up to 100 kHz. Expectedly, impedance logarithmically decreases for higher cell concentrations [13].

V. Conclusion

A measured performance comparison of our work with the state-of-the-art sensors [14-18] for biosensing applications is shown in Fig. 7. This work achieves the highest bandwidth of 100 kHz and a DR of 140.55 dB, with an area of only 0.39 mm^2 per secured transmitter-receiver channel. It supports a TIA bandwidth of 100 kHz with an integrated input-referred noise level of 9.48 pA_{RMS} at the expense of increased power compared to lower-bandwidth designs [14-17]. This work demonstrates the first secure multimodal sensor, implemented in 65 nm CMOS (Fig. 7), for sustainable biomanufacturing applications.

	This Work	ISSCC'23 [14]	ISSCC'22 [15]	ISSCC'21 [16]	ISSCC'20 [17]	AD5940 (Commercial) [18]
Application	Bioreactor	Bioreactor	Biosensing	Wound	Drugs	Electrochemical
Modality	EIS, CV, Amp#	Multimodal##	Amp	CA###, CV, FSCV####, SWV#####	S/H-CA######,SWV	CA, Amp, CV, EIS, SWV
Technology (nm)	65	180	180	180	65	N.R.
VDD (V)	1.2	1.8	1.8 - 2.2	1.2	N.R.	2.8 - 3.6
Operating Bandwidth (kHz)	**100**	0.016	N.R.	1	2.5	200
Input Noise Level (pA_{rms})	9.48	14	0.039	2	15.2	N.R.
Maximum Input Current (μA)	**±101**	±10	0.0003	±6.14	±0.8	±750†
Dynamic Range (dB)	**140.55**	114	78	129.7	100	N.R.
Area (mm^2)	0.39††	10.24	23.31	8	0.385	15.12†††
Total Power (mW)	1.39 (continuous) 0.079(duty cycled)*	0.017** 0.022(peak)	58***	0.049****	0.22*****	4.55
Security	**Yes (S-DSM)**	No	No	No	No	No

N.R.= Not Reported

#Amperometry
##Reported modalities are amperometry and pH
###Chronoamperometry
####Fast-Scan Cyclic Voltammetry
#####Square Wave Voltammetry
######Sample-and-Hold Chronoamperometry

†Normal current mode
††Per secured transmitter-receiver channel
†††Wafer level chip scale package from datasheet

*Duty cycled sensor power for 50 minutes of sleep and 202 seconds of measurement
**Estimated for the potentiostat channel
***Including pixel power and circuit
****Includes pattern/clock generator, regulators, and digital blocks
*****Average power with duty cycling

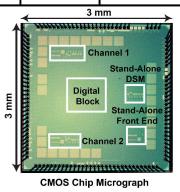

Fig. 7. Comparison with the state-of-the-art sensing platforms and commercial solutions for electrochemical measurements.

Acknowledgment

This publication was made possible with the support of The Bioindustrial Manufacturing and Design Ecosystem (BioMADE) and Schmidt Sciences; the content expressed herein is that of the authors and does not necessarily reflect the views of BioMADE or Schmidt Sciences. Additionally, this work was partially supported by Analog Devices Incorporation, Catalyst Foundation, and NSF CAREER program (2338792). The authors would like to thank Elizabeth Onderko and Mark Poole from Capra Biosciences for biomanufacturing process discussions, the Boston University Design Automation Manufacturing Processes (DAMP) Lab for providing the *E. coli* cell samples, and the Boston University Biological Design Center (BDC) for supporting the synthetic biology research infrastructure.

References

[1] C. L. Gargalo, et al., "Towards smart biomanufacturing: a perspective on recent developments in industrial measurement and monitoring technologies for bio-based production processes," Journal of Industrial Microbiology and Biotechnology, vol. 47, issue 11, Nov. 2020. DOI: 10.1007/s10295-020-02308-1.

[2] S. J. Kim, et al., "EQZ-LDO: A Near-Zero EDP Overhead, >10M-Attack-Resilient, Secure Digital LDO featuring Attack-Detection and Detection-Driven Protection for a Correlation-Power-Analysis-Resilient IoT Device," Symposium on VLSI Circuits, 2021. DOI: 10.23919/VLSICircuits52068.2021.9492345.

[3] K. Yang, et al., "Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey," IEEE Micro, vol. 37, issue 6, Nov./Dec. 2017. DOI: 10.1109/MM.2017.4241357.

[4] R. T. Yazicigil, et al., "Beyond Crypto: Physical-Layer Security for Internet of Things Devices," IEEE Solid-State Circuits Magazine, vol. 12, issue 4, Fall 2020. DOI: 10.1109/MSSC.2020.3021842.

[5] A. Yasar and R. T. Yazicigil, "Physical-Layer Security for Energy-Constrained Integrated Systems: Challenges and Design Perspectives," OJ-SSCS, vol. 3, 2023. DOI: 10.1109/OJSSCS.2023.3327326.

[6] A. C. Lazanas and M. I. Prodromidis, "Electrochemical Impedance Spectroscopy—A Tutorial," ACS Measurement Science Au, vol. 3, no. 3, pp. 162-193, 2023, doi: 10.1021/acsmeasuresciau.2c00070.

[7] Cogan SF, Ehrlich J, Plante TD. The effect of electrode geometry on electrochemical properties measured in saline. Annu Int Conf IEEE Eng Med Biol Soc. 2014;2014:6850-3. doi: 10.1109/EMBC.2014.6945202.

[8] Turick, C.E., Shimpalee, S., Satjaritanun, P. et al. Convenient non-invasive electrochemical techniques to monitor microbial processes: current state and perspectives. Appl Microbiol Biotechnol 103, 8327–8338 (2019). https://doi.org/10.1007/s00253-019-10091-y.

[9] C. De Cannière, "Trivium: A stream cipher construction inspired by block cipher design principles," Proc. Int. Conf. Inf. Secur., 2006. DOI: 10.1007/11836810_13.

[10] M. Song et al., "A 3.5mm×3.8mm Crystal-Less MICS Transceiver Featuring Coverages of ±160ppm Carrier Frequency Offset and 4.8-VSWR Antenna Impedance for Insertable Smart Pills," ISSCC, Feb. 2020. DOI: 10.1109/ISSCC19947.2020.9063083.

[11] M. Grujić and I. Verbauwhede, "TROT: A Three-Edge Ring Oscillator Based True Random Number Generator With Time-to-Digital Conversion," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, issue 6, June 2022. DOI: 10.1109/TCSI.2022.3158022.

[12] M. S. Turan, "Recommendation for the entropy sources used for random bit generation," Jan. 2018. DOI: 10.6028/NIST.SP.800-90B.

[13] Y.K. Lin, et al., "A New Biorecognition-Element-Free IDμE Sensor for the Identification and Quantification of *E. coli*.," Biosensors, Jul. 2022. DOI: 10.3390/bios12080561.

[14] Q. Lin, et al., "A 22μW Peak Power Multimodal Electrochemical Sensor Interface IC for Bioreactor Monitoring," ISSCC, Feb. 2023. DOI: 10.1109/ISSCC42615.2023.10067298.

[15] D. Hall, "A CMOS Molecular Electronics Chip for Single-Molecule Biosensing," ISSCC, pp. 204-205, Feb. 2022. DOI: 10.1109/ISSCC42614.2022.9731770.

[16] S.Y. Lu et al., "18.4 a wireless multimodality system-on-a-chip with time-based resolution scaling technique for chronic wound monitoring," ISSCC, Feb. 2021. DOI: 10.1109/ISSCC42613.2021.9365992.

[17] J. Chien et al., "A Cell-Capacitance-Insensitive CMOS Sample-and-Hold Chronoamperometric Sensor for Real-Time Measurement of Small Molecule Drugs in Whole Blood," ISSCC, Feb. 2020. DOI: 10.1109/ISSCC19947.2020.9063036.

[18] Analog Devices. "High Precision, Impedance, and Electrochemical Front End," AD5940/AD5941, 2019. URL: https://www.analog.com/media/en/technical-documentation/data-sheets/ad5940-5941.pdf