BioMEMS-Based Coding for Secure Medical Diagnostic Devices

Tuan Le, Gabriel Salles-Loustau, Laleh Najafizadeh, Mehdi Javanmard, Saman Zonouz
Electrical and Computer Engineering Department, Rutgers University

***Abstract*—Trustworthy and usable point-of-care solutions require not only effective disease diagnostic procedures to ensure delivery of rapid and accurate outcomes, but also lightweight privacy-preserving capabilities. In this paper, we present a Biomedical Microelectromachanical System (BioMEMS)-based sensor for portable, inexpensive smartphone-based biomarker detection. The biosensor presented here provides the ability for signal encryption at the physical sensor level to ensure patient's diagnostic confidentiality. Our results show that this design allow us to protect the samples measurements while accurately distinguish different test samples.**

I. Introduction

Healthcare management and delivery costs in developed countries are skyrocketing. In response to this trend, federal agencies have supported diverse lines of applied research in the use of technology for health monitoring and intervention [5], [10]. Applications such as point-of-care (POC) diagnostic devices takes advantage of state-of-the-art technologies to compile information about medical health securely and in real-time. POC enables a transition from reactive, hospital-centered to preventive, patient-centered and cost-effective health care.

Flow cytometry in microfluidic has been studied extensively as an alternate method for diagnosing and monitoring diseases such as HIV, malaria, and tuberculosis [1], [8]. However, current techniques require substantial laboratory work with stringent protocols. The possibility of integrating POC systems with mobile platforms has also been very recently demonstrated through the diagnosis of a series of conditions including vitamin-D deficiency and Kaposis Sarcoma disease [4], [6], [7]. These solutions either store the results in text file or distribute them over the network, exposing patient diagnostics to disclosure in case of data breach.

In this work we consider the design of a POC device biosensor for impedance cytometry. Our biosensor design addresses three major requirements:

***i)* portability and low cost.** Portable cytometry based POC devices can be used as the standard apparatus for medical diagnosis. The disposable biosensor contributes to the low cost of the test procedure. The low-cost constraint motivates the employment of widely deployed platforms such as smartphones to provide computational resources. The diagnostic solution should be easy-to-use to replace gold standard laboratory methods where highly trained technicians are required and must followed strict protocols.

***ii)* accuracy and performance.** Due to the importance of the medical diagnostic outcome, e.g., HIV diagnostic, the low-cost, portable biosensor should be designed without sacrificing the sensitivity of the diagnosis. The biosensor should be able to differentiate the biomarkers for diagnostic purposes. Furthermore, patients prefer accelerated testing procedures over the traditional clinical visit with longer time return of test result. Therefore, by using impedance cytometry biosensor and signal analysis, the POC micorfluidic device can perform diagnosis and return the result quickly comparing to the protracted practice at clinical visit.

***iii)* usable security and diagnostic confidentiality guarantees.** Patients are concerned about the confidentiality of their medical records [3]. Diagnostic disclosures may lead to undesired consequences such as insurance premium raises and negative social impacts. Currently, medical institutions are responsible for protecting the confidentiality of the patient diagnostics. In the proposed solution, the encryption mechanism is embedded in the sensor and is part of the data acquisition process. The encryption key is stored in the sensor and remain in the possession of the user.

Current methods to protect medical data leverage general purpose digital encryption algorithms such a DES, AES, Blowfish. All these ciphers operate on digital data, generating a digital ciphertext from a digital cleartext. In this paper we introduce an analog signal encryption scheme that generate an analog signal ciphertext. Contrary to scrambling techniques which typically operate on a plaintext signal, our sensor encryption mechanism is embedded in the signal acquisition process. Similarly to digital encryption techniques, our cipher robustness relies on the confidentiality of a randomly generated encryption key. The key corresponds to a one-time pad: the values embedded in the key correspond to the sensor parameters during data acquisition. Without the knowledge of these parameters it is impossible to analyze the acquired signal.

This paper is structured as follow: Section II present our approach for cytometry and encryption, Section III details the implementation the biosensor and Section IV show our results for our hardware-based encryption and test accuracy.

II. Overview

We introduce a new biosensor design for portable POC microfluidic diagnostic device with the ability of protecting the diagnostic confidentiality. The impedance cytometry biosensor utilizes the hardware-based analog encryption to

978-1-4577-0220-4/16/$31.00 ©2016 IEEE

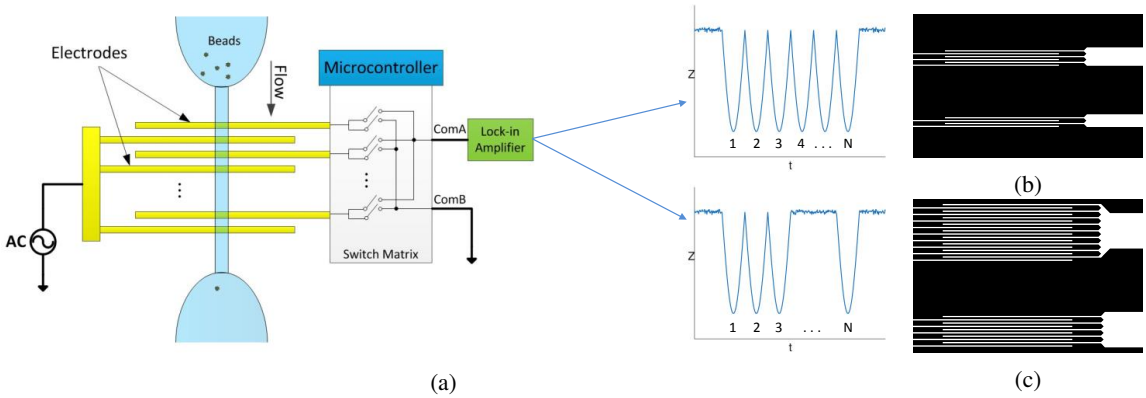


Fig. 1. Design of the integrated system. (a) Model of operation. Input electrodes commonly connected to an AC voltage source. Output electrodes are connected to an analog switch controlled by microprocessor. The controller randomly activates different subsets of electrodes, resulting in multiple peaks for each blood cell detected. (b) Design of the biosensor with 2 and 3 independent output electrodes. (c) Design of the biosensor with 5 and 9 independent output electrodes.

protect the cytometry measurements of cells passing through the channel. The design of multiple independent outputs can dynamically change its configuration (i.e., active output electrodes) to obfuscate the impedance measurement before sending it to the smartphone for signal analysis.

A microcontroller selects the random order of independent output electrodes and changes the configuration of biosensor active electrodes. The random selection of the microcontroller is stored on the POC device as the encryption key. The encrypted data is sent to smartphone for peaks analysis. The smartphone app analyzes the encrypted signal and counts the peaks caused by the impedance changes per passing particle through microfluidic device. The peak number does not necessarily correspond to the true number of particles that were presented, because more than one output electrodes may have been activated during data acquisition. The encryption key stored on the POC device corresponds to the number of active electrodes. Thus, the app must send the counted number of peaks back to the microfluidic device for decoding. The POC microfluidic device recovers the number of particles of different types and determines the user's disease condition through a simple threshold comparison, and notifies the user accordingly.

III. System Design

Our design expands the simple impedance cytometer [9] but uses multiple electrodes with multiple inputs shorted together and multiple independent outputs. Fig. 1a describes the operation model of the integrated system. We designed the microfluidic channel with an interdigitated multi-electrode pair configuration to mask the true count of cells passing through the microfluidic channel. Fig. 1b and Fig. 1c show the details of the computer aided design (CAD) of the sensing regions of the biosensors. The *lead* electrode in the array of output electrodes is defined as the electrode complemented only by one input electrode on one side. Thus, it will respond with a single voltage drop per passing cell; whereas the remaining output electrodes are surrounding on both sides by common excitation electrodes. Each of the remaining electrodes in the sensing regions will respond with a signature of double peak per passing cell.

Multi-Electrode Signal Encryption: A cell passing through the sensor channel generates multiple peaks thanks to the multiple electrodes. The output of the electrodes are selected or discarded through the multiplexer using a pseudo-random selection. This selection is randomly generated by the sensor microcontroller and constitutes the encryption key. The individual output from the electrodes are added together to form the cipher text. This encryption approach prevents a potential eavesdropper, without access to the signal encryption key, to discern the true number of cells that have passed by the channel. The strength of the biosensor's signal encryption methodology relies on the biosensor's reconfigurability to generate various signal fingerprints. The encryption key corresponds to a one-time pad scheme. The data acquisition time frame is split in periods of variable duration (from a few seconds up to a min). For each of this period, a different pattern of electrode is scheduled to be used. The key embeds the information about the period length and the sequence of electrode used.

System Integration: The microfluidic channel flow is driven by the external peristaltic pump, i.e., Harvard Apparatus 11 Pico Plus Elite. The Raspberry Pi microcontroller is used to generate the random selection sequence of the output electrodes in the microfluidic device through the 16:2 multiplexer MAX14661. The selected output sequence of the signal is recovered by the lock-in amplifier. We used a Zurich Instruments HF2IS impedance spectroscope coupled with a HF2TA trans-impedance amplifier to measure the electrical impedance across the microfluidic channel. The input electrode of the microfluidic channel is excited with a combination of $[500, 800, 1000, 1200, 1400, 2000, 3000, 4000]$kHz signals. Excitation voltage is at $1\,\mathrm{V}$ per excitation signal. The signal is sampled at $450\,\mathrm{Hz}$. The low pass filter is set to have cut off frequency at $120\,\mathrm{Hz}$.

To upload the encrypted signal to the signal analysis app on the smartphone, the controller (Raspberry Pi) is connected to the smartphone through a micro-USB to the USB cable. The signal analysis app leverages the Android USB accessory API [2], which allows the phone to detect the controller as soon as it is connected and launches the diagnostic user interface. The app has two purposes: it performs the signal

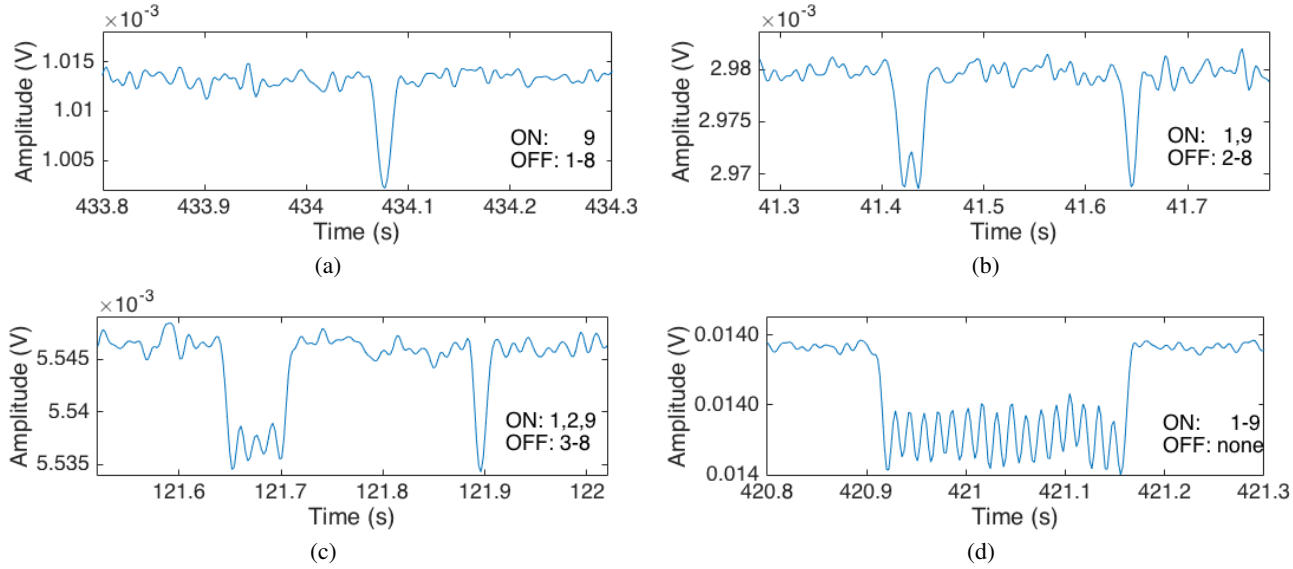
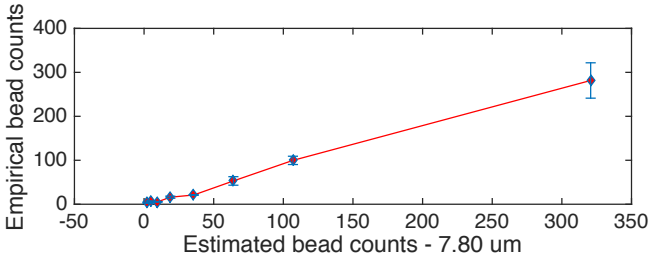
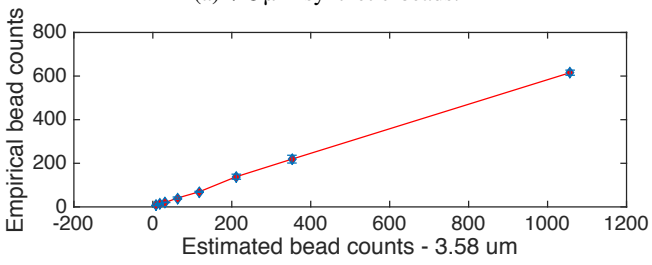


Fig. 2. Representative encrypted cytometry data of a sensor with 9 input electrodes and 9 independent output electrodes detecting a single bead. Pseudo-random sequence selection of output electrodes. (a) Signal of single bead when electrode 9 selected. (b) Signal of single bead when electrode 1 and 9 selected. (c) Signal of single bead when electrode 1,2, and 9 selected. (d) Signal of single bead when all electrodes selected (1-9). True number of peaks can only be detected/decrypted using unique key sequence.



(a) 7.8 µm synthetic beads.



(b) 3.58 µm synthetic beads.

Fig. 3. Measured bead count vs number of beads expected for different concentrations

analysis on the encrypted signal and it provides an interface for the user to start the blood test and provides a test progression feedback to the user on the screen.

IV. Evaluations

In our experiments, we evaluated the performance of the biosensor using micron-sized synthetic beads (7.8 µm and 3.58 µm - MicroChem) as well as blood cells, suspended in PBS 0.9 %. The solution is driven through the microfluidic channel at a rate of 0.08 µL.

To validate the flow rate in the microfluidic channel, the estimated fluid volume passing through the channel per unit of time is calculated using the time response of the bead passing an electrode pair. In Fig. 2, the estimate response time for the single peak is 20 ms. The approximated distance each bead travels when passing through a pair of electrodes is 45 µm (25 µm pitch, and 20 µm of two halves of electrode). The microfluidic channels are 30 µm in width and 20 µm in height. By dividing the volume of the solution passing through a pair of electrodes in the channel at the approximated time, the actual flow rate in the channel can be calculated to be 0.081 µL/min.

Fig. 2 illustrates how the sensor duplicates a peak generated for one electrode into multiple peaks signals to prevent the disclosure of number of beads passing through the channel. The figure shows the response of the biosensor to the 7.8 µm synthetic bead solution at 2 MHz. Fig. 2a shows the measured response of the biosensor when the *lead* output electrode is selected and the remaining output electrodes are routed to the ground port. Fig. 2b shows the response where the *lead* electrode is selected along with the last electrode. The *lead* electrode responds with a single peak whereas the remaining electrodes respond with double peaks per passing bead. Fig. 2c shows the response of the biosensor when the *lead* electrode 9 and electrode 1, 2 are selected. Fig. 2d shows the outcomes when all the electrodes are activated.

In peak-analysis, the accuracy of the biosensor is evaluated by comparing the empirically detected peaks and the estimated number of synthetic beads passing through the microfluidic channel. We diluted the 7.8 µm and 3.58 µm synthetic beads with PBS, which is a commonly used biological buffer that mimics physiological samples like blood. Synthetic beads are diluted at different concentrations to evaluate the empirical peak detection. The estimated number of elements in the solution is calculated according to the concentration information provided by the manufacturer. Four samples of each concentration are collected. The bead count data is taken from the first 5 min from each sample. Fig. 3a and Fig. 3b show the correlation of the empirical peak detec-

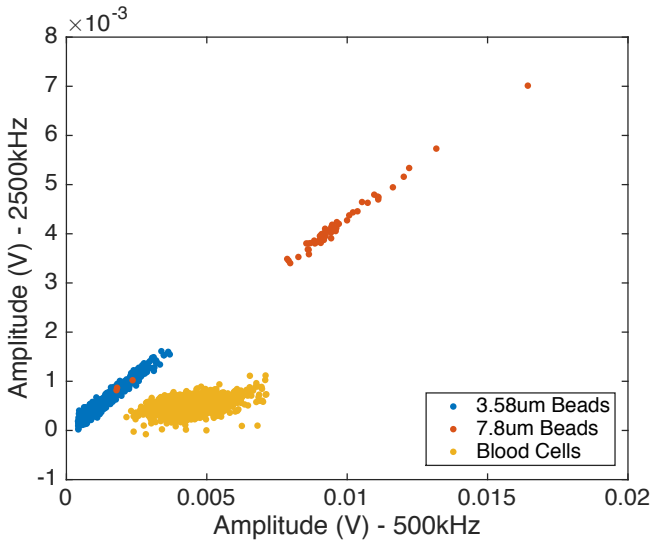


Fig. 4. Impedance differences of synthetic beads and blood cells.

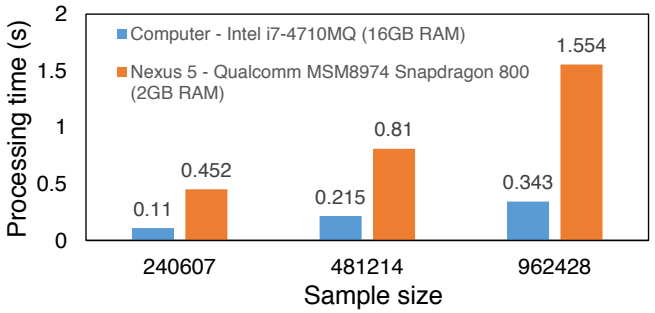


Fig. 5. Performances of data analysis on a computer and smartphone

tion to the estimated peak counts in the microfluidic channel for $7.8\,\mu\mathrm{m}$ and $3.58\,\mu\mathrm{m}$ synthetic beads. As expected, the empirical peak detection correlates to the estimated peaks when varying the concentrations. The discrepancy in bead counts is due to several reasons. For synthetic beads, the longer the duration of the experiments, the more error would be expected in the empirical bead counts as many beads sediment to the bottom of the inlet well never making it downstream to the sensor in the micro-channel. The other reason for the bead count loss is due to the beads being adsorbed to microfluidic channel walls. These are issues that can be ultimately resolved with optimization of channel material and surface chemistry, which was beyond the scope of the current work.

To validate the accuracy of the biosensor, we performed runtime diagnosis analysis multiple times over several blood samples. The typical diagnostics procedure takes a $0.1\,\mathrm{mL}$ of blood sample and completes all steps, including sensor encryption, mobile app signal processing, peak counts decoding and diagnostics, within 1 minute. Fig. 4 shows the impedance differentiation between the blood cells and synthetic beads at different excitation frequencies. Thus, the biosensor can utilizes the difference of dielectric properties and concentrations of cell types to give a reliable mobile diagnosis.

Fig. 5 shows performance comparison of the peak detection algorithm, when it runs on a standard computer system (possibly a cloud virtual machine) and on a smartphone device. It is noteworthy that a standard system provides much better performance than a mobile device, as the sample size grows larger. Aside from the storage capabilities, the enhanced computing power motivates the use of a cloud based service for handling peak detection and post-processing rather than using the smartphone. For smaller samples, however, the smartphone's app could be configured to perform the peak counting signal processing locally.

V. Conclusions and Future Works

In this paper, we introduced a new application for BioMEMS-based sensing in portable POC diagnostics solutions that provide secure, low-cost, and accurate outcomes through the use of smartphone computational resources. We described a in-sensor hardware-based analog signal encryption that enables cloud-based analysis for encrypted analog signals without disclosing measurements values. We implemented and integrated the biosensor circuitry and the software stack and evaluated its accuracy empirically using red blood cells and multiple solutions of synthetic beads.

The biosensor enables data encryption of the cell count at the hardware level. However, the encrypted signal still carries information about the cells. Specifically, the amplitude or width of the response peak can reveal information about the composition or shape of the cell. As future work, we plan to leverage two more parameters to protect both of these information: application of random gains to each output electrode to modify the original amplitude, and also continuous alteration of the fluid speed to create arbitrary widths for passing cells of identical types. These two parameters can be incorporated as part of the encryption key for signal transformation.

References

[1] P. Balakrishnan, M. Dunne, N. Kumarasamy, S. Crowe, G. Subbulakshmi, A. K. Ganesh, A. J. Cecelia, P. Roth, K. H. Mayer, S. P. Thyagarajan, and S. Solomon. An inexpensive, simple, and manual method of cd4 t-cell quantitation in hiv-infected individuals for use in developing countries. *JAIDS Journal of Acquired Immune Deficiency Syndromes*, 36(5):1006–1010, 2004.

[2] A. Developers. USB Accessory. https://developer.android.com/guide/topics/connectivity/usb/accessory.html, 2015. [Online; accessed 19-July-2015].

[3] J. M. Eisenberg. Can you keep a secret? *Journal of general internal medicine*, 16(2):131–133, 2001.

[4] S. Lee, V. Oncescu, M. Mancuso, S. Mehta, and D. Erickson. A smartphone platform for the quantification of vitamin d levels. *Lab on a Chip*, 14(8):1437–1442, 2014.

[5] C. LeRouge, V. Mantzana, and E. V. Wilson. Healthcare information systems research, revelations and visions. *European Journal of Information Systems*, 16(6):669, 2007.

[6] X. Liu, T.-Y. Lin, and P. B. Lillehoj. Smartphones for cell and biomolecular detection. *Annals of biomedical engineering*, 42(11):2205–2217, 2014.

[7] M. Mancuso, E. Cesarman, and D. Erickson. Detection of kaposi's sarcoma associated herpesvirus nucleic acids using a smartphone accessory. *Lab on a Chip*, 14(19):3809–3816, 2014.

[8] F. E. McKenzie, W. A. Prudhomme, A. J. Magill, J. R. Forney, B. Permpanich, C. Lucas, R. A. Gasser, and C. Wongsrichanalai. White blood cell counts and malaria. *Journal of Infectious Diseases*, 192(2):323–330, 2005.

[9] J. Mok, M. N. Mindrinos, R. W. Davis, and M. Javanmard. Digital microfluidic assay for protein detection. *Proceedings of the National Academy of Sciences*, 111(6):2110–2115, 2014.

[10] P. Shekelle, S. C. Morton, and E. B. Keeler. Costs and benefits of health information technology. 2006.