Microfluidic Encryption of On-Chip Biochemical Assays

Sk Subidh Ali[†], Mohamed Ibrahim[‡], Ozgur Sinanoglu[†], Krishnendu Chakrabarty[‡], and Ramesh Karri[↑]
[†]Indian Institute of Technology Tirupati,[†]New York University Abu Dhabi, [‡]Duke University, [↑]New York University

Abstract: Recent security analysis of digital microfluidic biochips (DMFBs) has revealed that the DMFB design flow is vulnerable to IP piracy, Trojan attacks, overproduction, and counterfeiting. An attacker can launch assay manipulation attacks against DMFBs that are used for clinical diagnostics in healthcare. Moreover, security for lab-on-chip has emerged as an important design criterion in view of the recent findings about spurious test results from Theranos Edison devices. We present encryption based on microfluidic multiplexers, wherein an assay is encrypted with a secret-key pattern of fluidic operations. Only an authorized user of the DMFB possesses the secret-key pattern and can get the correct assay outcome. Simulation results show that for practical assays, e.g., protein dilution, an 8-bit secret key is sufficient for overcoming threats to DMFBs.

I. Introduction

A. Background

Digital microfluidics is a lab-on-a-chip technology that enables miniaturized analysis systems for biochemical applications such as point-of-care clinical diagnostics [1] and DNA sequencing [2]. A number of techniques have been presented in recent years to advance design automation and optimization of digital microfluidic biochips (DMFBs) [3]. These include architectural-level synthesis, module placement, and droplet routing. The current commercial production of DMFB systems follows a custom application-specific design flow, where all stages of the design flow are performed in-house [4]. In the general-purpose design flow anticipated in the near future, outsourcing will be an attractive alternative and commercial software will supersede homegrown ad-hoc CAD software; third-party intellectual property (IP) blocks will replace the in-house libraries for synthesis. Eventually, mask production, fabrication and testing of DMFBs are likely to be outsourced [5]. While outsourcing will enable cost-effective DMFB production, it will imply that several steps in DMFB system design will rely on potentially untrusted third parties.

B. Security Threats to DMFBs

In the DMFB design flow shown in Figure 1, a biocoder provides the IP (the bioassay) in the form of a sequencing graph. The biocoder is the authorized owner of the IP. However, parties other than the biocoder in the design flow can be untrusted. We list below the following vulnerabilities associated with the DMFB design flow:

1) **Hardware Trojans in DMFBs:** A hardware Trojan is a malicious modification of the circuitry of an integrated circuit [6]. The objective of inserting a Trojan is to control, modify, and disable the system or leak sensitive information from the system. The lack of any security measures in DMFB design process allows a malicious designer to insert hardware Trojans by altering the design. A malicious individual in the foundry may also insert hardware Trojans into the DMFB. An attacker can insert a hardware Trojan by altering the calibration process for the embedded capacitive sensors or optical detectors, leading to incorrect readings during run-time. A malicious user can insert a Trojan by altering the actuation sequences, which are voltage patterns to the electrodes of a DMFB to control droplet transportations.
2) **IP Theft:** In DMFBs, the bioassay protocol is the proprietary IP that is generally given to the designer in the form of a sequencing graph. A malicious designer can sell the IP in black market. An attacker with physical access to a DMFB, can reverse-engineer the DMFB by depackaging, delayering, and image processing. DMFB designs are less complex compared to their CMOS counterpart, thus making them easier to reverse-engineer by adapting CMOS specific reverse-engineering techniques [7].
3) **Counterfeiting DMFBs:** An attacker may recycle used DMFBs and sell them as new; this can adversely affect the safety, security, and reliability of the DMFB application.
4) **Over-production of DMFBs:** An untrusted DMFB foundry may fabricate more DMFBs than authorized by the owner of the IP and sell them illegally.

C. Real world examples

Recently, Theranos inc. developed a proprietary handheld Edison blood testing device that takes blood from a patient's finger and performs a variety of blood tests. However, there is speculation that this proprietary blood-testing approach excessively dilutes the sample droplets and uses traditional blood-testing machines yielding spurious test results [8]. Similarly, the devices being used in the DNA lab of the Austin Police department altered the DNA test methodology from the standard [9]. Such altered tests results can misguide medical decisions. These two anecdotes point to the dilution/contamination attack on DMFBs reported in [5]. However, no countermeasures have been proposed against these and other attacks.

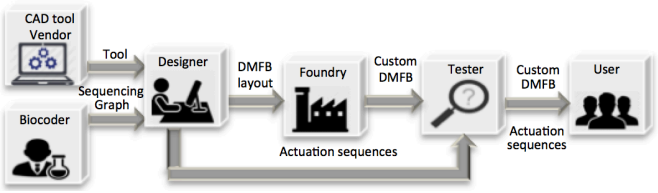

Fig. 1: DMFB design flow.

978-1-5090-2959-4/16/$31.00 2016 IEE

D. Contributions

In this paper, we develop a countermeasure by leveraging microfluidic logic operations. We introduce the concept of microfluidic encryption, where assay operations are multiplexed with additional microfluidic operations that are implemented using a carefully designed microfluidic multiplexer. The multiplexing is controlled by a secret microfluidic-pattern key that is known only to authentic users of the DMFB. If the correct key is provided during assay execution, the desired sequence of microfluidic operations will be permitted and the bioassay will be enabled. On the other hand, a wrong key will lead to incorrect assay execution.

We develop microfluidic multiplexer logic to enable fluidic input-based control of droplets. We propose a microfluidic encryption technique to protect assays against Trojans, DMFB IP piracy, overproduction, and counterfeiting. We present analysis to highlight the correlation between DMFB design parameters and security metric. Finally, we present case studies on benchmark assays to demonstrate the effectiveness of the countermeasure.

II. Microfluidic Encryption

Robust countermeasures are needed to address the aforementioned threats. Our premise is that protection at the microfluidic level will be especially effective to ensure the integrity of bioassay outcomes. The concept of hardware metering based protection of IP with a secret key has been explored for CMOS chips [10]. We propose to adapt this solution for DMFBs and incorporate microfluidic encryption into the synthesis of biochemistry protocols. This approach can be viewed as *encryption at the microfluidic level*, whereby the sequencing graph[1] G for a bioassay protocol is transformed to a different sequencing graph G' ($G \subset G'$) through a sequence of control data (the "secret key") that is known only to an authorized user. If the correct key is provided during assay execution, the desired sequence of microfluidic operations will be permitted and the bioassay will be enabled. On the other hand, if the key provided by a user does not match the secret key, the flow of droplets through the DMFB will be blocked and no detection results will be provided by the system.

A. Microfluidic Encryption Methodology

For microfluidic encryption, we propose the use of 2-to-1 fluidic multiplexers with two fluidic data inputs, one fluidic control input, and one fluidic data output. The control input can be viewed as one bit of the "secret key". A number of such multiplexers can be inserted into G to form G'. The sequencing graph G' executes the correct assay operations only if these multiplexers are controlled by the correct secret key input. Since only one droplet is forwarded to downstream assay operations, the additional droplets at some point must be routed to an on-chip waste reservoir. To prevent an attacker from making an inference about droplet transportation to the waste reservoir, the additional droplets can be held in randomly chosen temporary locations on the DMFB, and discarded with the waste resulting from the biochemical procedures at the end of the assay.

[1]The high-level specification of an assay is represented by a sequencing graph $G = (V, E)$, where a node $v \in V$ corresponds to a fluid-handling operation (e.g., dispensing, mixing, dilution, and detection) and an edge $e \in E$ between two nodes $(v1, v2)$ represents the dependency between them.

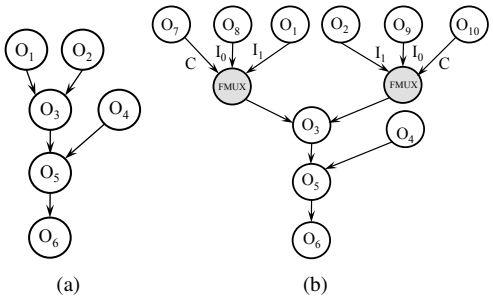

Fig. 2: Microfluidic encryption: (a) An assay that mixes three droplets, O_1, O_2, and O_3, and then the detection operation is done at O_6 on the resultant droplet. (b) Encrypted sequencing graph with two fluidic multiplexers (FMUX) to control the droplet generated from O_1 and O_2. The correct control input, i.e., the key, ensures that the droplets O_1 and O_2 are selected.

Figure 2(a) shows a segment of the sequencing graph of a generic bioassay, where the two dispensed droplets in O_1 and O_2 are mixed in O_3. The droplet resulting from O_3 is again mixed in O_5 with the droplet generated from O_4. A detection operation O_6 is performed on the droplet that results from O_5. The encrypted sequencing graph is shown in Figure 2(b). The two input droplets to mixer O_3 are controlled by the control inputs of the multiplexers. The presence of a control droplet (logic 1, as explained below) is known only to the authorized user. An inverse implementation can also be considered, whereby the absence of a control droplet (logic 0) forwards the required droplet. We envision strategic insertion of several such fluidic multiplexers in the sequencing graph; the associated presence (logic 1) or absence (logic 0) of control droplets constitute the secret key. Only an authorized user would know the bit pattern that "opens" all the fluidic multiplexers to forward droplets as required.

B. Realization of a Fluidic Multiplexer

Digital microfluidic logic gates were introduced in [11] to enable built-in self-test (BIST) for DMFBs. A number of key logical operations (e.g., AND, OR, and inverter) were experimentally demonstrated using a fabricated DMFB. We adopt the concept of microfluidic logic gates to develop a fluidic multiplexer. Figure 3 shows the sequencing graph of the fluidic multiplexer, where I_1 and I_2 are the inputs for the data droplets and C is the control input. The output droplet is produced at Z. A dotted edge e' between nodes (v_1, v_2) defines that during routing, droplet v_1 has to be transported to the electrode storing v_2, where $v_1, v_2 \in G$ and G is the sequencing graph. For example, in Figure 3(a), the droplet R_2 will be transported to electrodes storing two droplets generated by the S_1 split operation. This implies that R_2 will mix in W_1 and M_2 if and only if S_1 produced two half unit-

volume droplets. In the other case, the droplets will follow the sequencing graph without the dotted edges. Figure 3(b) shows the fluidic operations when the droplet C is present; the execution of the leftmost subgraph will transport the input droplet I_1 to Z while the other two subgraphs will result in half unit-volume droplets. Figure 3(c) shows the fluidic operations in the absence of C, where the execution of the subgraph on the right will lead to the transportation of the input I_2.

III. Aging reinforces DMFB Security

Aging has a greater impact on DMFBs as compared to their CMOS counterpart. It is known that DMFBs degrade quickly and must be discarded within a few hours [12]; the short lifetime can be attributed to the rapid degradation of electrodes during DMFB operation. In our framework, we take advantage of DMFB electrode degradation to enhance system security against potential attacks. We exploit the fact that electrodes can withstand only a limited number of actuations before dielectric breakdown occurs [13]. Therefore, an attacker can make only a limited number of attempts to break the security scheme (i.e., guess the secret key through trial and error) before the DMFB fails. Two DMFB-related parameters play a crucial role in order to characterize and evaluate the security countermeasure: (1) the number of electrode actuations per electrode; (2) the thickness of the dielectric layer. Electrode degradation (or lifetime) can be analyzed on the basis of the threshold voltage (V) needed to transport a droplet between adjacent electrodes based on the electrowetting phenomenon.

We propose to design and fabricate a DMFB such that it permits reliable actuation only for a certain duration, thus limiting the usability of the DMFB if an attacker attempts to obtain the secret key through brute-force trial and error. For example, given the dielectric thickness for the dielectric material, the designer can derive the breakdown voltage and the threshold voltage. Using these two values, we can determine the maximum number N of allowable electrode actuations for reliable execution of the DMFB. Since each attempt to run the target bioassay with a random key leads to a known number of electrode actuations, N can be used to derive an upper limit n ($n << N$) on the number of attempts that an attacker can make before the chip breaks down.

IV. Simulation Results

In this section, a detailed security analysis is provided to evaluate the effectiveness of microfluidic encryption. Microfluidic encryption is applied to three benchmark assays— in-vitro, PCR, and Protein— and area and performance overheads are obtained. We have used a custom C++ program to encrypt a given assay by optimally inserting multiplexers into the sequencing graph. The open-source DMFB synthesis tool [14] is used to synthesize assays. For the synthesis flow, we used list scheduler, left-edge placer, and the modified mazerouter [14].

A. Security Analysis

In this subsection, we examine the security benefits associated with the use of fluidic multiplexers.

1) Number of Electrode Actuations: Figure 4 shows the maximum number of electrode actuations corresponding to the number of multiplexers being used. Without encryption, in-vitro, PCR, and Protein assays require 8, 2, and 22 actuations, respectively. These numbers increase in a linear fashion with the number of multiplexers, necessitating an increase in the dielectric thickness in order to retain the same lifetime of the DMFB. On the other hand, a fixed dielectric thickness will degrade the lifetime of the DMFB with an increase in the number of multiplexers. By carefully choosing the dielectric thickness and the number of multiplexers, the designer can not only protect the DMFB against a brute-force attack, but also quantify the strength of this countermeasure. Since DMFBs are disposable and intended for one-time use, a reduction in the number of times that it can be used does not affect its applicability in practice.

2) Protection against brute-force attacks: The number of multiplexers defines a security metric for microfluidic encryption. As discussed in Section III, the designer can carefully choose the number of multiplexers and the DMFB dielectric thickness to thwart attacks. For example, with a 2.3 μm dielectric thickness and an eight-bit key, an attacker can be limited to only five brute-force attempts. Therefore, the attacker cannot exhaustively try all 256 possible keys. It may be noted that the microfluidic encryption is based on one common secret key to activate all the DMFB chips, as all these chips are generated based on the same encrypted sequencing graph. As shown in [15], there exists significant chip-to-chip variability in DMFB fabrication, characterization, and measurements. Such variability can be incorporated into the proposed fluidic encryption framework to assign a unique key to each DMFB.

3) Protection against hardware Trojan attacks: The hardware Trojan attacks described in [5] manipulate the assay outcome by altering the sequencing graph. In order to launch such a manipulation-based attack, the attacker must have a prior knowledge of the assay. Microfluidic encryption obfuscates the assay; therefore, the attacker cannot alter the assay to get a meaningful outcome that can pass scrutiny.

4) DMFB supply-chain security: In the proposed framework, any party in the DMFB supply chain other than the biocoder can be malicious. To ensure security, the biocoder will provide the designer only an encrypted sequencing graph for the assay, but does not hand over the secret key. Without the secret key, a malicious designer is thwarted from extracting the assay protocol, and hence, cannot steal the IP. A malicious foundry can overproduce DMFBs, but without the secret key, overproduced DMFBs will be useless. In the same way, it is evident that the proposed microfluidic encryption provides protection against counterfeiting.

B. Area Overhead

The area overhead is calculated as the number of electrodes in the electrode array. Our results show that the number of electrodes increases linearly with the number of multiplexers. Eight multiplexers lead to 286%, 139%, and 170% increase in

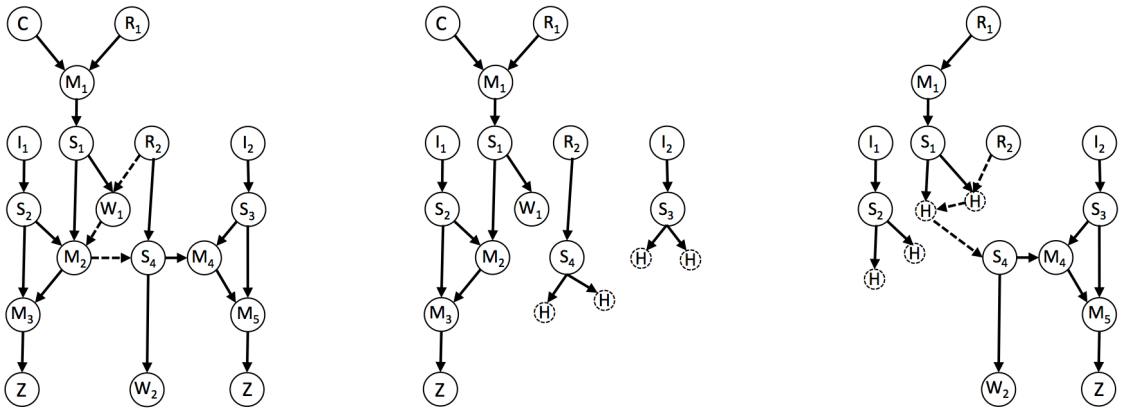

Fig. 3: Sequencing graph of the fluidic multiplexer: (a) Sequencing graph corresponding to the multiplexer. C, R, and I are control, reference, and input droplets, respectively. The dotted lines represent additional condition, i.e., during routing, droplet R will be transported to the electrodes storing droplets generated from S_1. (b) Multiplexing in the presence of the control droplet. I_1 is transported to Z by one of the droplets generated from S_1. Droplet R_2 will not be able to mix with the droplets generated from S_1, hence, splits into half volume droplets (shown as H). (c) Multiplexing in the absence the control droplet. In this case, R_2 will mix with two half-volume droplets generated from S_1, hence, I_2 will be transported to Z.

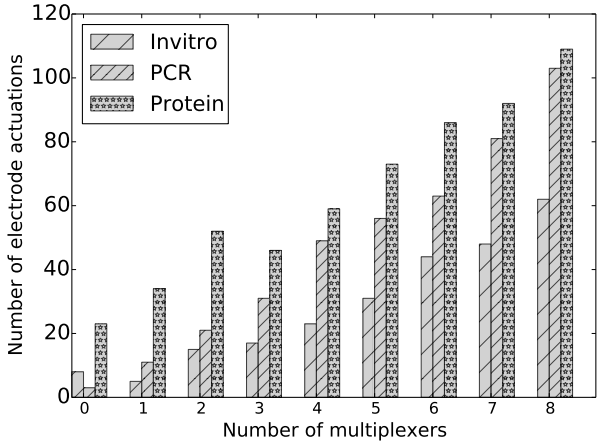

Fig. 4: Change in the number of electrode actuations with an increase in the number of multiplexers.

the number of electrodes for in-vitro, PCR, and Protein assays, respectively. The increase in the DMFB footprint will be much less than the increase in the number of electrodes, because in real DMFBs, the input/output pads are much larger than the actual microfluidic array [15].

V. Conclusions and Future Work

We have described the first microfluidic encryption strategy that protects biochemical protocols through the insertion of fluidic multiplexers in the DMFB design. These multiplexers are controlled by a secret key that is not revealed by the biocoder. Any attempt by an attacker to identify the secret key via repeated trials is thwarted by the short lifetime of DMFBs and the upper limit on the number of times an electrode can be actuated. The security provided by microfluidic encryption can be quantified in terms of the number of multiplexers inserted in the sequencing graph and the thickness of the dielectric layer. However, the security of the proposed microfluidic encryption is based on the assumption that each DMFB will have a unique key. In our future work, we plan to develop an efficient key management scheme to assign a unique key to each DMFB.

References

[1] R. Sista *et al.*, "Development of a digital microfluidic platform for point of care testing," *Lab on a Chip*, vol. 8, no. 12, pp. 2091–2104, 2008.

[2] D. J. Boles *et al.*, "Droplet-based pyrosequencing using digital microfluidics," *Analytical Chemistry*, vol. 83, no. 22, pp. 8439–8447, 2011.

[3] K. Chakrabarty, "Design automation and test solutions for digital microfluidic biochips," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 1, pp. 4–17, 2010.

[4] Illumina, "Illumina neoprep library prep system," http://www.illumina.com/systems/neoprep-library-system.html/.

[5] S. S. Ali *et al.*, "Security assessment of cyberphysical digitalmicrofluidic biochips," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 13, no. 3, pp. 1–14, 2015.

[6] M. Rostami *et al.*, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[7] R. Torrance *et al.*, "The state-of-the-art in IC reverse engineering," in *Proc. of CHES*, 2009, pp. 363–381.

[8] Vox Explainers, "The Theranos controversy, explained," http://www.vox.com/2015/10/20/9576501/theranos-elizabeth-holmes, 2015.

[9] Tony Cantu, "Austin Police Chief Shuts Down DNA Lab Amid Concerns Over Testing Methods," http://www.forensicmag.com/article/2016/06/austin-crime-lab-shut-down-over-concerns, 2016.

[10] Y. Alkabani *et al.*, "Active hardware metering for intellectual property protection and security," in *Proc. of USENIX Security*, 2007, pp. 291–306.

[11] Y. Zhao *et al.*, "Digital microfluidic logic gates and their application to built-in self-test of lab-on-chip," *IEEE Trans. Biomed. Circuits Syst.*, vol. 4, no. 4, pp. 250–262, 2010.

[12] C. Dong *et al.*, "On the droplet velocity and electrode lifetime of digital microfluidics: voltage actuation techniques and comparison," *Microfluidics and Nanofluidics*, vol. 18, no. 4, pp. 673–683, 2015.

[13] F. Mugele *et al.*, "Electrowetting: from basics to applications," *Journal of Physics: Condensed Matter*, vol. 17, no. 28, p. R705, 2005.

[14] D. Grissom *et al.*, "A field-programmable pin-constrained digital microfluidic biochip," in *Proc. of IEEE/ACM DAC*, 2013, pp. 1–9.

[15] K. Hu *et al.*, "Experimental demonstration of error recovery in an integrated cyberphysical digital-microfluidic platform," in *Proc. of IEEE BioCAS*, 2015, pp. 1–4.