Supply-Chain Security of Digital Microfluidic Biochips

Sk Subidh Ali, New York University, Abu Dhabi
Mohamed Ibrahim, Duke University
Jeyavijayan Rajendran, University of Texas at Dallas
Ozgur Sinanoglu, New York University, Abu Dhabi
Krishnendu Chakrabarty, Duke University

Digital microfluidic biochips (DMFBs) implement novel protocols for highly sensitive and specific biomolecular recognition. However, attackers can exploit supply-chain vulnerabilities to pirate DMFBs' proprietary protocols or modify their results, with serious consequences for laboratory analysis, healthcare, and biotechnology innovation.

Advances in digital microfluidics have led to the creation of miniaturized digital microfluidic biochips (DMFBs) for applications such as immunoassays for point-of-care medical diagnostics, DNA sequencing, and airborne particulate-matter detection.[1] Miniaturization's benefits include reduced reagent consumption, smaller sample requirements, reduced analysis time as a result of increased reaction speed, human intervention–free control of droplets via design automation, and low contamination risk.

Driven by technological advances and the promise of microbiology applications, algorithmic solutions have been developed that automate the design and optimization of DMFBs. Design automation research has focused on on-chip synthesis of biochemistry, sample preparation, chip I/O-count minimization, and defect tolerance.[2] Because these design tools automate DMFB design

0018-9162/16/$33.00 © 2016 IEEE

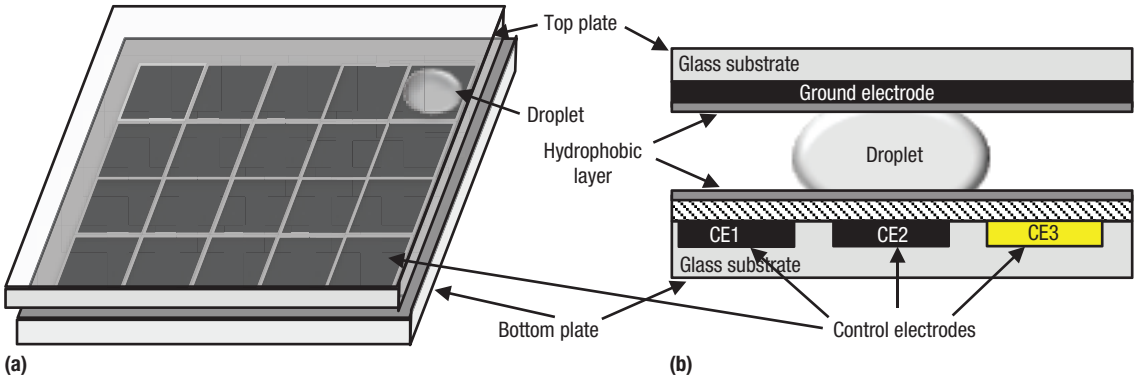

FIGURE 1. Schematic view of a digital microfluidic biochip (DMFB). (a) A DMFB with a 2D electrode array. (b) Side view of the DMFB with three unit cells, CE1–3. (Source: M. Pollack, A. Shenderov, and R. Fair, "Electrowetting-based Actuation of Droplets for Integrated Microfluidics," *Lab on a Chip*, vol. 2, no. 2, 2002, pp. 96–101.)

and on-chip bioassay execution, DMFB users such as biochemists and clinicians no longer need to intervene manually and can focus exclusively on developing innovative analytical chemistry protocols for biomolecular recognition. Yole Développement forecasts that the world market for microfluidic devices will grow from $1.1 billion in 2011 to $5.7 billion by 2018.[3] As an indicator of commercial success, Illumina, the industry leader in DNA sequencing, recently introduced microfluidic biochips to the marketplace for sample preparation.

Despite DMFBs' advantages for clinical diagnosis, immunoassays, and DNA sequencing, little attention has been devoted to their security. Like their CMOS counterparts, DMFB chips are also prone to malicious modifications (hardware Trojans), reverse-engineering, and counterfeiting. A Trojan in a DMFB could manipulate assay outcomes, disrupt the DMFB, or steal its secret information. Similarly, intellectual property (IP) piracy also threatens DMFBs. Generally, the DMFB's IP is the bioassay itself, which is proprietary to the individual or organization that developed it. If the DMFB falls into an attacker's hands, the attacker can reverse-engineer the DMFB to steal the IP. In this article, we shed light on security vulnerabilities in the supply chain of DMFBs and propose potential countermeasures.

DMFB SUPPLY CHAIN

A DMFB consists of a two-dimensional electrode array and on-chip reservoirs, as Figure 1a shows.[1] By utilizing the effect of electrowetting, nanoliter droplets containing biological samples and reagents can be manipulated on the chip without the need for external pressure sources. Figure 1b is a side view of three unit cells on a DMFB. The upper plate is a large electrode that covers all cells on the array and serves as the ground electrode for all unit cells. When the biochip is used, a common voltage is applied to the upper plate; thus, all the array's unit cells have the same voltage on their upper electrodes. The lower plate of the unit cell consists of an array of discrete control electrodes. During chip operation, the array's unit cells might have different voltages on their lower electrodes. The movement of droplets is determined by signals applied to the discrete electrodes. The term "control voltages applied to electrodes" refers to the voltages applied to the lower electrodes of the chip's unit cells.

Droplets of a bioassay are confined between the upper and lower electrodes. To move a droplet, a high voltage is applied to a unit cell adjacent to the droplet (the cell with a yellow-colored electrode in Figure 1b), and, simultaneously, a low voltage is applied to the cell currently occupied by the droplet. Variation in the voltage levels leads to different levels of interfacial tension across the droplet boundaries, and thus the droplet is forced to move. Note that the voltage drop across a cell can be changed over time to coordinate multiple droplets, depending on the protocol design. The sequence of voltage signals applied to an electrode over time is referred to as an actuation sequence.

The electrical parts of a DMFB include the memory, the electrodes, and the connection between the control pins and electrodes. The droplets and fluid-handling components such as mixers, storage units, and detectors make up the biochemical parts. The protocol implemented by the sequencing graph and the biochemical reactions between droplets represent the biochemical components.

Digital microfluidic systems were recently introduced into the marketplace; therefore, today's commercial production follows a fully customized design flow (www.siliconbiosystems.com). In this application-specific flow, all stages of the design flow are performed in-house. However, because of these systems' inherent reconfigurability, DMFB design is anticipated to transform from an application-specific to a general-purpose approach,[4] which will allow third parties to become involved in the DMFB design flow. Thus, potentially untrustworthy entities' participation in design and

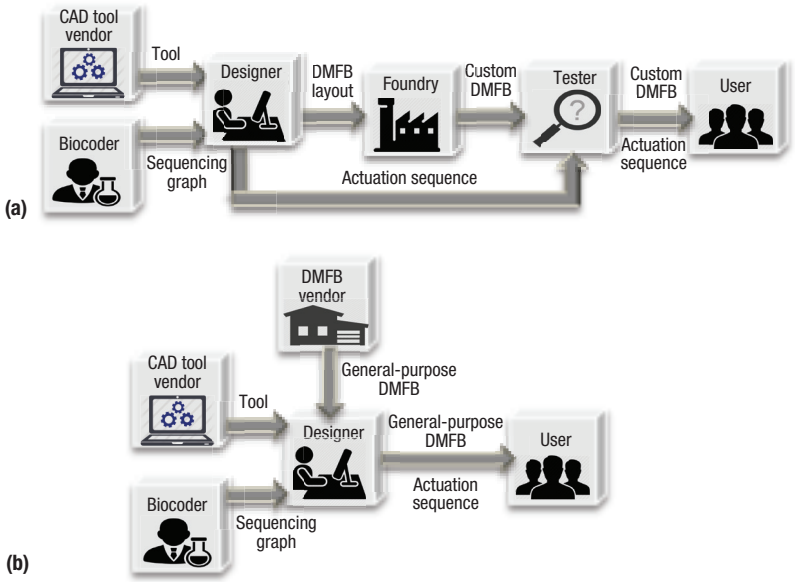

FIGURE 2. Participants in (a) a custom (application-specific integrated-circuit) DMFB design flow and (b) a general-purpose (field-programmable gate-array) DMFB design flow.

manufacturing could lead to DMFB security vulnerabilities.

In a custom DMFB design flow, shown in Figure 2a, biocoders, who convert the specification of the bioassay into a sequencing graph, control the DMFB platform. They send the biochemical protocol sequencing graph to the design house, from which they get the actuation sequences and the application-specific DMFB and use them to program the DMFB. The DMFB platform runs the assay according to the actuation sequences.

In a general-purpose DMFB design flow, shown in Figure 2b, a DMFB that can run any bioassay is procured.[4] The sequencing graph of a bioassay is synthesized onto the DMFB, and the corresponding actuation sequences are generated. In this design flow, it is reasonable to assume that the biocoder, designer, tester, and user are the same individual. This design flow applies to cyber-physical DMFB systems in which, based on sensor feedback, the synthesis step is repeated and new actuation sequences are generated on the fly.[2]

TROJANS

A hardware Trojan is a malicious modification that disables or destroys a system based on specific inputs or a specific time. Hardware Trojans are also designed to leak secret information embedded in integrated circuits (ICs). A Trojan taxonomy classifies these threats and helps develop frameworks to detect and mitigate them.[5]

Today's DMFBs lack security measures, making them attractive targets for Trojan attacks. A Trojan can be inserted into a DMFB system to manipulate the assay outcome, leak the sensitive and proprietary bioassay protocols used in DMFBs, or damage the DMFB so as to make it unusable. DMFB design flows are similar to those of CMOSs; therefore, most of the contemplated hardware Trojans for CMOS chips are applicable to DMFBs as well. A DMFB Trojan taxonomy is shown in Figure 3. Trojans can be broadly categorized based on Trojan insertion phase, abstraction level, trigger mechanism, effect, and location.

Insertion phase

A typical DMFB design flow traverses the following phases: specification, design, fabrication, testing and calibration, assembly, and in-field. As Figure 3 shows, DMFB Trojans can be inserted in any of these phases.

Specification (biocoding). The biocoders provide a high-level specification of the assay in the form of a sequencing graph along with the assay completion time and DMFB size. The biocoders themselves can be malicious, providing the malicious version of the assay to the design house. For example, they can add more dilution or mixing operations to the original assay to alter its outcome. During runtime, the original actuation sequences can be replaced by the malicious version, which, once executed, will alter the assay outcome.

Design. The designers receive the high-level specification of the assay and synthesize it to generate the actuation sequences and the DMFB layout. Designers can replace the sequencing graph with a malicious sequencing graph by altering the microfluidic library, which consists of different microfluidic functional modules such as mixers and storage units, along with their parameters such as width, length, and operation duration. For example, malicious designers can alter the mixing time or the incubation time, which will lead to an incomplete diffusion between the samples and the experimental reagents, resulting in incorrect assay outcome.

Fabrication. The DMFB is fabricated from the layout provided by the design house. A malicious entity in the foundry can insert a Trojan by tampering with the DMFB. For example, actuation voltage of certain electrodes can be altered. Reduced actuation voltage will not be able to actuate a droplet, whereas excessive actuation voltage might

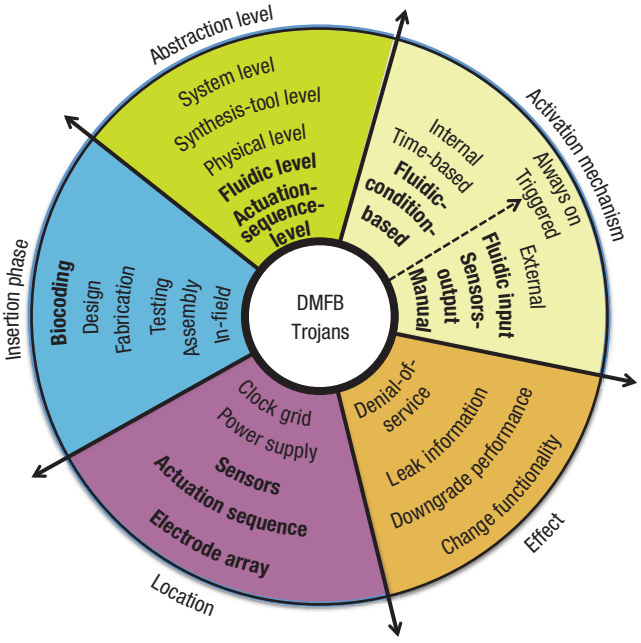

FIGURE 3. DMFB Trojan taxonomy. Trojan categories in bold text are unique to DMFBs.

degrade performance. Alternatively, material and chemical compositions can be altered during fabrication to degrade the effectiveness of the dielectric layer at the DMFB's bottom plate.

Testing and calibration. During testing, the fabricated DMFB is calibrated and tested for possible manufacturing-related defects. Unlike in CMOS testing, DMFB chip testers can also insert a Trojan. For example, malicious testers can tamper with the calibration process for the embedded capacitive sensors or optical detectors, leading to incorrect runtime readings.

Assembly. Integration engineers assemble the tested DMFB and other hardware components on a printed circuit board (PCB). These components, which ensure robust control of the chip, might include a ring oscillator circuit, a signal-processing module, a shift-register bank, and a controller memory. Even if all the components are trustworthy, malicious assembly can introduce security vulnerabilities in the platform. For instance, the signal-processing module can be tampered with to force it to alter sensor output.

In-field. In general-purpose DMFBs, the DMFB is configured to execute a specific test protocol. Attackers can modify these protocols in the field by changing the actuation sequences.

Abstraction level

As Figure 3 shows, Trojans can be inserted at the system, synthesis-tool, physical, fluidic, and/or actuation-sequence levels.

System. DMFB operation is based on the interaction among several domains, including electrical (electrode actuation), optical (detection), thermal (thermal cycling of samples), and fluidic (liquid viscosity). At this level, system designers define each domain's elements and required interconnections. A functional DMFB can be tampered with to perform malicious operations. For example, thermal cycling stability can be altered to invalidate the resulting DNA samples, causing inaccurate quantitative analysis.

Synthesis-tool. Synthesis CAD tools are used to convert a sequencing graph into actuation sequences and the DMFB layout. A malicious CAD tool can alter the design in the same way as a malicious designer can.

Physical. This level describes all the physical components in the digital microfluidic platform and their dimensions and locations. These components include the DMFB, hardware components, and wiring. Adversaries can insert Trojans by altering any of these components, their dimensions, or both.

Fluidic. At the fluidic level, the reagent can be tampered with by changing its electrowetting capability. A reagent droplet used in immunoassays can be transported over protein-fouled areas to modify its adhesion characteristics at the solid–liquid interface. Changing a droplet's adhesion characteristics alters its response to actuation frequency, which could lead to operational errors.

Actuation-sequence. With general-purpose DMFBs, the actuation sequence for a specific test protocol is loaded into the memory, by either the diagnostic lab or the designer. The actuation sequence can be compromised with Trojans by altering the type of operations performed or changing droplet routing, leading to corrupted execution of the test protocol.

Activation mechanism

An activation mechanism defines how a Trojan is triggered. A Trojan can be designed to always be active or to be activated by internal or external triggers. For example, Trojans designed to alter the calibration curve for a glucose bioassay are always active, whereas those designed to alter the mixing time or the incubation time can be trigger-based.

Internal triggers. Internal triggers can be based on a time instant (clock cycle), for example, manipulating the timer for the thermal cycling module. Similarly, a Trojan can be triggered by fluidic conditions, for example, when a sample concentration becomes lower than a certain threshold.

External triggers. External triggers can be based on a specific reservoir's fluidic content, a specific detector's output, or both. For example, a primer reservoir can be replaced with luciferase (a light-generating fluid) so that when a luciferase droplet is dispensed and mixed with a DNA template and nucleotides, the emitted light intensities (based on a target DNA sequence) trigger a Trojan. Also, external triggering can be performed manually; for example, the actuation sequence can be manually replaced by a malicious actuation sequence that launches an attack.

Effects

DMFB Trojans are designed for specific objectives: to change system functionality, downgrade performance, leak secret information, perform denial-of-service (DoS) attacks, and so on.

Changing system functionality. In DMFBs, a specific module's functionality can be changed to alter the assay outcome. For example, a Trojan can stealthily deactivate the intramagnet module, causing unsuccessful bead snapping in immunoassay protocols.

Downgrading performance. A Trojan can intentionally cause delivery of excessive voltage to the biochip electrodes, which in turn degrades the resulting electrowetting force from these electrodes over time.

Leak information. Owing to the multiphysics capability of the digital-microfluidic platforms, proprietary information can be easily leaked through interactions between the different domains. For example, an attacker can pirate the actuation sequences to leak the steps of a proprietary biochemical protocol.

DoS. DoS attacks can be launched to prevent correct operation of a DMFB or to corrupt the bioassay by tempering with droplets. For example, a Trojan can deliberately cause droplet contamination by forcing a droplet to follow a certain route to adsorb the residues of another droplet. Another example of a DoS attack is to force violation of the fluidic constraints between neighbor droplets.

Location

DMFB Trojans are also classified based on their location: electrode array, actuation sequences, sensors, power supply module, and clock grid. The power supply module is used to actuate the electrodes, whereas the clock is used to synchronize droplet movements. A Trojan can be inserted in any of these five locations. Trojans designed for performance degradation can be inserted in the DMFB, clock grid, or power-supply module. Changing a DMFB's functionality requires modifications in the actuation sequences; hence, the best location for a Trojan insertion would be the actuation sequences.

As shown in Figure 3, DMFBs create avenues for new types of Trojans that have not been encountered with CMOSs. Furthermore, these Trojans might span electrical, biochemical, and optical domains, making them potentially menacing and difficult to detect.

PIRACY ATTACKS

DMFBs typically incorporate proprietary information about biomolecular test protocols. Pharmaceutical companies devote billions of dollars and years of effort to designing proprietary test protocols to gain an edge over their competitors. Examples in DMFBs are HemoGenix's toxicity test, Nichols Institute Diagnostics' endocrinology test, Corrositex's corrosion test, Trovagene's test to detect human papillomavirus in bodily fluids, and Invitae's gene deletion and duplication procedure.

Piracy's impact

Attackers can reverse-engineer and pirate test protocols implemented in DMFBs. The semiconductor industry loses billions of dollars annually because of a similar problem.[6] Recently, *Vox* reported that researchers have reverse-engineered a diagnostic kit to detect IP piracy.[7] However, attackers can misuse this capability to steal IP because current DMFBs are not protected against such attacks. Piracy is a major concern for the healthcare industry because

- it undermines the billions of dollars and years of effort expended toward designing proprietary protocols,
- designers have no control over the distributed supply chain of DMFBs, and
- current DMFB design tools do not incorporate security as a design metric.

Threat model

Attackers are end users or rogue elements in the diagnostic lab. They have access to the platform (diagnostic kit), that is, the DMFB chip and its

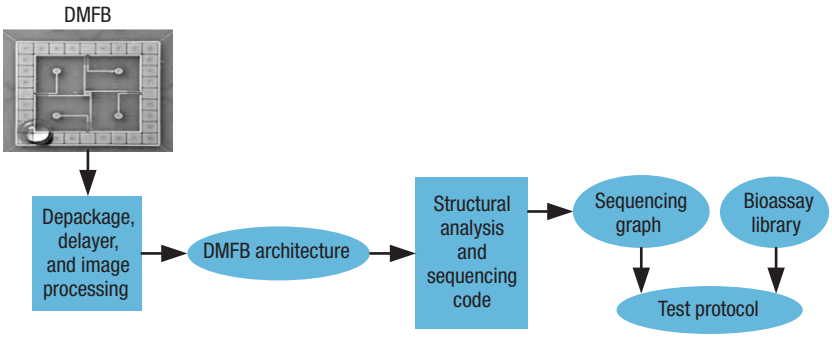

FIGURE 4. Pirating a DMFB proprietary test protocol. Attackers might buy a functional DMFB and depackage, delayer, and image the different layers and then reconstruct the DMFB architecture. A test-protocol recover attack aims to recover the proprietary protocol from the DMFB chip.

activation code. The attackers reverse-engineer the DMFB to obtain its physical architecture by depackaging, delayering, and image processing, as Figure 4 shows. These attacks have been observed on processors such as the NXP PN544 to extract the architecture. Note that DMFB designs are much simpler than these reverse-engineered processors, making them easier to reverse-engineer. From the DMFB's specification or datasheet, attackers can obtain information such as the latency (number of clock cycles required to complete the test), the reservoir ports where fluids are input, and the detector ports where test results are observed. Attackers can also read the sequencing code from the memory.

The attackers' objective is to retrieve and pirate the entire test protocol's sequencing graph. Consequently, they can reconstruct the underlying biomolecular protocol and recognize the constituent bioassays, fluidic-handling operations, and, potentially, reagents associated with the protocol. Legal aids can protect the healthcare industry against piracy attacks only when adequate protection is applied to the DMFBs. Several US courts have ruled that reverse-engineering is legal if the attacker does not spend "much" effort, time, and expense.[8] Thus, designers must ensure that attackers spend "significant" effort, time, and expense. Current DMFB design tools fail to satisfy this criterion.

In CMOS ICs, the functionality of the design is the IP to be protected and is in the electrical domain. In DMFBs, the sequencing graph is the IP to be protected and is distributed across the electrical and biochemical domains.

COUNTERFEITING

Apart from Trojan and piracy attacks, attackers might recycle and sell used DMFBs as new. Such devices are called counterfeits. Unlike in the case of ICs, where recycled chips still function but with reduced performance, recycled DMFBs do not work—the droplets and their sources are contaminated after use with bodily fluids. Because such defective DMFBs are easy to detect with conventional DMFB test protocols, counterfeits are less of a threat to DMFBs.

POTENTIAL DEFENSES

We propose reinforcing DMFB design methodology and tools with security, delivering resilience against reverse-engineering, IP piracy, and Trojans. Potential defense methodologies include the following:[9,10]

- *Watermarking* adds a digital signature to the DMFB design. Watermarks should be difficult to identify and modify, and should prove ownership; that is, the probability of two designers using the watermark should be negligible. Designers can embed watermark as synthesis constraints during DMFB design or actuation-sequence generation. Attackers will not be able to identify, erase, or modify a secure watermark. Consequently, if they copy and reproduce the design, the original designer can prove ownership by revealing the watermark in a court of arbitration—and the attacker will be punished through legal means. However, watermarking cannot protect against Trojans.
- *Metering* is similar to watermarking except that, along with the original designer's digital signature, the buyer's public signature is added to the DMFB design. Both signatures can be added as synthesis constraints during DMFB design. Metering's security properties are the same as watermarking's but add an additional property: during arbitration, a metering technique should reveal both the owner's and the buyer's signatures. This way, one can prove not only ownership, but also the source of leakage (for example, the diagnostic lab that helped the attacker). As with watermarking, metering cannot protect against Trojans because the design functionality is available for the attacker, who can create and hide a Trojan in the DMFB.
- *Side-channel fingerprinting* measures the parametric characteristics, such as power, area, delay, or droplet characteristics, of the DMFB manufactured at the untrusted foundry and compares them with a gold or statistical model. Any significant deviation would be

considered a Trojan. DMFBs are two to three orders of magnitude bigger than ICs. Hence, the effect of process variations on the side-channel parameters are less pronounced. Because attackers cannot hide the effect of a Trojan in process variations, Trojans are easier to detect.

- *Code analysis* can be performed on actuation sequences to detect Trojans inserted in the field. Furthermore, one can use cryptographic primitives such as encryption and hash functions to ensure the actuation sequences' confidentiality and integrity, thereby preventing Trojan attacks.
- *Obfuscation* of the DMFB design (architecture and actuation sequences) will render it impossible for attackers to reverse-engineer the functionality. Designers can use code-obfuscation techniques to hide the actuation sequences. Although obfuscation does not prevent attackers from copying and pirating the design, this technique can indirectly protect against Trojans because without a full understanding of the design, attackers might have difficulty crafting a meaningful and stealthy Trojan.
- *Locking* involves rendering the design unusable; that is, it produces incorrect outputs. The design works correctly—that is, produces correct outputs—only when the correct key is applied. A designer can add locks that control the flow of droplets between different microfluidic components. Only on applying the correct key will the droplets flow correctly; otherwise, they flow in an incorrect order, resulting in a wrong output. Designers can load the correct key after fabrication. The key is usually stored in a tamper-proof memory. Locking prevents attackers who are in the foundry, are end users, or are in the diagnostic lab from reverse-engineering or pirating the design. Because attackers in the foundry do not have access to the key, the pirated design is rendered useless. Attackers who are end users or in the diagnostic lab can reverse-engineer the design, but without the key they cannot make the reverse-engineered design functional. Because the key is stored in a tamper-proof memory, it is erased during reverse-engineering. Similarly, because locking uses a key to hide the functionality, an attacker cannot insert meaningful Trojans.

To summarize, obfuscation can prevent reverse-engineering and Trojans, but not piracy and counterfeiting. Watermarking and metering can enable detection of piracy and counterfeiting but not prevent them, and also cannot detect Trojans. Side-channel fingerprinting enables detection of Trojans inserted at the foundry, but cannot prevent reverse-engineering, piracy, and counterfeiting attacks. Code analysis can detect Trojans in the field, but not the other attacks. Locking prevents all four attacks, except for Trojans inserted in the field. Designers can pick one technique or a combination of techniques depending on their business model and overhead budget.

Techniques developed to protect CMOS devices cannot be directly used to protect DMFBs because CMOS devices are only in the electrical domain, whereas DMFBs span electrical, biochemical, and (if optical sensors are integrated) optical domains. DMFB protection techniques can nevertheless reuse the principles behind CMOS protection techniques while still spanning multiple domains. All these defense techniques can have electrical and biochemical equivalents or a combination of both. For example, DMFB watermarking and metering can embed the signature(s) in the actuation sequences and not just in the DMFB architecture. Side-channel fingerprinting can analyze the droplets' characteristics and not just the DMFB's power, area, and delay characteristics. Code-analysis techniques should consider both the electrical and biochemical components to detect attacks. As the DMFB IP spans both electrical and biochemical domains, obfuscation should be performed across both. The key used for locking can be specific chemicals and concentration and not just a digital key.

DMFBs face many of the same security issues as ICs. Currently, no technique can secure DMFBs against attacks. The protections developed to secure traditional ICs cannot be directly used for DMFBs: whereas microfluidics spans multiple energy domains—electrical, mechanical, fluidic, and biochemical—the techniques that protect ICs apply only to the electrical domain. Thus, there is an urgent need to develop techniques that will enable trustworthy DMFB designs—before attacks jeopardize the healthcare industry.

ABOUT THE AUTHORS

SK SUBIDH ALI is a postdoctoral research associate in the Department of Electrical and Computer Engineering at New York University, Abu Dhabi. His research focuses on hardware security, particularly side-channel analysis, fault analysis of crypto-chip, secure design for testability, and digital microfluidic biochip security. Ali received a PhD in computer science and engineering from the Indian Institute of Technology Kharagpur. Contact him at subidh.ali@nyu.edu.

MOHAMED IBRAHIM is a PhD student in the Department of Electrical and Computer Engineering at Duke University. His research interests include big data analytics for microbiology, CMOS VLSI design of microfluidic biochips, and microbiology-on-a-chip security. Ibrahim received an MSc in electrical engineering from Ain Shams University. He is a student member of IEEE. Contact him at mohamed.s.ibrahim@duke.edu.

JEYAVIJAYAN RAJENDRAN is an assistant professor in the Department of Electrical Engineering at the University of Texas at Dallas. His research interests include hardware security and emerging technologies. Rajendran received a PhD in electrical engineering from New York University. He is a member of IEEE and ACM. Contact him at jv.ee@utdallas.edu.

OZGUR SINANOGLU is an associate professor in the Department of Electrical and Computer Engineering and director of the Design-for-Excellence Lab at New York University, Abu Dhabi. His research interests include design-for-test, design-for-security, and design-for-trust for VLSI circuits. Sinanoglu received a PhD in computer science and engineering from the University of California, San Diego. Contact him at ozgursin@nyu.edu.

KRISHNENDU CHAKRABARTY is the William H. Younger Distinguished Professor in the Department of Electrical and Computer Engineering at Duke University, as well as a research ambassador at the University of Bremen and a Hans Fischer Senior Fellow at the Institute for Advanced Studies, Technical University of Munich. His research interests include testing and design-for-testability of integrated circuits; digital microfluidics, biochips, and cyber-physical systems; and optimization of enterprise systems and smart manufacturing. Chakrabarty is a Fellow of ACM and IEEE and a Golden Core Member of the IEEE Computer Society. Contact him at krish@ee.duke.edu.

REFERENCES

1. V. Srinivasan, V.K. Pamula, and R.B. Fair, "An Integrated Digital Microfluidic Lab-on-a-Chip for Clinical Diagnostics on Human Physiological Fluids," *Lab on a Chip*, vol. 4, no. 4, 2004, pp. 310–315.
2. M. Ibrahim, Z. Li, and K. Chakrabarty, "Advances in Design Automation Techniques for Digital-Microfluidic Biochips," *Formal Modeling and Verification of Cyber-Physical Systems*, R. Drechsler and U. Kühne, eds., Springer, 2015, pp. 190–223.
3. "2015 Microfluidic Applications in the Pharmaceutical, Life Sciences, In Vitro Diagnostic and Medical Device Markets," report, Yole Développment, June 2013; www.i-micronews.com/component/hikashop/product/p2015-microfluidic-applications-in-the-pharmaceutical-life-sciences-in-vitro-diagnostic-and-medical-device-markets.html.
4. D. Grissom and P. Brisk, "A Field-Programmable Pin-Constrained Digital Microfluidic Biochip," *Proc. 50th IEEE/ACM Design Automation Conference* (DAC 13), 2013, article no. 46.
5. R. Karri et al., "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," *Computer*, vol. 43, no. 10, 2010, pp. 39–46.
6. "Innovation Is at Risk as Semiconductor Equipment and Materials Industry Loses Up to $4 Billion Annually Due to IP Infringement," SEMI, 29 Apr. 2008; www.semi.org/en/Press/P043775.
7. J. Belluz, "The Theranos Controversy, Explained," *Vox*, 20 Oct. 2015; www.vox.com/2015/10/20/9576501/theranos-elizabeth-holmes.
8. R.M. Halligan, "Trade Secrets v. Patents: The New Calculus," *Landslide*, vol. 2, no. 6, 2010; www.americanbar.org/content/dam/aba/migrated/intelprop/magazine/LandslideJuly2010_halligan.authcheckdam.pdf.
9. S. Bhunia et al., "Hardware Trojan Attacks: Threat Analysis and Countermeasures," *Proc. IEEE*, vol. 102, no. 8, 2014, pp. 1229–1247.
10. F. Koushanfar, "Hardware Metering: A Survey," *Introduction to Hardware Security and Trust*, M. Tehranipoor and C. Wang, eds., Springer, 2011, pp. 103–122.