Secure Assay Execution on MEDA Biochips to Thwart Attacks Using Real-Time Sensing

TUNG-CHE LIANG, Duke University
MOHAMMED SHAYAN, New York University
KRISHNENDU CHAKRABARTY, Duke University
RAMESH KARRI, New York University

Digital microfluidic biochips (DMFBs) have emerged as a promising platform for DNA sequencing, clinical chemistry, and point-of-care diagnostics. Recent research has shown that DMFBs are susceptible to various types of malicious attacks. Defenses proposed thus far only offer probabilistic guarantees of security due to the limitation of on-chip sensor resources. A micro-electrode-dot-array (MEDA) biochip is a next-generation DMFB that enables the real-time sensing of on-chip droplet locations, which are captured in the form of a droplet-location map. We propose a security mechanism that validates assay execution by reconstructing the sequencing graph (i.e., the assay specification) from the droplet-location maps and comparing it against the golden sequencing graph. We prove that there is a unique (one-to-one) mapping from the set of droplet-location maps (over the duration of the assay) to the set of possible sequencing graphs. Any deviation in the droplet-location maps due to an attack is detected by this countermeasure because the resulting derived sequencing graph is not isomorphic to the original sequencing graph. We highlight the strength of the security mechanism by simulating attacks on real-life bioassays. We also address the concern that the proposed mechanism may raise false alarms when some fluidic operations are executed on MEDA biochips. To avoid such false alarms, we propose an enhanced sensing technique that provides fine-grained sensing for the security mechanism.

CCS Concepts: • **Security and privacy** → *Systems security*;

Additional Key Words and Phrases: MEDA biochips, computer security, biological system modeling, sensors, microfluidics

---

1 INTRODUCTION

A digital microfluidic biochip (DMFB) is composed of a two-dimensional electrode array that manipulates discrete fluid droplets. When driven by a sequence of control voltages, the electrode array can perform fluidic operations, such as dispensing, mixing, and splitting [9]. Because of the precise control over microfluidic operations, DMFBs are employed in lab-on-a-chip systems for biomolecular recognition, point-of-care diagnostics, and cell biology [10]. DMFBs have recently been commercialized. For example, Illumina, a leading DNA sequencing company, has announced the use of DMFBs in their NeoPrep NGS Library Prep product [1]; USDA has approved the Baebies SEEKER DMFB platform as a high-throughput laboratory solution for screening diseases in a newborn child [2].

As the platforms are being adopted for safety-critical applications [11], security and trustworthiness of DMFBs have become the important focus of research. It has been shown that DMFBs are susceptible to attacks such as actuation tampering and miscalibration and that the attacks lead to disastrous assay outcomes [6, 7, 32]. A randomized checkpoint-based security method for DMFBs was presented in Tang et al. [32]. This method randomly checks areas on the DMFB platform using a CCD camera in the cyberphysical system to capture droplet locations during bioassay execution. The use of a randomized checkpoint can thus provide an increased level of security. However, the images that are captured by high-resolution cameras require significant additional computing and memory resources. Therefore, checkpoint-based validation is limited by real-time computing resources and memory needed for analyzing real-time data from a high-resolution camera. Because of the limited hardware resources in cyberphysical DMFBs, the checkpoint-based validation does not provide security guarantees, and therefore it is unlikely to inspire confidence in the users of these DMFB systems.

The micro-electrode-dot-array (MEDA) architecture for DMFBs was introduced recently [14, 18, 33]. MEDA is composed of an array of identical microfluidic unit components named *micro-electrode cells* (MCs). Each MC consists of a micro-electrode, a semiconductor control circuit, and a sensing module that enables real-time sensing of on-chip droplets. The sensor data specifies the location, the size, and the shape of the on-chip droplets. The real-time sensor data can be used to validate the execution of a bioassay [35]. From a security perspective, MEDA is promising as it overcomes the resource constraints of a traditional DMFB.

In this article, we propose the first provable security solution for MEDA biochips by exploiting integrated droplet sensing. The proposed method can detect any operational attack and does not require CCD cameras for detection. The key contributions of this work are as follows:

- A security method that utilizes the information sensed from a MEDA biochip. This method automatically recognizes fluidic operations and constructs the dependencies between these operations to compare against the "golden" bioassay.
- A formal proof that the proposed security solution can reconstruct the sequencing graph (i.e., the assay specification).
- Demonstration of result-altering attacks on the *in vitro* glucose test assay [7] and denial-of-service attacks on the multiplexed *in vitro* diagnostics on human physiological fluids [31]. Our results show that the proposed defense can thwart these attacks.
- An enhanced sensing technique that prevents the security method from raising false alarms.

The remainder of this article is organized as follows. Section 2 explains the MEDA architecture. Section 3 models threats and attacks on MEDA biochips. Section 4 presents details of the proposed security method and theoretical results. Section 5 showcases the working of the proposed defense against simulated attacks on real-life bioassays. Section 6 demonstrates that the security
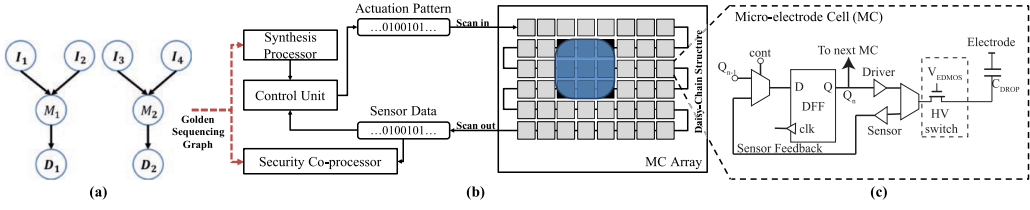
Fig. 1. (a) An example of the given sequencing graph. The nodes I_i, M_i, and D_i represent dispensing, merging, and detecting operations. (b) The MEDA biochip architecture consists of a synthesis processor, a control unit, and a two-dimensional MC array. The proposed security mechanism is loaded on a security co-processor physically separate from the synthesis processor. (c) The circuit schematic of the sensor and control module of the MC. Q_n denotes the nth cell in the daisy-chain structure.

mechanism may raise a false alarm because of sensing limitation. Section 7 further proposes a fine-grained sensing technique to avoid false alarms. Finally, conclusions are drawn in Section 8.

2 MEDA BIOCHIPS

In this section, we describe the MEDA biochip architecture and its working principle.

2.1 MEDA Biochip Architecture

A MEDA biochip platform is composed of a processor, a control unit, and a two-dimensional MC array, as shown in Figure 1(b). The MC integrates a micro-electrode, an activation circuit, and a sensing circuit, which is shown in Figure 1(c). These circuits allow fine-grained droplet control and real-time sensing [16]. The MCs are connected together to form a daisy chain (i.e., the MCs are connected in a sequence). The MCs can operate in two modes: actuation and sensing. The control bit for actuation is fed serially through the scan chain. In actuation mode, the micro-electrode with logic '1' is actuated using high voltage. Micro-electrodes actuated with the high voltage create a driving force to the on-chip droplets using the electrowetting-on-dielectric (EWOD) effect [27, 28]. The induced force can therefore manipulate droplets to perform many fluidic operations, such as transportation, merging, and splitting. Because droplets with biological samples are of nanoliter or picoliter volumes, a filler medium such as silicone oil is used between the two plates to avoid evaporation and to reduce the likelihood of cross-contamination. In sensing mode, the presence of a droplet is determined as follows. The capacitor formed by the lower and upper electrode plates is pre-discharged. Then the charge path is switched on. The charge time depends on the electrode capacitance; the presence of a droplet increases the permittivity and hence the capacitance of the electrode. The flip-flop within the MC samples the capacitor node voltage. The clock is tuned such that the flip-flop captures '1' when a droplet is present and '0' otherwise. The detection results are shifted out as a vector specifying droplet location, and this vector is referred to as the *droplet-location map*.

2.2 MEDA Biochip Working Principle

To carry out bio-chemical assays on MEDA biochips, the bioassays are interpreted as sequencing graphs that specify the relationships of fluidic operations. In the biochip design flow, the sequencing graphs are provided by the entity designing the bio-protocol IP, such as pharmaceutical and biotech companies. An example of a sequencing graph is illustrated in Figure 1(a). The bio-protocol designer uses a synthesis tool that is provided by CAD tool vendors. The synthesis tool is loaded on the processor, and it binds the operations to on-chip resources, generates an optimized schedule of these operations, and routes droplets on the biochip [20]. Based on the synthesis result, the

actuation patterns for the micro-electrodes are translated by the control unit, and the actuation patterns are shifted to the MC array through the daisy-chain structure sequentially. After an actuation pattern is activated on the MC array, a location map is scanned out to the control unit as a feedback of the scanned in actuation pattern [18]. As a result, the scanned-out droplet-location maps are cycle-by-cycle consecutive.

A provable security mechanism is proposed based on the consecutive droplet-location maps and the same sequencing graph for the synthesis processor. Details of this security mechanism will be explained in Section 4. To ensure that the control unit and the security mechanism are not simultaneously compromised, the security mechanism is installed in a separate monitoring co-processor, as shown in Figure 1(b). Note that the monitoring co-processor is physically separate from the synthesis processor. The synthesis processor is typically connected to the Internet for the purpose of loading new bioassays. The co-processor, however, is acquired along with the MEDA biochip, and it is not connected to the Internet.

3 ATTACKS ON MEDA BIOCHIPS

In this section, we present the motivation for attacks and discuss the threat model in the context of MEDA biochips.

3.1 Threat Model

Motivations for attacking a MEDA biochip vary based on the target application. In point-of-care diagnostics, an attack may endanger patient health by ensuring an incorrect prescription based on compromised test results. To compete with rivals, companies may be interested in corporate sabotage by disrupting scientific experiments. Other motivations include terrorism, bypassing of pollution control, and revenge [7].

We assume that the attacker is interested in changing fluidic operations during synthesis. The attacker can be the CAD tool vendor; the synthesis tools can be tampered with to alter routing paths and module placements. Operations can also be inserted or deleted. Since remote control of experiments is now possible [4, 5], for example, in environmental monitoring, an attacker can tamper with the assay by inserting malware in the synthesis processor or the control unit through the Internet. These attackers do not have to understand the detailed structure of each biochip to compromise the outcome of the assays. Although we consider attacks at the synthesis level, we assume that the operators of MEDA biochips are trustworthy (i.e., the samples and reagents are loaded as expected). The MC array is also assumed to be functioning as intended (i.e., micro-electrode actuation and capacitance detection are not compromised). Additionally, the proposed security solution is assumed to be trustworthy because it is loaded on a co-processor, which is physically separate from the control unit. Finally, the "golden" sequencing graph for the attack-detection method is assumed to be trustworthy because the sequencing graph is provided by the bio-protocol designer.

Example. Figure 2 shows an example of tampering with the synthesis result of the multiplexed *in vitro* diagnosis. The lactate and glucose levels in human physiological fluids are mixed and tested. These tests are important for diagnosing diseases such as diabetes, myocardial infarction, congestive heart failure, and septicemia [17]. The intended execution of multiplexed *in vitro* diagnosis is shown in Figure 2(a). When an adversary stealthily changes the routes during synthesis, as shown in Figure 2(b), sample/reagent contamination may occur. If the compromised result is detected by an online error-recovery method [22, 34], the re-execution of the assay will be triggered. The re-execution may, however, fail due to the same attack, and another re-execution will then be launched. As a result, the repeated execution of the assay will lead to the wastage of precious
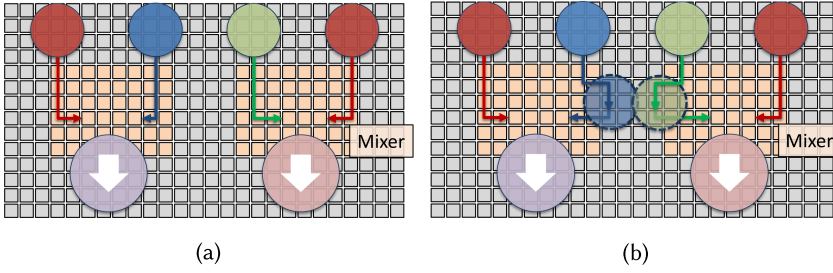
Fig. 2. Malicious routing of droplets during the execution of a bioassay. (a) Originally, two pairs of droplets are mixed in separate mixers. (b) Two droplets are contaminated due to malicious routing.
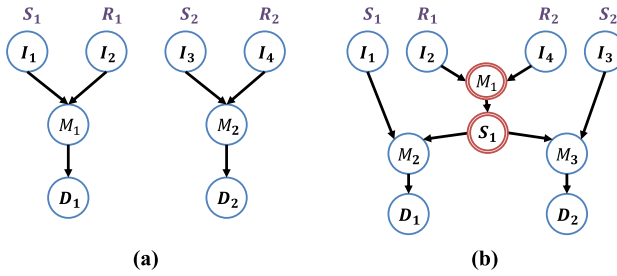

Fig. 3. Contamination of the assay is modeled by the inserting of extra merge and split steps in the sequencing graph. (a) The golden sequencing graph. (b) The modified sequencing graph. S_1, S_2, R_1, and R_2 represent plasma, serum, glucose oxidase, and lactate oxidase, respectively; the nodes I_i, M_i, D_i, and S_i represent dispensing, merging, detecting, and splitting operations.

samples and expensive reagents. Yet if the compromised result is not detected by an online error-recovery method, the erroneous results will be deemed to be correct. The treatment prescribed on the basis of the misdiagnosis may jeopardize the health of the patient.

3.2 Attack Modeling

To alter the outcome of the assay, an attacker can modify some of the operations in the assay. The adversary can introduce spurious assay operations or delete critical operations during synthesis. For instance, if an aliquot (smaller) droplet is maliciously extracted from one droplet and merged with another droplet during execution, the victim droplet is contaminated [34]. The attacker can also alter an operation in a subtle manner. For example, an original 1:1 split operation may be replaced with a 3:1 split [19, 23].

Example. Figure 3 shows the original and modified sequencing graphs of the multiplexed *in vitro* diagnosis. This attack is based on the misrouting example in Figure 2, where a sample/reagent contamination is introduced during execution. Although the adversary only changes the transportation paths of two droplets, an unwanted merge operation and an unwanted split operation are stealthily added to the original execution. Therefore, the erroneous results may mislead prescription and further jeopardize the health of the patient.

The attacker may launch different types of attacks to tamper with bioassay execution, and the time that the attacks are introduced may be different (e.g., before or after the synthesis). The assay can be tampered with before synthesis commences. The addition (deletion) of operations in the given assay leads to extra (fewer) nodes in the sequencing graph. During synthesis, the constraints on completion or incubation times might be manipulated so that operations do not finish correctly.

Table 1. Classification of Attacks

Attacks before synthesis	Modifications to the sequencing graph
Insert extra operations	Insert extra nodes
Delete operations	Delete nodes
Alter operations	Replace nodes
Attacks during synthesis	**Possible modifications**
Violate fluidic-distance design rule [16, 20, 31]	Insert extra merge and split steps
Attacks after synthesis	**Modifications to the sequential graph**
Overlap droplet routes	Insert extra merge and split steps
Replace input droplets of operations	Redirect input edges of nodes

Two droplets might be routed too close to each other, causing unwanted merging of these droplets. Attackers can also change the synthesis output so that the assay fails (e.g., the example in Figure 2 might result from a change in the synthesized route) The example in Figure 2 shows that an attacker can modify the routing paths *after synthesis*. The original paths obtained from synthesis do not incur any contamination. However, the modified paths result in extra merge and split steps. The resultant sequencing graph is shown in Figure 3(b). The attacker can also tamper with the bioassay outcome using a different approach. For instance, *before synthesis*, the attacker can introduce extra operations in the original sequencing graph (e.g., adding a merge operation and a split operation in the original sequencing graph). Even though this attack is introduced before synthesis, it also results in a similar contamination outcome involving two droplets. A classification of attacks is presented in Table 1. We classify attacks according to the synthesis phase during which they are introduced and map the related impacts to the input sequencing graph.

4 ENSURING SECURITY BY RECONSTRUCTING THE SEQUENCING GRAPH

As a countermeasure to the threats described in Section 3, we propose a security mechanism based on the reconstruction of the sequencing graph from real-time sensor data (i.e., the droplet-location maps). The reconstructed graph is compared against the golden sequencing graph, and any deviation is flagged as an error.

Recall that the droplet-location maps are generated cycle by cycle according to the MEDA biochip design. As a result, the exploitation of these sensor data introduces negligible overhead. Since each droplet-location map provides information of on-chip droplets at a certain time, we claim that the overall operations of a given assay can be reconstructed using the consecutive droplet-location maps.

To establish the preceding claim, we present a theorem—we lead up to it step by step using lemmas. These lemmas reveal the one-to-one mapping between fluidic operations and consecutive (i.e., in adjacent clock cycles) droplet-location maps. The recognized operations can be used to reconstruct a sequencing graph that is isomorphic to the "golden" sequencing graph when there is no attack. We first describe how each droplet-location map can be interpreted and introduce the notation that will be used later.

4.1 Interpretation of Droplet-Location Maps

Our goal is to identify locations of droplets at any timestep (clock cycle) from the scanned-out droplet-location map. Let the scanned-out droplet-location map at time t be denoted by the vector lm_t. The length of this vector is the number of micro-electrodes on the platform. A component $b_i \in \{0, 1\}$ of lm_t indicates whether the micro-electrode e_i is under a droplet at time t, where e_i is

---

ALGORITHM 1: Derive footprints from a droplet-location map

Input: A droplet-location map lm_t, the row length r
Output: A list of footprints FPs
 1: $FPs = \{\}$
 2: initial empty adjacency graph G_A
 3: **for** a component b_i in lm_t **do**
 4:   **if** ($b_i = 1$) **then** Add node n_i to G_A **end if**
 5: **end for**
 6: **for** a pair of nodes n_i and n_j in G_A **do**
 7:   **if** ($|i - j| = 1$ or $|i - j| = r$) **then**
 8:     Add an edge between n_i and n_j
 9:   **end if**
10: **end for**
11: **for** a connected component g_c in G_A **do**
12:   $fp = \{e_i | e_i$ is a node of the component $g_c\}$
13:   Add fp to FPs
14: **end for**
15: **return** FPs

---

the ith micro-electrode on the platform. The naming order for the micro-electrodes on a MEDA starts from the top-left corner to the bottom-right corner row by row. To represent the locations of all droplets in a compact manner, a droplet-location map is transformed to an undirected graph called the *adjacency graph* $G_A = (V_A, E_A)$. Note that $V_A = \{n_i | b_i = 1, \forall i\}$, where the node n_i corresponds to the micro-electrode e_i. For any given $n_x, n_y \in V_A$, an edge exists between n_x and n_y if the corresponding e_x and e_y are physically adjacent on the MEDA platform. Assuming that the number of micro-electrodes in a row of a MEDA is r, two micro-electrodes e_x and e_y are physically adjacent if either $|x - y| = 1$ or $|x - y| = r$. A connected component in G_A indicates a droplet's location (i.e., the droplet resides over the associated micro-electrodes in this component). We define the set of micro-electrodes that are associated with nodes of a connected component as a *footprint*; this represents a droplet's location. If a droplet d_x exists on the platform at time t, the set of nodes corresponding to this droplet's position is denoted by fp_t^x. The procedure for computing a droplet-location map is shown in Algorithm 1.

Example. Figure 4 shows two visualized droplet-location maps that are scanned out from a MEDA biochip at time $t - 1$ and time t, respectively. A droplet-location map $lm_{t-1} = (b_1, \ldots, b_{50})$ can be obtained at time $t - 1$, where only b_{12}, b_{13}, b_{18}, b_{19}, b_{22}, b_{23}, b_{28}, and b_{29} are equal to 1; the other elements of this vector are 0. The adjacency graph obtained from the droplet-location map lm_{t-1} is shown in Figure 5. Nodes in this graph represent the micro-electrodes e_{12}, e_{13}, e_{18}, e_{19}, e_{22}, e_{23}, e_{28}, and e_{29}, and edges between nodes indicate adjacency in the micro-electrode array. The two connected components indicate the locations of two droplets at time $t - 1$. Consequently, two footprints fp_{t-1}^x and fp_{t-1}^y are obtained, where $fp_{t-1}^x = \{e_{12}, e_{13}, e_{22}, e_{23}\}$ and $fp_{t-1}^y = \{e_{18}, e_{19}, e_{28}, e_{29}\}$.

4.2 Recognition of Fluidic Operations

Using the droplet-location maps for two consecutive time slots that are derived from the MEDA platform, we are able to recognize the droplet operations. In the example of Figure 4, two droplets are on the chip at times $t - 1$ and t. Let the left droplet be d_x and the right droplet be d_y, and suppose d_x is moved downward at time t. Using the two droplet-location maps lm_{t-1} and lm_t, four footprints are obtained: fp_{t-1}^x, fp_{t-1}^y, fp_t^x, and fp_t^y, where $fp_{t-1}^x = \{e_{12}, e_{13}, e_{22}, e_{23}\}$,
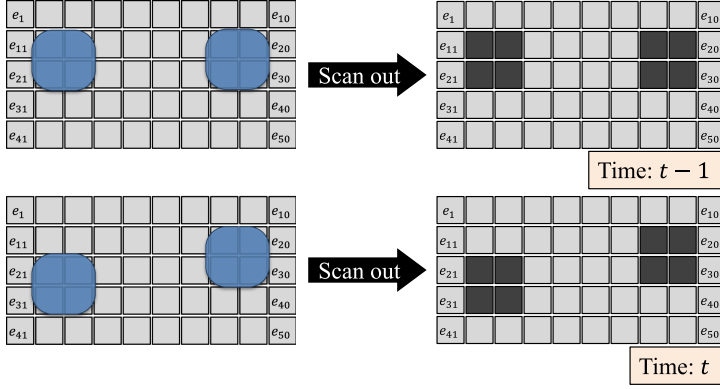
Fig. 4. Droplets on the MEDA platform and the visualized droplet-location maps over two consecutive time slots.

Fig. 5. The adjacency graph at time t-1 for the scenario shown in Figure 4.

$fp^y_{t-1} = \{e_{18}, e_{19}, e_{28}, e_{29}\}$, $fp^x_t = \{e_{22}, e_{23}, e_{32}, e_{33}\}$, and $fp^y_t = \{e_{18}, e_{19}, e_{28}, e_{29}\}$. By comparing the footprints at time $t - 1$ and the footprints at time t, we find that $fp^x_{t-1} \cap fp^x_t \neq \emptyset$ and that $fp^y_{t-1} \cap fp^y_t \neq \emptyset$. Moreover, the overlapping footprints have the same number of electrodes (i.e., $|fp^x_{t-1}| = |fp^x_t|$ and $|fp^y_{t-1}| = |fp^y_t|$). This example shows that the transportation of any droplet can be inferred by examining its footprints.

LEMMA 1. *A droplet d_x is transported on the MEDA platform between time slots $t - 1$ and t if and only if $fp^x_{t-1} \cap fp^x_t \neq \emptyset$ and $|fp^x_{t-1}| = |fp^x_t|$.*

The proofs of the lemmas are included in the appendix. Furthermore, all basic fluidic operations can be inferred by examining two consecutive droplet-location maps.

LEMMA 2. *A droplet d_x is dispensed on the MEDA platform between time slots $t - 1$ and t if and only if $fp^x_t \neq \emptyset$ and $fp^x_{t-1} = \emptyset$.*

LEMMA 3. *A droplet d_x is discarded from the MEDA platform between time slots $t - 1$ and t if and only if $fp^x_{t-1} \neq \emptyset$ and $fp^x_t = \emptyset$.*

The preceding operations are related to only one droplet. Other droplet operations on MEDA biochips include two droplets (e.g., merging and splitting).

LEMMA 4. *Two droplets d_x and d_y are obtained as a result of splitting a droplet d_z between time slots $t - 1$ and t if and only if $fp^x_t \neq \emptyset$, $fp^y_t \neq \emptyset$, $fp^z_{t-1} \neq \emptyset$, $fp^x_t \cap fp^z_{t-1} \neq \emptyset$, $fp^y_t \cap fp^z_{t-1} \neq \emptyset$, and $|fp^x_t| + |fp^y_t| = |fp^z_{t-1}|$.*

LEMMA 5. *A droplet d_x is obtained as a result of merging two droplets d_y and d_z on the MEDA platform between time slots $t - 1$ and t if and only if $fp^x_t \neq \emptyset$, $fp^y_{t-1} \neq \emptyset$, $fp^z_{t-1} \neq \emptyset$, $fp^x_t \cap fp^y_{t-1} \neq \emptyset$, $fp^x_t \cap fp^z_{t-1} \neq \emptyset$, and $|fp^x_t| = |fp^y_{t-1}| + |fp^z_{t-1}|$.*

We assume that droplets remaining on the platform until the end of assay execution are used for detection. The detection operation is therefore recognized by the following lemma.

Lemma 6. *A droplet d_x is detected on the MEDA platform at time T (end of the assay) if and only if $fp_T^x \neq \emptyset$.*

Using the preceding lemmas, all of the basic fluidic operations can be automatically inferred using location maps.

To increase the strength of the proposed defense, we also explicitly identify the type of reagent used in a dispensing operation. This can be accomplished by identifying the location of the dispensing port. Reagents are stored in separate reservoirs outside the MEDA platform, and they are dispensed through various channels to different locations on the platform to avoid contamination. A dispensing operation can be recognized by the footprint. Let the set of micro-electrodes where reagent A is dispensed on the platform be E_A. If a dispensing operation is recognized by Lemma 2 with a footprint fp_t^x, and $fp_t^x \cap E_A \neq \emptyset$, the dispensing operation must involve reagent A. Likewise, a splitting operation can also be specifically identified by the proposed method. Unlike a conventional DMFB that supports only a 1:1 splitting operation, a MEDA biochip enables unbalanced splitting operations (e.g., the 1:2 ratio). The proposed defense records the splitting ratio by determining the sizes of the resulting droplets. These details about the executed operations enable us to detect any deviations from the original assay.

4.3 Sequencing-Graph Construction

Since the droplet-location maps for an assay are obtained for consecutive time slots, the operations inferred from them are contiguous as well in time (i.e., each operation is related to a specifically identified previous operation and/or a similarly identified operation). Let the last droplet-location map of any assay execution be lm_T. The following lemma states that the droplet-location maps can be used to reconstruct the sequencing graph for an assay.

Lemma 7. *The sequencing graph can be reconstructed from a complete sequence of droplet-location maps from the start to the end of the assay (i.e., $(lm_1, lm_2, \ldots, lm_T)$).*

If we denote fluidic operations as nodes and add edges between consecutive operations, a graph is generated with the dispensing, discarding, transporting, merging, and splitting operations. However, the golden sequencing graph does not include transportation operations because the specific droplet transportation paths do not affect the outcome of the assay (as long as the steps of the bio-chemical protocol are correctly followed). As a result, nodes corresponding to droplet transportation operations are omitted, and their parent nodes and child nodes are connected by edges inserted in a post-processing step. This step leads to a graph G_{re}, which we refer to as the *reconstructed graph*.

If all operations from the given sequencing graph G_{in} are synthesized correctly on MEDA and not compromised by an attack, we can prove that G_{re} is isomorphic to G_{in}. In graph theory, two graphs are isomorphic if they contain the same number of graph vertices and the vertices are connected in the exact same way [8, 26]. The proof of the following theorem is included in the appendix.

Theorem 1. *If a sequencing graph G_{in} is synthesized on a MEDA biochip and the biochip is not compromised by an attack, the sequencing graph G_{re} reconstructed from the droplet-location maps is isomorphic to G_{in}. If an attack compromises one or more operations, G_{re} is no longer isomorphic to G_{in}.*

4.4 Detection of Attacks

Theorem 1 shows that attacks can be detected if G_{re} is not isomorphic to G_{in}. We propose an algorithm to check if G_{re} and G_{in} are isomorphic in linear time. The procedure for checking iso-morphism of G_{re} and G_{in} is shown in Algorithm 2. The algorithm first creates a hash table, H, to record nodes in G_{re}. A label indicates the shortest distance from the associated node to a near-est end node (e.g., the end nodes are always labeled with '0's). We refer to the node label as the node height in the graph. Note that there is no circle in any sequencing graph because nodes within specify distinct fluidic operations. Therefore, the time complexity of node labeling is in $O(N)$, where N is the number of nodes. After all nodes in G_{re} have been labeled, they are added to H. The hash key is a combination of the node type, the parent-node types, the children-node types, and the label; the hash value is the node itself. For any two nodes, n_i and n_j, from G_{re} and G_{in}, respectively, are the same if their hash keys are the same. According to graph theory [26], G_{re} and G_{in} are isomorphic if and only if $\exists n_i \in G_{re} \rightarrow \exists n_j \in G_{in}, n_i = n_j$. The algorithm traverses all nodes in G_{in} and compares each node to see if there is an identical node in G_{re} using H.

It is well known that the problem of checking graph isomorphism is NP-complete [8]. Therefore, there is no polynomial-time algorithm for checking graph isomorphism. However, prior work has shown that isomorphism testing of special kinds of graphs can be achieved in polynomial time [13, 15, 25, 29]. For example, the work in Hopcroft and Wong [15] presented a linear-time algorithm for isomorphism testing of planar graphs. The work in Luks [25] proved that we can use a polynomial algorithm for isomorphism testing of graphs whose vertex degree is bounded. Note that the sequencing graph is a directed tree, which means that the sequencing graph is also a planar graph and that the vertex degree of the sequencing graph is bounded. We show that the computational complexity of the proposed algorithm is in $O(N)$, where N is the number of the total nodes. The first procedure of the algorithm is node labeling, and it is in $O(N)$. Then the algorithm compares all nodes in a graph with that in another graph. In this procedure, the algorithm traverses all nodes in a graph; for each node, the algorithm calls the hashing table to see if an identical node exists in another graph. The computational complexity of calling the hash table is in $O(1)$. Therefore, the overall computational complexity is in $O(N)$.

The overall control flow of the proposed defense is shown in Figure 6. Assuming that the defense receives the golden sequencing graph and the consecutive location maps during bioassay execution (named from lm_1 to lm_T), the defense first identifies footprints using Algorithm 1. The defense next reconstructs G_{re} using the identified footprints (Lemma 7). By iteratively checking relationships of the footprints between two consecutive timesteps, all operations can be recognized, and G_{re} is reconstructed. After G_{re} is reconstructed, the defense compares the isomorphism between G_{in} and G_{re} using Algorithm 2. The result of Algorithm 2 reveals if an attack has been introduced (Theorem 1).

Note that the actuation patterns cannot be used to secure the execution of bioassays. Unlike sensor data, there is no one-to-one mapping between the synthesis result and the golden sequenc-ing graph. For example, to transport a droplet on the biochip, several sequences of actuation can be applied. In addition, the actuation patterns for a droplet may not be consecutive in the cycle-by-cycle sense. When a droplet waits on the biochip for later operations, no actuation pattern is applied to this droplet.

5 SIMULATION RESULTS

We simulated two real-life assays and different attacks on a state-of-art MEDA platform with 60 × 30 micro-electrodes [18] to demonstrate the effectiveness of the proposed defense. The assays
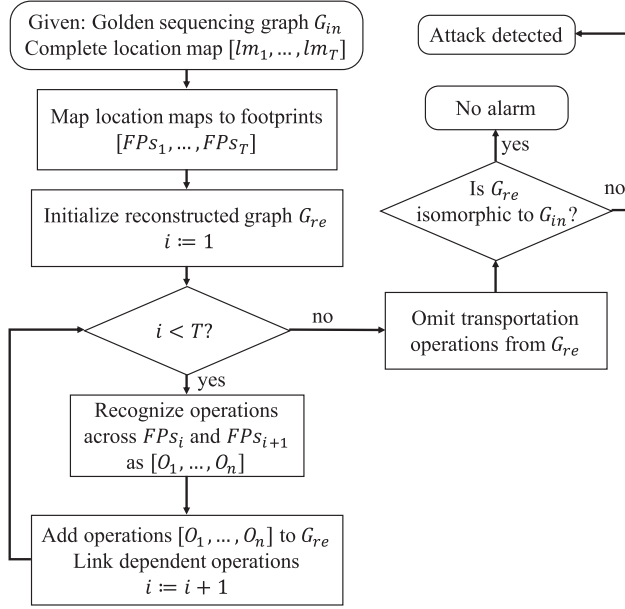
Fig. 6. Control flow corresponding to the proposed defense.

ALGORITHM 2: Check isomorphism of G_{re} and G_{in}

Input: G_{re} and G_{in}
Output: True if G_{re} is isomorphic to G_{in}; false otherwise.

 1: Initialize a hash table H
 2: **for** node n_i in G_{re} (in reverse) **do**
 3:     label height to n_i
 4:     add n_i to H
 5: **end for**
 6: **for** node n_j in G_{in} (in reverse) **do**
 7:     label height to n_j
 8:     **if** n_j is not a key in H **then**
 9:         **return** False
10:         remove n_j in H
11:     **end if**
12: **end for**
13: **if** H is empty **then**
14:     **return** True
15: **else**
16:     **return** False
17: **end if**

---

are synthesized using methods described in Li et al. [20], and location maps are generated by simulating assay execution.

5.1 Lactate, Glucose, and Pyruvate *In Vitro* Test

We first study attacks on multiplexed *in vitro* diagnostics of serum and plasma [31]. Glucose and lactate measurements are carried out in this procedure by mixing the samples from the patient,
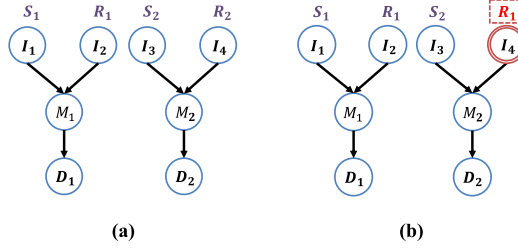
Fig. 7. The swapping-reagent attack. S_1, S_2, R_1, and R_2 represent plasma, serum, glucose oxidase, and lactate oxidase, respectively; the nodes I_i, M_i, D_i, and S_i represent dispensing, merging, detecting, and splitting operations, respectively. (a) The golden graph. (b) The reconstructed graph.

the glucose reagent, and the lactate reagent. The golden sequencing graph that represents the bioassay is shown in Figure 7(a). Two attacks are inserted in the synthesis phase to tamper with the results: (1) reduce the distance constraint between droplets to cause contamination; (2) swap input droplets before mixing procedures.

5.1.1 Attack 1. This attack was introduced in Figure 2; the minimum space constraint between glucose and lactate reagents is violated, and the paths of these droplets are maliciously routed to be too close. Thus, two droplets come in contact when they are transported to the corresponding mixers. The contaminated droplets cause the final detection results to be incorrect. Recall that the erroneous results may mislead prescription and jeopardize one's health. Our analysis method reconstructs the sequencing graph G_{re}; it contains extra operations (see Figure 3). The defense mechanism therefore provides an alarm because G_{in} is not isomorphic to G_{re}.

5.1.2 Attack 2. This attack stealthily swaps one of the dispense reagent with another for the mixing operation; hence, the detection outcome is compromised. Similar to Attack 1, the compromised detection may end up with disastrous consequences. Note that when the multiplexed *in vitro* assay is executed on biochips, operations are executed in parallel to shorten the overall execution time. This attack is thus hard to detect because there are numerous on-chip droplets. The proposed method reconstructs the graph shown in Figure 7. The defense procedure detects the attack; the analysis reveals that the reagent is different from that for G_{in}.

5.2 Glucose Test

We next demonstrate two other attacks on the glucose test assay. According to the 2017 National Diabetes Statistics Report from the Centers for Diseases Control and Prevention (CDC), an estimated 30.3 million people had diabetes in the United States in 2015 [3]. Patients with insulin-dependent diabetes must regularly monitor their blood sugar level through glucose tests so as to inject the appropriate amount of insulin. If the test result is maliciously tampered to result in a higher glucose reading, higher doses of insulin will be injected, leading to hypoglycemia. However, if the test result is altered to result in a lower glucose level, less insulin will be injected, resulting in hyperglycemia.

To test the concentration of the glucose level in a patient's sample, serial dilution is used to generate the calibration curve [7] (see the blue solid line in Figure 9, presented later). Given any sample, its glucose concentration is measured by comparing the absorbent reaction to the calibration curve. For example, if the absorbent-reaction rate of a sample is measured as 0.001, the concentration of this sample is interpolated as 100 mg/dL.

The golden sequencing graph of a glucose assay is shown in Figure 8(a), where Subgraph 1 and Subgraph 2 are used for generating a series of different concentrations. These known
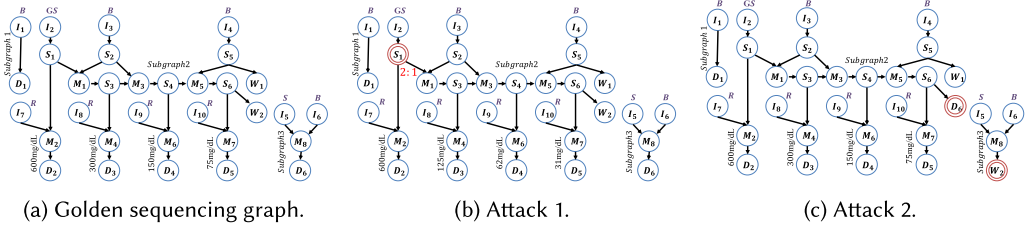
(a) Golden sequencing graph.   (b) Attack 1.   (c) Attack 2.

Fig. 8. The golden glucose test assay and two malicious attacks. B, GS, and S are buffer, glucose solution, and sample, respectively; the nodes I_i, M_i, D_i, W_i, and S_i correspond to dispensing, merging, detection, the discarding of a waste droplet, and splitting operations, respectively. (a) The graphs for Subgraph 1 and Subgraph 2 are used for generating the calibration curve, and the concentration of the sample in Subgraph 3 is tested and interpolated with the calibration curve. (b) An attack is stealthily introduced in the second splitting operation. The splitting ratio is changed from 1 : 1 to 2 : 1. (c) An attack is inserted during synthesis; the outcome droplet of Subgraph 3 is discarded and the waste droplet in Subgraph 2 is transported for detection.
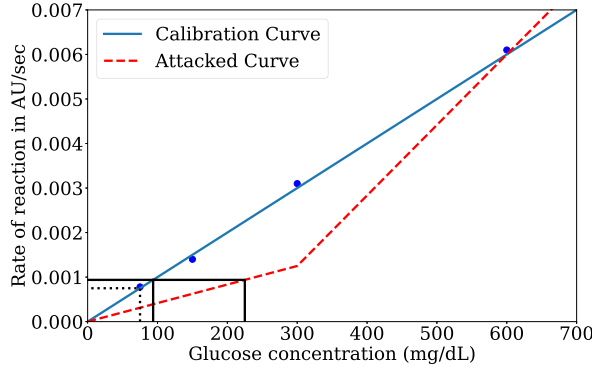

Fig. 9. Golden glucose calibration curve and the attacked calibration curve.

concentrations are used to plot the calibration curve. In this example, a golden glucose solution with concentration of 600 mg/dL is diluted to get the series of calibrated concentrations. The diluted concentrations are 600 mg/dL, 300 mg/dL, 150 mg/dL, 75 mg/dL, and 0 mg/dL. These concentrations with their absorbent rates are measured to draw the golden calibration curve. The sample in Subgraph 3 is tested to get the absorbent reaction rate, and by interpolating with the golden curve, the concentration of the sample is determined as 94 mg/dL. We next consider two possible attacks on the assay: (1) alter the calibration curve on Subgraph 2; (2) tamper the concentration for Subgraph 3 with a waste droplet.

5.2.1 Attack 1. This attack changes the volume ratio of first split in Subgraph 2, and the concentrations of the child nodes are therefore changed accordingly (see Figure 8(b)). If the attack succeeds without being detected, the calibration curve is also altered, which is plotted as a red dotted line in Figure 9. The glucose concentration of the sample is mistakenly interpreted as 225 mg/dL, and the outcome for the patient may be hypoglycemia because of the insulin overdose. Fortunately, the proposed defense can easily detect this attack. The reconstructed graph is shown in Figure 8(b), where the compromised splitting operation is doubly circled in red. The defense mechanism identifies the difference between G_{re} and G_{in} because the splitting ratios are specifically identified.
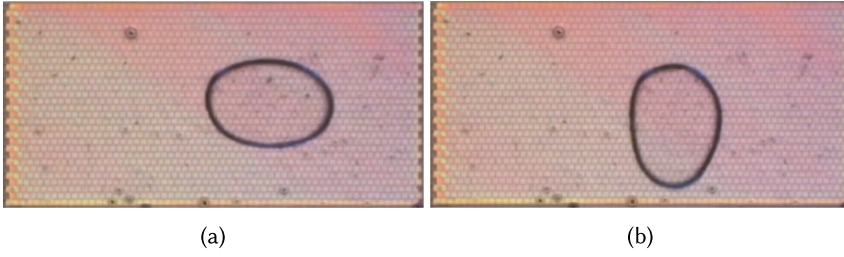
Fig. 10. An example of droplet morphing on a MEDA biochip, which was demonstrated using a MEDA biochip in the lab. Two different actuation patterns are applied to the same droplet, and the resultant droplet shapes are shown in (a) and (b), respectively.

5.2.2 Attack 2. This stealthy attack uses a waste droplet in Subgraph 2 and then discards the valuable sample and sends to the waste reservoir. The reconstructed graph is shown in Figure 8(c), where the two swapped operations are doubly circled in red. In this case, the glucose level is severely underestimated. As a result, the patient remains in hyperglycemia, which may lead to headache, fatigue, blurred vision, or even diabetic coma. However, such an undesirable consequence can be avoided because the proposed defense is able to detect the attack by comparing G_{re} with G_{in}.

6 DROPLET MORPHING AND FALSE ALARMS

In this section, we consider a case when droplets partially cover micro-electrodes. When this scenario occurs, the proposed security mechanism described in Section 4 may raise a false alarm based on the sensing data.

6.1 Droplet Morphing

MEDA biochips offer fine-grained control over droplets with many unique operations; one of these new operations is droplet morphing. An example of droplet morphing is shown in Figure 10. Two different actuation patterns are applied to the same droplet, and the shape of the droplet is changed accordingly. Even though the shape of a droplet is changed during droplet morphing, some characteristics of this droplet remain the same. Let the volume of a droplet d be $V(d)$, the gap height between two plates of the biochip be g, and the micro-electrode area that d occupies on the lower plate be $A(d)$. The volume of the droplet can be expressed as $V(d) = g \times A(d)$. When a droplet is morphed, $V(d)$ does not change, and neither does g. Therefore, $A(d)$ does not change after the morphing operation (i.e., the number of micro-electrodes that this droplet occupies does not change).

Note that when droplet morphing occurs, the droplet may partially overlap some micro-electrodes. An illustration of this scenario is shown in Figure 11. First, consider a droplet of size 5×3 on a MEDA biochip, as shown in Figure 11(a). Another actuation pattern is applied to the droplet, and the shape of the droplet changes to 3×5; the new shape of this droplet is shown in Figure 11(b). Even though the shape of the droplet changes, the number of micro-electrodes that this droplet occupies remains the same. However, when another actuation pattern is applied to the droplet, the shape of this droplet can change to 4×3.75, and some micro-electrodes under the droplet are partially overlapped by this droplet. Recall that the MC can only store 1-bit data for the sensing result (as mentioned in Section 2). For instance, if the sensing bit is 1, the micro-electrode is under a droplet. Because of the sensing limitation, the droplet may be sensed as being of size 4×4, which is different from the previously sensing result. Therefore, according
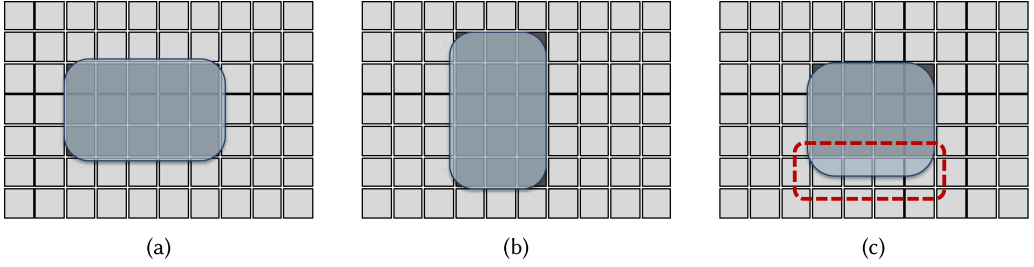
Fig. 11. Illustrations of droplet morphing and the corresponding actuation patterns. When actuation patterns are applied to a droplet, the shape of the droplet changes. The actuation patterns are marked in a dark gray color underneath the droplets. (a) The shape of the droplet is altered to 5×3 based on the underneath actuation pattern. (b) The shape of the droplet is converted to 3×5 based on the underneath actuation pattern. (c) The shape of the droplet is changed to 4×3.75 based on the underneath actuation pattern. Four micro-electrodes (highlighted in a red rectangle) are partially overlapped because of the shape.

to Lemma 1, the security mechanism described in Section 4 would raise a false alarm, indicating that an attack has been launched against the bioassay execution.

6.2 False Alarms

Based on the preceding example, we note that the security mechanism raises a false alarm when a droplet partially overlaps micro-electrodes. In this section, we first point out that the partially overlapping scenario leads to sensing inaccuracy in basic fluidic operations. We next present a theorem showing that the sensing inaccuracy results in a false alarm.

Assume that a droplet d_x is present on a MEDA biochip, and let the actual micro-electrode area that d_x occupies at time t be $A_t(d_x)$, where $A_t(d_x) \in \mathbb{N}$. The parameter $A(d_x)_t$ can be formulated as

$$A_t(d_x) = f_t(d_x) + p_t^+(d_x) + p_t^-(d_x), \tag{1}$$

where $f_t(d_x)$ represents the sum of the areas of micro-electrodes that are fully overlapped by d_x, $p_t^+(d_x)$ denotes the sum of the areas of micro-electrodes that are 50% or more overlapped by d_x, and $p_t^-(d_x)$ denotes the sum of the areas of micro-electrodes that are 50% or less overlapped by d_x.

In Section 4, we expressed the sensing result of a droplet as fp_t^x and denoted the droplet size sensed from a biochip as $|fp_t^x|$. Recall that when a MEDA biochip operates in sensing mode, micro-electrodes are charged with electric current, and the flip-flop within an MC samples the node voltage of the effective capacitor formed by the micro-electrode. The clock is tuned such that the flip-flop captures '1' when a droplet is present and '0' otherwise. Therefore, if a micro-electrode is 50% or more partially covered by a droplet, the sensing result captured in the MC is '1.' However, if a micro-electrode is 50% or less partially covered by a droplet, the sensing result captured in the MC is '0.' Based on these sensing outcomes, we can derive the following lemma.

LEMMA 8. *If a droplet d_x partially overlaps some micro-electrodes at time t, $|fp_t^x| \neq A_t(d_x)$ (i.e., the sensing result is inaccurate).*

PROOF. Because d_x partially overlaps some micro-electrodes, $p_t^+(d_x) \neq 0$ and $p_t^-(d_x) \neq 0$. According to the sensing outcomes, MCs that are associated with $f(d_x)$ or $p_t^+(d_x)$ store a '1' as the sensed bit, and MCs that are associated with $p_t^-(d_x)$ store a '0' as the sensed bit. Therefore, we can derive the following relationship:

$$|fp_t^x| = f(d_x) + \lceil p_t^+(d_x) \rceil. \tag{2}$$

From (1) and (2), we obtain $|fp_t^x| \neq A_t(d_x)$.   □

Using Lemma 8, we can prove that the security mechanism described in Section 4 raises a false alarm because droplets partially overlap micro-electrodes.

THEOREM 2. *If an inaccurate sensing result occurs at time t because droplets partially overlap some micro-electrodes during bioassay execution, the security mechanism raises a false alarm.*

PROOF. We prove the theorem by considering all possible fluidic operations. Let the partial overlap occur at time t during execution ($t \leq T$). According to Lemma 8, the partial overlap results in an inaccurate sensing result.

We first consider three fluidic operations that are relevant to the sensed size of a droplet: droplet transportation, droplet splitting, and droplet merging. Based on Lemma 1, a droplet is transported between time slots $t-1$ and t if $fp_{t-1}^x \cap fp_t^x \neq \emptyset$ and $|fp_{t-1}^x| = |fp_t^x|$. Consider the first scenario that a droplet d_x is transported between time slot $t-1$ and t and that d_x partially overlaps some micro-electrodes at time t. Because the sensing result of $|fp_t^x|$ is inaccurate, $|fp_{t-1}^x| \neq |fp_t^x|$. This transportation operation cannot therefore be recognized. Hence, the reconstructed G_{re} is not isomorphic to G_{in}. An alarm is raised even though no attack is launched against the biochip.

The second scenario is that the partial overlap happens when a droplet is split at time t. Lemma 4 states that two droplets d_x and d_y are obtained as a result of splitting a droplet d_z between time slots $t-1$ and t if $fp_t^x \neq \emptyset$, $fp_t^y \neq \emptyset$, $fp_{t-1}^z \neq \emptyset$, $fp_t^x \cap fp_{t-1}^z \neq \emptyset$, $fp_t^y \cap fp_{t-1}^z \neq \emptyset$, and $|fp_t^x| + |fp_t^y| = |fp_{t-1}^z|$. Since the partial overlap is assumed to happen at time t, the sensing result of $|fp_t^x|$ and/or $|fp_t^y|$ is inaccurate. Therefore, $|fp_t^x| + |fp_t^y| \neq |fp_{t-1}^z|$, and this splitting operation cannot be recognized. The reconstructed G_{re} is not isomorphic to G_{in}, and a false alarm is raised.

The third scenario is that two droplets are merged at time t. A droplet d_x is obtained as a result of merging two droplets d_y and d_z on the MEDA platform between time slots $t-1$ and t if $fp_t^x \neq \emptyset$, $fp_{t-1}^y \neq \emptyset$, $fp_{t-1}^z \neq \emptyset$, $fp_t^x \cap fp_{t-1}^y \neq \emptyset$, $fp_t^x \cap fp_{t-1}^z \neq \emptyset$, and $|fp_t^x| = |fp_{t-1}^y| + |fp_{t-1}^z|$. If droplet d_x partially overlaps some micro-electrodes at time t, $|fp_t^x| \neq |fp_{t-1}^y| + |fp_{t-1}^z|$. This merging operation cannot be recognized, and the reconstructed G_{re} is not isomorphic to G_{in}. Similar to the previous two scenarios, the security mechanism raises a false alarm.

The other three fluidic operations, including dispensing, discarding droplets as waste, and detection, are not relevant to the sensed size of a droplet (Lemma 2, Lemma 3, and Lemma 6). However, because of the fact that droplet-location maps are consecutive and that these operations must be performed in distinct locations on a MEDA biochip, these three fluidic operations must be associated with a previous/following droplet transportation. For example, if a droplet is dispensed at time t, the droplet must first be transported from the on-chip dispensing module to other modules for later operations. Even if the inaccurate sensing result does not affect dispensing recognition, the inaccurate sensing result has been proved to affect the associated droplet transportation. As a result, the reconstructed G_{re} is also not isomorphic to G_{in}. In such scenarios, the security mechanism also raises a false alarm. □

7 ENHANCING SENSING PRECISION TO AVOID FALSE ALARMS

In this section, we propose an enhanced sensing technique using the same MC design in MEDA biochips to prevent the false alarm described in Section 6. We first investigate the sensing function provided by the MEDA biochips and then propose a fine-grained sensing technique based on SPICE simulations. Finally, we show the effectiveness of the enhanced sensing technique by simulating bioassay execution with droplet-morphing operations.

7.1 Droplet Sensing in MEDA

The droplet-sensing function in an MC is achieved by timing the charging of the effective capacitance formed by a micro-electrode in the lower plate and the top plate [18]. An illustration of
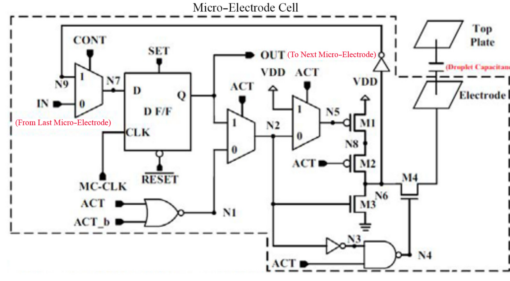
Fig. 12. Illustration of the MC circuit [18].

the MC circuit is shown in Figure 12. The overall sensing function has the following three steps. First, the top plate is connected to the ground voltage, and transistors M3 and M4 are turned on by the asserted ACT signal so that the micro-electrode is discharged. Second, the delay between ACT and ACT_b signals turns on transistors M1 and M2, and thereafter a charging current is injected into the micro-electrode. Third, the presence or absence of a droplet on a micro-electrode can result in different effective capacitances and the charging times. The MC-CLK signal is adjusted in such a way that a '0'/'1' bit is captured in the DFF without/with the presence of a droplet over the micro-electrode.

A droplet-location map, in a Boolean vector form, is scanned out from the MC daisy chain after sensing is accomplished. We use SPICE simulation to investigate the sensing function of a MEDA biochip. For the simulation, we use transistors from a 0.35-μm library, and we adopt the same macro-model for the extended-drain MOS (EDMOS) within an MC as in Li et al. [21]. Other than the MC circuit, we also calculate the effective capacitance for micro-electrodes using the following parameters. We set the gap g between two plates to be 25 μm, which is typical in digital microfluidics [12, 30]. Let the area of a micro-electrode be A, and $A = 50 \times 50$ μm^2 [14]. As a result, we can calculate the effective capacitance using the following equation:

$$C = \frac{\epsilon \times A}{g}, \tag{3}$$

where ϵ denotes the permittivity of the effective capacitance. Recall that silicone oil is used as a filler medium between the two plates to prevent both droplet evaporation and cross-contamination. Assuming that the temperature is 20°C, we can obtain values of water permittivity ϵ_w and silicon-oil permittivity ϵ_o as 710×10^{-12} (F/m) and 19×10^{-12} (F/m), respectively. As a result, the effective capacitance of a micro-electrode when a droplet is present can be calculated using (3): $C_w = \frac{\epsilon_w \times A}{g} = 8.875 \times 10^{-14}$ (F). Similarly, the effective capacitance of a micro-electrode when a droplet is not present can be calculated using the silicon-oil permittivity: $C_o = \frac{\epsilon_o \times A}{g} = 2.375 \times 10^{-15}$ (F). We simulate the sensing function based on the MC circuit and the calculated effective capacitance. The simulation result is shown in Figure 13. We note that it requires a longer time for a micro-electrode with a droplet present to charge the effective capacitance; when a droplet is present, the $N9$ node within the MC remains at 3.3 V longer than that for an MC without a droplet present. By adjusting the rising edge of the MC-CLK carefully, a Boolean result can be stored in the DFF, where a '1' indicates the presence of a droplet and a '0' otherwise.

7.2   Fine-Grained Sensing

According to Theorem 2, false alarms can be avoided if we can obtain the correct sensing result when a droplet partially overlaps some micro-electrodes during bioassay executions. Therefore, we propose an enhanced sensing technique that repeats the sensing function in MCs using various
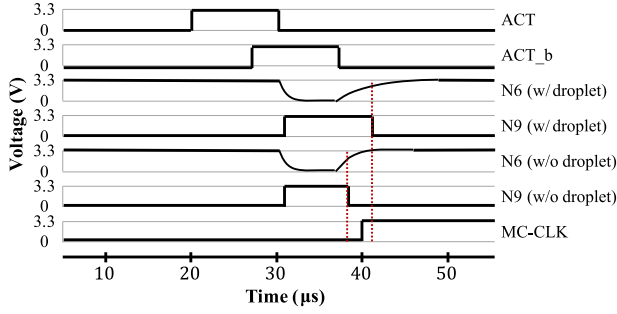
Fig. 13. Simulation results for the droplet-sensing in an MC.

delays of the rising edge of MC-CLK. If a micro-electrode is $p\%$ covered by a droplet, we can derive the corresponding effective capacitance using Equation (3) as

$$C = \left(\frac{p}{100} \times \epsilon_w + \frac{100 - p}{100} \times \epsilon_o \right) \frac{A}{g}.$$

The effective capacitance is a linear function of p. In addition, the delay of the rising edge of MC-CLK is designed to be changeable with the use of an integrated delay module [18]. Our simulation shows that by adjusting the rising edge of MC-CLK a few microseconds for multiple iterations, the sensing precision is improved from 1 micro-electrode to 0.1 micro-electrode. Let the sensing error for a droplet be E, whose unit is the number of micro-electrodes. Assume a droplet of size $w \times l$ is present on a MEDA biochip. For the original sensing function, $E \leq 2 \times (w + l) - 4$. With the enhanced sensing mechanism, the sensing error is less than $(2w + 2l - 4) \times 0.1$. For example, if a droplet is of size corresponding to 6×6 micro-electrodes, the corresponding sensing error is derived as $E \leq 2$.

Based on the simulation results, we modify the fluidic-operation lemmas and the security mechanism described in Section 4. Because the notation $|fp_t^x|$ for a droplet d_x ($|fp_x^x| \in \mathbb{Z}$) is not sufficient and precise for the enhanced sensing result, we now express the sensing area occupied by d_x at time t as $S_t(d_x)$, where $S_t(d_x) \in \mathbb{N}$. The sensing technique first estimates the sensing error E for each droplet using the following equation: $E = 0.1 \times S_t(d_x)$. Because Lemma 1, Lemma 4, and Lemma 5 are relevant to the sensing sizes of droplets, we modify them accordingly:

LEMMA 1 (ENHANCED). *A droplet d_x is transported on the MEDA platform between time slots $t - 1$ and t if and only if $fp_{t-1}^x \cap fp_t^x \neq \emptyset$ and $|S_{t-1}(d_x) - S_t(d_x)| \leq E$.*

LEMMA 4 (ENHANCED). *Two droplets d_x and d_y are obtained as a result of splitting a droplet d_z between time slots $t - 1$ and t if and only if $fp_t^x \neq \emptyset$, $fp_t^y \neq \emptyset$, $fp_{t-1}^z \neq \emptyset$, $fp_t^x \cap fp_{t-1}^z \neq \emptyset$, $fp_t^y \cap fp_{t-1}^z \neq \emptyset$, and $|S_{t-1}(d_z) - (S_t(d_x) + S_t(d_y))| \leq E$.*

LEMMA 5 (ENHANCED). *A droplet d_x is obtained as a result of merging two droplets d_y and d_z on the MEDA platform between time slots $t - 1$ and t if and only if $fp_t^x \neq \emptyset$, $fp_{t-1}^y \neq \emptyset$, $fp_{t-1}^z \neq \emptyset$, $fp_t^x \cap fp_{t-1}^y \neq \emptyset$, $fp_t^x \cap fp_{t-1}^z \neq \emptyset$, and $|S_t(d_x) - (S_{t-1}(d_y) + S_{t-1}(d_z))| \leq E$.*

The proofs of these lemmas can be derived using the proofs for the original lemmas because only the sensing size of a droplet d_t^x is changed from $|fp_t^x|$ to $S_t(d_x)$. The overall control flow of the proposed defense is modified according to these enhanced lemmas (see Figure 14). The enhanced defense does not employ the fine-grained sensing technique at every operational cycle. The new sensing technique performs the sensing function in MCs for a total of 10 times with various rising-edge delays in MC-CLK to obtain the 0.1-micro-electrode sensing precision. As a result, the sensing
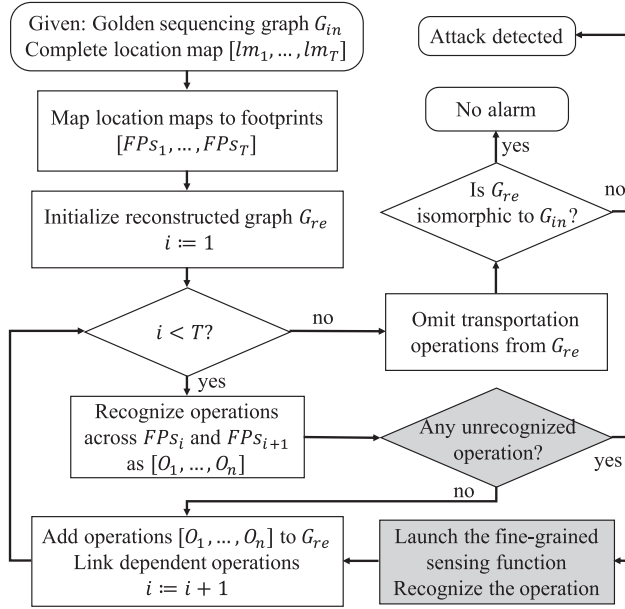
Fig. 14. Control flow corresponding to the proposed defense using the fine-grained sensing technique. New introduced steps are highlighted with a gray color.

technique incurs a 10X time overhead when compared with the original sensing function. Recall that both the actuation pattern and the sensing results are scanned using the same daisy-chain structure in a MEDA biochip. Therefore, slowing down a sensing function will stall the following scanned-in actuation patterns and the remaining fluidic operations. The timing overhead is not a concern, however, because the timescales of bio-protocols are much larger than the clock time period used in MEDA. To achieve an efficient security defense, the defense follows the same control flow as mentioned in Section 4, but when sensing sizes of a droplet d_x are different across two consecutive time slots (i.e., $|fp_t^x| \neq |fp_{t-1}^x|$), the enhanced security defense triggers the enhanced sensing technique to avoid false alarms.

7.3 Simulation Results

Similar to the simulations in Section 5, we simulated the multiplexed *in vitro* diagnostics of serum and plasma on a MEDA platform with 60×30 micro-electrodes [31] to demonstrate the effectiveness of the enhanced defense. Location maps are generated by simulating assay execution. We consider that droplets are 4×4. In contrast to the original assay in Section 5.1, we inserted two droplet-morphing operations during bioassay execution. The modified sequencing graph is shown in Figure 15(a). Even though we add two droplet-morphing operations, the outcome of the assay does not change. Because the bioassay outcome remains the same, a reliable security mechanism used during assay execution must not raise false alarms.

The first droplet-morphing operation is executed between time slot 23 and time slot 24. Figure 15(b) shows the droplet-morphing operation. The droplet is actuated by a 3×5 micro-electrode pattern underneath it. We simulated both the original security method and the enhanced security method based on the two sensing mechanisms. Figure 15(c) shows the sensing results for both the original sensing function and the enhanced sensing mechanism. Using the original sensing function, which does not consider the droplet overlap, the sensed size of the droplet is 15 instead of
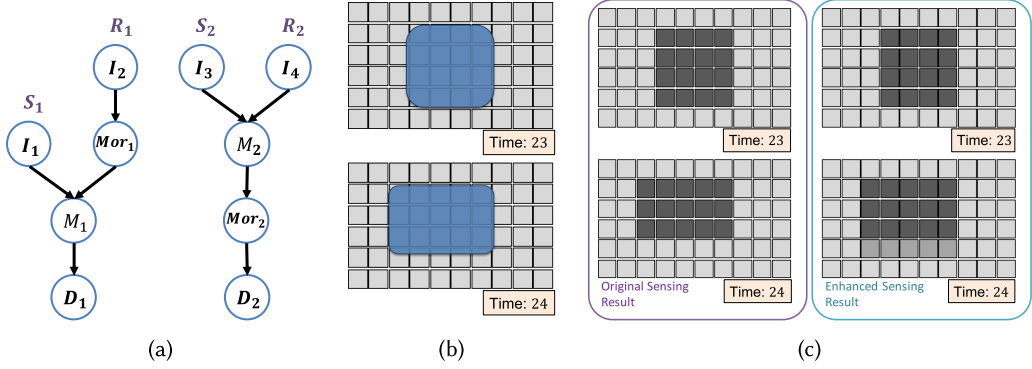
Fig. 15. Droplet morphing during bioassay execution. (a) The modified sequencing graph for multiplex *in vitro* diagnostics with extra droplet-morphing operations. The nodes I_i, M_i, D_i, S_i, and Mor_i represent dispensing, merging, detecting, splitting, and morphing operations, respectively. (b) The first droplet-morphing operation is inserted between time slot 23 and time slot 24. (c) The original sensing function captures the droplet size as 16 at time slot 23 and the droplet size as 15 at time slot 24. However, the enhanced sensing mechanism captures the droplet size as 16 at time slot 23, and it also captures the droplet size as 16 at time slot 24.

16. The erroneous result leads to an unrecognized fluidic operation, and consequently the security mechanism raises a false alarm that indicates an attack has been introduced. However, using the enhanced sensing mechanism, the droplet size at time slot 24 is computed correctly. The enhanced sensing mechanism indicates that 15 micro-electrodes are fully covered by the droplet and 5 micro-electrodes are 20% partially covered by the droplet. Therefore, the droplet size is derived as $15 + 5 \times 0.2 = 16$. Because the sensed droplet size is consistent, the enhanced security method does not raise a false alarm.

8 CONCLUSION

We have presented a lightweight, but effective, security solution for MEDA biochips. This approach can detect malicious attacks in the MEDA platform. We have shown that the provably secure assay execution can be guaranteed using this solution. Simulation results for two real-life assays demonstrate the effectiveness of this solution for thwarting attacks and preventing harmful consequences. We have also provided a fine-grained sensing technique to enhance the defense so that false alarms can be avoided.

APPENDIX: PROOFS OF LEMMAS AND THEOREM 1

We present proofs for the lemmas and theorems stated in the article. To help readers better understand the proofs, we list our notation in Table 2.

LEMMA A.1. *If a droplet d_x exists on the chip at time slots $t - 1$ and t, $fp_t^x \cap fp_{t-1}^y = \emptyset$ for any other droplet d_y.*

PROOF. Let the footprint of droplet d_x at time $t - 1$ be fp_{t-1}^x and the droplet closest to d_x at time $t - 1$ be d_y. Due to the need for a safe distance between droplets [20], the minimal distance between fp_{t-1}^x and fp_{t-1}^y is four micro-electrodes. For fp_t^x and fp_{t-1}^y to overlap, the droplet d_x has to move pass through at least four micro-electrodes in a single cycle. According to Lai et al. [18], the length of one actuation cycle is 110 ms, and the length of one micro-electrode is 37 μm. This implies that d_x must move at a velocity of at least $(4 \times 37)/110 = 1.35$ mm/s. This velocity is

Table 2. Notation Used for the Proofs

Symbols	Description
G_{in}	Input sequencing graph
G_{re}	Reconstructed sequencing graph
n_i	ith node in sequencing graph
I_i	ith dispensing operation in sequencing graph
S_i	ith splitting operation in sequencing graph
M_i	ith merging operation in sequencing graph
W_i	ith waste-droplet discarding operation in sequencing graph
D_i	ith detection for droplets in sequencing graph
lm_t	Location map as a Boolean-value vector generated at time t
t	Time scale in range $0 < t \leq T$, $t \in \mathbb{N}$
T	End time of assay execution, $T \in \mathbb{N}$
d_x	A droplet x on a given MEDA biochip
fp_t^x	Set of electrodes that represents the location of a droplet d_x at time t
U	Universal set of all the micro-electrodes in the MEDA platform

well above the upper limit of 1 mm/s [20]. Therefore, a droplet cannot overlap with other droplet's footprint from the previous cycle.   □

LEMMA A.2. *A droplet d_x exists on a MEDA biochip at times $t - 1$ and t if and only if $fp_t^x \neq \emptyset$, $fp_{t-1}^x \neq \emptyset$, and $fp_t^x \cap fp_{t-1}^x \neq \emptyset$.*

PROOF. ($\Rightarrow$) Suppose a droplet d_x exists at $t - 1$ and t. Thus, $fp_t^x \neq \emptyset$ and $fp_{t-1}^x \neq \emptyset$. The proof of $fp_t^x \cap fp_{t-1}^x \neq \emptyset$ is obvious from that fact that a droplet must overlap adjacent micro-electrodes to ensure movement. Next we prove the "if" part. A non-empty footprint fp_{t-1}^x indicates that a droplet d_x exists at time $t - 1$. Likewise, a non-empty fp_t^x indicates that a droplet d_x exists at time t. Assume that these two droplets are not the same, and let the droplet at $t - 1$ be $d_{\bar{x}}$. Since $fp_t^x \cap fp_{t-1}^x \neq \emptyset$, d_x must move to the previous location of droplet $d_{\bar{x}}$ at time t. This contradicts Lemma A.1. Hence, the two droplets d_x and $d_{\bar{x}}$ are actually the same.   □

LEMMA 2 (RESTATED). *A droplet d_x is dispensed on the MEDA platform between time slots $t - 1$ and t if and only if $fp_t^x \neq \emptyset$ and $fp_{t-1}^x = \emptyset$.*

PROOF. ($\Rightarrow$) The droplet d_x does not appear on the platform until time t. As a result, the footprints of d_x before time $t - 1$ are empty sets, and the footprints of droplet d_x after time t are not empty sets.

($\Leftarrow$) From Lemma A.2, we know that if fp_{t-1}^x or fp_t^x is an empty set, d_x must not exist at both $t - 1$ and t. We also know that $fp_t^x \neq \emptyset$ indicates that d_x exists on the platform at time t. Thus, d_x must not exist on the platform at time $t - 1$. Hence, the droplet is dispensed to the platform at time t.   □

LEMMA 3 (RESTATED). *A droplet d_x is discarded from the MEDA platform between time slots $t - 1$ and t if and only if $fp_{t-1}^x \neq \emptyset$ and $fp_t^x = \emptyset$.*

PROOF. ($\Rightarrow$) The droplet d_x exists on the platform until time $t - 1$, implying $fp_{t-1}^x \neq \emptyset$ and $fp_t^x = \emptyset$.

($\Leftarrow$) Based on Lemma A.2, we know that if fp_{t-1}^x or fp_t^x is an empty set, d_x must not exist at both $t - 1$ and t. Since $fp_{t-1}^x \neq \emptyset$ indicates that d_x exists on the platform at time $t - 1$, d_x must not exist on the platform at t. Hence, we conclude that d_x is discarded to waste reservoirs at t.   □

LEMMA 1 (RESTATED). *A droplet d_x is transported on the MEDA platform between time slots $t - 1$ and t if and only if $fp_{t-1}^x \cap fp_t^x \neq \emptyset$ and $|fp_{t-1}^x| = |fp_t^x|$.*

PROOF. ($\Rightarrow$) Since d_x exists at $t - 1$ and t, $fp_{t-1}^x \cap fp_t^x \neq \emptyset$ by Lemma A.2. The volume of a droplet equals to the droplet's bottom area times the gap between upper and lower plates. Since the volume of d_x and the gap between plates do not change over time, the bottom area of d_x remains the same (i.e., $|fp_t^x| = |fp_{t-1}^x|$).

($\Leftarrow$) By Lemma A.2, we know that these two footprints indicate the same droplet d_x. In addition, $fp_{t-1}^x \neq \emptyset$ indicates the area where d_x locates at time $t - 1$, and so does $fp_t^x \neq \emptyset$. As a result, the droplet is transported at time t. □

LEMMA 4 (RESTATED). *Two droplets d_x and d_y are obtained as a result of splitting a droplet d_z between time slots $t - 1$ and t if and only if $fp_t^x \neq \emptyset$, $fp_t^y \neq \emptyset$, $fp_{t-1}^z \neq \emptyset$, $fp_t^x \cap fp_{t-1}^z \neq \emptyset$, $fp_t^y \cap fp_{t-1}^z \neq \emptyset$, and $|fp_t^x| + |fp_t^y| = |fp_{t-1}^z|$.*

PROOF. ($\Rightarrow$) Assume that we divide the droplet d_z into two smaller droplets at time $t - 1$, and let them be $d_{\bar{x}}$ and $d_{\bar{y}}$, which has the same volume of the droplets d_x and d_y, respectively, and $fp_{t-1}^{\bar{x}} \cap fp_t^x \neq \emptyset$, $fp_{t-1}^{\bar{y}} \cap fp_t^y \neq \emptyset$. We first consider d_x and $d_{\bar{x}}$. According to Lemma 1, $fp_{t-1}^{\bar{x}} \cap fp_t^x \neq \emptyset$ and $|fp_{t-1}^{\bar{x}}| = |fp_t^x|$. We also know that $fp_{t-1}^{\bar{x}} \subset fp_{t-1}^z$ because the droplet $d_{\bar{x}}$ is part of the droplet d_z. As a result, $fp_t^x \cap fp_{t-1}^z \neq \emptyset$. Likewise, for d_y and $d_{\bar{y}}$, we know $fp_t^y \cap fp_{t-1}^z \neq \emptyset$. Since $|fp_{t-1}^{\bar{x}}| + |fp_{t-1}^{\bar{y}}| = |fp_{t-1}^z|$, $|fp_{t-1}^{\bar{x}}| = |fp_t^x|$, and $|fp_{t-1}^{\bar{y}}| = |fp_t^y|$, we can obtain $|fp_t^x| + |fp_t^y| = |fp_{t-1}^z|$.

($\Leftarrow$) Let $fp_{t-1}^{\bar{x}} + fp_{t-1}^{\bar{y}} = fp_{t-1}^z$, where $fp_{t-1}^{\bar{x}} \cap fp_t^x \neq \emptyset$, $fp_{t-1}^{\bar{y}} \cap fp_t^y \neq \emptyset$, $|fp_{t-1}^{\bar{x}}| = |fp_t^x|$, and $|fp_{t-1}^{\bar{y}}| = |fp_t^y|$. From Lemma 1, we can infer that a droplet d_x is transported from the area above $fp_{t-1}^{\bar{x}}$ to the area above fp_t^x at time t. Since $fp_{t-1}^{\bar{x}} \subset fp_{t-1}^z$, the droplet d_x was part of the droplet d_z at time $t - 1$. Hence, d_x is extracted from the droplet d_z. Likewise, we can infer that d_y is also extracted from the droplet d_z. As a result, d_x and d_y are obtained as a result of splitting a droplet d_z between time slots $t - 1$ and t. □

LEMMA 5 (RESTATED). *A droplet d_x is obtained as a result of merging two droplets d_y and d_z on the MEDA platform between time slots $t - 1$ and t if and only if $fp_t^x \neq \emptyset$, $fp_{t-1}^y \neq \emptyset$, $fp_{t-1}^z \neq \emptyset$, $fp_t^x \cap fp_{t-1}^y \neq \emptyset$, $fp_t^x \cap fp_{t-1}^z \neq \emptyset$, and $|fp_t^x| = |fp_{t-1}^y| + |fp_{t-1}^z|$.*

PROOF. ($\Rightarrow$) Because d_x exists at t, $fp_t^x \neq \emptyset$. The droplet d_x can be viewed as two droplets $d_{\bar{y}}$ and $d_{\bar{z}}$ connecting together, where the volume of $d_{\bar{y}}$ equals to the volume of droplet d_y and the volume of $d_{\bar{z}}$ equals to the volume of droplet d_z. These two droplets are transported as d_x and d_y at t, respectively. According to Lemma 1, $fp_t^{\bar{y}} \cap fp_{t-1}^y \neq \emptyset$, $fp_t^{\bar{z}} \cap fp_{t-1}^z \neq \emptyset$, $|fp_t^{\bar{y}}| = |fp_{t-1}^y|$, and $|fp_t^{\bar{z}}| = |fp_{t-1}^z|$. Since droplets $d_{\bar{y}}$ and $d_{\bar{z}}$ are two parts of the droplet d_x, $fp_t^x = fp_t^{\bar{y}} \cup fp_t^{\bar{z}}$. Hence, $fp_t^x \cap fp_{t-1}^y \neq \emptyset$, $fp_t^x \cap fp_{t-1}^z \neq \emptyset$, and $|fp_t^x| = |fp_{t-1}^y| + |fp_{t-1}^z|$.

($\Leftarrow$) fp_t^x can be partitioned into two footprints $fp_t^{\bar{y}}$ and $fp_t^{\bar{z}}$, where $|fp_t^{\bar{y}}| = |fp_{t-1}^y|$, $|fp_t^{\bar{z}}| = |fp_{t-1}^z|$, $fp_t^{\bar{y}} \cap fp_{t-1}^y \neq \emptyset$, and $fp_t^{\bar{z}} \cap fp_{t-1}^z \neq \emptyset$. According to Lemma 1, the droplet d_y is transported to the area above $fp_t^{\bar{y}}$, and the droplet d_z is transported to the area above $fp_t^{\bar{z}}$ at time t. Since two footprints $fp_t^{\bar{y}}$ and $fp_t^{\bar{z}}$ are subsets of the footprint fp_t^x, two droplets d_y and d_z are actually two parts of the droplet d_x at time t (i.e., they merge as the droplet d_x at time t). □

LEMMA 6 (RESTATED). *A droplet d_x is detected on the MEDA platform at time T (end of the assay) if and only if $fp_T^x \neq \emptyset$.*

PROOF. The proof is obvious from the assumption that on-chip droplets at the end of the assay are for detection. □

LEMMA 7 (RESTATED). *The sequencing graph can be reconstructed from a complete sequence of droplet-location maps from the start to the end of the assay (i.e., $(lm_1, lm_2, \ldots, lm_T)$).*

PROOF. Let fp_t^x be any footprint obtained at t, where $1 < t \le T$, and $fp_t^x \subset U$. The operation of d_x at t can be inferred from fp_{t-1}^x. Because location maps are consecutive, the dependencies between the contiguous operations are also acquired. Hence, a sequencing graph can be reconstructed from the complete sequence of location maps, and G_{re} can be obtained by omitting transportation operations from this graph.   □

THEOREM 1 (RESTATED). *If a sequencing graph G_{in} is synthesized on a MEDA biochip and the biochip is not compromised by an attack, the sequencing graph G_{re} reconstructed from the droplet-location maps is isomorphic to G_{in}. If an attack compromises one or more operations, G_{re} is no longer isomorphic to G_{in}.*

PROOF. Let n_i be ith node in G_{in} where $n_i \in \{I_i, D_i, S_i, M_i, W_i\}$. After the assay is synthesized on a MEDA biochip, there exists a footprint fp_t^i for operation n_i at time t. The operation n_i in G_{re} is reconstructed from fp_t^i based on Lemma 7. Since node n_i can represent any operation in G_{in}, G_{in} and G_{re} must be isomorphic.

Based on the attack classification in Table 1 from the article, two kinds of modification on G_{in} are (1) node change and (2) edge redirection. In the first scenario, assume n_i in G_{in} is compromised by an attack and n_i is replaced with $\bar{n}_i$. After the assay is synthesized on a MEDA biochip, there exists a footprint fp_t^i for operation $\bar{n}_i$. The operation $\bar{n}_i$ is reconstructed in G_{re} from fp_t^i based on Lemma 7. Since $n_i \ne \bar{n}_i$, G_{re} is not isomorphic to G_{in}. In the second scenario, assume there is an edge from n_i to n_j in G_{in}, and the edge is redirected from n_k to n_j due to an attack. After the compromised assay is synthesized on a MEDA biochip, there exist footprints for operations of n_k, n_j, and transportation from n_k to n_j. These operations are reconstructed in G_{re} based on Lemma 7, and there is an edge connecting n_k to n_j. Because the edge from n_k to n_j is not the same as the edge from n_i to n_j, G_{re} is not isomorphic to G_{in}.   □

ACKNOWLEDGMENT

REFERENCES

[1] Illumina. 2014. NeoPrep NFS Library Prep with Digital Microfluidics. Retrieved December 17, 2019 from https://support.illumina.com/content/dam/illumina-marketing/documents/products/brochures/brochure-neoprep.pdf.

[2] Baebies. 2016. FDA Advisors Approve of Baebies' SEEKER Analyzer for Newborns. Retrieved December 17, 2019 from https://www.baebies.com/fda-advisors-back-approval-baebies-seeker-analyzer-newborns/.

[3] Centers for Disease Control and Prevention. 2017. National Diabetes Statistics Report. Retrieved December 17, 2019 from https://www.cdc.gov/diabetes/data/statistics/statistics-report.html.

[4] Transcriptic. 2018. Home Page. Retrieved December 17, 2019 from https://www.transcriptic.com/.

[5] Emerald Cloud Lab. 2018. Home Page. Retrieved December 17, 2019 from https://www.emeraldcloudlab.com/.

[6] Sk Subidh Ali, Mohamed Ibrahim, Jeyavijayan Rajendran, Ozgur Sinanoglu, and Krishnendu Chakrabarty. 2016. Supply-chain security of digital microfluidic biochips. *Computer* 49, 8 (2016), 36–43.

[7] Sk Subidh Ali, Mohamed Ibrahim, Ozgur Sinanoglu, Krishnendu Chakrabarty, and Ramesh Karri. 2016. Security assessment of cyberphysical digital microfluidic biochips. *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 13, 3 (2016), 445–458.

[8] John Adrian Bondy and Uppaluri Siva Ramachandra Murty.1976. *Graph Theory with Applications.* Vol. 290. Macmillan London.

[9] Kihwan Choi, Alphonsus H. C. Ng, Ryan Fobel, and Aaron R. Wheeler. 2012. Digital microfluidics. *Annual Review of Analytical Chemistry* 5 (2012), 413–440.

[10] Wei-Lung Chou, Pee-Yew Lee, Cing-Long Yang, Wen-Ying Huang, and Yung-Sheng Lin. 2015. Recent advances in applications of droplet microfluidics. *Micromachines* 6, 9 (2015), 1249–1271.

[11] Richard B. Fair, Andrey Khlystov, Tina D. Tailor, Vladislav Ivanov, Randall D. Evans, Vijay Srinivasan, Vamsee K. Pamula, Michael G. Pollack, Peter B. Griffin, and Jack Zhou. 2007. Chemical and biological applications of digital-microfluidic devices. *IEEE Design & Test of Computers* 24, 1 (2007), 10–24.

[12] Shih-Kang Fan, Tsung-Han Hsieh, and Di-Yu Lin. 2009. General digital microfluidic platform manipulating dielectric and conductive droplets by dielectrophoresis and electrowetting. *Lab on a Chip* 9, 9 (2009), 1236–1242.

[13] Jean-Loup Faulon. 1998. Isomorphism, automorphism partitioning, and canonical labeling can be solved in polynomial-time for molecular graphs. *Journal of Chemical Information and Computer Sciences* 38, 3 (1998), 432–444.

[14] Yingchieh Ho, Gary Wang, Kelvin Yi-Tse Lai, Yi-Wen Lu, Keng-Ming Liu, Yun-Ming Wang, and Chen-Yi Lee. 2016. Design of a micro-electrode cell for programmable lab-on-CMOS platform. In *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'16)*. 2871–2874.

[15] John E. Hopcroft and Jin-Kue Wong. 1974. Linear time algorithm for isomorphism of planar graphs. In *Proceeedings of the ACM Symposium on Theory of Computing*. ACM, New York, NY, 172–184.

[16] Oliver Keszocze, Zipeng Li, Andreas Grimmer, Robert Wille, Krishnendu Chakrabarty, and Rolf Drechsler. 2017. Exact routing for micro-electrode-dot-array digital microfluidic biochips. In *Proceedings of the ACM Asia and South Pacific Design Automation Conference (ASP-DAC'17)*. ACM, New York, NY, 708–713.

[17] Ryoji Kurita, Katsuyoshi Hayashi, Xu Fan, Katsunobu Yamamoto, Takeshi Kato, and Osamu Niwa. 2002. Microfluidic device integrated with pre-reactor and dual enzyme-modified microelectrodes for monitoring in vivo glucose and lactate. *Sensors and Actuators B: Chemical* 87, 2 (2002), 296–303.

[18] Kelvin Yi-Tse Lai, Yu-Tao Yang, and Chen-Yi Lee. 2015. An intelligent digital microfluidic processor for biomedical detection. *Journal of Signal Processing Systems* 78, 1 (2015), 85–93.

[19] Zipeng Li, Kelvin Yi-Tse Lai, Krishnendu Chakrabarty, Tsung-Yi Ho, and Chen-Yi Lee. 2017. Sample preparation on micro-electrode-dot-array digital microfluidic biochips. In *Proceedings of the IEEE Computer Society Annual Symposium on VLSI*. IEEE, Los Alamitos, CA, 146–151.

[20] Zipeng Li, Kelvin Yi-Tse Lai, Po-Hsien Yu, Krishnendu Chakrabarty, Tsung-Yi Ho, and Chen-Yi Lee. 2017. Droplet size-aware high-level synthesis for micro-electrode-dot-array digital microfluidic biochips. *IEEE Transactions on Biomedical Circuits and Systems* 11, 3 (2017), 612–626.

[21] Zipeng Li, Kelvin Yi-Tse Lai, Po-Hsien Yu, Krishnendu Chakrabarty, Tsung-Yi Ho, and Chen-Yi Lee. 2017. Structural and functional test methods for micro-electrode-dot-array digital microfluidic biochips. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 37, 5 (2018), 968–981.

[22] Zipeng Li, Kelvin Yi-Tse Lai, Po-Hsien Yu, Krishnendu Chakrabarty, Miroslav Pajic, Tsung-Yi Ho, and Chen-Yi Lee. 2016. Error recovery in a micro-electrode-dot-array digital microfluidic biochip. In *Proceedings of the IEEE International Conference on Computer Aided Design (ICCAD'16)*. IEEE, Los Alamitos, CA, 1–8.

[23] Tung-Che Liang, Yun-Sheng Chan, Tsung-Yi Ho, Krishnendu Chakrabarty, and Chen-Yi Lee. 2019. Sample preparation for multiple-reactant bioassays on micro-electrode-dot-array biochips. In *Proceedings of the ACM Asia and South Pacific Design Automation Conference (ASP-DAC'19)*. ACM, New York, NY, 468–473.

[24] Tung-Che Liang, Mohammed Shayan, Krishnendu Chakrabarty, and Ramesh Karri. 2019. Execution of provably secure assays on MEDA biochips to thwart attacks. In *Proceedings of the ACM Asia and South Pacific Design Automation Conference (ASP-DAC'19)*. ACM, New York, NY, 51–57.

[25] Eugene M. Luks. 1982. Isomorphism of graphs of bounded valence can be tested in polynomial time. *Journal of Computer and System Sciences* 25, 1 (1982), 42–65.

[26] Brendan D. McKay. 1981. *Practical Graph Isomorphism*. Department of Computer Science, Vanderbilt University, Nashville, TN.

[27] Michael G. Pollack, Alexander D. Shenderov, and R. B. Fair. 2002. Electrowetting-based actuation of droplets for integrated microfluidics. *Lab on a Chip* 2, 2 (2002), 96–101.

[28] Catherine Quilliet and Bruno Berge. 2001. Electrowetting: A recent outbreak. *Current Opinion in Colloid & Interface Science* 6, 1 (2001), 34–39.

[29] Ronald C. Read and Derek G. Corneil. 1977. The graph isomorphism disease. *Journal of Graph Theory* 1, 4 (1977), 339–363.

[30] Ehsan Samiei and Mina Hoorfar. 2015. Systematic analysis of geometrical based unequal droplet splitting in digital microfluidics. *Journal of Micromechanics and Microengineering* 25, 5 (2015), 055008.

[31] Fei Su, William Hwang, and Krishnendu Chakrabarty. 2006. Droplet routing in the synthesis of digital microfluidic biochips. In *Proceedings of the IEEE Design, Automation, and Test in Europe Conference (DATE'06)*, Vol. 1. IEEE, Los Alamitos, CA, 1–6.

[32] Jack Tang, Mohamed Ibrahim, Krishnendu Chakrabarty, and Ramesh Karri. 2017. Secure randomized checkpointing for digital microfluidic biochips. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 37, 6 (2017), 1119–1132.

[33] Gary Wang, Daniel Teng, and S.-K. Fan. 2011. Digital microfluidic operations on micro-electrode dot array architecture. *IET Nanobiotechnology* 5, 4 (2011), 152–160.

[34] Zhanwei Zhong, Zipeng Li, and Krishnendu Chakrabarty. 2017. Adaptive error recovery in micro-electrode-dot-array biochips based on droplet-aliquot operations and predictive analysis. In *Proceedings of the IEEE International Conference on Computer Aided Design (ICCAD'17)*. IEEE, Los Alamitos, CA, 615–622.

[35] Zhanwei Zhong, Zipeng Li, Krishnendu Chakrabarty, Tsung-Yi Ho, and Chen-Yi Lee. 2018. Micro-electrode-dot-array digital microfluidic biochips: Technology, design automation, and test techniques. *IEEE Transactions on Biomedical Circuits and Systems* 13, 2 (2018), 292–313.