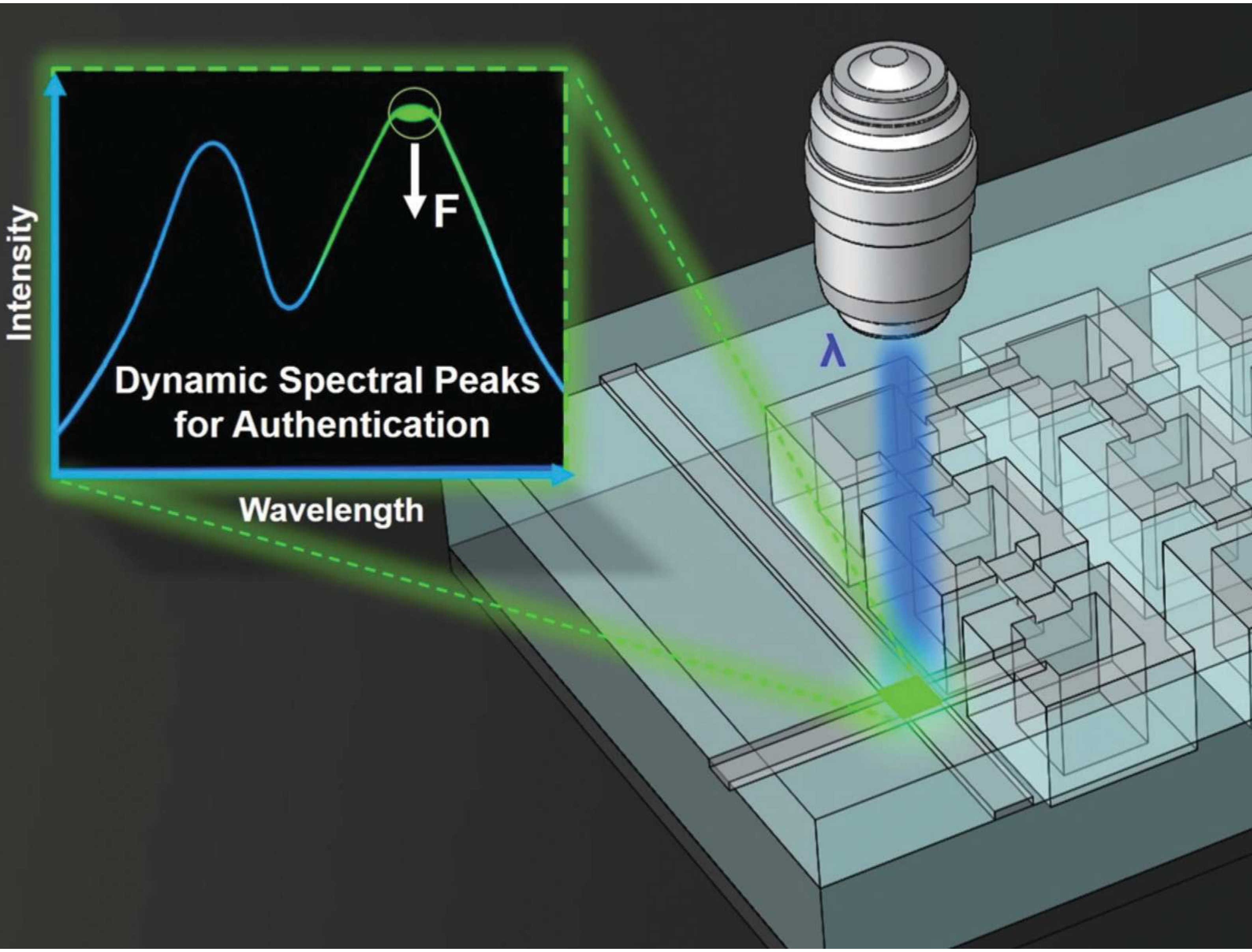
Volume 23
Number 19
7 October 2023
Pages 4149–4368

Lab on a Chip

Devices and applications at the micro- and nanoscale

rsc.li/loc



ISSN 1473-0197

ROYAL SOCIETY
OF **CHEMISTRY**

PAPER
Navajit Singh Baban *et al.*
Material-level countermeasures for securing
microfluidic biochips

Lab on a Chip

ROYAL SOCIETY OF CHEMISTRY

PAPER

View Article Online
View Journal | View Issue

Check for updates

Cite this: *Lab Chip*, 2023, **23**, 4213

Material-level countermeasures for securing microfluidic biochips†

Navajit Singh Baban, *[a] Sohini Saha,[b] Sofija Jancheska,[c] Inderjeet Singh,[a] Sachin Khapli,[a] Maksat Khobdabayev,[a] Jongmin Kim,[a] Sukanta Bhattacharjee,[d] Yong-Ak Song, [aef] Krishnendu Chakrabarty[g] and Ramesh Karri[c]

Received 17th April 2023, Accepted 13th August 2023

DOI: 10.1039/d3lc00335c

rsc.li/loc

Flow-based microfluidic biochips (FMBs) have been rapidly commercialized and deployed in recent years for biological computing, clinical diagnostics, and point-of-care-tests (POCTs). However, outsourcing FMBs makes them susceptible to material-level attacks by malicious actors for illegitimate monetary gain. The attacks involve deliberate material degradation of an FMB's polydimethylsiloxane (PDMS) components by either doping with reactive solvents or altering the PDMS curing ratio during fabrication. Such attacks are stealthy enough to evade detection and deteriorate the FMB's function. Furthermore, material-level attacks can become prevalent in attacks based on intellectual property (IP) theft, such as counterfeiting, overbuilding, *etc.*, which involve unscrupulous third-party manufacturers. To address this problem, we present a dynamic material-level watermarking scheme for PDMS-based FMBs with microvalves using a perylene-labeled fluorescent dye. The dyed microvalves show a unique excimer intensity peak under 405 nm laser excitation. Moreover, when pneumatically actuated, the peak shows a predetermined downward shift in intensity as a function of mechanical strain. We validated this protection scheme experimentally using fluorescence microscopy, which showed a high correlation (R^2 = 0.971) between the normalized excimer intensity change and the maximum principal strain of the actuated microvalves. To detect curing ratio-based attacks, we adapted machine learning (ML) models, which were trained on the force-displacement data obtained from a mechanical punch test method. Our ML models achieved more than 99% accuracy in detecting curing ratio anomalies. These countermeasures can be used to proactively safeguard FMBs against material-level attacks in the era of global pandemics and diagnostics based on POCTs.

Introduction

Microfluidics is the interdisciplinary study of fluid manipulation at microliter or nanoliter volumes. A microfluidic biochip (also known as a lab-on-a-chip) encapsulates the capabilities of a laboratory by integrating different biochemical functionalities into a single miniaturized device.[1,2] Biochip components typically consist of microchannels, microvalves, micropumps, micromixers, microseparators, and reaction chambers. Biochips are ultra-fast in their intended operations, *i.e.*, dispensing, mixing, splitting, transportation, *etc.*, because of a very small amount of samples compared to traditional test tube-based laboratories.[3] They have been a game-changer in biological computing such as enzymatic, deoxyribonucleic acid (DNA) and proteomic analysis, genetic and polymerase chain reaction (PCR) studies, molecular biology procedures, surface immunoassays, medical diagnostics, cell culture, environmental sampling and toxicity monitoring, *etc.*[3,4]

Microfluidic biochips offer various advantages over conventional test-tube-based laboratory techniques, which include reduced sample volume, faster biochemical reactions, higher system throughput, automation, and ultra-sensitive detection.[5] They attain miniaturization without the need for extra equipment and thus are revolutionizing biomedical

[a] *Division of Engineering, New York University Abu Dhabi, Abu Dhabi, United Arab Emirates. E-mail: nsb359@nyu.edu*
[b] *Department of Electrical and Computer Engineering, Duke University, Durham, USA*
[c] *Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University, New York, USA*
[d] *Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, India*
[e] *Department of Chemical and Biomolecular Engineering, Tandon School of Engineering, New York University, New York, USA*
[f] *Department of Biomedical Engineering, Tandon School of Engineering, New York University, New York, USA*
[g] *School of Electrical, Computer and Energy Engineering, Arizona State University, Phoenix, Arizona, USA*

† Electronic supplementary information (ESI) available. See DOI: https://doi.org/10.1039/d3lc00335c

applications such as point-of-care tests (POCTs),[6] amplification platforms,[7] biomolecular recognition,[8] antigen detection,[8] and personalized cancer treatment.[9] Thus, they can potentially advance global healthcare by meeting urgent needs for diagnostic tests in places with limited laboratory facilities.

To date, 47% of the global population has little or no access to diagnostics.[10] Further, the need for the increased availability of diagnostic tests for public health has never become more evident than in the global response to the recent coronavirus disease 2019 (COVID-19) pandemic.[11] The pandemic highlighted years of under-investment and neglect that led to a gross inequity in access to diagnostics.[10] Fortunately, the pandemic has also expedited the development of new technologies and solutions for microfluidic biochips that can reduce the global diagnostic gap.[10] Millions of biochips for COVID-19 detection are used globally every day in hospitals, primary healthcare facilities, workplaces, and people's homes.[12] A recent World Health Organization (WHO) report estimated that more than 140 million test kits were shipped through the United Nations (UN) portal alone during the COVID-19 pandemic.[13]

Following the COVID-19 response, the benefits of these biochips have been viewed as an opportunity to stimulate diagnostic innovation for improving access to a broader range of tests in resource-limited settings. We draw attention to the following market projections: the molecular diagnostics market is projected to be worth 31.8 billion United States dollars (USD) by 2026, up from 17.8 billion USD in 2021, a 79% increase.[14] Further, the global microfluidics market is projected to be worth 58.8 billion USD, growing at a compound annual growth rate (CAGR) of 23.2%.[15] The biochip (lab-on-a-chip and microarrays) market is projected to register a CAGR of 13.9% during the forecast period of 2022–2027.[16] Moreover, the global POCT market is projected to be worth 72 billion USD by 2024 from 43.3 billion USD in 2022, with a CAGR of 10%.[17] Thus, there is a strong case for investment in the mass deployment of microfluidic biochips in health systems and communities across the globe.

As biochips are becoming increasingly popular, there are growing opportunities for commercialization and deployment, as evident from the sales, investment, and acquisitions reported by microfluidic companies.[3,18] With the growing likelihood of commercial adoption, there is a higher possibility that the biochips will be attacked by unscrupulous adversaries with malicious motivations for personal and illegal gains. To ensure economy of scale and cost reduction, biochip companies have been using outsourcing and horizontal supply-chain models for their goods and services, which involve untrusted third-party partners.[19–21] Due to third-party involvement, the associated material-level threat landscape increases considerably, posing the risk of malicious and intellectual property (IP)-theft attacks.[20–23] Attacks on microfluidic biochips have emerged as a critical rising threat. The severity of such attacks lies in the potential to harm patients, compromise healthcare, lose trust among health practitioners and clinicians, waste resources, and have negative economic consequences. This scenario calls for immediate attention and countermeasures to maintain the reliability, confidentiality, and trustworthiness of biochips.

The manufacturing and use of microfluidic biochips include component materials such as silicon, glass, polymers, reagents, and ancillary instruments such as sensors, pumps, and networked computers.[19] From the material point of view, an industry survey based on a sample of selected microfluidic companies showed that 59% of all commercially available devices are made of polymers (mainly thermoplastics).[12] Published data indicates that, in academic research laboratories, 55% of the fabricated devices are made of polydimethylsiloxane (PDMS), a transparent thermosetting polymer.[12] In contrast to other polymers, PDMS has the following attractive properties: excellent replicability from micro-molds, easy to pattern by soft lithography, flexibility (unbreakable compared to glass), optical transparency, affinity to permanently bond with glass *via* the plasma bonding technique, biocompatibility, gas permeability, and non-toxicity.[1,3,4,12,19,24–28] Thus, the microfluidics community has embraced PDMS to build microfluidic devices. Therefore, this work focuses on material-level attacks on PDMS-based microfluidic biochips.

The fabrication of PDMS-based microfluidic biochips includes replicating the liquid PDMS (mixed with the curing agent) from a master-mold after the mixture gets fully cured by heating. As PDMS fabrication involves liquid-to-solid conversion *via* thermal treatment, any deliberate tampering with PDMS while it is in a liquid state would show its deteriorating effect after curing, *i.e.*, in the solid state. This makes biochips vulnerable to material-level attacks that can compromise or fail the biochip altogether, leading to the repetition of experiments, which is undesirable due to high reagent costs and limited availability of samples.[8] Thus, the above vulnerabilities and associated repercussions can motivate attackers to cause material-level attacks. It is, therefore, essential to safeguard biochips against such attacks.

Microfluidic biochips can be mainly categorized into two types based on the underlying technologies used for their operation: digital microfluidic biochips (DMFBs) and flow-based microfluidic biochips (FMBs). DMFBs use discrete droplets on an electrode array leveraging the principle of electrowetting-on-dielectric, while FMBs manipulate fluid flow in microchannels using pumps and valves.[1,8,20,29] In this work, we specifically target PDMS-based FMBs due to the presence of PDMS microfluidic valves in such systems, unlike DMFBs that don't use microfluidic valves for their operation.[8]

Microfluidic valves are made out of thin PDMS membranes; these valves are crucial for controlling the fluid flow in a network of microchannels.[8,19,20,30] Microscale fluid flow can be automatically controlled by adjusting the pressure of the microvalves for fluidic operations such as mixing, incubating, filtering, and washing.[1,8,20,30] Microfluidic valves, along with recent advances in microfabrication techniques, have enabled large-scale integrated microfluidic circuitry that allows massively-parallel biochemical processing and immediate POCTs.[8,20] Thus, any attack on a microfluidic valve would greatly affect the FMBs' performance, leading to low quality and even faulty diagnostics.

In this work, we experimentally studied material-level vulnerabilities of PDMS-based FMBs, where an attacker can carry out the attack by adding reactive solvents or altering material parameters such as the PDMS curing ratio during fabrication. Through benchtop techniques, we demonstrated two scenarios of material-level attacks on FMBs. The first is a material adulteration attack, where the attacker (present in the fabrication unit) can add undesirable chemicals to the FMB's microvalves during manufacturing. The deliberately added chemicals preserve the original optical transparency of PDMS and, thus, are unlikely to be detected *via* microscopy-based quality control. However, during actual use by the end-user, the attacked valve would cause problems such as block, leak, and microvalve degradation,[8] leading to tampered results or denial of service.[1,3,8] The second attack involving material adulteration is a curing-ratio-based attack where an attacker (present in the fabrication unit) alters the ratio of the PDMS precursor–curing agent mixture, making the material viscoelastic-sticky.[31,32] This would induce problems such as microvalve sticking,[31,32] microvalve degradation,[8] and microchannel biofouling in the FMBs.[33,34]

Another scenario where material-based attacks can become prevalent is related to intellectual property (IP) theft using reverse engineering, which can provide an attacker with information about the FMB's materials and their associated use.[20,22] After having the information about the materials and their properties *via* reverse engineering, the attacker can intentionally alter the material property (through material adulteration) of the reverse-engineered FMB's material components to fail the FMB and defame the legitimate FMB manufacturer.

Furthermore, reverse engineering attacks involve stealing the biochip architectural layout, material information, component-level netlist, and information about the bio-protocol without incurring development costs.[20,22] Using the stolen information, adversaries can then carry out piracy of IP and test protocols, counterfeiting, and overbuilding of biochips for illegal monetary gain.

To circumvent such material-level attacks, we present countermeasures in the form of watermarking and machine-learning (ML)-based schemes. We categorize the attacks into two categories: (1) IP-theft attacks, which include reverse-engineering, counterfeiting, piracy, and overbuilding attacks, and (2) malicious material-level attacks.

For IP-theft attacks, we present the first material-level watermarking scheme for FMBs. The scheme utilizes a perylene-labeled fluorescent dye,[35–41] synthesized in our laboratory, to embed spectral watermarks in the microvalves of FMBs. The proposed scheme incorporates the addition of a perylene-labeled fluorescent dye at certain microvalve locations, which are undetectable within the visible range (wavelength of 400–700 nm). The locations themselves act as a watermark, which can only be detected and quantified using the intensity–wavelength response recorded by a relevant spectrometer or confocal microscope with an excited wavelength of 405 nm.

Moreover, the watermark can show a dynamic shift in the excimer peaks under mechanical strain, like the one found in an actuated PDMS microvalve giving the watermarking scheme two-factor authentication capabilities. Using the watermarks, the pirated or counterfeited FMBs could be identified and discarded by the end-user or the FMB company that received the fabricated FMB from a third-party manufacturer. We experimentally verified this countermeasure using laboratory-made PDMS valves ranging in size from the macro to micro-level and provided a calibration curve to design the watermarks.

We provide a security analysis for the material-level attacks based on randomized checkpointing and full independent Bernoulli trial-based checking schemes, which FMB manufacturers can use for their quality control to safeguard the manufactured FMBs. With respect to the watermarking scheme, we present a Boolean quantity called quality assessment using the involved parameters and sensor values, which a watermark designer or verifier can use to design or verify the watermarks.

As a countermeasure against curing ratio attacks, we present a novel machine-learning (ML) method that can detect maliciously altered curing ratios with an accuracy of 99%. This countermeasure is based on a mechanical punch test[42] that locally deforms the material to provide force-displacement data, which we use to train our ML models.

We explored three ML models (random forest, Naive Bayes, and decision tree) and three feature selection methods (Pearson correlation, recursive feature elimination, and backward elimination) for curing ratio anomaly detection. We trained our ML models by splitting the data into the training set (70%) and the test set (30%). The models were trained on the complete dataset (9056 data points), which was derived from feature selection methods such as the filter method (Pearson correlation) and wrapper methods (recursive feature elimination and backward elimination).[43,44] All of our ML models achieved more than 99% accuracy in detecting the curing ratio anomalies. The following section presents the adversarial model and related prior studies before we discuss our results.

Adversarial model

The manufacturing of an FMB involves many steps and requires multiple third-party entities, some of which might be untrusted. Adversaries may hire attackers to jeopardize FMBs from a competitor FMB firm out of malicious motivation.[42] The attacker can introduce material-level variation in the FMBs' embedded components to produce incorrect or cause a denial of service. The aim of such an attacker is to jeopardize trust in the healthcare industry, create false or misleading test results to degrade the integrity of related diagnostics research, and make health practitioners lose trust in and discontinue using biochips. The adversaries' economic interests will then be satisfied as the customers would switch to other biochip companies in the marketplace. With the advent of manufacturing-as-a-service,[45] FMBs have become more vulnerable to material-level attacks.[20,45]

Fig. 1 illustrates the adversarial model and highlights the vulnerable points corresponding to a material-level attack.[20,45–47] The model has five parties: the customer, the FMB company, the designer, the manufacturer, and the quality control unit. The process flow of a typical FMB service is shown in Fig. 1. A typical service starts with a customer submitting a request for an FMB (route 1). After the service request is generated, it is sent to the design unit (route 2). The design unit sends the design files to the manufacturing unit (either in-house or outsourced, route 3). An attacker in the manufacturing unit alters the material properties of the FMB's PDMS either by adding harmful chemicals or changing the curing ratio to perform the material-level attack. The attacked biochip reaches the quality control team (route 4) and evades fault detection owing to the stealthy nature of the attack. Finally, the attacked FMB is delivered to the customer (route 5).

Biochip manufacturing units within the process can be classified as either in-house or outsourced.[20,23,47] In-house manufacturing units refer to internal facilities within an organization that handle the production and manufacturing of goods or components, providing greater control and flexibility over the manufacturing process.[1,20] On the other hand, outsourced manufacturing units refer to external facilities or suppliers that are contracted by organizations to produce goods or components on their behalf, allowing for cost savings, access to specialized expertise, and scalability.[23,47]

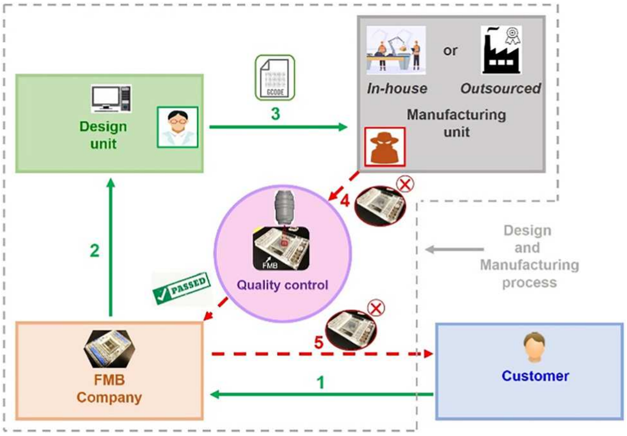


Fig. 1 Adversarial model for a material-level attack. A customer places an FMB order received by the FMB company (route 1). The FMB company sends the order to the design unit (route 2). The design team sends the design files to the manufacturing unit (either in-house or outsourced, route 3). However, an attacker in the manufacturing unit carries out the material-level attack. The attacked biochip reaches the quality control unit (route 4) and escapes detection. Finally, the compromised biochip is delivered to the customer (route 5).

Biochip companies often favor outsourced manufacturing units over in-house manufacturing units for several reasons: outsourcing provides companies with the opportunity to leverage cost savings, tap into specialized expertise offered by external facilities or suppliers, and achieve scalability. In contrast, in-house manufacturing offers greater control and flexibility but may come with higher costs and resource requirements.[48–53]

Regardless of the manufacturing approach chosen, it is important to acknowledge the potential presence of attackers in the manufacturing unit who may engage in material-level attacks. Both external attackers hired by adversaries and insiders with malicious intentions can compromise the security of the biochip production process. When comparing the threat landscape in outsourced and in-house units, attacks in the outsourced setting may be easier to execute due to the higher level of trust involved. However, in-house attackers can exploit this trust and perform attacks, assuming that the compromised products will pass light quality control trials.

To mitigate these risks, it is crucial to implement stringent and state-of-the-art quality control trial techniques. These techniques should be versatile enough to detect attacked biochips in both the outsourced and in-house manufacturing scenarios, ensuring the integrity and reliability of the biochip products.

Related prior work

Previous studies investigating the cyber-physical security of FMBs have encompassed various aspects of attacks and defenses such as hardware-level secure-by-design and vulnerability analysis[1,8,19,20,54] as well as associated security metrics and trade-offs.[3,21,22,55,56]

Specifically, Tang *et al.* presented a high-level overview of attacks and defenses concerning FMBs.[19] To test FMBs, Hu *et al.* presented a method for automated testing of FMBs based on a behavioral abstraction of physical defects in microchannels and microfluidic valves.[8] They modeled flow and control paths in the FMB as a logic circuit composed of Boolean gates, which were mapped to fluidic operations involving pumps and pressure meters in the FMB. They compared feedback from pressure meters with expected responses based on their logic circuit model to identify the defects.

Recent work by Baban *et al.* reported structure-level attacks and defenses for FMBs that explored malicious structural modification of FMB micro-reaction chambers to produce false-negative coronavirus disease of 2019 (COVID-19) results.[20] They adopted deep learning (DL)-based anomaly detection algorithms to circumvent such attacks. Their DL-based countermeasure recorded a 96% validation accuracy in recognizing such deliberately induced microstructural anomalies.

Furthermore, Baban *et al.* presented a novel structure-level watermarking scheme for FMBs by increasing the height of the micro reaction chambers or microchannels at specific locations to obtain fluorescent watermarks that can be detected and quantified using fluorescence microscopy.[20] However, no material-level watermarking schemes have been proposed for FMBs where the watermark is embedded inherently in the material of the FMB.

Le *et al.* introduced a smartphone-based sample-level watermarking solution for impedance flow cytometry based POCTs, offering cytocoded authentication services.[57,58] Each authentication password consists of a specific count of synthetic micro-beads with distinct dielectric characteristics. These beads, combined with the blood sample, are used to authenticate the user to the cloud server based on statistical analysis and bead characteristics. Additionally, they introduced a barcoding scheme at the sample level to generate a unique authentication string.[59] This string is based on the sizes of synthetic micro-beads, which serve as identifiers for individual test results on the remote storage device.

Chen *et al.* proposed a systematic framework for inserting and detecting hardware Trojans in FMBs.[60] Shayan *et al.* presented a microfluidic valve-based Trojan design based on a thicker microvalve membrane that would require more pressure than usual to function, leading to anomalous valve response.[23] Such a valve response can be used to launch attacks such as contamination, denial of service, and parameter tampering causing FMBs to malfunction.

Material-level Trojan attacks have been proposed for 3D printed objects, which can result in catastrophic operational failures. Le *et al.* introduced a class of Trojan stealthy attacks called physical logic bombs on 3D printed objects.[61] These embedded logic bombs utilize smart materials, residual stress, and shape memory effects to modify the structural design of the printed product, leading to potential catastrophic failures. To counter these attacks, they proposed mitigation strategies that involve the use of dielectric sensing and computed tomography (CT) techniques for real-time and post-production monitoring of the printing processes. They achieved an average accuracy of 94.6% in identifying these attacks within a single printing layer.

IP-theft attacks have also received attention; Chen *et al.* demonstrated a layout-level reverse-engineering attack using image analysis.[22] To thwart reverse-engineering of the bio-protocol, recent work by Shayan *et al.* presented a design obfuscation scheme by carefully inserting dummy valves in the FMB.[1,30]

With respect to watermarking solutions for FMBs, a previous study demonstrated a watermarking technique by hierarchically embedding secret signatures using the mixing ratio, incubation time, and sensor calibration to protect the bio-protocols (bio-protocol level watermarking) in DMFBs.[29] The same bio-protocol level watermarking scheme can be used for FMBs.

In regard to watermarking solutions for 3D-printed objects, Bayens *et al.* investigated a material-level side-channel approach as the verification scheme. They embedded micromarkers within the 3D-printed objects during manufacturing, using gold nanorods (GNRs) and 3,3′-diethylthiatricarbocyanine iodide (DTTCI). To authenticate the embedded micromarkers on a material basis, they utilized surface-enhanced Raman spectroscopy (SERS).[46]

In order to prevent the sale of compromised biochips, ML-based anomaly detection has been used to mitigate structure-level attacks on FMBs.[20] In previous studies, we have seen that different anomaly/outlier detection techniques[62–65] have been used to separate anomalous data instances that deviate quantifiably from truth values. Recently, we have seen an increase in the usage of ML-based techniques for anomaly detection. For example, fuzzy logic,[66] Bayesian approach,[67,68] genetic algorithm,[69,70] neural network,[71,72] and traditional ML[73,74] methods have proved to provide prominent results for anomaly detection. To date, there has been no utilization of machine learning techniques incorporating material characterization data for securing FMBs against material-level attacks.

In summary, no material-level attacks and defenses have thus far been explored for FMBs. In this work, we focus on providing cyber-physical security solutions against malicious material-level and IP-theft attacks.

Methods

Reverse engineering analysis on a commercial FMB

A reverse engineering analysis was conducted on a commercial FMB using the nanoindentation technique, as well as bright-field and scanning electron microscopy. The purpose of this analysis was to infer information about the Young's modulus of the PDMS material and gain insights into the structural characteristics of the microreaction chambers, microfluidic lines, and valves. The FMB was cut both longitudinally (L, along the major length) and transversely (T, perpendicular to the major length) to obtain a cut chip portion. The cut portion was then subjected to nanoindentation characterization to determine the Young's modulus of the PDMS material used in the commercial FMB (Text S1†). Additionally, bright-field and scanning electron microscopy techniques were employed to examine the structural layout of the cut chip portion.

Attack characterization

With regard to material degradation attack using reactive chemicals, we conducted a comparison of three cases to characterize material-level attacks: PDMS control, PDMS + *t*-butyl alcohol, and PDMS + hexadecane. Hexadecane and *t*-butyl alcohol were specifically chosen as reactive chemicals due to their capability to slow down the formation of PDMS crosslinking networks, leading to degradation of material properties, while preserving the optical transparency of the original PDMS.[75–77] We employed an Instron® universal testing machine to subject both the control and doped samples to uniaxial deformation in order to assess the degree of material degradation. The ASTM D412 C standard dog-bone shaped (33 mm long × 6 mm wide × 1 mm thick) samples were subjected to uniaxial deformation at a displacement rate of 5 mm s^{-1}, and the resulting force values were recorded using a 50 N load cell for post analysis.

Adhesion peel tests are effective in characterizing the adhesive behavior of PDMS and providing information about the PDMS curing ratio.[78] We conducted adhesion peel tests for curing ratios ranging from 10 : 1 to 50 : 1 to assess the susceptibility to curing ratio attacks. We utilized a 50 μm thick plain PDMS film (top layer) bonded to a glass coverslip (170 μm thick, 24 mm long, and 24 mm wide) through plasma bonding. The composite glass coverslip was then pressure-sensitively bonded to a 3 mm thick PDMS layer (bottom layer) with varying curing ratios. The peeling test was performed using an Instron® universal testing machine with a 50 N load cell, where the glass coverslip was peeled from the hanging end (5 mm overhang) at a displacement rate of 5 μm s^{-1} under controlled displacement conditions.

Uniaxial spectral analysis

To spectrally analyze the ASTM D412 C dog bone-shaped samples during uniaxial deformation, we utilized 0.3 wt% of perylene silane to dope with PDMS, which provided the most favorable mechanoresponsive outcomes compared to other weight percentage samples due to the dye's concentration-based chemical compatibility with PDMS.[37–39] The doped samples were subjected to uniaxial deformation at a displacement rate of 0.1 mm s^{-1}, and the resulting force values were recorded using a 50 N load cell. The intensity–wavelength response for various strains was recorded using a spectrometer with a laser excitation wavelength of 405 nm.[37]

Biaxial spectral analysis

Circular PDMS microvalves ranging from 4 mm to 350 μm were fabricated and dyed with 0.3 wt% perylene silane to measure the excimer intensity change during biaxial deformation. The valves were subjected to a known suction pressure of 1000 mbar for actuation, and their response was analyzed using spectral scans conducted with a confocal microscope. A laser beam with a wavelength of 405 nm was directed from the bottom of the microscope stage through a dry 20× objective lens with a numerical aperture (NA) of 0.75. Finite element method (FEM) models were employed to estimate the maximum principal strains of the deformed valves, considering the correlation between the response of the dye and uniaxial tensile strain. The maximum principal strain, which provides an accurate measure of the extent of maximum tensile deformation under a biaxial stress state,[78] was selected as the key parameter of interest. Experimental data points, derived from both FEM models and confocal spectral scanning, were utilized to construct a linear regression model that correlates excimer intensity change with the maximum principal strain.

Results

Material-level attacks on FMBs

Fig. 2 shows the attack demonstration results obtained experimentally on PDMS. Fig. 2A shows a commercial FMB that uses PDMS for its structural components. Fig. 2B shows the top-view bright-field microscopy image of the FMB locating the repeating unit of the integrated fluidic circuit (IFC)[20] with the microvalves. The IFC's repeating unit consists of a reaction chamber connected by sample and reagent lines, which are mediated by a microfluidic valve pneumatically controlled by a control line.[20] Fig. 2C shows the cross-sectional (T) view obtained by scanning electron microscopy (SEM), which reveals structural information about the reaction chamber, reagent line channel, and microvalve junction. The microvalve junction consists of flow and control channels separated by a microvalve membrane. The membrane can block the fluid flow when pneumatically actuated.

Fig. 2D shows stress–strain plots, illustrating the degraded material properties of PDMS + *t*-butyl alcohol and PDMS + hexadecane compared to PDMS-only controls. Quantitatively, the PDMS + *t*-butyl alcohol samples failed at significantly low strain values: 60% and 67% low strain values compared to the PDMS-only controls. Fig. 2E shows a significant 82% reduction in strain energy per unit volume for PDMS + *t*-butyl alcohol samples. For PDMS + hexadecane samples, a significant 86% reduction in strain energy per unit volume (signifying fracture toughness) was recorded compared to PDMS-only controls. Furthermore, Fig. 2F shows a significant 67% and 64% reduction in peak stress (signifying fracture strength) for PDMS + *t*-butyl alcohol and PDMS + hexadecane samples, respectively, compared to PDMS-only controls. Hence, the results highlight a substantial degradation in PDMS samples' fracture and toughness properties when doped with hexadecane and *t*-butyl alcohol.

To demonstrate the material adulteration attack at the valve-level, we made a hexadecane-doped PDMS circular macrovalve (4 mm diameter) and compared its response under 1000 mbar pressure with the pure PDMS counterpart using a digital image correlation (DIC) setup (Text S2†). As a result, the doped PDMS membrane ruptured while the pure PDMS membrane remained intact under the same 1000 mbar pressure, corroborating the results obtained in Fig. 2D–F.

The observed results in material degradation attacks can be explained as follows. When hexadecane and *t*-butyl alcohol are added to the PDMS, they act as solvents for the PDMS oligomers. The solubility parameter of hexadecane and *t*-butyl alcohol are 8.0 $cal^{1/2}$ $cm^{-3/2}$ and 10.6 $cal^{1/2}$ $cm^{-3/2}$, respectively.[76,77] The values are close to the solubility parameter of PDMS (7.3 $cal^{1/2}$ $cm^{-3/2}$), meaning hexadecane

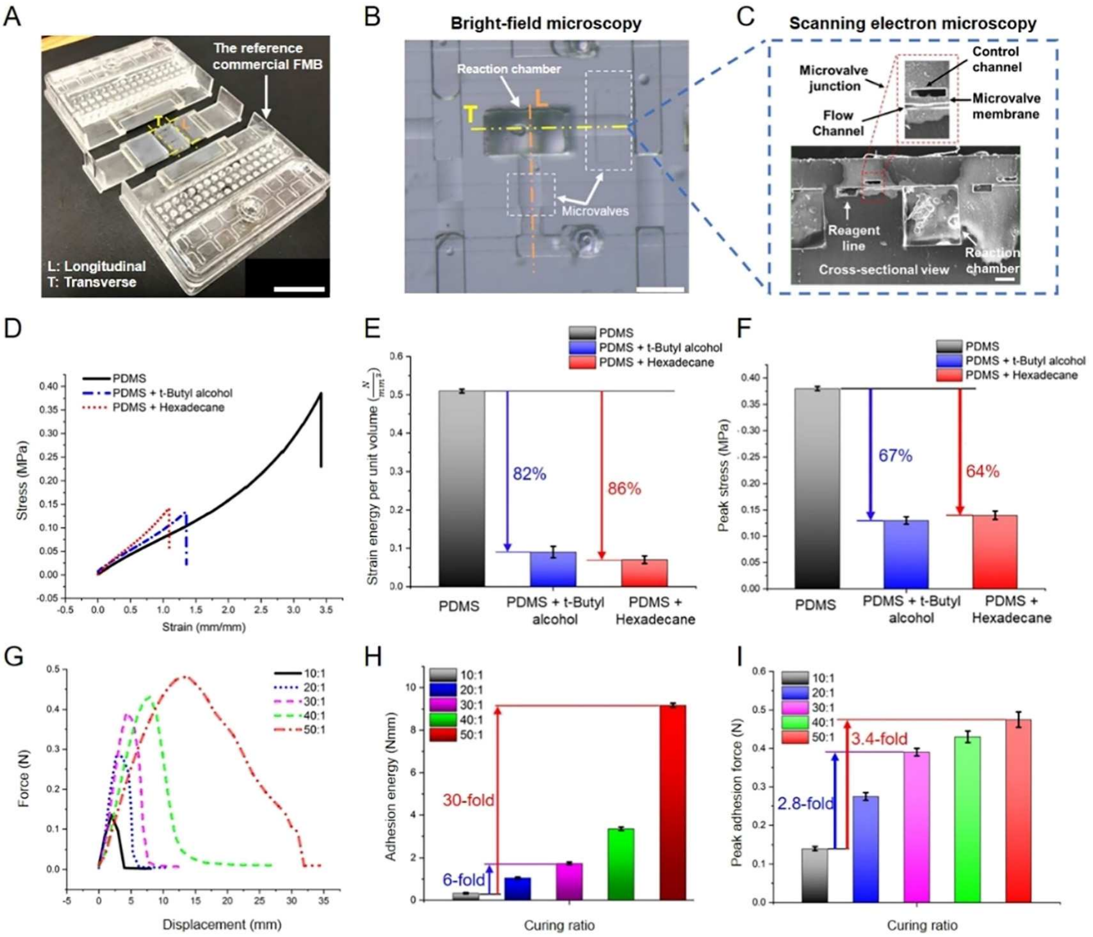


Fig. 2 Material-level attack demonstration. A) A longitudinally (L) and transversely (T) cut PDMS-based commercial FMB. The scale bar is 3 cm. B) The top view shows microvalves and the L and T cuts given for the scanning electron microscopy (SEM) image of the related cross-sectional view. The scale bar is 125 μm. C) The SEM cross-sectional view (T) shows the microvalve junction containing the flow and control channels separated by the microvalve membrane. The scale bar is 100 μm. D) The stress–strain responses recorded from uniaxial tensile tests (ASTM D412 C) of PDMS samples (1 mm thick) show significant material property degradation. E) Strain energy per unit volume comparison recorded significantly reduced energies for PDMS + *t*-butyl alcohol (82% reduction) and PDMS + hexadecane (86% reduction). F) Peak stress comparison recorded a significantly reduced stress for PDMS + *t*-butyl alcohol (67% reduction) and PDMS + hexadecane (86% reduction). G) Force-displacement responses for curing ratios ranging from 10 : 1 to 50 : 1. H) Adhesion energy comparisons show a 6-fold increase and 30-fold increase in the energy for the 30 : 1 and 50 : 1 curing ratios, respectively, compared to the 10 : 1 curing ratio. I) Peak adhesion force comparisons show a 2.8-fold increase and 3.4-fold increase in the force for the 30 : 1 and 50 : 1 curing ratios, respectively, compared to the 10 : 1 curing ratio. The number of samples (*n*) was equal to 5, and the error bar represents the standard deviation (sd) for the results presented in Fig. 2D–I.

and *t*-butyl alcohol are good compatible solvents for PDMS. This can lead to a dilution of the PDMS oligomer concentration, reducing the degree of cross-linking and causing the loosened polymeric network, which can decrease the toughness of the PDMS. In addition, hexadecane and *t*-butyl alcohol-doped PDMS are transparent, so the composition change of chemical levels driven by the stealthy attack is hardly detectable. However, such an invisible inhomogeneity can lead to the formation of voids or defects within the polymer network, which can further contribute to the decrease in toughness and fracture.[75]

Regarding the curing ratio attack, Fig. 2G displays the results of the peel test conducted using a mechanical peel test setup on PDMS layers with varying curing ratios.[78] The results record a significant improvement in the adhesion energies for the samples whose curing ratio was more than 10 : 1. Fig. 2H shows the adhesion energies of curing ratios 20 : 1 to 50 : 1 compared to the 10 : 1 ratio. A significant 6-fold increase in the adhesion energy was recorded for 30 : 1 compared to the 10 : 1 curing ratio. Notably, a 30-fold increase in adhesion was recorded for 50 : 1 compared to the 10 : 1 curing ratio.

Similarly, Fig. 2I shows the peak adhesion force of curing ratios 20 : 1 to 50 : 1 compared to the 10 : 1 ratio. A significant 2.8-fold increase in the peak adhesion force was recorded for 30 : 1 compared to the 10 : 1 curing ratio, and a 3.4-fold increase in the peak adhesion force was recorded for 50 : 1 compared to the 10 : 1 curing ratio. Thus, the peel test results highlighted the significantly increased adhesion strength and toughness for the higher curing ratio PDMS samples compared to the standard 10 : 1 ratio sample. An attacker can leverage curing ratio-guided adhesion response to carry out attacks such as microvalve sticking,[31,32] microvalve degradation,[8] and microchannel biofouling[33,34] in FMBs.

Moreover, by using a higher curing ratio compared to the standard 10 : 1 curing ratio, adversaries can reduce manufacturing costs, especially for those involved in counterfeiting, overbuilding, and piracy. For example, suppose an attacker (hired by the adversary organization) chooses a 20 : 1 curing ratio instead of the standard 10 : 1 curing ratio. In that case, they need to add 50% less curing agent than the original. Thus, 50% less material will be used for the fabrication, helping the adversary to save 50% in terms of manufacturing cost. However, altering curing ratios to save manufacturing costs would inadvertently affect the FMB's performance owing to problems associated with curing ratio attacks. Thus, checking and ensuring the correct curing ratio of the manufactured FMBs before sending them to end-users is essential.

Material-based attacks are likely to be more prevalent in IP-theft-scenarios on FMBs; thus, it is necessary to watermark FMBs at the material level to validate the authentic provenance of materials used in fabrication. Therefore, we present below the first material-level spectral watermarking scheme to secure FMBs against IP-theft-based attacks.

Material-level watermarking for FMBs

We developed a dynamic spectral material-level countermeasure to protect FMBs against IP-theft-based attacks. The countermeasure involves dynamic material-level watermarking for PDMS-based FMBs (with microvalves) using a perylene-labeled fluorescent dye. We synthesized the fluorescent dye in our laboratory, which we added into PDMS to make it a mechanoresponsive material.[38,40] Fig. 3A shows the characterization results obtained from uniaxially deforming the PDMS–perylene silane (0.3 weight percentage, wt%) samples as per ASTM D412 C[78] standard. The deformed samples recorded substantial shifts in the monomer, and excimer peaks, seen in the intensity–wavelength curves. The results regarding the uniform distribution of the dye in PDMS, replicability of excimer intensity peaks, and the effect of the concentration of the dye on the excimer intensity peaks can be found in Text S3.†

The results in Fig. 3A show a distinct downward shift in the excimer intensity with progressing strain. Comparatively,

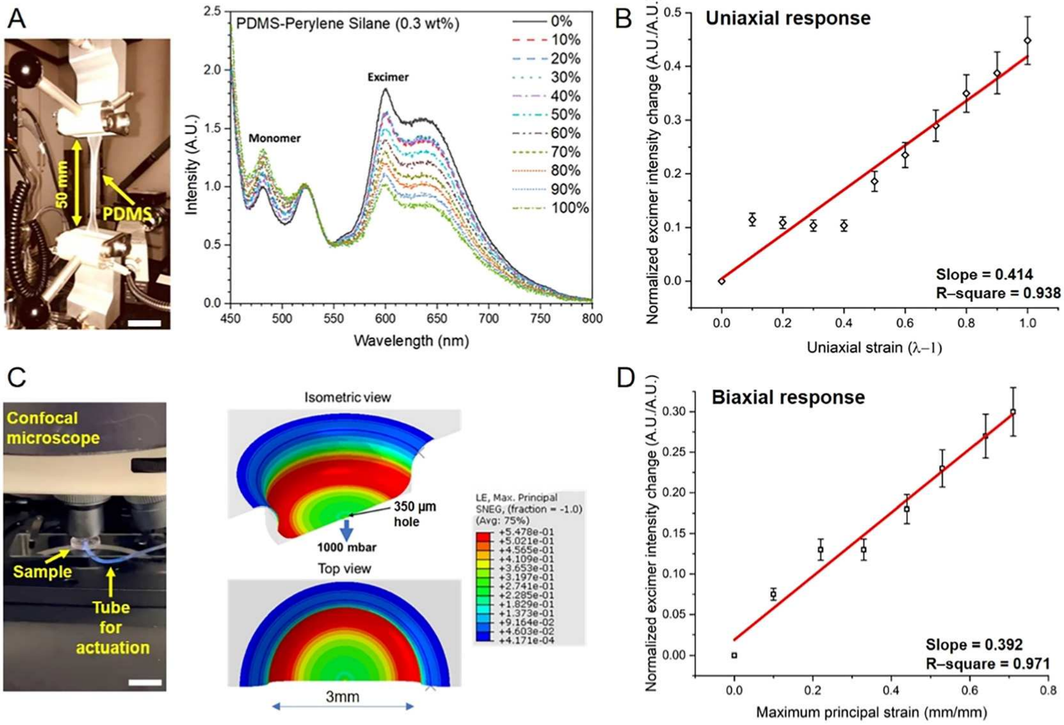


Fig. 3 Spectrometric countermeasure against IP-theft-based attacks. A) ASTM D412 C tensile test setup to characterize the intensity–wavelength response of PDMS–perylene silane (0.3 wt%) samples. The scale bar is 10 mm. The intensity–wavelength relationship of PDMS–perylene silane (0.3 weight percentage, wt%) shows a shift in monomer and excimer intensity peaks for uniaxial strains. B) Uniaxial response: normalized excimer intensity changes in good correlation with uniaxial strains. The linear regression fit records the slope as 0.414 and the *R*-squared value as 0.938. The *n* was equal to 5, and the error bar represents the standard deviation. C) Confocal microscopy setup showing the circular valve samples and the tube for pneumatic actuation. The scale bar is 8 mm. The finite element modeling (FEM) results from a 3 mm circular PDMS valve actuated under 1000 mbar pressure *via* a 350 μm hole to obtain maximum principal strain contour plots. D) Biaxial response: normalized excimer intensity changes in good correlation with maximum principal strains. The linear regression fit records the slope as 0.392 and the *R*-squared fit as 0.971. The *n* was equal to 5, and the error bar represents the standard deviation.

the monomer peak shows a slight upward shift with progressing strain. Due to the large shifts recorded for the excimer intensity with mechanical strains, we chose the excimer shifts only to be our watermark basis ensuring effective strain sensing. Fig. 3B shows a linear regression model between normalized (with respect to 0% strain intensity) excimer intensity change and uniaxial strain, $\lambda - 1$, where λ is the extension ratio (final sample's length/original sample's length). The model shows a good correlation between the parameters with the *R*-squared value of 0.938. The slope of the uniaxial regression model was recorded to be 0.414. The strain state in the ASTM D412 C samples was uniaxial; however, there exists a biaxial strain state when a microvalve is actuated due to the biaxial deformation of the associated microvalve membrane. Therefore, we made circular PDMS microvalves ranging from 4 mm to 350 μm to obtain excimer intensity change readings corresponding to associated biaxial deformations. The readings of the dyed valves were obtained *via* spectral scans done using a confocal microscope, as seen in Fig. 3C.

Furthermore, we developed finite element method (FEM) models to estimate the maximum principal strains of the deformed valves (Text S4†). Out of different strains that could have been used to estimate the valve's biaxial strain, we chose the maximum principal strain to take into account the obtained dye's response that showed a good correlation with uniaxial tensile strain, as seen in Fig. 3B.[26–78] The experimental data points were plotted using maximum principal strains (obtained from the FEM models) and normalized excimer peaks' intensity change (obtained from the confocal spectral scanning) to obtain a linear regression model, seen in Fig. 3D. The model shows a good correlation between the parameters with the *R*-squared value of 0.971. The slope of the biaxial regression model was recorded to be 0.392, which is also in close agreement with the slope of the uniaxial regression model, *i.e.*, 0.414. As strains are dimensionless parameters, therefore, even though the valves were circular in geometry, the linear model can be used to predict and design microvalves with rectangular geometry, as seen in the commercial FMB. Hence, Fig. 3D can be used as

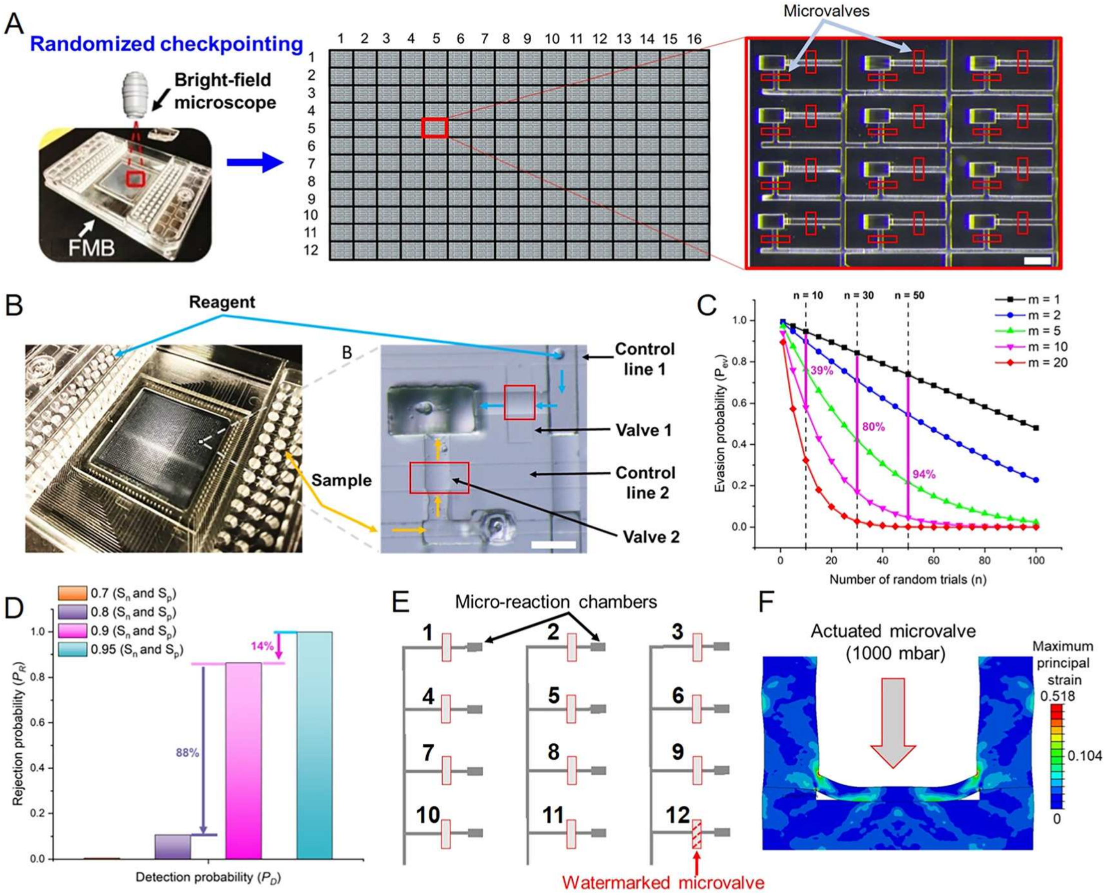


Fig. 4 Security and performance metrics for material-level attacks and watermarking scheme. A) Randomized checkpointing scheme using a bright-field microscope. The view shows 12 reaction chambers of our lab-made FMB replicated using the dimensions of the reference commercial FMB. The scale bar is 250 μm. B) A bright-field microscopy view showing sample and reagent lines along with the control lines needed to actuate two microvalves. The scale bar is 125 μm. C) Security metric results for the randomized checkpointing scheme. D) The rejection *versus* detection probability results for different sensitivity and specificity of the detecting microscopes. E) A schematic showing 12 microvalves, out of which 1 is watermarked. F) FEM simulation of the reference FMB's microvalve actuation with the maximum principal strain contour plot.

a calibration curve to design the mechanoresponsive behavior of the dyed-watermarked microvalves under pneumatic actuation.

Security analysis for the attack and the watermarking scheme

For PDMS-based FMBs, microvalves are the most critical components attackers can target (at the material level) because the associated ultra-thin membrane mechanically deforms under pneumatic actuation. Further, attackers can design their attacks targeted at microvalves as per the quality control checking scheme opted by the FMB company. For example, in resource-constrained settings, randomized checkpointing strategies are beneficial.[79,80] Here, the checking is done randomly to detect faults in the fabricated FMBs.[20]

Fig. 4A shows the randomized checkpointing scheme where a bright-field microscope is used to detect any visible anomalies or defects on an FMB. The commercial FMB, chosen as a reference for this work, had 2304 micro-reaction chambers. Using a suitable zoom, we could optimally fit 12 micro-reaction chambers with associated microfluidic lines and microvalves. With this view, the FMB's micro-components can be seen clearly to detect any visible anomalies or defects. Thus, keeping in view 2304 micro-reaction chambers and 12 (4 rows and 3 columns) micro-reaction chambers in the microscopy trial, we divided the top view of the whole FMB into 12 rows and 16 columns. This led to 192 (12 rows × 16 columns) microscopy trials needed to scan the whole FMB, where each trial can accommodate 12 micro-reaction chambers with the associated 24 microvalves (schematically shown), seen in Fig. 4A. Each reaction chamber is connected to two microfluidic valves, as shown in Fig. 4B. We assume that if at least 1 out of 192 microscopy trials shows anomalies with the microvalves, then that FMB would be discarded during the quality control trial.

We developed a security metric for the randomized checkpointing scheme, as shown in eqn (1). Note that M is the total number of microscopy views (each showing 24 microvalves to be checked) to scan the whole FMB, and m is the number of abnormal views where attacked microvalves are spotted. Note that n is the number of random trials to detect abnormal views, and P_{ev} is the evasion probability during the quality control trial with a bright-field microscope.

We assume that the quality control checker utilizes a known method to detect abnormal microvalves *via* a bright-field microscope, such as spotting inconsistencies with the microvalve's shape, optical texture, membrane warpage, *etc.* Further, we assume that the microscope is 100% sensitive and specific in detecting abnormal microvalves. Notably, the detection method using bright-field microscopy is effective even with a microscope that is less than 100% sensitive or specific. However, the detection probability gets significantly decreased with microscopes that have sensitivity or specificity less than 90%.[20]

An attacker aims to increase m as much as possible to make the attack lethal. However, increasing m decreases P_{ev}. To quantify this, we present a security analysis by plotting P_{ev} *vs.* n for different m. Fig. 4C shows the results of the randomized checkpointing security analysis. For $m = 1$, P_{ev} decreases linearly as n increases. For $m > 1$, the response showed an exponential decrease in P_{ev} with the increase in n. A 39% decrease in P_{ev} was recorded when $m = 10$ compared to $m = 1$ for $n = 10$. For $n = 30$ and $m = 10$, P_{ev} reduced to 80%, and for $n = 50$ and $m = 10$, it reduced to 94%. Thus, we found that there is a trade-off in the randomized checkpointing scheme, wherein an attacker has to optimally choose m based on n to maximize P_{ev}. The information about n is based on the quality control team's checking regime, which an attacker would like to know to determine on m while maximizing P_{ev}. Thus, it is essential to keep knowledge about n hidden from potential attackers.

$$P_{\text{ev}} = \left(1-\frac{m}{M}\right)\left(1-\frac{m}{M-1}\right)\left(1-\frac{m}{M-2}\right)\ldots\ \ldots\left(1-\frac{m}{M-(n-1)}\right) \tag{1}$$

Next, we evaluate the effect of sensitivity (S_{n}) and specificity (S_{p}) of the detecting instruments in detecting defects during quality control inspections. We define S_{n} to be the conditional probability of detecting the attacked microvalves when the valves are actually attacked. Further, we define S_{p} to be the conditional probability of not detecting the attacked microvalves when the valves are not attacked. In other words, S_{n} is the true positive rate and S_{p} is the true negative rate for detection.

In contrast to the randomized checkpointing scheme, we assume that the quality control checker does not opt for a randomized checkpointing scheme but scans the whole FMB by doing 192 trials and optically checking 24 microvalves in each trial. Here, we focus our attention on a particular microscopy trial showing 24 microvalves (Fig. 4A). Thus, the checker has to check 24 times to cover all the 24 microvalves leading to 24 trials for a particular microscopy view.

$$P_{\text{D}} = (S_{\text{n}})^{a}\cdot(S_{\text{p}})^{24-a} \tag{2}$$

To devise a security metric for the above case, we used independent Bernoulli trials[20] to determine the detection probability (P_{D}) of the faulty or compromised microvalves as a function of S_{n} and S_{p}. We consider a view showing 24 microvalves, out of which a microvalves are attacked. Eqn (2) gives the relationship dependence of P_{D} on S_{n}, S_{p}, and a.[20]

For $a = 1$, the probability of rejecting the FMB (P_{R}) under an event of detecting at least one attacked microvalve is given by eqn (3) and (4), where k denotes the number of anomaly detection events out of 24 trials.[20] A fabricated FMB is rejected if at least one of the checking trials identifies an attacked microvalve. Assuming that the checker knows the anomaly detection scheme to detect attacked microvalves, P_R for at least one out of 24 trials is given by eqn (5).

$$P_R = P(k \geq 1) = 1 - P(k = 0) \tag{3}$$

$$P(k = 0) = C(24, 0)(P_D)^0(1 - P_D)^{24-0} \tag{4}$$

$$P_R = 1 - (1 - P_D)^{24} \tag{5}$$

Fig. 4D shows P_R for different values of P_D, which is guided by the S_n and S_p values of the detecting microscopes. We recorded a 14% decrease in P_R for S_n and S_p both equal to 0.9 compared with $S_n = S_p = 0.95$. For $S_n = S_p = 0.8$, we recorded a significant (88%) decrease in P_R compared to the case of $S_n = S_p = 0.9$. Thus, in the scenario of a full checking scheme as opposed to a randomized checkpointing scheme, attackers can exploit the limitations associated with the detecting instruments' sensitivity and specificity to carry out their attacks while successfully evading quality control trials.[20]

Next, we present a security analysis for the material-level watermarking scheme. Fig. 4E shows a schematic consisting of 12 microvalves associated with 12 micro-reaction chambers. Out of the 12 microvalves, only one microvalve is watermarked. Our material-level watermarking scheme consists of a two-step parameter authentication process. The first step includes recognizing the correct location of embedded watermarked microvalves *via* fluorescence spectroscopy methods. The second step comprises validating the shift in the excimer peak under microvalve actuation as designed by the FMB company.

Let p^i and c^i be the *i*th parameter value and *i*th parameter resolution, respectively, for designing the watermark. Let $p^i \in [\nu^i_{\min}, \nu^i_{\max}]$ be the acceptable range determined by $\nu^i_{\min}$ and $\nu^i_{\max}$, which are the minimum and maximum acceptable values of p^i, respectively. Therefore, the number of possible discrete values (N^i_{val}) that p^i can take is given by eqn (6).[29]

$$N^i_{\text{val}} = \frac{\nu^i_{\min} - \nu^i_{\max}}{c^i} \tag{6}$$

We consider the locations of the watermarks to be our first parameter, which the end-users are aware of, but this information is not available to attackers. Therefore, p^1 belongs to the chosen watermark locations on the microvalves. To identify locations on the FMB, we map the coordinates of the microvalve locations to integers starting from 1, as shown in Fig. 4E. The microvalve locations are mapped starting from 1 to 12, with the 12th location corresponding to the watermarked microvalve. Let L be the set of all microvalve locations that could be used for embedding watermarks and l be the subset of L denoting the set of chosen watermark locations.

Considering the case presented in Fig. 4E, only one microvalve has been chosen for the watermark. We have $\nu^1_{\min} = |l|$ where $|l|$ (cardinality of set l) is equal to 1, *i.e.*, $\nu^1_{\min} = |l| = 1$. Similarly, $\nu^1_{\max} = |L| = 12$ (maximum possible locations), and c^1 (location resolution) is equal to 1. After applying eqn (6), we get $N^1_{\text{val}} = 11$, implying that p^1 can take 11 possible discrete real values for the location-wise design of the watermarks. However, in the reference FMB shown in this paper, there are 4608 microvalves making $N^1_{\text{val}} = 4607$. This greatly enhances watermark location options to include randomness in the watermarking design (either individual FMB-wise or lot-wise), where the designer has many location options to embed watermarks—ensuring better security against the identification of the embedded watermarks by attackers.

Next, for the second step of our watermarking design, we use the decrease in the excimer intensity under microvalve actuation to be the value of p^2. As per the results shown in Fig. 3B and D, we consider $c^2 = 0.1$ (or 10%) due to the minimum 10% strain required to capture a measurable difference in excimer intensity change.[37–39] Thus, in this scenario, $\nu^2_{\min} = 0.1$ and $\nu^2_{\max} = 1$, considering 100% strain to be the maximum limit. After applying eqn (6), we get $N^2_{\text{val}} = 9$ illustrating 9 discrete states for strain sensing as a function of applied pneumatic pressure. However, due to the micro-level clearance space given for actuation, as seen in Fig. 2C, maximum principal strains near 10% are realized, see Fig. 4F. This limits the possible number of actuation states to only one, which is the minimum strain needed to record the measurable difference in the excimer intensity change and as per the pre-set $c^2 = 0.1$ (or 10%).

Thus, for p^2, as per the commercial FMB's microvalve design having $c^2 = 0.1$ (or 10%), there can be only two states: non-actuated and actuated. The non-actuated state shows no change in the excimer intensity peak. In comparison, the actuated state shows a decrease in the intensity peak corresponding to set $c^2 = 0.1$ (or 10%).

Next, we present a Boolean quantity called quality assessment (QA$_i$) for the *i*th parameter based on the associated sensor output (s^i).[29] In this work, s^i is the excimer intensity coming from the fluorescent dye added to PDMS microvalves under suitable excitation. If the sensor reading s^i is in the specified range (within the error limits, $E^i_{\min}$ and $E^i_{\max}$) designed by the FMB manufacturer, then QA$_i$ is deemed to be acceptable ("good"), else QA$_i$ is unacceptable ("bad"), formalized below in eqn (7).

For the first parameter p^1, which is a watermark location; the fluorescence response (when excited by a laser, 405 nm) should show excimer and monomer peaks as s^1, under allowed error limits, $E^i_{\min}$ and $E^i_{\max}$, similar to the response shown in Fig. 3A, then, QA$_1$ is acceptable. If the location shows no sensor outputs or outputs out of error limits, then QA$_1$ is unacceptable. Similarly, for the second parameter, which is the normalized excimer intensity change (p^2) under actuation, the fluorescence response should show a predetermined excimer intensity change (s^2) based on calibration curves similar to Fig. 3B and D within allowed error limits. In such a case, QA$_2$ is acceptable.

$$\mathrm{QA}_i = \begin{cases} \text{good} & \text{if } E^i_{\min} \le s^i \le E^i_{\max} \\ \text{bad} & \text{otherwise} \end{cases} \tag{7}$$

Machine learning-based countermeasure against material-level attacks

To develop a countermeasure against material-level attacks carried out either for malicious or counterfeiting reasons, we used a simple mechanical punch test setup with a 50 N load cell. For proof of concept of this countermeasure, we selected the curing-ratio-alteration attack model and generated curing ratio-dependent force-displacement data using the setup. We then used the data to train our ML models for curing ratio anomaly detection. Fig. 5A shows a commercial FMB where sample and reagent fluids mix in the PCR area, mainly made up of PDMS consisting of microchannels, micro reaction chambers, and microvalves. The enlarged view shows the PCR area made out of PDMS. As the PDMS area is crucial for the functionality of the FMB, it is essential to ensure that the curing ratio of the PCR area's PDMS is the standard one, which is 10 : 1.[42,81]

Fig. 5B shows PDMS samples made out of curing ratios ranging from 5 : 1 to 50 : 1. Optically, no change in transparency was observed for the samples having curing ratios other than 10 : 1. As there is no change in the optical transparency, it is unlikely to detect an altered PDMS curing ratio unless the PDMS samples are mechanically deformed and sensed. Thus, we developed a simple mechanical punch test setup to punch the PDMS samples in a displacement-controlled way and record the force-displacement data. Fig. 5B shows the force-displacement data for the PDMS sample with a 40 : 1 curing ratio. The data points were linearly fitted to obtain a straight line whose slope was used to estimate the modulus of the PDMS samples.[42] Fig. 5C shows the mechanical punch test done on the samples with 10 : 1 and 40 : 1 curing ratios. Furthermore, Fig. 5C shows the modulus values obtained from samples with 5 : 1 to 50 : 1 curing ratios. The response recorded an exponential decrease in the modulus with the increase in the curing ratio indicating the deteriorated material properties of PDMS due to the altered curing ratios.

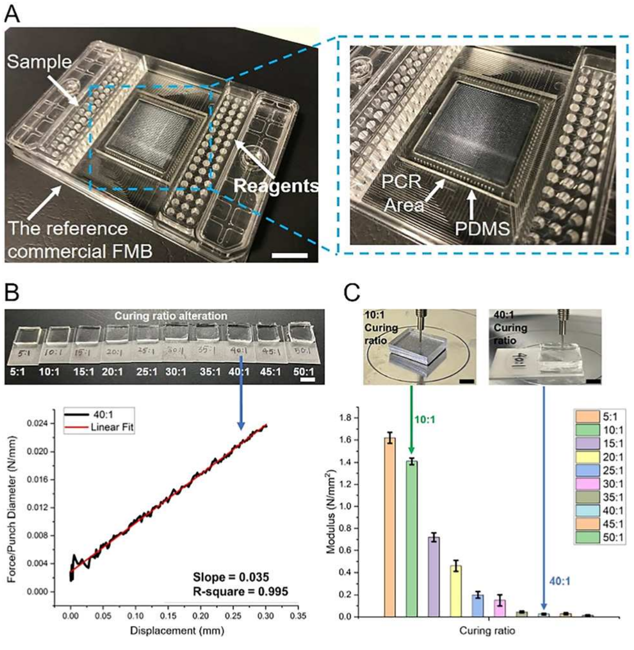


Fig. 5 Mechanical punch test results for PDMS with different curing ratios. A) A commercial FMB used for genotyping. The PCR area is made out of PDMS. The scale bar is 1.5 cm. B) PDMS samples with different curing ratios ranging from 5 : 1 to 50 : 1. The punch test response of the 40 : 1 sample. The scale bar is 1 cm. C) Punch test on the samples having 10 : 1 and 40 : 1 curing ratios. The scale bars each are 2 mm. The bar graph shows modulus *vs.* curing ratio results obtained by the punch test method. The *n* was equal to 5, and the error bar represents the standard deviation.

To train our ML models, we used data from the punch test for detecting curing ratio anomalies in FMBs. We created a multi-step pipeline that takes raw input data for different curing ratios of the punch test, generates more relevant feature data, and filters the resulting set for informative features. If the user's data points exactly match the data points available in our dataset, then we are able to detect an anomaly and decipher the corresponding curing ratio. Otherwise, we utilize our machine learning models both on the set of informative features and on the set of all features available. Our model can predict the anomaly's class if there is an anomaly. If our model reports that the user's values fall within the curing 10 : 1, which is the standard, then we go back to acquire more data and move forward with our pipeline. Fig. 6 shows the steps in our multi-step pipeline.

In order to detect anomalies from the punch test, we used three supervised ML algorithms: decision tree, naïve Bayes, and ensemble methods such as random forest regressors. The details of these models can be found in Text S5.† These three supervised ML algorithms were suitable for our labeled dataset and have successfully predicted curing ratio-based anomalies. We applied these classifiers to the input data before and after performing feature selection. Our goal was to generate different experimental settings and see which combination of features and classifiers yielded the highest prediction performance.

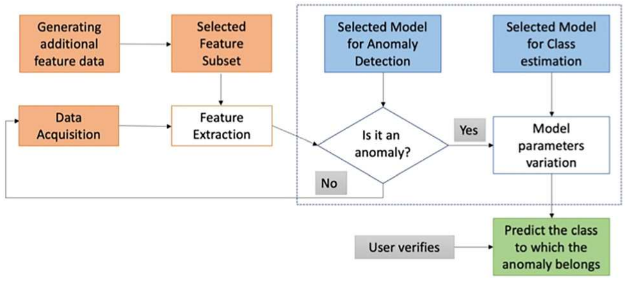

Generating additional feature data
Selected Feature Subset
Selected Model for Anomaly Detection
Selected Model for Class estimation
Data Acquisition
Feature Extraction
Is it an anomaly?
Yes
No
Model parameters variation
User verifies
Predict the class to which the anomaly belongs

Fig. 6 Multi-step pipeline for our ML models.

The raw input data received from the punch test consists of two data features: displacement and force. We had these two features for each of the ten curing ratios 5 : 1, 10 : 1, 15 : 1, 20 : 1, 25 : 1, 30 : 1, 35 : 1, 40 : 1, 45 : 1, and 50 : 1. Since these two features did not provide us with sufficient insights to distinguish between the curing ratios, we generated additional data features from the displacement and force data. For this task, we used the lingress function from the Python library. More specifically, we passed the displacement data on the *x*-axis and the force data on the *y*-axis of the lingress function. As an output of the lingress function, we got the following newly generated data features: the slope of the regression line (slope), the intercept of the regression line (intercept), correlation coefficient (*r* value), *P*-value for a hypothesis test whose null hypothesis is that the slope is zero (*p*-value), standard error of the estimated gradient (stderr), standard error of the intercept (intercept_stderr), and coefficient of determination (*R*-squared).

We explore different feature selection methods to improve our ML models' performance for curing ratio anomaly detection. For classification and regression tasks, it is often useful to remove features that do not help model accuracy.[82,83] The removal of extraneous variables tends to lower variance in the predicted values and reduces the likelihood of overfitting. Moreover, determining which features are helpful in prediction can help point toward underlying mechanisms of the given problem, from which domain experts can work to develop new hypotheses. Text S5† discusses our approaches for selecting useful features for our anomaly detection ML models.

In order to train our ML models, we split the data into two sets – the training set (70%) and the test set (30%). The models were trained on the complete dataset as well as the reduced dataset developed from the feature selection methods, which were based on the mechanical punch test data. After training the three different ML models without feature selection, we were able to achieve an accuracy of 88%. However, with the inclusion of our feature selection/extraction methods and testing over an ensemble of different models, we got more than 99% accuracy on our test dataset, as shown in Table 1. The results indicate that the inclusion of the most significant features can appreciably improve the ML models' performance. Furthermore, Table 1 gives six performance evaluation measures of the proposed methods, consisting of mean absolute error (MAE), mean squared error (MSE), root mean squared error (RMSE), mean absolute percentage error (MAPE), explained variance score, and mean squared log error.

Discussion

FMBs have seen rapid commercialization and deployment for clinical diagnostic and laboratory research in recent years. However, the horizontal supply-chain and outsourced manufacturability of FMBs introduce vulnerabilities to malicious and IP-theft-based attacks. There is a need to generate design files and execute the design files in a foundry (ideally either by a third-party or in-house manufacturing unit) to fabricate the final product. These design and manufacturing stages are susceptible to material-level attacks, where an attacker can introduce material property variation in the FMBs' embedded components, leading to low-quality diagnostics.

PDMS is usually used to make the FMBs' reaction chambers, microfluidic lines, and microvalves. The fabrication steps of PDMS-based FMBs involve replicating the liquid PDMS (mixed with the curing agent) from a master-mold after the mixture gets fully cured by heating. After heating, the PDMS becomes an elastomeric solid. To attack FMBs at the material level, an attacker could mix or pour reactive chemicals during fabrication. The attack would degrade the component material's functionality during the FMB's service time. For example, chemicals such as *t*-butanol and hexadecane can alter the chemical structure of PDMS by inhibiting the related curing kinetics, which can degrade its mechanical properties such as modulus, toughness, fracture strength, *etc.*[75–77] Notably, the addition of these deteriorating chemicals does not alter the optical transparency of the original PDMS. Thus, it is unlikely to detect using light microscopes whether the PDMS material is doped with harmful chemicals. Hence, an attacker can exploit this vulnerability to carry out a material-level attack, which would likely go undetected during microscopy-based quality control checking.

In this work, we specifically focused on microvalves. This choice was driven by the critical role these valves play in enabling the independent operation of reaction chambers within the IFC, ultimately allowing for the achievement of digital PCR.[5,20,84] In digital PCR, microfluidic valves play a crucial role in partitioning the reaction mixture into individual micro-reaction chambers, each containing a single DNA molecule or target of interest.[84–86] Through precise control of valve opening and closing, the sample can be

Table 1 ML models and their performance scores

ML model	Accuracy score	Mean absolute error (MAE)	Mean squared error (MSE)	Root mean squared error (RMSE)	Mean absolute percentage error (MAPE)	Explained variance score	Mean squared log error (MSLE)
Decision tree classifier	0.9996	0.00364	0.0182	0.135	0.000364	1	0.000267
Random forest regressor	0.9997	0.00283	0.0115	0.107	0.000279	1	0.000159
Naïve Bayes	0.9992	0.00364	0.0182	0.135	0.000303	1	0.000161

divided and distributed into these individual chambers, facilitating the amplification and analysis of individual DNA molecules.[5,20,22,84,87]

Companies have leveraged microfluidic valves to develop revolutionary biochips in various fields, such as medical diagnostics, pharmaceutical research, biotechnology, environmental monitoring, and industrial automation.[5,8,20,24,84,88–90] However, attacks on microfluidic valves can have an impact on the flow control due to the associated pressure-driven flow mechanics.[8,24,90] As one of the most critical components with a chip-wide impact, attacks on microfluidic valves can significantly compromise the flow functionality of the biochip. The valve material, being soft and elastomeric, is inherently susceptible to chemical attacks, while channel and chamber materials, made of injection-molded hard plastic, are resistant to such attacks. Consequently, the valves, serving as vital flow-control elements, are the most vulnerable components in the microfluidic chip when it comes to material-based attacks. In contrast, attacks on other components, such as microfluidic channels and reaction chambers, do not directly impact the flow control.[20]

Furthermore, microfluidic valves are susceptible to Trojan attacks due to their inherent flexibility. In such attacks, an attacker can introduce deteriorating or reactive chemicals specifically targeted at the valve area during the manufacturing process. The introduction of these chemicals, which degrade the valve material, can result in characteristics that make the valve prone to fractures. If an attacker applies high-frequency cyclic deformations of the valve membrane, it has the potential to cause catastrophic failure by initiating and propagating cracks. These Trojan attacks are particularly stealthy because during quality control trials, the valve may not undergo the intended cyclic deformations as designed, but only a limited number of deformations to meet production time constraints. Thus, the manifestation of an attack would not occur during the quality control trial but rather after it has been triggered by an attacker, following the successful passing of the trial. Moreover, the defender would not know which valves have been targeted for the Trojan attacks, and it is highly unlikely that all valves can be tested for a large number of high-frequency actuations.

With respect to the curing ratio attacks, adjusting the curing ratio of the valve can result in viscoelastic behavior, meaning it exhibits time and temperature-dependent elasticity. This characteristic makes the valve vulnerable to stealthy attacks that may not be detected during quality control trials. The reason for this is that these trials are typically conducted soon after valve manufacturing and at the intended normal temperature. However, over time, if an attacker maliciously alters the temperature or strains after the biochip has passed the quality trial, the effects of the attack can manifest during the actual use of the biochip by the end user.

Using a commercial FMB as a reference, we investigated material-based attacks. Through benchtop experiments, we demonstrated how FMBs could be attacked *via* material property alteration of PDMS used to make the PCR region containing micro reaction chambers, valves, and channels. First, in an attempt to reverse engineer the FMB, we investigated the structural layout of the FMB using light and electron microscopy techniques. Second, we verified that the material used in the chosen reference commercial FMB is PDMS (10 : 1 curing ratio) *via* nanoindentation tests. Then, we altered the PDMS material properties by adding solvents (*t*-butyl alcohol and hexadecane) as well as the curing ratio during fabrication. Note that both attacks were optically invisible to detect as the chosen chemicals and the curing ratio alteration effectively preserved the optical transparency of the PDMS. Thus, the attacks were stealthy enough to evade microscopy-based quality control trials.

For PDMS doped with *t*-butanol and hexadecane, the fracture strength significantly decreased (by 70%) compared to the pristine PDMS-only samples. In addition, the doped PDMS samples failed with much less strain (61% for *t*-butyl alcohol and 69% for hexadecane), indicating that the mechanical properties got greatly degraded by adding the extra chemicals. Moreover, the attack showed an 82% and 86% decrease in strain energy per unit volume when *t*-butyl alcohol and hexadecane were added to pure PDMS, respectively. Strain energy per unit volume is the area under the stress–strain curve till fracture. It signifies the energy stored in the material during deformation, irrespective of the sample dimensions, and thus is a material property. Hence, the added reactive chemicals significantly decreased the strain-energy-absorbing capacity (or toughness), making the resulting PDMS prone to fracture under considerably less deformation than the original. Similarly, we recorded a significant 67% and 64% decrease in peak stress (signifying the material's strength) for *t*-butyl alcohol and hexadecane-doped PDMS, respectively.

In summary, we experimentally demonstrated that adding stealthy and harmful chemicals such as *t*-butyl alcohol and hexadecane can significantly degrade the mechanical properties of PDMS. Attackers in the manufacturing unit can use such chemicals to target specific microvalves during fabrication to cause material-level attacks.

The second attack we demonstrated was a curing ratio alteration attack where an attacker alters the PDMS curing ratio, making the material sticky and viscoelastic. We performed adhesion experiments to demonstrate the curing ratio alteration attack to compare the compromised sample's adhesion properties with the standard 10 : 1 curing ratio samples. We recorded a 6-fold and 30-fold increase in adhesion energy for the 30 : 1 and 50 : 1 curing ratios, respectively, compared to the 10 : 1 curing ratio. Similarly, regarding adhesion strength, we recorded a 2.8-fold and 3.4-fold increase for the 30 : 1 and 50 : 1 curing ratios, respectively, compared to the 10 : 1 curing ratio. Thus, changing the PDMS curing ratio during fabrication can greatly affect the adhesion and viscoelastic properties of PDMS. An attacker in the manufacturing entity can exploit this vulnerability to deliberately induce problems such as microvalve sticking,[31,32] microvalve degradation,[8] and microchannel biofouling[33,34] in FMBs.

It is unlikely to optically distinguish among PDMS samples having different curing ratios, especially when PDMS structures are made at the micro level making the attack highly stealthy. However, the PDMS becomes softer and stickier with less curing agent (or higher curing ratio). For curing ratios above 30 : 1, the PDMS becomes highly viscoelastic with a mushy or jelly-like consistency, which can likely be detected when subjected to mechanical stress through vicinal structures. This can make the 30 : 1 and above curing ratios detectable under mechanical stress, limiting its stealthiness during quality control trials. Thus, there is a trade-off in a curing ratio attack, where the attacker would tend not to go beyond the 30 : 1 curing ratio out of the fear of getting detected but would likely choose a curing ratio less than 30 : 1 to keep his attack optimally stealthy.

Another scenario where material-based attacks can become prevalent is related to IP theft using reverse engineering, which can provide an attacker with information about the FMB's materials and their associated use.[20,22] After having the information about the materials and their properties *via* reverse engineering, the attacker can intentionally alter (through material-based attacks) the material property of the reverse-engineered FMB's material components to fail the FMB and defame the original FMB company.

Furthermore, given the high cost associated with the development of molecular diagnostic tools, IP theft using reverse engineering can result in counterfeiting, overbuilding, IP, and test protocol piracy attacks for illegal monetary gain or material alterations (*e.g.*, cheaper materials) to save the cost. Thus, to prevent such attacks, it is imperative to secure FMBs using hidden watermarks that cannot be seen or copied by attackers.[20] These watermarks can be used to validate the authentic provenance of the biochip and claim ownership in the event of suspicion.

This work presents the first material-level watermarking scheme as a countermeasure against IP-theft-based attacks for FMBs. The proposed countermeasure incorporates the addition of PDMS-compatible fluorescent dye at specific microvalve locations during the fabrication of the FMB. The locations can act as a watermark, which can only be detected by a spectrophotometer to be quantified and checked against the predesigned intensity–wavelength response. Further, the fluorescent watermark can show a dynamic shift in its excimer intensity peaks under mechanical deformation. We leveraged this mechanoresponsive aspect of the fluorescent dye to impart a two-factor authentication-like feature to the watermark, where the first authentication belongs to finding embedded watermark locations, while the second belongs to matching with the designed spectral shift of the excimer intensity under pneumatic actuation. We characterized the intensity–wavelength response of the fluorescent dye as a function of uniaxial strains using ASTM D412 C samples. The linear regression model between normalized excimer intensity change and uniaxial strain recorded a good correlation with an R-squared value of 0.938.

Furthermore, to account for biaxial strains found in the microvalves under actuation, we fabricated circular PDMS microvalves with different dimensions ranging from 4 mm to 350 μm and added the fluorescent dye to them. After scanning the valve region with laser light (405 nm), we recorded a unique spectral (intensity–wavelength) response with smooth monomer and excimer peaks using a confocal microscope. No such peaks were recorded for the reference PDMS samples. Thus, the watermarks' fluorescence response remained specific and sensitive to the dyed locations on the PDMS layer. Moreover, under actuation, the response showed a reduction in the excimer intensity peak, which remained specific to the maximum principal strain of the actuated valve membrane under pressure.

To rationally design the watermarks, we presented a regression model obtained from the biaxial test done on the dyed PDMS valve samples. The model (normalized excimer intensity change *vs.* maximum principal strain) showed a good correlation with an R-squared value of 0.971. The slope of the linearly fitted line (slope = 0.392) can be used to predict the excimer intensity change based on the maximum principal strain of the PDMS microvalves within acceptable error limits. Thus, using the presented characterization techniques, a material-level watermark designer can rationally design the watermarks based on the microvalve's dimensions and the strain it undergoes when pneumatically actuated.

We have presented a security analysis for the material-level attack and the watermarking scheme. For the randomized checkpointing scheme, we found that there is an attack trade-off where an attacker has to optimally choose m based on n to maximize P_{ev}. The information about n is based on the quality control team's checking regime, which an attacker needs to know to decide on m while maximizing P_{ev}. Thus, it is essential to keep knowledge about n hidden from potential attackers. Furthermore, in the scenario of a full checking scheme as opposed to a randomized checkpointing scheme, we showed using a security metric that attackers can exploit limitations associated with the detecting instruments' sensitivity (S_{n}) and specificity (S_{p}) to carry out their attacks while successfully evading quality control trials.

Given the disposable nature of these biochips, conducting quality control tests on the entire batch using liquid DNA samples is not feasible. Instead, a random sampling approach is employed, where a liquid test DNA sample is loaded into a randomly selected chip, and the results are evaluated afterward. However, this sampling approach creates an opportunity for attackers to selectively introduce their attacks on randomly chosen biochips from the batch, rather than targeting the entire batch. In such a scenario, the likelihood of the attack evading detection during the quality control session increases exponentially as the number of random attack detection trials decreases,[20] similar to the trends we presented in the randomized checkpointing results shown in Fig. 4C.

Regular systematic tests conducted by biochip companies, such as leakage, blockage, shorts (short circuits in the IFC) and opens (open circuits in the IFC), which are mainly electrical and pneumatic tests[8,90] are unable to detect stealthy material-level attacks that require microscopic observation for detection using microscopes. Assuming a high-quality microscope with 100% sensitivity and specificity, we have provided security metrics based on randomized checkpointing scenarios in which valves undergo random inspections for defects. However, the random nature of this inspection scheme enables successful evasion, with evasion likelihood increasing exponentially as the number of random trials decreases, as depicted in Fig. 4C.

Moreover, even if the inspection scheme involves scanning the entire fabricated microfluidic biochip (FMB) to detect defects or areas of attack, there are still possibilities for successful evasion, as depicted in Fig. 4D, due to the limited sensitivity or specificity of the detecting microscope. Therefore, despite the implementation of regular systematic tests and microscopic observation, potential loopholes exist that attackers can exploit to evade quality control checks. Thus, defenders need to be aware of these security assessment metrics and trade-offs and consider additional robust and resilient countermeasures to enhance biochip security.

While biochip companies may develop special tests in the future to detect material-level attacks or defects, currently there is a lack of knowledge regarding the design, vulnerabilities, and impact of such tests. This study emphasizes the need to understand the challenges associated with developing effective tests and the potential security trade-offs involved in order to strengthen biochip security. The findings highlight the importance of adopting a comprehensive approach that goes beyond routine pneumatic and electrical tests. The study encourages the exploration of alternative strategies, such as the ones proposed in this paper, to ensure the resilience and reliability of biochips in the face of stealthy attacks.

Our material-level watermarking scheme consisted of a two-step authentication process with associated parameters (p^i). The first step includes recognizing the correct location of embedded watermarked microvalves (p^1) *via* fluorescence spectroscopy methods. The second step comprises validating the shift in the excimer peak under microvalve actuation (p^2) as designed by the FMB company. Using a metric based on the resolution (c^i) and the acceptable range ($p^i \in [v^i_{\min}, v^i_{\max}]$), we provided the number of possible discrete values (N^i_{val}) that p^i can take for designing the watermark. For example, for the commercial FMB used as the reference for this work, we found $N^1_{\text{val}} = 4607$, which greatly enhanced watermark location options to include randomness in the watermarking design to watermark FMBs either lot-wise or individual-wise.[20] However, $N^2_{\text{val}} = 1$ because of only 10% maximum principal strain associated with microvalve actuation concerning the reference FMB.

For the material-level watermarking scheme, we presented a Boolean quantity called quality assessment (QA$_i$) of *i*th parameter (p^i) based on the associated sensor output (s^i). In this work, s^i is the excimer intensity peak recorded from the dyed PDMS microvalves *via* a spectrometer with a suitable excitation wavelength. If the sensor reading s^i is in the specified range (within the error limits, $E^i_{\min}$ and $E^i_{\max}$) designed by the FMB company, then QA$_i$ is good, else QA$_i$ is bad. A watermark designer can use such metrics to rationally design the material-level watermarks for FMBs.

We developed a novel ML-based defense against curing-ratio-alteration attacks (done for malicious or counterfeiting reasons). We used a simple mechanical punch test setup to generate curing ratio-dependent force-displacement data. We then used the data to train our ML models for curing ratio anomaly detection. In order to train our ML models, we split the data into two sets – the training set (70%) and the test set (30%). The models were trained on the complete dataset as well as the reduced dataset developed from the feature selection methods. After training the three different ML models without feature selection, we were able to achieve an accuracy of 88%. However, with the inclusion of our feature selection/extraction methods and testing over an ensemble of different models, we got more than ~99% accuracy on our test dataset. The obtained results showed that including the most significant features can appreciably improve the ML models' performance.

As shown in Table 1, our three ML models (decision tree classifier, random forest regressor, and Naive Bayes) have similar accuracy scores. This means that they can predict the curing ratio of the punch test with utmost accuracy. However, the random forest regressor performs the best among the three ML models with an accuracy score of 99.97%. The reason being it uses multiple decision trees for training purposes and gathers prediction data from each tree to improve the accuracy score. In addition, the performance metrics in Table 1 support our claim that random forest regressor gives the best results. Mainly, the MAE, MSE, RMSE, and MSLE values are the lowest for our random forest regressor, indicating that the least error value is observed when random forest regressor is used for predicting the curing ratio.

Conclusions

Flow-based microfluidic biochips (FMBs) have seen rapid commercialization and deployment in recent years for biological computing, POCTs, biomolecular recognition, and clinical diagnostics. Following the COVID-19 response, their business opportunities and commercialized deployment have grown exponentially. However, the outsourcing of FMB manufacturing makes them susceptible to material-level malicious and intellectual property (IP)-theft-based attacks. Material-level attacks on FMBs target key materials by doping harmful chemicals to the material components, which will compromise the component's functionality during the service period. The repercussions of such attacks can be severe, with the potential to harm patients, cause resource wastage, and lead to economic consequences. Thus, looking ahead and proactively safeguarding diagnostic-related FMBs against material-level attacks launched by adversaries is essential.

This work demonstrates the first material-level attacks on representative polydimethylsiloxane (PDMS)-based FMBs. The attacks involve adding harmful chemicals or altering the curing ratio to PDMS in its liquid state. The attack shows a deteriorating effect on the material and adhesion properties of the PDMS after curing while preserving the original optical transparency, thus making it unlikely to be detected *via* microscopes during quality control trials. We demonstrated the attack experimentally by adding hexadecane and *t*-butyl alcohol to the pristine PDMS. The attack greatly degraded the mechanical and adhesion properties of the doped PDMS, as recorded by the respective ASTM D412 C tensile and adhesion tests. Attacks of such sorts can become prevalent in IP-theft-based attacks such as counterfeiting, overbuilding, reverse engineering, *etc.* Thus, we developed a contactless spectrometric material-level countermeasure to protect FMBs against IP-theft-based attacks.

The countermeasure involves dynamic material-level watermarking for PDMS-based FMBs (with microvalves) using a perylene-labeled fluorescent dye. When added to a microvalve, the dyed microvalve shows a unique excimer intensity peak under 405 nm laser excitation. Further, when the microvalve is pneumatically actuated, the excimer peak exhibits a mechanoresponsive behavior by offering a predetermined downward shift in its intensity as a function of mechanical strain. Through benchtop experiments, we validated the scheme using fluorescence microscopy, which showed a high correlation (R^2 = 0.971) between the normalized excimer intensity change and the maximum principal strain of the actuated microvalves. Furthermore, we presented security metrics for randomized and non-randomized checkpointing schemes, as well as quality assessment parameters for effective design and verification of the watermarks. The models and metrics can be used to rationally design the material-level watermarks to check the authentic provenance of the materials used in FMBs.

Moreover, we adapted machine learning (ML) models to detect material-level anomalies in FMBs. The ML models were trained on the force-displacement data obtained from a mechanical punch test method. In total, we explored three ML models (random forest, Naive Bayes, and decision tree) for curing ratio anomaly detection. We have achieved around 99% accuracy in detecting anomalies to quote the best results among the adapted ML models. The ML-based countermeasure can be used against general material-based attacks, such as adding reactive solvents or altering the curing ratio. In this work, we demonstrated the proof of concept for the curing-ratio-alteration attack.

In summary, the material-level countermeasures we present can be used to proactively safeguard FMBs against material-level attacks in the era of global pandemics and point-of-care diagnostics.

Author contributions

Conceptualization: NSB, SS, SJ, IS, JK, SB, YAS, KC, RK. Methodology: NSB, SS, SJ, IS, SK, MK, JK, SB, YAS, KC, RK. Investigation: NSB, SS, SJ, IS, SK, MK, JK, SB, YAS, KC, RK. Visualization: NSB, SS, SJ, IS, SK, JK, SB, YAS, KC, RK. Supervision: NSB, SB, YAS, KC, RK. Writing—NSB, SS, SJ, IS, SK, MK, JK, SB, YAS, KC, RK. Writing—review & editing: NSB, SS, SJ, IS, SK, JK, SB, YAS, KC, RK.

Conflicts of interest

There are no conflicts to declare.

Acknowledgements

We thank and acknowledge the technical support from the Core Technology Platforms (CTP) at NYU Abu Dhabi, especially Dr. Rachid Rezgui for his support in the spectral analysis. We thank Dr. Agyapal Singh for helping us with the DIC setup. Further, we thank the National Science Foundation (NSF) for providing us with the grants: Karri was supported in part by NSF awards 1833624 and 2049311, and Chakrabarty was supported in part by NSF under grant no. 2049335.

References

1 M. Shayan, S. Bhattacharjee, A. Orozaliev, Y. A. Song, K. Chakrabarty and R. Karri, *IEEE Trans. Inf. Forensics Secur.*, 2021, **16**, 2076–2089.

2 M. I. Mohammed, *Nature*, 2022, **605**(7910), 429–430.

3 D. Gountia and S. Roy, *J. Inf. Secur. Appl.*, 2021, **58**, 102773.

4 M. I. Mohammed, *Nature*, 2022, **605**, 429–430.

5 X. Xie, T. Gjorgjieva, Z. Attieh, M. M. Dieng, M. Arnoux, M. Khair, Y. Moussa, F. Al Jallaf, N. Rahiman, C. A. Jackson, L. El Messery, K. Pamplona, Z. Victoria, M. Zafar, R. Ali, F. Piano, K. C. Gunsalus and Y. Idaghdour, *Processes*, 2020, **8**, 1425.

6 C. Wang, M. Liu, Z. Wang, S. Li, Y. Deng and N. He, *Nano Today*, 2021, **37**, 101092.

7 S.-R. Joung, C. J. Kang, Y.-S. Kim, M. B. Kulkarni and S. Goel, *Eng. Res. Express*, 2020, **2**, 042001.

8 K. Hu, T. Y. Ho and K. Chakrabarty, in *IEEE 31st VLSI Test Symposium (VTS)*, 2013, pp. 1–6.

9 N. Mahhengam, A. F. G. Khazaali, S. Aravindhan, A. O. Zekiy, L. Melnikova and H. Siahmansouri, *Crit. Rev. Anal. Chem.*, 2021, **52**, 1863–1877.

10 K. A. Fleming, S. Horton, M. L. Wilson, R. Atun, K. Destigter, J. Flanigan, S. Sayed, P. Adam, B. Aguilar, S. Andronikou, C. Boehme, W. Cherniak, A. N. Cheung, B. Dahn, L. Donoso-Bach, T. Douglas, P. Garcia, S. Hussain, H. S. Iyer, M. Kohli, A. B. Labrique, L.-M. Looi, J. G. Meara, J. Nkengasong, M. Pai, K.-L. Pool, K. Ramaiya, L. Schroeder, D. Shah, R. Sullivan, B.-S. Tan and K. Walia, *Lancet*, 2021, **398**, 1997–2050.

11 S. Kleinert and R. Horton, *Lancet*, 2021, **398**, 1945–1947.

12 A. Edoardo Ongaro, Z. Ndlovu, E. Sollier, C. Otieno, P. Ondoa, A. Street and M. Kersaudy-Kerhoas, *Lab Chip*, 2022, **22**, 3122–3137.

13 *Global analysis of health care waste in the context of COVID-19*, **https://www.who.int/publications/i/item/9789240039612**, (accessed 30 July 2022).

14 *Molecular Diagnostics Market worth $30.2 billion by 2027*, **https://www.marketsandmarkets.com/PressReleases/molecular-diagnostic.asp**, (accessed 23 December 2021).

15 *Microfluidics Market Size, Growth by Product, Application, Research, Manufacturing, End User & Region Global Forecasts to 2026*, **https://www.marketsandmarkets.com/Market-Reports/microfluidics-market-1305.html**, (accessed 30 July 2022).

16 *Lab-on-a-chip and microarrays (biochip) market – growth, trends and forecasts (2023–2028)*, **https://www.mordorintelligence.com/industry-reports/biochip-product-market**, (accessed 30 July 2022).

17 *Point of Care/Rapid Diagnostics Market worth $75.5 billion by 2027*, **https://www.marketsandmarkets.com/PressReleases/point-of-care-diagnostic.asp**, (accessed 26 July 2022).

18 M. Shayan, S. Bhattacharjee, R. Wille, K. Chakrabarty and R. Karri, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2021, **40**, 143–156.

19 J. Tang, M. Ibrahim, K. Chakrabarty and R. Karri, in *IEEE 26th Asian Test Symposium (ATS)*, IEEE Computer Society, 2017, pp. 115–120.

20 N. S. Baban, S. Saha, A. Orozaliev, J. Kim, S. Bhattacharjee, Y.-A. A. Song, R. Karri and K. Chakrabarty, *IEEE Trans. Biomed. Circuits Syst.*, 2022, **16**, 1261–1275.

21 J. Tang, M. Ibrahim, K. Chakrabarty and R. Karri, in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Institute of Electrical and Electronics Engineers Inc., 2019, vol. 38, pp. 589–603.

22 H. Chen, S. Potluri and F. Koushanfar, in *IEEE International Conference on Computer Design (ICCD)*, Institute of Electrical and Electronics Engineers Inc, 2017, pp. 9–16.

23 M. Shayan, S. Bhattacharjee, Y. A. Song, K. Chakrabarty and R. Karri, in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Institute of Electrical and Electronics Engineers Inc., 2020, pp. 1037–1042.

24 N. S. G. K. Devaraju and M. A. Unger, *Lab Chip*, 2012, **12**, 4809–4815.

25 H. Fallahi, J. Zhang, H. P. Phan and N. T. Nguyen, *Micromachines*, 2019, **10**, 830.

26 N. S. Baban, A. Orozaliev, S. Kirchhof, C. J. Stubbs and Y. A. Song, *Science*, 2022, **375**, 770–774.

27 N. S. Baban, A. Orozaliev, C. J. Stubbs and Y.-A. Song, *Bioinspiration Biomimetics*, 2022, **17**, 036002.

28 B. M. Z. Newby and M. K. Chaudhury, *Langmuir*, 1997, **13**, 1805–1809.

29 M. Shayan, S. Bhattacharjee, J. Tang, K. Chakrabarty and R. Karri, *IEEE Trans. Inf. Forensics Secur.*, 2019, **14**, 2901–2915.

30 M. Shayan, S. Bhattacharjee, Y. A. Song, K. Chakrabarty and R. Karri, in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Institute of Electrical and Electronics Engineers Inc., 2019, pp. 210–215.

31 A. Lamberti, S. L. Marasso and M. Cocuzza, *RSC Adv.*, 2014, **4**, 61415–61419.

32 C.-H. Lin, C.-Y. Huang, J.-Y. Ho and H.-Y. Hsueh, *ACS Appl. Mater. Interfaces*, 2020, **12**, 22365–22377.

33 L. Vroman, A. L. Adams, G. C. Fischer and P. C. Munoz, *Blood*, 1980, **55**, 156–159.

34 F. K. Balagaddé, L. You, C. L. Hansen, F. H. Arnold and S. R. Quake, *Science*, 2005, **309**, 137–140.

35 E. Dahan and P. R. Sundararajan, *Eur. Polym. J.*, 2015, **65**, 4–14.

36 T. Guner, E. Aksoy, M. M. Demir and C. Varlikli, *Dyes Pigm.*, 2019, **160**, 501–508.

37 F. Cellini, S. Khapli, S. D. Peterson and M. Porfiri, *Appl. Phys. Lett.*, 2014, **105**, 061907.

38 F. Cellini, L. Block, J. Li, S. Khapli, S. D. Peterson and M. Porfiri, *Sens. Actuators, B*, 2016, **234**, 510–520.

39 F. Cellini, L. Zhou, S. Khapli, S. D. Peterson and M. Porfiri, *Mech. Mater.*, 2016, **93**, 145–162.

40 C. Weder, *J. Mater. Chem.*, 2011, **21**, 8235–8236.

41 N. A. A. Rossi, E. J. Duplock, J. Meegan, D. R. T. Roberts, J. J. Murphy, M. Patel and S. J. Holder, *J. Mater. Chem.*, 2009, **19**, 7674–7686.

42 I. K. Lin, K. S. Ou, Y. M. Liao, Y. Liu, K. S. Chen and X. Zhang, *J. Microelectromech. Syst.*, 2009, **18**, 1087–1099.

43 I. M. Nasir, M. A. Khan, M. Yasmin, J. H. Shah, M. Gabryel, R. Scherer and R. Damaševičius, *Sensors*, 2020, **20**, 6793.

44 R. Ruiz, J. C. Riquelme and J. S. Aguilar-Ruiz, *J. Intell. Fuzzy Syst.*, 2002, **12**, 175–183.

45 A. Tiwari, E. J. Villasenor, N. Gupta, N. Reddy, R. Karri and S. T. S. Bukkapatnam, in *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security*, Association for Computing Machinery (ACM), 2021, vol. 11, pp. 11–21.

46 C. Bayens, T. Le, L. Garcia, R. Beyah, M. Javanmard and S. Zonouz, in *USENIX Security Symposium*, 2017, pp. 1181–1198.

47 S. Bhattacharjee, J. Tang, M. Ibrahim, K. Chakrabarty and R. Karri, in *2018 IEEE 23rd European Test Symposium (ETS)*, IEEE, 2018, vol. 2018-May, pp. 1–6.

48 *Illumina Deepens Commitment to Customers in China with New Manufacturing Site*, **https://www.illumina.com/company/news-center/press-releases/2022/137f42ca-e5b6-43d1-9406-7f8bebf831fe.html**, (accessed 15 June 2023).

49 *Emulate|Organ-Chips for Research & Development*, **https://emulatebio.com/**, (accessed 15 June 2023).

50 *Illumina|Sequencing and array-based solutions for genetic research*, **https://www.illumina.com/**, (accessed 15 June 2023).

51 *Standard BioTools|Standard BioTools*, **https://www.standardbio.com/**, (accessed 15 June 2023).

52 *Emulate and Minifab Announce Strategic Manufacturing Partnership to Accelerate the Scaling and Commercialization of Emulate's Human Emulation System™*, **https://schott-minifab.com/item/38-emulate-and-minifab-partnership**, (accessed 14 June 2023).

53 *Fluidigm Delivers More Than One Billion Microscopic NanoFlex™ Valves|Business Wire*, **https://www.businesswire.**

com/news/home/20110505005451/en/Fluidigm-Delivers-More-Than-One-Billion-Microscopic-NanoFlex™-Valves, (accessed 15 June 2023).

54 Y. Zhu, B. Li, T. Y. Ho, Q. Wang, H. Yao, R. Wille and U. Schlichtmann, in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 1–8.

55 M. Shayan, S. Bhattacharjee, Y. A. Song, K. Chakrabarty and R. Karri, *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 2019, **27**, 2755–2766.

56 J. Tang, M. Ibrahim, K. Chakrabarty and R. Karri, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2020, **39**, 1003–1016.

57 T. Le, G. Salles-Loustau, L. Najafizadeh, M. Javanmard and S. Zonouz, *Proc. - 46th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks, DSN 2016*, 2016, pp. 583–594.

58 T. Le, G. Salles-Loustau, P. Xie, Z. Lin, L. Najafizadeh, M. Javanmard and S. Zonouz, *IEEE Sens. J.*, 2017, **17**, 5807–5816.

59 G. Salles-Loustau, T. Le, L. Najafizadeh, S. Zonouz and M. Javanmard, *Biomed. Microdevices*, 2018, **20**, 1–9.

60 H. Chen, S. Potluri and F. Koushanfar, in *C18th IEEE International New Circuits and Systems Conference (NEWCAS)*, Institute of Electrical and Electronics Engineers Inc., 2020, pp. 158–161.

61 T. Le, S. Etigowni, S. Liang, X. Peng, J. Qi, M. Javanmard, S. Zonouz and R. Beyah, in *Annual Computer Security Applications Conference*, Association for Computing Machinery, 2021, pp. 732–747.

62 M. Sabokrou, M. Fayyaz, M. Fathy and R. Klette, *IEEE Trans. Image Process.*, 2017, **26**, 1992–2004.

63 M. Sabokrou, M. Khalooei, M. Fathy and E. Adeli, in *IEEE conference on computer vision and pattern recognition*, 2018, pp. 3379–3388.

64 W. Li, V. Mahadevan and N. Vasconcelos, *IEEE Trans. Pattern Anal. Mach. Intell.*, 2014, **36**, 18–32.

65 Y. Cong, J. Yuan and J. Liu, in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE Computer Society, 2011, pp. 3449–3456.

66 M. Nakano, A. Takahashi and S. Takahashi, *Knowl.-Based Syst.*, 2017, **131**, 113–124.

67 H. N. Akouemo and R. J. Povinelli, *Int. J. Forecast.*, 2016, **32**, 948–956.

68 S. Mascaro, A. Nicholson and K. Korb, *Int. J. Approx. Reason.*, 2014, **55**, 84–98.

69 Y. Li, L. Guo, Z. H. Tian and T. B. Lu, *Comput. Commun.*, 2008, **31**, 4018–4025.

70 A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão and M. L. Proença, *Expert Syst. Appl.*, 2018, **92**, 390–402.

71 Z. Chiba, N. Abghour, K. Moussaid, A. El Omri and M. Rida, *Comput. Secur.*, 2018, **75**, 36–58.

72 T. Kubota and W. Yamamoto, *Procedia Manuf.*, 2019, **30**, 83–89.

73 V. J. Hodge and J. Austin, *Artif. Intell. Rev.*, 2004, **22**, 85–126.

74 M. Injadat, F. Salo, A. B. Nassif, A. Essex and A. Shami, in *IEEE global communications conference (GLOBECOM)*, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 1–6.

75 M. Abshirini, M. C. Saha, M. Cengiz Altan and Y. Liu, *Mater. Des.*, 2021, **212**, 110194.

76 A. Perevedentsev, P. N. Stavrinou, D. D. C. Bradley and P. Smith, *J. Polym. Sci., Part B: Polym. Phys.*, 2015, **53**, 1481–1491.

77 J. N. Lee, C. Park and G. M. Whitesides, *Anal. Chem.*, 2003, **75**, 6544–6554.

78 N. S. Baban, A. Orozaliev, C. J. Stubbs and Y. A. Song, *Phys. Rev. E*, 2020, **102**, 012801.

79 J. Tang, M. Ibrahim, K. Chakrabarty and R. Karri, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2018, **37**, 1119–1132.

80 J. Tang, M. Ibrahim and K. Chakrabarty, *IEEE Des. Test*, 2019, **36**, 5–13.

81 S. Patil, A. Malasi, A. Majumder, A. Ghatak and A. Sharma, *Langmuir*, 2012, **28**, 42–46.

82 M. R. Segal, *Machine Learning Benchmarks and Random Forest Regression*, Center for Bioinformatics and Molecular Biostatistics, University of California, San Francisco, 2004, https://escholarship.org/uc/item/35x3v9t4.

83 X. W. Chen and M. Wasikowski, in *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2008, pp. 124–132.

84 R. Ramakrishnan, J. Qin, R. C. Jones and L. Suzanne Weaver, *Methods Mol. Biol.*, 2013, **949**, 423–431.

85 E. A. Ottesen, W. H. Jong, S. R. Quake and J. R. Leadbetter, *Science*, 2006, **314**, 1464–1467.

86 X. Mao, C. Liu, H. Tong, Y. Chen and K. Liu, *Am. J. Transl. Res.*, 2019, **11**, 7209.

87 C. J. Wang and A. Levchenko, *Methods Mol. Biol.*, 2009, **500**, 203–219.

88 *Microfluidics|Fluidigm*, https://www.fluidigm.com/products-services/technologies/microfluidics, (accessed 16 January 2022).

89 *Fluidigm Delivers More Than One Billion Microscopic NanoFlex™ Valves|Business Wire*, https://www.businesswire.com/news/home/20110505005451/en/Fluidigm-Delivers-More-Than-One-Billion-Microscopic-NanoFlexTM-Valves, (accessed 12 July 2022).

90 X. Huang, T. Y. Ho, W. Guo, B. Li, K. Chakrabarty and U. Schlichtmann, *ACM Comput. Surv.*, 2021, **54**, 1–29.