3-2024

Harnessing the advances of MEDA to optimize multi-PUF for enhancing IP security of biochips

Chen DONG

Xiaodong GUO

Sihuang LIAN

Yinan YAO

Zhenyi CHEN

See next page for additional authors

Citation

DONG, Chen; GUO, Xiaodong; LIAN, Sihuang; YAO, Yinan; CHEN, Zhenyi; YANG, Yang; and LIU, Zhanghui. Harnessing the advances of MEDA to optimize multi-PUF for enhancing IP security of biochips. (2024). *Journal of King Saud University - Computer and Information Sciences*. 36, (3), 1-14.
Available at: https://ink.library.smu.edu.sg/sis_research/8716

Journal of King Saud University - Computer and Information Sciences 36 (2024) 101996

HOSTED BY

Contents lists available at ScienceDirect

Journal of King Saud University - Computer and Information Sciences

journal homepage: www.sciencedirect.com

Harnessing the advances of MEDA to optimize multi-PUF for enhancing IP security of biochips

Chen Dong [a], Xiaodong Guo [a], Sihuang Lian [a], Yinan Yao [a], Zhenyi Chen [b], Yang Yang [c], Zhanghui Liu [a,*]

[a] College of Computer and Data Science, Fuzhou University, Fujian, China
[b] Department of Computer Science and Engineering, University of South Florida, 33620, Tampa, FL, USA
[c] School of Computing and Information Systems, Singapore Management University, Singapore, 188065, Singapore

ARTICLE INFO

MSC:
0000
1111

Keywords:
MEDA biochips
Multi-PUF
IP protection
Hardware security
Modeling attack

ABSTRACT

Digital microfluidic biochips (DMFBs) have a significant stride in the applications of medicine and the biochemistry in recent years. DMFBs based on micro-electrode-dot-array (MEDA) architecture, as the next-generation DMFBs, aim to overcome drawbacks of conventional DMFBs, such as droplet size restriction, low accuracy, and poor sensing ability. Since the potential market value of MEDA biochips is vast, it is of paramount importance to explore approaches to protect the intellectual property (IP) of MEDA biochips during the development process. In this paper, an IP authentication strategy based on the multi-PUF applied to MEDA biochips is presented, called bioMPUF, consisting of Delay PUF, Split PUF and Countermeasure. The bioMPUF strategy is designed to enhance the non-linearity between challenges and responses of PUFs, making the challenge–response pairs (CRPs) on the MEDA biochips are difficult to be anticipated, thus thwarting IP piracy attacks. Moreover, based on the easy degradation of MEDA biochip electrodes, a countermeasure is proposed to destroy the availability of piracy chips. Experimental results demonstrate the feasibility of the proposed bioMPUF strategy against the brute force attack and modeling attack.

1. Introduction

Digital microfluidic biochips (DMFB) as a promising field-programmable platform can manipulate discrete fluidic droplets on a chip, called as lab-on-chips as well (Poddar et al., 2021b). Compared with technologies of conventional biochemical laboratories, DMFBs have advantages including low cost (Shayan et al., 2020a), high accuracy (Guo et al., 2022), portability (Poddar et al., 2021a), minimal human intervention (Dong et al., 2020), etc. Accordingly, DMFBs have emerged as a critical candidate to be deployed in biochemical applications, such as sample preparation (Poddar and Bhattacharya, 2022), protein extraction (Ji et al., 2022), and polymerase chain reaction (PCR) tests (Shi et al., 2022). DMFBs have been leveraged in infectious disease testing by Babies, a commercial company focusing on newborn screening (Babies, 2023). Due to the programmable structure of DMFBs, the diagnostic platform FINDER, a near-patient newborn testing platform, has been updated to offer RT-PCR tests for SARS-CoV-2 (Babies, 2020).

One of the significant limitations of DMFBs is lacking a sensitive sensing system to detect droplets, thus the inability to detect on-chip situations in real time (Zhong et al., 2020). A novel structure called a micro-electrode-dot-array (MEDA), has been constructed on DMFBs to overcome drawbacks with conventional structure (Keszocze et al., 2017). MEDA is a concept based on sea-of-micro-electrodes, which have 10–20 times the electrodes of DMFBs in the chip with an identical scale. Hence, droplets on MEDA biochips will be manipulated with fine-grained, and perform some specific functions, such as aliquot split (Ibrahim et al., 2021), diagonal movement (Liang, 2021), shape morphing (Elfar et al., 2021), etc. Moreover, since each micro-electrode

* Corresponding author.
E-mail addresses: dongchen@fzu.edu.cn (C. Dong), xiaodong.guo0328@gmail.com (X. Guo), sihlian@foxmail.com (S. Lian), y2ann@qq.com (Y. Yao), zhenyichen@usf.edu (Z. Chen), yang.yang.research@gmail.com (Y. Yang), lzh@fzu.edu.cn (Z. Liu).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2024.101996
Received 12 October 2023; Received in revised form 13 February 2024; Accepted 27 February 2024
Available online 6 March 2024

on MEDA biochips is integrated with a sensitive sensing system, in addition to the original advantages, the MEDA biochip enables droplet detection and real-time error recovery (Zhong and Chakrabarty, 2020).

Undoubtedly, biochips would bring huge social and economic benefits. The market is expected to grow at a compound annual growth rate of 25.15% from 2022 to 2027, growing at USD 43,273.01 million (Technavio, 2023). As DMFBs have been widely used in biochemical fields, security threats and drawbacks of DMFBs are being uncovered (Zhong et al., 2018; Gountia, 2023). MEDA biochips as the next-generation DMFBs, have a large potential market, intellectual property (IP) of MEDA is attractive to malicious people. Recently proposed IP protection solutions can effectively improve the security of biochip IPs (Shayan et al., 2019; Dong et al., 2021; Bhattacharjee et al., 2019), but cannot handle the situation where the authorized user is the attacker. Furthermore, with the increasing number of third-party participating during design and manufacturing flow, IP piracy of MEDA biochips is becoming a knotty challenge (Dong et al., 2021).

Physical unclonable functions (PUFs) as the hardware security primitive is an extremely effective method to protect IP, which is achieved by extracting inevitable manufacturing deviation to generate the key with tamper-resistant, i.e., "hardware fingerprint" (Cui et al., 2020). In Hsieh et al. (2017), authors proposed two novel PUF strategies, which leveraged the variation deriving from droplet operations, like transportation and split, to acquire PUF outputs. Moreover, in Lin et al. (2018), a comprehensive system based on the concept of Hsieh et al. (2017) has been proposed. This system has been utilized to thwart IP piracy and Trojan attacks simultaneously, which is capable of achieving a 94% success rate in a 15 × 15 DMFB. In recent years, the idea of constructing a composite PUF by several single PUFs for FPGA (Field Programmable Gate Array) has been proposed, called multi-PUF, which can obtain better performance with reasonable resource overhead (Hemavathy and Bhaaskaran, 2023). In integrated circuits (ICs), multi-PUF has been demonstrated to improve security metrics in a single PUF and is resistant to modeling attacks based on machine learning (ML) (Tripathy et al., 2021).

Although the existing PUFs in DMFBs can be applied in MEDA biochips, the sensitive sensing system and fine-grained control for MEDA biochips can be sufficient to support developing more advanced and specialized PUF strategies. In addition, in view of the excellent performance of multi-PUF in ICs, it is worth protecting the IP of MEDAs. Accordingly, in this paper, a strategy of multi-PUF for MEDA biochips is presented, named bioMPUF. Due to the sensitive sensing ability, the accuracy of PUF identity verification will be improved depending on the real-time property and location of droplets. The bioMPUF deployed in MEDA biochips can achieve the balance between performance and overhead better. Moreover, in order to combat piracy manufacturers, a countermeasure is developed to shrink the lifespan of pirated biochips.

The key contributions of this paper are as follows:

- Proposing a multi-PUF strategy for MEDA biochips firstly, called bioMPUF, which is constructed by two types of single PUFs. The strategy aims to improve the efficiency of protecting the IP of MEDA biochips.
- Formulating the calculation method for the length of response for bioMPUF. The bit number of responses is allowed to be customized by users according to different security requirements.
- Presenting a countermeasure against pirated MEDA biochips. This measure can shrink the lifespan of pirated devices by offering actuation sequences with high on-chip resource consumption.
- Demonstrating the effectiveness of bioMPUF in brute force attacks and the modeling attacks by experiments.

The rest of this paper is organized as follows. Section 2 presents background knowledge relevant to this work and summarizes previous work. Section 3 describes the threat model and explains the motivation for this work. Section 4 describes the overall framework and workflow of the bioMPUF. Section 5 presents the detailed design of the bioMPUF on the MEDA biochip. Section 6 demonstrates the effectiveness of the bioMPUF through experiments and security analysis. Section 7 is the conclusion.

2. Background

In this section, the MEDA biochip architecture for developing more advanced PUFs and how it works is described. Then, the advantages of MPUF are briefly described. Finally, the related work is summarized.

2.1. MEDA biochips architecture

Fig. 1(a) shows the schematic view of a MEDA biochip, the main part of the MEDA biochip is two parallel plates with a spacing in the middle, where the top plate serves as a grounded electrode, and the bottom plate integrates a two-dimensional microelectrode cell (MC) array (Datta et al., 2022). As shown in Fig. 1(b), both the top and bottom plates are made of insulating and hydrophobic materials. The use of insulating materials for the top and bottom plates effectively isolates the droplets and channels inside the biochip to prevent unwanted current leakage and to ensure that the electric field is concentrated in the desired area of the droplet, thus better controlling the droplet's movement and morphology changes (He and Hu, 2020). The use of hydrophobic materials allows for easier manipulation and positioning of the droplets, preventing them from sticking to the plate for precise fluidic manipulation (Guo et al., 2022). In addition, silicone oil fills the gap between the two plates, allowing the droplets to move more smoothly while preventing droplet evaporation and somewhat reducing the risk of droplet cross-contamination (Ji et al., 2023).

The platform of MEDA biochip is composed of a processor, a control unit and a two-dimensional MC array, as shown in Fig. 1. Adjacent MCs are connected in a daisy-chain structure (Zhang et al., 2023). An MC consists of a micro-electrode, an activating circuit, and a sensing circuit. The activating circuit is utilized to generate the driven force to manipulate droplets. The sensing circuit can timely sense location and property of droplets and return them to the processor. Compared to conventional DMFBs, MCs on MEDA have real-time sensing capabilities in addition to the ability to perform fine-grained droplet control (Chan and Lee, 2022). The sensitive real-time sensing capability enhances the reliability during the execution of biochemical protocols. Each MC is independently controlled. Therefore, MEDA allows MCs to be dynamically grouped to form fluidic modules of different shapes and sizes, such as mixers (Howladar et al., 2021). In addition, the control unit contains a biochip layout map, a fluidic operation manager, and a droplet location map, as shown in Fig. 1(c). The fluidic operation manager can convert fluidic instructions to a model suitable for MCs, and the real-time locations of droplets will be stored in the droplet location map (Liang et al., 2020).

2.2. MEDA biochips working principle

The discrete droplets on MEDA biochips route between the top plate and the bottom plate. When the high voltage V is employed on an electrode near the droplet, a voltage difference will be generated as the electrode occupied by the droplet indicates the low voltage (Howladar et al., 2020). Accordingly, the electric field deriving from voltage difference is utilized to alter the interfacial tension between the droplet and the bottom plate surface, thus changing the apparent contact angle $\theta(V)$. Hence, the droplet moves to the high voltage electrode from the low one. The phenomenon is termed as the electrowetting-on-dielectric (EWOD) (Cho and Pan, 2008), which can be modeled by the Lippmann–Young equation:

$$\cos\theta(V) = \cos\theta(0) + \frac{\epsilon_0\epsilon_r V^2}{2d\gamma_{LG}} \tag{1}$$

where $\theta(0)$ is the contact angle with zero voltage, d presents the thickness of the dielectric layer, γ_{LG} indicates the liquid–gas interfacial

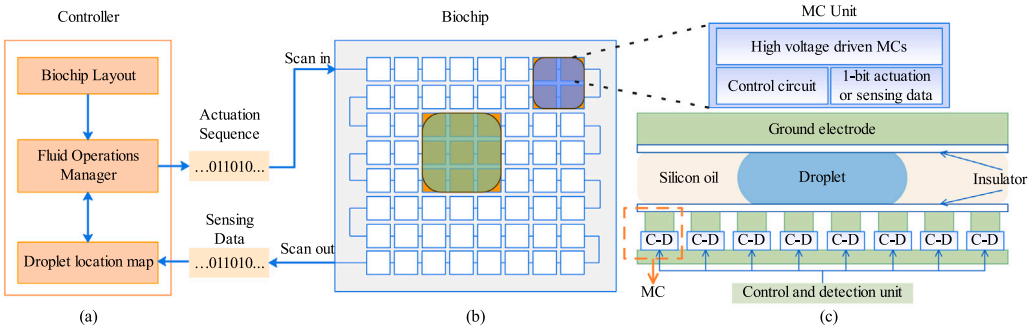

Fig. 1. The overall architecture of the MEDA biochip platform. Where (**a**) is the controller used to control the execution of biochemical protocols, (**b**) is the main body of the MEDA biochip, and (**c**) is a cross-section of the MEDA biochip (Shayan et al., 2020b).

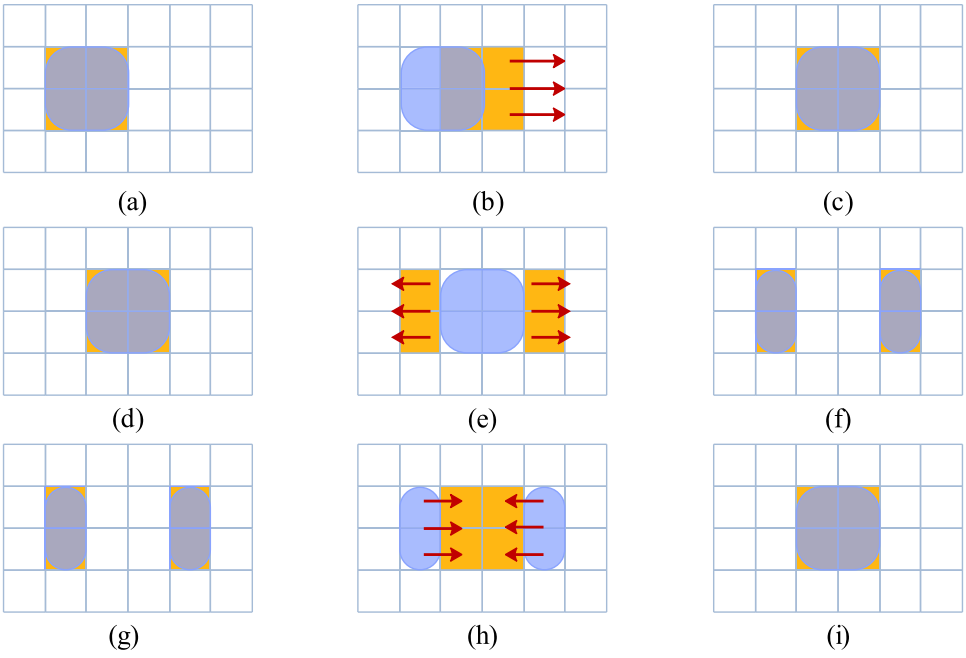

Fig. 2. The MEDA biochip performs fluid manipulations by controlling the state of the MCs. Among them, (**a**)-(**c**) is droplet movement, (**d**)-(**f**) is droplet splitting, and (**g**)-(**i**) is droplet merging.

tension, and ϵ_0 and ϵ_r are represented the permittivity of vacuum and the permittivity of the bottom insulator, respectively.

As shown in Fig. 2, according to the principle of EWOD, various basic fluidic operations can be implemented by applying a series of electric potentials to the MCs on the MEDA, including:

Moving: As shown in Fig. 2(a)–(c), changing the state of the neighboring MCs to the right of the current position of the droplet by applying a voltage to them produces an asymmetric change in the interfacial tension, which drives the droplet to move to the right.

Splitting: As shown in Fig. 2(d)–(f), a 2 × 2 droplet splits horizontally with the left and right MCs turned on and the MCs currently covered by the droplet turned off. By applying hydrophilic forces of equal magnitude to both sides of the droplet to stretch the droplet to both sides, the electrode in the center closes to pinch off the droplet into two sub-droplets.

Mixing: As shown in Fig. 2(g)–(i), the merging operation can be regarded as the reverse of the splitting operation. Based on the same principle, the inner 2 sets of 1 × 2 electrodes are opened and the outer electrodes are closed to drive two 1 × 2 sub-droplets in order to merge into one large 2 × 2 droplet.

In addition, MEDA is capable of advanced fluidic operations such as diagonal shifts, unequal splitting and morphing.

2.3. PUF and MPUF

In the field of IC authentication, PUF is a low-consumption, secure and reliable authentication method. It is different from general encryption techniques that store the key in a certain place, but use the uncertainty that exists in the physical system itself to generate unpredictable output. Moreover, its encryption and decryption keys are generated and do not need to be stored. Therefore, it is popular for its uniqueness and unclonability, randomness and unpredictability, Resistance to Attacks, Real-Time Generation and One-Time Use, and is widely used in IC authentication, hardware metering and certified execution scenarios (Yoon et al., 2020). Although a single-PUF shows great potential for biochip intellectual property protection due to its characteristics (Hsieh et al., 2017), there are some drawbacks, including vulnerability to modeling attacks, sensitivity to noise, performance fluctuations, and high on-chip resource overheads (Kokila and Ramasubramanian, 2019; Aseeri et al., 2018).

To overcome these limitations, MPUF strategies have emerged in IC field. MPUF strategy is a new PUF design paradigm that utilizes several different lightweight PUFs as design components and combines them according to certain rules to become a cost-effective composite PUF (Ebrahimabadi et al., 2021). The MPUF strategy usually causes the response of one PUF to obfuscate the response of another PUF

in a non-linear manner, making it necessary for an attacker to attack the combination of multiple different PUFs through the combination of multiple PUF instances, which can significantly improve the resistance to modeling attacks (Cui et al., 2020). By using PUFs with low resource overhead as components, MPUF policies do not occupy too much on-chip resources during execution. At the same time, the effect of noise can be averaged out, thus improving the stability of its performance.

In the IC field, various combinations of multi-PUF strategies have been developed and used to enhance IP protection. In the field of biochip IP protection, MPUF is also expected to improve the resistance to modeling attacks. The combination of advanced fluidic manipulation based on MEDA biochips with MPUF is likely to develop finer-grained and more advanced IP protection strategies.

2.4. Previous work

As a next-generation microfluidic biochemical experimental platform, the medical and market value of MEDA biochips is undoubtedly enormous, but its IP protection still needs to be further explored. In this regard, some advanced IP protection strategies have recently been proposed to counter the threat of IP piracy.

Watermarking: In Shayan et al. (2019), by taking advantage of the inherent variability of the parameters, the authors proposed an integer linear programming-based DMFB watermarking solution, which can insert the secret signature of the copyright owner into the parameters of the biochemical protocol. This solution is also applicable to MEDA, but it can only be used to prove copyright ownership and cannot defend against piracy attacks.

Logical encryption: In Bhattacharjee et al. (2019), the authors "lock" the biochemical assay by inserting virtual "mixing-splitting" operations into the original biochemical protocol in order to blur the number of "mixing-splitting" operations. The original biochemical assay can be executed correctly only if the correct secret key is obtained, otherwise the assay results will be incorrect due to the execution of additional virtual "mixing-splitting" operations. In Dong et al. (2021), an IP-protection method called MEDASec was developed. This method logically encrypts the "mixing-splitting" operation and introduces a key-coupled enhancement circuit module for increased attack resistance. However, for the solutions in Dong et al. (2021) and Bhattacharjee et al. (2019), once an attacker obtains the key as a legitimate user, then the biochemical protocol can be executed on a pirated biochip.

PUF: In Hsieh et al. (2017), they introduced PUFs that exploit the inherent manufacturing differences of the electrodes to generate keys and insert additional finite state machines (FSMs) to lock the DMFBs. However, when the electrodes are severely degraded, an authorized user may not be able to authenticate the user and a single-PUF is more susceptible to modeling attacks (Lin et al., 2018).

In summary, there are still some issues to be resolved with respect to IP protection in MEDA. In particular, existing methods do not provide a good defense against IP piracy when the authorized user is a potential attacker. In order to cope with this situation, this work develops an IP protection strategy for MEDA biochips called bioMPUF. The aim is to fully utilize the advantages of MPUF to provide a low-cost and effective protection solution for the IP of MEDA biochips and to introduce countermeasures to proactively fight against biochip piracy.

3. Threat and motivation

Before introducing BioMPUF, a brief description of the threat model of MEDA biochip IP is presented. Then, the motivation for this study is revealed.

3.1. Threat model

The impact of pirated MEDA biochips is undoubtedly huge. Once pirated MEDA biochips enter the market, they can be purchased by unsuspecting consumers. Pirated biochips may be tampered with by attackers or their commissioned foundries, and their performance and reliability are often not guaranteed, resulting in potentially erroneous or inaccurate results or malfunctions. As the appearance of pirated biochips is highly similar to that of genuine biochips, the companies concerned will not only suffer financial losses, but also lose the trust of users, which will result in reputational damage (Jin et al., 2023).

In order to further explain the significance of this work more clearly, here, two threat models that this IP protection work may face are discussed.

Reverse Engineering Attack: The threat model of reverse engineering attack on MEDA biochip IP is shown in Fig. 3. In this paper, the MEDA biochip vendors and the bioprotocol designers are assumed to be trustworthy and will not leak any confidential information proactively. Malicious actors may come from end-users, who have access to the entities of biochips (Chen et al., 2020). The attacker first analyzes an authorized MEDA biochip through reverse engineering, then intercepts internal signals as well as employs side-channel attacks to infer IP authentication details. Through logic analysis, simulation and emulation, the attacker attempted to emulate the authentication process and generate a similar counterfeit biochip. Eventually, the attackers succeeded in creating counterfeit biochips with appearance and functionality similar to the genuine biochip, which could be used for unauthorized purposes. The motivation of attackers could be a financial benefit, harming others, technology acquisition, etc.

ML-Based Modeling Attack: The ML-based modeling attack is achieved by constructing a challenge–response model of the MEDA biochip. This attack aims to utilize the output of PUF to construct a model to predict the behavior of PUF in order to disrupt its non-clonable nature. In general, the modeling process consists of two main phases: preprocessing and learning, as shown in Fig. 4. The known CRPs will be used to train the model to predict the response to a given challenge (Aseeri et al., 2018; Mills et al., 2021). First, the input challenges are preprocessed, and then the model is trained using machine learning methods Model evaluation is performed after successful completion of training. Commonly used machine learning models include linear regression (LR), support vector machines (SVM), neural networks (NN) etc (Cui et al., 2020; Ebrahimabadi et al., 2021; Ucci et al., 2019).

As field-programmable devices, MEDA biochips have the ability to achieve many bio-protocols within an identical structure (Zhong et al., 2018). Thus, the authorized devices will request the appropriate biochemical assay for different purposes. However, in order to reduce cost, attackers will not establish corresponding bioassay libraries for counterfeit MEDA biochips. Instead, they may link the pirated biochip with an authorized bioassay library to obtain the results of an existing biochemical protocol assay. This type of attack greatly reduces the cost and technical difficulty of biochip piracy. Moreover, only in a few cases of copyright disputes, the attacker (pirate) may face the risk of legal sanctions. The existing defense methods do not enforce countermeasures against the pirates, which allows the attackers to obtain huge financial rewards with only little investment.

3.2. Motivation

As biochips are widely used in biology, medicine, and other fields, protecting their IP security and trustworthiness becomes critical. In order to address the scenario described in the above threat model, this paper proposes a defense against MEDA biochip piracy and countermeasures to ensure the security and reliability of the devices. To better understand why there is a need to explore new defense strategies, the motivations for this work are discussed below:

Defensing Against Piracy Attacks: Due to the specificity of the process and materials used to manufacture MEDA biochips, there is a greater chance that an attacker could attack the IP of the device through reverse engineering and simulation, etc. Existing DMFB's IP protection technology cannot be directly applied to MEDA's IP protection. The fact that potential attackers may be licensed end-users further

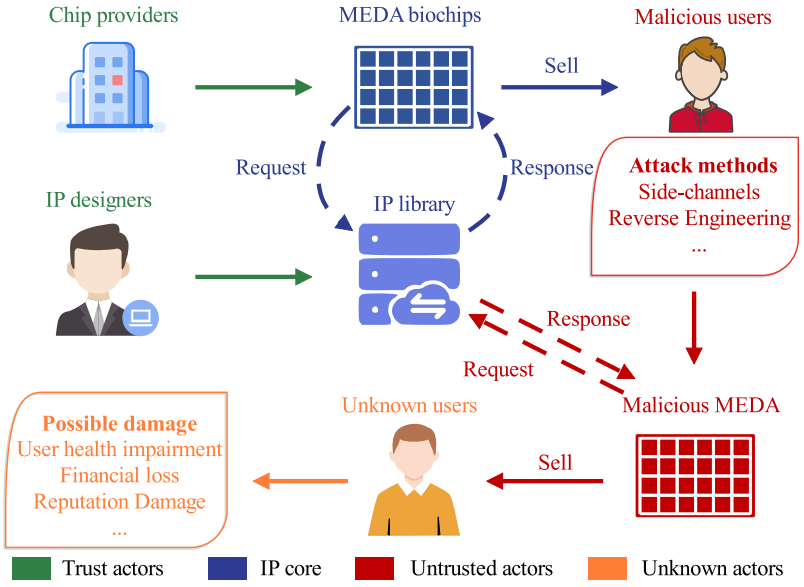

Fig. 3. The reverse engineering threat model for MEDA biochips. End users are potential attackers who can crack the IP of authorized MEDA biochips through reverse engineering, so as to manufacture counterfeit biochips and sell them to other users.

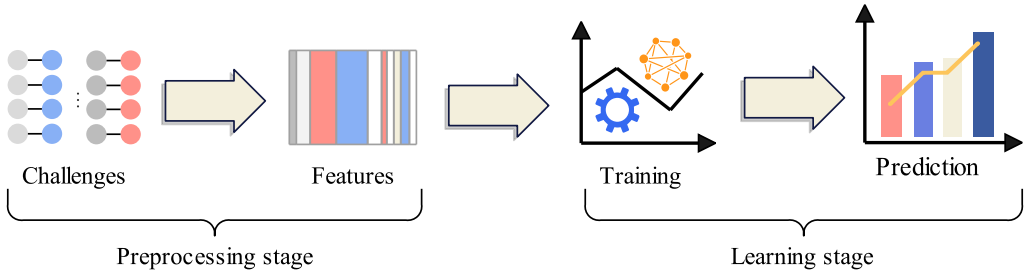

Fig. 4. A general procedure for performing a modeling attack on PUF. In the preprocessing stage, after preprocessing the collected training set, it is input to the learning stage to train the ML model and evaluate its performance.

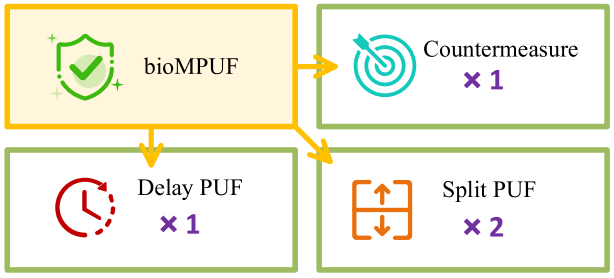

Fig. 5. Components overview of BioMPUF. It consists of a delayed PUF, two split PUFs, and a countermeasure against piracy.

emphasizes the difficulty and need for more robust protection strategies. **Countering Piracy Attacks**: Although a number of advanced defense techniques have recently been proposed that could be effective in improving the security of biochip intellectual property. However, it is difficult to achieve complete defense, especially against strong-willed attackers. Defenders are often in a passive position once IPR is successfully pirated or attacked, and there are limitations in that pirates can only be punished through legal channels in the event of a copyright dispute. Therefore, it is necessary to consider more flexible defense strategies that can be proactively countered to minimize losses after an attack.

Enhancing Security with Multi-PUF: While PUF is physically unclonable, it is not unclonable at the mathematical level. It has been shown that CRPs of the PUF can be cracked by machine learning modeling methods. The single PUF protection strategy may be inadequate in terms of security for biochip IP protection. Multi-PUF protection strategies have been shown to have higher security in the field of IP protection for ICs (Kokila and Ramasubramanian, 2019), and can effectively resist ML-based modeling attacks while maintaining performance.

Against this background, this work aims to propose a novel IP protection strategy for biochips to address the challenges faced. This work will explore the potential benefits of implementing a multi-PUF protection strategy and how proactive countermeasures can be taken to improve IP security after an attack has occurred. By understanding the limitations and challenges of existing approaches, this work derives the motivation for the research to open up new research ideas for IP protection of MEDA biochips by addressing these issues and proposing more effective MEDA biochip IP protection strategies that can respond to and counterattack the actions of attackers.

4. Overview of BioMPUF

Due to sensitive sensing systems and fine-grained operations, responses of PUFs on MEDA biochips can be captured more accurately than those on DMFBs (Liang et al., 2020). Accordingly, PUFs technology will emerge as a promising measure of IP protection for MEDA biochips. In this section, a novel design paradigm for PUFs on MEDA biochips is presented, which is constructed by several single PUFs and called bioMPUF. Then, its overall workflow is described.

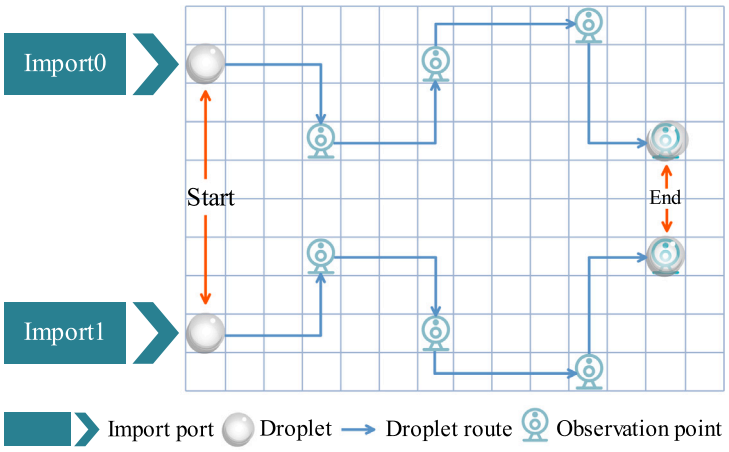

Fig. 6. Illustrations of delay PUFs. A delay PUF uses the delay difference between two droplets with the same path to define the challenges, and several observation points on the path are used to record the order of droplet arrival, i.e. delay.

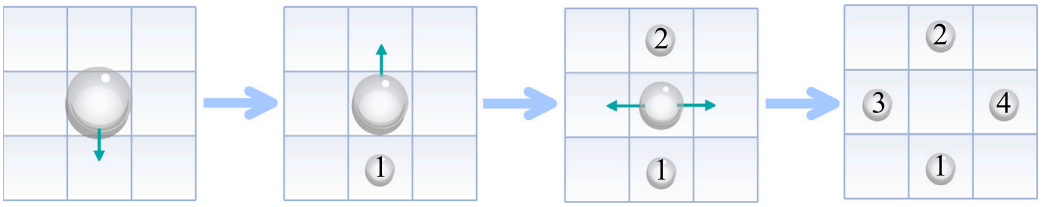

Fig. 7. Illustrations of split PUFs. This split PUF uses the volume difference between two droplets of the same droplet to define the challenges.

4.1. The overall framework of BioMPUF

The bioMPUF in this paper consists of a delay PUF and two split PUFs, and provides a countermeasure that can destroy the pirated MEDA biochips, as shown in Fig. 5. In bioMPUF, challenges are composed of routes and split operations of droplets, and responses will be generated based on information captured by sensors integrated with MCs on MEDA biochips.

Delay PUF: The delay PUF in MEDA biochip utilize the delay difference of two droplets that have identical paths. As shown in Fig. 6, the droplet D_0 is dispensed by the $import_0$, and the other one, D_1, is derived from the $import_1$. Depending on the inherent fabricating difference in each electrode, D_0 and D_1 travel in the same routes but will not arrive at goal electrodes simultaneously. Hence, the paths of droplets can be defined as challenges of the delay PUFs.

Split PUF: The split PUFs have leveraged the volume difference between two droplets, deriving from an identical droplet. As shown in Fig. 7, the droplet D is split into droplets D_0 and D_1, defined as the challenge of split PUF. Since the size of droplets will not be identical for each splitting, different responses will be produced according to inevitable differences.

Countermeasure: The countermeasure is a measure taken by the system that will cause harm to attackers while defending against attacks. In previous work, PUFs implemented on DMFBs and MEDA biochips can only be utilized to protect IPs without any impact on pirated devices. In bioMPUF, once the pirated MEDA biochip is detected, the countermeasure will be launched and offer an actuation sequence with high overhead to the pirated biochip, thus accelerating degradation for electrodes on the chip.

The bioMPUF strategy is based on a multi-PUF design paradigm that exploits the inherent manufacturing differences of MEDA biochips to obtain PUF responses that can be used to verify the legitimacy of the biochip. In this work, the primary focus is on harnessing the advantages of MEDA's sensitive sensing system and fine-grained operations to develop efficient PUF security technologies. Currently, exploration into other advanced features of the MEDA biochip, such as its support for flexible droplet sizes, has not been undertaken. In addition to the basic authentication function of PUF, bioMPUF also contains the first anti-piracy attack measure for MEDA biochips, which can reduce the experimental accuracy and lifetime of the biochip without touching the pirated biochip. By combining these three components, not only can the anti-piracy capability of MEDA Biochip intellectual property be effectively enhanced, but also the counter-attack against pirated MEDA biochips can be carried out. How the three components work together is described in the next subsection.

4.2. The overall workflow of BioMPUF

Fig. 8 illustrates the detailed workflow of the proposed bioMPUF, which can be roughly divided into three stages, i.e., standard CRP database construction, authentication, and triggering anti-attack countermeasure. The main tasks of each stage are described below.

Stage 1. Construction of standard CRP database

Step 1. The designer designs challenge C for the MEDA biochip. This challenge contains a Delay PUF challenge C_D and a Spit PUF challenge C_S.

Step 2. The challenge C_D is performed on this unsold MEDA biochip to generate the response R_D, and the challenge C_S is performed to generate the response R_S.

Step 3. After receiving the response, the biochip controller performs an obfuscation operation on R_D and R_S to get the golden response R_G.

Step 4. The gold response R_G is stored in the CRP database, forming a CRP with the corresponding challenge C. The CPR will be used for Stage **3** responses matching.

Stage 2. Authentication

Step 5. Before a user can use this MEDA biochip, authentication is required to gain access to the actuation sequences. The external controller of the biochip sends a request to the service provider to obtain the biochemical protocol, the request information includes license information, protocol name, etc.

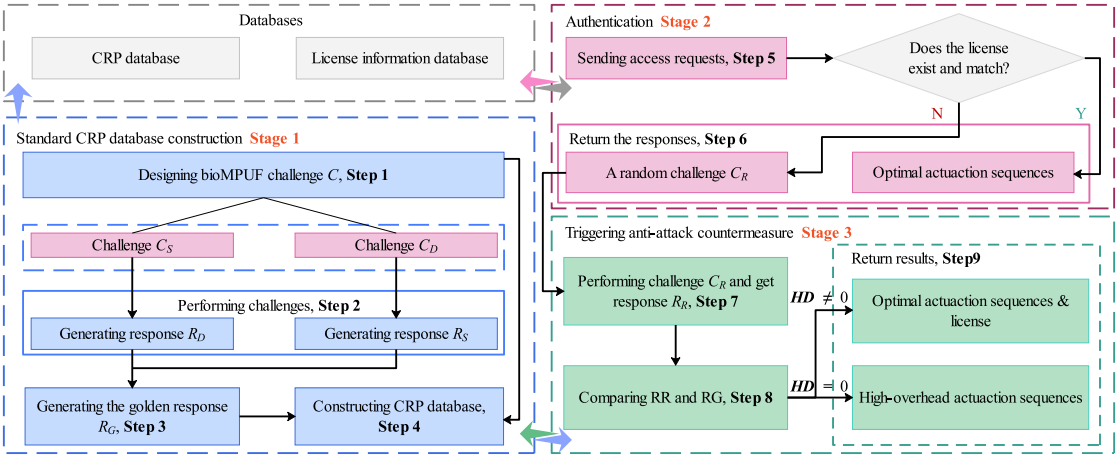

Fig. 8. The workflow for implementing bioMPUF on MEDA biochips to combat IP piracy. It consists of three main stages: standard CRP database construction, authentication, and triggering anti-attack countermeasure.

Step 6. After receiving the request from the biochip, the service provider first determines whether the chip is a genuine biochip based on the request information. If it is a licensed biochip, the optimal actuation sequence is returned and the flow ends; otherwise, a random challenge C_R is returned and the request goes to Stage **3**.

Stage 3. Countermeasure of triggering anti-attack

Step 7. The MEDA biochip performs the received challenge C_R and returns the obtained response R_R to the service provider for the next validation step.

Step 8. The service provider compares the response R_R returned by the biochip with the standard response R_G in the database and calculates the Hamming distance HD between the two.

Step 9. If $HD = 0$, it means that the biochip is a genuine biochip, the service provider returns the optimal actuation sequences and unique license code, and this request ends. If $HD \neq 0$, the anti-attack mechanism of bioMPUF will be activated, and the actuation sequences with high overhead will be returned, and the flow is over.

In bioMPUF, only the biochip that has not passed the authentication will trigger the anti-attack measures, while the legitimate biochip will obtain a license code after passing the first authentication, which replaces the PUF authentication as the legitimacy proof of the biochip, thus reducing the biochip loss due to the authentication.

5. The BioMPUF on MEDA

This section describes the detailed design of bioMPUF on MEDA, including the Delay PUF, the Split PUF and the countermeasure.

5.1. The delay PUF in BioMPUF

The Delay PUF in MEDA biochips works by causing a pair of droplets to move a symmetrical route, and due to inherent manufacturing differences in the electrodes, each droplet does not take the same amount of time to move an equal distance, which is the time delay of the droplet pair. Since droplet volume is critical to travel time, delay PUF needs to be performed as the first step in the bioMPUF implementation process. As paths of test droplets D_0 and D_1 dispensing from $import_0$ and $import_1$ are challenges for delay PUFs, q ($q \in Z^+$, q is even number) observation points are evenly set in each path to produce $q-$bit responses, as illustrated in Fig. 6. If D_0 reaches the goal electrode firstly, a 1-bit response "0" will be output. Conversely, if the D_0 is not faster than the D_1, response "1" will be obtained. Moreover, n ($n \in Z^+$) cycles of delay PUFs will be executed on a MEDA biochip. Accordingly, $R_D^i = (a_1^i, a_2^i, \ldots, a_q^i)$ is introduced that denotes the delay PUF response of the ith pair of droplets after passing through all observation points. a_m^i ($m = 1, 2, \ldots, q$, $i = 1, 2, \ldots, n$) from R_D^i is determined as

$$a_m^i = \begin{cases} 0, & \text{if } t_{m0}^i \leq t_{m1}^i \\ 1, & \text{if } t_{m0}^i > t_{m1}^i \end{cases} \tag{2}$$

where a_m^i denotes the response of the ith pair of droplets at the mth observation point, t_{m0}^i and t_{m1}^i mean the time taken for the ith pair of droplets dispensed by $import_0$ and $import_1$ from the initial position to the mth observation point, respectively. Hence, there is $q \times n$-bit response which will be output in a delay PUF.

Example 1. As shown in Fig. 9, droplets D_0 and D_1 are emitted from the distribution ports $import_0$ and $import_1$ are emitted. The droplet pair reaches the destination electrodes E_0 and E_1 through the path indicated by the orange arrows. There is also an observation point, O_0 and O_1, respectively, on the droplet path, which, together with the destination electrodes, form a system of observation points for the time-delayed PUF. According to Fig. 9, at the observation points O_0 and O_1, D_0 arrives before D_1, while at the destination electrode, D_1 leads. In this case $q = 2$, and according to Eq. (2), $R_D = 01$.

5.2. The split PUF in BioMPUF

The Split PUF of bioMPUF takes advantage of the difference between the volumes of droplets after performing the splitting operation to design the CRPs of PUF. Due to the different biochips, or the different locations where the splitting operation is performed, there will be a certain degree of volume difference between the droplets split uniformly from the same droplet. Each pair of droplets will be split to accomplish split PUFs after each cycle of delay PUF. There are q droplets that are split from each original droplet. Depending on the order of splitting, these droplets can be denoted by a set $D = \{d_1, d_2, \ldots, d_q\}$. Since sensing systems cannot guarantee that the droplet volume will be exactly the same as the standard volume in each execution cycle, the bias derived by sensors is one of the elements to be considered in the response design. For the purpose of enhancing fault tolerance, the coupling between droplets should be reduced. Hence, responses in the proposed split PUFs are generated by comparing the volume difference between two droplets adjacent to each other in the set D and each droplet participates only once in the comparison.

Depending on volume difference of droplets, $R_S^{ij} = (b_1^{ij}, b_2^{ij}, \ldots, b_q^{ij})$ is introduced that indicates the split PUFs response of the ith pair of droplets dispensed by $import_j (j \in \{0, 1\})$. $b_{2u-1}^{ij}, b_{2u}^{ij}$ ($u = 1, 2, \ldots, \frac{q}{2}$,

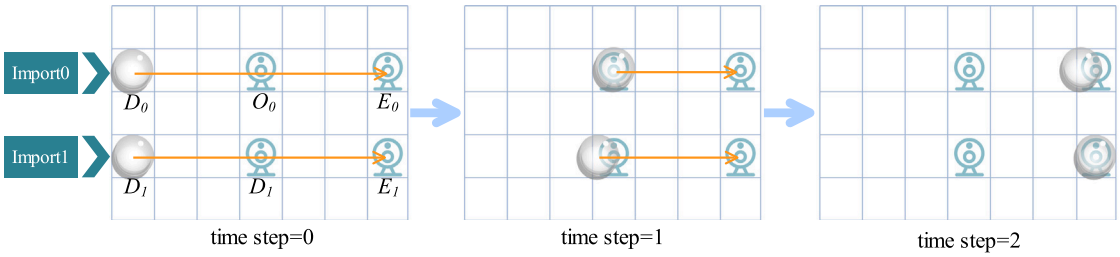

Fig. 9. An example of generating a response for delay PUF. The two droplets are dispensed by two ports respectively, and are routed to the terminal along the orange line, and there are two observation points on each path.

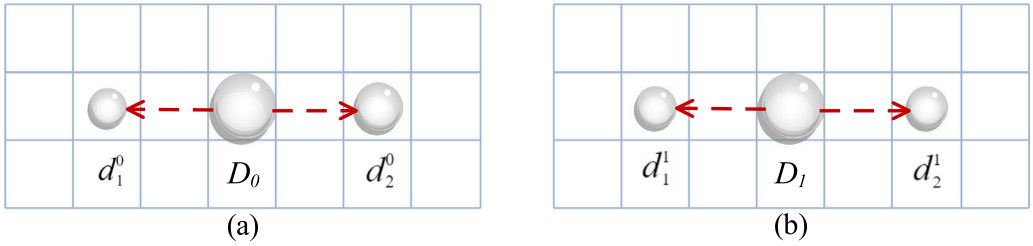

Fig. 10. After the delay PUF shown in Fig. 9 is completed, a split PUF is executed. The volume size relationship between the two sub-droplets d_1^0 and d_2^0 from the first droplet is, $V_1^0 < V_2^0$, while the two sub-droplets split from the second droplet have the same volume.

$i = 1, 2, \ldots, n$) from R_S^{ij} is calculated as

$$b_{2u-1}^{ij}, b_{2u}^{ij} = \begin{cases} 01, & V_{2u-1}^{ij} > V_{2u}^{ij} \\ 10, & V_{2u-1}^{ij} < V_{2u}^{ij} \\ 11, & V_{2u-1}^{ij} = V_{2u}^{ij} \\ 00, & otherwise \end{cases} \tag{3}$$

where V_{2u-1}^{ij} and V_{2u}^{ij} present the volumes of the d_{2u-1} and d_{2u} deriving from the D_j in the ith pair of droplets, respectively. "01" means that volume of D_{2u-1} is larger than the D_{2u}. "10" indicates that the converse situation of "01". The equal volumes of D_{2u-1} and D_{2u} are denoted by "11". In addition, *otherwise*, which is presented by "00", indicates other states that are different from the above, such as droplet absence. Therefore, $2q \times n$-bit response will be output in a split PUF.

In split PUFs, however, since there are two responses that will be generated in each cycle, they need to be pre-processed to combine into a response for the current cycle in split PUFs. R_S^i, which is seen as the response of the current cycle in split PUFs, is obtained as

$$R_S^i = R_S^{i0} \times R_S^{i1} \ mod \ 2^Q \tag{4}$$

$$Q = \frac{BN}{n} \tag{5}$$

where Q determines the bit counts of responses, BN is the bit number of final responses, and n is the number of cycles included in the IP verification process.

Example 2. In Fig. 10, it can be observed that the droplet, after completing the delay PUF in Fig. 9, accomplishes the split PUF within one cycle. Since the droplet only passes through two observation points on the delay PUF to get a 2-bit response, the droplet only needs to perform splitting once in the split PUF, and $BN = 2$. d_1^0 and d_2^0 of the sub-droplets split by D_0 correspond to the volume relationship of $V_1^0 < V_2^0$, and thus according to Eq. (3). The split PUF response of D_0 is $R_S^0 = 10$; on the other hand, the sub-droplets d_1^1 and d_2^1 split by D_1 correspond to the volume relationship of $V_1^1 = V_2^1$, and its corresponding response is $R_S^1 = 11$. Then, according to Eq. (4), $R_S = R_S^0 \times R_S^1 \ mod \ 2^2$, i.e., $R_S = 10$.

5.3. Error analysis

This work is centered on the security of the system. To streamline the problem, an assumption is made that the droplets involved in the delay PUF are of identical size, enabling a more focused discussion on pertinent security issues. In practical applications, when dispensing droplets of uniform size, there exists a minimal potential volume discrepancy (within ±1% unit volume (Poddar et al., 2020)). Drawing from prior research on the relationship between droplet velocity and size (Li et al., 2017), it is observed that within a specific size range, the rate of change in droplet velocity is relatively low, and the speed difference induced by a 1% volume disparity is generally below 1%. For instance, for a 10 × 10 droplet, when the volume increases by 44% (to 12 × 12), the velocity decreases by approximately 14% (about 0.01 mm/s). Based on (Hsieh et al., 2017), two single PUFs, namely Route PUF and Split PUF, were proposed. In addition, Lin et al. (2018) successfully developed a PUF-based security protection system for DMFBs. Minor errors in the design of PUFs on biochips are tolerable. For the sake of discussing security in this paper, the routing time error resulting from dispensing error is considered acceptable within the set minimum value ε. Due to limitations in industrial experience, this paper opts to designate ε as an empirical value, adjustable based on specific scenarios.

To further tackle the allocation error scenario, preprocessing is conducted before the droplets initiate. This preprocessing phase capitalizes on the advantages of the MEDA by using multiple-unit volume droplets to control volume errors within a more confined range. Specifically, for a liquid droplet with dimensions of length $l_{droplet}$ and width $w_{droplet}$, the maximum relative volume error EV_{Max} induced by the maximum dispensing error ED_{Max} can be described by Eq. (6).

$$EV_{Max} = \frac{ED_{Max}}{l_{droplet} \times w_{droplet}} \tag{6}$$

Since the maximum absolute allocation error is fixed, i.e., ED_{Max} is 1%, the impact of dispensing errors is smaller for larger droplets. For instance, for a 1 × 1 droplet, the maximum volume error generated by the dispensing operation is 1%. However, for a 3 × 3 droplet, the volume error is within 1/9%. Subsequently, both droplets are routed simultaneously along the specified path to accurately assess the performance of the delay PUF.

In general, considering the profits from piracy, the manufacturing process used for genuine MEDA biochips is comparatively more sophisticated than the process for manufacturing pirated biochips. The electrode performance is more stable, and the probability of obtaining different results when executing PUF multiple times is relatively low. However, during the actual execution of PUF, there is still a small probability that the responses generated by the user-side execution of delay PUF and split PUF may differ from the golden response. To mitigate the sensitivity of bioPUF to errors, this paper introduces a response error threshold in Section 5.5. When this response is not entirely identical to the golden response, it is initially identified as a suspected pirated biochip. However, through comparison with the threshold, it is finally determined whether the biochip is a pirated one.

5.4. Response length design

For PUFs, the length of the response is closely related to the IP security of the biochip. In general, the longer and more complex the response, the less likely it is to be cracked and the more secure it is. However, in practice, a highly secure PUF design is not suitable for every application. Especially in MEDA biochips, if certain electrodes on the biochip are activated too much during PUF validation, it may lead to accelerated degradation of these electrodes and shorten the biochip lifetime. In addition, both the manufacturing cost and the usage cost of biochips are important considerations for developers. Therefore, the response length of bioMPUF is not predetermined, and developers should consider the following limitations in order to formulate the appropriate length according to the actual needs.

5.4.1. Security

If high security is required, it is a suitable candidate that each MEDA biochip corresponds to a unique response of PUF. s_1 denotes the minimum number of bits needed in the mode. s_1 can be obtained as

$$s_1 = \lceil log_2 tal \rceil \tag{7}$$

where $tal \in Z^+$ indicates the number of MEDA biochips.

5.4.2. Lifespan

The lifespan of MEDA biochip depends on the number of times the electrodes are activated (Elfar et al., 2021). Accordingly, if MEDA biochip lifespan loss reduction in the IP verification is required, part of repeating responses should be allowed while ensuring that attackers hardly obtain real responses by brute force attacks. The minimum number of bits needed in the mode is presented by s_2, which can be acquired as

$$s_2 = \lceil log_2 act \rceil \tag{8}$$

where $act \in Z^+$ means the number of activations of a single electrode.

5.4.3. Space

The size of MEDA biochip is an essential factor that impacts the scale for challenges of delay PUFs. Normally, in a small MEDA biochip, routes of droplets will be shorter than a larger biochip so that the number of observation points will also decrease. s_3 is assumed as the area ratio of the current MEDA biochip to the maximum one. s_3 is defined as

$$s_3 = \frac{l \times w}{A_{max}}, \quad 0 < l \times w < A_{max} \tag{9}$$

where A_{max} denotes the area of the maximum MEDA biochip, and $l \in Z^+$ and $w \in Z^+$ indicate the length and width of the MEDA biochip, respectively.

5.4.4. Manufacturing cost

If the manufacturing cost of MEDA biochips is restricted, compared with biochips owning adequate budget, the number of IP verified cycles in the current biochip will be reduced in order not to consume excessive resource on-chip. s_4 presents the cost ratio of the current MEDA biochip to the maximum one. s_4 is expressed as

$$s_4 = \frac{cost}{C_{max}}, \quad 0 < cost \le C_{max} \tag{10}$$

where the cost of current biochip is represented as $cost$, and C_{max} indicates the maximum manufacturing cost of MEDA biochips.

In general, the pursuit of heightened uniqueness often necessitates more frequent activation of electrodes or sensors on the MEDA biochip, consequently leading to a reduction in the biochip's lifespan. To some extent, the mathematical complementarity between uniqueness and biochip lifespan is evident, prompting designers to delicately balance these factors. In addition, the path length of the delay PUF's droplets and the number of observation points are influenced by the size of the MEDA biochip. Larger MEDA biochips typically require more checkpoints and longer testing paths. As the size of the MEDA increases, the deployment of observation points also increases, implying an associated increase in manufacturing costs. If manufacturing costs are constrained, it becomes necessary to appropriately reduce the authentication cycle to avoid excessive on-chip resource consumption. In essence, designers must balance the impact of the size and manufacturing cost constraints of the MEDA biochip on the final response length. Hence, the bit number of responses can be formulated as

$$BN = \left(c_1 s_1 + c_2 s_2\right) \times \left[1 + \left(c_3 s_3 + c_4 s_4\right)\right] \tag{11}$$

$$c_1 + c_2 = 1, c_1 \in \{0, 1\}, c_2 \in \{0, 1\} \tag{12}$$

$$c_3 + c_4 = 1, c_3 \in [0, 1], c_4 \in [0, 1] \tag{13}$$

where c_i is the weight of each factor s_i $(i = 1, 2, 3, 4)$. Designers can determine c_i depending on the security requirements of MEDA biochips on various scenes.

Since the response of delay PUF R_D^i does not need to be preprocessed, it can participate in calculation directly. Hence, after two responses within split PUFs have been combined into a response, the final response R can be acquired by this response and the response of delay PUF as follows

$$R = R_D^i \oplus R_S^i \tag{14}$$

Here, the computation generating the final response can be customized by the designer according to security level requirements. Its primary purpose is to prevent ML modeling attacks. The choice of using the XOR operation is motivated by the fact that current ML methods employed for modeling attacks on PUFs predominantly rely on traditional linear classifiers. The XOR operation is introduced here to effectively disrupt the functionality of traditional linear classifiers or regressors, thereby enhancing resistance against modeling attacks based on traditional ML methods.

5.5. The countermeasure of IP piracy

The Countermeasure of anti-piracy attack is one of the key components of bioMPUF and is the first countermeasure for MEDA biochips to harm pirated devices. The measure is triggered when the biochip returns a response R that differs from the standard response R_G in the database. The MEDA biochip electrodes have a maximum number of activations N, and some commonly used electrodes are rendered useless once they reach the limit of their use. For example, if one of the electrodes cannot be activated while a droplet is performing a dilution operation, the dilution operation of the droplet fails, which means that even if the subsequent operations are performed normally, an erroneous result will be obtained in the end.

Based on this characteristic, the counter-attack measure proposed in this paper accelerates the aging of electrodes by returning a high overhead driving sequence corresponding to the biochemical protocol

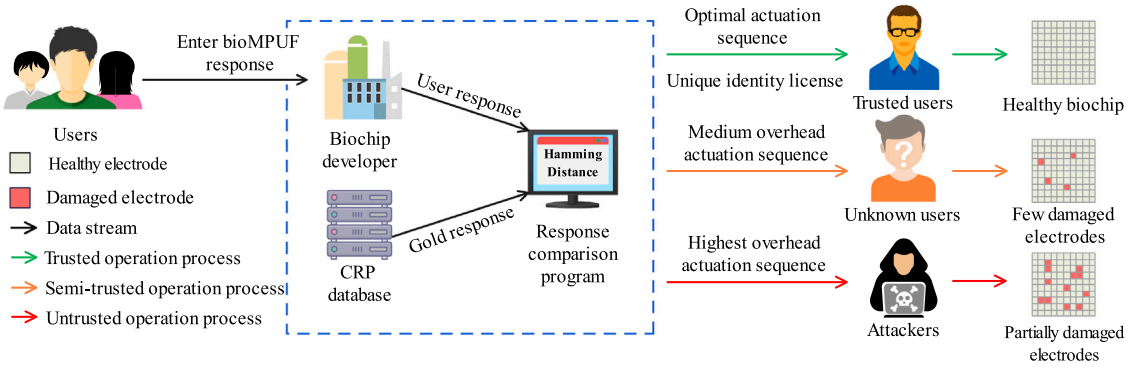

Fig. 11. A workflow of BioMPUF's countermeasures against piracy attacks to counteract piracy. The service provider compares the response R obtained from the execution of challenge C by the biochip with the golden response R_G in the database. Then, based on the comparison result, it chooses to return the driver sequence with different overheads to ensure the normal operation of the licensed biochip or accelerate the aging of the pirated biochip.

to the suspected pirated biochip, thus activating certain electrodes of the biochip multiple times. The measure returns driver sequences with different overheads to different biochips by determining the degree of suspected piracy through the Hamming distance. Since the service provider still provides the driver sequence, users of pirated biochips think that they have bypassed the service provider's detection, thus making it difficult to detect the difference between the current sequence and the normal sequence. This measure can shorten the lifespan of pirated biochips to varying degrees without requiring access to the pirated biochips.

Fig. 11 shows the complete flow of the proposed countermeasure against IP piracy, and the main steps are as follows.

Step 1. Calculate the hamming distance (HD) between the response R of the MEDA biochip and the standard response R_G in the CRP database. $HD(R, R_G)$ is formulated as

$$HD(R, R_G) = \sum_{i=1}^{n} R(i) \oplus R_G(i) \tag{15}$$

where $i(i = 1, 2, \ldots, n)$ is the serial number of components in R and R_G. Depending on the value of HD, the IP of MEDA biochip can be determined whether it is authorized or not. If $HD = 0$, then go to the next step, otherwise skip to Step **3**.

Step 2. If $HD = 0$, since R and R_G are exactly identical, the biochip copyright can be considered as authorized. Accordingly, the IP provider will return an optimal actuation sequence and a unique identity license to the MEDA biochip. Thus, IP providers can recognize MEDA biochips by identity license instead of PUF verifying. The validation flow is completed.

Step 3. If $0 < HD(R, R_G) \leq HD_{threshold}$, then go to the next step, otherwise go to Step **5**. $HD(R, R_G)$ is formulated as

$$HD_{threshold} = len(R) \times p_E \tag{16}$$

where, p_E is the threshold error probability. p_E is defined such that MEDA biochips can be identified as unauthorized if and only if the ratio of response error to response length $len(R)$ exceeds it.

Step 4. When $0 < HD(R, R_G) \leq HD_{threshold}$, since differences between R and R_G is less than p_E, the MEDA biochip will not be considered as an unauthorized device. Thus, the IP provider will return an actuation sequence with medium overhead. If the biochip is verified successfully in the subsequent PUF verification, it can be regarded as an authorized device. The validation flow ends.

Step 5. When $HD(R, R_G) > HD_{threshold}$, comparing with above, the MEDA biochip can be judged as a pirated device. Accordingly, the IP provider will send back the actuation sequence with the highest overhead. The validation flow ends.

Due to the overhead of the actuation sequence including time, reagents, lifespan, etc., performing the actuation sequence with maximum overhead on a pirated biochip will lead to shrunk lifespan, wasted reagents, abnormal results, etc. According to the findings in Liang (2021) and Elfar et al. (2021), an exploration of the relationship between electrode degradation and the number of activations was conducted, which could be described by Eq. (17).

$$D_{ij}^{(N_{act})} \approx \tau^{N_{act}/q} \in [0, 1] \tag{17}$$

where D_{ij} is the electrode degradation function, $\tau \in [0.5, 0.7]$ and q are aging parameters, N_{act} is the number of times the electrode has been activated. Based on the experiments in Elfar et al. (2021), at $\tau = 0.5$, $q = 200$, the electrode degrades approximately 30% after around 100 activations and 50% after around 200 activations. For unauthorized pirated biochips, it is necessary to execute a high-cost actuation sequence to activate more MCs, thereby shortening the biochip's lifespan. Additionally, unauthorized MEDA biochips require further validation during subsequent use, and the process incurs additional reagent costs. The countermeasure is designed to disrupt the availability of pirated MEDA biochips, thus causing financial losses to attackers.

6. Experiments and analysis

In this section, experiments and security analyses are performed with the aim of evaluating the overall security of the proposed bioMPUF on MEDA biochips. Specifically, the bioMPUF is compared with single-PUF in controlled experiments, demonstrating that the bioMPUF has higher security. In addition, the security and effectiveness of bioMPUF is further demonstrated against common attacks in Section 6.4.

6.1. Experimental setting

This experiment uses a C++ program to simulate the proposed bioMPUF strategy. The experiment is implemented by a computer with 16 GB of RAM and a 3.60 GHz Intel Core i5 processor running a 64-bit Windows 10 operating system. Since different bit responses correspond to different security, the performance of bioMPUF is evaluated in terms of uniqueness rate, incorrect determination rate (IDR) and resistance to modeling attacks by taking 8-bit, 12-bit, 16-bit, 18-bit, and 24-bit responses and assigning them a CRP sample set of 1000, 5000, 10,000, 25,000 and 50,000 records, respectively.

6.2. Evaluation metrics

In order to better evaluate the effectiveness of bioMPUF, several evaluation metrics are discussed in this subsection.

6.2.1. Uniqueness rate

The uniqueness rate refers to the proportion of the total number of biochips in the same batch of MEDA biochips where the response

Table 1
Uniqueness of single PUFs with different lengths on different sample sizes.

No. of biochips	12-bit			16-bit			18-bit			24-bit		
	Min	Max	Avg	Min	Max	Avg	Min	Max	Avg	Min	Max	Avg
1000	70.1	76.2	72.39	92.5	99.5	97.12	96.6	99.2	98.06	100	100	100
5000	20.78	23.84	22.51	87.48	90.38	89.36	89.92	91.9	90.26	99.72	100	99.94
10 000	–	–	–	78.18	80.52	79.22	80.25	83.15	81.65	99.76	99.9	99.82
25 000	–	–	–	50.64	53.29	52.52	60.18	61.74	61.15	99.45	99.73	99.60
50 000	–	–	–	19.95	21.8	22.67	37.66	38.53	38.10	98.74	99.08	98.86

* where the unit of Uniqueness rate is %, i.e. the unit of data in the table is %.

obtained from the same challenge operation is not duplicated, which reflects the uniqueness of the biochip response. The uniqueness rate U can be described as

$$U = (1 - \frac{N_d}{N_t}) \times 100\% \tag{18}$$

where N_t is the total number of biochips, and N_d is the number of chips in the same batch with duplicate responses. The higher the uniqueness rate, the lower the number of duplicate responses in the CRP sample set, which means the probability of the biochip being cracked by brute force attack decreases.

6.2.2. Incorrect determination rate

The IDR is the probability that the service provider mistakenly judges a pirated biochip as a licensed biochip or a licensed biochip as a suspected pirated biochip in the process of determining whether the biochip is genuine. The IDR can be described as

$$I_d = \frac{N_m}{N_t} \times 100\% \tag{19}$$

where, N_m is the number of misjudged biochips. If the IDR is high, the authority of the service provider will be questioned. In addition, a biochip that suffers from a misjudgment must be verified again by the PUF, which consumes the life of the biochip and the user's cost of use.

6.2.3. ML modeling prediction success rate

The ML modeling prediction success rate is the probability that an ML attack model successfully predicts a CRP sample from a MEDA biochip. The ML modeling prediction success rate does not mean that a higher rate indicates a worse performance of the bioMPUF, nor does a lower rate indicate a better performance of the bioMPUF, but rather that a probability closer to that of a random guess indicates a better performance of the bioMPUF. In theory, if an attacker gets enough CRP samples, they can peer into the patterns in the CRP samples with the help of machine learning modeling techniques to predict the responses corresponding to the challenges. This will undoubtedly pose a great threat to the security of PUF. Therefore, having sufficient resistance to modeling attacks is crucial for PUF.

In addition, this experiment introduces a single PUF as a control experiment in terms of unique rate and false positive rate.

6.3. Results and analysis

Given that the experimental design is aimed at validating the performance of security technologies and does not encompass other advanced features of the MEDA biochip, including its specific size and droplet sizes. This decision has been made to clearly focus on the core objectives of the study and streamline the complexity of the experiments. In conjunction with the evaluation metrics, this subsection analyzes the results of the following three sets of experiments.

Experiment 1: The higher the uniqueness rate, the lower the response repetition rate, resulting in higher security for CRP. Taking the delay single PUF as a reference, this experiment randomly generates challenges of different scales and lengths for bioMPUF. Subsequently, the final responses are obtained through computation to simulate the randomness of CRP in the chip manufacturing scenario. This process is repeated for 30 rounds to eliminate randomness. Tables 1 and 2 demonstrate the uniqueness of responses for single PUFs and bioMPUF, respectively. If there are a large number of duplicate responses in a CRP sample set, this implies that the corresponding MEDA biochip has an increased probability of being cracked by brute-force attacks.

Depending on Tables 1 and 2, when the length of response is 12 bits, the low uniqueness presents in both single PUFs and bioMPUF. As the 12-bit response can only satisfy 2^{12} possibilities, if the upper limit is exceeded, responses will duplicate on a large scale. In contrast, single PUFs and bioMPUF exhibit excellent uniqueness when the length of response is 24 bits.

Overall, the uniqueness of bioMPUF is better than that of single PUFs, especially in larger sample sets. This is because when the delay PUF is duplicated, the split PUF is not necessarily duplicated, which can reduce the possibility of duplication in the final response to a certain extent. For example, especially, in the 50,000 CRP sample set, the average uniqueness is 82.63% in bioMPUF, but is 38.10% in single PUF. Accordingly, compared with the single PUF, the bioMPUF can thwart brute force attacks better.

Experiment 2: During the execution of PUF verification procedures, discrepancies may arise between the behavior of droplets on the user's biochip and the behavior observed by the service provider during testing. Additionally, sensor systems might exhibit deviations, leading to differences between the actual response of the biochip and the standard response. In such cases, the service provider may identify the biochip as a suspected counterfeit based on $HD \neq 0$, which may include a small portion of legitimate biochips' verification requests. The IDR signifies the difficulty in recognizing one response as another. A high IDR raises questions about the credibility of IP ownership. Furthermore, biochips that undergo erroneous judgments must undergo PUF verification again, consuming both the biochip's lifespan and the user's operational costs.

Assuming that the error between the actual response and the standard response does not exceed 10%, it is considered an error judgment. In other words, the HD between the actual response and the standard response should be less than 10% of the length. Of course, the response error threshold can be set by the designer according to specific requirements. In each round of testing in this experiment, two challenges and their corresponding responses for a legitimate biochip were defined. Then, different sample sizes of CRP for both single PUF and bioMPUF were randomly generated to simulate suspected counterfeit chips. In this context, the challenge for the single PUF is the same as the delay PUF challenge in bioMPUF, and its response is directly derived from the challenge. The response of bioMPUF is calculated from two challenges. In practical scenarios, only a very small fraction of requests from suspected counterfeit chips may originate from legitimate biochips that failed to pass authentication due to errors, while the majority comes from counterfeit chips. Using a random approach to generate CRP simulates scenarios where suspected counterfeit biochips are more closely aligned with real-world applications.

This experiment conducted 30 rounds of simulated experiments for each response length and each sample size. Fig. 12 illustrates the IDR of bioMPUF and single PUFs at different response lengths and sample sizes. This includes the average IDR, as well as the best and worst-case IDR. It can be observed that, for both PUF and bioMPUF, the IDR

Table 2
Uniqueness of bioMPUF with different lengths on different sample sizes.

No. of biochips	12-bit			16-bit			18-bit			24-bit		
	Min	Max	Avg	Min	Max	Avg	Min	Max	Avg	Min	Max	Avg
1000	74.7	81.7	78.68	97.2	99.8	98.61	99	100	99.64	100	100	100
5000	28.36	30.7	29.55	91.72	94.12	92.75	97.4	98.52	98.02	99.96	100	99.998
10 000	–	–	–	85.17	87.21	85.88	95.54	96.72	96.21	99.88	100	99.4
25 000	–	–	–	68.00	69.16	68.62	89.26	91.27	90.76	99.68	99.92	99.80
50 000	–	–	–	46.18	47.31	46.85	82.31	83.18	82.63	99.72	99.82	99.76

* where the unit of Uniqueness rate is %, i.e. the unit of data in the table is %.

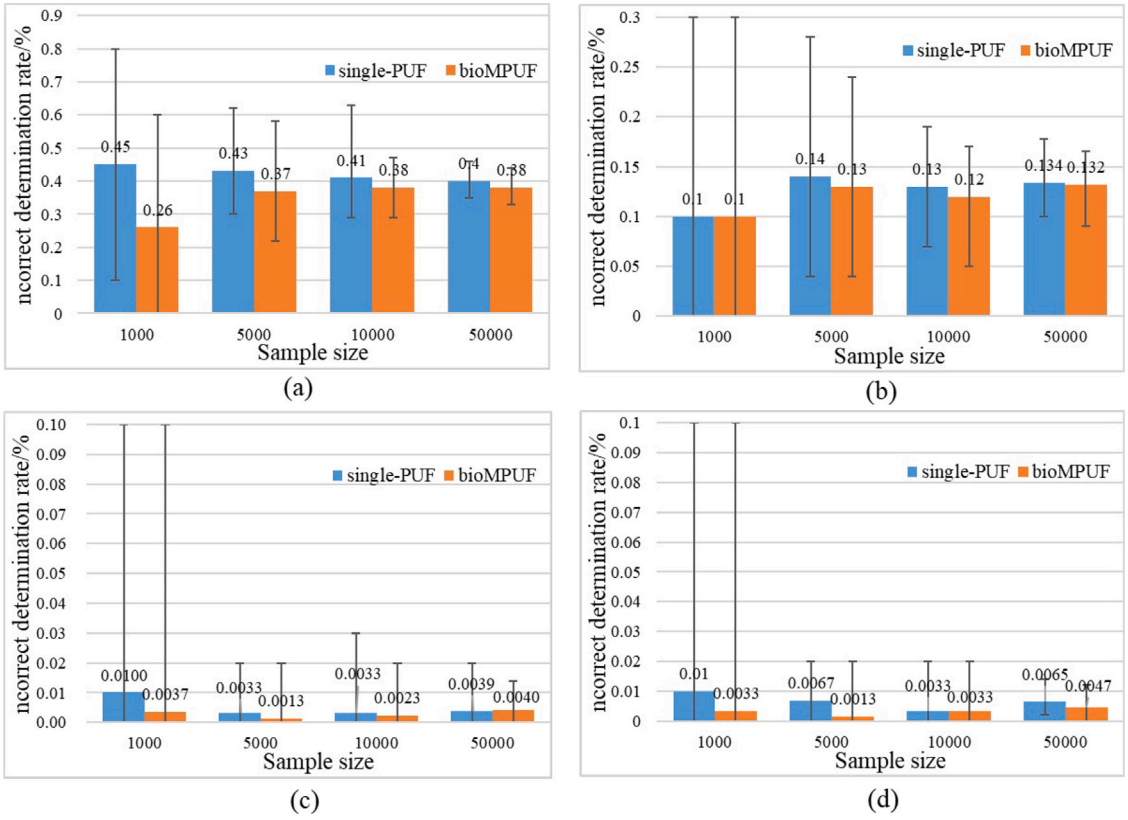

Fig. 12. The incorrect determination rates for single PUF and bioMPUF for the response length of (**a**) 8-bit, (**b**) 12-bit, (**c**) 16-bit and (**d**) 18-bit, respectively.

decreases as the response length increases when the sample size is fixed. Moreover, in most cases, bioMPUF performs better than single PUF in terms of IDR. The reason for this phenomenon is that bioMPUF excels in uniqueness compared to single PUF. Under the same sample size, bioMPUF can achieve better coverage of the final responses than individual PUFs. For example, with a sample size of 1000 and a response length of 8 bits, bioMPUF can generate 256 different response sequences, while the single PUF may only cover 240 response sequences, leading to an increased repetition rate of a particular response sequence in single PUFs. In other words, counterfeiters would need to manufacture more biochips that generate different responses to potentially pass the verification process.

Experiment 3: This experiment is conducted from the perspective of an attacker, simulating a modeling attack initiated after obtaining the CRP dataset. Due to the widespread application of traditional linear machine learning models in PUF modeling attacks, this experiment employs two models, LR and SVM, to perform modeling attacks on bioMPUF. A delay single PUF is used as a control in the experiment. Fig. 13a and Fig. 13b show the prediction rates of LR and SVM for CRP sample sets. According to Machida et al. (2015), the ideal prediction rate is 50%, which indicates that the prediction result of machine learning has the same probability as random guessing, which indicates predicting failure.

It can be seen that when the sample set is 10,000, LR and SVM have the highest prediction rates for 32-bit responses, which are 54.01% and 54.09%, respectively. This shows that the proposed bioMPUF has good resistance to LR and SVM ML-based modeling attacks.

From these experiments, it is easy to see that with limited CRP samples, even if the legitimate user is an attacker, it is difficult to directly access the service provider's biochemical protocol database through the pirated MED biochip. To further verify this conclusion, the next section analyzes the security of bioMPUF.

6.4. Security analysis

The objective of proposed bioMPUF is to protect the IP of MEDA biochip from violating by malicious actors in more aspects, such as the brute force attack (Hsieh et al., 2017), the ML-based modeling attack (Ebrahimabadi et al., 2021), piracy and counterfeiting (Yoon et al., 2020), etc. To analyze the security of bioMPUF, there are several attacks have been considered.

6.4.1. Brute force attack

Depending on the advantages of simplicity and low overhead, the brute force attack has gained the favor of attackers. They attempt to reconstruct the real CRPs database by exhausting the combination of

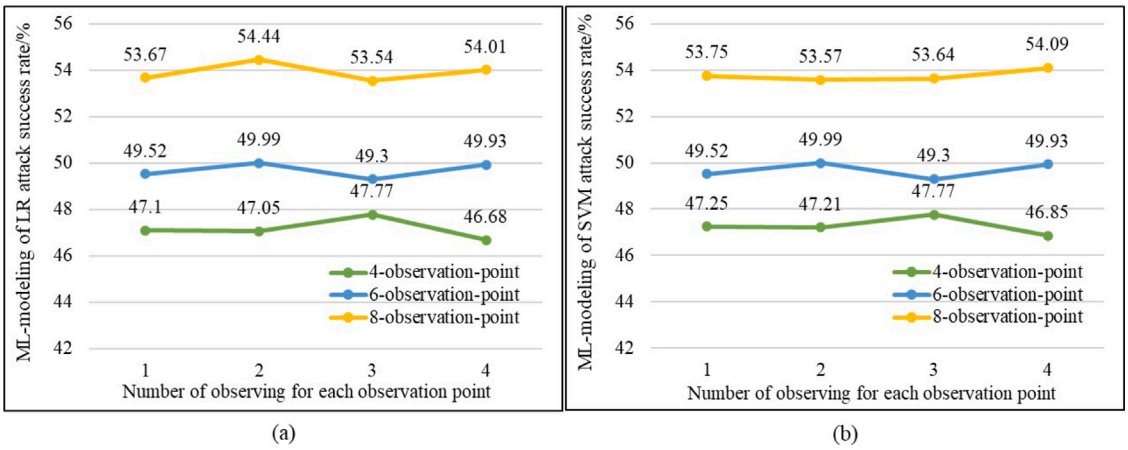

Fig. 13. ML modeling prediction success rate where (**a**) is the success rate of LR-based modeling attacks, and (**b**) is the success rate of SVM-based modeling attacks.

all CRPs in the PUF. However, this is unlikely to succeed in this paper. The minimum number of response bits of bioMPUF is determined by the lifespan of MEDA biochip. If a single electrode on a biochip can withstand up to d activating, the response sequence is at least $\lceil log_2 d \rceil$ bits. Theoretically, hence, the number of trials required to obtain a CRP is greater than the upper limit of electrode activating. Normally, designers will develop responses with more bits depending on the actual application.

In addition, if brute force attacks are utilized, the aging of the electrodes will accelerate as frequent activating, thus not only leading to lifespan shrinking, but also causing an inability to acquire accurate responses. Therefore, complete CRP databases are hard to obtain by brute force attacks.

6.4.2. Piracy and counterfeiting

Attackers can perform RE attacks or side-channel analysis attacks on MEDA biochip designs and then pirate them. These pirated MEDA biochips are not authorized and cannot be authenticated by bioMPUF. Moreover, once they are recognized as unauthorized biochips during the authentication process, bioMPUF's countermeasures will be triggered to accelerate the aging of the pirated biochips. Counterfeiting refers to an attacker's efforts to sell old MEDA biochips by recycling them and then packaging them as new ones. Unlike traditional ICs, a MEDA biochip that has been used many times may have most of its electrodes so badly aged that they are unable to actuate droplet movement and thus unable to perform biochemical protocols, not just a performance degradation. The use of test protocols is easily detected, so counterfeiting poses very little threat to MEDA's IP security (Hsieh et al., 2017).

6.4.3. ML-based modeling attack

The ML-based modeling attacks are implemented by utilizing to construct challenge–response models of MEDA biochips. The known CRPs will be leveraged to train models to predict responses of given challenges.

In this paper, LR and SVM which are common analysis methods of machine learning, are employed to analyze the ability of resistance of bioMPUF to the ML-based modeling attacks. The objective of LR is to attempt to learn a linear model from given data to predict real-valued output markers as accurately as possible. On the other hand, the SVM has been designed for binary classification tasks and aims to define an optimal hyperplane that separates samples from different classes (Mahdavinejad et al., 2018). If data set $DS = \{(\boldsymbol{x}_1, y_1), (\boldsymbol{x}_2, y_2), \ldots, (\boldsymbol{x}_m, y_m)\}$ is given as input parameters. The basic types of LR and SVM are as follows

$$f_{LR}(\boldsymbol{x}) = \boldsymbol{\omega}^T \boldsymbol{x} + b, \tag{20}$$

$$f_{SVM}(\boldsymbol{x}) = \min_{\boldsymbol{\omega}, b} \frac{1}{2} \|\boldsymbol{\omega}\|^2 \quad \text{s.t. } y_i(\boldsymbol{\omega}^T \boldsymbol{x}_i + b) \geq 1, i = 1, 2, \ldots, m. \tag{21}$$

where $f_{LR}(\boldsymbol{x})$ and $f_{SVM}(\boldsymbol{x})$ are indicated outputs of LR and SVM, $\boldsymbol{\omega} = (\omega_1; \omega_2; \cdots; \omega_m)$ means the weight or coefficient of the input $\boldsymbol{x}$, and b is a constant. $\boldsymbol{\omega}$ and b are learning objectives of models.

In the ICs, ML modeling techniques have become one of the major threats to PUFs. Many CRP models with strong PUFs can be successfully predicted by machine learning with an accuracy of around 90%, e.g., arbiter PUF, ring oscillator PUF, etc (Tripathy et al., 2021).

One of the most common measures to improve the resistance of PUF designs to modeling attacks is to increase the non-linearity of models, since machine learning has been applied to solve numbers of linear problems efficiently. The proposed model of bioMPUF is obtained by Eqs. (4) and (14). Since both modulo and XOR are nonlinear operations, the proposed bioMPUF has the ability to resist ML-based modeling attacks.

7. Conclusion

In this paper, bioMPUF, an IP protection strategy on MEDA biochips, has been proposed. This strategy based on multi-PUF design not only improves the unpredictability of CRP and enhances the resistance to modeling attacks by increasing the nonlinearity of the PUF of the MEDA biochip, but also effectively defends against brute force attacks, counterfeiting, and piracy. In addition, a countermeasure is introduced that can accelerate the degradation of the MC to destroy the available pirated biochips. The experimental results and security analysis show that the bioMPUF strategy is an effective IP anti-piracy solution for MEDA biochips.

In the future, the additional advanced features of MEDA biochips, such as flexible droplet sizing and advanced fluidic operations, are expected to garner attention, providing support for the advancement of PUF technologies. These discoveries will be continuously monitored, explored further in ongoing research, and contribute to the continuous innovation and development of IP security in the field of biochips.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 62372110, No. 62072109), the Natural Science Foundation of Fujian Province (No. 2021J01616), Fujian Province Technology and Economy Integration Service Platform under Grant 2023XRH001.

References

Aseeri, A.O., Zhuang, Y., Alkatheiri, M.S., 2018. A machine learning-based security vulnerability study on xor pufs for resource-constraint internet of things. In: 2018 IEEE International Congress on Internet of Things. ICIOT, IEEE, pp. 49–56.

Babies, 2020. FINDER SARS-CoV-2 test for detection of COVID-19. https://baebies.com/products/sars-cov-2-rt-pcr-test/.

Babies, 2023. Developing innovative products and services to provide a healthy start. https://baebies.com/.

Bhattacharjee, S., Tang, J., Poddar, S., Ibrahim, M., Karri, R., Chakrabarty, K., 2019. Bio-chemical assay locking to thwart bio-IP theft. ACM Trans. Des. Autom. Electron. Syst. (TODAES) 25 (1), 1–20.

Chan, Y.-S., Lee, C.-Y., 2022. A programmable bio-chip with adaptive pattern-control micro-electrode-dot-array. IEEE Trans. Circuits Syst. II 69 (11), 4513–4517.

Chen, H., Potluri, S., Koushanfar, F., 2020. Security of microfluidic biochip: Practical attacks and countermeasures. ACM Trans. Des. Autom. Electron. Syst. (TODAES) 25 (3), 1–29.

Cho, M., Pan, D.Z., 2008. A high-performance droplet routing algorithm for digital microfluidic biochips. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 27 (10), 1714–1724.

Cui, Y., Gu, C., Ma, Q., Fang, Y., Wang, C., O'Neill, M., Liu, W., 2020. Lightweight modeling attack-resistant multiplexer-based multi-PUF (MMPUF) design on FPGA. Electronics 9 (5), 815.

Datta, P., Chakraborty, A., Pal, R.K., 2022. Attack-detection and-recovery: An integrated approach towards attack-tolerant cyber-physical digital microfluidic biochips. IETE J. Res. 1–13.

Dong, C., Liu, L., Liu, H., Guo, W., Huang, X., Lian, S., Liu, X., Ho, T.-Y., 2020. A survey of DMFBs security: State-of-the-art attack and defense. In: 2020 21st International Symposium on Quality Electronic Design. ISQED, IEEE, pp. 14–20.

Dong, C., Liu, L., Liu, X., Liu, H., Lian, S., 2021. MEDASec: Logic encryption scheme for micro-electrode-dot-array biochips IP protection. In: Proceedings of Great Lakes Symposium on VLSI. ACM, pp. 277–282.

Ebrahimabadi, M., Younis, M., Lalouani, W., Karimi, N., 2021. A novel modeling-attack resilient arbiter-PUF design. In: 2021 34th International Conference on VLSI Design and 2021 20th International Conference on Embedded Systems. VLSID, IEEE, pp. 123–128.

Elfar, M., Liang, T.-C., Chakrabarty, K., Pajic, M., 2021. Formal synthesis of adaptive droplet routing for MEDA biochips. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 41 (8), 2504–2517.

Gountia, D., 2023. Reliability issues in state-of-the-art microfluidic biochips: A survey. IETE Tech. Rev. 1–16.

Guo, W., Lian, S., Dong, C., Chen, Z., Huang, X., 2022. A survey on security of digital microfluidic biochips: Technology, attack, and defense. ACM Trans. Des. Autom. Electron. Syst. (TODAES) 27 (4), 1–33.

He, H., Hu, H., 2020. Field-level digital microfluidic biochips trojan detection based on hamming distance. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference. ITNEC, vol. 1, IEEE, pp. 640–643.

Hemavathy, S., Bhaaskaran, V.K., 2023. Arbiter PUF-a review of design, composition, and security aspects. IEEE Access.

Howladar, P., Roy, P., Chatterjee, S., Rahaman, H., 2020. Chip level design in MEDA based biochips: application of daisy chain based actuation. Microsyst. Technol. 26, 2337–2351.

Howladar, P., Roy, P., Rahaman, H., 2021. Droplet transportation in MEDA-based biochips: An enhanced technique for intelligent cross-contamination avoidance. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 29 (7), 1451–1464.

Hsieh, C.-W., Li, Z., Ho, T.-Y., 2017. Piracy prevention of digital microfluidic biochips. In: Proceedings of Asia and South Pacific Design Automation Conference. IEEE, pp. 512–517.

Ibrahim, M., Zhong, Z., Bhattacharya, B.B., Chakrabarty, K., 2021. Efficient regulation of synthetic biocircuits using droplet-aliquot operations on MEDA biochips. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 41 (8), 2490–2503.

Ji, W., Guo, X., Pan, S., Ho, T.-Y., Schlichtmann, U., Yao, H., 2022. GNN-based concentration prediction for random microfluidic mixers. In: Proceedings of the 59th ACM/IEEE Design Automation Conference. pp. 763–768.

Ji, W., Yao, X., Yao, H., Ho, T.-Y., Schlichtmann, U., Yin, X., 2023. SOAER: Self-obstacle avoiding escape routing for paper-based digital microfluidic biochips. In: Proceedings of the Great Lakes Symposium on VLSI 2023. pp. 255–260.

Jin, R., Hu, J., Min, G., Mills, J., 2023. Lightweight blockchain-empowered secure and efficient federated edge learning. IEEE Trans. Comput..

Keszocze, O., Li, Z., Grimmer, A., Wille, R., Chakrabarty, K., Drechsler, R., 2017. Exact routing for micro-electrode-dot-array digital microfluidic biochips. In: Proceedings of Asia and South Pacific Design Automation Conference. IEEE, pp. 708–713.

Kokila, J., Ramasubramanian, N., 2019. Enhanced authentication using hybrid puf with fsm for protecting ips of soc fpgas. J. Electron. Test. 35, 543–558.

Li, Z., Lai, K.Y.-T., Yu, P.-H., Chakrabarty, K., Ho, T.-Y., Lee, C.-Y., 2017. Droplet size-aware high-level synthesis for micro-electrode-dot-array digital microfluidic biochips. IEEE Trans. Biomed. Circuits Syst. 11 (3), 612–626.

Liang, T.-C., 2021. Parallel droplet control in MEDA biochips using multi-agent reinforcement learning. In: International Conference on Machine Learning.

Liang, T.-C., Shayan, M., Chakrabarty, K., Karri, R., 2020. Secure assay execution on MEDA biochips to thwart attacks using real-time sensing. ACM Trans. Des. Autom. Electron. Syst. 25 (2), 1–25.

Lin, C.-Y., Huang, J.-D., Yao, H., Ho, T.-Y., 2018. A comprehensive security system for digital microfluidic biochips. In: Proceedings of IEEE International Test Conference in Asia. IEEE, pp. 151–156.

Machida, T., Yamamoto, D., Iwamoto, M., Sakiyama, K., 2015. Implementation of double arbiter PUF and its performance evaluation on FPGA. In: Proceedings of Asia and South Pacific Design Automation Conference. IEEE, pp. 6–7.

Mahdavinejad, M.S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., Sheth, A.P., 2018. Machine learning for Internet of Things data analysis: A survey. Digit. Commun. Netw. 4 (3), 161–175.

Mills, J., Hu, J., Min, G., 2021. Multi-task federated learning for personalised deep neural networks in edge computing. IEEE Trans. Parallel Distrib. Syst. 33 (3), 630–641.

Poddar, S., Banerjee, T., Wille, R., Bhattacharya, B.B., 2020. Robust multi-target sample preparation on MEDA biochips obviating waste production. ACM Trans. Des. Autom. Electron. Syst. (TODAES) 26 (1), 1–29.

Poddar, S., Bhattacharjee, S., Fang, S.-Y., Ho, T.-Y., Bhattacharya, B.B., 2021a. Demand-driven multi-target sample preparation on resource-constrained digital microfluidic biochips. ACM Trans. Des. Autom. Electron. Syst. (TODAES) 27 (1), 1–21.

Poddar, S., Bhattacharya, B.B., 2022. Error-Tolerant Biochemical Sample Preparation with Microfluidic Lab-On-Chip. CRC Press.

Poddar, S., Fink, G., Haselmayr, W., Wille, R., 2021b. A generic sample preparation approach for different microfluidic labs-on-chips. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 41 (11), 4612–4625.

Shayan, M., Bhattacharjee, S., Tang, J., Chakrabarty, K., Karri, R., 2019. Bio-protocol watermarking on digital microfluidic biochips. IEEE Trans. Inf. Forensics Secur. 14 (11), 2901–2915.

Shayan, M., Bhattacharjee, S., Wille, R., Chakrabarty, K., Karri, R., 2020a. How secure are checkpoint-based defenses in digital microfluidic biochips? IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 40 (1), 143–156.

Shayan, M., Liang, T.-C., Bhattacharjee, S., Chakrabarty, K., Karri, R., 2020b. Toward secure checkpointing for micro-electrode-dot-array biochips. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 39 (12), 4908–4920.

Shi, J., Fu, P., Zheng, W., 2022. A design method based on Bayesian decision for routing-based digital microfluidic biochips. Analyst 147 (6), 1076–1085.

Technavio, 2023. Biochips Market Report, Size, Share & Growth [2023 Global Report]. URL https://www.technavio.com/report/biochips-market-analysis.

Tripathy, S., Rai, V.K., Mathew, J., 2021. MARPUF: Physical unclonable function with improved machine learning attack resistance. IET Circuits Devices Syst. 1–10.

Ucci, D., Aniello, L., Baldoni, R., 2019. Survey of machine learning techniques for malware analysis. Comput. Secur. 81, 123–147.

Yoon, S., Kim, B., Kang, Y., Choi, D., 2020. PUF-based authentication scheme for IoT devices. In: Proceedings of International Conference on Information and Communication Technology Convergence. IEEE, pp. 1792–1794.

Zhang, L., Li, Z., Huang, X., Chakrabarty, K., 2023. Enhanced built-in self-diagnosis and self-repair techniques for daisy-chain design in MEDA digital microfluidic biochips. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst..

Zhong, Z., Chakrabarty, K., 2020. IJTAG-based fault recovery and robust microelectrode-cell design for MEDA biochips. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 39 (12), 4921–4934.

Zhong, Z., Li, Z., Chakrabarty, K., Ho, T.-Y., Lee, C.-Y., 2018. Micro-electrode-dot-array digital microfluidic biochips: Technology, design automation, and test techniques. IEEE Trans. Biomed. Circuits Syst. 13 (2), 292–313.

Zhong, Z., Liang, T.-C., Chakrabarty, K., 2020. Enhancing the reliability of MEDA Biochips using IJTAG and wear leveling. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 40 (10), 2063–2076.