IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 30 October 2023, accepted 27 November 2023, date of publication 4 December 2023,
date of current version 13 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3339386

RESEARCH ARTICLE

A Reliable and Secure Mobile Cyber-Physical Digital Microfluidic Biochip for Intelligent Healthcare

YINAN YAO[1], (Member, IEEE), DECHENG QIU[1], HUANGDA LIU[1], ZHONGLIAO YANG[1], XIMENG LIU[1], (Senior Member, IEEE), YANG YANG[2], (Member, IEEE), AND CHEN DONG[1], (Member, IEEE)

[1]College of Computer and Data Science, Fuzhou University, Fuzhou 350108, China
[2]School of Computing and Information Systems, Singapore Management University, Singapore 178902

Corresponding author: Chen Dong (dongchen@fzu.edu.cn)

This work was supported in part by the Fund of Fujian Province Digital Economy Alliance, National Natural Science Foundation of China, under Grant 62372110 and Grant 62072109; and in part by the Natural Science Foundation of Fujian Province under Grant 2020J01500 and Grant 2021J01616.

ABSTRACT Digital microfluidic, as an emerging and potential technology, diversifies the biochemical applications platform, such as protein dilution sewage detection. At present, a vast majority of universal cyberphysical digital microfluidic biochips (DMFBs) transmit data through wires via personal computers and microcontrollers (like Arduino), consequently, susceptible to various security threats and with the popularity of wireless devices, losing competitiveness gradually. On the premise that security be ensured first and foremost, calls for wireless portable, safe, and economical DMFBs are imperative to expand their application fields, engage more users, and cater to the trend of future wireless communication. To this end, a new cyber-physical DMFB called *PortableLab* is proposed in this paper, which guarantees data security through wireless sensors at low cost. After considering the security, computing consumption, and cost, a mobile module is added. In addition, the improved Advanced Encryption Standard (AES) and Cyclic Redundancy Check (CRC) algorithms are utilized to ensure the integrity and confidentiality of data transmission. Ultimately, all the security analysis, cost analysis, and experimental results on multiple protocols demonstrate the feasibility of the proposed PortableLab DMFB in time and space.

INDEX TERMS DMFB, security, wireless, mobile, low-cost, healthcare.

I. INTRODUCTION

The pandemic caused by Covid-19 has challenged the entire traditional healthcare system and exposed its weaknesses to the public. AXA reported in 2023 that some people experienced significant mental stress as a result of the pandemic [2]. Fortunately, the pandemic also contributed to the development of human society. Examples include intelligent factories [3], natural language processing, chip security [4], etc. Telemedicine is an exchange of clinical/medical-related information from one destination to another employing information and communication technology (ICT) [5]. Despite the necessity of telemedicine being fully aware of contagious diseases, an unmet need remains for reliable, portable endpoint healthcare devices. Biochips, an emerging platform for biochemical reagent preparation, can perform specific tasks faster than traditional manual operations by automating and refining operations to achieve this challenge. Therefore, it can be anticipated that biochips will, as industrialization advances, significantly promote the development of existing intelligent healthcare systems. Hence, digital microfluidic biochip, integrating the basic operations of reaction, separation, and detection in biological, chemical, and medical analysis processes onto a microchip and automatically completes the analysis, is a powerful emerging technology that manages precise manipulation of droplets from nanoliter to microliter as well as complex experimental analysis [6].

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

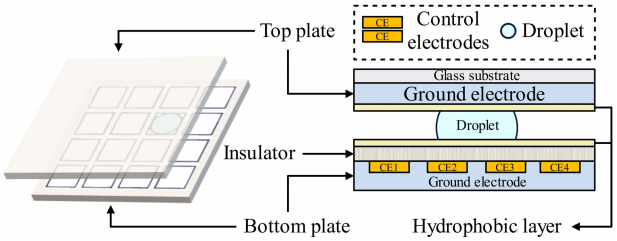


FIGURE 1. Structure of a DMFB array as viewed from the side.

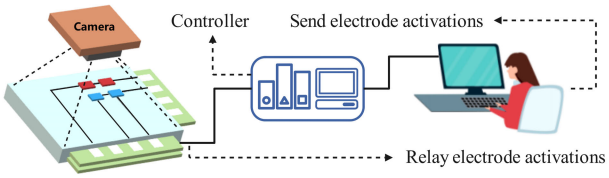


FIGURE 2. Schematic of a traditional cyberphysical DMFB model.

According to the latest statistics, the global microfluidic product market size is expected to reach USD 12.38 billion in 2025 [7]. In the past 20 years, DMFBs have been extensively studied because of their affordability and automation ability. Distinctive from the flow-based microfluidic biochips, DMFB is composed of a two-dimensional electrode array and peripheral devices, such as heaters, optical detectors, and control pin devices [8], as shown in Figure 1.

Previously, Alistar designed a DMFB platform called OpenDrop that took DMFB out of the lab [1], [2], though its defects can never be neglected: (1) the analysis module is embedded inside the platform, which would make the biochemical protocols vulnerable to theft, and (2) it is unable to be freed from the constraints of the lab and requires the latest biochemical protocols to be wired and downloaded from the host. Nevertheless, our proposed PortableLab will enable actuation sequences to be transferred through wireless modules, thus allowing the accessibility of the latest biological protocols and real-time analysis results for any end-users at home, outdoors, and not in a clinic.

The reconfigurability of DMFBs and the convenience of software control have facilitated research in chip automation design and application. Plowing into substantial capital innovations in biochemical analysis and cyberphysical models is indispensable in developing bio-protocols. Meanwhile, rapid commercialization has led to more frequent piracy attacks [9], [10], so biochemical protocol protection should be attached to great importance to prevent certain economic losses.

Therefore, this paper proposes PortableLab, which allows the microcontroller to transmit data wirelessly to the server. Since DMFBs transmit data remotely, the biological protocol is likely to be stolen by piracy attacks. In [11], Jalalitabar et al. listed the threats of hardware Trojans in wireless sensor networks.

The paper exploits encryption and verification algorithms to ensure the complete and indecipherable data. Symmetric algorithms are usually applied to encrypt data, while asymmetric algorithms usually serve as encrypt keys. Therefore, PortableLab encrypts the data with the AES algorithm and optimizes s-box queries using logic gate circuits [12]. CRC algorithms often retain data accuracy in communication, endowed with vigorous error detection ability, cost-effective property, a convenient encoder, and a detection circuit. The contributions of our work are summarized as follows.

- A secure DMFB model with wireless communication PortableLab is first proposed, and the working principles and parameters are introduced.
- An improved encryption algorithm based on AES and CRC algorithms is designed for low-cost wireless DMFB communication; this algorithm guarantees the bioassay is indecipherable and unmodifiable between the microcontroller and remote servers.
- Security evaluation parameters are defined, which are designed to evaluate the performance of the PortableLab.

The remainder of this paper is organized as follows. Section II describes the structure and principle of DMFB. Section III presents the Cyberphsical DMFB and communication models, the flow of the overall model, and the protection between the data-defined feasibility analysis, including security and cost, in Section IV. Experimental results are shown in Section V to demonstrate the feasibility of PortableLab, and conclusions are drawn in Section VI.

II. BACKGROUND AND MOTIVATION

Here, the traditional cyberphysical DMFB model, wireless module combined with DMFB, related work of this article, and the motivation for proposing PortableLab will be described.

A. TRADITIONAL CYBERPHYSICAL DMFB MODEL

Traditional cyber-physical DMFB model containing DMFB, camera, and microcontroller. Figure 2 shows the traditional cyberphysical DMFB model. The conventional method is that the microcontroller (such as Arduino) is directly connected to the DMFB, while the personal computer communicates with the microcontroller through the universal serial bus [13]. The controller can apply a voltage to the DMFB to actuate the droplets.

The sequence of these control voltages is activated through a high-level synthesis flow, and the measurement is specified in the form of a directed acyclic graph (DAG). The correct actuation control signal can enable DMFB to perform distribution, transport, separation, and mixing operations. There are integrated circuit clips on both sides of the DMFB and connect to the microcontroller. There are two parallel plates with electrodes, and the surface of the plate is coated with an isolation layer and a hydrophobic layer to facilitate the driving of droplets. Applying a voltage V below to change the tension of the droplet on the substrate causes the droplet to deform. This phenomenon is called electrowetting on dielectric and is modeled using the

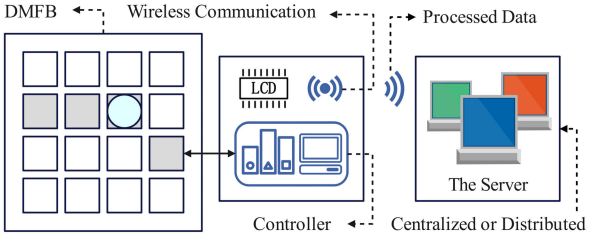


FIGURE 3. Schematic of portableLab model.

Lippmann-young equation.

$$\cos\theta_v = \cos\theta_0 + \frac{\varepsilon_0\varepsilon_r v^2}{2d\gamma_{lg}} \tag{1}$$

where $\cos\theta_v$ is the contact angle when voltage is applied, θ_0 is the contact angle when no potential is applied, ε_0 is the vacuum dielectric constant, ε_r is the relative permittivity, γ_{lg} is the liquid-gas interfacial tension, $2d$ is an electric double layer at the interface between solid and liquid after applying voltage. Based on these basic functions, DMFB can be utilized for bioassays such as protein dilution and sewage detection. However, during the development of the biochemical protocol, a large amount of capital and manpower are required, and the current biochip has many security problems [6]. Therefore, intellectual property should be protected when considering new solutions to prevent theft by malicious attackers.

B. WIRELESS MODULE

With the rapid development of the Internet of Things (IoT) technology, wireless modules are applied in various IoT devices. Wireless modules such as ESP8266 have a lower cost compared to other wifi modules. The compact form factor (24*16mm) makes it possible to embed a multitude of devices. This chip utilizes a 3.3V DC power supply with low power consumption and nothing seriously lost packet. The wireless wifi module is a double-edged sword, which causes some problems while bringing convenience [14].

Wireless sensor network technology solves the problem of long-distance data transmission by providing low-cost and low-power wireless communication. Most companies have realized that with the invention of low-cost, low-power wireless sensors, wireless communication is one of the most economical ways to transmit data [15]. While both parties are communicating, other devices are untrusted third parties. Therefore, it is necessary to establish an encryption algorithm to ensure data security in wireless transmission.

C. RELATED WORK

Currently, DMFB can be applied in many fields, including neonatal diagnosis [16], sample preparation [17], drug discovery [18], etc. Regarding functional classification, DMFB can be divided into customized DMFB and universal DMFB [19]. Customized DMFB can be custom-designed and manufactured according to specific experimental requirements and application scenarios and implement one or more pending biological detections on the chip [9]. Common customized DMFBs include Clinical Diagnostics DMFB and Environmental Analysis DMFB. Customized DMFB needs to meet specific experimental requirements and application scenarios, so it is unsuitable for diverse experiments. At the same time, when customized DMFB needs to conduct different types of experiments, the chip may need to be redesigned, resulting in higher costs and time. Invest. General-purpose DMFBs are usually designed to perform different bioassays based on field-programmable electrode arrays [20] and, therefore, have high flexibility. At the same time, because general-purpose DFMBs have standardized designs and can be mass-produced, they have lower costs and are suitable for a wide range of research and experiments. Common general-purpose DMFBs include DropBot and OpenDrop. Among them, the open-source platform DropBot proposed by Fobel et al. is used to precisely control and operate the flow and merger of tiny droplets [21]. To bring this technology from the laboratory to a broader range of applications and reduce costs, Alistar designed OpenDrop, a small platform that makes biological experiments more convenient [1]. So far, in the field of DMFB, OpenDrop mainly implements the download of the latest biological protocols through wired transmission with the host device. This still has certain limitations for it to go out of the laboratory. The PortableLab proposed in this article combines wireless modules with droplet microfluidic technology to enable biological experiments to be performed anytime and anywhere.

D. MOTIVATION

In the future, biochips will have broad market prospects, but at present, the main usage scenarios of biochips are still laboratories. If biochips are liberated from laboratory constraints to a greater extent, the popularity of biochips can be significantly promoted. Therefore, there is a need for a digital biochip platform that can use the latest biological protocols anytime and anywhere. Although OpenDrop has solved this pain point to a large extent, it currently has problems such as being easily stolen, and it needs to connect and download the latest biological protocols from the host. Therefore, it still has deficiencies in portability and security. Thus, this article combines the wireless module with the biological microfluidic chip platform to ensure that the biological microfluidic platform can use the latest biological protocols to conduct bioassays anytime and anywhere and to prevent biological protocols from being stolen on the chip platform. At the same time, to prevent the biological protocol from being stolen during wireless transmission, this article uses improved Advanced Encryption Standard (AES) and Cyclic Redundancy Check (CRC) algorithms to ensure the integrity and confidentiality of data transmissions.

III. APPLICATION

A. LARGE HOSPITAL AND SMALL CLINICS

In large hospitals, the commonly used detection performed by DMFB is the clinical analysis, which usually includes the

detection of metabolites, electrolytes, liver function markers, and kidney function markers in physiological samples, which requires a laboratory host for each department. Clinical diagnosis of these markers in an offline setting is inconvenient [22] since the assays require the integration of many workflows. Besides, it is a waste of resources for different hosts to handle protocols from various hospital departments, and it is impossible to remotely manage updates to the latest protocols.

In small clinics, some disease detection is impossible due to expensive equipment. End-users handing over critical data processing to cloud servers will significantly reduce operating costs, and clinics only purchase mobile DMFB devices, which lowers the threshold to detect diseases. End-users in large hospitals and clinics will protect their privacy if all detection results are available only to trusted cloud servers. In PortableLab, the data processing procedures are kept in a fixed place, which will reduce the cost and increase the portability of DMFB in hospitals and small clinics.

B. BIOLOGICAL REACTION

The DMFB platform has many biological field applications, where general biological reactions are performed for PCR, cell culture, and immunoassays. Reference [23] utilizes digital microfluidic chips to culture embryos automatically and maintains complete control of embryos through protocols.

C. CHEMICAL REACTION

In chemical reactions, the DMFBs have been used to synthesize various micro-particles. Test tubes perform various operations for conventional chemical reactions, which wastes many valuable reagents. The DMFB can operate on tiny droplets of about 30 picoliters, which results in less waste of reagents [24]. The Wheeler group reacts with thiobenzoic acid, yet the chemical can only be stored at 2 to 8 degrees Celsius, which would limit the reaction temperature. There are also some problems in the movement of chemicals, such as temperature, moderate control, chemical reagent hazards, and temporal stability. Chemical reactions for different protocols also imply the need for different DMFBs, which can significantly increase the reaction cost. PortableLab enables these chemicals to react without moving and can utilize multiple protocols on a single device and get real-time results from the cloud server.

D. ENVIRONMENTAL DETECTION

In environmental detection, which is the detection of microbial concentrations in various environments such as sewage, air, and soil, the DMFBs can monitor the levels of substances in real time and allow experts to determine the environment from the data. The previous model could not detect in real-time and required experts to observe at the detection location. Environmental detection requires real-time analysis of the data. Since the composition of microorganisms in the environment is diverse, utilizing a single protocol for detection is impossible, and different protocols are necessary. In PortableLab, microorganisms in the environment can be detected in real-time. The data is sent to a cloud server for processing, eliminating the need for on-site observation by experts. It is also possible to load new reaction protocols to detect substances, eliminating the need for multiple DMFBs and avoiding wasted resources.

E. AT-HOME DETECTION

The DMFB detects various minor illnesses; some simple tests can be performed without a hospital. For example, the DMFB performs a polymerase chain reaction on DNA, a reaction that detects pneumonia infection. Reference [25] proposed using a microfluidic platform to detect Mycoplasma pneumonia, a method that would identify Mycoplasma pneumonia by detecting changes in the RNA sequence. Home detection is essential since mycoplasma infections usually have an insidious onset followed by days or weeks of slowly worsening dry cough, fever, and discomfort. However, different protocols are required for other diseases, and typical microfluidic platforms need to change protocols frequently to correspond to various diseases. PortableLab can provide different protocols for home detection, allowing different family members to detect other diseases. For chronic illnesses that need to be monitored, the data can also be transferred to a cloud server for real-time analysis and privacy protection of the results.

IV. MOBILE MICROFLUIDICS PLATFORMS

Here, the new cyberphysical DMFB model and its internal communication mode will be described. Then, the whole process involved and the algorithm steps will be described.

A. THE OVERALL PORTABLELAB MODEL FLOW

In the model flow shown in Figure 4, biological and chemical engineers need to propose biochemical analysis. For example, the detection of protein requires the biuret reagent. When using the biuret reagent, must first add 0.1g/ml sodium hydroxide solution, and then add 0.01g/ml aqueous solution of copper sulfate. The sequence graph is determined according to the sequence graph specification and sequence analysis. The sequence graph needs to conform to the chip design specifications, and the chip engineer turns the sequence diagram and sequence analysis into the corresponding chip actuation sequence. These actuation sequences will be encrypted and verified by the algorithm and then sent to the microcontroller through the wireless module. When the microcontroller receives the data, it will execute the decryption and verification algorithm to ensure that the data will be complete and indecipherable in the transmission process. The microcontroller will use the interpreted data to generate the actuation sequence and then control DMFB for scheduling, placement, and routing operations. In PortableLab, the keys required for encryption and authentication algorithms will be embedded in the microcontroller before the vendor sells.

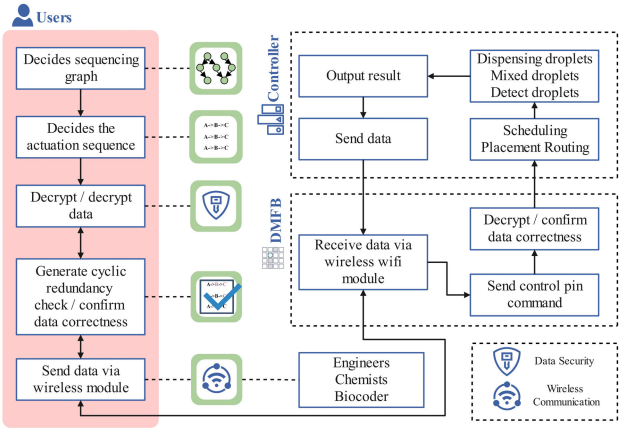


FIGURE 4. The overall framework of the proposed PortableLab.

Algorithm 1 Decryption and Verify Splicing Check Bit

Input: c, actuation sequence ciphertext block
Output: p, actuation sequence plaintext block, k, cipher key
while *Presence of unprocessed ciphertext blocks* **do**
  while *The C to decrypt isn't null.* **do**
    if *! c % G(x)* **then**
      return false;
  end
  $\langle k^{(0)}, k^{(1)}, \ldots, k^{(10)} \rangle \leftarrow$ KeySchedule(k) ;
  $c \leftarrow$ AddRoundKey(p,$k^{(0)}$) ;
  for *each* $i \in \{1,2,\ldots,10\}$ **do**
    $c \leftarrow$ Invshiftrow(c);
    $c \leftarrow$ InvSubBytes(c);
    $c \leftarrow$ AddRoundKey(c,$k^{(i)}$);
    $c \leftarrow$ InvMixColumns(c);
  end
  $c \leftarrow$ Invshiftrow(c);
  $c \leftarrow$ InvSubBytes(c);
  $c \leftarrow$ AddRoundKey(c,$k^{(10)}$);
end
return c;

In the data part, this paper will apply encryption and verification algorithms to protect the data from being read and tampered with in transmission. Therefore, the synthesis problem to be considered in this framework is defined as:

Input: A synthesized actuation sequence $\mathcal{AS} = (as_1, as_2, \ldots, as_n)$; the key K used by the encryption algorithm; the integer R used to the validation algorithm.

Output: A verified and encrypted algorithms actuation sequence $\mathcal{AS}_{EV} = (as'_1, as'_2, \ldots, as'_n)$.

Objective: Plaintext $\mathcal{AS} = (as_1, as_2, \ldots, as_n)$ ensures its data security through encryption algorithm, and ciphertext $\mathcal{AS}_E = (as'_1, as'_2, \ldots, as'_n)$ ensures its data integrity through verification algorithm. Moreover, data encryption and verification are reliable in terms of time feasibility.

B. THE PORTABLELAB MODEL AND COMMUNICATION PATTERN

In this part, we will briefly introduce the PortableLab with a wireless and describe the communication module and model applied.

The traditional model requires a personal computer to control DMFB through wired for biological protocol analysis, which significantly limits the application scenarios of DMFB. Therefore, a wireless module is applied to realize data communication. This PortableLab will alter this method, as shown in Figure 3. The controller, DMFB, and liquid crystal display (LCD) are integrated to transmit data to the server through esp8266. The server sends the encrypted control signal to the controller through esp8266, and the controller converts it into an actuation sequence to control DMFB. When the DMFB executes the biological protocol, the results will be returned to the server for processing through the microcontroller, and the server will send it to the microcontroller for presentation through the wireless module, allowing the end-user to view the analysis results in real time. Because of the insecurity of wireless communication, the threat of hardware trojan is increasingly severe. The server will encrypt the data before sending it and decrypt it when the microcontroller receives it.

Among PortableLab's interface communications, the controller turns data to the internal memory of the programmable logic controller (PLC) through the RS-232 communication interface. When performing biometrics, the PLC will read the electrode actuation sequence in the memory to deactivate the DMFB electrode to actuate the droplet. After the DMFB executes a series of bioassays, the sensing system detects the resulting droplets, turns the analog signal into voltage or current, and transmits it to the controller. The controller turns the encrypted result into the server through the wireless module.

The inter-integrated circuit (I2C) bus will transfer data between the microcontroller and the wireless sensor. The I2C bus has two bi-directional serial lines, one of which is serial clock (SCL), and the other is serial data (SDA). In data transmission, SCL is the high level for valid data, SDA is the high level for binary "1", and the low level for binary "0". When the SCL voltage is low, the SDA's voltage is level-switched. The embedded control code contains only numbers and letters converted to their corresponding binary numbers through the ASCLL code table.

C. DATA PROTECTION

Here, we describe the detailed steps of PortableLab's encryption and verification algorithm for data transmission and illustrate the optimization of the algorithm for microcontrollers.

Define the activation sequence in PortableLab as $AS = (As_1, As_2, \ldots, As_i, \ldots, As_n)$, $As_i \in ACSLL$ code. The encryption of the activation sequence is primarily concerned with how the data satisfies the AES encryption

Algorithm 2 Encryption and Generating Splicing Check Bit

Input: $P = (p_1, p_2, \ldots, p_n)$, actuation sequence plaintext block, k, cipher key, polynomial G(x)
Output: c, actuation sequence ciphertext block
while *Presence of unprocessed plaintext blocks* **do**
  $\langle k^{(0)}, k^{(1)}, \ldots, k^{(10)} \rangle \leftarrow$ KeySchedule(k) ;
  $c \leftarrow$ AddRoundKey(p,$k^{(0)}$) ;
  for *each* $i \in \{1,2,\ldots,10\}$ **do**
    $c \leftarrow$ SubBytes(c);
    $c \leftarrow$ ShiftRows(c);
    $c \leftarrow$ MixColumns(c);
    $c \leftarrow$ AddRoundKey(c,$k^{(i)}$);
  end
  $c \leftarrow$ SubBytes(c);
  $c \leftarrow$ ShiftRows(c);
  $c \leftarrow$ AddRoundKey(c,$k^{(10)}$);
  while *The C to be encrypted isn't null* **do**
    Initialize flag;
    if c & *flag* **then**
      c $\leftarrow c \oplus G(x)$; G(x) $\gg 1$;
    else
      G(x) $\gg 1$;
    end
    flag $\gg 1$;
  end
end
return c;

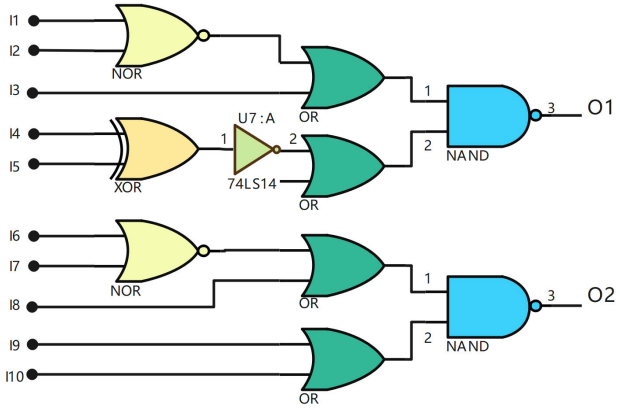


FIGURE 5. A part of the F28 inverter.

algorithm for byte SubBytes, ShiftRows, MixColumns, and key AddRoundKey. Before encrypting the data, the activation sequence is formatted and the characters are mapped to the corresponding binary code $AS' = (As_1', As_2', \ldots, As_i', \ldots, As_n')$ through *ASCLL* code, where $As_i' = (b_7, b_6, b_5, b_4, b_3, b_2, b_1)$, consists of 8 binary numbers.

SubBytes: set $F = S\{(b_7, b_6, b_5, b_4), (b_3, b_2, b_1, b_0)\}$ in PortableLab, where (b_7, b_6, b_5, b_4) and (b_3, b_2, b_1, b_0) consist of rows and columns of the S-box respectively. The new hexadecimal code $F' = (AS1_{hex}, AS2_{hex})$ is obtained by checking the S-box. Queries at the S-box can waste a large amount of time, and previous work will optimize queries. In this part, the logic-gate circuit-based optimization proposed by Reyhani-Masoleh et al. [12], which is more applicable to the PortableLab model. Due to mass production at PortableLab, it is convenient to attach small-scale logic gate modules to the microcontroller. Figure 5 shows a part of the F28 inverter. Its experiments are based on the implementation of STM 65nm technology, and the results show that a total of 149 gate circuits are required, including 8 XNOR2, 32 NAD2, 8 NOT, 8 NOR2, 2 OAI22, 2 OAI32, and 16 MUXI21, where the latency is 1.159*us* and the area is 508.04um^2. This is a negligible burden on the microcontroller.

MixColumns: the GF (2^8) finite field multiplication is denoted by $\circ$. The modulo multiplication of its polynomial is $m(x) = x^8 + x^4 + x^3 + x + 1$. $M = (m_1, m_2, \ldots, m_n)$ will be obtained by a fixed confusion matrix $M(F'(x))$. $M_{i+x}[F'(x)] = [F'[i] \circ 02; F'[i]; F'[i]; F[i] \circ 03]$, where x ranges from 1 to 4.

AddRoundKey: define the add round key in the formula $AS_E = expankey[Round \ll 4+x_i]$, where *expankey* is an array of keys, and *Round* represents an encrypted round. Since the key is 16 bits, x_i will be traversed from 1 to 16. The activation sequence encryption and decryption in PortableLab will be transformed multiple times by the above four operations, and finally, the data $AS_E[x]$ will be obtained.

In the CRC algorithm, both parties should preset $i{\cdot}n$ *bit* integer $P = (p_1, p_1, \ldots, p_i)$, and calculate $i{\cdot}(n-k)$ bit $F = (f_1, f_2, \ldots, f_i)$ through data $D = (d_1, d_2, \ldots, d_i)$. And require:

$$\begin{cases} T \bmod P == 0 \\ T = 2^{n-k}D + F \end{cases} \tag{2}$$

Before sending, $T = (d_1{+}f_1, d_2{+}f_2, \ldots, d_i{+}f_i)$ is generated according to the above formula and sent to the receiver. Algorithm 1 shows the encryption and verification process.

Once the data is received, it will be validated. After successful data validation, the data will be decrypted in the opposite way of the encryption algorithm, as in Algorithm 2.

V. EXPERIMENTS AND EVALUATION

Here, we analyze the security of the model and describe the time and space complexity and other hardware costs of the model. In this part, the experiment simulates the communication of the decryption and verification algorithm in PortableLab.

A. EXPERIMENTS SETTING

The control executed in this experiment is stm32f103ze, and the wireless module is ESP8266. It uses different external crystals to test the time required for the AES and CRC algorithm to execute in stm32f103ze and judge the feasibility by time. The controller performed in this experiment is stm32f103ze, and the wireless module is ESP8266. It utilizes

different external crystals to test the time required for the AES-ECB model and CRC algorithm to execute in stm32f103ze and judge the feasibility by time. In Table 1, different types of STM32 microcontrollers, according to different performances, are listed.

B. SECURITY ANALYSIS

The key is the most essential concern for cryptographic algorithms, and attempts to analyze the key are called attacks. Typical attacks are brute force attacks, differential cryptanalysis, and square attacks. Therefore, key crack may not be feasible due to the following:

a) Brute Force Attack. Let 2^k is the key length (in bits), the attacker will decrypt the intercepted ciphertext with all possible 2^k keys until a meaningful block of plaintext is acquired. After obtaining the plaintext, the attacker compares the corresponding keys for decryption until they are equivalent. Then, the key is adopted to verify the correctness of the other plaintexts. A brute force attack with an average time complexity of 2^{k-1} encryption would entail 2^{k-1} rounds of encryption.

b) Differential cryptanalysis. In the differential cryptanalysis a principle, let (X,+) be a finite group of exchanges. $\Delta x = x_1 - x_2$ is the difference between x_1 and x_2. The function $f : X \to Y$, Δx is the input difference of $f(x)$, and $\Delta f(x)$ is the output difference corresponding to (x_1, x_2). Therefore, the differential corresponds to the following transition probability.

$$P_f(\alpha, \beta) = \frac{1}{|X|^2} \times \{(x_1, x_2) : f(x_1) - f(x_2) = \beta | x_1 - x_2 = \alpha\} \quad (3)$$

A differential distribution matrix is a matrix D_f with $P_f(\alpha, \beta)$ as the value of β rows and α columns.When the key is deciphered by differential cryptanalysis, the attacker requires many plaintext pairs. In [26], the time complexity corresponding to the aes-129 7-round attack requires $2^{192.2}$ table checks to select the number of plaintexts. However, a round of encryption with a time complexity equivalent to 20 table lookups corresponds to a time complexity of about 2^{125} times. The key isn't taken for different chip types, so the solution will be impossible to crack our model.

c) Square attacks. Square was proposed by Rijndael's designer as one of the most effective options for plaintext attacks. In a round of keys, since each round can crack the previous round of keys when a particular round is cracked, it is possible to derive all the subkeys. The Square attack is the process of guessing and determining the subkey, and when the guess is correct, the entire key is defeated. In [27], Tunstall derives an attack complexity of 2^{154} for seven rounds but cannot threaten AES-192 except for quantum computation.

C. MEMORY CONSUMPTION

When decrypting the verification, the required algorithm cost should be considered. The following time complexity function is utilized to evaluate the algorithm.

$$T(n) = O(f_{add}(n)) + O(f_{sub}(n)) + O(f_{mix}(n)) + O(f_{shitf}(n)) \quad (4)$$

where $O(f_{add}(n))$ is equal to $O(logN)$, $O(f_{sub}(n))$, $O(f_{mix}(n))$ and $O(f_{shift}(n))$ are equal to $O(1)$, $O(logN)$ and $O(N)$ respectively. For the algorithm space occupation, only the s-box in the AES algorithm takes a lot of space. However, due to the fixed s-box, the space complexity is constant.

In the market, the price of STM32F103 is lower than $1, which can be repeated utilization. ESP8266 integrates ultra-low-power 32-bit miniature in a smaller size. It supports RTOS, IEEE802.11 b/g/n protocol, and a complete TCP / IP protocol stack. The price of an ESP8266 is lower than $1.5, and it can be repeated utilization.

D. TIME CONSUMPTION

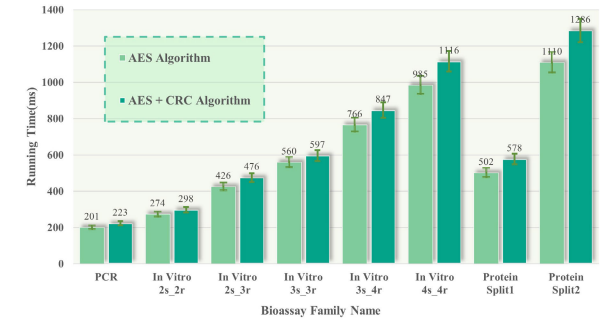
Table 2 lists the program size and flash consumption of 10 different protocols in different layouts after dictionary compression in conjunction with state machine optimization. The ten protocols are *PCR and invitro 2S_ 2r, InVitro 2s_ 3r, InVitro 3s_ 3r, InVitro 3s_ 4r, InVitro 4s_ 4r, Protein, Protein split1, Protein split2, and Protein split3*. These detection protocols are ten common benchmarks in peer-review publications [13]. The dictionary is represented as a vector of bit vector D, and the hash table H is utilized to improve performance. Let S_i be the ith state of the linear Moore machine and B_i be the corresponding bit vector. Initially, both D and H are empty. Each operation phase is transformed into a loop to reduce the number of states, while the routing phase (assuming no repetition) maintains the linear structure of the original state machine. The boundary between the operation and routing phases is determined by scheduling, placement, and routing solutions; extracting this information from bit vector sequences is unnecessary. These operations will cause the droplets in DMFB to decompose,

TABLE 1. Multiple stm32-based microcontrollers.

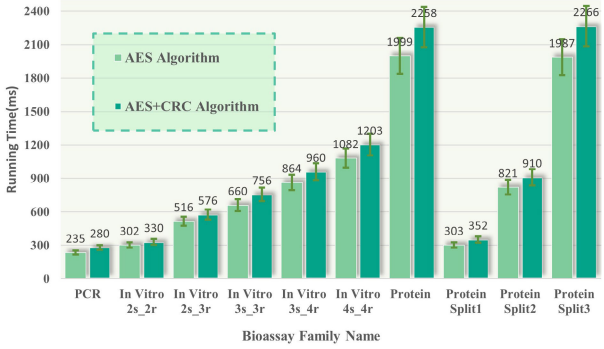
Chip model	Kernel	Word size	Fmax	Flash	Voltage
STM32L0xx	Cortex-M0	32bit	32MHz	64KB	1.71-3.6V
STM32F1xx	Cortex-M3	32bit	72MHz	64KB	2.0-3.6V
STM32F4xx	Cortex-M4	32bit	168MHz	192KB	1.8-3.6V

TABLE 2. Program size(KB) and flash occupation(Bit) in different placer.

Method	KAMER Placer		Virtual Topology Placer	
	Program Size	Flash Occupation	Program Size	Flash Occupation
PCR	4608	6537	5632	7544
IV 2s_2r	6144	8056	7,168	9080
IV 2s_3r	10240	12152	11776	13688
IV 3s_3r	12800	14712	16384	18296
IV 3s_4r	18432	20344	18432	20344
IV 4s_4r	29184	31096	29184	31096
Pr	FAIL	FAIL	48128	50040
Pr Split1	20992	22904	7680	9592
Pr Split2	35328	37240	19456	21368
Pr Split3	FAIL	FAIL	47616	49528



(a) KAMER Placer



(b) Virtual Topology Placer

FIGURE 6. **Runtime on different protocols.**

mix, and detect. After a series of operations, the DMFB will output the reaction results, and the microcontroller will give feedback on the results to the biological and chemical engineers.

The model needs to decrypt and validate the program. When decrypting, the framework needs to consider the program's running time. Because the execution of the microcontroller will cause the corresponding energy consumption, these protocols utilize different placement methods: keep all maximum empty rectangles (KAMER) and virtual topology (VT). KAMER is when an operation is generated; it will search a data structure that stores the maximum empty rectangles (MERs) and select an MER to place. The MER will be rebuilt when the operation is complete. Instead, the virtual topology identifies chip regions in advance to ensure reasonable routing paths between the regions. When a function is generated, the virtual topology can select any free region that supports the operation. In Figure 5, the maximum transmission time of the scheme is less than 2.5s. Therefore, the scheme is feasible in terms of time. The minimum flash memory space of STM32F103 is 16kb, which can also satisfy the experimental requirements.

VI. CONCLUSION

This paper studies the problem of general-purpose DMFB transmitting biological protocol remotely and proposes a PortableLab with a wireless module. Meanwhile, encryption and authentication algorithms ensure data transfer security between the microcontroller and the server. With this model, the DMFB enables the remote transmission of biological protocols at a cost that only slightly increases the completion time of the bioassay. In the future, cryptographic algorithms and the compatibility of biochips with wireless modules could be optimized to optimize time and space.

REFERENCES

[1] M. Alistar and U. Gaudenz, "OpenDrop: An integrated do-it-yourself platform for personal use of biochips," *Bioengineering*, vol. 4, no. 2, p. 45, May 2017.

[2] AXA. (2023). *Mind-Health-Report*. [Online]. Available: https://www.axa.com/en/about-us/mind-health-report

[3] Q. Hong, Z. Chen, C. Dong, and Q. Xiong, "A dynamic demand-driven smart manufacturing for mass individualization production," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2021, pp. 3297–3302.

[4] C. Dong, Y. Yao, Y. Xu, X. Liu, Y. Wang, H. Zhang, and L. Xu, "A cost-driven method for deep-learning-based hardware trojan detection," *Sensors*, vol. 23, no. 12, p. 5503, Jun. 2023.

[5] S. Bhatia, A. K. Dubey, R. Chhikara, P. Chaudhary, and A. Kumar, *Intelligent Healthcare*. Cham, Switzerland: Springer, 2021.

[6] S. S. Ali, M. Ibrahim, O. Sinanoglu, K. Chakrabarty, and R. Karri, "Security assessment of cyberphysical digital microfluidic biochips," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 13, no. 3, pp. 445–458, May 2016.

[7] *Global Microfluidics Market Will Surpass USD 12,380 Million By 2025*. [Online]. Available: https://www.zionmarketresearch.com/

[8] X. Huang, T.-Y. Ho, W. Guo, B. Li, and U. Schlichtmann, "MiniControl: Synthesis of continuous-flow microfluidics with strictly constrained control ports," in *Proc. 56th ACM/IEEE Design Autom. Conf. (DAC)*, Las Vegas, NV, USA, Jun. 2019, pp. 1–6.

[9] C.-W. Hsieh, Z. Li, and T.-Y. Ho, "Piracy prevention of digital microfluidic biochips," in *Proc. 22nd Asia South Pacific Design Autom. Conf.*, Chiba, Japan, Jan. 2017, pp. 512–517.

[10] C. Dong, L. Liu, H. Liu, W. Guo, X. Huang, S. Lian, X. Liu, and T.-Y. Ho, "A survey of DMFBs security: State-of-the-art attack and defense," in *Proc. 21st Int. Symp. Quality Electron. Design (ISQED)*, Santa Clara, CA, USA, Mar. 2020, pp. 14–20.

[11] M. Jalalitabar, M. Valero, and A. G. Bourgeois, "Demonstrating the threat of hardware trojans in wireless sensor networks," in *Proc. 24th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Las Vegas, NV, USA, Aug. 2015, pp. 1–8.

[12] A. Reyhani-Masoleh, M. Taha, and D. Ashmawy, "New area record for the AES combined S-box/inverse S-box," in *Proc. IEEE 25th Symp. Comput. Arithmetic (ARITH)*, Los Alamitos, CA, USA, Jun. 2018, pp. 145–152.

[13] D. Grissom, C. Curtis, S. Windh, C. Phung, N. Kumar, Z. Zimmerman, J. McDaniel, N. Liao, and P. Brisk, "An open-source compiler and PCB synthesis tool for digital microfluidic biochips," *Integr., VLSI J.*, vol. 51, pp. 169–193, Sep. 2015.

[14] K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "INFECT: INconspicuous FEC-based trojan: A hardware attack on an 802.11a/g wireless network," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, McLean, VA, USA, May 2017, pp. 90–94.

[15] C.-Y. Lin, J.-D. Huang, H. Yao, and T.-Y. Ho, "A comprehensive security system for digital microfluidic biochips," in *Proc. IEEE Int. Test Conf. Asia (ITC-Asia)*, Harbin, China, Aug. 2018, pp. 151–156.

[16] J. Washburn and D. S. Millington, "Digital microfluidics in newborn screening for mucopolysaccharidoses: A progress report," *Int. J. Neonatal Screening*, vol. 6, no. 4, p. 78, Oct. 2020.

[17] S. Bhattacharjee, Y.-L. Chen, J.-D. Huang, and B. B. Bhattacharya, "Concentration-resilient mixture preparation with digital microfluidic lab-on-chip," *ACM Trans. Embedded Comput. Syst.*, vol. 17, no. 2, pp. 1–12, Mar. 2018.

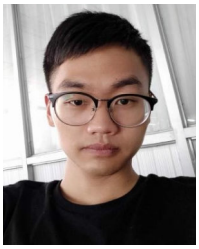
[18] S. Momtahen, M. Taajobian, and A. Jahanian, "Drug discovery acceleration using digital microfluidic biochip architecture and computer-aided-design flow," *Int. J. Eng.*, vol. 32, no. 8, pp. 1169–1176, 2019.

[19] W. Guo, S. Lian, C. Dong, Z. Chen, and X. Huang, "A survey on security of digital microfluidic biochips: Technology, attack, and defense," *ACM Trans. Design Autom. Electron. Syst.*, vol. 27, no. 4, pp. 1–33, Jul. 2022.

[20] D. Grissom and P. Brisk, "A field-programmable pin-constrained digital microfluidic biochip," in *Proc. 50th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, May 2013, pp. 1–9.
[21] R. Fobel, C. Fobel, and A. R. Wheeler, "DropBot: An open-source digital microfluidic control system with precise control of electrostatic driving force and instantaneous drop velocity measurement," *Appl. Phys. Lett.*, vol. 102, no. 19, pp. 1–10, May 2013.
[22] M. G. Pollack, V. K. Pamula, V. Srinivasan, and A. E. Eckhardt, "Applications of electrowetting-based digital microfluidics in clinical diagnostics," *Expert Rev. Mol. Diag.*, vol. 11, no. 4, pp. 393–407, May 2011.
[23] H.-H. Shen, S.-K. Fan, C.-J. Kim, and D.-J. Yao, "EWOD microfluidic systems for biomedical applications," *Microfluidics Nanofluidics*, vol. 16, no. 5, pp. 965–987, May 2014.
[24] M. J. Jebrail, M. S. Bartsch, and K. D. Patel, "Digital microfluidics: A versatile tool for applications in chemistry, biology and medicine," *Lab Chip*, vol. 12, no. 14, p. 2452, 2012.
[25] E. Wulff-Burchfield, W. A. Schell, A. E. Eckhardt, M. G. Pollack, Z. Hua, J. L. Rouse, V. K. Pamula, V. Srinivasan, J. L. Benton, B. D. Alexander, D. A. Wilfret, M. Kraft, C. B. Cairns, J. R. Perfect, and T. G. Mitchell, "Microfluidic platform versus conventional real-time polymerase chain reaction for the detection of mycoplasma pneumoniae in respiratory specimens," *Diagnostic Microbiol. Infectious Disease*, vol. 67, no. 1, pp. 22–29, May 2010.
[26] J. Lu, O. Dunkelman, N. Keller, and J. Kim, "New impossible differential attacks on AES," in *Proc. 9th Int. Conf. Cryptol.*, D. R. Chowdhury, V. Rijmen, and A. Das, Eds. Berlin, Germany, 2008, pp. 279–293.
[27] M. Tunstall, "Improved 'partial sums'-based square attack on AES," in *Proc. 9th Int. Joint Conf. E-Business Telecommun. (ICETE)*, Rome, Italy, 2012, pp. 25–34.

YINAN YAO (Member, IEEE) was born in Zhejiang, China. He is currently pursuing the degree with the College of Computer and Data Science, Fuzhou University. He has published several papers and received one computer software copyright registration during his graduate studies. He has contributed to two monographs in the field of security. His research interests include biochips, integrated circuit security, and privacy protection. He is a member of CCF. He was a recipient of the University's Outstanding Student Scholarship, from 2017 to 2020, and the Outstanding Undergraduate Graduate Award. In 2023, he received the Graduate Outstanding Student Scholarship.

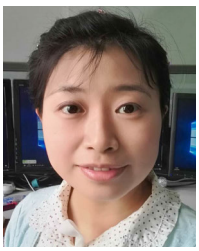
DECHENG QIU was born in Guangdong, China. He is currently pursuing the M.S. degree with the College of Computer and Data Science, Fuzhou University, China. His research interests include artificial intelligence and hardware security.



HUANGDA LIU received the degree from the College of Computer and Data Science, Fuzhou University. His research interests include intelligent computing, integrated circuit security, and security design.

ZHONGLIAO YANG was born in Guizhou, China. He is currently pursuing the degree with the College of Computer and Data Science, Fuzhou University. His research interests include digital microfluidic biochip heuristic algorithms and security design.

XIMENG LIU (Senior Member, IEEE) received the B.Sc. degree in electronic engineering and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2010 and 2015, respectively. He is currently a Full Professor with the College of College of Computer and Data Science, Fuzhou University. He is also a Research Fellow with the School of Information Systems, Singapore Management University, Singapore. He has published more than 100 articles on the topics of cloud security and big data security, including articles in IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON SERVICE COMPUTING, and IEEE INTERNET OF THINGS JOURNAL. His research interests include cloud security, applied cryptography, and big data security. He is a member of ACM and CCF. He was awarded the Minjiang Scholars Distinguished Professor, the Qishan Scholars at Fuzhou University, and the ACM SIGSAC China Rising Star Award, in 2018. He served as a Program Committee Member for several conferences, such as the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, the 2017 IEEE Global Communications Conference, and the 2016 IEEE Global Communications Conference. He served as the Lead Guest Editor for *Wireless Communications* and *Mobile Computing*.



YANG YANG (Member, IEEE) received the B.Sc. and Ph.D. degrees from Xidian University, Xi'an, China, in 2006 and 2011, respectively. She is currently a Full Professor with the College of Computer Science and Big Data, Fuzhou University. She is also a Research Fellow with the School of Computing and Information Systems, Singapore Management University. She has published more than 60 articles in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON SERVICES COMPUTING, IEEE TRANSACTIONS ON CLOUD COMPUTING, and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. Her research interests include information security and privacy protection.

CHEN DONG (Member, IEEE) received the B.S. and M.S. degrees from the College of Computer and Data Science, Fuzhou University, China, in 2002 and 2005, respectively, and the Ph.D. degree in computer science from the Computer School, Wuhan University, China, in 2011. She was a Visiting Researcher with the University of California at Los Angeles, from 2015 to 2016. She is currently an Associate Professor with the College of Computer and Data Science, Fuzhou University. Her research interests include artificial intelligence, hardware security, intelligent computing, and integrated circuit physical design.