# MEDAguard:基于逻辑加密的微电极点阵生物芯片知识产权保护方案

刘灵清[1],董 晨[1,3],刘西蒙[1,2],柳煌达[1],连思璜[1],陈 潇[1]
(1. 福州大学计算机与大数据学院,福建福州 350116; 2. 网络系统信息安全福建省高校重点实验室,福建福州 350116;
3. 福建省网络计算与智能信息处理重点实验室,福建福州 350116)

**摘 要:** 在微电极点阵(Micro-Electrode-Dot-Array,MEDA)生物芯片外包生产的过程中,未受保护的芯片设计知识产权容易遭受盗窃或过度生产攻击.本文提出一种基于逻辑加密的微电极点阵生物芯片的知识产权保护方案,称为MEDAguard,该方案使用生化协议中的废液滴和输入液滴构成逻辑加密模块,实现对生化协议的锁定,从而保护生化协议在外包生产过程中不被窃取.针对破解密钥最常用的暴力攻击法,提出一种安全性评价指标,用于评估生成的生化试剂是否符合浓度标准.采用多组仿真实验模拟攻击者对MEDAguard实施暴力攻击,实验结果表明MEDAguard能够有效地抵抗暴力攻击.

**关键词:** 微电极点阵;生物芯片;逻辑加密;知识产权保护;外包生产
**中图分类号:** TP309 **文献标识码:** A **文章编号:** 0372-2112(2022)02-0440-06
**电子学报URL:**http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210556

# MEDAguard: A Logic Encryption Scheme for Micro-Electrode-Dot-Array Biochips IP Protection

LIU Ling-qing[1], DONG Chen[1,3], LIU Xi-meng[1,2], LIU Huang-da[1], LIAN Si-huang[1], CHEN Xiao[1]
(1. *College of Computer and Data Science, Fuzhou University, Fuzhou, Fujian* 350116, *China*;
2. *Key Laboratory of Information Security of Network Systems, Fuzhou University, Fuzhou, Fujian* 350116, *China*;
3. *Fujian Key Laboratory of Network Computing and Intelligent Information Processing, Fuzhou University, Fuzhou, Fujian* 350116, *China*)

**Abstract:** In the process of outsourcing the production of micro-electrode-dot-array(MEDA) biochips, the unprotected IP(intellectual property) of the chip design is vulnerable to theft or overproduction attacks. This paper proposes a logic encryption-based IP protection scheme for micro-electrode-dot-array biochips, called MEDAguard, which uses waste droplets and input droplets from bioassay to form logic encryption modules to lock the bioassay, thereby protecting it from theft during the outsourcing process. In addition, a security evaluation metric is proposed to assess whether the generated biochemical reagents meet the concentration criteria for compliance against the brute-force attack method most commonly used to break the key. Finally, several simulations are used to simulate a brute-force attack on MEDAguard, and the results show that MEDAguard can effectively resist brute-force attacks.

**Key words:** micro-electrode-dot-array; biochip; logic encryption; intellectual property protection; outsourcing production

## 1 引言

生物芯片(biochip)是一种新兴的生化试剂制备平台,其工作的核心是用机器自动化制备试剂以替代人工操作.相较于传统实验室中的人工操作,生物芯片具有高度自动化、精细化、可大规模部署和分析速度快等优点.随着产业化的推进,生物芯片带来的巨大社会及经济效益不容小觑.

数字微流控生物芯片(Digital MicroFluidic Biochip,DMFB)是生物芯片领域研究的主要方向之一[1].作为数字微流控生物芯片的最新代产品,基于微电极点阵

收稿日期:2021-04-30;修回日期:2021-09-14;责任编辑:覃怀银
基金项目:国家自然科学基金(No.62072109,No.U1804263);福建省自然科学基金(No.2020J01500)

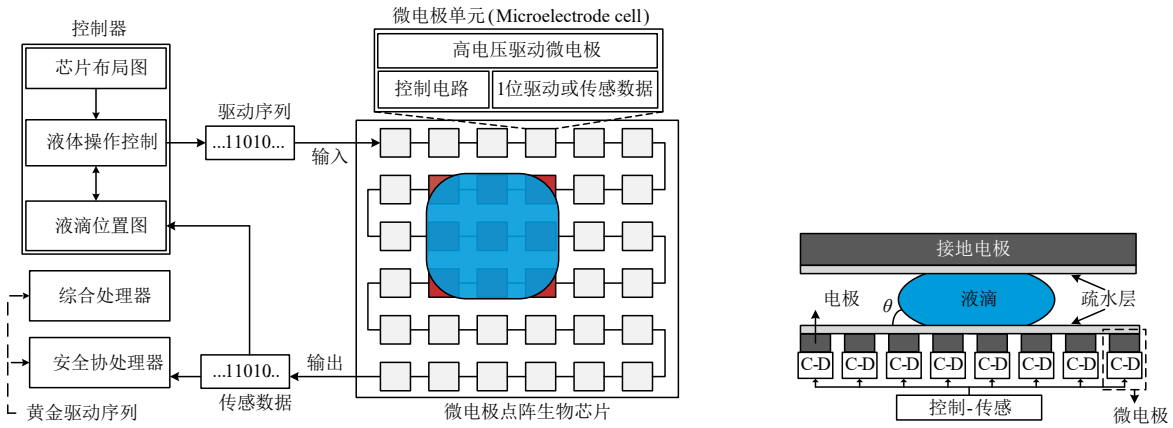
(Micro-Electrode-Dot-Array,MEDA)架构的数字微流控生物芯片(后文简称为微电极点阵生物芯片)正逐渐被学术界所关注. 微电极点阵生物芯片中的电极比传统数字微流控生物芯片的电极小10到20倍[2],这使得微电极点阵生物芯片能够突破传统数字微流控生物芯片的资源限制,实现对液滴的精细化控制[3]、对液滴路径的实时监控[4]和对角移动液滴[5]等操作.

微电极点阵生物芯片作为一个新兴的产品,未来市场价值可期,保护知识产权不被盗取是首当其冲的安全问题. 目前涉及微电极点阵生物芯片的知识产权保护领域的研究十分稀少. Liang等人[6]设计了一种应用于微电极点阵生物芯片的可编程的菊花链(daisy-chain)结构. 可编程的菊花链结构为微电极点阵生物芯片提供一次性可编程的能力,用于加密知识产权. 然而,这种方法需要大约0.4%的额外空间开销. Bhattacharjee等人[7]提出了一种虚假的混合-分离操作(dummy mix-split operations)来加密微流控生物芯片的生化协议. 这个方案需要在生化协议中插入额外的混合-分离操作.

## 2　背景

### 2.1　微电极点阵生物芯片的架构

如图1(*a*)中所示,微电极点阵生物芯片系统包括控制器、综合处理器、安全协处理器和微电极生物芯片. 微电极生物芯片的侧视图如图1(*b*),主体部分由两块间隔的平板构成,其中顶板作为接地电极,底板下有一个二维微电极阵列,液滴在顶板和底板之间移动,液滴与底板的接触角为$\theta$. 微电极单元包括一个高电压驱动微电极、控制电路和传感电路. 相邻的微电极单元被连接在一起构成菊花链.




(*a*)　微电极点阵生物芯片的结构示意图　　(*b*)　微电极点阵生物芯片侧视图

图1　微电极点阵生物芯片的架构

### 2.2　微电极点阵生物芯片工作原理

生物芯片使用微流控技术,工作原理大致上可以分为两种,一种在电极上施加电压控制离散液滴,另一种通过阀门控制流体流动[8,9]. 微电极点阵生物芯片采用第一种工作原理,通过施加一系列的电压调整液滴与平板之间的接触角$\theta(V)$[10],控制离散的液滴在两块平板之间移动,这应用了EWOD(ElectroWetting-On-Dielectric)原理,可用Lippmann-Young方程建模:

$$\cos\theta(V)=\cos\theta(0)+\left(\frac{\epsilon_0\epsilon_r}{2d\mathrm{Y}_{\mathrm{LG}}}\right)V^2 \tag{1}$$

其中$V$是两块平板间的电压,$\theta(0)$是未施加电压时的平衡接触角,$\epsilon_0$是真空中的介电常数,$\epsilon_r$是底部绝缘体的介电常数,$d$是其厚度,$\mathrm{Y}_{\mathrm{LG}}$是气体和液体界面的张力.

微电极点阵生物芯片控制每个微电极单元上被施加的电压,精细化控制离散液滴,并实现一些生化试剂的基本操作,如混合、分离等,这些基本操作构成生化协议.

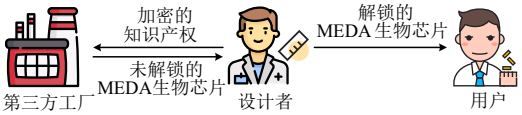
### 2.3　不可信的外包制造流程

设计者拥有知识产权. 微电极点阵生物芯片的知识产权包括芯片布局(chip layout)和驱动序列. 设计者需要在芯片布局上实现生化协议以生成驱动序列. 传统的微电极点阵生物芯片设计与制造的流程如图2(*a*)所示. 设计者将芯片设计版图和驱动序列发送给第三方工厂. 第三方工厂制造芯片并集成驱动序列即为微电极点阵生物芯片. 最终,微电极点阵生物芯片被销售给用户. 上述的设计和制造流程将设计与制造的过程分离,简化了生产的复杂性. 然而,制造过程中引入了不可信的第三方. 知识产权持有者将知识产权发送给第三方工厂后,知识产权即面临潜在的安全威胁,如针对知识产权的盗窃或过度生产攻击.

为保护知识产权在设计与制造过程中的安全性,

本文提出一种增强的微电极点阵生物芯片设计与制造流程,如图2(*b*)所示. 设计者对知识产权进行加密后送往第三方工厂进行代工制造,在制造的过程中知识产权对于第三方工厂相当于一个黑盒. 制造完成后,第三方工厂将未解锁的微电极点阵生物芯片发送给设计者,由设计者解锁后再销售给用户.


(*a*) 传统的微电极点阵生物芯片设计与制造流程




(*b*) 增强的微电极点阵生物芯片设计与制造流程

图2 微电极点阵生物芯片设计与制造流程

## 3 微电极点阵生物芯片的知识产权保护方案

### 3.1 问题描述

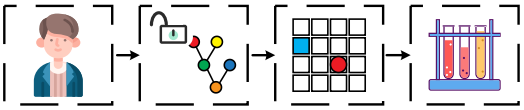
假设微电极点阵生物芯片的设计与制造流程如图2(*b*)所示. 本文需要解决的问题可以被描述为:

输入:(1)微电极点阵生物芯片的数字库中包括每种片上流体功能模块(如混合,分离和分配等)的尺寸、执行时间和位置. (2)生化协议通常被设计者制作成序列图(sequencing graph)的形式. 序列图通常是一个有向无环图 $G=(V,E)$,其中 $V=\{V_1,V_2,\cdots,V_L\}$ 代表在生化协议中的 $L$ 个操作,$E=\{(V_x,V_y),1\leqslant x,y\leqslant L\}$ 代表各个操作之间的依赖关系.

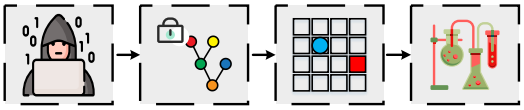
输出:一种对生化协议的知识产权保护方案.

### 3.2 MEDAguard的总体描述

微电极点阵生物芯片的知识产权大体上可分为两种类型:芯片设计版图和生化协议. 本文提出的MEDAguard方案通过在生化协议中插入额外的逻辑加密模块使得知识产权在生产的过程中近似于黑盒. 使用MEDAguard之后,正常用户和未授权的用户使用微电极点阵生物芯片的认证过程如图3(*a*)和3(*b*)所示. 在正常的销售渠道中,微电极点阵生物芯片在完成制造后送回设计者手中,设计者使用正确的激活密钥 $K$ 激活后销售给用户. 但如果攻击者与第三方工厂合作,过度生产一批非法的、未激活的微电极点阵生物芯片,此时攻击者就需要对 $K$ 进行破解. 在图3(*a*)中,用户从知识产权的持有者购买已解锁的微电极点阵生物芯片,在正常的使用流程下生成合格的试剂. 而在图3(*b*)中,攻击者通过过度生产攻击得到一批未经解锁的微电极点阵生物芯片,输入错误的激活密钥将会生成不合格的、无法达到要求的试剂.



(*a*) 用户正常使用已激活的微电极点阵生物芯片的流程



(*b*) 攻击者试图使用未激活的微电极点阵生物芯片的流程

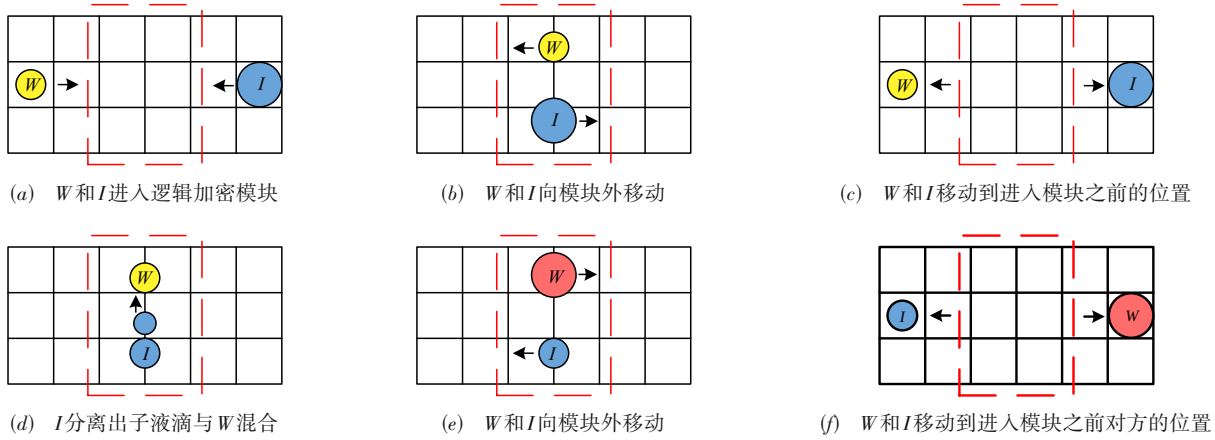
图3 微电极点阵生物芯片的使用流程

### 3.3 MEDAguard中逻辑加密模块的设计

受限于平台资源不足,数字微流控生物芯片只能提供(1:1)混合模型,即混合-分离操作仅能操控两个相同大小的液滴[11]. 作为下一代的数字微流控生物芯片,微电极点阵生物芯片提供($m$:$n$)混合模型,即多重混合模型. 在(1:1)混合模型中,大小相等的两个输入液滴进行混合,混合后的液滴分离成大小相等的两个输出液滴. ($m$:$n$)混合模型支持输入两个任意大小的液滴,进行混合,并将混合后的液滴分离成两个任意大小的液滴,分离比例即 $m$ 和 $n$ 由设计者指定.

MEDAguard中逻辑加密模块的输入为废液滴和生化协议中的某一液滴,根据激活密钥是否与预设密钥相同执行不同的操作. 如果激活密钥与预设密钥符合,逻辑加密模块不对两个输入的液滴进行操作;但如果激活密钥与预设密钥不符合,逻辑加密模块将对两个输入的液滴进行交换.

逻辑加密模块工作流程的示例如图4所示. 图4(*a*)中的两个液滴 $W$ 和 $I$ 为逻辑加密模块的两个输入,分别代表废液滴和生化协议中的某一液滴. 在微电极的驱动下,两个液滴向中间移动. 当激活密钥正确时,逻辑加密模块将按照图中(*a*)→(*b*)→(*c*)的顺序进行. 在(*b*)阶段,$W$ 和 $I$ 进入逻辑加密模块的区域仅作停留就直接输出,不做任何操作. 当激活密钥错误时,逻辑加密模块将按照图中(*a*)→(*d*)→(*e*)→(*f*)的顺序进行. 在(*d*)阶段,$W$ 和 $I$ 将互相调整至对方的体积大小,如图4(*d*)中所示,此时 $I$ 的体积大于 $W$(如果 $W$ 的体积大于 $I$,操作将相反),$I$ 分离出子液滴与 $W$ 混合,混合后的 $W$ 和分离后的 $I$ 向模块外移动. 在(*f*)中 $W$ 和 $I$ 移动到进入模块之前对方的位置. 对比图4(*c*)和图4(*f*),输入错误的激活密钥,$W$ 和 $I$ 的位置和液滴大小都进行了交换,$W$ 替代 $I$ 进行后续的生化协议.

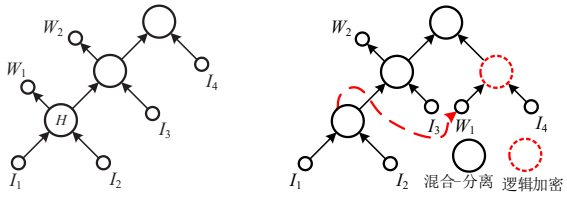



(a) W和I进入逻辑加密模块　(b) W和I向模块外移动　(c) W和I移动到进入模块之前的位置

(d) I分离出子液滴与W混合　(e) W和I向模块外移动　(f) W和I移动到进入模块之前对方的位置

图4　MEDAguard中逻辑加密模块工作流程的示例,其中W为废液滴,I为生化协议中的某一液滴,液滴的移动轨迹如箭头所示

接下来,以一个序列图为示例,说明插入逻辑加密模块到序列图的过程. 图5为在一个序列图中插入逻辑加密模块的例子. 图5(b)在原序列图中插入一个逻辑加密模块,$W_1$和$I_4$为逻辑加密模块的两个输入. $W_1$是混合-分离操作$H$的废弃液滴,$H$进行反应的时间先于逻辑加密模块. $H$的反应结束之后$W_1$停留在液滴储存区,等待$I_4$作为逻辑加密模块的输入,其逻辑路线如图中红色虚线所示. 生化反应进行到逻辑加密模块时,模块验证激活密钥,仅密钥正确时输出$I_4$.




(a) 示意序列图　(b) 插入逻辑加密模块后的序列图

图5　插入逻辑加密模块的示例序列图

### 3.4　逻辑加密模块的选择方案

插入逻辑加密模块的目标是使得攻击者输入错误的密钥时尽可能地影响生化协议的输出试剂,避免因输出试剂中各成分的浓度变化过小而被微电极点阵生物芯片的容错(fault tolerant)机制忽略.

为提高逻辑加密模块对输出试剂的影响,逻辑加密模块的影响因子应尽可能地大,逻辑加密模块的影响因子IF定义如下:

$$\mathrm{IF}=\frac{\mathrm{VAL}(I)}{\mathrm{OUT}}+\frac{\mathrm{VAL}(W)}{\mathrm{WASTE}} \tag{2}$$

其中,VAL(·)为当前液滴的质量函数,OUT代表输出试剂的质量,WASTE代表总废液滴的质量.

从影响因子的定义中可以看出,影响因子越大,攻击者输入错误的密钥对输出试剂的影响也越大. 插入的逻辑加密模块数量过多会影响生化协议的运行时间,应尽可能的控制逻辑加密模块的数量,为此设定一个阈值$\mathrm{IF}_{\mathrm{th}}$,插入的逻辑加密的影响因子应满足:

$$\mathrm{IF}_i\geqslant\mathrm{IF}_{\mathrm{th}},1\leqslant i\leqslant S \tag{3}$$

其中,$S$代表逻辑加密模块的总数.

## 4　安全性分析

### 4.1　暴力攻击

最简单、常见的暴力攻击是新兴平台最大的安全威胁. 通过使用暴力攻击,激活微电极点阵生物芯片时攻击者不需要获取平台内部的知识,仅通过逐个尝试即可非法地获取密钥. 因此,过小的密钥空间会使得攻击者有机可乘.

本文提出的MEDAguard方案,假设生化协议中包含$S$个逻辑加密模块,攻击者需要考虑的密钥空间大小为$2^S$. 随着逻辑加密模块的增加,攻击者需要探索的密钥空间呈指数级别增加,且微电极点阵生物芯片每运行一次生化协议需要消耗试剂和时间,因此只需插入合适数量的逻辑加密模块即可使攻击者使用暴力攻击的开销变得不可接受.

### 4.2　安全指标

最终的输出试剂需要与目标输出试剂进行比较,判断其中化合物的浓度是否在一定的误差范围之内. 对于不同的生化协议或者不同的激活密钥,生成的试剂都会有所不同. 本文提出的安全指标用于评估生化协议的输出试剂是否在误差允许的范围之内.

假设实际的输出试剂由$N$个输入试剂组成,$I$为输入试剂的集合,表示为$I=\{I_i,1\leqslant i\leqslant N\}$. 对实际的输出试剂进行生化分析,取其中的$q$,测量其中化合物的质量可得$I_i$质量集合$M=\{M_i,1\leqslant i\leqslant N\}$. 对目标生化协议中的输出试剂进行同样操作,可得目标$I_i$质量集合$G=\{G_i,1\leqslant i\leqslant N\}$. 设一个集合$E=\{E_i,1\leqslant i\leqslant N\}$,表示实际$I_i$

与目标$I_i$质量差的百分比，其中$E_i$可表示为

$$E_i=\frac{\left|M_i-G_i\right|}{G_i},1\leqslant i\leqslant N \tag{4}$$

由设计者为每个$I_i$指定一个可容许的最大质量差百分比$T=\{T_i,1\leqslant i\leqslant N\}$. 如果实际$I_i$与目标$I_i$的质量差的百分比小于$GE_i$，则可判断此化合物在输出试剂中的浓度符合标准. 故设一个0-1集合表示$E_i$是否在可容许的范围内，$B=\{B_i,1\leqslant i\leqslant N\}$，其中$B_i$的定义为

$$B_i=\begin{cases}0, \text{ if } E_i>T_i\\1, \text{ if } E_i\leqslant T_i\end{cases} \tag{5}$$

最后，引入一个安全指标(SeCurity, SC)用来评价实际的输出试剂是否符合标准，SC的定义为

$$\mathrm{SC}=\prod_{i=1}^{N}B_i \tag{6}$$

安全指标的算法流程归纳为算法1所示.

**算法1 安全指标**

**输入：**输入试剂集合$I$，输出试剂$O$，目标输出试剂$R$，$I$的质量集合$G$和可容许的最大质量差百分比$T$

**输出：**安全指标SC

取$q$ ml的$O$分析其中$I_i$的质量得到实际$I_i$的质量集合$M$
再取$q$ ml的$R$分析其中$I_i$的质量得到目标$I_i$的质量集合$G$
FOR $1\leqslant i\leqslant N$ DO
  计算实际$I_i$与目标$I_i$质量差的百分比
  $E_i\leftarrow|M_i-G_i|/G_i$
END FOR
FOR $1\leqslant i\leqslant N$ DO
  IF $E_i>T_i$ THEN
    $I_i$在$O$中的浓度不符合标准
    $B_i\leftarrow 0$
  ELSE
    $I_i$在$O$中的浓度符合标准
    $B_i\leftarrow 1$
  END IF
END FOR
FOR $1\leqslant i\leqslant N$ DO
  $\mathrm{SC}\leftarrow \mathrm{SC}\times B_i$
END FOR
RETURN SC

### 4.3 时间开销与空间开销

**时间开销：**MEDAguard在序列图中插入逻辑加密模块，由设计者输入解锁的密钥后生化协议照常运行，额外的时间开销来自插入的逻辑加密模块，因此时间开销为$O(n)$.

**空间开销：**本文提出的MEDAguard需要集成存储密钥的防篡改存储器. 防篡改存储器比一个微电极相比小得多，在微电极点阵生物芯片上集成了约1 800个微电极[7]，因此MEDAguard产生的额外空间开销可以忽略不计.

## 5 仿真实验及结果

本文使用Python在一台具有16 GB RAM、3.30 GHz Intel Core i5四核处理器和64位Windows 10操作系统的计算机上搭建仿真实验平台. 实验使用Python编写代码仿真模拟生化协议运行，并通过随机生成激活密钥模拟攻击者暴力攻击. 仿真实验中对两个加入MEDAguard方案的生化协议进行仿真，模拟攻击者在无正确密钥的情况下对MEDAguard进行暴力攻击，仿真实验结果如表1所示.

实验中使用随机生成的仅包含混合-分离操作的生化协议$\mathrm{biossay}_1$和$\mathrm{biossay}_2$，其构造如图5所示，因此混合-分离操作的数量与生化协议的长度成正比. $\mathrm{biossay}_1$实验的运行时间为2.53 s，$\mathrm{biossay}_2$实验的运行时间为3.81 s. 为简单起见，用于评价输出试剂的安全指标中的$T_i$相等，如$T=\{1/20,1/20,1/20,1/20\}$. 每个测试组包含1 000个随机序列(与正确密钥不同)作为激活密钥，故当安全指标SC=0时，MEDAguard防御暴力攻击成功，表中所示的百分比数据为当前生化协议在插入指定数量的逻辑加密模块时防御暴力攻击成功的比例.

从表1中的数据可以看出，总体上，随着$T_i$的减小和逻辑加密模块数量的增加，MEDAguard防御攻击者暴力攻击的成功率呈现上升的趋势，仅有少数的仿真实验组略有下降. 因此，若要提升安全性可提高检测的精度(减小$T_i$的值)或增加逻辑加密模块的数量. 实验中，$\mathrm{biossay}_2$实验组中在插入逻辑加密模块数量为3、7、10时，实验的运行时间分别为0.18 s、0.19 s、0.21 s，

**表1 暴力攻击仿真实验结果**

| 生化协议 | 混合-分离 | 逻辑加密模块 | $T_i=1/20$ | $T_i=1/50$ | $T_i=1/100$ | $T_i=1/500$ |
|---|---|---|---|---|---|---|
| | | 3 | 95.0% | 98.5% | 99.7% | 100.0% |
| $\mathrm{biossay}_1$ | 30 | 7 | 99.0% | 98.2% | 99.5% | 100.0% |
| | | 10 | 99.9% | 100.0% | 100.0% | 100.0% |
| | | 3 | 94.6% | 97.2% | 99.7% | 99.8% |
| $\mathrm{biossay}_2$ | 50 | 7 | 96.8% | 98.3% | 99.0% | 100.0% |
| | | 10 | 99.0% | 100.0% | 99.8% | 100.0% |

因此增加逻辑加密模块会额外增加生化协议的运行时间,故插入逻辑加密模块时需要同时考虑安全性和额外时间开销. 对比 $\text{biossay}_1$ 和 $\text{biossay}_2$,在同一 $T_i$ 值以及插入相同数量的逻辑加密模块的情况下,$\text{biossay}_1$ 防御暴力攻击的成功率相比于 $\text{biossay}_2$ 高. 根据 $\text{biossay}_1$ 和 $\text{biossay}_2$ 中的混合-分离操作数量可以推论:生化协议中混合-分离操作越多(生化协议的长度越长),为保持同等水平的安全性,需要插入的逻辑加密模块越多.

## 6　结语

本文提出了一种基于逻辑加密的微电极点阵生物芯片的知识产权保护方案 MEDAguard. MEDAguard 在生化协议中插入额外的逻辑加密模块,通过判断用户输入的激活密钥是否正确,决定是否用废液滴替换生化协议中的液滴. 仿真实验结果表明,MEDAguard 可以防御攻击者的暴力攻击,从而防范针对知识产权的盗版攻击和过度生产攻击.

### 参考文献


[1] DONG C, LIU L, LIU H, et al. A survey of DMFBs security: State-of-the-art attack and defense[C]//Proceedings of International Symposium on Quality Electronic Design. Santa Clara, USA: IEEE, 2020: 14-20.

[2] LAI K Y T, YANG Y T, LEE C Y. An intelligent digital microfluidic processor for biomedical detection[J]. Journal of Signal Processing Systems, 2015, 78(1): 85-93.

[3] SHAYAN M, BHATTACHARJEE S, LIANG T C, et al. Shadow attacks on MEDA biochips[C]//IEEE/ACM International Conference on Computer-Aided Design. San Diego, USA: IEEE, 2018: 1-8.

[4] KESZOCZE O, LI Z, GRIMMER A, et al. Exact routing for micro-electrode-dot-array digital microfluidic biochips[C]//Proceedings of the Asia and South Pacific Design Automation Conference. Chiba, Japan: IEEE, 2017: 708-713.

[5] ZHONG Z, LI Z, CHAKRABARTY K. Adaptive error recovery in MEDA biochips based on droplet-aliquot operations and predictive analysis[C]//IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers. Irvine, USA: IEEE, 2017: 615-622.

[6] LIANG T C, CHAKRABARTY K, KARRI R. Programmable daisychaining of microelectrodes to secure bioassay IP in MEDA biochips[J]. IEEE Transactions on Very Large Scale Integration Systems, 2020, 28(5): 1269-282.

[7] BHATTACHARJEE S, TANG J, PODDAR S, et al. Biochemical assay locking to thwart bio-IP theft[J]. ACM Transactions on Design Automation of Electronic Systems, 2019, 25(1): 1-20.

[8] MA J, LEE S M Y, YI C, et al. Controllable synthesis of functional nanoparticles by microfluidic platforms for biomedical applications-a review[J]. Lab on a Chip, 2017, 17(2): 209-226.

[9] LI C W, YU G, JIANG J, et al. A microfluidic linear node array for the study of protein-ligand interactions[J]. Lab on a Chip, 2014, 14(20): 3993-3999.

[10] HE J L, CHEN A Te, LEE J H, et al. Digital microfluidics for manipulation and analysis of a single cell[J]. International Journal of Molecular Sciences, 2015, 16(9): 22319-22332.

[11] LIANG T C, CHAN Y S, HO T Y, et al. Sample preparation for multiple-reactant bioassays on micro-electrode-dot-array biochips[C]//Proceedings of the Asia and South Pacific Design Automation Conference. New York, USA: ACM, 2019: 468-473.


### 作者简介


**刘灵清**　男,1997年生于福建福州. 现为福州大学计算机与大数据学院硕士研究生. 主要研究方向为生物芯片安全.
E-mail: liulqing07@foxmail.com

**董　晨(通讯作者)**　女,1979年生于陕西西安. 现为福州大学讲师、硕士生导师. 主要研究方向为集成电路、生物芯片、人工智能芯片安全设计、人工智能、大数据等.
E-mail: dongchen@fzu.edu.cn

**刘西蒙**　男,1988年生于陕西西安. 现为福州大学教授、博士生导师. 主要研究方向为隐私计算、密文数据挖掘、大数据隐私保护、可搜索加密等.
E-mail: snbnix@gmail.com

**柳煌达**　男,1997年生于福建泉州. 现为福州大学计算机与大数据学院硕士研究生. 主要研究方向为生物芯片安全、人工智能.
E-mail: hdaliu@foxmail.com

**连思璜**　女,1996年生于福建泉州. 现为福州大学计算机与大数据学院硕士研究生. 主要研究方向为生物芯片安全.
E-mail: sihlian@foxmail.com

**陈　潇**　女,1996年生于福建福州. 现为福州大学计算机与大数据学院硕士研究生. 主要研究方向为生物芯片安全.
E-mail: chenx2653@foxmail.com