Piracy Prevention of Digital Microfluidic Biochips

Ching-Wei Hsieh[1], Zipeng Li[2], and Tsung-Yi Ho[1]
[1]***National Tsing Hua Univ.*** [2]***Duke Univ.***

Outline

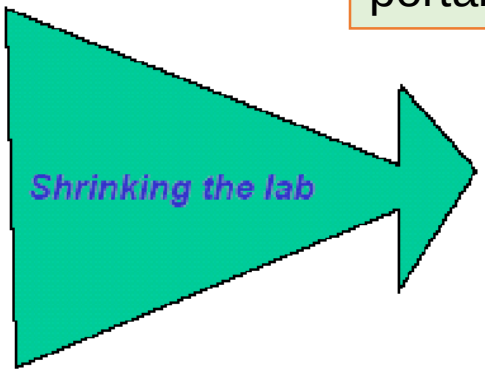
- Background
- Developed PUFs
- Authentication Flow of DMFBs
- Security Analysis
- Experiment
- Conclusions

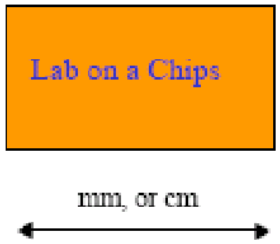
Biochips

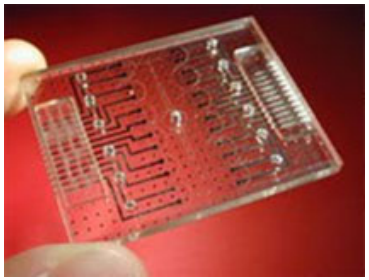
- What is biochip?
  - ➢Clinical diagnosis
  - ➢Environmental monitoring
  - ➢DNA analysis

Higher throughput, smaller sample/reagent consumption, better portability

Conventional Diagnostic Analyzer

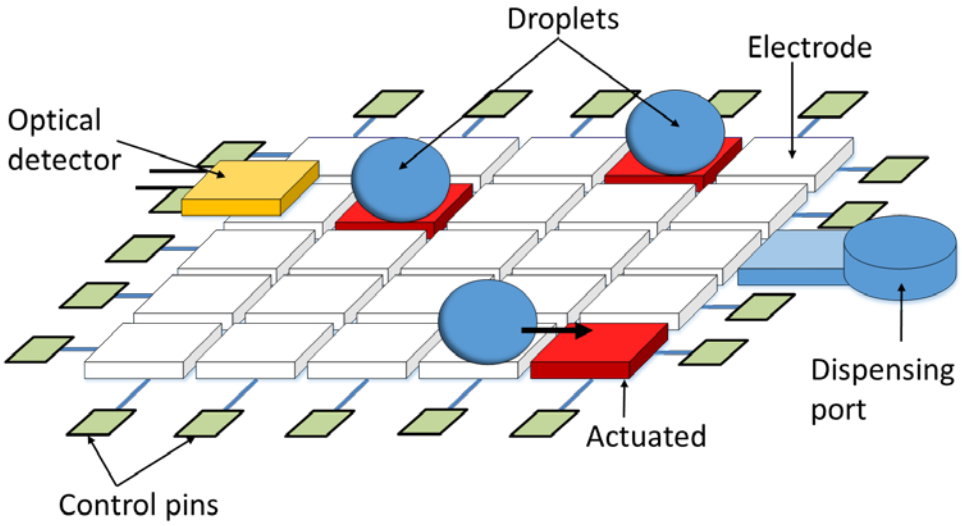


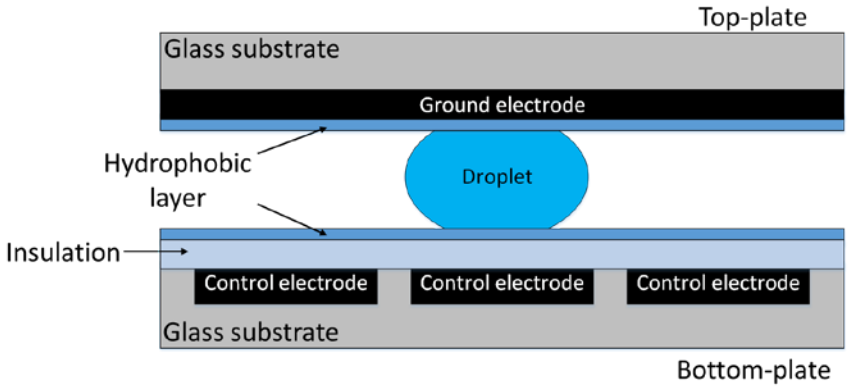




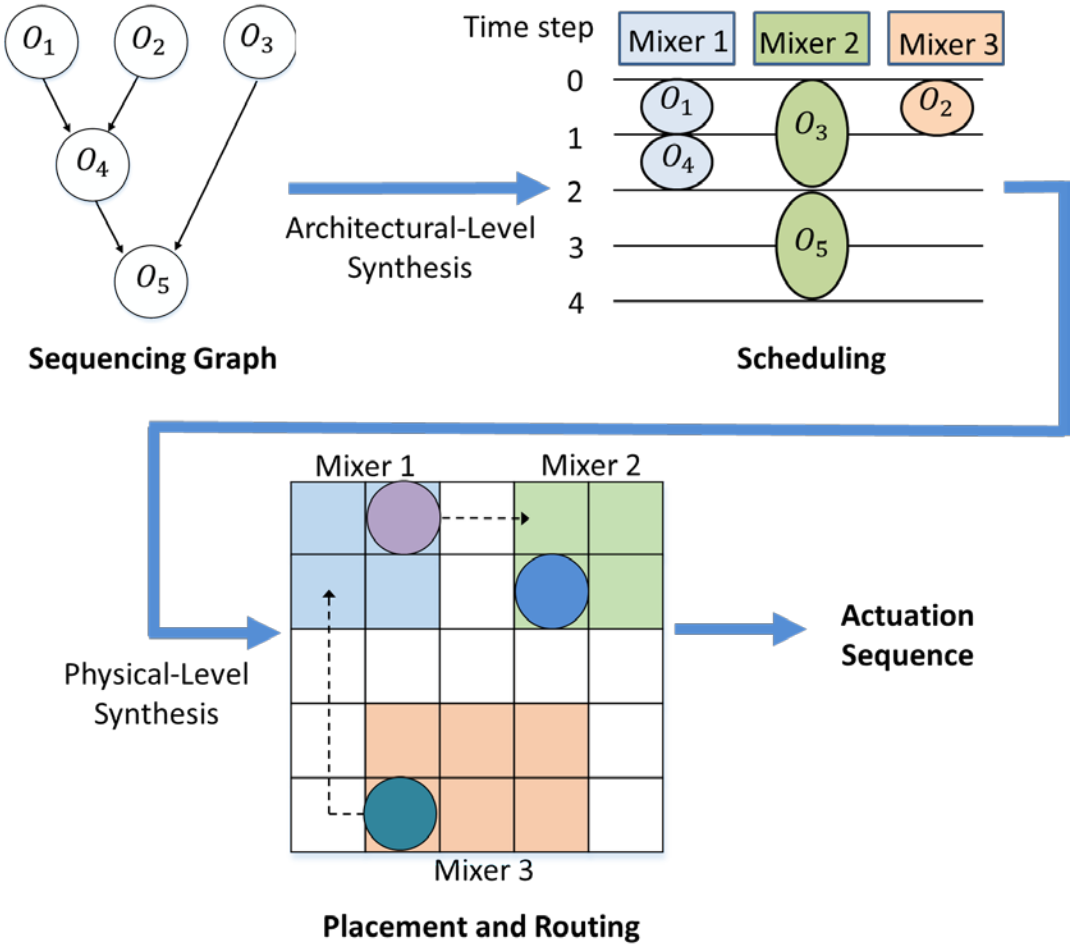
Digital Microfluidics

- Digital microfluidic biochip (DMFB)
  - ➢Droplets are addressed on an array of electrodes.
  - ➢Droplets can be manipulated by applying potential to electrodes based on the principle of Electrowetting on Dielectric (EWOD).





The CAD Flow of DMFBs



Security Vulnerability

- Over production
  - Fabricate more unauthorized DMFBs and sell them illegally.
- Counterfeiting
  - Recycle used DMFBs and sell them as new.
- Piracy attack
  - Intellectual Property (IP) stealing.

IC vs DMFB

- Conventional approach uses secret keys to perform authentication.

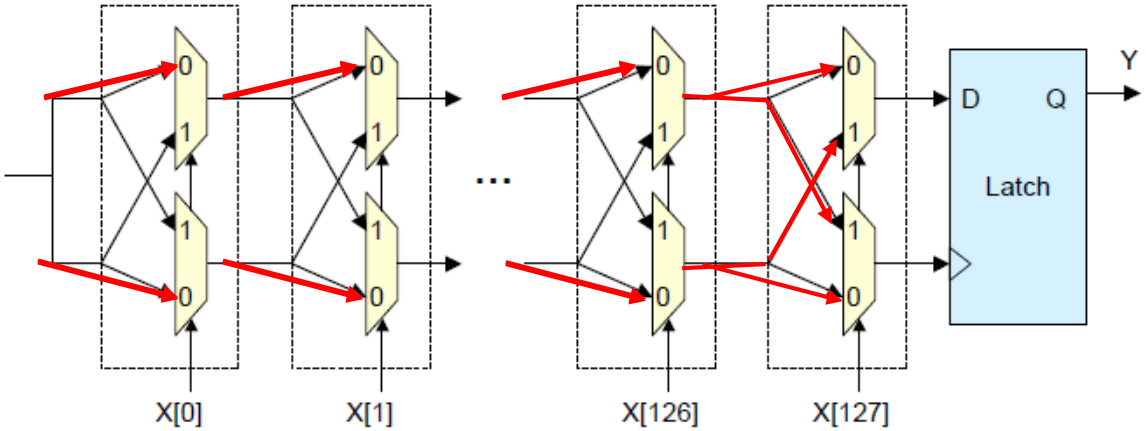
- There is no memory and logic gate integrated on DMFB to store secret keys.

Physical Unclonable Function (PUF)

- PUF is used to generate secret keys for performing authentication.
- PUF exploits the random physical variations to generate device-specific challenge response pairs (CRPs).
  - Persistent and Unpredictable
  - Unclonable
  - Tamper Evident

Arbiter PUF

- Delay paths with the same layout length



1 if top path is faster, else 0

128-bit Challenge

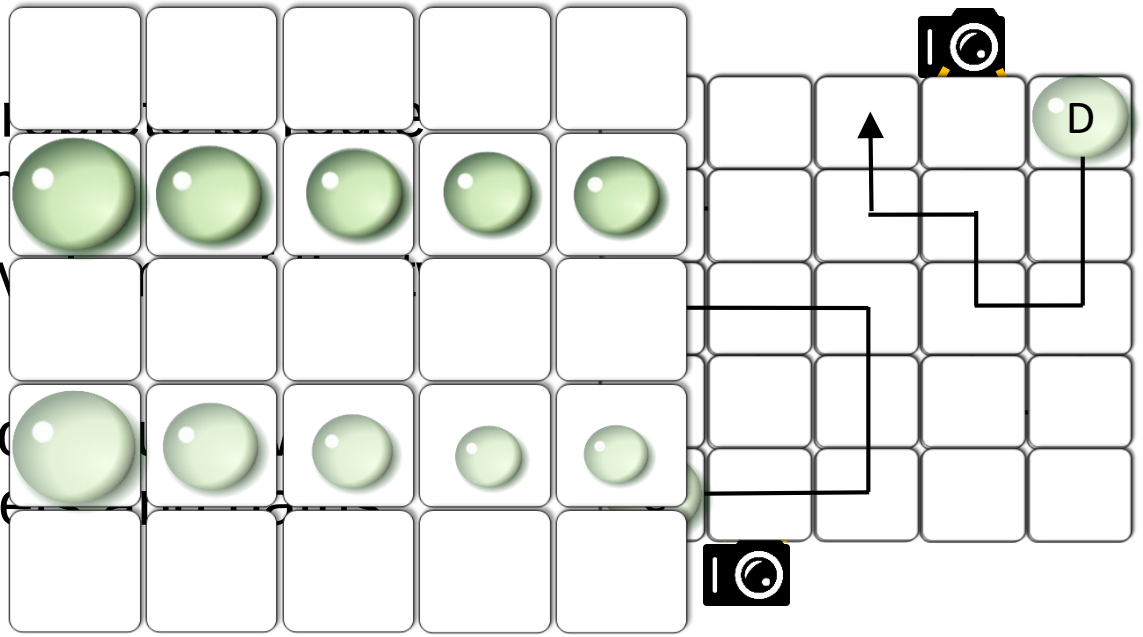
				Response
0	0	0	0	1
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1

G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in Proceedings of ACM/IEEE Design Automation Conference, pp. 9–14, 2007.

Route PUF

- Utilizes the variation during the droplet transportation.

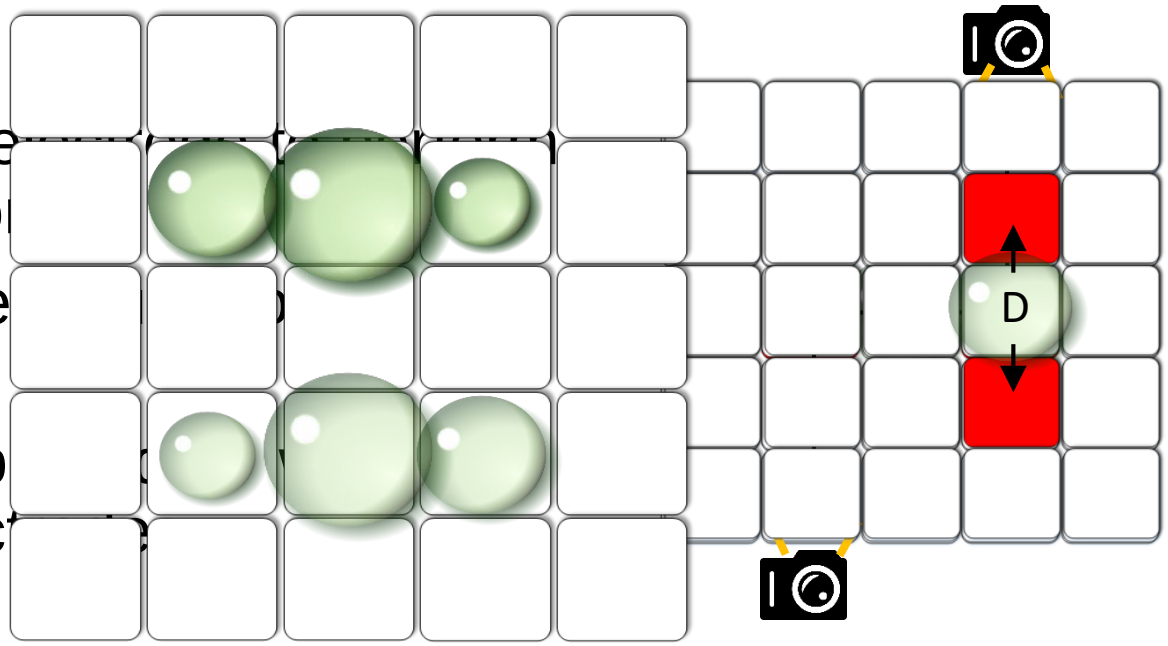
1. Choose two di
   in same distar
2. Compare the v
   droplets.
3. Repeat the pro
   different drople



Split PUF

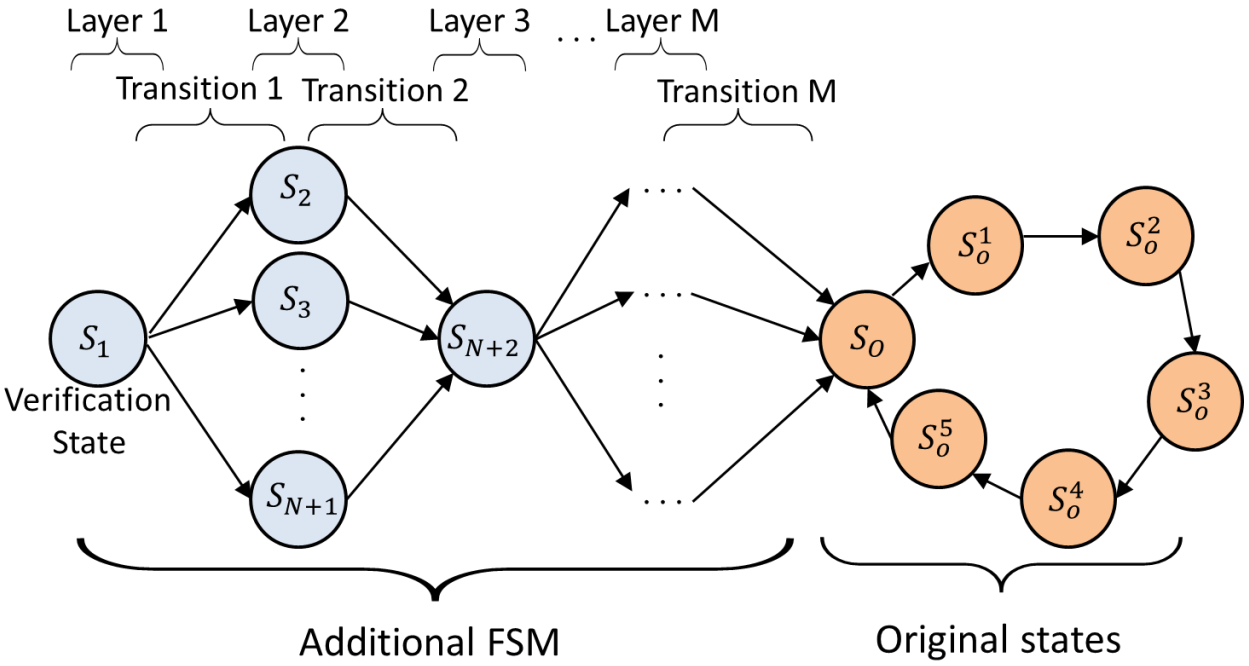
- Utilizes the volume difference of droplets after being split.

1. Choose the e
   split operatio
2. Compare the
   droplets.
3. Repeat the p
   different elec

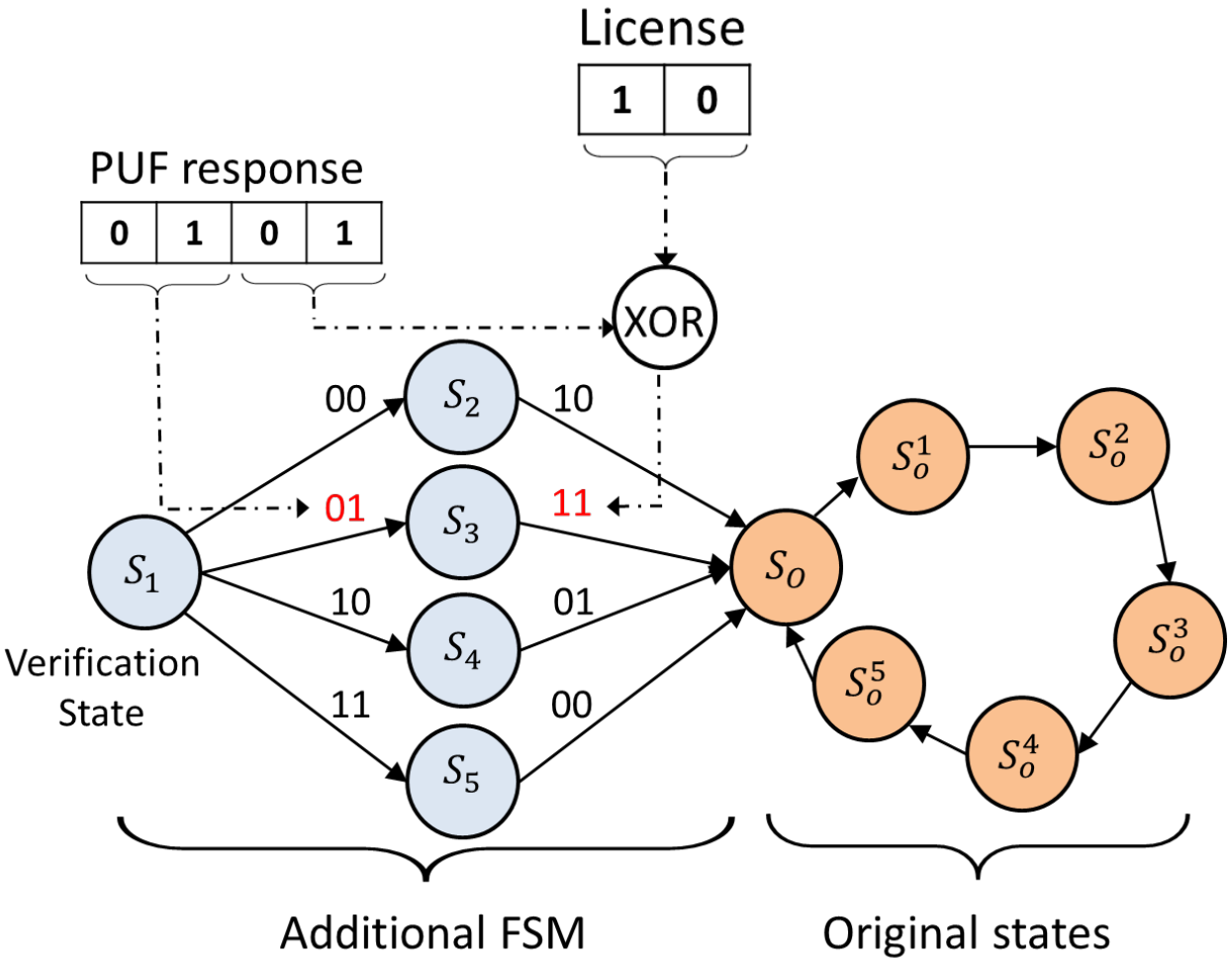


Locking DMFBs by Additional FSM

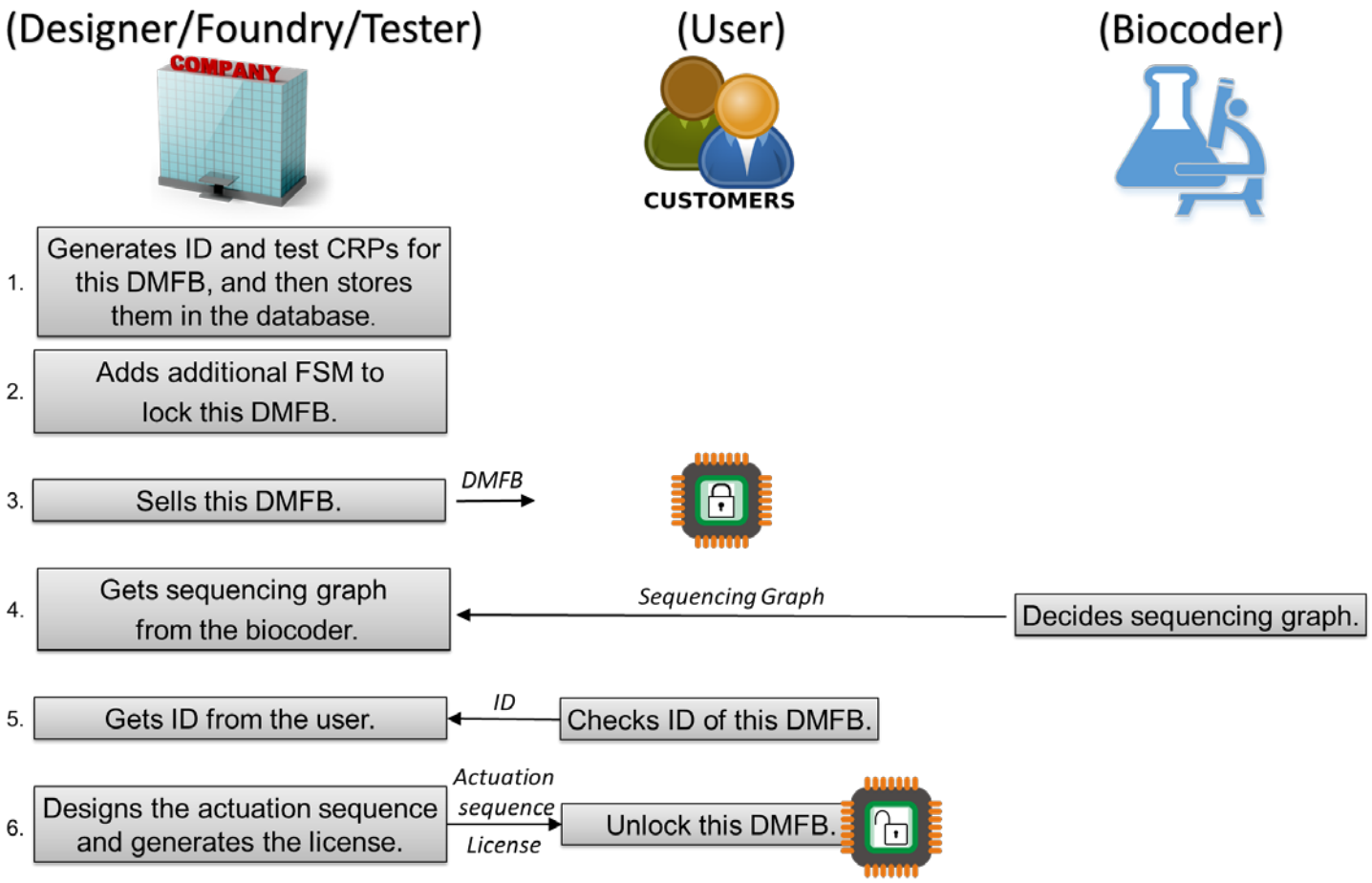
- The control signals for DMFB are determined by the current state of the finite-state machine (FSM).
- Add redundant states to lock DMFBs.



Unlocking by PUF Response and License



Authentication Flow of DMFBs



Security analysis

- Brute force
  - Unlock the DMFB by guessing the correct license and PUF responses.
- Simulating PUF
  - Use machine learning techniques to attack.
- Counterfeiting
  - recycle used DMFB and sell them.

Experiment of Proposed PUF

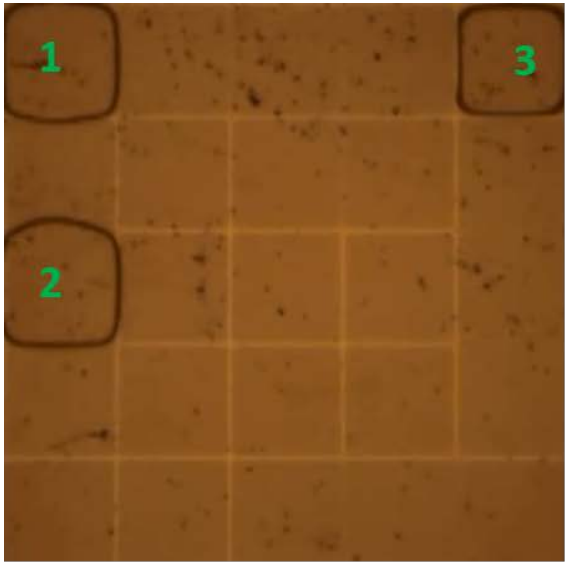
- The volume decreases due to the absorption at the electrode surface and evaporation.
- The error probability associated with each operation is called the intrinsic error limit.
- E_{op}^{tran} is $\sqrt{I^2 + (E_{intr}^{tran})^2}$
- E_{op}^{slt} is $\sqrt{I^2 + 2(E_{intr}^{slt})^2}$

$\boldsymbol{I}$ **:** error limit at the start of the operation.

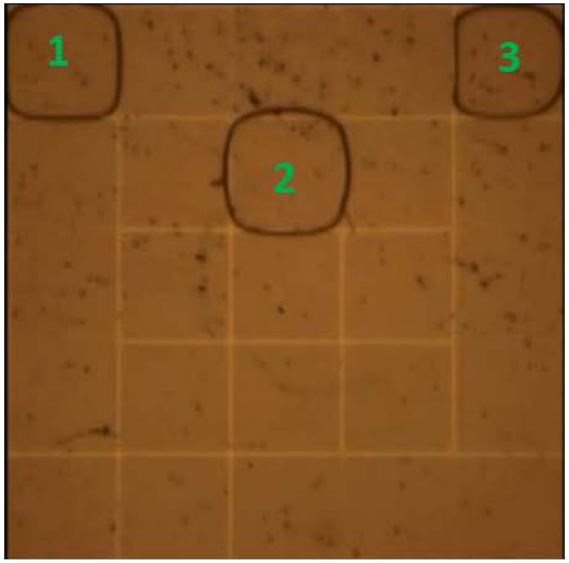
Y. Zhao, T. Xu, and K. Chakrabarty, “Integrated control-path design and error recovery in the synthesis of digital microfluidic lab-on-chip,” ACM Journal on Emerging Technologies in Computing Systems, vol. 6, p. 11, 2010.

Experiment of Proposed PUF

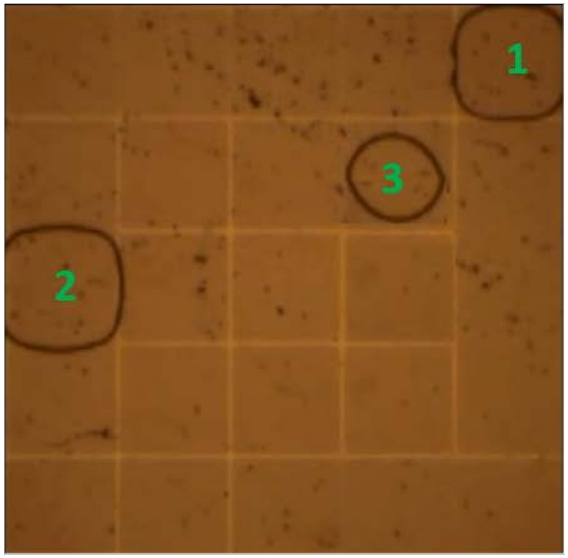
- Difference of volume becomes obvious after more number of executed operations.



(a)



(b)



(c)

Duke microfluidics lab : *http://microfluidics.ee.duke.edu/*

Conclusions

- We have presented the first authentication method to secure DMFBs from the piracy attack.
- We have proposed the novel PUF which utilizes the inherent variation of electrodes on DMFBs to generate secret keys for authentication.
- We have demonstrated the feasibility of our proposed PUF.

Thank You