Biochip Security

Ramesh Karri
rkarri@nyu.edu
Collaborators: J. Tang. O. Sinanoglu (NYU) ,
M. Ibrahim, K. Chakrabarti (Duke U)
http://cyber.nyu.edu

Sponsors: Army Research Office, NYU CCS and CCS-AD

CENTER FOR
CYBER SECURITY

Outline

NYU TANDON SCHOOL OF ENGINEERING

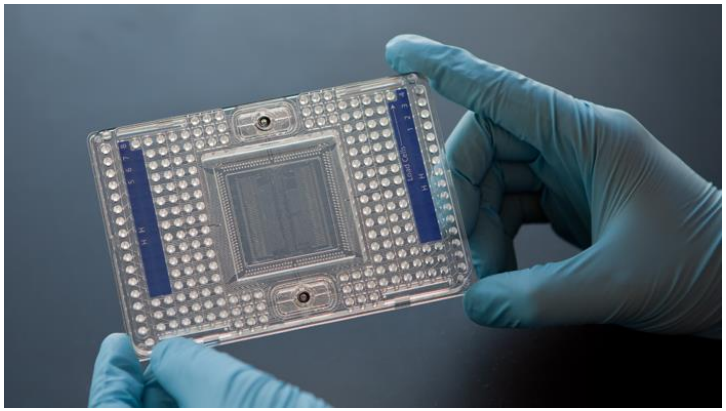
- Overview of Biochips/Microfluidics
- Biochip Security Challenges
  - Scandals in the News
  - Calibration Attacks
  - Scattering of Fluids
  - Denial of Service
- Defenses
  - Randomizing Checkpoints
- Takeaways !!

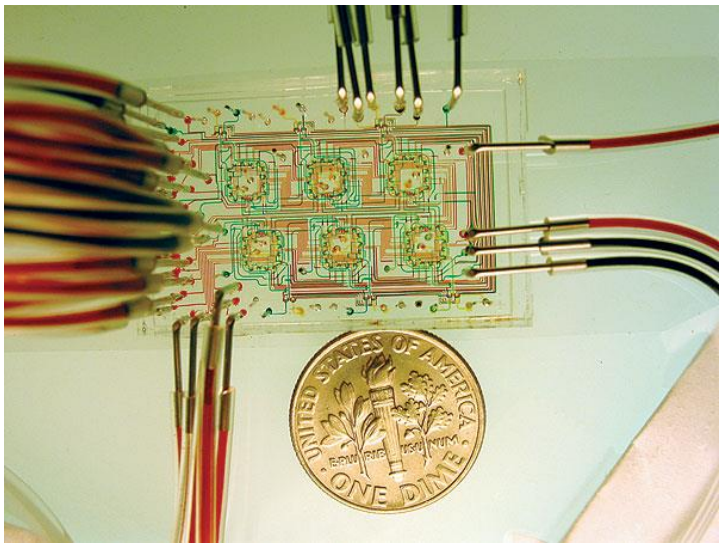
CENTER FOR CYBER SECURITY

What is microfluidics?

NYU TANDON SCHOOL OF ENGINEERING

- Field of physics/manipulation of minute volumes of fluids (micro Litres to femto Litres)
- Lab-on-a-chip—goal: shrink laboratory procedures
- Benefits
  - Lower sample/reagent usage
  - Parallel processing
  - Low energy consumption
  - Automation
  - Portability
  - Scaling of physical effects

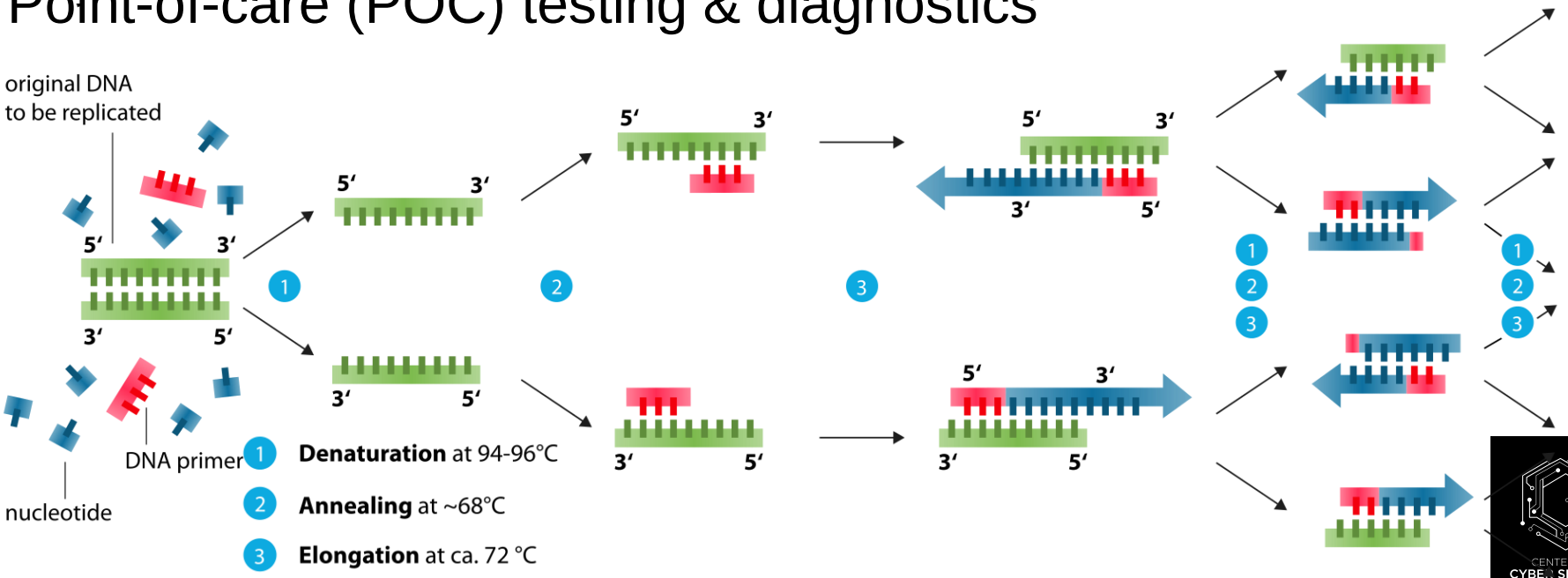




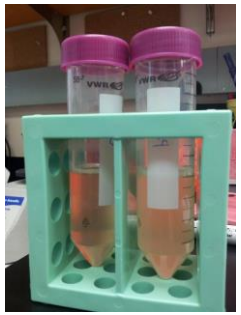
CENTER FOR CYBER SECURITY

What are its Applications?

- Inkjet printers
- Enzymatic assays
- Polymerase chain reaction (PCR); DNA analysis
- Proteomics (study of proteins)
- Point-of-care (POC) testing & diagnostics



Lab-on-Chip: Review



Bench-top: Test tubes, centrifuge, bulky analyzers

illumina

Microfluidic biochips

☑ Automation
☑ Integration
☑ Miniaturization

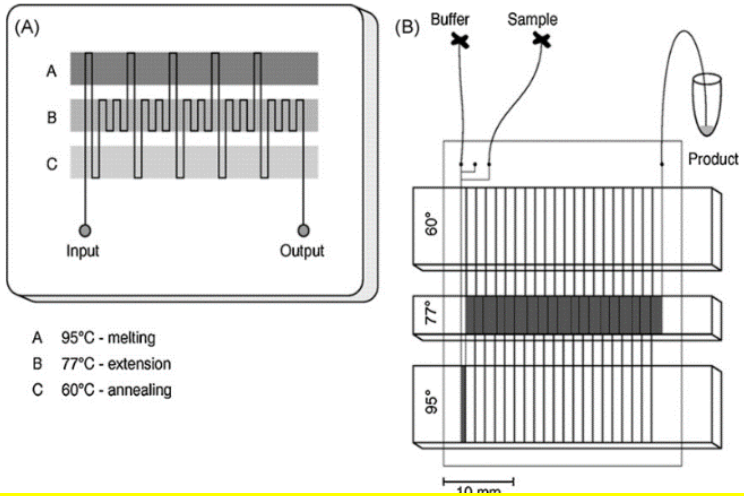
☑Automation
☒ Integration
☒Miniaturization

CENTER FOR CYBER SECURITY

Microfluidic Design Paradigms

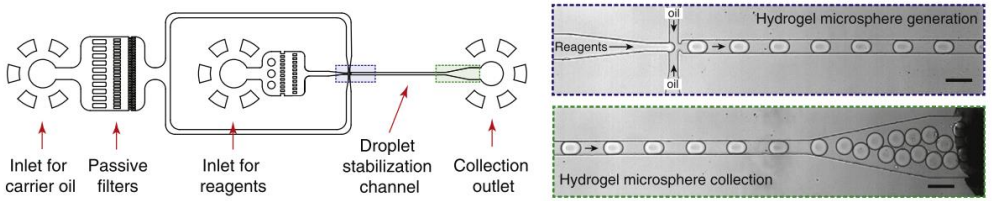
NYU TANDON SCHOOL OF ENGINEERING

Continuous-flow

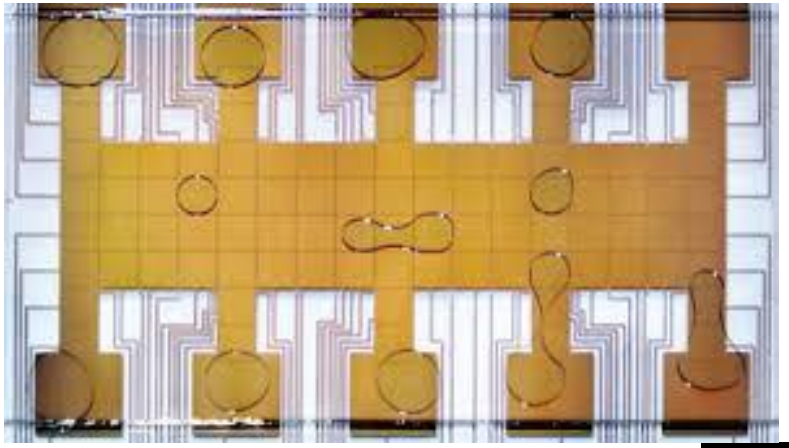


Kopp, Martin U., Andrew J. De Mello, and Andreas Manz. "Chemical amplification: continuous-flow PCR on a chip." *Science* 280.5366 (1998): 1046-1048.

Droplet-based



Klein, A. M., Mazutis, L., Akartuna, I., Tallapragada, N., Veres, A., Li, V., … Kirschner, M. W. (2015). Droplet Barcoding for Single-Cell Transcriptomics Applied to Embryonic Stem Cells. *Cell*, *161*(5), 1187–1201.

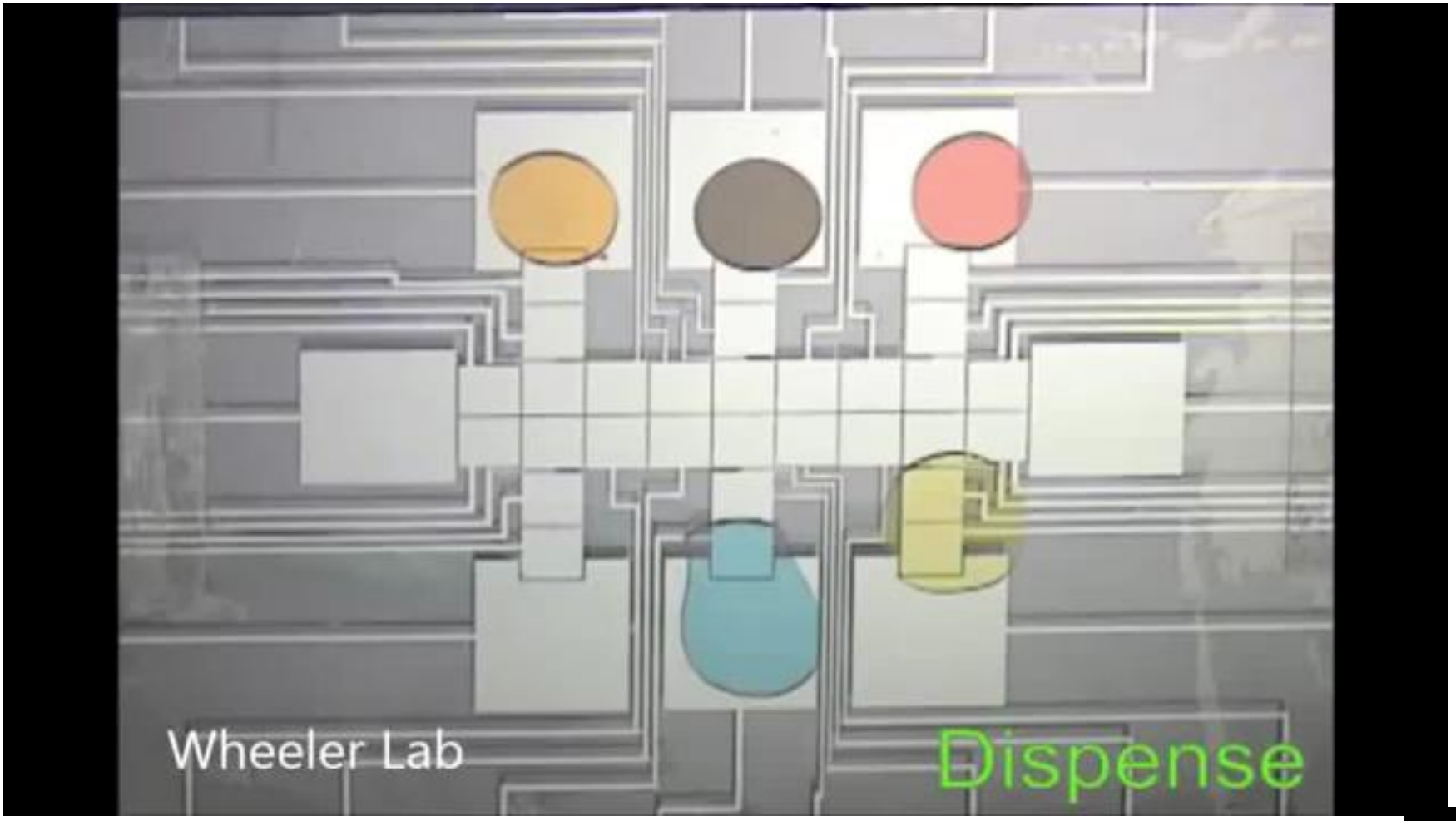


Digital Microfluidics

CENTER FOR CYBER SECURITY

Digital Microfluidic Biochips

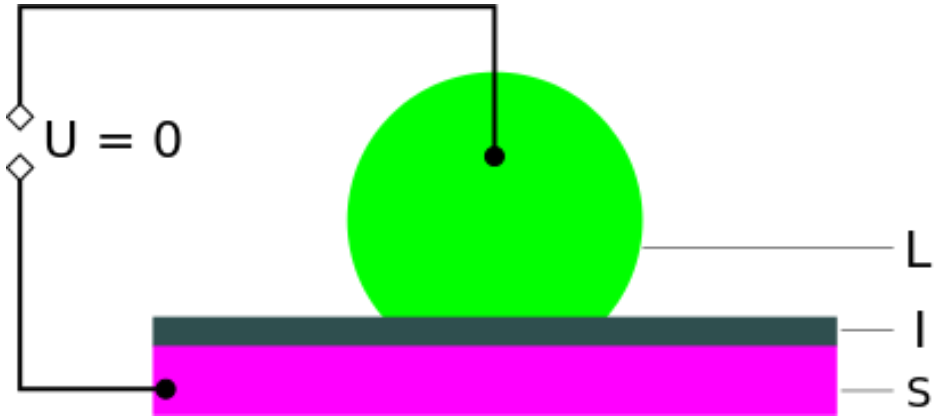
NYU TANDON SCHOOL OF ENGINEERING

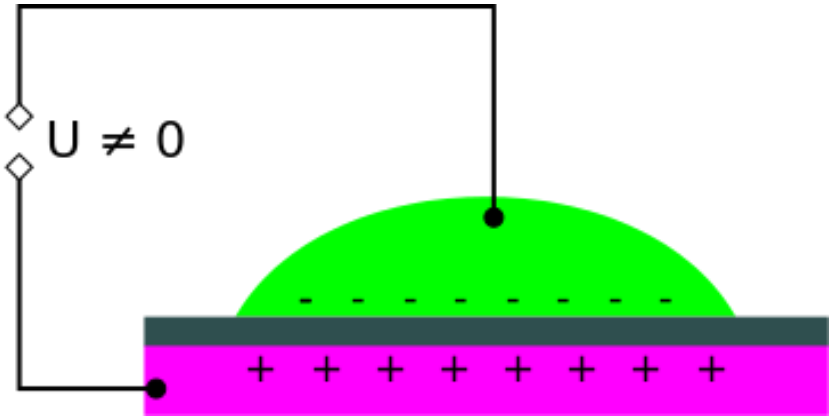


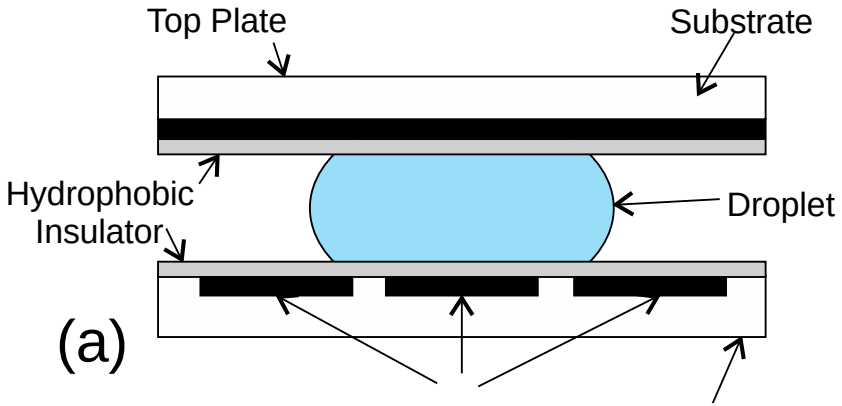
CENTER FOR CYBER SECURITY

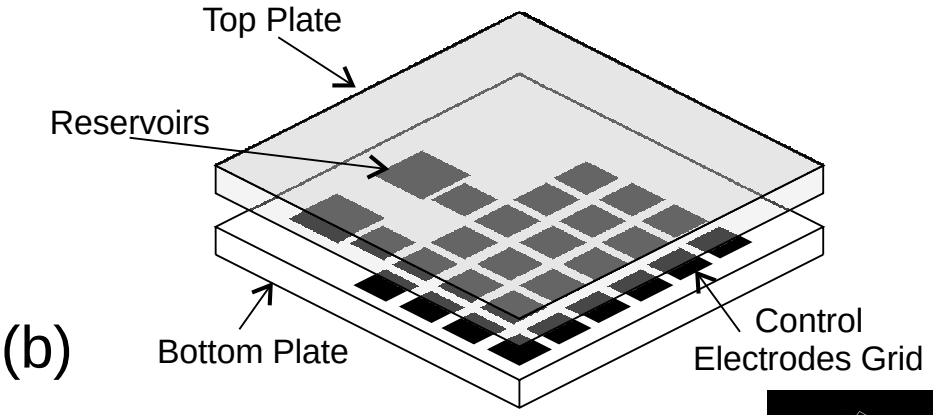
Digital Microfluidic Biochips

NYU TANDON SCHOOL OF ENGINEERING



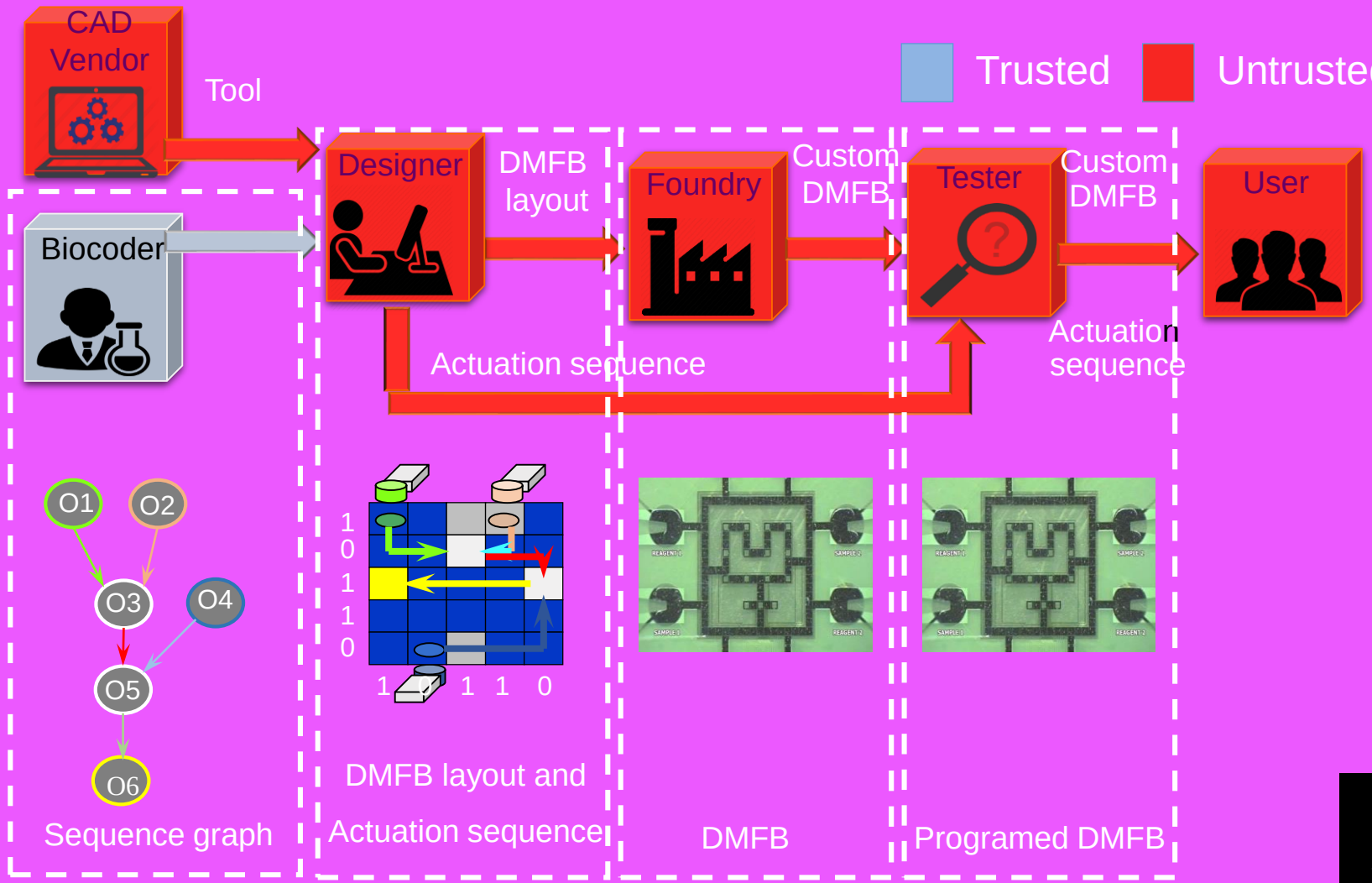






CENTER FOR CYBER SECURITY

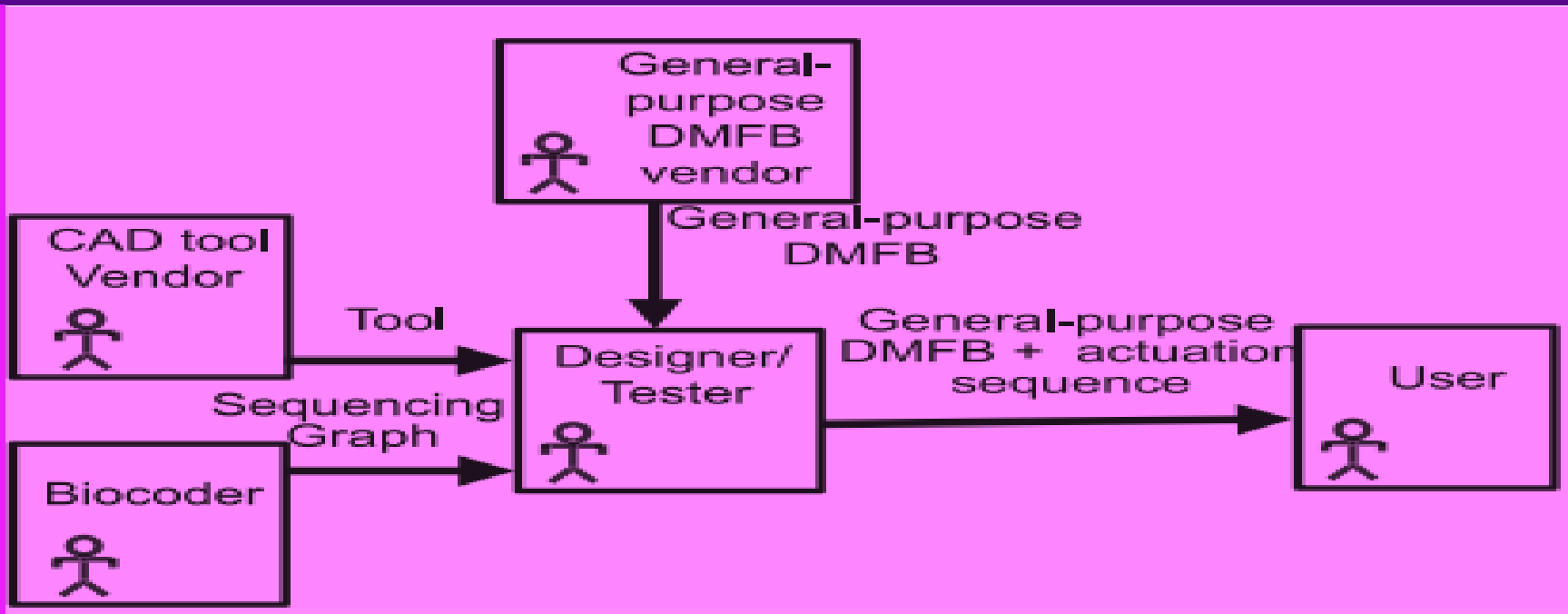
DMFB Design Flow



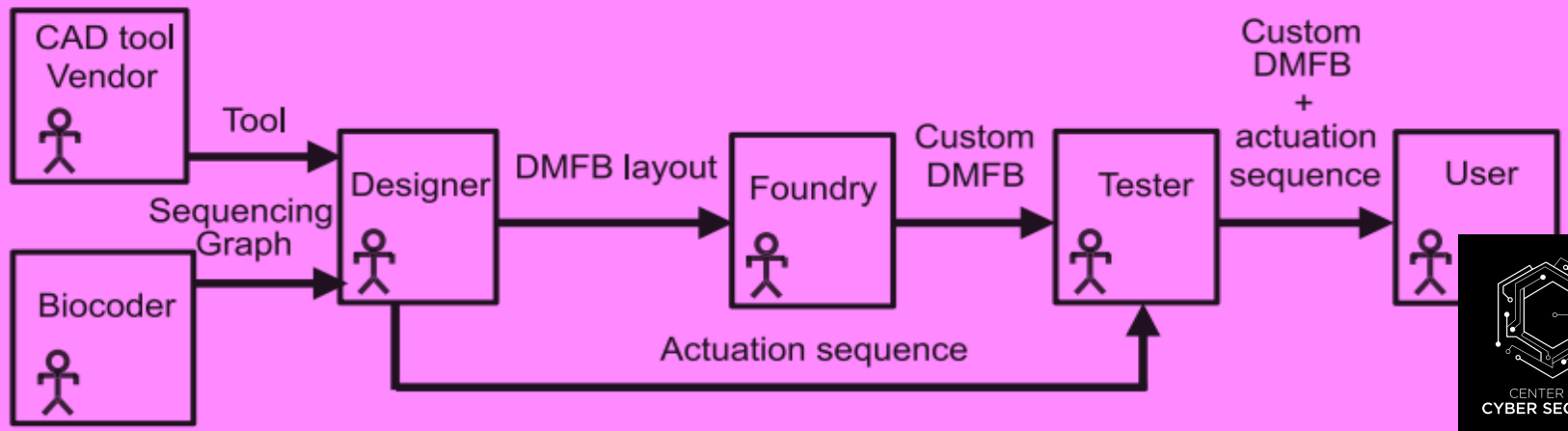
DMFB Design Flow: Actors

NYU TANDON SCHOOL OF ENGINEERING

General-purpose Design Flow

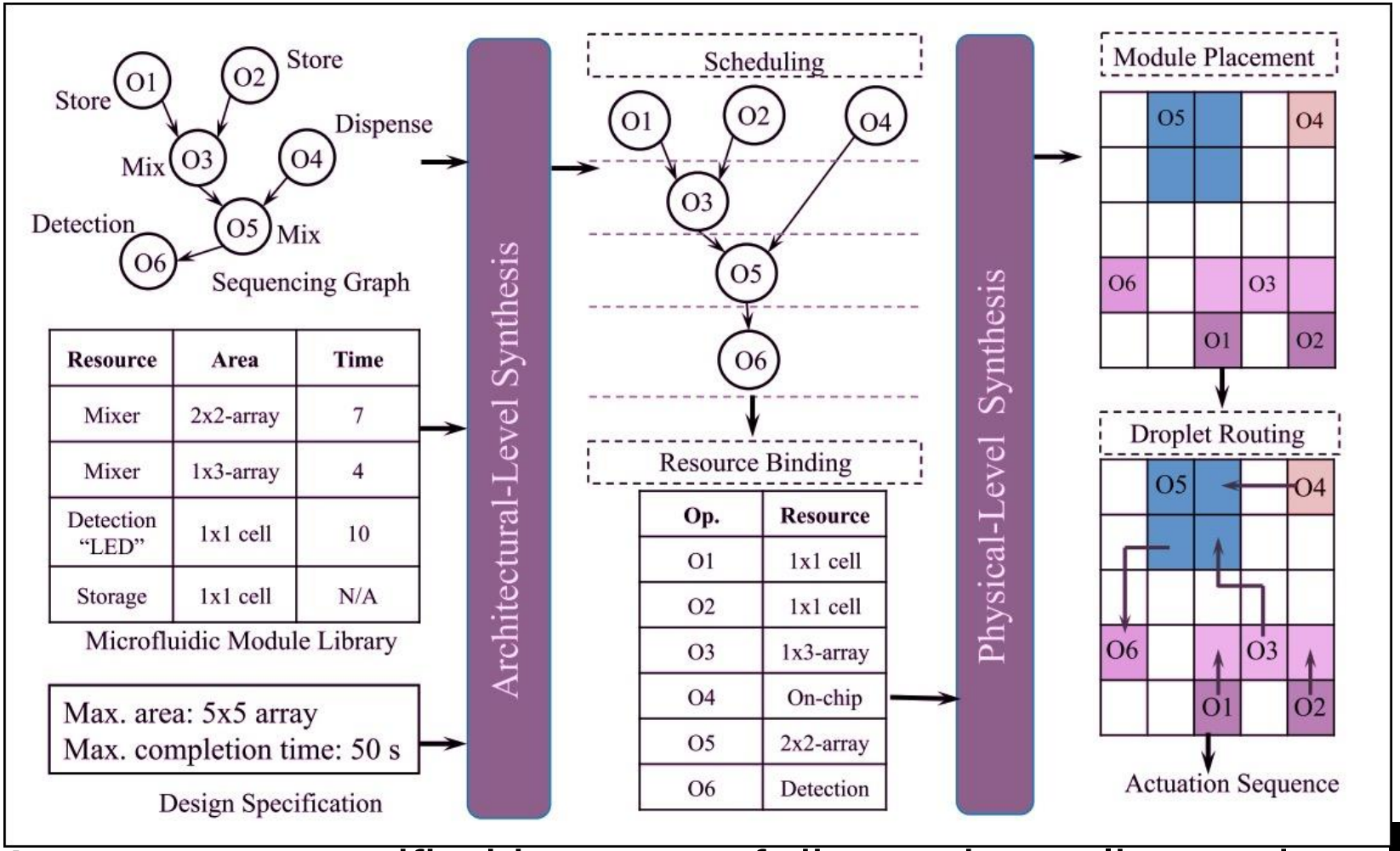


Custom Design Flow



CENTER FOR CYBER SECURITY

DMFB Synthesis



- Assays are specified in terms of directed acyclic graph
- Assay is synthesized to form electrode actuation sequenc

Outline

- ~~Overview of Biochips/Microfluidics~~
- Biochip Security Challenges
  - Scandals in the News
  - Calibration Attacks
  - Scattering of Fluids
  - Denial of Service
- Defenses
  - Randomizing Checkpoints
- Takeaways !!

The Theranos Scandal

NYU TANDON SCHOOL OF ENGINEERING

theranos

one tiny drop changes everything.

At Theranos, we're working to shape the future of lab testing. Now, for the first time, our high-complexity CLIA-certified laboratory can perform your tests quickly and accurately on samples as small as a single drop.

TECH

Theranos Voids Two Years of Edison Blood-Test Results

Company led by Elizabeth Holmes withdraws all Edison results from 2014 and 2015, issues tens of thousands of corrected blood-test reports

By JOHN CARREYROU
May 18, 2016 8:16 p.m. ET

Theranos Inc. has told federal health regulators that the company voided two years of results from its Edison blood-testing devices, according to a person familiar with the matter.

WSJ

CENTER FOR CYBER SECURITY

The Big Brother

Jenna McLaughlin

June 10 2016, 1:53 p.m.

NSA Looking to Exploit Internet of Things, Including Biomedical Devices, Official Says

THE NATIONAL SECURITY AGENCY is researching opportunities to collect foreign intelligence – including the possibility of exploiting internet-connected biomedical devices like pacemakers, according to a senior official.

"We're looking at it sort of theoretically from a research point of view right now," Richard Ledgett, the NSA's deputy director, said at a conference on military technology at Washington's Newseum on Friday.

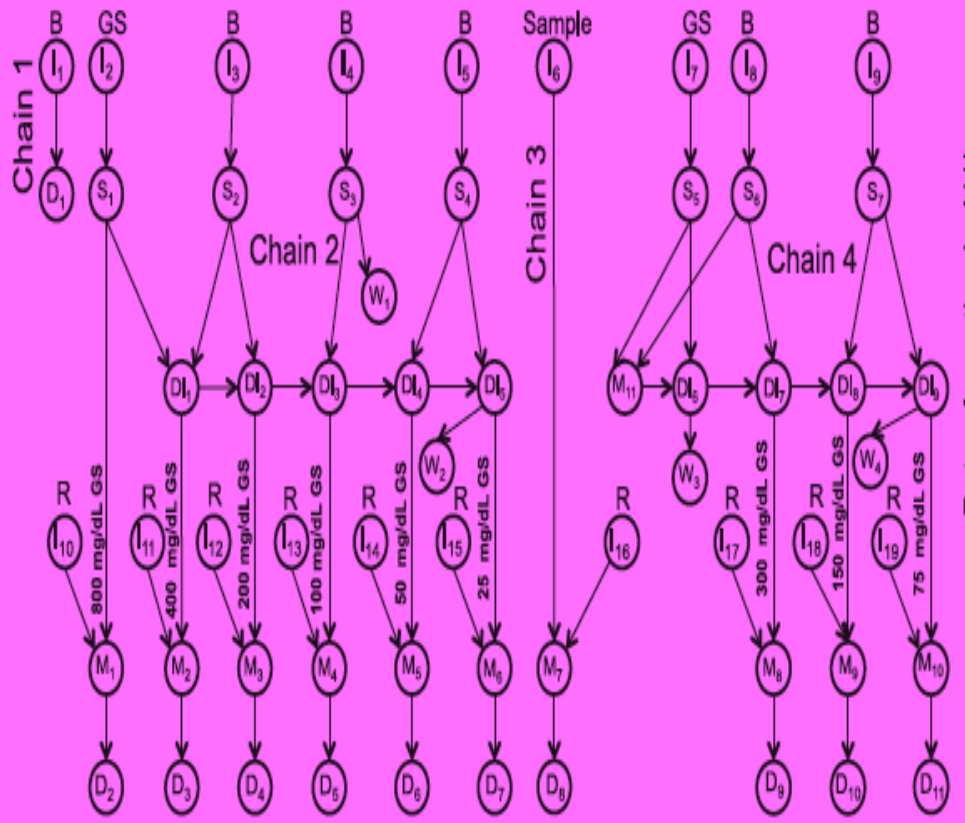
Biomedical devices could be a new source of information for the NSA's data hoards – "maybe a niche kind of thing ... a tool in the toolbox," he said, though he added that there are easier ways to keep track of overseas terrorists and foreign intelligence agents.

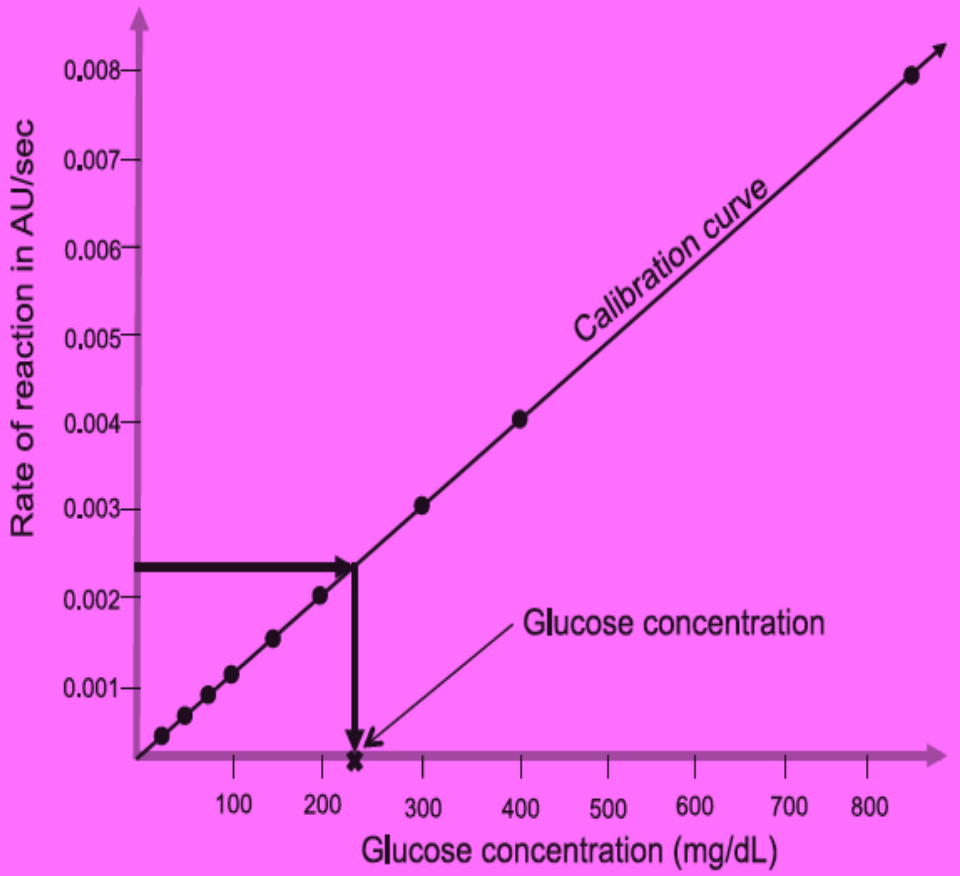
The Intercept_

Outline

- ~~Overview of Biochips/Microfluidics~~
- Biochip Security Challenges
  - ~~Scandals in the News~~
  - Calibration Attacks
  - Scattering of Fluids
  - Denial of Service
- Defenses
  - Randomizing Checkpoints
- Takeaways !!

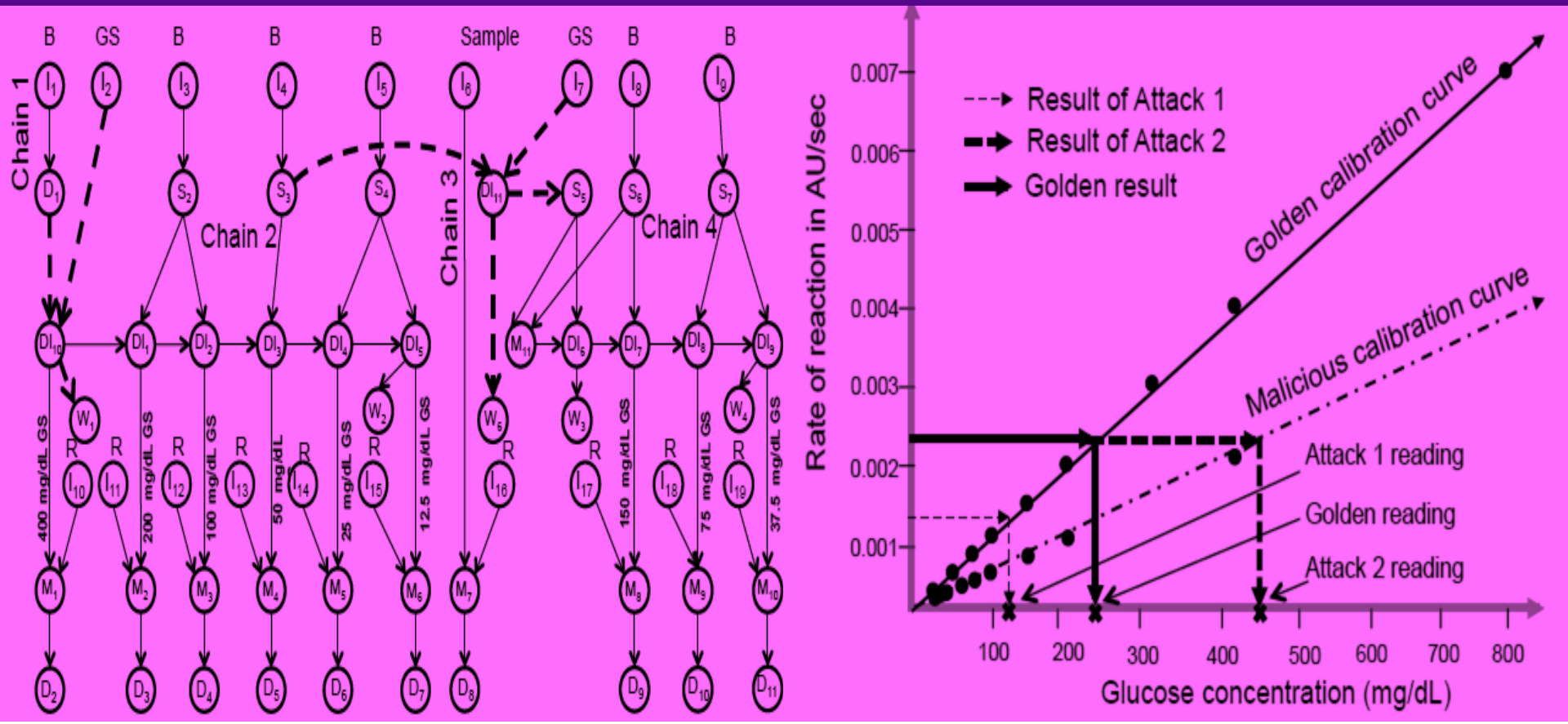
Glucose Assay





Glucose assay: measures blood glucose level

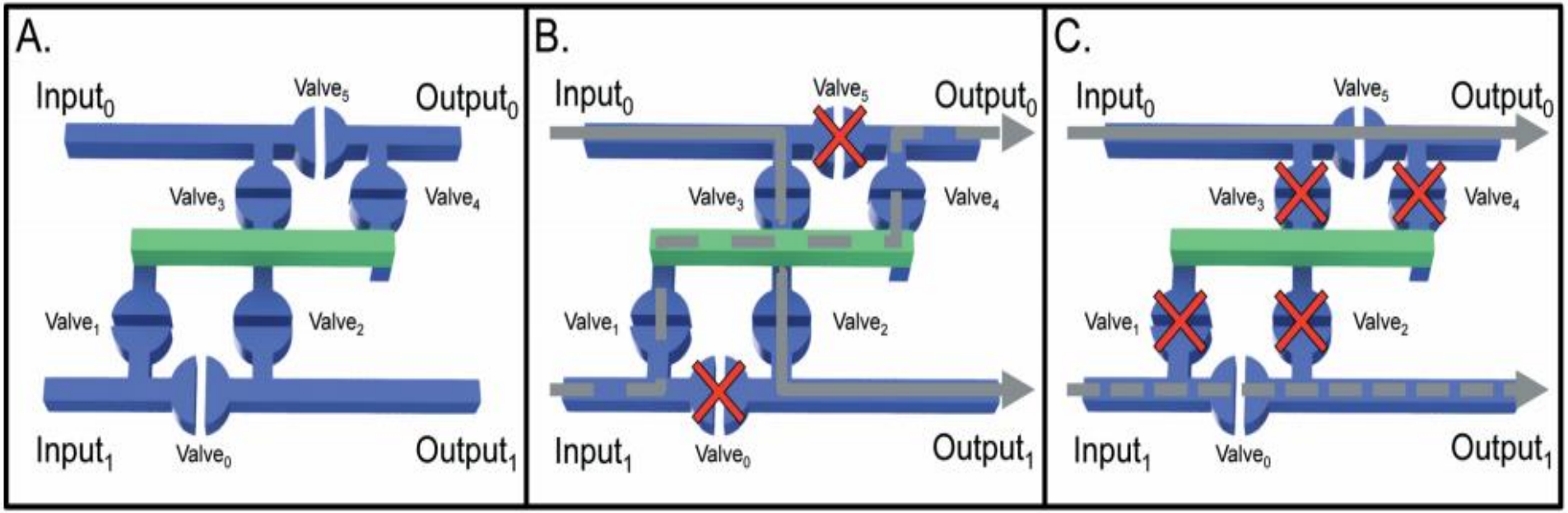
Tampering with Glucose Assay?



- Contamination: Mix waste buffer with glucose solution
- Change calibration curve

Ali, S., Ibrahim, M., Sinanoglu, O., Chakrabarty, K., & Karri, R. (2015). Security Assessment of Cyberphysical Digital Microfluidic Biochips. *IEEE/ACM Transactions on Computational Biology and Bioinformatics / IEEE, ACM*.

Attack on Cont. Flow Biochips

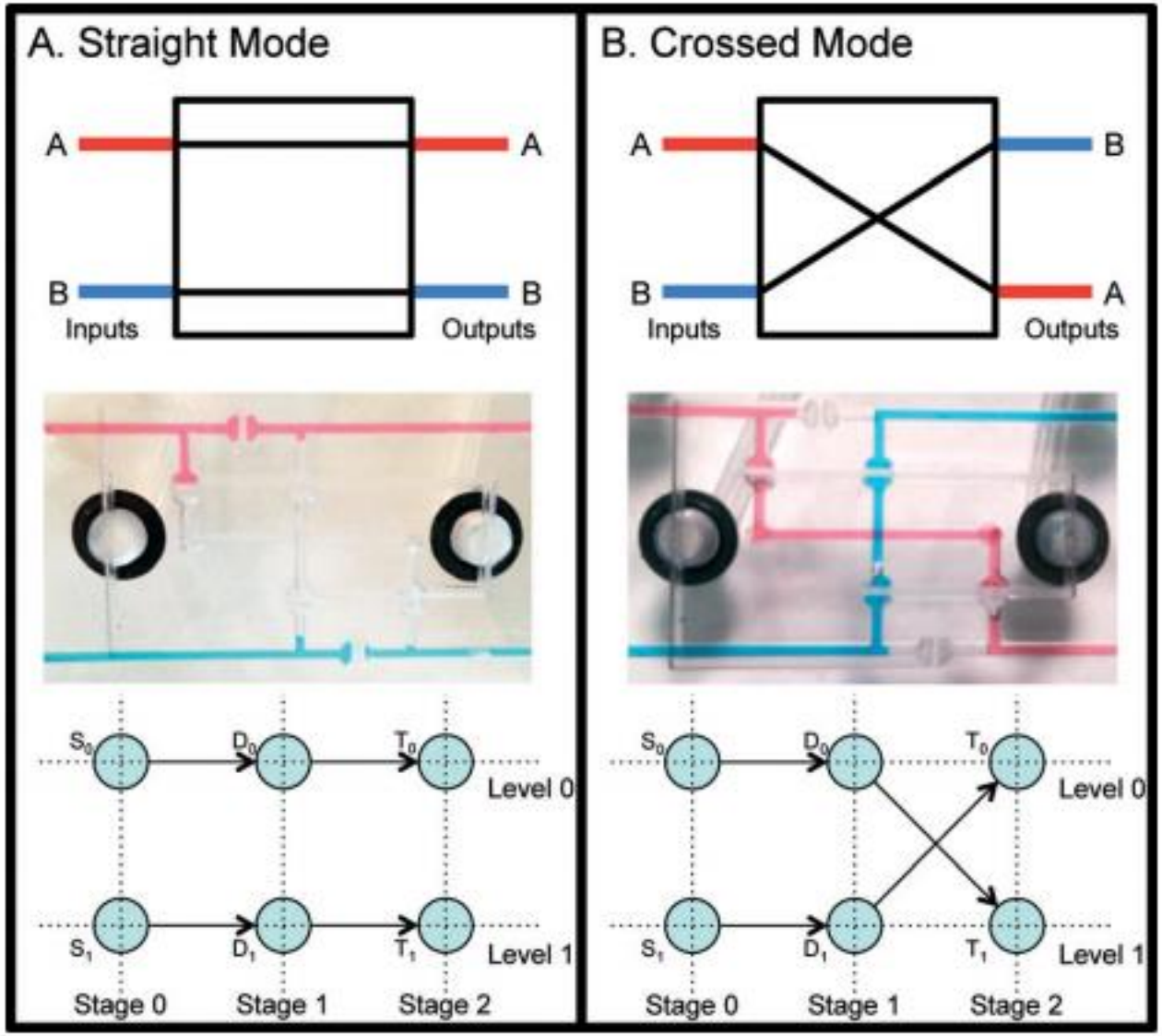


Continuous flow biochips can be reconfigured by transposers

Tang, J., Ibrahim, M., Chakrabarty, K., and Karri, R. (2017). Security Tradeoffs in Microfluidic Routing Fabrics. IEEE ICCD 2017

The Transposer Primitive

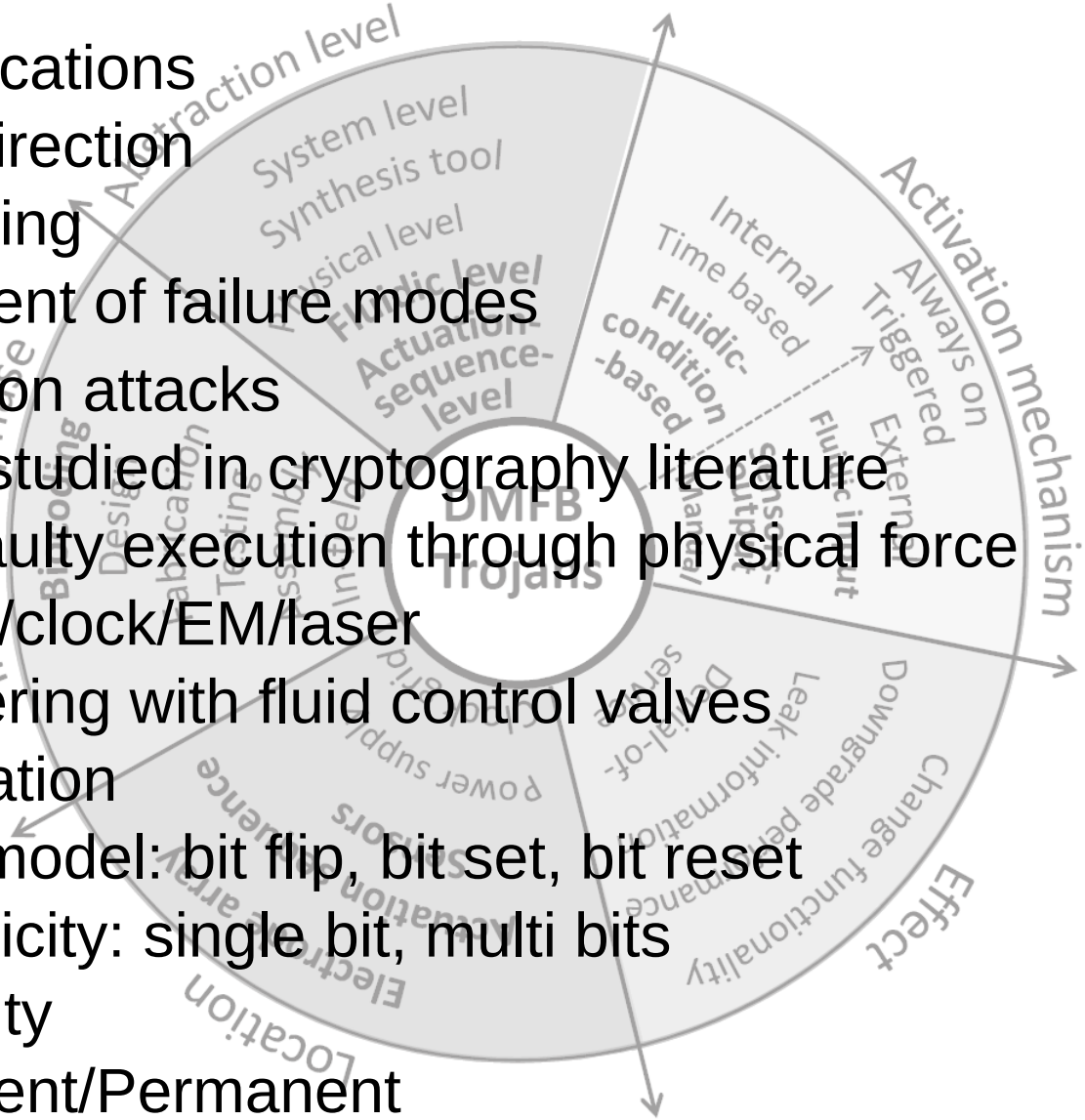
NYU TANDON SCHOOL OF ENGINEERING



CENTER FOR CYBER SECURITY

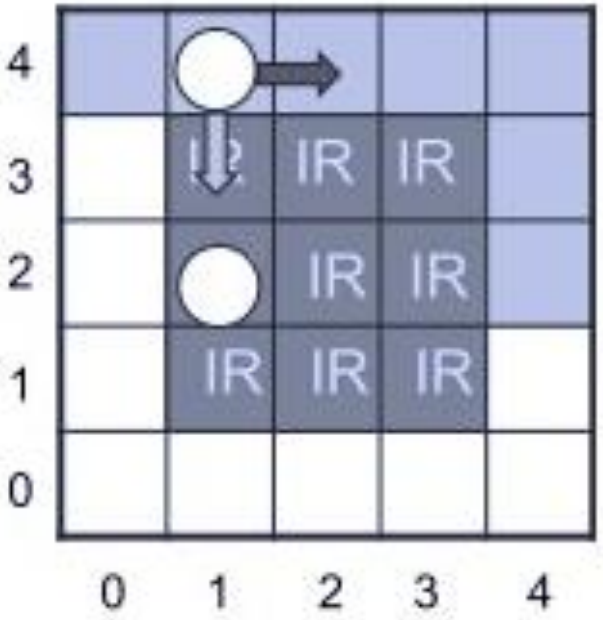
Attacks on Transposers

- Attack implications
  - Fluid redirection
  - Fluid mixing
  - Inducement of failure modes
- Fault injection attacks
  - Actively studied in cryptography literature
  - Induce faulty execution through physical force
    - Power/clock/EM/laser
    - Tampering with fluid control valves
  - Classification
    - Fault model: bit flip, bit set, bit reset
    - Multiplicity: single bit, multi bits
    - Modality
    - Transient/Permanent

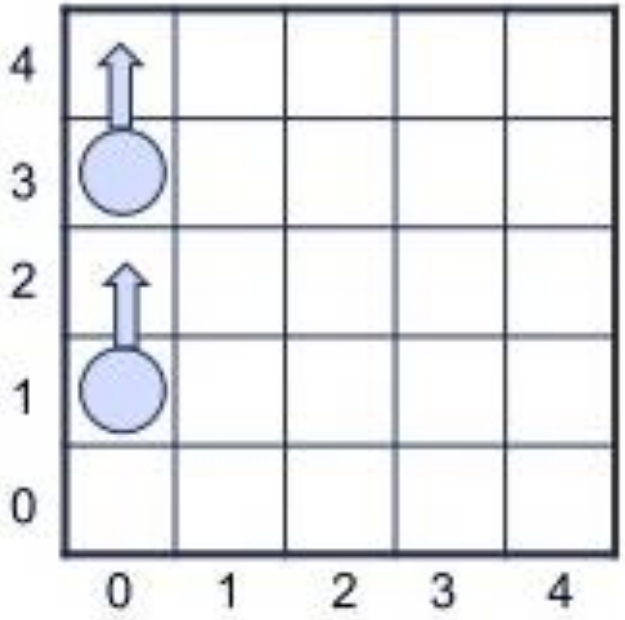


DoS Attacks

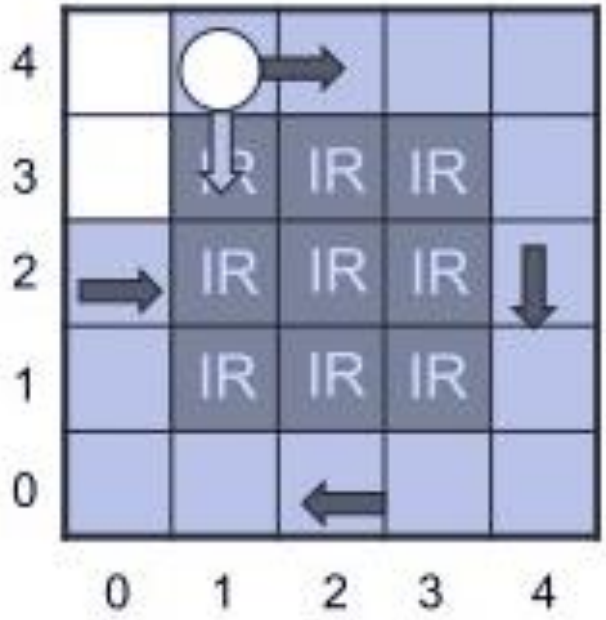
Denial-of-service: prevent device from working as intended



Interference region violation



Droplet collision



Circuitous routing

Ali, S., Ibrahim, M., Sinanoglu, O., Chakrabarty, K., & Karri, R. (2015). Security Assessment of Cyberphysical Digital Microfluidic Biochips. *IEEE/ACM Transactions on Computational Biology and Bioinformatics / IEEE, ACM*.

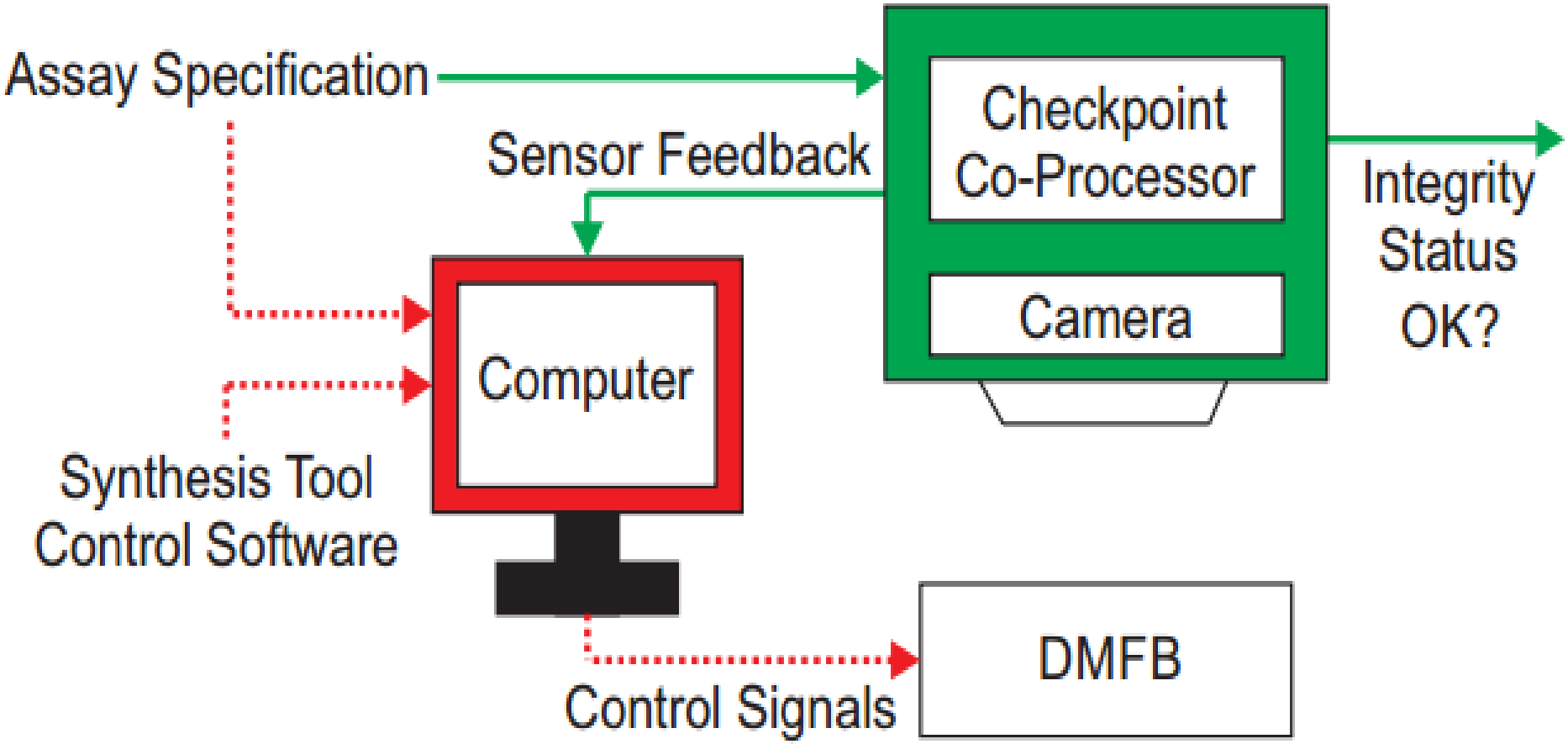
Outline

NYU TANDON SCHOOL OF ENGINEERING

- ~~Overview of Biochips/Microfluidics~~
- ~~Biochip Security Challenges~~
  - ~~Scandals in the News (3)~~
  - ~~Calibration Attacks~~
  - ~~Scattering of Fluids~~
  - ~~Denial of Service~~
- Defenses
  - Randomizing Checkpoints
- Takeaways !!

CENTER FOR CYBER SECURITY

Cyberphysical DMFBs



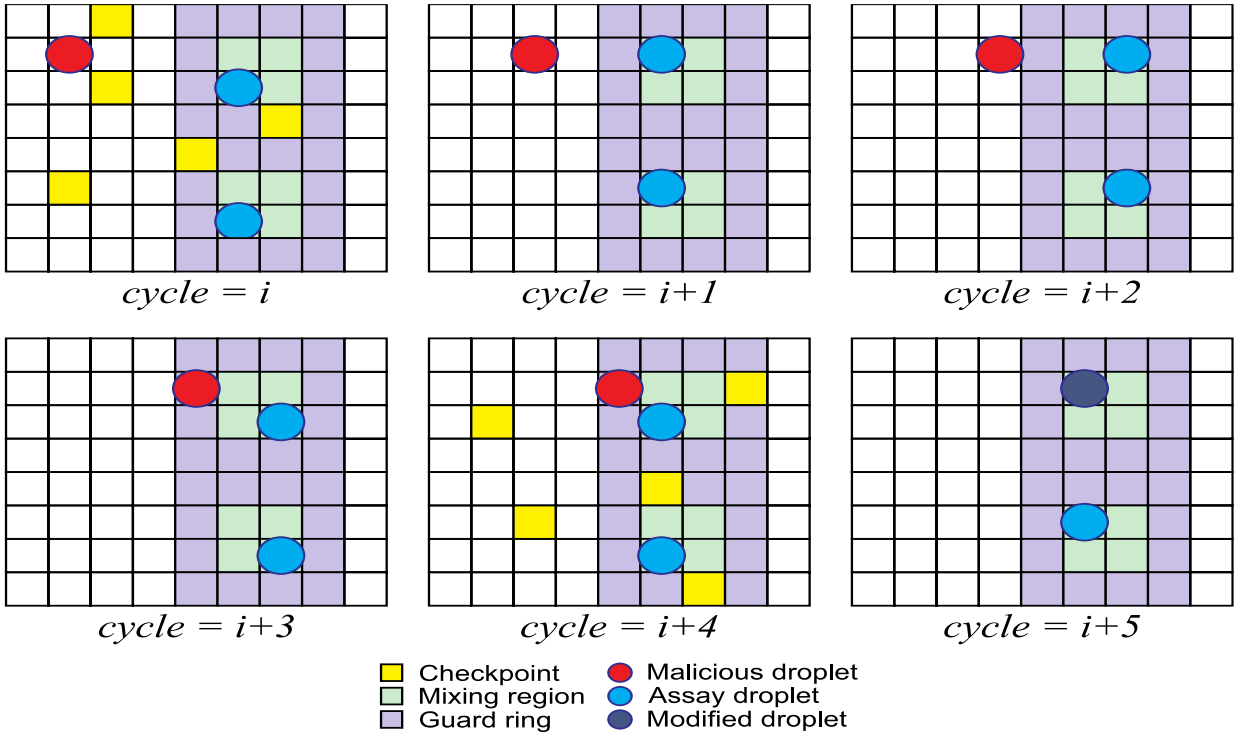
Randomizing Checkpoints

NYU TANDON SCHOOL OF ENGINEERING

Error recovery provides some guarantees against mal. modification

Deterministic, so adversary can simply route around them

Introduce checkpoints that are random in both time and space



Tang, J., Ibrahim, M., Chakrabarty, K., & Karri, R. (2016). Securing Digital Microfluidic Biochips by Randomizing Checkpoints. In Proc. 2016 International Test Conference. Fort Worth, TX.

Modeling a Malicious Route

NYU TANDON SCHOOL OF ENGINEERING

- Metric: *probability that a malicious route evades detection by checkpoints.*
- Let E be the evasion event
- Assuming checkpoints are selected independently, then

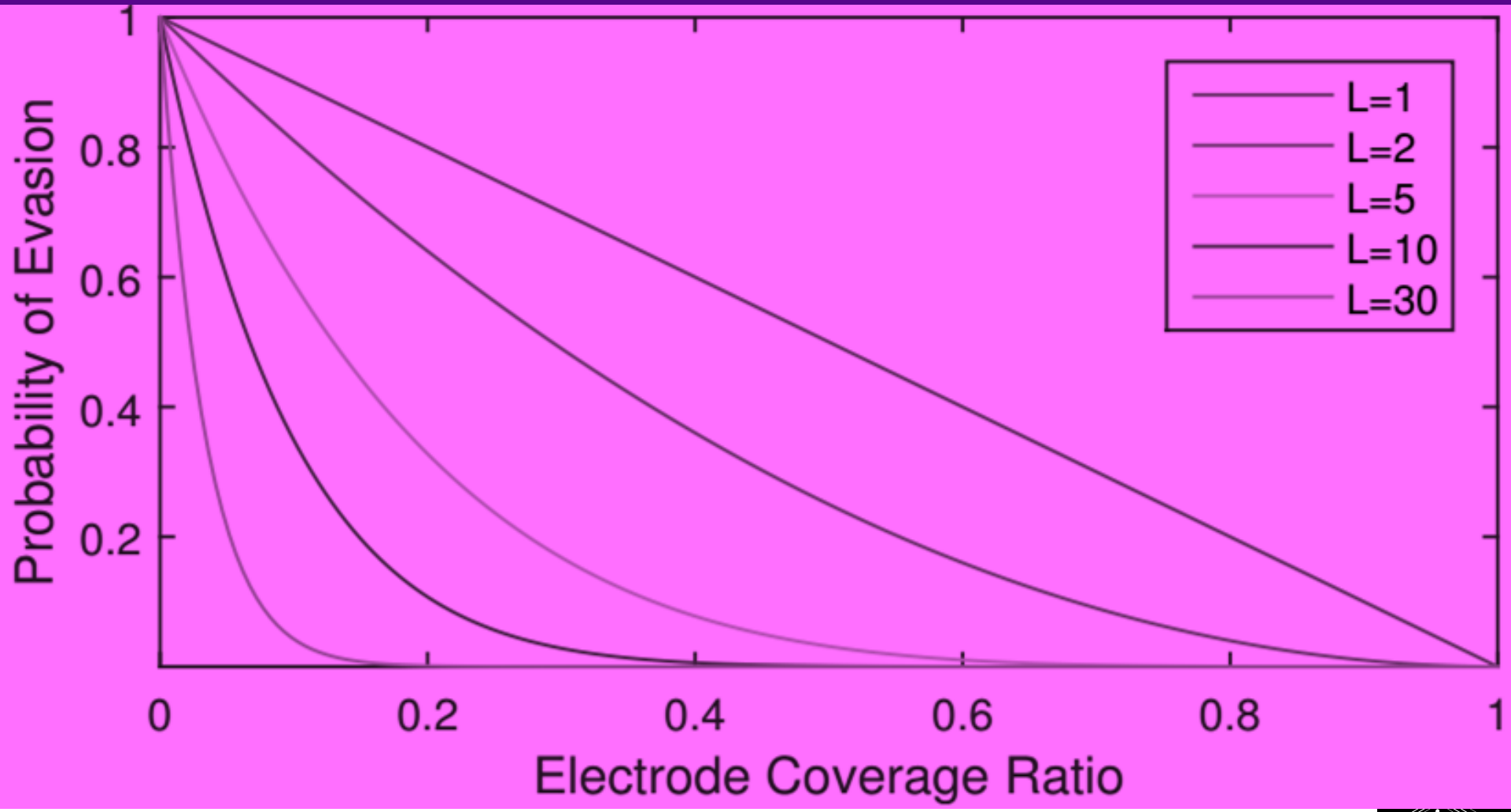
$$P(E) = \prod_{i=1}^{L} \left((1-c) + c\left(1 - \frac{k}{s}\right)\right) = \left(1 - \frac{ck}{s}\right)^{L}$$

- L is the length of the malicious route
- c is the probability that electrodes are monitored
- k is number of checkpoints
- s is number of electrodes in the array

(k/s is the electrode coverage ratio)

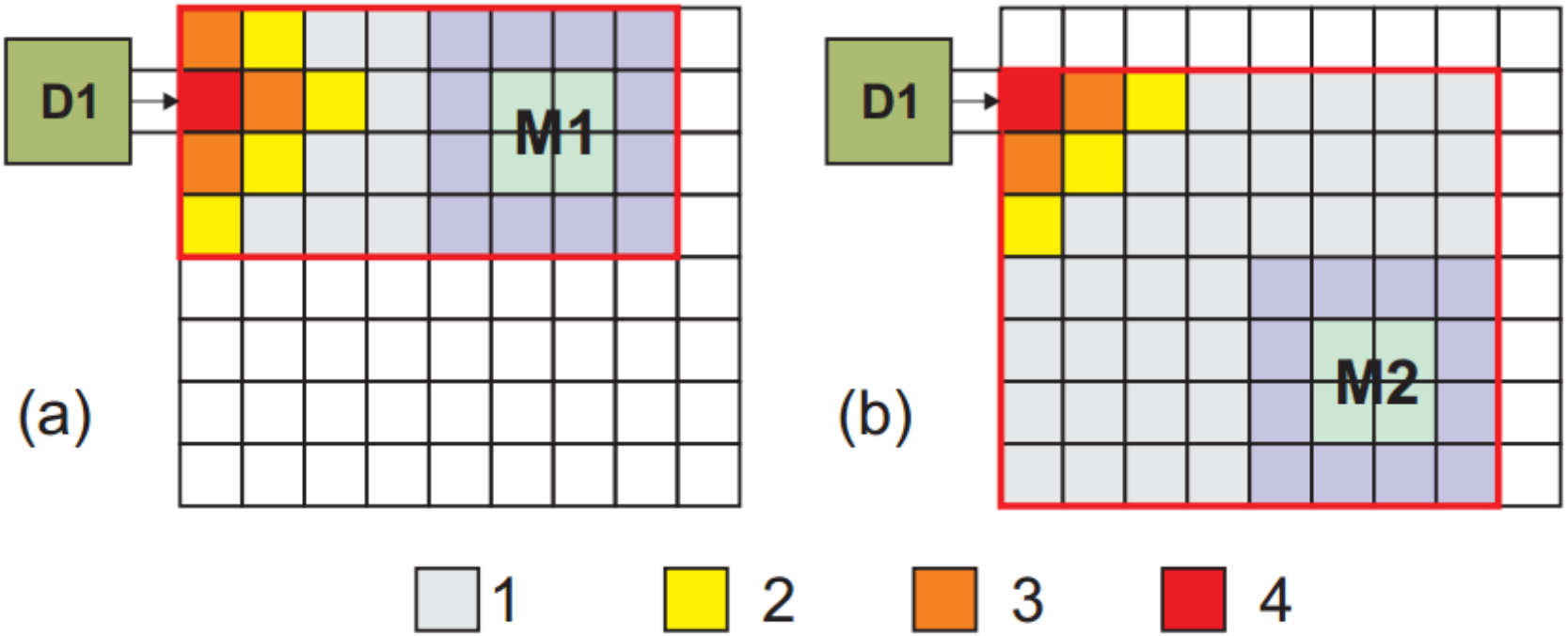
CENTER FOR CYBER SECURITY

Probability of Evasion



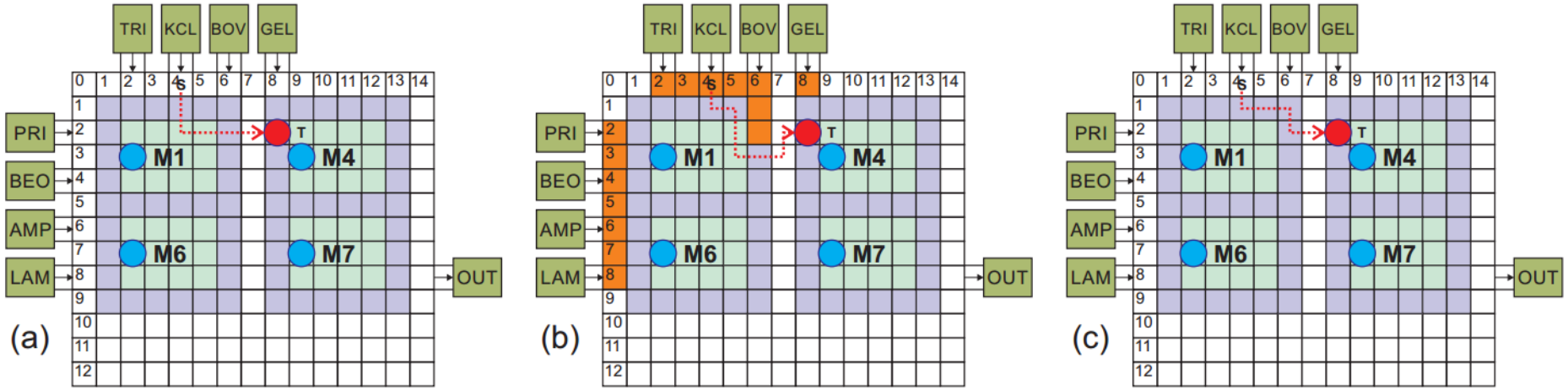
Prob evasion decreases exponentially with length of malicious

Supplement w/ Static Checkpoints



- Place static checkpoints ~between sources and destinations
- Sources get more weight
- Enumerate all possible combinations of (source, destination)
- Add weighting matrices to form a ranking matrix
- Select static checkpoints from ranked electrodes

PCR Denial of Service



- Dispense KCL to M4 Mixer ➔reduces PCR quality
- Static checkpoints cause route to become longer
- Error recovery in M1, but length is same as in (a)

Outline

NYU TANDON SCHOOL OF ENGINEERING

- ~~Overview of Biochips/Microfluidics~~
- ~~Biochip Security Challenges~~
  - ~~Scandals in the News (3)~~
  - ~~Calibration Attacks~~
  - ~~Scattering of Fluids~~
  - ~~Others: Denial of Service~~
- ~~Defenses~~
  - ~~Randomizing Checkpoints~~
- Takeaways !!

CENTER FOR CYBER SECURITY

Takeaways: Market Outlook

NYU TANDON SCHOOL OF ENGINEERING

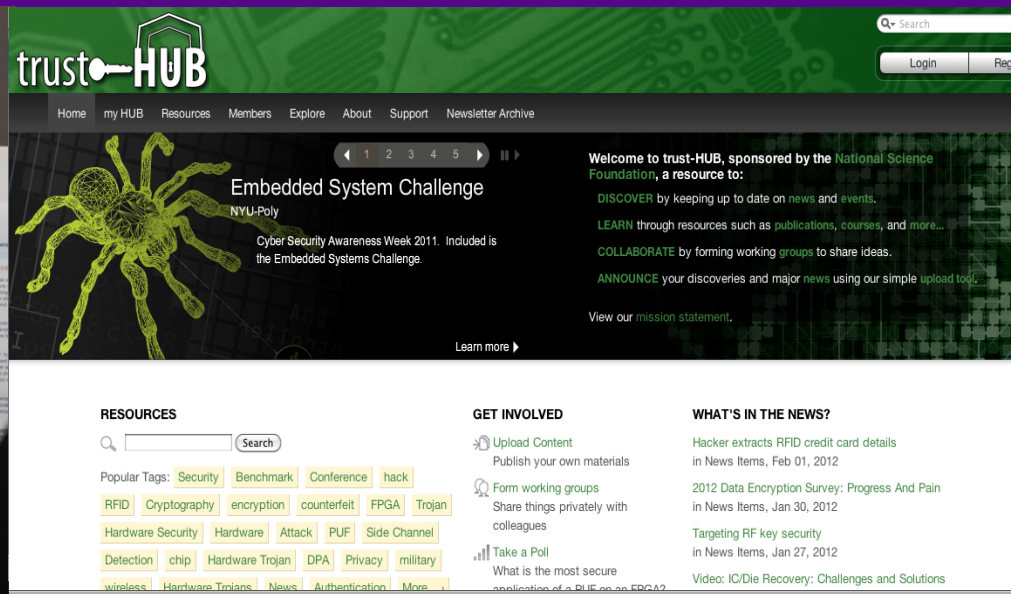
GLOBAL MARKET FOR BIOCHIPS BY END-USE INDUSTRY, THROUGH 2020 ($ MILLIONS)

End Use Industry	2014	2015	2020	CAGR% 2015-2020
Clinical	1,723.2	2,339.1	14,720.0	44.5
Drug discovery and development	1,136.4	1,257.3	2,137.0	11.2
Research tools	785.3	822.2	1,099.0	6.0
Applied	229.3	257.1	465.0	12.6
Total	3,874.2	4,675.7	18,421.0	31.6

Source: BCC Research

Takeaway: Build Capacity

NYU TANDON SCHOOL OF ENGINEERING



- A red-team blue-team competition for hardware security
- Organized for the last decade or so
- N. America (NYC), Europe (Valence), MENA (Abu Dhabi), Asia (IIT K)
- 200+ students (graduate, undergraduate, high school)
- Hardware security benchmarks
- Challenges included Trojans, PUFs, Malicious processors

isis.poly.edu/esc

www.trusthu

CENTER FOR CYBER SECURITY

Publications

NYU TANDON SCHOOL OF ENGINEERING

1. J. Tang, M. Ibrahim, K. Chakrabarty, and R. Karri, Secure Randomized Checkpointing for Digital Microfluidic Biochips, IEEE Transactions on Computer-Aided Design, to appear, 10.1109/TCAD.2017.2748030
2. J. Tang, M. Ibrahim, K. Chakrabarty, K. and R. Karri, Security Implications of Cyberphysical Flow-based Microfluidic Biochips, Proc. IEEE Asian Test Symposium, Nov 2017, to appear
3. J. Tang, M. Ibrahim, K. Chakrabarty, and R. Karri, Security Trade-offs in Microfluidic Routing Fabrics, IEEE International Conference on Computer Design, Nov. 2017, to appear
4. J. Tang, R. Karri, M. Ibrahim and K. Chakrabarty, Securing digital microfluidic biochips by randomizing checkpoints, IEEE International Test Conference, 2016.
5. S. S Ali, M. Ibrahim, O. Sinanoglu, K. Chakrabarty and R. Karri, Security Assessment of Cyberphysical Digital Microfluidic Biochips, IEEE/ACM Transactions on Computational Biology and Bioinformatics, 13(3), pp. 445-458, May-Jun 2016.

CENTER FOR CYBER SECURITY

CENTER FOR CYBER SECURITY

http://cyber.nyu.edu