

# Index

## A

- Actuation sequences, 8, 25, 41, 43–45, 51–57, 60, 62–70, 74, 76, 80, 94, 103, 106
- Actuation tampering
  - commercial microfluidic platforms, 26–27
  - countermeasures, 135
  - CPMBs, 109
  - denial-of-service, 25
  - DMFB, 75, 81
  - dPCR (*see* Digital polymerase chain reaction (dPCR))
  - prevention technologies, 51
  - sensor data processing, 55
- Attack surfaces
  - design theft, 24–25
  - DoS, 23–24
  - hardware and software, 22
  - information leakage, 25
  - modification of functionality, 24
  - network-based attacks, 56
  - network interfaces, 19
  - reading forgery, 23
  - scenarios, 41
  - taxonomy, 20–21

## B

- Biochips
  - biological samples, 31
  - CAD tool vendor, 5
  - CPMB (*see* Cyberphysical microfluidic biochip (CPMB))
  - DMFBs (*see* Digital microfluidic biochips (DMFBs))

- FMFBs (*see* Flow-based microfluidic biochips (FMFBs))
- MEDA, 136
- microfluidic biochip, 1, 23–25, 27, 34, 38, 109, 110
  - self-contained microfluidic, 3
  - self-destruct/self-clean, 137
  - SensorPUFs, 137
  - tamper resistant (*see* Tamper resistance)
- Blood diagnostics, 34–36

## C

- Charge-coupled device (CCD), 9, 39, 42, 95
- CompactFlash (CF) card, 27
- Compatibility degree (CD), 54–55, 60, 61, 75
- Copy number variations (CNVs), 29
- Cyberphysical integration, 1, 3–4, 19, 21, 23, 79
- Cyberphysical microfluidic biochip (CPMB)
  - DMFBs and FMFBs, 1
  - manipulation of fluids, 1
  - microfluidics (*see* Microfluidics)
  - modification of functionality, 24
  - physical characteristics, 21
  - randomizing checkpoints (*see* Randomized checkpoints)
  - security implications, 19, 38–40
  - security opportunities, 42–43
  - tampering attack, 51
  - threats, security, 44–45
- Cyberphysical systems, 22, 23, 38, 132

**D**

- Denial-of-service (DoS), 23–24, 44, 76, 81, 96, 111, 131
- Digital microfluidic biochips (DMFBs)
  - checkpoint-based error recovery, 9
  - commercialization, 10
  - vs. droplet microfluidics, 6
  - electrowetting-on-dielectric, 7–8
  - high-level synthesis, 8–9
  - open-source platforms, 10–11
  - pin-constrained, 10 (*see* Tamper resistance)
  - structure, 7
- Digital microfluidics, 10, 11, 39, 136
- Digital polymerase chain reaction (dPCR)
  - commercial chip-based, 26
  - cost and resource requirements, 30
  - microfluidic technologies, 28
  - reactions and valve actuations, 26
  - simulated attack, 28–29
  - surface immunoassays, 12
  - target DNA, 27, 28
- DNA forensics, 37–38, 125
- Drug doping, 36–37

**E**

- Electrode addressing, 52–53
- Electrode coverage ratio, 85
- ElectrodeWeight, 91–93

**F**

- Fabrication, 4–7, 11, 22–25, 32, 42, 44
- Flow-based microfluidic biochips (FMFBs)
  - commercialization, 13
  - cyberphysical, 110
  - fabrication, 11
  - FPVAs, 12
  - microvalves, 12
  - routing crossbars, 13
- Forensic DNA barcoding
  - experimental results, 128–130
  - security implications, 124–125
  - tamper-mitigating routing graph, 125–128
- Fully-programmable valve arrays (FPVAs), 12

**I**

- Indicator droplets
  - actuation sequence, 62
  - ILP (*see* Integer linear programming (ILP))
  - performance, 70–71
  - probability of detection, 73

- problem statement, 63
  - vs. security metrics, 72
  - tamper resistance (*see* Tamper resistance)
- Integer linear programming (ILP)
  - based synthesis, 119–120
  - formulation, 75
  - heuristic synthesis algorithms, 128
  - indicator droplet insertion, 63–66
  - sliding window approximation, 67–69
- Intellectual property (IP)
  - attacks, 22
  - cyberphysical microfluidic devices, 24
  - microfluidics, 24
  - piracy, 19
  - protection, 136

**M**

- Micro-electrode-dot-array (MEDA), 44, 76, 136
- Microfluidics
  - amenability, 20
  - applications, 6
  - blood diagnostics, 34–36
  - chemical and biological sciences, 32
  - commercial platforms attacks, 26–27
  - computer-aided design, 4
  - CPMB (*see* Cyberphysical microfluidic biochip (CPMB))
  - cyberphysical integration, 3–4, 23, 24, 39–40
  - definition, 2
  - design flows, 5–6
  - digital, 10
  - DMFBs (*see* Digital microfluidic biochips (DMFBs))
  - FBMBs (*see* Flow-based microfluidic biochips (FBMBs))
  - high-level synthesis, 8
  - information leakage, 25
  - next-generation commercial devices, 19
  - platforms, 22
  - self-contained biochips, 3
  - small scale fluid manipulation, 1
  - sub-microliter domain, 2
- Microvalves, 11, 12
- Mitigation
  - active/passive methods, 109
  - CPMBs, 109
  - high-level security assessment, 109
  - microfluidic routing fabrics, 110
  - security assessment (*see* Security)
- Multilayer soft lithography, 11

**P**

- Patient data privacy, 31
- Pin-constrained DMFBs, 10, 53, 60, 70, 135
- Pin mapping, 11, 51, 54, 60–62, 64–66, 68, 74–76, 138
- Polymerase chain reaction (PCR)
  - DNA amplification, 80
  - dPCR (*see* Digital polymerase chain reaction (dPCR))
  - microfluidic devices, 38
  - pin mappers, 70
  - random checkpoints, 96–98
    - with error recovery, 98–99
    - and static, 98
  - and targeted DNA sequencing, 13
- Probability mass function (PMF), 83, 84, 86, 117, 125, 127
- Public safety, 6, 31–32

**R**

- Randomized checkpoints
  - assay's progression, 83
  - biased probability distributions
    - decomposition of probability of evasion, 87
    - PMF, 86
    - probability of evasion, 86–87
    - security, 87–88
  - commercial 3-plex immunoassay, 99–101
  - DMFB controller, 79, 82
  - PCR, 96–99
  - probability of evasion, 84–85
  - proposed system, 83–84
  - realistic system constraints, 95–96
  - static checkpoint placement
    - heuristic placement, 91–93
    - minimal provably secure placement, 89–91
    - problem statement, 89
    - security, 94–95
    - temporal randomization, 93
  - threat model (*see* Threat models)
  - TNT, 101–104
- Redundant units (RUs), 53–54, 57–58, 60, 67, 75
- Routing fabric analysis
  - evaluating security, 116–117
  - flow-based, 109
  - modeling preliminaries, 114–115
  - physical graph model, 115
  - prototyping, 13
  - routing graph model, 115–116

synthesis (*see* Synthesis)

*See also* Mitigation

**S**

- Security
  - attack constraints, 56
  - biased distributions, 87–88
  - checkpoint-based error recovery, 94–95
  - defense and public safety, 31–32
  - dPCR (*see* Digital polymerase chain reaction (dPCR))
  - experimental demonstration, 138
  - implications, 19, 38–40
  - metrics
    - coverage, 57–58
    - pin disturbance, 58–59
    - probability of detection, 59–60
  - mitigation
    - attack implications, 112–113
    - single pneumatic control line, 110
    - threat model, 111–112
  - motivations, 22–23
  - opportunities, 42–43
  - patient data privacy, 31
  - pin mapper, 51
  - refinement, threat model, 57
  - research integrity, 32–33
  - self-erasure and self-destruction, 137
  - tamper resistance, 53–55
  - taxonomy (*see* Taxonomy)
  - threat models, 21–22, 55
  - threats, 44–45
  - vulnerabilities, 5
  - See also* Trust
- Self-contained microfluidic biochips, 3
- Self-destruction, 137
- Self-erasure, 137
- Synthesis
  - algorithm, 126
  - CAD tool vendor, 6
  - DMFB, 10, 96
  - high-level, 8–9, 43
  - in-vitro protein, 7
  - routing fabric analysis
    - caveats, 123
    - fast, 120–122
    - ILP-based, 119–120
    - problem statement, 118–119
    - routing graph reduction, 122–123
  - routing graph construction, 129
  - toolchain, 137

**T**

- Tampering
  - actuation (*see* Actuation tampering)
  - mitigating routing fabrics (*see* Mitigation)
  - resistant (*see* Tamper resistance)
- Tamper resistance
  - baseline performance, 70
  - broadcast addressing, 52–53
  - comparisons, 74–75
  - CPMB, 51
  - electrode weighting, 75
  - performance with indicator droplets, 70–71
  - pin mapping (*see* Pin-constrained DMFBs)
  - probability of detection, 71–73
  - problem statement, 60
  - proposed solution, 60–62
  - security analysis (*see* Security)
- Taxonomy
  - attack surfaces, 20–21
  - motivations, 22–23
  - threat models, 21–22
- Threat models
  - attack
    - classification, 82
    - modeling, 81
  - attacker location, 22
  - denial-of-service, 80–81
  - DMFB platform, 55
  - field-level, 22
  - manufacturing-level, 22
  - physical tampering, 111–112
  - refinement, 57
  - taxonomy, 20
  - technical and operational abilities, 21
- Transposer, 13, 110, 112–124, 127, 129–132, 138
- Trinitrotoluene (TNT)
  - calibration curve attacks, 102–103
  - colorimetric assay being, 103, 104
  - DMFB, 103, 104
  - explosive chemical compound, 101–102
- Trust
  - and security (*see* Security)
  - SensorPUFs, 136–137