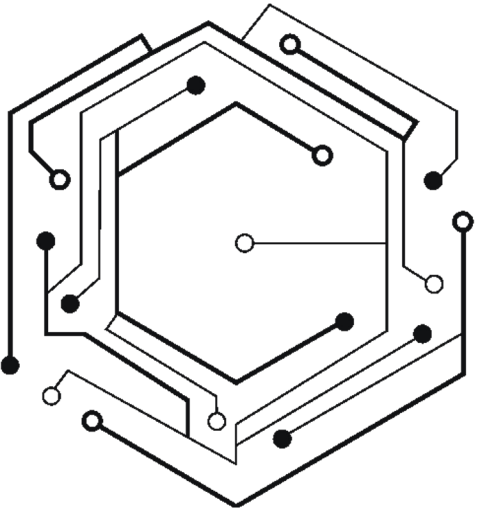
NYU Center for Cybersecurity



NYU CENTER FOR CYBER SECURITY

https://cyber.nyu.edu/

Ramesh Karri
cell: 917 363 9703
email: rkarri@nyu.edu

Talk: High-Level Approaches to Hardware Security

Mission

NYU Center for Cybersecurity

NYU Center for Cybersecurity (CCS) is an interdisciplinary center dedicated to

- Research to secure the cyber infrastructure
- Educate the next generation of cybersecurity professionals and the workforce
- Shape public discourse on the policy and legal aspects of cybersecurity.

NYU TANDON

NYU COURANT

NYU LAW

جامعة نيويورك ابوظبي
NYU ABU DHABI

NYU STEINHARDT

NYU STERN

NYU ROBERT F. WAGNER GRADUATE SCHOOL OF PUBLIC SERVICE

http://cyber.nyu.edu/

NYU Center for Cybersecurity

J. Cappos, Tandon, S/W Supply Chain Security

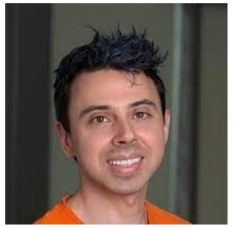
B. Dolan-Gavitt, Tandon, S/W Security AI

Y. Dodis, Courant Crypto

S. Garg, Tandon, H/W Security and AI

R. Milch, Law, Security

R. Karri, Tandon, H/W supply chain Security



D. Mccoy, Tandon, Security & Privacy

R. Greenstadt, NYU-Tandon, Security, Privacy

M. Maniatakos, NYU-AD, Sys Security

N.Memon, Tandon, Digital Forensics, AI

J. German, Law, Security

N. Gupta, Tandon, DM Suplly Chain Security

C. Popper, NYU-AD Wireless and 5G Security

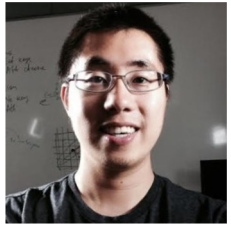
B. Reagan, NYU-Tandon, Privacy Comp. Archs.

S. Raskoff, Law

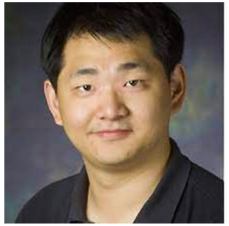
K. Ross, NYU-Shanghai, Soc Networks Privacy

O. Sinanoglu, NYU-AD, H/W Security

L. Subramanian, Courant, Sys Security



D. Huang, NYU-Tandon, Privacy



Q. Zhu Tandon, Game theory

R. Zimmerman, Wagner, Risk

Research Impact

NYU Center for Cybersecurity

- Over 20 Faculty PIs across multiple Departments, Schools and Campuses
- Mentoring about 80 PhD students and ten researchers
- Research Areas
  - Critical infrastructure security (e.g. powergrid, PLC, transportation)
  - Supply Chain Security (H/W, S/W, Digital Manufacturing)
  - Security and Privacy of AI (Security of LLMs, Backdoors in MLs, Deepfakes)
  - AI for Security (Hardware, Firmware, Software, Systems)
  - Hardware Accelerators for Post Quantum Crypto, Encrypted Computation
  - Digital Forensics
  - Usable Security and User Behavior
  - Interdisciplinary approaches to cybersecurity
- Funded by DARPA, ONR, ARO, AFOSR, NSF, Industry, etc.
- Raised > $40 Million over six years (2016-2022)
- Service on TPCs of top Cybersecurity Conferences (S&P, USENIX, CCS, NDSS).
- Space: 10,000 Sq ft in NYU-NY + 8,000 Sq ft in NYU-AD
- Dual PhD Program with Indian Institute of Technology, Kanpur, India
- In progress: NYUNY-NYUAD Joint PhD Program in Cybersecurity

Research Collaborations and Funding

NYU Center for Cybersecurity

Some of our past collaborators:

Universities

Gov't and NGOs

Industry

Education/Workforce Development: Impact

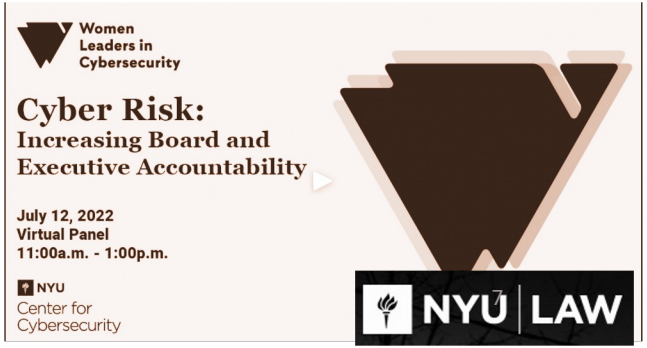
NYU Center for Cybersecurity

- One of the earliest to offer degrees in Cyber Security (circa 1998)
- Triple distinction
  - NSA Center of Excellence in Information Assurance Education
  - NSA Center of Excellence in Information Assurance Research
  - NSA Center of Excellence in Cyber Operations
- Hosts the NSF/NSA CyberCorps Program
  - Robust research and training partnership with federal agencies
  - Placed over 120 US Citizen students in US Govt agencies
- Developed the MS in Cybersecurity
- Launched the Cyber Fellows Program (affordable online MS in Cybersecurity)
- Designed and Offered MS in Cyber Risk and Strategy (joint with NYU Law)
- Built a Bridge to Cyber (to transition non-STEM students into cyber workforce)
- Innovated the stackable credentials (one month cybersecurity modules)

Outreach Programs: Impact

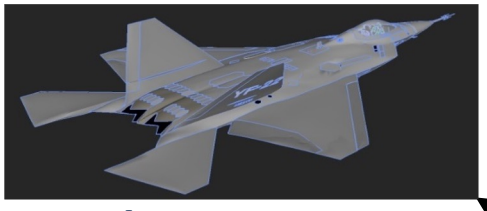
NYU Center for Cybersecurity

- CSAW (csaw.io): celebrating its 19th year
  - Largest student cyber competition in US
  - Largest CTF
  - First Embedded Security Challenge
  - High School (Red) Challenge
  - Cyber Policy Challenge
  - Applied Research Competition
  - First Cyber Journalism Award
  - 10,000+HS and college students
  - Worldwide: MENA (NYU-AD, SUP-COM Tunis), India (IIT Kanpur), Europe (France), Israel (Haifa), Mexico
- Cybersecurity club: https://www.osiris.cyber.nyu.edu/
- Cyber boot-camp for High School STEM Educators
- Hackers in residence
- Sloan/AIG Speaker Series
- https://www.womenleadersincybersecurity.org



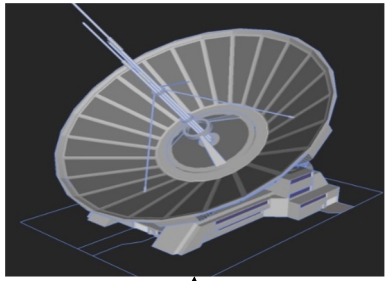
Applications of Integrated Circuits

NYU Center for Cybersecurity

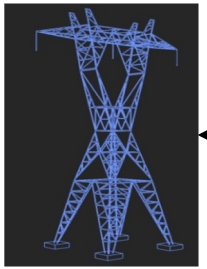


Aerospace

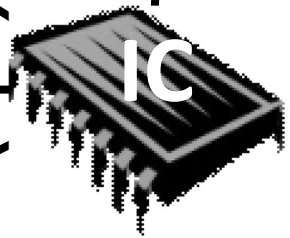
Communications



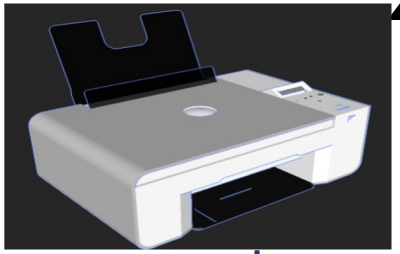
Healthcare



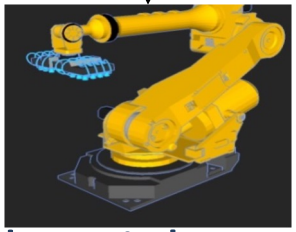
Energy



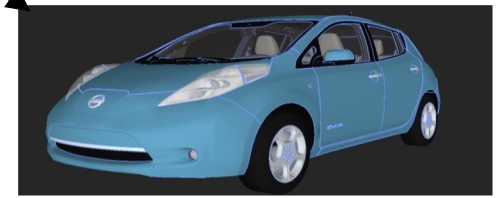
Appliances



Consumer electronics

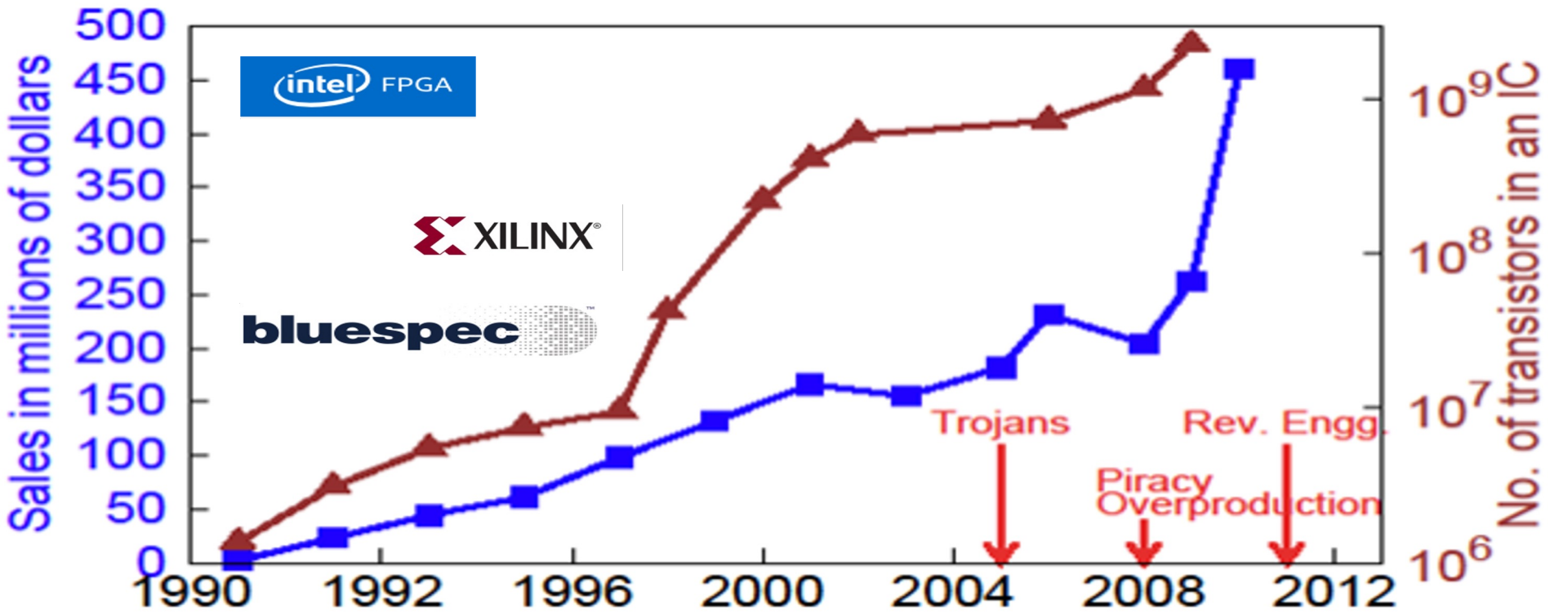


Industrial Control



High-Level H/W Design

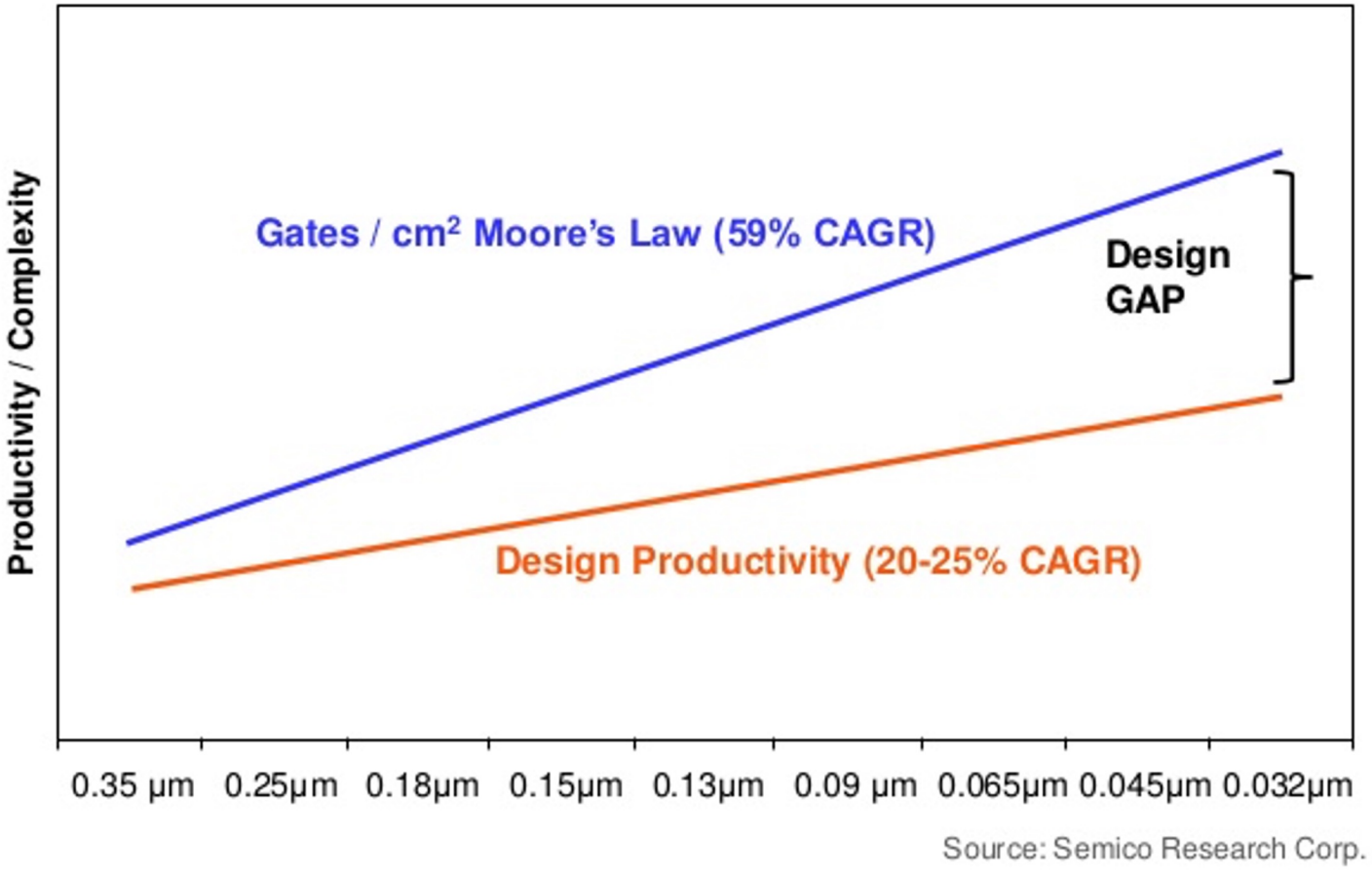
NYU Center for Cybersecurity



CALYPTO Design · Optimize · Verify ↔ Mentor Graphics ↔ Oasys ↔ FORTE DESIGN SYSTEMS ↔ cadence

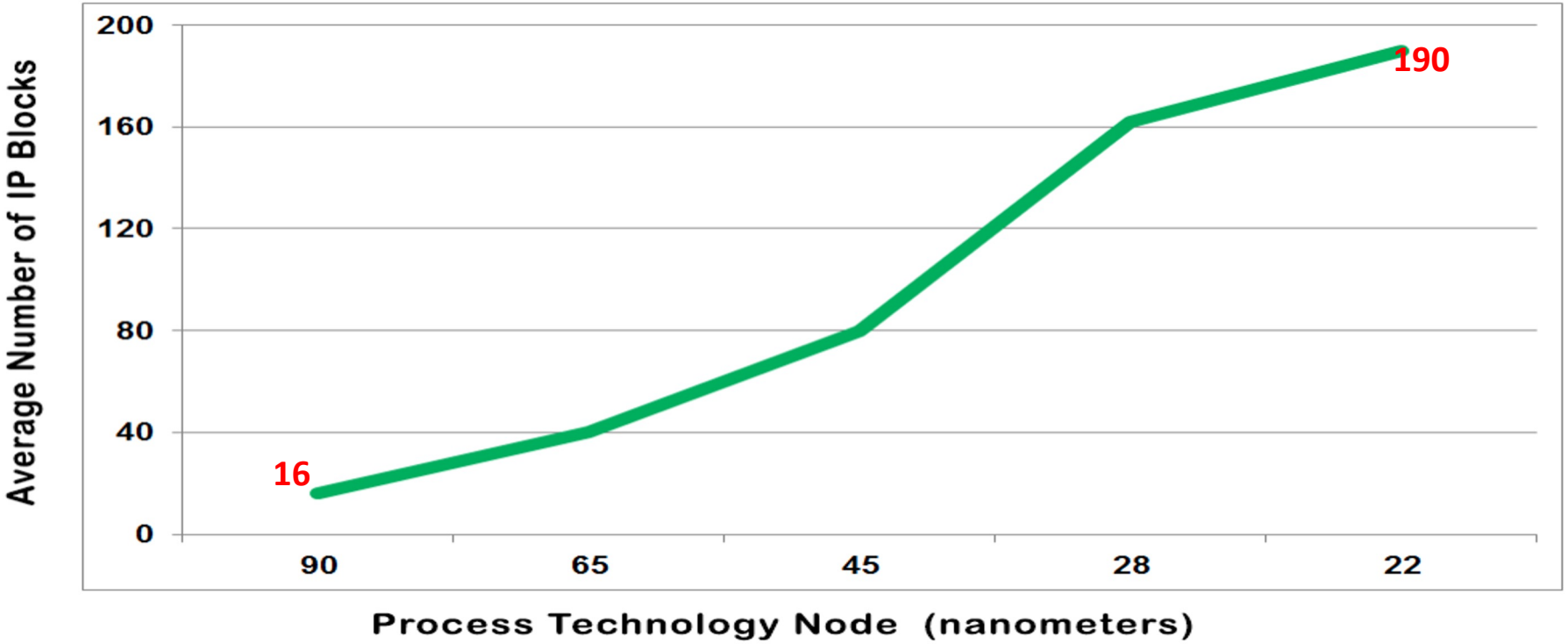
HLS is a Productivity Tool

NYU Center for Cybersecurity



More 3rd Party IPs in a Design

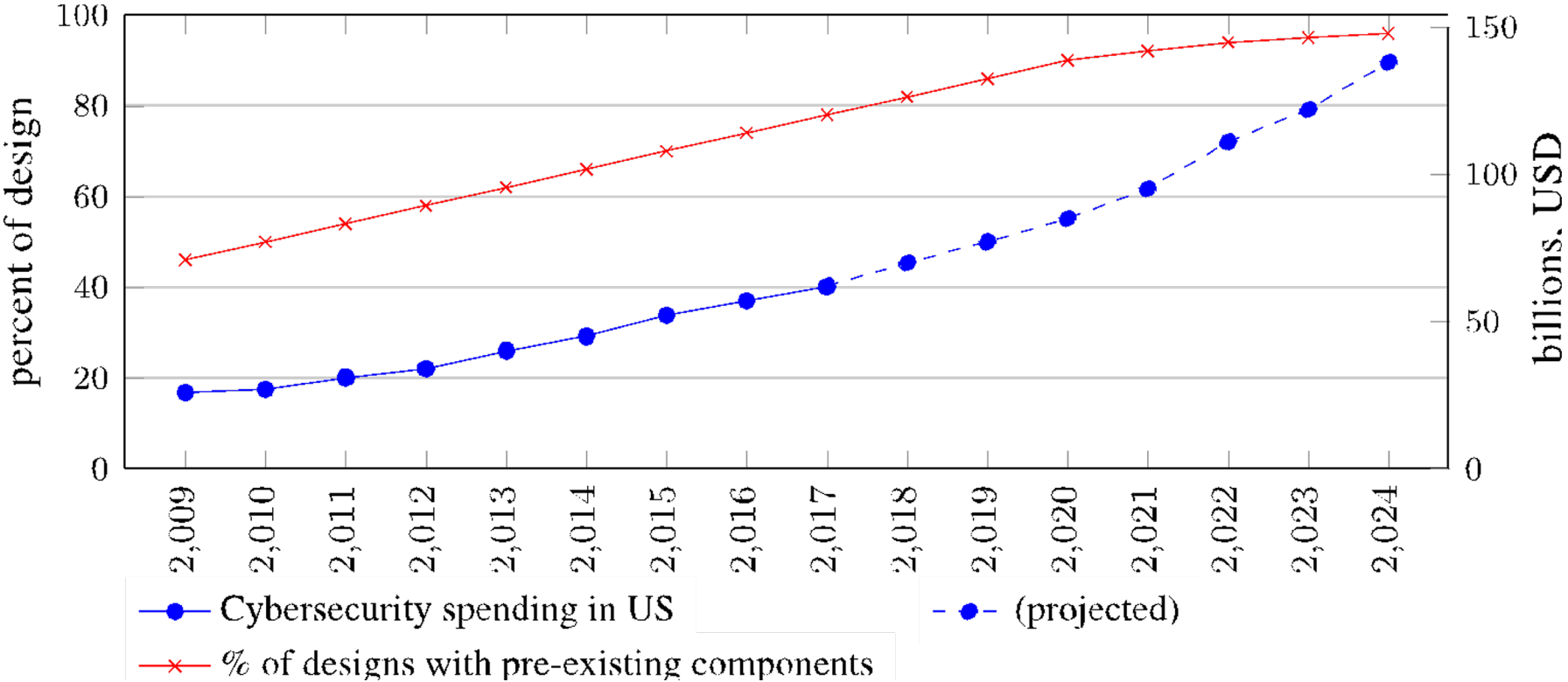
NYU Center for Cybersecurity



(International Business Strategies, 2012)

Accelerator-based Design

NYU Center for Cybersecurity

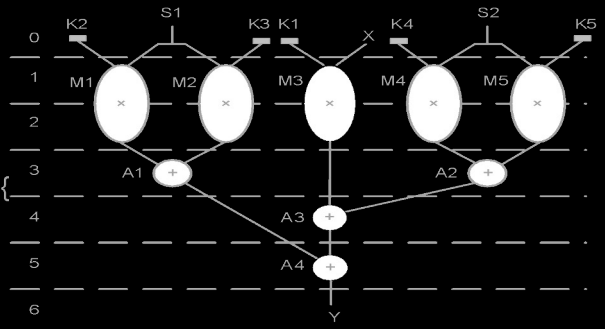


High-Level Design Flow

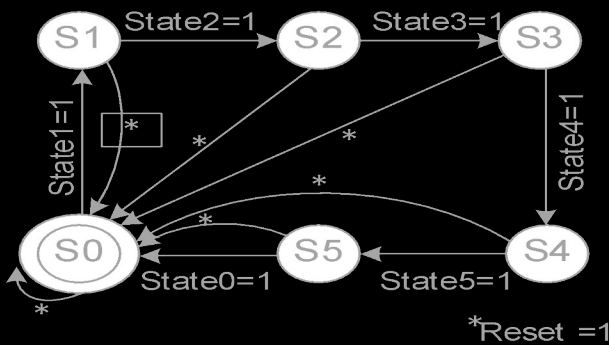
NYU Center for Cybersecurity

```
int main (int X, int *Y, int *Z1, int *Z2 : num16) {
        int in1 = (X * K1);
        Y = biquad(in1, K2, K3, K4, K5, *Z1, *Z2);
        return Y;
}
int biquad(int in, int a1, int a2, int b1, int b2, int *Z1, int *Z2){
        int state = in + (a1 × *Z1) + (a2 × *Z2);
        return state + (b1 × *Z1) + (b2 × *Z2);
}
```

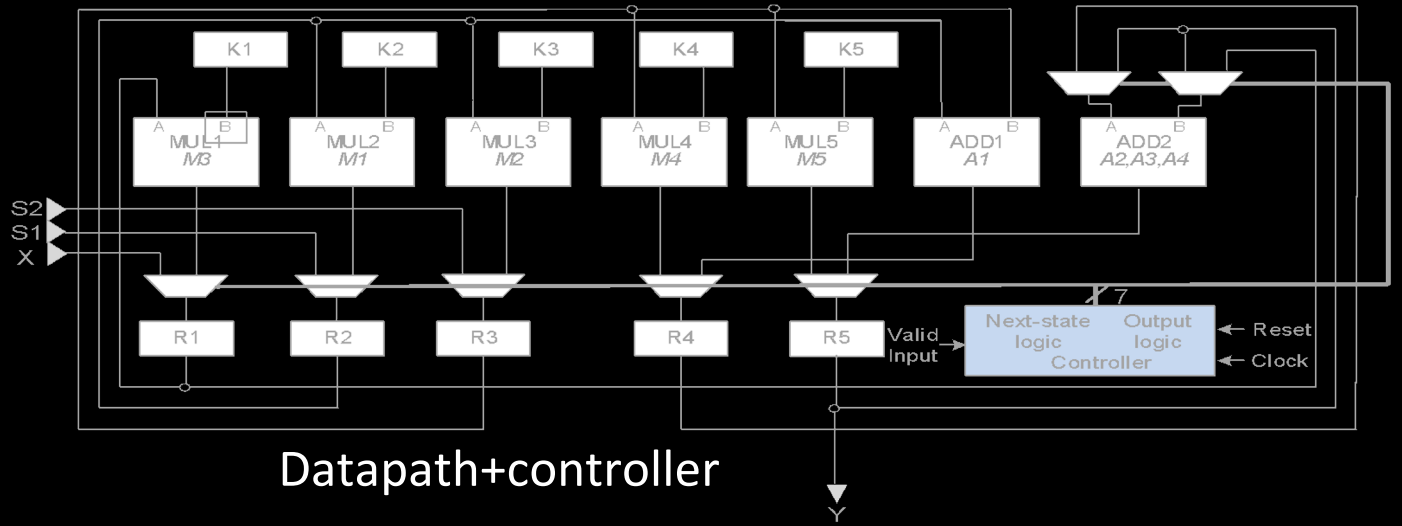
c-specification of biquad filter



Scheduling and binding

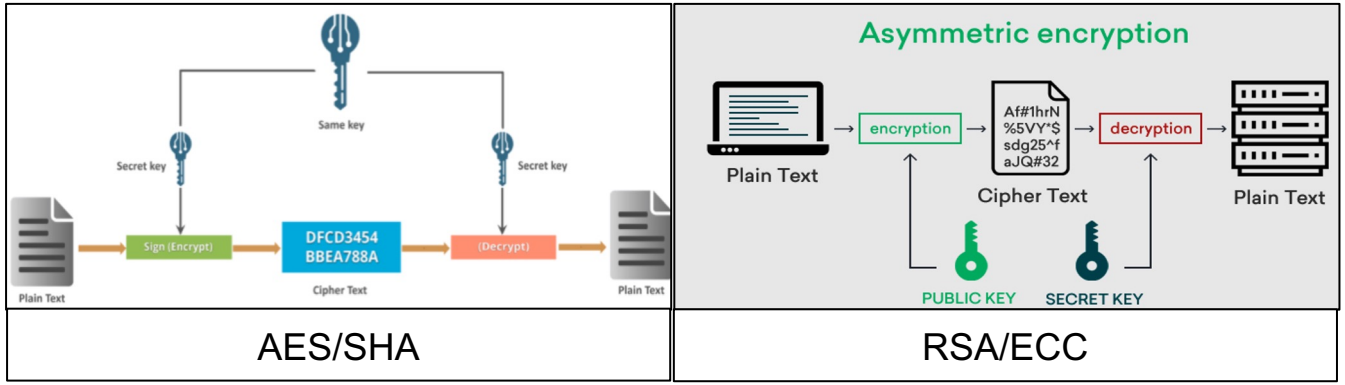


Finite state machine



Datapath+controller

Post Quantum Crypto

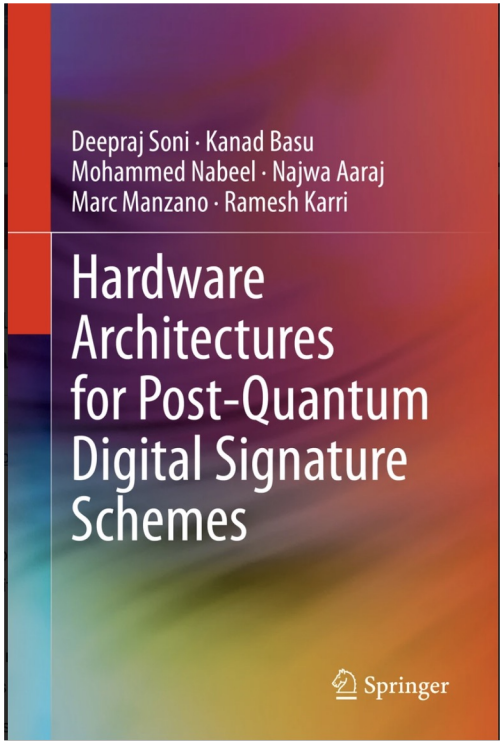


- Quantum computers can break RSA and Elliptic Curve Crypto
- Quantum computers cannot break AES and SHA
- PQC algorithms are Asymmetric Crypto replacements to RSA/ECC
  - Key Encapsulation Mechanism (KEM)
  - Signature-Generation/Verification

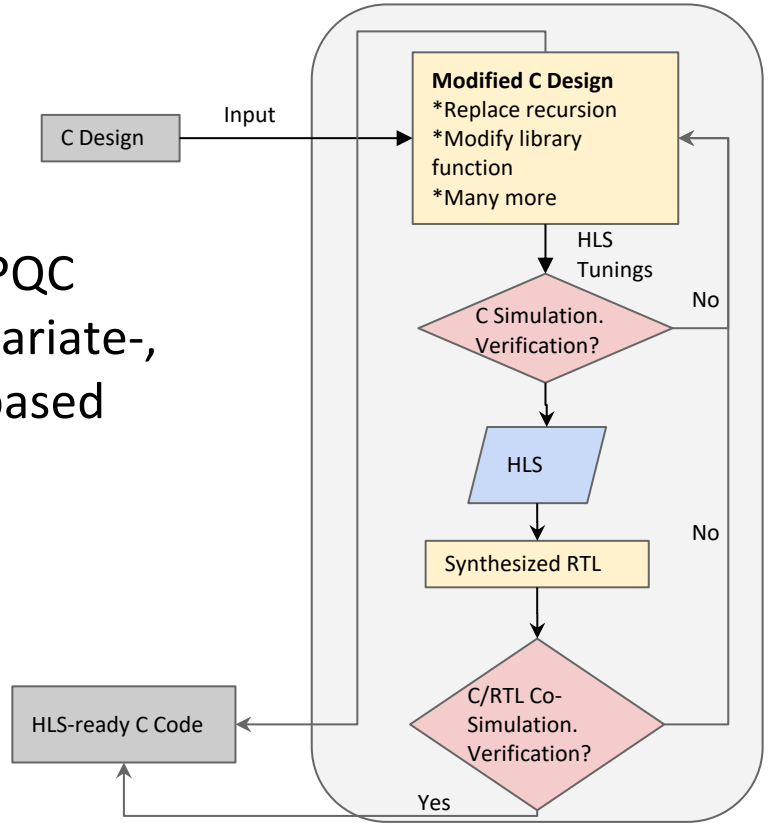
NIST PQC Standardization

- Round 1 -> 82 submissions: Evaluated for security
- Round 2 -> 26: Security, hardware/software perf, power
- Round 3 -> 15: Security, hardware/software perf, power
- Winners
  - Digital Signatures: Crystals-Dilithium, Falcon, Sphincs
  - KEM: CRYSTALS-KYBER (a fourth round….

C→FPGA/ASIC Rnd 2 Candidates



We implemented round 2 PQC candidates: Lattice-, Multivariate-, Code-, Hash- and Isogeny-based



Security-Aware HLS of Accelerators

NYU Center for Cybersecurity

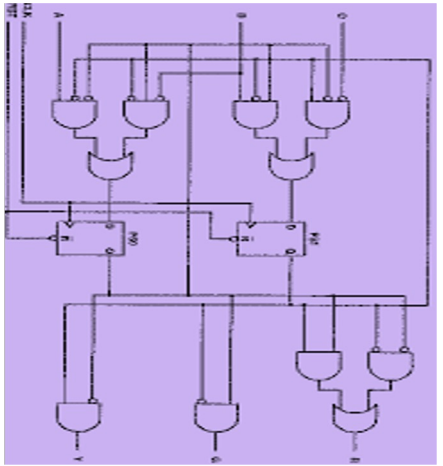
Hard to secure

Semantic Information

C/C++ → RTL → Netlist

```
for (i=0; i<N; i++)
        c[i] = a[i]+b[i];
        .....
```

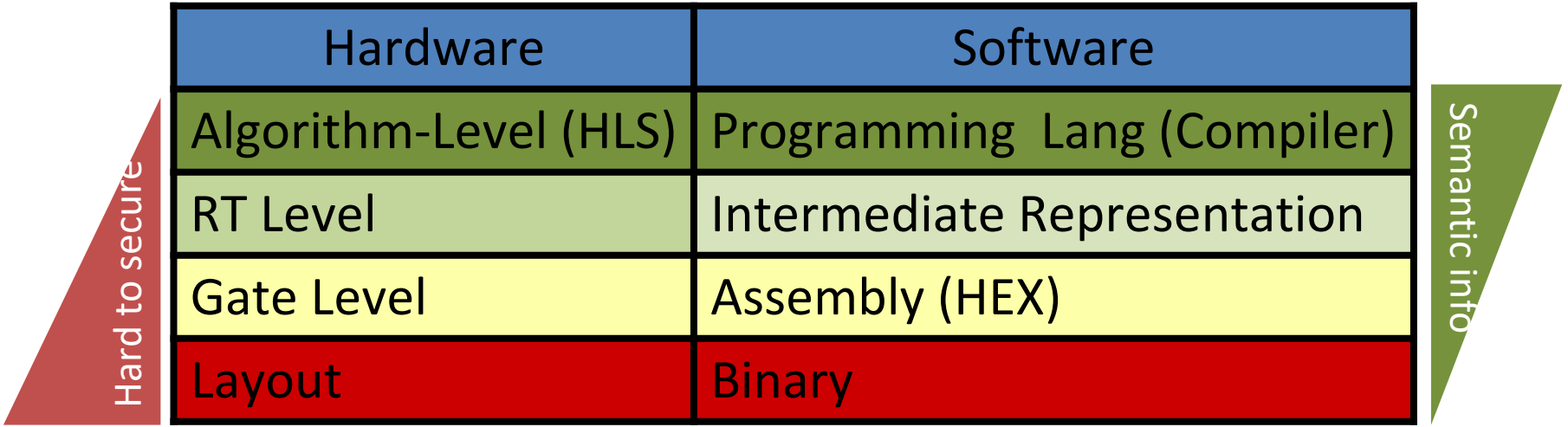
```
always @ posedge clk
        a[i] <= b[i] + c[i];
        .....
```



Security-Aware HLS

NYU Center for Cybersecurity

- Promising to add security constraints
- HLS in Hardware vs Programming Lang/Compilers in Software
- Semantics: sensitive constants, critical operations, protected control flow, run-time dependencies (sensitive IP)



Takeaways

NYU Center for Cybersecurity

- High-Level is a promising level to Design (Security) Accelerators

  K. Basu, D. Soni, N. Mohammed, R. Karri, *NIST Post Quantum Cryptography: A Hardware Evaluation Study, Jan 2019*; iacr eprint

- High-Level is a promising level to Design-in Security

  C Pilato, S Garg, K Wu, R Karri, F Regazzoni, *Securing Hardware* Accelerators*: A New Challenge for High-Level Synthesis,* (a Perspective Paper), IEEE Embedded Systems Letters, *DOI*: 10.1109/LES.2017.2774800

- HLS can be used for Trojan Detection and Isolation

  J. Rajendran, O Sinanoglu, and R Karri, *Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach*, IEEE Trans VLSI, 24(9): 2946-2959, Sep 2016, DOI: 10.1109/TVLSI.2016.2530092

  J. Rajendran, H. Zhang, O. Sinanoglu *and* R. Karri, *High-level synthesis for security and trust,* IEEE Intl On-Line Testing Symposium, pp. 232-233. July 2013, doi: 10.1109/IOLTS.2013.6604087

- HLS can be used to Watermark Designs

  C. Pilato and K. Basu and M. Shayan and F. Regazzoni and R. Karri, *High-Level Synthesis of Benevolent Trojans*, Design Automation Test in Europe Conference, pp. 1118—1123, March, 2019.

- HLS can be used for Seamless and Meaningful Design Obfuscation

  C. Pilato, F. Reggazoni, S. Garg and R. Karri, *TAO: Techniques for Algorithm Level Obfuscation During High-Level Synthesis*, IEEE/ACM Design Automation Conference, June 2018, DOI: 10.1109/DAC.2018.8465830.

- HLS can be used for Seamless and Meaningful Taint Propagation

  C. Pilato, F. Reggazoni, S. *Garg* and R. Karri, *TaintHLS: High-Level Synthesis For Dynamic Information Flow Tracking*, IEEE Trans. CAD, DOI: 10.1109/TCAD.2018.2834421

- HLS-generated Designs can be Reverse Engineered !

  J. Rajendran, A. Ali, O. *Sinanoglu* and R. Karri, *Belling the CAD: Toward Security-Centric Electronic System Design,* IEEE Trans. CAD, Vol 34, No. 11, pp. 1756-1769, Nov 2015, DOI: 10.1109/TCAD.2015.2428707.

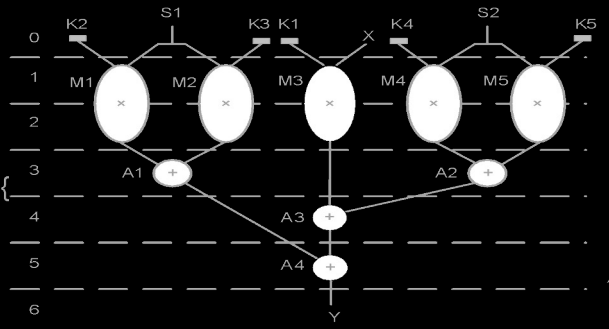
- A Black-Hat can use High-Level Synthesis to undermine Designs (weaken crypto, drain battery, etc)

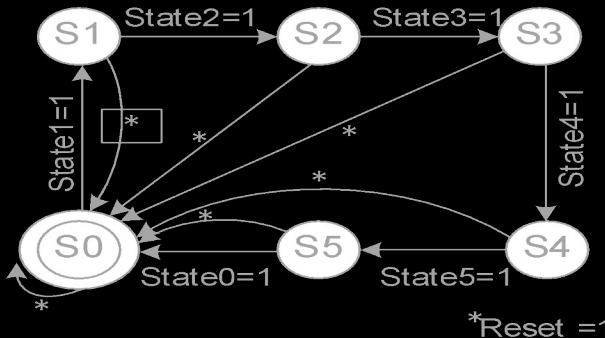
  C Pilato, K Basu, F Regazzoni, R Karri, *Black-Hat High-Level Synthesis: Myth or Reality?* IEEE Trans. VLSI, DOI: 10.1109/TVLSI.2018.2884742

Can HLS Undermine Security?

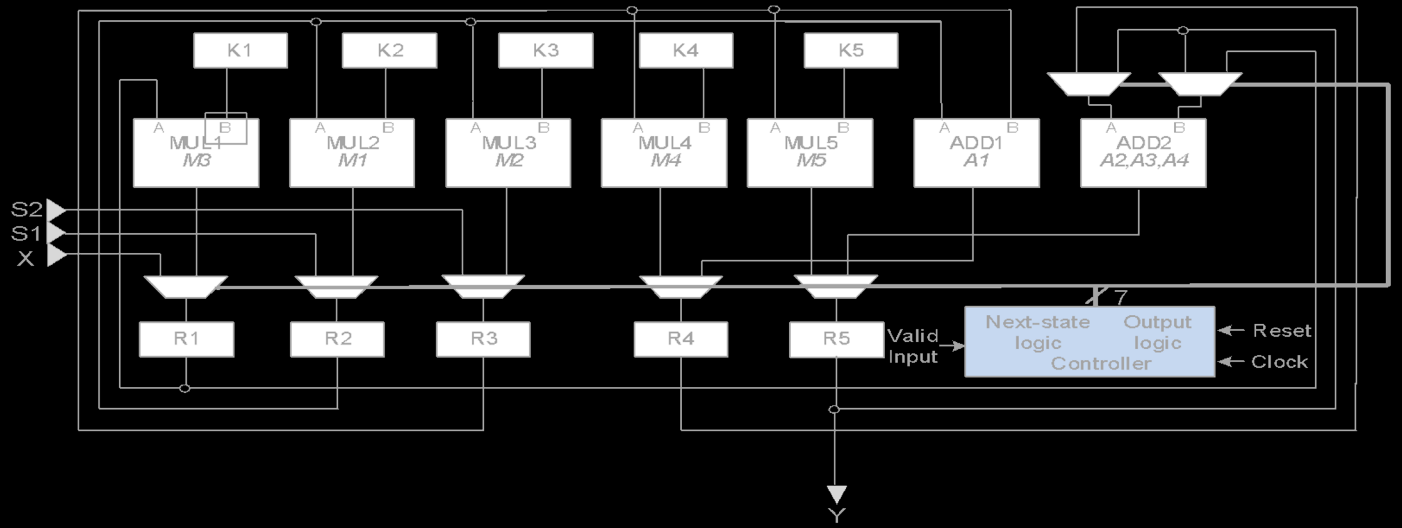
NYU Center for Cybersecurity

```
int main (int X, int *Y, int *Z1, int *Z2 : num16) {
        int in1 = (X * K1);
        Y = biquad(in1, K2, K3, K4, K5, *Z1, *Z2);
        return Y;
}
int biquad(int in, int a1, int a2, int b1, int b2, int *Z1, int *Z2){
        int state = in + (a1 × *Z1) + (a2 × *Z2);
        return state + (b1 × *Z1) + (b2 × *Z2);
}
```

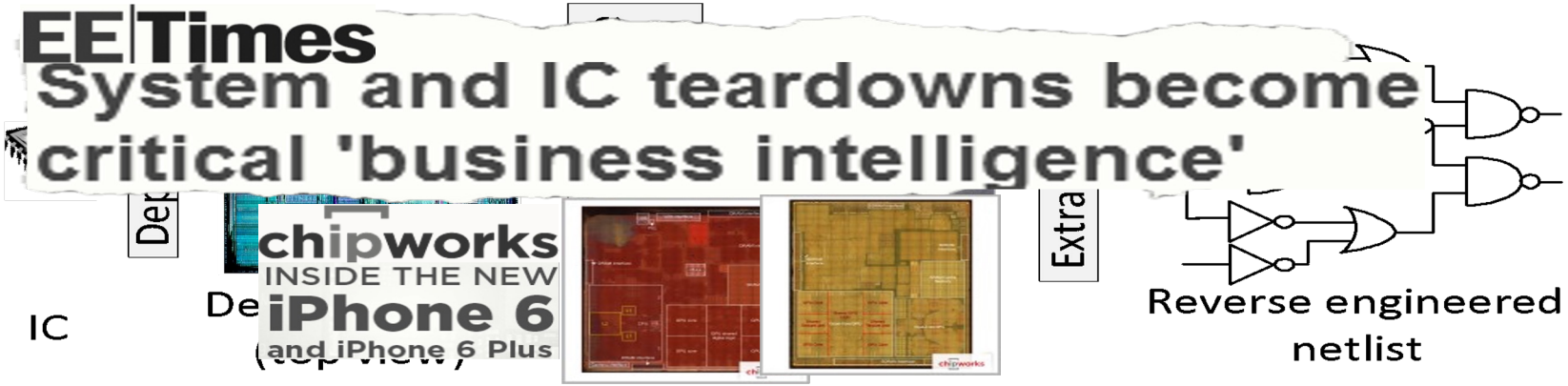




Can HLS undermine security of the design?



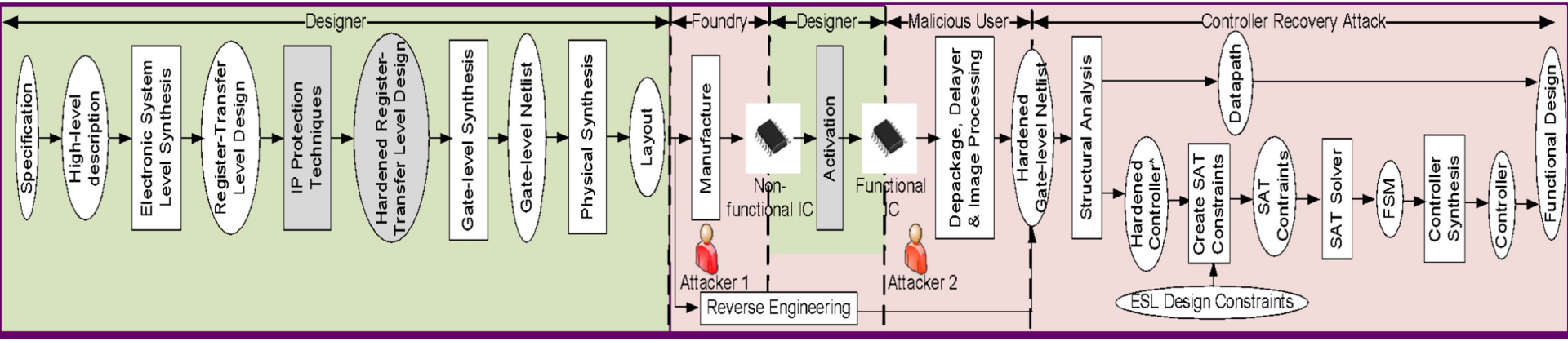
Threat: Reverse Engineering



- Legal: to detect piracy
  - Identify device technology, functionality, design
  - Chipworks
- Illegal: piracy, IP theft and Trojan insertion
  - Malicious user, Malicious SoC integration house, Malicious foundry

HLS-based Reverse Engineering

NYU Center for Cybersecurity

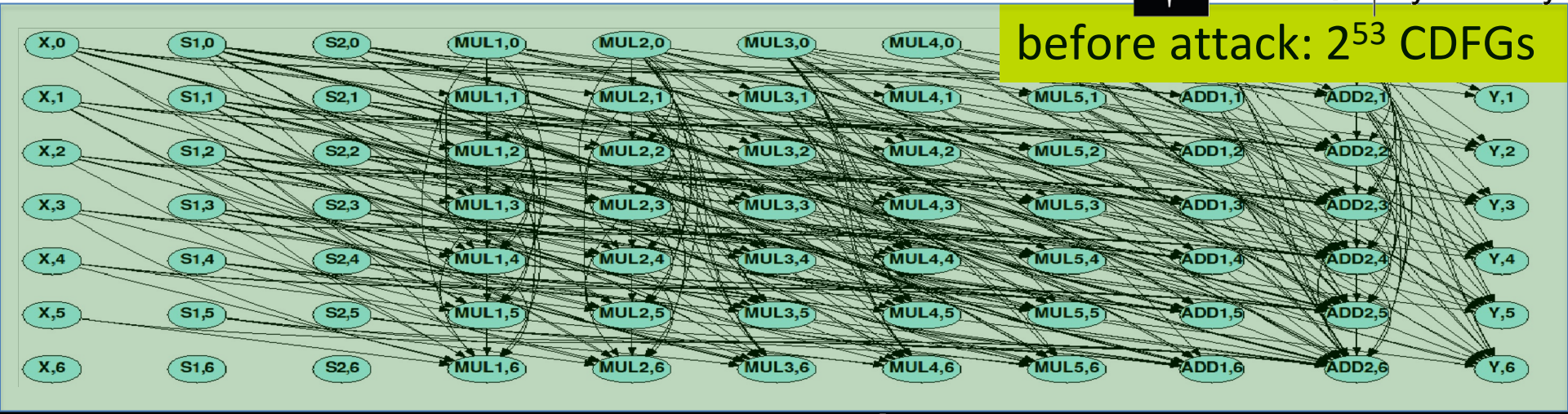


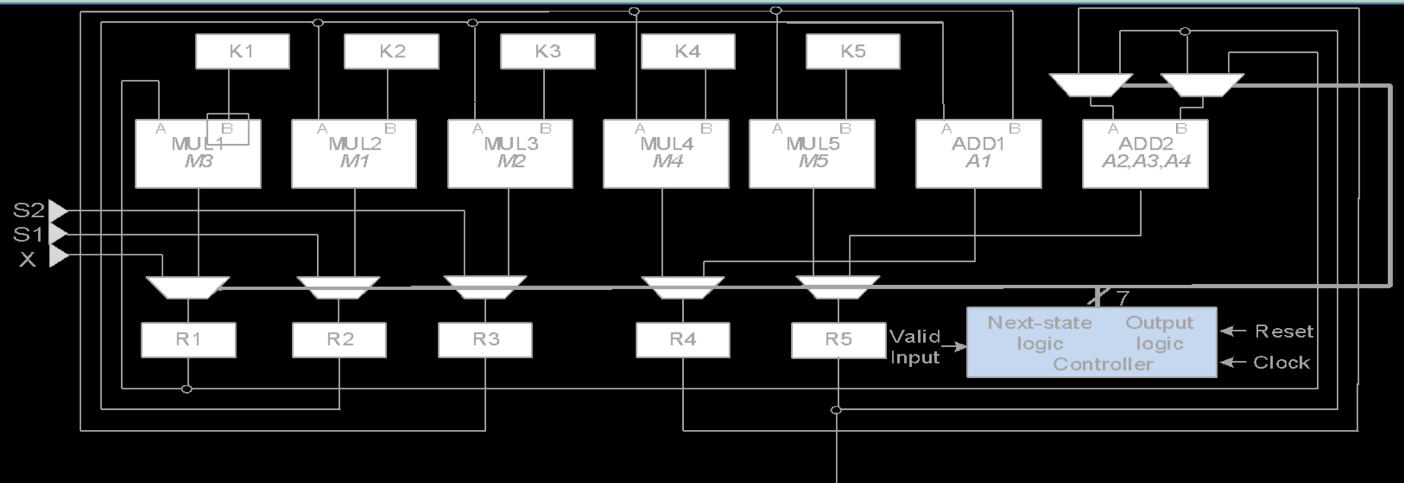
J. Rajendran, A. Ali, O. Sinanoglu and R. Karri, Belling the CAD: Toward Security-Centric Electronic System Design, IEEE Transactions on CAD, Vol 34, No. 11, pp. 1756-1769, November, 2015.

Security Metric: # of CDFGs

NYU Center for Cybersecurity

before attack: 2^{53} CDFGs

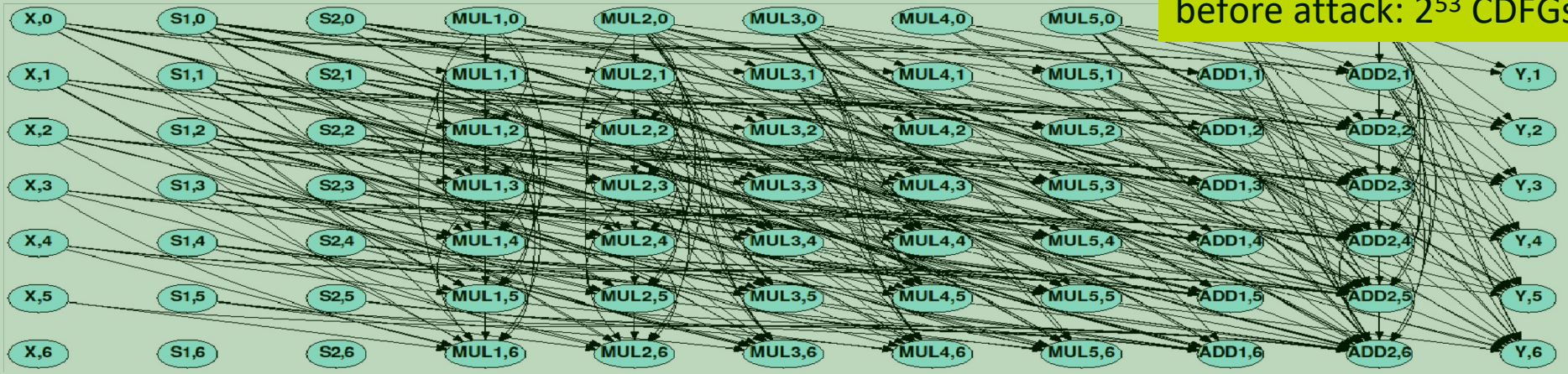


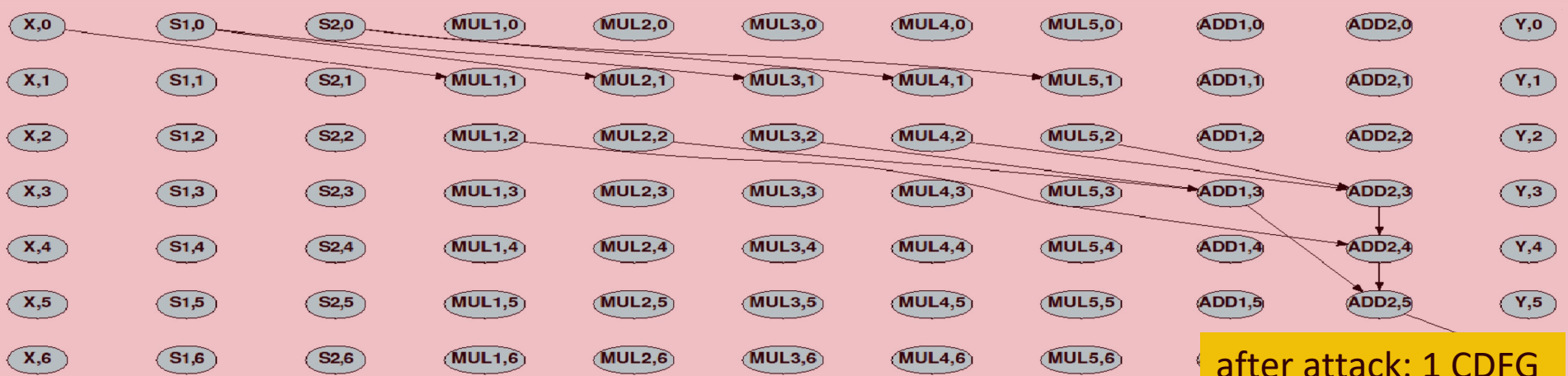


Security Metric: # of CDFGs

NYU Center for Cybersecurity

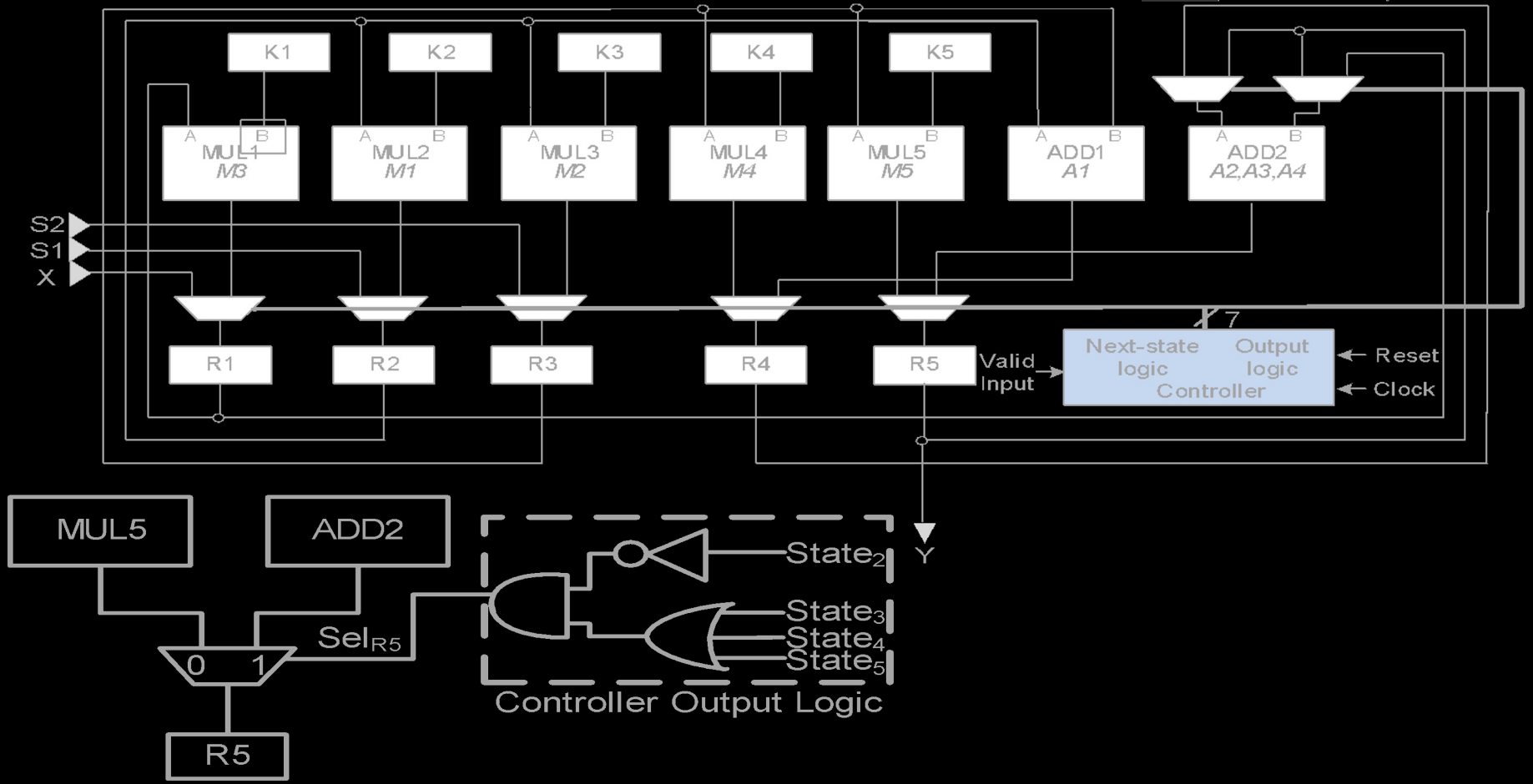
before attack: 2^{53} CDFGs



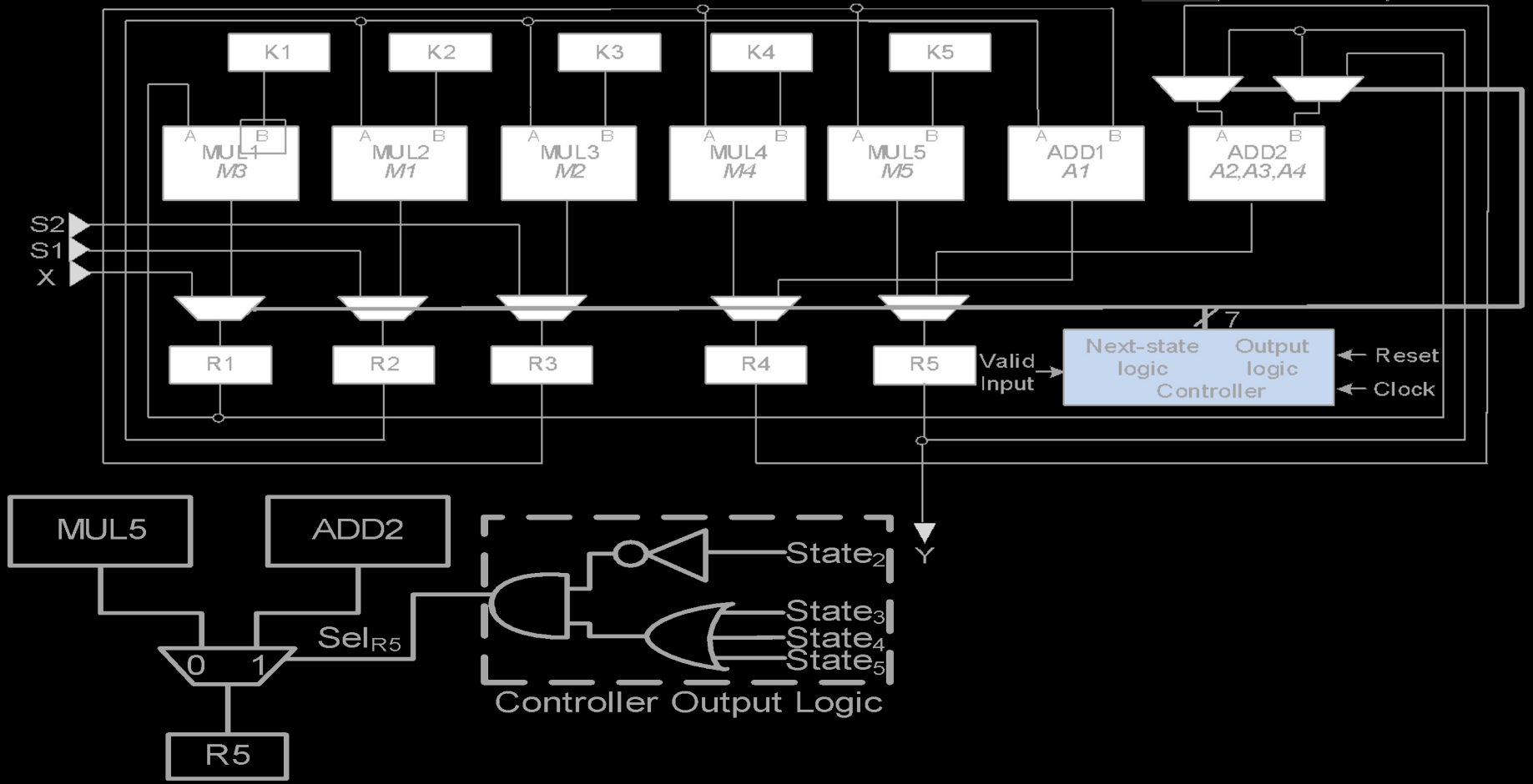


after attack: 1 CDFG

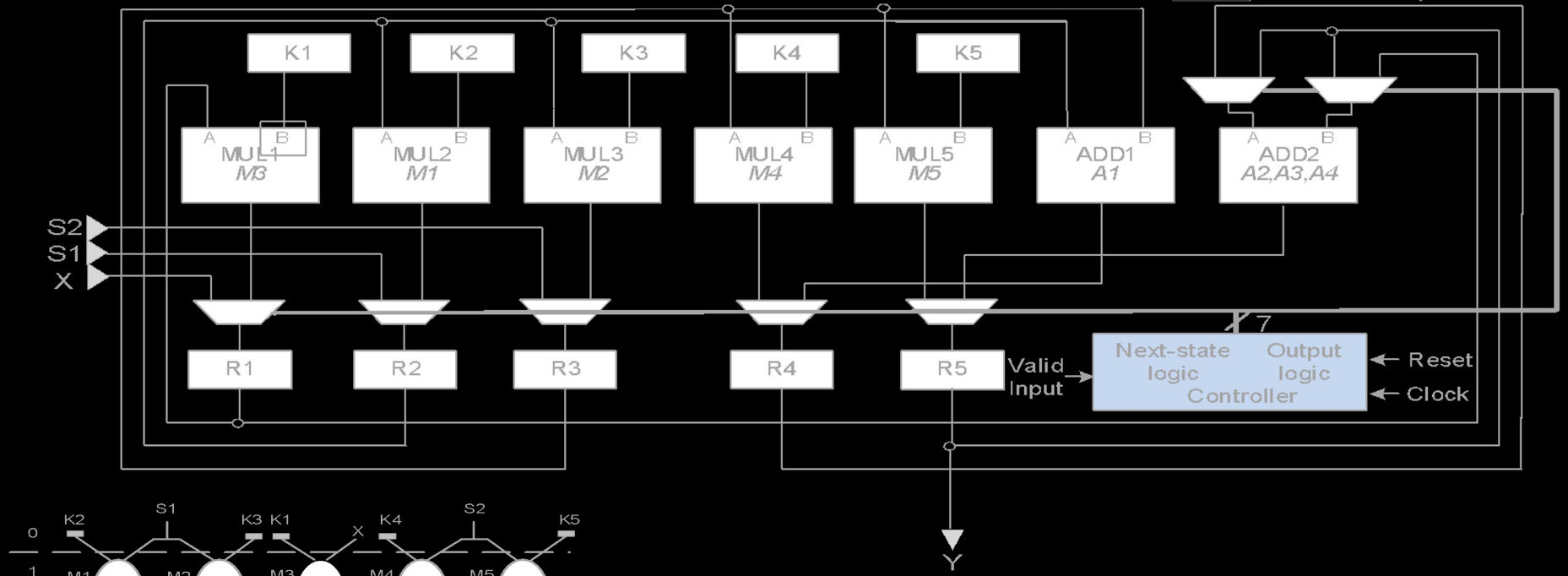
Datapath Constraints

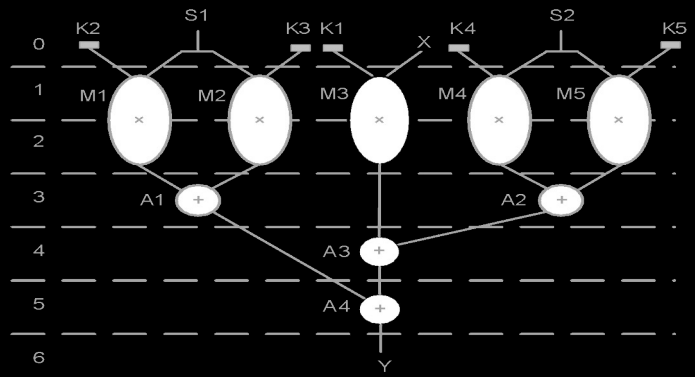


Controller Constraints



Input-Output Constraints





Security Metric: # of CDFGs

NYU Center for Cybersecurity

Design	ESL Constraints			
	# 1	# 1 – # 4	# 1 – # 6	# 1 – # 7
BQF	2^{53}	2^{52}	2^{33}	2^{2}
Arai	2^{246}	2^{160}	2^{118}	2^{3}
Chem	2^{3526}	2^{717}	2^{606}	2^{4}
Dir	2^{731}	2^{160}	2^{118}	2^{3}
Feig_dct	2^{3790}	2^{606}	2^{512}	2^{4}
Honda				
Lee				
Mcm	2^{716}	2^{160}	2^{118}	2^{3}
Pr	2^{319}	2^{216}	2^{160}	2^{3}
Wang	2^{321}	2^{215}	2^{160}	2^{3}
Snow3g	2^{383}	2^{80}	2^{53}	2^{3}
Kasumi	$\geq 2^{1000000}$	2^{757749}	2^{752363}	2^{9}

# of CDFGs reduce drastically using HLS constraints

J. Rajendran, A. Ali, O. Sinanoglu and R. Karri, Belling the CAD: Toward Security-Centric Electronic System Design, IEEE Transactions on CAD, Vol 34, No. 11, pp. 1756-1769, November, 2015.

Belled the CAD!

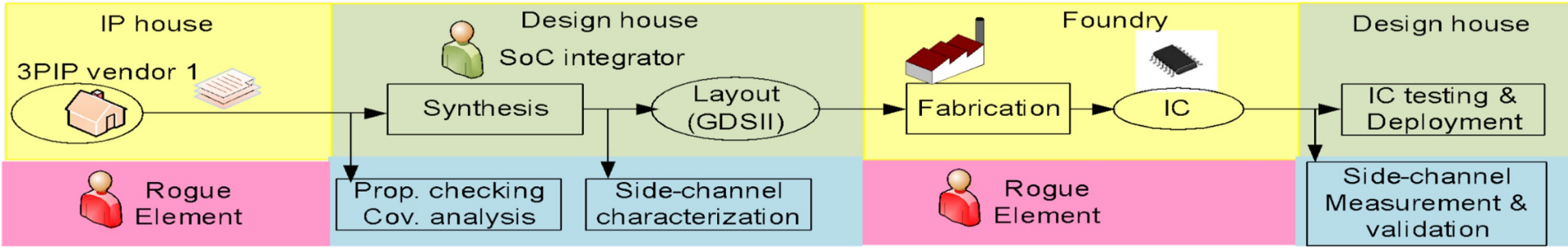
NYU Center for Cybersecurity

Design	Tools A,B, C, D & E: Non-pipelined and Resource-Constrained				
	Attack Success			Attack Cost	
	No. of compare points	% compare points matched	Equivalence checking	# of SAT literals	Time for solving SAT (s)
BQF	16	100	Pass	1050	0.01
Arai	128	100	Pass	5166	0.02
Chem	240	100	Pass	2415264	43
Dir	48	100	Pass	32448	0.75
Feig_dct	1024	100	Pass	517545	5.17
Honda	144	100	Pass	191565	1.10
Lee	128	100	Pass	10374	0.05
Mcm	128	100	Pass	56160	0.35
Pr	128	100	Pass	12320	0.01
Wang	128	100	Pass	11520	0.04
Snow3g	32	100	Pass	27720	0.17
Kasumi	64	100	Pass	8090016	143

All benchmarks reverse engineered in <30 minutes
Functionally equivalent and structurally identical!

J. Rajendran, A. Ali, O. Sinanoglu and R. Karri, Belling the CAD: Toward Security-Centric Electronic System Design, IEEE Transactions on CAD, Vol 34, No. 11, pp. 1756-1769, November, 2015.

Threat: Malicious 3PIP (Trojans)



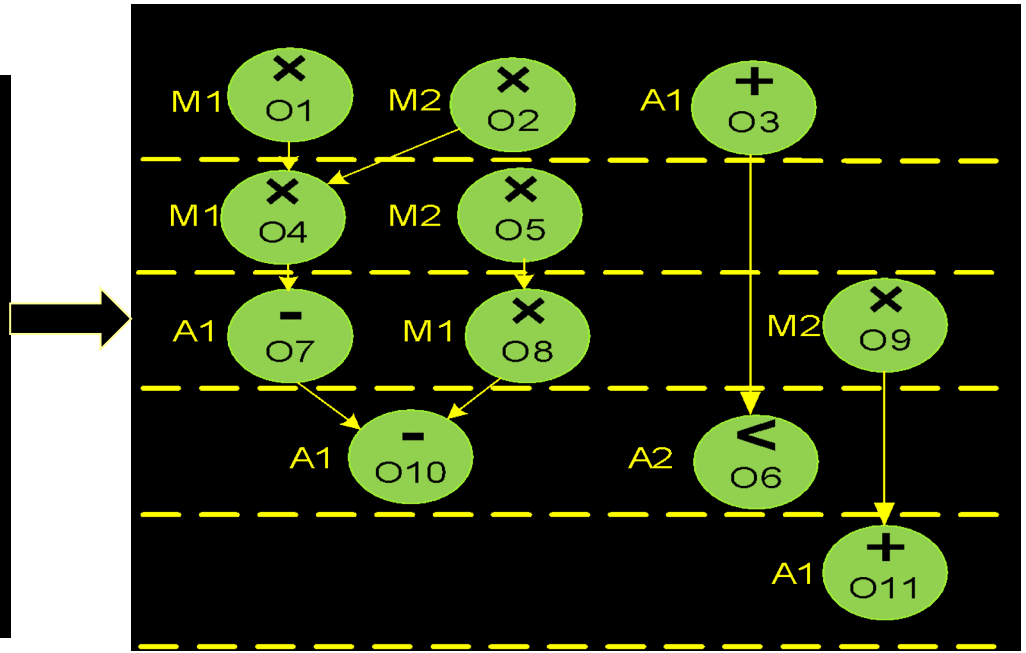
- 3PIP vendors are not trusted; may insert trojans
  - Trojans cause wrong outputs
  - Distributed: in different modules from same vendor may collude
- SoC integrator is trusted
  - SoC integrator uses components from 3PIP vendors
  - 3PIPs are integrated into a system and synthesized
- SoC is manufactured at an off-shore foundry
- The manufactured hardware is tested and deployed

J. Rajendran, O Sinanoglu, and R Karri, Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach, IEEE Trans VLSI, 24(9): 2946-2959, Sep 2016, DOI: 10.1109/TVLSI.2016.2530092

HLS for Trojan Detection

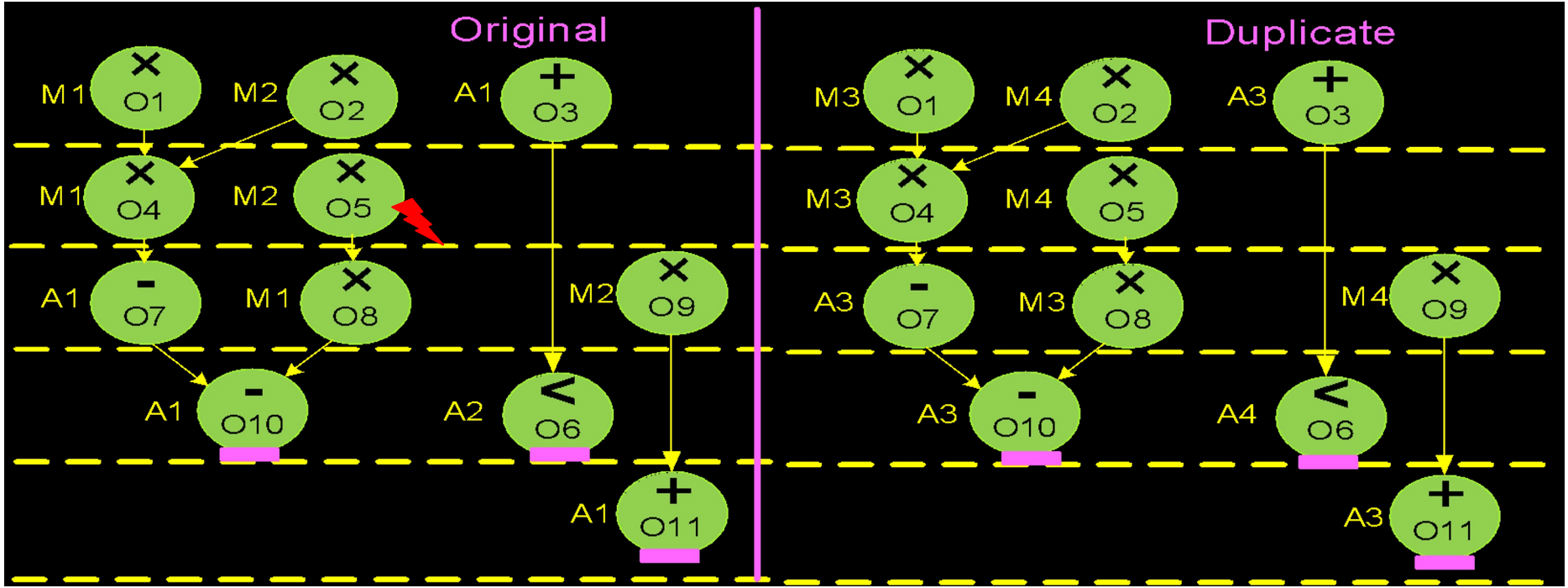
NYU Center for Cybersecurity

```
While (x < a)
{
    x1 = x + dx
    u1 = u – 3xudx – 3ydx
    y1 = y + udx
    x = x1; u = u1; y = y1
    }
```



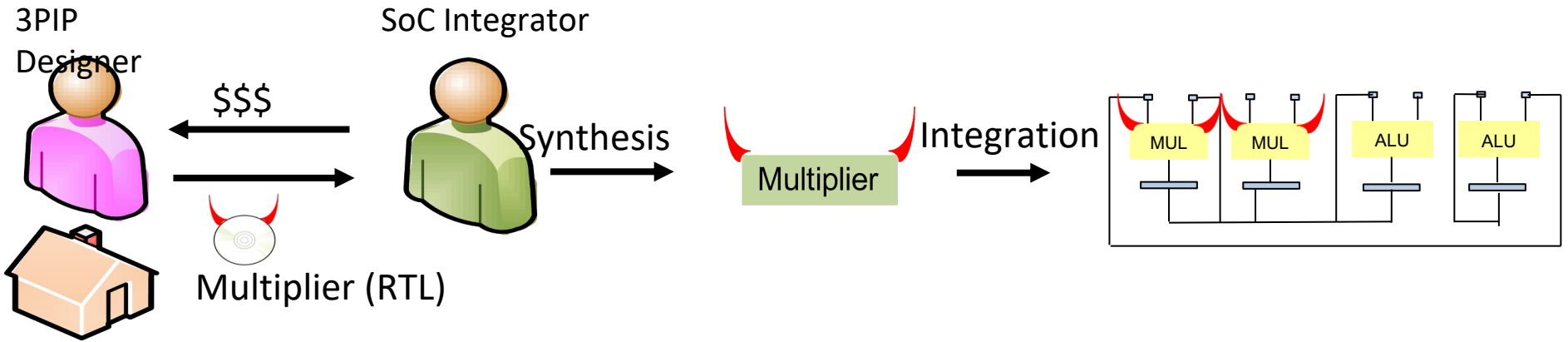
Detect “Natural” Faults

NYU Center for Cybersecurity



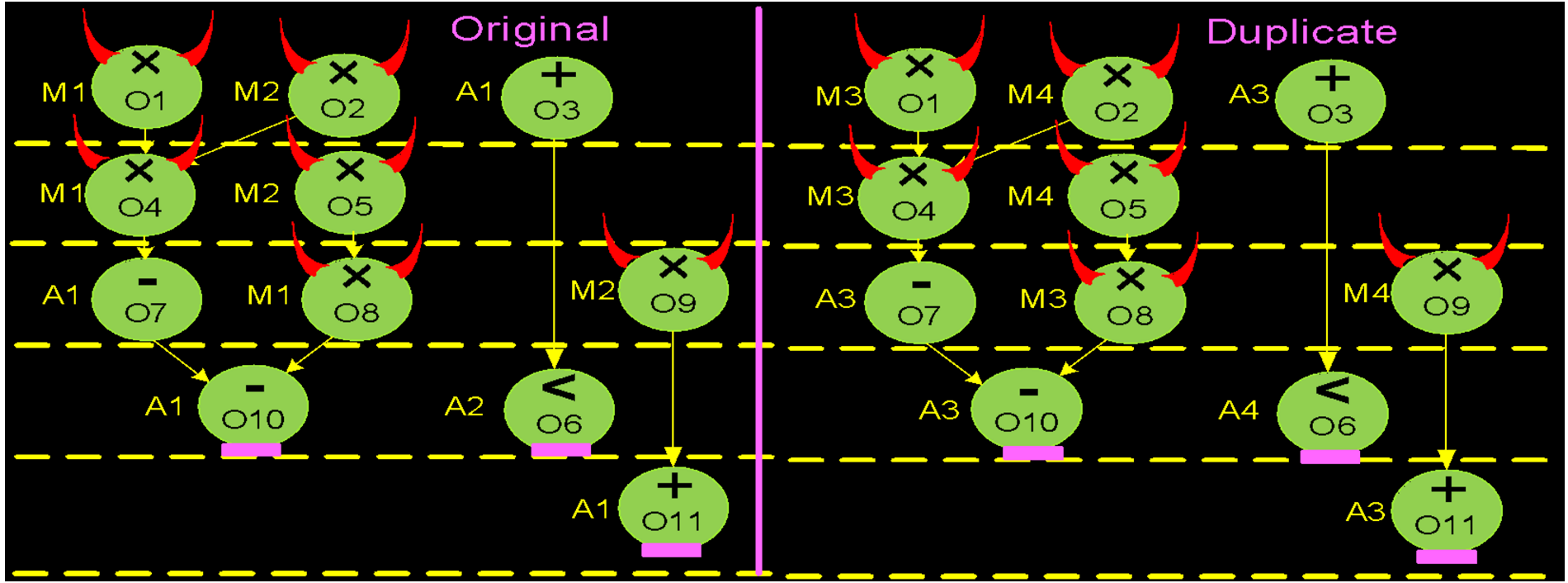
Malicious 3PIPs

NYU Center for Cybersecurity



J. Rajendran, O Sinanoglu, and R Karri, Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach, IEEE Trans VLSI, 24(9): 2946-2959, Sep 2016, DOI: 10.1109/TVLSI.2016.2530092

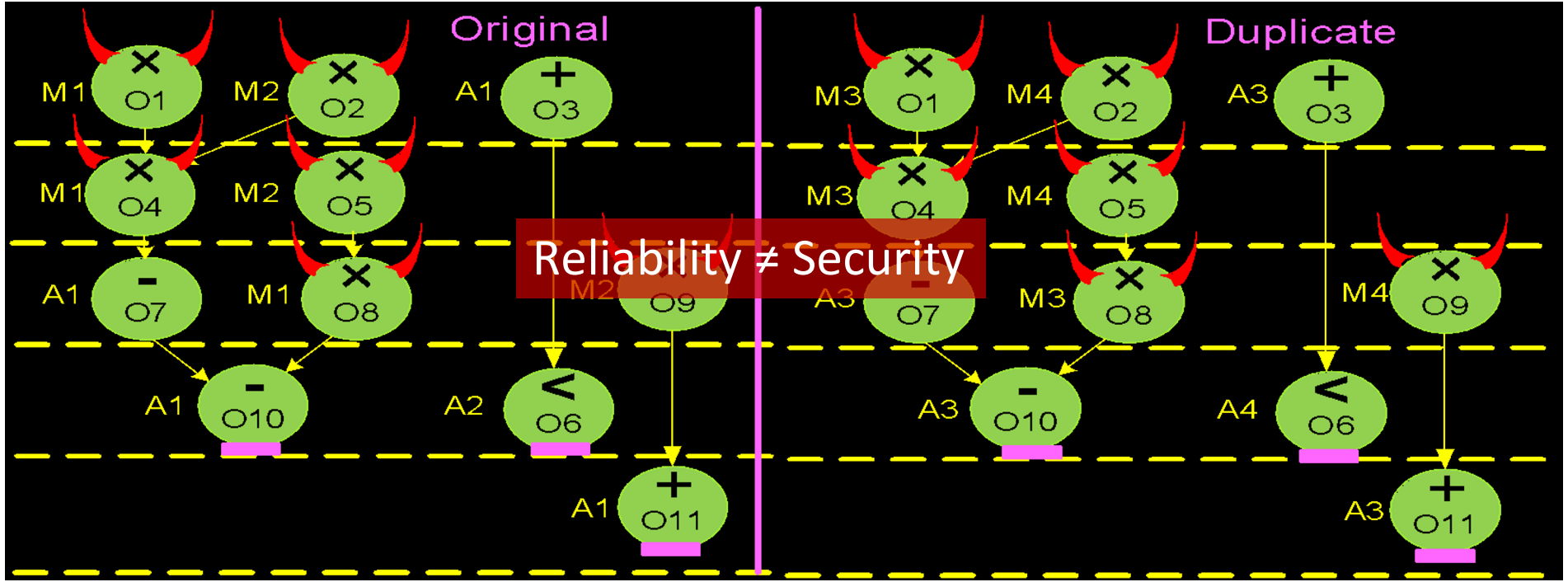
Detect Trojan: Duplicate+Check



- Components with Trojans produce same “malicious” outputs
- Checkers cannot detect malicious outputs
- Violates assumption for reliability

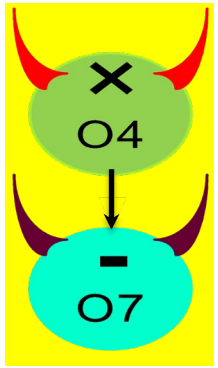
Detect Trojan: Duplicate+Check

NYU Center for Cybersecurity

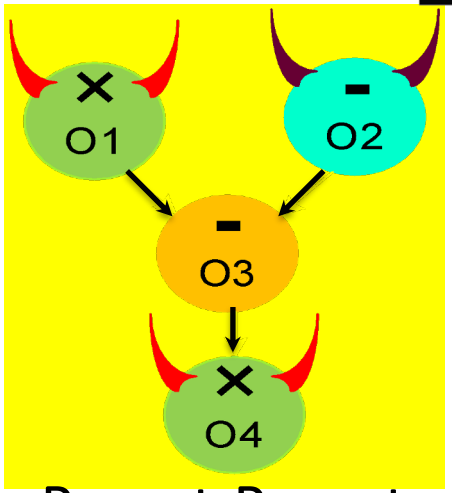


- Components with Trojans produce same “malicious” outputs
- Checkers cannot detect malicious outputs
- Violates assumption for reliability

Trojans May Collude



Parent-Child



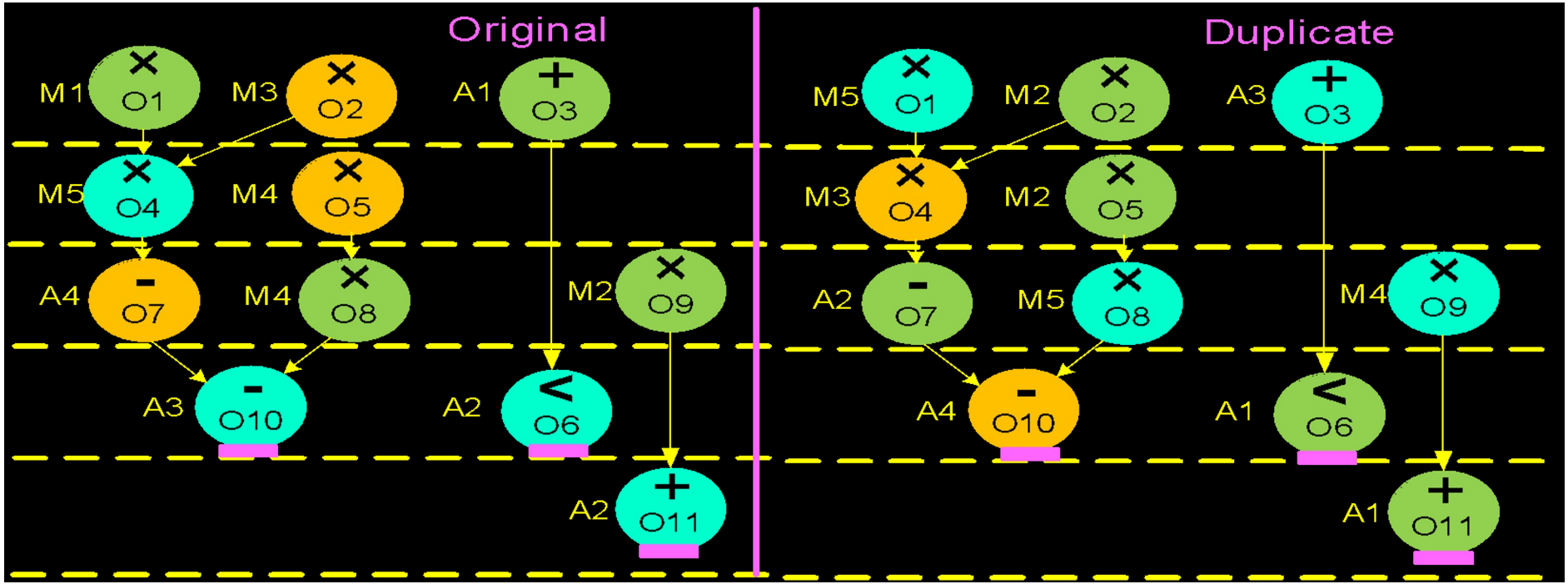
Parent-Parent

- Prevent collusions: Map operations to diverse components
- Parent-Child collusion: Map parent, child ops on diverse components
- Parent-Parent collusion: Map at least one parent on a component from a different vendor

J. Rajendran, O Sinanoglu, and R Karri, Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach, IEEE Trans VLSI, 24(9): 2946-2959, Sep 2016, DOI: 10.1109/TVLSI.2016.2530092

Detect Trojan: Duplicate+Diversify

NYU Center for Cybersecurity

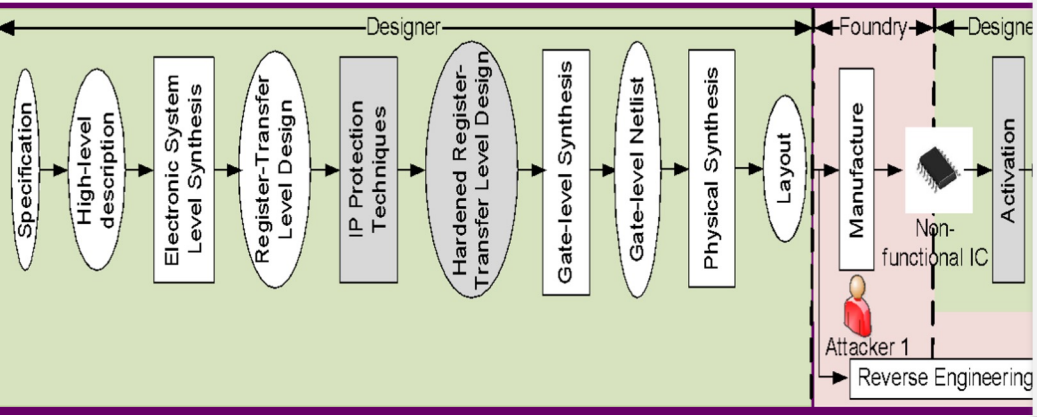


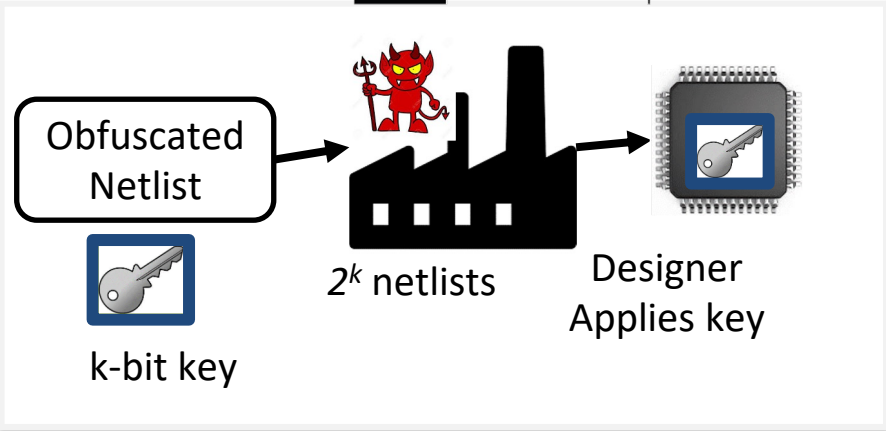
Duplicate + Diversify: 3 vendors; 3 multiplier 4 adder/compare/subtracts

Prevent Parent-Child Collusion and Parent-Parent Collusion

J. Rajendran, O Sinanoglu, and R Karri, Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach, IEEE Trans VLSI, 24(9): 2946-2959, Sep 2016, DOI: 10.1109/TVLSI.2016.2530092

Threat: IP Theft

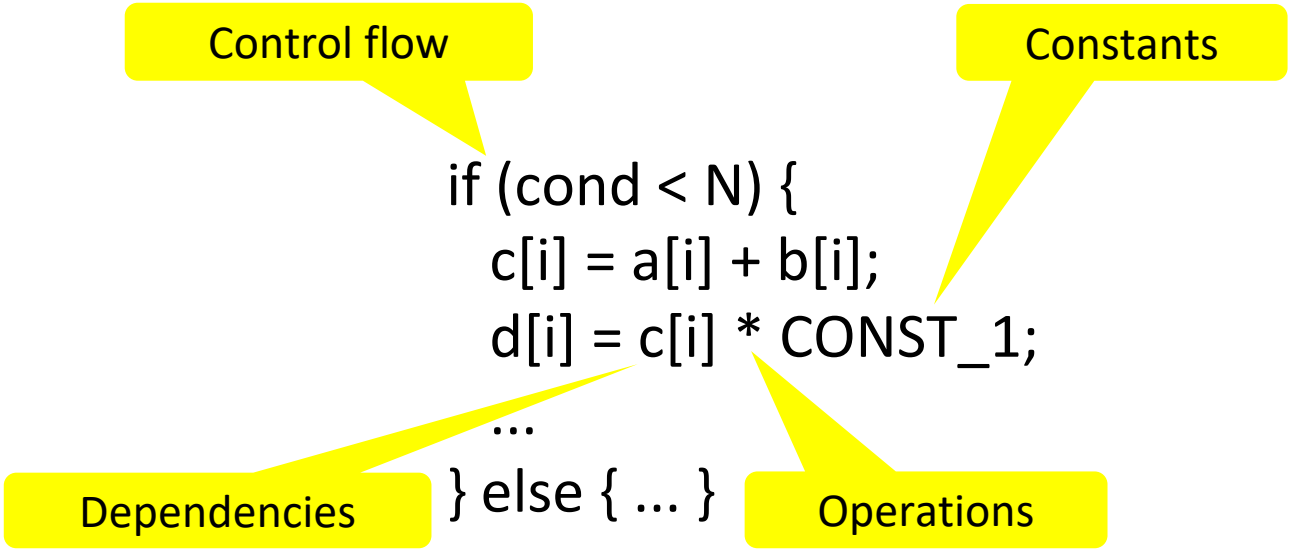




- Attacker capabilities
  - Is (in) the Foundry
  - Has the GDSII
  - Does not have access to a (activated/)functional IC
- Objective: Recover the design

C. Pilato, F. Reggazoni, S. Garg and R. Karri, "TAO: Techniques for Algorithm Level Obfuscation During High-Level Synthesis," Proc IEEE/ACM Design Automation Conf, June 2018.

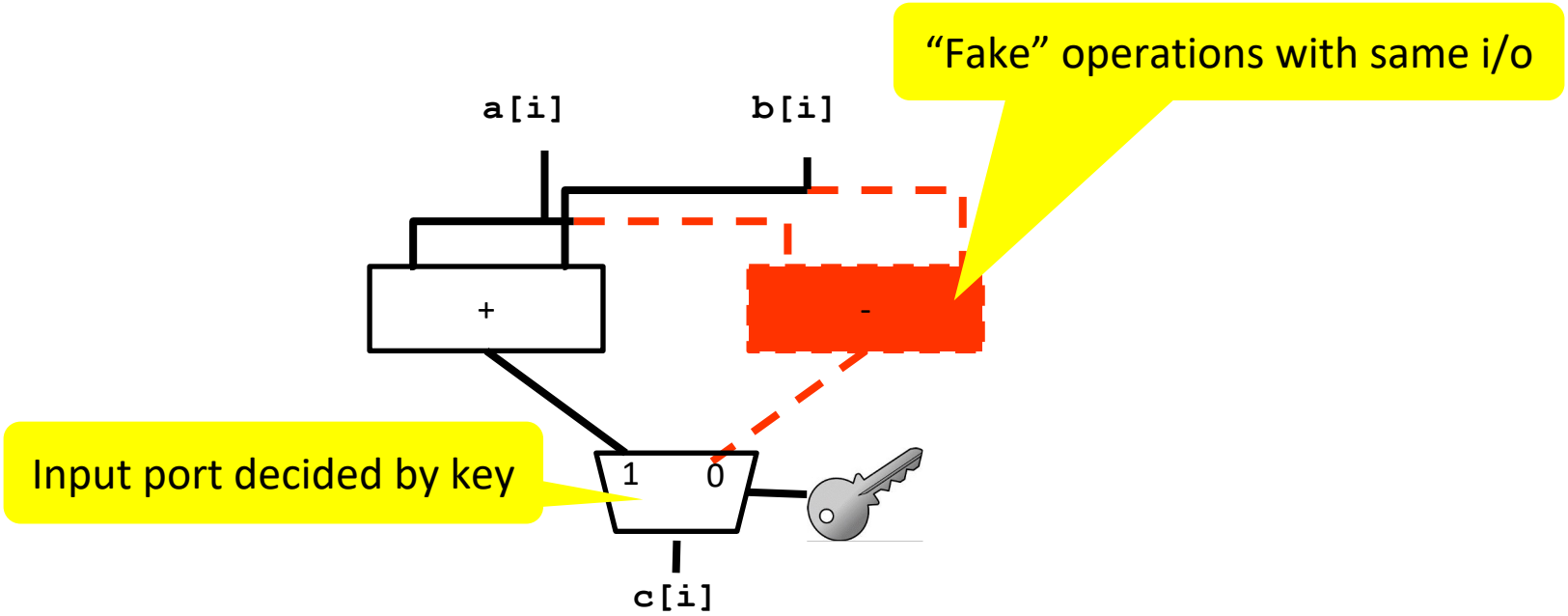
HLS Obfuscation



C. Pilato, F. Reggazoni, S. Garg and R. Karri, “TAO: Techniques for Algorithm Level Obfuscation During High-Level Synthesis,” Proc IEEE/ACM Design Automation Conf, June 2018.

Obfuscate Operations

- Gives intelligence on what the algorithm does
- Operator variants can camouflage correct operation
- Correct result is propagated only with the correct key

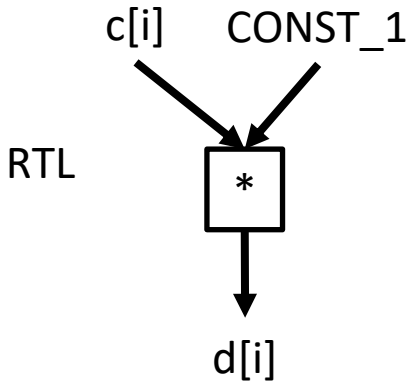


Obfuscate Constants

NYU Center for Cybersecurity

- Hard-coded values used by algorithm (coefficients, thresholds, …)
- Information is maintained at RTL
- Extensively optimized during logic synthesis

C/C++: d[i] = c[i] * CONST_1;



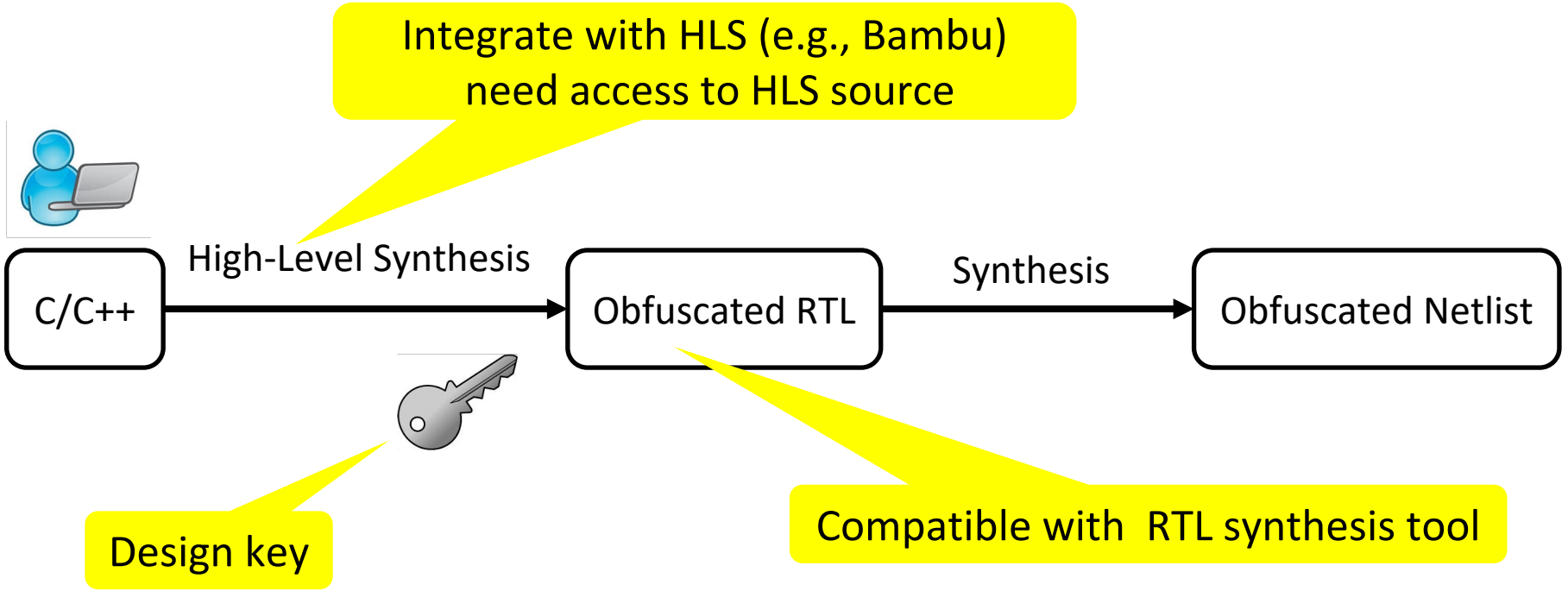
Obfuscated	Not obfuscated
Data co-efficients	Reset values
Signal extensions	Signal polarity
Mask values	

No impact on security

No impact on semantics

HLS Obfuscation Flow

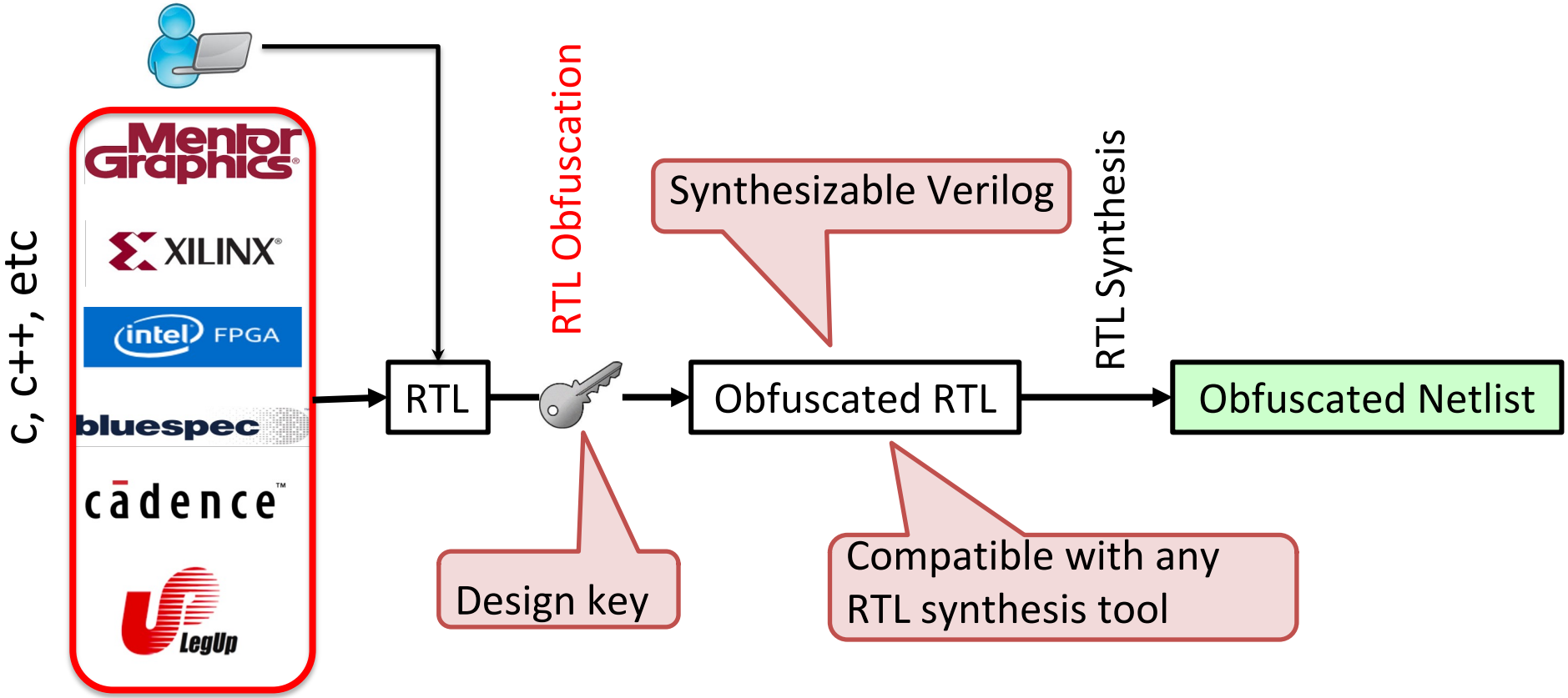
NYU Center for Cybersecurity



Semantic Obfuscation: Branches, Dependencies, Operations, Constants

RTL Transformations for Security

NYU Center for Cybersecurity



Conclusions

NYU Center for Cybersecurity

- High-Level is a promising level to Design Security Accelerators

  K. Basu, D. Soni, N. Mohammed, R. Karri, *NIST Post Quantum Cryptography: A Hardware Evaluation Study, Jan 2019*; iacr eprint
- High-Level is a promising level to Design-in Security

  C Pilato, S Garg, K Wu, R Karri, F Regazzoni, *Securing Hardware* Accelerators*: A New Challenge for High-Level Synthesis,* (a Perspective Paper), IEEE Embedded Systems Letters, *DOI*: 10.1109/LES.2017.2774800
- HLS can be used for Trojan Detection and Isolation

  J. Rajendran, O Sinanoglu, and R Karri, *Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach*, IEEE Trans VLSI, 24(9): 2946-2959, Sep 2016, DOI: 10.1109/TVLSI.2016.2530092

  J. Rajendran, H. Zhang, O. Sinanoglu *and* R. Karri, *High-level synthesis for security and trust,* IEEE Intl On-Line Testing Symposium, pp. 232-233. July 2013, doi: 10.1109/IOLTS.2013.6604087
- HLS can be used to Watermark Designs

  C. Pilato and K. Basu and M. Shayan and F. Regazzoni and R. Karri, *High-Level Synthesis of Benevolent Trojans*, Design Automation Test in Europe Conference, pp. 1118—1123, March, 2019.
- HLS can be used for Seamless and Meaningful Design Obfuscation

  C. Pilato, F. Reggazoni, S. Garg and R. Karri*, TAO: Techniques for Algorithm Level Obfuscation During High-Level Synthesis*, IEEE/ACM Design Automation Conference, June 2018, DOI: 10.1109/DAC.2018.8465830.
- HLS can be used for Seamless and Meaningful Taint Propagation

  C. Pilato, F. Reggazoni, S. *Garg* and R. Karri, *TaintHLS: High-Level Synthesis For Dynamic Information Flow Tracking*, IEEE Trans. CAD, DOI: 10.1109/TCAD.2018.2834421
- HLS-generated Designs can be Reverse Engineered !

  J. Rajendran, A. Ali, O. *Sinanoglu* and R. Karri, *Belling the CAD: Toward Security-Centric Electronic System Design,* IEEE Trans. CAD, Vol 34, No. 11, pp. 1756-1769, Nov 2015, DOI: 10.1109/TCAD.2015.2428707.
- A Black-Hat can use High-Level Synthesis to undermine Designs (weaken crypto, drain battery, etc)

Intersection of Design, Security and Large Language Models (LLMs)

NYU Center for Cybersecurity

Ramesh Karri, Siddharth Garg, Shailaja Thakoor, Jason Blocklove, Baleegh Ahmad, Jitendra Bhandari, Animesh Chowdhury

Hammond Pearce, UNSW, Sydney, Australia

Ben Tan, U. Calgary, Canada

Rahul Kande and J. Rajendran, Texas A&M University

2021-2023: LLM-written code !

NYU Center for Cybersecurity

iblnews.org

Home › Top News › StarCoder, a New Free Co

StarCoder, a New Free Code-Generating Model Alternative to GitHub's Copilot

By **IBL News** - May 8, 2023

reddit PROGRAMMING comments other discussions (18)

2660

GitHub Copilot · Your AI pair programmer (copilot.github.com)

submitted 2 months ago by violinclipper 4 & 14 more

581 comments share save hide give award report crosspost

The Verge

GitHub and OpenAI launch an AI Copilot tool that generates its own code

GitHub and OpenAI have launched a technical preview of a new AI tool called Copilot, which lives inside the Visual Studio Code editor

Hacker News new | threads | past | comments | ask | show | jobs | submit

GitHub Copilot (copilot.github.com)

2905 points by todsacerdoti 75 days ago | hide | past | favorite | 1272 comments

TechTalks HOME BLOG TIPS & TRICKS WHAT IS INT

Home › Blog › What OpenAI and GitHub's "AI pair programmer" means for the softwa

Blog

What OpenAI and GitHub's "AI pair programmer" means for the software industry

By **Ben Dickson** - July 5, 2021

Introducing GitHub Copilot: your AI pair programmer

Nat Friedman

INTERESTING ENGINEERING JOBS Subscribe | Log In

Open AI's Codex tool claims to help developers write code faster, better

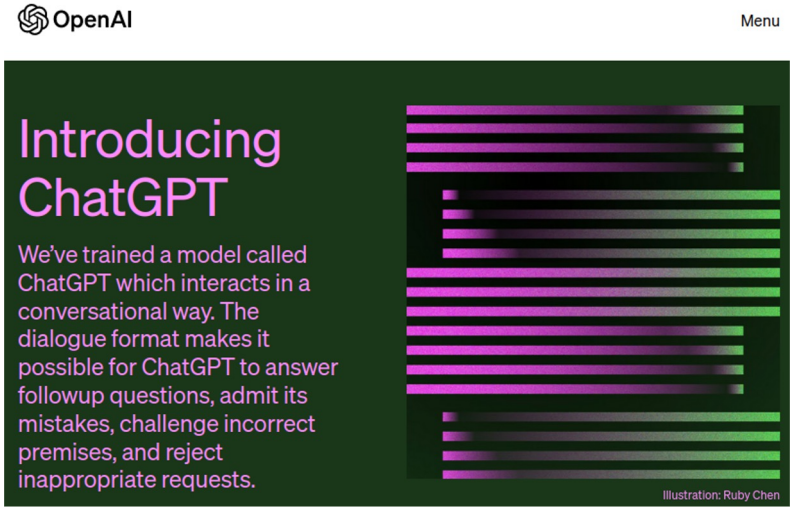
It can't fix the code when it does not work though.

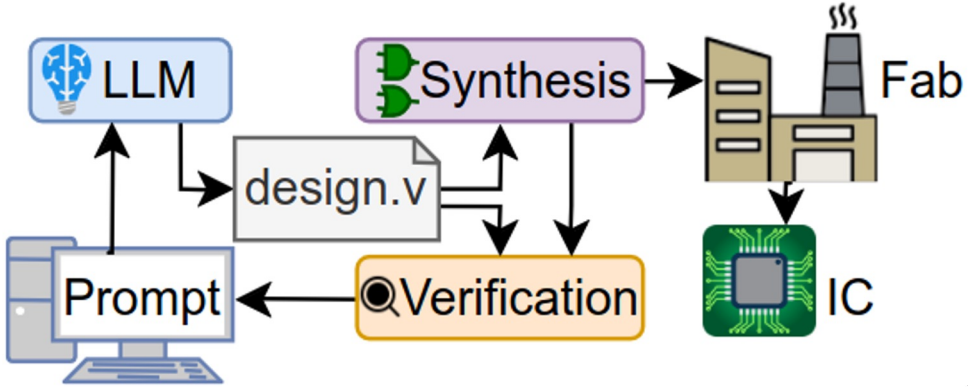
Ameya Paleja

Created: Mar 07, 2023 08:02 AM EST

Conversational LLMs In H/W Design

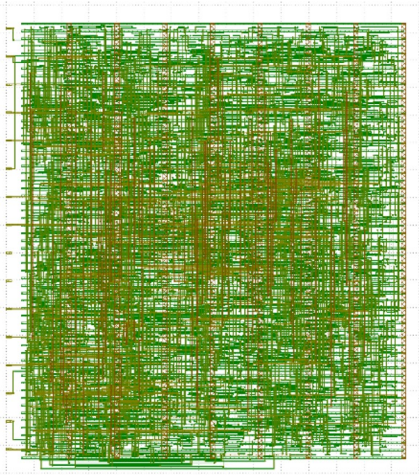
NYU Center for Cybersecurity






```
Let us make a brand new microprocessor design together. We're severely constrained on space and I/O. We have to fit in 1000 standard cells of an ASIC, so I think we will need to restrict ourselves to an accumulator based 8-bit architecture with no multi-byte instructions. Given this, how do you think we should begin?
```

Fig. 10. 8-bit accumulator-based processor: Starting co-design prompt



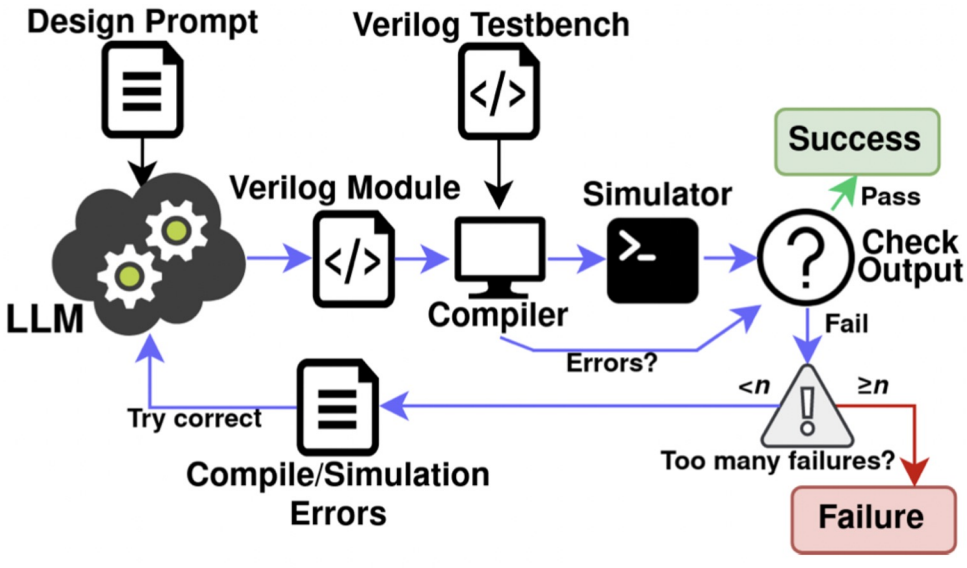
Component	Count
Comb. Logic	999
Diode	4
Flip Flops	168
Buffer	126
Tap	300

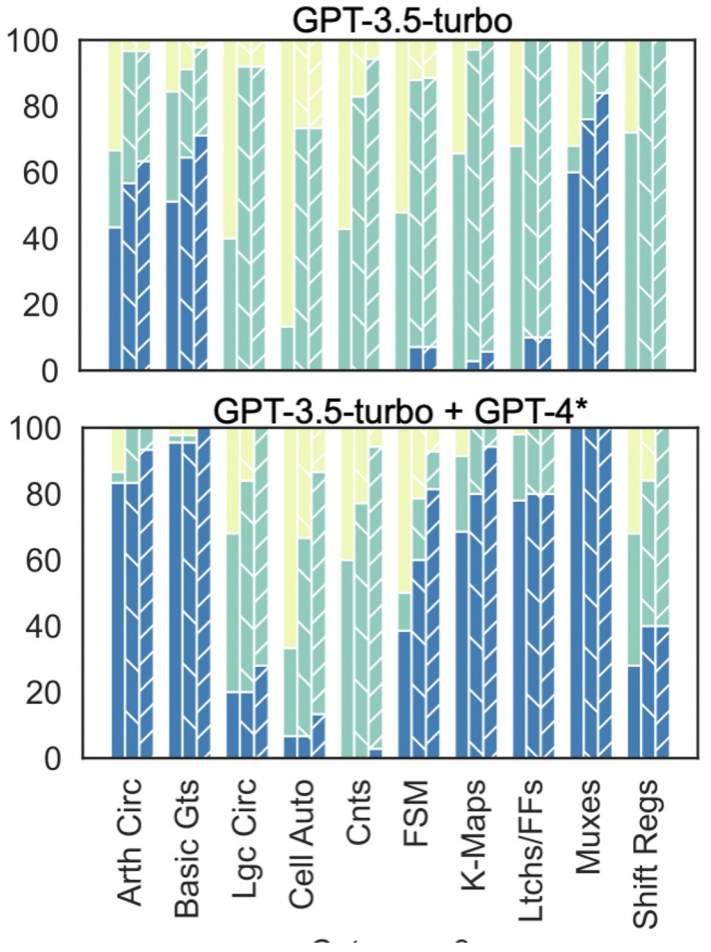
Above: (a) Components.

Left: (b) Final processor GDS render by 'klayout', I/O ports on left side, grid lines = 0.001 um.

HDL Generation: LLM+Feedback

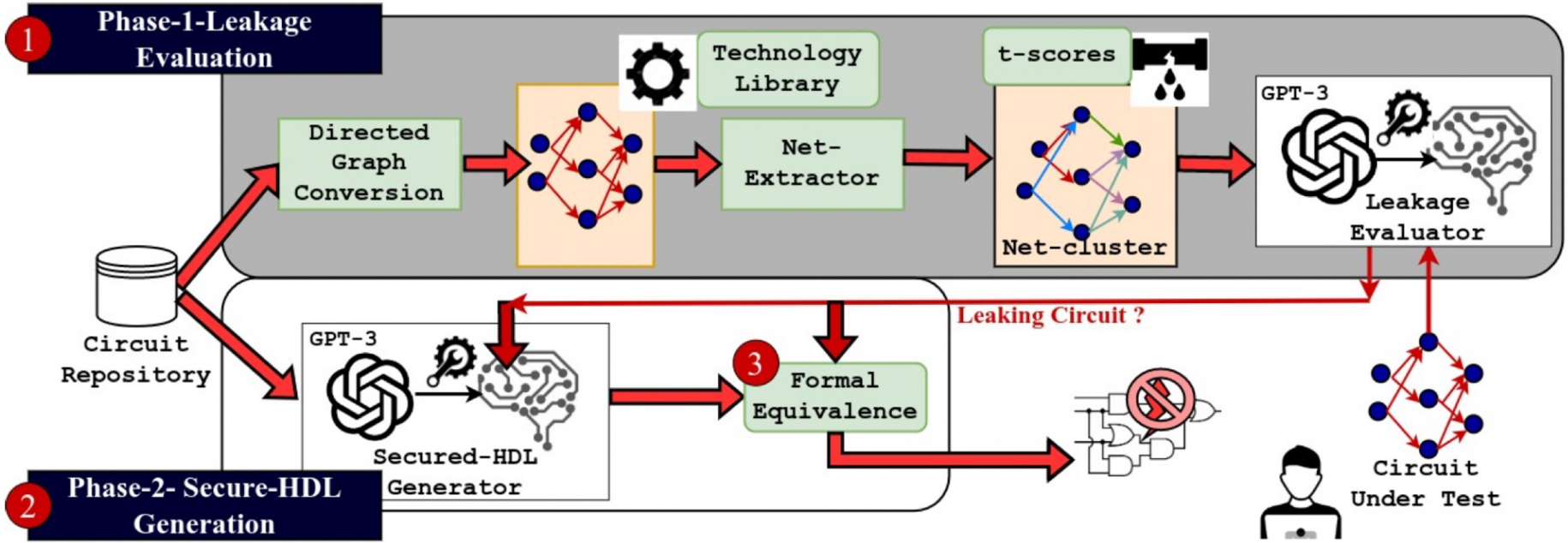
NYU Center for Cybersecurity





(w/o) Feedback (n=0) — Success — Simulation Error — Compile Error
(w) Feedback (n=5) — Success — Simulation Error — Compile Error
(w) Feedback (n=10) — Success — Simulation Error — Compile Error

Secure HDL Generation: Masking



Further Directions

NYU Center for Cybersecurity

- The first Verilog LLM, DAVE **(MLCAD '20)**: https://arxiv.org/abs/2009.01026
- Evaluating LLMs in Security **(S&P'22, Best Paper)**: https://arxiv.org/abs/2108.09293
- Training Verilog LLMs **(DATE '23, Best Paper Finalist)**: https://arxiv.org/abs/2212.11140
- Conversational LLMs for HW Design (**MLCAD'23**): https://arxiv.org/abs/2305.13243
- Bug repair with LLMs **(S&P'23)**: https://arxiv.org/abs/2112.02125
- AutoChip: Automating HDL Generation Using LLM Feedback: https://arxiv.org/pdf/2311.04887.pdf
- Hardware bug repair with LLMs: https://arxiv.org/abs/2302.01215
- Hardware assertions with LLMs: https://arxiv.org/abs/2306.14027
- Security bug finding with LLMs: https://arxiv.org/abs/2306.12643
- Secure Chip Design with LLMs: https://dl.acm.org/doi/abs/10.1145/3605769.3623989

https://github.com/JBlocklove/LLMs-for-EDA-Tutorial

NYU Center for Cybersecurity

?

Cell: 917 363 9703
rkarri@nyu.edu
http://cyber.nyu.edu