Enhancing Cybersecurity with Trusted Hardware

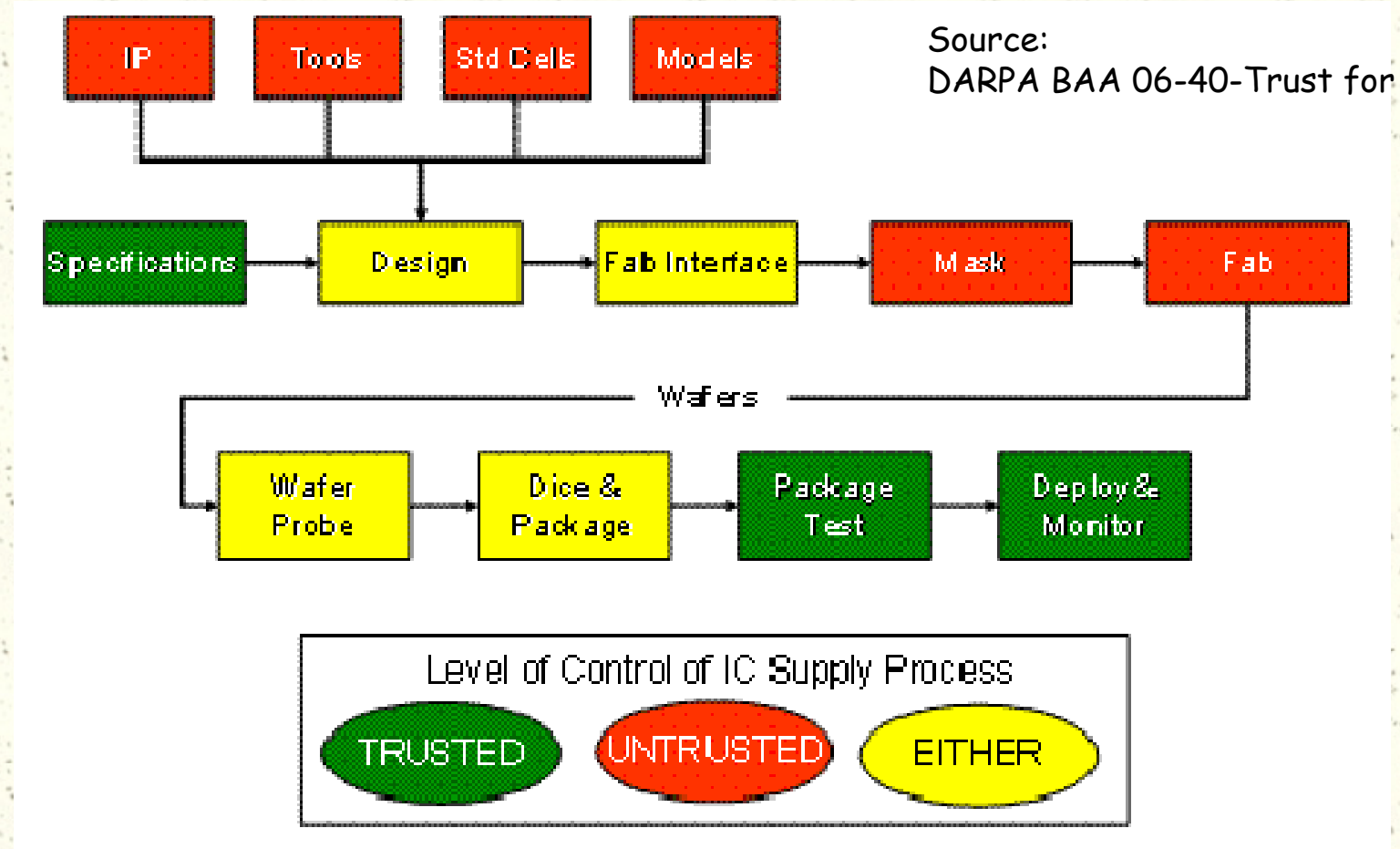
Electrical and Computer Engineering Dept.
Institute for Systems Research and MC^2
Gang Qu
gangqu@umd.edu

You can't and should not trust the hardware you are given

- Side Channel Attacks
- Hardware Trojans
  - Killer switch
  - Time bomb
- Untrusted Microchip Supply Chain
  - Hardware counterfeiting
  - Hardware design intellectual property

Trust in Microchip Supply Chain

- Trust becomes an issue with offshore foundry & design complexity



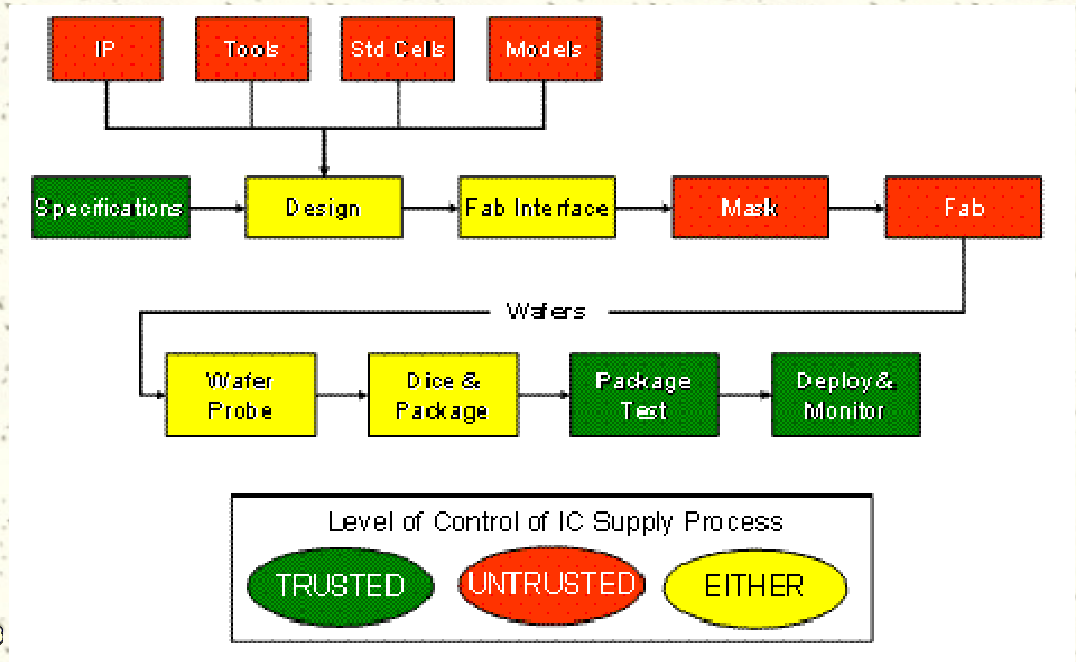
Source:
DARPA BAA 06-40-Trust for IC

Trust in Microchip Supply Chain

- Trust becomes an issue with offshore foundry & design complexity

=> How to ensure the final chip does exactly what we ask?

- "No Less": are all the design specification met?
- "No more": does the chip do anything extra beyond what is asked?



Source:
DARPA BAA 06-40- Trust for IC

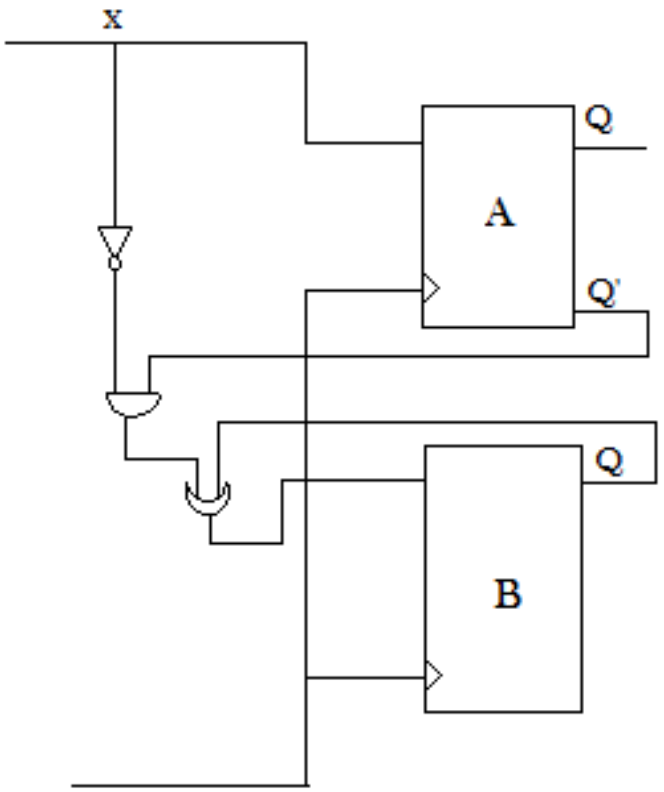
What Does Trust Mean?

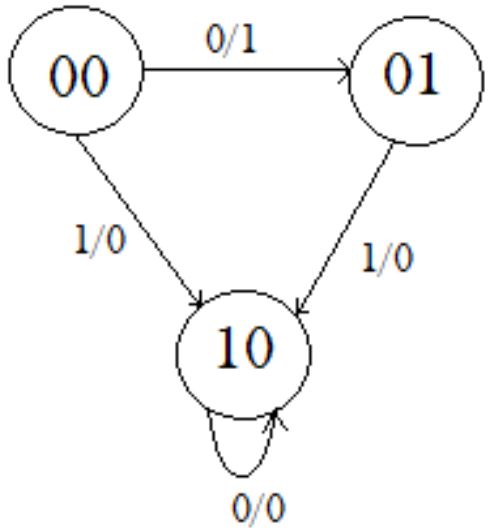
- Find a 3rd degree polynomial f(x) s.t.
  - f(1) = 0
  - f(2) = 0
- Answers:

1. $f(x) = x^2-3x+2 = (x-1)(x-2)$
2. $f(x) = x^3-2x^2-x+2 = (x-1)(x-2)(x+1)$
3. $f(x) = x^3-4x^2+5x-2 = (x-1)^2(x-2)$
4. $f(x) = x^3-5x^2+8x-4 = (x-1)(x-2)^2$

- Which one(s) can be trusted?

Trust in System/Chip Design

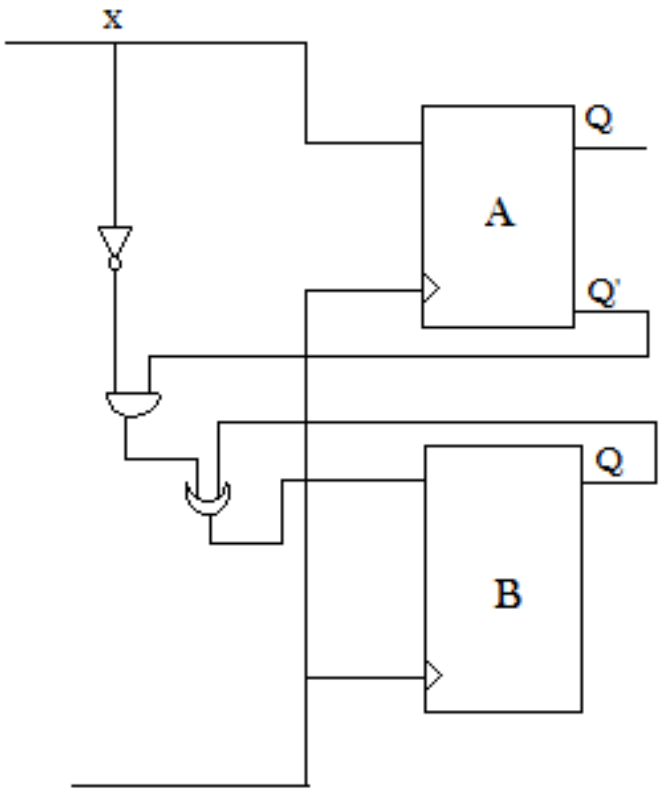


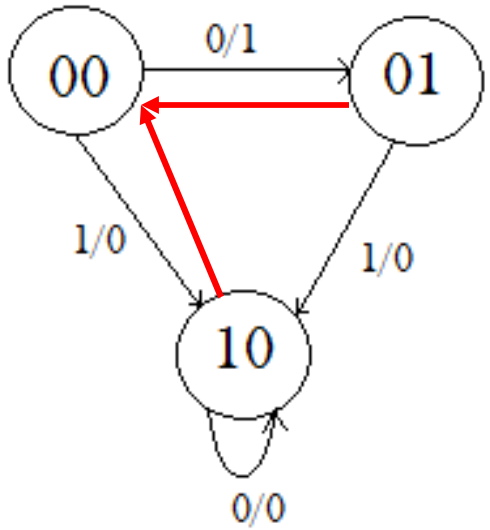


A	B	x	A'	B'
0	0	0	0	1
0	0	1	1	0
0	1	0	-	-
0	1	1	1	0
1	0	0	1	0
1	0	1	-	-

What if A=0, B=1, x=0?

Trust in System/Chip Design

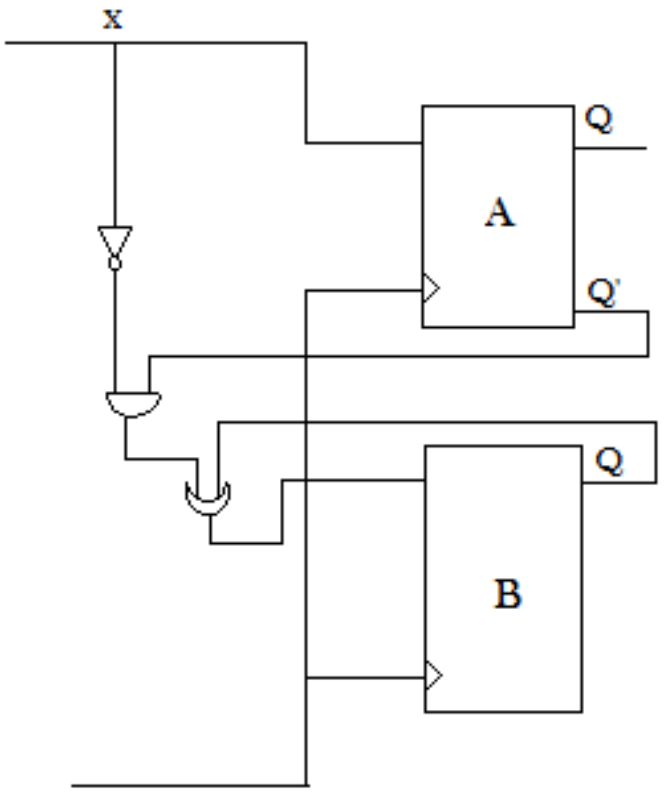


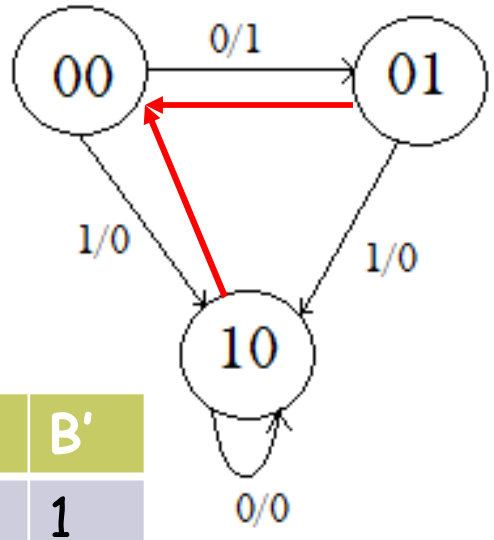


A	B	x	A'	B'
0	0	0	0	1
0	0	1	1	0
0	1	0	0	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	0

What if A=0, B=1, x=0?

Trust in System/Chip Design

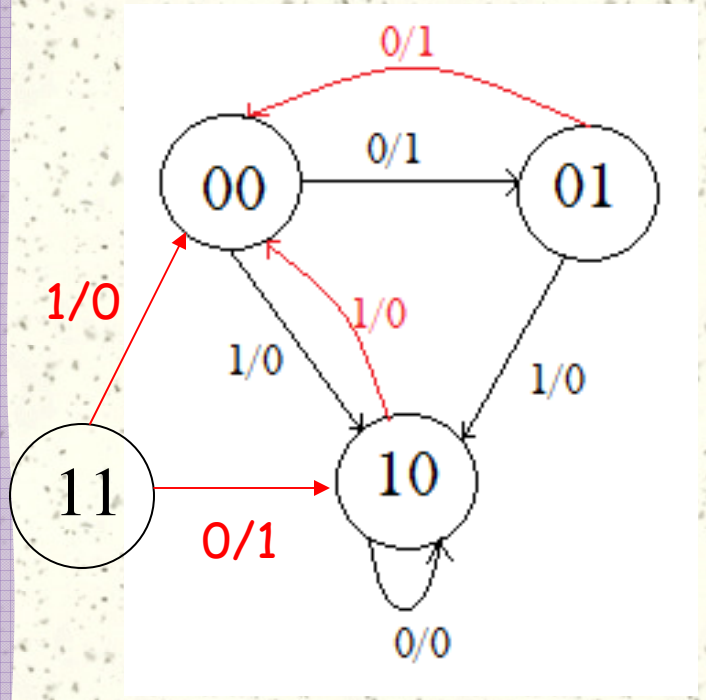


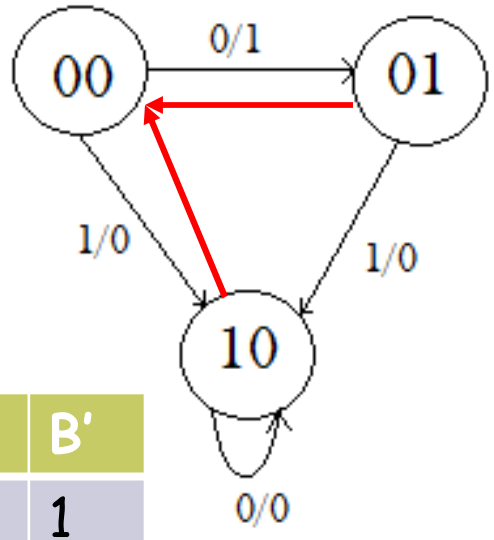


A	B	x	A'	B'
0	0	0	0	1
0	0	1	1	0
0	1	0	0	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	0
1	1	0	1	0
1	1	1	0	0

It is even worst than this

Trust in System/Chip Design





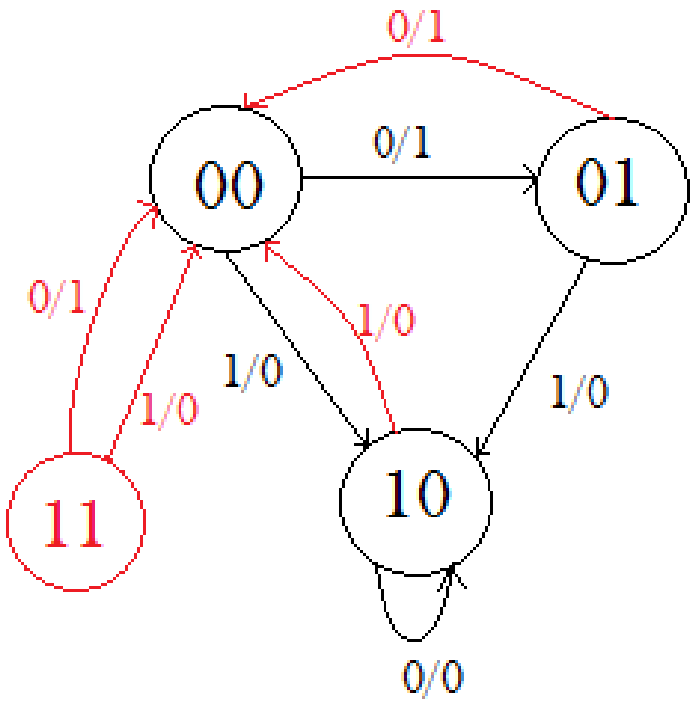
A	B	x	A'	B'
0	0	0	0	1
0	0	1	1	0
0	1	0	0	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	0
1	1	0	1	0
1	1	1	0	0

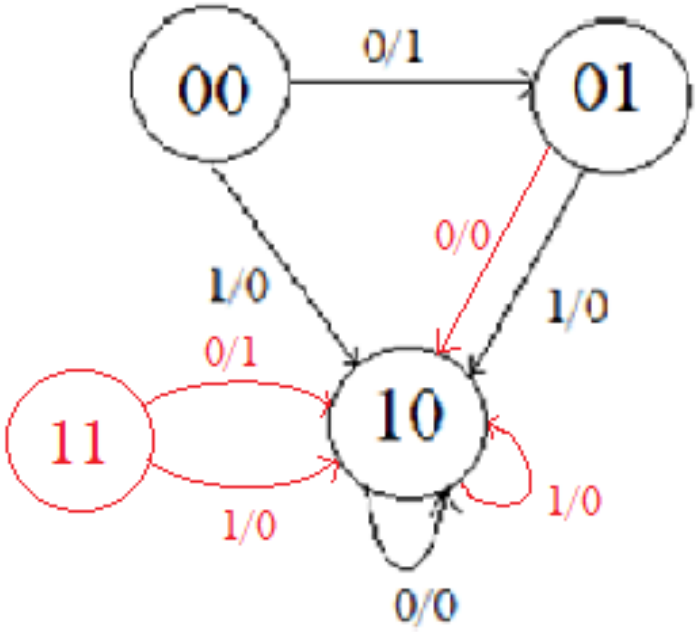
It is even worst than this

1. Trust in System/Chip Design

- Worst or best scenario
- How to ensure trust?
- Worst or best scenario

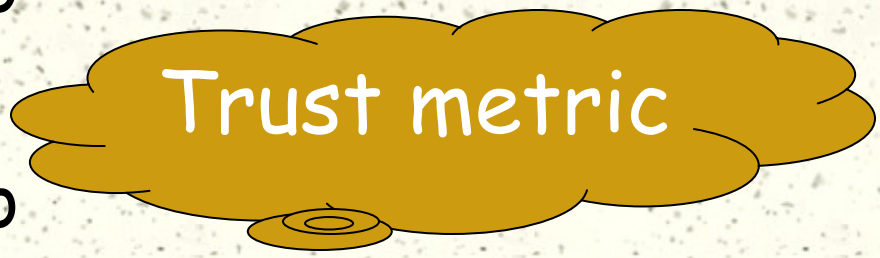
Trust metric





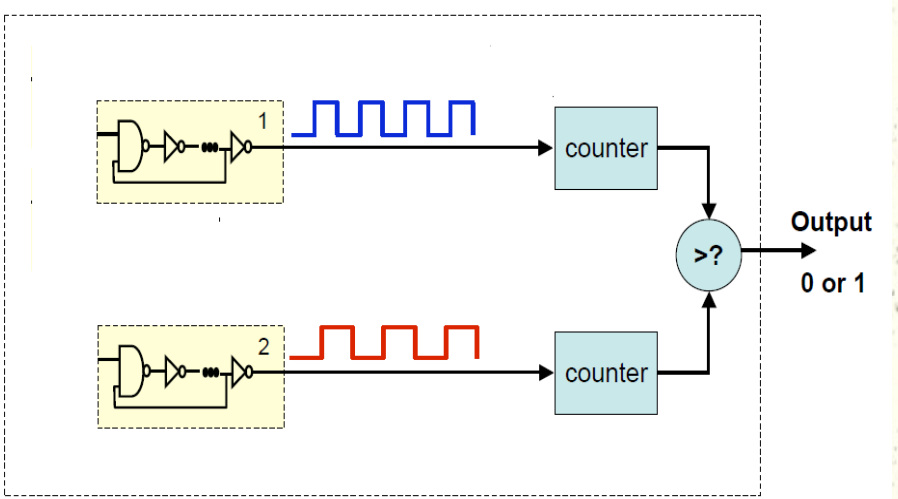
1. Trust in System/Chip Design

- Worst or best scenario
- How to ensure trust?
- Worst or best scenario
- Publications:
  - J. Gu, G. Qu, and Q. Zhou. "Information Hiding for Trusted System Design", (DAC 2009).
  - L. Yuan, P. Pari, and G. Qu. "Finding Redundant Constraints for FSM Minimization", (AAAI 2004).
  - L. Yuan and G. Qu. "Information Hiding in Finite State Machine", (IHW 2004).



2. Physically Unclonable Function

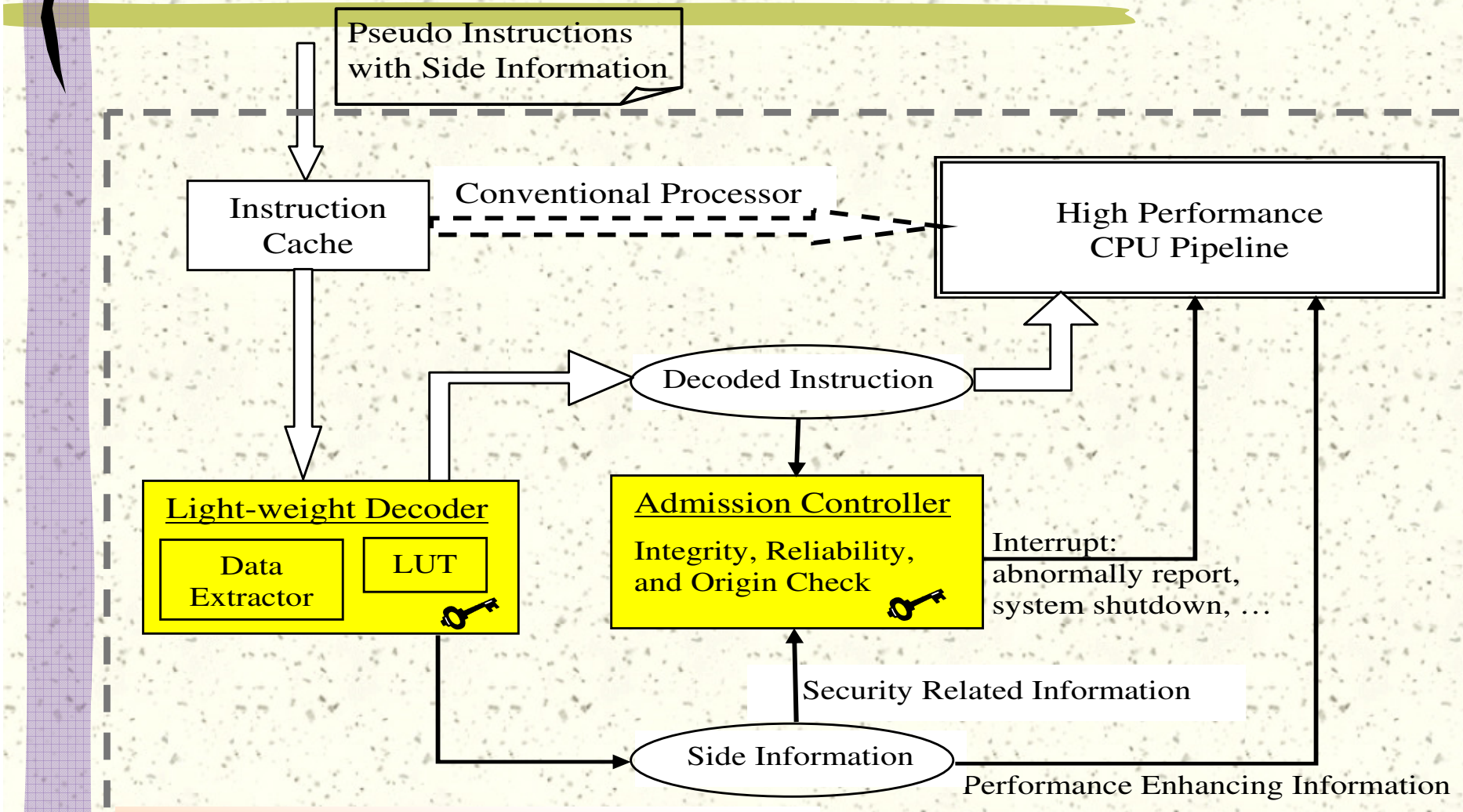
- What is PUF?
- PUF in security:
  - Store/generate key
  - Device identificatior
- Silicon PUF: process variation
  - Delay based: Arbiter PUF, Ring Oscillator PUF
  - Memory based: SRAM PUF, Butterfly PUF
- Example: RO PUF
  - 1 if top path is faster, 0 otherwise



2. Physically Unclonable Function

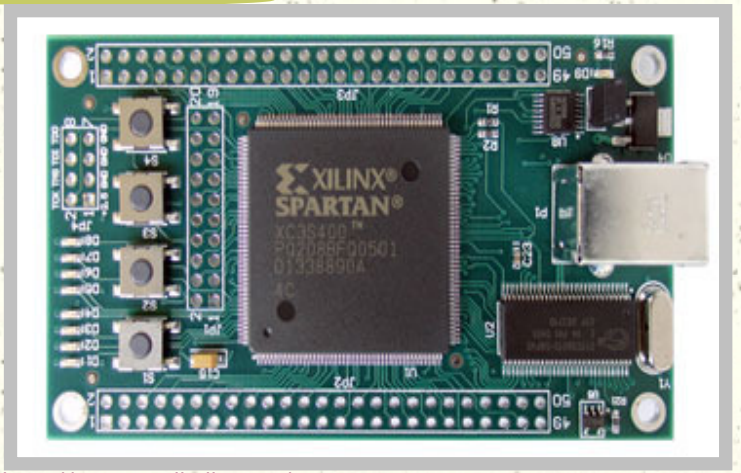
- Challenges
  - Hardware efficiency
  - Reliability under all operating environment
  - Security against potential attacks
- Publications
  - C. Yin and G. Qu. "Temperature-Aware Cooperative Ring Oscillator PUF," (HOST 2009).
  - C. Yin and G. Qu. "LISA: Maximizing RO PUF's Secret Extraction," (HOST 2010).
  - C. Yin and G. Qu. "A Regression-Based Entropy Distiller for RO PUFs," (DAC 2012).
  - C. Yin and G. Qu. "Kendall Syndrome Coding (KSC) for Group-Based RO PUFs," (DAC 2012).

3. Trusted Executing Environment



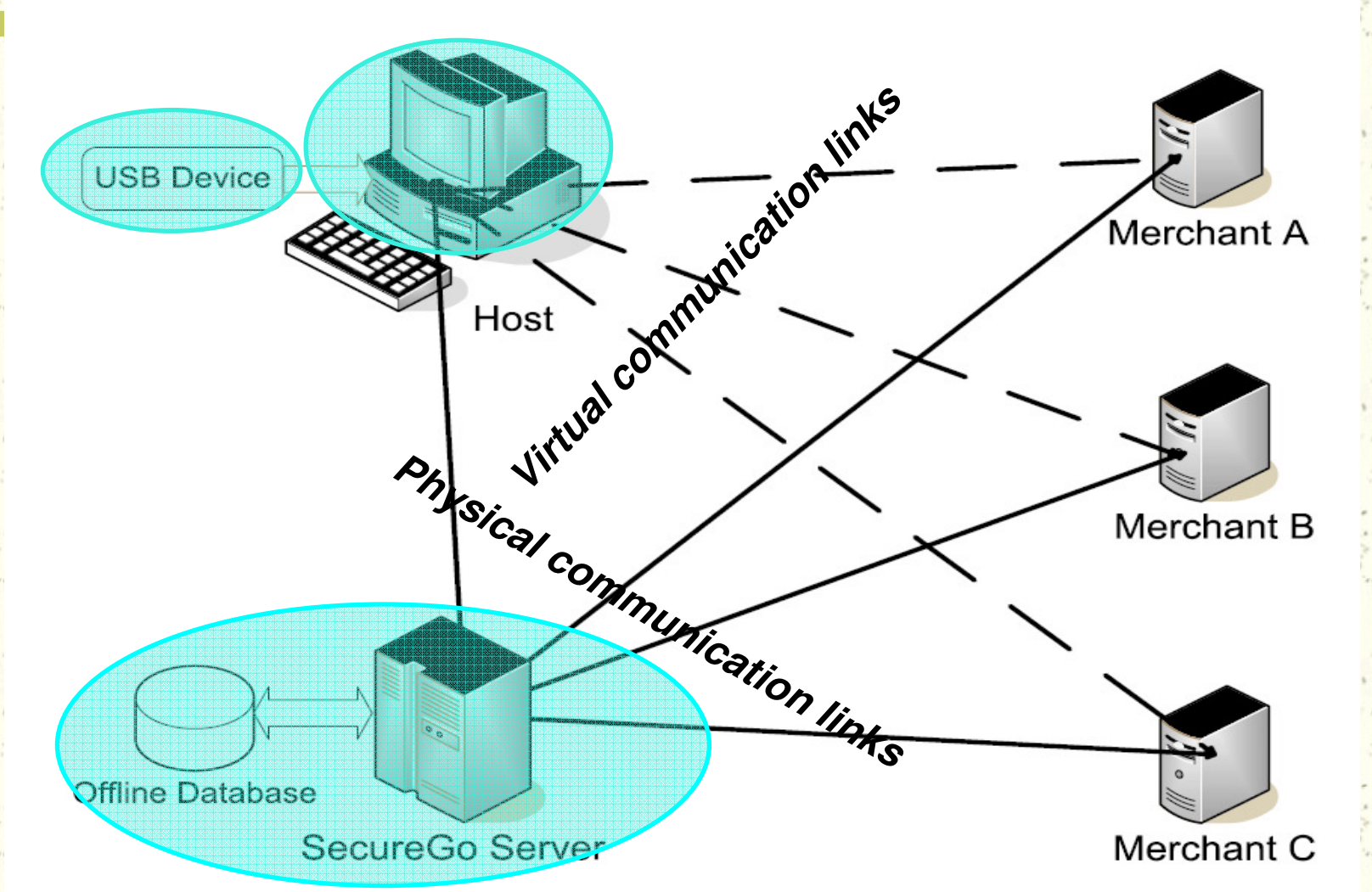
3. Trusted Executing Environment

- FPGA Prototyping
  - Area (0.2%)
  - Power (0.07%)
- Applications:
  - Mobile code, mobile devices
  - Trust
  - Sensor and sensor networks.
- Publications:
  - M. Taylor, C. Yin, M. Wu, and G. Qu. "A Hardware-Assisted Data Hiding Based Approach in Building High Performance Secure Execution Systems," (HOST 2008).
  - A. Swaminathan, Y. Mao, M. Wu, and Krishnan Kailas: "Data Hiding in Compiled Program Binaries for Enhancing Computer System Performance," (IHW 2005).



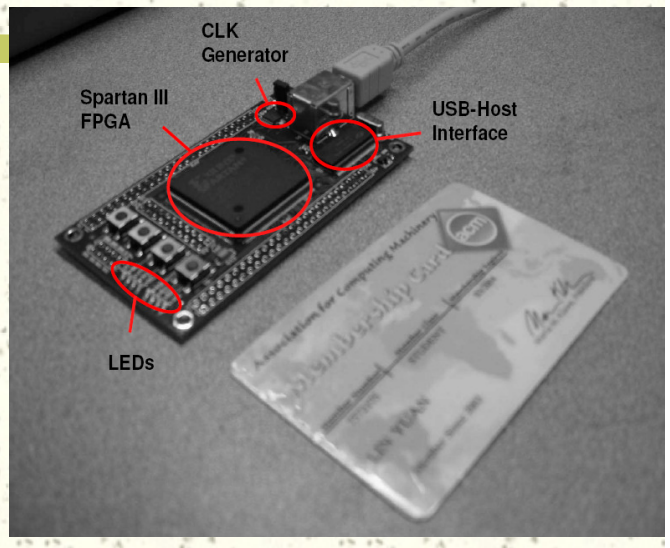
http://www.opalkelly.com/

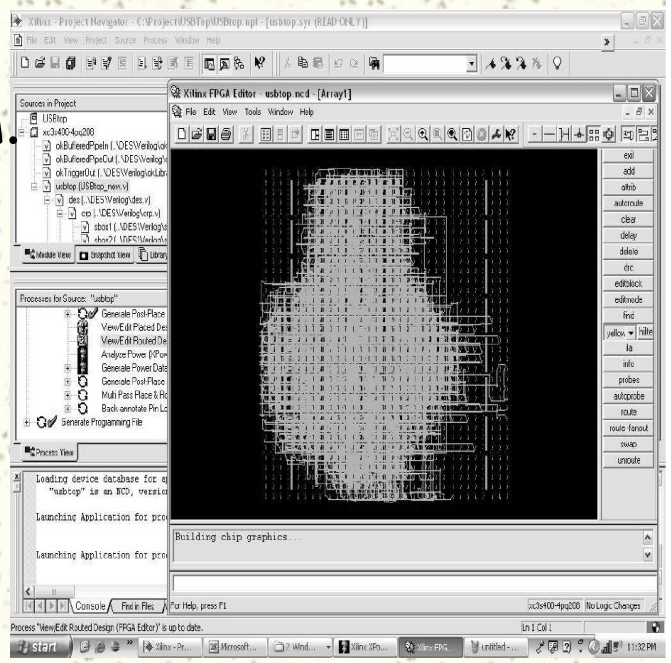
4. The SecureGo System



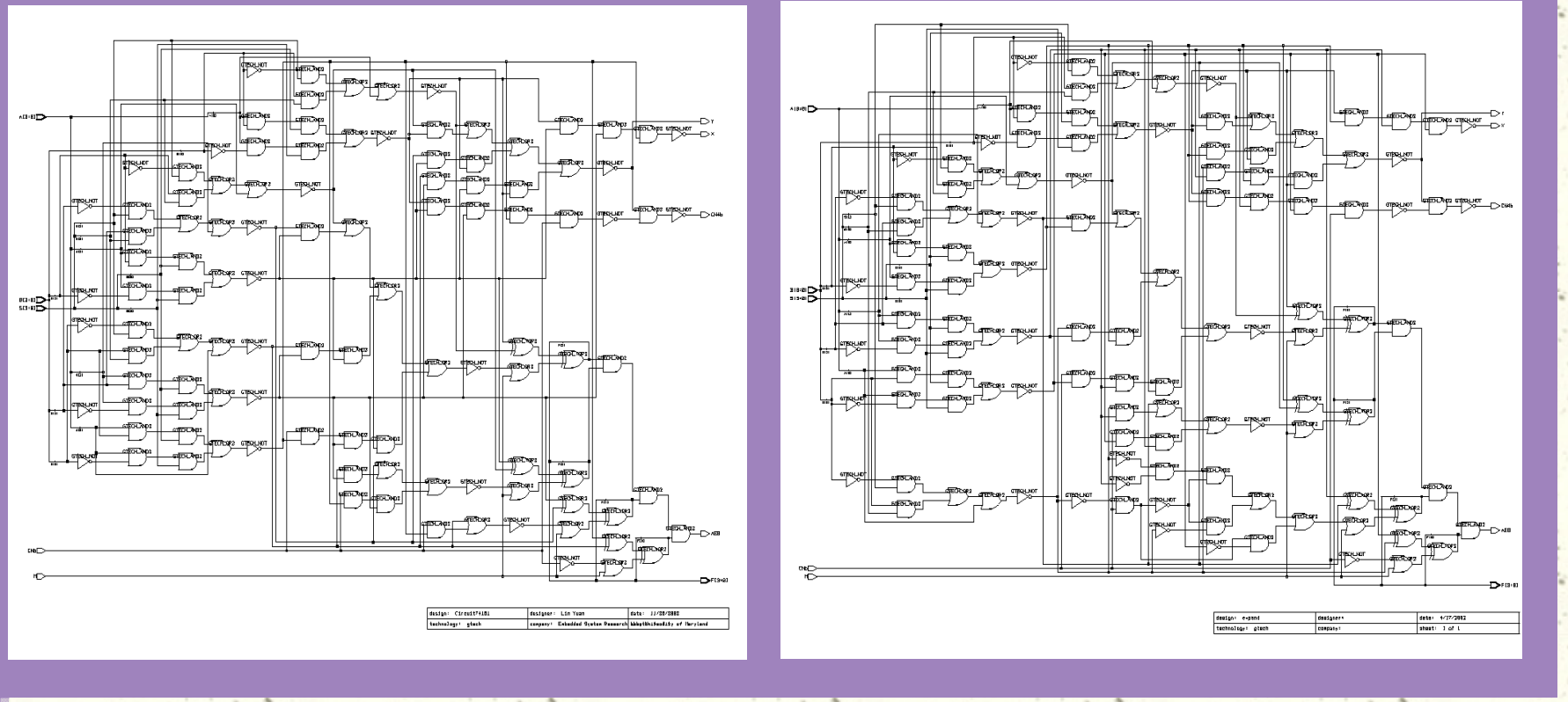
4. The SecureGo System

- Speed:
  - RSA: 50K cycles @ 100MHz
  - T-DES: 4.8K cycles @ 38MHz
  - USB connection: 12Mbps
  - 1 transaction: less than 1 ms
- Hardware resource:
  - Size: <170K gates, or 4mmx4mm.
  - Power: < 0.5mW per transaction
- Security:
  - Credit card fraud
  - identity theft
  - E-commerce



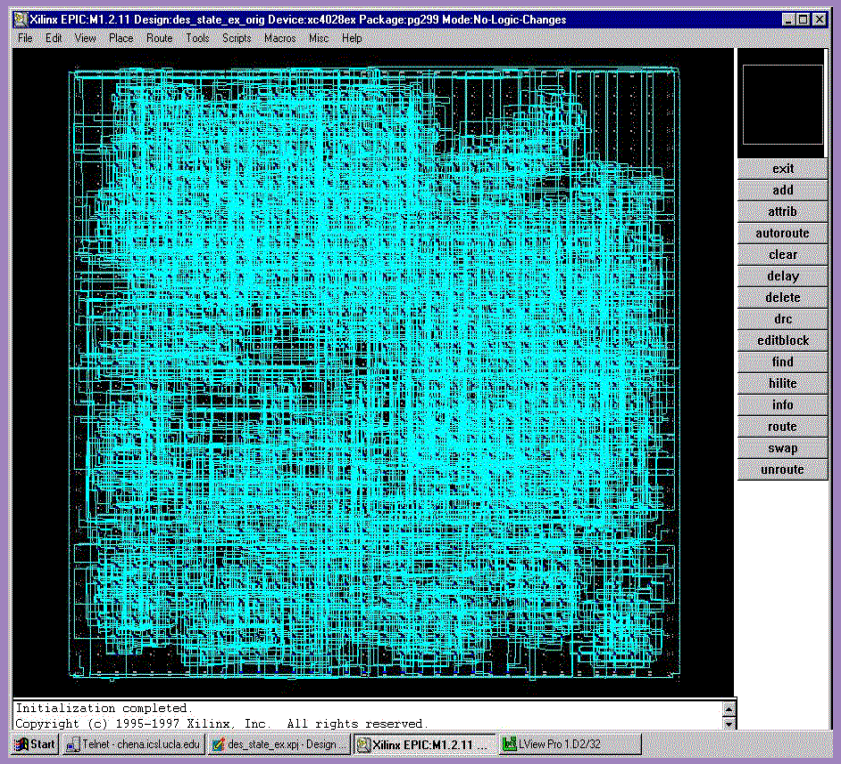


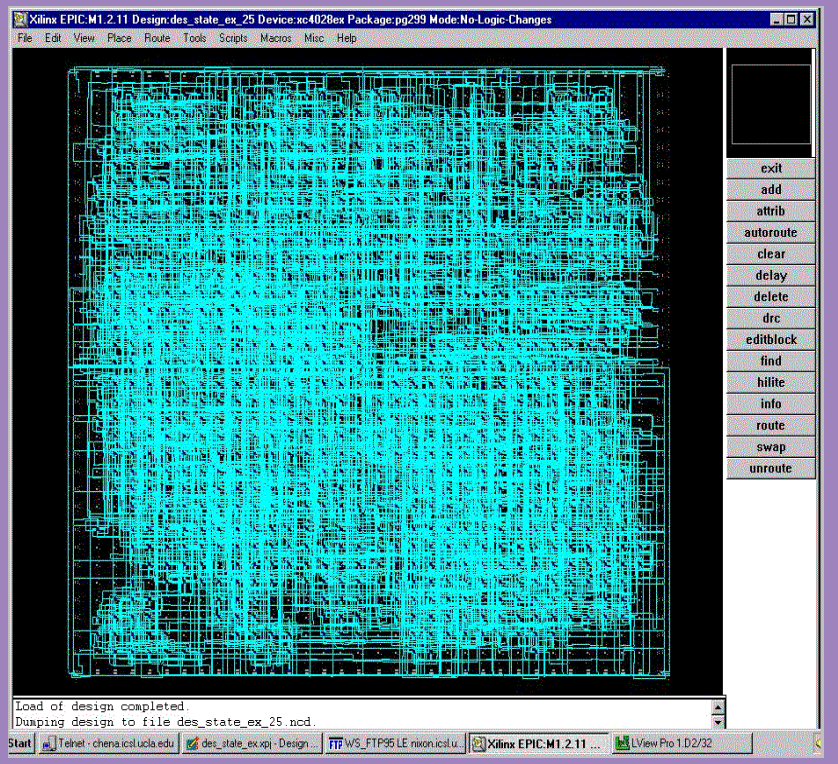
5. Counterfeiting & IP Protection



A 4-bit ALU: Original gate-lever circuit and the same design with message "UMCP TERPS" embedded.

5. Counterfeiting & IP Protection





DES: Same functionality, area, and performance with a 4768-bit watermark embedded in the FPGA design

Hardware in Security and Trust

- Enabler.
- Enhancer.
- Enforcer.
- Our research activities:
  - Trusted system/IC (integrated circuit) design
  - High performance trusted computing platform
  - PUF based security and trust
  - Intellectual property protection (counterfeiting)
  - Energy efficiency
  - Embedded systems, sensors, defense applications.