Enhancing Cybersecurity with Trusted Hardware

Electrical and Computer Engineering Dept.
Institute for Systems Research and MC²
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

Level of Control of IC Supply Process

- Trusted
- Untrusted
- Either

Source: DARPA BAA 06-40-Trust for IC
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

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

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$x$</th>
<th>$A'$</th>
<th>$B'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
What if $A=0$, $B=1$, $x=0$?
Trust in System/Chip Design

It is even worst than this
Trust in System/Chip Design

It is even worst than this
1. Trust in System/Chip Design

# Worst or best scenario
# How to ensure trust?
# Worst or best scenario
1. Trust in System/Chip Design

- Worst or best scenario
- How to ensure trust?
- Worst or best scenario
- Publications:
2. Physically Unclonable Function

What is PUF?

PUF in security:
- Store/generate key
- Device identification

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. “Kendall Syndrome Coding (KSC) for Group-Based RO PUFs,” (DAC 2012).
3. Trusted Executing Environment

Conventional Processor

High Performance CPU Pipeline

Pseudo Instructions with Side Information

Instruction Cache

Decoded Instruction

Light-weight Decoder

Data Extractor

LUT

Admission Controller

Integrity, Reliability, and Origin Check

Security Related Information

Side Information

Performance Enhancing Information

High-Performance Trusted Processor

Interrupt: abnormally report, system shutdown, …
3. Trusted Executing Environment

- FPGA Prototyping
  - Area (0.2%)
  - Power (0.07%)

- Applications:
  - Mobile code, mobile devices
  - Trust
  - Sensor and sensor networks.

- Publications:
4. The SecureGo System

Virtual communication links

Physical communication links

USB Device

Host

Offline Database

SecureGo Server

Merchant A

Merchant B

Merchant C
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.