Hardware in Cyber Security: from Enabler to Enhancer to Enforcer

Dr. Gang Qu, Carson Dunbar, Mingze Gao, Tanvir Arafin

30 THIRTY YEARS OF SYSTEMS RESEARCH EXCELLENCE

INSTITUTE FOR SYSTEMS RESEARCH
A. JAMES CLARK SCHOOL OF ENGINEERING

Hardware Security Overview

Hardware is the root of computation and communication. It is the **enabler** of any software, algorithm, or communication protocols. All computation will eventually be carried out by hardware, namely the processor or the circuits. Dedicated hardware such as accelerators and secure co-processors are built as system performance **enhancer**. Hardware is becoming the **enforcer** for security, trust, and privacy protection in the Internet of Things era.

Hardware -- the **weakest link** in cyber security

- Intrusive physical attacks
- Side-channel attacks, including power analysis, timing attacks, and electromagnetic attacks
- Untrusted supply chain (from design to fabrication)
- Hardware Trojan horse
- Hardware intellectual property (IP) theft
- Integrated circuit counterfeiting

Hardware – **great promises** for security :

- IP protection: watermarking, fingerprinting, metering, obfuscation, split fabrication, …
- Countermeasures against physical and side-channel attacks
- Trojan detection and prevention
- Hardware security primitives
- Lightweight cryptography

Future of the research

Hardware security design in the Internet of Things (IoTs)

We are entering into an era of IoTs. The explosion in the number of interconnected devices makes it a challenge to guarantee their security, the security of their networks, and the privacy of the data collected by them. Future research needs to address the following unique challenges when designing hardware (THINGS) for IoTs:

- Security
- Privacy
- Trust
- Ultra low power

Hardware has the intrinsic advantages to solve these challenges.

Security theory and practice for nano-devices

Effectiveness of existing security techniques and the metrics to predict the security properties and vulnerabilities of the next generation of nano-devices and systems needs to be reevaluated. Future research in this direction will focus on

- Developing a universal security theory for evaluation and design of nano-scale devices
- Implementation of innovative security primitives
- Providing a comprehensive system of first principles on which to base design, evaluation, and prediction of security performance of nano scale devices.

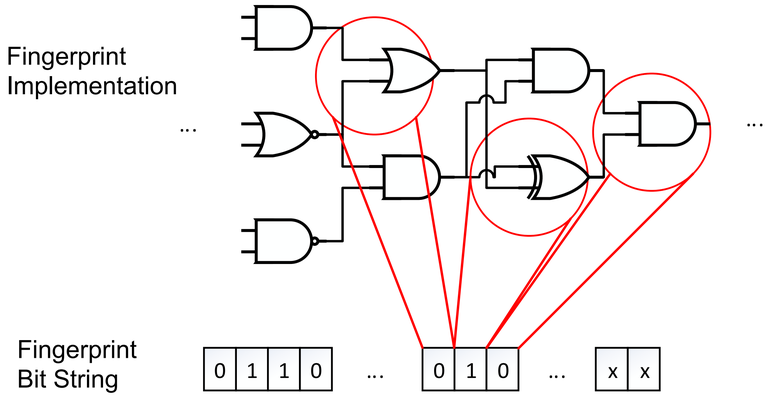
Intellectual Property (IP) Protection

Fingerprinting:

Our work focuses on creating practical fingerprints that allow us to track integrated circuits (ICs) to prevent IP theft

This is accomplished by applying small changes to circuitry during the design phase. These small variances give a unique code to every IC so that they can be identified at a later time.

Methods Developed To Efficiently Fingerprint ICs:
1. Observability Don't Care Fingerprinting
2. Satisfiability Don't Care Fingerprinting
3. Scan Chain Fingerprinting
4. Finite State Machine Manipulation Fingerprinting



Locations for possible fingerprint changes and the unique bit string to represent an individual IC

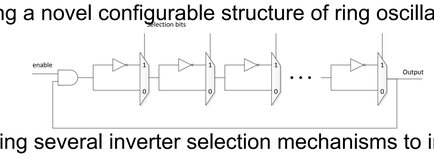
Physical Unclonable Functions (PUFs)

Silicon PUFs are generated by utilizing unique features in each piece of the silicon during chip fabrication which are caused by manufacturing variations.

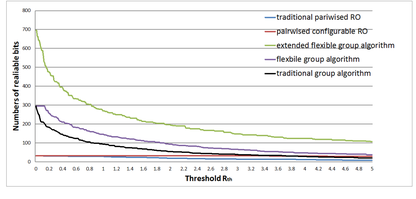
One bit response can be generated from the pair of ring oscillators (RO) if one is faster or slower than the other.

Our contributions includes:

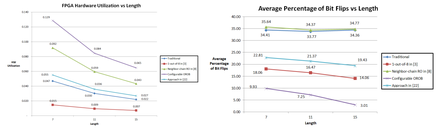
1. Proposing a novel configurable structure of ring oscillator



2. Developing several inverter selection mechanisms to increase the robustness/reliability and hardware utilization and efficiency.



3. Implementing our designed configurable RO PUF on 6 FPGA boards.

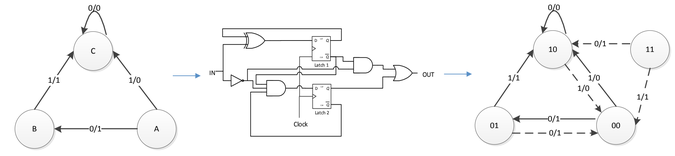


4. Proposing an anti-cloning mechanism by exploring the IC's intrinsic sensitivity of voltage.

Trusted Integrated Circuits (IC) and System Design

Trapdoors in Traditional Design

- Existing design tools are developed for performance optimization, not security and trust
- It is possible (and many times relatively easy) to find trapdoors in traditional designs. (Random walk attack, fault injection attack)



Original Finite State Machine (FSM) specification (left) Minimized circuit mapping for FSM (center) FSM after circuit mapping, with potential loss of security due to new paths (right)

Hardware Trojan Horses

- Intentionally added by malicious adversary during design time
- Incur little or no design overhead
- Can be hard to detect and remove
- Relatively well-known and rich literature

Our Contributions on Trusted IC Design

- Trust CANNOT be ADDED after design (trapdoors exist)
- Building "traps" to attract HTH and facilitate HTH detection
- IC obfuscation and design manipulation to eliminate or restrict the space of HTH

Funding Sources: AFOSR, AFRL, ARO, DARPA, LTS

Email: gangqu@umd.edu

MeshSec Lab