A Taxonomy of Hardware Attacks

IC Lifecycle
- Design/Synthesis
- Fabrication
- Testing
- Post-Deployment
- Split Manufacturing

A chip is split into metal layer and active layer, which can be used for
- Approximate computation
- End-to-end encryption
- Process variation
- Resource overheads
- Automated proof generation

Key Feature: very low overhead

Prior Defenses
- Split Manufacturing:
  - A chip is split into metal layer and active layer, and the metal layer is fabricated in a trusted foundry to prevent the complete exposure of the design to the offshoring foundry

Hardware Obfuscation:
- Inserting additional key-based logic to obfuscate the netlist

Key Challenges:
- Functionality obfuscation
- Layout obfuscation

IP Piracy

A malicious trojan may manipulate engineering layout files to obtain original netlist and he can gain profit by:
- Claiming the ownership of it
- Overbuilding the IC

Prior Defenses
- Split Manufacturing:
  - A chip is split into metal layer and active layer, and the metal layer is fabricated in a trusted foundry to prevent the complete exposure of the design to the offshoring foundry

Hardware Obfuscation:
- Inserting additional key-based logic to obfuscate the netlist

Future Work

Side-Channel Attack Resilient Architecture

Recently, different side-channel attacks have been applied successfully to retrieve keys from DES, RSA and AES. Power analysis measures the power consumption of an encryption and correlates that with the underlying keys. Timing analysis measures the time of an encryption to retrieve the keys. Many cache timing side-channel attacks have been demonstrated very successfully.

Power Trace of an DES Encryption

Side-Channel Attacks in Cryptography

Power Analysis measures the power consumption of an encryption and correlates that with the underlying keys.

Timing Analysis measures the time of an encryption to retrieve the keys. Many cache timing side-channel attacks have been demonstrated very successfully.

Security Analysis and Enhancement of Split Manufacturing in 2D IC

Split Manufacturing in 2D IC:
- A 2D IC can be split into active device layer and metal layer
  - Active layer (gate) is outsourced for advanced fabrication
  - Metal layer (interconnection) is performed by a trusted foundry

Side-Channel Attack Model: proximity attack + machine learning attack
- Proximity attack: two connected gates are usually placed close by
- Machine learning attack: learn the hidden interconnection based on the observed output differences between reconstructed and original ICs

Security Analysis and Enhancement of Three Hardware Obfuscation Models

Three Hardware Obfuscation Models:
- XOR/UNOR locking
- Signal wire permutation
- Reconfigurable block

Analysis and Enhancement:
- Security analysis of three models based on novel machine learning attack that intends to learn the secret keys
- Security enhancement techniques for each models to achieve the optimal defense results with low performance overheads

IP Piracy Prevention Based on 2.5D IC Technology

2.5D IC Security Benefits
- The interception can be hardened in a trusted foundry to prevent complete exposure of a design and thus prevent IP piracy

Secure Partitioning (Functionality obliteration):
- Partitioning a netlist F into two sub-netlists F1 and F2 with cut wires
- Goal: H(D(F1/F2)) > 50%
- Normal approach: min-cut partitioning
- Secure approach: select cut-wires with high controllability and observability

Secure Placement (Layout obliteration):
- Reduce the correlation between layout proximity and connection of two gates
- Goal: connectivity - 0 percentage of correctly guessed hidden wire
- Secure Approach: simulated annealing cost function $Cost = f(Area, Wirelength, Connectivity)$

Security Analysis and Enhancement of Three Hardware Obfuscation Models

Current Research

Temperature-tracking Based Run-time Trojan Detection

Motivation
- Test-time approaches: may miss some Trojan infected ICs due to:
  - Limited amount of test
  - Lack of Trojan activation
  - Inactive Trojans have small impact on delay/power
- Run-time monitoring approaches:
  - Monitor the IC throughout its lifecycle
  - Need a low-overhead solution

Avg. Power Consumption of RS232-T500 Benchmark

Why is the Attack Successful?
- The correct output response from a functional circuit can be utilized as a reference to determine how good a key is
- The effective key space is not large enough since 50% of the 2-bit permutation cells can be correctly permuted by simple random guessing
- The correlation between output HD and the key correctness is strong

Two security enhancement approaches:
- Key space enlarging using n-bit permutation cells
- Reducing the correlation between output HD and key correctness by creating an interlock structure

IP Piracy Prevention Based on 2.5D IC Technology

2.5D IC Security Benefits
- The interception can be hardened in a trusted foundry to prevent complete exposure of a design and thus prevent IP piracy

Secure Partitioning (Functionality obliteration):
- Partitioning a netlist F into two sub-netlists F1 and F2 with cut wires
- Goal: H(D(F1/F2)) > 50%
- Normal approach: min-cut partitioning
- Secure approach: select cut-wires with high controllability and observability

Secure Placement (Layout obliteration):
- Reduce the correlation between layout proximity and connection of two gates
- Goal: connectivity - 0 percentage of correctly guessed hidden wire
- Secure Approach: simulated annealing cost function $Cost = f(Area, Wirelength, Connectivity)$

Security Analysis and Enhancement of Three Hardware Obfuscation Models

Three Hardware Obfuscation Models:
- XOR/UNOR locking
- Signal wire permutation
- Reconfigurable block

Analysis and Enhancement:
- Security analysis of three models based on novel machine learning attack that intends to learn the secret keys
- Security enhancement techniques for each models to achieve the optimal defense results with low performance overheads

IP Piracy Prevention Based on 2.5D IC Technology

2.5D IC Security Benefits
- The interception can be hardened in a trusted foundry to prevent complete exposure of a design and thus prevent IP piracy

Secure Partitioning (Functionality obliteration):
- Partitioning a netlist F into two sub-netlists F1 and F2 with cut wires
- Goal: H(D(F1/F2)) > 50%
- Normal approach: min-cut partitioning
- Secure approach: select cut-wires with high controllability and observability

Secure Placement (Layout obliteration):
- Reduce the correlation between layout proximity and connection of two gates
- Goal: connectivity - 0 percentage of correctly guessed hidden wire
- Secure Approach: simulated annealing cost function $Cost = f(Area, Wirelength, Connectivity)$

Security Analysis and Enhancement of Three Hardware Obfuscation Models

Three Hardware Obfuscation Models:
- XOR/UNOR locking
- Signal wire permutation
- Reconfigurable block

Analysis and Enhancement:
- Security analysis of three models based on novel machine learning attack that intends to learn the secret keys
- Security enhancement techniques for each models to achieve the optimal defense results with low performance overheads

IP Piracy Prevention Based on 2.5D IC Technology

2.5D IC Security Benefits
- The interception can be hardened in a trusted foundry to prevent complete exposure of a design and thus prevent IP piracy

Secure Partitioning (Functionality obliteration):
- Partitioning a netlist F into two sub-netlists F1 and F2 with cut wires
- Goal: H(D(F1/F2)) > 50%
- Normal approach: min-cut partitioning
- Secure approach: select cut-wires with high controllability and observability

Secure Placement (Layout obliteration):
- Reduce the correlation between layout proximity and connection of two gates
- Goal: connectivity - 0 percentage of correctly guessed hidden wire
- Secure Approach: simulated annealing cost function $Cost = f(Area, Wirelength, Connectivity)$

Security Analysis and Enhancement of Three Hardware Obfuscation Models

Three Hardware Obfuscation Models:
- XOR/UNOR locking
- Signal wire permutation
- Reconfigurable block

Analysis and Enhancement:
- Security analysis of three models based on novel machine learning attack that intends to learn the secret keys
- Security enhancement techniques for each models to achieve the optimal defense results with low performance overheads

IP Piracy Prevention Based on 2.5D IC Technology

2.5D IC Security Benefits
- The interception can be hardened in a trusted foundry to prevent complete exposure of a design and thus prevent IP piracy

Secure Partitioning (Functionality obliteration):
- Partitioning a netlist F into two sub-netlists F1 and F2 with cut wires
- Goal: H(D(F1/F2)) > 50%
- Normal approach: min-cut partitioning
- Secure approach: select cut-wires with high controllability and observability

Secure Placement (Layout obliteration):
- Reduce the correlation between layout proximity and connection of two gates
- Goal: connectivity - 0 percentage of correctly guessed hidden wire
- Secure Approach: simulated annealing cost function $Cost = f(Area, Wirelength, Connectivity)$

Security Analysis and Enhancement of Three Hardware Obfuscation Models

Three Hardware Obfuscation Models:
- XOR/UNOR locking
- Signal wire permutation
- Reconfigurable block

Analysis and Enhancement:
- Security analysis of three models based on novel machine learning attack that intends to learn the secret keys
- Security enhancement techniques for each models to achieve the optimal defense results with low performance overheads

IP Piracy Prevention Based on 2.5D IC Technology

2.5D IC Security Benefits
- The interception can be hardened in a trusted foundry to prevent complete exposure of a design and thus prevent IP piracy

Secure Partitioning (Functionality obliteration):
- Partitioning a netlist F into two sub-netlists F1 and F2 with cut wires
- Goal: H(D(F1/F2)) > 50%
- Normal approach: min-cut partitioning
- Secure approach: select cut-wires with high controllability and observability

Secure Placement (Layout obliteration):
- Reduce the correlation between layout proximity and connection of two gates
- Goal: connectivity - 0 percentage of correctly guessed hidden wire
- Secure Approach: simulated annealing cost function $Cost = f(Area, Wirelength, Connectivity)$