Hardware Security

Mani Soma

Acknowledgements

- DARPA Broad Agency Announcements (BAAs) for IC Trust
- IEEE Hardware-Oriented Security and Trust workshops (HOST)
- Numerous papers in IEEE transactions / journals / magazines

Motivation

- Security and trust in fabless industry
- Protection against hardware attacks
  - Similarity with software / network attacks
- Protection against access to secured information
  - anti-tampering
- IP protection (anti-piracy)

Security issues in fabless industry

Security issues (2)

Key questions

- Does the IC perform its intended functions and nothing more?
- Is the design true to specifications?
  - validation issues
- For reconfigurable devices, does the configuration data accurately represent the specification, design, and synthesis?
More specific issues

- Check for unknown behaviors: how?
- Check for inserted circuits during fab (trojan)
  - check for additional unintended functions
- Validation that IC follows specifications
- Check for authentication
- Many common methods with test methods
  - “good” chip vs. “bad” or “untrusted” chip
  - test generation and design-for-test

Topics in hardware security

- Smart cards
- Watermarking of designs
  - IC fingerprinting, metering, DRM
  - Physically unclonable functions (PUFs)
- Hardware Trojan detection
- Attacks using aging, radiation, dielectric breakdown
- Obfuscation of designs
- Locking methods

Example

Method 1 and results

- IC with 1E6 transistors
- 64-bit adder with 2,048 transistors
- 2 altered transistors (“rogue” or trojans)
  - need to be detected
  - detection method
  - scan GDS-II file and compare polygons
- results
  - detect 5 “rogue” transistors
    - 1 true rogue (50% detection probability)
    - 4 false rogues (4E-6 false alarm probability)

Method 2 and results

- Generate test vectors to verify design function
- Detect function abnormalities
  - whole adder is bad
  - 100% detection probability
  - false alarm probability
    - good circuits could fail the tests
    - 2.048E-3 false alarm
- Much faster but with probability tradeoffs

Anti-piracy Methods

- IP protection
  - attacker has all design information
    - netlist, GDS-II file, test vectors
- Methods for authentication
  - IC registration
    - physically unclonable function (PUF)
  - Key locking IC
    - spatial variability
    - added FSM / XOR for obfuscation
    - combined XOR / key bits with public keys
Watermarking methods

- RFID tags
  - active or passive
  - easy to break or eavesdrop
- Digital watermarking
  - horizontal: mark specific step of synthesis or fabrication with unique signature
  - vertical: at higher functional level, signs all the lower levels

PUFs

- Fundamental idea
  - use variability-induced delays or switching thresholds for authentication
  - process variations create unique chip signature even for chips on the same wafer
- One-way function to map a challenge to a set of responses
  - IC is uniquely identified when in response to challenge(s), its response(s) is/are in the correct set

Delay-based PUFs

- ASICs / FPGAs
- Popular in smart cards, RFID, remote IC activation
- Analog timing difference on two paths with arbiter digital output
  - 1 if edge on first path arrives first

Delay PUFs (2)

- Path segments
  - same designed delay
    - differences due to process variations
      - uniqueness
  - challenge: selector bits $C_i = 1..N$
    - $C_i=1$ straight through; $C_i=0$ switch path (4 delays)
    - response = arbiter output
    - different IC = different response for same challenge
- Multiple-bit response outputs
  - $N=64$ or higher, arbiter output bits = 20 or higher

Delay PUFs (3)

- May be reverse-engineered
- Add non-linearity / programmability for robustness
  - feed-forward PUFs
  - unequal delay PUFs
  - interleaved PUFs
  - programmable PUFs

Delay PUFs (3)

- Distribute switch box segments over the chip
- Considerations
  - predictability of responses
  - Hamming distance between challenges vs. Hamming distance between responses
  - two challenges giving rise to the same response (collision)
  - sensitivity of PUF to process variations, defects, ambient conditions, etc.
Latch-based PUF
- Chip ID generator using latches
  - Use threshold offset in a latch to generate 1 bit
- Structure similar to RAM

Latch-based PUF (2)
- ID word size: 128 or larger
  - example design: read out all latches serially to form the ID
  - increasing Hamming distance between 2 adjacent chips
  - statistical post-processing to avoid unstable bits and achieve better chip identification
  - Also in popular use

FSM-based locking method
- Add states to an existing FSM
  - or use unused states (many!)
  - ID generator drives a normal FSM into unused states
  - secure key transitions back to normal state; otherwise lock

FSM lock design
- Unclonable ID generator
  - a PUF
- Key: supplied by designer (programmable)
  - remote key input possible
- Features
  - difficult to clone the PUF
  - reverse-engineer modified FSM: intractable
  - attack via combinational redundancy removal: difficult if FSM states are used in system logic

Public-Key Cryptography (PKC)
- Message encrypted by sender and decrypted by receiver
  - sent over untrusted medium
  - one-way hard-to-reverse functions
    - high-precision integer multiplication
    - modular exponentiation
    - number-factoring algorithms
- Chip ID application to lock chip or IP block

PKC process
- IP holder: generates Master Keys (MK)
  - MK-Pub and MK-Pri
  - embed MK-Pub on chip
  - locks specific IP and generates Common Key (CK) randomly
- Chip generates Random Chip Keys (RCK)
  - stored in programmable fuses permanently
  - Fab sends RCK-Pub to IP holder (secured channel)
- IP holder
  - encrypts CK with MK-Pri and RCK-Pub to generate Input Key (IK)
  - sends IK (secured channel) to Fab
  - Fab / Chip decrypts IK using MK-Pub and RCK-Pri to re-generate CK to unlock IP
PCK flow

Conclusion

- Focus on anti-piracy to assist with final project
  - state-of-the-art methods
    - still growing
    - how to attack?
- Other topics in hardware security
  - slide 8
  - all important and more work being done
- Growing research areas in IC design