MOLES:
Malicious Off-chip Leakage Enabled by Side-channels

Lang Lin*
Wayne Burleson*
Christof Paar* #

*University of Massachusetts Amherst, USA
#Ruhr University Bochum, Germany

ICCAD, November 2009

This work is supported by NSF Grants 0916854, 0627529
MOLES: Malicious Off-chip Leakage Enabled by Side-channels

Lang Lin*
Wayne Burleson*
Christof Paar*#

*University of Massachusetts Amherst, USA
#Ruhr University Bochum, Germany

ICCAD, November 2009

This work is supported by NSF Grants 0916854, 0627529
Power analysis attack in deep-submicron circuits:


Process variation impacts on power analysis attacks:


The concept and FPGA implementation of Trojan side-channels:

What are/is MOLES?

- In the spy world, moles are “double agents”

Notable moles

- James Hall III – An Army warrant officer and intelligence analyst in Germany who sold eavesdropping and code leaks to East Germany and the Soviet Union from 1983 to 1988.
- Mubin Shaikh and the Second mole in Toronto terrorism case

- In this work, MOLES is “Malicious Off-chip Leakage Enabled by Side-channels”
  - A novel class of hardware Trojans to intentionally leak secret information
  - Hidden communication channel
Threat Model

Design Company

Untrusted Foundry

Insider Attacker

Evaluator

Attacker

Design deliverables

Compromised IC

IC deployment

The secret key is 01010110.

Parties:

- Insider Attacker: implant MOLES
- Evaluator: IC test lab (Common Criteria …)
- Attacker: extract the secret information
Challenges in Hiding

Mission of the *insider attacker*: to hide the implanted Trojans to evade the *evaluators!*

- Where to hide on a chip?
- How to trigger?
- How large is the implementation?
- How to evade various post-silicon validations?
  - Layout inspection
  - Function tests
  - Security evaluation tests
MOLES Uses Side-channels

- Inherent side-channels of IC:
  - electromagnetic radiation, power consumption, path delay
- We engineer a side-channel to convey secret information:
  - Analog signals: no violation to the functions
  - Hard to test by traditional methods
  - Unique exploitability: attackers control the design

MOLES circuitry

- Key bus
  - X0
  - X1

X1: 1 0 0 0 0 0 1 0 0 1 1 1 1 1
X0: 0 0 0 0 0 1 0 0 1 1 0 1 1 0

Transient Power

0 2Tc 4Tc 6Tc 8Tc 10Tc 12Tc 14Tc
Challenges in Detection

REQUIREMENT: Only attackers can detect, while evaluators cannot!

1. Detection under low information leakage signal-to-noise power ratio (SNR)
   - Noise power at the global power grid (esp. non-crypto circuits)
   - Process variation

   Attackers can amplify SNR by performing many measurements of the side-channel leakage.

2. Unique exploitability

   Attackers can modulate (encrypt) the side-channel leakage by pseudo-random sequences.
Spread-Spectrum Techniques

Advantages:
1. Spread the side-channel leakage over a long time for hiding
2. Only the attackers gain knowledge of the modulation
3. Can leak multi-bit key simultaneously by code division

An experimental MOLES circuit using CDMA methods:
20-degree Linear Feedback Shift Register to leak 8-bit secret keys through capacitive loads
Design Spaces

- How many key bits to leak?
  - Attackers often leak partial secret key bits to reduce the key searching space
- How big is the load capacitance?
- How to implement the Pseudo-Random Number Generator (initial state, feedback loop)?
- How to model the “noise” power?
- What type of side-channels for a generic MOLES?
  - Power, but can be electromagnetic or timing side-channels
Design Flow

Determine design spaces

Design of MOLES circuit

MOLES implantation

Power Trace generation

Design of crypto circuit

NO

Key extraction by attackers?

NO

YES!

Detection by evaluators?

YES!

Design Verification

YES!

SNR calibration

Simulated measurement power (SMP) profile

Determine the noise model

SPICE

MATLAB

Design done!
MOLES Works!

- Implementation: AES substitution box compromised by a MOLES circuit leaking 8-bit key 01010110
- Device model: 45nm predictive technology model
- Number of power traces analyzed VS. differential power (DP)
- Solid lines: correct key guesses; Dash lines: wrong key guesses
- RPT (required number of power traces)
- -20dB SNR with additive Gaussian white noise model
Properties of MOLES

- Usually larger than 10000 RPT to extract all key bits
- Key value impacts ---- very weak
- Noise power impacts on RPT ---- near inverse-linear dependence on SNR (in dB)
CONCLUSION: demonstration of MOLES for the first time

- MOLES can leak multi-bit secret information
- Attackers can uniquely exploit MOLES

Constructive uses in the future!

- Enhancing the chip testability
  - Post-silicon validation
  - Built-In Self-Test (BIST)
- Cryptography applications
  - IC fingerprinting, PUF
  - Crypto primitives