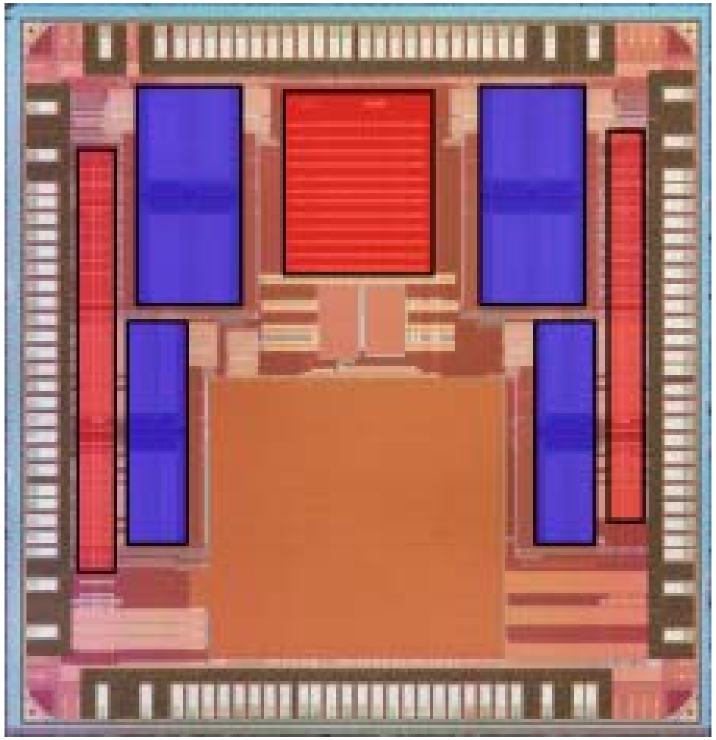
MOLES: Malicious Off-chip Leakage Enabled by Side-channels



Lang Lin*

Wayne Burleson*

Christof Paar*[#]

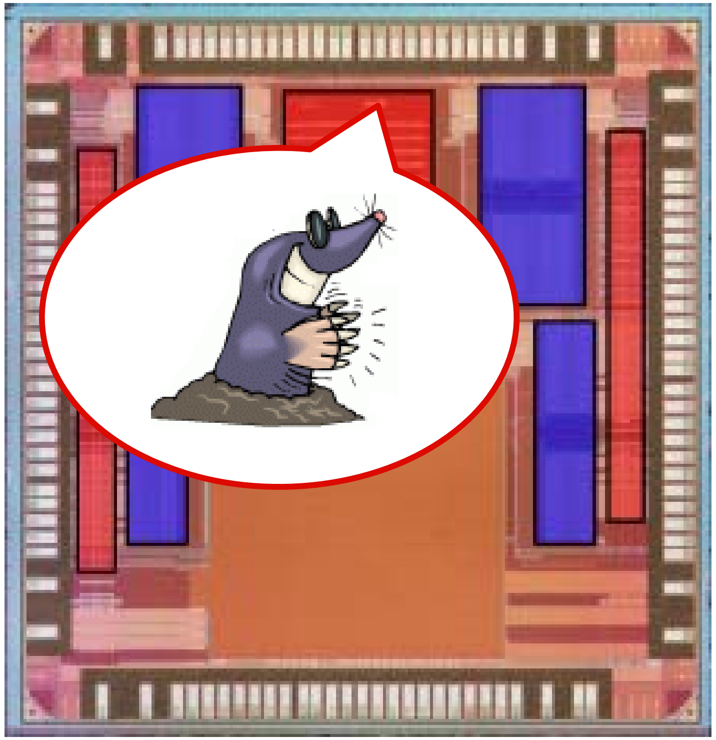
*University of Massachusetts Amherst, USA

[#]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

Our recent related research www.RFID-CUSP.org

- Power analysis attack in deep-submicron circuits:

  "Leakage-Based Differential Power Analysis (LDPA) on Sub-90nm CMOS Cryptosystems," by L. Lin and W. Burleson,
  In IEEE International Symposium on Circuits and Systems (**ISCAS**), May 2008.

- Process variation impacts on power analysis attacks:

  "Analysis and Mitigation of Process Variation Impacts on Power-Attack Tolerance," by L. Lin and W. Burleson,
  In Proceedings of ACM/IEEE Design Automation Conference (**DAC**), July 2009.

- The concept and FPGA implementation of Trojan side-channels:

  "Trojan side-channels: lightweight hardware Trojans through side-channel engineering," by L. Lin, M. Kasper, T. Guneysu, C. Paar and W. Burleson,
  In Workshop on Cryptographic Hardware and Embedded Systems (**CHES**), September 2009.

What are/is MOLES?

- In the spy world, moles are "double agents"

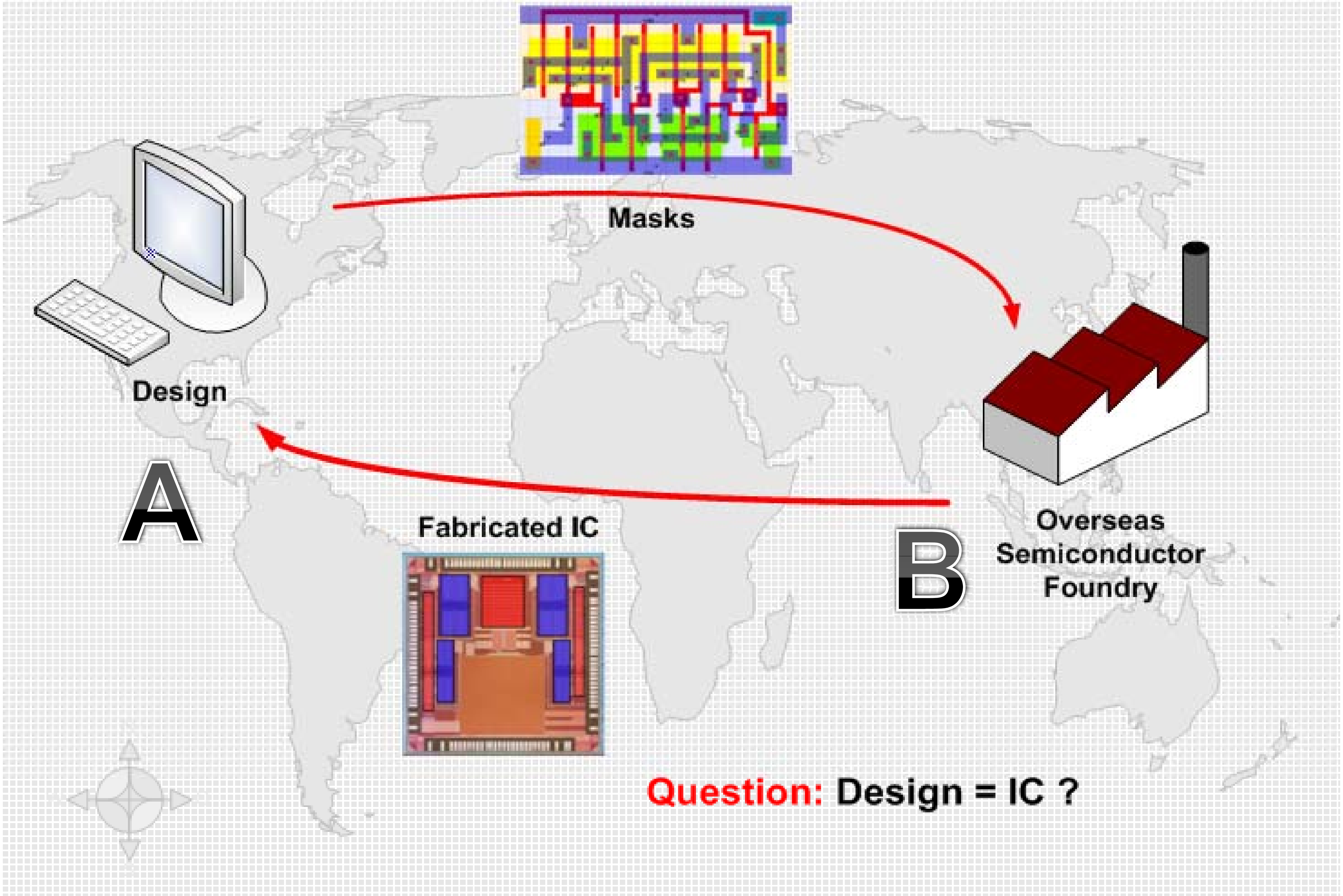
WIKIPEDIA

Notable moles

[edit]

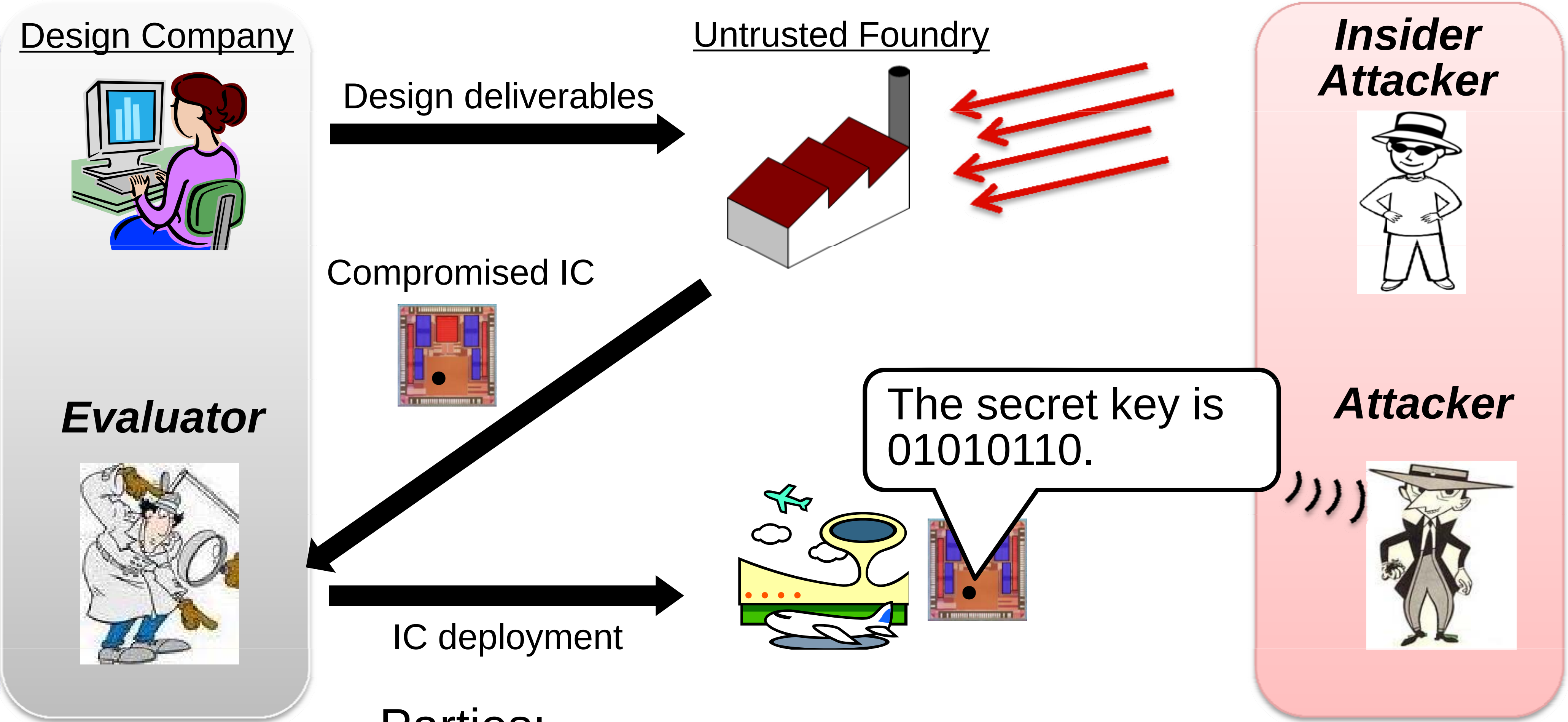
- Aldrich Ames – Arrested for spying for the Soviet Union and Russia from 1985 to 1994.
- James Hall III – An Army warrant officer and intelligence analyst in Germany who sold eavesdropping and code secrets to East Germany and the Soviet Union from 1983 to 1988.
- Mubin Shaikh and the Second mole in 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



“High performance microchip supply”, Defense Science Board, 2005;
“The hunt for the kill switch”, IEEE Spectrum, 45-5, pp. 34-39, 2008.

Threat Model



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

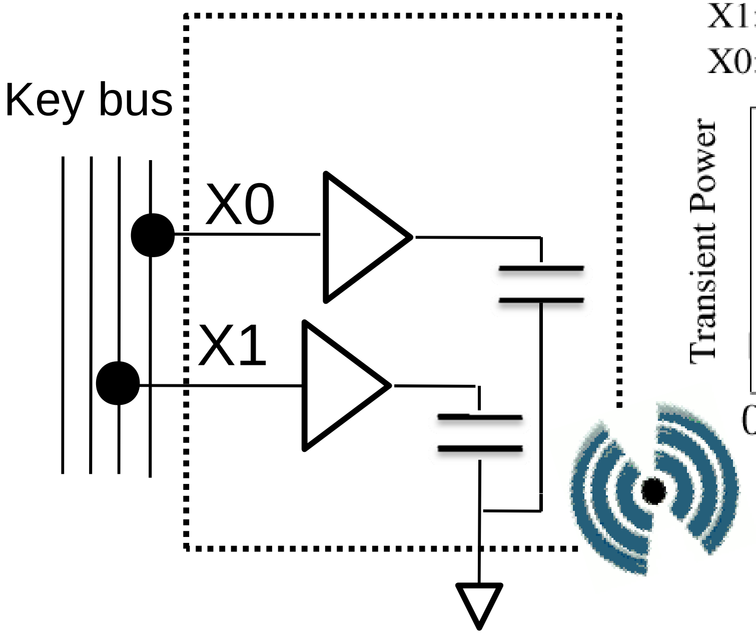
MOLES Uses Side-channels

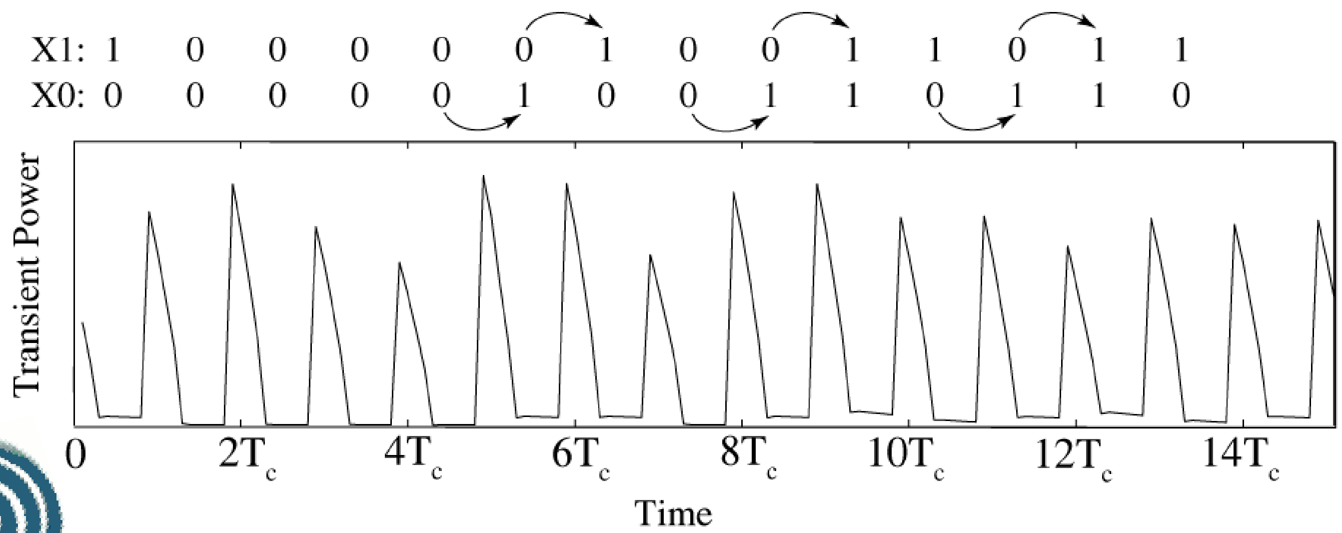
- Inherent side-channels of IC:

  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





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.

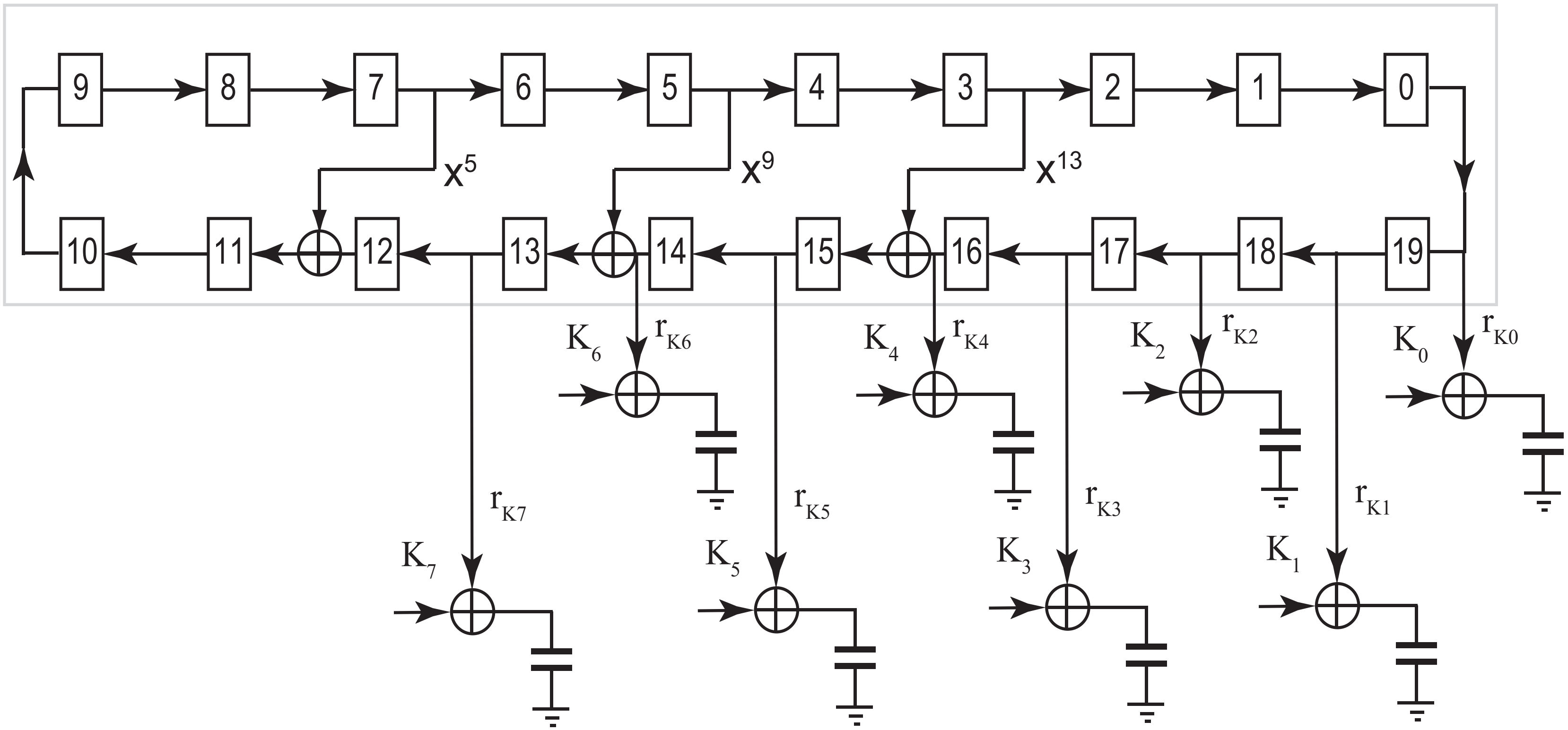
2. Unique exploitability

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



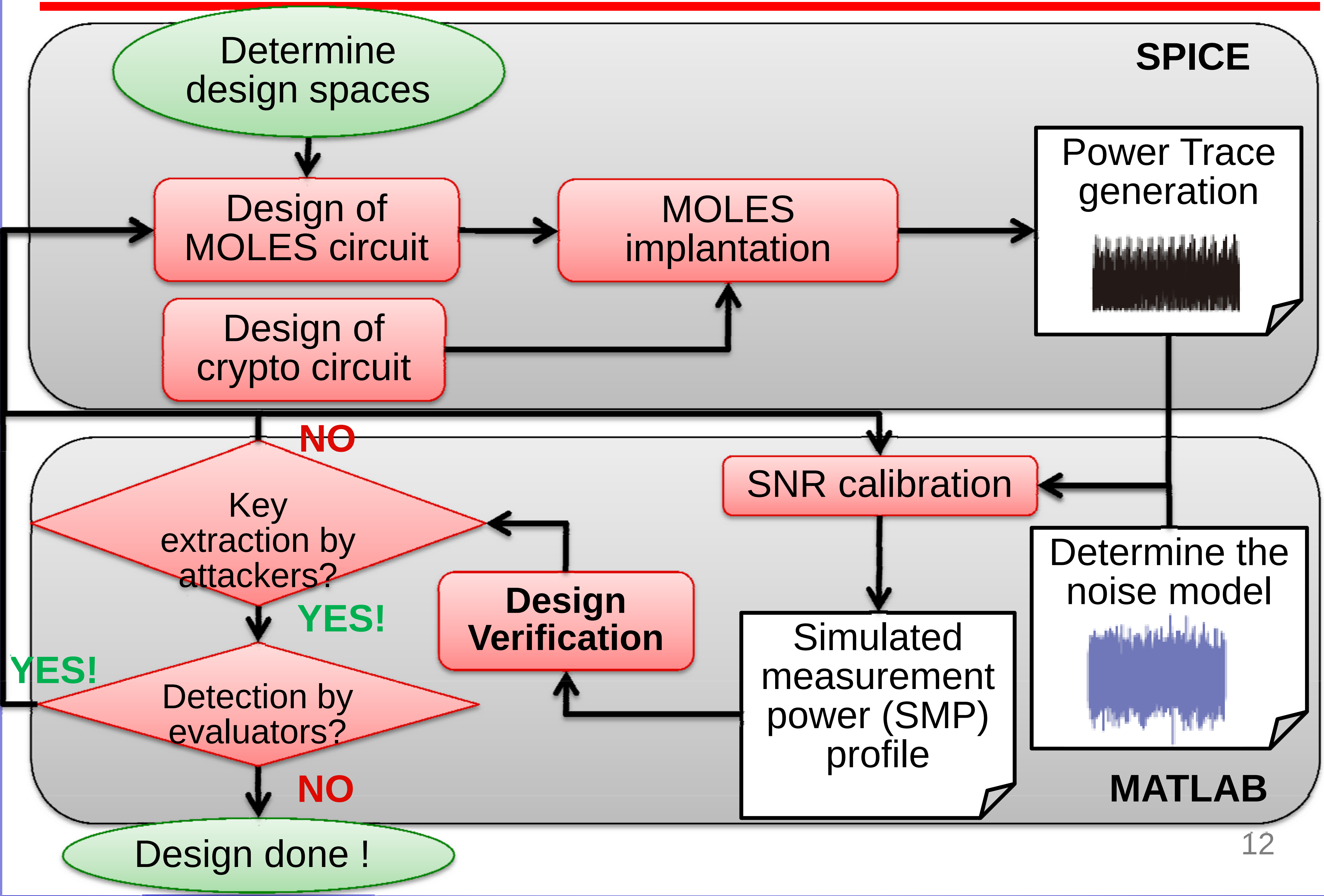
An experimental MOLES circuit using CDMA methods:

20-degree Linear Feedback Shift Register to leak 8-bit secret keys through capacitive loads

Design Spaces

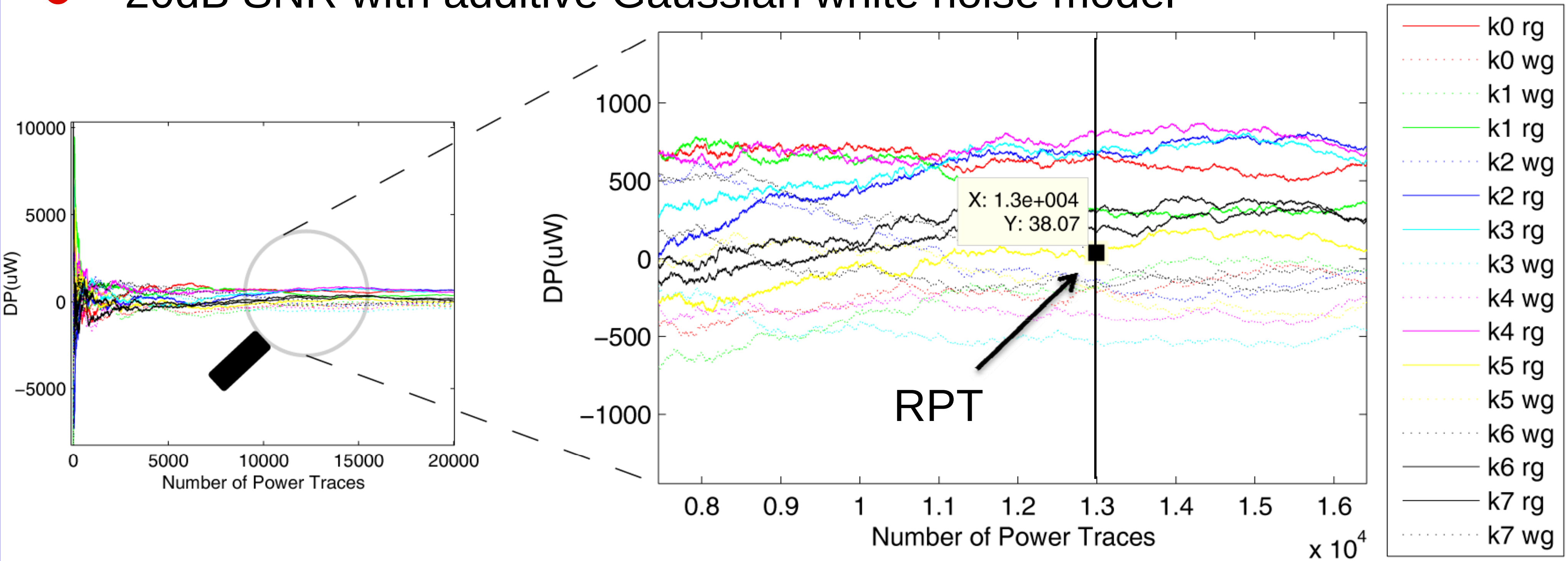
- How many key bits to leak?
  - Attackers often leak partial secret key bits to reduce the key searching space
- How big is the load capacitance?
- How to implement the Pseudo-Random Number Generator (initial state, feedback loop)?
- How to model the “noise” power?
- What type of side-channels for a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

Design Flow


SPICE
Determine design spaces
Design of MOLES circuit
MOLES implantation
Power Trace generation
Design of crypto circuit
NO
SNR calibration
Key extraction by attackers?
YES!
Design Verification
Determine the noise model
YES!
Detection by evaluators?
Simulated measurement power (SMP) profile
NO
MATLAB
Design done !

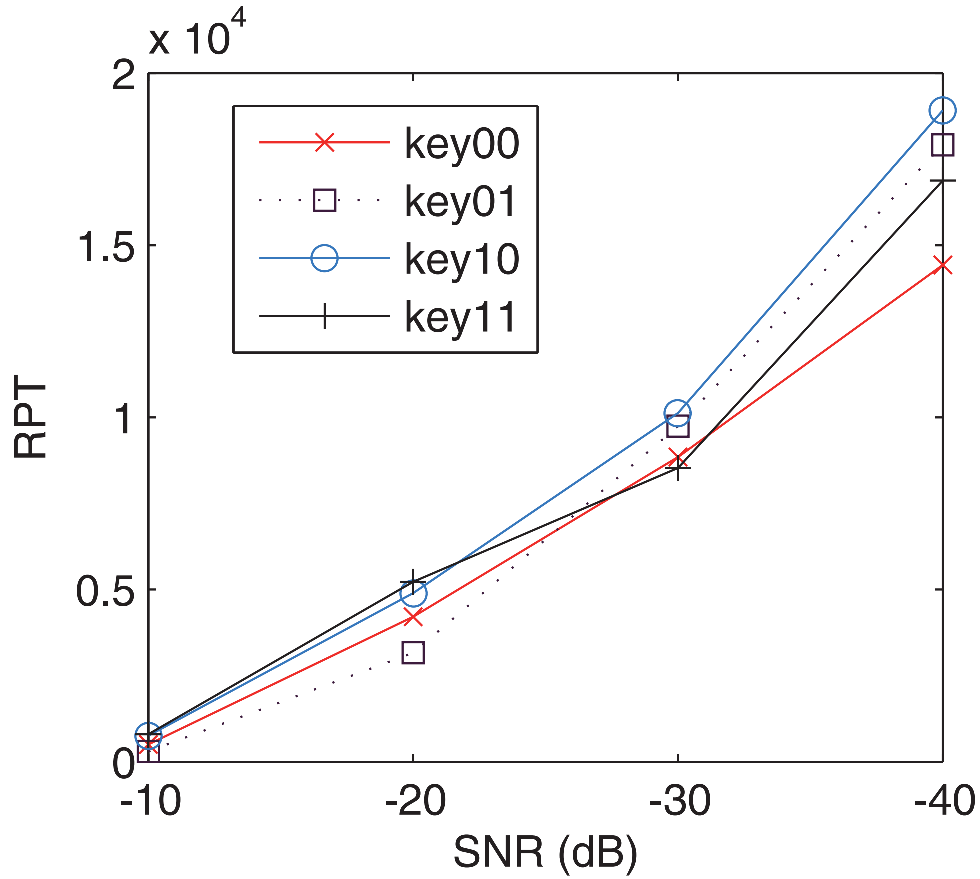
MOLES Works!

- 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 and Future Work

CONTRIBUTION: 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