Rationale

*Why is this lesson important? Why does the student need this lesson? How does this lesson fit in the larger module?*

Attackers may temporarily possess a tag or be close enough to read a tag. This makes tag security difficult. The security threats to tags and the corresponding mitigation techniques are important topics for RFID INFOSEC.

Objective(s)

*What will the student know, be able to do, and value at the end of this lesson? This is smaller amounts of information than the module objectives.*

The student will be able to list general mitigation techniques for preventing counterfeiting of tags, describe Gen2 techniques to mitigate tampering with tag data and to mitigate tag cloning, and list different types of side-channel information and the corresponding attacks.

Exploration

*Explicit concepts related to the Module goal are explored. It is at this point that the student will be provided basic information about the topic and the chance to explore some basic concepts about the topic. This is where the instructor imparts information.*

- Tag counterfeiting/cloning
  - Mitigation
    - Tag authentication
    - Physical unclonable functions (PUFs)
    - Electronic fingerprint (E-fingerprint)
  - Tampering with tag data
    - Gen2 mitigation techniques
      - Lock
      - Permalock
      - Tag identification (TID) memory
  - Side-channel attacks
    - Types
      - Power
      - Timing
      - Electromagnetic
• Fault injection
  • Synchronous versus asynchronous circuits
  • The effectiveness and drawback of traditional delay-insensitive asynchronous circuits in mitigating power- and timing-based side-channel attacks
    o NULL Convention Logic
    o Multi-rail encoding
    o DATA-NULL cycle
    o Pro’s and Con’s in balancing switching activity
    o How about time delay
  • Why Dual-spacer Dual-rail Delay-insensitive asynchronous Logic (D³L) is better
    o Dual-spacer truth table
    o Modified DATA-Spacer cycle
    o Switching activity analysis
    o D³L circuit design
    o Timing-based attack mitigation

Reflection
Several questions are posed to the student to answer and then often discuss as a class. This is an attempt to determine whether the student "gets" the basic concepts delivered above. If they do get it, move on to engagement. If they do not get it, go back to exploration above. It could be as simple as asking a few probing questions or as complex as asking the student to write a paper.

• What is side-channel information and how is it measured?
• Why in synchronous circuits, do different data patterns cause different power and delay?
• How does NCL improve balancing the power fluctuation among different data processed and what are the drawbacks?
• How does D³L mitigate side-channel attacks?

Engagement
Concepts learned in the Exploration are further developed by conducting experiments, designing and building solutions, and solving problems. This is an attempt to cause the student to apply the new knowledge. By applying the new knowledge, the student is much more likely to retain this information. This engagement could be accomplished through a debate, an experiment, a problem solving activity, or anything else that would cause the student to demonstrate understanding and competence.

• The knowledge of side-channel attacks will be tested in quizzes
• The knowledge of NCL and D³L in mitigating side-channel attacks will be tested in quizzes and homework assignments
Expansion

Provide opportunities for students to expand the concepts to more general or global situations including connection to the Module goal. Expand back to the big ideas of the module and prepare for the next lesson.

- How do you design a D^{3}L gate at the transistor-level?
- Is there any way to reduce the overhead caused by dual-rail encoding while maintaining the perfect balance of switching activity among different data patterns?

Lesson Assessment

Assess student understanding of the lesson content. This does not have to be a full-blown examination. It could be a graded homework assignment, a quiz, a performance examination, a graded problem solving activity, or something similar.

- Quizzes
- Homework assignments

Equipment

- None

Software

- None

References


Copyright Notice
This material is Copyright © 2008, 2009 by Jia Di and Dale R. Thompson. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or incorporated in commercial documents without the written permission of the copyright holder.

Acknowledgment
These materials were developed through a grant from the National Science Foundation at the University of Arkansas. Any opinions, findings, and recommendations or conclusions expressed in these materials are those of the author(s) and do not necessarily reflect those of the National Science Foundation or the University of Arkansas.

Liability Release
The curriculum activities and lessons have been designed to be safe and engaging learning experiences and have been field-tested with university students. However, due to the numerous variables that exist, the author(s) does not assume any liability for the use of this product. These curriculum activities and lessons are provided as is without any express or implied warranty. The user is responsible and liable for following all stated and generally accepted safety guidelines and practices.