RFID INFOSEC Homework #4, ver. 2.1
Tag Layer
Assigned Oct. 11 and Due Oct. 20, 2010

Name: __________________________________________

ID: ________________________________

37 pts.

Show all your work. Without proper justification and details of steps, correct answers alone may not carry full credit.

Notes:
- Minus 3 points if your homework is not stapled in the upper left-hand corner.
- Minus 2 points if you use the back of your paper. Please only use a single side.
- Minus 2 points if you present the worked problems out of order. In other words, please present the problems in the order assigned, 1, 2, 3, ...

1. Describe the differences between Class-1 and Class-2 tags as described in the Gen2 specification. Circle the difference that affects security the most. (5 pts.)

2. What group of circuits on a tag implements the protocol? (2 pts.)

3. What group of circuits on a tag modifies and reflects the signal from the reader to communicate with the reader? (2 pts.)

4. Are there an odd or even number of inverters in the ring oscillator on a tag? Why? (3 pts.)

5. If a reader wants to access the 32-bit TID stored in the tag memory, what parameter(s) does it need to provide to the tag? Locate and review the Gen2 specification to answer this question. (5 pts.)

6. Describe the three basic operations between readers and tags. (3 pts.)

7. In Gen2, the tag picks a random number from what range of numbers when preloading the slot counter after the tag receives the Query command with Q=3 from the reader? (3 pts.)

8. What is the system purpose of the tag slot counter? (3 pts.)

9. A Gen2 tag begins with the session S1 flag set to B. After 7 seconds of the tag being powered on by the reader carrier, the reader has not refreshed the S1 flag. What is the flag for S1? (2 pts.)

10. Describe the timing-based PUF as described in class. (3 pts.)

11. List one mitigation technique for the relay attack. (2 pts.)

12. Describe the fault-injection side-channel attack. (2 pts.)

13. What is an advantage of using NCL or D3L logic instead of conventional logic? (2 pts.)