Trojans I(A)

Multiple choice:
1) Hardware Trojans are designed by adversaries to accomplish any of the following except
a) Reduce the reliability of the chip
b) Leak sensitive information
c) Reconfigure to become a different product that can be sold on the black market
d) Provide a back-door to disable or destroy the chip

2) Stealthy insertion strategies undertaken by the adversary are best detected because of the observer effect
a) By functional testing
b) By sensitive parametric methods
c) By logic testing
d) By physical observation using a microscope

Trojans I(B)
1) The methods used to detect Soft Trojans include

Multiple choice:
1) Malicious insertion can occur at any of the points during the lifecycle of the IC except
a) In 3rd party IP
b) In the transfer process of wafers to testing facilities
c) In the design of PCBs that contain the ICs
d) None of the above

2) The two most attractive insertion points for adversaries are
a) System integration and deployment
b) CAD tools and place and route
c) Generation and application of test vectors during manufacturing test
d) Subversion of soft IP blocks and layout modifications

Trojans I(C)
1) Information leakage hardware Trojans are difficult to detect because

Multiple choice:
1) Small functionally-disruptive hardware Trojans are risky because
a) They are not capable of implementing any type of disruptive function
b) They might be accidentally detected
c) They might not work for the adversary
d) They occupy a small region and therefore can cause a large leakage current anomaly

2) Selectively inserted hard-IP Trojans are attractive for adversaries in applications that
a) Are designed to leak sensitive information
b) Require direct and immediate control over the infected chip
c) Require only a very small layout to implement the needed functionality
d) Control missile chips

Trojans I(D)
1) The costs associated with failure analysis tools

2) Why do trusted authorities who apply test vectors designed to functionally activate the Trojan target random-pattern resistant nodes?

Multiple choice:
1) The following are challenges with detecting HT detection except
a) HT and bugs share many of the same characteristics and finding all bugs is generally infeasible
b) The appropriate detection strategy will vary greatly depending on the insertion point
c) They are fabricated in nanometer technologies and therefore are difficult to see
d) Task of identifying an HT is akin to finding a needle in a haystack

2) A Hard-IP Trojan Taxonomy includes all of the following categories except
a) Physical characteristics
b) Action characteristics
c) Power characteristics
d) Activation charactistics

Trojans I(E)

Multiple choice:

1) The drawbacks of using logic testing to functionally activate HTs include all of the following except
a) Logic testing can only be used to effectively detect small Trojans
b) Leakage HTs cannot be detected
c) Automatic test pattern generation algorithms that generate tests for hard-to-detect nodes have very long runtimes
d) The HT logic tests generated and applied can cause the chip to overheat and burn out

2) The benefits of parameteric methods for detecting HTs include all of the following except
a) The amount of data collected from the chips is small and easy to analyze
b) They are non-destructive
c) They can potentially detect information leakage Trojans
d) They can be made to be very sensitive to very small HT signal anomalies