SCACounterMeasures I(A)

Multiple choice:

1) The fundamental principle that SPREAD is based on is best described as

a) A noise injection technique

b) A masking technique that hides data correlations

c) Both a masking and noise injection technique

d) A technique that reconfigures the underlying hardware implementation as a means of disrupting correlations that DPA leverages to deduce internal secrets

2) Dynamic partial reconfigurations is used within SPREAD to

a) Reconfigure AES primitives such as the SBOX with diverse implementations of the function

b) Reconfigure the entire AES engine on-the-fly

c) Reconfigure the data registers, scrambling the order in which the rounds are carried out

d) Reconfigure the order of the datapath operations

SCACounterMeasures I(B)

Multiple choice:

1) The three synthesis directed implementation diversity techniques include all of the following except

a) Changing the functional behavior of design being synthesized
b) Changing the timing constraints
c) Changing the standard cell library used in the behavioral synthesis
d) Making inconsequential changes to the behavioral or netlist descriptions

2) Leakage in the power trace introduced by the DPR operation is likely to difficult to leverage because of the following except

a) Power consumption by the AES engine itself will superimpose on the DRP power consumption, obscuring features produced by the DPR operation
b) The power consumed by the DPR operation is insignificant and therefore will be difficult or impossible to measure by the adversary
c) Each of the SBOX locations will produce a different power transient, increasing the number of distinctive power traces
d) The nonce generator will add artifacts to the DPR power trace