Side-Channel Attacks I(A)

Multiple choice:

1) Side-channel attacks are defined by any of the following except
a) Measurements of electro-magnetic radiation from the chip
b) Measurements of temperature contours within the chip
c) Measurements of the digital input-output behavior of the chip
d) Measurements of the power supply transient signals of the chip

2) Conditional branches can be used to extract information when
a) The condition depends on the value of a key bit
b) The number of instructions that are executed depends on the key bit
c) The execution speed of the conditional branch depends on the key bit
d) All of the above

Side-Channel Attacks I(B)

Multiple choice:

1) Simple power analysis (SPA) countermeasures include all of the following except
a) Designing custom ASIC implementations
b) Reversing the operations carried out by encryption algorithms
c) Removing conditional branch dependencies that use key bits in the condition
d) Recoding microcode used by microprocessors to make them nearly equal in terms of power consumption

2) Differential power analysis (DPA) leverages all of the following except
a) Correlations that occur as data is manipulated by encryption algorithms
b) Signal averaging as a mechanism to reduce noise
c) Fourier analysis to determine the frequency characteristics of the power traces
d) Simulation experiments to determine the output behavior of, e.g. the SBOX as a means of partitioning power supply traces into two groups

Side-Channel Attacks I(C)

Multiple choice:
1) Differential power analysis (DPA) create two groups of power traces based on which of the following
a) The value of an SBOX output bit determined from simulation of a set of plaintexts
b) The value of a key bit under attack
c) The behavior observed in the power trace waveforms
d) The difference in the behavior of two power trace waveforms

2) Manufacturing test methods that leverage power supply signals to detect defects need to account for an additional source of variation that DPA does not need to consider, which is
a) Process variation effects
b) Temperature variations
c) Measurement noise
d) EM interference