PUFs II(A)

1) Distinguish between a weak and strong PUF

2) Why are PUFs used for encryption not threatened by model building

Multiple choice:

1) The following usage scenarios are relevant to PUF except

a) Encryption
b) Identification
c) Authentication
d) Differential Power Analysis

2) The following benefits are associated with strong PUFs when used for authentication except

a) The provide a very large challenge-response space
b) They are tamper evident
c) They eliminate NVM
d) Their responses do not need to be reproduced

PUFs II(B)

1) What are the important statistical metrics for encryption?

Multiple choice:

1) Which of the following statistical metrics can be relaxed when PUFs are used for encryption key generation?

a) Reliability
b) Uniqueness
c) Randomness
d) Exponential CRP space

2) The following is true regarding the arbiter PUF except

a) The paths through each switch box are matched in delay
b) Meta-stability can occur for some challenges and result in unstable response bits
c) The amount of entropy is proportional to the number of challenges, which is exponential
d) An arbiter is a circuit structure that decides which of the two paths is faster

PUFs II(C)

1) Briefly describe a technique that can be used to allow a weak PUF to serve the role of a strong PUF, e.g., for authentication.

Multiple choice:

1) Improvements to the arbiter PUF to improve its resistance to model-building attacks include

a) Transforming the original version into feed-forward and XOR-mixed versions
b) Round-robin challenge shifting
c) Encryption of its output responses
d) Using randomly chosen challenges

2) The ring oscillator (RO) PUF measures Entropy by

a) Time the transition around the ring using a high precision delay measurement technique
b) Counting the number of oscillations over a fixed delta t time interval
c) Monitoring the power supply transient signal generated on the supply rail
d) By having the RO output drive an edge detector circuit that counts edges

PUFs II(D)

1) What is the maximum number of independent bits that can be obtained from an RO PUF with *n* ROs?

Multiple choice:

1) The number of bits that can be derived from *n* RO is given by each of the following except

a) n*(n-1)/2
b) log_base2(n!)
c) n
d) n/2

2) The metal PUF measures metal resistance variations using a technique called

a) A 4-wire measurement method
b) An analog-to-digital converter
c) A method based on Ohm’s law
d) A shorting device method

PUFs II(E)
1) What is the value produced by the voltage-to-digital converter of the metal PUF is proportional to?

Multiple choice:
1) The voltage-to-digital converter of the metal PUF creates a digital value referred to as
a) A counter value
b) A PUF number
c) A thermometer code
d) An n-bit integer

2) The error avoidance scheme used by the metal PUF uses which of the following
a) An inclusion region
b) Two thresholds and an exclusion region
c) An arbiter
d) An analog-to-digital-converter

PUFs II(F)
1) What represents the entropy source for the HELP PUF?

Multiple choice:
1) The HELP PUF measures delays in
a) A test structure with identically designed elements
b) An arbitrarily synthesized functional unit
c) A specialized test structure built from XOR gates
d) A string of inverters connected in a ring

2) Clock stobing involves all of the following except
a) Fine phase shifting Clk2 forward with respect to Clk1
b) Applying a 2-vector sequence repeatedly
c) Examining the output of an XOR gate to determine when the path is timed
d) Estimating the path delay based on the number of gates in the path

PUFs II(G)

1) Briefly describe the unique feature of the HELP algorithm that makes it a strong PUF, i.e., enables the distribution effect.

Multiple choice:

1) The terms PNR and PNF refer to

a) Forward and reverse processing operations on path delays
b) Two thresholds associated with path delays
c) Pseudo-random numbers
d) Rising and falling path delays respectively

2) The HELP algorithm is unique because it applies a transformation to

a) A group of path delays
b) Individual path delays
c) Pairs of path delays
d) Three tuples of path delays

PUFs II(H)

1) Briefly describe why leveraging chip-to-chip variations as the only source of Entropy is dangerous for a PUF.

Multiple choice:

1) Leveraging chip-to-chip variations as the only source of Entropy is dangerous because

a) There is a risk that bitstrings from different chips will be vastly different

b) As the chip population gets large, subsets of chips with very similar performance will produce similar bitstrings

c) Chip-to-chip variations do not exist in some fabrication facilities

d) Chip-to-chip variations cannot be counted on to add bias

2) The TVComp component of the HELP algorithm applies a

a) Fourier transform

b) Convolution operation

c) Linear transformation

d) Hilbert transform

PUFs II(I)

1) What is the purpose of the HELP Margining scheme?

Multiple choice:

1) Path length bias occurs in the HELP PUF because

a) Paths of different length are measured and compared

b) No attempt is made to match path delays in the hand layout of the functional unit

c) The synthesis tools are non-optimal

d) The implementation tools are non-optimal

2) The HELP Margining scheme is

a) A bit-flip avoidance scheme

b) An error-correction scheme

c) A scheme used to assign a modPNDco a bit value of 0 or 1

d) A compensation technique

PUFs II(J)

Multiple choice:
1) The probability of failure for HELP for a Margin of 3 is approximately
a) 1 in 10,000
b) 1 in 1,000
c) 1 in 1,000,000
d) 1 in 10,000,000

2) The pass criteria for the NIST statistical tests is given as the number of chip bitstrings that pass the test, which with 500 chips is
a) 450
b) 488
c) 300
d) 500