PUFBasedProtocols (A)
1) What is the primary benefit of a controlled PUF for authentication?

Multiple choice:
1) The characteristics of the base-case PUF-based authentication protocol with unprotected interface
a) It is privacy preserving, lightweight and is resistant to denial-of-service (DOS) attacks
b) It is simple, can use an error-tolerant matching scheme and is subject to DOS attacks
c) It is lightweight, provides mutual authentication and is susceptible to model-building attacks
d) It is simple, is not subject to DOS attacks but is susceptible to model-building attacks

2) The primary benefit of a controlled PUF for authentication is
a) It is lightweight and uses no cryptographic primitives
b) It can be used with PUFs that are not model-building resistant
c) It can use an error-tolerant matching scheme
d) It rejects random challenges sent by an adversery

PUFBasedProtocols (B)
1) What must the server do to the stored response bitstring it has in its secure database in a reverse fuzzy extractor scheme?

Multiple choice:
1) The reverse fuzzy extractor PUF-based protocol is characterized as
a) A protocol that reverses Gen and Rep where the token precisely reproduces the response
b) A protocol that reverses Gen and Rep where the token hashes it response before transmitting it
c) A protocol that reverses Gen and Rep where the token produces a noisy response
d) A protocol that reverses Gen and Rep where the token accepts challenges from the server

2) The reverse fuzzy extractor requires the server to
a) To error correct the token's response to match it to the stored response
b) To store large numbers of responses for each token
c) To send challenges to the token during enrollment
d) To error correct the stored response in an attempt to match it to the noisy response sent by the token

PUFBasedProtocols (C)
1) Briefly describe a unique capability of the slender PUF protocol.

Multiple choice:
1) A unique capability of the slender PUF protocol is
a) It allows any arbitrary challenge from the exponential CRP to be applied during authentication
b) It is able to precisely reproduce response bitstrings
c) It is able to precisely model the arbiter PUFs as mathematical models across variations in temperature and voltage conditions
d) It is able error correct response bitstrings without helper data

2) The primary benefit of substring matching used within the slender PUF protocol is
a) It allows fuzzy matching to be carried out on the server
b) It requires only a substring portion of the response bitstring to match the stored response
c) It reveals only a portion of the response bitstring generated by the PUF, making model-building more difficult
d) It is faster because only a substring needs to be matched by the server

PUFBasedProtocols (D)

1) Briefly describe how desynchronization attacks are prevented in an authentication protocol that uses chaining.

Multiple choice:

1) Protocol 5 protects against desynchronization attacks on the chaining operation by

a) Synchronizing periodically with the server

b) Storing information in a non-volatile memory on the token

c) Identifying and discarding adversary attempts to authenticate with the server

d) Having the server store a backup copy of the information used in the previous authentication operation

2) The t_sub_2 from the pseudo-random function is used

a) To identify the current token to the server

b) To XOR encrypt the response r_sub_2 used in the next authentication

c) As a key to a HMAC to generate a digest m

d) As an identifier to verify the server in a mutual authentication operation

PUFBasedProtocols (E)

Multiple choice:
1) The server commits to updating its database with a new response and secret key from the token after
a) The server confirms that the helper data has not been manipulated by an adversary
b) The server confirms that the helper data nor the response r_sub_2 have not been manipluated by an adversary
c) The server confirms that the t_sub_1 generated from an entry in the database matches that obtained from token
d) The server confirms that the response r_sub_2 has not been manipulated by an adversary

2) The primary drawback of Protocol 5 is
a) Its huge database storage requirements
b) Its suspectability to DPA attacks that are designed to steal the token-generated z_prime_sub_1 secret, that once learned by the adversary, can result in DOS for the token
c) The requirement that the token precisely reproduce the response bitstring
d) The requirement that the server do an exhaustive search of the database

PUFBasedProtocols (F)

1) Briefly describe the primary benefit of storing timing data instead of PUF response bitstrings in the HELP protocol.

Multiple choice:

1) Challenge generation for the HELP protocol is non-trivial because

a) The Entropy source is not well defined

b) The Entropy source is similar to an identically designed test structure

c) The Entropy source does not implement a real function and therefore is undefined

d) The Entropy source is an actual functional unit where determining which paths are sensitized by a challenge is an NP-complete (difficult) problem

2) The primary benefit of storing timing data instead of PUF response bitstrings by the HELP protocol is

a) The ability of the HELP algorithm to generate large numbers of response bitstrings from the stored timing data

b) The simplifications that can be implemented for the HELP enrollment operation

c) The fact that timing data can be error corrected efficiently

d) The fact that timing data is a better match to what the PUF actually produces

PUFBasedProtocols (G)
1) What can happen to a fixed PND if it is included in different distributions within the HELP algorithm?

Multiple choice:
1) The distribution effect implemented by the HELP algorithm is best characterized as
a) A method that allows an exponential number of groups of PND to be selected from a larger set
b) A method that leverages the distributions from different chips to add diversity to the response bitstrings
c) A method that processes groups of PND where the distributions associated with the group can each have distinct statistical mean and range characteristics
d) A method that adds complexity to bitstring generation by processing large groups of PND

2) TVComp makes it possible for a fixed PND to
a) Produce the same PNDc value but a different bit value
b) Produce a distinct PNDc but the same bit value
c) Produce a distinct PNDc and distinct bit value
d) Produce the same PNDc and same bit value

PUFBasedProtocols (H)
1) Briefly describe why the Dual Helper Data scheme within HELP improves response bitstring reliability, i.e., what does it leverage?

Multiple choice:
1) The Dual Helper Data scheme improves response bitstring reliability by
a) Leveraging only the helper data generated by the server using data stored in its secure database
b) Leveraging the helper data generated by both the token and server
c) Leveraging the Modulus scheme implemented on the token
d) Levearging the TVComp process carried out on the server

2) The Dual Helper Data scheme requires
a) A server-stored PNR or PNF to change by more than 2*Margin in order for a bit flip error to occur
b) The bit generated by the token to be classified as weak in order for a bit flip error to occur
c) A modPNDc generated by the token needs to move because of uncompensated TV noise a distance defined by more than 2*Margin in order for a bit flip error to occur
d) The bit generated by the server to be classified as weak in order for a bit flip error to occur

PUFBasedProtocols (I)

1) Why are a common set of challenges used in the initial phase of the HELP protocol?

Multiple choice:

1) A common set of challenges are used in the initial phase of the HELP protocol to

a) Carry out a privacy-preserving ID phase which can optionally serve as token authentication

b) Make it easy to carry out server authentication

c) Avoid needing to carry out an exhaustive search on the secure database by the server

d) Simply challenge generation during enrollment

2) Which step(s) carried out by the server during the initial phase can be skipped during server authentication in Phase II?

a) Generation of helper data by both the token and server

b) Exhaustive search of the database

c) The running of the PNDiff and TVComp operations

d) The running of the Modulus and Margin operations