

PUF-Based Authentication (A)

1) The tamper evidence property of PUFs provides protection against

Multiple choice:

1) A truly strong PUF has

- a) A very large CRP space and are machine learning resistant
- b) A small entropy source by a very large CRP space
- c) A large entropy source but a small CRP space
- d) A small CRP space but are machine learning resistant

2) Secure Sketches provide

- a) Randomness extractors
- b) Error correction
- c) Randomness extractors and error correction
- d) Secure approximate authentication

PUF-Based Authentication (B)

1) Name the two secure sketch methods that we discussed.

Multiple choice:

1) A secure sketch is composed of

- a) A sketch and randomness extractor method
- b) A randomness extractor and error correction method
- c) A sketch and error correction method
- d) A sketch and recover procedure

2) Two secure sketch methods include

- a) Code-offset and linear transformation methods
- b) Linear transformation and syndrome methods
- c) Parity check and syndrome methods
- d) Code-offset and syndrome methods

PUF-Based Authentication (C)

1) What is the purpose of a reverse fuzzy extractor, i.e., why was it proposed?

Multiple choice:

1) The basic idea behind a reverse fuzzy extractor is

- a) To reverse error correction and secure sketch on the token and server
- b) To reverse sketch and recover on the token and server
- c) To reverse sketch and randomness extractor on the token and server
- d) To reverse recover and error correction on the token and server

2) During authentication, the token in a reverse fuzzy extractor scheme performs

- a) Recover and then randomness extraction
- b) Random extraction and then recover
- c) Sketch and then randomness extraction
- d) Randomness extraction and then sketch