QClss 24/25 QKD Homework 3: QKD with Noise

Due Dec 23 at 3:59am **Points** 10 **Questions** 10
Available Dec 10 at 7pm - Dec 23 at 3:59am 12 days
Time Limit 60 Minutes **Allowed Attempts** 3

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	30 minutes	6 out of 10

Answers will be shown after your last attempt

Score for this attempt: **6** out of 10
Submitted Dec 22 at 9:55pm
This attempt took 30 minutes.

Last Attempt Details:

Time:	30 minutes
Current Score:	6 out of 10
Kept Score:	6 out of 10

2 More Attempts available

Take the Quiz Again

(Will keep the highest of all your scores)

Question 1 — 1 / 1 pts

Suppose we have a two state protocol, where Asja chooses randomly between Z and X basis and prepares state $|0\rangle$ if Z basis is chosen and state $|+\rangle$ if X basis is chosen. She then sends the prepared state to Balvis who selects randomly between X and Z basis for measurement. Balvis's basis choice matches with Alice's basis choice

- in 25% cases
- in 33% cases
- ◉ in 50% cases
- always

Question 2 — 1 / 1 pts

In Privacy Amplification, Asja and Balvis pair up their bits by agreed random permutation and announce the addition modulo 2 of their paired bits.

- True
- ◉ False

Question 3

1 / 1 pts

Asja and Balvis pair up their bits by agreed random permutation. BB84 is secure only if this random permutation is kept secret.

- ○ True
- ◉ False

Question 4

1 / 1 pts

If initial bit string is: 11011010, then parity bit is

- ○ 0
- ◉ 1

Incorrect

Question 5

0 / 1 pts

Error correction and privacy amplification can work if Asja and Balvis each use their own permutations.

- ◉ True
- ○ False

Question 6

1 / 1 pts

Privacy amplification is used to

- ○ to error correction
- ○ do sifting
- ◉ eliminate Eve's information
- ○ do error estimation

Question 7

1 / 1 pts

After Privacy amplification

- ○ Espian has 50% knowledge
- ○ Randomness in the key is eliminated
- ◉ Key is totally secure

- Further information is revealed to Espian

Incorrect

Question 8

0 / 1 pts

In an error correction protocol, Asja and Balvis pair up their qubits and both do addition modulo 2 of their pairs. They then announce their result, If the result matches, they keep the 2nd bit and throw away the first bit. Asja and Balvis should randomly permute all the bits in the beginning and announce the permutation

- to eliminate eve's information
- to have different pairing than Eve.
- to distribute the errors evenly
- To correct errors

Incorrect

Question 9

0 / 1 pts

Above protocol will

- make the key to be totally error free after one round
- eliminate randomness in the key
- reveal no further information to Espian
- None of the options

Incorrect

Question 10

0 / 1 pts

In six-state protocol, Asja and Balvis do not need to announce their basis after key distribution.

- True
-
- False
-

Quiz Score: **6** out of 10