





Homework 2

Each question is worth 2 points. The multiple-choice questions have 1, 2, or 3 correct answers and will be graded as follows:

- 1 Point for marking all correct answers
- 1 Point for not marking any incorrect answers
- Not marking any answer/marketing all 4 answers will be graded as 0 points

Example:

			
<input type="checkbox"/> (correct answer)	<input checked="" type="checkbox"/> (correct answer)	<input checked="" type="checkbox"/> (correct answer)	<input checked="" type="checkbox"/> (correct answer)
<input type="checkbox"/> (wrong answer)	<input type="checkbox"/> (wrong answer)	<input checked="" type="checkbox"/> (wrong answer)	<input checked="" type="checkbox"/> (wrong answer)
<input type="checkbox"/> (correct answer)	<input checked="" type="checkbox"/> (correct answer)	<input checked="" type="checkbox"/> (correct answer)	<input checked="" type="checkbox"/> (correct answer)
<input type="checkbox"/> (wrong answer)	<input type="checkbox"/> (wrong answer)	<input type="checkbox"/> (wrong answer)	<input checked="" type="checkbox"/> (wrong answer)
(0 Points)	(2 Points)	(1 Point)	(0 Points)

Questions

1. In the Lelantus protocol, transactions are kept confidential using which of the following?

- Pedersen Commitments
- Ring Signatures
- Anonymous Sending
- Anonymous Receiving

2. Which operations are defined in the Lelantus protocol?

- Mint
- Spend
- Delete
- JoinSplit

3. What is Σ -protocol?

- A common way to construct zero-knowledge proofs.
- A three-way communication protocol (Alice to Bob/Bob to Alice/Alice to Bob) to convince Bob that Alice knows a secret.
- A two way communication protocol (Alice sends her public key A to Bob/Bob sends his public key B to Alice) to establish a shared secret $abG = aB = bA$ between the two of them.
- A signature.

4. What are examples of zero-knowledge proofs (ZKP)?

- 1-in- N Σ -protocol in the Lelantus protocol.
- Building a Bitcoin block is a ZKP of having done the work of finding a nonce.
- A signature is a proof of knowledge of the private key.
- A MimbleWimble transaction is a ZKP that the resulting Pedersen Commitment only has one generator, i.e. $X=0G+yH$, without revealing y .

5. What does it mean that a Pedersen Commitment $X = vG + sH$ opens to 0 or 1?

- $X = 0G + 0H$ or $X = 1G + 1H$
- $X = 0G + sH$ or $X = vG + 1H$
- $X = 0G + 1H$ or $X = 1G + 0H$
- $X = 0G + sH$ or $X = 1G + sH$

6. What is the purpose in Lelantus of proving that a Pedersen Commitment X opens to 0 or 1?

- We can encode the coefficient for members of an anonymity set. Only one coefficient is 1 and every other one is 0. This way, we can prove that we know one element of the set, without revealing which one.
- Such a proof is not directly used in Lelantus at all. It is just an example of a zero-knowledge proof.
- We hide the denomination of a coin by adding arbitrarily many elements, each of which has an amount of 0 or 1. A verifier does not know how much the sum is, only that the transaction is valid.
- We can prove knowledge about whether a serial number has already been used (Pedersen Commitment opens to 1) or not (Pedersen Commitment opens to 0).

7. What is not a primary use for a verifiable delay function?

- To produce public randomness
- To mitigate "grinding" attacks
- To ensure blocks are not produced faster than network propagation
- To reduce a blockchain's capacity

8. What is the primary concern with using a verifiable random function?

- The underlying mathematical assumptions
- The use of a public key infrastructure
- The ability to generate many public keys
- Byte overflows

9. What is a zero-knowledge method of probabilistically demonstrating that you know a solution to a graph coloring problem?

(Graph coloring means that you know how to assign a color (red, blue, green, yellow) to each node in a graph so that no 2 nodes connected by an edge share the same color. This was not covered in class, so please think freely.)

10. What proof technique would you use to convince someone you know the pre-image of a hash without revealing it?
