Reading Questions for Tuesday, February 19, 2019

We ask you to submit comments on the following paper by midnight Monday February 18:

- Zerocoin: Anonymous Distributed E-Cash from Bitcoin.
- Zerocash: Decentralized Anonymous Payments from Bitcoin.

Your comments should include both answers to the specific reading questions and generic response about the paper. You are welcome to include any questions you have about the paper in your comments. After submitting your own comments, you'll be able to see others' submitted comments. You can comment on others' submissions and answer raised questions on Canvas. Discussion on Canvas is strongly encouraged.

Please also read the other two links that we provided. We do not ask you to submit comments for them though.

1 Reading Questions

1. Describe Bitcoin's weakness that led to the creation of Zerocoin and how Zerocoin fixes it. Your answer should include an overview of zero-knowledge proofs and why they made sense for Zerocoin's implementation.
2. What are the differences between Zerocoin and Zerocash? What advantages and disadvantages do you think each one has?

2 Generic Response

Respond to the paper following the guidelines in the course syllabus (under "Submit Comments and Presenting Papers").