CSEC 519
Blockchain and Cryptocurrency Technologies
Homework 4
Deadline 11 June 2025 13:40
NO LATE SUBMISSIONS !!!!!!

The following questions are related to the paper **Zerocoin: Anonymous Distributed E-Cash from Bitcoin** by Miers *et al.*

1. (10 Points) **Laundry Service:** Mix networks are referred to as *laundry service* in this paper. What are the limitations/risks of these services?

2. (20 Points) **One-way Accumulators:** To check that C is in the set $(C_1, C_2, \ldots C_N)$, one can check $(C = C_1) \vee (C = C_2) \vee \ldots \vee (C = C_N)$.
   (a) What is the problem in this approach?
   (b) How one-way accumulators are useful in this case?

3. (10 Points) **Balance:** What is the aim of the *Balance* property?

4. (20 Points) **Anonymity:** Regarding the *Anonymity* game, the attackers aim to obtain $b = b'$. Here we have $b \in \{0, 1\}$ and $b' \in \{0, 1\}$. The advantage of the attacker is defined by $|Pr[b = b'] - \frac{1}{2}|$. According to this definition:
   (a) What is the highest possible advantage?
   (b) What is the advantage of the attacker that randomly guesses b'?

5. (10 Points) **Transaction Size:** What is the transaction size limit of Bitcoin and is this limit high enough to store Zerocoin's zero-knowledge proofs?

6. (10 Points) **Security in Bits:** What are the 3 bit sizes of parameters chosen by the authors? Can you justify the different security levels in these choices?

7. (10 Points) **Open Problems:** What are the 3 open problems this work leaves?

8. (10 Points) **Bonus:** List the typos you find in this paper.

The following question is related to the paper **Zerocash: Decentralized Anonymous Payments from Bitcoin** by Ben-Sasson *et al.*

1. (10 Points) What are the advantages of Zerocash compared to Zerocoin?

NOTE: You are expected to submit your homework as a single PDF file.