Ozan Cinci
2448223

HW4

Part 1:

1) Operators can steal funds, track coins, or simply go out of business, taking users' funds with them.
2)
    a)
    Such "OR proofs" have size O(N), which renders them impractical for all but small values of N
    b)
    Along with the appropriate membership witnesses for each item in the set, the spender needs only prove knowledge of one such witness. In practice, this can reduce the cost of the spender's proof to O(log N) or even constant size.

3) The Balance property aims that an attacker cannot spend more coins than s/he mints, even when s/he has access to coins and spend transactions produced by honest parties.
4)
    a) The Pr[b=b'] ranges from 0 to 1. When it is 1, the highest possible advantage happens, which is 0.5.
    b) When an attacker randomly guesses, its probability of correct guessing is 0.5. So the advantage will be calculated as 0.5-0.5 = 0. So the advantage of the attacker that randomly guesses is ZERO.
5)
No, it is not high enough to store Zerocion's zero knowledge proofs. The average transaction size of bitcoin is around 1-2KB and the limit of the transaction size is 10KB.
6) 1024 bits, 2048 bits, 3072 bits
7)
    1. The need for a double-discrete logarithm proof leads to large proof sizes and verification times.
    2. In Bitcoin, counterfeiting a coin is not computationally prohibitive, it is merely computationally costly, requiring the user to obtain control of at least 51% of the network. In ZeroCoin, it is provided that the cost of computing such a discrete log is greater than the value of a zerocoin, forging a coin is not profitable. How small this allows us to make the coins is an open question.
    3. It can facilitate money laundering by circumventing legally binding financial reporting requirements
8) Typos found are highlighted with yellow.

item in the set. The spender need only prove knowledge of one such witness. In practice, this can reduce the cost of the spender's proof to $O(log\ N)$ or even constant size.

Part 2:

1)

- Augmented privacy: It provides transaction privacy by hiding transaction details.
- Compact transactions: Its transactions' size are more compact hence smaller.
- Efficiency: It provides verification of transactions with minimal computational burden. It uses less resources.
- Faster Verification: Verification time is smaller.
- Anonymity: It hides the details of inputs and outputs. Transaction history is not visible on the blockchain. It prevents calculation of the coin amount that a user has.