Middle East Technical University Department Of Cyber Security

CSEC 519

Blockchain and Cryptocurrency Technologies

Spring 2024-2025

Fourth Assignment

Name Surname: Alkım Doğan
Student ID: 2521482

1 Zerocoin

1.1

1. Operators can steal funds.
2. Operators can track coins.
3. Operators can simply go out of business, taking users' funds with them.

1.2

1. Such proofs are called **OR** proofs, whose complexity is $\mathcal{O}(N)$ which renders them impractical for all but small values of N.
2. **One-Way accumulators** allow parties to combine many elements into a constant-sized data structure, while efficiently proving that one specific value is contained within the set. Therefore, this sentence means the complexity gets lower with this data structure. Our complexity reduces to $\mathcal{O}(logN)$

1.3

The primary aim is to prevent someone from spending more coin then he has minted even when he has access to coins and spend transactions produced by honest parties.

1.4

1.4. a)

Assume that attacker always guess the correct values. So, probability of b = b' becomes 100%. Since it is defined as $|Pr[b = b']| - 0.5$, we plug into 1 and we get $1 - 0.5 = 0.5$ as a final result. Therefore, highest possible advantage is equal to 50% mathematically.

1.4. b)

For an attacker randomly guessing, the probability of $b = b'$ becomes equal to 0.5. If we plug this value into the formula just like the above question, we would have $|0.5 - 0.5| = 0$. So, the result is 0, meaning no advantage at all.

1.5

The transaction size limit of Bitcoin is said to be 10 KB and most transactions are about 1-2 KB in the paper. Additionally, proofs produced by spend exceeds 10 KB. Therefore, Bitcoin's limit is **NOT** enough for Zerocoin's proof.

1.6

There are 1024, 2048, 3072 bits of length. They said these numbers corresponds to RSA modulus. RSA is based on integer factorization that has subexponential solution (Pollard's Rho's algorithm as far as I remember from CSEC 507). The standard for RSA is 3072 bits that corresponds to 128 bit AES security due to mentioned algorithm. The 2048 bit RSA corresponds to the 112 bit AES security. Finally, the 1024 bit RSA corresponds to the 80 bit AES security. Hence, longer the bits, more secure the system will be.

1.7

I will mention each open problem one by one briefly.

- Although their scheme is workable, the need for a double-discrete logarithm proof means larger proof sizes, longer verification time. We may say it is not very efficient and scalable as far as the paper described.
- In Bitcoin, security relies on DLP and CPU power to solve hash puzzles. Second one lead to 51% attack. These issues make system heavier in terms of computation and so on. This also means there is a trust model system that people will not collaborate to exceed 51%. Rather than this system, we can build a system with weak assumption such that the cost of computing a discrete log exceeds the value of the resulting counterfeit coins.
- Bitcoin may facilitate money laundering as we see in the lectures as well. The paper states that there may be a protocol modification so that clients maintain anonymity while demonstrating compliance with reporting requirements.

1.8

I have detected a typo in the second page of the paper.

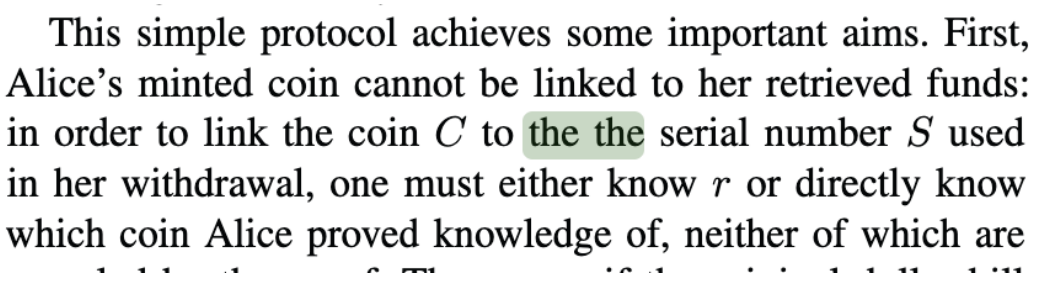
This simple protocol achieves some important aims. First, Alice's minted coin cannot be linked to her retrieved funds: in order to link the coin C to the the serial number S used in her withdrawal, one must either know r or directly know which coin Alice proved knowledge of, neither of which are

Figure 1: Double **THE** detected

2 Zerocash

2.1

- Zerocash reduces the size of transactions spending a coin by 97.7% compared to Zerocoin.
- Zerocash reduces the spend-transaction verification time by 98.6% compared to Zerocoin.
- Zerocash allows for anonymous transactions of variable amounts, which Zerocoin does not allow.
- Unlike Zerocoin, Zerocash hides transaction amounts and the values of coins held by users.
- Zerocash allows for payments to be made directly to a user's fixed address (without user interaction), which is not available in Zerocoin.