CPSC 490 Project Proposal: An Anonymous Reputation System Resistant against Tracking and Intersection Attacks

Tony Jiang and Ian Zhou
Advisor: Ennan Zhai
February 8, 2018

Abstract

AnonRep, built by Ennan Zhai and published in 2016, is a practical anonymous reputation system that allows its users to have the benefits of reputation without letting anyone, even the maintainers of the servers, track the actions of its users; users can post messages anonymously and other users can give feedback on the messages (e.g. by voting the message up or down) anonymously [1]. The system employs a variety of cryptographic primitives including verifiable shuffles and linkable ring signatures to achieve this anonymity. However, AnonRep is prone to long-term intersection attacks. A user with very high reputation may lose her anonymity because people will be able to link any message posted with high reputation to her. We fix this problem by using a blockchain-based solution in which users can post messages with with any reputation that is less than or equal to their current reputation, while still preserving the anonymity guarantees of the original AnonRep system. In this project, I will implement the blockchain-based extension and the cryptographic primitives of our proposed system.

1 Background

AnonRep is a decentralized system for anonymous reputation that operates in a series of message-and-feedback rounds that last anywhere from a few
minutes to an entire day. Each round consists of three phases: announcement, message posting, and feedback. Each user has a long-term pseudonym that is maintained by each server. Each server also stores the encrypted reputation scores of each user. They are encrypted in a manner such that no single server can decrypt the score; all of the servers are required in order to decrypt the score, so as long as at least one server is not colluding with the other servers, anonymity can be preserved.

In the announcement phase, the servers collectively create a table of encrypted one-time pseudonyms (from the clients’ long-term pseudonyms) and their respective decrypted reputation scores.

In the message posting phase, clients post messages using these one-time pseudonyms to a global message board maintained by all of the servers.

In the feedback phase, clients provide positive or negative feedback to the posted messages (such as a vote up or vote down on the reputation score of the user). We update the reputation scores before the next round begins.

A shortcoming of AnonRep is that it is prone to intersection attacks. A user with a unique reputation score, for example, one that is much higher than all the other users, has little anonymity. This is because other users will be able to link any message posted by a user with that high of a reputation to her.

Our proposed solution to this vulnerability is to tokenize reputation into a “reputation coin” on the blockchain. Users will have their reputation in different “wallets” that they use to post messages. If another user votes up a message, one of the wallets used to post the message will gain a reputation coin. If the message is downvoted, one reputation coin will be removed from one of the wallets, unless there is no more reputation left in the wallets. We will use CoinShuffle to make transactions on the blockchain anonymous.

2 Project Outline

We will take the following steps to execute our project:

1. Understand the current literature on anonymous reputation and the cryptographic primitives used in the AnonRep paper.

2. Find or implement the aforementioned cryptography libraries for use in our project.
3. Implement the original AnonRep in Python.

4. Implement the blockchain-based extension described in the background section.

5. Run analyses to determine the scalability of our system as the number of clients and servers increases.

6. If time permits, make further optimizations on AnonRep to protect against other vulnerabilities or make it faster and more scalable.

3 Deliverables

The main deliverables involve code making up the system we build and a report with our learnings, results, and future directions. I will focus more on the mathematical aspects, implementing the cryptographic primitives and blockchain aspects of the project. My main contributions will be

- A Python implementation of cryptographic primitives and algorithms that are not readily-available such as:
  - Verifiable Shuffle
  - Linkable Ring Signature
  - CoinShuffle

- A Python implementation of the blockchain environment that will be used for AnonRep.

References