COMP 4901W – Final Project

A. K. Goharshady

Release Date: April 20, 2023

Deadline: May 15, 2023 (23:59 HKT)

This project accounts for 30% of your total grade. You should submit your solution as two files, one `pdf` and one `sol`. As usual, handwritten and scanned solutions will not be accepted since the TAs might be unable to read your handwriting. However, you can draw your figures, if any, by hand. Your solution should be entirely your own work. All submissions will go through a strict plagiarism check. If we detect plagiarism, it will cause a grade of F for the whole course. The deadline is firm and no extensions can be granted.

No resubmissions are allowed for the final project.

You will get 0 points for the entire project if your code does not compile in Remix.

This is an open-ended project. Do not worry about losing a few points or not being able to achieve some of the requirements. The cut-off for an A grade in this course is NOT fixed at 90%. We expect that many of the students who will end up earning A/A+ would nevertheless be unable to solve several parts of this project and lose 10-15 points.

If you are a UG student and achieve a perfect 30/30 in this project, Amir will offer you a fully-funded MPhil+PhD position in his research group. The assumption is that no more than two students would achieve this. In the unlikely event that there are more than two perfect scores, an interview will be organized.

Background

You plan to set up a blockchain-based casino in the fictional country of Schweizerland. This casino supports only one type of bet: the bettor puts down a deposit of 1 Schweizerlandish schilling, which is conveniently equal to 0.01 ETH. With probability 0.5, the bet is won and you have to pay them 2 schillings. Similarly, with probability 0.5, the bet is lost and you get to keep their schilling.

The Schweizerlandish authorities are quite strict and they want to make sure that you cannot fraudulently control the result of the bets. So, they require you to prove to them that the bets are actually fair. However, they are also pretty open-minded (or at least they claim to be) and are willing to help you in the generation of the required random numbers. Specifically, they have heard that you have a protocol in mind in which a random number can be generated by the participation of any number n of players. The authorities require you to ensure that they always control at least $t = \lceil \frac{n}{2} + 1 \rceil$ of the players, so that the public can trust your casino. They also require your protocol to be open to the public, so that anyone can sign up and contribute to the random number generation if they wish to do so.

Unfortunately, although the public trusts the authorities, you as the casino owner cannot trust them. You worry that they might use their huge influence in the RNG process to tamper with the results and help their friends win a lot of bets in your casino.

Finally, although you are aware of the standard methods of random number generation on the blockchain, none of them really appeal to you. They are all slow and take a long time to generate even one random number. Your bettors like to see the results of their bets immediately. You cannot ask a bettor to wait for a VDF to be computed, or for many RNG participants to reveal their choices or perform secret reconstruction. They expect almost-instant results, i.e. within a few blocks.

So, you go to the authorities and propose the following scheme:

1. At the beginning of the day, we use a specialized RNG protocol with the above properties required by the authorities, to generate a random number r. However, we ensure that r is only visible to the casino and no one else has any information about it.
2. We fix a deterministic pseudo-random number generator function, e.g. the `rand()` function in a standard implementation of C, which can have any seed.
3. The casino deposits a huge amount of money in the smart contract.
4. Each bettor deposits 1 schilling for each bet and also provides a random number k of their choosing. These are recorded in the smart contract. In response, the casino uses $k + r$ as the seed and computes a random number, i.e. it performs `srand(`$k + r$`);  `x` = rand();` The casino discloses neither r nor x. It only tells the smart contract whether x is even or odd. This announcement is recorded in the contract. If x is even, the bettor has won. Otherwise, they have lost. The contract pays the bettor accordingly.
5. At the end of the day, the casino announces the value of r that was used during the day. The authorities and every bettor can verify that (i) r was really generated by the RNG process of Step 1 and was therefore not under the casino's control, and (ii) the casino did not cheat in any of the bets.
6. If any cheating is detected, it can be reported to the smart contract, which would use the casino's deposit to pay twice as much as their losses to the wronged bettors.
7. If no cheating is reported to the smart contract after a fixed deadline, or if all the reports were false, the casino can get its money back.

Your proposal is acceptable to the authorities, but they want to see more details.

Your Project

Design a protocol that solves the problem above and satisfies the following additional requirements. Submit your protocol as a single file named `protocol.pdf`, explaining its steps, the requirements it satisfies (1–7, a–j), and arguments for why it satisfies the claimed requirements. Then, implement it in Solidity and submit the code as a single file named `contract.sol`. If you cannot satisfy all the requirements, try to achieve as many of them as possible. Similarly, if you cannot implement all parts, make as much progress as possible and explain your progress in your `pdf` file. For simplicity, you can have any implementation of `srand` and `rand` that you like in your code. We will not care if these are not really pseudo-random number generators.

The additional requirements:

a. The RNG process at Step 1 above should be open to everyone for participation as players, but you have to automatically give control of at least t of the players to the authorities. You can assume that the authorities have provided you with their public key (address).
b. The result r of the RNG process at Step 1 above should only be visible to you (the casino). Ideally, it should be encrypted using your public key, so that no one else can decrypt it.
   Hint: Look into non-RSA encryption schemes and a concept called "homomorphic encryption".
c. The RNG at Step 1 should be tamper-proof. Specifically:
   - The casino should not be able to tamper with the result even if it colludes with all the players who are not controlled by the authorities.
   - The authorities should not be able to tamper with the result even if they collude with all the players who are not controlled by the casino. You can assume that at least one RNG player is controlled by the casino.
   - No one else should be able to tamper with the result, including blockchain miners.
d. The RNG at Step 1 should be unpredictable. No one, including the casino and the authorities, should be able to guess r or obtain any information about it before it is delivered in an encrypted format to the casino. Similarly, at any time strictly before the casino's announcement at Step 5, no one other than the casino should be able to find any information about r. This must hold even if the authorities collude with all non-casino players to predict r. We assume the casino would not leak r before Step 5 since it would cause them to lose all the bets.
e. The value r should be generated uniformly at random. You can assume that r is supposed be a 16-bit integer. Thus, each value between 0 and $2^{16} - 1$ should have the same probability 2^{-16} of being the chosen r. If you wish, you can also use larger bounds for r.
f. The RNG of Step 1 should not ever fail. You can assume that the players controlled by the authorities will perform all steps of the RNG to completion and that they will not cheat in any detectable way. However, if your protocol allows the authorities to cheat and not be detected, they might choose to do so. On the other hand, you cannot assume anything about the other RNG players.
g. All players in the RNG should receive incentive payments that ensures they are incentivized to honestly follow the protocol until its completion. These payments should come from the casino's deposit.
h. In Step 5, the casino should be able to reveal the value of r and prove to everyone that the revealed value is the same r that was generated in Step 1. Any cheating by the casino should also be detectable. Such cheating should be provable to the contract so that it can penalize the casino.
i. The deposit put by the casino should be large enough to ensure the bettors can be compensated twice the money they lost in case the casino cheats.
j. Your smart contract should not have any of the vulnerabilities discussed in the lectures.