COMP 4901W - 最终项目

A.K. Goharshady 发布日

期：2012年4月20日2023年

4月20日

截止日期：2023年5月15日（香港时间

23:59）。

这个项目占你总成绩的30%。你应该以两个文件的形式提交你的解决方案，一个PDF文件和一个SOL文件。像往常一样，手写的和扫描的解决方案将不被接受，因为助教可能无法阅读你的笔迹。然而，你可以用手画出你的数字，如果有的话。你的解决方案应该完全是你自己的作品。所有提交的材料都将经过严格的抄袭检查。如果我们发现有抄袭行为，将导致整个课程的成绩为F。截止日期是确定的，不允许延期。

最终项目不允许重新提交。

如果你的代码不能在Remix中编译，你的整个项目将得到0分。

这是一个开放式的项目。不要担心失去几分或无法达到某些要求。本课程的A级分数线并不固定为90%。我们预计，许多最终获得A/A+的学生仍将无法解决这个项目的几个部分，并失去10-15分。

如果你是一名本科生，并且在这个项目中取得了30/30的完美成绩，阿米尔将为你提供他的研究小组中一个全额资助的硕士+博士职位。我们的假设是，不会有超过两名学生达到这一目标。如果不太可能有两个以上的满分，我们将组织一次面试。

背景介绍

你计划在虚构的国家Schweizerland建立一个基于区块链的赌场。这个赌场只支持一种类型的赌注：投注者投入1瑞士先令的存款，方便地说，这相当于0.01个ETH。在概率为0.5的情况下，赌注获胜，你必须支付给他们2先令。同样，在概率为0.5的情况下，赌注输了，你可以保留他们的先令。

瑞士当局相当严格，他们希望确保你不能以欺诈方式控制投注结果。因此，他们要求你向他们证明赌注确实是公平的。然而，他们也相当开明（或者至少他们声称开明），愿意帮助你生成所需的随机数。具体来说，他们听说你有一个协议，其中随机数可以由任何数量的n个玩家参与生成。当局要求你确保他们始终控制着至少$t = \lfloor \frac{n}{2} + 1 \rfloor$的玩家，这样公众才能信任你的赌场。他们还要求你的协议对公众开放，这样任何人都可以注册并为随机数的生成做出贡献，如果他们愿意这样做。

不幸的是，虽然公众信任当局，但你作为赌场老板却不能信任他们。你担心他们会利用他们在RNG过程中的巨大影响力来篡改结果，帮助他们的朋友在你的赌场中赢得大量的赌注。

最后，尽管你知道区块链上随机数生成的标准方法，但它们都没有真正吸引你。它们都很慢，甚至需要很长的时间来生成一个随机数。你的投注者喜欢立即看到他们的投注结果。你不能要求投注者等待VDF的计算，或等待许多RNG参与者透露他们的选择或进行秘密重建。他们期望几乎是即时的结果，即在几个区块内。

因此，你去找当局，提出以下计划：

1. 在一天的开始，我们使用一个专门的RNG协议，具有当局要求的上述属性，生成一个随机数r。然而，我们确保r只对赌场可见，没有其他人有任何信息。
2. 我们固定一个确定性的伪随机数发生器函数，例如C语言标准实现中的rand()函数，它可以有任何种子。
3. 赌场在智能合约中存入巨额资金。
4. 每个下注者为每个赌注存入1先令，同时提供一个他们选择的随机数k。这些都被记录在智能合约中。作为回应，赌场使用$k + r$作为种子并计算一个随机数，即执行srand($k + r$); x = rand(); 赌场既不透露r也不透露x，它只告诉智能合约x是偶数还是奇数。这一公告被记录在合同中。如果x是偶数，投注者就赢了。否则，他们就输了。合同会相应地支付给赌客。
5. 在一天结束时，赌场会公布当天使用的r值。当局和每个投注者都可以验证：（i）r确实是由步骤1的RNG过程产生的，因此不在赌场的控制之下；（ii）赌场没有在任何投注中作弊。
6. 如果发现任何作弊行为，可以向智能合约报告，智能合约将使用赌场的押金向受损失的

投注者支付两倍于其损失的金额。

7. 如果在固定期限后没有人向智能合约报告作弊行为，或者所有报告都是假的，那么赌场可以拿回自己的钱。

你的建议对当局来说是可以接受的，但他们希望看到更多细节。

您的项目

设计一个能解决上述问题并满足以下额外要求的协议。将你的协议作为一个名为protocol.pdf的文件提交，解释它的步骤，它所满足的要求（1-7，a-j），以及它为什么满足所要求的论据。然后，用Solidity实现它，并将代码作为一个名为contract.sol的文件提交。如果你不能满足所有的要求，那就尽可能多地实现它们。同样地，如果你不能实现所有的部分，尽可能地取得进展，并在你的pdf文件中解释你的进展。为了简单起见，你的代码中可以有任何你喜欢的srand和rand的实现。如果这些不是真正的伪随机数生成器，我们也不会在意。

额外的要求：

a. 上述步骤1的RNG过程应该对每个人开放，让他们作为玩家参与，但你必须自动将至少t个玩家的控制权交给当局。你可以假设当局已经向你提供了他们的公钥（地址）。

b. 上述步骤1的RNG过程的结果r应该只对你（赌场）可见。理想情况下，它应该使用你的公钥进行加密，这样其他人就无法解密。
提示：研究一下非RSA加密方案和一个叫做 "同态加密 "的概念。

c. 步骤1的RNG应该是防篡改的。具体而言：
   - 赌场即使与所有不受当局控制的玩家勾结，也不应该对结果进行篡改。
   - 即使当局与所有不受赌场控制的玩家勾结，也应该无法篡改结果。你可以假设至少有一个RNG玩家是被赌场控制的。
   - 其他任何人都不应该能够篡改结果，包括区块链矿工。

d. 步骤1的RNG应该是不可预测的。任何人，包括赌场和当局，都不应该能够猜到r，或者在它以加密的形式传递给赌场之前获得任何相关信息。同样地，在严格意义上的赌场在步骤5宣布之前的任何时候，除了赌场之外，没有人能够找到关于r的任何信息。即使当局与所有非赌场玩家串通起来预测r，这一点也必须成立。我们假设赌场不会在第5步之前泄露r，因为这将导致他们失去所有的赌注。

e. 数值r应该是均匀地随机生成的。你可以假设r应该是一个16位的整数。因此，在0和2^{16} - 1之间的每个值应该有相同的概率2^{-16}，成为所选择的r。如果你愿意，你也可以对r使用更大的界限。

f. 步骤1的RNG不应该失败。你可以假设由当局控制的玩家会完成RNG的所有步骤，他们不会以任何可检测的方式作弊。然而，如果你的协议允许当局作弊而不被发现，他们可能会选择这样做。另一方面，你不能对其他RNG玩家做任何假设。

g. RNG中的所有玩家都应该得到奖励金，确保他们被激励诚实地遵守协议，直到完成协议。这些款项应该来自赌场的存款。

h. 在步骤5中，赌场应该能够揭示r的价值，并向大家证明所揭示的价值与步骤1中产生的r相同

。赌场的任何作弊行为也应该可以被发现。这种作弊行为应该可以向合同证明，以便它可以对赌场进行惩罚。

i. 赌场投入的保证金应该足够大，以确保在赌场作弊的情况下，投注者可以得到两倍于他们损失的资金赔偿。
j. 你的智能合约不应该有讲座中所讨论的任何漏洞。