- day1-lecture.pdf + day1-recording
- lecture_day2.pdf + day2-recording
- lecture-3.pdf + day3-recording
- lecture-day4.pdf + day4-recording

  Guest lectures-
  BlockEthDev on secure circuits

Quizzes with answers-:
All code sources. Audit challenge starts in Day5 sources.
https://github.com/Veridise/zk-secureum-workshop-23-quiz-sources

1. Quiz1
2. Quiz2
3. Quiz3
4. Quiz4
5. Audit Challenge description -: Welcome to the final day of the ZK Secureum workshop! At this point you should be fairly familiar with ZK concepts and potential bugs that might occur during development. So, let's put that knowledge to the test. For this challenge, you are called to audit a protocol that simultaneously supports anonymously signaling, (à la. Semaphore from Ethereum Foundation) and anonymous NFT auctions. However, due to a tight deadline, our engineers had to pull several all-nighters to finish the project. And as we all know, a by-product of all-nighters is a good amount of bugs. Can you prevent our engineers from becoming a headline in rekt? If so, please upload an audit report with all the issues you can spot in the code (both the circuits and the contracts). Make sure to mark each issue with one of the following severity levels and also describe its impact:
   - Critical: the project will definitely get hacked upon deployment.
   - High: the project will likely get hacked, but an attacker will need some luck on their side.
   - Medium: the project will likely get hacked, but the impact of the hack won't be detrimental.
   - Low: the project might get hacked, but the attack surface and impact are minimal.
   - Warning: the project won't get hacked, but code quality can be improved.
   - Info: the project won't get hacked, but the developers follow bad engineering practices.

   And don't forget all the tools you have in your arsenal. Use you SaaS account wisely Audit Report has 100 points