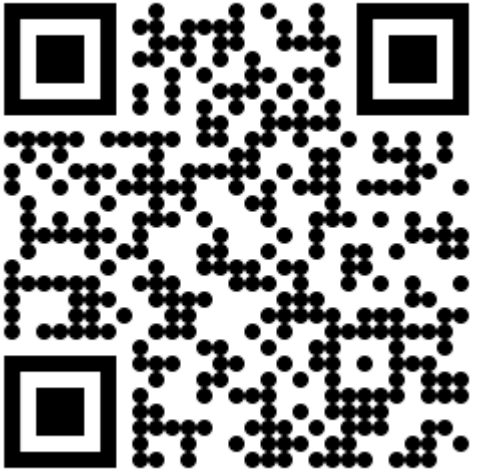
You can already start working!

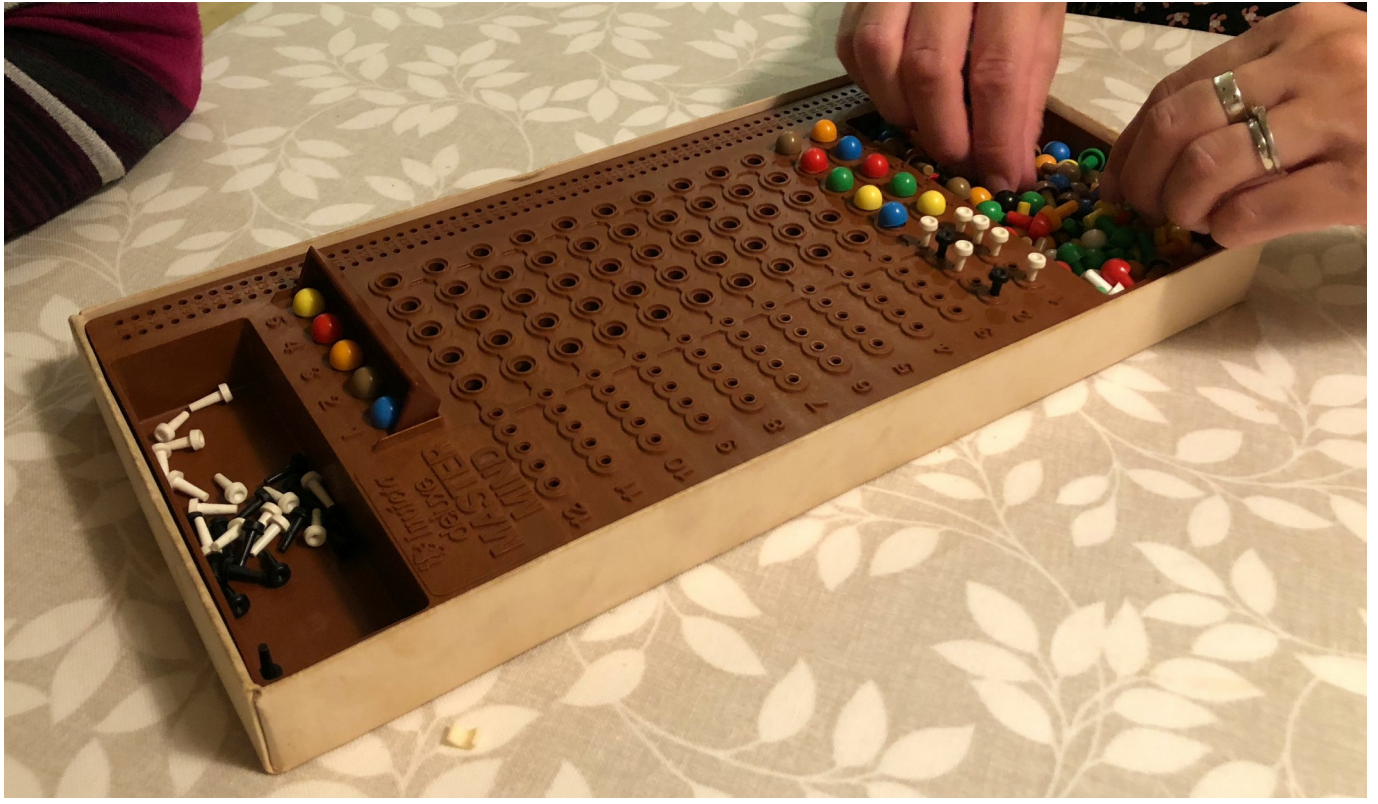


https://n.ethz.ch/~kklier/download/zkp/

Zero-Knowledge Proofs

Exercises Week 13: Circom/SnarkJS Part III

Last Time: Designing a Circuit for Mastermind

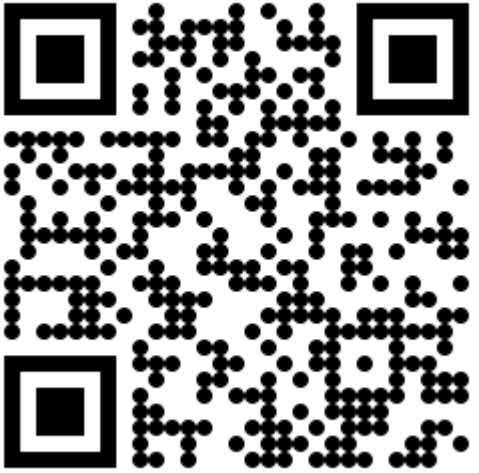


Today: App for Playing the Game

```
Usage: mastermind [options] [command]

App for playing provably secure Mastermind

Options:
  -V, --version                   output the version number
  -h, --help                      display help for command

Commands:
  set_zkey_file <file>            Takes a path to the zkey file (circuit
                                  specific)
  set_vkey_file <file>            Takes a path to the verification key file
                                  (circuit specific)
  init                            Initializes the game by setting the random
                                  color sequence and committing to it.

  compute_proof <guess...>
  verify <proof> <publicSignals>  takes a proof and public signals als
                                  stringified JSON objects and verifies the
                                  SNARK
  help [command]                  display help for command
```

For Your Convenience

- Files from last time (e.g. Docker Image)
- Template files for Mastermind NodeJS App
- README.html



https://n.ethz.ch/~kklier/download/zkp/

Roadmap for Today

https://n.ethz.ch/~kklier/download/zkp/

1) Optional: Form groups of 2–3 people

2) Copy `mastermind_app/` to local files

3) Complete templates in `index.js`

4) Play the game :D