Zero-knowledge Sudoku

Graduate

Leonardo Ravani

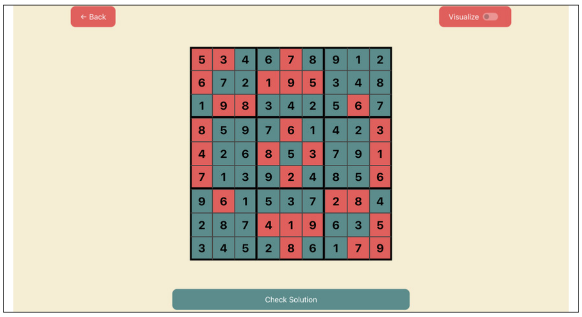
Tobias Kistler

Definition of Task: Imagine sharing that you know a secret without revealing the secret itself. This is what zero-knowledge proofs (ZKPs) aim to do. With ZKP you have a prover who claims knowledge of something and a verifier who checks this claim. A practical example would be proving that you are not color blind without mentioning it. If a verifier has two identical trinkets that only differ in color, he can show you one at a time, switching which one behind his back. You will be able to tell if he switched them, based on their color. The goal of this project is to further explore current technologies revolving around ZKP and understand possible adaptations to a web-application. In this case, a website where you can solve puzzles.

Approach: An online puzzle application was created that keeps the solutions of individual users safe using ZKP. A user can solve a logic-based puzzle like Binairo or Sudoku and check the validity of their solution without it ever leaving the device or being stored on a server by sharing only a ZKP of the solution. To further strengthen the security, the following two checks have been implemented. Firstly making sure the solution matches the original puzzle, and secondly matching the userID that generated the proof to the user that sent the proof. These checks prevent reusing a proof to “solve” other puzzles or for them to be reused by another user.
To implement this application, different ZKP frameworks were considered. Circom and snarkjs were selected because of their active development, clear documentation and good web development capabilities.

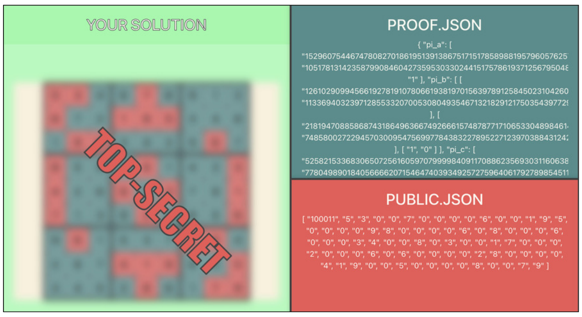
Result: The final result is a secure application that demonstrates how ZKPs can be utilized realistically for a practical use case beyond cryptocurrencies. This highlights their broader potential in secure digital interactions. In most applications, the impact of ZKPs is not visible. The ZKP-Puzzles application aims to visualize how ZKPs enhance data security, which is something that is usually hidden from the user.

A solved sudoku puzzle. The cells with a red background colour signify the original, unsolved puzzle.
Own presentment



5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

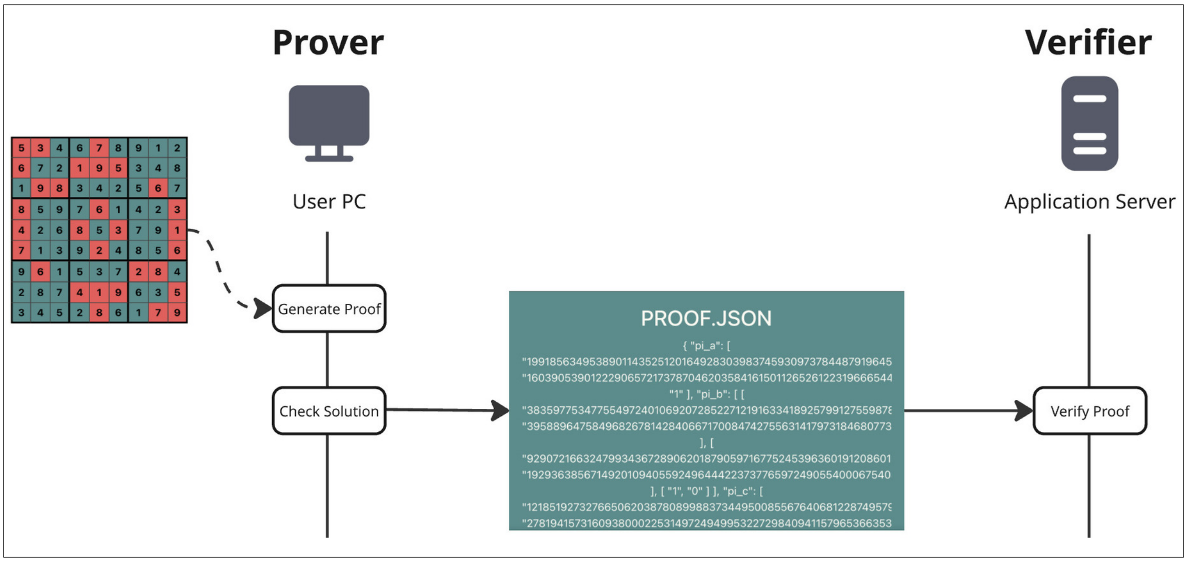
When checking the solution with "visualize" enabled the proof- and public-json are displayed.
Own presentment



```
{ "pi_a": [
"15296075446747808270186195139138675171517858988195796057625
"10517813142358799084604273595303302441517578619371256795048
"1" ], "pi_b": [ [
"12610290994566192781910780661938197015639789125845023104260
"11336940323971285533207005308049354671321829121750354397729
], [
"21819470885868743186496366749266615748787717106533048984614
"74858002722945703009547569977843832278952271239703884312427
], [ "1", "0" ] ], "pi_c": [
"52582153368306507256160597079999840911708862356930311606388
"77804989018405666207154647403934925727596406179278985451
```

```
[ "100011", "5", "3", "0", "0", "7", "0", "0", "0", "0", "6", "0", "0", "1", "9", "5",
"0", "0", "0", "0", "9", "8", "0", "0", "0", "0", "6", "0", "8", "0", "0", "0", "6",
"0", "0", "0", "3", "4", "0", "0", "8", "0", "3", "0", "0", "1", "7", "0", "0", "0",
"2", "0", "0", "0", "6", "0", "6", "0", "0", "0", "0", "2", "8", "0", "0", "0", "0",
"4", "1", "9", "0", "0", "5", "0", "0", "0", "0", "8", "0", "0", "7", "9" ]
```

A simplified flow diagram of the ZKP process. From generating to verifying the proof.
Own presentment



5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

```
{ "pi_a": [
"19918563495389011435251201649283039837459309737844879196458
"16039053901222906572173787046203584161501126526122319666544
"1" ], "pi_b": [ [
"38359775347755497240106920728522712191633418925799127559878
"39588964758496826781428406671700847427556314179731846807733
], [
"92907216632479934367289062018790597167752453963601912086018
"19293638567149201094055924964442237377659724905540006754
], [ "1", "0" ] ], "pi_c": [
"121851927327665062038780899883734495008556764068122874957
"27819415731609380002253149724949953227298409411579653663533
```

Advisor
Dr. Daniel Tschudi

Co-Examiner
Dr. Chen-Da Liu Zhang, Web 3.0 Technologies Foundation

Subject Area
Cyber Security