Sudoku verification with characteristic polynomials

Vadym Fedyukovych

Platin.io

IECMSA 2018

About

Sudoku is an example. Yes/No verification, NOTHING else.
Compare with electronic signatures:
private key is hidden while verification.

Interactive and non-interactive proof systems,
Cabbage-goat-wolf-boat complexity puzzle.
Schnorr protocol and zk-SNARKs.
Decision making by rejecting alternative hypothesis.
Negligible error of accepting a false statement.

Reduced complexity with characteristic polynomials:
sets, graphs..

Problem statement and state of the art

Platin
Proof of Location Blockchain

Conflicting interests and solution:
buyer verifies that solution is valid and matches the puzzle,
without access to solution.

Maxwell-Bowe pioneering sudoku verification:
`https://github.com/zcash-hackworks/pay-to-sudoku`
`https://bitcoincore.org/en/2016/02/26/`
`zero-knowledge-contingent-payments-announcement/`

How to explain zero-knowledge protocols to your children
`http://pages.cs.wisc.edu/~mkowalcz/628.pdf`
The Incredible Machine
`https://medium.com/qed-it/the-incredible-machine-4d1270d7363a`

Characteristic polynomials and reducing complexity

Platin
Proof of Location Blockchain

For a set $\mathcal{S}$ of finite field elements, consider polynomial representation:

$$f(z) = \prod_{s \in \mathcal{S}} (1 + zs)$$

Set equality is verified as equivalent polynomials. Polynomial equivalence is verified as equality as a random point.
Sudoku solution validity as set equality for all rows, columns, blocks:
`http://www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO/`

Implementation
`https://github.com/vadym-f/Sudoku_solvability_proof`
Circuit complexity is $5N^4$ field multiplication gates,
for a puzzle of $N^2 \times N^2$.

Conclusion

Platin
Proof of Location Blockchain

Verification with Yes/No only
Characteristic polynomials as intermediate language
Implemented and on github