7th International Eurasian Conference on Mathematical Sciences and Applications (IECMSA-2018), August 28-31, 2018, Kyiv, Ukraine

SUDOKU VERIFICATION WITH CHARACTERISTIC POLYNOMIALS

Vadym Fedyukovych [1]

Abstract. Sudoku solution verification was demonstrated [1] at Bitcoin workshop, Financial Crypto 2016. This verification is solving a conflict of interests: seller wants to send his solution only after receiving the payment, and buyer wants to be sure solution is valid before he pays. This conflict was resolved with a SNARK proof and a pay-to-script transaction [2]. The key property of this proof is, solution validity can be verified in a way that solution itself is not available to the verifying party.

Polynomial representation was shown useful for proving statements about graphs, in particular, for verifying equivalent statements about characteristic polynomials. Interactive proof systems of reduced communication complexity were constructed [3, 4] that could be considered an extension of Schnorr proof with higher degrees of the challenge of verifier. SNARKs is recent development [5] in non-interactive proofs, and a core part of Zcash coins system.

To investigate applicability of polynomial representation idea in the constext of SNARKs, we introduce polynomial representation for Sudoku solution. This representation extends solution verification originally introduced at [6]. We test validity of each set representing all rows, columns, and blocks of the solution with characteristic polynomials. We test that each such polynomial is equivalent to the pre-defined polynomial produced from the expected set. We introduce an R1CS circuit for verifying whether solution is valid and whether it matches the puzzle. A SNARK proof can be produced with this circuit, with sudoku solution serving as the witness. Unlike Bowe-Maxwell, our circuit only does two verifications as stated, and could be extended to also test hash pre-image serving as the encryption key. Our circuit complexity is $5N^4 + 3N^2$ constraints (multiplication gates) for Sudoku instance of $N^2 \times N^2$ size. We confirm our analysis by implementing this ciruit [7] with libsnark [8]. We conclude that polynomial representations could be benefitial in the context of non-interactive proof systems in terms of reduced circuit complexity.

Keyword: Set characteristic polynomial, Non-interactive proof system, Zero knowledge.
AMS 2010: 11B34, 03F99.

References

[1] `https://github.com/zcash-hackworks/pay-to-sudoku`

[2] `https://bitcoincore.org/en/2016/02/26/zero-knowledge-contingent-payments-announcement/`

[3] G. Di Crescenzo, V. Fedyukovych, Zero-knowledge proofs via polynomial representations, International Conference on Mathematical Foundations of Computer Science, 335-347, 2012.

[4] V. Fedyukovych, An argument for Hamiltonicity, Cryptology ePrint Archive, Report 2008/363, 2008.

[5] R. Gennaro, C. Gentry, B. Parno, M. Raykova, Quadratic span programs and succinct NIZKs without PCPs, EUROCRYPT 2013.

[6] R. Gradwohl, M. Naor, B. Pinkas, G.N. Rothblum, Cryptographic and physical zero-knowledge proof systems for solutions of sudoku puzzles, International Conference on Fun with Algorithms, 166-182, 2007.

[7] `https://github.com/vadym-f/Sudoku_solvability_proof`

[8] `https://github.com/scipr-lab/libsnark`

[1] Platin.io, Kiev, Ukraine, vadym dot fedyukovych via gmail.com