Private verification from ancient caves to sigma protocols to SNARKs

Vadym Fedyukovych

Platin.io

IFIP Summer School on Privacy and Identity Management
2018

Easy introduction into zero knowledge and non-interactive proofs

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`

Witness indistinguishable and witness hiding protocols
U Feige, A Shamir.

Zero knowledge definition:
An algorithm exists producing indistinguishable simulated transcript.

Schnorr protocol

Common: group generator g, public key p.
Private input: secret x such that $p = g^x$.
Prover response is *a linear polynomial* in challenge.

1. Initial random α

$$u = g^{\alpha}$$

2. Random challenge of Verifier c
3. Response of the Prover

$$r = cx + \alpha$$

4. Verifier accepts if

$$g^r p^{-c} = u$$

'Special soundness' is a single acceptable choice of c for an 'arbitrary' prover.

Quadratic in challenge of Verifier

Distance from (x_n, y_n) to (x_l, y_l) is at most d:
(Lagrange theorem on four squares)

$$d^2 - ((x_n - x_l)^2 + (y_n - y_l)^2) = \sum_{j=1}^{4} a_j^2 \quad (1)$$

Replace secret location (x_n, y_n) and difference a_j
with responses of Schnorr protocol

$$z^2 d^2 - (((zx_n + \beta_x) - zx_l)^2 + ((zy_n + \beta_y) - zy_l)^2) - \sum_{j=1}^{4} (za_j + \alpha_j)^2$$
$$= z^2 \times 0 + \ldots \quad (2)$$

. . . and then pick some $z = c$ at random as the challenge.
Number of acceptable choices of c is bounded by degree of verification polynomial.

Set characteristic polynomial

Consider a multi-set S of ring elements.
Definition: set characteristic polynomial is

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

Informal: a product of relatively prime polynomials.
Applicability for proving statements, like a set of user attributes, or a set of cards covering particular sudoku row, column or block.

Graph characteristic polynomial for proving graph isomorphism, colorability, hamiltonicity, 'friends' connectivity in social networks (with hidden identity).

A bird-view of SNARKs

- Statement as a circuit (an input for library functions)
- From circuit to polynomial divisibility. Quotient polynomial as the witness.
- Vefifying divisibility relation at a random point. “Toxic waste” is a hidden argument value chosen at random.

1. Having a circuit, produce proving and verifying public keys.
2. Having proving key and wire assignments, produce a proof.
3. Verify SNARK proof with the other public key.

SNARK circuit and deciding sudoku solution

'Reference' set of cards, numbered $1 \ldots N^2$ for a $N^2 \times N^2$ sudoku.
`http://www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO/`
Testing equality of each set to the reference set, as equivalent characteristic polynomials. Evaluating polynomials at a random point.

This circuit was implemented with libsnark:
`https://github.com/vadym-f/Sudoku_solvability_proof`
Circuit complexity is $5N^4$ field multiplication gates.

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/`

Thank you! Questions time

Platin
Proof of Location Blockchain

- Definitions and Schnorr protocol
- Higher degree in challenge. Case of 'less than' with distance.
- SNARKs; verifying solution with set characteristic polynomials for sudoku rows, columns, blocks.