Cryptography is..

confidentiality (encryption),
integrity (message was not changed - signatures and MAC-codes),
non-repudiation (who signed this message? - PKI),
selective disclosure including anonymity (privacy, GDPR)
traffic hiding (onion routing, tor) . . .
Public-key and secret-key systems.

Interactive proof systems - verifying statements about secrets.
Zero knowledge. Non-interactive proofs. Proof of location - Platin.

Top news in 2017 - Bitcoin, blockchain, other coins.
Public keys and signatures as spending authorization in Bitcoin.
zkSNARK proofs in blockchain for anonimity, Zcash coins.

Interactive proof systems

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

Quantum proofs, T.Vidick and J.Watrous
https://arxiv.org/pdf/1610.01664

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

$$u = g^{\alpha} \pmod{\text{prime modulus}}$$

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

$$r = cx + \alpha \pmod{\text{prime group order}}$$

4. Verifier accepts if

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

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

SNARKs and polynomial representation

Sudoku solution verification

`https://github.com/vadym-f/Sudoku_solvability_proof`

IFIP Summer School

`https://www.ifip-summerschool.org/programme/`

Quantum Cryptography is..

- *Producing common key* by two parties communicating over a quantum+classical channels. 'True' random numbers.
  Measurement in 'the same' and 'wrong' basis.
  Measuring squeezed states and sieving for small-error cases.
- *Algorithms for quantum computers* for popular signature and encryption schemes: factorization and discrete logarithm, including elliptic curves. Shor algorithm. Zoo of algorithms.
- *Quantum-resistant schemes* replacing factorization and DL: lattices, isogenies of elliptic curves, multivariate,
  with no known fast algorithms for quantum computers.
  Hierarchy of small subgroups in 'isogeny' schemes,
  points map as a private key and curve equation as public key.
  Vélu formulae for calculating the map.