

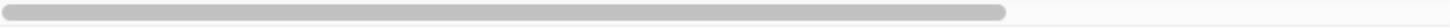
News

1. I will be gone this Wednesday (10) and Thursday (11th).
2. "By storing the passwords in clear text, the company knowingly violated its duty to ensure data security in the processing of personal data," and was fined E20k. EU court has claimed that the storage of a "message digest" that uniquely identifies a user is a violation of GDPR.
3. Fake fingerprints can unlock a smartphone.
https://motherboard.vice.com/en_us/article/bjenyd/researchers-created-fake-master-fingerprints-to-unlock-smartphones
4. Webauthn standard for site access.

zk-SNARKs

1. The acronym zk-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," and refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier.
2. What is it - cave
3. Overview of how it will all work

Steps in a General Purpose zk-SNARK

1. Computation
 2. Algebraic Circuit
 3. Rank 1 Constraint System (R1CS)
 4. Quadratic Arithmetic Program (QAP)
 5. Linear PCP: provers are restricted to computing linear (or affine) functions of mess
 6. Linear Interactive Proof
 7. zk-SNARK
- 

Mini Sudoku Example

Sudoku

Solving a Sudoku puzzle is equivalent to deciding whether there is a valid graph vertex coloring using colors, where $k = n^2$ in your $n^2 \times n^2$ Sudoku instance. The graph coloring problem is known to be NP-complete for values of $k > 2$, so 9x9 Sudoku is still hard.

Also Sudoku have a single unique solution.

[]	[2]
[1]	[]

[]	[3]
[4]	[]

Sudoku Solved

[3		4]	[2		1]
[1		2]	[4		3]

[2		1]	[3		4]
[4		3]	[1		2]

Questions that can be asked: 1. What is the (random substituted) original puzzle? 2. What is the (r.s.) values for a 4x4 block? (And the block that I would like to see) 3. What are the (r.s.) values for a column? 4. What are the (r.s.) values for a row?

Random Substitution:

1 -> 4
 4 -> 2
 2 -> 3
 3 -> 1

For row 2?

My Solution:

[1		2]	[4		3]
---	---	--	---	---	---	---	--	---	---

With substitutions?

[4 | 3] [2 | 1]

Was anything given away?

Keep asking until you are satisfied that the solver has a solution.

References

1. <https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6>