How to prove you know something (without saying it)

Presenter: Clément Humbert

Joint research between C4DT: Linus Gasser, Carine Dengler, Ahmed Elghareeb

And SICPA: Luca Multazzu, Darko Kulic

Plan

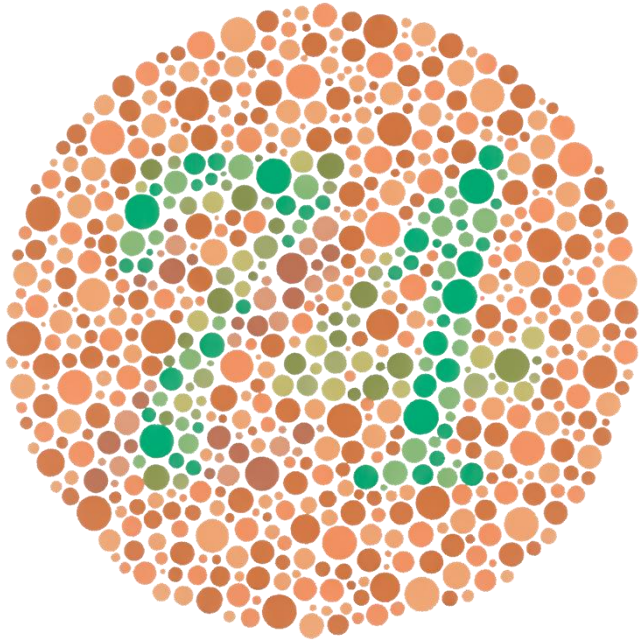
- What are ZKPs ?
- What can we do with ZKPs ?
- What are we using ZKPs for ?

What are ZKPs ?

Zero-Knowledge Poodles for dummies

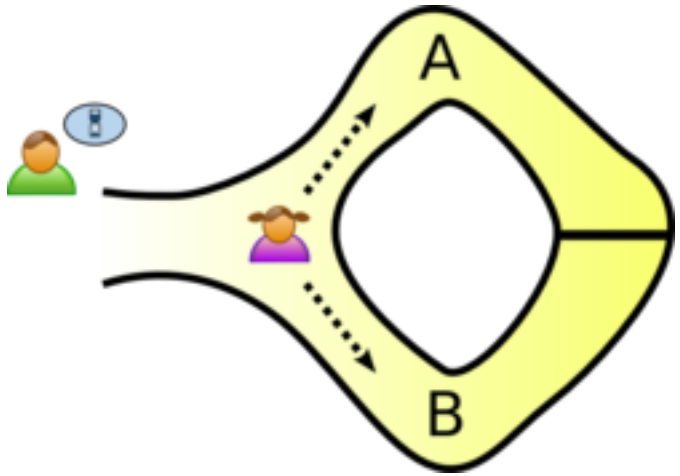
“It’s magic” – and other examples

- **Colored balls**
- Cave’s password
- Where’s waldo
- Peggy’s red card



“It’s magic” – and other examples

- Colored balls
- **Cave’s password**
- Where’s waldo
- Peggy’s red card

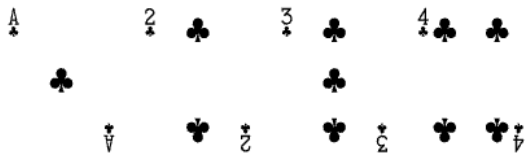


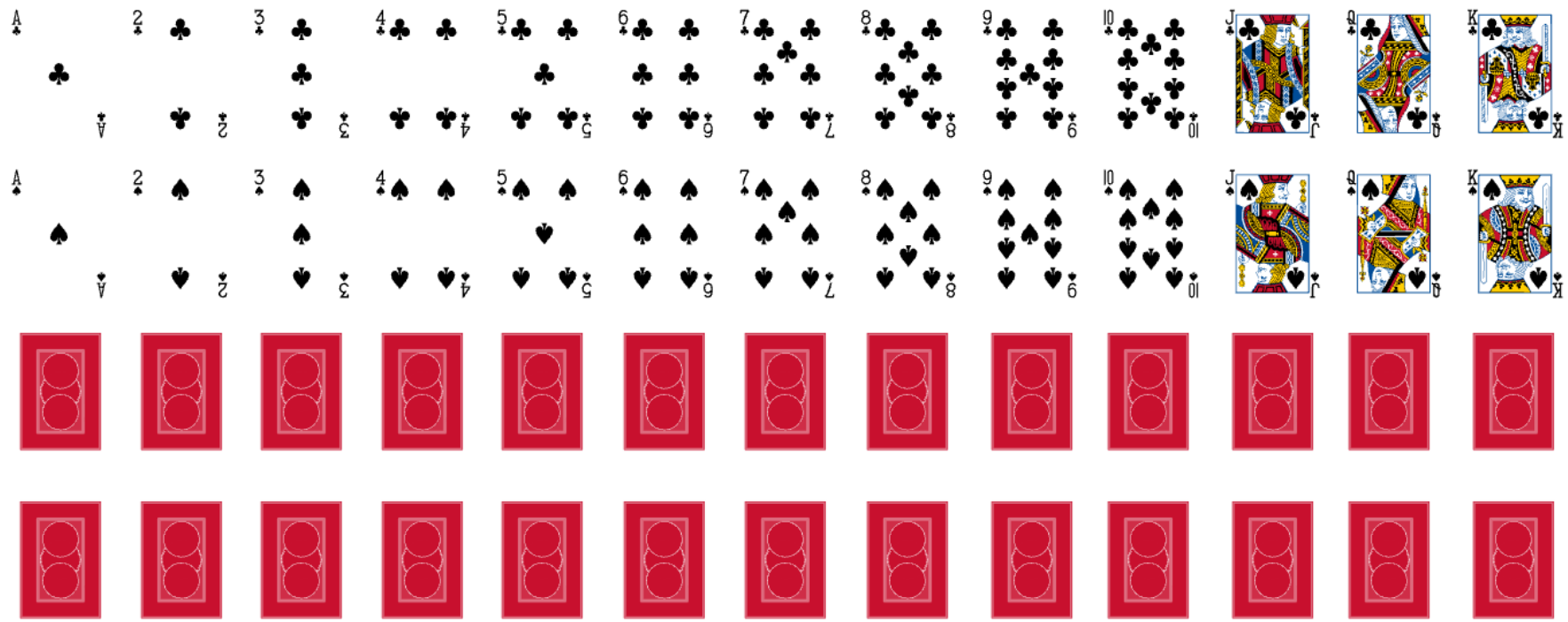
“It’s magic” – and other examples

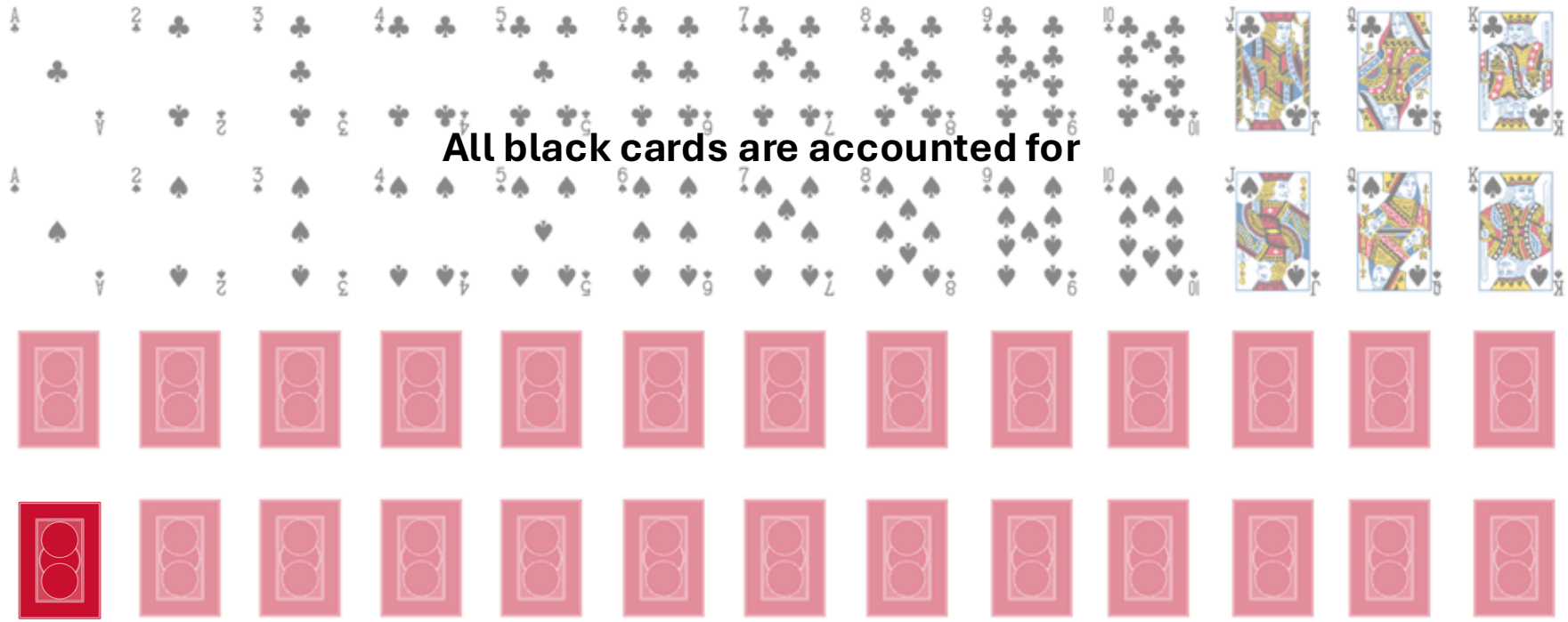
- Colored balls
- Cave’s password
- **Where’s waldo**
- Peggy’s red card

“It’s magic” – and other examples

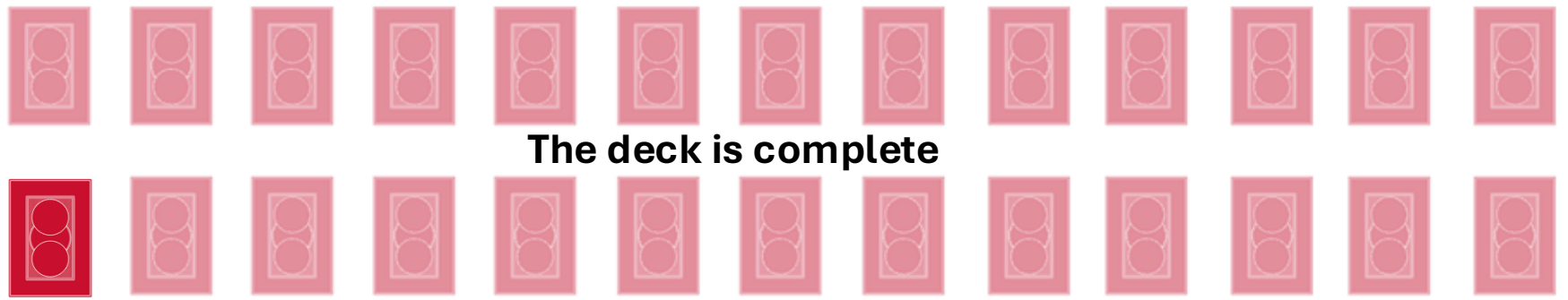
- Colored balls
- Cave’s password
- Where’s waldo
- **Peggy’s red card**





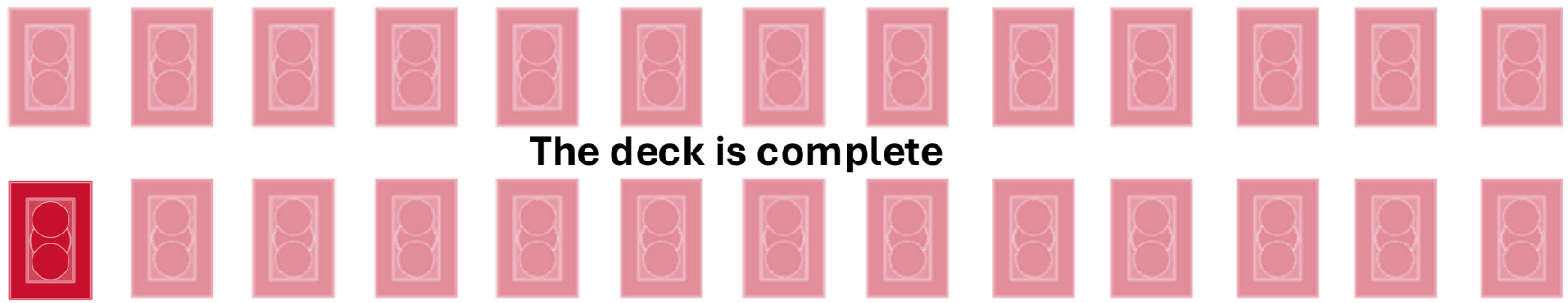

All black cards are accounted for

All black cards are accounted for



The deck is complete

All black cards are accounted for



The deck is complete

Peggy’s card is face down with the other red cards

What is a ZKP ?

A ZKP is an interactive protocol in which a prover tries to convince a verifier that a statement is true without revealing more than the statement and its truth value.

- **Completeness**: the verifier will always be convinced if the statement is indeed true.
- **Soundness**: the prover cannot produce a proof that the statement is true if it’s not.
- **Zero-Knowledge**: the interaction does not reveal more information than the statement’s truth value.

Peggy's cards properties

- **Completeness** After the protocol has ended, if Peggy has a red card, Victor can see that all the black cards in the deck have been drawn and is convinced that Peggy has a red card.
- **Soundness** If Peggy is cheating, she'll be unable to produce all the black cards for Victor to count. There's no chance she can convince Victor.
- **Zero-Knowledge** Thanks to red cards being kept face down, Victor does not learn anything more about Peggy's card than its color. This holds no matter how many time the protocol is repeated

What can we do with ZKPs ?

Collect them like they’re Pokémons

zkVMs, Smart Contracts, B[redacted]kch[redacted]n

- **ZCash** uses ZKPs to anonymize senders, recipients and transacted amount while retaining proof of validity of transactions.
- **zkVMs** are virtual machines that create a proof of correct execution for the programs they execute. Verifiers can ensure correct execution with less work than redoing the computation.
- **Transactions rollups** bundle the correctness of a bunch of transactions into a proof that requires less work for verifier.

Digital identity, digital cash, supply chain

- **Digital identity** can make use of ZKPs to allow identity-holders to prove statements about themselves without oversharing information.
- **Digital cash** can use ZKPs to ensure compliance to cash transaction regulations without compromising the privacy guarantees of cash.
- **Supply chain** can use ZKPs to prove compliance to industry and market regulations without exposing sensitive business information.

Marketing

Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly

https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/

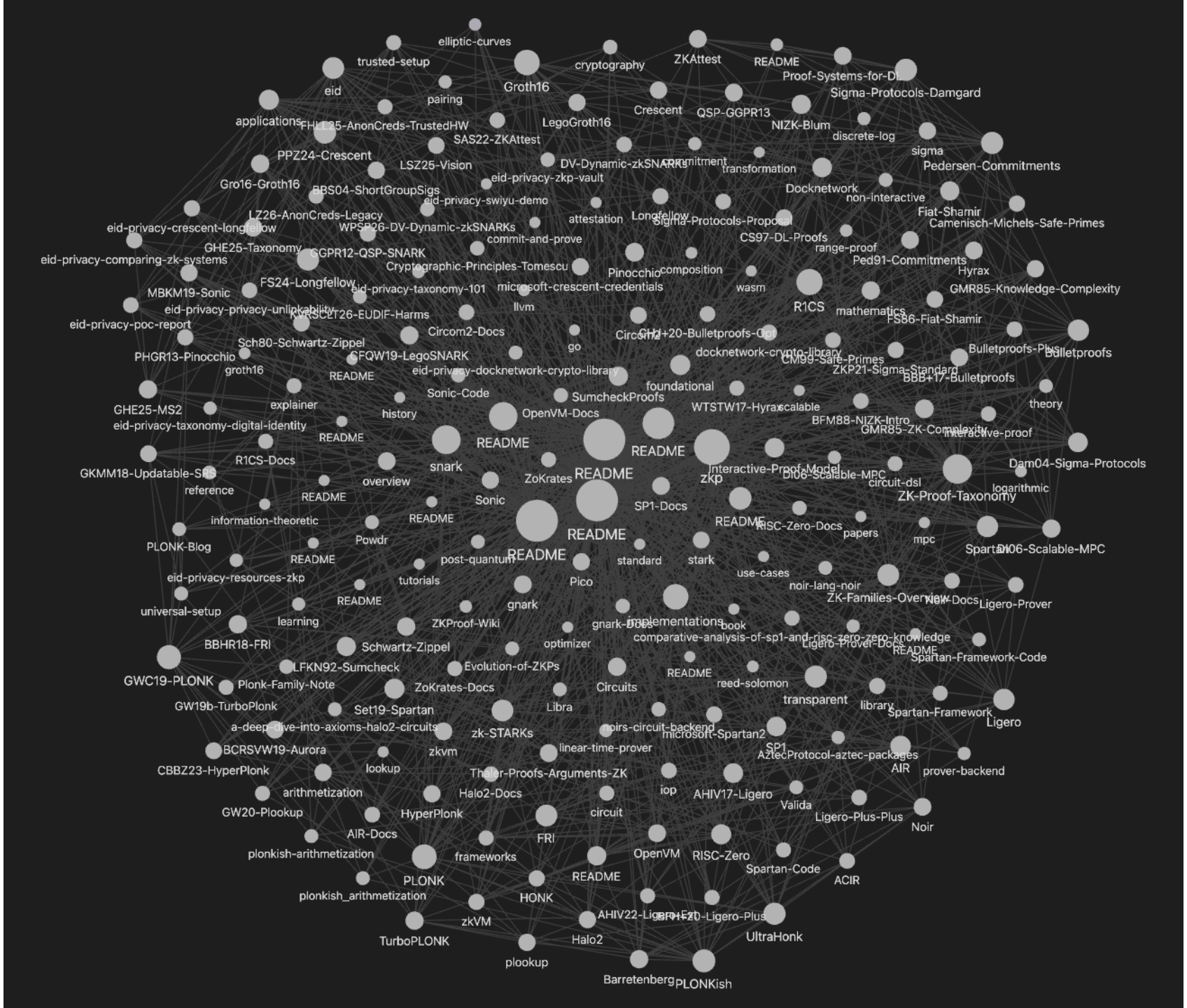
Marketing

Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly

https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/

We beat Google's zero-knowledge proof of quantum cryptanalysis

https://blog.trailofbits.com/2026/04/17/we-beat-googles-zero-knowledge-proof-of-quantum-cryptanalysis/


elliptic-curves
trusted-setup
cryptography
ZKAttest
README
Proof-Systems-for-DL
Groth16
eid
pairing
Sigma-Protocols-Damgard
Crescent
QSP-GGPR13
applications
FHLL25-AnonCreds-TrustedHW
LegoGroth16
NIZK-Blum
discrete-log
SAS22-ZKAttest
sigma
PPZ24-Crescent
LSZ25-Vision
DV-Dynamic-zkSNARKs
transformation
Pedersen-Commitments
eid-privacy-zkp-vault
Gro16-Groth16
BBS04-ShortGroupSigs
Docknetwork
non-interactive
eid-privacy-swiyu-demo
Fiat-Shamir
LZ26-AnonCreds-Legacy
attestation
Longfellow
Camenisch-Michels-Safe-Primes
eid-privacy-crescent-longfellow
WPSP26-DV-Dynamic-zkSNARKs
Sigma-Protocols-Proposal
commit-and-prove
CS97-DL-Proofs
range-proof
GHE25-Taxonomy
GGPR12-QSP-SNARK
Ped91-Commitments
eid-privacy-comparing-zk-systems
Cryptographic-Principles-Tomescu
Pinocchio
composition
Hyrax
FS24-Longfellow
eid-privacy-taxonomy-101
microsoft-crescent-credentials
wasm
GMR85-Knowledge-Complexity
MBKM19-Sonic
eid-privacy-privacy-unlinkability
llvm
R1CS
mathematics
KVRSCLT26-EUDIF-Harms
FS86-Fiat-Shamir
eid-privacy-poc-report
Circom2-Docs
Circomlz
CHJJ+20-Bulletproofs-Opt
Sch80-Schwartz-Zippel
go
Bulletproofs-Plus
Bulletproofs
PHGR13-Pinocchio
CFQW19-LegoSNARK
docknetwork-crypto-library
CM99-Safe-Primes
groth16
README
eid-privacy-docknetwork-crypto-library
ZKP21-Sigma-Standard
BBB+17-Bulletproofs
foundational
Sonic-Code
SumcheckProofs
theory
GHE25-MS2
explainer
history
OpenVM-Docs
WTSTW17-Hyrax
scalable
BFM88-NIZK-Intro
eid-privacy-taxonomy-digital-identity
GMR85-ZK-Complexity
interactive-proof
README
README
README
README
Dam04-Sigma-Protocols
R1CS-Docs
snark
GKMM18-Updatable-SRS
ZoKrates
zkp
Interactive-Proof-Model
Dl06-Scalable-MPC
circuit-dsl
overview
logarithmic
reference
README
Sonic
SP1-Docs
ZK-Proof-Taxonomy
information-theoretic
README
README
RISC-Zero-Docs
papers
mpc
Powdr
PLONK-Blog
Spartan
Dl06-Scalable-MPC
README
post-quantum
README
standard
stark
eid-privacy-resources-zkp
tutorials
Pico
use-cases
noir-lang-noir
ZK-Families-Overview
README
gnark
Ligero-Prover
universal-setup
learning
ZKProof-Wiki
gnark-book
implementations
book
comparative-analysis-of-sp1-and-risc-zero-zero-knowledge
BBHR18-FRI
Schwartz-Zippel
optimizer
Ligero-Prover-Docs
README
Spartan-Framework-Code
GWC19-PLONK
LFKN92-Sumcheck
Evolution-of-ZKPs
README
Plonk-Family-Note
ZoKrates-Docs
Circuits
reed-solomon
transparent
library
GW19b-TurboPlonk
Set19-Spartan
Libra
Spartan-Framework
Ligero
a-deep-dive-into-axioms-halo2-circuits
zk-STARKs
noirs-circuit-backend
microsoft-Spartan2
SP1
BCRSVW19-Aurora
zkvm
linear-time-prover
AztecProtocol-aztec-packages
AIR
CBBZ23-HyperPlonk
lookup
Thaler-Proofs-Arguments-ZK
prover-backend
arithmetization
Halo2-Docs
iop
AHIV17-Ligero
GW20-Plookup
HyperPlonk
circuit
Valida
Ligero-Plus-Plus
Noir
AIR-Docs
FRI
plonkish-arithmetization
frameworks
OpenVM
RISC-Zero
Spartan-Code
ACIR
PLONK
README
plonkish_arithmetization
HONK
AHIV22-Ligero
zkVM
TurboPLONK
Halo2
UltraHonk
plookup
Barretenberg
PLONKish

Limitations and frontier being worked on

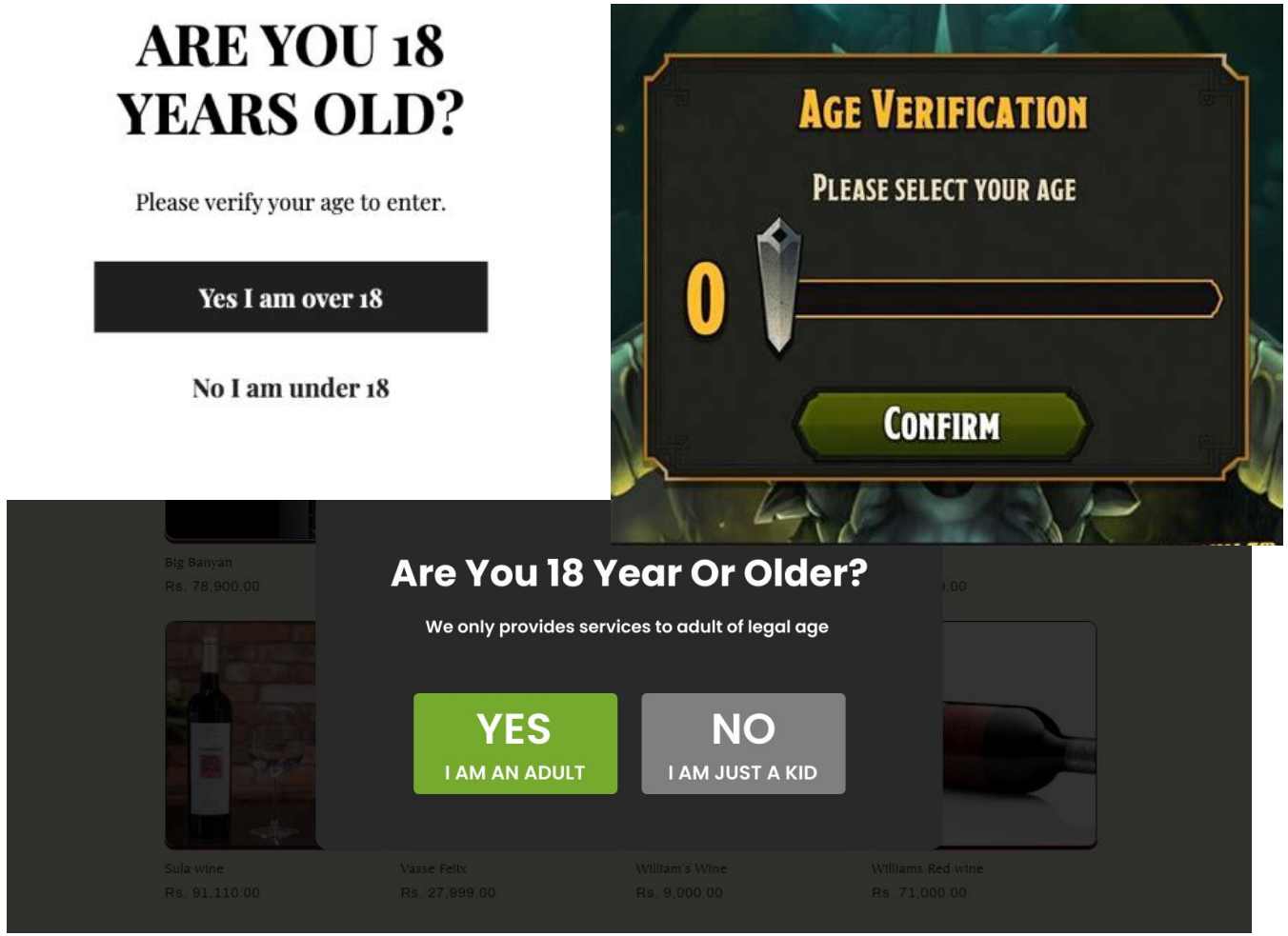
- ZKPs are computing intensive, an important issue when it comes to consumer-centric use cases
- Concrete performance of post-quantum secure schemes is not ideal
- Auditability of implementations and circuits leaves to be desired
- ZKPs cannot prevent context-specific overreach

Digital identity, digital cash, supply chain (2)

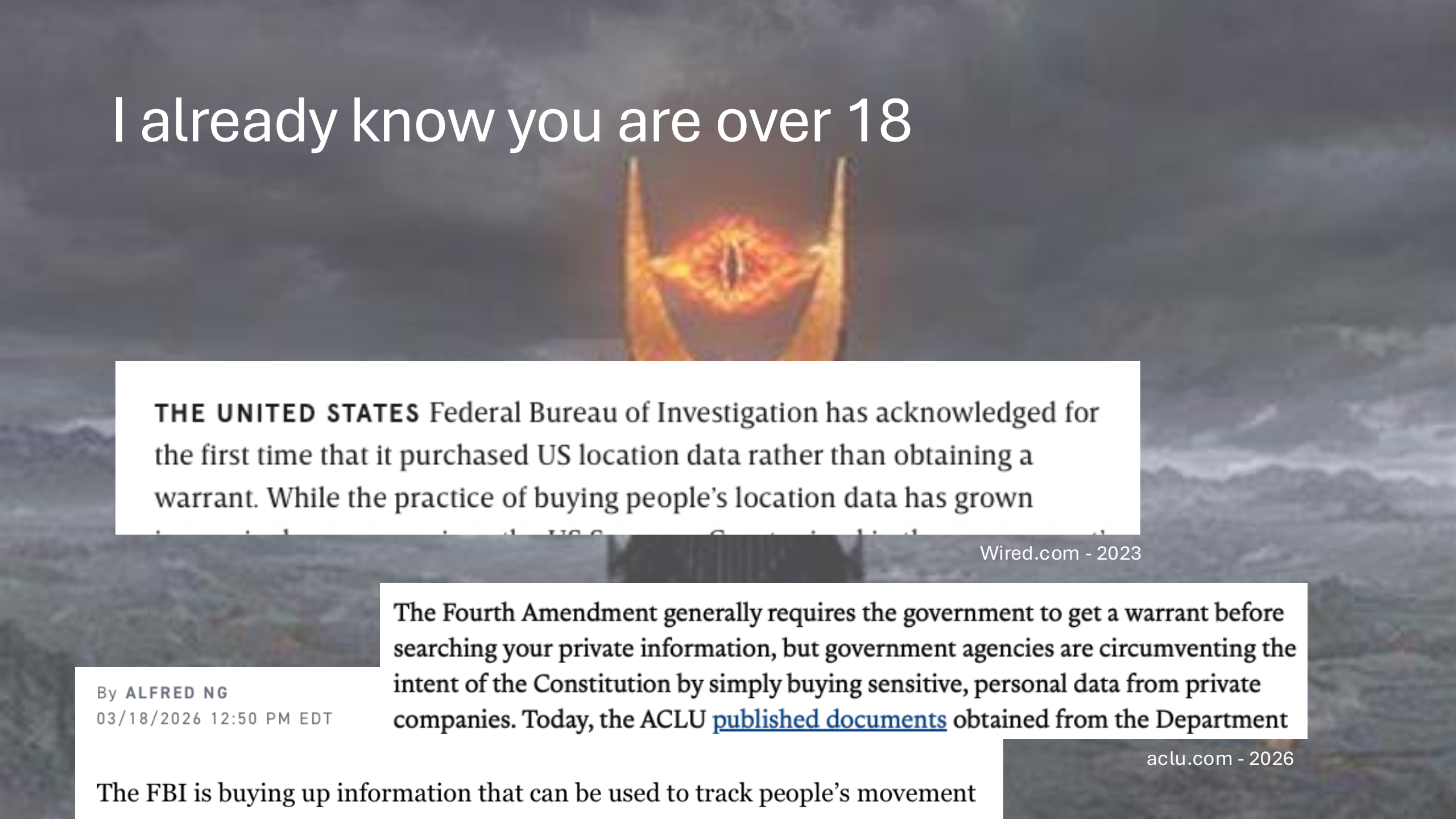
- **Digital identity** can make use of ZKPs to allow identity-holders to prove statements about themselves without oversharing information.
- **Digital cash** can use ZKPs to ensure compliance to cash transaction regulations without compromising the privacy guarantees of cash.
- **Supply chain** can use ZKPs to prove compliance to industry and market regulations without exposing sensitive business information.

Easing the privacy vs. oversight tensions: e-ID, ZKPs, age verification

Trust me bro, I’m over 18



I already know you are over 18



THE UNITED STATES Federal Bureau of Investigation has acknowledged for the first time that it purchased US location data rather than obtaining a warrant. While the practice of buying people's location data has grown

Wired.com - 2023

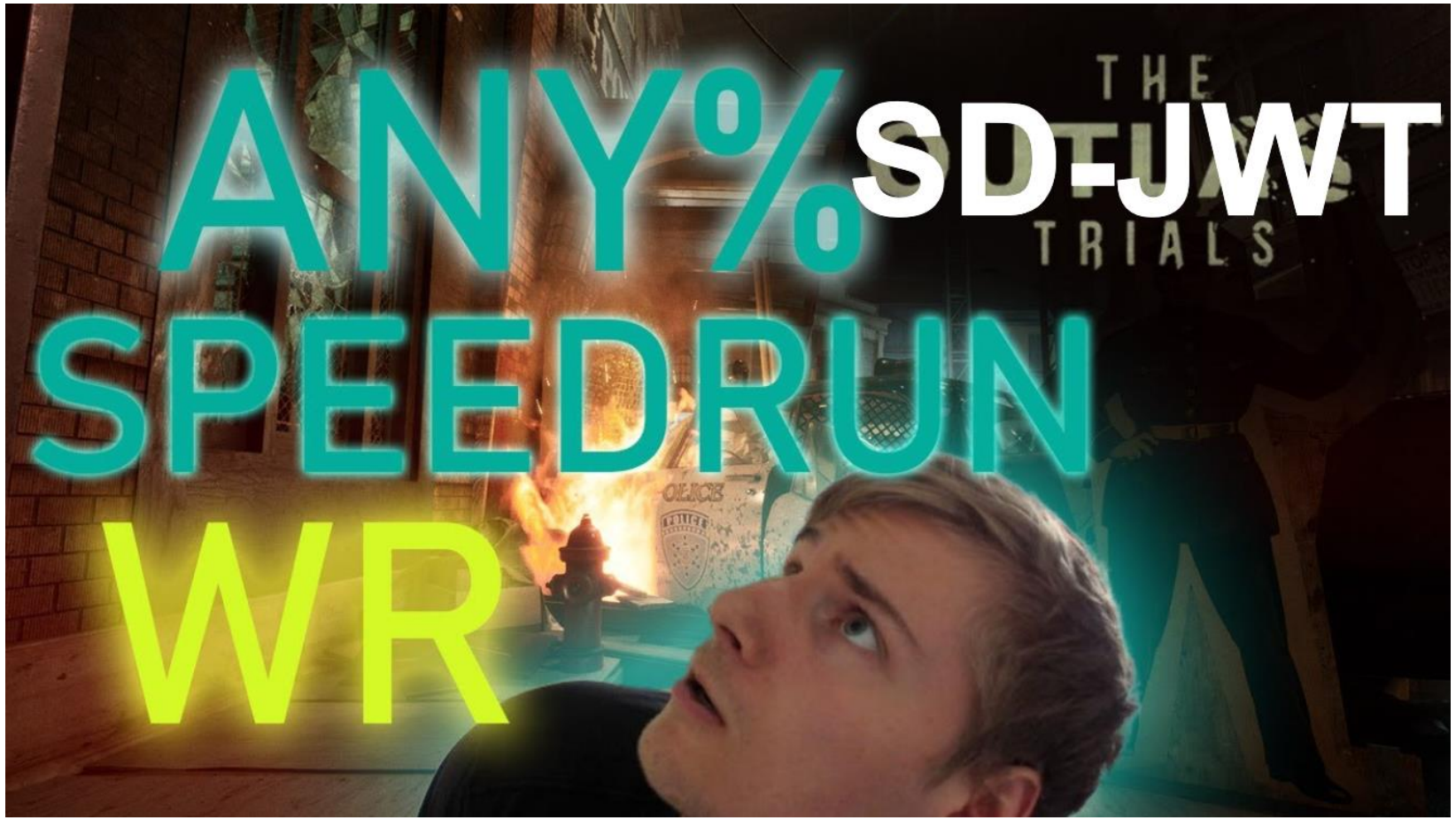
The Fourth Amendment generally requires the government to get a warrant before searching your private information, but government agencies are circumventing the intent of the Constitution by simply buying sensitive, personal data from private companies. Today, the ACLU published documents obtained from the Department

aclu.com - 2026

By **ALFRED NG**
03/18/2026 12:50 PM EDT

The FBI is buying up information that can be used to track people's movement

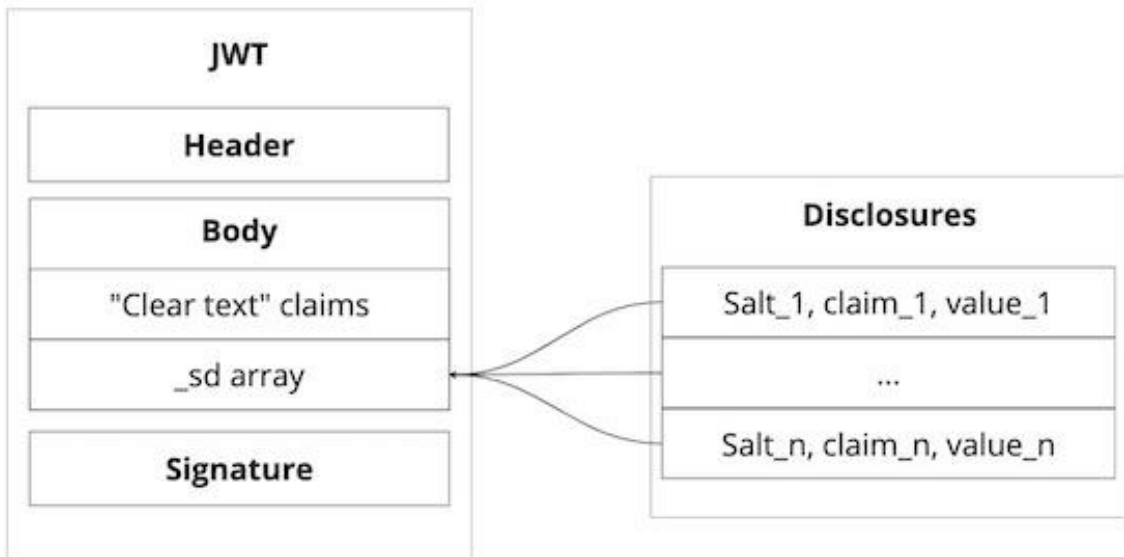
The Swiss E-ID


ANY%
SD-JWT
SPEEDRUN
WR
THE
TRIALS

The SD-JWT: eyJhbGciOiAiRVMyNTYiLCAidHlwIjogImV4YW1wbGUrc2Qtand0In0.eyJfc2QiOiBbIjhsWGFfOHRaSkpUUFM5TGdlTnZ3RS1CZVVtRlFhYmQwcTMxWVJUdTNVM3ciLCAiVGhyTHJxc0JHaFlqMDZFNENSTXdOOEVtUkt4SDJOX052WndEU3JvZ0pVYyJdLCAid2FsayI6ICJkdWNrIiwgIl9zZF9hbGciOiAic2hhLTI1NiJ9.7V-u4ljVBleGgz4hatR-7GAgzSgvkbnQahM3vYIMm7OgE3BaffQfsEn6H3IslyrYT13YHQJa5qwZxj4wlF4sUw

Decoded body:

```
{
  "_sd": [
    "8lXa_8tZJJTPS9LgeNvwE-BeUmFQabd0q31YRTu3U3w",
    "ThrLrqsBGhYj06E4CRMwN8EmRKxH2N_NvZwDSrogJUc"
  ],
  "walk": "duck",
  "_sd_alg": "sha-256"
}
```




```
Disclosures:
[
    DpE9LJ2SHaR23KFuCtCSbQ, <---
    look, <--- claim name"
    duck <--- claim value"
]
[
    -JldcDGqa00ImdPUCFUvlA, <---
    quack, <--- claim name"
    duck <--- claim value"
]
```

Proving set inclusion:
"I am a Swiss citizen"

Proving arithmetic statement: "I'm over 18"

Cred. type

Signature

Information revealed with controlled impact on privacy.

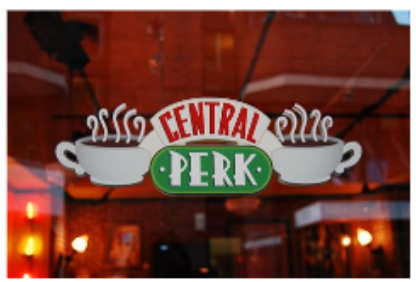
age > 18

Signature

Uniquely identifying information. Correlation is trivial.

Ville de Lausanne

~~Can~~ try to correlate information
Will



Proving set inclusion:
"I am a Swiss citizen"

Proving arithmetic statement: "I'm over 18"

Cred. type

Signature

Information revealed with controlled impact on privacy.

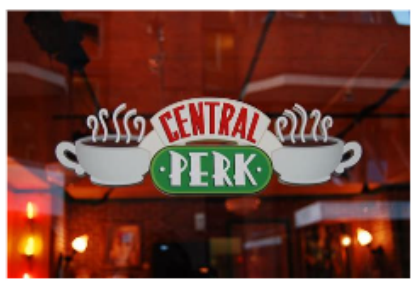
Proving knowledge of signature

age > 18

Signature

Ville de Lausanne

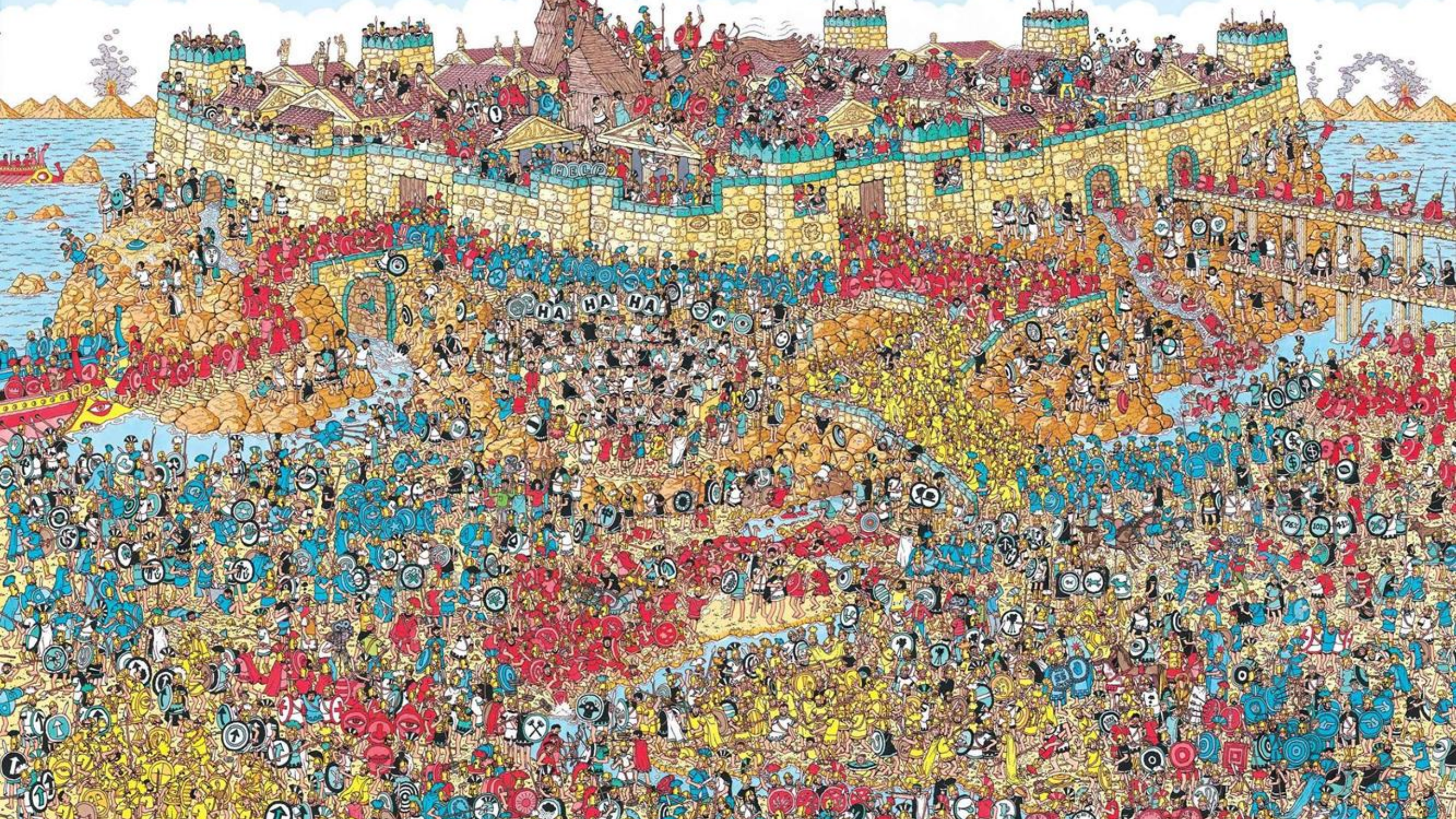
~~Can~~ try to correlate information
Will



Concrete constraints that require work

- Adherence to accepted standards (IETF SD-JWT, ISO mDoc, …). These are less-that-optimal formats for ZKPs and lead to big proofs.
- Needs to work on consumer phones, whereas most ZKP schemes focus on verifier’s efficiency.
- Needs to satisfy the trust and liability constraints of a public infrastructure, complicated or inflexible setups are undesirable.
- Needs to satisfy a level of auditability and maintainability.

Are ZKPs enough ?

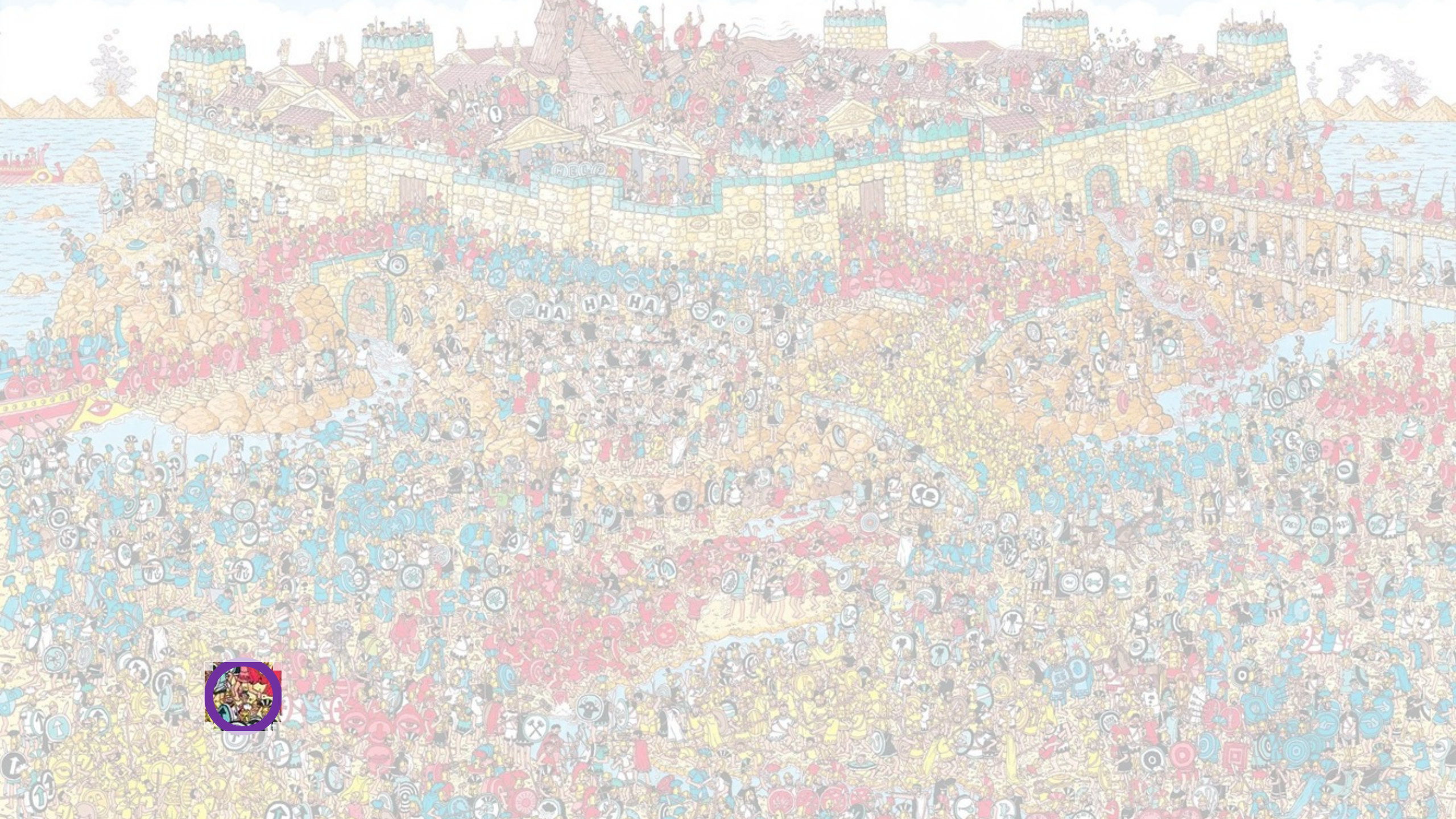

HA HA HA

Q&As

In which we do the exact opposite of ZKPs

References

- All the abstract examples: https://en.wikipedia.org/wiki/Zero-knowledge_proo
- Best blog on the internet about e-ID and ZKPs: https://eid-privacy.github.io
- Linus' treasure cave of ZKP papers: https://eid-privacy.github.io/zkp-vault/#resources-index
- SD-JWT for developers: https://github.com/chumbert/sd-jwt-crash-course
- Swiyu (Swiss e-ID): https://www.eid.admin.ch/en/swiyu-coming-soon-e


HA HA HA