



Vega: Low-Latency Zero-Knowledge Proofs over Existing Credentials

Darya Kaviani Srinath Setty

Berkeley Microsoft Research

IEEE S&P '26

Why Private IDs?

Age verification laws



Age prediction in ChatGPT

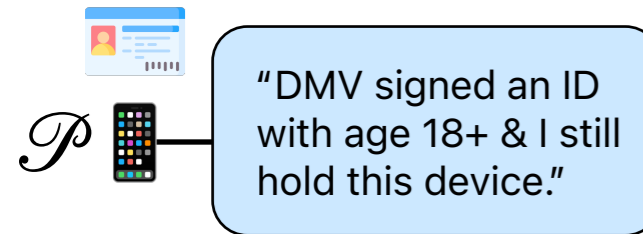
Updated: 11 days ago

This feature is rolling out globally. In the EU, age prediction will roll out in the coming weeks to account for regional requirements.

Identity verification on Claude

Updated over 3 weeks ago

Being responsible with powerful technology starts with knowing who is using it. Identity verification helps us prevent abuse, enforce our usage policies, and comply with legal obligations.

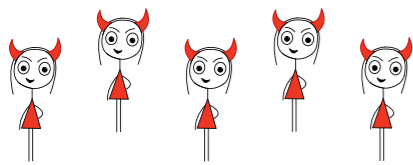


Can we **prove** facts about a credential without ever revealing it?

The Deployment Dilemma of Existing Solutions

Trusted setup

Performance



High prover costs for clients



High verifier costs

Scheme (ms)	Setup	Offline	Prove	Verify	Transparent
Crescent [PPZ24]	106,158	25,653	182	89	No
Longfellow [FS24]	5,590	—	501	244	Yes
Vega	51	65	92	23	Yes

5.4x prover
10.6x verifier



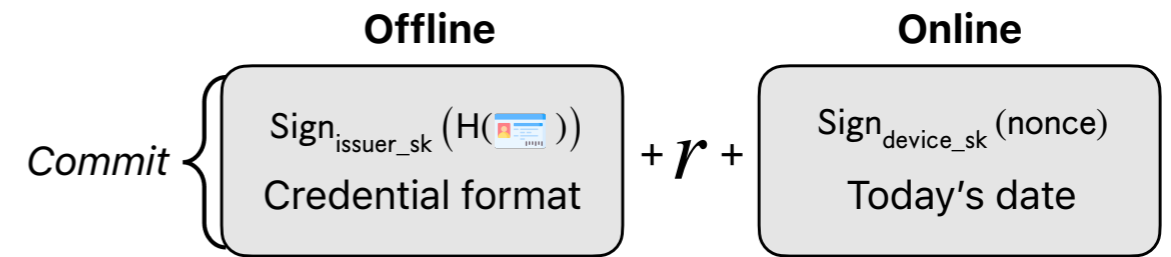
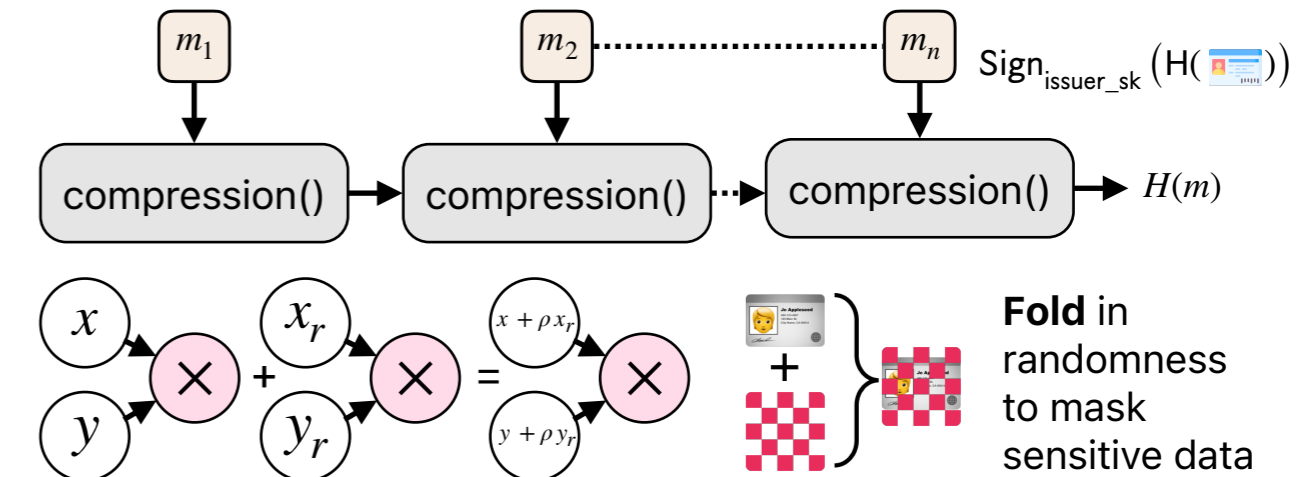
Tests planned in the EU Digital Identity Wallet large-scale pilot WE BUILD

To be specified in the ETSI TS 119 476-2 on ZKP for the EU-DIW

Key Techniques

Fold compression instances

Fold-&-reuse proving for efficient precomputation, hashing, & zero-knowledge.



```

{
  "valueDigests": {
    "org.iso.18013.5.1": {
      "birthDate": "h'4a3c...", ...
    }, ...
  },
  "docType": "org.iso.18013.5.1.mDL",
  "validityInfo": {
    "validUntil": "2028-11-01T00:00:00Z",
  },
}

```

Ex. mDL

Lookup-centric arithmetization for hashing & efficient parsing.

Lookup expiry follows **validUntil**

Index	Value
0	d_1
1	d_2
...	...
$n-1$	d_n

Lookup the intermediary digest for length-hiding