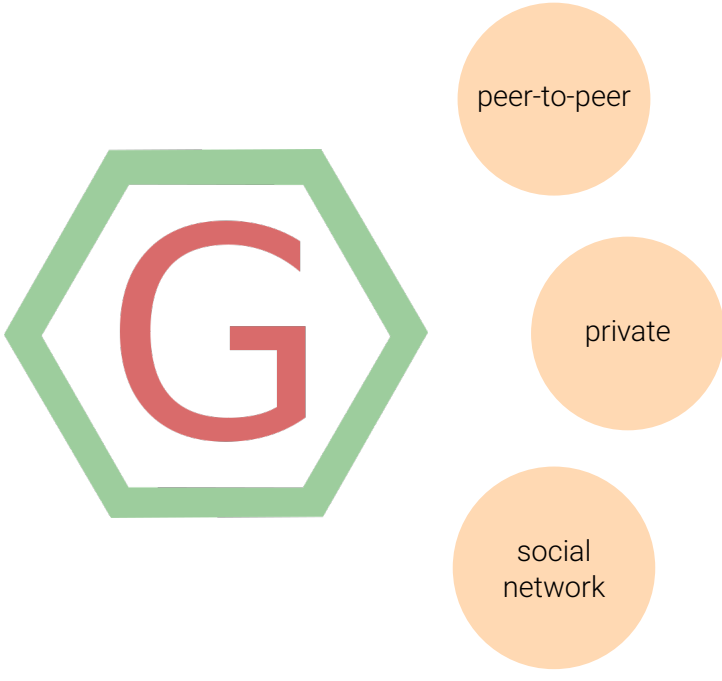
Flick.rs

Creating Hogwarts' Flickr without magic

Ruben De Smet, Thibaut Vandervelden, Tom Godden

January 15, 2021

VRIJE
UNIVERSITEIT
BRUSSEL



De Smet *et al.*, 2018

peer-to-peer

private

social network

access control: large ACLs

De Smet *et al.*, 2018

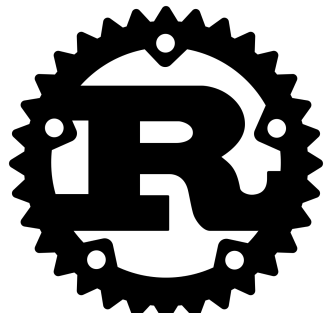
attribute based encryption

VRIJE
UNIVERSITEIT
BRUSSEL


GRYFFINDOR

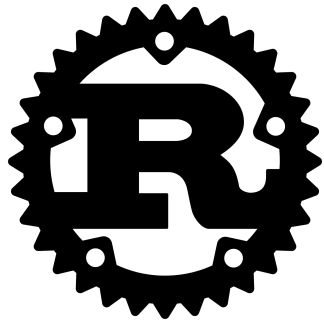

GRYFFINDOR


GRYFFINDOR



Decentralised ABE scheme, Yan Michalevsky and Marc Joye 2018

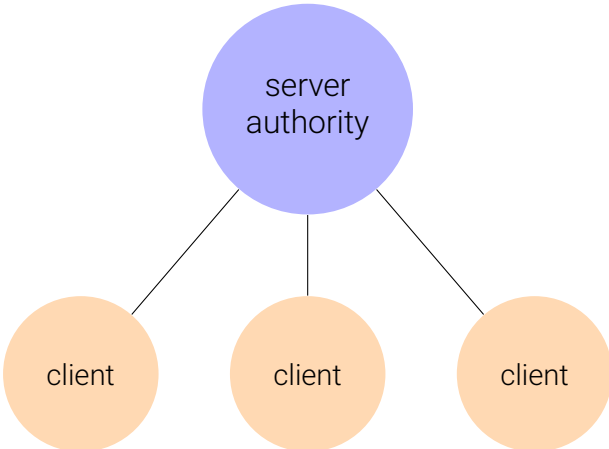
DIPPE



Decentralised ABE scheme, Yan Michalevsky and Marc Joye 2018

demo application

VRIJE
UNIVERSITEIT
BRUSSEL

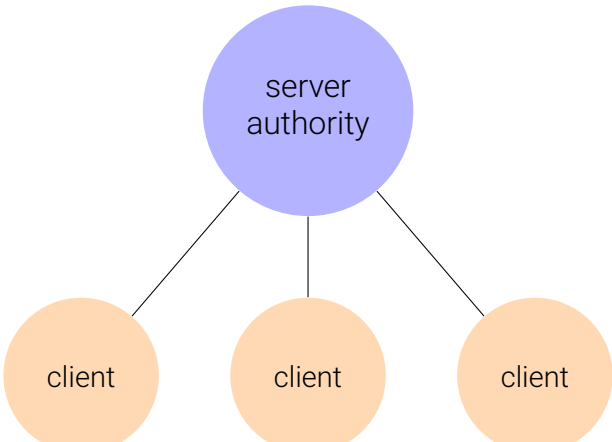


flick.rs

https://flickrs.
opencloudedge.be

SCAN ME

Architecture

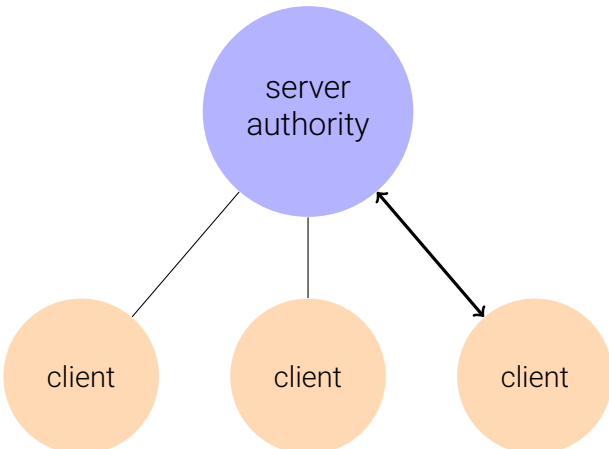


authority server on Kubernetes

client web browser and WASM

`https://flickrs.opencloudedge.be`

Architecture



Setup:

1. Download webpage and WASM
2. Fetch authority key
3. Request `UserPrivateKey`

Upload (hybrid encryption):

1. Select attributes
2. Hybrid encryption ChaCha20Poly1305-DIPPE
3. Upload to server

Fetch images:

1. Fetch all images
2. Hybrid decryption.

`https://flickrs.opencloudedge.be`

preliminary benchmarks

- In production Kubernetes: ±1 k user registrations per second on single machineEPYC Rome 16-core, 64 GB.
- Encryption with 16 attributes $k = 2$: ±350 ms[1]

. . . future work: compare with CiFEr/GoFE.

[1] Threadripper 1920X, 32 GB

Results & Caveats

We have

- a complete Rust implementation with 90 %+ test coverage of DIPPE
- …compilable to WebAssembly
- extensive documentation and tested example code: `https://etrovub.gitlab.io/smartnets/cife-rs/doc/cife_rs/abe/dippe/index.html`
- a live demo[2]

…but …

- hash-to-curve is stubbed as `return` G, although tested as `return` $\mathcal{H}(msg) \cdot G$.
- serialization does not use point compression
- interop between CiFEr, GoFE and CiFE-rs untested

[2] …which hopefully didn't fail!