¿Cómo demostrar que soy yo sin tener que ir a una notaría?

En tiempos de cuarentena general se requiere demostrar la identidad sin estar presente.

- Zenroom

Zenroom is a secure language interpreter of both Lua and its own secure domain specific language (DSL) to execute fast cryptographic operations using elliptic curve arithmetics.

The Zenroom VM is very small, has no external dependency, is fully deterministic and ready to run end-to-end encryption on any platform: desktop, embedded, mobile, cloud and even web browsers.

Zencode is the name of the DSL executed by Zenroom: it is similar to human language and can process large data structures while operating cryptographic transformations and basic logical operations on them.

- Una autoridad central (trusted issuer) puede generar pares de claves publica y privada.
- El ciudadano puede firmar documentos con su clave pública
- zero-knowledge proof: **Cryptography scheme to proof information, without sharing the information** Attribute based credentials
  - https://www.crowdcast.io/e/zenroom-workshop/register
  - https://www.youtube.com/watch?v=y7XYx5qBX3s

¿Como verificar si una cédula aparece en una lista de cédulas encriptadas?

El caso piloto es: BOB, quien pertenece a COLECTIVO A, quiere consultar si ALICIA ya fue beneficiaria de algún programa de su ALCALDIA, se requiere preservar la privacidad de ALICIA entonces se asume que BOB no muestra los datos privados de ALICIA y que ALCALDIA no muestra los datos privados de ninguno de sus ciudadanos. El sistema que le permita a BOB consultar a ALCALDIA preservando la privacidad, debería servir para que BOB consulte también si ALICIA está como beneficiaria de COLECTIVO B o ONG A etc.

Aproximación 1 Se reciben hashes y se comparan con hashes locales

Esta aproximación es vulnerable a alguien que haga una lista de hashes con todos los números de cédulas posibles. (¿se podría optimizar agregando un salt?)

JUAN hace el reporte encripta la cédula de ALICIA y la guarda en un archivo (próximamente será un archivo remoto)

```
echo -n 43123456 | sha256sum  >> /tmp/data
```

BOB consulta si la cedula de ALICIA está presente en el archivo

```
grep -Rwi -i -nr  -c "`echo -n 43123456 | sha256sum`"  /tmp/data
[1]
```

El número [1] representa el número de veces que la cédula está en el archivo de cédulas, si el archivo donde se guardan las cédulas es remoto, los administradores de la máquina remota verían los hashes de las cédulas ej:83cb4accb6bc1ebe5620dd7257d44de1d2d62fe50a9e3a89ac521fdc7dc3e7a8, no los números de cédula.

Referencias

- https://www.sitepoint.com/how-to-search-on-securely-encrypted-database-fields/
- Ley 1448 de 2011 (artículo 153) http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/ley144810062011.pdf
- Artículo 2.2.3.1 del Decreto Único Reglamentario 1084 de 2015

Casos donde se podría usar

- https://www.semana.com/semana-tv/semana-noticias/articulo/en-veremos-sesiones-virtuales-del-congreso-faltan-herramientas-de-seguridad/660784
- https://twitter.com/QuinteroCalle/status/1244763367060967426?s=20
- https://medium.com/@jaromil/decentralized-privacy-preserving-proximity-tracing-cryptography-made-easy-af0a6ae48640

Encuesta Alcalde

- La Alcaldía de MACONDO como (trusted issuer) puede generar pares de claves publica y privada para cada Cedula
- BOB recibe sus claves (¿web?)
- BOB llena la encuesta, (¿cada campo es firmado por su clave privada?)
- Contratista ACME va a usar IA sobre la encuesta:
    - ACME recibe las encuestas y las claves públicas
        - ¿cómo des-encripta las respuestas para hacer su análisis?
        - ¿unos campos como lat long y síntomas podrían ir des-encriptados?
        - ¿ACME debería recibir un par de llaves?
        - ¿ACME puede proveer el algoritmo que se corre en la máquina de BOB y se genera un reporte animizado desde la fuente?
        - ¿Cómo puede ACME comparar datos de BOB y ALICIA?

¿Cómo hacer trazabilidad al uso de mis datos privados entregados en una emergencia?

¿Trazabilidad al acceso?

De alguna manera se sabe quien accedió, ¿copió? los datos Problema: No se sabe el uso final de los datos, no se sabe si la destruyo.

Relacionados con el tema

http://monthlyreview.org/2016/02/01/france-an-algorithmic-power/

que diferencia hay en sumar los 2 primeros digitos de una cedula a sumar todos para genrar un hash con la suma y la cedula

se podria hacer un algorimo que haga una lista y que sume los digitos que se nesesiten ya sea 2 o todos

que se neseita para verificar

para verificar se debe tener el hash o el numero de la ceudula y comparar con uno de los 2

se tiene ? como verificar tiene\tiene	entidad hash	entidad cc	persona hash	persona cc
entidad hash	x	O	comparar si son iguales ambos son iguales	encriptar la cedula de la persona y compar si son iguales los hash
entidad cc	O	x	encriptar la cedula que tiene almacenada la entidad y compar si son iguales ambos son iguales	comparar si son iguales ambos son iguales
persona hash	comparar si son iguales ambos son iguales	encriptar la cedula que tiene almacenada la entidad y compar si son iguales ambos son iguales los hash	x	O

persona cc	encriptar la cedula de la persona y compar si son iguales los hash	comparar si son iguales ambos son iguales	O	x

x no aplica

0 no tiene sentido que se va a comparar aguacates con aguacates = la misma persona con la misma persna desde el mismo punto

se hiso un prototipo del progrma donde se puede proteger el hash enlace al protipo

Misc

- https://btcclj.com/posts-output/2020-06-18-elliptic-curve-cryptography-i/
- https://qvault.io/2020/09/17/very-basic-intro-to-elliptic-curve-cryptography/