



SAKUNDI

Identidad digital: conservando la privacidad - implementación y casos de uso

Andrés Gómez Ramírez

2025



Andrés Gómez Ramírez

- Ingeniero de sistemas
- Doctor en ciberseguridad en la Universidad de Frankfurt y el CERN
- Investigador en seguridad de Blockchain
- Co-founder Sakundi.io

- <https://x.com/kuronosec>
- <https://github.com/kuronosec>
- <https://github.com/kuronosec/zikuani>

Problemas:



Información privada y sensible de las personas disponible en Internet en niveles alarmantes

WIRED

NEGOCIOS CULTURA GADGETS IDEAS CIENCIA MEDIO AMBIENTE SEGURIDAD POLITICA INTELIGENCIA ARTIFICIAL SUMMIT 2024

CHIARA CRESCENZI

SEGURIDAD 8 DE JULIO DE 2024

La mayor filtración de datos de la historia ha expuesto 10 mil millones de contraseñas

El expediente "RockYou2024", publicado en un foro de *hackers*, pone en riesgo la seguridad de millones de personas.



ROD DODD/GETTY IMAGES

Problemas:



Información privada y sensible de las personas disponible en Internet en niveles alarmantes

infobae

Últimas Noticias

Política

Economía

Dólar hoy

Deportes

Sociedad

Policiales

Newsletters

TECNO >

Datos privados de casi 3.000 millones de personas habrían sido vendidos en la dark web por una gran suma de dinero

Según una demanda, se habrían expuesto nombres completos, direcciones y números de seguridad social de las personas afectadas

Problemas:



Información privada y sensible de las personas disponible en Internet en niveles alarmantes

Tiempo de Lectura: 2 minutos



-  El 80% de la información que los hackers de Conti
-  robaron a Costa Rica ya fue publicada. Así lo informó
-  el Gobierno este lunes 25 de abril.

Problemas:



No tengo nada que esconder, entonces no me preocupa...

**¿INTENTARON ESTAFARLO CON
UN NÚMERO TELEFÓNICO
PARECIDO AL DE SU BANCO? 3
CONSEJOS PARA DETECTAR EL
ENMASCARAMIENTO DE
LLAMADAS**

COMPARTIR



Problemas:

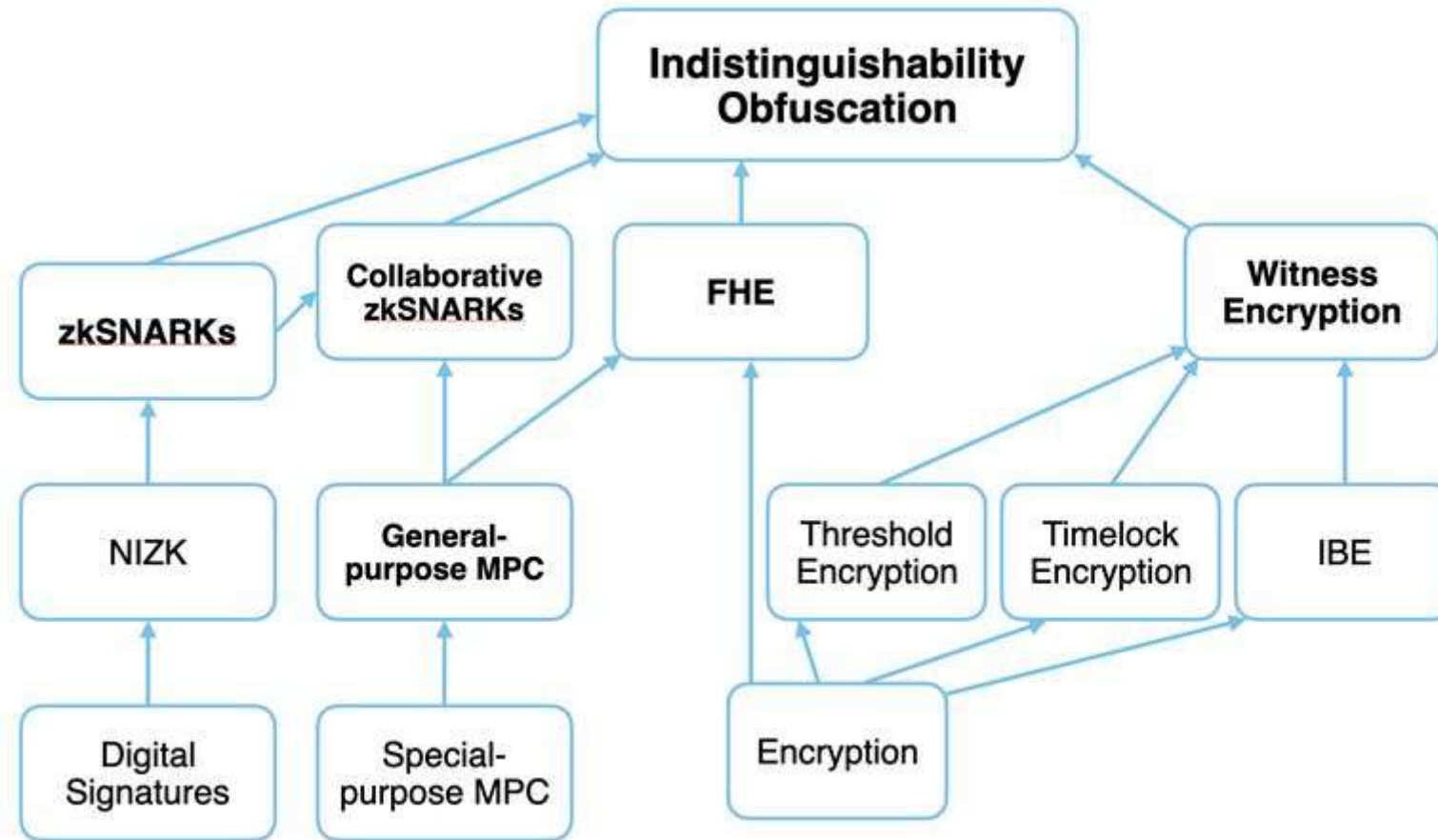


No tengo nada que esconder, entonces no me preocupa...

elpais.com

**Los usos criminales de los ‘deepfakes’
se disparan: estafas, pornografía y
suplantación de identidad**

Programmable cryptography



Zero-knowledge-proofs:



La mejor solución para la filtración constante de datos sensibles de los usuarios, es que estos no estén expuestos en Internet en primer lugar

Zero Knowledge Proof

1

One party (**the prover**) has to prove to another party (**the verifier**) that a certain statement is true.

2

But, they must do so **without revealing any other additional information** apart from the fact that the statement is true.



VERIFIER
Offers challenge



SECRET DATA



PROVER
Generates response



Zero-knowledge-proofs



- Zcash
- L2 sobre Ethereum
- Rollups
- Zero-knowledge rollups
- Starknet
- Aztec
- No sólo privacidad sino también eficiencia

Zikuani



We have developed Zikuani, a zero-knowledge proof (ZKPs) infrastructure solution to enhance the digital identity system. Our goal is to strengthen citizens' privacy by minimizing data collection, enabling individuals to access a wide range of valuable services without disclosing sensitive information and at the same time reducing the risk of identity fraud

Government identity

- ▶ Use your ID or passport to prove your identity. Prove that you are not a bot, that you are older than 18 years old, with less probability of fraud
- ▶ **Keep your privacy**
Keep your identity data on your device
- ▶ **Reduce identity theft and fraud**
Everything is verified cryptographically, no risk of fake ID images or fake face pictures

Zikuani: <https://zikuani.app>



The image shows a landing page for the Zikuani app. The background is a dark purple with a subtle grid pattern. On the left side, there are decorative white circuit-like lines. The main heading 'Zikuani' is in a large, light blue font. Below it, the subtitle 'Privacy Infrastructure using Zero-Knowledge Proofs' is in a smaller, white font. A tagline 'Proof your identity while preserving your privacy' is centered below the subtitle. Three feature boxes are arranged horizontally: 'Tampering-proof Identity' with a green shield icon, 'Super Fast' with a blue lightning bolt icon, and 'Easy to Use' with a purple padlock icon. At the bottom, there are two buttons: a blue 'Access Platform' button and a grey 'Learn More' button.

Zikuani

Privacy Infrastructure
using Zero-Knowledge Proofs

Proof your identity while preserving your privacy

-  Tampering-proof Identity
-  Super Fast
-  Easy to Use

[Access Platform](#) [Learn More](#)

Firma Digital en Costa Rica



- Certificados X.509
- RSA
- SHA256
- Firmados por el Banco Central
- Firma legalmente válida
- Con uso muy extendido en el país
- Autenticación y firma revelan datos del portador

Zikuani: <https://github.com/kuronosec/zikuani>

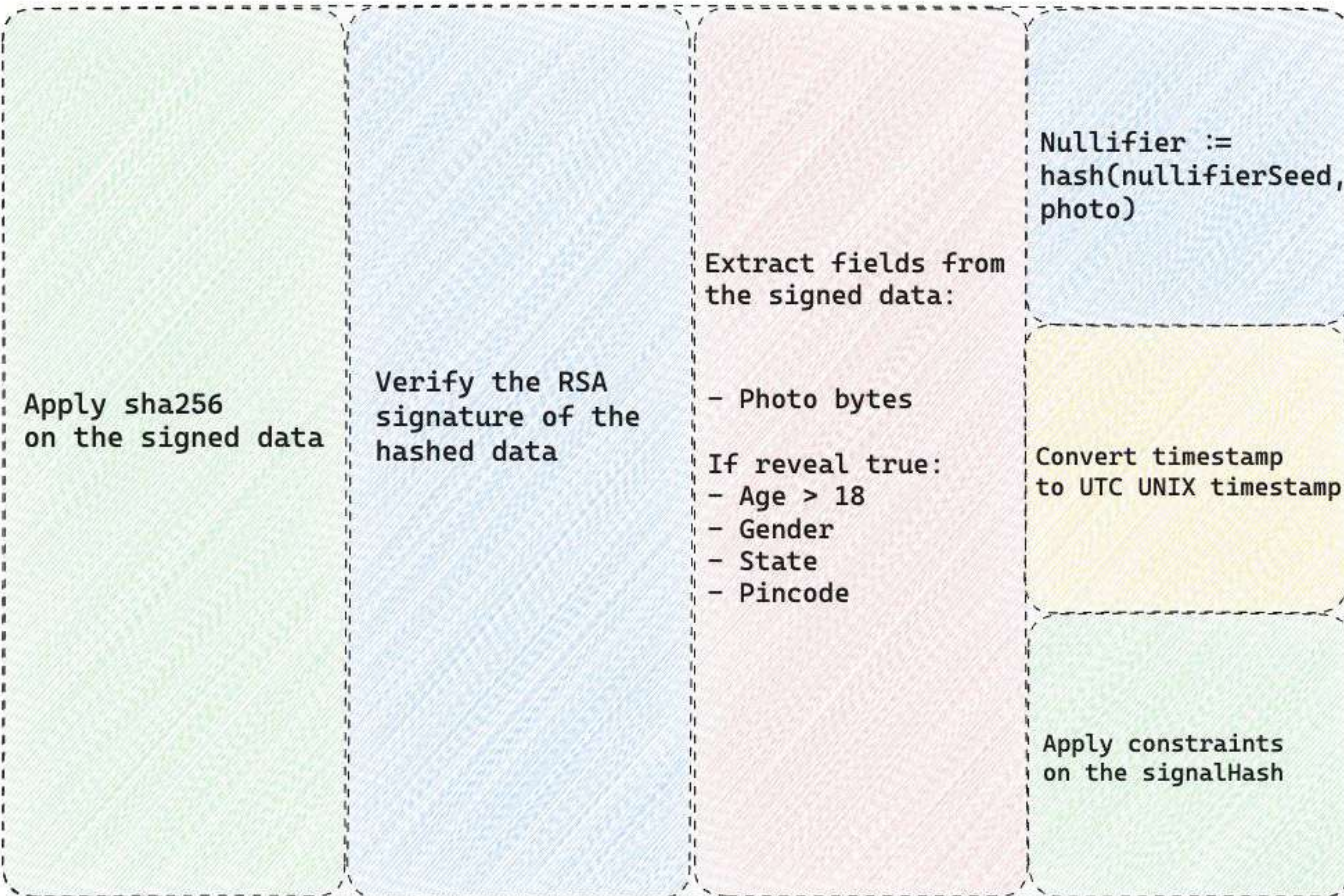


Circuit - aadhaar-verifier

Inputs

Private - Signature
Private - Signed Data
Public - RSA Public Key
Public - signalHash
Public - nullifierSeed
Public - revealAgeAbove18
Public - revealGender
Public - revealState
Public - revealPinCode

Optional Parameters

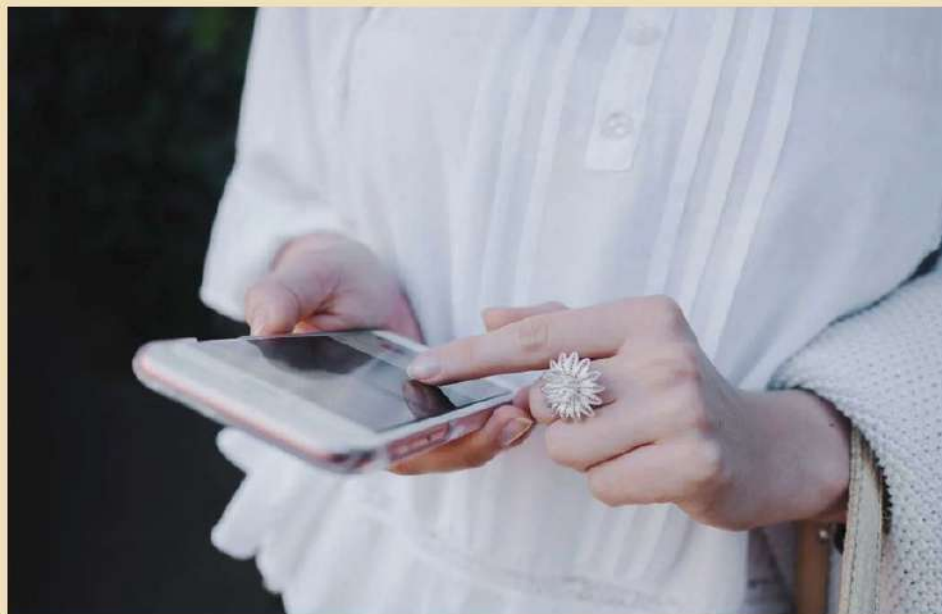


Outputs

nullifier
timestamp
pubKeyHash
signalHash
nullifierSeed
ageAbove18
Gender
State
Pincode

Only if
requested

De la Firma Digital a la Cédula Digital



Fotografía con fines ilustrativos.

Cédula digital se implementará en tercer trimestre de 2025 y tendrá un costo inicial de \$2.600, informa TSE

Las capacidades “pone home” en los sistemas de identidad digital

¿Podemos hacer lo mismo con los pasaportes?



rarimo

zk Passport

Allow users to Prove who they are – without revealing any data

Build in

 Privacy:

NFC chip scans never leave a device
Only zero knowledge proof is shared

Casos de Uso



- Anonymous authentication
- Decentralized anonymous voting
- Anonymous proof of humanity
- Health data privacy
- Know Your Customer
- Privacy-Preserving Verification
- Anti-Sybil Mechanisms
- DAO Governance
- Quadratic Funding (QF)
- Wallet Recovery
- Y muchos más

Votación descentralizada y anónima:

<https://github.com/kuronosec/zk-voto-digital>



- Usuarios validan su pertenencia a un grupo sin revelar identidad (Ciudadania)
- Usuarios envían su voto por medio de una verifiable credential con ZKP
- Los votos son procesados en la Blockchain, que presenta muy altas garantías anti modificación
- El proceso es totalmente transparente, resultados se obtienen muy rápido
- Pueden ser corroborado por cualquier persona
- Identidad del votante permanece anónima
- Prueba de concepto en la red Polygon y BlockDAG (Testnet)

Votación usando Zikuani: <https://voto.sakundi.io>



ZK Voto Digital[Cómo funciona](#)[Voto Digital](#)[Crear Propuesta](#)[Ver Resultados](#)[Instalar Zikuani](#)ES

0x86E6...A8bE
● BlockDAG Testnet

Votación Anónima Segura con Blockchain y Pruebas de Conocimiento Cero

Preserva tu privacidad mientras pruebas tu identidad ciudadana

Participa en procesos democráticos sin revelar información personal. Verifica tu identidad, emite votos anónimos y contribuye a un futuro más transparente.

Votación usando Zikuani: <https://voto.sakundi.io>



Seleccionar Método de Autenticación

Elige cómo quieres verificar tu identidad para votar

Conectado como: 0x86E67a05324A55AF6B2b3bF1A5cBA1778C56A8bE

Método de Autenticación:

☐  Firma Digital

☒  Pasaporte

País del Pasaporte:

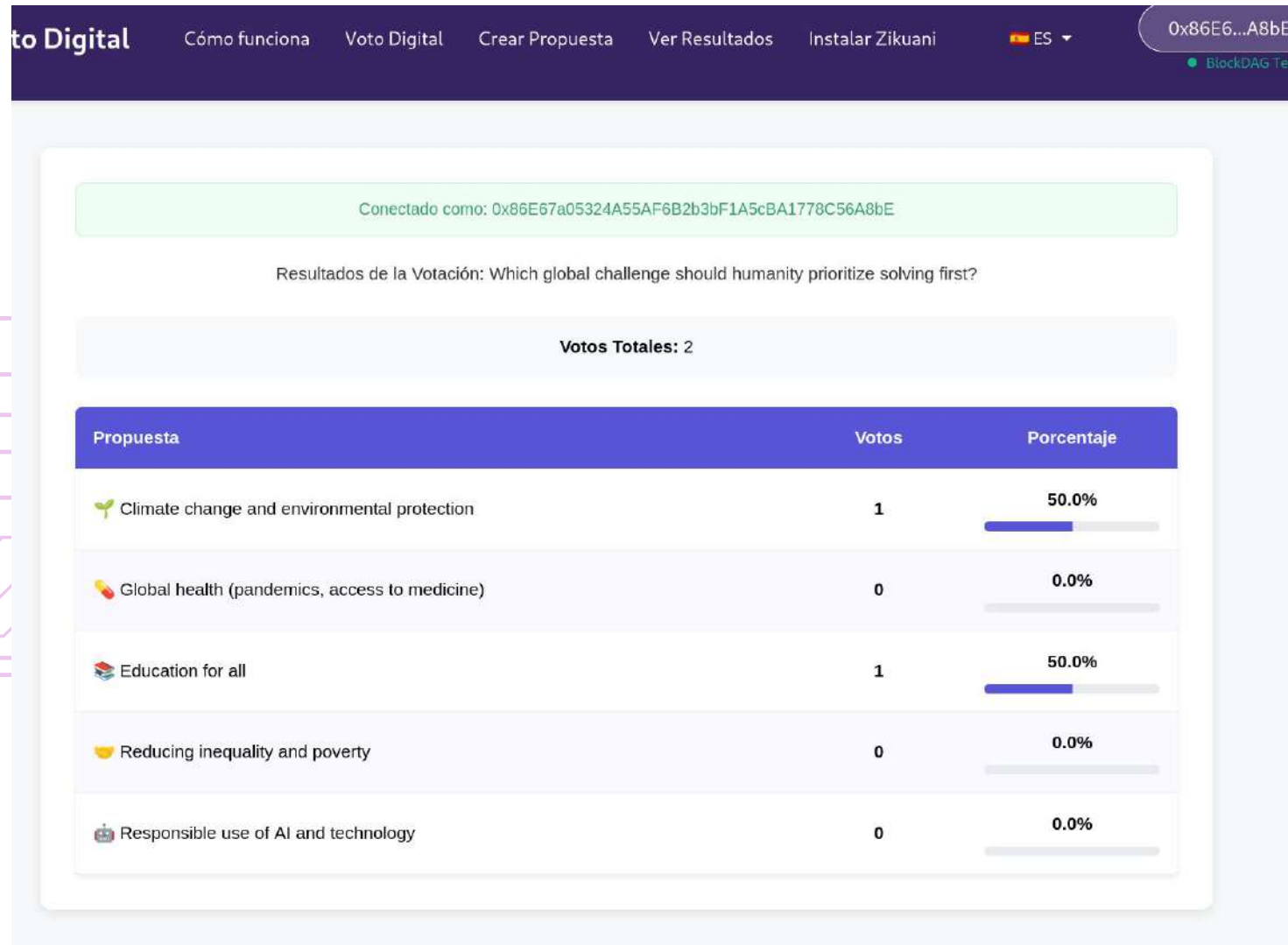
 Costa Rica (CRI) ✓

Continuar

Información

Usa tu pasaporte físico con la aplicación RariMe para verificar tu identidad de forma privada y segura.

Votación usando Zikuani: <https://voto.sakundi.io>



Para más información

- <https://zikuani.app/es/>
- <https://github.com/kuronosec/zikuani>
- <https://github.com/kuronosec/zk-voto-digital>
- <https://docs.sakundi.io/es/>



SAKUNDI

Contact us:



andres.gomez@sakundi.io



sakundi.io



[@kuronosec](https://twitter.com/kuronosec)



[@kuronosec](https://t.me/kuronosec)

Muchas Gracias!

