Privacy Preserving Cryptographic Toolbox

A survey with applications to Sovereign Identity

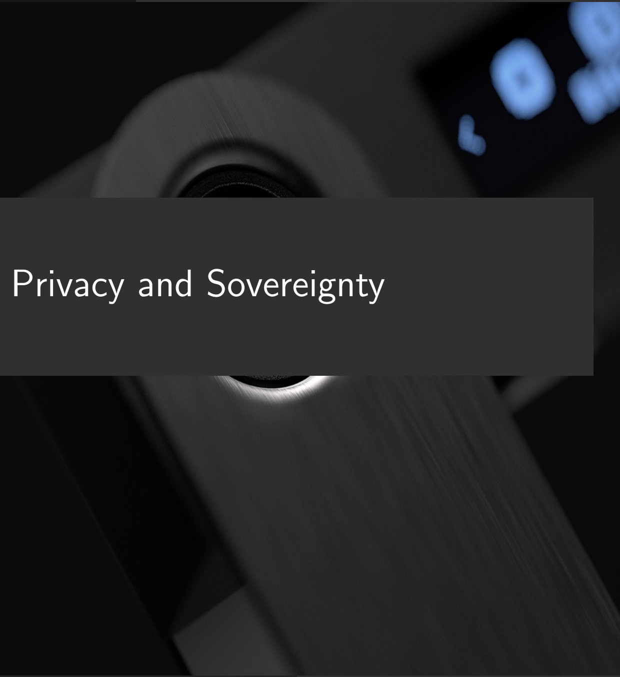
Renaud Dubois

Ledger
Innovation Team

June 10, 2022

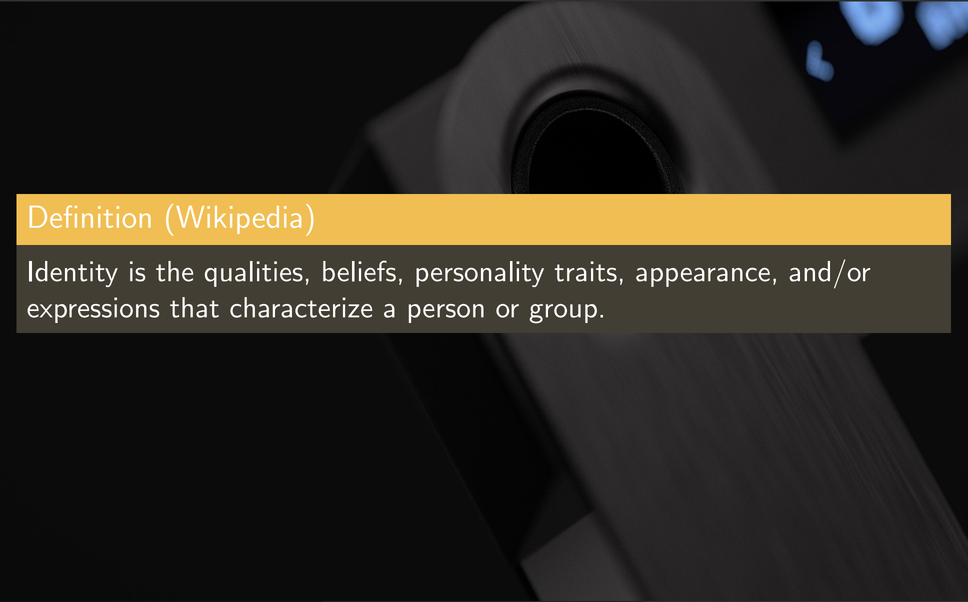
Summary

1. Identity, Privacy and Sovereignty
   - Identity
   - Privacy
   - Self Sovereignty
   - Anonymous Credentials
2. Privacy-Preserving Cryptographic Toolbox
   - Commitment
3. Pictures
4. boxes and columns



Identity, Privacy and Sovereignty

Identity



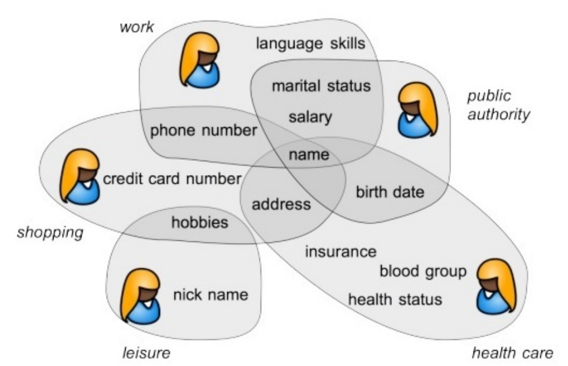
Definition (Wikipedia)

Identity is the qualities, beliefs, personality traits, appearance, and/or expressions that characterize a person or group.

Identity

Definition ([CL16])

Digital identity is a collection of attributes someone knows about.



From now on we will refer Identity, Privacy and Sovereignty as Digital ones.

Privacy

Definition (Wikipedia)

Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

Vires in Numeris

Definition (IND-PRIV2)

Privacy

Definition (Wikipedia)

Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

Vires in Numeris

- Alphabet+Meta : 3G€
- Nym's Fund : 0.3 G€
- RGPD : 1G€ in France

Definition (IND-PRIV2)

Privacy

Definition (Wikipedia)

Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

Vires in Numeris

- Alphabet+Meta : 3G€
- Nym's Fund : 0.3 G€
- RGPD : 1G€ in France

Definition (IND-PRIV2)

- Privacy domain is unclear : no RGS or unique primitive
- Survey (Kahoot)

Privacy at Ledger

Use cases

- Ledger Database : update of Ledger Live links accounts
- Device ID : links desktops and phones
- Ledger Live : genuine check
- Registering to a conference with Ether Fee

Noob Remarks

- We have privacy legal, but no privacy tech's or dungeon

Take offline solutions as priority, reduce collected information at maximum.

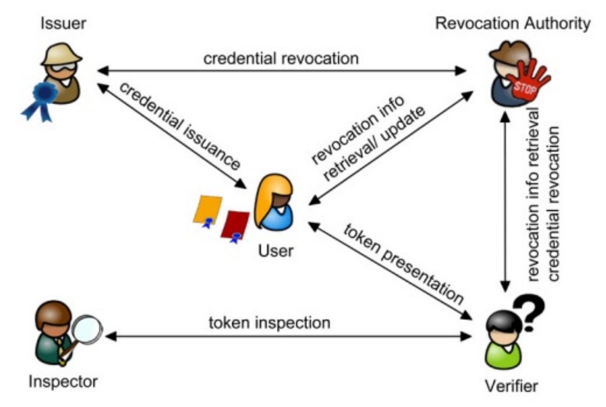
Self Sovereign Identity (SSI)

Definition (Wikipedia)

Self-sovereign identity (SSI) is an approach to **digital identity** that gives individuals control of their digital identities.

In the litterature, the Cryptographic solution is referred as Anonymous Credentials (AC) or Attribute Based Signature. The notion of control implies that the user decides which attribute is revealed.

Anonymous Credentials



Anonymous Credentials Recipee

Ingredients

- Commitment : Digital sealed envelope, polynomial Commitment, Functional Commitment. Enables range-proof (Monero), serial number hiding (Zerocoin), universal proofs.
- Signatures with efficient protocols : Proof friendly, Structure Preserving, Group, Linkable . . .
- Zero Knowledge Proof : proof a Knowledge of a value, without revealing it. From single value to universal.

Privacy-Preserving Cryptographic Toolbox

Basic Commitment

Digital Analog of Sealed envelope.

Basic Commitment

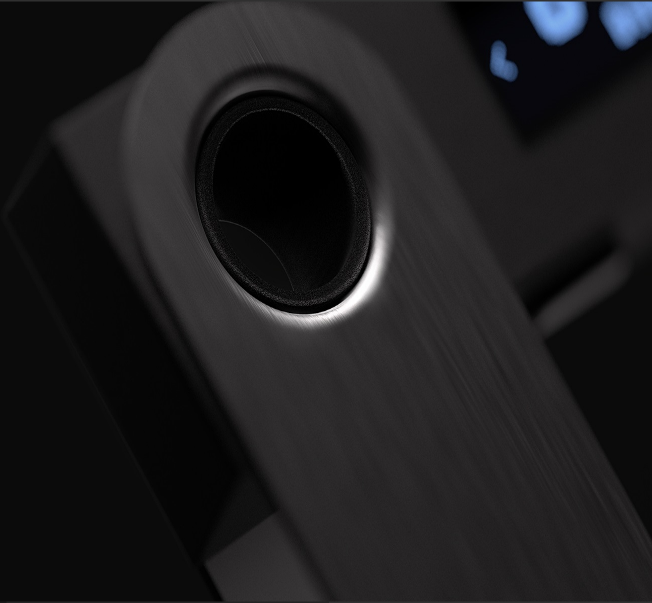
Prover

Verifier

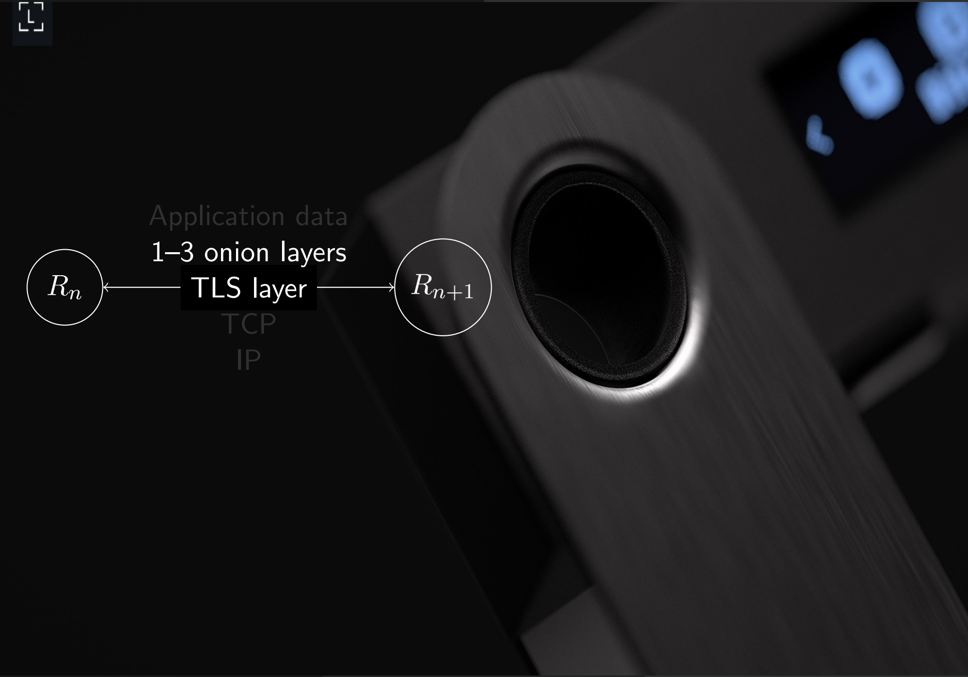
$$com = H(m,r) \qquad \xrightarrow{com}$$

$$\xrightarrow{(m,r)} \qquad com \overset{?}{=} H(m,r)$$

Pedersen Additive Homomorphic Commitment



totocs



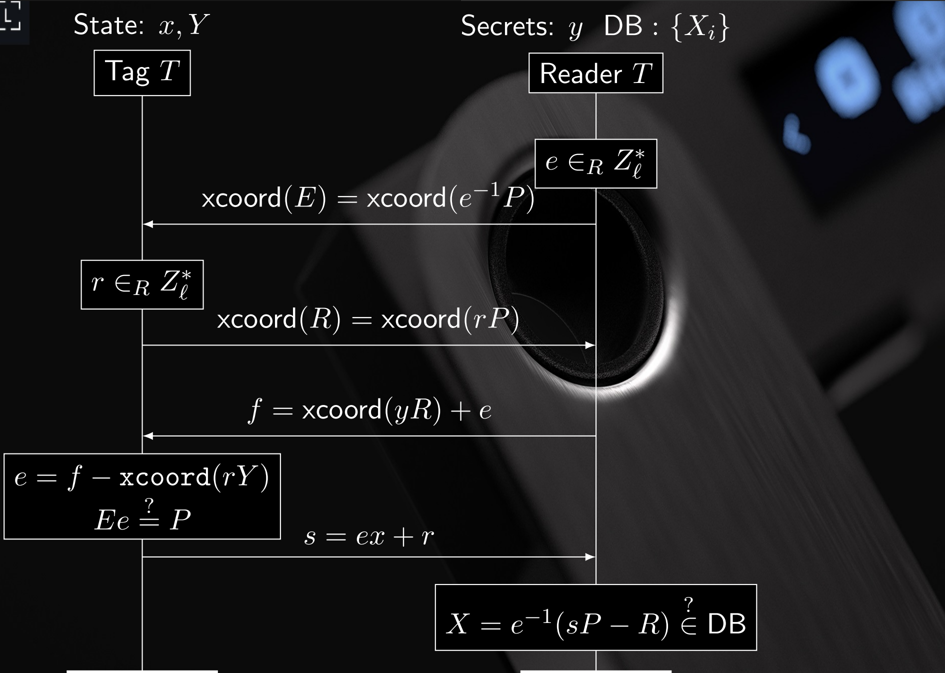
Application data

1–3 onion layers

TLS layer

TCP

IP



State: x, Y

Secrets: y DB : $\{X_i\}$

Tag T

Reader T

$e \in_R Z_\ell^*$

xcoord(E) = xcoord$(e^{-1}P)$

$r \in_R Z_\ell^*$

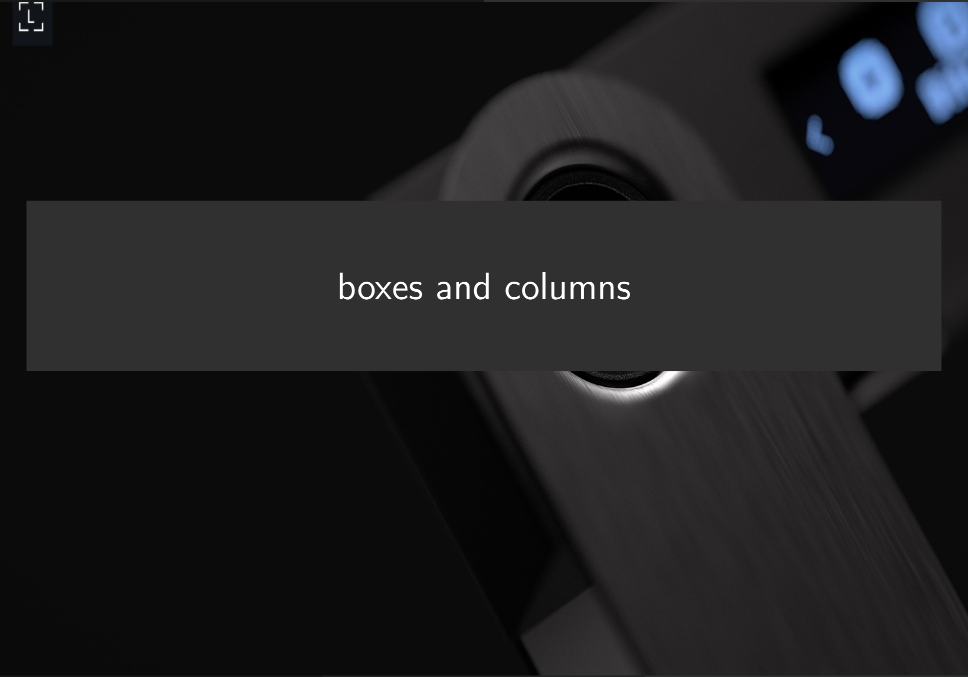
xcoord(R) = xcoord(rP)

f = xcoord$(yR) + e$

$$e = f - \texttt{xcoord}(rY)$$
$$Ee \overset{?}{=} P$$

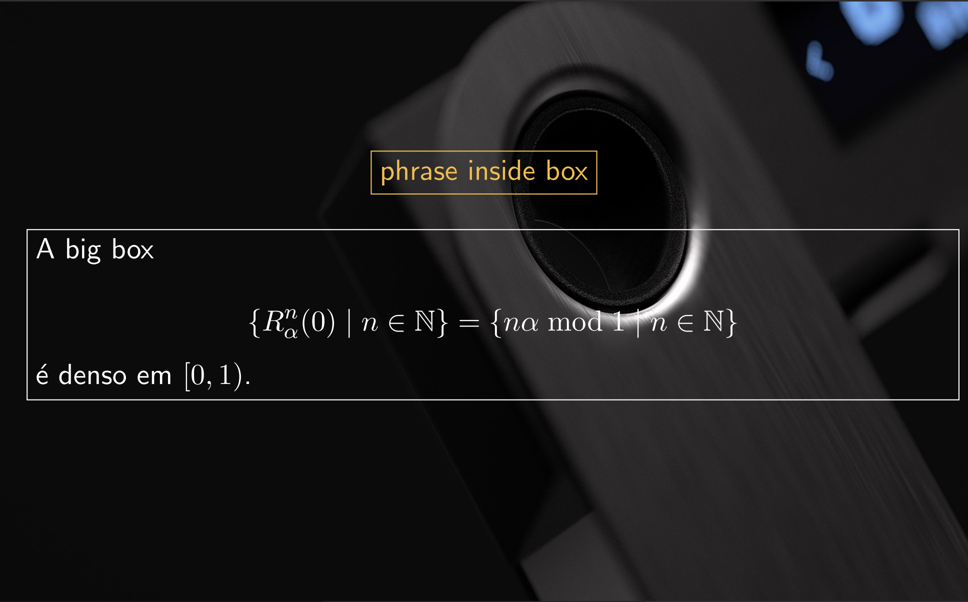
$s = ex + r$

$$X = e^{-1}(sP - R) \overset{?}{\in} \text{DB}$$



boxes and columns

Box



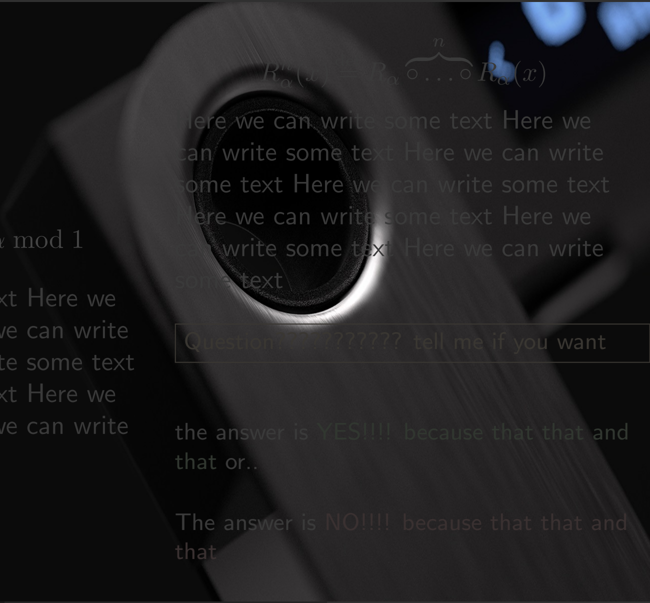
phrase inside box

A big box

$$\{R_\alpha^n(0) \mid n \in \mathbb{N}\} = \{n\alpha \bmod 1 \mid n \in \mathbb{N}\}$$

é denso em $[0, 1)$.

Two Columns entire page



Obs: $\alpha \overset{\text{def}}{=} \log b \in \mathbb{R} \backslash \mathbb{Q}$

$$\begin{aligned} R_\alpha \colon [0,1) &\longrightarrow [0,1) \\ x &\longmapsto x + \alpha \bmod 1 \end{aligned}$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

$$R^n_\alpha(x) = R_\alpha \overbrace{\circ \ldots \circ}^{n} R_\alpha(x)$$

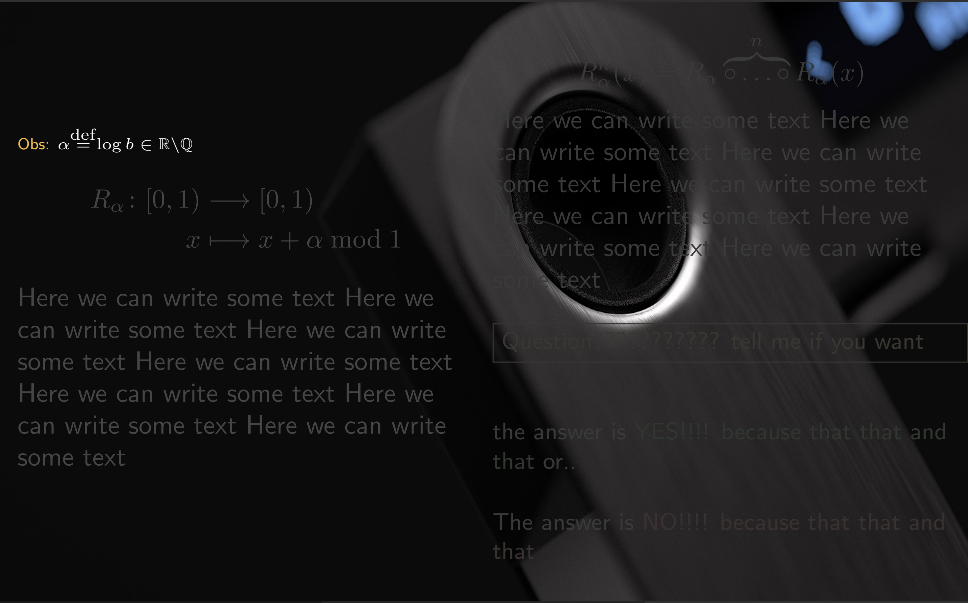
Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

Question????????????? tell me if you want

the answer is YES!!!! because that that and that or..

The answer is NO!!!! because that that and that

Two Columns entire page



Obs: $\alpha \overset{\text{def}}{=} \log b \in \mathbb{R} \backslash \mathbb{Q}$

$$\begin{aligned} R_\alpha : [0,1) &\longrightarrow [0,1) \\ x &\longmapsto x + \alpha \bmod 1 \end{aligned}$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

$$R_\alpha^n(x) = R_\alpha \overbrace{\circ \ldots \circ}^{n} R_\alpha(x)$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

Question??????????? tell me if you want

the answer is YES!!!! because that that and that or..

The answer is NO!!!! because that that and that

Two Columns entire page

Obs: $\alpha \overset{\text{def}}{=} \log b \in \mathbb{R} \backslash \mathbb{Q}$

$$\begin{aligned} R_\alpha : [0,1) &\longrightarrow [0,1) \\ x &\longmapsto x + \alpha \bmod 1 \end{aligned}$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

$$R_\alpha^n(x) \overset{\text{def}}{=} R_\alpha \overbrace{\circ \ldots \circ}^{n} R_\alpha(x)$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

Question??????????? tell me if you want

the answer is YES!!!! because that that and that or..

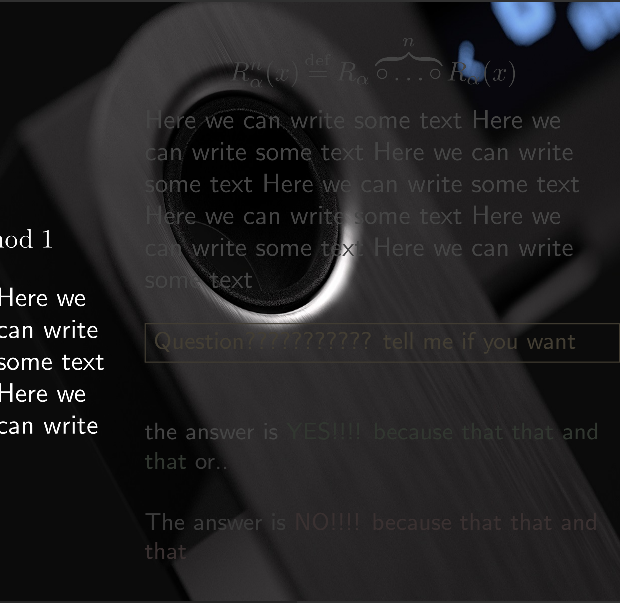
The answer is NO!!!! because that that and that

Two Columns entire page

Obs: $\alpha \overset{\text{def}}{=} \log b \in \mathbb{R} \backslash \mathbb{Q}$

$$\begin{aligned} R_\alpha \colon [0,1) &\longrightarrow [0,1) \\ x &\longmapsto x + \alpha \bmod 1 \end{aligned}$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text



$$R_\alpha^n(x) \overset{\text{def}}{=} R_\alpha \overbrace{\circ \ldots \circ}^{n} R_\alpha(x)$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

Question???????????? tell me if you want

the answer is YES!!!! because that that and that or..

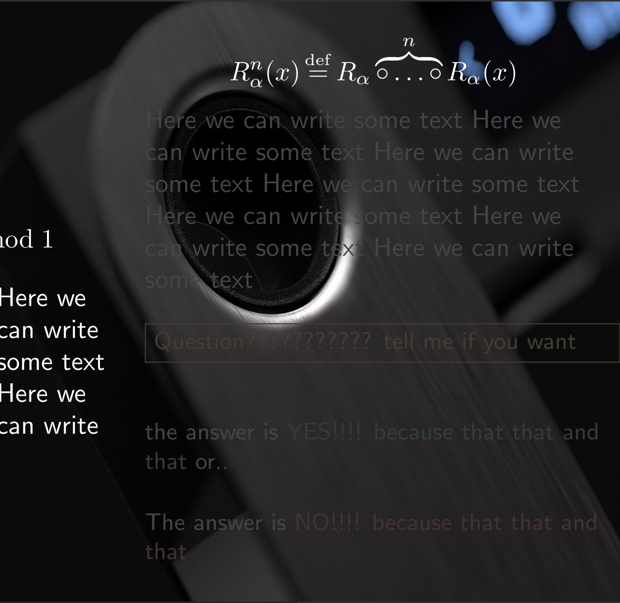
The answer is NO!!!! because that that and that

Two Columns entire page

Obs: $\alpha \overset{\text{def}}{=} \log b \in \mathbb{R}\backslash\mathbb{Q}$

$$\begin{aligned} R_\alpha \colon [0,1) &\longrightarrow [0,1) \\ x &\longmapsto x + \alpha \bmod 1 \end{aligned}$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text



$$R_\alpha^n(x) \overset{\text{def}}{=} R_\alpha \overbrace{\circ \ldots \circ}^{n} R_\alpha(x)$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

Question??????????? tell me if you want

the answer is YES!!!! because that that and that or..

The answer is NO!!!! because that that and that

Two Columns entire page

Obs: $\alpha \overset{\text{def}}{=} \log b \in \mathbb{R}\backslash\mathbb{Q}$

$$\begin{aligned} R_\alpha : [0,1) &\longrightarrow [0,1) \\ x &\longmapsto x + \alpha \bmod 1 \end{aligned}$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

$$R^n_\alpha(x) \overset{\text{def}}{=} R_\alpha \overbrace{\circ \ldots \circ}^{n} R_\alpha(x)$$

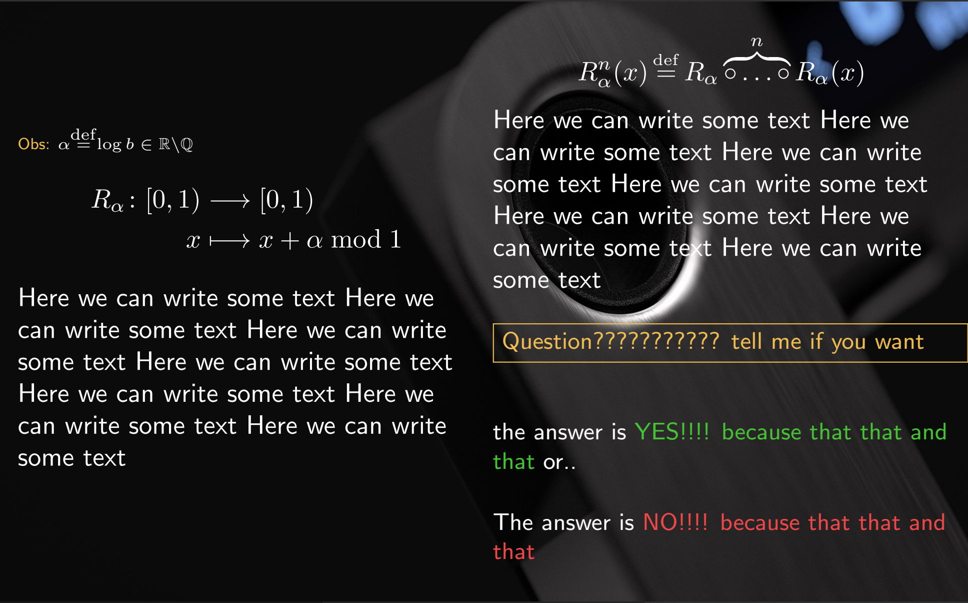
Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

Question?????????? tell me if you want

the answer is YES!!!! because that that and that or..

The answer is NO!!!! because that that and that

Two Columns entire page



Obs: $\alpha \overset{\text{def}}{=} \log b \in \mathbb{R}\backslash\mathbb{Q}$

$$\begin{aligned} R_\alpha \colon [0,1) &\longrightarrow [0,1) \\ x &\longmapsto x + \alpha \bmod 1 \end{aligned}$$

Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

$$R_\alpha^n(x) \overset{\text{def}}{=} R_\alpha \overbrace{\circ \ldots \circ}^{n} R_\alpha(x)$$

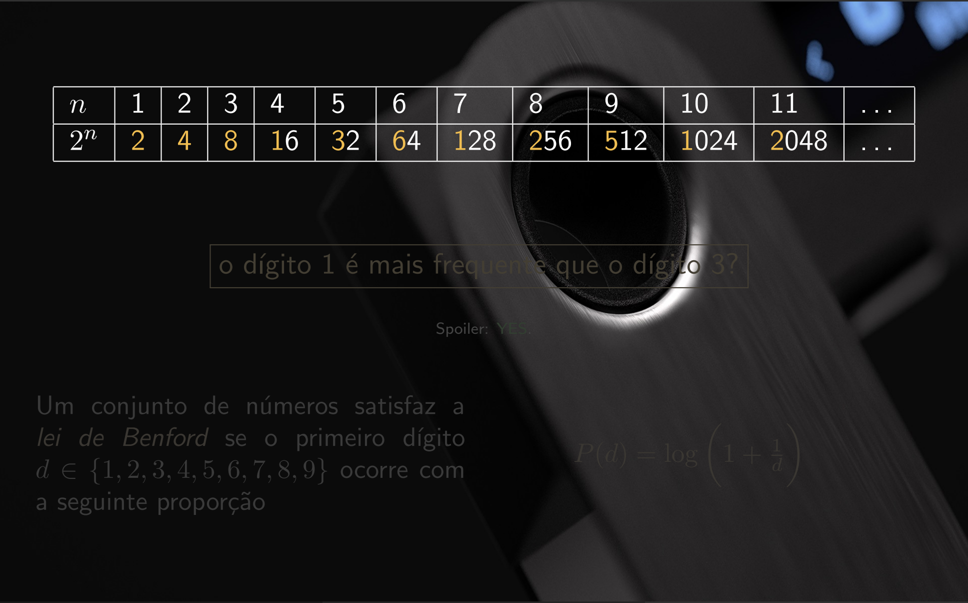
Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text Here we can write some text

Question?????????? tell me if you want

the answer is YES!!!! because that that and that or..

The answer is NO!!!! because that that and that

Table and minipage



n	1	2	3	4	5	6	7	8	9	10	11	$\dots$
2^n	2	4	8	16	32	64	128	256	512	1024	2048	$\dots$

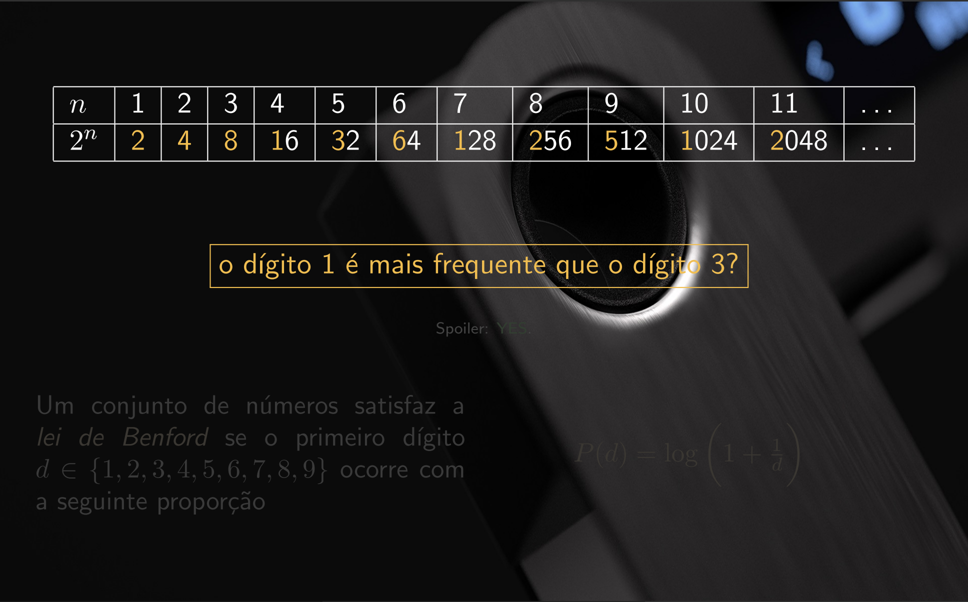
o dígito 1 é mais frequente que o dígito 3?

Spoiler: YES.

Um conjunto de números satisfaz a *lei de Benford* se o primeiro dígito $d \in \{1,2,3,4,5,6,7,8,9\}$ ocorre com a seguinte proporção

$$P(d) = \log\left(1 + \frac{1}{d}\right)$$

Table and minipage



n	1	2	3	4	5	6	7	8	9	10	11	...
2^n	2	4	8	16	32	64	128	256	512	1024	2048	...

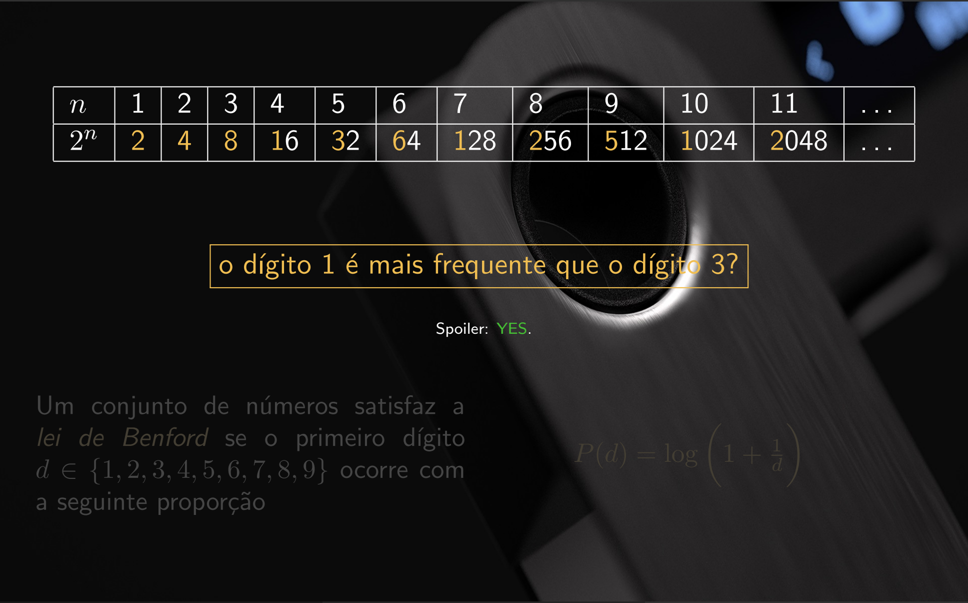
o dígito 1 é mais frequente que o dígito 3?

Spoiler: YES.

Um conjunto de números satisfaz a *lei de Benford* se o primeiro dígito $d \in \{1,2,3,4,5,6,7,8,9\}$ ocorre com a seguinte proporção

$$P(d) = \log\left(1 + \frac{1}{d}\right)$$

Table and minipage



n	1	2	3	4	5	6	7	8	9	10	11	...
2^n	2	4	8	16	32	64	128	256	512	1024	2048	...

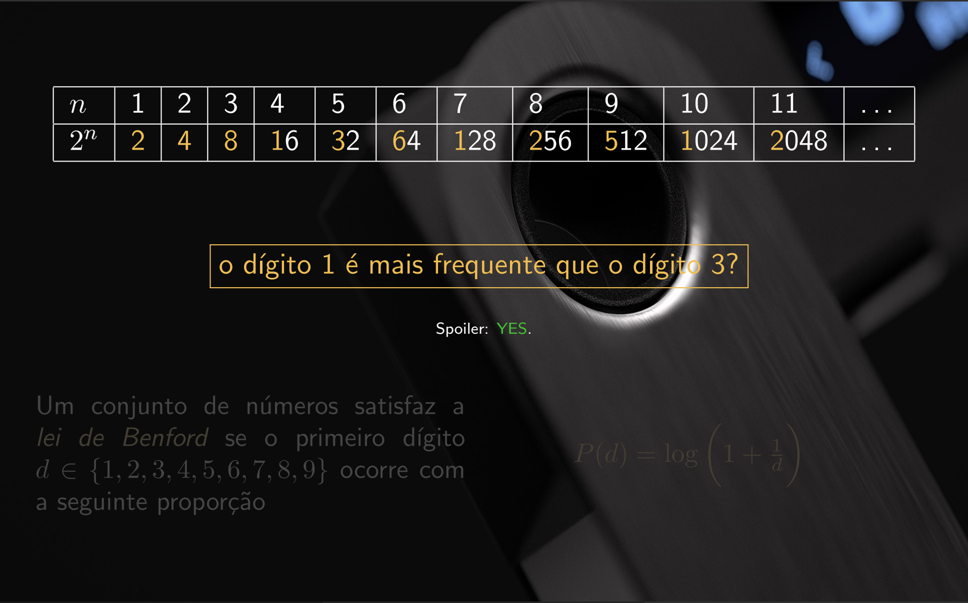
o dígito 1 é mais frequente que o dígito 3?

Spoiler: YES.

Um conjunto de números satisfaz a *lei de Benford* se o primeiro dígito $d \in \{1,2,3,4,5,6,7,8,9\}$ ocorre com a seguinte proporção

$$P(d) = \log\left(1 + \frac{1}{d}\right)$$

Table and minipage



n	1	2	3	4	5	6	7	8	9	10	11	...
2^n	2	4	8	16	32	64	128	256	512	1024	2048	...

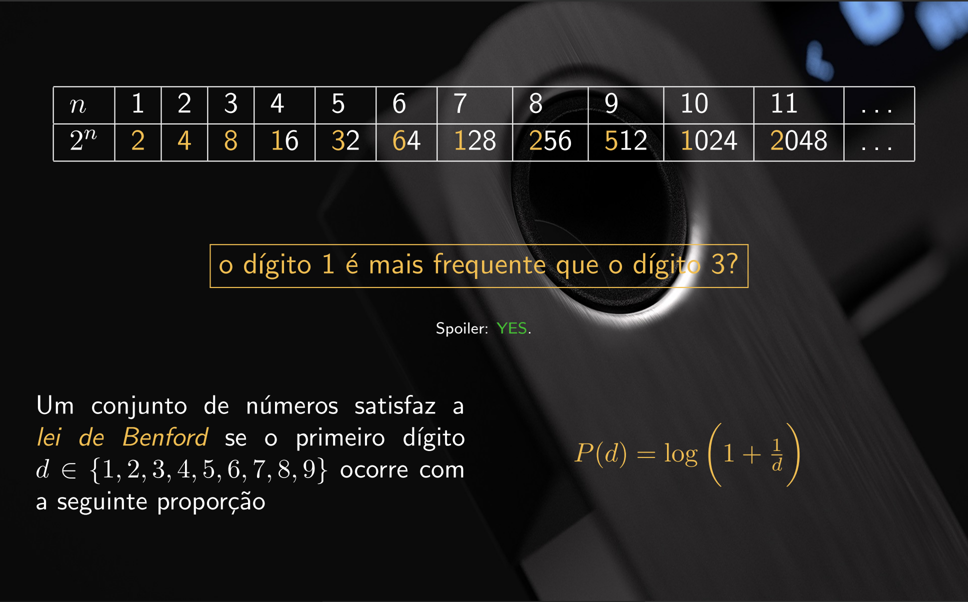
o dígito 1 é mais frequente que o dígito 3?

Spoiler: YES.

Um conjunto de números satisfaz a *lei de Benford* se o primeiro dígito $d \in \{1,2,3,4,5,6,7,8,9\}$ ocorre com a seguinte proporção

$$P(d) = \log\left(1 + \frac{1}{d}\right)$$

Table and minipage



n	1	2	3	4	5	6	7	8	9	10	11	$\dots$
2^n	2	4	8	16	32	64	128	256	512	1024	2048	$\dots$

o dígito 1 é mais frequente que o dígito 3?

Spoiler: YES.

Um conjunto de números satisfaz a *lei de Benford* se o primeiro dígito $d \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ocorre com a seguinte proporção

$$P(d) = \log\left(1 + \frac{1}{d}\right)$$

Questions ?