23.10.2024

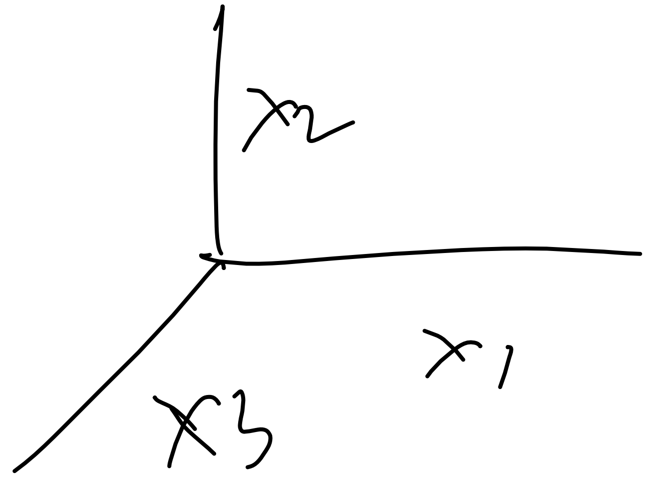
Polynomial Identity Testing :

x_3 $\quad P(x_1, x_2) = x_1 - x_2.$

(α, α).

"finite fields"

$\frac{\deg(P)}{|S|}$



$\mathbb{R}^3$ $\quad \underbrace{x_3 - x_1 + x_2 = 0}$

$$P(x_1, \dots, x_n) = x_1^k \underbrace{Q(x_2, \dots, x_n)}_{\wedge} + R(x_1, \dots, x_n)$$

$x_1^{<k}$

$$(r_1, \dots, r_n) \longrightarrow (\underbrace{-, r_2, \dots r_n}_{})$$

$$(r_1, - \dots -)$$

$$= x_1^k Q(r_2, \dots, r_n) + R(x_1, r_2, \dots r_n)$$

$$E: \; Q(r_2, \dots, r_n) = 0, \quad \le \frac{\deg(Q)}{|S|}$$

$$F|E: \; \underline{r_1^k Q(r_2, \dots, r_n) + R(r_1, r_2 \dots, r_n) = 0}$$

$$\leq \frac{\deg(P) - \deg(Q)}{|S|}.$$

$$\underline{\overline{F} \wedge \overline{E}} \Rightarrow P(r_1, \ldots r_n) \neq 0.$$

$$P(r_1, \ldots r_n) = 0 \Rightarrow F \vee E.$$

$$\underline{\Pr[P(r_1, \ldots r_n) = 0]}$$

$$\leq \Pr[F \vee E]$$

$$= 1 - \Pr[\overline{F} \wedge \overline{E}]$$

$$= 1 - \underbrace{\Pr[\overline{E}]}_{\geq} \cdot \underbrace{\Pr[\overline{F} \mid \overline{E}]}_{\geq}$$

rough

$\underline{A} \Rightarrow \underline{B}$

$\underline{\Pr[B] \geq \Pr[A]}.$

$$\leq 1 - \left(1 - \frac{\deg(Q)}{|S|}\right) \cdot \left(1 - \frac{\deg(P) - \deg(Q)}{|S|}\right).$$

$$= \frac{\deg(P)}{|S|} - \left(\qquad \right)$$

$$\leq \frac{\deg(P)}{|S|}.$$

$\Rightarrow$ The induction step holds!

One-sided error

- if $P \equiv 0 \Rightarrow$ never commit a mistake.
- if $P \not\equiv 0 \Rightarrow$ commit a mistake w.p. $\leq \frac{\deg(P)}{|S|}$.

repeat r times:

$$\left(1 - \frac{\deg(P)}{|S|}\right)^{r}$$

$e^{x} \geq 1+x$

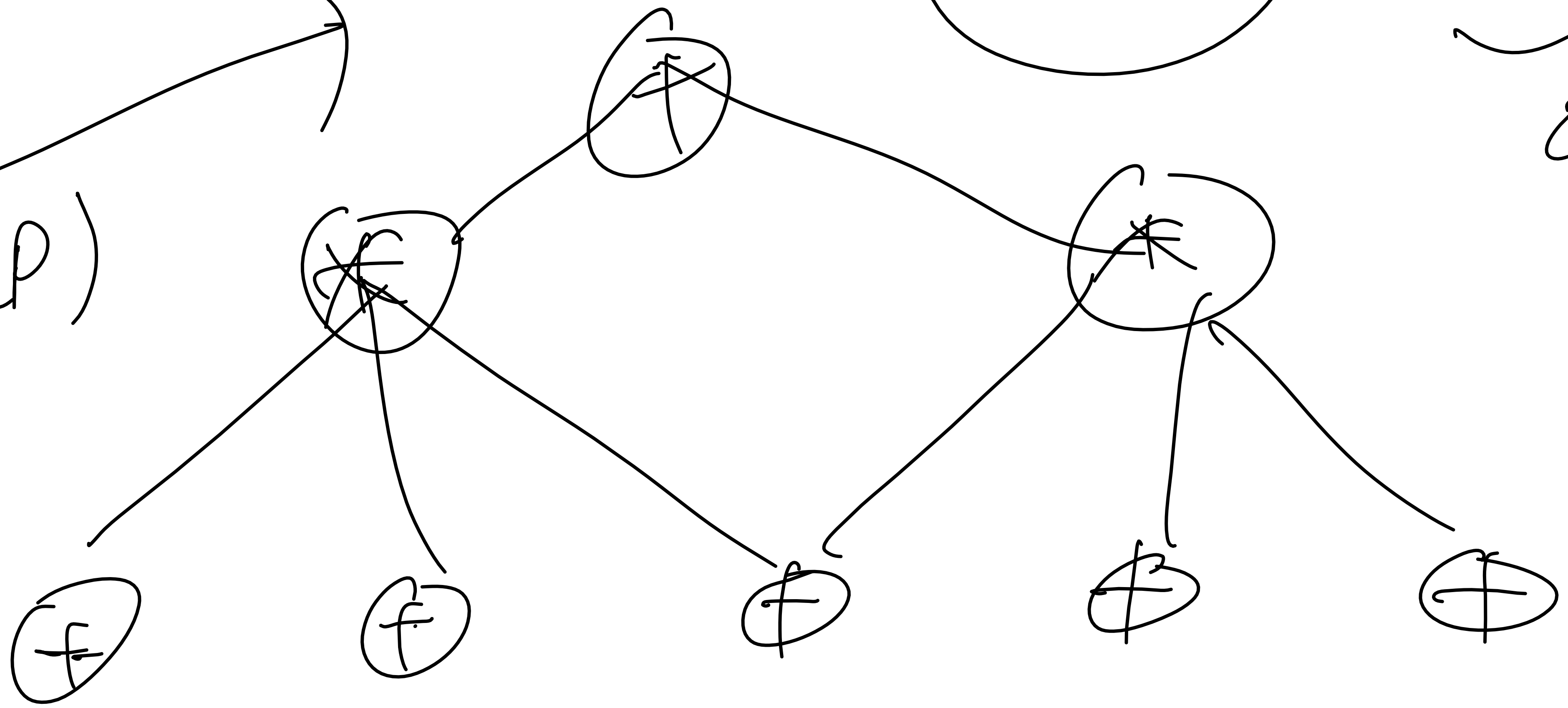
$$\leq e^{-\frac{\deg(P)}{|S|} \cdot r} \leq \delta.$$

$$r \geq \ln\frac{1}{\delta} \cdot \frac{|S|}{\deg(P)}$$ suffices.

time complexity: $O\left(\ln\frac{1}{\delta} \frac{|S|}{\deg(P)}\right)$ many evaluations!

$O(n)$.

$$|S| \geq 2\deg(P)$$



2^n many monomials!.

Success prob: $\geq 1-\delta$ if $P \not\equiv 0$.

always if $P \equiv 0$

No deterministic algo. for PIT known till date!

Radonized Data Structures

	Hashing	expected complexity
- insert	$O(\log n)$	$O(1)$
- search	$O(\log n)$	$O(1)$
- delete.	$O(\log n)$	$O(1)$.
	AVL Tree	hashing.

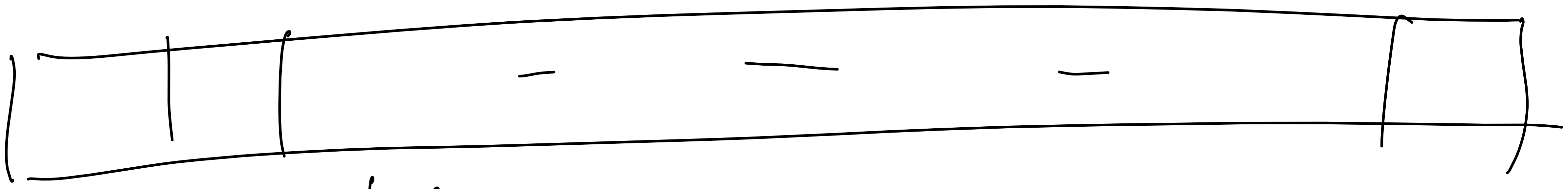
n = size of database.

Cyber Security:

blacklist of IP address.

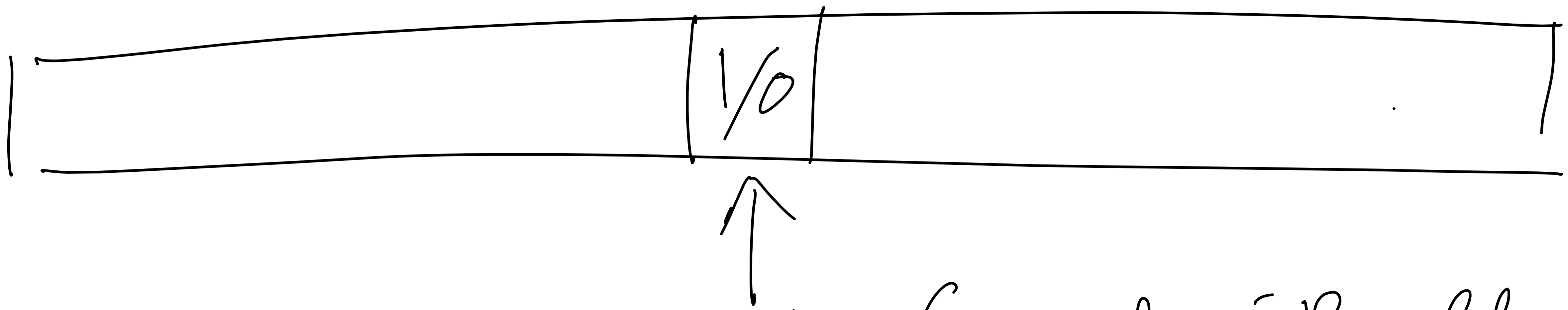
1000

One idea:



linked list.

Second idea:



entry for each IP addr.

32 bit.

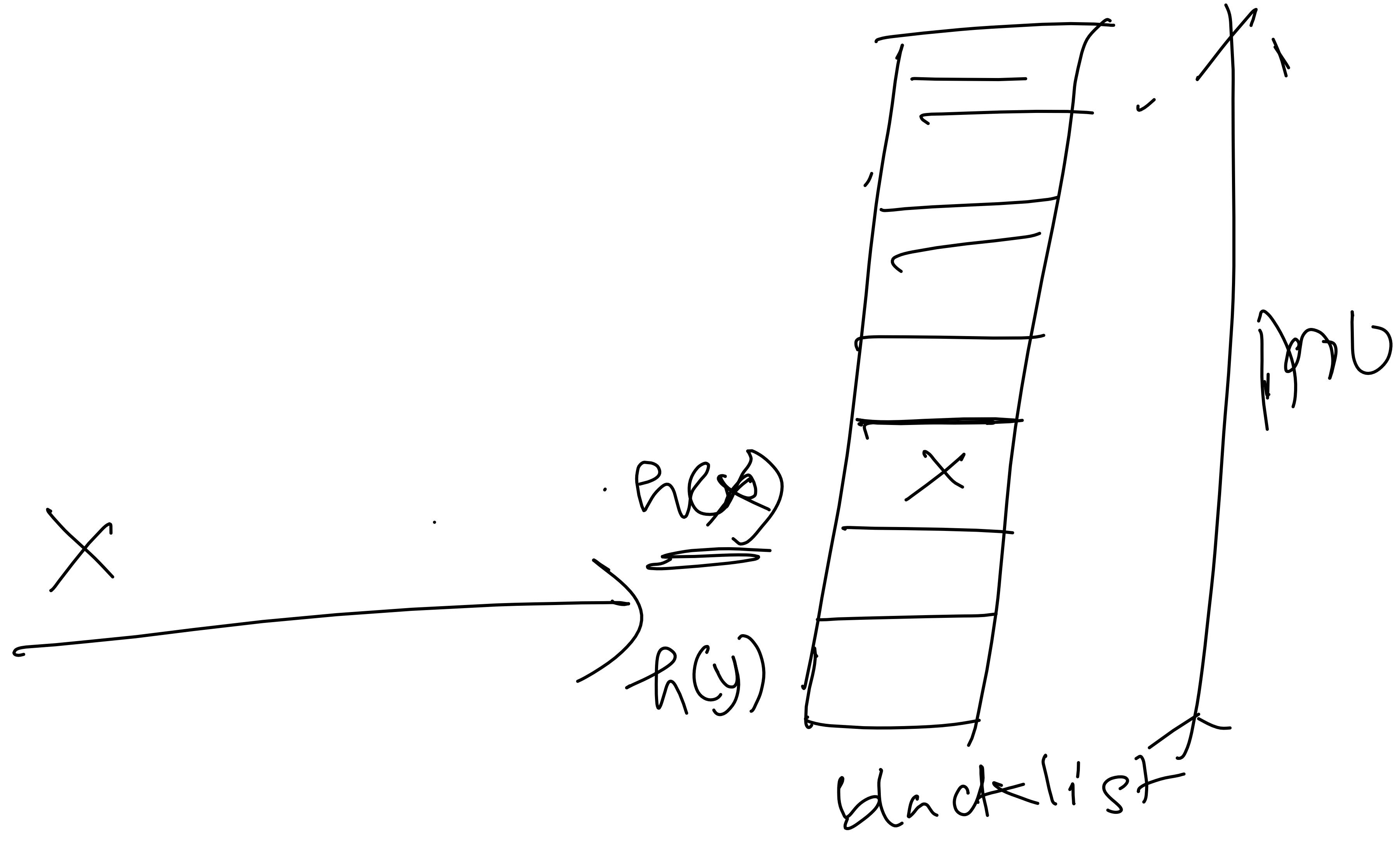
2^{32} size array : huge waste of space.

$h(x) \longrightarrow$ index of another array

black list.

ip address.

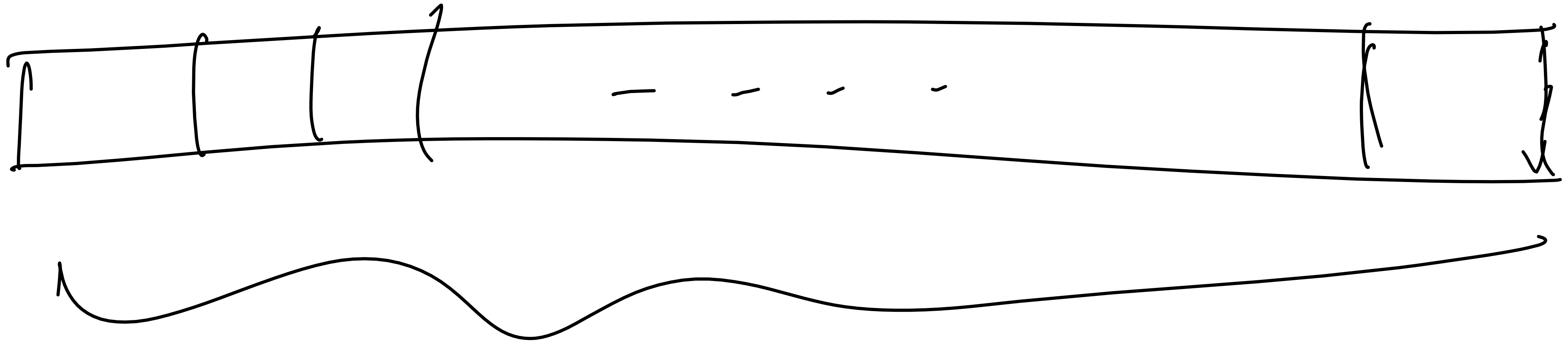
h :



1000 IP address

one bad.

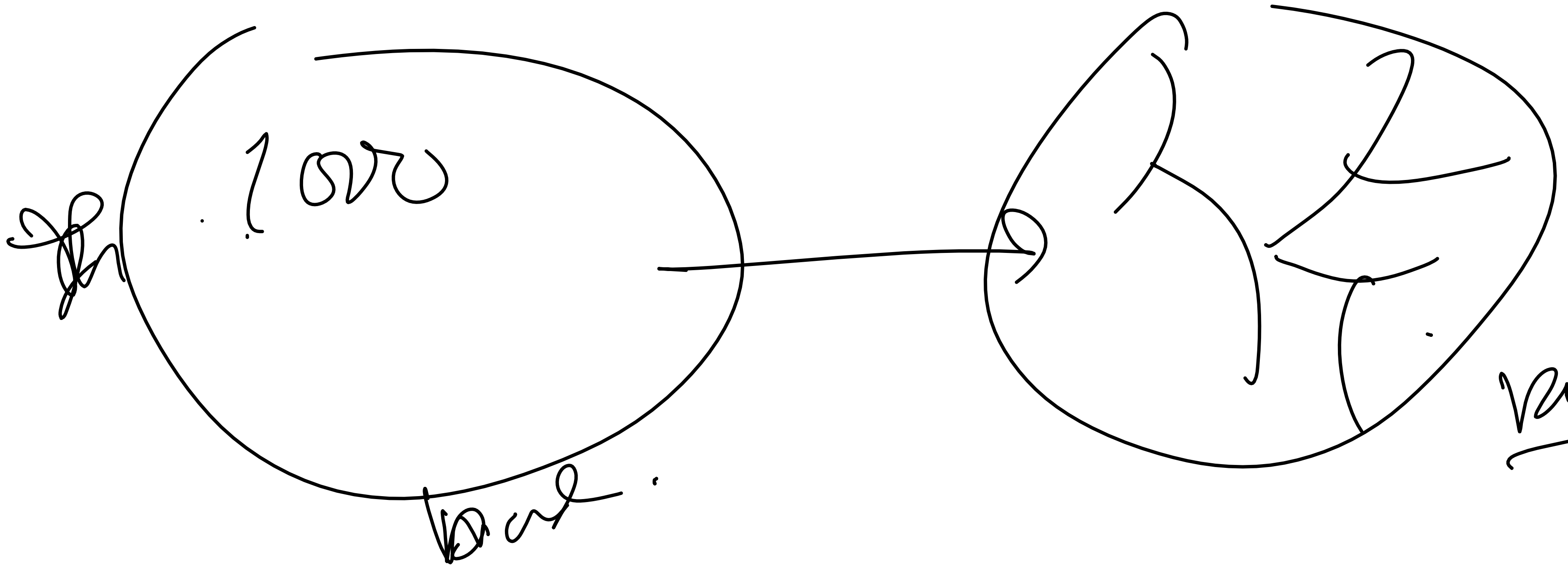
Ideally what do we want?



array of size 1000.

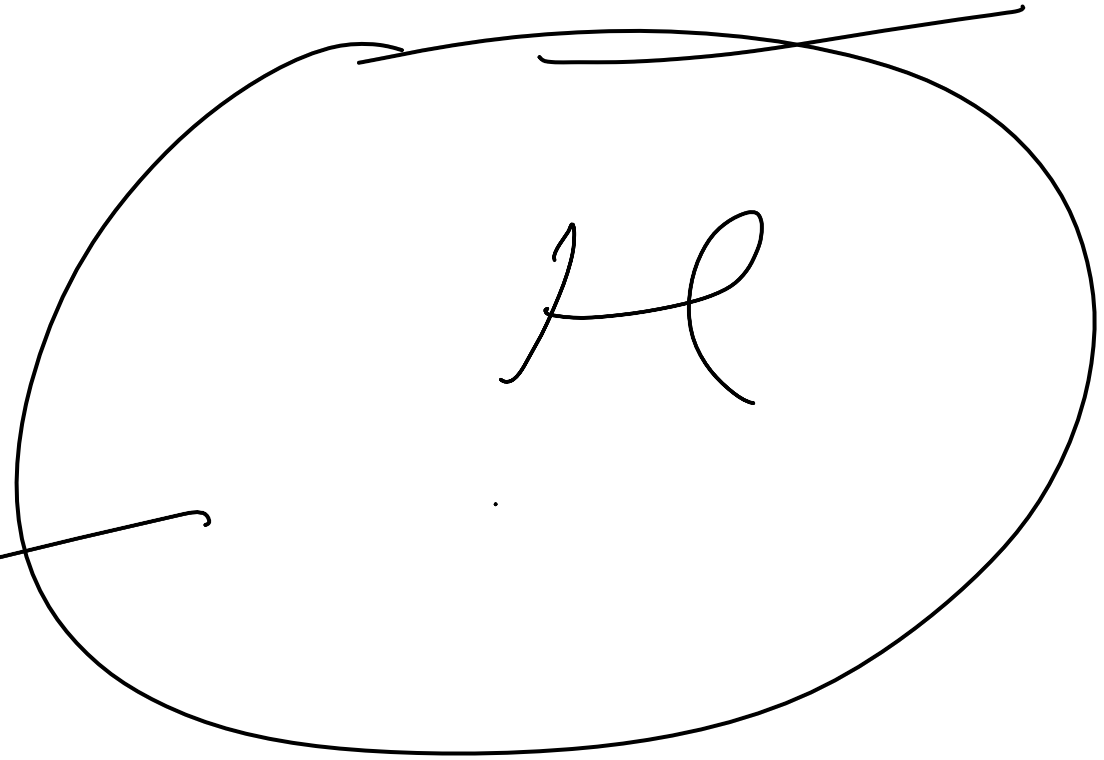
fix a mapping $1000 \to 1000$.

What is the problem?



random mappings

$x \rightarrow h(x)$



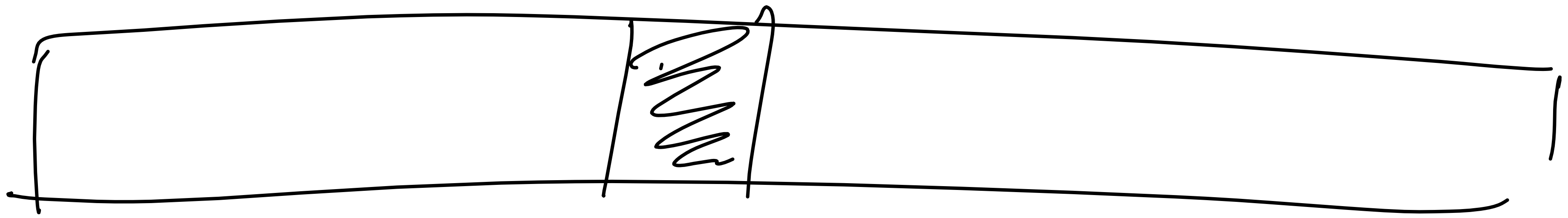
$h \in \mathcal{H}$

- each function is deterministic
- you choose a function randomly from big $\mathcal{H}$.

$2^{32} \longrightarrow 1000.$

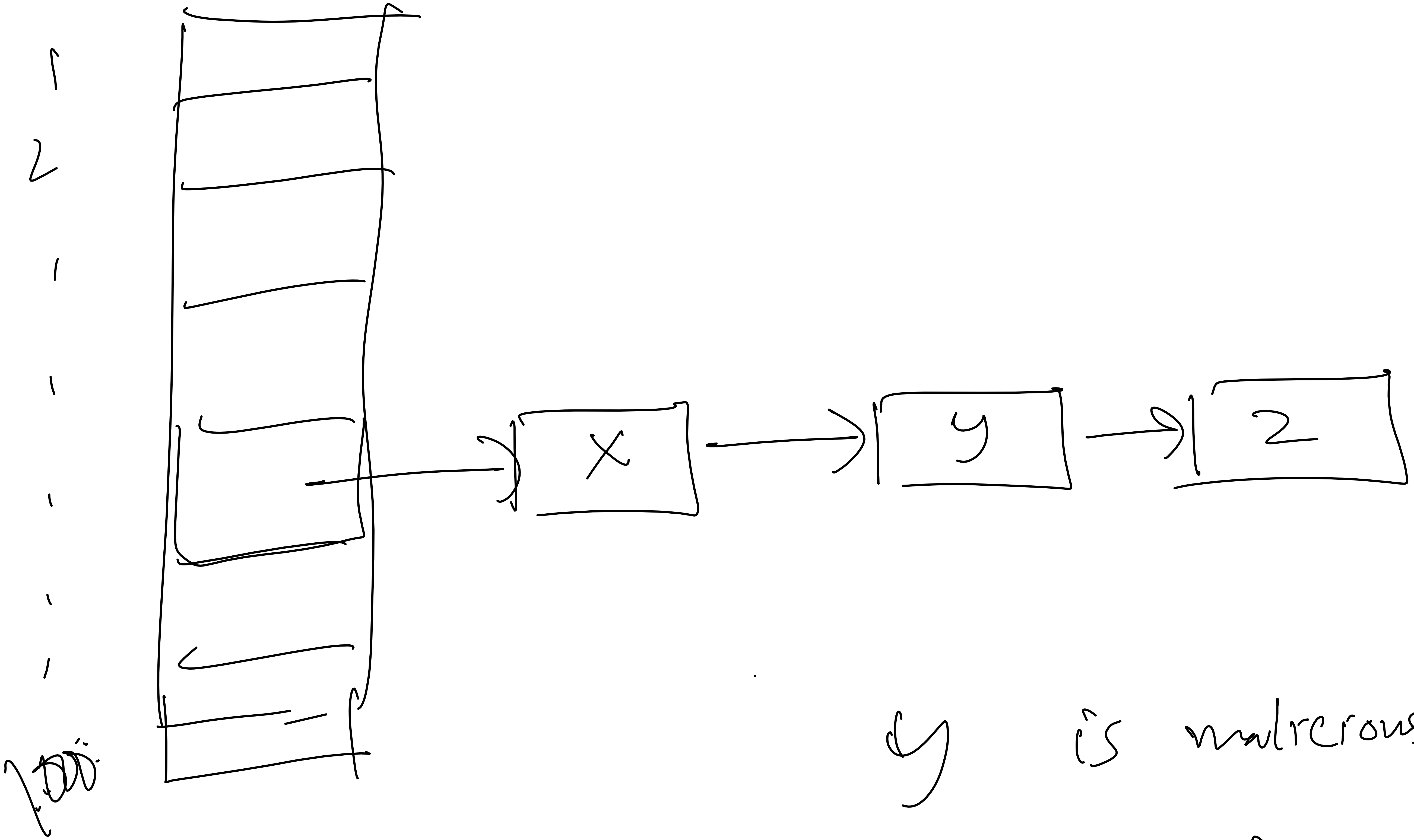
$G\left(2^{32}/1000\right)$

Collision



$x, y \qquad G(x) = G(y)$

$h(x) = h(y) = h(z)$



y is malicious.

$w \quad h(w) = h(x) = h(y) = h(z).$

w is a good user!

Ideal ~~ly~~ properties of hash function.

(1) it should minimize the collision!

(2) it should be easy to compute!

$$h : U \longmapsto \{1, \ldots, M\} = [M]$$

huge size

$|M|$ is small.

Gold Standard for ~~stats~~ hashing :

Universal family of hash functions (universal hashing).

$\mathcal{H}$: be a big class of hash functions each hash function mapping $U \to [M]$.

Def^n [Universal family] : A family of hash functions $\mathcal{H}$ is called universal if $\forall x, y \in U$.

$$\Pr_{h \in \mathcal{H}} \left[h(x) = h(y) \right] \leq \frac{1}{M}.$$

universal

	a	b
h_1	0	0
h_2	0	1

	a	b
h_1	0	1
h_2	1	0

universal.

$\leq \frac{1}{2}$

	a	b	c
h_1	0	0	1
h_2	1	1	0
h_3	1	0	1

not universal family.

$x = a,\ y = b.$

$h : U \to$ ~~[illegible]~~ $\{0, 1\}$

$U = \{a, b, c\}$.

b

	a	b
h_1	0	0
h_2	1	0
h_3	0	1

universal

	a	b
h_1	0	0
h_2	1	1

not universal.

Why are universal families interesting

Claim: Let $x_1, x_2, \ldots, x_n$ be any sequence of items.
(think of n inserts back to back).

If we choose $h \in \mathcal{H}$ randomly where $\mathcal{H}$ is universal

$h : U \to [M]$.

$$\boxed{\mathbb{E}[\#\text{ collision}] < \frac{n}{M}}$$