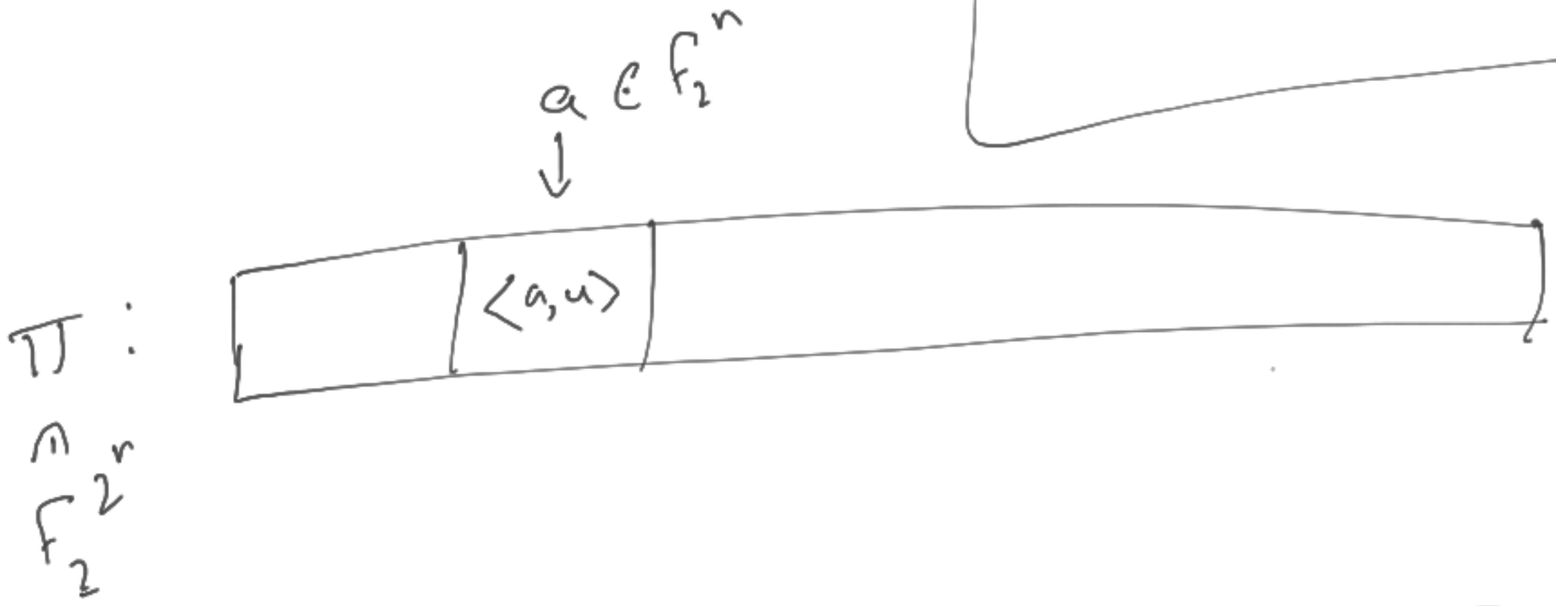
Simple PCP for ML

Given $A \in \mathbb{F}_2^{m \times n}$, $b \in \mathbb{F}_2^m$,
does there exist $u \in \mathbb{F}_2^n$: $Au = b$?

A - full rank



V^{Π}: Pick $r \leftarrow \mathbb{F}_2^m$, check that $\Pi[r^T A] = r^T b$

$Au = b \Rightarrow \forall r \in \mathbb{F}_2^m : r^T A u = r^T b \Rightarrow H_u[r^T A] = r^T b$

If no such u: if $\Pi = H_v$ for some v, $\Pr_r[\Pi[r^T A] = r^T b] = \frac{1}{2}$

Error-Correcting Code

$\forall u \in \mathbb{F}_2^n \longrightarrow Hu$

$\forall$ distinct u, v : Hu and Hv differ on at least $\frac{1}{2}$ locations

Sender

u Hu —noisy→ Receiver

noisy Hu

Can still recover u

u

$l_u(a) = \langle a, u \rangle$

message → multivariate linear fn.

Hadamard code

message → univariate low-degree polynomials

Reed-Solomon code

multivariate low-degree polynomials

Reed-Muller code

Local Testing Hadmard Code (Linearity Testing)

$\exists V : \Pi[a] = H_V[a]$ for atleast 0.99 fraction of $a \in F_2^n$

$\exists$ linear function $\ell : F_2^n \to F_2$ s.t. for at least 0.99 frac of $a \in F_2^n$: $\Pi[a] = \ell(a)$

L^{Π} : 1. Sample $a, b \in F_2^n$

2. Check that $\Pi[a] \oplus \Pi[b] = \Pi[a \oplus b]$

Thm: $\exists$ L^{Π} that makes $O(1)$ queries to Π, runs in $O(n)$ time, and:

- If $\Pi = H_v$ for some $v \in F_2^n$, L^{Π} always accepts
- If, for all $v \in F_2^n$, Π and H_v differ in at least 0.01 fraction of locations, L^{Π} accepts with prob. ≤ 0.01

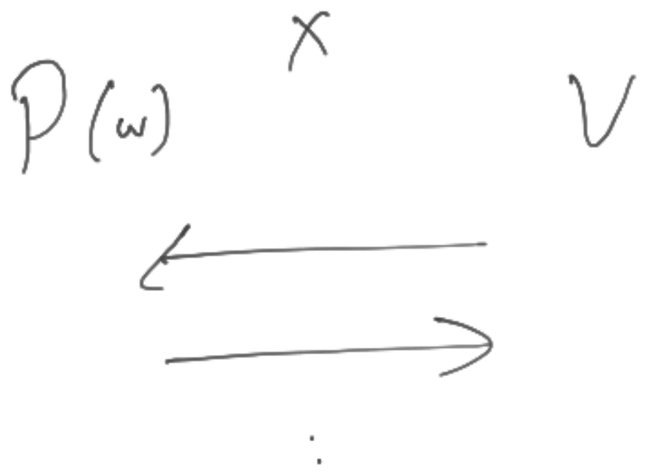
$A, b \quad \exists u : Au = b$?

Π : H_u

V^{Π} : 1. Run 2^{Π} to check $\Pi \approx H_u$ for some u

2. Sample $r \in F_2^m$, check $\Pi[r^T A] = r^T b$

Arguments:

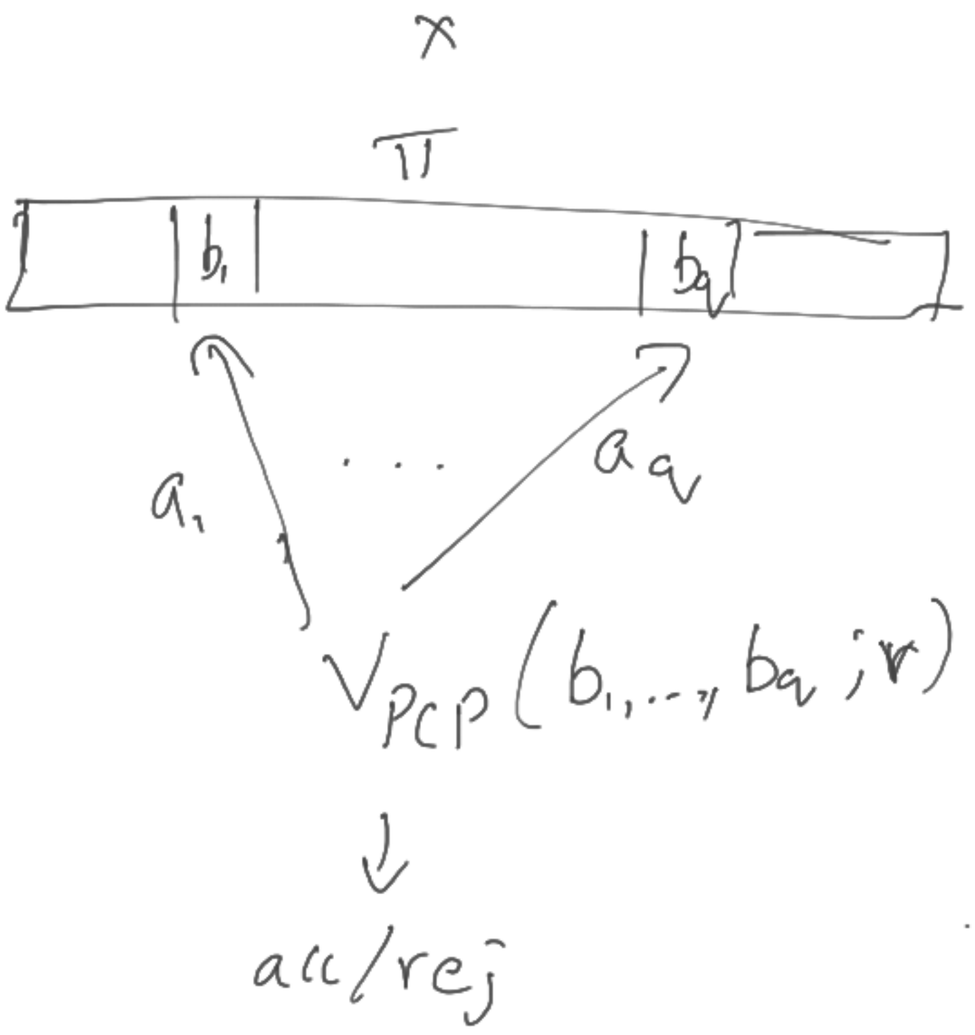


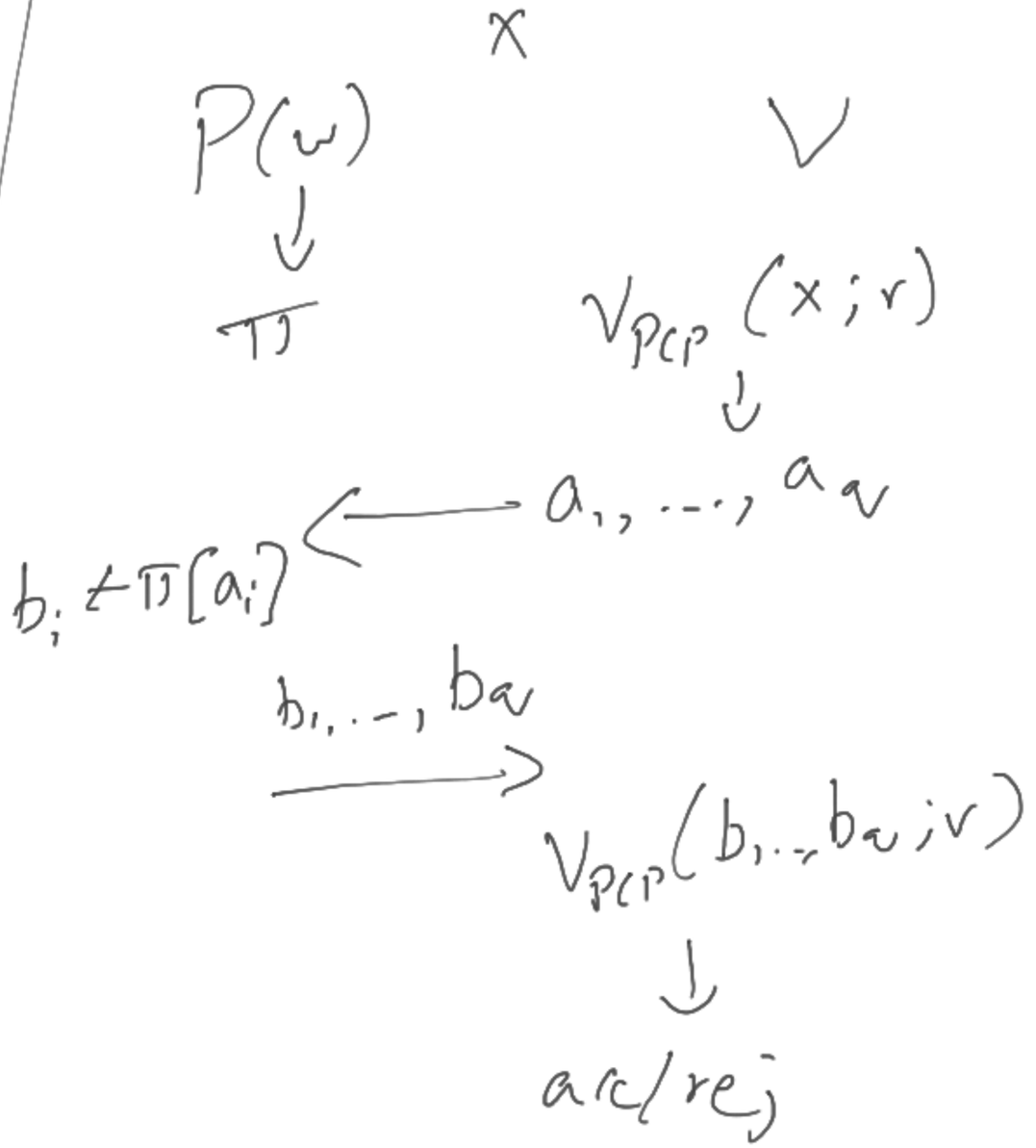
P, V both randomised polynomial time

Completeness: If $x \in L$ $\exists w$ s.t.
$\langle P(w), V \rangle(x)$ accepts w.p. $\geq 1 - \text{negl}(|x|)$

Soundness: If $x \notin L$, then
for any poly-time P^*:
$\langle P^*, V \rangle(x)$ accepts w.p. $\leq \text{negl}(|x|)$

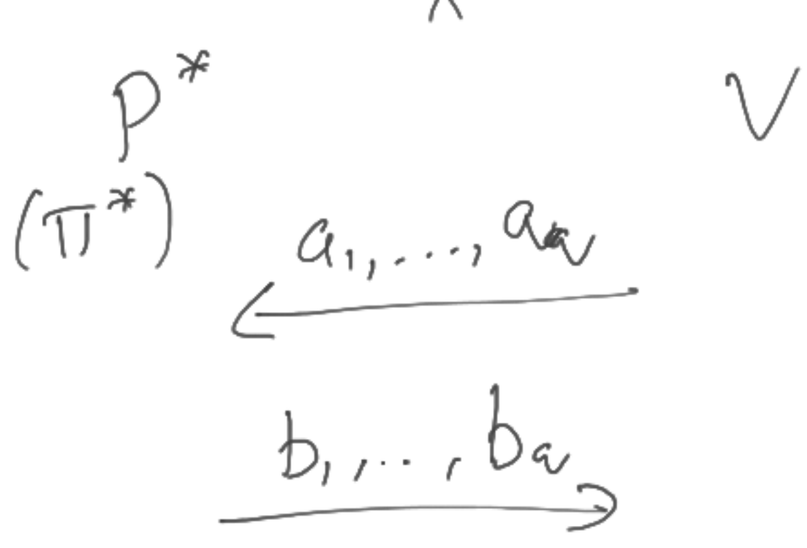
Arguments from PCPs:





If P is always honest $\longrightarrow$ $\langle P, V \rangle$ is an IP

If P^* is consistent $\longrightarrow$ $\langle P, V \rangle$ is an IP



P^* is consistent if

$\exists\ \pi^*$ s.t. for any a_i,

$b_i = \pi^*[a_i]$

Collision-Resistant Hash Function

$$H = \{ h : \{0,1\}^m \longrightarrow \{0,1\}^n \}$$

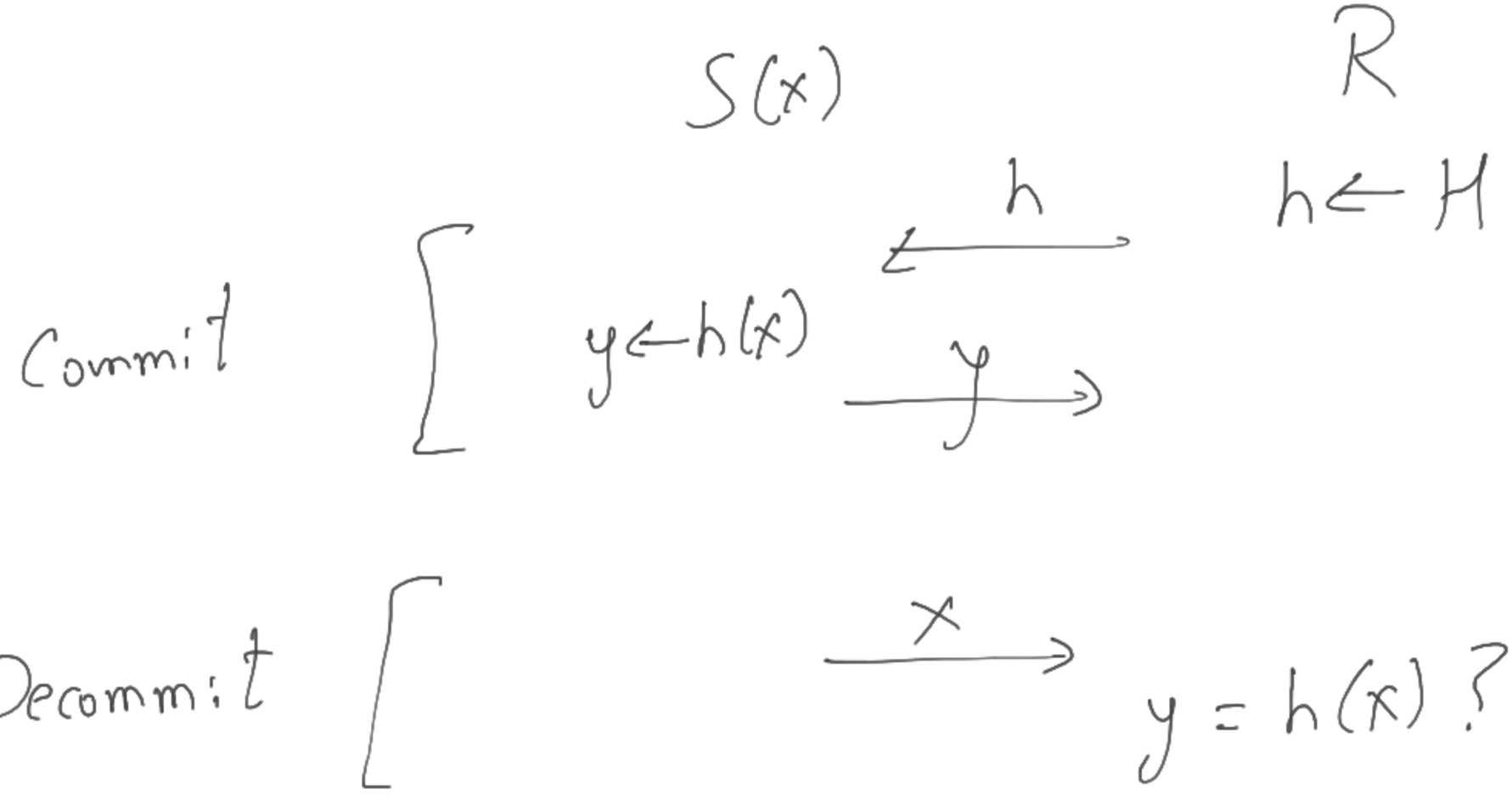
- Shrinking: $n << m$
- Collision Resistance: $\forall$ PPT $\mathcal{A}$: if $h \leftarrow H$ and

$$(x, x') \leftarrow \mathcal{A}(h),$$

$$Pr[x \neq x' \wedge h(x) = h(x')] < negl(n)$$

- Efficiency: Can sample $h \in H$ and evaluate it in poly time

Given CRHF $H = \{h : \{0,1\}^m \to \{0,1\}^n\}$

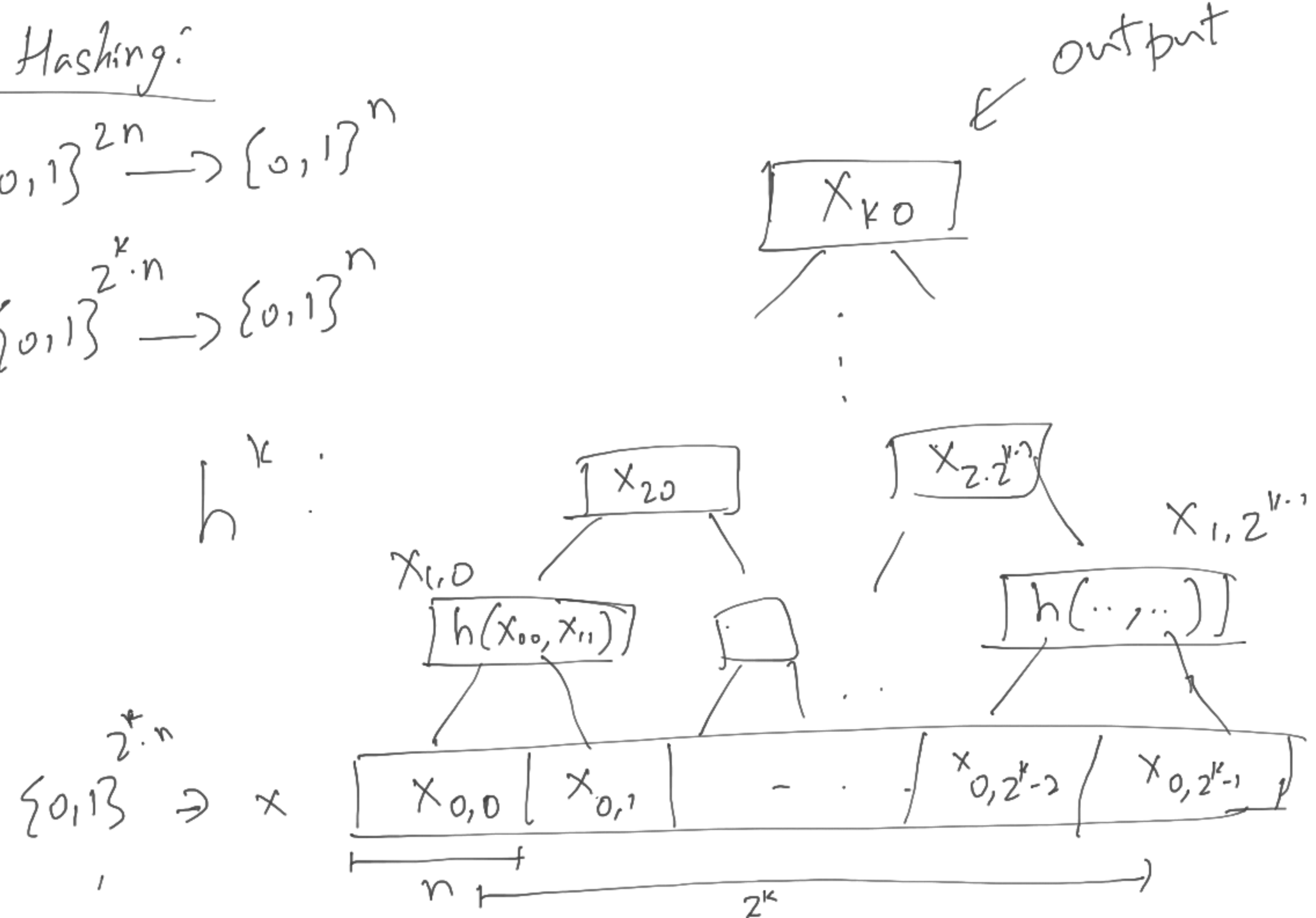


Merkle Hashing:

$h: \{0,1\}^{2n} \longrightarrow \{0,1\}^n$

$k \in \mathbb{N}$

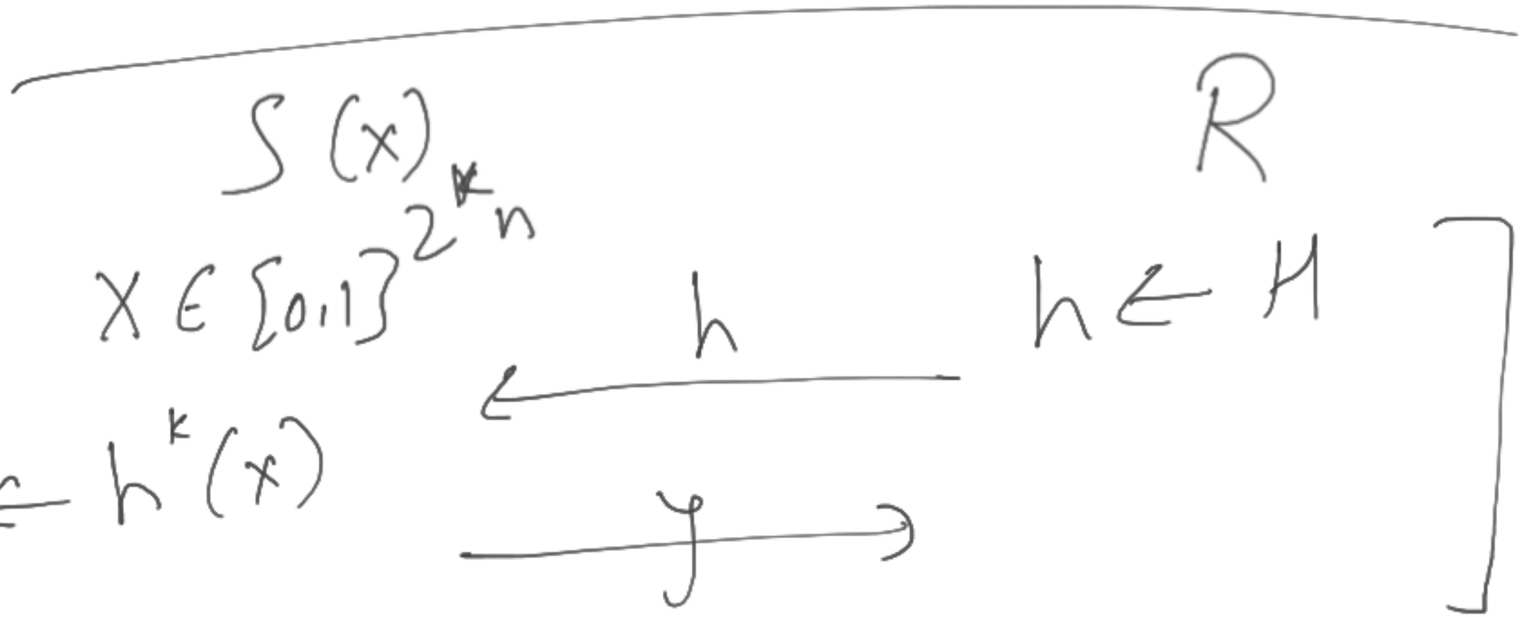
$h^k: \{0,1\}^{2^k \cdot n} \longrightarrow \{0,1\}^n$



$$H = \{h : \{0,1\}^{2n} \to \{0,1\}^n\} \longrightarrow H^k = \{h^k : \{0,1\}^{2^k n} \to \{0,1\}^n\}$$

- If H is CRHF, so is H^k
  (if $k = O(\log n)$)

CRHF $H = \{h : \{0,1\}^{2n} \to \{0,1\}^n\}$

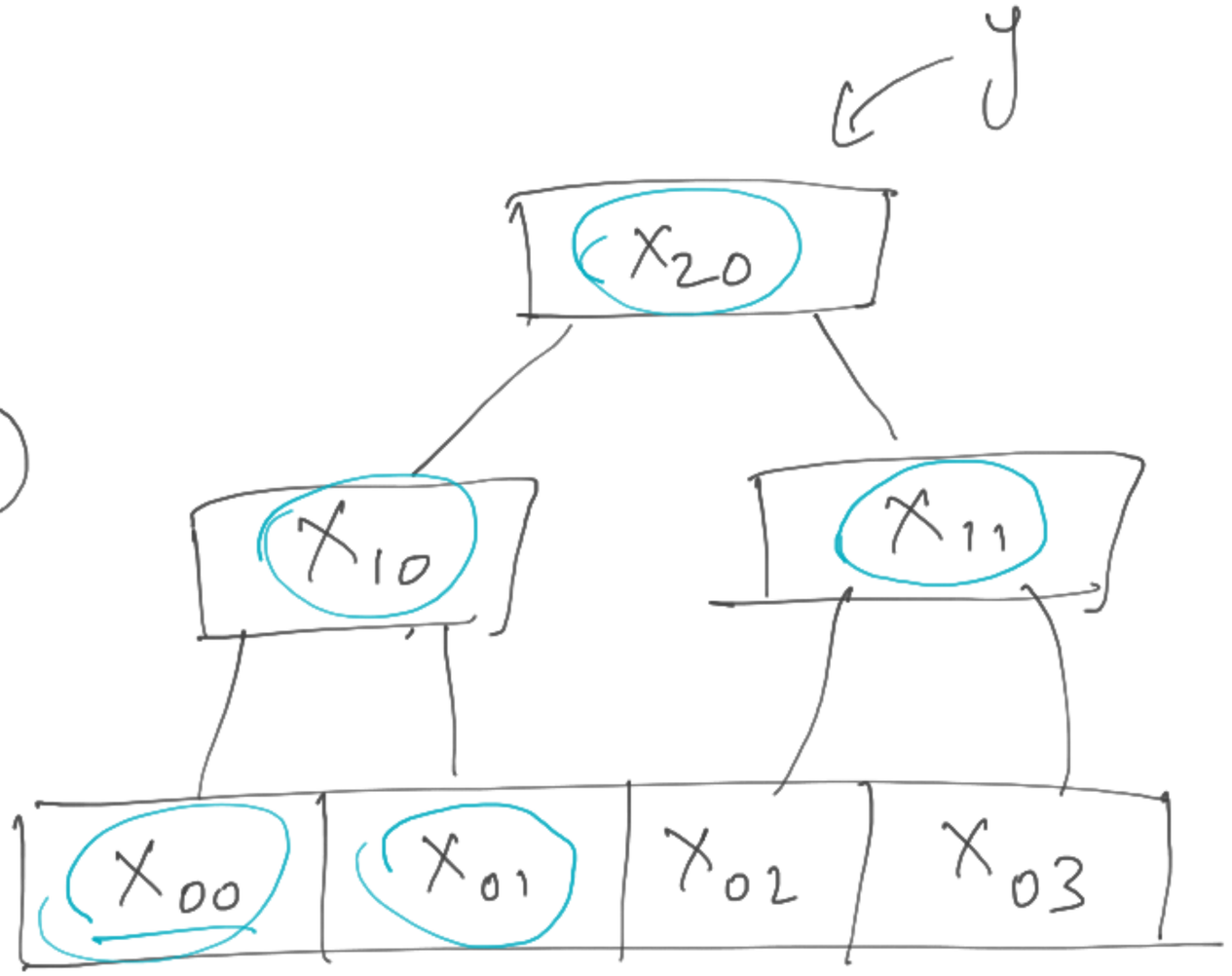


To decommit x_{0i}, send hash values along path from x_{0i} to x_{k0}, along with siblings → Check hashes along this path, and that root is the same as y (Decommit)

$k = 2$

$|x| = 2^k \cdot n$

want: $O(kn)$



$x_{20} = h(x_{10}, x_{11})$

$x_{10} = h(x_{00}, x_{01})$

$x_{11} = h(x_{02}, x_{03})$