From last lab:

1) Deleting the last bit of key
2) Setting the last bit to 0

Deleting

$\rho_{ideal} = 2^{-n}\sum_k |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes \rho_E$

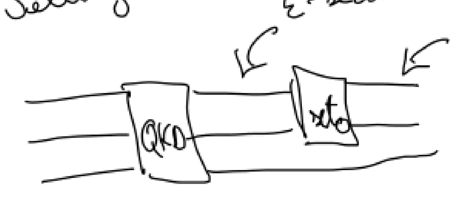
$tr_{last}\, \rho_{ideal} = 2^{-n}\sum_k tr_{last} |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes \rho_E = 2^{-(n-1)} \sum_{k\in\{0,1\}^{n-1}} |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes \rho_E \in S^{(n-1\text{ bits})}_{Ideal}$

$n=2$, no ρ_E

$tr_{last} \sum_{k\in\{0,1\}^2} 2^{-2}|k\rangle\langle k| = 2^{-2}\left(tr_{last}\, |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|\right) =$

$= 2^{-2}\left(2|0\rangle\langle 0| + 2|1\rangle\langle 1|\right) = \frac{1}{2}\left(\sum_{k\in\{0,1\}} |k\rangle\langle k|\right)$

Setting the bit to 0



After setting to 0: (in last case) this we keep

$\rho_{real} = 2^{-n}\sum_{k\in\{0,1\}^{n-1}} |k0\rangle\langle k0| \otimes |k0\rangle\langle k0| \otimes \cancel{\rho_E}$

keep last bit

$2^{-n}\sum_{k\in\{0,1\}^n} |k\rangle\langle k| \otimes |k\rangle\langle k| = \rho_{ideal}$

Is this close to any ρ_{ideal}? Simplify by deleting ρ_E

$TD(\rho_{real}, \rho_{ideal}) \geq TD(\mathcal{E}(\rho_{real}), \mathcal{E}(\rho_{ideal})) = TD\left(|0\rangle\langle 0|, \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right) =$

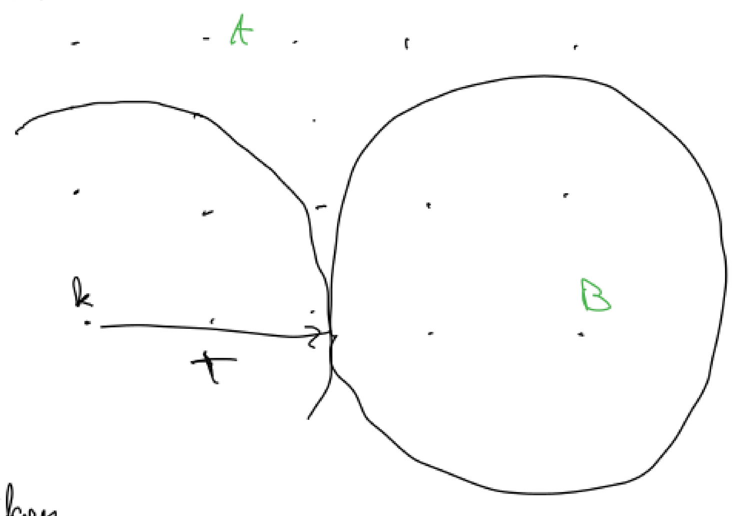
$= \left\| \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix} \right\| = \left(\frac{1}{2} + \frac{1}{2}\right)\frac{1}{2} = \frac{1}{2}$

Error Correction -> RND Extraction

What if RND Extraction -> Error correction

$k_1 \neq k_2$ $\geq t$ errors

$H(k_1)$ $H(k_2)$



$H: \{0,1\}^* \to \{0,1\}^l$

$H(\cdot) = 0$

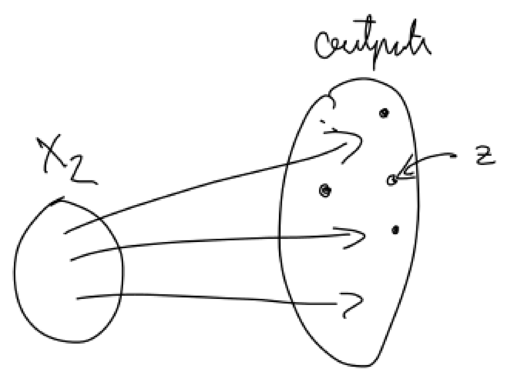
* Uniform
* One - way $\Pr\left[x \xleftarrow{\$} X, x' \leftarrow A(h(x)) : h(x') = h(x)\right] = negl$

---

n bit

$x = (\underbrace{x_1}_{n-k} \,||\, \underbrace{x_2}_{k})^T$ $x = x_1 + x_2$

n-k: Eve knows; k: Entropy of the key; Secret



$H: \{0,1\}^n \to \{0,1\}^l$ $\underline{l > k}$

$A \xleftarrow{\$} M^{l\times n}_{\mathbb{F}_2}$

$H(x) = Ax$ uniform hash function

$y = H(x) = Ax = A(x_1 + x_2) = \underbrace{Ax_1}_{\text{Eve knows}} + Ax_2$

$\langle z, y\rangle = \langle z, Ax_1\rangle + \underbrace{\langle z, Ax_2\rangle}_{0} = \underbrace{\langle z, Ax_1\rangle}_{\text{Eve knows}}$

Eve knows $\langle z, y\rangle$ => XOR of some of the key

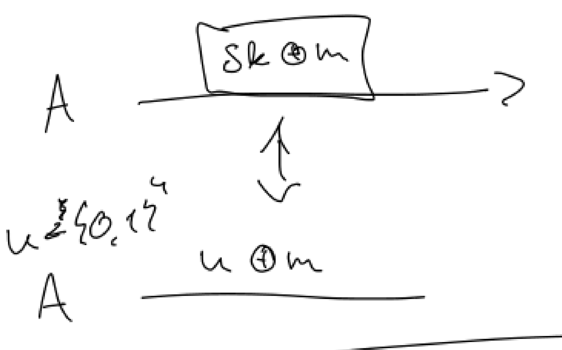
A_{x_2}

2^k inputs $2^k < 2^l$

2^l outputs

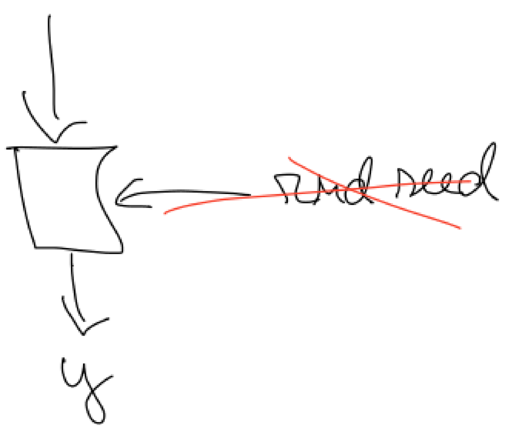
Find vector z that is orthogonal to all images of x_2

$\forall x_2: \langle z, Ax_2\rangle = 0$



Deterministic randomness extractor? (key)

(bits Eve knows || unknown bits)



f is a fixed random oracle

$f \xleftarrow{\$} F$

$f(x)$:
  d[x] is not set:
    $y \xleftarrow{\$} Y$
    d[x] = y
    return y
  else:
    return d[x]

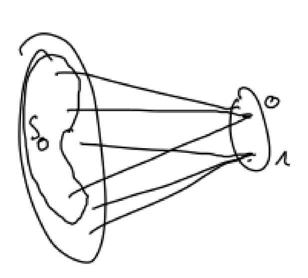
Input space is n bits

Output space is 1 bit

H(x) is unif. random

Want: For every n-bit input source of at least n-1 bits of entropy the output is close to unif. random

$S_i = f^{-1}(i)$



let S_0 be largest

$|S_0| = \frac{|X| \leftarrow \text{input space}}{|Y| \leftarrow \text{output space}}$

let K be RV over S_0

$\forall x: \Pr[K = x] = \frac{1}{|S_0|} = \frac{|Y|}{|X|} = \frac{2}{2^n} \Rightarrow 2^{n-1}$ entropy on n-1 bits

Take S_0 as input source

↳ Has n-1 bits of entropy

↳ output is always 0