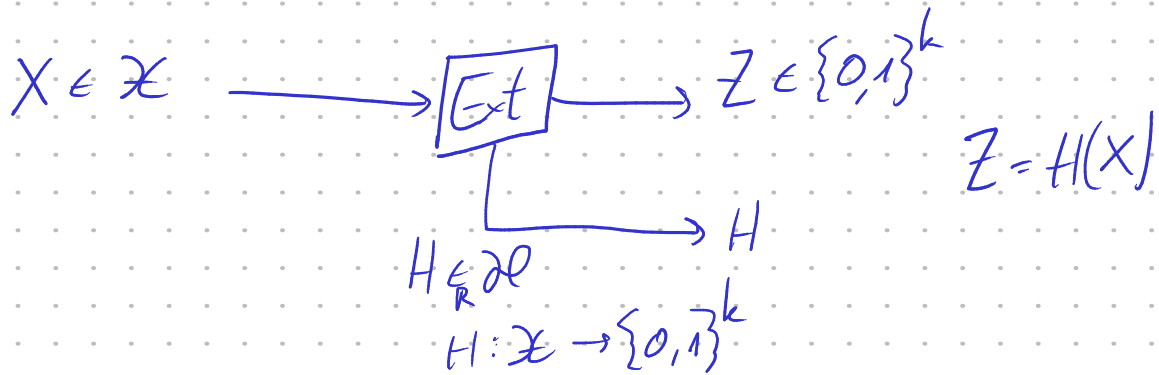


$$P_A[\text{error}] \leq 2^{H_{\max}(X) - R}$$

Extractor d'info one-shot



→ On veut que Z soit uniforme du point de vue d'un adversaire qui connaît p_X et qui apprend H

⇒ On veut que

$$\| \underbrace{p_{ZH}}_{\text{cas réel}} - \underbrace{u_Z \times p_H}_{\text{cas idéal}} \|_1 \leq \text{négligeable} \quad \left(= 2^{\frac{1}{2}(k - H_{\min}(X))} \right)$$

$(H_2(X))$

$\mathcal{H}$: ensemble des fonctions de hachage : n'importe quel ensemble de fonctions b.g.

$$\forall x \neq x' \in \mathcal{X}, \quad P_H \left[H(x) = H(x') \right] \leq 2^{-k}$$

→ Fonction aléatoire (sur tous les fonctions), fonction linéaire, ...

Pn: $\|p_{Z|H} - u_Z \cdot p_H\|_1 = \mathbb{E}_H \|p_{Z|H} - u_Z\|_1$

$$\left(\begin{aligned} p_{Z|H}(z, h) &= p_H(h) \cdot p_{Z|H}(z|h) \\ \sum_{z, h} |p_{Z|H}(z, h) - 2^{-k} \cdot p_H(h)| &= \sum_{z, h} p_H(h) |p_{Z|H}(z|h) - 2^{-k}| \\ &= \mathbb{E}_H \| \sim \|_1 \end{aligned} \right)$$

On veut utiliser l'inégalité de Cauchy-Schwarz pour bornes

C-S : $\vec{u}, \vec{v} \in \mathbb{R}^n$, $\langle \vec{u}, \vec{v} \rangle \leq \sqrt{\langle \vec{u}, \vec{u} \rangle \langle \vec{v}, \vec{v} \rangle}$

$$\langle \vec{u}, \vec{v} \rangle = \sum_i u_i v_i = \sqrt{\left(\sum_i u_i^2 \right) \left(\sum_j v_j^2 \right)}$$

Écrivons $\|p_{Z|H} - u_Z\|_1$ comme $\langle \vec{u}, \vec{v} \rangle$ où

$$\begin{aligned} \vec{u} &= p_{Z|H} - u_Z \text{ vu comme un vecteur dans } \mathbb{R}^{2^k} \\ \vec{v} &= \begin{cases} 1 & \text{si } p_{Z|H}(z) \geq 2^{-k} \\ -1 & \text{sinon} \end{cases} \end{aligned}$$

$$\begin{aligned} \Rightarrow \|p_{Z|H} - u_Z\|_1 &= \langle \vec{u}, \vec{v} \rangle \leq \sqrt{\left(\sum_i u_i^2 \right) \left(\sum_j v_j^2 \right)} \\ &= \sqrt{\left(\sum_z (p_{Z|H}(z) - 2^{-k})^2 \right) \left(\sum_z (+1)^2 \right)} \\ &= 2^{k/2} \cdot \sqrt{\sum_z (p_{Z|H}(z) - 2^{-k})^2} \end{aligned}$$

$$\sum_h P_H(h) \cdot \|p_{Z|H=h} - u_Z\|_1 \leq \sum_h P_H(h) \cdot 2^{h/2} \sqrt{\sum_z (p_{Z|H=h}(z) - 2^{-h})^2}$$

(inégalité de Jensen)
 $\mathbb{E}_x f(X) \leq f(\mathbb{E}(X))$
 si f est concave

$$\leq 2^{h/2} \sqrt{\sum_h P_H(h) \sum_z (p_{Z|H=h}(z) - 2^{-h})^2}$$

Regardons la somme à l'intérieur :

$$\begin{aligned} & \sum_z (p_{Z|H=h}(z) - 2^{-h})^2 \\ &= \sum_z \left(p_{Z|H=h}(z)^2 - 2 \cdot 2^{-h} \cdot p_{Z|H=h}(z) + 2^{-2h} \right) \\ &= \left(\sum_z p_{Z|H=h}(z)^2 \right) - 2 \cdot 2^{-h} + 2^{-h} \\ &= \underbrace{\left(\sum_z p_{Z|H=h}(z)^2 \right)}_{\text{à calculer}} - 2^{-h} \end{aligned}$$

$$= \sum_z \left(\sum_{x: h(x)=z} p_x(x) \right)^2 = \sum_z \sum_{x, x': h(x)=h(x')=z} p_x(x) p_{x'}(x')$$

$$= \sum_{x, x': h(x)=h(x')} p_x(x) p_{x'}(x')$$

→ Ramenons l'espérance sur H :

$$\rightarrow \sum_h P_H(h) \cdot \sum_{x, x': h(x)=h(x')} p_x(x) p_{x'}(x')$$

$$= \sum_{x, x'} p_x(x) p_x(x') \cdot \sum_{h: h(x)=h(x')} P_H(h)$$

$$= \sum_{x, x'} p_x(x) p_x(x') \cdot \underbrace{P_H[H(x)=H(x')]}_{\text{Nos fonction de hachage satisfait}}$$

$$\forall x \neq x' \quad P_H[H(x)=H(x')] \leq 2^{-k}$$

$$= \sum_x p_x(x)^2 + \sum_{x \neq x'} p_x(x) p_x(x') \cdot 2^{-k}$$

$$\leq \sum_x p_x(x)^2 + \underbrace{\sum_{x, x'} p_x(x) p_x(x')}_{=1} \cdot 2^{-k}$$

$$= \sum_x p_x(x)^2 + 2^{-k}$$

$\Rightarrow$ L'expression à l'intérieur de la racine carrée est égale à

$$\sum_h P_H(h) \sum_z (p_{z|H=h}(z) - 2^{-k})^2 \leq \sum_x p_x(x)^2$$

$$= \mathbb{E}_x [p_x(x)]$$

$$= \mathbb{E}_x [2^{-S(x)}]$$

$$(\text{Déf de } H_\alpha(x) : 2^{(1-\alpha)H_\alpha(x)} = \mathbb{E}_x [2^{(1-\alpha)S(x)}])$$

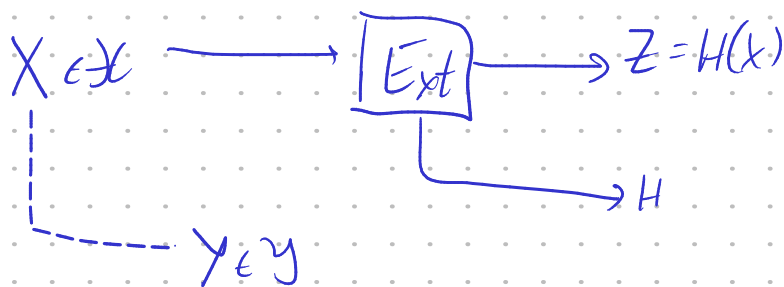
$$\hookrightarrow \alpha = 2$$

$$\Rightarrow \sum_h p_H(h) \sum_z (p_{Z|H=h}(z) - 2^{-k})^2 \leq 2^{-H_2(X)}$$

$$\Rightarrow \|p_{Z^k} - u_Z \times p_H\|_1 \leq 2^{k/2} \cdot \sqrt{2^{-H_2(X)}} \\ = 2^{\frac{1}{2}(k - H_2(X))} \leq 2^{\frac{1}{2}(k - H_{\min}(X))}$$

$$\text{car } H_2(X) \geq H_{\min}(X).$$

□



→ Idee: L'adversaire connaît Y et p_{XY} , et on veut que Z soit indépendant de Y et uniforme.

$$\|p_{Z^k|Y} - u_Z \times p_Y \times p_H\|_1 \leq \text{négligeable} \quad (= 2^{\frac{1}{2}(k - H_2(X|Y))})$$

$$\text{car } p_{XYZH}(x, y, z, h) = \frac{1}{|2^k|} p_{XY}(x, y) \mathbb{1}(h(x) = z),$$

$$\underline{P_1}: \|p_{Z^k|Y} - u_Z \times p_Y \times p_H\|_1 = \sum_{y, z, h} \left| p_{Z^k|Y=y}(z, h) - 2^{-k} \cdot p_Y(y) \cdot \frac{1}{|2^k|} \right| \\ = \sum_{y, z, h} p_Y(y) \left| p_{Z^k|Y=y}(z, h) - 2^{-k} \cdot \frac{1}{|2^k|} \right| \\ = \sum_y p_Y(y) \underbrace{\|p_{Z^k|Y=y}(z, h) - u_Z \times u_H\|_1}_1$$

On peut appliquer notre thm
dessus.

$$= \sum_y p_y(y) \cdot 2^{\frac{1}{2}(k - H_2(X|Y=y))}$$

$$= \mathbb{E}_Y \left[2^{\frac{1}{2}(k - H_2(X|Y=Y))} \right]$$

$$\underbrace{H_2(X|Y=Y)}_{\text{VA}}$$

$$VA = H_2(X|Y=y)$$

avec prob $p_y(y)$.

$H_2(X|Y) \rightarrow$ nombre fixe

(Entropie de Rényi conditionnelle:

$$2^{\frac{1-\alpha}{\alpha} H_\alpha(X|Y)} = \mathbb{E}_Y \left[2^{\frac{1-\alpha}{\alpha} H_\alpha(X|Y=Y)} \right]$$

Ici, on a $\alpha = 2$

$$\Rightarrow 2^{-\frac{1}{2} H_2(X|Y)} = \mathbb{E}_Y \left[2^{-\frac{1}{2} H_2(X|Y=Y)} \right]$$

$$= 2^{\frac{1}{2}k} \cdot \mathbb{E}_Y \left[2^{-\frac{1}{2} H_2(X|Y=Y)} \right] = 2^{\frac{1}{2}k} \cdot 2^{-\frac{1}{2} H_2(X|Y)}$$

$$= 2^{\frac{1}{2}(k - H_2(X|Y))}$$

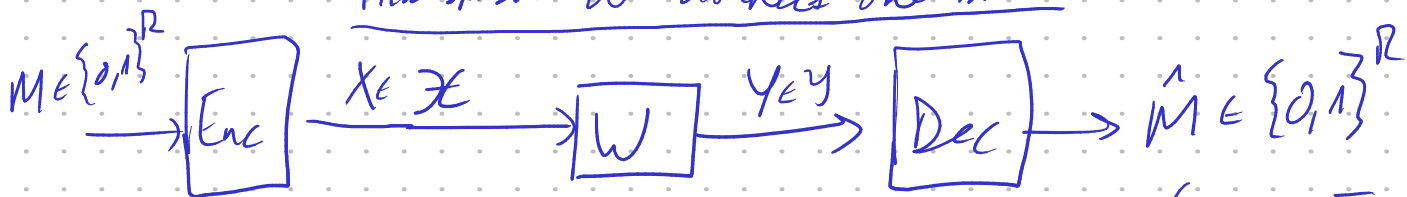
□

Compression: $P_n[\text{erreur}] \leq 2^{H_{\max}(X|Y) - R}$

$\uparrow H_{\max}$

Extraction d'info: $\|(\text{cas réel}) - (\text{cas idéal})\|_1 \leq 2^{\frac{1}{2}(k - H_2(X|Y))}$

Transmission de données one-shot



On veut $\Pr[\hat{M} \neq M] \leq \text{négligeable}$ ($= 2^{R - \underbrace{I_{\min}(X;Y)_{p \in W}}_{\max_p I_{\min}(X;Y)_{p \in W}}}$)

$$I_{\min}(X;Y) = I_{\frac{1}{2}}(X;Y)$$

Def [Informations mutuelles de Rényi]. Si X, Y sont deux VA, $\alpha \in (0,1) \cup (1,\infty)$, alors:

$$2^{\frac{\alpha-1}{\alpha} I_{\alpha}(X;Y)} = \mathbb{E}_Y \left[2^{\frac{\alpha-1}{\alpha} D_{\alpha}(p_{X|Y=y} \| p_X) \right]$$

et

$$2^{(\alpha-1) D_{\alpha}(p \| q)} = \mathbb{E}_{X \sim p} \left[2^{(\alpha-1)(S(X)_p - S(X)_q)} \right]$$

- Pr.
- Soit p_x une distribution quelconque sur X , et soit $c: \{0,1\}^R \rightarrow X$ un code choisi au hasard selon p_x .
 - On va utiliser le décideur suivant:

$$d(\hat{m} | y) = \frac{2^{\frac{1}{2} S(c(\hat{m}); y)}}{\sum_{m'} 2^{\frac{1}{2} S(c(m'); y)}}$$

→ La probabilité d'erreur ne dépend pas du message car on choisit le code au hasard

$$\begin{aligned}
 P_n[\hat{m} \neq 0^R | Y=y, \mathcal{C}=\{c(0^R), \dots, c(1^R)\}, M=0^R] \\
 = \sum_{\hat{m} \neq 0^R} d(\hat{m}|y) = \sum_{\hat{m} \neq 0^R} \frac{2^{\frac{1}{2}S(c(\hat{m});y)}}{\sum_{m'} 2^{\frac{1}{2}S(c(m');y)}} \\
 \leq 2^{-\frac{1}{2}S(c(0^R);y)} \sum_{\hat{m} \neq 0^R} 2^{\frac{1}{2}S(c(\hat{m});y)}.
 \end{aligned}$$

Vu que Y est indépendant de $c(\hat{m})$ pour tout $\hat{m} \neq 0^R$:

$$\mathbb{E}_{c(\hat{m})} \left[2^{\frac{1}{2}S(c(\hat{m});y)} \right] = \mathbb{E}_{X \sim p_X} \left[2^{\frac{1}{2}S(X;y)} \right]$$

$$= 2^{-\frac{1}{2}D_{\frac{1}{2}}(p_{X|Y=y} \| p_X)}$$

$$P_n[\hat{m} \neq 0^R | Y=y, M=0^R] = \mathbb{E}_{c(\hat{m})} \left[2^{-\frac{1}{2}S(c(0^R);y)} \cdot 2^{R - \frac{1}{2}D_{\frac{1}{2}}(p_{X|Y=y} \| p_X)} \right]$$

$$= 2^{-D_{\frac{1}{2}}(p_{X|Y=y} \| p_X) + R}$$

$$\begin{aligned}
 \mathbb{E}_Y[\text{---}] &= \mathbb{E}_Y \left[2^{R - D_{\frac{1}{2}}(p_{X|Y=y} \| p_X)} \right] \\
 &= 2^{R - I_{\frac{1}{2}}(X;Y)_{p \times W}}.
 \end{aligned}$$