Lecture 4 KEY DISTILLATION - PRIVACY AMPLIFICATION

4.1 SECURITY DEFINED

Security $P_{XY} = U_X P_Y$

$x \in \{0,1\}^n \quad N = 2^n$

$$p(x,y) = u(x)p(y)$$
$$= \frac{1}{N} p(y)$$

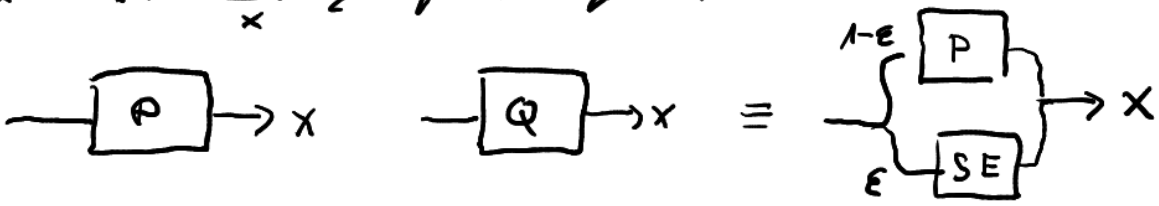
More realistic

$|P_{XY} - U_X P_Y| < \varepsilon$ X is ε-secure with respect to Y

↑ statistical distance

it is indeed a metric ✓

$$|P_X - Q_X| = \sum_x \frac{1}{2} |p(x) - q(x)|$$



$|P_X - Q_X| \leq \varepsilon$ $\quad \varepsilon \approx 10^{-20}$

4.2 Statistical Distance and Predictability

$$|P_{XY} - U_X P_Y| < \varepsilon \quad \longleftrightarrow \quad P_g(x|y) = \sum_y p(y) \max_x p(x|y)$$

$$|P_X - U_X| = \sum_x \frac{1}{2} \left|p(x) - \frac{1}{N}\right| \leq \frac{1}{2} \sqrt{N} \sqrt{\sum_x \left(p(x) - \frac{1}{N}\right)^2}$$

↑ Cauchy's inequality $\quad \vec{a} \cdot \vec{b} \leq |a||b|$

$$= \frac{\sqrt{N}}{2} \sqrt{\sum_x \left(p(x)^2 - 2p(x)\frac{1}{N} + \frac{1}{N^2}\right)} = \frac{\sqrt{N}}{2} \sqrt{\sum_x p(x)^2 - \frac{1}{N}}$$

$$\leq \frac{\sqrt{N}}{2} \sqrt{p_{max} - \frac{1}{N}} = \frac{1}{2} \sqrt{\frac{p_{max} - \frac{1}{N}}{\frac{1}{N}}}$$

$$|P_X - U_X| \leq \frac{1}{2} \sqrt{\frac{p_{max} - \frac{1}{N}}{\frac{1}{N}}}$$

$$|P_{XY} - U_X P_Y| = \frac{1}{2} \sum_{x,y} \left| p(x,y) - \frac{1}{N} p(y) \right|$$

$$= \frac{1}{2} \sum_{x,y} p(y) \left| p(x|y) - \frac{1}{N} \right|$$

$$\leq \frac{1}{2} \sum_{y} p(y) \sqrt{\frac{p(x|y)_{max} - \frac{1}{N}}{\frac{1}{N}}}$$

$$\leq \frac{1}{2} \sqrt{\frac{\sum_y p(y)\, p(x|y)_{max} - 1/N}{1/N}}$$

$$= \frac{1}{2} \sqrt{\frac{P_g(X|Y) - 1/N}{1/N}}$$

$p_1 f(y_1) + p_2 f(y_2)$
$\leq f(p_1 y_1 + p_2 y_2)$

$$|P_{XY} - U_X P_Y| \leq \frac{1}{2} \sqrt{\frac{P_g(X|Y) - 1/N}{1/N}}$$

Is it good enough ? YES → ✓

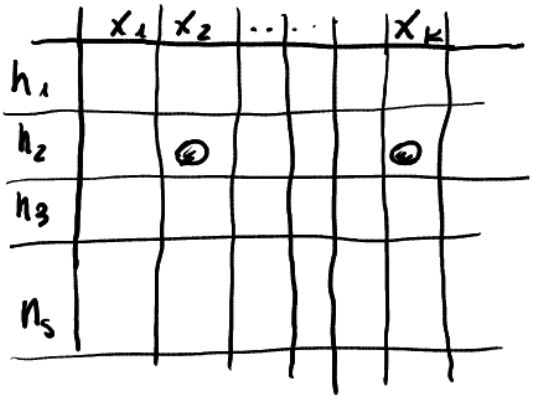
NO → HASHING

4.3 HASHING

$$h_S : \{0,1\}^n \longrightarrow \{0,1\}^L$$

$N = 2^n$ $\quad L = 2^L$

$$Pr\left(h_S(x) = h(x')\right) \leq \frac{1}{L}$$



ALICE/BOB $\quad$ EVE

$$P_g(Z|Y) \leq P_g(X|Y) + (1 - P_g(X|Y)) \frac{1}{L} \leq P_g(X|Y) + \frac{1}{L}$$

$$|P_{ZY} - U_Z P_Y| \leq \frac{1}{2} \sqrt{\frac{P(Z|Y) - \frac{1}{L}}{\frac{1}{L}}} \leq \frac{1}{2} \sqrt{\frac{P_g(X|Y)}{1/L}} = \frac{1}{2} \sqrt{P_g L}$$

Let $P_g(x|y) = \left(\frac{1}{2}\right)^k$ $\quad k = -\log \sum_y p(y) \max_x p(x|y)$

$k = H_{min}(X|Y)$

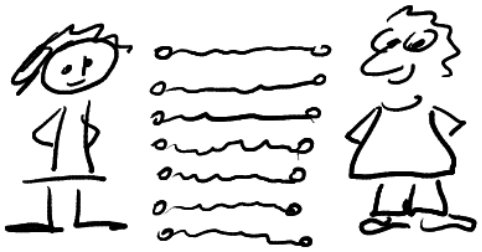
$$|P_{ZY} - U_2 P_Y| \leq \left(\frac{1}{2}\right)^{\frac{k-l}{2}}$$

We can extract at most

$$l = k - 2\log\frac{1}{\varepsilon} = H_{min}(X|Y) - 2\log\frac{1}{\varepsilon}$$

bits which are ε-secure

4.4 SUMMARY



1. TEST FOR $\mathcal{I}^+$
2. ESTIMATE Q
3. $P_g(x|y) = \frac{1}{2} + \sqrt{Q(1-Q)}$
4. $P_g(x|y) \rightarrow H_{min}(x|y) = -\log P_g(x|y)$
5. Hashing $\quad l = H_{min}(X|Y) - 2\log\frac{1}{\varepsilon}$

   bits which are ε-secure