Then, $SD(Y; U) \leq \varepsilon$.

Proof. By definition:

$$SD(Y; U) = \frac{1}{2} \sum_{y \in \mathcal{Y}} \left| \Pr[Y = y] - \Pr[U = y] \right|$$

$$= \frac{1}{2} \sum_{y \in \mathcal{Y}} \left| \Pr[Y = y] - 1/|\mathcal{Y}| \right|$$

Let $q_y = \Pr[Y = y] - 1/|\mathcal{Y}|$

and $s_y = \begin{cases} 1 & \text{if } q_y > 0 \\ -1 & \text{else} \end{cases}$

($\vec{q} = (q_y)_{y \in Y}$; $\vec{s} = (s_y)_{y \in Y}$)

Hence,

$$SD(Y;U) = \frac{1}{2} \sum_{y \in Y} q_y s_y$$

$$= \frac{1}{2} \langle \vec{q}, \vec{s} \rangle$$

$$\leq \frac{1}{2} \sqrt{\langle \vec{q}, \vec{q} \rangle \cdot \langle \vec{s}, \vec{s} \rangle}$$

(by Cauchy-Schwarz)

$$\geq \frac{1}{2} \sqrt{\sum_{y \in \mathcal{Y}} q_y^2 \cdot |\mathcal{Y}|}$$

Now, we analyze term $\sum_y q_y^2$:

$$\sum_{y \in \mathcal{Y}} q_y^2 = \sum_{y \in \mathcal{Y}} \left(\Pr[Y = y] - 1/|\mathcal{Y}| \right)^2$$

$$= \sum_{y \in \mathcal{Y}} \left(\Pr[Y = y]^2 + 1/|\mathcal{Y}|^2 \right.$$

$$- 2 \Pr[Y = y] \Big)$$

$$= \underbrace{\sum_{y \in Y} \Pr[Y = y]^2}_{Col(Y)} + \frac{1}{|Y|} - \frac{2}{|Y|}$$

$$= Col(Y) - \frac{1}{|Y|}$$

$$\leq \frac{1}{|y|}\left(1+4\varepsilon^2\right) - \frac{1}{|y|}$$

$$= \frac{4\varepsilon^2}{|y|}$$

Then:

$$SD(Y;U) \leq \frac{1}{2}\sqrt{\frac{4\varepsilon^2}{|y|}\,|y|}$$

$$= \varepsilon \qquad \blacksquare$$

Next, we apply the lemma to prove the Theorem:

Proof (of THM). We will let

$$Y = (S, Ext(S, X))$$

$$= (S, h(S, X))$$

and compute $Col(Y)$:

$$Col(Y) = \sum_{y \in \mathcal{Y}} Pr[Y = y]^2$$

$$= Pr[Y = Y']$$

$$= Pr[S = S' \wedge h(S, X) = h(S', X')]$$

$$= Pr[S = S' \wedge h(S, X) = h(S, X')]$$

$$= Pr[S = S'] \cdot Pr[h(S, X) = h(S, X')]$$

$$= 2^{-d} \cdot Pr[h(S, X) = h(S, X')]$$

$$= 2^{-d} \cdot \Big(\Pr[X = x'] + \Pr[h(S,X) = h(S,x') \wedge X \neq x'] \Big)$$

$$\leq 2^{-d} \left(2^{-k} + 2^{-\ell} \right)$$

$$= \frac{1}{2^{d+\ell}} \left(2^{\ell-k} + 1 \right)$$

$$\leq \frac{1}{2^{d+\ell}} \left(2^{2-2\log(1/\varepsilon)} + 1 \right)$$

$$= \frac{1}{|y|} \cdot \left(4 \cdot \varepsilon^2 + 1\right)$$

COMPUTATIONAL SECURITY

Summary: We know that without ANY assumption we can't do symmetric crypto and randomness generation with some strong guarantees.

- Privacy: $|msg| = |key|$ and one-time only.

- Integrity: Same as above.

- Randomness: We can't extract more than k from min-entropy k.

Next, we want to overcome all these limitations. We'll do so at the price of assumptions:

1) Adversary vs comp. BOUNDED

2) There exists hard problems.

We will make conditional statements:

THM If problem X is HARD (against efficient solvers), then cryptosystem Π is SECURE (against efficient adversaries).

Consequence: If Π not secure, $\exists$ efficient solver for X!

Depending on what X is, the

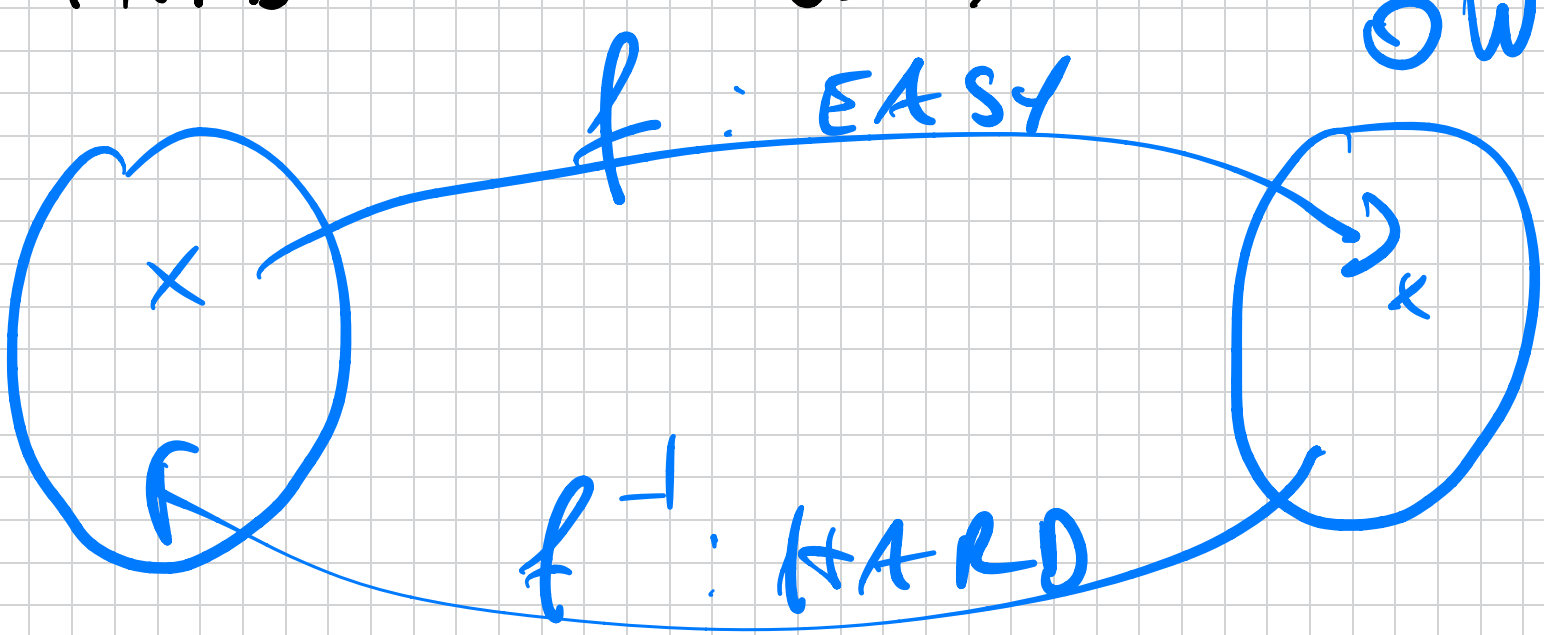
above could be GROUND BREAKING.

Examples:

- $X =$ "$P \neq NP$"
- $X =$ "FACTORING IS HARD"
- $X =$ "DISCRETE LOG IS HARD"
- ----

We are not able to just assume $P \neq NP$.

We will need "stronger" assumptions: ONE-WAY FUNCTIONS: These are functions f that are EASY to compute but HARD to invert:



Clearly, OWF $\Rightarrow$ $P \neq NP$. Why?

Because if $P = NP$, OWF do not exist as checking if $f(x) = y$ is efficient and thus it's in NP = P.

We cannot exclude that $P \neq NP$, but still OWF do not exist.

To better understand this, we can refer to the following worlds considered by RUSSEL IMPAGLIAZZO:

- ALGORITHMICA, $P = NP$

- HEURISTICA, $P \neq NP$ but no "average-hard puzzles"

- PESSILAND, $P \neq NP$ but no OWF.

- MINICRYPT, OWFs exist.

- CRYPTOMANIA, OWFs + "public-key crypto".

First, we must start by fixing a model of computation: Turing machines.
Efficient computation: Poly-time TMs.
Let's be generous: Adversaries can use any amount (polynomial) of RANDOMNESS: PPT TMs (Probabilistic Polynomial-time TM).
In what comes next, one could follow two approaches:

1) CONCRETE SECURITY: Security holds w.r.t. t-time TMs except w.p. $\leq \varepsilon$ for concrete parameters ($t = 2^{20}$ steps, $\varepsilon = 2^{-80}$.).

2) ASYMPTOTIC SECURITY: Let $\lambda \in \mathbb{N}$ be a security parameter. Adversaries are poly(λ)-time PPT TMs. What about ε = ??

ε = negligible $\approx$ $negl(\lambda)$.

DEF (NEGLIGIBLE) $\varepsilon : \mathbb{N} \to \mathbb{R}$ is NEGLIGIBLE if $\forall$ $p(\lambda) = poly(\lambda)$

$\exists$ $\lambda_0 \in \mathbb{N}$ s.t. $\forall$ $\lambda > \lambda_0$ we have

$$\varepsilon(\lambda) \leq 1/p(\lambda) .$$

(In other words, $\varepsilon(\lambda) \leq O(1/p(\lambda))$

$\forall$ $p(\lambda) = poly(\lambda)$.)