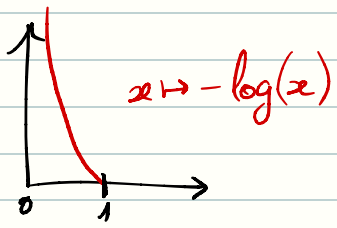
III/ The g-leakage

1) Min-entropy leakage

Given a random variable X, the min-entropy is defined as:

$$H_\infty(X) = -\log\left(\max_x \mathbb{P}(X=x)\right)$$



The bigger it is, the harder the guessing is.

Let consider X and Y, two random variables, the the conditional min-entropy is given by:

$$H_\infty(X|Y) = -\log\left(\max_x \mathbb{P}(X=x|Y)\right)$$

↓ Take the average over all possible values of y.

Knowing Y, it should be easier for the attacker to guess the correct value of X. Therefore $H_\infty(X) \geq H_\infty(X|Y)$.

The min-entropy leakage is finally defined by:

$$L_\infty(X,Y) = H_\infty(X) - H_\infty(X|Y)$$

Remark: H_∞ has some entropy properties: the flatter the distribution is, the bigger H_∞ is. It measures the randomness by considering the best 1-try possible attacker.

Min-entropy leakage can be written as:

$$L_\infty(X,Y) = \log\left(\frac{\max_x \mathbb{P}(X=x|Y)}{\max_x \mathbb{P}(X=x)}\right)$$

2) The main problem with min-leakage

Example: Let X contain 1000 different passwords 10-bits long.
Let Y be one of these 1000 passwords.

$L_\infty(X,Y) = 10$ bits

We now consider a user having one of these 1000 passwords. We want to measure how this user is in trouble. The probability of guessing it is 2^{-10} without the leak, and $0{,}001 + 0{,}999 \cdot 2^{-10} = 0{,}00198\ldots$

Then $L_\infty(X_{user}, Y) = \log\left(\frac{0{,}00198}{2^{-10}}\right) \approx 1{,}016$ bits

And the attacker might be very happy!

But a whole password has been completely leaked! Min-entropy is not sufficient for this type of threats. The g-leakage is a generalization of the min-entropy leakage.

3) The g-function

Let $(\mathcal{X}, \mathcal{Y}, \mathbb{P}_{Y|X})$ be a channel. We call $\pi := \mathbb{P}_X$ the prior, and the posterior is given by $\pi(x)\mathbb{P}_{Y|X}(y,x)$. The prior vulnerability is given by $V(X) = \max_x \pi(x)$, and the posterior vulnerability is written $V(X|Y) = \sum_{y \in \mathcal{Y}} \max_x \pi(x)\mathbb{P}_{Y|X}(y,x)$.

As a reminder, $H_\infty(X) = -\log(V(X))$, $H_\infty(X|Y) = -\log(V(X|Y))$ and $L_\infty(X,Y) = \log\frac{V(X|Y)}{V(X)}$.
The min-capacity is then defined as $ML_\infty(\mathbb{P}_{Y|X}) = \sup_{\mathbb{P}_X} L_\infty(X,Y)$, realized for the uniform prior.

Let $x \in \mathcal{X}$ be the secret. Given a guess $w \in \mathcal{X}$, we define between 0 and 1 how much is the attacker happy with w by the gain function $g : \mathcal{X}^2 \to [0,1]$.

Example: In the min-entropy case, g is defined by $g : (w,x) \mapsto \begin{cases} 1 \text{ if } x = w \\ 0 \text{ otherwise} \end{cases}$
This is called the identity g function, g_{id}.

This is better for clarity if we use $\mathcal{W}$ for the space of guesses instead of $\mathcal{X}$ but this doesn't change the core idea. Formally, $g : \mathcal{W} \times \mathcal{X} \to [0,1]$.

- The prior g-vulnerability is defined by $V_g(X) = \max_w \mathbb{E}[g(w, X)]$.
- The posterior g-vulnerability is defined by $V_g(X|Y) = \mathbb{E}_{\hat{Y}}[V_g(X|Y=\hat{Y})]$.

Other forms are shown on the paper but this one makes the link with PML.

$$\begin{aligned} V_g(\pi, C) &= \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi[x] C[x,y] g(w,x) \\ &= \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} p(x,y) g(w,x) \\ &= \sum_{y \in \mathcal{Y}} p(y) V_g(p_{X|y}) \end{aligned}$$

Dynamic posterior vulnerability $V_g(X|Y=y)$.

Dynamic g-leakage $\log \frac{V_g(X|Y=y)}{V_g(X)}$.

- The g-entropy is defined by $H_g(X) = -\log(V_g(X))$
- The g-leakage is defined by $L_g(X,Y) = H_g(X) - H_g(X|Y)$.
- The g-capacity is defined by $ML_g(\mathbb{P}_{Y|X}) = \sup_{\mathbb{P}_X} L_g(X,Y)$.

Theorem:

$\forall w \in \{\text{vulnerability, entropy, leakage, capacity}\}$, gid-w coincides with min-w.

4) Special g-functions

Let $d : \mathcal{X} \to \mathbb{R}_+$ be a distance. Since $\mathcal{X}$ is finite, let $d^* = \max_{c \in \mathcal{X}^2} d(c)$.

A gain function induced from d could be $1 - \frac{d(x,y)}{d^*}$, or $e^{-d(x,y)}$.

Let $\mathcal{W} \subseteq \mathcal{P}(\mathcal{X})$ be the set of possible guesses. Then it is usual that $\mathcal{W}$ is a partition of $\mathcal{X}$ and that we want to know on which set the secret x is.

Let $k \in \mathbb{N}^*$. We then define $\mathcal{W} = \{W \in \mathcal{P}(\mathcal{X}) \mid |W| = k\}$. Let us compute the prior of g_W-vulnerability: $\max_W \mathbb{E}[g_W(w, X)] = \max_{x_0 \neq x_1 \neq x_2} \pi(x_0) + \pi(x_1) + \pi(x_2)$.

This is exactly what we expect of a prior vulnerability within k tries!

We then easily define:

- the k-tries prior vulnerability
- the k-tries posterior vulnerability
- the k-tries min-entropy
- the k-tries min-leackage
- the k-tries min-capacity

Going further:

IV. MATHEMATICAL PROPERTIES OF g-VULNERABILITY AND g-LEAKAGE

V. RESULTS ON CHANNEL CAPACITY

VI. COMPARING CHANNELS

VII. RELATED WORK