1 Papers referred to

- Mário S. Alvim, Konstantinos Chatzikokolakis, and Annabelle McIver. **Axioms for Information Leakage**.

2 Bounds on Extended g-leakage

- Let $X \to Y \to Z$ be a Markov chain. Classical information theory tells us that the mutual information between X and Y bounds the mutual information between X and Z. i.e. $I(X;Y) \geq I(X;Z)$. This is known as data processing inequality. A similar result has been proven for g-leakage in the paper above. But for classic information theory, we also know that for any Markov chain, the reverse chain is also Markovian, so $I(Y;Z) \geq I(X;Z)$. There seems to be no analogous results in the literature in the g-leakage setting, even though one would expect something similar.
- The difficulty in the g-leakage case is that the gain function corresponds to $I(Y;Z)$ and $I(X;Z)$ takes different arguments. In the previous definition, they are $g_1 : \mathcal{W}_1 \times Y$ and $g_2 : \mathcal{W}_2 \times X$ respectively. For our extended definition, they are $g_1 : \mathcal{W}_1 \times Y \times Z$ and $g_2 : \mathcal{W}_2 \times X \times Z$ respectively. So they g-vulnerabilities seems to be incomparable.
- We show that in fact we can extend data processing inequality to g-leakage and extended g-leakage by considering some classes of gain functions. We start by considering gain functions with same guessing space.

3 Results on extended g-leakage

- We denote the channel between X and Y be C, and the channel between Y and Z by R. Let the gain function between X and Y be $g_1 : \mathcal{W} \times X \times Y$, and gain function between X and Z be $g_0 : \mathcal{W} \times X \times Z$. There are two conditions we can find between g_1 and g_0 so that we can use EV_{g_1} to bound EV_{g_0}.
- The first inequality comes by 'considering the future'.

$$
\begin{aligned}
& EV_{g_1}(\pi, C) \\
=& \sum_{y \in Y} \Pr(y) \max_{w \in \mathcal{W}} \sum_{x \in X} \Pr(x \mid y) g_1(w, x, y) \\
=& \sum_{z \in Z} \sum_{y \in Y} \Pr(y \mid z) \Pr(z) \max_{w \in \mathcal{W}} \sum_{x \in X} \Pr(x \mid y) g_1(w, x, y) \\
\geq& \sum_{z \in Z} \Pr(z) \max_{w \in \mathcal{W}} \sum_{x \in X} \sum_{y \in Y} \Pr(y \mid z) \Pr(x \mid y) g_1(w, x, y) \\
=& \sum_{z \in Z} \Pr(z) \max_{w \in \mathcal{W}} \sum_{x \in X} \sum_{y \in Y} \Pr(x, y \mid z) g_1(w, x, y)
\end{aligned}
$$

- So if $\sum_{y \in Y} \Pr(x, y \mid z) g_1(w, x, y) \geq \Pr(x \mid z) g_0(w, x, z)$ holds for all w, x, z then we have the desired bound. By re-arranging the inequalities, we get

$$g_0(w, x, z) \leq \sum_{y \in Y} \Pr(y \mid x, z) g_1(w, x, y) \tag{1}$$

  for all w, x, z. The right hand can be interpreted as weighted gain function of g_0, where the adversary considers all possible intermediate values of Y.

- The second inequality comes by 'considering the past'.

$$\begin{aligned} & EV_{g_2}(\pi, R) \\ = & \sum_{z \in Z} \Pr(z) \max_{w \in \mathcal{W}} \sum_{y \in Y} \Pr(y \mid z) g_2(w, y, z) \\ = & \sum_{z \in Z} \Pr(z) \max_{w \in \mathcal{W}} \sum_{x \in X} \sum_{y \in Y} \Pr(x, y \mid z) g_2(w, y, z) \end{aligned}$$

- So if $\sum_{y \in Y} \Pr(x, y \mid z) g_2(w, y, z) \geq \Pr(x \mid z) g_0(w, x, z)$ holds for all w, x, z then we have the desired bound. By re-arranging the inequalities, we get

$$g_0(w, x, z) \leq \sum_{y \in Y} \Pr(y \mid x, z) g_2(w, y, z) \tag{2}$$

  for all w, x, z.

4 Further Work

- We can generalise the result to longer Markov chains
- The bounds are still very inflexible in the sense that we need to analyse everything with respect to the full channel. Our goal is to find conditions on arbitrary gain functions such that we can bound the g-vulnerability on full channel with those of sub-channels.