Statistical Estimation of Min-Entropy Leakage

Tom Chothia Yusuke Kawamoto

School of Computer Science, University of Birmingham, United Kingdom

April 2014

Abstract

This manuscript presents new results on statistically estimating min-entropy leakage, which gives a confidence interval of the leakage.

1 Introduction

Information theory and statistics are employed to quantify the amounts of information leakage from systems. An analyst can statistically estimate information leakage of secret values in a system by observing only some (and not all) trial runs of the system. For example, Chatzikokolakis et al. [1] provide a method that analyses trial runs of systems and estimates the mutual information of the secrets from the observable outputs when the secrets and observables take discrete values. The method includes a rigorous evaluation of possible errors of the estimated leakage, and Chothia et al. [3] applies this to quantify information leakage from Java programs.

This manuscript deals with the statistical estimation of another kind of leakage measure, called *min-entropy leakage*. This measure is used to quantify the vulnerability of secrets to single-attempt guessing attacks [7]. We present a technique for statistically estimating the min-entropy leakage of a system, given independent and identically distributed trial runs of the system. In particular we calculate a confidence interval of the estimated leakage value, i.e., an interval that contains the true min-entropy leakage value with some confidence, for example, more than 95%. We also present another way of calculating a confidence interval based on previous work and compare the two approaches.

We implemented these new estimation algorithms in our tool leakiEst [2], which supports the estimation of several kinds of leakage measures from datasets that are generated from trial runs of a system. A wide range of experiments using the tool shows that the confidence interval calculated by our algorithm is indeed effective in evaluating the possible errors of estimated min-entropy leakage values, while the estimation of min-entropy leakage requires many more trial runs than that of mutual information.

2 Preliminaries

A *(discrete) channel* is a triple $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ consisting of a finite set $\mathcal{X}$ of (discrete) secret input values, a finite set $\mathcal{Y}$ of (discrete) observable output values and a $\#\mathcal{X} \times \#\mathcal{Y}$ matrix $P_{Y|X}$. Each element $P_{Y|X}[x, y]$ of the channel matrix is the conditional probability of having an observable $y \in \mathcal{Y}$ given a secret $x \in \mathcal{X}$ in a system. Given a secret input distribution P_X on $\mathcal{X}$, the joint probability of having a secret $x \in \mathcal{X}$ and an observable $y \in \mathcal{Y}$ is defined by $P_{XY}[x, y] = P_X[x]P_{Y|X}[x, y]$.

When the specification of a system is unknown or too large to examine all possible runs of the system, it is impossible or very difficult for us to precisely calculate the channel matrix or joint distribution for the system. Thus, instead of trying to obtain the exact channel matrix or joint distribution, we statistically estimate them from some trial runs of the system.

Let us consider L trial runs of the system that are independent and identically distributed. Let $\hat{s}(x, y)$ be the frequency of trial runs with a secret $x \in \mathcal{X}$ and an observable $y \in \mathcal{Y}$. Then the empirical probability of having a secret x and an observable y is defined by $P^L_{XY}[x, y] = \frac{\hat{s}(x,y)}{L}$. Also, let $\hat{u}(x)$ be the frequency of a secret $x \in \mathcal{X}$; i.e., $\hat{u}(x) = \sum_{y \in \mathcal{Y}} \hat{s}(x, y)$. Then the empirical probability of having a secret x is defined by $P^L_X[x] = \frac{\hat{u}(x)}{L}$.

Next we present the definition of *min-entropy leakage* [7], which measures the vulnerability of secrets to single-attempt guessing attacks.

- The *a priori vulnerability* is defined as a min-entropy: $V(X) = \max\limits_{x \in \mathcal{X}} P_X[x]$.
- The *a posteriori vulnerability* is defined as a conditional min-entropy: $V(X|Y) = \sum\limits_{y \in \mathcal{Y}} \max\limits_{x \in \mathcal{X}} P_{XY}[x, y]$.
- The *min-entropy leakage* is defined by $\mathcal{L}(X; Y) = -\log_2 V(X) + \log_2 V(X|Y)$.

We finally recall the definition of binomial distributions. A *binomial (or Bernoulli) trial* is an experiment with two possible outcomes "success" and "failure" (e.g. coin-flipping). For a positive integer L and a probability p, the *binomial distribution* $B(L, p)$ is the discrete probability distribution of the number of successes in a sequence of L independent binomial trials, each being a success with the probability p. The distribution $B(L, p)$ has a mean of Lp and a variance of $Lp(1 - p)$.

3 Estimating Min-Entropy Leakage Using χ^2 Tests

In this section we present a novel method for estimating the min-entropy leakage from trial runs of the system. The estimation gives a point estimate of a leakage and its (more than) 95% confidence interval. Note that this new approach can be applied to the systems where secrets and observables have *discrete* values. We assume that the analyst does not know the secret input distribution P_X in advance and so estimate it as well from trial runs of the system.

We obtain the following point estimates from the empirical secret distribution P^L_X and the empirical joint distribution P^L_{XY}.

- The point estimate of the a priori vulnerability $V^L(X) = \max\limits_{x \in \mathcal{X}} P^L_X[x]$.
- The point estimate of the a posteriori vulnerability $V^L(X|Y) = \sum\limits_{y \in \mathcal{Y}} \max\limits_{x \in \mathcal{X}} P^L_{XY}[x, y]$.
- The point estimate of the min-entropy leakage $\widehat{\mathcal{L}}(X; Y) = -\log_2 V^L(X) + \log_2 V^L(X|Y)$.

Given L independent and identically distributed trial runs, the frequency $\hat{s}(x, y)$ of having a secret $x \in \mathcal{X}$ and an observable $y \in \mathcal{Y}$ follows the binomial distribution $B(L, P_{XY}[x, y])$, where $P_{XY}[x, y]$ is the *true* joint probability of a secret x and an observable y occurring. On the other hand, the binomial distributions $B(L, P_{XY}[x, y])$ and $B(L, P_{XY}[x', y'])$ for any $x, x' \in \mathcal{X}$ with $x \neq x'$ and $y, y' \in \mathcal{Y}$ with $y \neq y'$ are correlated, as their observed frequencies must sum to the total number of trial runs; i.e., $\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \hat{s}(x, y) = L$. Therefore the estimation of a confidence interval using the exact distribution takes too long time. Instead, we perform Pearson's χ^2 tests [6, 4] for a large number L of trial runs in order to estimate a confidence interval of the min-entropy leakage.

The estimation of a confidence interval is based on the fact that, with a high probability, each observed frequency $\hat{s}(x, y)$ of having a secret $x \in \mathcal{X}$ and an observable $y \in \mathcal{Y}$ is close to the "expected frequency" $P_{XY}[x, y]L$, where $P_{XY}[x, y]$ is the true probability we want to estimate. By applying χ^2 tests, we evaluate the probability that the observed frequencies $\hat{s}(x, y)$ come from the joint probabilities $P_{XY}[x, y]$. Given the observed frequencies $\hat{s}(x, y)$ and the expected frequencies $P_{XY}[x, y]L$, the χ^2 test statistics is defined by:

$$\chi^2 = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} \frac{(\hat{s}(x, y) - P_{XY}[x, y]L)^2}{P_{XY}[x, y]L}.$$

Since $P_{XY}[x, y]$ is not a conditional probability but a joint probability, it is regarded as a one-way table and this test statistics follows the χ^2 distribution with $(\#X \cdot \#Y - 1)$ degrees of freedom. Note that we can obtain the value $\chi^2_{(0.05,k)}$ from the χ^2 table. We denote by $\chi^2_{(0.05,k)}$ the test statistics with upper tail area 0.05 and k degrees of freedom.

The goal of our new method is to obtain a (more than) 95% confidence interval of min-entropy leakage $\mathcal{L}(X; Y)$ between the secret and observable distributions X, Y. It suffice to calculate the 95% confidence intervals of the min-entropy $H_\infty(X) = -\log_2 \max_{x\in\mathcal{X}} P_X[x]$ and the conditional min-entropy $H_\infty(X; Y) = -\log_2 \sum_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} P_{XY}[x, y]$ respectively.

We first present a way of obtaining the confidence interval of the conditional min-entropy $H_\infty(X; Y)$ as follows. Given L independent and identically distributed trial runs of the system, we obtain the observed frequencies $\hat{s}$. Then we construct expected frequencies $s_{\max}$ that give the largest a posteriori vulnerability among all expected frequencies that satisfy:

$$\chi^2_{(0.05,\#\mathcal{X}\#\mathcal{Y}-1)} = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} \frac{(\hat{s}(x, y) - s_{\max}(x, y))^2}{s_{\max}(x, y)}.$$

More specifically, $s_{\max}$ is constructed by increasing only the maximum expected frequencies $\max_{x\in\mathcal{X},y\in\mathcal{Y}}$ $s_{\max}(x, y)$ and by decreasing others, while keeping the total number of frequencies as L; i.e., $\sum_{x\in\mathcal{X},y\in\mathcal{Y}}$ $s_{\max}(x, y) = L$. From $s_{\max}$ we calculate the empirical distribution $P^{\text{post}}_{\max}[x, y] = \frac{s_{\max}(x,y)}{L}$. Next, we construct expected frequencies $s_{\min}$ that give the smallest a posteriori vulnerability. Keeping the total number of frequencies as L, we repeat to decrease the current maximum expected frequency and increase small frequencies until we obtain

$$\chi^2_{(0.05,\#\mathcal{X}\#\mathcal{Y}-1)} = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} \frac{(\hat{s}(x, y) - s_{\min}(x, y))^2}{s_{\min}(x, y)}.$$

Then we calculate the corresponding distribution $P^{\text{post}}_{\min}$ by $P^{\text{post}}_{\min}[x, y] = \frac{s_{\min}(x,y)}{L}$. From $P^{\text{post}}_{\max}$ and $P^{\text{post}}_{\min}$ we obtain the following confidence interval of the conditional min-entropy:

Lemma 3.1 *The lower bound $H^{\min}_\infty(X; Y)$ and upper bound $H^{\max}_\infty(X; Y)$ for the 95% confidence interval of the conditional min-entropy $H_\infty(X; Y)$ are respectively given by:*

$$H^{\min}_\infty(X; Y) = -\log_2 \sum_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} P^{\text{post}}_{\max}[x, y],$$
$$H^{\max}_\infty(X; Y) = -\log_2 \sum_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} P^{\text{post}}_{\min}[x, y].$$

Next, we compute the confidence interval of the min-entropy $H_\infty(X)$. Given the observed frequencies $\hat{u}$, we construct expected frequencies $u_{\max}$ that give the largest a priori vulnerability such that

$$\mathcal{X}^2_{(0.05,\#\mathcal{X}-1)} = \sum_{x\in\mathcal{X}} \frac{(\hat{u}(x) - u_{\max}(x))^2}{u_{\max}(x)}.$$

We calculate the empirical distribution $P^{\text{prior}}_{\max}[x] = \frac{u_{\max}(x)}{L}$. Similarly, we construct expected frequencies $u_{\min}$ giving the smallest a priori vulnerability, and calculate the corresponding distribution $P^{\text{prior}}_{\min}$ by $P^{prior}_{\min}[x, y] = \frac{s_{\min}(x,y)}{L}$. Then the 95% confidence interval of the min-entropy is defined by the following.

Lemma 3.2 *The lower bound $H^{\min}_\infty(X)$ and upper bound $H^{\max}_\infty(X)$ for the 95% confidence interval of the conditional min-entropy $H_\infty(X)$ are respectively given by:*

$$H^{\min}_\infty(X) = -\log_2 \max_{x\in\mathcal{X}} P^{\text{prior}}_{\max}(x)$$
$$H^{\max}_\infty(X) = -\log_2 \max_{x\in\mathcal{X}} P^{\text{prior}}_{\min}(x).$$

By Lemmas 3.1 and 3.2 we obtain a more than 95% confidence interval of the min-entropy leakage:

Theorem 1 *The lower bound $\mathcal{L}^{\min}(X;Y)$ and upper bound $\mathcal{L}^{\max}(X;Y)$ for a more than 95% confidence interval of the min-entropy leakage $\mathcal{X}(X;Y)$ are defined respectively:*

$$\mathcal{L}^{\min}(X;Y) = H^{\min}_\infty(X) - H^{\max}_\infty(X;Y)$$
$$\mathcal{L}^{\max}(X;Y) = H^{\max}_\infty(X) - H^{\min}_\infty(X;Y).$$

Note that our estimation of min-entropy leakage requires a large number of trial runs (usually many more than that required to estimate mutual information) to ensure that no more than 20% of the non-zero expected frequencies are below 5, which is a prerequisite for χ^2 tests.

4 Another Approach with Looser Bounds

This section presents another way of calculating a confidence interval for the min-entropy leakage. Note that this approach can be applied to the systems where secrets and observables have *discrete* values.

4.1 Useful Lemmas

The confidence interval for min-entropy leakage is calculated using two propositions in previous work. The following proposition is found as Proposition 1 in [8]:

Proposition 1 *Let P_Z be a probability distribution over a set $\mathcal{Z}$ of values. Let P^L_Z be the empirical probability distribution over $\mathcal{Z}$ obtained by observing L trial runs drawn from the distribution P_Z. Then for any $\epsilon_1 > 0$,*

$$\mathbf{Pr}\left[\ \left|\max_{z\in\mathcal{Z}} P_Z[z] - \max_{z\in\mathcal{Z}} P^L_Z[z]\right| > \epsilon_1\ \right] \le 2\exp\left(-\frac{L\epsilon_1^2}{2}\right).$$

The following proposition is found as Equation (2.3) in [5], which is derived from the Bernstein inequality:

Proposition 2 *Let P_Z be a probability distribution over a set $\mathcal{Z}$ of values. Let P_Z^L be the empirical probability distribution over $\mathcal{Z}$ obtained by observing L trial runs drawn from the distribution P_Z. Then for any $z \in \mathcal{Z}$ and any $\epsilon_2 > 0$,*

$$\mathbf{Pr}\left[\ \left|P_Z[z] - P_Z^L[z]\right| > \epsilon_2\ \right] \leq 2\exp\left(-\frac{6L\epsilon_2^2}{3+4\epsilon_2}\right).$$

4.2 Confidence Interval for Estimated Min-Entropy Leakage (when the input distribution is known)

We give another way of calculating the confidence interval for the min-entropy leakage. We first consider the case where the analyst knows the secret input distribution P_X. This calculation is faster than the approach in the previous section while giving looser bounds.

Let L_y be the number of trial runs with an observable $y \in \mathcal{Y}$, and L be the total number of trial runs; i.e., $L = \sum_{y\in\mathcal{Y}} L_y$. Let $P_{X|Y}[x,y]$ be the conditional probability of having a secret $x \in \mathcal{X}$ given an observable $y \in \mathcal{Y}$; i.e., $P_{X|Y}[x,y] = \frac{P_{XY}[x,y]}{P_Y[y]}$. Similarly we define the empirical conditional probability $P_{X|Y}^{L_y}[x,y]$. Using the two propositions we obtain the following theorem on a confidence interval of the min-entropy leakage $\mathcal{L}(X;Y)$.

Theorem 2 *Let $\epsilon_1, \epsilon_2 > 0$, and*

$$\begin{aligned}
\mathcal{L}^{lw} &= -\log V(X) + \log\left(\textstyle\sum_{y\in\mathcal{Y}} \max\left(0,\ (\max_{x\in\mathcal{X}} P_{X|Y}^{L_y}[x,y] - \epsilon_1)(P_Y^L[y] - \epsilon_2)\right)\right),\\
\mathcal{L}^{up} &= -\log V(X) + \log\left(\textstyle\sum_{y\in\mathcal{Y}} \left(\max_{x\in\mathcal{X}} P_{X|Y}^{L_y}[x,y] + \epsilon_1\right)\left(P_Y^L[y] + \epsilon_2\right)\right),\\
C(y) &= \left(1 - 2\exp\left(-\tfrac{L_y\epsilon_1^2}{2}\right)\right)\left(1 - 2\exp\left(-\tfrac{6L\epsilon_2^2}{3+4\epsilon_2}\right)\right).
\end{aligned}$$

Then

$$\mathbf{Pr}\left[\ \mathcal{L}^{lw} \leq \mathcal{L}(X;Y) \leq \mathcal{L}^{up}\ \right] > \prod_{y\in\mathcal{Y}} C(y).$$

Proof: Let $y \in \mathcal{Y}$. By Proposition 1,

$$\mathbf{Pr}\left[\ \max_{x\in\mathcal{X}} P_{X|Y}^{L_y}[x,y] - \epsilon_1 \leq \max_{x\in\mathcal{X}} P_{X|Y}[x,y] \leq \max_{x\in\mathcal{X}} P_{X|Y}^{L_y}[x,y] + \epsilon_1\ \right] > 1 - 2\exp\left(-\frac{L_y\epsilon_1^2}{2}\right).$$

By Proposition 2,

$$\mathbf{Pr}\left[\ P_Y^L[y] - \epsilon_2 \leq P_Y[y] \leq P_Y^L[y] + \epsilon_2\ \right] > 1 - 2\exp\left(-\frac{6L\epsilon_2^2}{3+4\epsilon_2}\right).$$

Let $C(y) = \left(1 - 2\exp\left(-\frac{L_y\epsilon_1^2}{2}\right)\right)\left(1 - 2\exp\left(-\frac{6L\epsilon_2^2}{3+4\epsilon_2}\right)\right)$. By $P_{XY}[x,y] = P_{X|Y}[x,y]P_Y[y]$,

$$\mathbf{Pr}\left[\ \left(\max_{x\in\mathcal{X}} P_{X|Y}^{L_y}[x,y] - \epsilon_1\right)\left(P_Y^L[y] - \epsilon_2\right) \leq \max_{x\in\mathcal{X}} P_{XY}[x,y] \leq \left(\max_{x\in\mathcal{X}} P_{X|Y}^{L_y}[x,y] + \epsilon_1\right)\left(P_Y^L[y] + \epsilon_2\right)\ \right] > C(y).$$

Therefore

$$\mathbf{Pr}\left[\ \mathcal{L}^{lw} \leq \mathcal{L}(X;Y) \leq \mathcal{L}^{up}\ \right] > \prod_{y\in\mathcal{Y}} C(y).$$

□

We can indeed calculate the confidence interval using the above theorem. Given a confidence level C_0 (e.g. 0.975), we can numerically obtain $\epsilon_1, \epsilon_2 > 0$ that satisfies $C_0 = \prod_{y \in \mathcal{Y}} C(y)$.

4.3 Confidence Interval for Estimated Min-Entropy Leakage (when the input distribution is also estimated)

Next we give a way of calculating the confidence interval for the min-entropy leakage $\mathcal{L}(X;Y)$ when the analyst does not know the exact secret input distribution P_X but can estimate it from trial runs of the system.

Theorem 3 *Let* $\epsilon_1, \epsilon_2, \epsilon_3 > 0$, *and*

$$\begin{aligned}
\mathcal{L}^{lw} &= -\log\left(\max_{x \in \mathcal{X}} P^L_X[x] + \epsilon_3\right) + \log\left(\textstyle\sum_{y \in \mathcal{Y}} \max\left(0,\ (\max_{x \in \mathcal{X}} P^{L_y}_{X|Y}[x,y] - \epsilon_1)(P^L_Y[y] - \epsilon_2)\right)\right),\\
\mathcal{L}^{up} &= -\log\left(\max(0, \max_{x \in \mathcal{X}} P^L_X[x] - \epsilon_3)\right) + \log\left(\textstyle\sum_{y \in \mathcal{Y}} \left(\max_{x \in \mathcal{X}} P^{L_y}_{X|Y}[x,y] + \epsilon_1\right)\left(P^L_Y[y] + \epsilon_2\right)\right),\\
C(y) &= \left(1 - 2\exp\left(-\tfrac{L_y \epsilon_1^2}{2}\right)\right) \cdot \left(1 - 2\exp\left(-\tfrac{6L\epsilon_2^2}{3+4\epsilon_2}\right)\right).
\end{aligned}$$

Then

$$\mathbf{Pr}\left[\ \mathcal{L}^{lw} \le \mathcal{L}(X;Y) \le \mathcal{L}^{up}\ \right] > \left(1 - 2\exp\left(-\frac{L\epsilon_3^2}{2}\right)\right) \cdot \prod_{y \in \mathcal{Y}} C(y).$$

Proof: By Proposition 1,

$$\mathbf{Pr}\left[\ \max_{x \in \mathcal{X}} P^L_X[x] - \epsilon_3 \le \max_{x \in \mathcal{X}} P_X[x] \le \max_{x \in \mathcal{X}} P^L_X[x] + \epsilon_3\ \right] > 1 - 2\exp\left(-\frac{L\epsilon_3^2}{2}\right).$$

Let $y \in \mathcal{Y}$. As shown in the proof for Theorem 2,

$$\mathbf{Pr}\left[\ \left(\max_{x \in \mathcal{X}} P^{L_y}_{X|Y}[x,y] - \epsilon_1\right)\left(P^L_Y[y] - \epsilon_2\right) \le \max_{x \in \mathcal{X}} P_{XY}[x,y] \le \left(\max_{x \in \mathcal{X}} P^{L_y}_{X|Y}[x,y] + \epsilon_1\right)\left(P^L_Y[y] + \epsilon_2\right)\ \right] > C(y).$$

Therefore, by $\mathcal{L}(X;Y) = \log\left(\dfrac{\sum_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}} P_{XY}[x,y]}{\max_{x \in \mathcal{X}} P_X[x]}\right)$, we obtain

$$\mathbf{Pr}\left[\ \mathcal{L}^{lw} \le \mathcal{L}(X;Y) \le \mathcal{L}^{up}\ \right] > \left(1 - 2\exp\left(-\frac{L\epsilon_3^2}{2}\right)\right) \cdot \prod_{y \in \mathcal{Y}} C(y).$$

□

5 Evaluation of the Two Approaches

According to some experiments, both of the two estimation methods give confidence intervals that contain the true leakage value with probabilities more than 95%. The estimation method using χ^2 tests (in Section 3) gives much better bounds than the estimation method using the previous work (in

Section 4). The estimation method based on the previous work give better bounds when the analyst knows the secret distribution P_X (in Section 4.2) than when he does not (in Section 4.3).

We will present experimental results to compare the two methods in a future version of this manuscript or in a journal paper.

It is worth noting that our point estimates of min-entropy leakages contain *positive* errors, like the point estimates of mutual information. Some experiments show that the point estimates are slightly above the true leakage. Therefore, like the estimation of mutual information in [1], some value should be subtracted from a point estimate of min-entropy leakage. Currently we are investigating a method for correcting point estimates to remove their positive errors.

6 Min-Entropy Leakage in Non-Terminated Systems

This section presents the measurement of min-entropy leakage in non-terminated discrete systems. Given a non-terminated discrete system, we define infinite sequences of secret input and observable output random variables at discrete times. Let $X^{(n)}$ and $Y^{(n)}$ be the secret and observable random variables at discrete time n in the system. For each integer n, we define the joint probability $P^{(n)}_{XY}[x, y]$ of having a secret $x \in \mathcal{X}$ and an observable $y \in \mathcal{Y}$ at discrete time n in the system. Then we can define the min-entropy leakage $\mathcal{L}(X^{(n)}; Y^{(n)})$ at time n.

6.1 Unbounded Number of Inputs

We first consider systems where there are unbounded number of secrets. We show that the min-entropy leakage can decrease when the number of secrets increases.

Proposition 3 *There exists a system such that* $\mathcal{L}(X^{(n)}; Y^{(n)}) > \mathcal{L}(X^{(n+1)}; Y^{(n+1)})$ *for some integer* n.

Proof: Let us consider a system where the joint probability distributions $P^{(1)}_{XY}$ and $P^{(2)}_{XY}$ at times 1 and 2 are defined in Tables 1 and 2 respectively.

$P^{(1)}_{XY}$	$Y^{(1)} = 0$	$Y^{(1)} = 1$
$X^{(1)} = 0$	0.3	0.2
$X^{(1)} = 1$	0.2	0.3

Table 1: The joint probability distribution $P^{(1)}_{XY}$ at time 1

$P^{(2)}_{XY}$	$Y^{(2)} = 0$	$Y^{(2)} = 1$
$X^{(2)} = 0$	0.3	0.2
$X^{(2)} = 10$	0.15	0.1
$X^{(2)} = 11$	0.05	0.2

Table 2: The joint probability distribution $P^{(2)}_{XY}$ at time 2

Then $\mathcal{L}(X^{(1)}; Y^{(1)}) = -\log\max(0.3 + 0.2, 0.2 + 0.3) + \log(\max(0.3, 0.2) + \max(0.2, 0.3)) = \log\frac{0.6}{0.5}$ and $\mathcal{L}(X^{(2)}; Y^{(2)}) = -\log\max(0.3+0.2, 0.15+0.1, 0.05+0.2)+\log(\max(0.3, 0.15, 0.05)+\max(0.2, 0.1, 02)) = \log\frac{0.5}{0.5}$. Therefore $\mathcal{L}(X^{(1)}; Y^{(1)}) > \mathcal{L}(X^{(2)}; Y^{(2)})$. □

By this proposition, $\mathcal{L}(X^{(n)}; Y^{(n)})$ can decrease when the number of secrets increases. Hence the min-entropy leakage $\lim_{n\to\infty} \mathcal{L}(X^{(n)}; Y^{(n)})$ in non-terminated discrete systems may not exist. This is different from the mutual information, which converges when n tends to infinity [3].

6.2 Bounded Number of Inputs

Next we consider systems where there are bounded number of secrets.

Proposition 4 *Consider a system where the number of secrets is fixed after time n_0. Then $\mathcal{L}(X^{(n)}; Y^{(n)})$ converges when n tends to infinity.*

Proof: For any integer n, $\mathcal{L}(X^{(n)}; Y^{(n)})$ is bounded above: $\mathcal{L}(X^{(n)}; Y^{(n)}) \leq -\log V(X^{(n)})$. For any $n \geq n_0$, by $X^{(n)} = X^{(n_0)}$, $\mathcal{L}(X^{(n)}; Y^{(n)})$ is non-decreasing: $\mathcal{L}(X^{(n)}; Y^{(n)}) \leq \mathcal{L}(X^{(n+1)}; Y^{(n+1)})$. Therefore the min-entropy leakage $\mathcal{L}(X^{(n)}; Y^{(n)})$ converges when n tends to infinity. □

References

[1] Konstantinos Chatzikokolakis, Tom Chothia, and Apratim Guha. Statistical Measurement of Information Leakage. In *Proc. TACAS*, pages 390–404, 2010.

[2] Tom Chothia, Yusuke Kawamoto, and Chris Novakovic. A Tool for Estimating Information Leakage. In *Proc. of the 25th International Conference on Computer Aided Verification (CAV 2013)*, volume 8044 of *Lecture Notes in Computer Science*, pages 690–695. Springer, July 2013.

[3] Tom Chothia, Yusuke Kawamoto, Chris Novakovic, and David Parker. Probabilistic Point-to-Point Information Leakage. In *Proc. of the 26th IEEE Computer Security Foundations Symposium (CSF 2013)*, pages 193–205. IEEE Computer Society, June 2013.

[4] David M Diez, Christopher D Barr, and Mine Cetinkaya-Rundel. *OpenIntro Statistics*. CreateSpace, 2012.

[5] S. Dutta and A. Goswami. Mode estimation for discrete distributions. *Mathematical Methods of Statistics*, 19(4):374–384, 2010.

[6] Karl Pearson. X. on the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *Philosophical Magazine Series 5*, 50(302):157–175, 1900.

[7] Geoffrey Smith. On the Foundations of Quantitative Information Flow. In *Proc. FOSSACS*, pages 288–302, 2009.

[8] István Vajda. Extraction of random bits for cryptographic purposes. *Tatra Mt. Math. Publ.*, 25:91–107, 2002.