**ASSESSING PRIVACY RISKS USING PROBABILISTIC PROGRAMMING**

Raúl Pardo (raup@itu.dk), Willard Rafnsson (wilr@itu.dk), Christian Probst (cprobst@unitec.ac.nz) and Andrzej Wąsowski (wasowski@itu.dk)

**PROBLEM**

- What can the attackers (Kalo and Kali) say about Alice’s age (a) after observing that the output of the program (o) is 55.3?  
- What attacker learned more about Alice’s age by observing the output of the program?

**Method**

1. **Prior/Posterior knowledge about Alice’s age.**
   - Kalo’s posterior reduces to a point distribution (no uncertainty).
   - Kali’s posterior still has a large standard deviation (some uncertainty).

2. **Analysis Phase**
   - Use Bayesian inference to compute the posterior distribution using the elements of the model.
   - Both Kalo and Kali learned that Alice is not underage.

3. **Prior/Posterior knowledge about Alice’s age**
   - Kalo’s knowledge about Alice’s age is more precise than Kali’s.
   - Kalo’s uncertainty about Alice’s age is much lower than Kali’s.
   - Kalo’s knowledge has changed more than Kali’s after observing the output.
   - The output contains more information about Alice’s age for Kalo than for Kali.

**privacy risk analyses**

- Expectation/Standard deviation:
  - Kalo: \( \mathbb{E}[a] = 55.3 \pm \sigma[a] = 55.3 \)
  - Kali: \( \mathbb{E}[a] = 55.3 \pm \sigma[a] = 55.3 \pm 0.01 \)  
  - Kalo: 64 ± 14

- Probability query:
  - Kalo: \( P(a \leq 18|a = 55.3) = 0.004 \)

- Shannon Entropy:
  - Kalo: \( H(a|a = 55.3) = -3.08 \)  
  - Kali: \( H(a|a = 55.3) = 5.83 \)

- KL-divergence:
  - Kalo: \( D_{KL}(a = 55.3||a) = 5.64 \)  
  - Kali: \( D_{KL}(a = 55.3||a) = 0.77 \)

- Mutual Information:
  - Kalo: \( I(a; O) = 9.37 \)  
  - Kali: \( I(a; O) = 0.60 \)

**Quantitative Information Flow metrics and other statistics**

- *Kalo*’s knowledge about Alice’s age is more precise than *Kali*’s.
- *Kalo*’s uncertainty about Alice’s age is much lower than *Kali*’s.
- Both *Kalo* and *Kali* learned that Alice is not underage.
- *Kalo*’s knowledge has changed more than *Kali*’s after observing the output.
- The output contains more information about Alice’s age for *Kalo* than for *Kali*.

Probabilistic programming can be effectively used to perform a wide range of quantitative analyses to find privacy leaks in data science programs.