Differential Privacy Relaxations

Damien Desfontaines*, Balázs Pejó**

Differential Privacy (DP) [1] offers privacy according to a provable and quantifiable amount. Since its original introduction, more than hundred relaxations have been proposed to adapt it to different contexts or assumptions. These new definitions enable practitioners to get privacy guarantees, even in cases that are not covered by the original DP definition.

All these relaxations can be classified into seven dimensions based on which aspect of the original definition they modify. We highlight these dimensions by reformulating DP and describe all dimensions and their usual motivations.

*An attacker with **perfect knowledge (B)** and **infinite computation power (C)** is **unable (R)** to **distinguish (D)** whether **someone is in the data (N)**, **uniformly (V)** across users, even in the **worst-case scenario (Q)**.*

- **Q**uantification of Privacy Loss: Relaxes DP by defining how the privacy loss is quantified across outputs. Usual motivations are to average risk and improve the composition property.
- **N**eighborhood Definition: Relaxes DP by specifying which properties are protected from the attacker. Usual motivations are protecting specific data or multiple individuals.
- **V**ariation of Privacy Loss: Relaxes DP by varying the privacy loss across inputs. The usual motivation is modeling users with different privacy requirements.
- **B**ackground Knowledge: Relaxes DP by defining how much prior knowledge the attacker has. The usual motivation is to use less noise in the mechanism.
- **D**efinition of Privacy Loss: Relaxes DP by using different formalism to describe the attacker's success. The usual motivation is to explore other intuitive notions of privacy.
- **R**elativization of Knowledge Gain: Relaxes DP by defining what is the attacker's knowledge gain relative to. The usual motivation is guaranteeing privacy for correlated data.
- **C**omputational Power: Relaxes DP by defining how much computational power the attacker has. The usual motivation is to use DP in a multi-party context.

References

1. C. Dwork. Differential privacy. *Encyclopedia of Cryptography and Security*, pages 338–340, 2011.

* ETH Zürich / Google, damien@desfontain.es
** University of Luxembourg, balazs.pejo@uni.lu