Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

# Pufferfish Privacy and its relation to Differential Privacy

When collecting and analyzing vast amounts of data in a database, the privacy of an individual is an increasing concern nowadays. Differential privacy [3] is a well-established and accepted privacy notion that quantifies the amount of information that is leaked about an individuals by retrieving statistics from a database. However, it cannot represent the impact of correlations between individuals' data on the privacy leakage.

Pufferfish privacy [1] has been proposed as an alternative privacy measure, which extends differential privacy to more sophisticated and comprehensive privacy requirements. Most importantly, it can quantify privacy in cases when data of different users is correlated, as it is the case in social networks. In [2], the so-called Wasserstein mechanism has been proposed which achieves pufferfish privacy, and has similarities with the well-known Laplace mechanism for differential privacy.

The goal of this seminar topic is to understand the difference between differential privacy and pufferfish privacy, and analyze how pufferfish privacy can be achieved by the Wasserstein mechanism.

[1] D. Kifer and A. Machanavajjhala, “Pufferfish: A framework for mathematical privacy definitions,” ACM Trans. Database Syst., vol. 39, no. 1, p. 3:1-3:36, Jan. 2014.

[2] S. Song, Y. Wang, and K. Chaudhuri, “Pufferfish Privacy Mechanisms for Correlated Data.” arXiv, Mar. 12, 2017.

[3] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," Foundations and Trends® in Theoretical Computer Science, 9(3–4), 211-407, 2014.

## Prerequisites

- knowledge in probability theory and statistics
- (optional) previous knowledge about differential privacy

## Contact

Luis Maßny (luis.massny@tum.de)

## Advisors

Luis Maßny