Cryptology ePrint Archive: Report 2011/071

Information-theoretic Bounds for Differentially Private Mechanisms

Gilles Barthe and Boris Köpf

Abstract: There are two active and independent lines of research that aim at quantifying the amount of information that is disclosed by computing on confidential data. Each line of research has developed its own notion of confidentiality: on the one hand, differential privacy is the emerging consensus guarantee used for privacy-preserving data analysis. On the other hand, information-theoretic notions of leakage are used for characterizing the confidentiality properties of programs in language-based settings.

The purpose of this article is to establish formal connections between both notions of confidentiality, and to compare them in terms of the security guarantees they deliver. We obtain the following results. First, we establish upper bounds for the leakage of every $\eps$-differentially private mechanism in terms of~$\eps$ and the size of the mechanism's input domain. We achieve this by identifying and leveraging a connection to coding theory. Second, we construct a class of $\eps$-differentially private channels whose leakage grows with the size of their input domains. Using these channels, we show that there cannot be domain-size-independent bounds for the leakage of all $\eps$-differentially private mechanisms. Moreover, we perform an empirical evaluation that shows that the leakage of these channels almost matches our theoretical upper bounds, demonstrating the accuracy of these bounds.

Finally, we show that the question of providing optimal upper bounds for the leakage of $\eps$-differentially private mechanisms in terms of rational functions of $\eps$ is in fact decidable.

Category / Keywords: Differential Privacy, Information theory.

Publication Info: Accepted for publication at CSF '11

Date: received 10 Feb 2011, last revised 25 Apr 2011

Contact author: boris koepf at imdea org