Research a New Tradeoff Method Between Privacy and Utility in Differential privacy

panjun sun (sunpanjun2008@163.com)
Shanghai Jiao Tong University https://orcid.org/0000-0002-4634-5886

Research Article

Keywords: Differential privacy, mutual information, minimum privacy leakage, Shannon communication theory, iterative approximation, limited distortion.

Posted Date: June 14th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-579007/v1

Abstract

The solution of the contradiction between privacy protection and data utility is a research hotspot in the field of privacy protection. Aiming at the problem of tradeoff between privacy and utility in the scenario of differential privacy offline data release, the optimal differential privacy mechanism is studied by using the rate distortion theory. Firstly, based on Shannon communication theory, the noise channel model of differential privacy is abstracted, and the mutual information and the distortion function is used to measure the privacy and utility of data publishing, and the optimization model based on rate distortion theory is constructed. Secondly, considering the influence of associated auxiliary background knowledge on mutual information privacy leakage, a mutual information privacy measure based on joint events is proposed, and a minimum privacy leakage model is proposed by modifying the rate distortion function. Finally, aiming at the difficulty in solving the Lagrange multiplier method, an approximate algorithm for solving the mutual information privacy optimization channel mechanism is proposed based on the alternating iterative method. The effectiveness of the proposed iterative approximation method is verified by experimental simulation. At the same time, the experimental results show that the proposed method reduces the mutual information privacy leakage under the condition of limited distortion, and improves the data utility under the same privacy tolerance

Full Text

This preprint is available for download as a PDF.

Figures

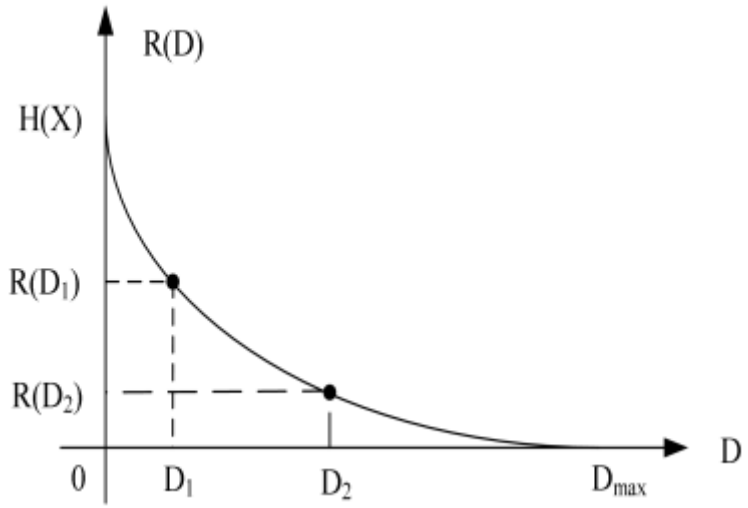


Figure 1

Rate distortion function

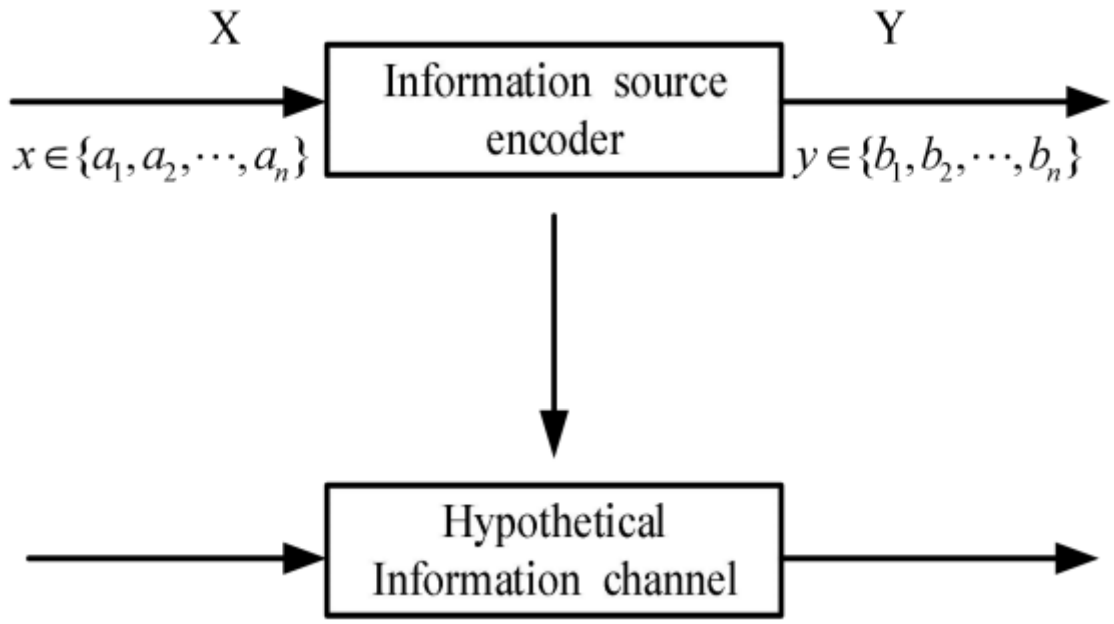


Figure 2

Source encoder as information channel

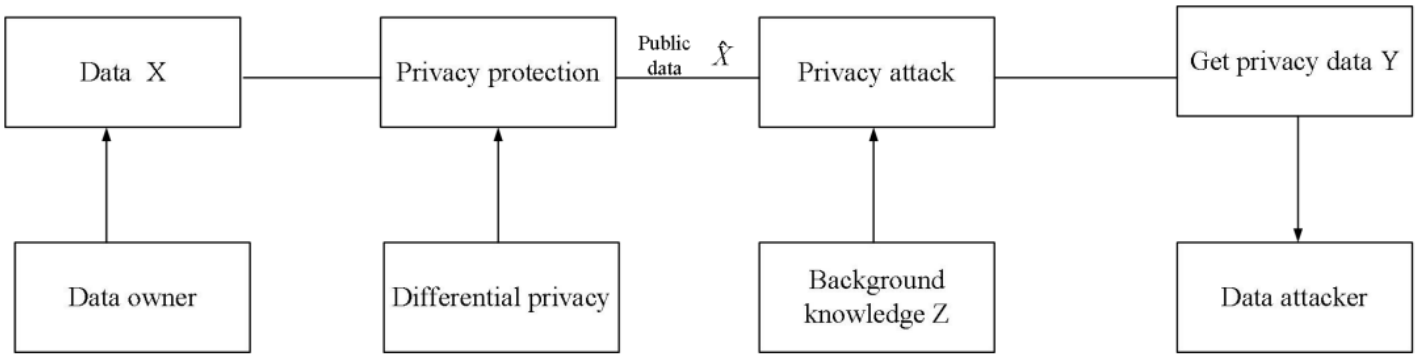


Figure 3

The model construction of this paper

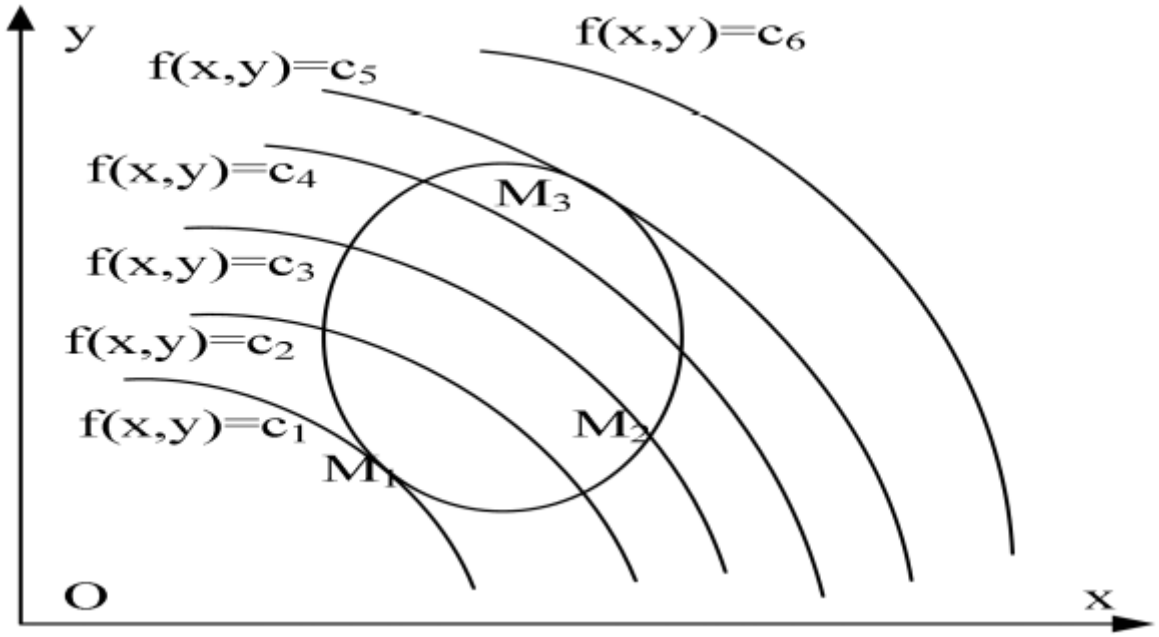
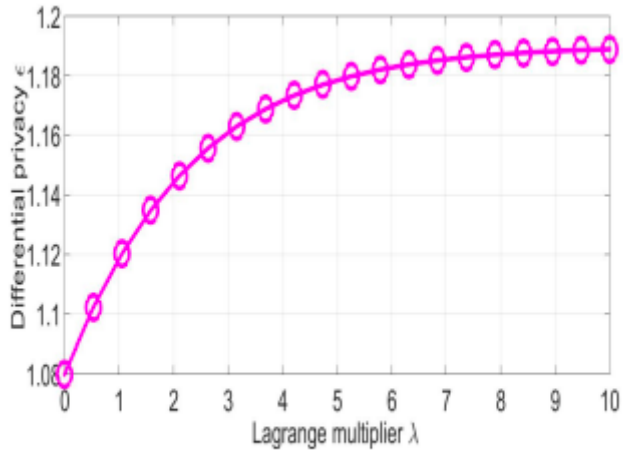
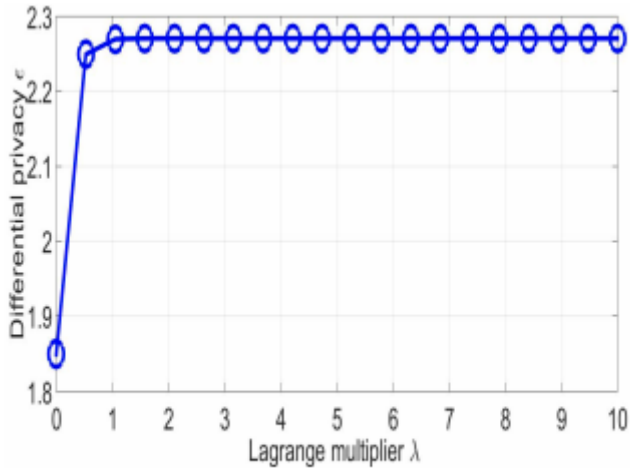


Figure 4

Geometric curve of Lagrange multiplier method



(1)



(2)

Figure 5

Lagrange multipliers with auxiliary knowledge and differential privacy parameter, (1) no auxiliary knowledge, (2) auxiliary knowledge

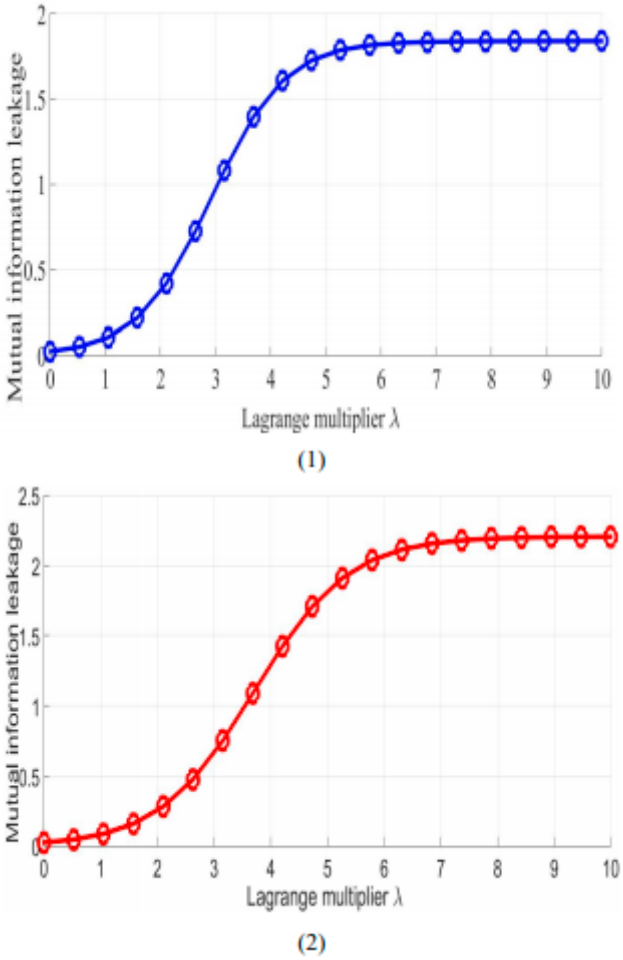


Figure 6

Lagrange multipliers and mutual information, (1) no auxiliary knowledge, (2) auxiliary knowledge

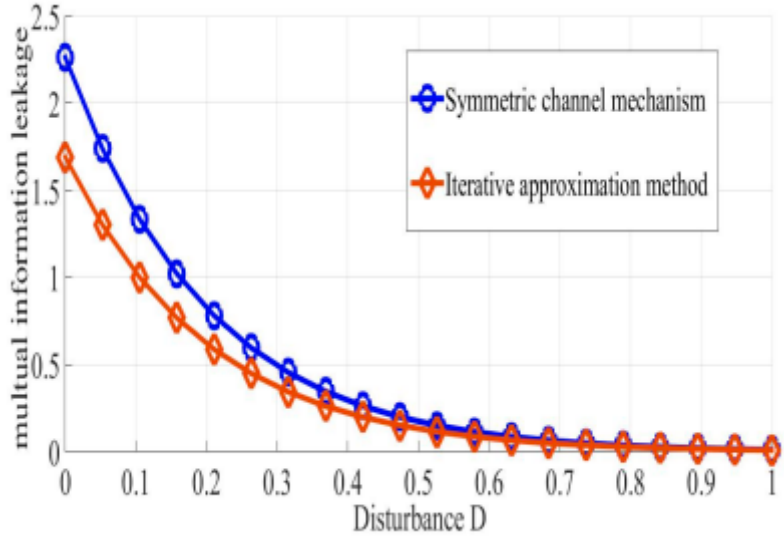


Figure 7

Comparison of two differential privacy channel

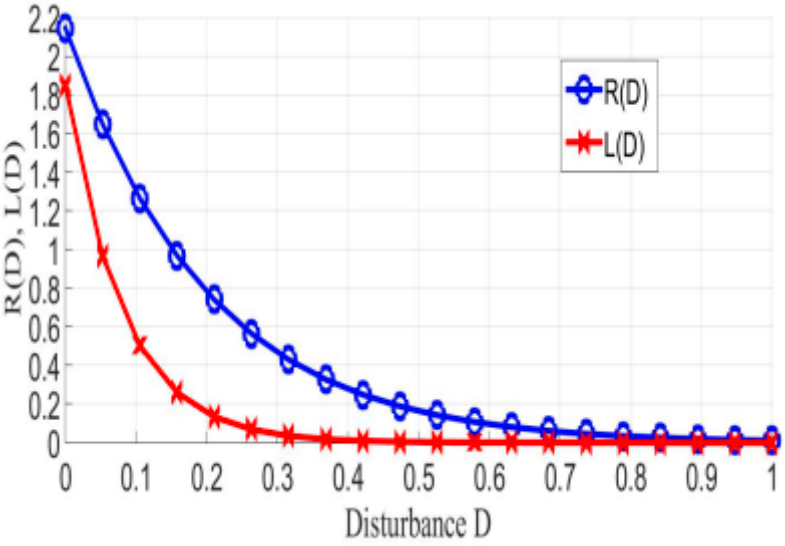


Figure 8

Rate distortion and privacy leakage trends

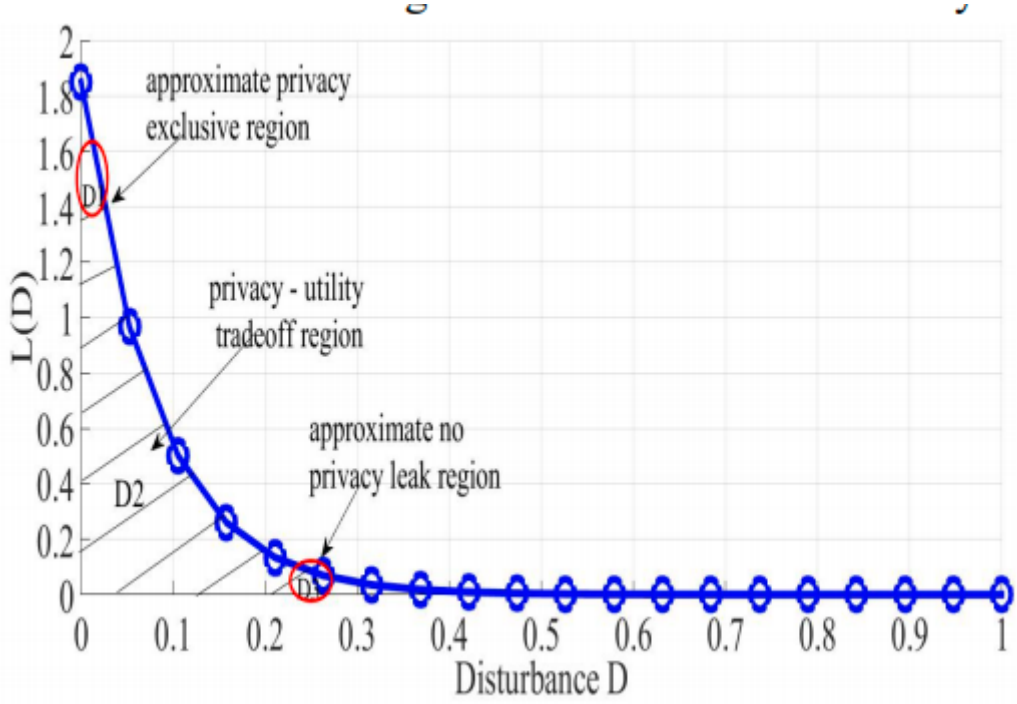


Figure 9

Tradeoff region of privacy and utility