Contextually Private Mechanisms

Contextually Private Mechanisms

ANDREAS ALEXANDER HAUPT, Massachusetts Institute of Technology, USA
ZOË KETTLER HITZIG, Harvard University, USA

Consider a mechanism design environment in which a designer sequentially queries agents' private information to determine the outcome of a choice rule. The designer's social and technological environment constrains the set of access *protocols* that it can use. In high-tech environments, arbitrary cryptographic protocols are admissible, and so privacy concerns do not constrain the set of available choice rules. In other environments, privacy desiderata are needed to guide design. A protocol is *contextually private* for a choice rule if each piece of information learned about each participant is needed to determine the outcome. We characterize choice rules that can be implemented with a contextually private protocol under different assumptions about the class of admissible protocols. Under the assumption that private information must be elicited sequentially from uniquely-identified agents, the serial dictatorship and the first-price auction have contextually private implementations. However, no other k^{th}-price auction has a contextually private implementation, nor does any stable choice rule (in college assignment) or individually rational and efficient choice rule (in house assignment). Under a more generous assumption, which additionally allows the designer to anonymously count the number of agents whose private information has a certain property, the designer has wider scope: we describe a contextually private tâtonnement-like implementation of several choice rules that are not contextually private under the stricter assumption.

The full article: https://arxiv.org/abs/2112.10812

CCS Concepts: • **Social and professional topics → Privacy policies**; • **Applied computing → Economics**.

Additional Key Words and Phrases: mechanism design, privacy, extensive-form games

EC '22, July 11–15, 2022, Boulder, CO, USA.

ACM ISBN 978-1-4503-9150-4/22/07.
https://doi.org/10.1145/3490486.3538259