

MIT Open Access Articles

Contextually Private Mechanisms

The MIT Faculty has made this article openly available. ***Please share*** how this access benefits you. Your story matters.

Citation: Haupt, Andreas and Hitzig, Zo?. 2022. "Contextually Private Mechanisms."

As Published: <https://doi.org/10.1145/3490486.3538259>

Publisher: ACM|Proceedings of the 23rd ACM Conference on Economics and Computation

Persistent URL: <https://hdl.handle.net/1721.1/146424>

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

Terms of Use: Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.



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

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

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

© 2022 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-9150-4/22/07.

<https://doi.org/10.1145/3490486.3538259>