

Lines of Research

Vicenç Torra

October, 2013

Institut d'Investigació en Intel·ligència Artificial (IIIA-CSIC), Bellaterra, Catalonia

Research Lines

Lines of research

- Types of data
 - Graphs and online social networks
 - Search logs
 - ★ Respondent privacy (AOL-like approach); User privacy
 - Documents
 - ★ Document sanitization: removing sensitive information from the document

Lines of research

- Topics
 - Differential privacy
 - Application of differential to different types of data
 - Connections (criticisms) between differential privacy and already existing approaches

Lines of research

Venues: (Security, Cryptography, Databases, Statistics, Official Statistics)

- Journals

- Transactions on Data Privacy (IIIA-CSIC, Open Access, from 2008)
- Journal of Privacy and Confidentiality (CMU, Open Access, from 2009)
- IEEE Security and Privacy (IEEE, from 2003)

- Conferences

- S&P IEEE Symposium on Security and Privacy
- PETS - Privacy Enhancing Technologies
- WPES - Workshop On Privacy In The Electronic Society
- PST - Conference on Privacy, Security and Trust
- PSD - Privacy in Statistical Databases

Lines of research

Privacy at IIIA-CSIC (I)

- Disclosure risk.
 - Formalization of reidentification (in terms of imprecise probabilities)
 - Specific-disclosure risk measures (against microaggregation, rank swapping)
 - Machine learning for improving disclosure risk measures

Lines of research

Privacy at IIIA-CSIC (II)

- Masking methods
 - *Classical* methods
 - ★ microaggregation, rank swapping, PRAM
 - ★ Genetic algorithms for improving IL, DR (postrandomization)
 - ★ Genetic algorithms for PRAM
 - Documents
 - ★ Document sanitization
 - ★ Indexes for documents
 - Graphs and online social networks
 - ★ Perturbative approaches for graphs and social networks
 - ★ k-anonymity
- Privacy agent for anonymous database search
 - Queries Google with several virtual partial identities (manages user's identity, classifies queries to identities)

Thank you