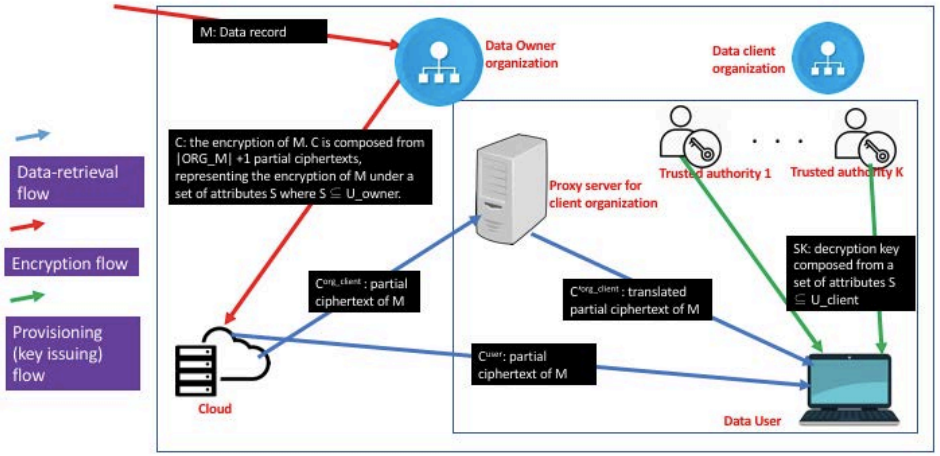
Hiding Hay in a Haystack: Integrating Censorship Resistance into the Mainstream Internet

Challenge:

- Privacy-preserving interorganizational data sharing



Data-Sharing System Architecture

Solution:

- One key innovation is a novel twist on attribute-based encryption, which we call *attribute translation*.
- Translation is performed by a *semi-trusted proxy.*

CNS 1409599, Yale University
Joan Feigenbaum

Scientific Impact:

- Attribute translation, which we use to enable inter-organizational database queries that preserve organizational privacy, may find other applications in multi-party data architectures.
- We provide the community with an additional example of how cryptographic protocols can enable government agencies to obtain information they need without indiscriminate, bulk data collection.

Broader Impact:

- Government agencies will be able to query private companies' databases (e.g., phone metadata collections) without learning anything they do not need to know about the data or the database schema.
- Several PhD students have been supported in whole or in part.