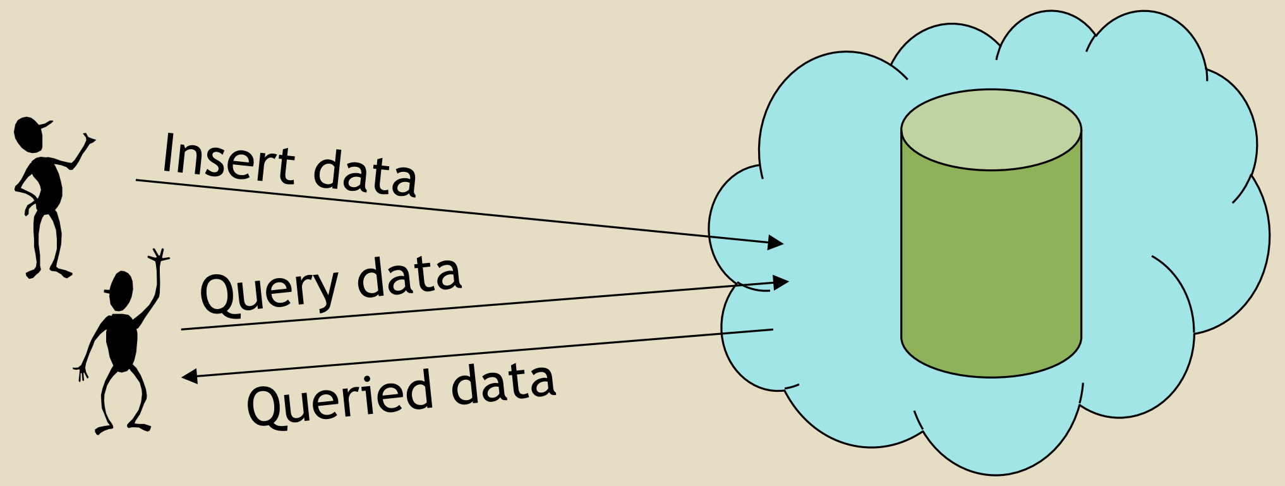
Efficiently-Searchable Encryption

Award ID 0831184

PI: Alexandra (Sasha) Boldyreva, Georgia Institute of Technology

Problem

- Client offloads data storage and management to remote database server/cloud
- Client queries and updates data over the network
- Data is sensitive and provider untrusted



Desired properties

- Security (as much as possible)
- Functionality (various query types, data encrypted by users on-the-fly)
- Efficiency (logarithmic-time search)

It is challenging to satisfy all properties simultaneously

Prior work

Previous solutions either

- provide strong security, but either
  - require linear scan of the data on each query, or
  - require pre-processing of the whole data by the user, or
- are ad-hoc with no provable-security analysis

Project contributions

Overview

- We seek provably secure efficiently-searchable encryption schemes which have the aforementioned desired properties
- We look at both public-key and symmetric-key settings

- We address
  - ① exact-match queries
  - ② range queries
  - ③ fuzzy queries, which tolerate typos or for noisy data, such as biometrics

- For each topic (see table below) we
  - ① design new appropriate security definitions
  - ② propose new schemes
  - ③ prove them secure

	Setting	Symmetric key	Public key
Query type	Exact match queries	Efficiently-searchable authenticated encryption (ESE) [ABO07]	Deterministic encryption (DE) and Efficiently-searchable encryption (ESE) [BBO07,BFOR08,BFO08]
	Range queries	Order-preserving encryption (OPE) [BCLO09,BCO11]	No meaningful security can be achieved
	Fuzzy search queries (search tolerating typos or for noisy data like biometrics)	Efficient fuzzy-searchable encryption (EFSE) [BC12-13]. Work in progress, more work is needed	Open problem

Impact

- Three PhD students graduated with their theses built upon this sponsored research (two of which relied solely on this project)
- DE and OPE have been implemented and incorporated as part of CryptDB project [PRZB12], which was recently featured in Forbes magazine
- OPE is being considered for adoption by several companies
- More than 10 publications sponsored by the award (with eight in top conferences), and approximately 400 citations

Interested in meeting the PI? Attach post-it note below or email sasha@gatech.edu

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27-29th 2012, National Harbor, MD