

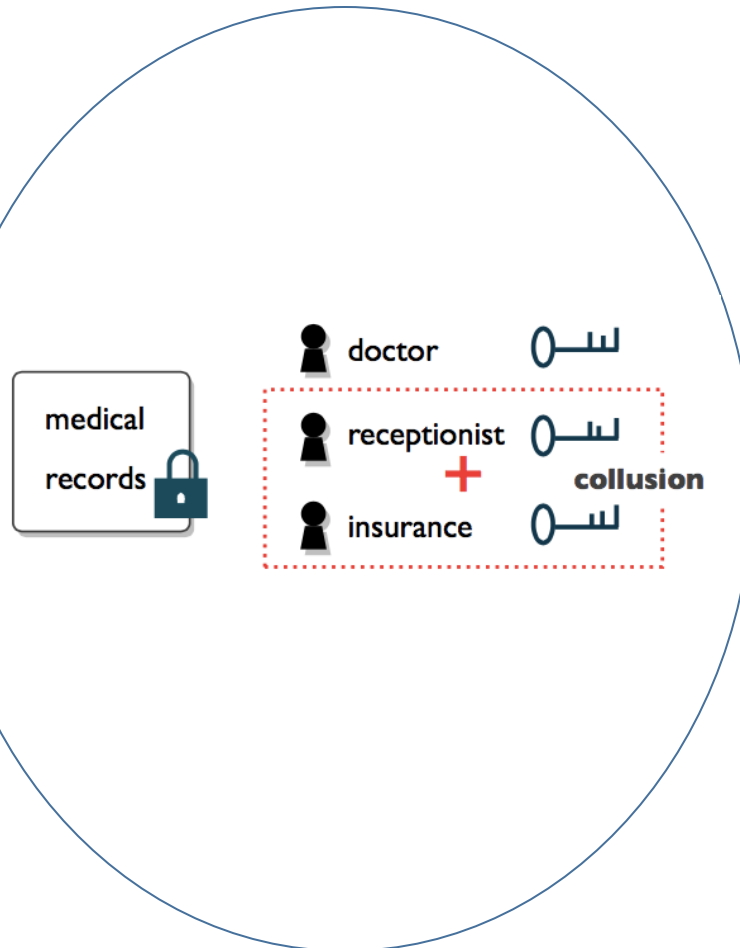
SaTC: Small: New Challenges in Functional Encryption

Challenge:

Can we encrypt data while enabling fine-grained access control and selective computation, as is necessary to protect big, complex data?

Solution:

- Investigate emerging paradigm of functional encryption
- Advanced frontiers of efficient and expressive schemes



Scientific Impact:

- Enables outsourcing data while preserving user privacy
- New techniques and applications in the broader field of cryptography

Broader Impact:

- Dissemination via New York Area Crypto Day, and Workshop for Cryptography for Big Data.
- Participation in IETF TLS 1.3 standards

NSF 1445424

Tal Malkin tm2118@columbia.edu

Hoeteck Wee hw2240@columbia.edu