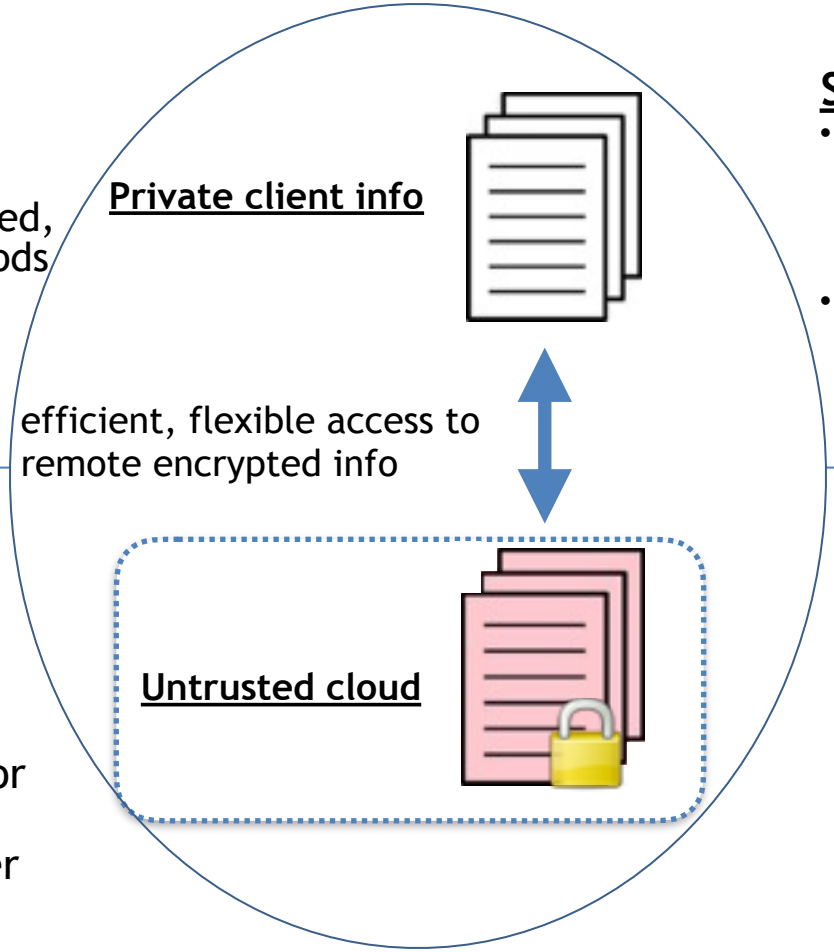
Cryptography for Secure Outsourcing

Challenge:

- Cloud systems are routinely compromised, but mitigation methods like client-side encryption are often inconvenient and slow.



Solution:

- Multi-methodology combining theory and empirical approaches
- New attacks on prior systems, new constructions, lower bounds

Scientific Impact:

- Push crypto theory towards practical deployment by analyzing security in practice, and designing around new insights
- Prove lower bounds showing that some goals are impossible

Broader Impact:

- Attacks on two industry systems (one deployed, one in beta) have been patched
- New constructions of searchable encryption being implemented in industry
- Summer “math camp” class on crypto

PI: David Cash (Rutgers University)
Award #1453132