ALPTEKİN KÜPÇÜ

Assistant Professor of Computer Science and Engineering

KOÇ
UNIVERSITY

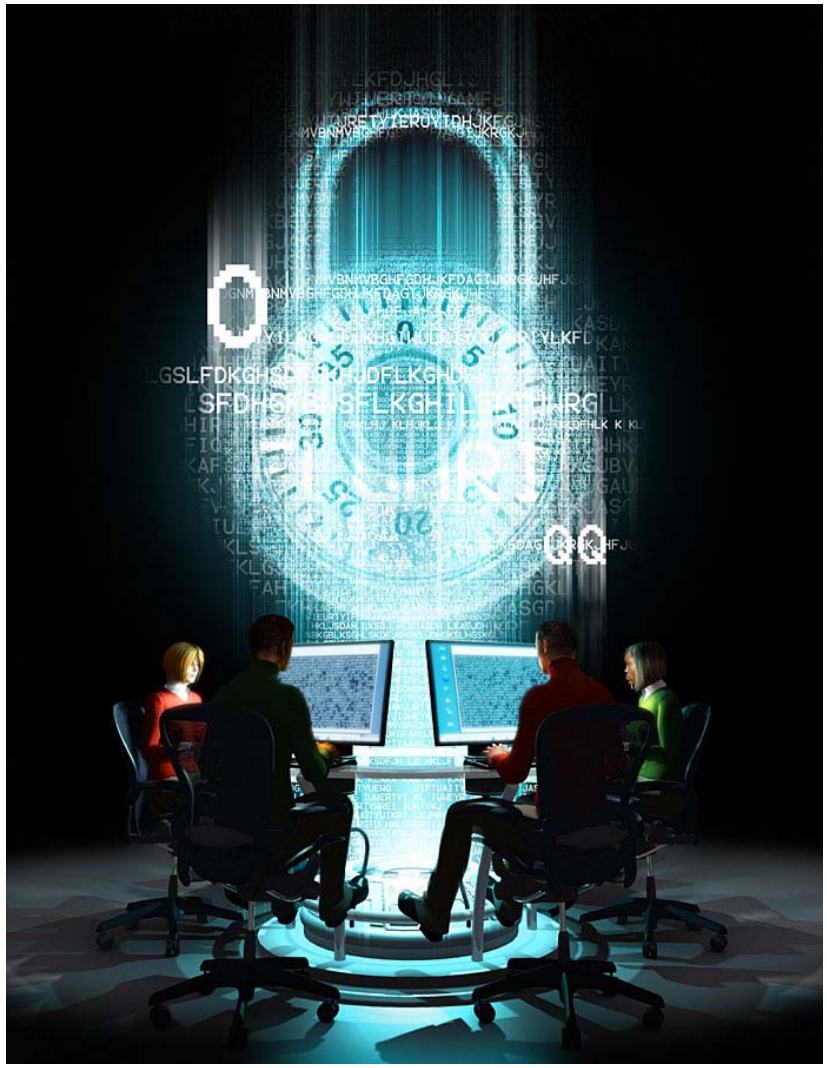
General

Ph.D., Brown University (2004-2010)
Asst. Prof., Koç University (2010-)

Cryptographic protocols can efficiently and scalably be used to provide security and privacy for the next generation cloud systems.

Research Topics

- **Core Research**
  - Cryptography
  - Security
  - Privacy
- **Application Areas**
  - Cloud Computation
  - Cloud Storage
  - Peer-to-Peer Systems
  - Electronic Cash
  - Electronic ID Cards
  - Password-based Authentication
  - ...



Cloud Computation

[BCEJKL08]

Challenges:

Outsource a job to a more powerful entity, or multiple small entities, and get correct results, without wasting own resources.

Current Generation:

Amazon Mechanical Turk, SETI@Home, etc.
Job is not well-defined.
Results can be faked.
No provable guarantees.

Techniques:

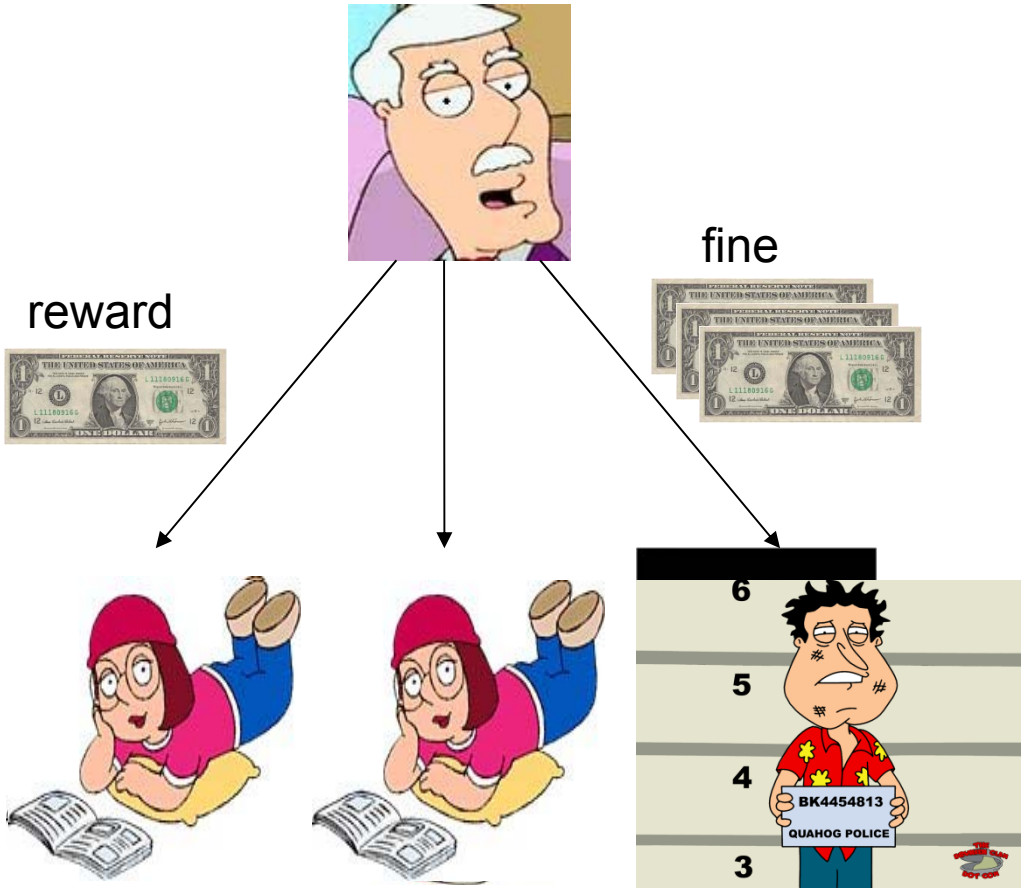
Game Theory and Mechanism Design, augmented with cryptographic techniques to deal with Byzantine users.

Next Gen Cloud Computation

[BCEJKL08]

Our Solutions:

Guaranteed high fraction of correct results, even in presence of malicious users. Malicious users cannot force the boss to perform tons of extra work.



Cloud Storage

[EKPT09][K12][EK12][CKW12]

Challenges:

Outsource storage of data to a more powerful entity, or multiple small entities, while data will be kept intact, or you will get compensated.

Current Generation:

Amazon S3, Google Drive, Dropbox, etc.
No guarantee that file will be kept intact (i.e. No modifications or deletions).

Techniques:

Cryptography, as well as secure protocol design, probability, and error-correcting codes (erasure codes).

Next Gen Cloud Storage

[EKPT09]

UPDATE

PROOF OF UPDATE

CHALLENGE

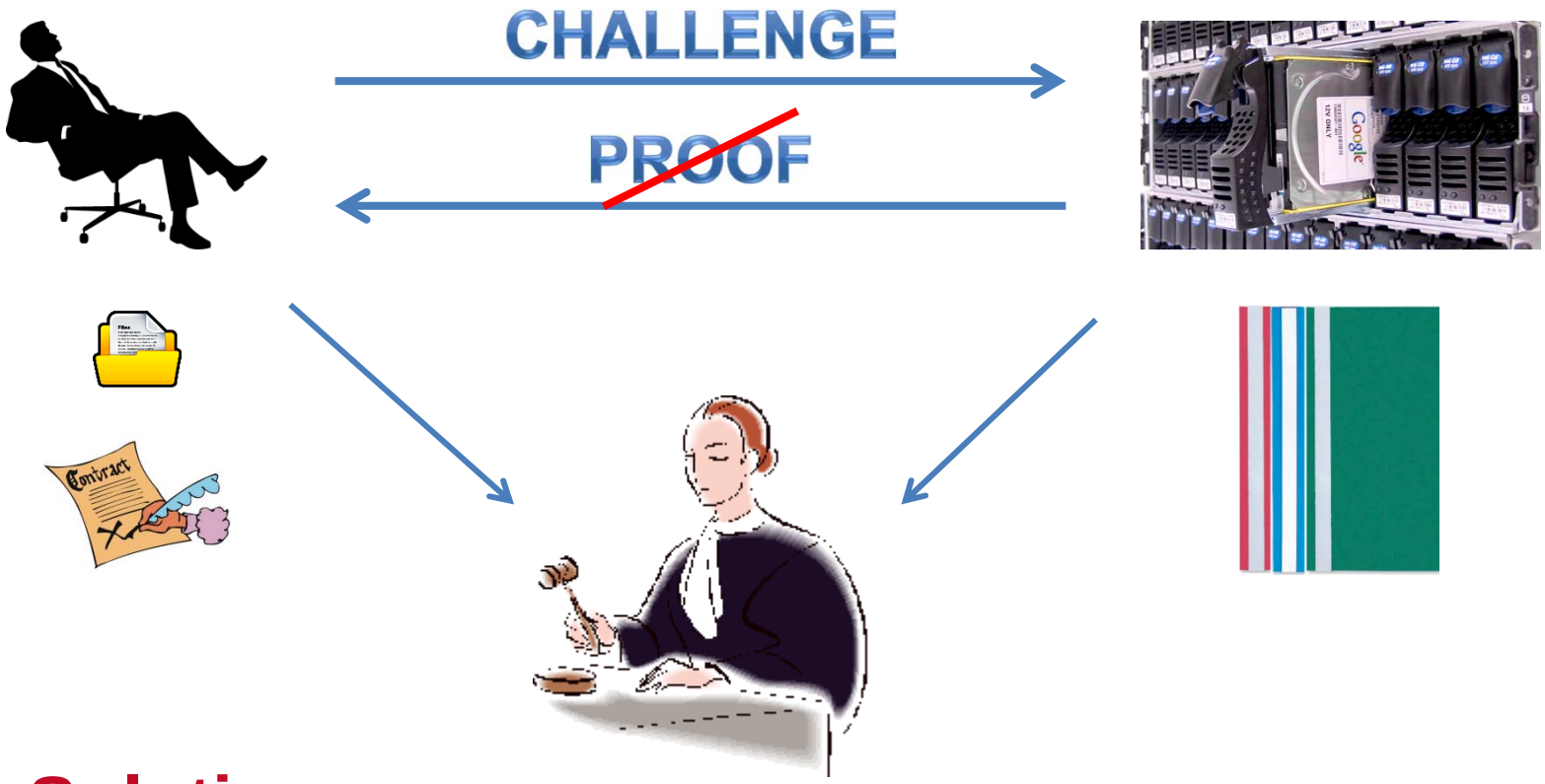
PROOF

Our Solutions:

Guaranteed high probability detection of integrity loss of data.

Next Gen Cloud Storage

[K12]



Our Solutions:

Automated official arbitration system with compensation (via e-cash).

Peer-to-Peer Systems

[BCEJKLR07][KL09][KL10a][KL10b][KL12]

Challenges:

Incentivize peers to contribute to the system, thereby increasing overall system performance and fault tolerance.

Techniques:

Cryptography (fair exchange protocols and electronic cash), together with economic analysis and game-theoretic models.

Our Solutions:

Forced fair contribution by peers both increase the fault tolerance of the system, as well as increased performance.

Electronic Cash

[BCEJKLR07][MEKHL10]

Applications:

Electronic commerce, privacy-protecting protocols, anonymous credentials and electronic identity cards.

Use Cases:

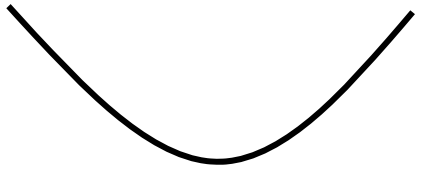
Cryptographic protocol design, virtual economies, automated payments, and even official arbitration mechanisms.

Future Uses:

Accountability issues can be handled through e-cash while preserving privacy (e.g., in GPS, transport, or cloud systems).

Efficient Cryptography

TOPIC	RELATED WORK	OUR WORK
Cloud Storage network overhead	N/A	10 KB
Cloud Storage computation overhead	N/A	1 ms
Judge Arbitration network overhead	25 KB	80 bytes
Judge Arbitration computation overhead	1 second	2 ms
P2P Fairness network overhead (over 2.8 GB)	225 MB	1.8 MB
P2P Fairness computation overhead (over 1.5 hours)	42 minutes	40 seconds



2-3 orders of magnitude

Collaboration Areas

- **Other possibilities:**
  - **Outsourced Databases**
    - Privacy (e.g., PIR, obfuscation)
  - **Usable Security**
    - Password-based Authentication and OTP
  - **Peer-to-Peer Systems**
    - Fair (video) streaming
  - **Anonymous Credentials (and E-cash)**
    - Electronic ID and Passport
  - **Electronic Health**
    - Privacy-preserving Information Sharing

ALPTEKİN KÜPÇÜ

Assistant Professor of Computer Science and Engineering

http://crypto.ku.edu.tr

KOÇ
UNIVERSITY

References

- [BCEJKLR07] Mira Belenkiy, Melissa Chase, Chris Erway, John Jannotti, Alptekin Küpçü, Anna Lysyanskaya, and Eric Rachlin. “Making P2P Accountable without Losing Privacy”. ACM WPES, 2007.
- [BCEJKL08] Mira Belenkiy, Melissa Chase, Chris Erway, John Jannotti, Alptekin Küpçü, and Anna Lysyanskaya. “Incentivizing outsourced computation”. NetEcon, 2008.
- [KL09] Alptekin Küpçü and Anna Lysyanskaya. “Brief Announcement: Impossibility Results on Optimistic Fair Exchange with Multiple Autonomous Arbiters”. PODC 2009. Full version available as Cryptology ePrint Archive Report 2009/069.
- [EKPT09] Chris Erway, Alptekin Küpçü, Charalampos Papamanthou, and Roberto Tamassia. “Dynamic Provable Data Possession”. ACM CCS 2009. Full version available as Cryptology ePrint Archive Report 2008/432.
- [KL10a] Alptekin Küpçü and Anna Lysyanskaya. “Usable Optimistic Fair Exchange”. CT-RSA 2010. Full version available as Cryptology ePrint Archive Report 2008/431.
- [KL10b] Alptekin Küpçü and Anna Lysyanskaya. “Optimistic Fair Exchange with Multiple Arbiters”. ESORICS, 2010.
- [MEKHL10] Sarah Meiklejohn, Chris Erway, Alptekin Küpçü, Theodora Hinkle, and Anna Lysyanskaya. “Enabling Efficient Implementation of Zero-Knowledge Proofs and Electronic Cash with ZKPDL”. USENIX Security, 2010.
- [K10] Alptekin Küpçü. “Efficient Cryptography for the Next Generation Secure Cloud: Protocols, Proofs, and Implementation”. Lambert Academic Publishing, 2010.
- [KL12] Alptekin Küpçü and Anna Lysyanskaya. “Usable Optimistic Fair Exchange”. Computer Networks, 2012, 56, 50-63.
- [ABK12] Tolga Acar, Mira Belenkiy, and Alptekin Küpçü. “Single Password Authentication”. Under submission, 2012.
- [K12] Alptekin Küpçü. “Official Arbitration and its Application to Secure Cloud Storage”. Under submission, 2012.
- [EK12] Mohammad Etemad and Alptekin Küpçü. “Transparent, Distributed, and Replicated Dynamic Provable Data Possession”. Under submission, 2012.
- [CKW12] David Cash, Alptekin Küpçü, and Daniel Wichs. “Dynamic Proofs of Retrievability via Oblivious RAM”. Under submission, 2012.