ALPTEKİN KÜPÇÜ
Assistant Professor of Computer Science and Engineering
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
  - ...

2012 Alptekin Küpçü - Koç University
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.
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.
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).
Our Solutions:
Guaranteed high probability detection of integrity loss of data.
Next Gen Cloud Storage

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

BCEJKLR07][MEKHL10]
## Efficient Cryptography

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

2-3 orders of magnitude
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
References


