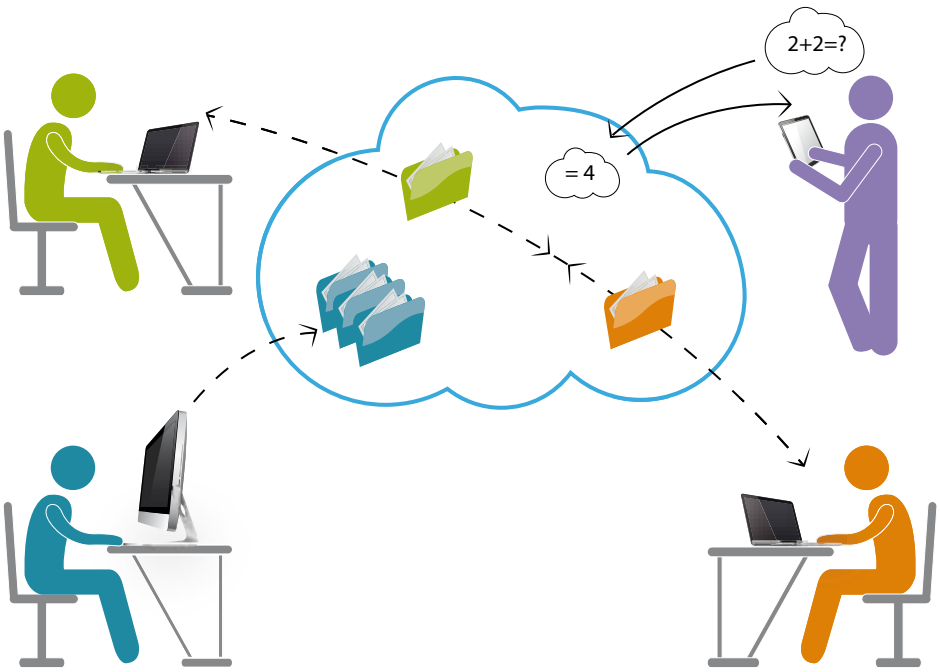
Efficient Cryptography for the Next Generation Secure Cloud

Secure Your Virtual Existence!

Alptekin Küpçü Assistant Professor of Computer Science and Engineering, Koç University



Koç University Cryptography, Security, and Privacy Research Group prepares highly-efficient and thoroughly-secure solutions for global problems.

We all benefit from the endless alternatives that cloud provides us regarding our storage, computation, and distribution needs. For example, Dropbox or Wuala store our data in the cloud, so that we can reach it anywhere, anytime. Amazon EC2 and SETI@Home projects let us outsource a computational job that is beyond our computer's capabilities to the cloud. This way, more powerful machines or multiple other computers help us solve the problem. Rapidshare and BitTorrent are pervasive examples that help us distribute the files that we want to share with friends or with the world, easily, without overloading our own resources. Unfortunately, all these benefits are not without any risk!

Do you use Dropbox, Sugarsync, Box, Google Drive, or a similar service? If so, do you know that these companies are not responsible in case of a loss of or modification to your data on their servers? Unfortunately, none of the current cloud storage systems provide any provable guarantees about the integrity of your data. Yet, by using cryptographic techniques, it is possible to check for the integrity of the stored data, and get an appropriate proof.

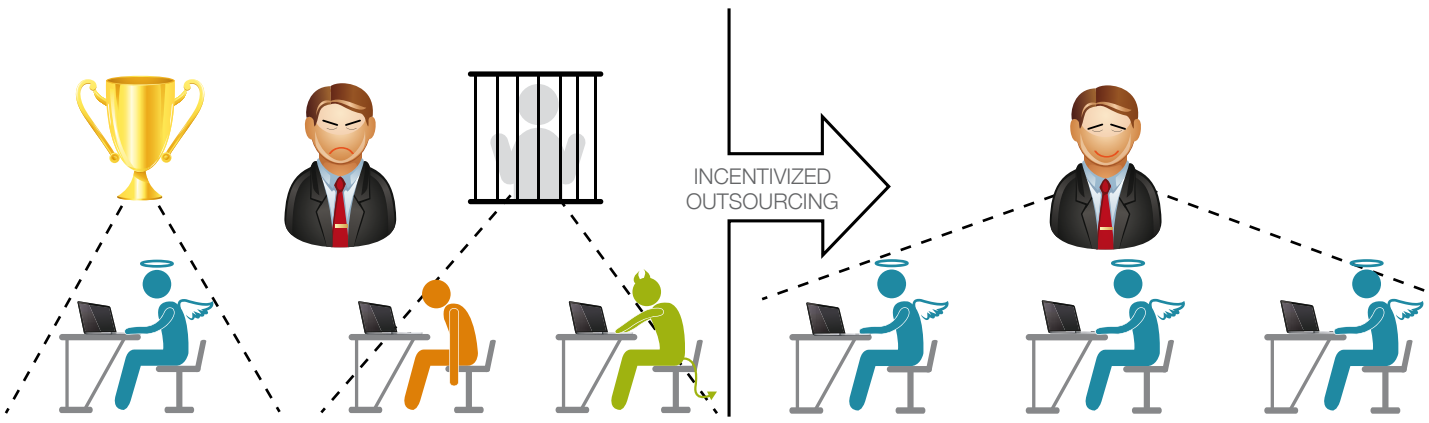
Our group focuses on providing efficient cryptographic solutions to problems in the current-generation cloud systems, so that the next-generation cloud services will be provably secure by design.

Our cloud storage system keeps a very small amount of local information about your data in the cloud. Using this information, you may easily update your data, and hence obtain the corresponding updated local information. Whenever you would like to, you may challenge the server to prove to you that your data is still kept intact. If the proof fails when verified with your local data, this means the server has corrupted or lost your data, and hence you may contact a judge at an official court and ask for the payment of a warranty amount. You do not even need to wait in queues outside court houses: The judge can be an automated computer, and even the payments can be made online. Parts of this research are supported by respected cloud companies Koç Sistem and Türk Telekom. Therefore, you get the chance to change people's lives by implementing a prototype using our cryptographic library, and we should expect to see real deployments soon.

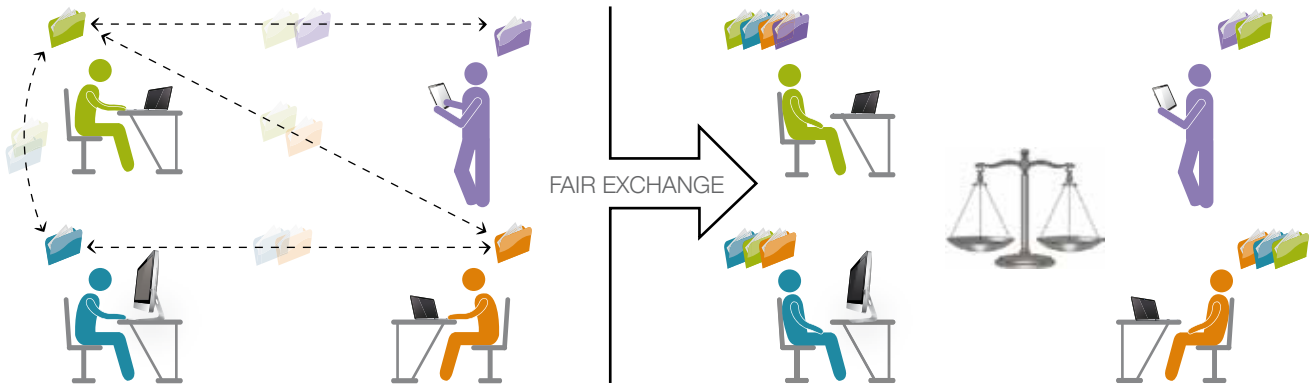
Have you ever participated as a contractor in a cloud computation project such as SETI@Home, Folding@Home, or Electric Sheep? Did you ever try to send a fake result just to improve your reputation? Did you wonder how those people at the top of the list manage to perform so well? Again, current outsourced computation systems have no mechanisms to guarantee correctness of the results. Using cryptography, together with game theory and mechanism design techniques, we provide a very high level of guarantee on the correctness of the returned result, even if some contractors try to cheat.

Once in a while, you would like to be the boss: you want to outsource a computation job. There is no doubt that you would like to obtain guaranteed correct results. Since the existing systems do not provide you with such a warranty, you decide to use our system. Parameters of our outsourcing system can be tweaked such that you decide on the level of guaranteed correctness; whether you want it 99% correct, or 99.9% correct, or even more. Furthermore, our system allows you to reward honest contractors giving you the correct results, and fine malicious contractors who try to cheat.

Have you ever used BitTorrent, Kazaa, Napster, etc. for downloading files? Don't you always stop uploading whenever you receive the whole file? One of the reasons your download is not as fast as it can be is that many people do the same: These free-riders choose to stop uploading a file



Cryptography can make unimaginable things possible…



whenever their download is complete. Mostly, people stop contributing to a system as soon as they obtain all the service they want to. Only altruistic participants continue contributing to the system, without expecting a reward in return. Using cryptographic fair exchange techniques, it is possible to guarantee that everyone contributes to the system as much as they download, thus increasing the system efficiency and speed by increasing contribution.

In a fair exchange scenario, we have two parties, Alice and Bob, who have one item each (e.g., files) that they would like to exchange. Fairness means either Alice obtains Bob's file and Bob obtains Alice's file, or neither party obtains anything. Applying the fair exchange idea to BitTorrent means that one needs to participate in uploading, to be able to download. This solves the free-riding problem of BitTorrent, forcing all downloaders to participate and upload, thereby increasing overall efficiency of the system. Furthermore, fair exchange idea is not limited by usage in BitTorrent. If you believe that the Internet should be fair, you may choose to join our "Fairness in the Cloud" project (equivalent of NSF Career Project), sponsored by TÜBİTAK (The Scientific and Technological Research Council of Turkey), and work on applying fairness on various online systems, including cloud computation and storage.

If you join the Cryptography, Security, and Privacy Research Group at Koç University, you will be setting sail to a whole new world of seemingly impossible reality. Cryptography can make unimaginable things possible…

References:

[Book] Alptekin Küpçü. "Efficient Cryptography for the Next Generation Secure Cloud: Protocols, Proofs, and Implementation". Lambert Academic Publishing, 2010.

[CloudStorage] Chris Erway, Alptekin Küpçü, Charalampos Papamanthou, and Roberto Tamassia. "Dynamic Provable Data Possession". In proceedings of ACM CCS, 2009.

[CloudComputation] Mira Belenkiy, Melissa Chase, Chris Erway, John Jannotti, Alptekin Küpçü, and Anna Lysyanskaya. "Incentivizing Outsourced Computation". In proceedings of NetEcon, 2008.

[FairExchange] Alptekin Küpçü and Anna Lysyanskaya. "Usable Optimistic Fair Exchange". Computer Networks, 2012, vol. 56, pp. 50-63.

[Library] Sarah Meiklejohn, Chris Erway, Alptekin Küpçü, Theodora Hinkle, and Anna Lysyanskaya. "ZKPDL: Enabling Efficient Implementation of Zero-Knowledge Proofs and Electronic Cash". In proceedings of USENIX Security, 2010. http://github.com/brownie/cashlib

Alptekin Küpçü has received his Ph.D. degree from Brown University Computer Science Department in 2010. Since then, he has been working as an assistant professor at Koç University College of Engineering, leading the Cryptography, Security & Privacy Research Group he has founded. His research mainly focuses on applied cryptography, and its intersection with cloud security, privacy, peer-to-peer networks, and mechanism design.

He has various honors and awards, and several pending patent applications. Within the past 2 years, he has been involved in 6 funded research projects, of 4 of which he has been the principal investigator. For more information, visit http://crypto.ku.edu.tr