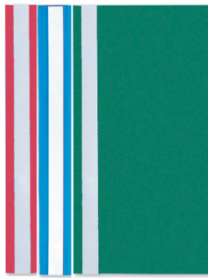
Official Arbitration for Cloud Storage

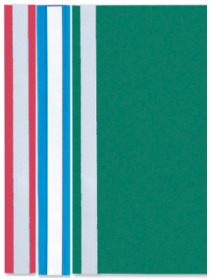
Alptekin Küpçü

KOÇ UNIVERSITY

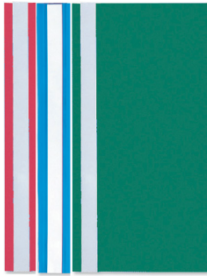
Cloud Storage



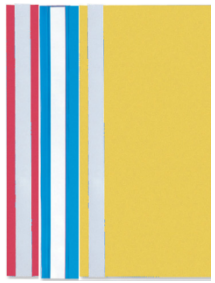
Cloud Storage



Cloud Storage

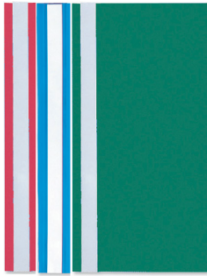


Untrusted Storage



Untrusted Storage

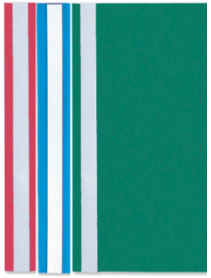
Provable Storage



Provable Storage

CHALLENGE

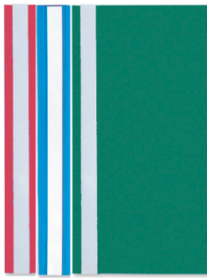
PROOF



Provable Storage

CHALLENGE

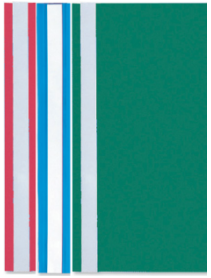
PROOF



Dynamic Provable Storage

UPDATE

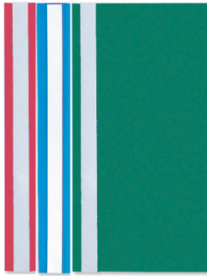
PROOF



Problem

CHALLENGE

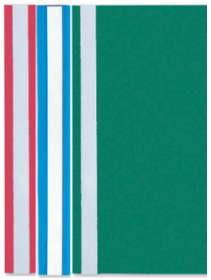
PROOF



Public Verifiability

CHALLENGE

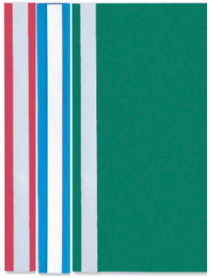
PROOF



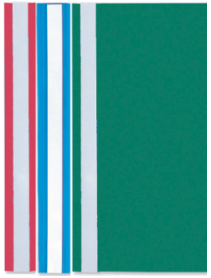
Public Verifiability

CHALLENGE

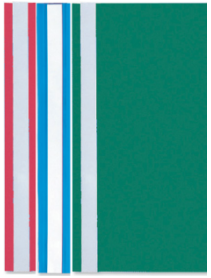
PROOF



Arbitratable Provable Storage



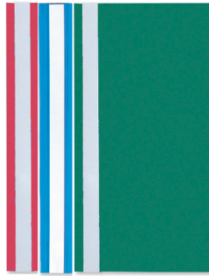
Arbitratable Provable Storage



Official Arbitration

CHALLENGE

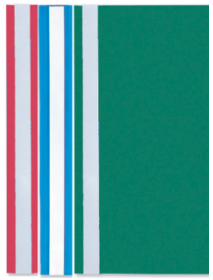
PROOF



Official Arbitration

CHALLENGE

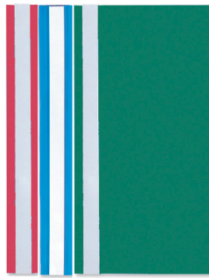
PROOF



Official Arbitration

CHALLENGE

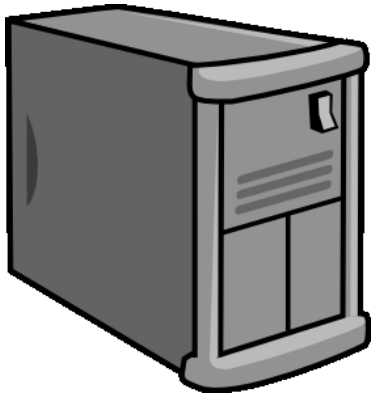
PROOF

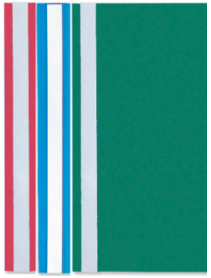


Automated Official Arbitration

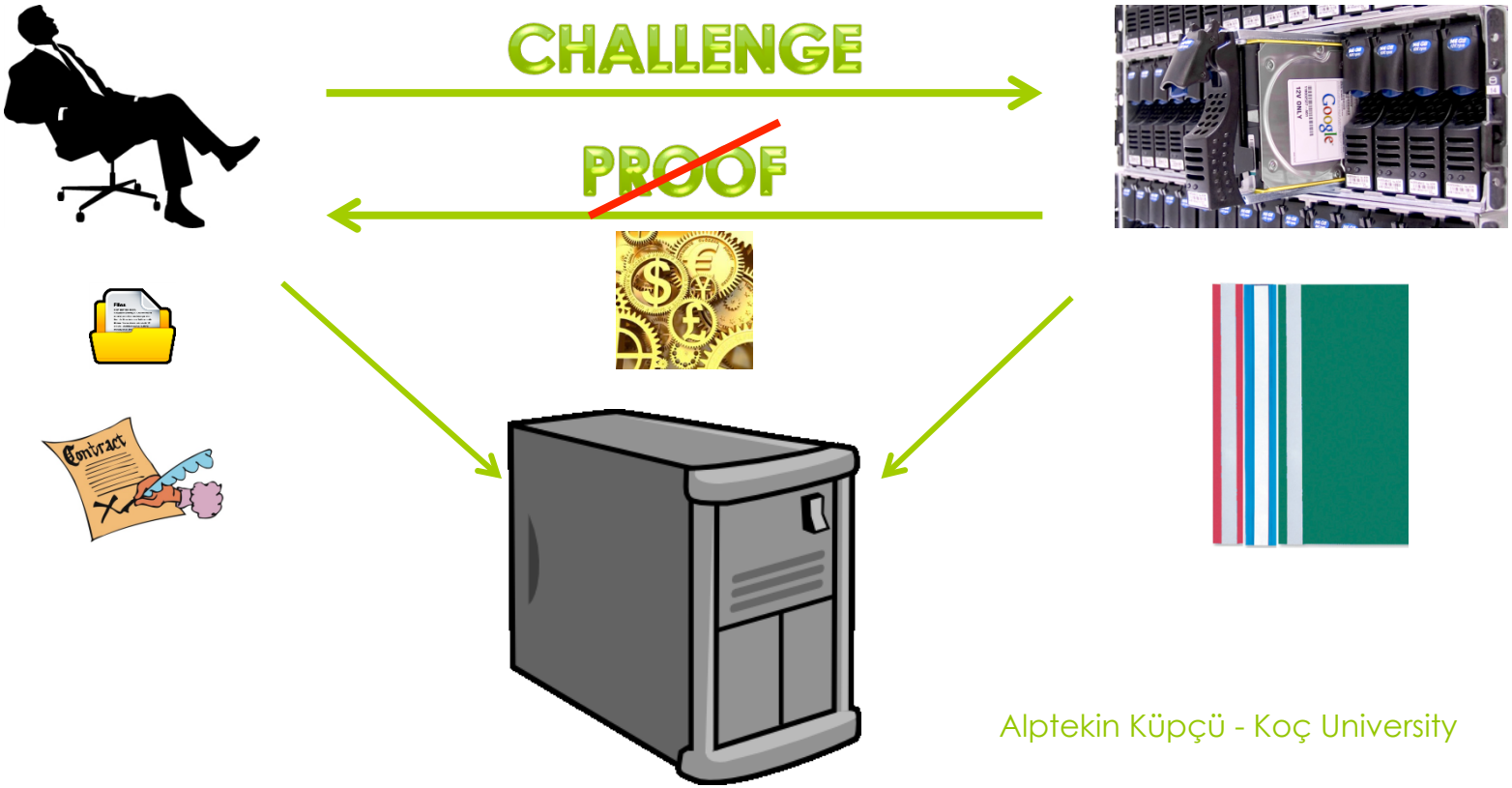
CHALLENGE

PROOF





Automated Warranty



Performance

		Rsync/Tcl/ Samba
Repo	# of commits	~25000
Naive method	Total Network Overhead	610 MB
	Total Computation Overhead	7 hours
Our novel method	Total Network Overhead	2 MB
	Total Computation Overhead	51 seconds
	Network Overhead per Commit	80 bytes
	Computation Overhead per Commit (client + server total)	2 ms

Contributions

- Official Arbitration
  - Not public verifiability
  - Judge can just be a computer
  - Payments can be automated
- 2-3 orders of magnitude efficiency gains
  - Only 80 bytes and 2 ms overhead

Thank You

- Check eprint for full paper (soon)

crypto.ku.edu.tr