Cloud Auditing

Giuseppe Ateniese
Sapienza-University of Rome

Cloud Computing

- Model for enabling access and sharing of computing resources
- Fast provision and minimal management
- Cost saving and IT agility
- NIST Cloud Computing Program: Cloud Auditor

NIST Cloud Computing Standards & Reference Model

- “...a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” (NIST)

Essential Characteristics (NIST)

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured Service

Service Models (NIST)

- Cloud Software as a Service (SaaS)
- Cloud Platform as a Service (PaaS)
- Cloud Infrastructure as a Service (IaaS)

Deployment Models (NIST)

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

Actors

- Cloud Consumer
- Cloud Provider
- Cloud Auditor: “A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.” (NIST)

Cloud Auditor

- Security auditing
- Verification of compliance
- Privacy impact auditing

Cloud Cryptography

- Provable Data Possession
- Proxy Re-Encryption
- Searchable Encryption

Provable Data Possession

Archival Storage Outsourcing

- Electronic records legislation requires:
  - Data be retained for several years
  - Data be available
- Outsourcing data to third parties:
  - Avoids initial setup cost
  - Maintenance and scalability

Third parties cannot be trusted

- Remote servers can misbehave:
  - Reduce cost / increase profit (“freeloading” – Lillibridge et al.)
  - Discard data that is not accessed or rarely accessed (stored on secondary tapes, etc.)
  - Hide data loss incidents due to management errors, hardware failures, attacks, etc.

Our focus: Archival Storage

- Remote servers retain tremendous amounts of data
- Only small parts of the data are retrieved
- Data is stored for a long time (forever)

Source:
www.loc.go

Provable Data Possession

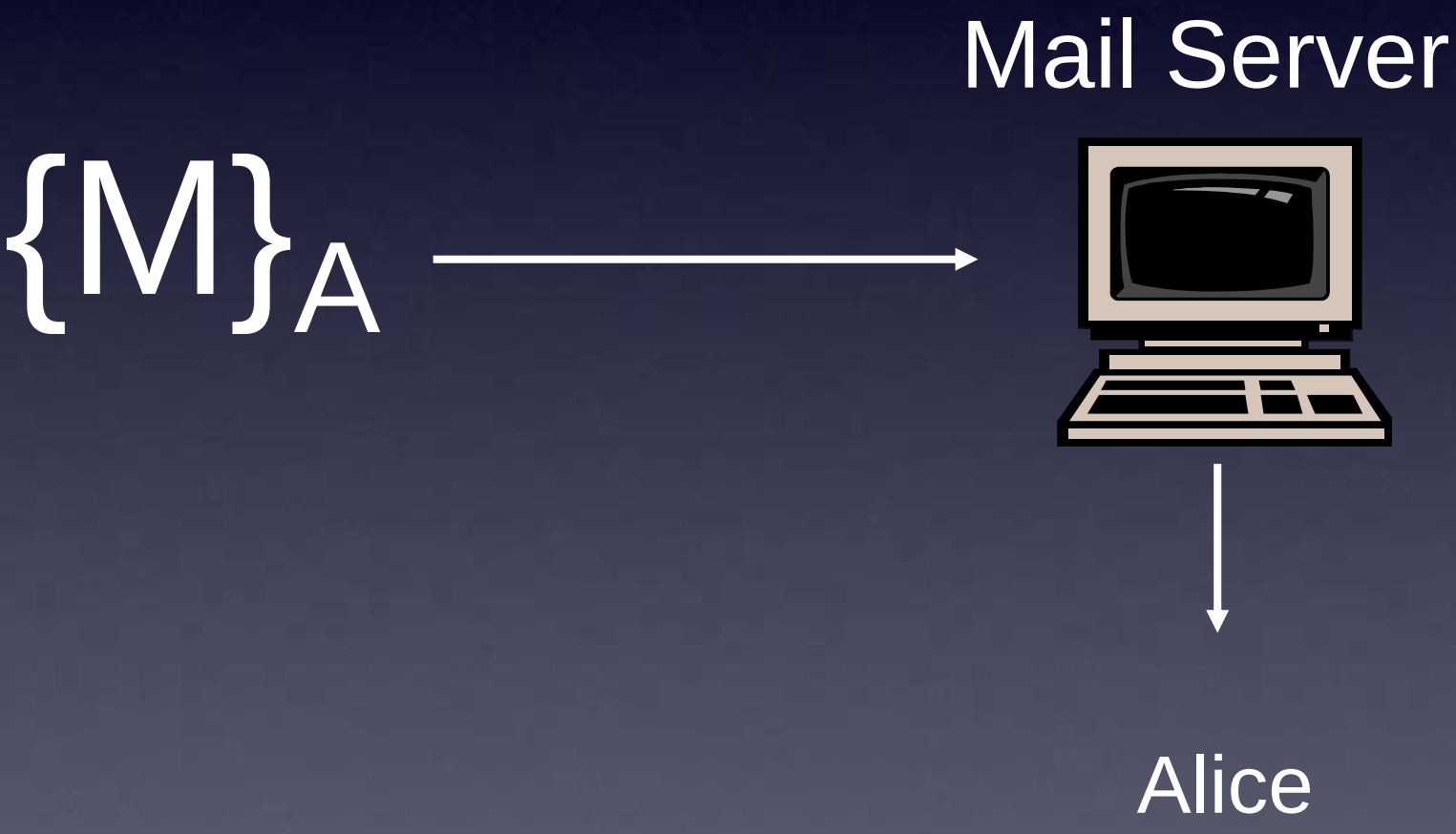
- Can my cellphone verify that the entire content of the Library of Congress is stored and available online?
- We provided the first provably-secure and practical PDP schemes
- We showed experimentally that PDP can be used for very large data sets

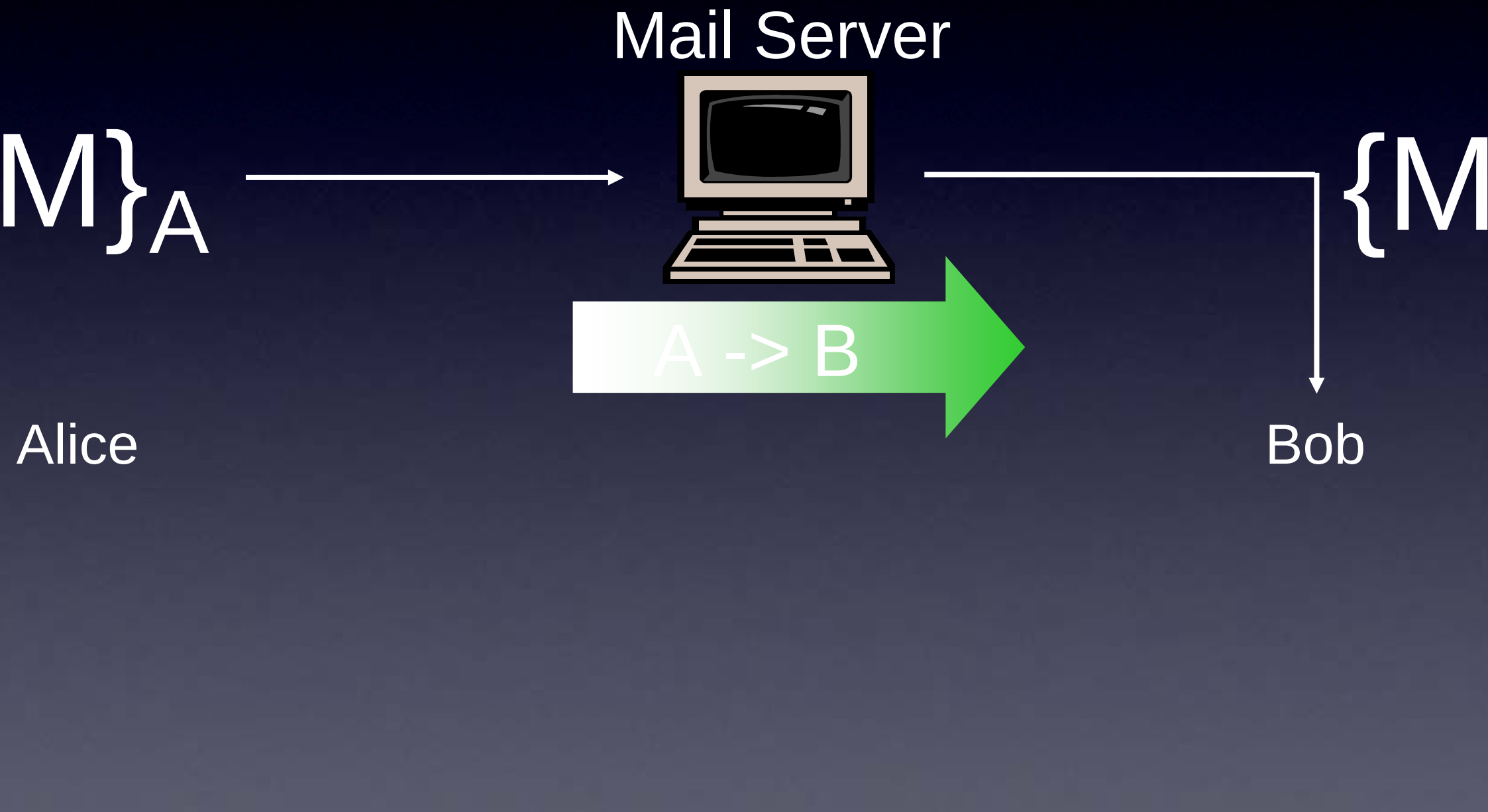
Review of PDP

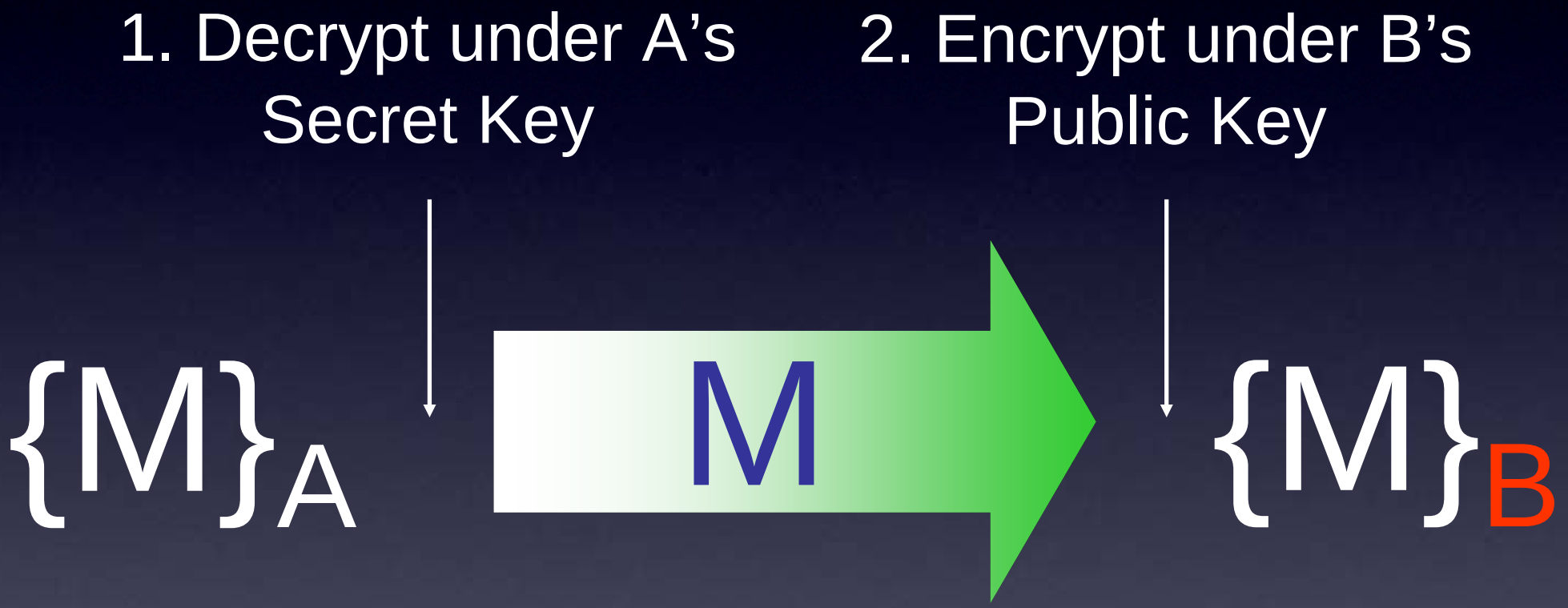
- Trivial schemes that do not work:
  - Check data upon retrieval
  - Ask the storage server (google) to MAC the entire archive
  - Ask the storage server to send a subset of randomly-picked file blocks along with their MACs
- Our target: Aggregate MACS and DO NOT send file blocks!

Proxy Re-encryption: Providing access rights in the Cloud

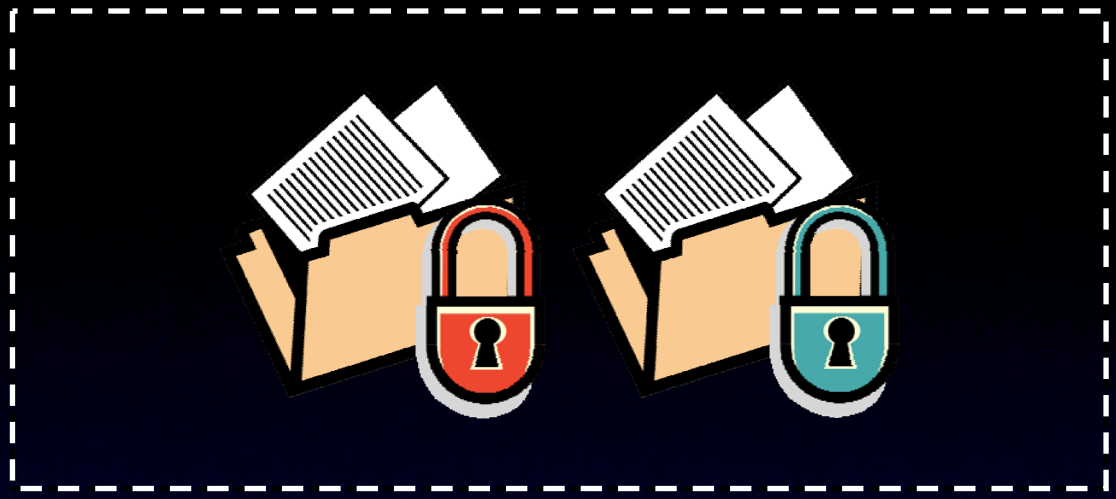
PRE: An Example




Mail Server
M}A
{M
A -> B
Alice
Bob

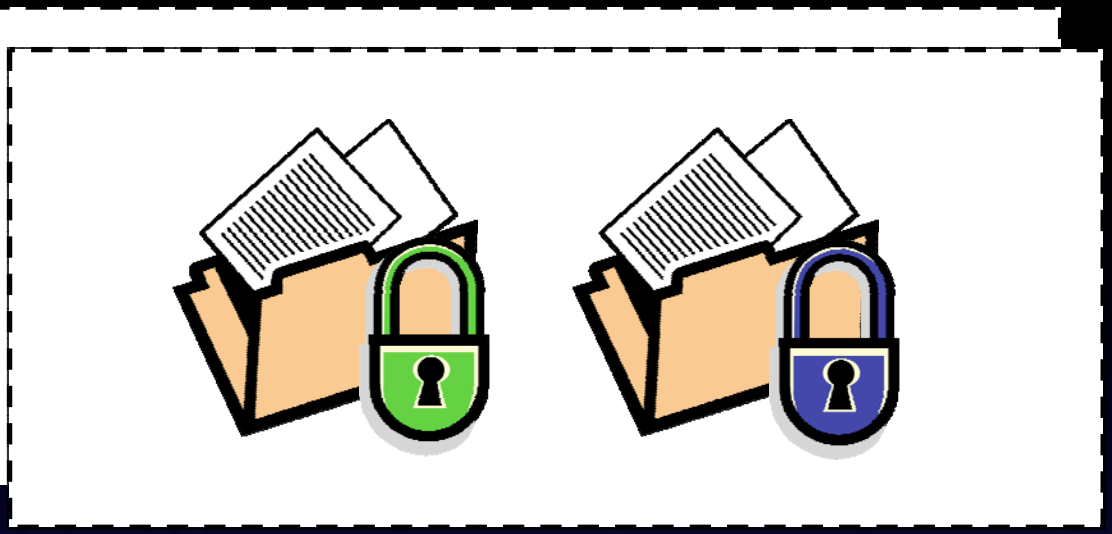

1. Decrypt under A’s Secret Key
2. Encrypt under B’s Public Key
{M}A
M
{M}B

1. Plaintext NOT revealed
2. $rk_{A->B}$ does not reveal secrets



Encrypted File Store

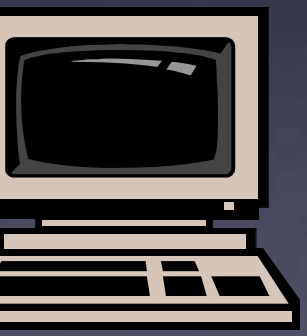
Clients



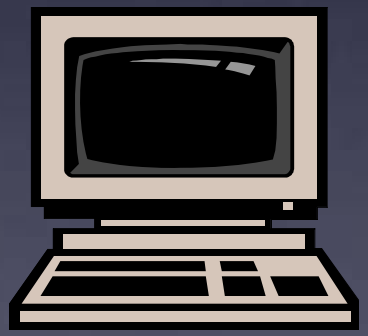
Encrypted File Store(s)

Deliver Key?
(Yes/No)

Key Server

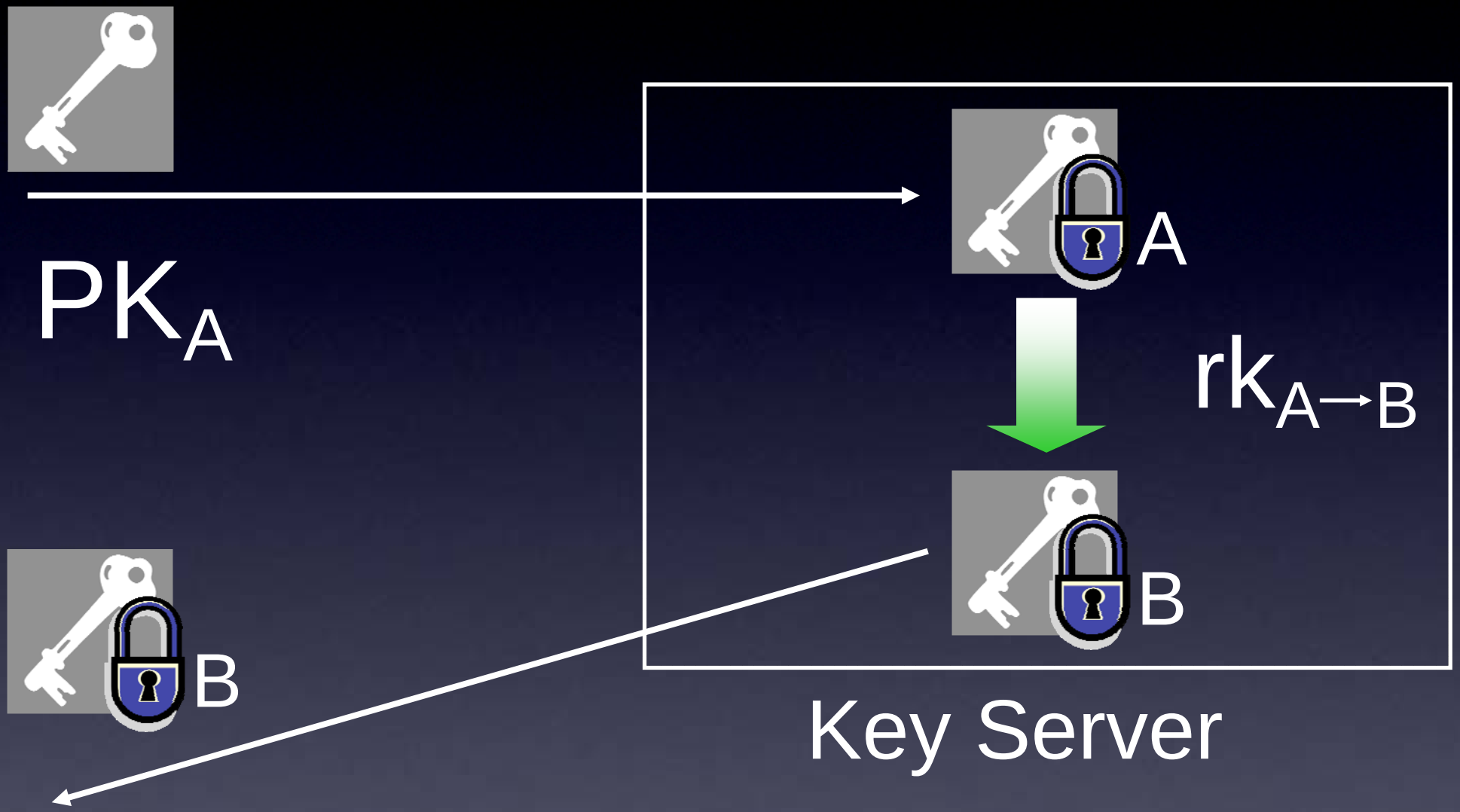


Client 1



Client 2

- Online server is vulnerable
- Content owner must trust Key Server
- Server operator has complete access to keys


PK_A
A
$rk_{A \rightarrow B}$
B
B
Key Server

Searchable Encryption

Searchable Encryption

- Symmetric and Asymmetric Crypto
- A trapdoor allows the Cloud provider to search on encrypted data
- The content is kept private
- Still inefficient...

Conclusions

- Cloud Cryptography: Great business opportunity
- Provable Data Possession is cool :)
- Provide access rights to encrypted content via PRE
- Searchable Encryption
- Much more...