Chasm: Fault-Tolerant, Information-Theoretic Secure Cloud Backup

Alex Grinman, Akshay Ravikumar, Julian Fuchs, Kevin Li

I’m sure there are plenty of existing “secure” back-up solutions…so why?

- **Existing cecure backup Solutions:**
  - Mozy, Carbonite, Crashplan, Backblaze
- **Bad usability, no fault-tolerance, and confidentiality:**
  - **Passwords** lost/leaked, easy to brute force
  - **Password-based keys** same low entropy problem, same lost password problem
  - **Local AES keys:** computer crashes? no recovery
  - **Long-lived ciphertexts under weak keys**
- **What is a good threat model?**

Threat model

Threat model

- **Adversaries:**
    1. Cloud storage service is curious, wants to gather information to sell
    2. Nation state compels cloud service to reveal user data by means of law
    3. Hackers break into a cloud service and steal user data

Threat model

- **Adversaries:**
    1. Cloud storage service is curious, wants to gather information to sell
    2. Nation state compels cloud service to reveal user data by means of law
    3. Hackers break into a cloud service and steal user data
- **Threats:**
    - Cloud services are computationally powerful!
    - Can brute force passwords or password-derived encryption keys
    - Denial-of-service by removing access to encrypted/ plaintext data

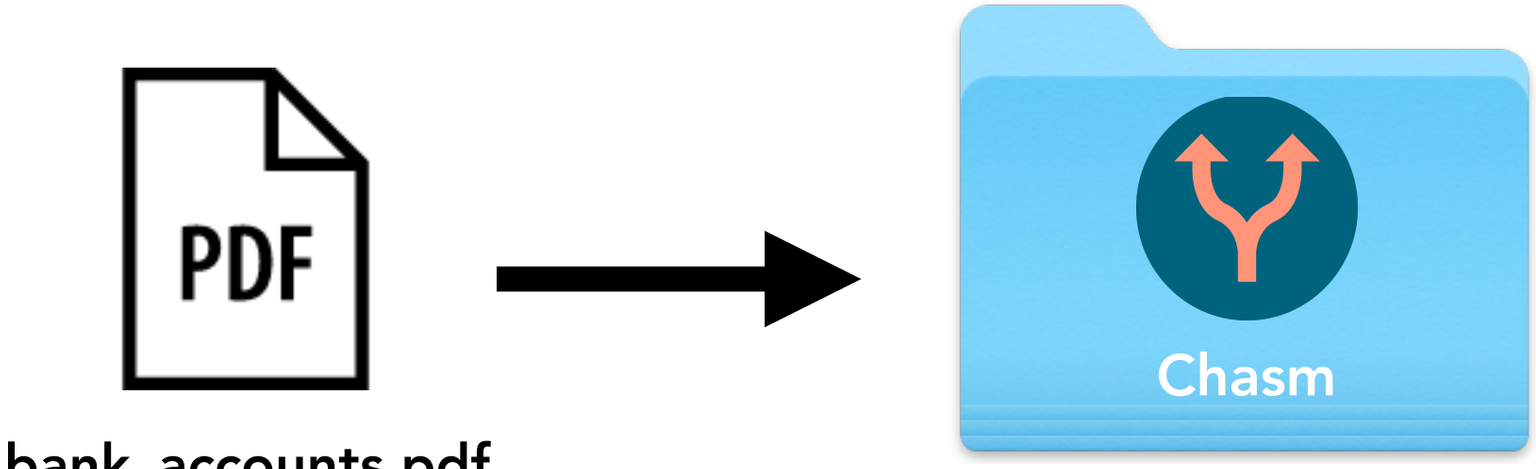
How does Chasm work?

1. **You** specify **≥ 2** cloud stores like:
    - Dropbox
    - Google Drive
    - iCloud Drive
    - Microsoft One Drive
    - AWS
2. **Chasm** creates a “secure” **chasm folder** in your home directory
3. **You** can now simply drag & drop files into the folder

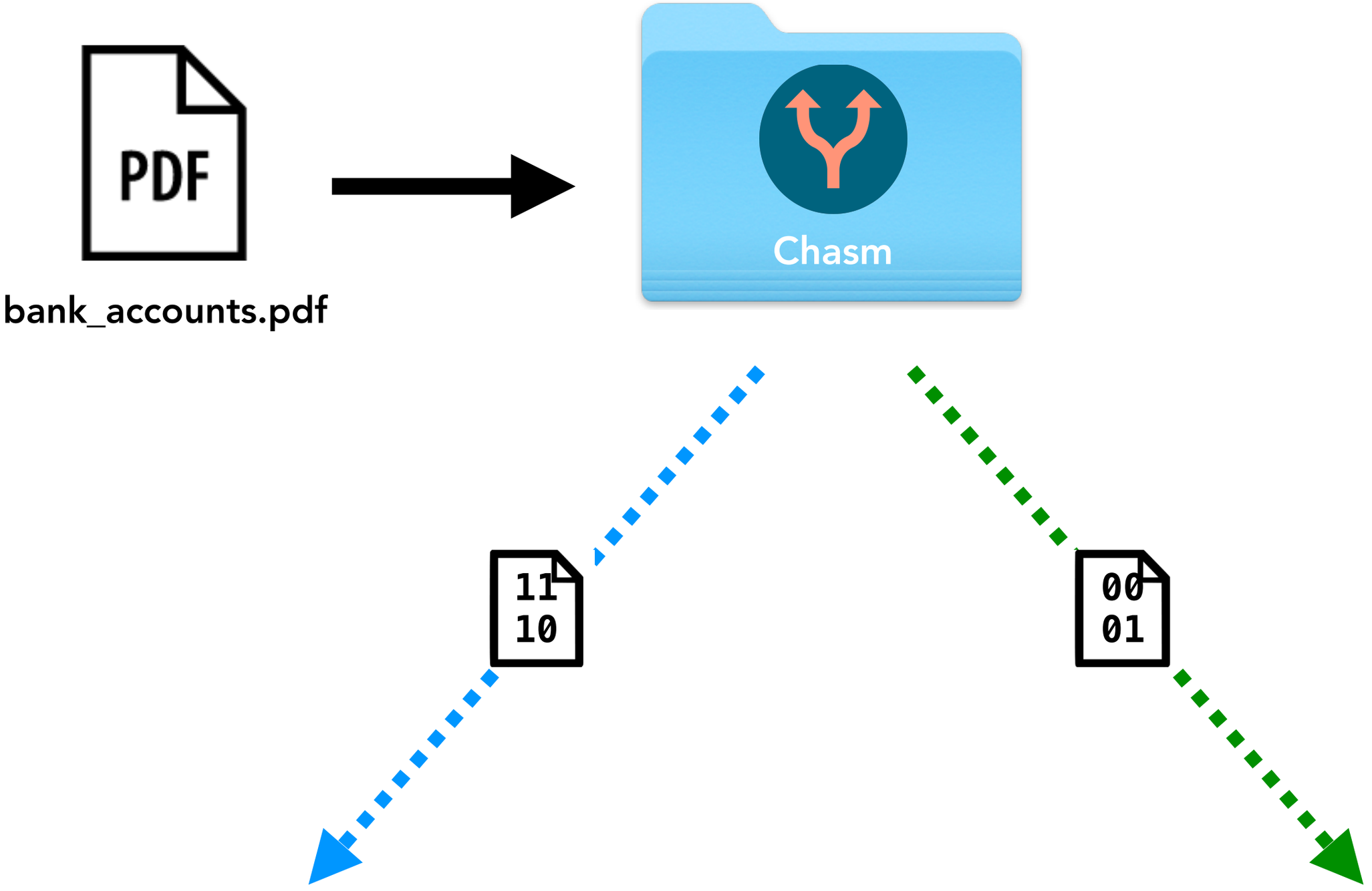
How does Chasm work?

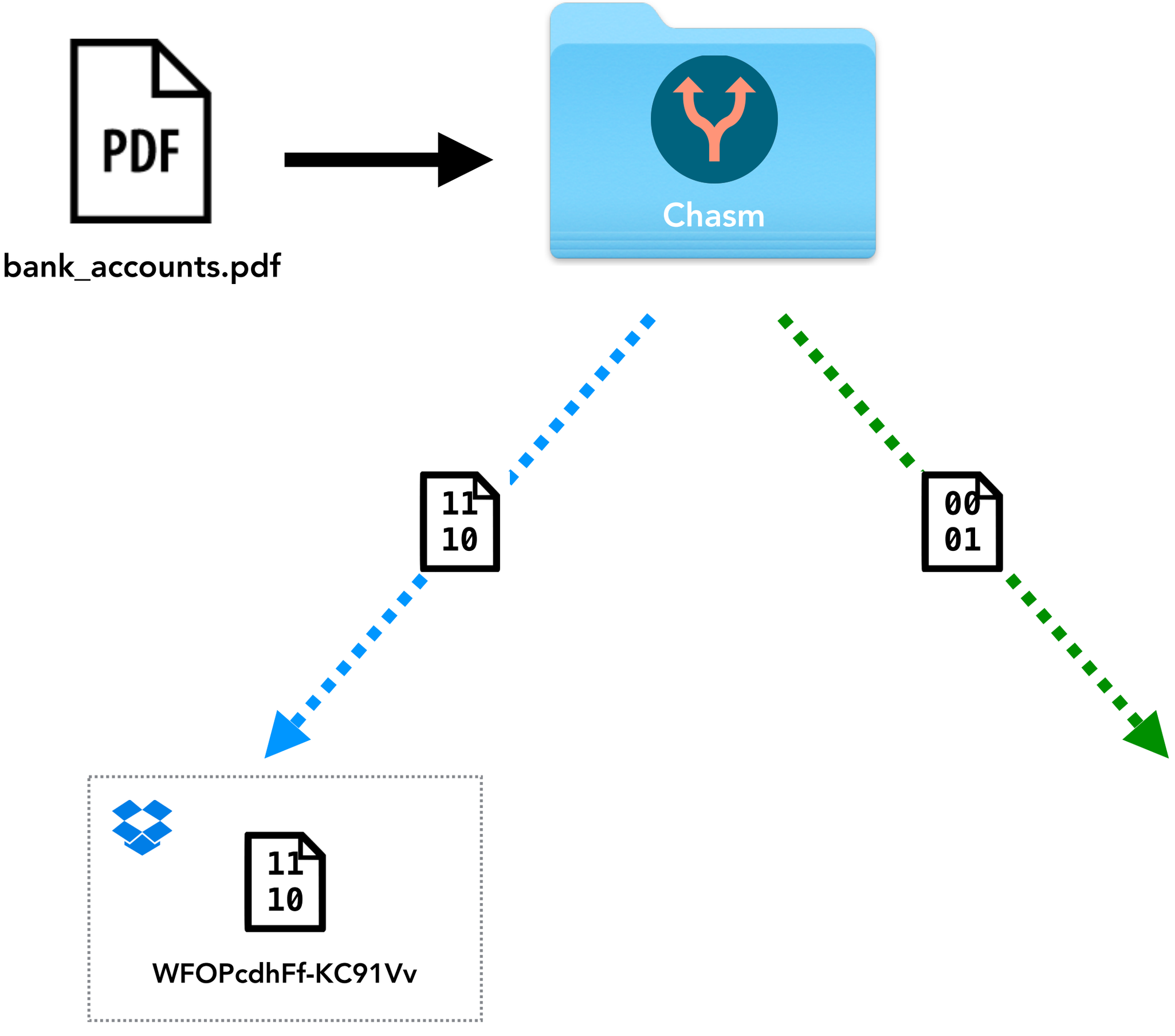
- Chasm listens for file-system events on the **chasm folder**
- When a new file is added to the **chasm folder**, the file is secret shared using the **K-out-of-N** Shamir's **Secret Sharing Scheme**
- Each share is sent to a different cloud store
- **N** = # of cloud stores
- **K** = recoverability threshold (by default **N**)

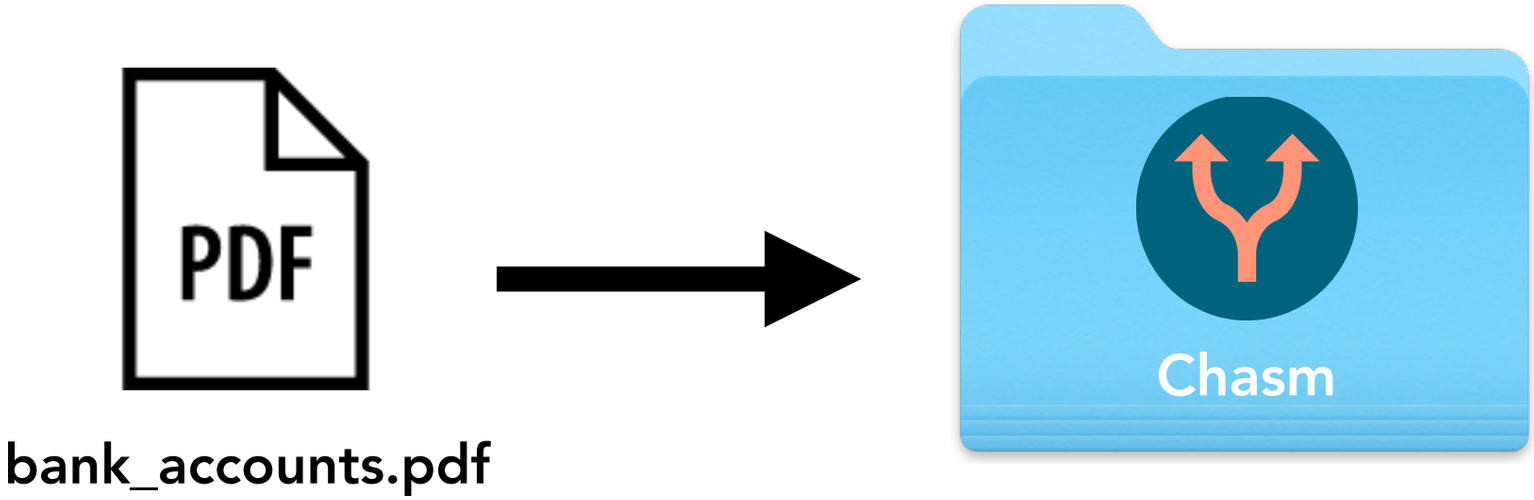
bank_accounts.pdf

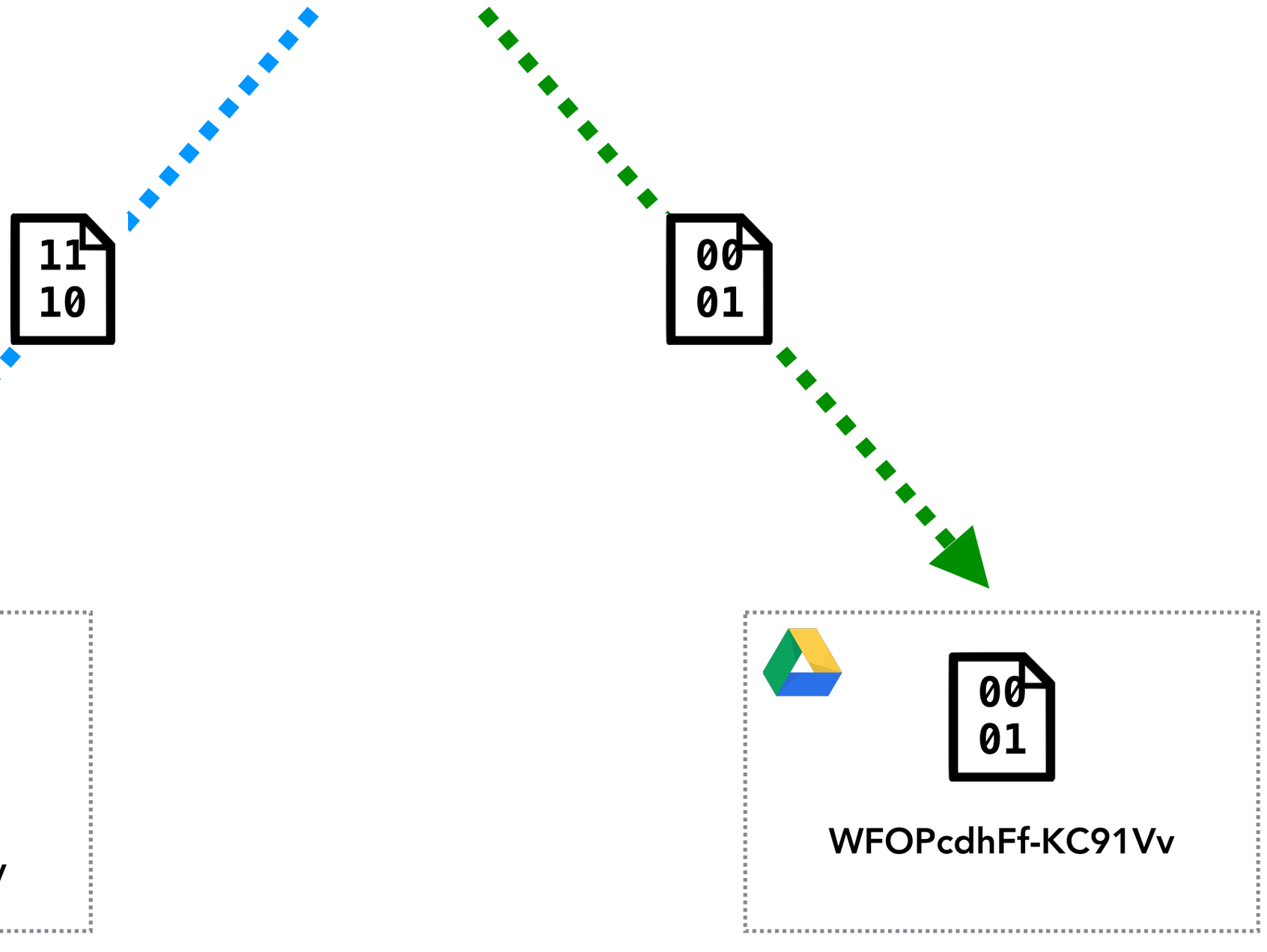


bank_accounts.pdf


PDF
bank_accounts.pdf
Chasm
11
10
00
01


PDF
bank_accounts.pdf
Chasm
11
10
00
01
11
10
WFOPcdhFf-KC91Vv


PDF
bank_accounts.pdf
Chasm


11
10
00
01
11
10
WFOPcdhFf-KC91Vv
00
01
WFOPcdhFf-KC91Vv

DEMO TIME!

System Guarantees

- **Information-Theoretic Confidentially** of data if less than K-out-of-N cloud services collude

- **Fault-tolerance** lost data is recoverable if at least K-out-of-N cloud services available

- **Integrity** of data if at least K-out-of-N cloud services are honest (achieved by taking majority)

Win on usability

- No passwords to remember
- Easy setup & restore
- Drag & drop to secure
- Most user’s already have existing cloud services like Dropbox, Drive, iCloud, etc…

Vulnerabilities
(& how we can fix some of them)

- Cloud stores can determine the number of files and the size of each file

- A network adversary can potentially combine outbound shares as they are being sent

- I use the same password for everything?

Vulnerabilities
(& how we can fix some of them)

- Cloud stores can determine the number of files and the size of each file
  - **Use fixed size blocks!**
- A network adversary can potentially combine outbound shares as they are being sent

- I use the same password for everything?

Vulnerabilities
(& how we can fix some of them)

- Cloud stores can determine the number of files and the size of each file
  - **Use fixed size blocks!**
- A network adversary can potentially combine outbound shares as they are being sent
  - **Most cloud stores operate over TLS**
- I use the same password for everything?

Vulnerabilities
(& how we can fix some of them)

- Cloud stores can determine the number of files and the size of each file
  - **Use fixed size blocks!**
- A network adversary can potentially combine outbound shares as they are being sent
  - **Most cloud stores operate over TLS**
- I use the same password for everything?
  - **Turn on 2FA.**

Related Systems

- **"Simulating cloud environment for HIS backup using secret sharing."** (Kyoto University Hospital)
  - Hospitals can secret share data to backup to different remote sites
- **"Responsive Security for Stored Data."** (Georgia Institute of Technology)
  - A secure system that improves on replicated state machines with secret sharing schemes
- **No consumer cloud backup services using secret sharing**

Questions?