Secure Cloud Storage
&
Best Senior Project Story

ALPTEKİN KÜPÇÜ

Associate Professor of Computer Science and Engineering

Ph.D. Brown University

KOÇ
UNIVERSITY

Alptekin Küpçü

- B.S., Bilkent University, 2000-2004
- Ph.D., Brown University, 2004-2010
- Faculty, Koç Üniversitesi, 2010-
  - 3 post-doctoral researcher alumni
  - 4 phd & 4 ms student alumni
    - EPFL Switzerland, KU Leuven Belgium, University of Virginia USA, LinkedIn USA, NTU Singapore, Dapper Labs Canada
  - Hiring for blockchain project (2 phd, 2 ms, 1 post-doctoral)
- Visiting Scholar
  - METU , 2020
  - Bilkent University, TOBB ETU, IZTECH, 2019
  - Microsoft Research, 2013 & 2015
  - Yahoo! Labs, 2015

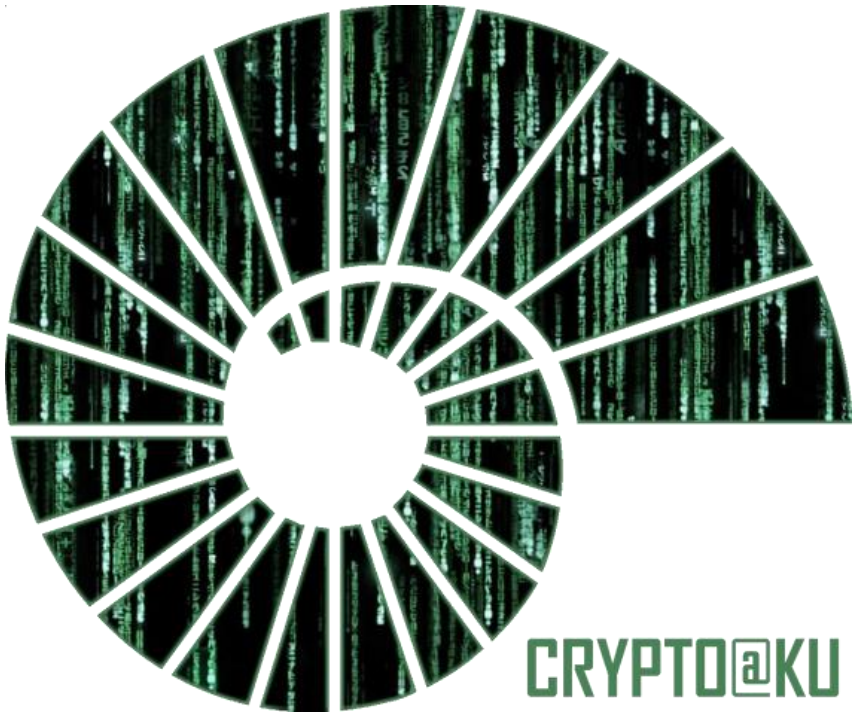
Collaborations & Awards

- UCL, UK
- Maryland University, Virginia University, Brown University, Northeastern University, Rutgers University, USA
- EPFL, Switzerland
- Salzburg University, Austria
- KU Leuven, Belgium
- Bilkent University, Ege University, Turkey
- Microsoft Research, Yahoo! Labs, IBM Research, USA
- TEB, IDEA, Koç Sistem, Türk Telekom, Turkey

- Science Academy, BAGEP outstanding young scholar
- Turkish Academy of Sciences, GEBİP outstanding young scholar
- ODTÜ Parlar Foundation, Research Encouragement Award
- Royal Society of UK, Newton Advanced Fellowship
- IEEE Senior Member
- ACM Senior Member
- 4 teaching awards from Koç University
- 6 international patents

Cryptography, Security, and Privacy Research Group

- **Core Research**
  - Cryptography
  - Security
  - Privacy
- **Application Areas**
  - Cloud Computing
  - Passwords and Authentication
  - Smart Homes and IoT
  - Peer-to-peer Systems
  - Blockchain Applications
  - E-ID and E-Health Systems
  - Game Theory and Mechanism Design
  - Provable Security
  - ...



Goal

Cryptographic protocols can efficiently and scalably be used to provide security and privacy for the next generation systems.

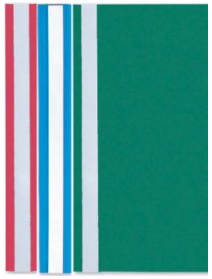
Overview

- **Secure Cloud Storage**
  - **Problems**
  - **Solutions**
  - **Summary**

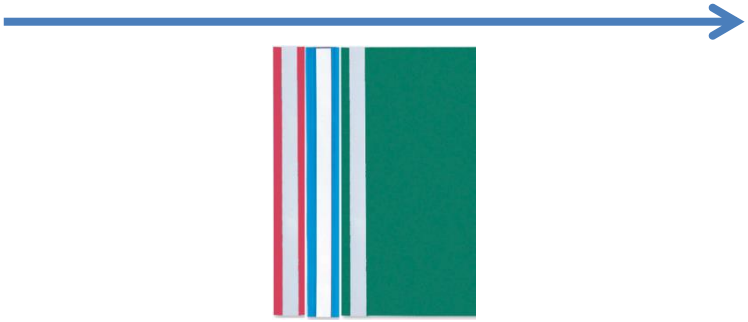
Overview

- Secure Cloud Storage
  - Problems
  - Solutions
  - Summary

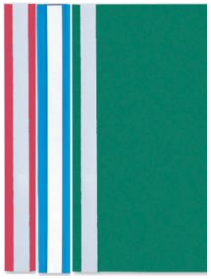
Outsourced Storage



Outsourced Storage



Outsourced Storage



Untrusted Storage

INTEGRITY

Untrusted Storage

INTEGRITY

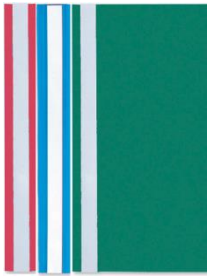
Untrusted Storage

CONFIDENTIALITY

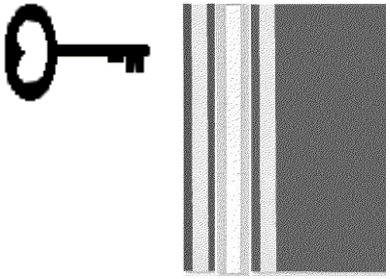
Overview

- **Secure Cloud Storage**
  - **Problems**
  - **Solutions**
  - **Summary**

Confidentiality

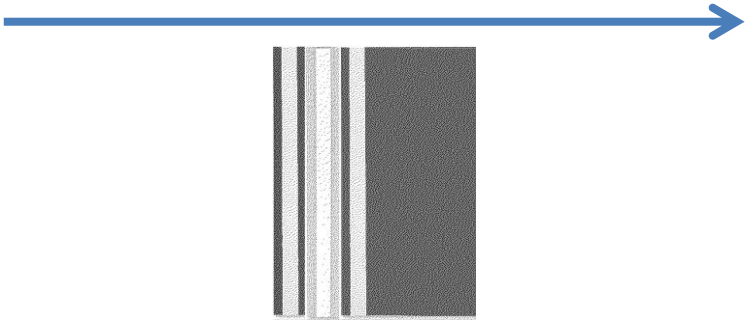


Confidentiality



ENCRYPT

Confidentiality



Confidentiality

Integrity: Naïve Solution 1

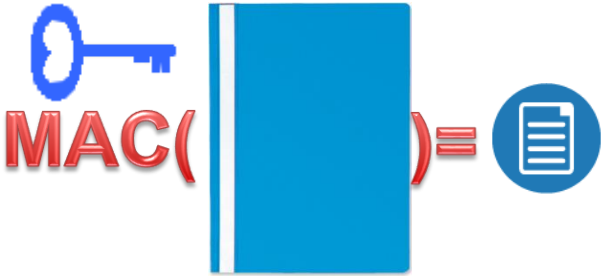
Integrity: Naïve Solution 1

Integrity: Naïve Solution 1

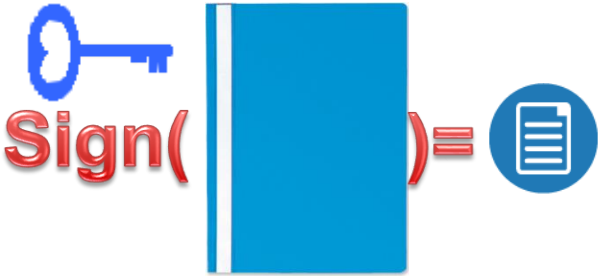
Integrity: Naïve Solution 1

Integrity: Naïve Solution 1

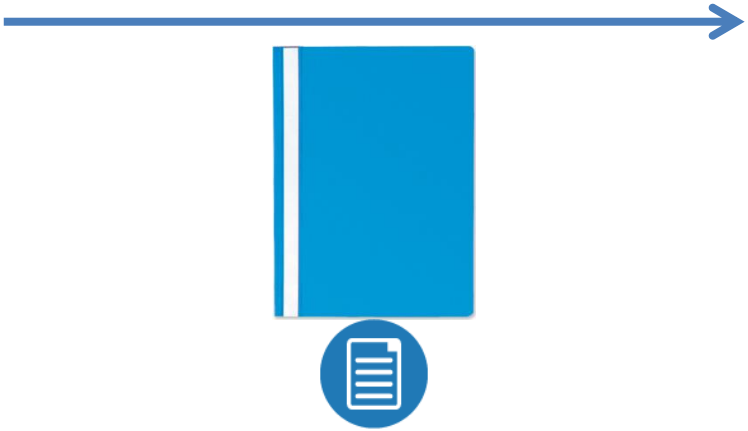
Integrity: Naïve Solution 2



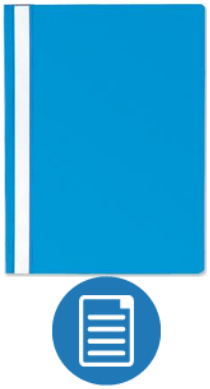
Integrity: Naïve Solution 2



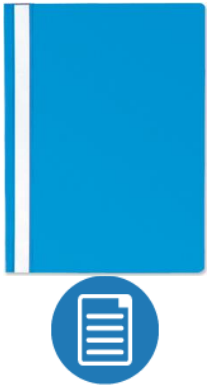
Integrity: Naïve Solution 2

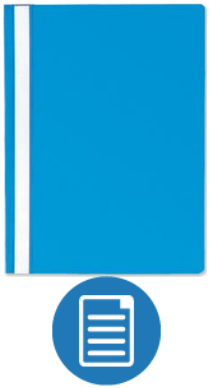


Integrity: Naïve Solution 2

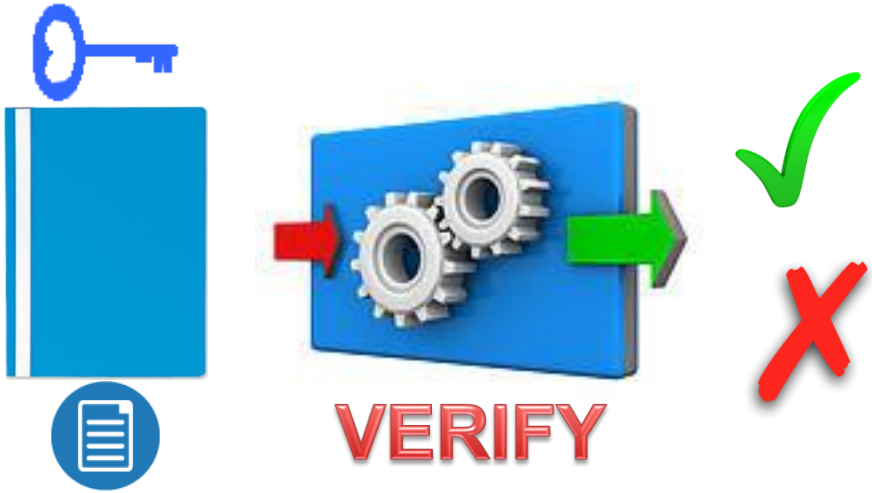


Integrity: Naïve Solution 2

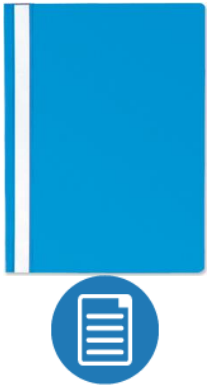


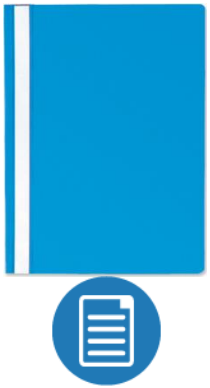


Integrity: Naïve Solution 2

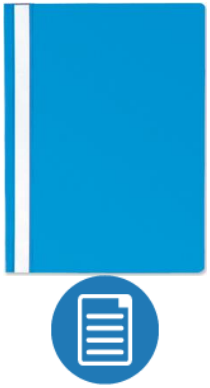


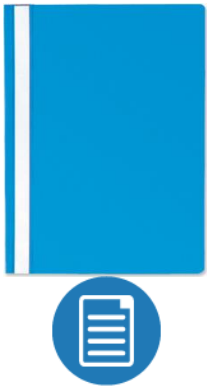
Problem with Naïve Approaches



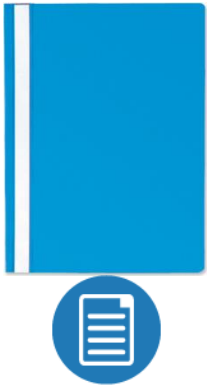


Problem with Naïve Approaches





Problem with Naïve Approaches



Overview

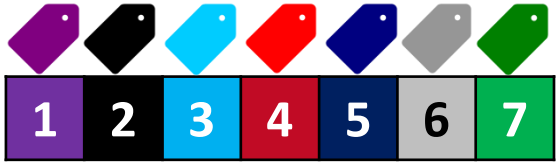
- **Secure Cloud Storage**
  - **Problems**
  - **Efficient Solutions**
  - **Summary**

Provable Data Possession

[ABCHKPS ACM CCS 2007]

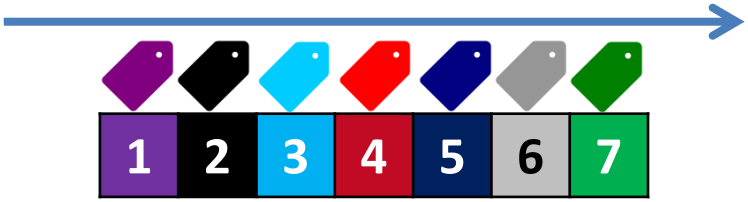
Provable Data Possession

[ABCHKPS ACM CCS 2007]



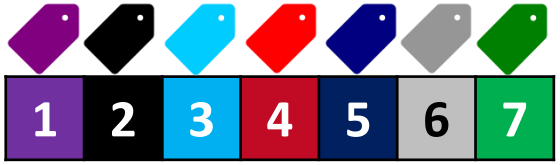
Provable Data Possession

[ABCHKPS ACM CCS 2007]



Provable Data Possession

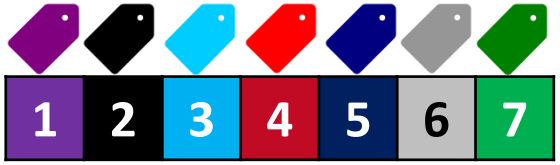
[ABCHKPS ACM CCS 2007]



Provable Data Possession

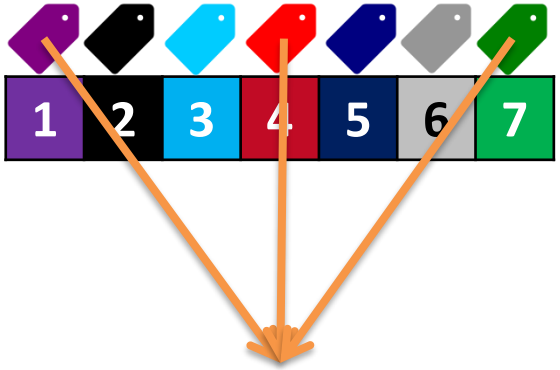
[ABCHKPS ACM CCS 2007]

CHALLENGE: 1 4 7



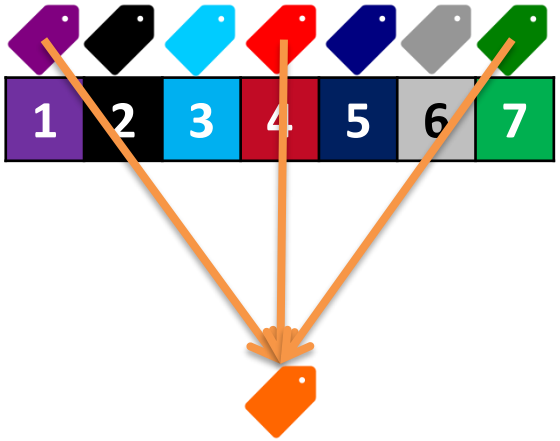
Provable Data Possession

[ABCHKPS ACM CCS 2007]



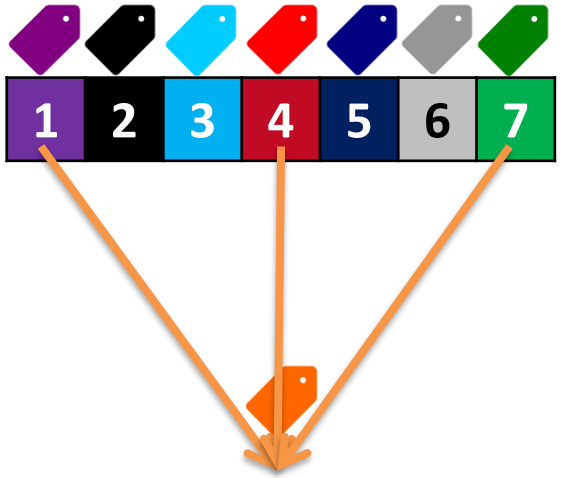
Provable Data Possession

[ABCHKPS ACM CCS 2007]



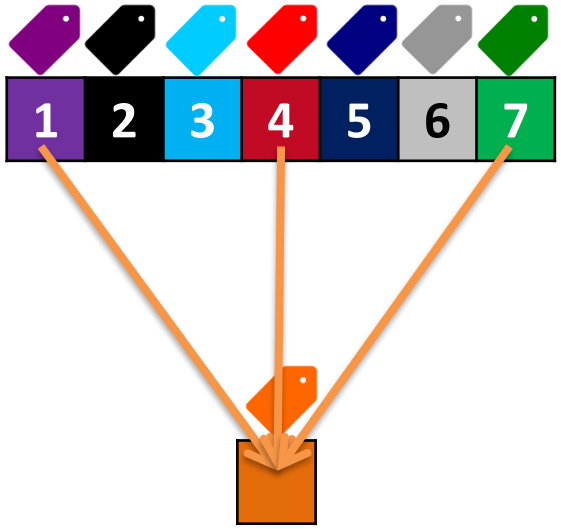
Provable Data Possession

[ABCHKPS ACM CCS 2007]



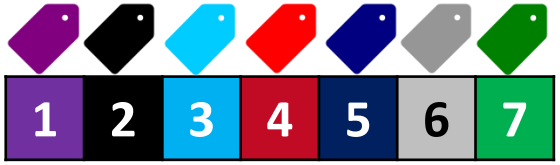
Provable Data Possession

[ABCHKPS ACM CCS 2007]



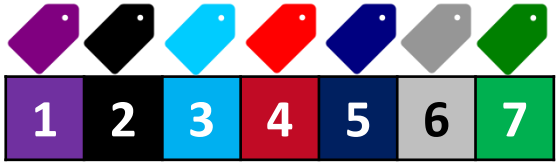
Provable Data Possession

[ABCHKPS ACM CCS 2007]



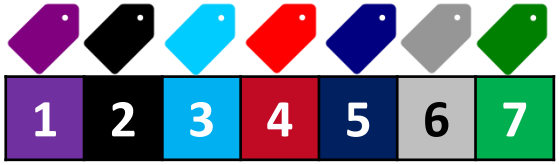
Provable Data Possession

[ABCHKPS ACM CCS 2007]



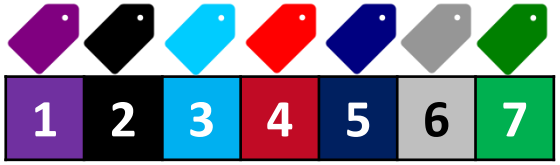
Provable Data Possession

[ABCHKPS ACM CCS 2007]

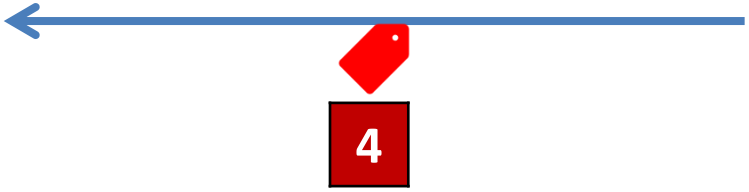


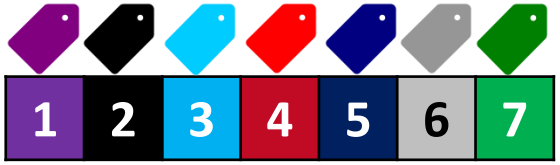
PDP is for Static Data

CHALLENGE: 4

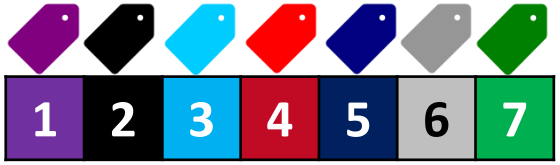


PDP is for Static Data

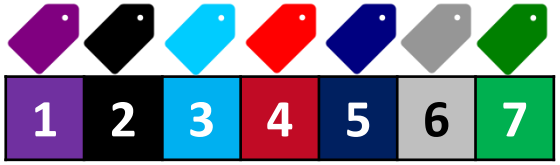




PDP is for Static Data

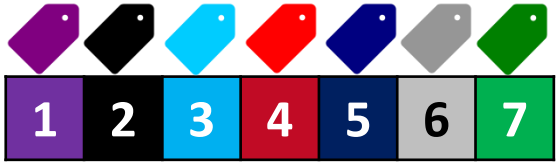


PDP is for Static Data



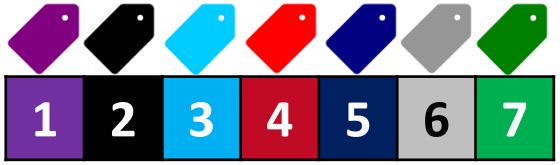
PDP is for Static Data

PDP is for Static Data

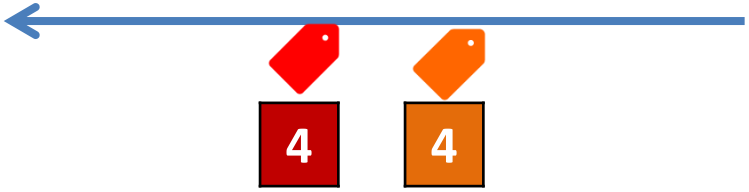


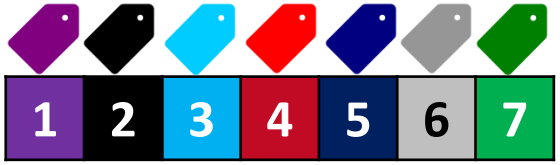
PDP is for Static Data

CHALLENGE: 4

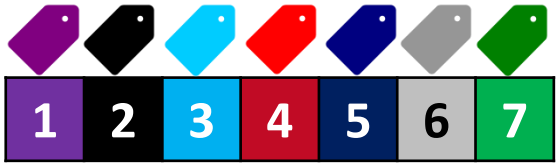


PDP is for Static Data





PDP is for Static Data



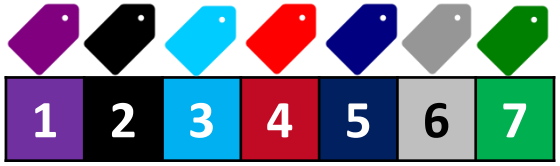
PDP is for Static Data

Overview

- **Secure Cloud Storage**
  - **Problems**
  - **Efficient Dynamic Solutions**
  - **Summary**

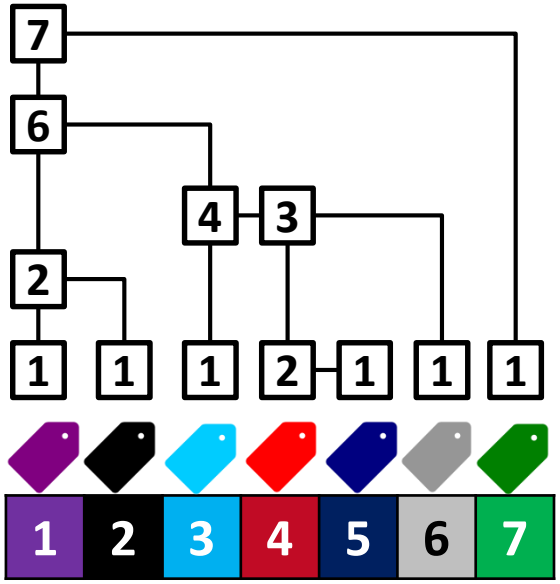
Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

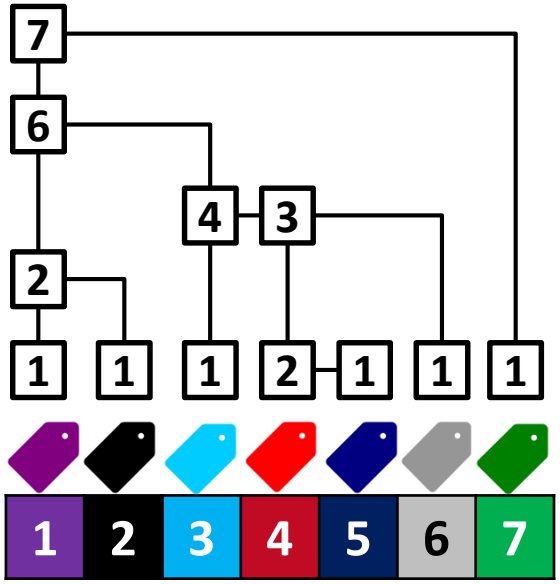


Rank-Based Authenticated Skip List

Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

Search for 5

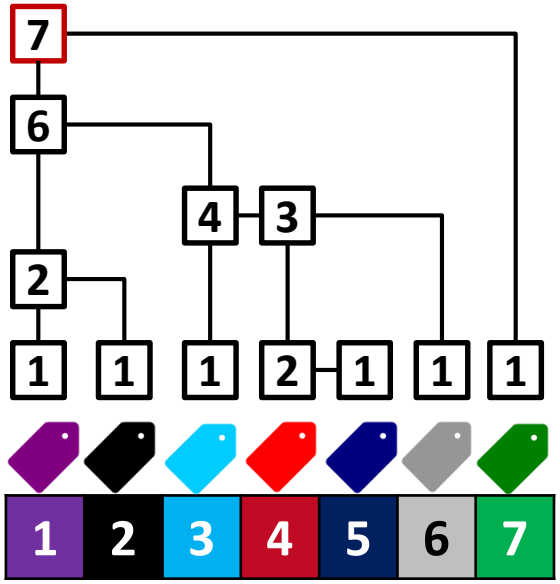


Rank-Based

Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

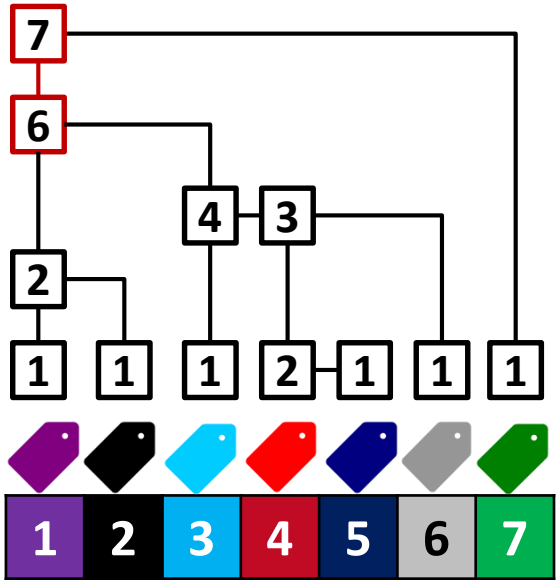
Search for 5



Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

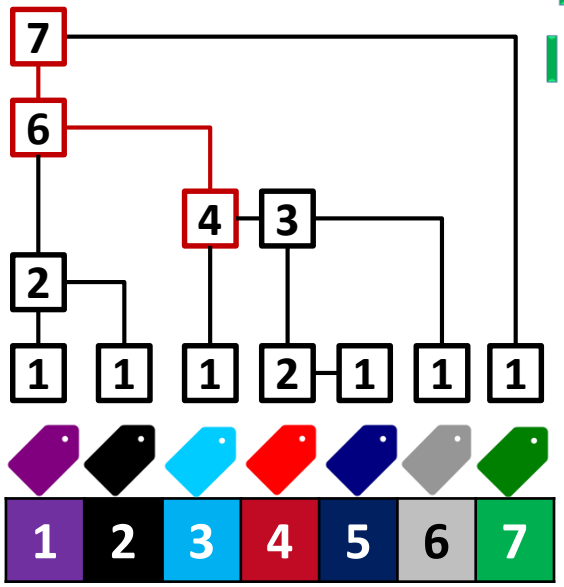
Search for 5



Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

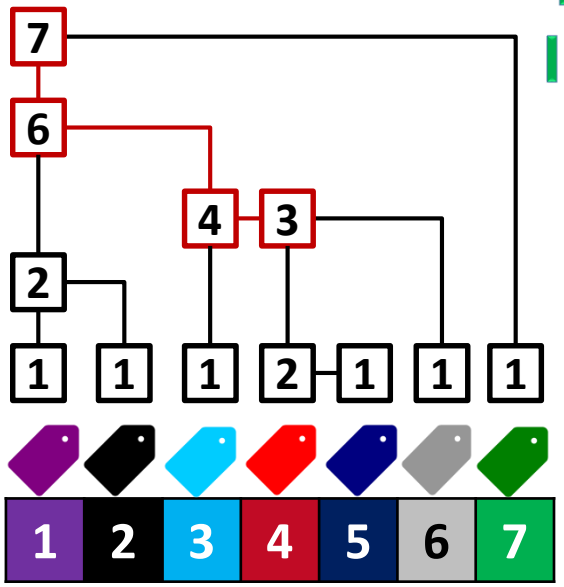
CONTINUE SEARCHING,
BUT SEARCH FOR 5-2=3
IN THE REMAINING PART



Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

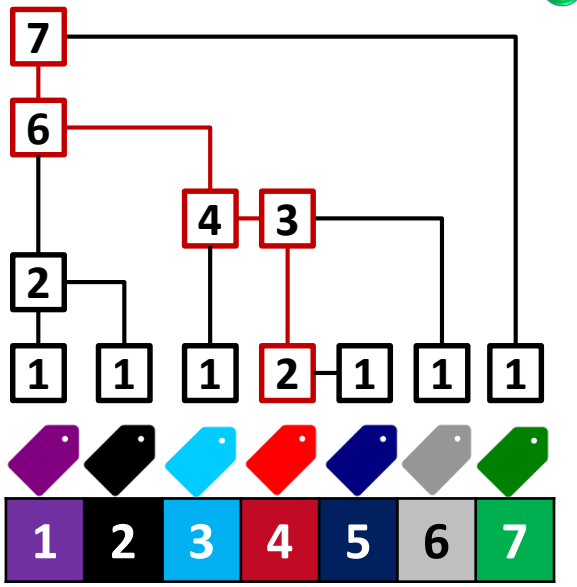
CONTINUE SEARCHING, BUT SEARCH FOR 3-1=2 IN THE REMAINING PART



Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

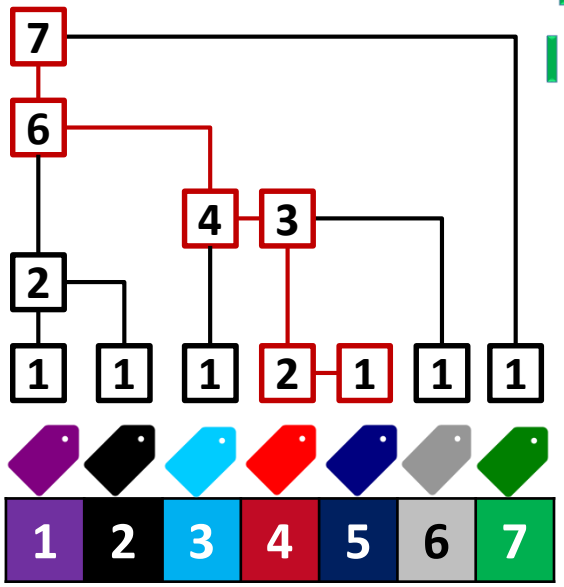
CONTINUE SEARCHING 2



Dynamic Provable Data Possession

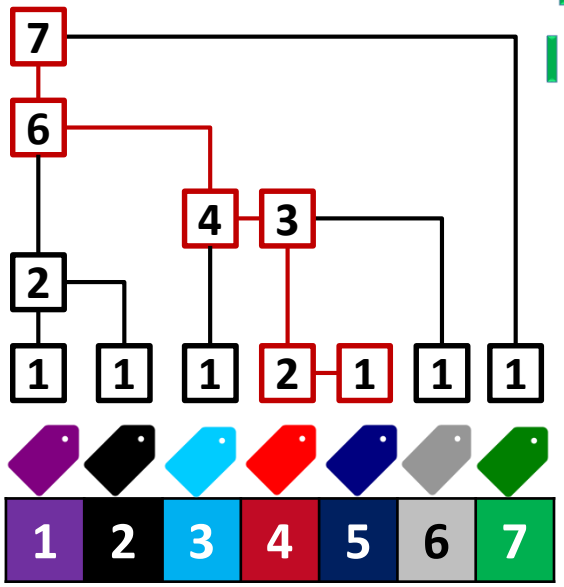
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

CONTINUE SEARCHING,
BUT SEARCH FOR 2-1=1
IN THE REMAINING PART



Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

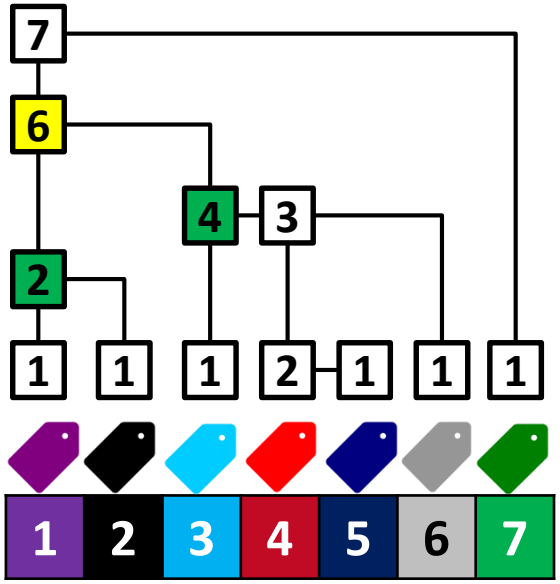


CONTINUE SEARCHING, BUT SEARCH FOR 2-1=1 IN THE REMAINING PART

SEARCH FOR 1 MEANS FOUND IT

Dynamic Provable Data Possession

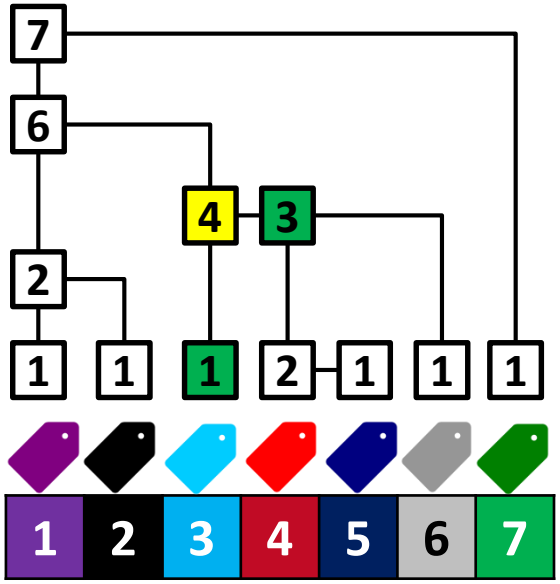
[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Authenticated

Dynamic Provable Data Possession

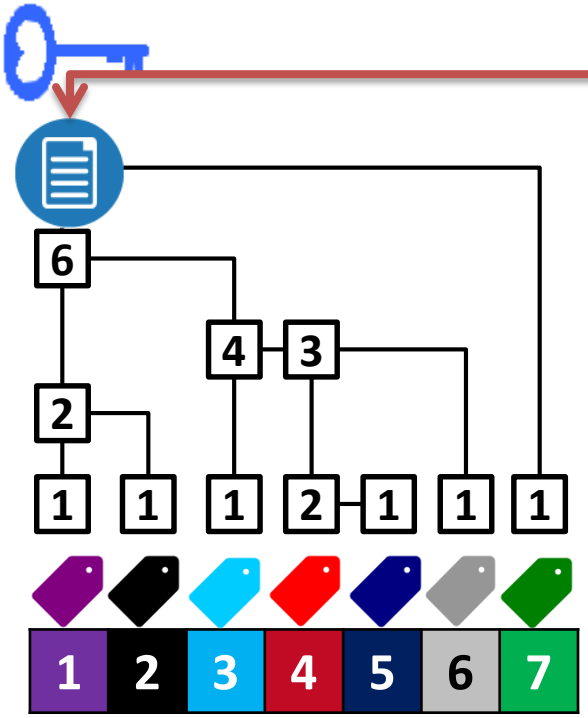
[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Authenticated

Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]

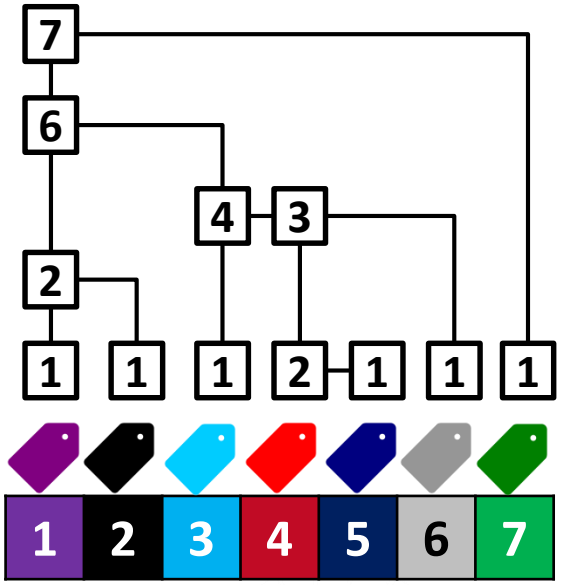


Digest (Metadata)

Rank-Based Authenticated Skip List

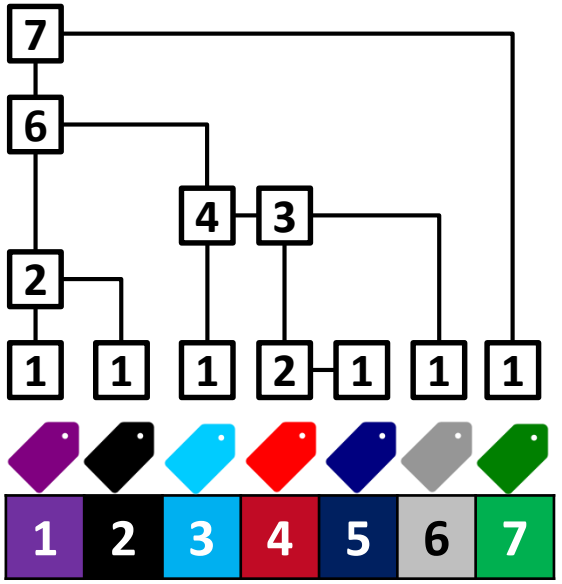
Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Dynamic Provable Data Possession

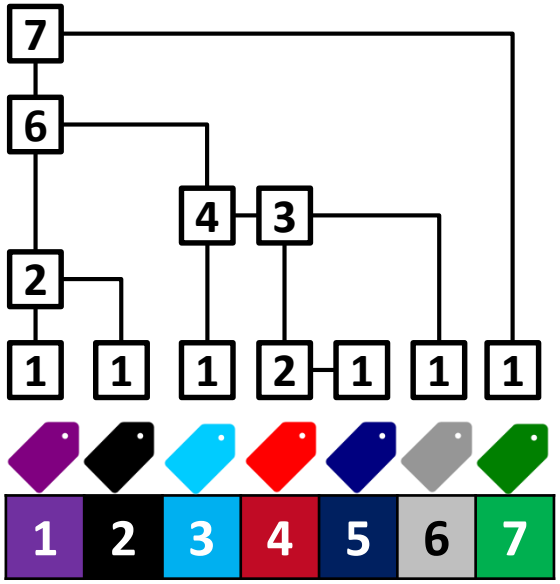
[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Dynamic Provable Data Possession

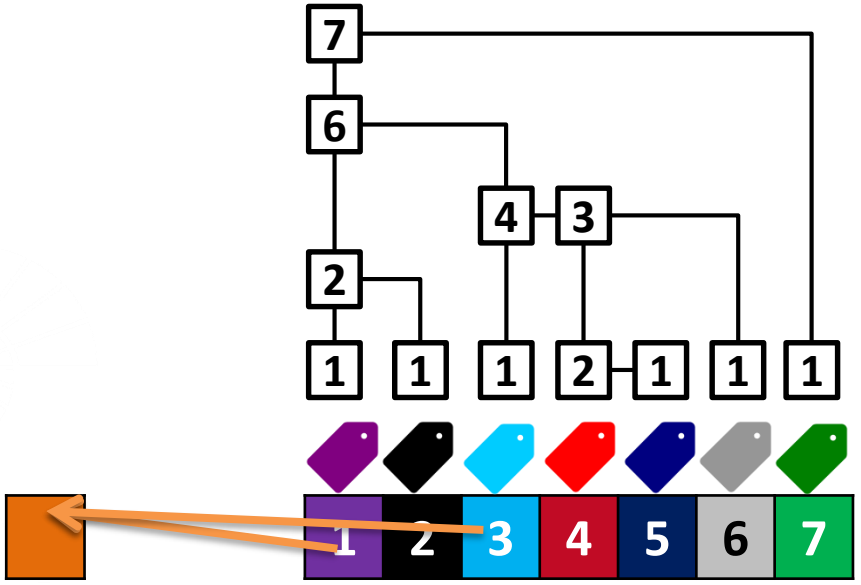
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

CHALLENGE: 1 3



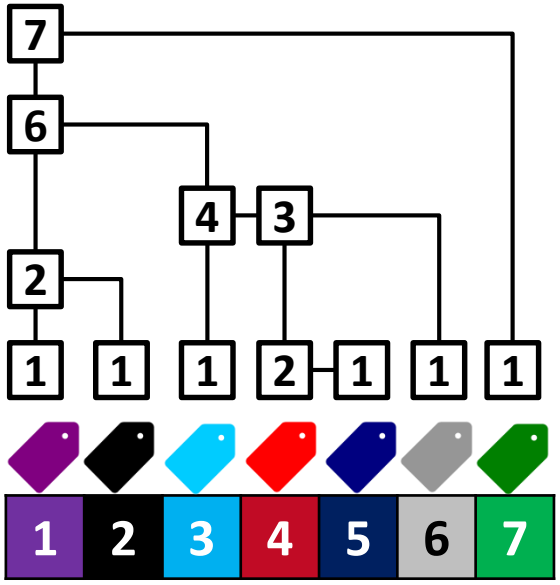
Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]



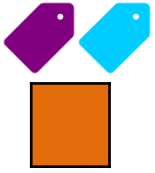
Dynamic Provable Data Possession

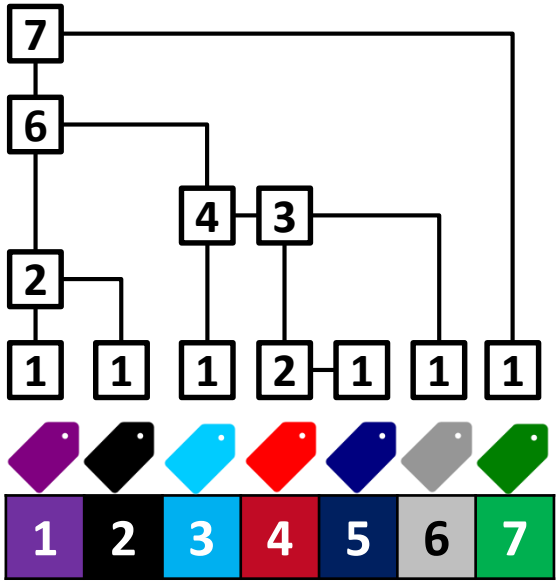
[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Dynamic Provable Data Possession

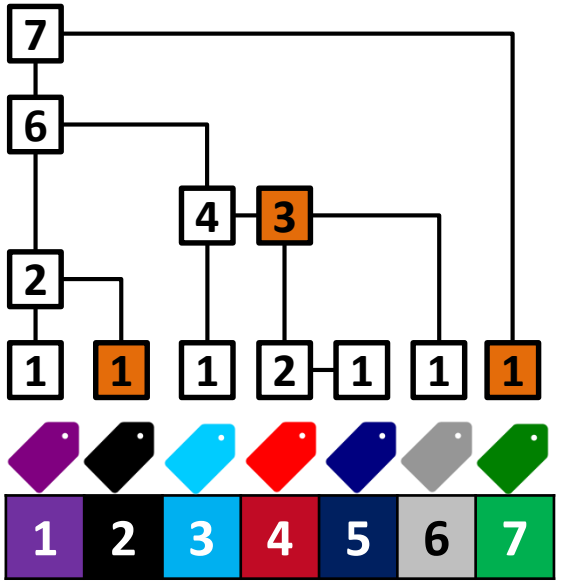
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

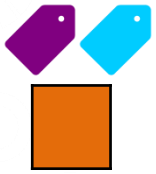




Dynamic Provable Data Possession

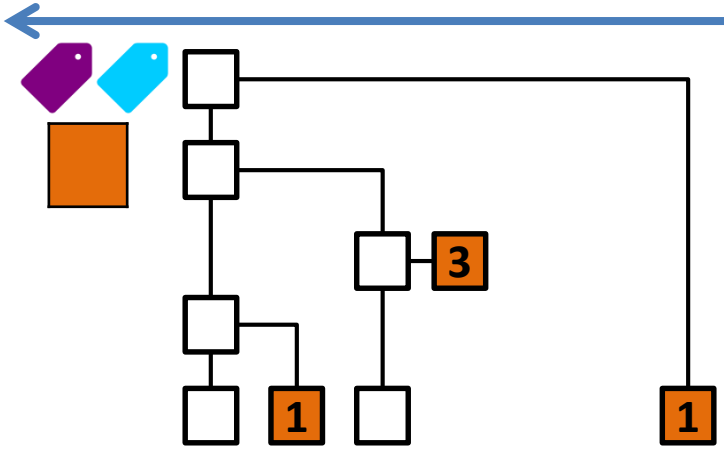
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

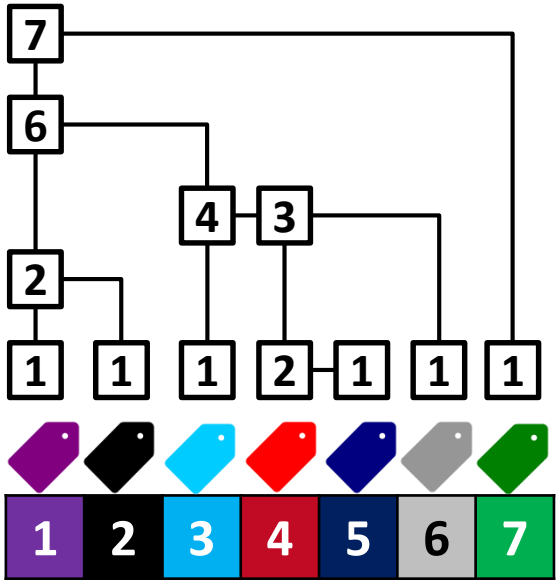




Dynamic Provable Data Possession

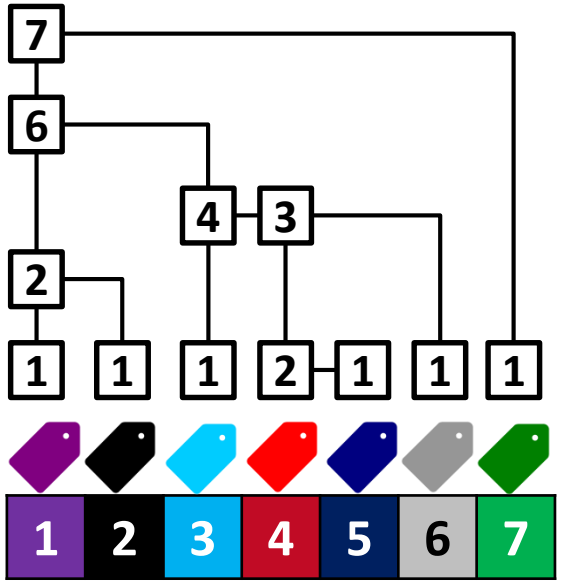
[EKPT ACM CCS 2009 & ACM TISSEC 2015]





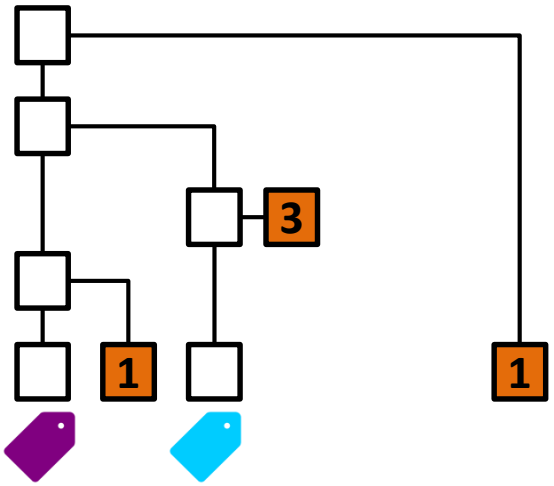
Dynamic Provable Data Possession

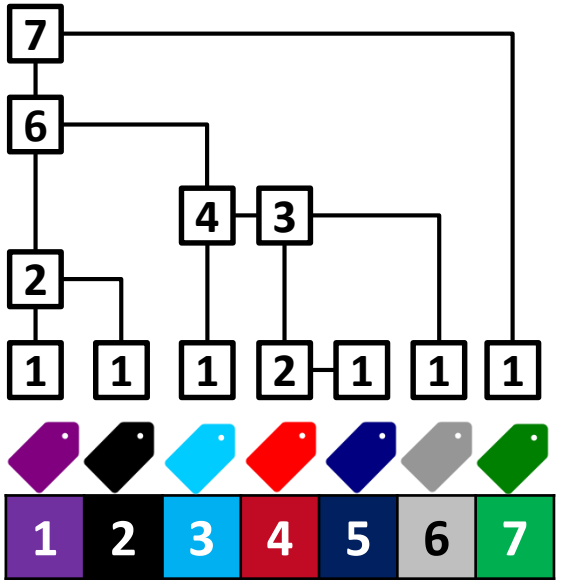
[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Dynamic Provable Data Possession

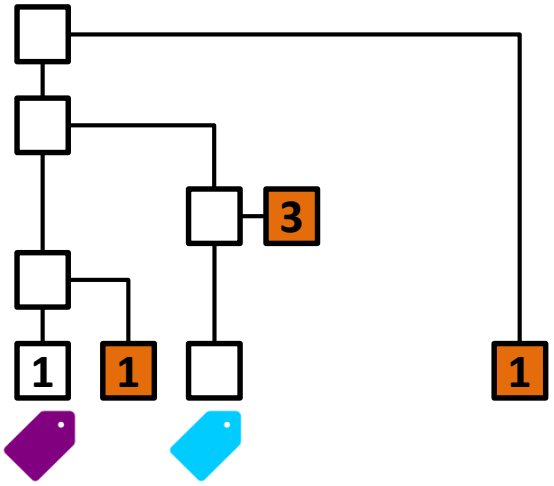
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

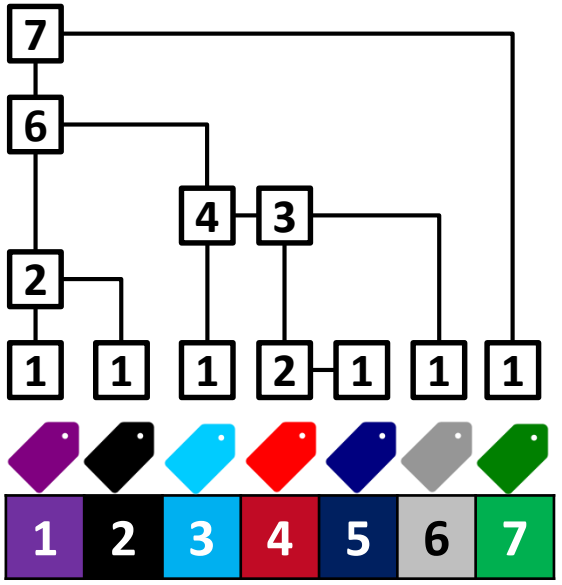




Dynamic Provable Data Possession

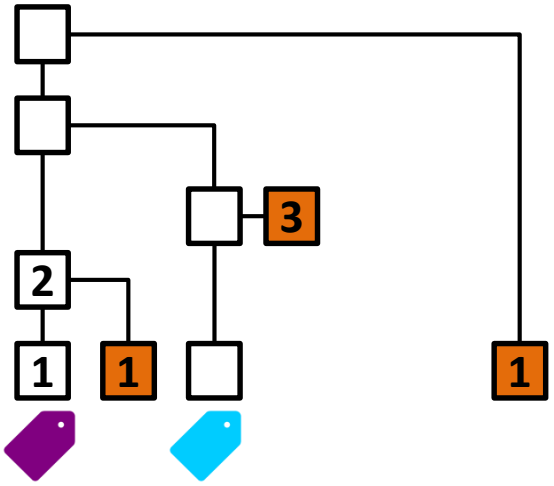
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

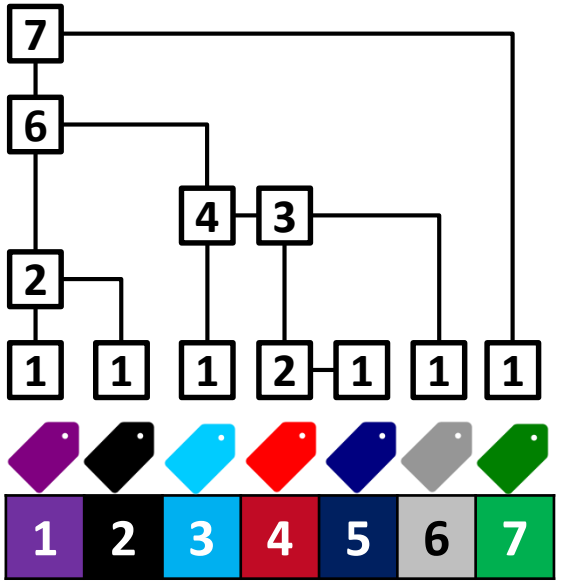




Dynamic Provable Data Possession

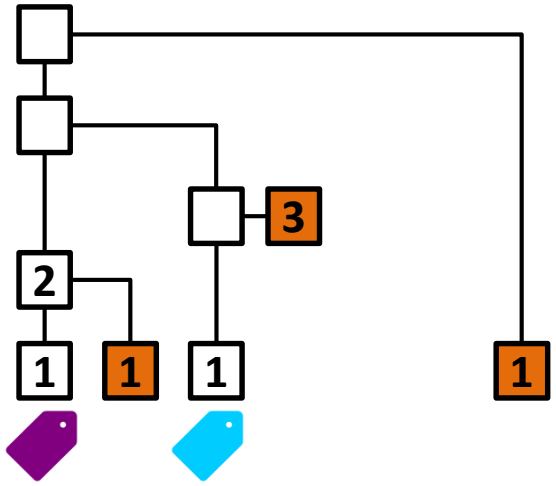
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

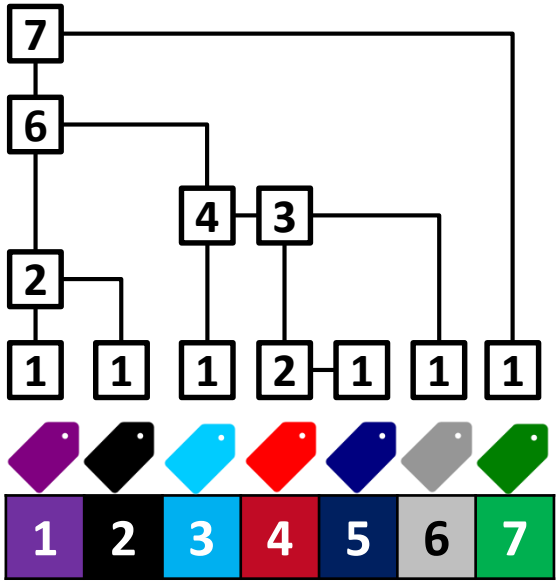




Dynamic Provable Data Possession

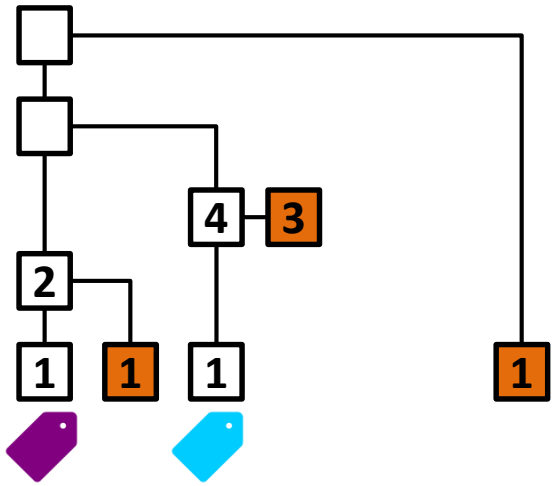
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

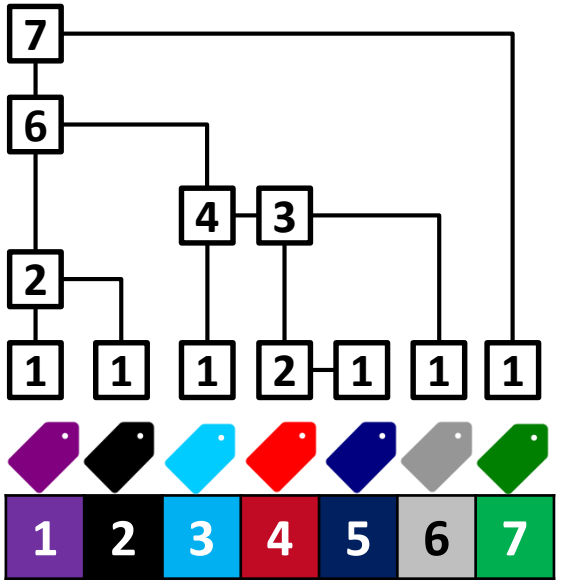




Dynamic Provable Data Possession

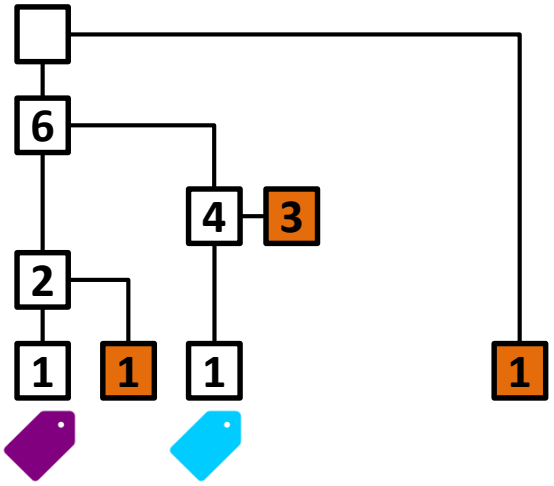
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

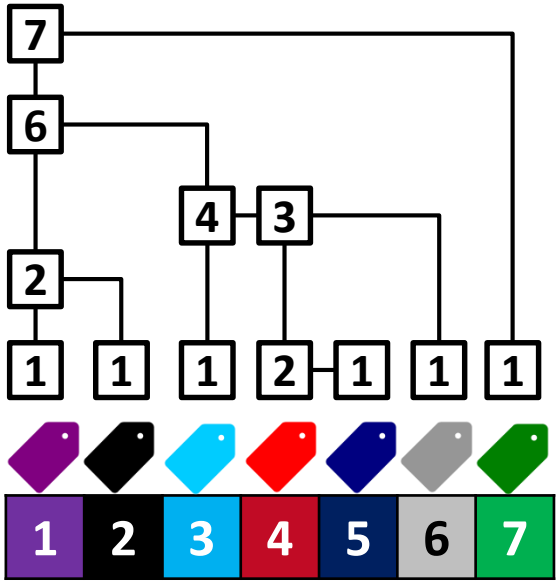




Dynamic Provable Data Possession

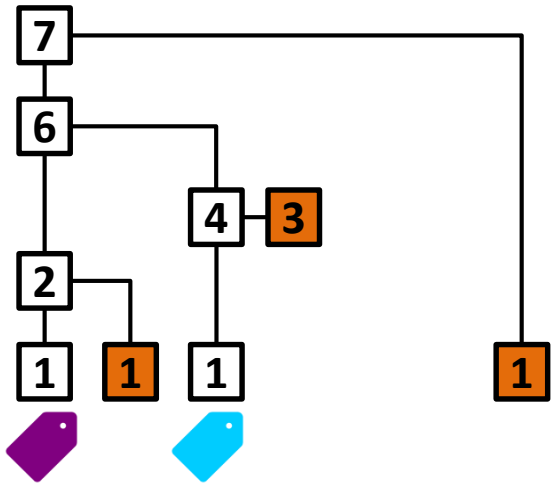
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

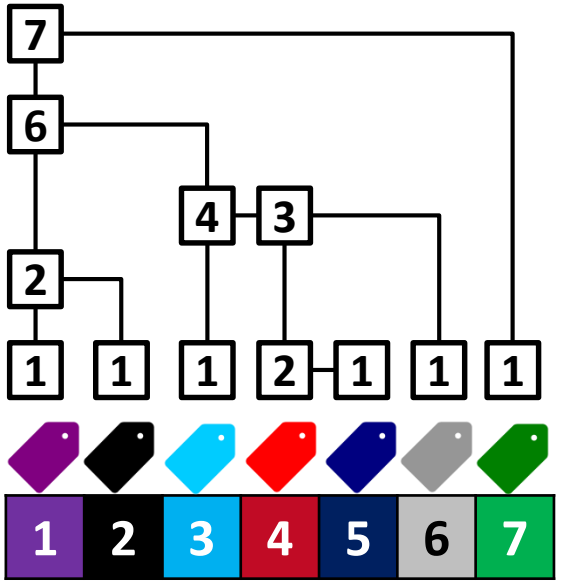




Dynamic Provable Data Possession

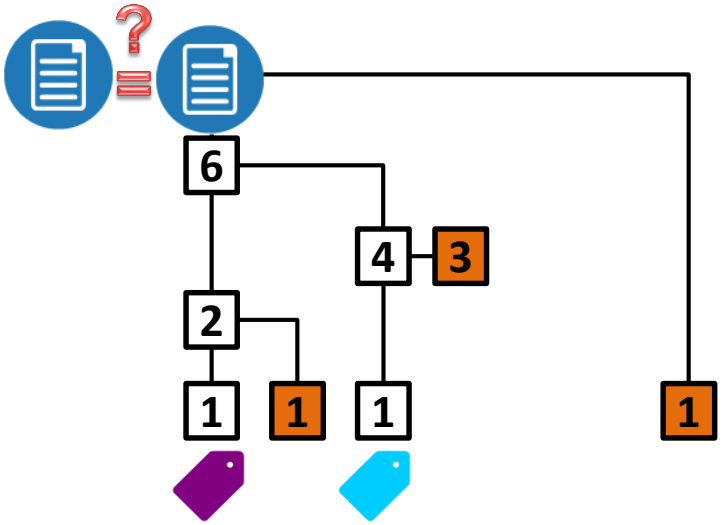
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

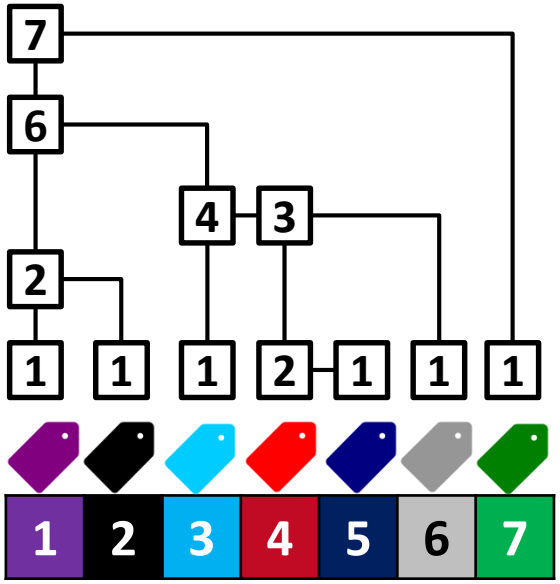




Dynamic Provable Data Possession

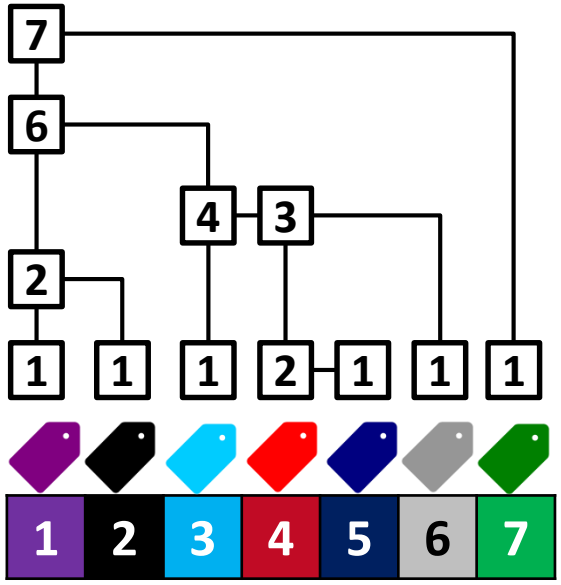
[EKPT ACM CCS 2009 & ACM TISSEC 2015]





Dynamic Provable Data Possession

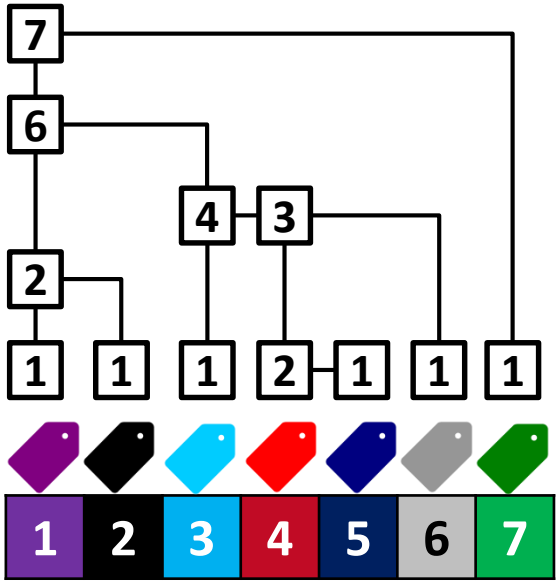
[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Dynamic Provable Data Possession

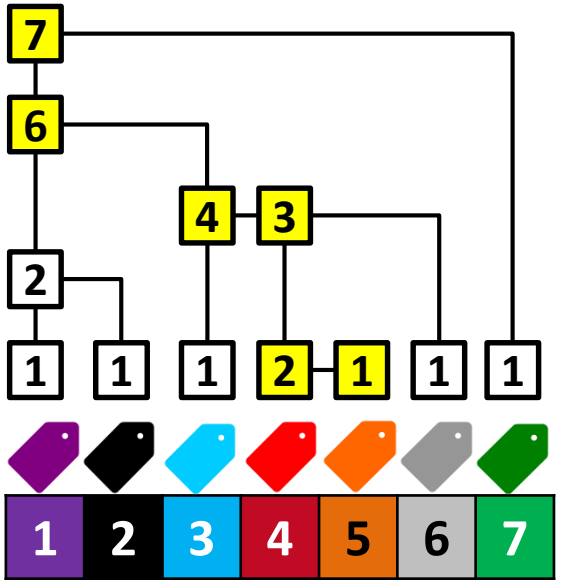
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

MODIFY



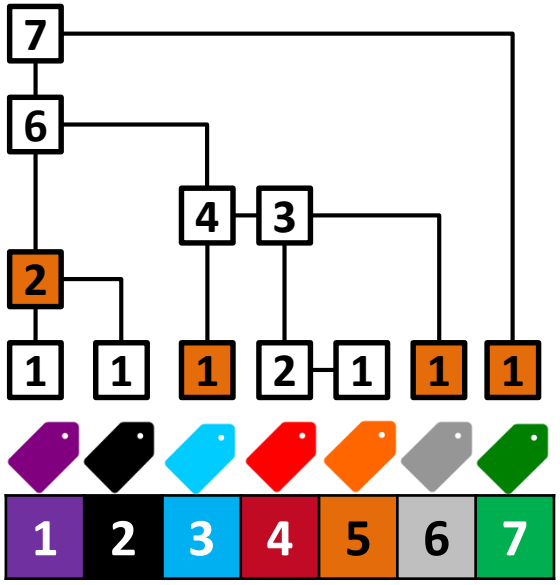
Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]



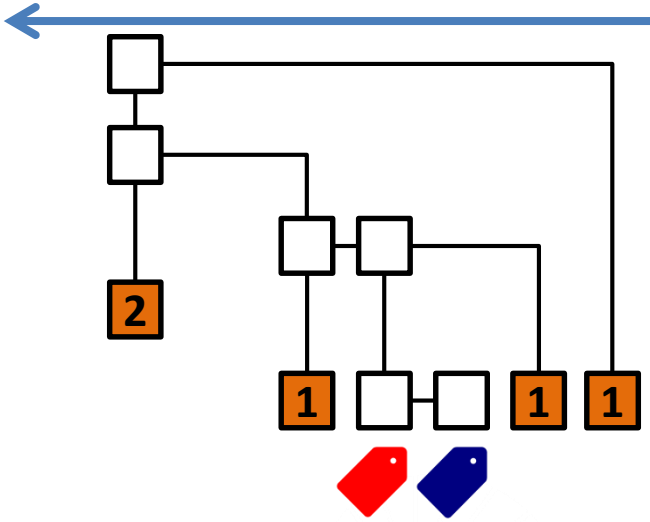
Dynamic Provable Data Possession

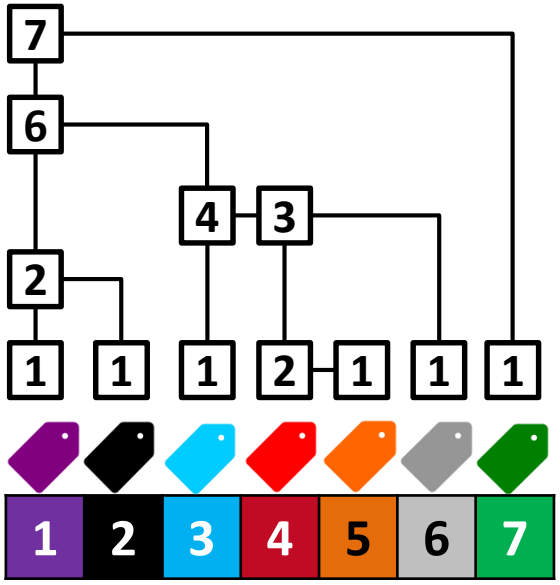
[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Dynamic Provable Data Possession

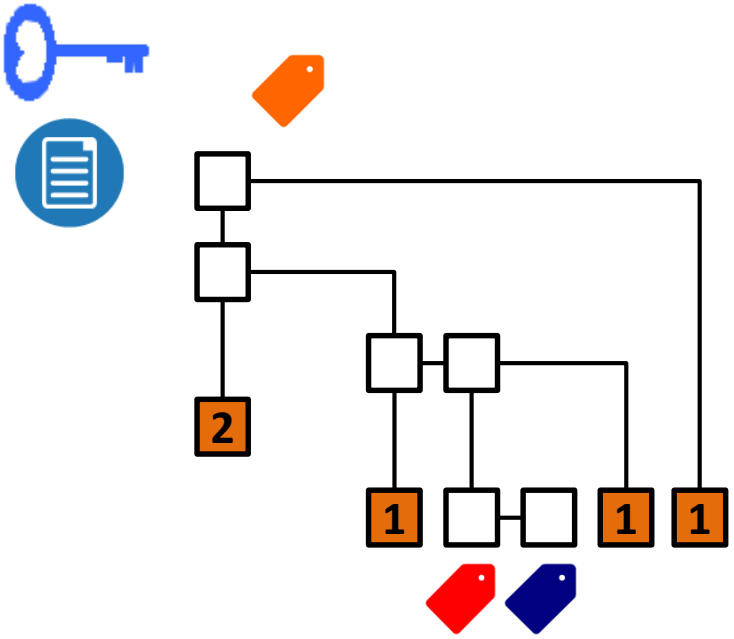
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

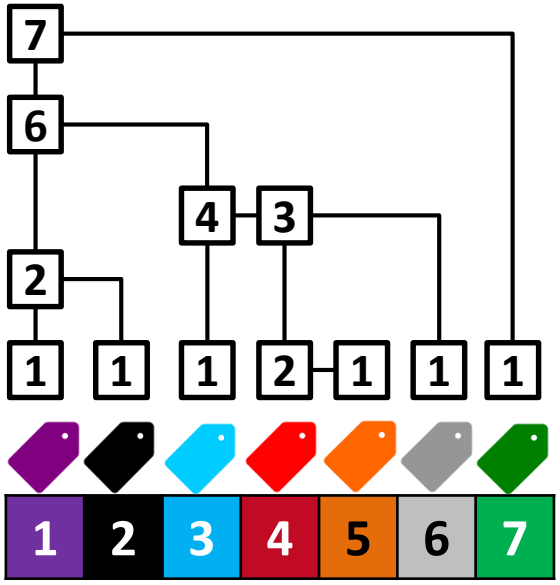




Dynamic Provable Data Possession

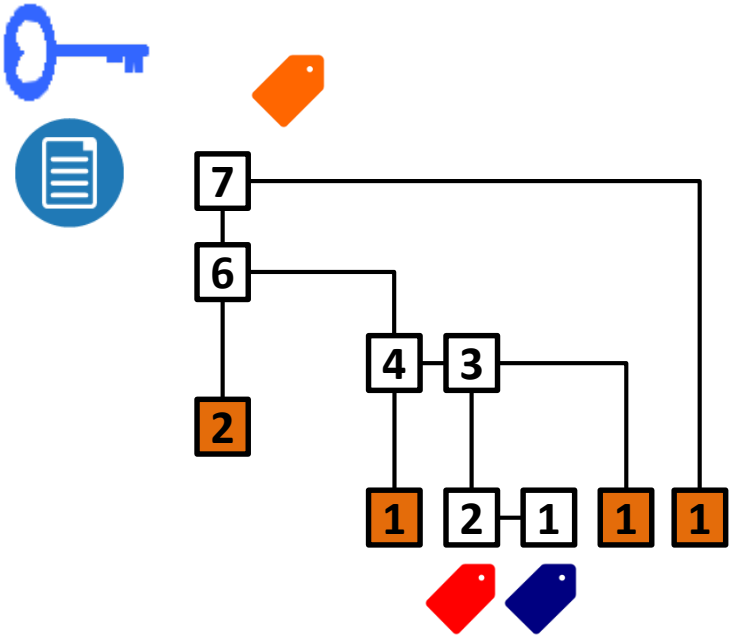
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

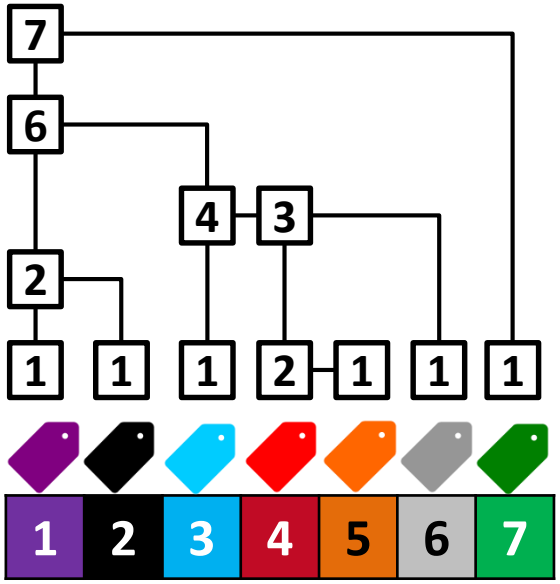




Dynamic Provable Data Possession

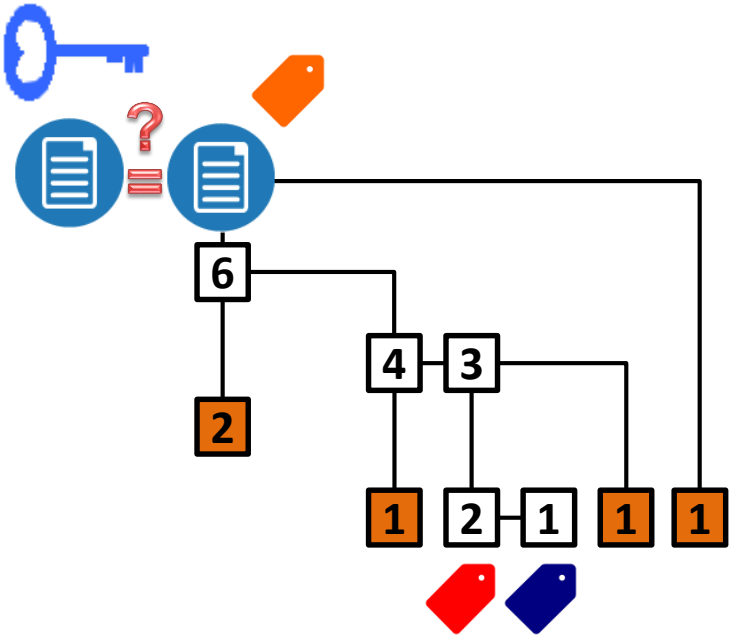
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

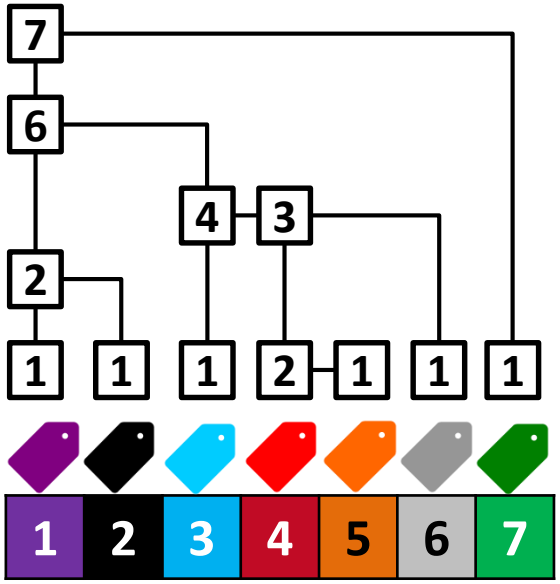




Dynamic Provable Data Possession

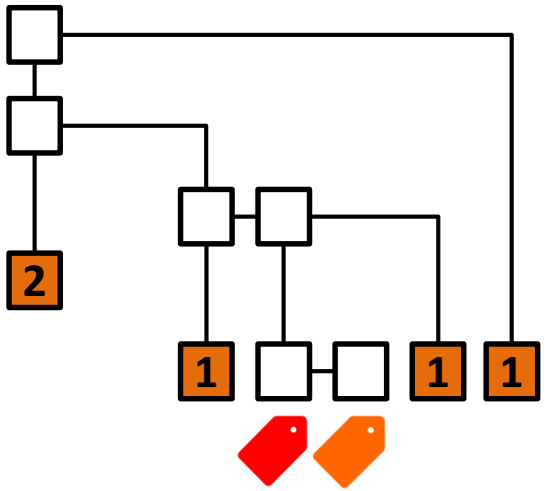
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

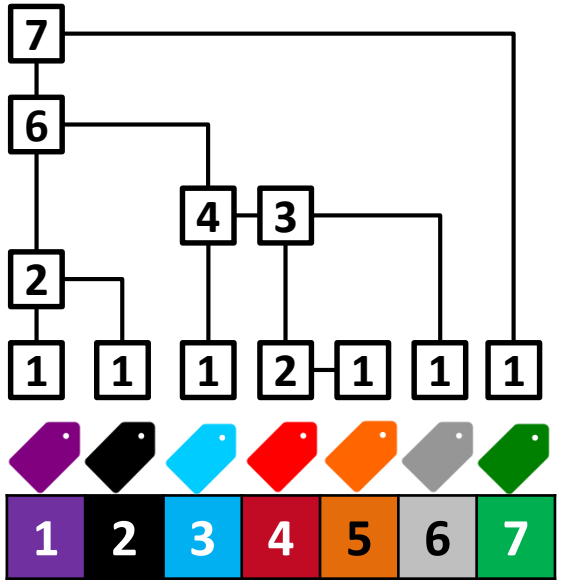




Dynamic Provable Data Possession

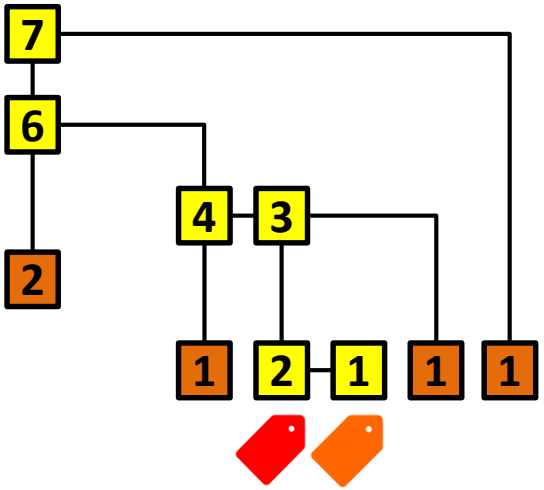
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

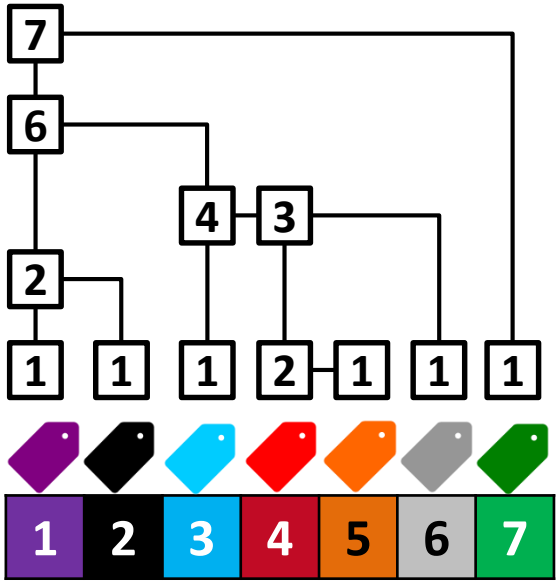




Dynamic Provable Data Possession

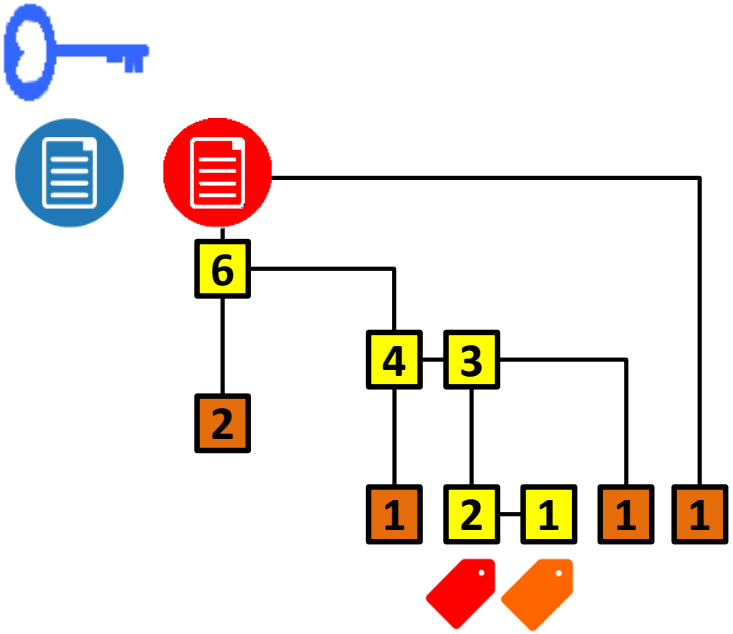
[EKPT ACM CCS 2009 & ACM TISSEC 2015]

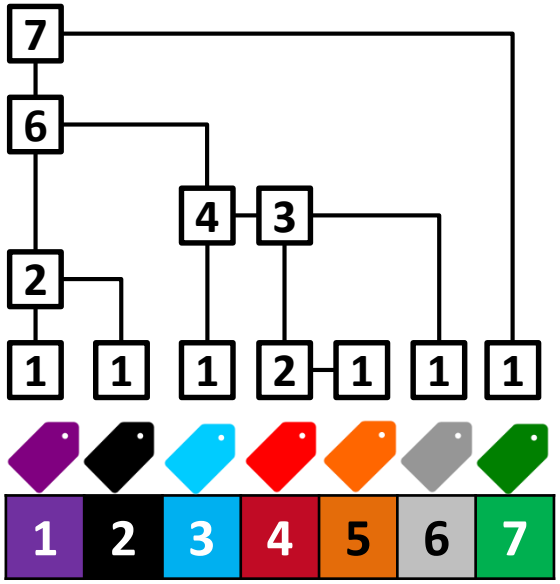




Dynamic Provable Data Possession

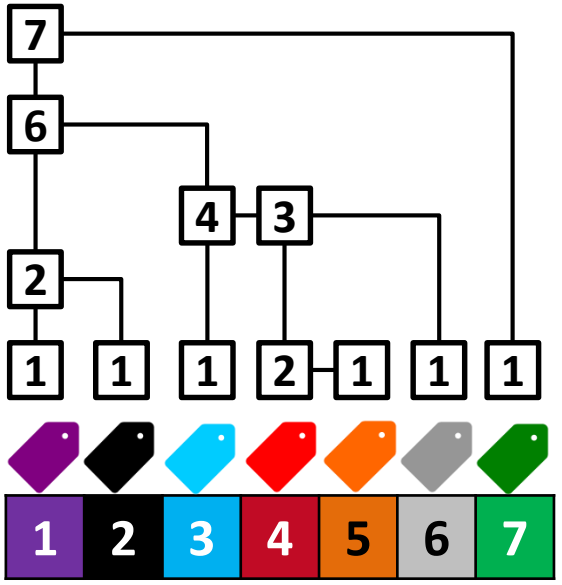
[EKPT ACM CCS 2009 & ACM TISSEC 2015]





Dynamic Provable Data Possession

[EKPT ACM CCS 2009 & ACM TISSEC 2015]



Overview

- **Secure Cloud Storage**
  - **Problems**
  - **Solutions**
  - **Summary**

Further Work

- **Distribution and Replication [EK13a]**
  - **Without increasing complexity**
- **Failure Resiliency [CKW13][CKW17]**
  - **Via error-correcting and erasure codes**
- **PDP vs. POR [EK16][EK19b]**
  - **POR uses erasure codes**
  - **PDP is more efficient**
- **What happens when the proof fails?**
  - **Official arbitration [K15]**
    - **NOT public verifiability**

READING LIST

- **Static PDP and POR**
  - Ateniese et al. ACM CCS 2007 & ACM TISSEC 2011, *Provable Data Possession*
  - Shacham and Waters. ASIACRYPT 2008 & Journal of Cryptology 2013, *Compact POR*
- **Dynamic PDP**
  - Erway, Küpçü, Papamanthou, Tamassia. ACM CCS 2009 & ACM TISSEC 2015, *Dynamic Provable Data Possession*
  - Etemad and Küpçü. ACNS 2013, *Distributed, and Replicated DPDP*
  - Esiner, Küpçü, Özkasap. ICC 2014, *FlexList*
  - Esiner, Kachkeev, Braunfeld, Küpçü, Özkasap. ACM TOS 2016 *FlexDPDP*
  - Etemad and Küpçü. ACM CSUR 2020, *Generic DPDP*
- **Dynamic POR**
  - Cash, Küpçü, Wichs. EUROCRYPT 2013 & Journal of Cryptology 2017, *PORAM*
  - Shi et al. ACM CCS 2013, *Practical DPOR*
  - Chandran et al. TCC 2014, *Locally Updatable and Locally Decodable Codes*
  - Etemad and Küpçü. ACM CCSW 2016. *Generic DPOR from PDP and DPDP.*
- **Official Arbitration**
  - Küpçü. The Computer Journal 2015, *Official Arbitration*

Conclusion

- **Cloud Storage**
  - **Can efficiently provide confidentiality and integrity of data, among multiple servers**
    - **Proof and verification times on the order of milliseconds**
    - **Proof size is a few hundred KB for a few GB file**
  - **Can handle whole file systems or version control systems**

Funding Acknowledgement

- **TÜBİTAK** 111E019, 112E115, 114E487, 115E766, 119E088
- **Royal Society Newton Advanced Fellowship** NA140464
- **BAGEP** 2016
- **TÜBA GEBİP** 2017
- **European Union COST Actions** IC1206, IC1306
- **Koç Sistem**
- **Türk Telekom** 11315-06

BİLİM AKADEMİSİ

COST ACTION IC1206

DE-ID De-identification for privacy protection in multimedia content.

cost

CryptoAction

TÜRK TELEKOM

KoçSistem

TÜBA

EXCELLENCE IN SCIENCE THE ROYAL SOCIETY

Newton Fund

Entrepreneurship Timeline

- **2001: Bilkent CS 102 project**
  - **Maplab Map Simulator**
- **2004: Bilkent CS 492 Senior Project**
  - **Kaşif: Best Senior Project Award**
  - **Google Maps Beta was launched in 2005**
- **2008-2010: while still in USA**
  - **Brown University PRIME Entrepreneurship Program**
  - **Rhode Island Center for Innovation**
- **2020: TÜBİTAK BİGG awards, co-founded:**
  - **FineSci Technology Inc.**
  - **Xtinge Technology Inc.**

ALPTEKİN KÜPÇÜ

Associate Professor of Computer Science and Engineering

crypto.ku.edu.tr
finesci.com
xtinge.com

KOÇ UNIVERSITY