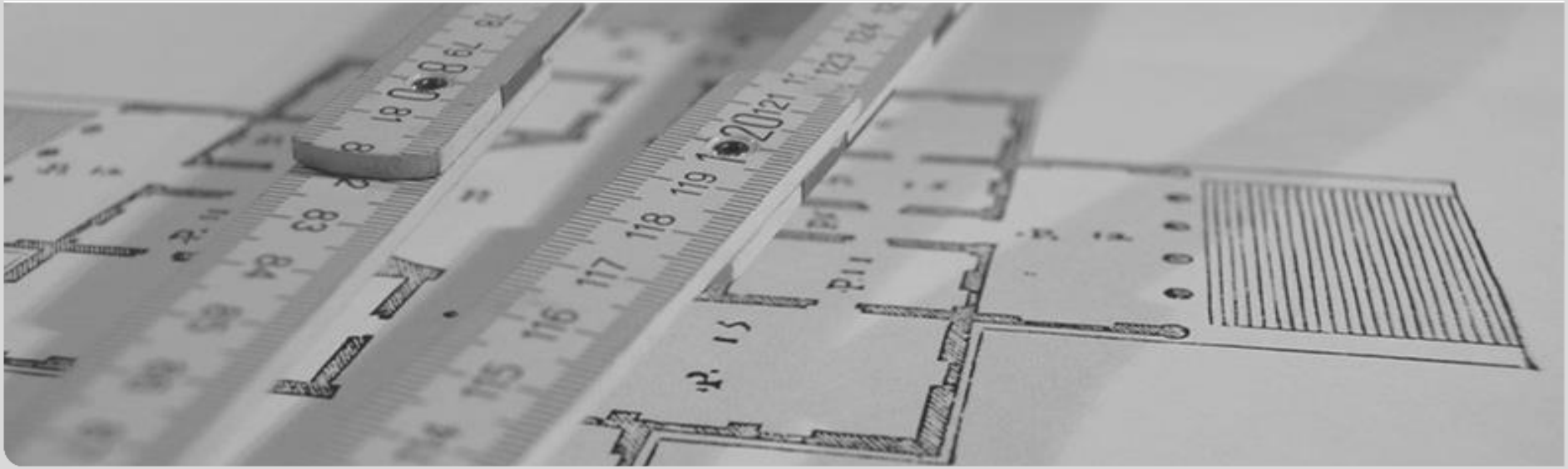
Karlsruher Institut für Technologie

Broadcast Encryption

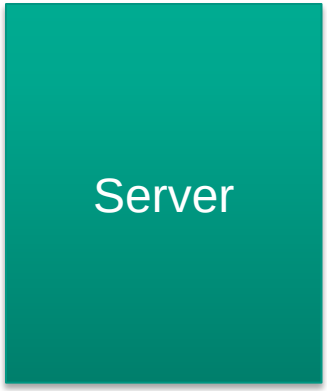
20.03.2013

PSE 2012/13

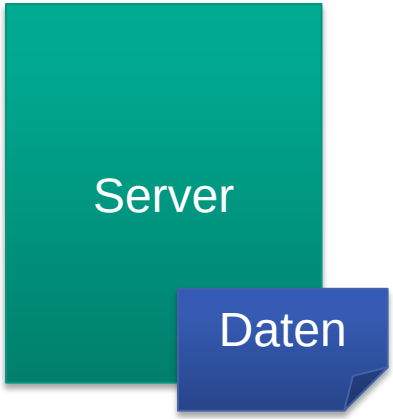


Mohammed Abu Jayyab, Niklas Baumstark, Tobias Gräf, Amrei Loose, Christoph Michel

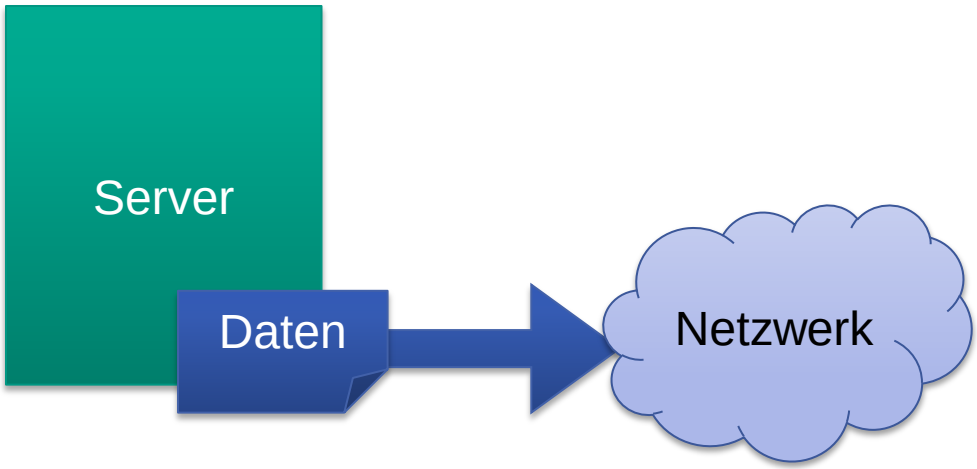
Broadcast-Verschlüsselung



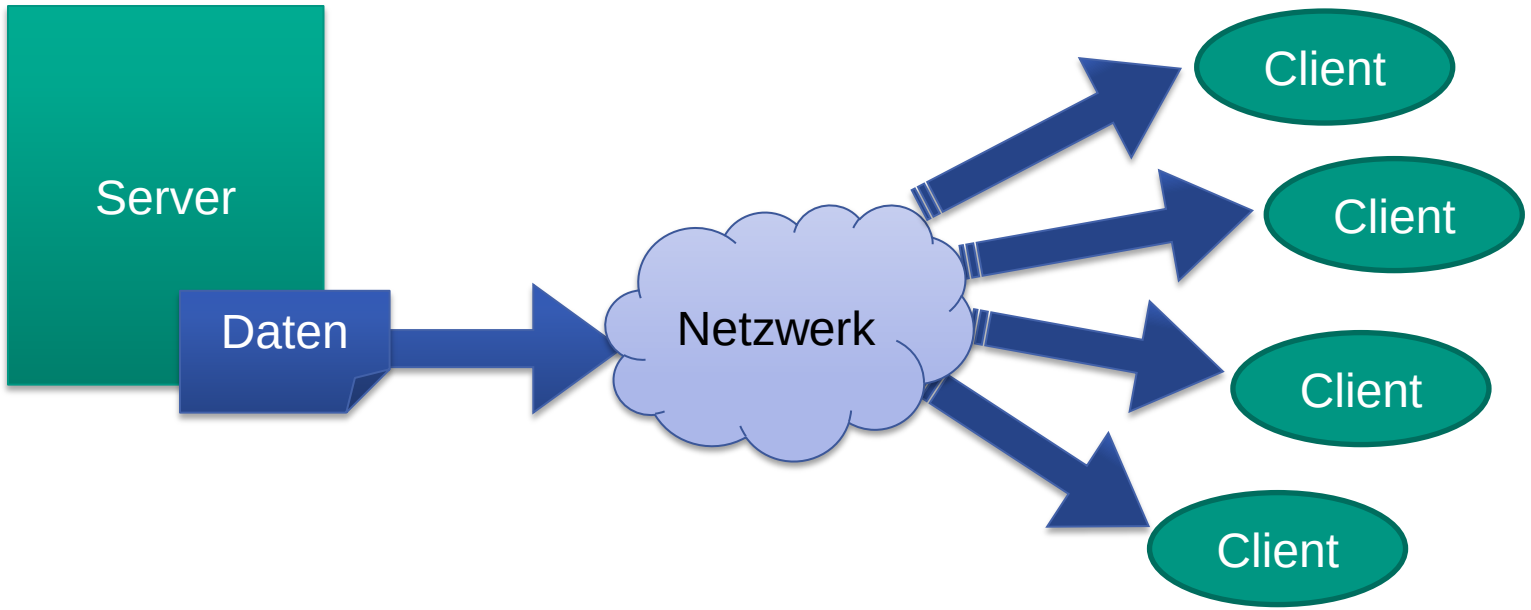
Broadcast-Verschlüsselung



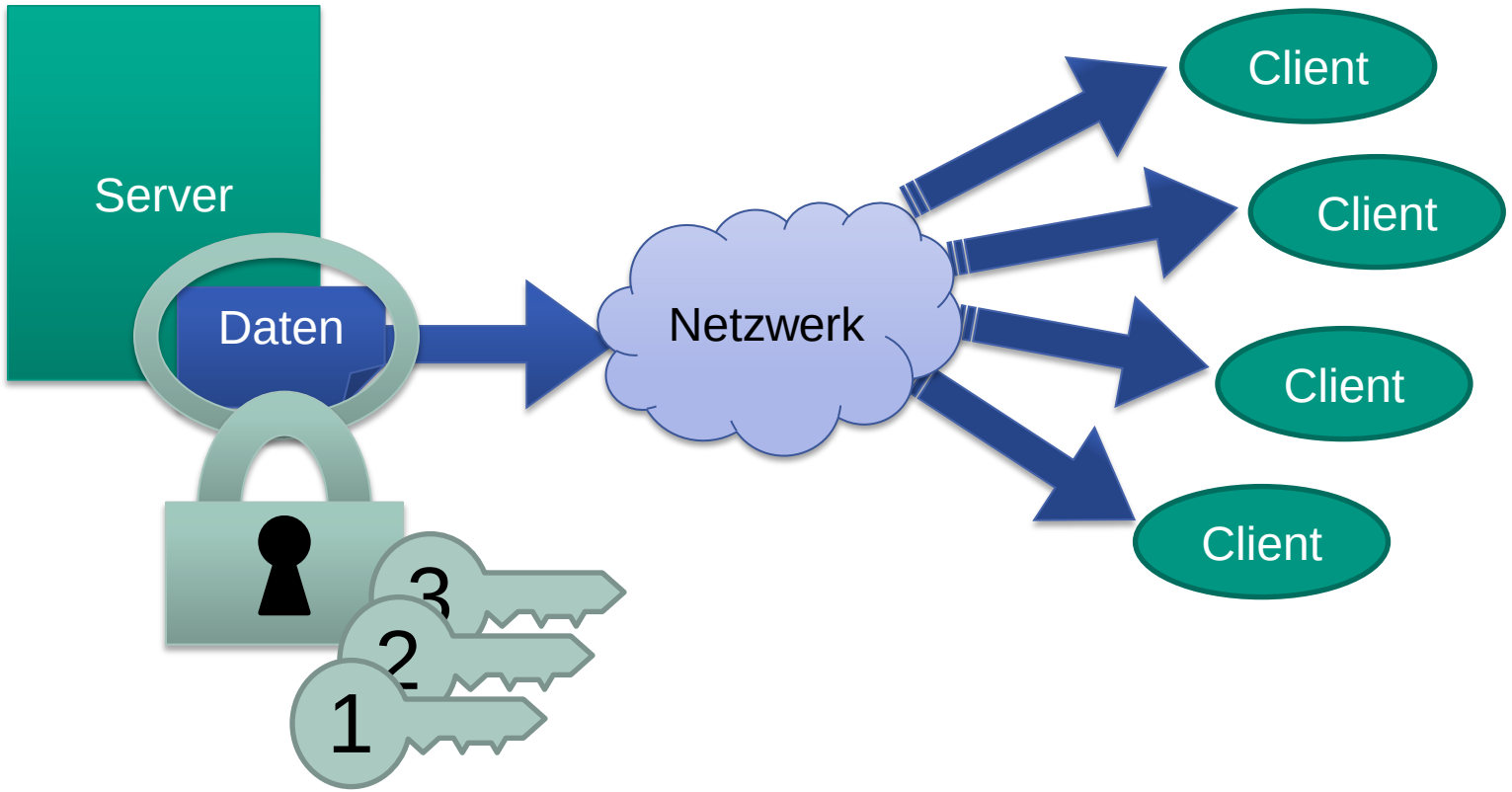
Broadcast-Verschlüsselung



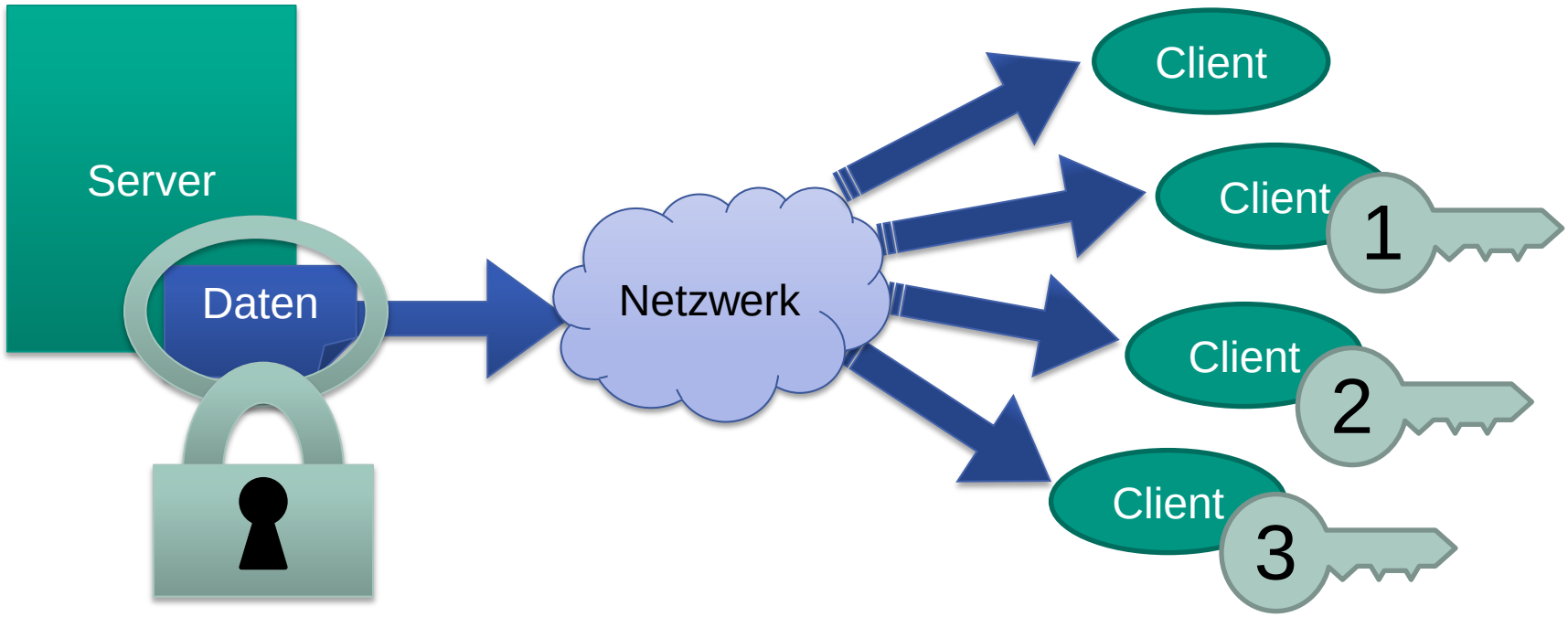
Broadcast-Verschlüsselung



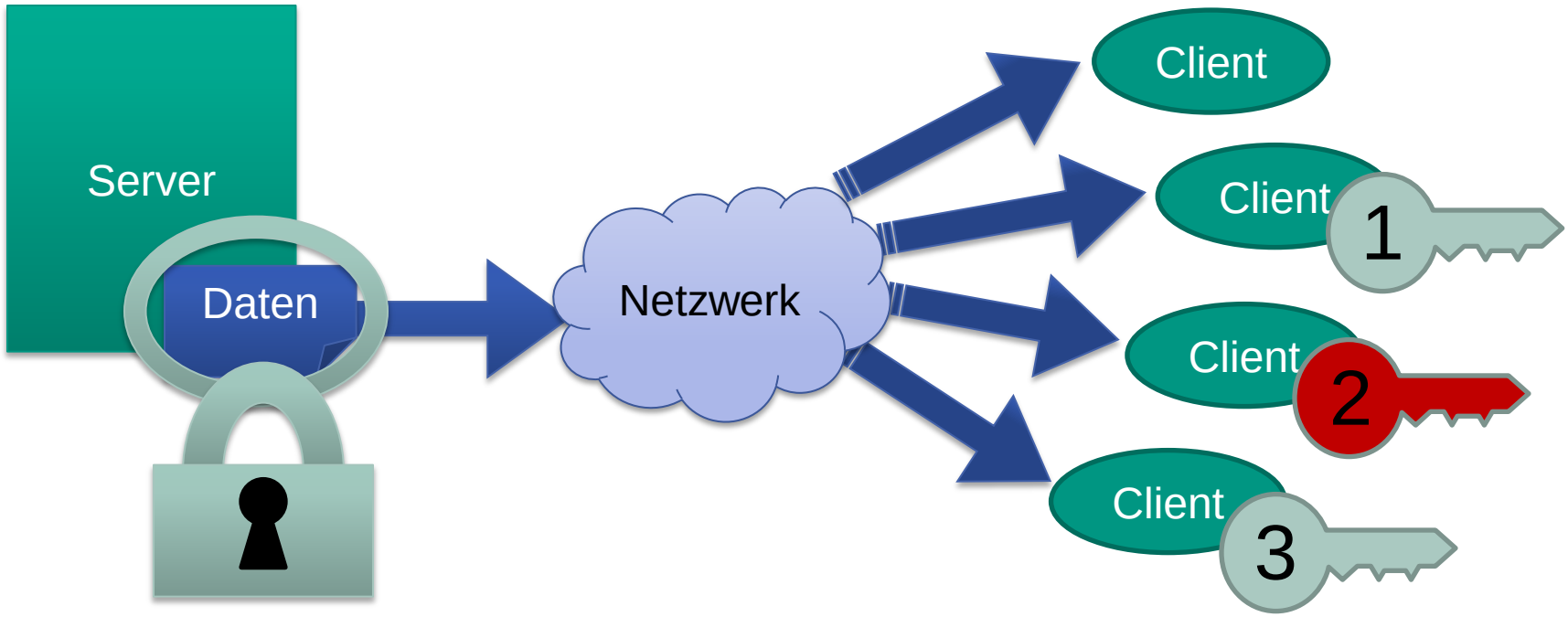
Broadcast-Verschlüsselung



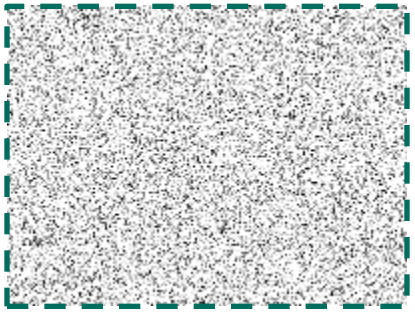
Broadcast-Verschlüsselung

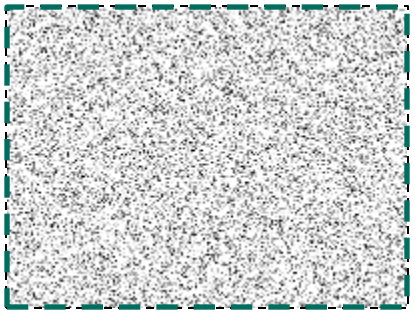


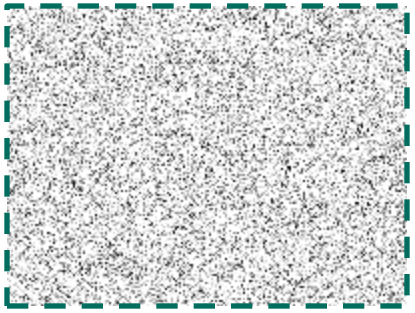
Broadcast-Verschlüsselung

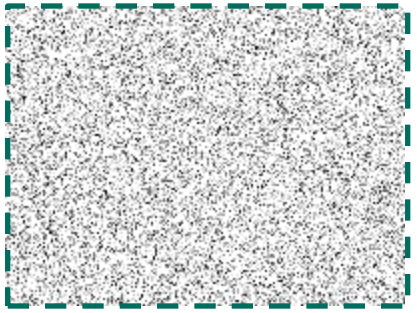


Shamirs-Secret-Sharing

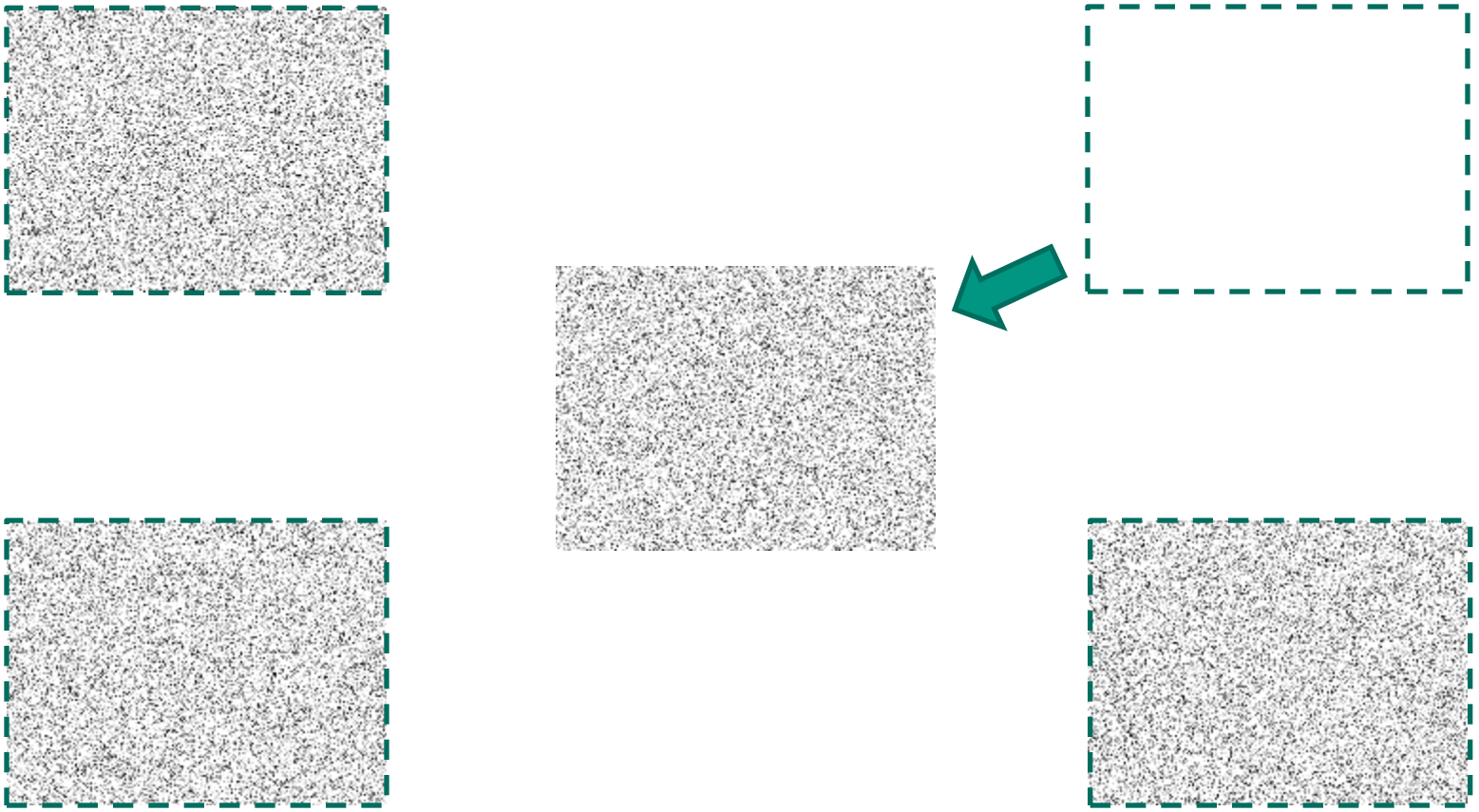




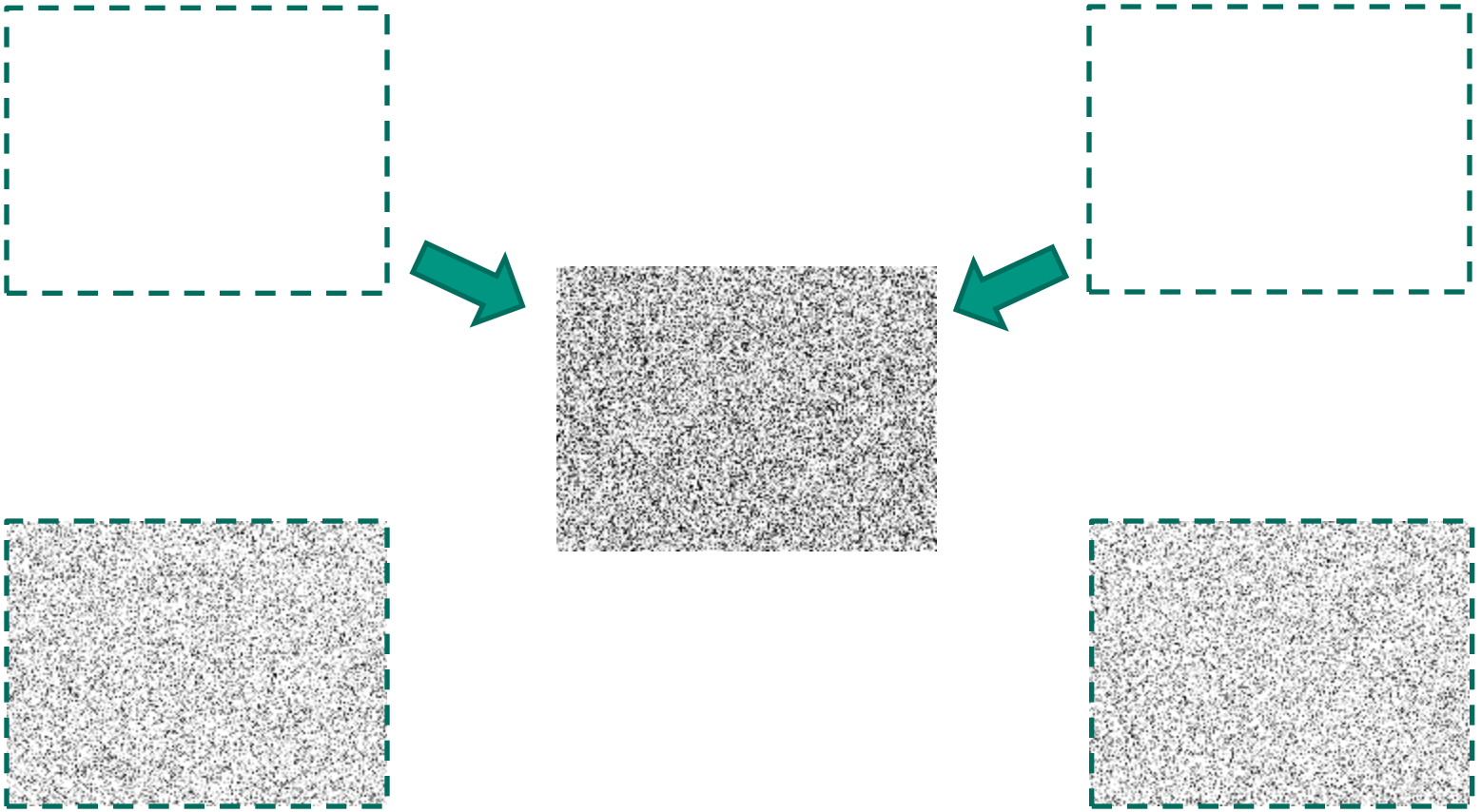




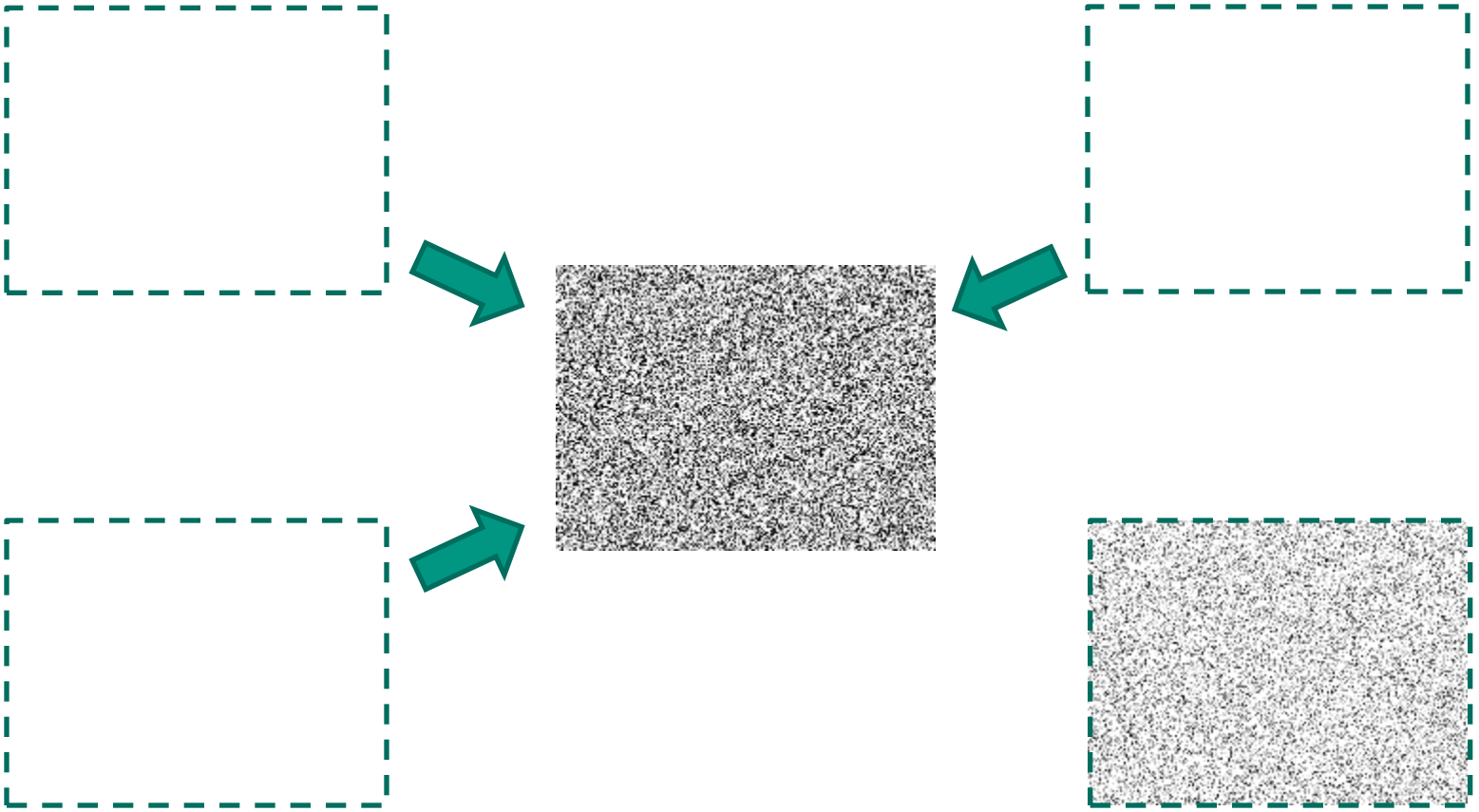
Shamirs-Secret-Sharing



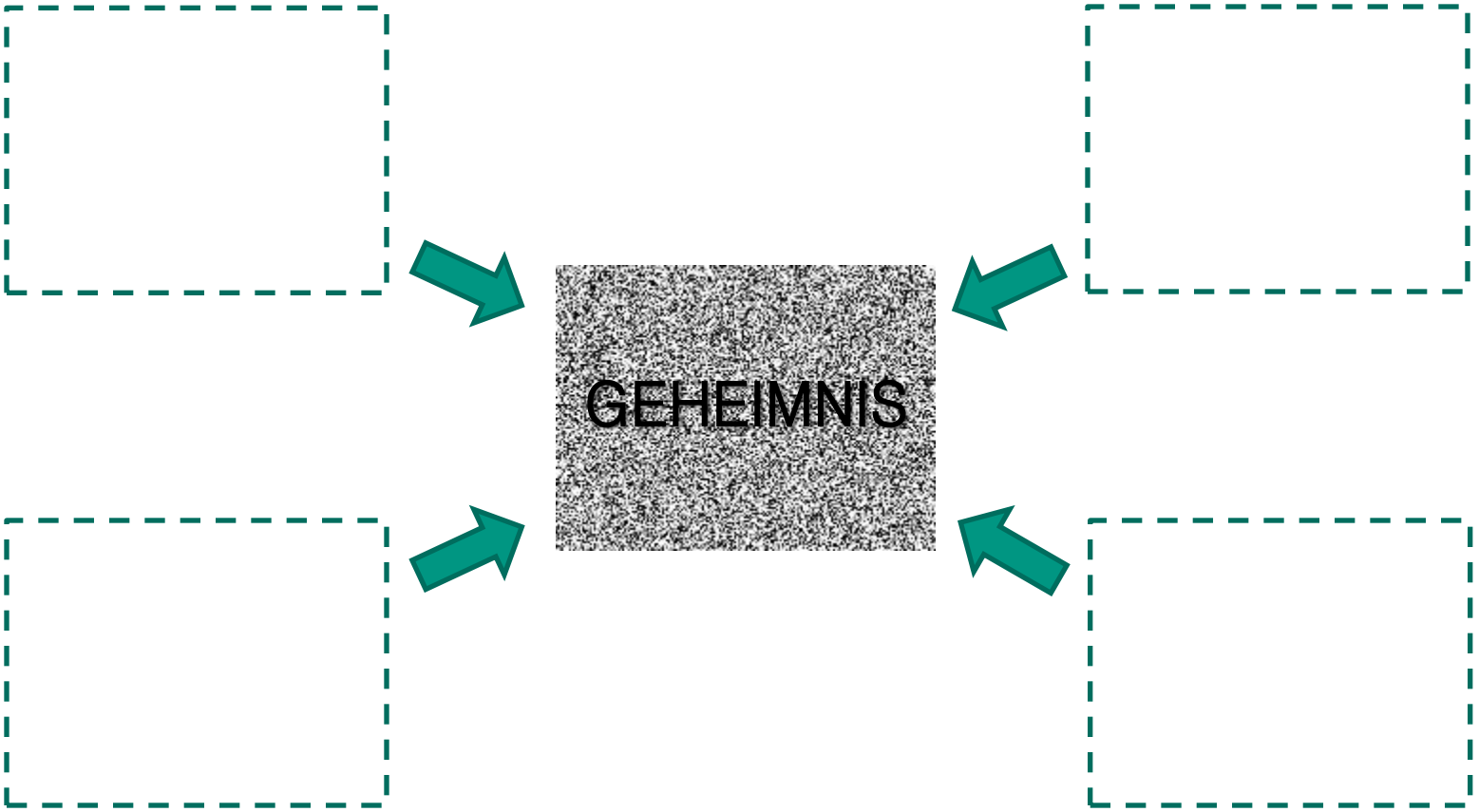
Shamirs-Secret-Sharing



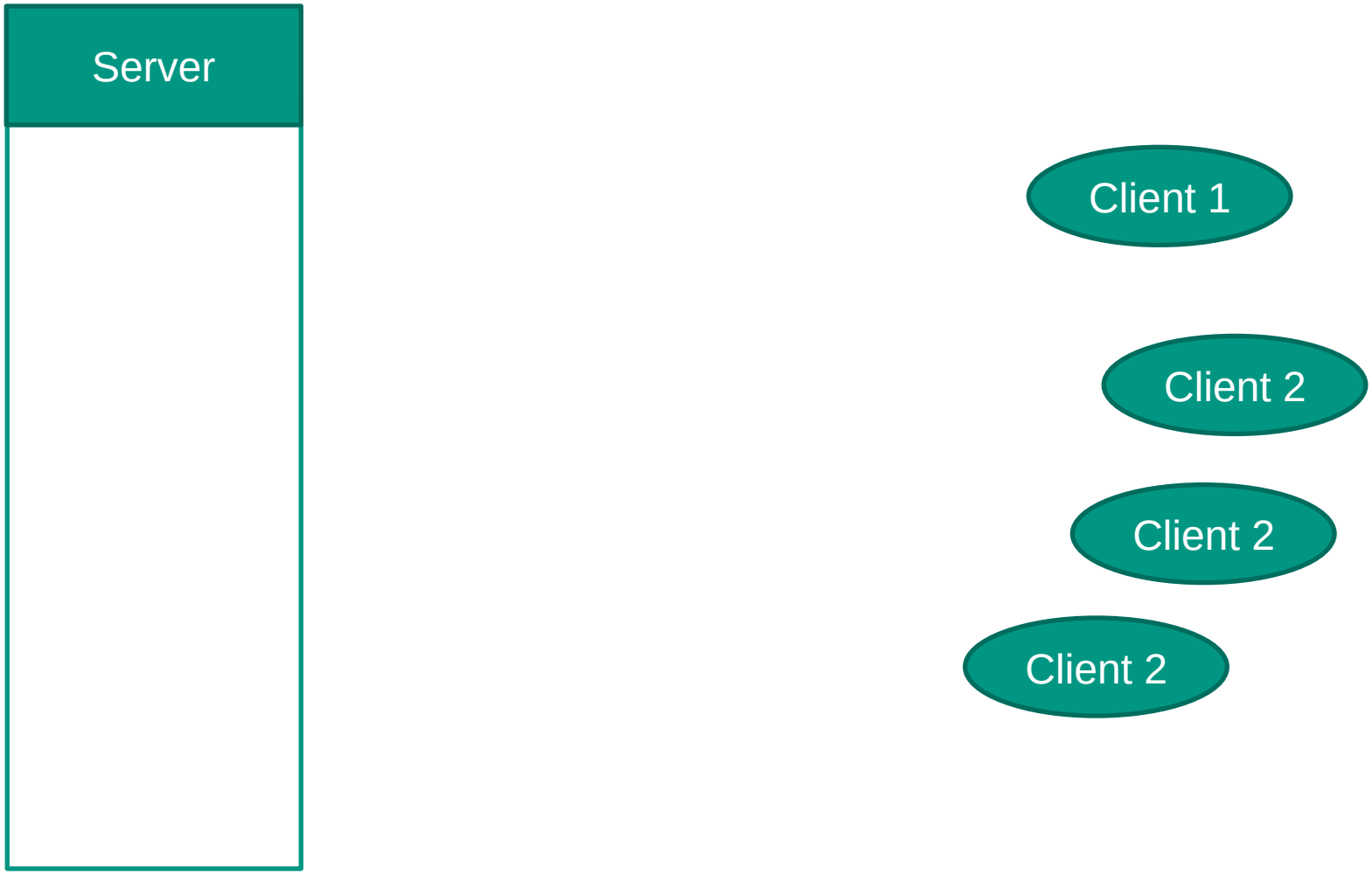
Shamirs-Secret-Sharing



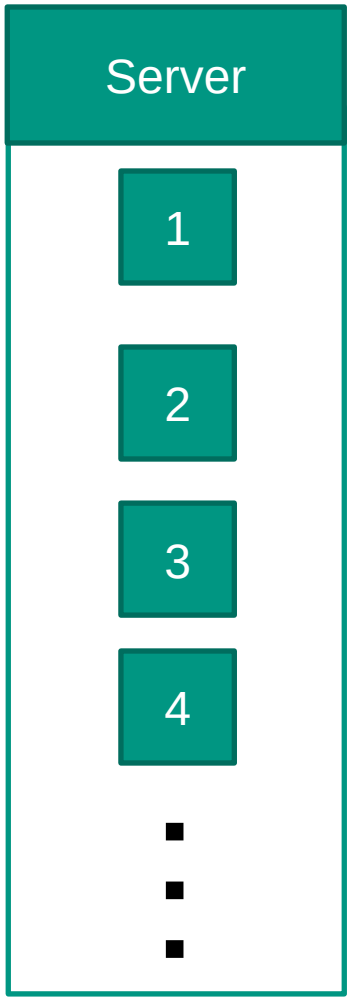
Shamirs-Secret-Sharing

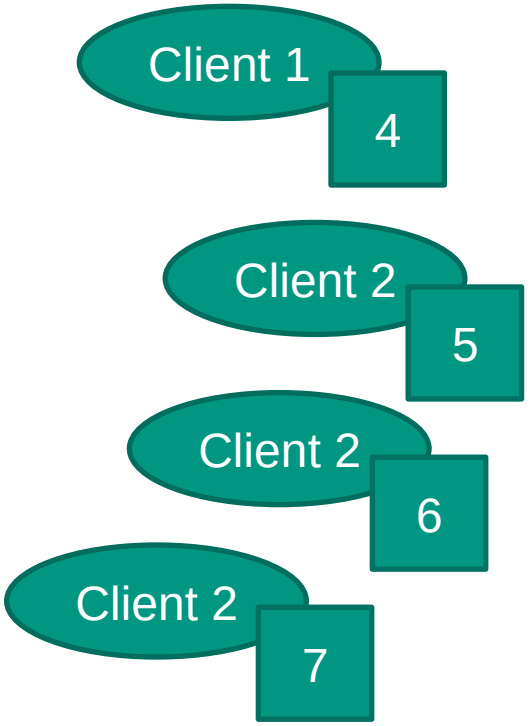


Naor-Pinkas-Revoke-Scheme

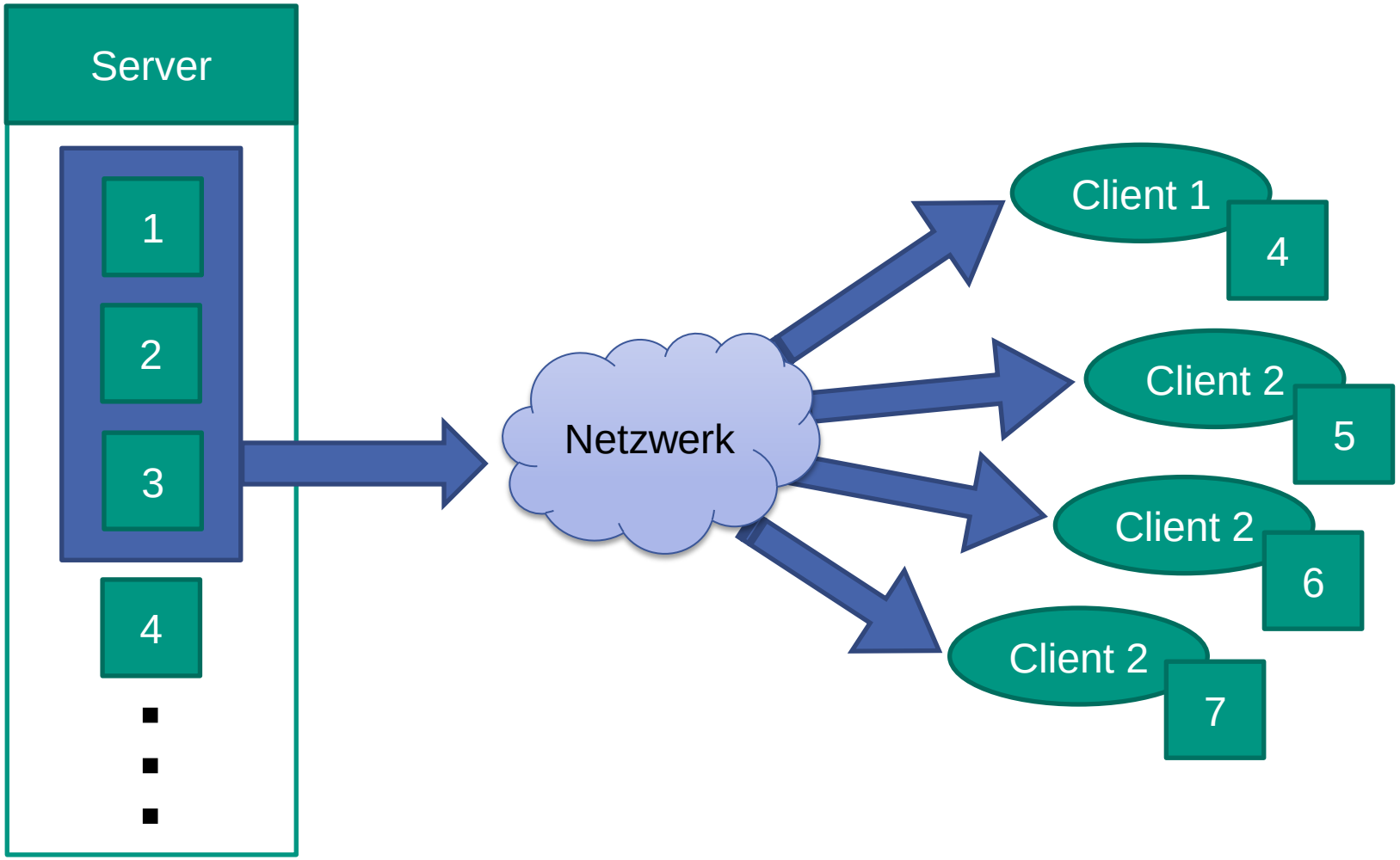


Naor-Pinkas-Revoke-Scheme

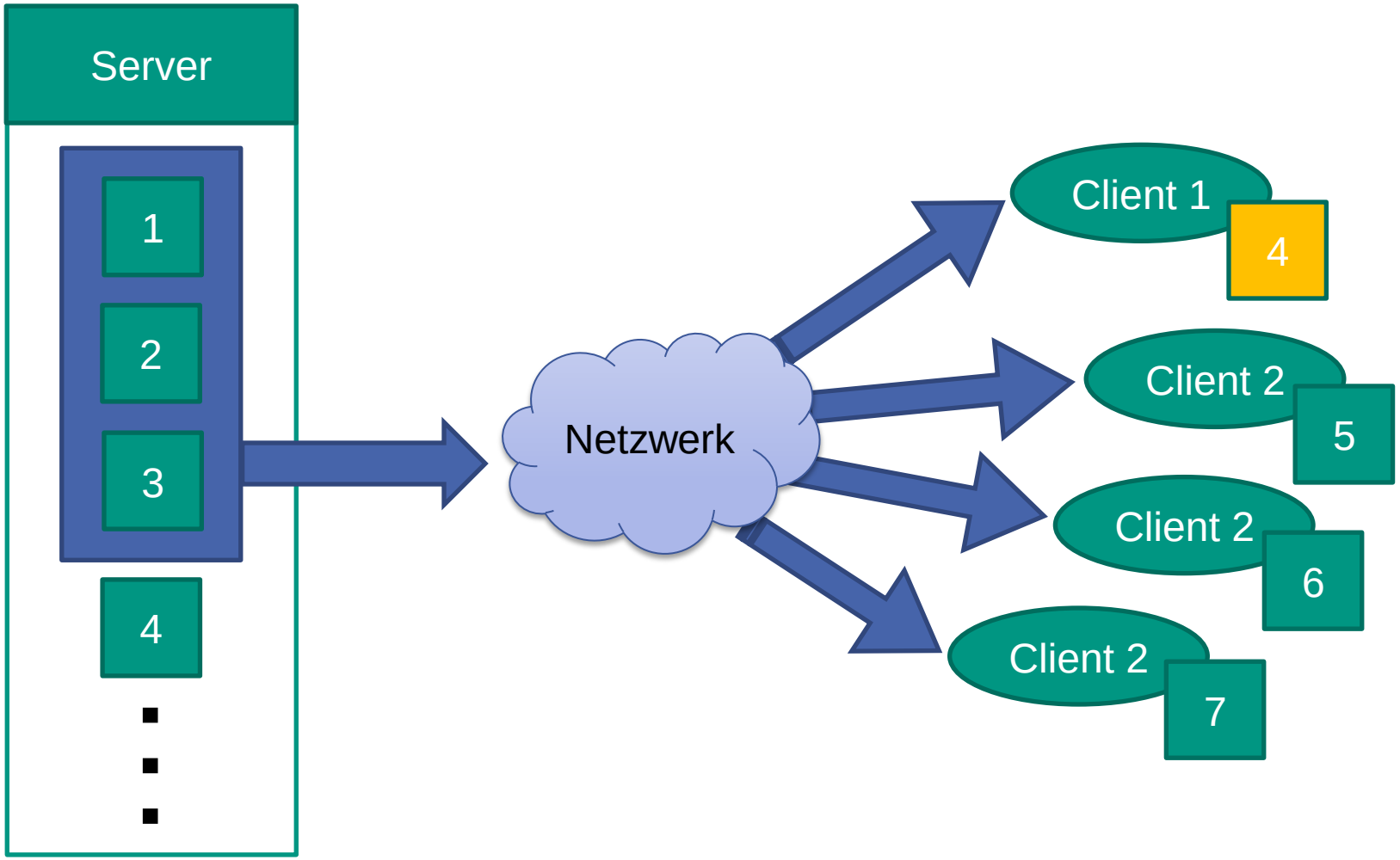




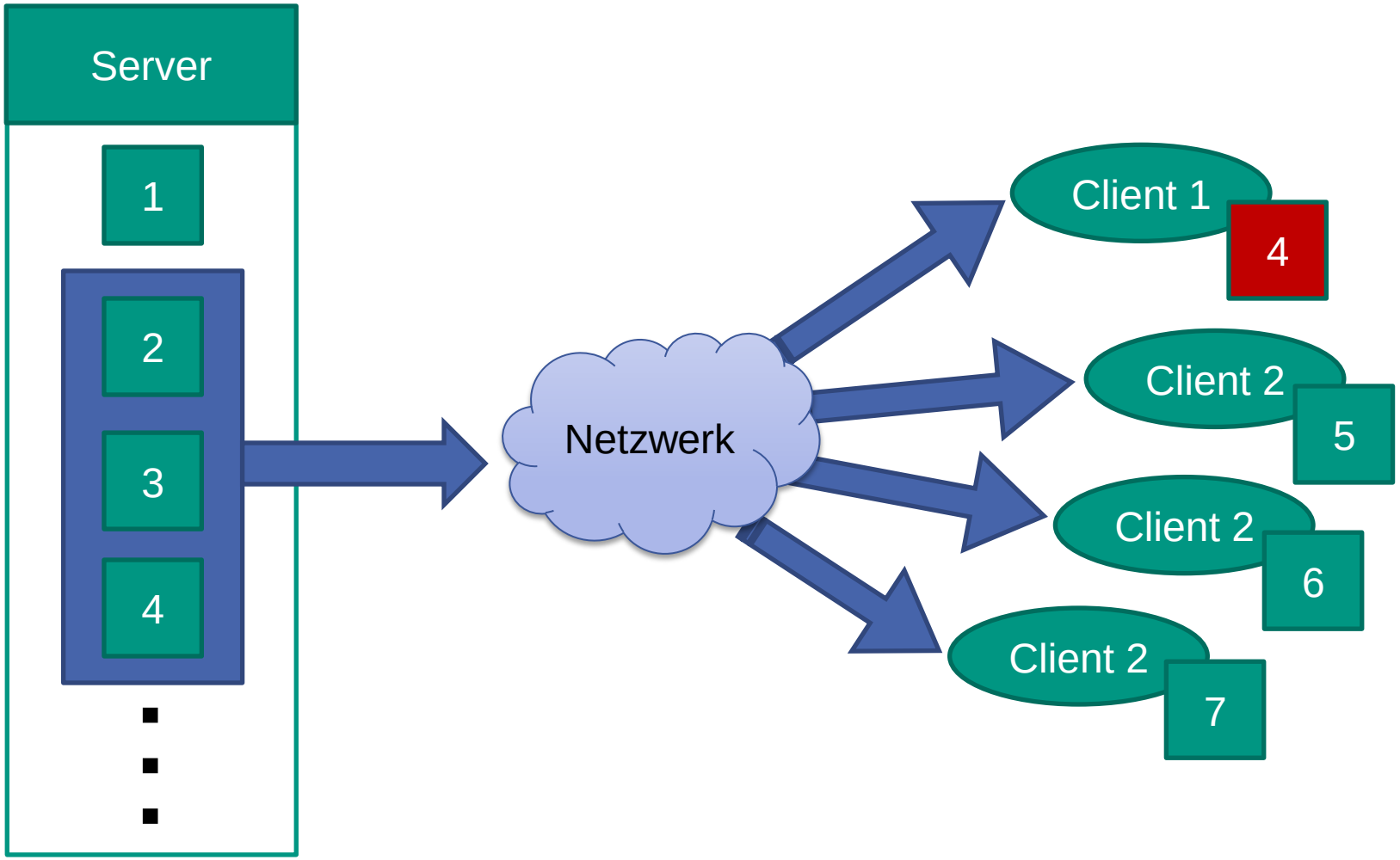
Naor-Pinkas-Revoke-Scheme



Naor-Pinkas-Revoke-Scheme



Naor-Pinkas-Revoke-Scheme



Unser Projekt

- Broadcast-Verschlüsselung in der Praxis ausprobieren
- Entwicklung eines Produkts
  - Anbieter will Inhalte durch Server verbreiten
  - Rechenstarke Smartphones verbreitet: Android
  - Soll für Benutzer möglichst einfach sein
- Entstanden ist: **CryptoCast**

  → Client-Server-Kombination für Broadcast mit Verschlüsselung

Technisches

- Server
  - Java und C++
  - Konsolenanwendung
    - Benutzerverwaltung
    - Verschlüsselung
    - Senden beliebiger Datenströme
- Client
  - Android ab 2.3
  - Empfangen
  - Entschlüsseln
  - Wiedergeben der Inhalte (bei uns: MP3)

Statistik

- ~7400 Zeilen Code
  - wesentliche Anteile und Aufwand für Kryptographie
- durch Optimierungen bis zu 5000 ausschließbare Benutzer
- Gesamtzahl der Benutzer nur durch das Netzwerk beschränkt

Produktvorführung