Einführung in Verschlüsselung

Jens Kühnel
beim Chemnitzer
Linuxtag 2018

Über mich

- Seit 2000 Freiberuflicher Linux-Trainer, -Buchautor und -Administrator

- Seit 2017
  - 10% Freiberufler
  - 90% Angestellter Sysadmin bei der Deutschen Börse Frankfurt

Über diesen Vortrag

- Keinerlei Mathe

- Extrem Vereinfacht
  - Nicht falsch
  - aber sehr viele Dinge fehlen

Was ist Verschlüsselung

- Sichere und Unveränderte Kommunikation
- Vorraussetzung:
  - Netzwerk unsicher
  - Client und Server sicher

- Kerkhoffs Prinzip:
  - Halte den Schlüssel geheim
  - aber den Algorithmus muss offen

Bausteine

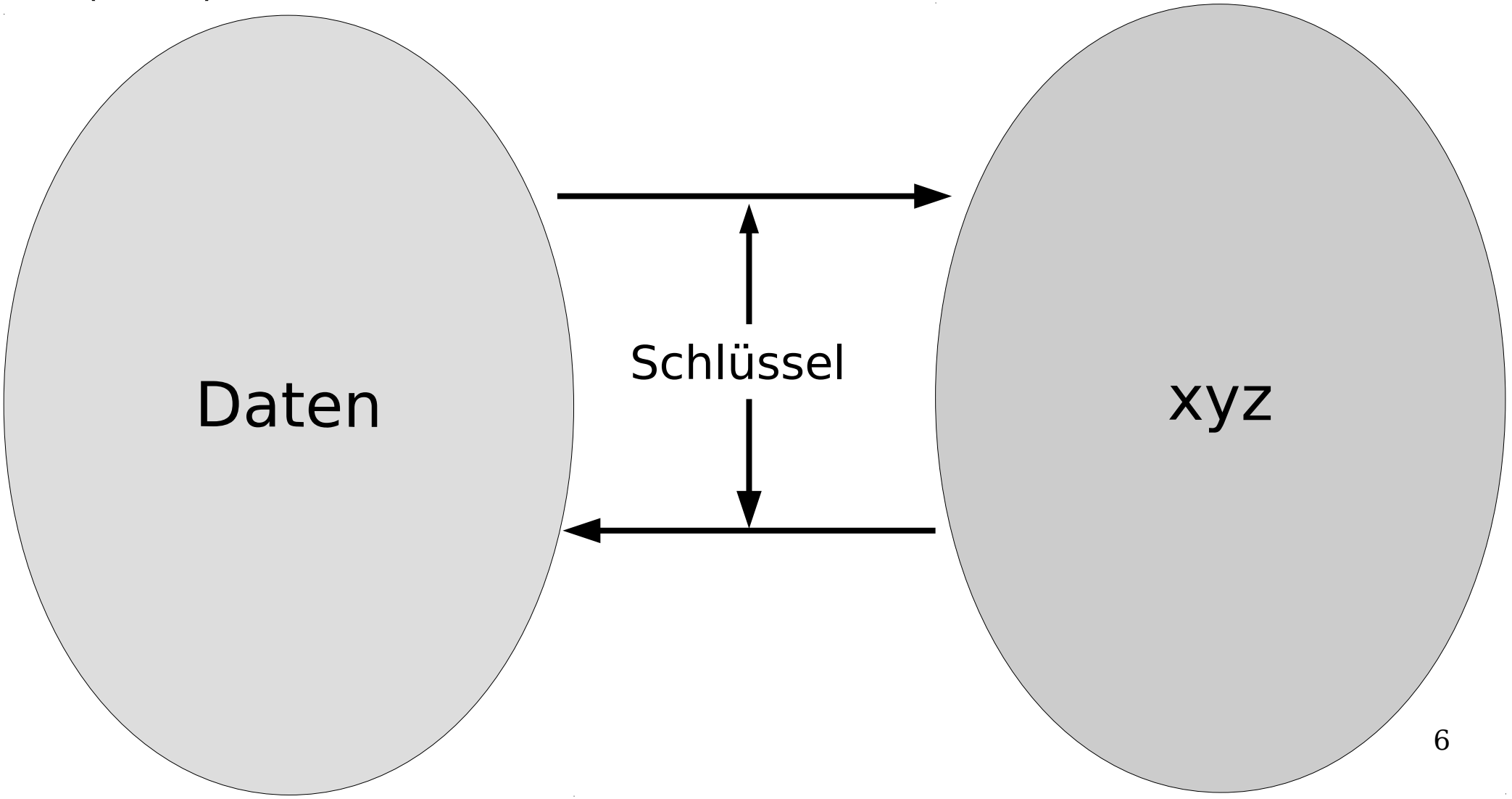
- Symetische Verschlüsselung
- Asymetrische Verschlüsselung
- Signing
- Hash
- (MAC)
- (Keyexchange)

symetrische Verschlüsselung

zB:

- AES
- Blowfish
- (3DES)

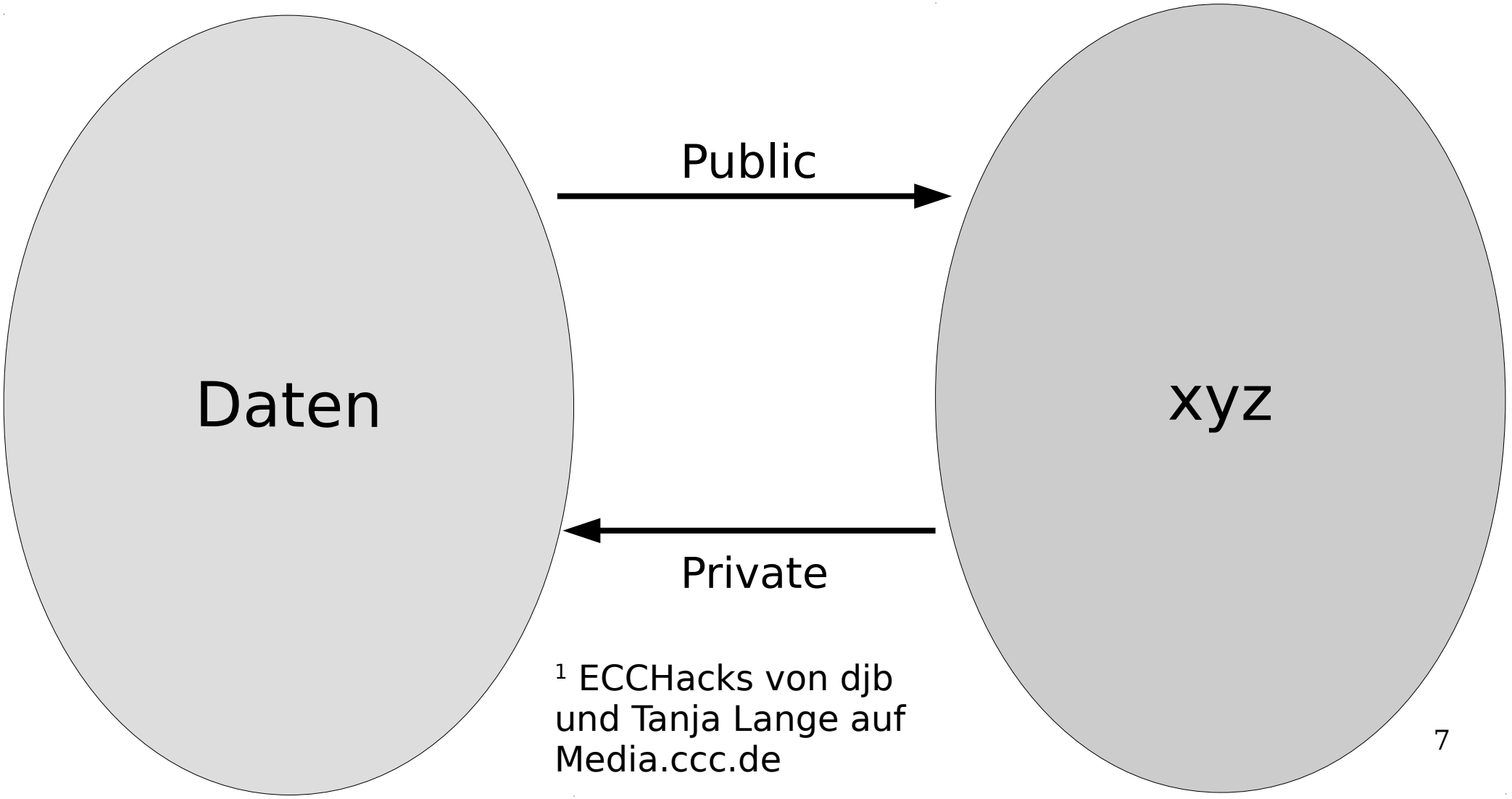
Schlüssellänge:
128-256 Bit



asymetrische Verschlüsselung

zB:
- RSA (DSA)
- Elyptic Curves [1]

Schlüssellänge:
(2048-) 4096 Bit
128 – 256 Bit

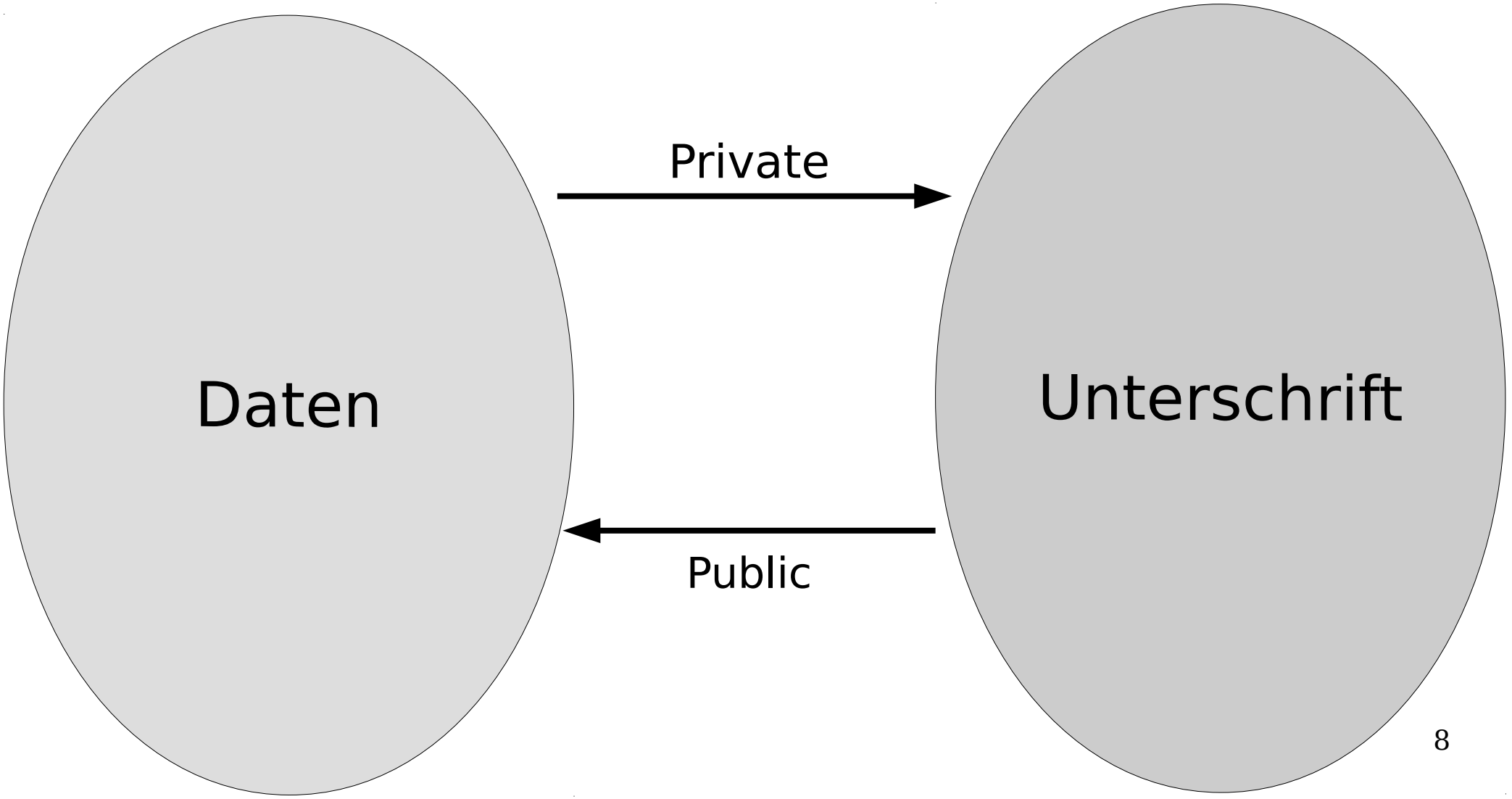


[1] ECCHacks von djb und Tanja Lange auf Media.ccc.de

digitale Unterschrift

zB:

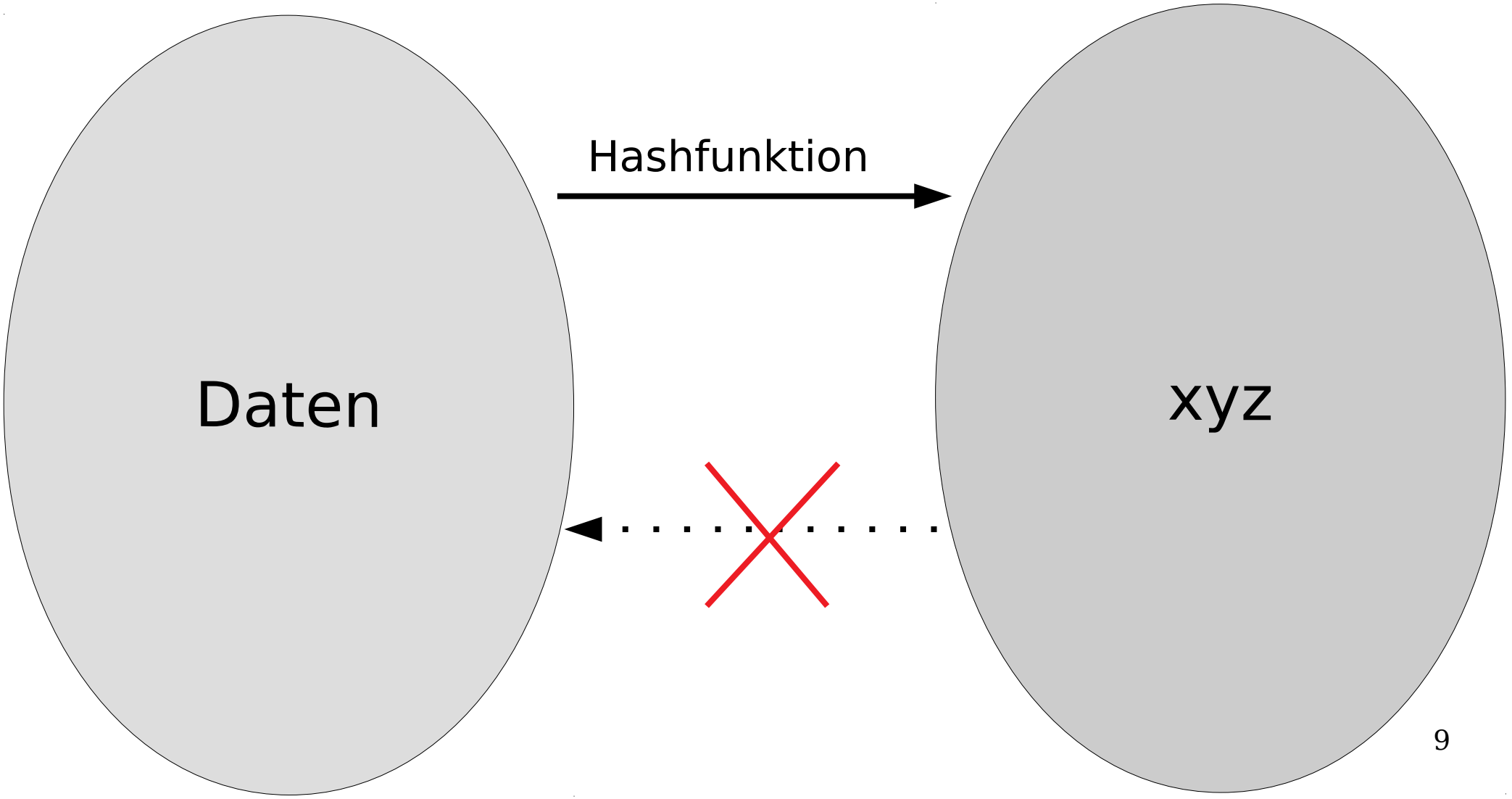
- CA + PKI
- X509
- GPG



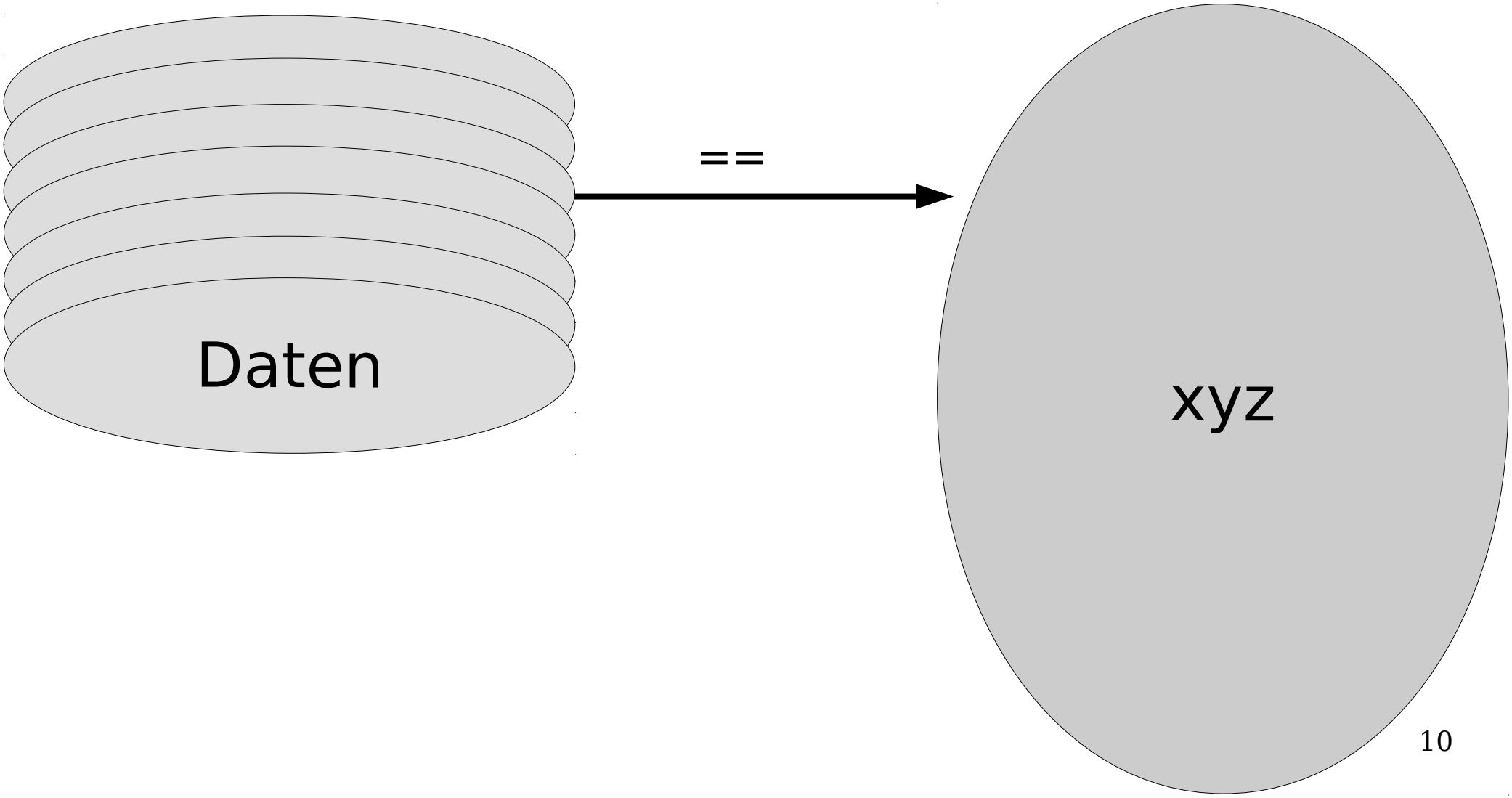
Hash

zB:

- (MD5,SHA)
- SHA256,SHA512



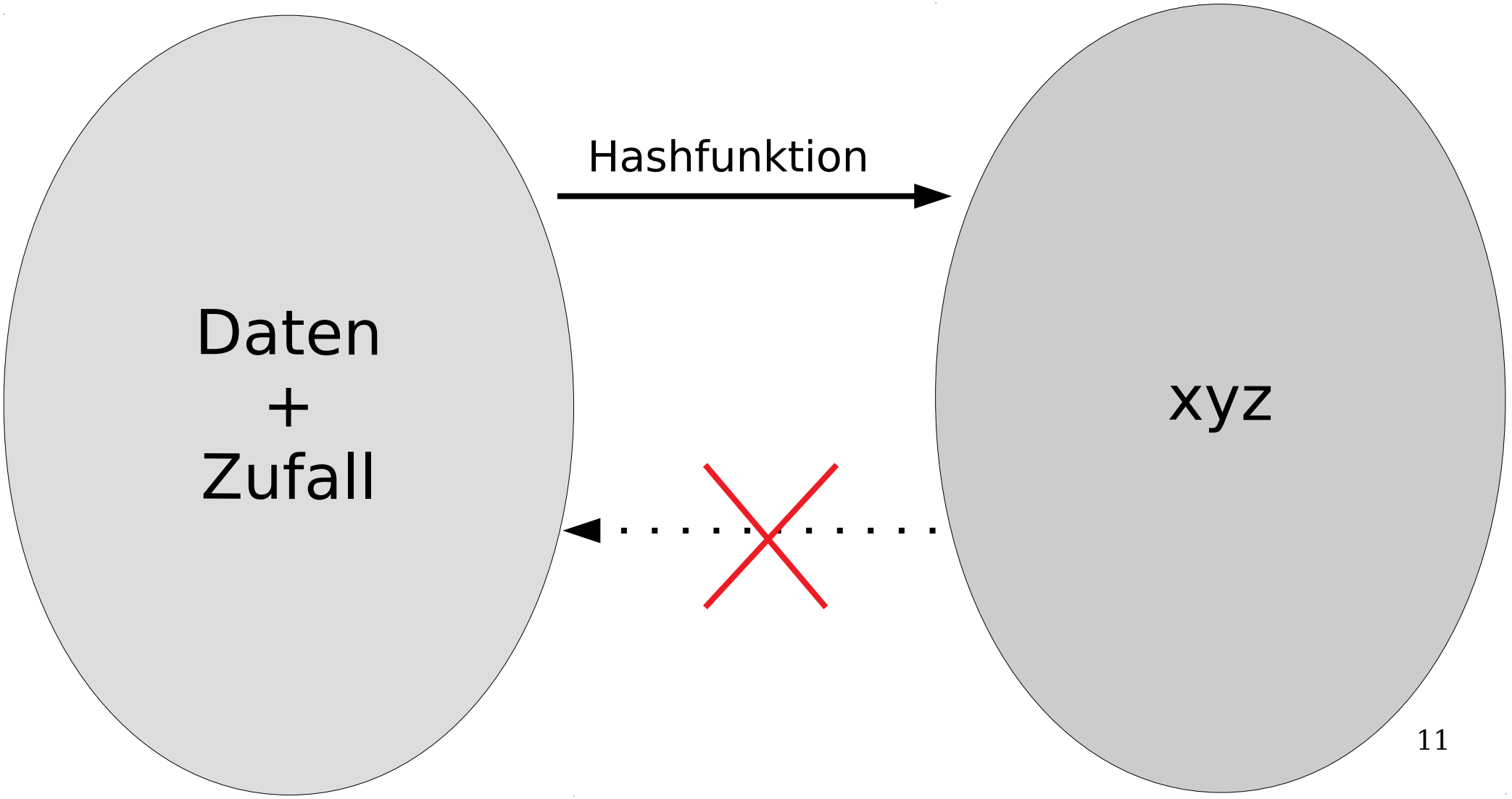
Wörterbuchangriff



Gegen-Wörterbuchangriff

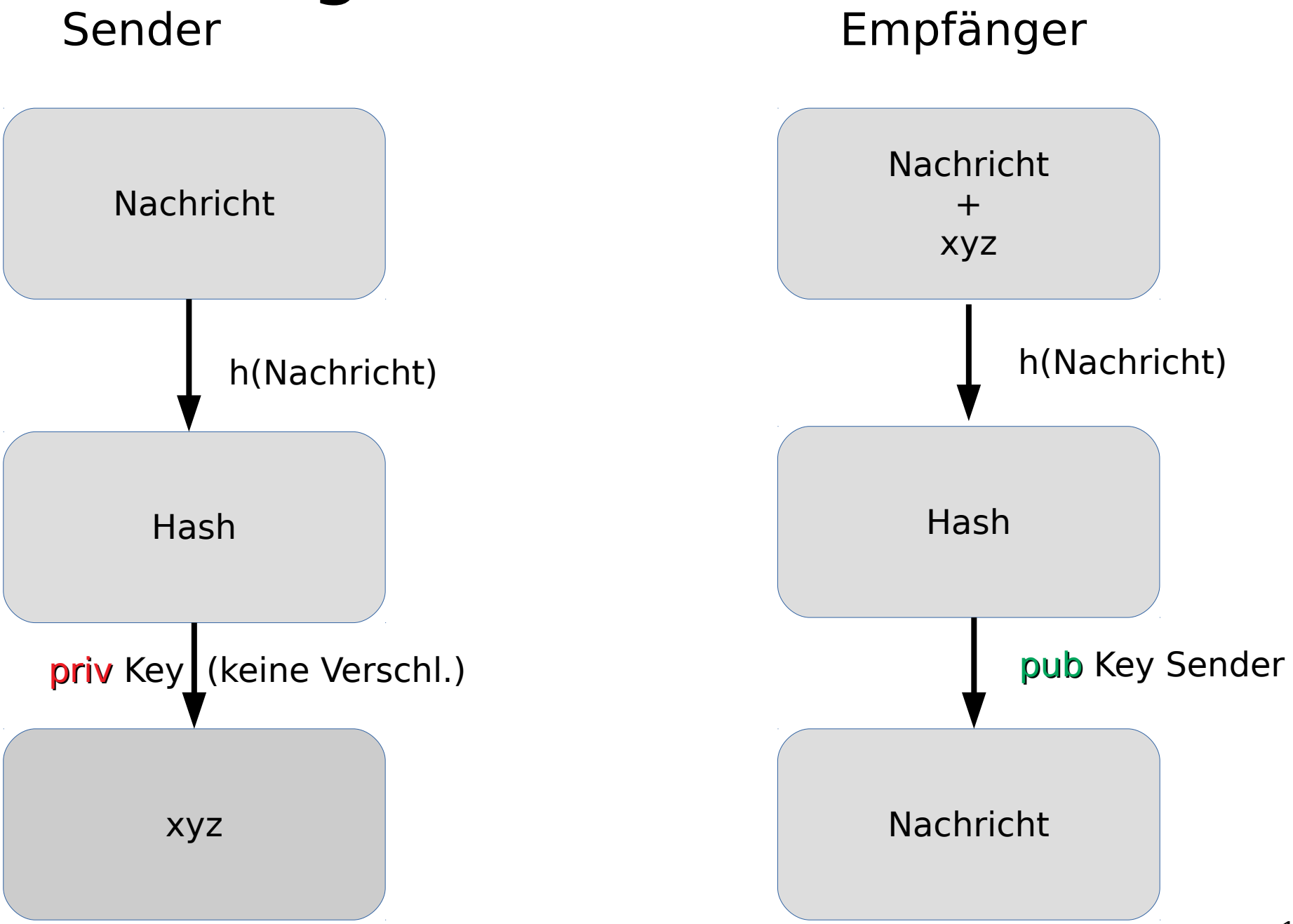
zB:

- SSHA
- BCrypt

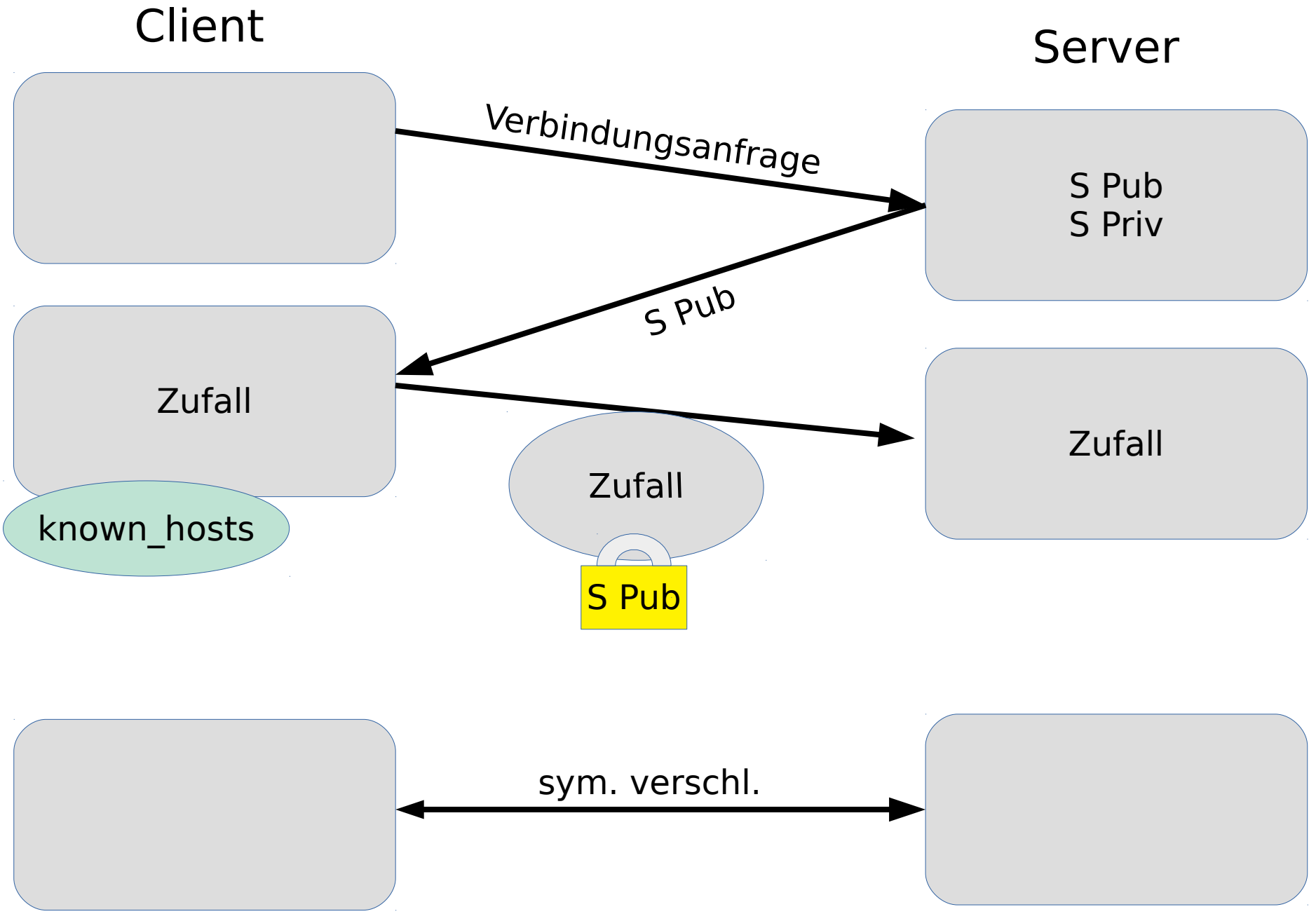


Zusammenfügen

digitale Unterschrift



ssh1


Client
Server
Verbindungsanfrage
S Pub
S Priv
S Pub
Zufall
Zufall
known_hosts
Zufall
S Pub
sym. verschl.

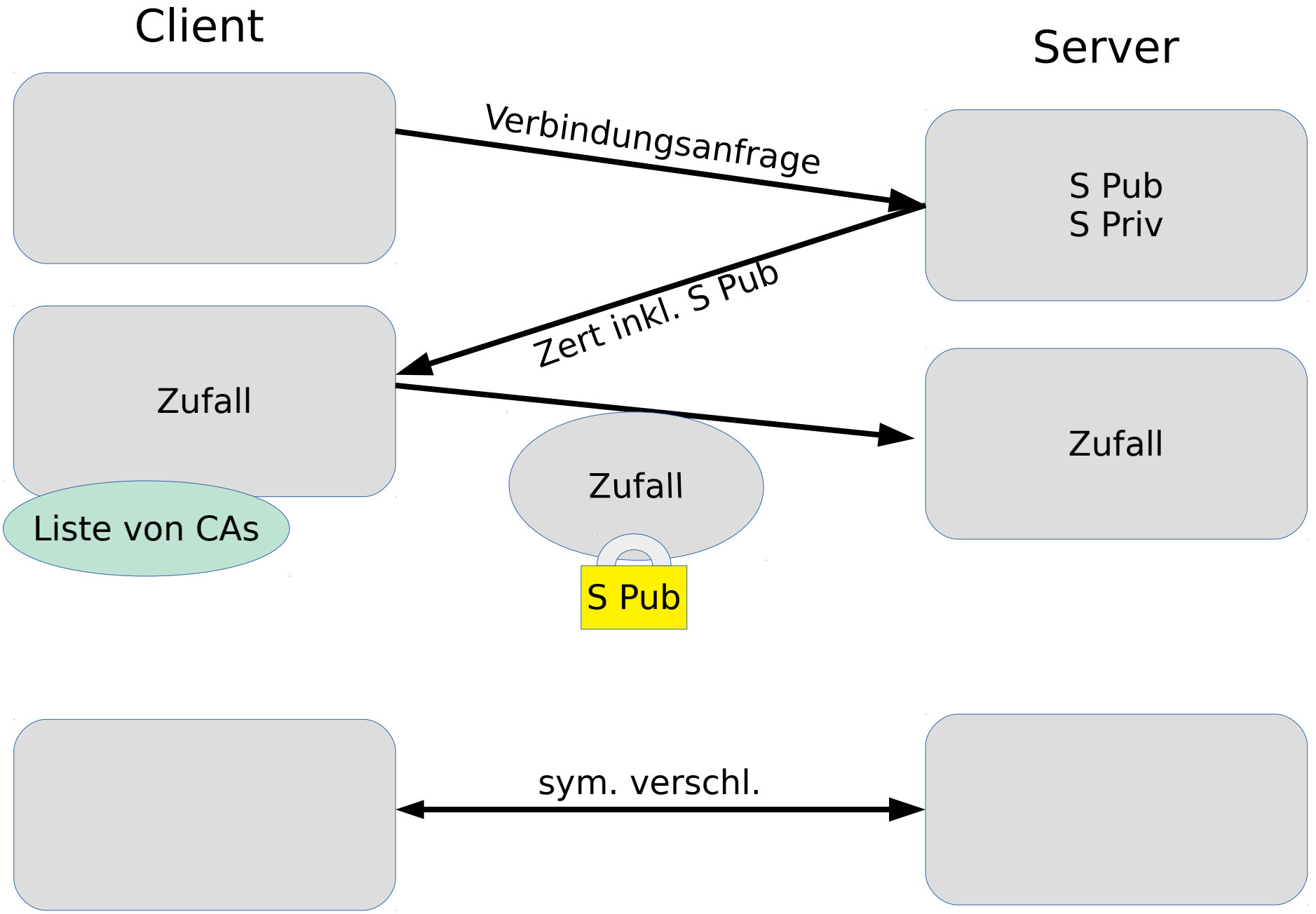
Zertifikate aka. Server Pass

Zertifikat

- Seriennummer
- Aussteller
- Gültig
- Subject Name
- Subject Publickey

- Zertifikats Unterschrift

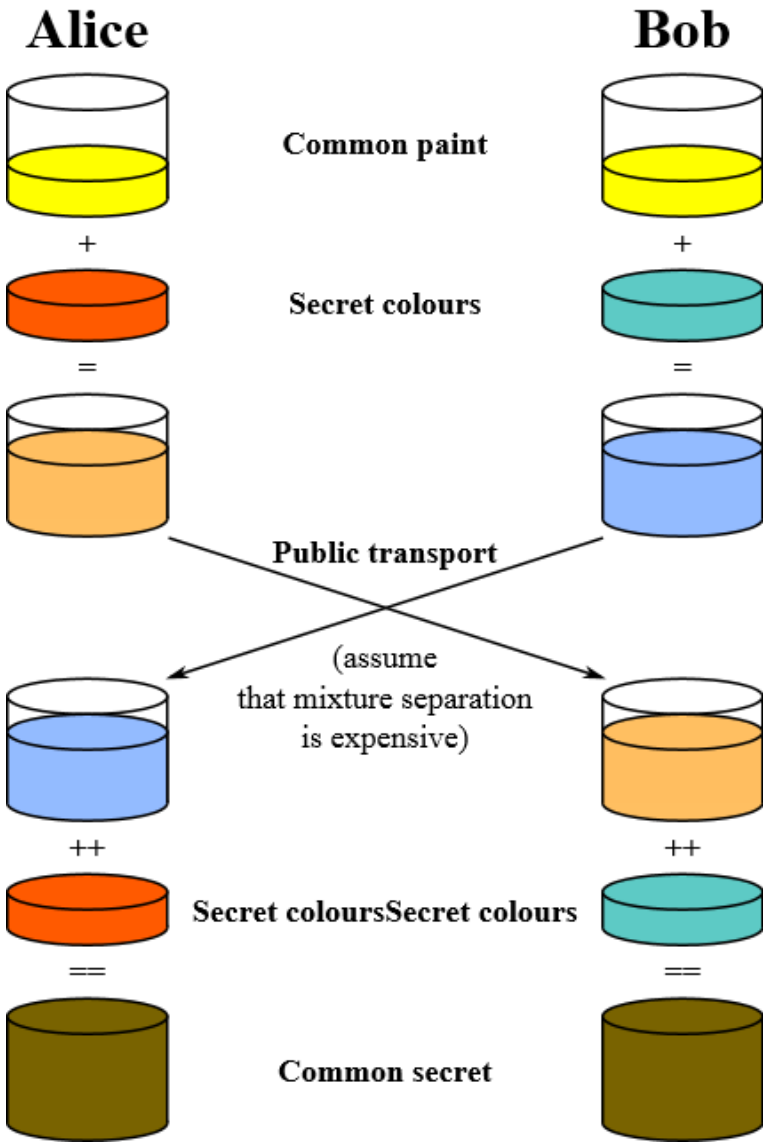
TLS (zu einfach)



Vielen Dank!
Fragen?

Diffie Hellmann

- Der aktuelle amerikanische Präsident



Quelle: https://de.wikipedia.org/wiki/Diffie-Hellman-Schlüsselaustausch