UNIVERSITY OF MANNHEIM

Kryptografische Alternativen zum Hardware Security Module (HSM)

Prof. Dr. Frederik Armknecht

Lehrstuhl Praktische Informatik IV: Dependable Systems Engineering

Disclaimer

- Ziele dieses Vortrages
  - Kryptografischen Funktionalitäten des HSM (Hardware Security Module)
  - Vorstellung und Besprechung möglicher Alternativen
  - Diskussionsgrundlage

- Keine Ziele des Vortrages
  - Kritik am1 beA
  - Konkrete Alternativvorschläge

Agenda

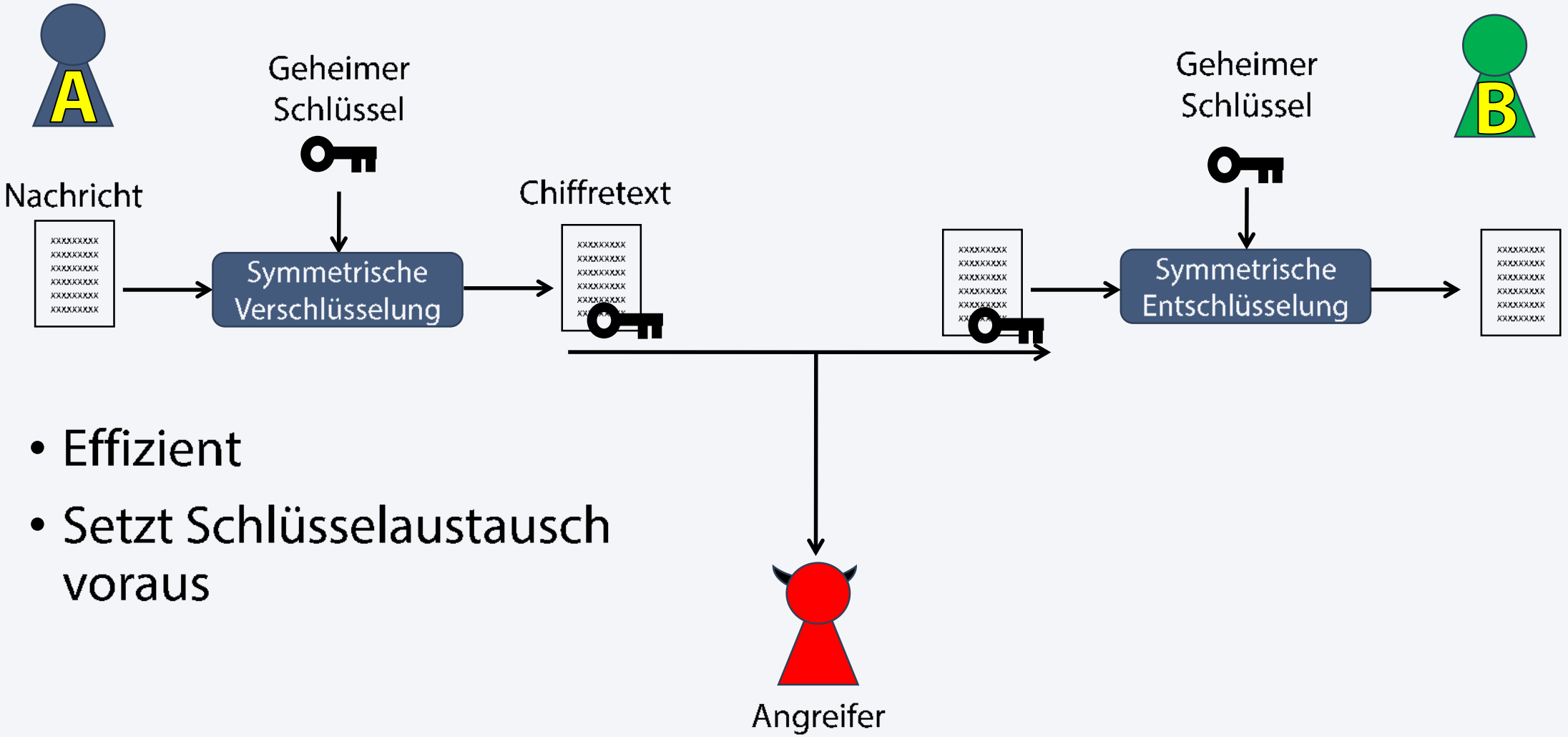
UNIVERSITY OF MANNHEIM

- Die Rolle des HSM
- Ansatz 1: Proxy Re-Encryption
- Ansatz 2: Secret Sharing
- Ansatz 3: Zertifikate
- Fazit

UNIVERSITY OF MANNHEIM

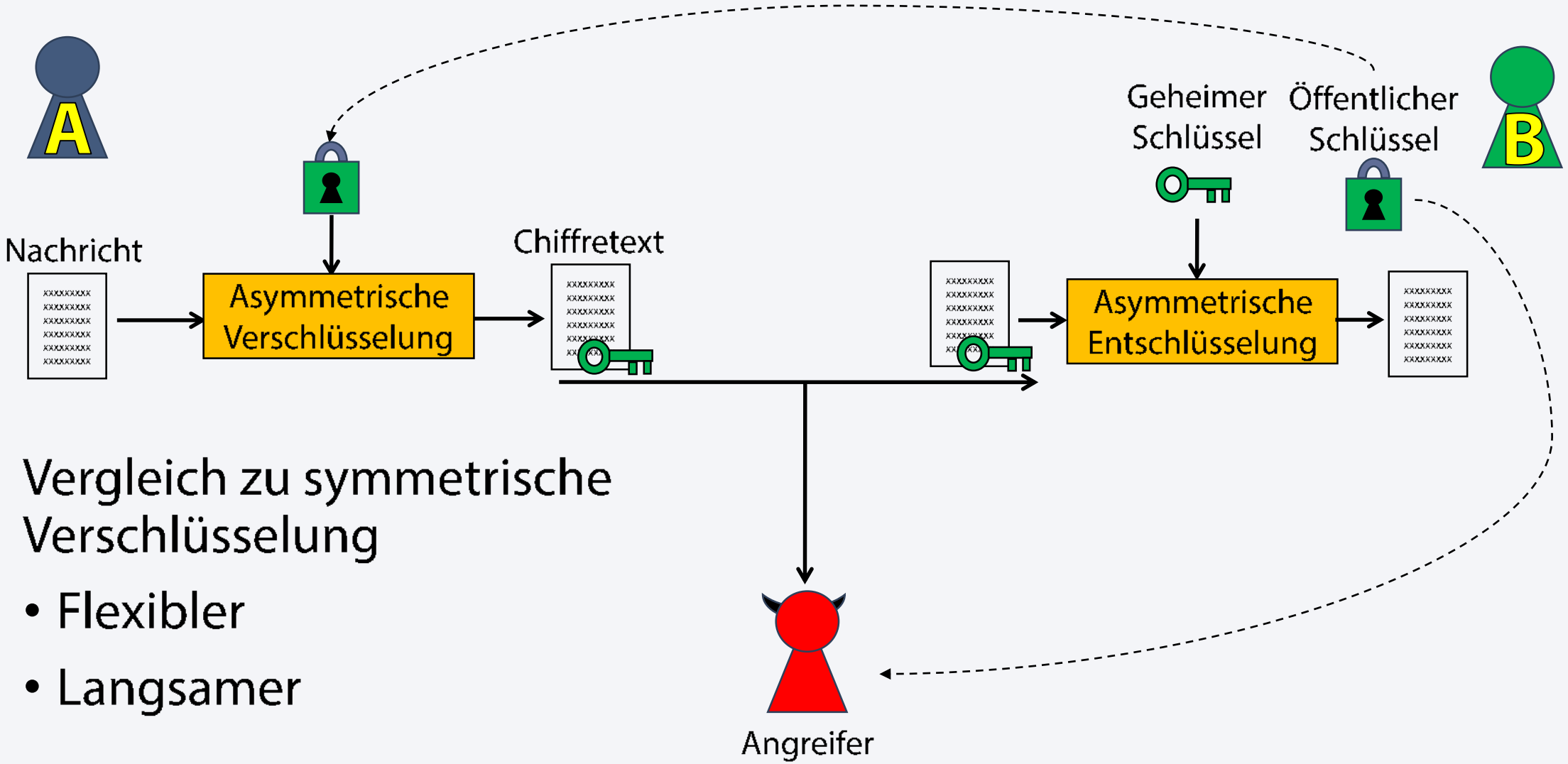
Die Rolle des HSM

Symmetrische Verschlüsselung



- Effizient
- Setzt Schlüsselaustausch voraus

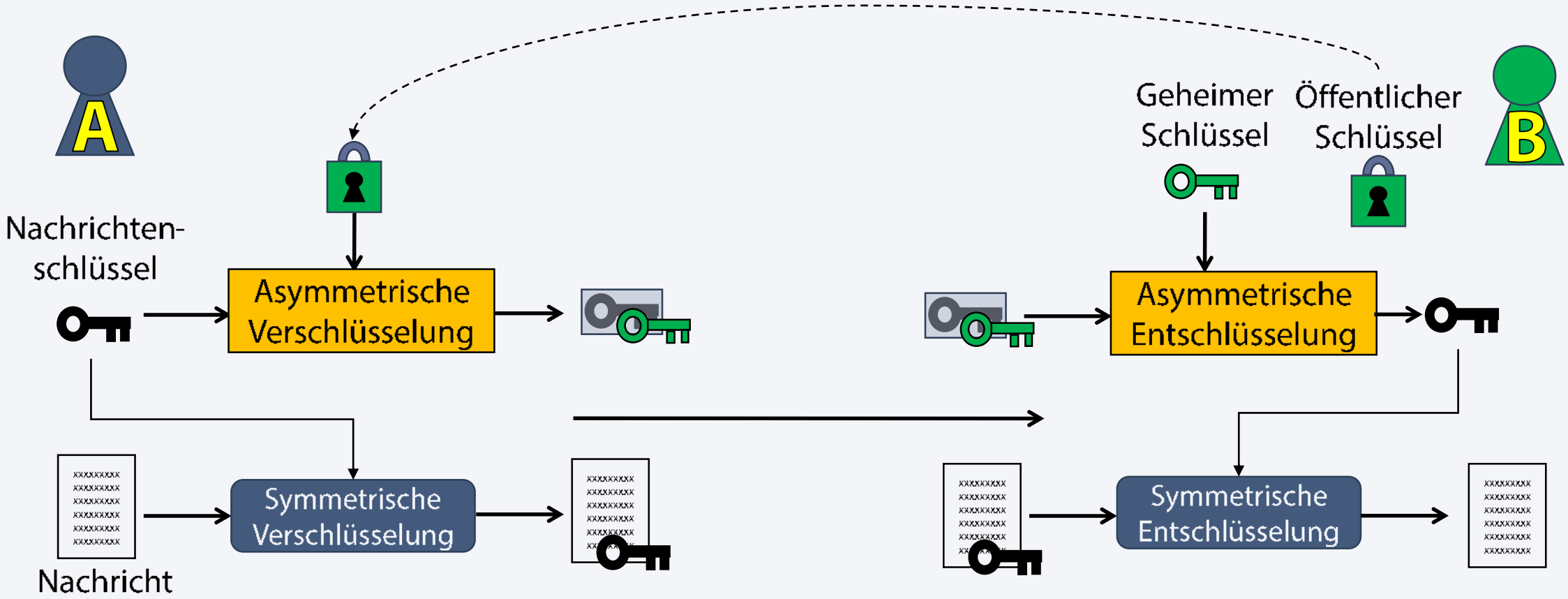
Asymmetrische Verschlüsselung



Vergleich zu symmetrische Verschlüsselung

- Flexibler
- Langsamer

Hybride Verschlüsselung

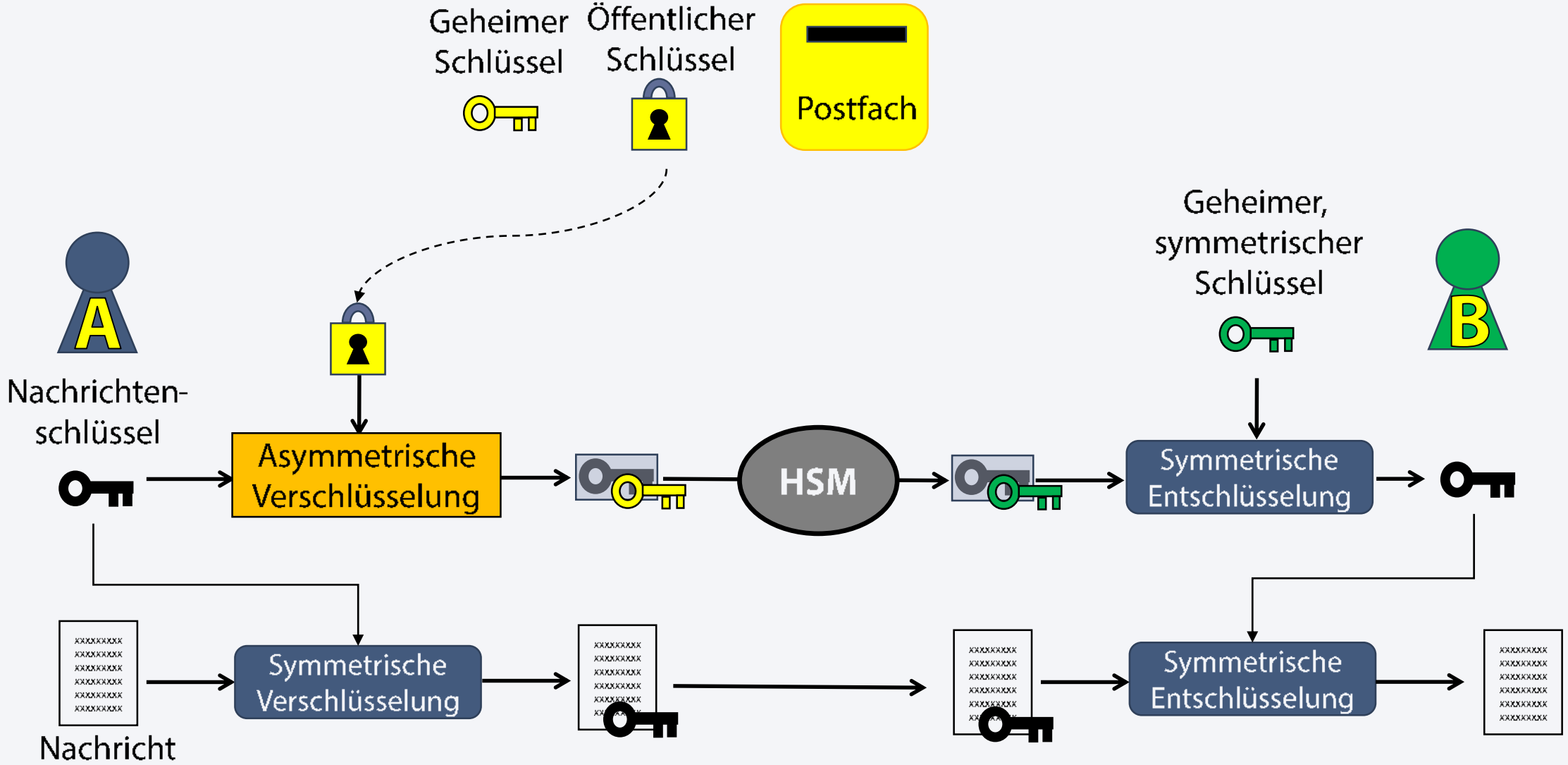


Rolle des HSM

1. Zugriffskontrolle
2. Umverschlüsselung
   - Involviert potentiell unterschiedliche Schlüssel
   - Öffentliche Schlüssel des neuen Empfängers
   - Geheimer Schlüssel des ursprünglichen Empfängers
   - Symmetrischer Schlüssel des neuen Empfängers
   - Temporäre Nachrichtenschlüssel
   - …

Im Folgenden Fokus auf Umverschlüsselung

Umverschlüsselung: Szenario

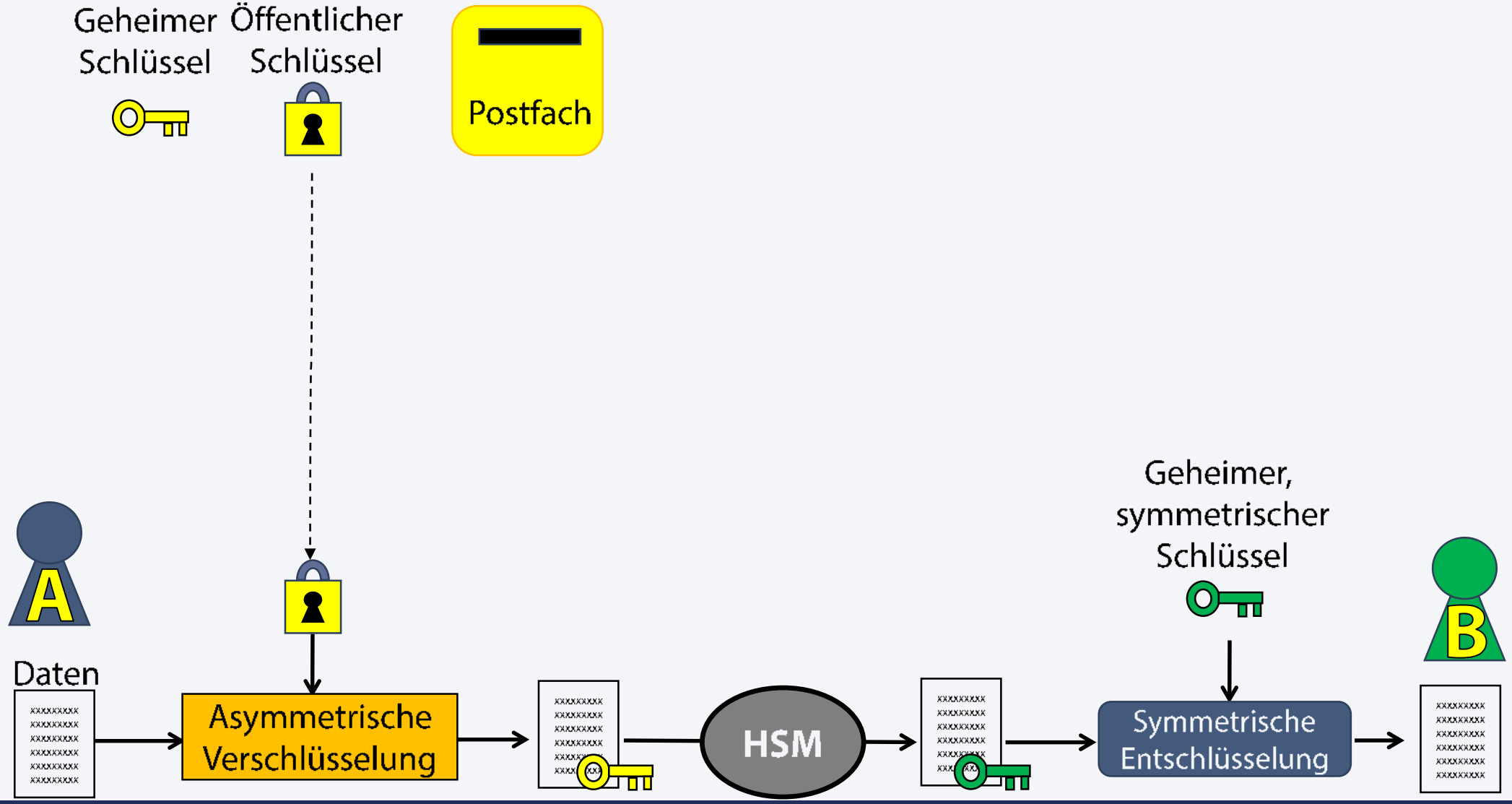


Ende-zu-Ende-Verschlüsselung?

UNIVERSITY OF MANNHEIM

- Wikipedia:
  - „Unter Ende-zu-Ende-Verschlüsselung (englisch „end-to-end encryption“, „E2EE“) versteht man die **Verschlüsselung übertragener Daten über alle Übertragungsstationen hinweg**.“
  - „**Nur die Kommunikationspartner** (die jeweiligen Endpunkte der Kommunikation) **können die Nachricht entschlüsseln**.“
- Dies ist hier nicht gegeben. Das HSM ist durch Umverschlüsselung auf einen bekannten Schlüssel in der Lage, die Daten letztendlich auch zu entschlüsseln.
- Aus Sicherheitssicht besteht die Verschlüsselung daher nur bis zum HSM und nicht bis zum endgültigen Empfänger.

Umverschlüsselung: reduziertes Szenario



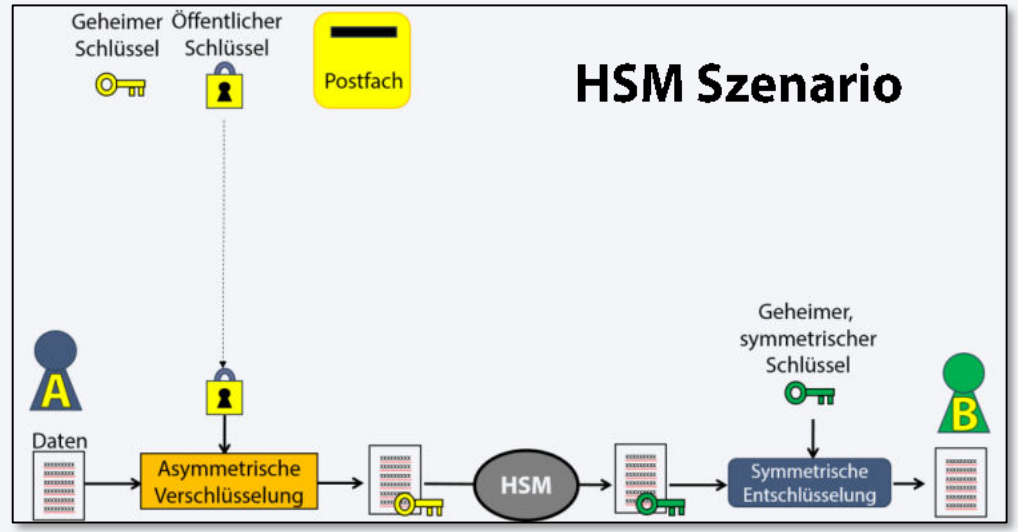
HSM: Mögliche Probleme

UNIVERSITY OF MANNHEIM

- Sicherheit
  - Es gibt kein 100% sicheres System
  - Sicherheit ergibt sich eher dadurch, dass der erwartete Aufwand, ein System anzugreifen, unverhältnismäßig hoch ist zum erwarteten „Nutzen“
  - Die Anhäufung sensibler Daten (Schlüssel) in einem System (HSM) erhöht diesen „Nutzen“ und macht das HSM zu einem besonderen Angriffsziel
- Zuverlässigkeit
  - HSM stellt „Single Point of Failure“ dar
  - Wenn dieses ausfällt oder keine ausreichenden Kapazitäten bereitstellt, wird der gesamte Ablauf behindert oder fällt sogar aus
- Konsequenz: eine Verteilung der Rollen des HSM kann sowohl Sicherheit als auch Zuverlässigkeit erhöhen

Ansatz 1: Proxy Re-Encryption

Proxy Re-Encryption: Szenario



Geheimer Schlüssel

Öffentlicher Schlüssel

C

A

Daten

Asymmetrische Verschlüsselung

Proxy

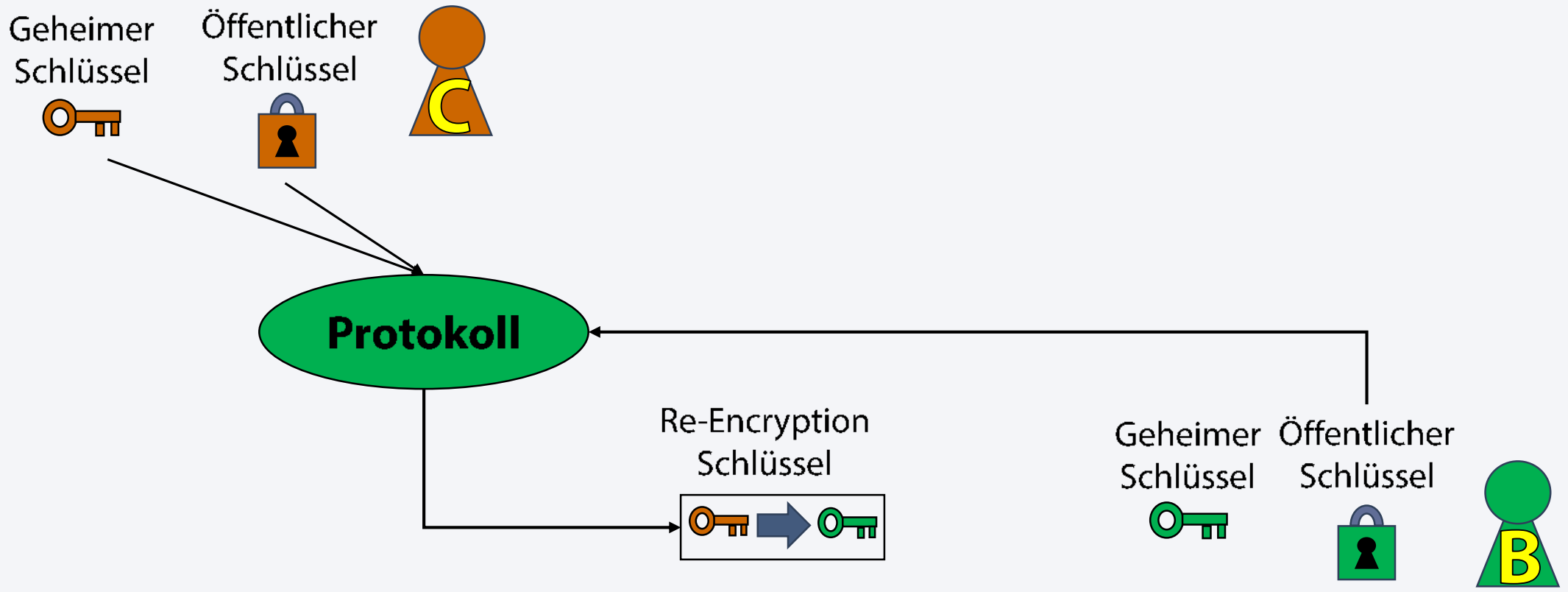
Geheimer Schlüssel

Öffentlicher Schlüssel

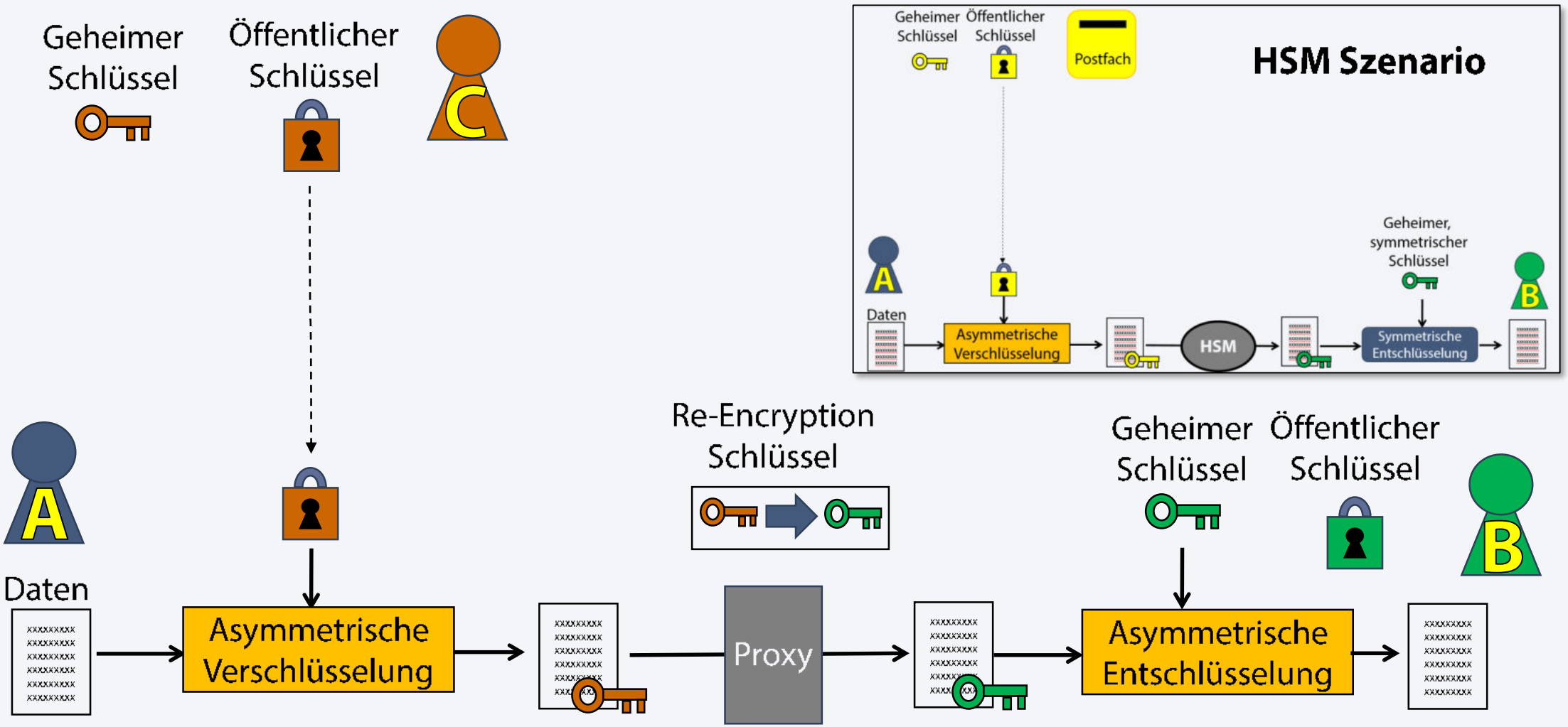
B

Asymmetrische Entschlüsselung

Proxy Re-Encryption: Ablauf (1)



Proxy Re-Encryption: Ablauf (2)



Stand der Forschung

Schemes	Properties								
	Unidirectional	Multi-use	Key-private	Transparent	Key-optimal	Non-interactive	Non-transitive	Temporary	Collusion-resistant
Blaze [6]	×	✓	×	✓	✓	×	×	×	×
Ateniese [12]-1	✓	×	✓	✓	✓	✓	✓	×	weak
Ateniese [12]-2	✓	×	✓	✓	✓	✓	✓	×	weak
Ateniese [13]	✓	×	✓	✓	✓	✓	✓	✓	weak
Canetti [15]-1	×	✓	×	✓	✓	×	×	×	×
Canetti [15]-2	×	✓	×	✓	✓	×	×	×	×
Libert [30]-1	✓	×	✓	×	✓	✓	×	×	✓
Libert [30]-2	✓	×	✓	×	✓	✓	×	✓	✓
Deng [29]	×	×	✓	×	✓	×	×	×	×
Shao [31]-1	✓	×	✓	✓	×	✓	✓	×	✓
Shao [31]-2	✓	×	✓	✓	×	✓	✓	✓	✓
Chow [36]	✓	×	✓	✓	✓	✓	✓	×	✓
Canard [73]	✓	×	✓	✓	✓	✓	✓	×	✓
Shao [43]	✓	✓	✓	×	✓	✓	✓	×	✓
Isshiki [46]	✓	×	✓	×	✓	✓	✓	×	✓

Quelle: Quin et al.: *„A Survey of Proxy Re-Encryption for Secure Data Sharing in Cloud Computing „*

- **Non-interactive:** Geheimer Schlüssel des Empfängers muss nicht offengelegt werden
- **Temporary:** Entschlüsselungsrechte können entzogen werden
- **Collusion-resistant:** Proxy und ursprünglicher Empfänger können nicht geheimen Schlüssel des neuen Empfängers bestimmen

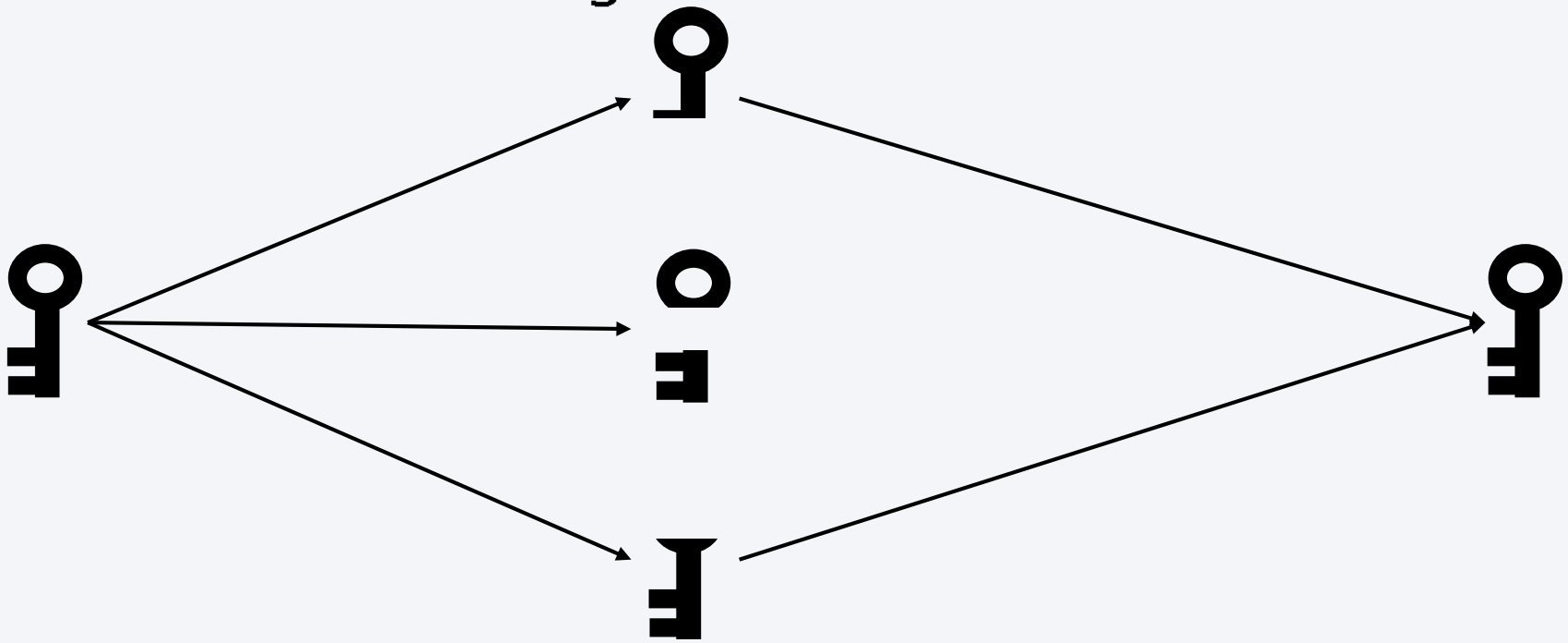
Diskussion

- Vorteile
  - Proxy muss nicht vertraut werden (HSM schon)
- Nachteile
  - (Beschränkung auf asymmetrische Verschlüsselungsverfahren)
  - Ursprünglicher Empfänger muss involviert werden
  - Aufwand?
- Benennung von Vertreter/Mitarbeiter
  - Erfordert die Involvierung des ursprünglichen Empfängers (hier „B“)
  - „B“ kann Vertreter „C“ benennen, indem er den entsprechenden Re-Encryption Schlüssel berechnet und bspw. diesen „C“ zur Verfügung stellt

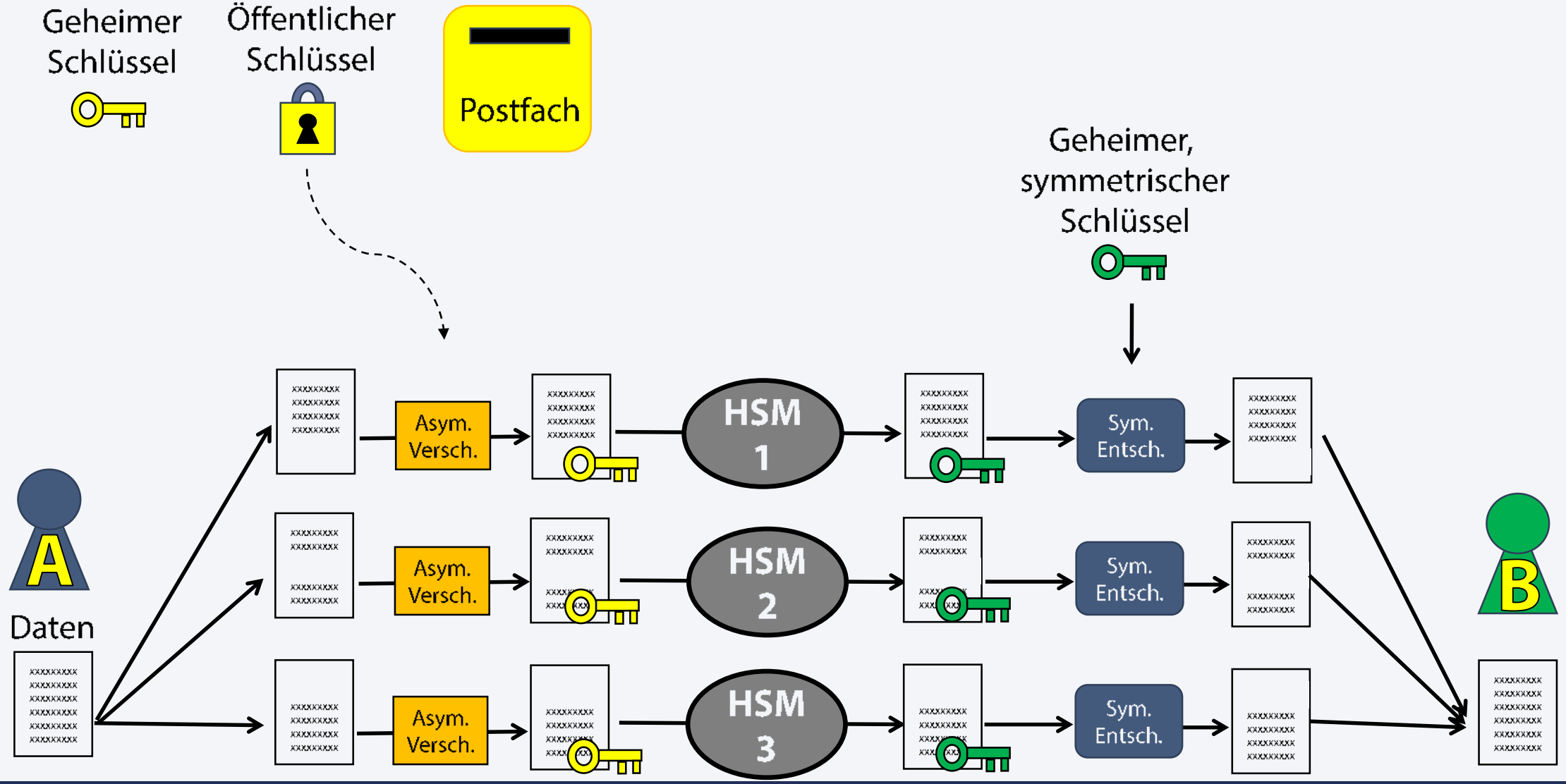
Ansatz 2: Secret Sharing

Prinzip

- Geheimnis wird auf n Shares aufgeteilt
- Kann aus k Shares rekonstruiert werden
- Weniger als k Shares ⇒ keine Information über Geheimnis
- Beispiel: 2-aus-3 Secret Sharing



Mögliche Anwendung

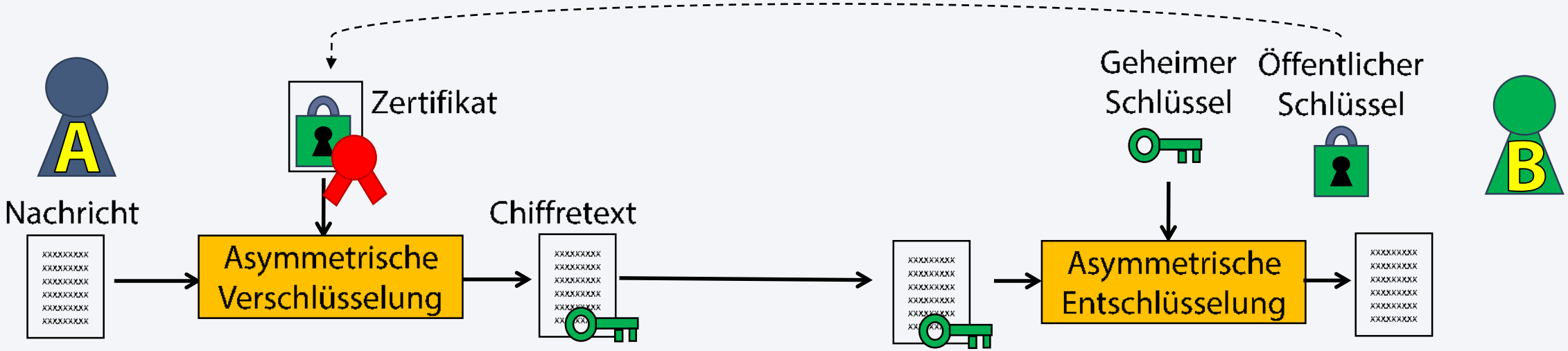


Diskussion

- Vorteile
  - Einzelnem HSM muss nicht vertraut werden
  - Anzahl Shares kann u.U. erweitert/reduziert werden
  - Sicherheit erhöhen durch unterschiedliche Schlüssel pro HSM
- Nachteile
  - Aufwand?
  - Mindestanzahl an vertrauenswürdigen HSMs
  - Zuverlässigkeit?
- Benennung von Vertreter/Mitarbeiter
  - Funktioniert wie bisher mit dem Unterschied, dass diese Information allen HSMs mitgeteilt werden müsste.

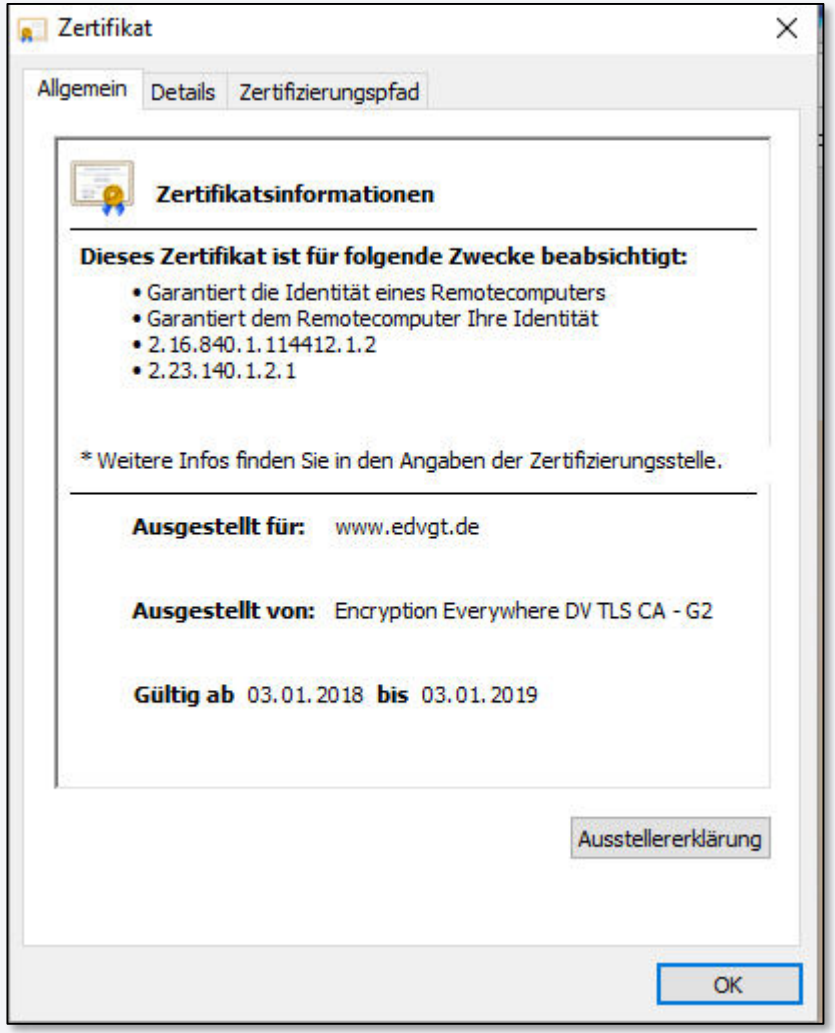
Ansatz 3: Zertifikate

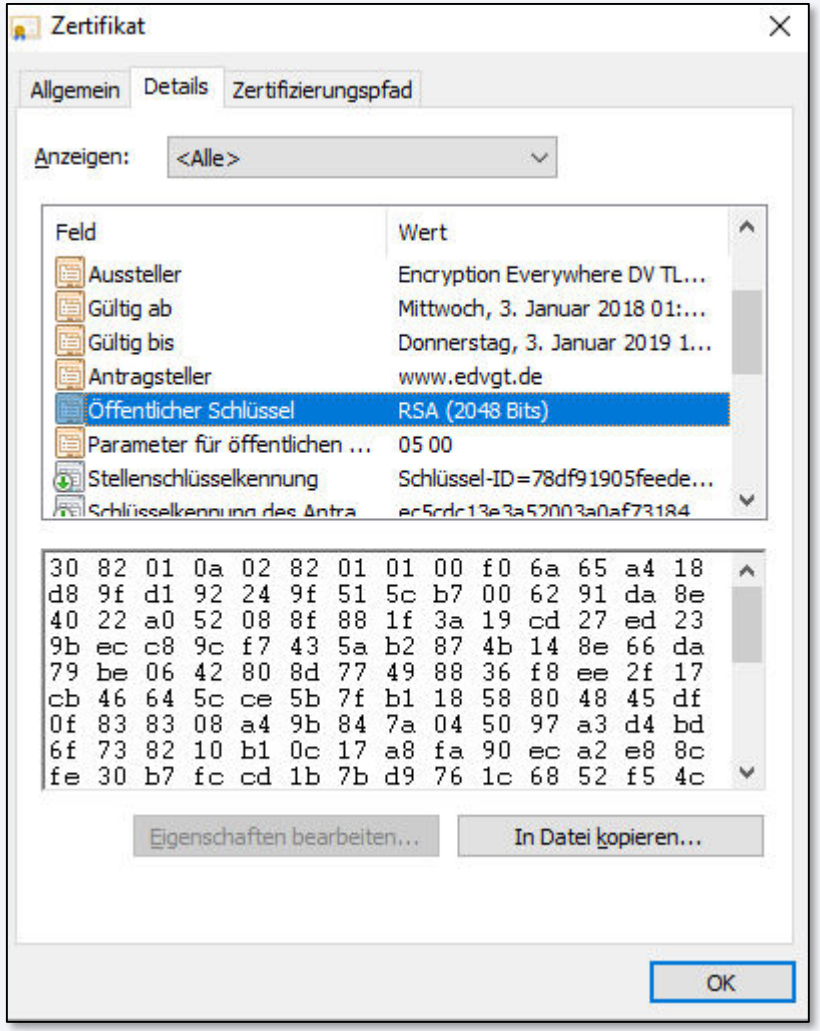
Zertifikat: Prinzip



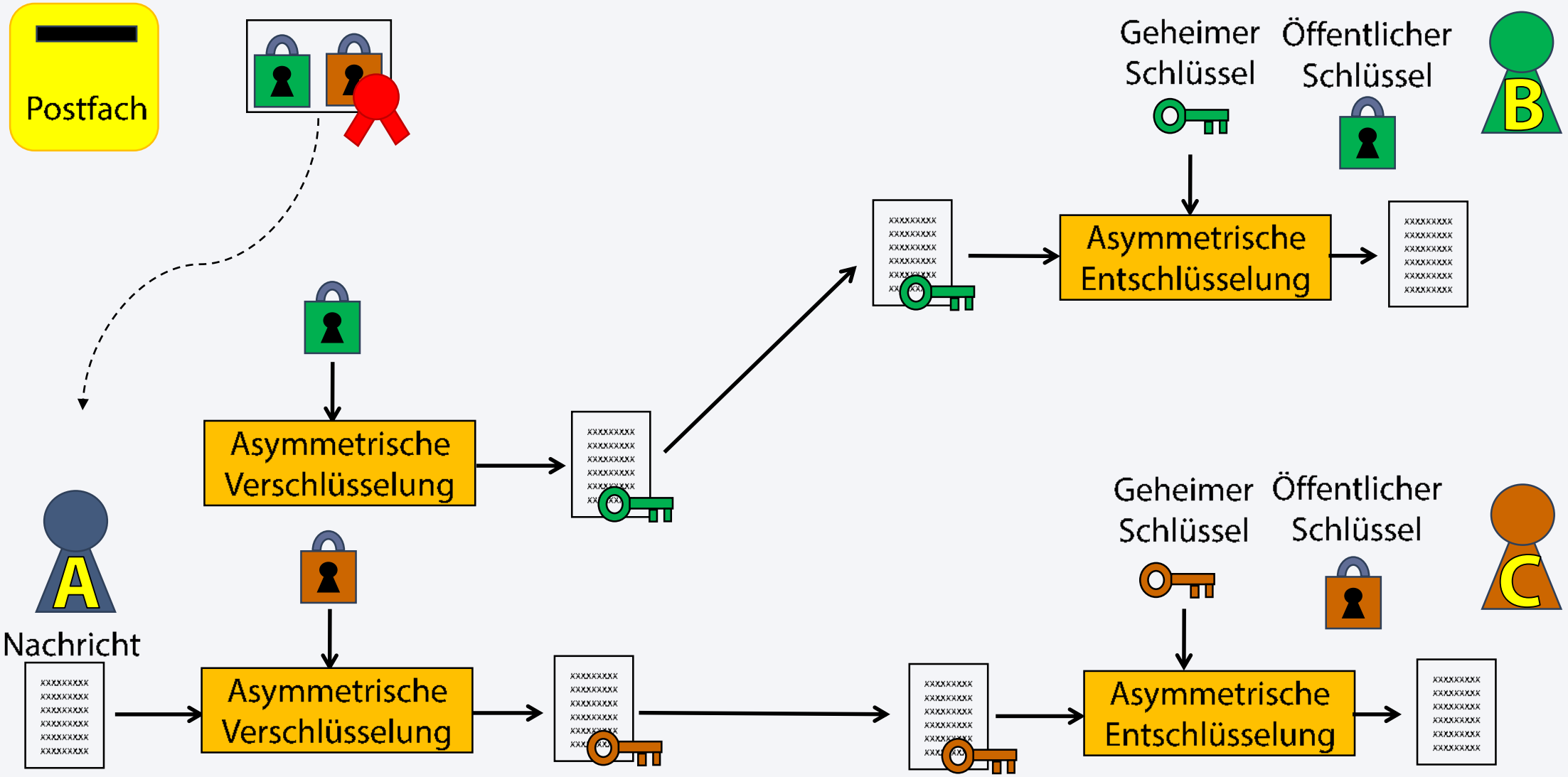
- Bestätigt Gültigkeit des Schlüssels
  - Ersteller
  - Ablaufdatum
  - Widerruf

Zertifikat: Beispiel





Mögliche Anwendung



Diskussion

- Zertifikat
  - Gibt alle gültigen Mitglieder zum aktuellen Zeitpunkt an
  - Sollte ohnehin abgefragt werden (Bsp. Widerruf)
- Vorteile
  - Echte Ende-zu-Ende-Verschlüsselung
  - Gängige Praxis
  - Kein HSM notwendig
- Nachteile
  - Empfänger nicht erreichbar, verstorben, etc.
  - Höherer Aufwand für Sender
- Benennung von Vertreter/Mitarbeiter
  - Vertreter etc. würden direkt im aktuell gültigen Zertifikat benannt werden. Genauer: diese Zusatzinformation wird mit dem Zertifikat mitgeliefert und mittels eines im Zertifikat genannten Schlüssels signiert
  - Verschlüsselung wird dann direkt für alle Empfänger durchgeführt

Mögliche Lösung

- Hinterlegen des Schlüssels an einem sicheren Ort
- Alternative: Secret Sharing

Fazit

Fazit

- Kryptografische Rolle des HSM
  - Umverschlüsselung von Daten (insbs. Schlüssel)
  - Generell: Verwendung eines HSM problematisch
- Mögliche kryptografische Alternativen
  - Proxy Re-Encryption
  - Secret Sharing
  - Zertifkate
- Beurteilung
  - Ansätze haben unterschiedliche Vor- und Nachteile
  - Kommen allesamt ohne HSM aus
  - Falls beA grundlegend überarbeitet wird, sollten diese in Betracht gezogen werden (falls nicht bereits geschehen)