Berlin, 10.06.2025

HOMOMORPHE VERSCHLÜSSELUNG
EINE KRYPTOLOGISCHE PERSPEKTIVE

Dr. Matthias Minihold (Referatsleiter Kryptologie)
Agentur für Innovation in der Cybersicherheit GmbH

Das Cloud-Zeitalter

„Cloud Computing ist das Rückgrat der Digitalisierung“

Digitalisierung im Cloud-Zeitalter bedeutet:

- Exponentieller **Datenzuwachs** (Privat, Medizinisch, Verwaltung, …)
- Verlagerung **sensibler Daten in gemeinsam genutzte Clouds**

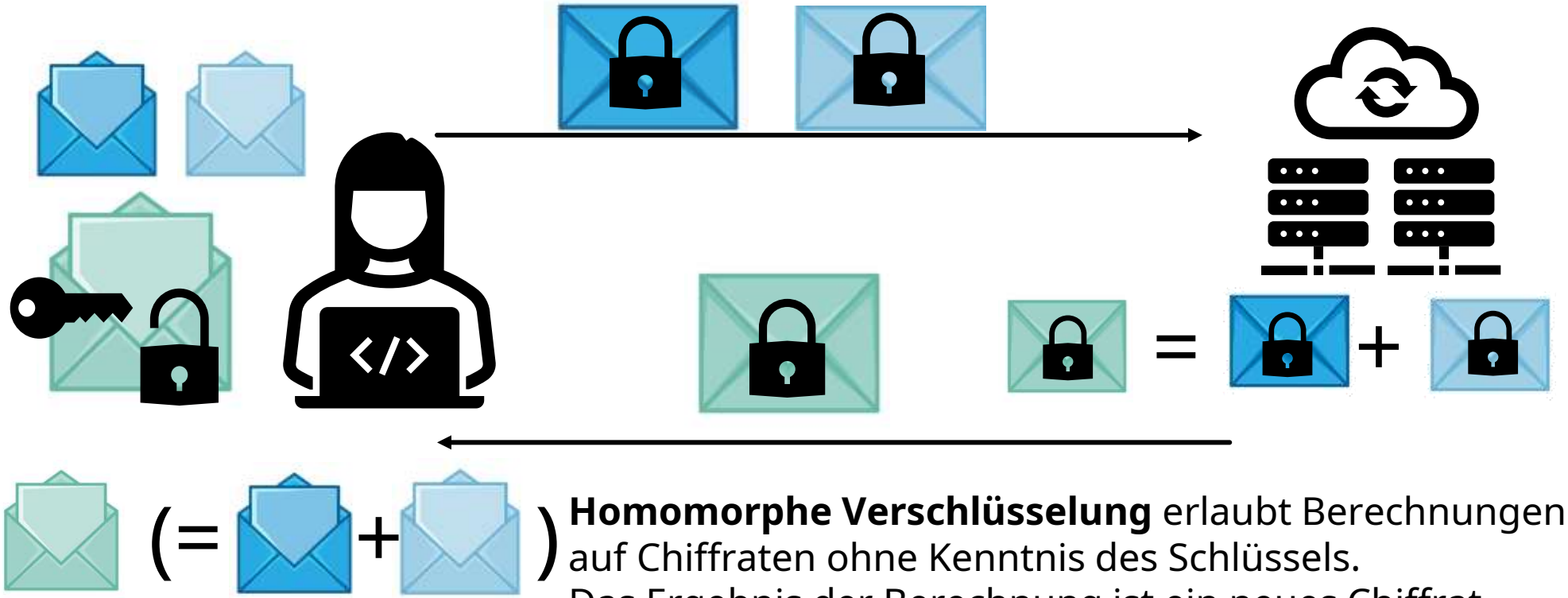
Anforderungen: Vertraulichkeit, Integrität und Verfügbarkeit

Kernfrage: Wie bleibt **Sicherheit und Datenschutz** gewahrt?

🎯 Ziel: **Sichere Speicherung, Nutzung und Verarbeitung** in der Cloud.

(VOLL)HOMOMORPHE VERSCHLÜSSELUNG

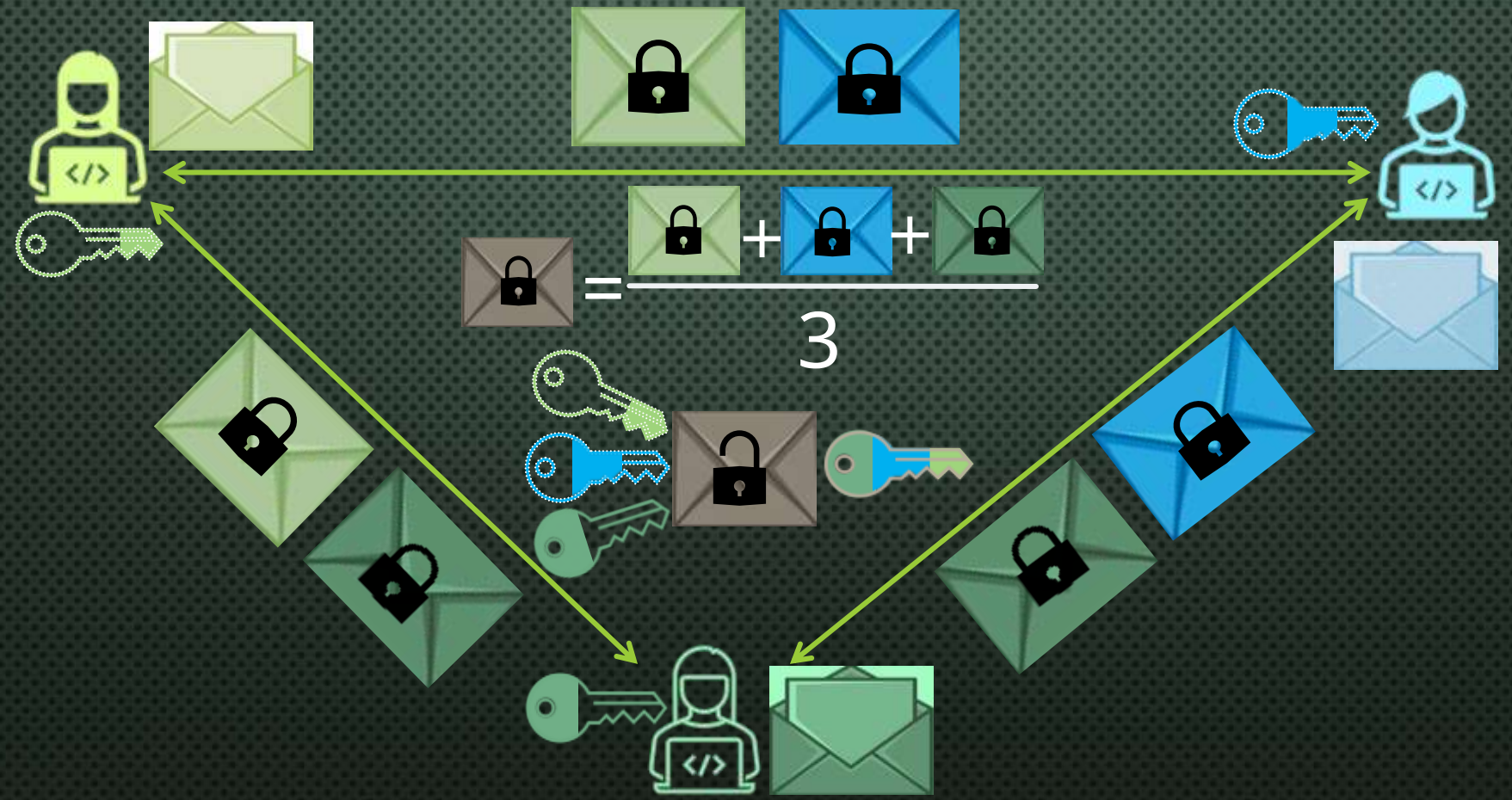
SCHEMA / PROTOKOLLABLAUF



Homomorphe Verschlüsselung erlaubt Berechnungen auf Chiffraten ohne Kenntnis des Schlüssels.
Das Ergebnis der Berechnung ist ein neues Chiffrat.

MULTIPARTY COMPUTATION

ANDERE SZENARIEN PROFITIEREN VON MPC (Z.B.: VIA SECRET SHARING)



Homomorphe Verschlüsselung

Varianten

- Partially Homomorphic Encryption (PHE): ermöglicht Anwendung **einer** mathematischen Operation auf den verschlüsselten Daten.

  Entweder additiv homomorph **oder** multiplikativ homomorph

- Somewhat Homomorphic Encryption (SHE): ermöglicht (begrenzte) Anwendung **mehrerer** mathematischer Operationen auf den Daten.

- Fully Homomorphic Encryption (FHE): ermöglicht **beliebig oftmalige** Anwendung mathematischer Operationen auf verschlüsselten Daten.

BEGRIFFSERKLÄRUNG HOMOMORPHISMUS

DEFINITION: GRUPPE

Eine Gruppe ist ein Paar $(G,\circ)$. G ist eine Menge und $\circ$ eine zweistellige Verknüpfung $\circ: G \times G \to G$ und $(a,b) \mapsto a \circ b$.

mit den folgenden Eigenschaften:

- *Assoziativität* $\forall\, a,b,c \in G : (a \circ b) \circ c = a \circ (b \circ c)$
- *neutrales Element:* $\exists\, e \in G\ \forall a \in G : a \circ e = e \circ a = a$
- *inverses Element:* $\forall a \in G\ \exists\, a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$

Eine Gruppe heißt abelsch, wenn das Kommutativgesetz gilt:

$$\forall\, a,b \in G :\ a \circ b = b \circ a$$

BEGRIFFSERKLÄRUNG HOMOMORPHISMUS

DEFINITION: GRUPPENHOMOMORPHISMUS

Seien $(G,\circ)$ und $(F,\diamond)$ Gruppen, dann heißt die Abbildung $f\colon G \longrightarrow F$ Gruppenhomomorphismus, wenn $\forall\, a,b \in G$ gilt:

$$f(a \circ b) = f(a) \diamond f(b)$$

Beispiel: Die Exponentialfunktion $f(x) = e^x$ ist ein *Homomorphismus* der additiven Gruppe der reellen Zahlen in die multiplikative Gruppe der positiven reellen Zahlen. Es gilt: $f(a+b) = e^{a+b} = e^a e^b = f(a)f(b)$.

Modulare Arithmetik

Zahlenbeispiel

Modulare Arithmetik basiert auf „Division mit Rest“;
$a \; mod \; p = r$ heißt, dass beim Teilen von a durch p Rest r bleibt.

$$69 \; mod \; 11 \; = 3 \qquad 69 \; mod \; 10 \; = 9$$

$$69 = 6 * 11 + 3 \qquad 69 = 6 * 10 + 9$$

Der konkrete Faktor ist egal!

Der konkrete Faktor ist egal!

Homomorphe Verschlüsselung

Ver- und Entschlüsselung

Um ein Bit $m \in \{0,1\}$ zu verschlüsseln, wählt man ganze Zahlen q und p zufällig, mit der Bedingung $2r < p - 1$ und definieren die Ganzzahl c als Chiffretext wie folgt:

$$c = pq + 2r + m$$

Der Rest c $mod\ p$ hat damit die gleiche Parität wie der Klartext m.

Entschlüsselung: Mit dem geheimen Schlüssel p bekommt man den Klartext:

$$c\ (mod\ p) = 2r + m\ und\ somit\colon\ m = \big(c\ (mod\ p)\big)(mod\ 2)$$

HOMOMORPHE VERSCHLÜSSELUNG - ADDITION

ZAHLENBEISPIEL

WIR BETRACHTEN DIE **SUMME** ZWEIER CHIFFRETEXTE

$$c_1 = pq_1 + 2r_1 + m_1,\ c_2 = pq_2 + 2r_2 + m_2,$$

$$c_1 + c_2 = p(q_1 + q_2) + 2(r_1 + r_2) + (m_1 + m_2).$$

ENTSCHLÜSSELUNG: MIT DEM GEHEIMEN SCHLÜSSELS p KANN MAN DIE SUMME ENTSCHLÜSSELN:

$$(c_1 + c_2)\ (mod\ p) = 2(r_1 + r_2) + (m_1 + m_2),$$
$$m_1 + m_2 = \big((c_1 + c_2)(mod\ p)\big)(mod\ 2).$$

MIT DER RANDBEDINGUNG: $2(r_1 + r_2) < p - 2 \xrightarrow{\text{D. H.}} r_i < \frac{p-2}{4}$.

HOMOMORPHE VERSCHLÜSSELUNG - ADDITION

ZAHLENBEISPIEL

$c_1 = pq_1 + 2r_1 + m_1,$

$c_2 = pq_2 + 2r_2 + m_2,$

$c_1+c_2 = p(q_1 + q_2) + 2(r_1 + r_2) + (m_1+m_2).$

Beispiel: $c_1 = 11 * 6 + 4 * 2 + 1 = 75,$

$c_2 = 11 * 5 + 3 * 2 + 0 = 61,$

$c_1+c_2 = 134 = 11(6 + 5) + (4 + 3)2 + (1 + 0) = 121 + 14 + 1.$

DER GEHEIME SCHLÜSSEL SEI $p = 19,$ $\xrightarrow{\text{D. H.}}$ $r_i < \frac{17-2}{4} = 4.25,$ *SEIEN* $r_1 = 4, r_2 = 3,$

UND DIE NACHRICHTENBITS GEGEBEN ALS $m_1 = 1$ UND $m_2 = 0.$

ENTSCHLÜSSELUNG: MIT DEM SCHLÜSSEL $p = 19$ KANN MAN DIE SUMME BERECHNEN.

$(c_1+c_2)\ (mod\ p) = 2(r_1 + r_2) + (m_1+m_2),$

$m_1 + m_2 = \big((c_1+c_2)(mod\ p)\big)(mod\ 2).$

Beispiel: $134\ (mod\ 19) = 7 * 19 + 1\ (mod\ 19) = 1,$

$m_1+m_2 = 1 + 0 = 1 = 1\ (mod\ 2).$

HOMOMORPHE VERSCHLÜSSELUNG - MULTIPLIKATION

ZAHLENBEISPIEL

WIR BETRACHTEN DAS **PRODUKT** ZWEIER CHIFFRETEXTE

$$c_1 = pq_1 + 2r_1 + m_1, \quad c_2 = pq_2 + 2r_2 + m_2,$$

$$c_1c_2 = p(q_1q_2p + 2q_1r_2 + 2q_2r_1 + q_1m_2 + q_2m_1) + 2(2r_1r_2 + m_1r_2 + m_2r_1) + (m_1m_2).$$

ENTSCHLÜSSELUNG: MIT DEM GEHEIMEN SCHLÜSSEL p KANN MAN DAS PRODUKT ENTSCHLÜSSELN:

$$(c_1c_2)\ (mod\ p) = 2(2r_1r_2 + m_1r_2 + m_2r_1) + (m_1m_2),$$

$$m_1m_2 = \big((c_1c_2)(mod\ p)\big)(mod\ 2).$$

ES GILT DIE RANDBEDINGUNG: $2(2r_1r_2 + r_2 + r_1) < p - 1 \xrightarrow{\text{D. H.}} r_i < \frac{\sqrt{p}-1}{2}$.

Fully Homomorphic Encryption (FHE)
Bootstrapping

- **Homomorphic Encryption** erlaubt **begrenzte** Anzahl an Rechenoperationen.
- Anwendung homomorpher Operationen führt zu **Fehlerwachstum im Chiffrat**.
- **Hauptinnovation** für FHE war die Einführung der **Bootstrapping-**Technik, die **Chiffretexte auffrischt** und das **Fehlernivaeu verringert,** um weiterzurechnen.
- Durch **Fully Homomorphic Encryption** können **mathematische Operationen beliebig oft** auf FHE-verschlüsselten Datensätzen angewendet werden.

Herausforderungen für Encrypted Computing

Skalierung, Vertrauen und Rechtslage

1. …bezüglich Effizienz & Skalierung

 Homomorphe Verschlüsselung: **algorithmisch** Effizienz **steigern**

 Sichere Mehr-Parteien Berechnung: **Kommunikationsaufwand senken**

2. …bezüglich Vertrauenswürdige Umgebung & Kryptoaktualität

 Notwendigkeit **auditierbarer & offener Implementierungen**

 Mathematische Erkenntnisse, **Kryptanalyse** & Seitenkanalangriffe

3. …bezüglich Rechtslage & Datenflüsse

 Internationale **Cloudanbieter** ↔ **Datenschutz** europäisch & national