Homomorphe Verschlüsselung – Theorie und Praxis

Marvin Hahn
Julian van Dyken

Exposé für die Lehrveranstaltung
Spezielle Verfahren der IT-Sicherheit

im Studiengang
Informatik

Hochschule Emden/Leer
Prof. Dr. Patrick Fehlke
M.Eng. Frederik Gosewehr

7. Oktober 2025

Inhaltsverzeichnis

1 Einleitung

Normalerweise muss man verschlüsselte Daten entschlüsseln, um darauf Operationen ausführen zu können. Nutzende müssen daher einen Teil ihrer Privatsphäre einbüßen, damit die Daten verarbeitet werden können. Dies stellt bei sensiblen Daten ein Risiko dar. Mit homomorpher Verschlüsselung gibt es die Möglichkeit, solche Operationen direkt auf den verschlüsselten Daten durchzuführen. Dadurch bleiben sensible Informationen geschützt. Nutzende bekommen das Ergebnis in verschlüsselter Form zurück und können es dann selber entschlüsseln. Es ist also so, als ob die Berechnungen direkt auf den entschlüsselten Daten durchgeführt wurden. Nützlich ist sowas beispielsweise beim Sammeln von Stimmen oder auch bei Cloud-Computing.

2 Das Ziel der Ausarbeitung

Das Ziel unserer Ausarbeitung ist, die grundlegende Theorie hinter homomorpher Verschlüsselung zu erklären und deren Anwendung in der Praxis. Wir differenzieren zwischen den und erläutern die verschiedenen Arten der homomorphen Verschlüsselung. Dazu werden wir eine strukturierte Übersicht der aktuellen Verfahren erarbeiten und Beispiele für praktische Anwendungen aufzeigen. Diese werden dann von uns auf Basis der aktuellen Forschung – insbesondere hinsichtlich zukünftigen Quantencomputings – bewertet.

3 Kern der Arbeit

Der Kern unserer Arbeit wird auf der Praxis homomorpher Verschlüsselung liegen.

4 Forschungsfragen

- **Was ist die Kernidee hinter homomorpher Verschlüsselung?**
- **Welche Arten von homomorpher Verschlüsselung gibt es?**
  - Welche Vor- und Nachteile bringen diese?
  - Wie funktioniert die Mathematik dahinter?
- **Wie kann man homomorphe Verschlüsselung in der Praxis einsetzen?**
  - Wo ist es eventuell schon im Einsatz?
  - Wie sehen die Entwicklungstendenzen dieser Technik(en) aus?
  - In welchen thematischen Gebieten lohnt sich homomorphe Verschlüsselung?
- **Ist homomorphe Verschlüsselung post-quanten-sicher?**

5 Theorien

- **Welche Theorien gibt es?**
  - $E(m_1) \bigstar E(m_2) = E(m_1 \bigstar m_2), \quad \forall m_1, m_2 \in M.$
  - Arten: partial (partiell), somewhat (eingeschränkt), full (vollständig)
  - Squashing
  - Bootstrapping
- **Beispielhafte Verfahren**
  - *Partiell homomorphe Verschlüsselung*
    - RSA
    - Goldwasser-Micali
    - ElGamal
    - Benaloh
    - Paillier
  - *Eingeschränkt homomorphe Verschlüsselung*

        * BGN
    - *Vollständig homomorphe Verschlüsselung*
        * Ideale gitterbasierte Schemen
        * Schemen über Integer
        * LWE(Learning With Errors)-basierte Schemen
        * NTRU-Like FHE Schemes

- **Anknüpfungspunkte an bekannten Verfahren**
    - RSA
    - ElGamal

6 Methodisches Vorgehen

- **Literaturrecherche**
    - Suche in wissenschaftlichen Datenbanken (SpringerNature)

7 Literatur

Literatur

Scott, Chacon und Straub Ben (2010). *Pro Git*. 2. Aufl. Apress.