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

5. 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. Dabei gehen wir insbesondere auf die verschiedenen Arten der homomorphen Verschlüsselung ein (partial, somewhat, full). Wir beantworten, was genau diese Arten bedeutet und geben Beispiele für die praktischen Anwendungen. Diesbezüglich wird es eine Bewertung auf basis der aktuellen Forschung geben, ob und welche dieser Arten tatsächlich praktisch einsetzbar sind.

3 Kern der Arbeit

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

4 Mögliche Fragen zum beantworten

- **Was ist die Kernidee hinter Homomorpher Verschlüsselung?**
- **Welche Arten von homomorpher Verschlüsselung gibt es?**
  - Welche Vor- und Nachteile gibt es?
- **Auf welchen mathematischen Grundlagen basieren die Arten?**
- **Wie kann man homomorphe Verschlüsselung in der Praxis einsetzen?**
  - Wo ist es eventuell schon im Einsatz?
  - Was ist in Zukunft noch möglich?
  - In welchen Gebieten lohnt es sich?
- **Ist homomorphe Verschlüsselung post-quanten sicher?**

5 Theorien mit denen wir uns auseinander setzen

- **Welche Theorien gibt es?**
  - Grundlegende Theorie: partial, somewhat, full
  - Bootstrapping
- **Wo wollen wir anknüpfen?**
  - Zunächst am Beispiel bekannter Methoden (z.B. RSA oder ElGamal) die Theorie erklären

6 Literatur

Literatur

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