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 damit Operationen durchzuführen z.B. Aufaddieren der Stimmen bei einer Wahl oder Daten für Maschinelles lernen. Der Nutzer muss daher einen Teil seiner Privatsphäre einbüßen, damit diese Verarbeitet werden können. Das birgt Risiken, weil die Informationen wer für wen gestimmt hat sehr sensibel sind und man auch nicht unbedingt Google seine sensiblen Daten für Maschinelles lernen zur Verfügung stellen möchte. Mit Homomorpher Verschlüsselung gibt es die Möglichkeit solche Operationen direkt auf den verschlüsselten Daten durchzuführen. Dadurch bleiben sensible Informationen geschützt. Auf die Beispiele von eben bezogen bedeutet das, dass es möglich ist ein Modell zu haben, was die Daten Homomorph auswertet, dass bedeutet, man gibt seine Informationen verschlüsselt an einen Anbieter, dieser kann diese dann auswerten und Berechnungen ausführen. Das Ergebnis dieser Berechnungen ist dann immer noch verschlüsselt. Dann bekommt man das Ergebnis zurück und kann es einfach entschlüsseln. Es ist also so, als ob die Berechnungen direkt auf dem Entschlüsselten Daten durchgeführt wurden.

2 Das Ziel der Ausarbeitung

Das Ziel unserer Ausarbeitung ist, die grundlegende Theorie hinter Homomorpher Verschlüsselung zu erklären und die Anwendung dieser 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 praktische Anwendungen. Diesbezüglich wird es eine Bewertung, ob und welche dieser Arten tatsächlich Praktisch einsetzbar sind, auf Basis der aktuellen Forschung.

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 HE einzusetzen?
- **Ist Homomorphe Verschlüsselung post quanten sicher?**

5 Theorien mit denen wir uns auseinander setzen wollen

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