BusinessCode

IT for future

Homomorphe Verschlüsselung in der Praxis

Grundlagen, Einsatzmöglichkeiten und Herausforderungen

8. Mai 2025

Alexander Goth

Who is BusinessCode?

A STRONG AND RELIABLE BUSINESS PARTNER SINCE 1999

CONSULTING

TECHNOLOGY

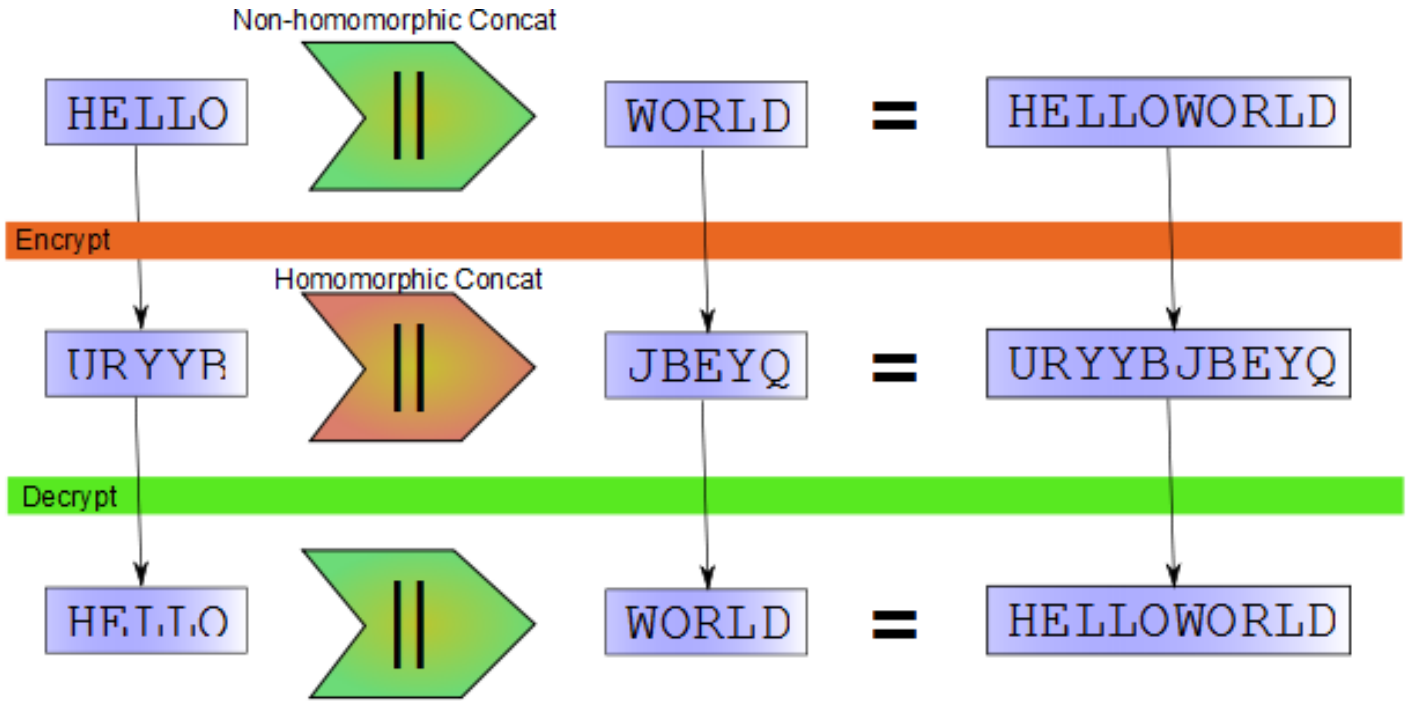
IMPLEMENTATION

RUN & SUPPORT

End-2-End Support

- Supporting our customer globally for more than 20 years out of Bonn (Germany)
  - Nearshore competence center in Crete (Greece)
- Supporting international corporations and SMEs
- Strong industry expertise in logistics and beyond
- Experience from more than 500 successful projects
- Since the management-buy-out in 2020 BusinessCode is owned by its employees

ROT13 (bzw. Caesar-Verschlüsselung)



RSA-Kryptosystem

- Die asymmetrische RSA-Verschlüsselung besitzt eine oft unbeachtete homomorphe Eigenschaft: Sie kann die Multiplikation zweier verschlüsselter Werte ohne vorherige Entschlüsselung durchführen.

- Die Verschlüsselung eines Wertes m erfolgt bei RSA durch Potenzieren mit dem öffentlichen Schlüssel e, modulo N:

$$c = m^e \bmod N.$$

Daraus folgt, dass für die verschlüsselte Multiplikation zweier Werte a und b folgendes gilt:

$$(a^e \bmod N) \cdot (b^e \bmod N) = (a^e \cdot b^e) \bmod N = (a \cdot b)^e \bmod N.$$

Die Multiplikation zweier verschlüsselter Werte ist also äquivalent zur Verschlüsselung des multiplizierten Wertes $a \cdot b$.

Restklassenverschlüsselung (AGCD-Problem)

- Verschlüsselt man einen Klartext a mit einer großen Primzahl p als Schlüssel und pro Chiffretext je einer großen Zufallszahl r nach der Formel

$$a' = a + r \cdot p,$$

so kann man mit den Chiffretexten a', b' Additionen und Multiplikationen ausführen. Die Entschlüsselung des Rechenergebnisses c mit $c = c' \bmod p$ gelingt, solange es kleiner als p bleibt.

Homomorphe Verschlüsselung

- Die *partially homomorphic encryption* (PHE) umfasst Verfahren, die nur eine Art von Operation unterstützen, entweder Addition oder Multiplikation, aber nicht beide gleichzeitig.

Homomorphe Verschlüsselung

- Die *partially homomorphic encryption* (PHE) umfasst Verfahren, die nur eine Art von Operation unterstützen, entweder Addition oder Multiplikation, aber nicht beide gleichzeitig.

- Die *fully homomorphic encryption* (FHE) unterstützt sowohl Addition als auch Multiplikation auf verschlüsselten Daten. Das bedeutet, dass jede beliebige Funktion, die durch eine Kombination dieser beiden Operationen dargestellt werden kann, auf den verschlüsselten Daten ausgeführt werden kann.

Homomorphe Verschlüsselung

- Die *partially homomorphic encryption* (PHE) umfasst Verfahren, die nur eine Art von Operation unterstützen, entweder Addition oder Multiplikation, aber nicht beide gleichzeitig.

- Die *somewhat homomorphic encryption* (SWHE) erlaubt eine Kombination von beiden Operationen, jedoch nur bis zu einem bestimmten Grad oder einer bestimmten Anzahl von Operationen.

- Die *leveled fully homomorphic encryption* (Leveled FHE) ist so konzipiert, dass sie Berechnungen in verschiedenen „Levels“ oder „Schichten“ durchführen kann. In der Regel können in einem Level beliebig viele Additionen und eine begrenzte Anzahl von Multiplikationen durchgeführt werden.

- Die *fully homomorphic encryption* (FHE) unterstützt sowohl Addition als auch Multiplikation auf verschlüsselten Daten. Das bedeutet, dass jede beliebige Funktion, die durch eine Kombination dieser beiden Operationen dargestellt werden kann, auf den verschlüsselten Daten ausgeführt werden kann.

Homomorphe Verschlüsselungssysteme

- Das Brakerski-Gentry-Vaikuntanathan (BGV, 2011) Schema (s. https://eprint.iacr.org/2011/277).
- Das Brakerski/Fan-Vercauteren (BFV, 2012) Schema (s. https://eprint.iacr.org/2012/144).
- Das Cheon-Kim-Kim-Song (CKKS, 2017) Schema (s. https://en.wikipedia.org/wiki/HEAAN#CKKS_plaintext_space).
- TFHE: Fast Fully Homomorphic Encryption over the Torus (s. https://tfhe.github.io/tfhe/).

_____
https://fhe.org/
https://homomorphicencryption.org/
https://github.com/jonaschn/awesome-he
https://s0l0ist.github.io/seal-sandbox/

Private Set Intersection (PSI)

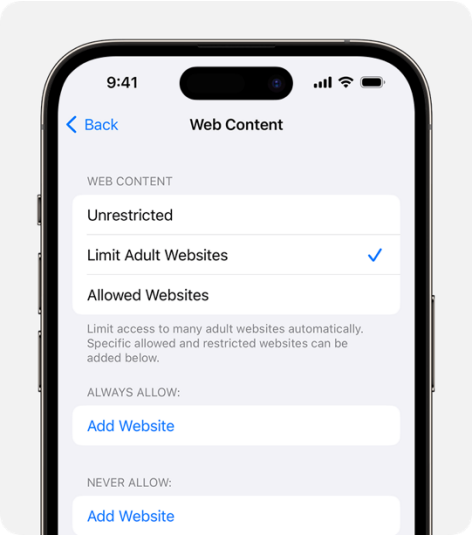
- Microsoft setzt das heute schon im Edge-Browser ein, um herauszufinden, ob Benutzernamen und Passwörter an die Öffentlichkeit gelangt sind:

  Wenn man Zugangsdaten im Edge-Browser speichert, verwendet er ein FHE-basiertes Protokoll, um
  große Leak-Datenbanken abzufragen und den Nutzer im Notfall zu warnen. In dem ganzen Prozess
  bekommt Microsoft nur mit, dass eine solche Abfrage stattfindet.

_____
https://www.microsoft.com/en-us/research/blog/password-monitor-safeguarding-passwords-in-microsoft-edge/

Private Information Retrieval (PIR)

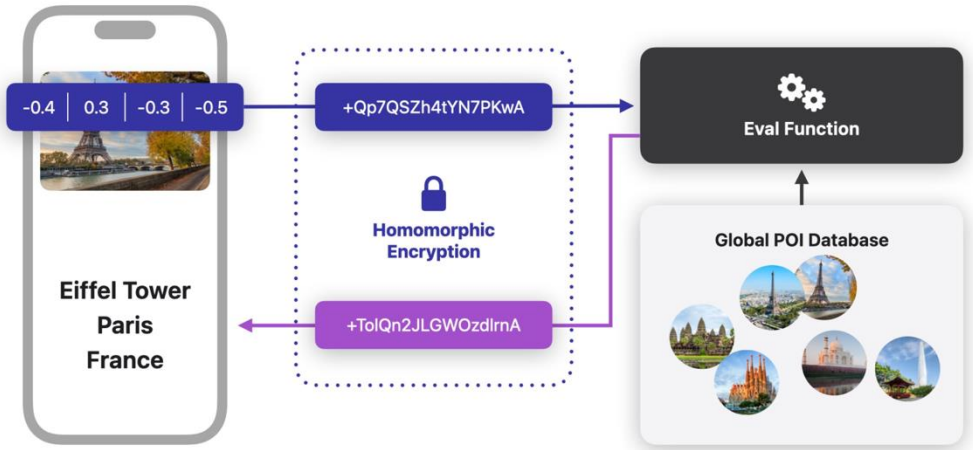
- Automatische Filterung von Webseiten, um den Zugriff auf nicht jugendfreie Inhalte in Safari und anderen Apps zu beschränken.



_____
https://machinelearning.apple.com/research/homomorphic-encryption

Private Information Retrieval (PIR)

- Automatische Verschlagwortung von Fotos, die mit der Handykamera aufgenommen wurden, die es dem Nutzer ermöglicht, seine Fotobibliothek nach bestimmten Orten, wie Sehenswürdigkeiten, zu durchsuchen.



_____
https://machinelearning.apple.com/research/homomorphic-encryption

Ausblick

- Datenschutzfreundliche KI-Modelle: KI-Modelle könnten auf verschlüsselten Daten trainiert werden, sodass Unternehmen von den Vorteilen von maschinellem Lernen profitieren können, ohne die Privatsphäre der Benutzer zu gefährden.

Ausblick

- Datenschutzfreundliche KI-Modelle: KI-Modelle könnten auf verschlüsselten Daten trainiert werden, sodass Unternehmen von den Vorteilen von maschinellem Lernen profitieren können, ohne die Privatsphäre der Benutzer zu gefährden.

- Finanzdienstleistungen: Banken und Finanzinstitute könnten homomorphe Verschlüsselung nutzen, um Kreditentscheidungen oder Risikobewertungen auf Basis verschlüsselter Kundendaten durchzuführen, ohne die Daten selbst zu sehen.

Ausblick

- Datenschutzfreundliche KI-Modelle: KI-Modelle könnten auf verschlüsselten Daten trainiert werden, sodass Unternehmen von den Vorteilen von maschinellem Lernen profitieren können, ohne die Privatsphäre der Benutzer zu gefährden.

- Finanzdienstleistungen: Banken und Finanzinstitute könnten homomorphe Verschlüsselung nutzen, um Kreditentscheidungen oder Risikobewertungen auf Basis verschlüsselter Kundendaten durchzuführen, ohne die Daten selbst zu sehen.

- Gesundheitswesen: Forscher könnten auf verschlüsselten Patientendaten Analysen durchführen, um neue Behandlungsmethoden zu entwickeln, ohne die Privatsphäre der Patienten zu gefährden.

Ausblick

- Datenschutzfreundliche KI-Modelle: KI-Modelle könnten auf verschlüsselten Daten trainiert werden, sodass Unternehmen von den Vorteilen von maschinellem Lernen profitieren können, ohne die Privatsphäre der Benutzer zu gefährden.

- Finanzdienstleistungen: Banken und Finanzinstitute könnten homomorphe Verschlüsselung nutzen, um Kreditentscheidungen oder Risikobewertungen auf Basis verschlüsselter Kundendaten durchzuführen, ohne die Daten selbst zu sehen.

- Gesundheitswesen: Forscher könnten auf verschlüsselten Patientendaten Analysen durchführen, um neue Behandlungsmethoden zu entwickeln, ohne die Privatsphäre der Patienten zu gefährden.

- Personalisierte Werbung: Werbetreibende könnten auf verschlüsselten Nutzerdaten basierende Analysen durchführen, um personalisierte Werbung zu schalten, ohne die persönlichen Daten der Nutzer offenzulegen.

Zusammenfassung

- Wir haben erklärt, was homomorphe Verschlüsselung ist, und einige Beispiele wie ROT13 und RSA betrachtet.
- Wir haben die vier Ausprägungen der homomorphen Verschlüsselung kennengelernt: PHE, SWHE, Leveled FHE und FHE.
- Wir haben die am häufigsten in Implementierungen verwendeten homomorphen Verschlüsselungssysteme BGV, BFV, CKKS und TFHE angesprochen.
- Wir haben die beiden Anwendungsgebiete PSI und PIR behandelt, praktische Beispiele dazu vorgestellt und einen Ausblick auf zukünftige Entwicklungen gegeben.