Advancements in Homomorphic Encryption for Secure Data Processing

A breakthrough in cryptography for privacy and security

Venkata Nedunoori |IEEE Digital Privacy Workshop | 10/07/2024

Why Homomorphic Encryption?

- Concern with data privacy and security.
- Key sectors healthcare and finance.
- Limitations of Traditional Encryption methods .
- Homomorphic Encryption

How Homomorphic encryption works?

Compute on encrypted data without needing to decrypt.

Locked box vs Unlocked box.

Ensures privacy at all stages of data processing.

Types of Homomorphic encryption.

Types of Homomorphic encryption

Partially Homomorphic Encryption (PHE): Supports a limited set of operations (either addition or multiplication but not both).

Somewhat Homomorphic Encryption (SHE): Supports both addition and multiplication but only up to a certain complexity or depth (due to noise accumulation during computation).

Fully Homomorphic Encryption (FHE): FHE supports unlimited numbers of both addition and multiplication operations. It can be used to carry out complex computations on encrypted data, like running machine learning algorithms or statistical analysis.

Historical Development of Homomorphic Encryption

1978: RSA Encryption

Introduced multiplicative homomorphism (supports multiplication on encrypted data).

Limited to one operation (multiplication), not practical for broader use.

1982: Goldwasser-Micali Cryptosystem

Supported additive homomorphism (addition on encrypted data).

Important step, but still restricted to one operation (addition).

1990s - Early 2000s:

Early concepts of FHE, theorizing both addition and multiplication on encrypted data.

No practical schemes yet, due to computational inefficiency.

2009: Gentry’s Breakthrough

First viable FHE using lattice-based cryptography.

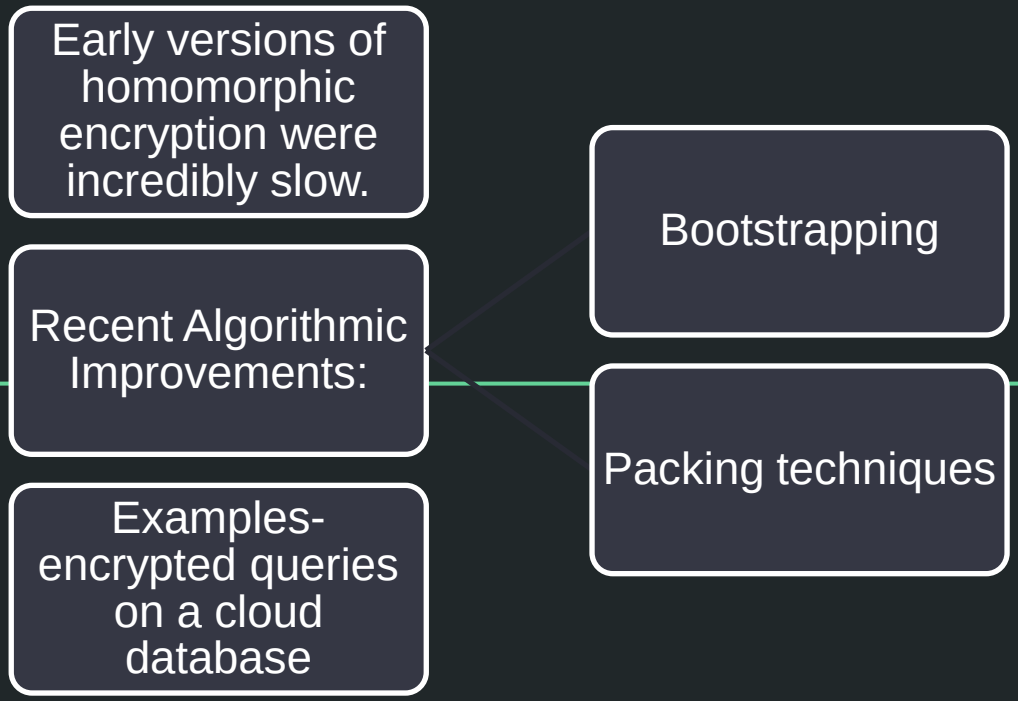
Introduced bootstrapping

2010-Current:

Ongoing improvements to reduce computational overhead and make FHE more practical for real-world applications (Leveled FHE, batching, parallelization).

Development of cryptographic libraries (e.g., SEAL, HELib, TFHE) to facilitate implementation.

Recent Algorithmic Improvements



Hardware Acceleration: Speeding up HE

- Another game changer
- CPUs are not well-suited to handling the high computational demands of HE.
- Specialized hardware
  - GPUs (Graphics Processing Units)
  - FPGAs (Field-Programmable Gate Arrays).
- Microsoft's SEAL library and IBM's HELib and Google’s TFHE offer optimized solutions that take advantage of GPU acceleration
- Applications: secure, privacy-preserving cloud computing in a reasonable timeframe.

Security Enhancements and Quantum Resistance

- HE doesn’t just solve the privacy issue, it’s also an incredibly secure form of cryptography- lattice-based cryptography

- Quantum computing-Risks for encryption

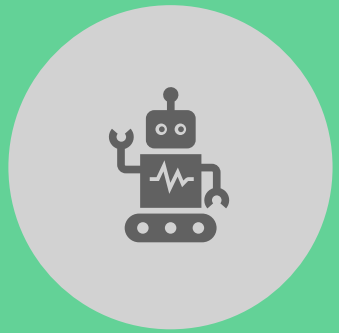
- Quantum Resistant

-Future proof technology

Key Applications of Homomorphic Encryption

CLOUD COMPUTING

HEALTHCARE/FINANCE/ENERGY



MACHINE LEARNING

Challenges and future direction

PERFORMANCE

INTEGRATION

STANDARDIZATION

Conclusion

HOMOMORPHIC ENCRYPTION IS A REVOLUTIONARY TECHNOLOGY THAT IS CHANGING THE WAY WE THINK ABOUT DATA PRIVACY AND SECURITY.

PRIVACY-PRESERVING COMPUTATION

Contact

Thank you!

vnedunoori@gmail.com