Developing Accelerators for Homomorphic Encryption

Mehmet Berkay Çatak, Rümeysa Bilik, Efe İzbudak,
Eren Özilgili, Cenker Şahin

Erkay Savaş

August 6, 2024

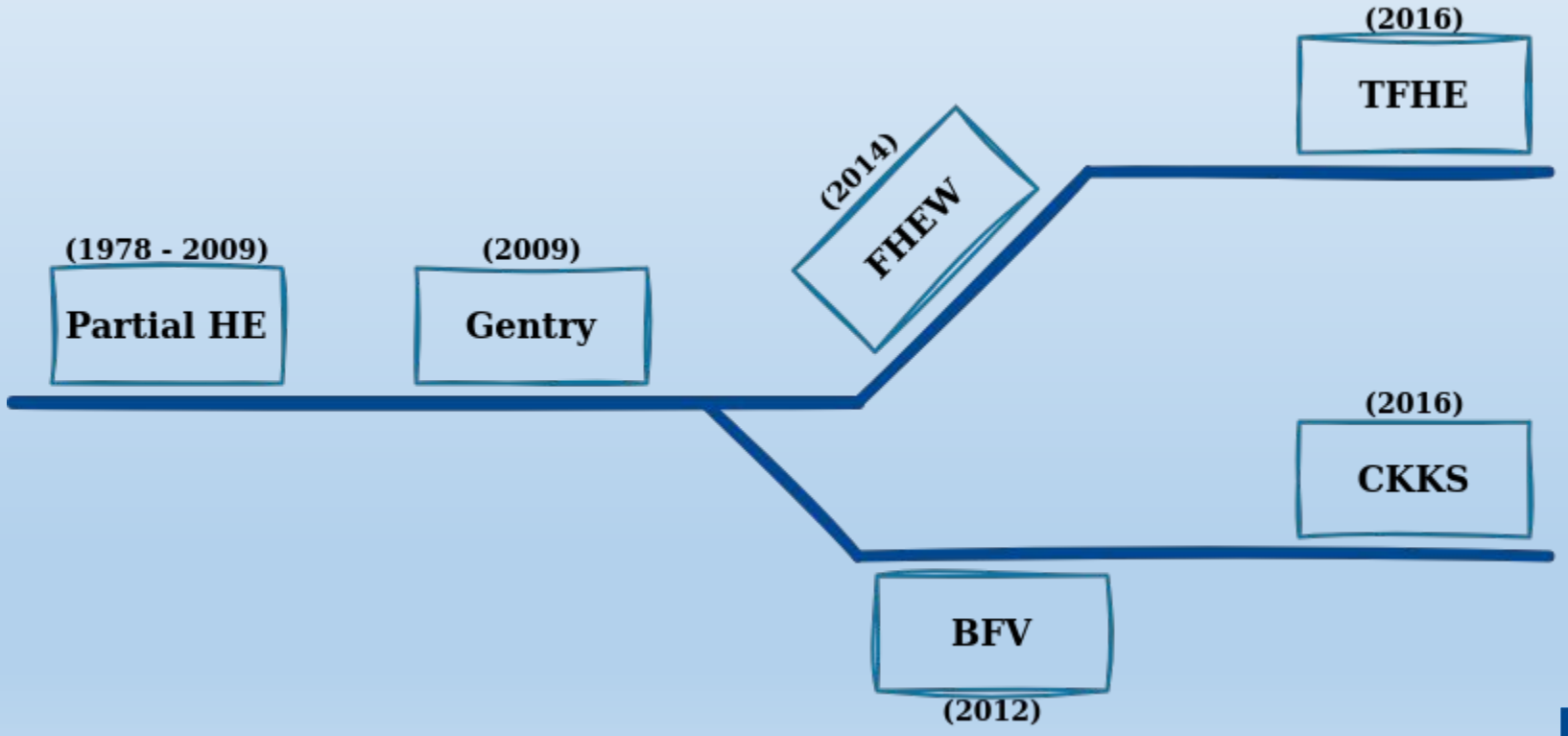
Outline

1. Homomorphic Encryption
    1.1. Examples
    1.2. Schemes
    1.3. Advantages
    1.4. Disadvantages
2. Research Question
3. Hardware Acceleration
4. Our Progress and Aim

Sabancı Üniversitesi

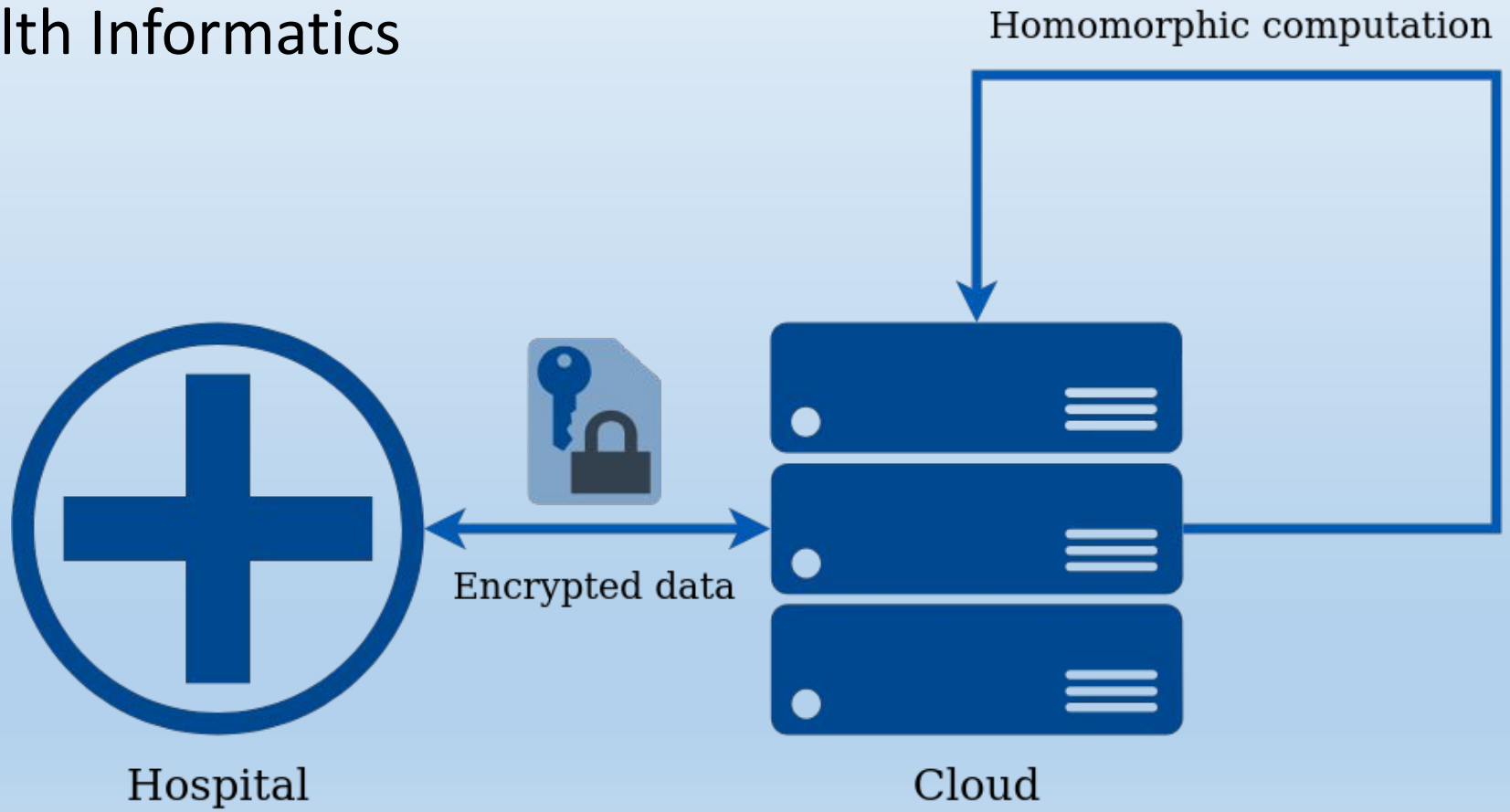
What is Homomorphic Encryption?

- Encryption schemes which allow a third-party to perform computation on encrypted data



Examples of Homomorphic Encryption

- Health Informatics



Examples of Homomorphic Encryption

- Health Informatics
- Privacy-Preserving Machine Learning

Examples of Homomorphic Encryption

- Health Informatics
- Privacy-Preserving Machine Learning
- Secure Voting Systems

Examples of Homomorphic Encryption

- Health Informatics
- Privacy-Preserving Machine Learning
- Secure Voting Systems
- Financial Transactions and Fraud Detection

Advantages of Homomorphic Encryption

- Confidential computing

Advantages of Homomorphic Encryption

- Confidential computing
- Data Monetization

Advantages of Homomorphic Encryption

- Confidential computing
- Data Monetization
- Reduced trust requirements

PURE PROGRAM FOR UNDERGRADUATE RESEARCH

Sabancı Üniversitesi

Advantages of Homomorphic Encryption

- Confidential computing
- Data Monetization
- Reduced trust requirements
- Interoperability

PURE PROGRAM FOR UNDERGRADUATE RESEARCH

Sabancı Üniversitesi

Advantages of Homomorphic Encryption

- Confidential computing
- Data Monetization
- Reduced trust requirements
- Interoperability
- Integrity assurance

Homomorphic Encryption Schemes

- CKKS (Cheon-Kim-Kim-Song) (Cheon et al., 2017):
  - Approximate computation
  - Leveled encryption scheme
  - Appropriate for machine learning, scientific computation
- TFHE (Fast Fully Homomorphic Encryption over the Torus) (Chillotti et al., 2019):
  - Exact computation
  - Fast bootstrapping
  - General use case

Sabancı Üniversitesi

Disadvantages of Homomorphic Encryption

- High Computational Cost

Disadvantages of Homomorphic Encryption

- High Computational Cost
- Performance Overhead

Disadvantages of Homomorphic Encryption

- High Computational Cost
- Performance Overhead
- Complexity of Implementation

Disadvantages of Homomorphic Encryption

- High Computational Cost
- Performance Overhead
- Complexity of Implementation
- Increased Data Size

Research Question

How can we accelerate homomorphic encryption?

PURE PROGRAM FOR UNDERGRADUATE RESEARCH

Sabancı Üniversitesi

Hardware Acceleration

- Using specialized hardware to perform tasks more efficiently

Hardware Acceleration

- Using specialized hardware to perform tasks more efficiently
- Three main types:
  - CUDA
  - FPGA
  - ASIC

Our Progress and Aim

- Python implementations of homomorphic encryption algorithms
- Python wrapper for CUDA HE library
- Hardware implementations of algorithms with Verilog

PURE PROGRAM FOR UNDERGRADUATE RESEARCH

Sabancı Üniversitesi

References

Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. *Advances in Cryptology – ASIACRYPT 2017*, 409–437. https://doi.org/10.1007/978-3-319-70694-8_15

Chillotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2019). TFHE: Fast fully homomorphic encryption over the torus. *Journal of Cryptology*, *33*(1), 34–91. https://doi.org/10.1007/s00145-019-09319-x

PURE PROGRAM FOR UNDERGRADUATE RESEARCH

Sabancı Üniversitesi