Privacy-preserving Exchange and Processing of Confidential Data Using Homomorphic Encryption

Mirza Ćutuk
Dr. Eduardo Solana
Dr. Lionel Clavien

Privacy-preserving platform for data utilization

IB Cloak

Homomorphic Encryption for real-world use cases

A secure, privacy-preserving, multi-party data processing platform, that can be used securely by participating entities to store and process data, while preserving user privacy and keeping the entities accountable.

Non-arithmetic Operations

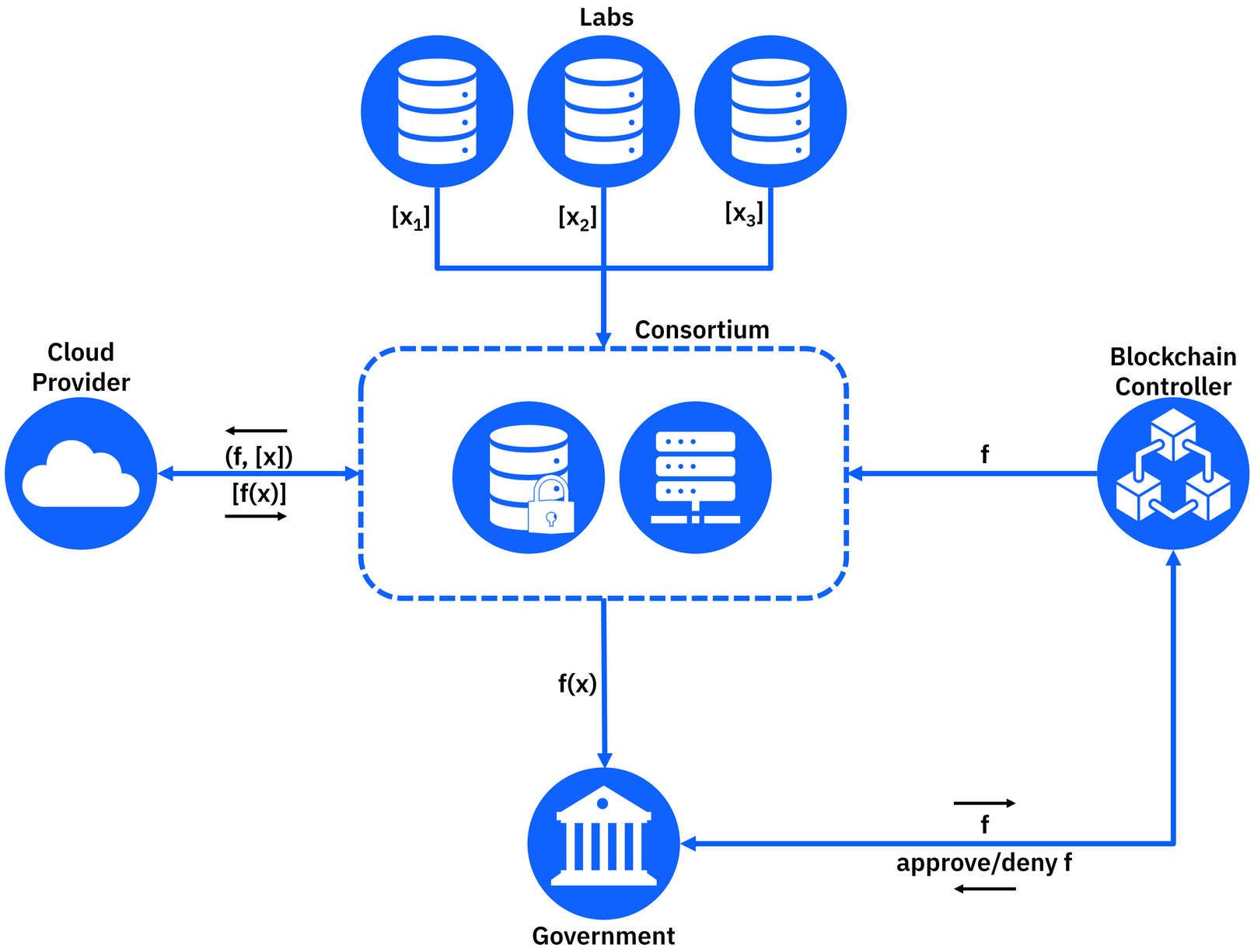
sign, min, max, less than and higher than for ciphertext filtering

Arithmetic Operations

mean, variance, standard deviation, and standard error

Linear Regression

homomorphic variant of simple linear regression with gradient descent



Lattigo
FHE Library

PostgreSQL
Encrypted Database

Dash App
Consortium Frontend

Flask Server
Consortium Backend

Hyperledger Fabric
Blockchain Controller

IB Cloak: Privacy Preservation of the Future

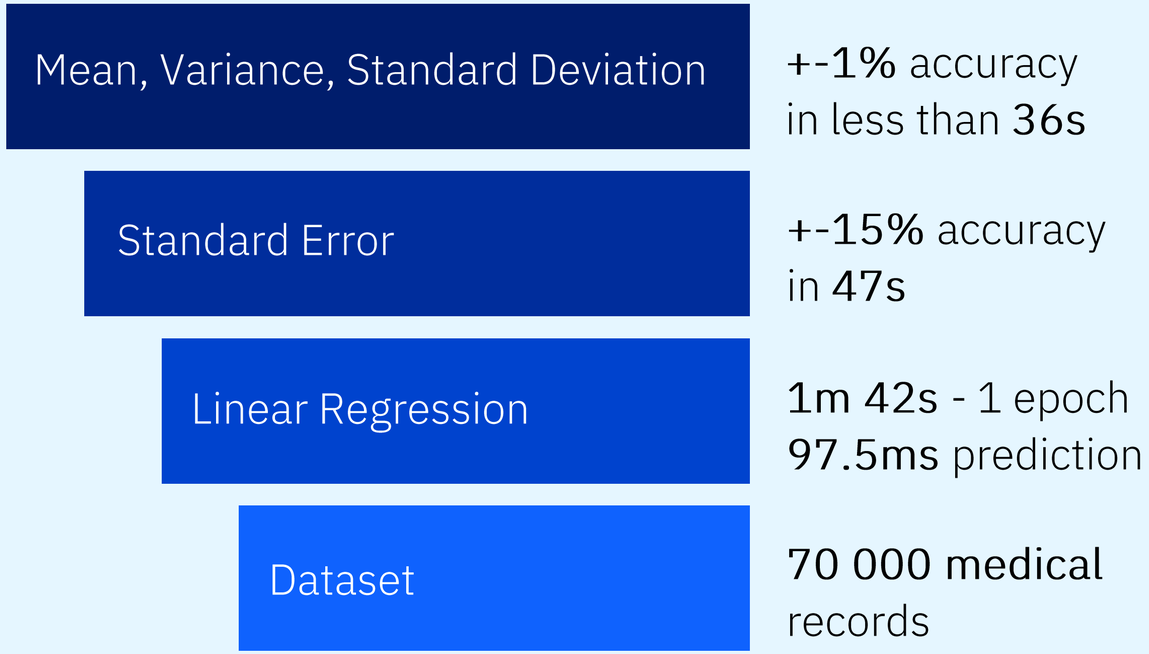
Our approach to preserving privacy with FHE showed that sufficiently efficient systems with a respectable level of security are a reality.

Use cases for:

- Data Exchange
- Insight extraction
- Machine Learning/Artificial Intelligence

Questions related to the practical side of FHE:

- Offline decryption
- Large key size
- Large ciphertext size
- Time to bootstrap
- Computational requirements



Thank you!

Mirza Ćutuk, MSc
mcutuk@inno-boost.com
https://www.linkedin.com/in/mirza-cutuk