encrypt

A scalable and practical privacy-preserving framework

Fully Homomorphic Encryption

Fully Homomorphic Encryption with OpenFHE: Privacy-Preserving Protocols for PIR and Decision Tree Evaluation

OBJECTIVE

Enable computation on encrypted data using FHE for:

- Private Information Retrieval (PIR)
- Encrypted decision tree evaluation

TOOLS

- OpenFHE library
- Custom Paillier library

FHE Implementation

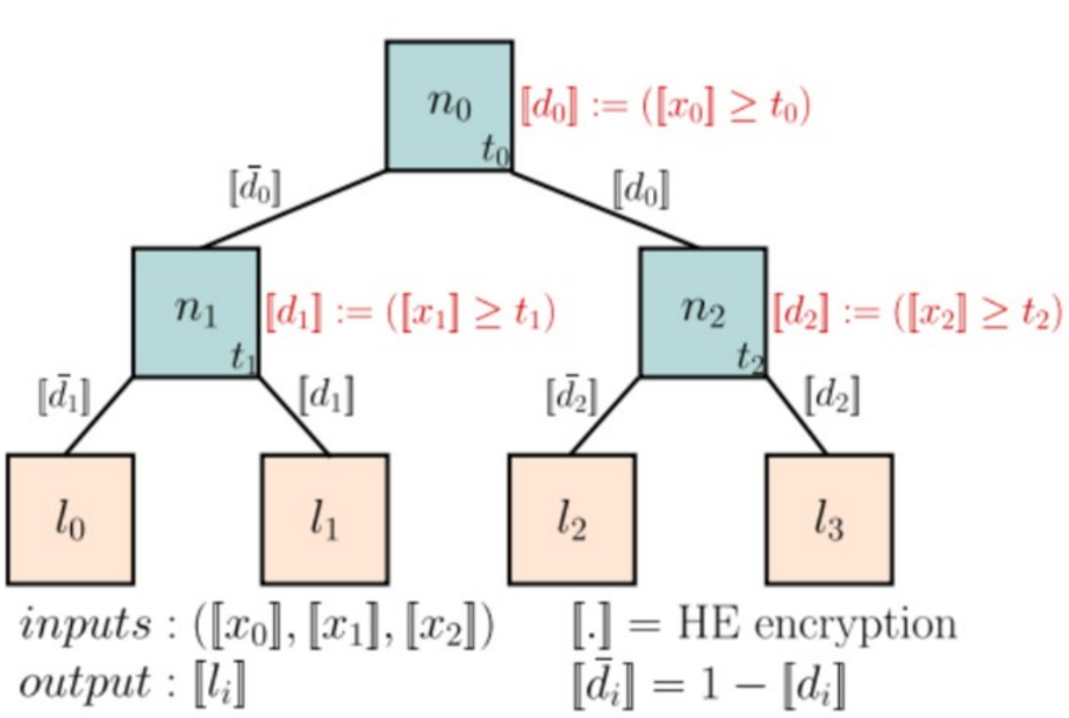
- OpenFHE with BGV scheme used for encrypted computation
- Custom Paillier variant enables 1-level multiplication

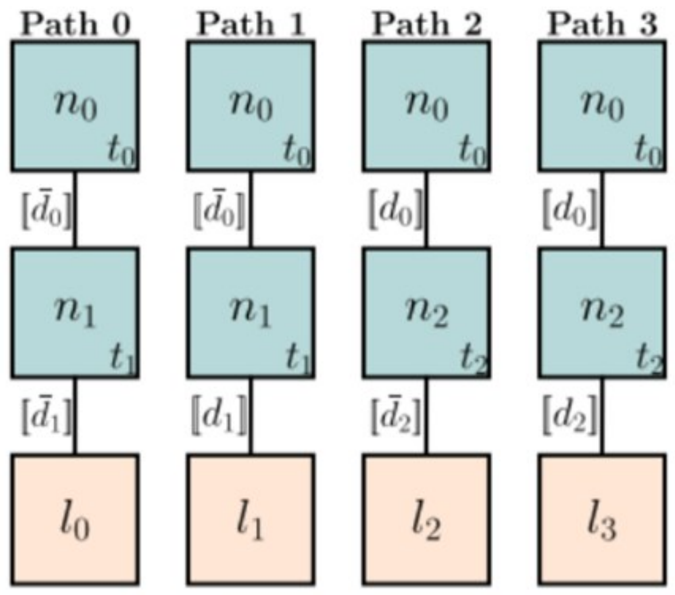
Private Information Retrieval

- Single-multiplication PIR for blind DB searches
- Reduced ciphertext size and lower computation cost

Decision Tree Evaluation

- Encrypted attribute comparisons to thresholds
- Non-interactive traversal using BGV multiplications





Optimisation

- Tuned parameters
- Hardware acceleration

Results Summary

- Efficient Private Information Retrieval
- Encrypted trees privacy-preserving classification
- OpenFHE outperforms older libraries
- Paillier variant: Simpler, more secure, standard-friendly

Funded by the European Union

This work is supported by the European Union's Horizon Europe programme under grant agreement No 101070670.