Find if there is a path of more than k length from a source with EVA

Term Project Presentation

Baran Tunc
baran.tunc@metu.edu.tr

Wireless Systems, Networks and Cybersecurity Laboratory
Department of Computer Engineering
Middle East Technical University
Ankara Turkey

June 22, 2022

Outline of the Presentation

1. The Problem
2. The Contribution
3. Background
   What is FHE?
   What is SEAL?
4. FHE Implementation
5. Results
6. Conclusions

Agenda

1 The Problem

2 The Contribution

3 Background

4 FHE Implementation

5 Results

6 Conclusions

The problem

The algorithm and the expectation of the project

Find if there is a path of more than k length from a source

Given a graph, a source vertex in the graph and a number k, find if there is a simple path (without any cycle) starting from given source and ending at any other vertex such that the distance from source to that vertex is at least ‘k’ length.

In this project, this problem solving will be implemented to a fully homomorphic encryption.

Agenda

1. The Problem
2. The Contribution
3. Background
4. FHE Implementation
5. Results
6. Conclusions

FHE Approach and Implementation

This known network problem ”Find if there is a path of more than k length from a source” has a solution in conventional networks.

In this term project, solution to this problem (algorithm) will be implemented in a FHE network using:

- Microsoft SEAL: a FHE network scheme,
- Microsoft EVA: a SEAL program compiler,
- Python: a programming language,
- pyEVA: an EVA python library.

Agenda

1 The Problem

2 The Contribution

3 Background

4 FHE Implementation

5 Results

6 Conclusions

What is FHE?

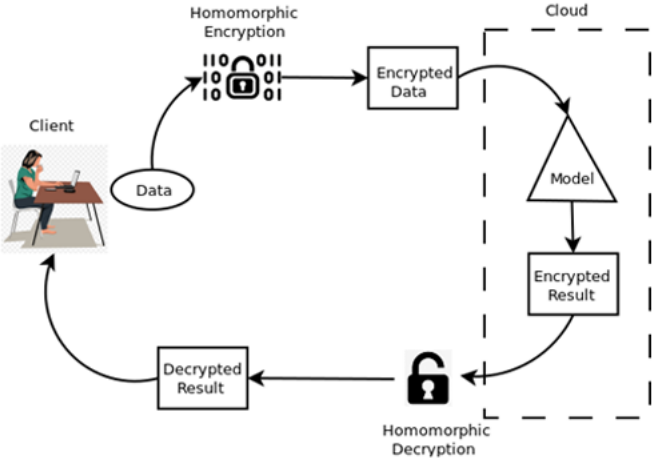
Definition of FHE

Fully homomorphic encryption (FHE) is an encryption scheme that enables analytical functions to be run directly on encrypted data while yielding the same encrypted results as if the functions were run on plaintext [1].

[1] https://inpher.io/technology/what-is-fully-homomorphic-encryption

How does FHE work?

Work flow of the FHE



What is SEAL?

With SEAL homomorphic encryption, cloud providers never have unencrypted access to the data they store and compute on. Computations can be performed directly on encrypted data. The results of such encrypted computations remain encrypted, and can be decrypted only by the data owner by using the secret key. Most homomorphic encryption uses public-key encryption schemes, although the public-key functionality may not always be needed [2]

[2] https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/homomorphic-encryption-seal

Agenda

1. The Problem
2. The Contribution
3. Background
4. **FHE Implementation**
5. Results
6. Conclusions

Conventional Algorithm for Solution

When a network is given, finding if there is a path of more than k length from a source can be explained with an example.

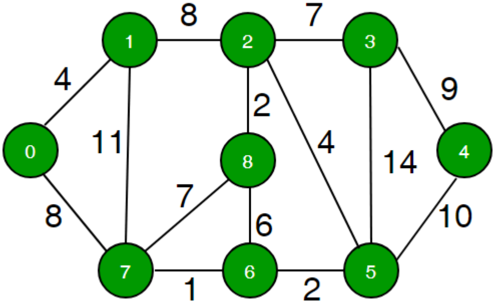


Figure: Nodes and connecting paths of a network example

Computational Challenges

Using a FHE scheme, limits its computational operations to only addition, subtraction, multiplication, negation and shifting bit-wise right/left with the given encrypted values.

Therefore you cannot use any type of comparison, condition or logic other than manipulating vectors for the purpose.

In order to protect the privacy of the sender's data and at the same time to implement such an algorithm to FHE scheme, a non-cycle networks solution is chosen to work on in this term project.

Implementing this algorithm to cyclic networks in FHE was tried and ended up with too much time consuming for this term project.

FHE Solution

Compromise

A non-cycle n-nodes network with randomly generated path length will be generated by the software to be used as a input.

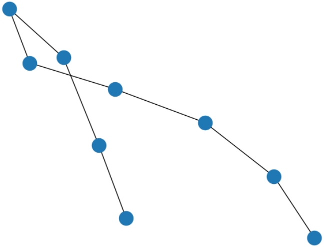
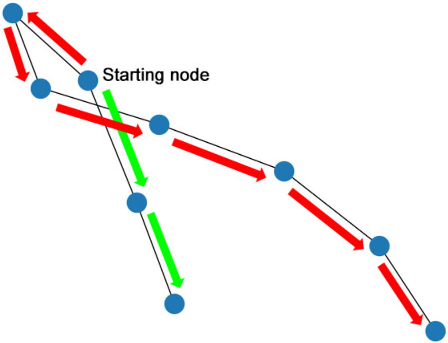


Figure: Network example to be implemented on FHE

FHE Solution

Calculation

Using the network input, next step is developing an FHE friendly algorithm to go from the source node to both directions, and then return the summations of the paths from the source node to end node.



Agenda

1 The Problem
2 The Contribution
3 Background
4 FHE Implementation
5 **Results**
6 Conclusions

Repeatability and Computational Error

After 1000 tries, method seems to be consistently able to calculate the correct results every time without errors.

Averages for 9 nodes input can be given as:

Table: Average Time and Error

compile time (ms)	1.41
key generation time (ms)	20.93
encryption time (ms)	48.01
execution time (ms)	10.91
decryption time (ms)	6.52
reference execution time (ms)	0.14
mean square error (%)	9.43e-19

Agenda

1 The Problem
2 The Contribution
3 Background
4 FHE Implementation
5 Results
6 Conclusions

Conclusions

In this term project, an implementation of FHE into a known network problem ”Finding if there is a path of more than k length from a source” was done. FHE approach was applied successfully to solve the problem for non-cycle networks using Microsoft SEAL and EVA compiler via python. Client side generated network was converted to vector and then python dictionary format and fed to the EVA Program.

Values were encrypted on client side and sent to server for calculations to be done as encrypted. Left and right hand side available path length summations were done and results were sent back to client still-encrypted. Client was able to decrpyt and get the desired results. Further work is needed to implement on networks with cycles.

References

- Microsoft. (2022) Homomorphic encryption with seal. [Online]. Available: https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/homomorphic-encryption-seal
- inpher.io. (2022) What is fully homomorphic encryption? [Online]. Available: https://inpher.io/technology/what-is-fully-homomorphic-encryption/
- Microsoft. (2022) Eva - compiler for microsoft seal. [Online]. Available: https: //github.com/microsoft/EVA
- tutorialspoint.dev. (2022) Writing methodology. [Online]. Available: https://tutorialspoint.dev/data-structure/graph-data-structure/find-if-there-is-a-path-of-more-than-k-length-from-a-source

Questions

THANK YOU

Find if there is a path of more than k length from a source with EVA

Term Project Presentation

presented by Baran Tunc
baran.tunc@metu.edu.tr

June 22, 2022

?