Analysis of Security-Cost Trade-off of Fully Homomorphic Encryption Schemes

Kais Chaabouni
ENSIMAG
Grenoble INP
Grenoble, France
kais.chaabouni@ensimag.imag.fr

Amrit Kumar
ENSIMAG-Ecole Polytechnique
Grenoble INP
Grenoble, France
amrit.kumar@ensimag.imag.fr

ABSTRACT

Abstract

Keywords

Fully Homomorphic Encryption, Security, Cost

1. INTRODUCTION

Motivation and significance of fully homomorphic encryption scheme such as Gentry's lattice-based scheme. This work evaluates the efficiency of FHE implementations for operations varying from XOR to sort on remote machines. Trade-off between cost and security is analyzed.

2. GENTRY'S FULLY HOMOMORPHIC SCHEME

FHE

2.1 The Framework

Overview of the algorithm and its complexity.

2.2 Example

Description using a typical operation like modular multiplication of two n-bit vectors. Comparison with partial homomorphic encryption scheme such as RSA.

3. EXPERIMENTAL EVALUATION OF COST

Describe the FHE algorithm and its corresponding implementation choice. Installation, set-up procedure and usage of the implementation. We detail the measurements to be taken, like Wall time, CPU time and memory usage based on certain security or algorithmic parameters.

Statistical analysis of the measurements using minimum, max, mean and standard deviation.

4. EVALUATION ON BENCH MARKS

We describe the system parameters and test vectors. This section also includes description of the process of evaluation for the following operations :

As the hCrypt implementation provides us with the two gates : `XOR` and `AND` which form a complete set of functional gates. The $\neg$`a` is `XOR(a,1)` while `OR(a,b)` is `XOR(XOR(a,b), AND(a,b))`.

XOR of n-bits. We start with the simplest operations on bits. `XOR` of n-bits requires $n-1$ `XOR` gates.

Majority of n-bits. Majority bit will be evaluated with the following circuit :

$$\prod_{i=1}^{n} a_i + \sum_{i=1}^{n} (\prod_{j!=i} a_j) \neg a_i$$

Hence it uses (n^2-1) `AND` gates and n `OR` gates.

Sum of integers of n-bits. Sum of two integers can be performed using an n-bit adder based on `full-adder` circuits. The cost of a full adder circuit is 2 `XOR` to calculate the sum and the cost of calculating $3 - bit$ majority function for the carry.

Sum of arbtrary integers

- Sum of :
  - bounded integers

  - unbounded integers

- String sorting with the following methods :
  - Insertion sort
  - Merge sort
  - Quick Sort
- Matrix product

Sorting is tested on a sorting network where comparator gates are used. For insertion sort we would need $n(n-1)/2$ such gates. Each comparator is designed using the following algorithm.

Algorithm 1: Comparator

```
Data: $(a_0, a_1, \ldots, a_{n-1})$, $(b_0, b_1, \ldots, b_{n-1})$
Result: Return Max(a,b) and Min(a,b)
1 aIsGreater=0;
2 for $i \leftarrow n-1$ to 0 do
3     aIsGreater=aIsGreater $+\neg(b_i)a_i$ ;
4 for $i \leftarrow 0$ to $n-1$ do
5     $Max_i$ = aIsGreater*$a_i$ + $\neg(aIsGreater) * b_i$ ;
6     $Min_i$ = $\neg(aIsGreater) * a_i$ + aIsGreater*$b_i$ ;
7 return($(Max_0, Max_1, \ldots, Max_{n-1})$,
  $(Min_0, Min_1, \ldots, Min_{n-1})$)
```

Each comparator gate uses n `AND` gate and n `OR` gates and n `NOT` gates to find which one of the bit sequence is bigger and then to regenerate the maximum and the minuimum it would require $4n$ `AND` gates $2n$ `NOT` and `OR` gates.

For each operation, we provide the initial algorithm and the results obtained. Observations based on the measurements are described.

5. ANALYSIS OF THE RESULTS

Trade-off analysis on the results obtained. Comparison with other protocols in terms of gain with security-cost trade-off.

Observations and recommendations on the cost and security trade-off.

6. CONCLUSION

Conclusion

7. REFERENCES