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
We present a study on variants of fully homomorphic schemes and the trade-off cost/security of basic operations on bits, integers, strings...

Keywords
Fully Homomorphic Encryption, Security, Cost

1. INTRODUCTION(1 PAGE)
Partial HME, Gentry's scheme from SWHME to FHE via bootstrapping. The purpose fo FHE, the protocl in general. Remote processing of computations on encrypted input transforms a native program into another program which has a higher circuit depth. The objective of this article is to analyse the security-cost tradeoff of remote computations. The implementations that exist and the organisation of the article. With citations to the referenced articles and papers.

2. FULLY HOMOMORPHIC SCHEME(1 PAGE)
A general structure of the scheme.

2.1 Two Variants of Fully Homomorphic Encryption Scheme
A brief description of the two FHE schemes with their algorithmic complexity of the different stages in the scheme. -> Smart Vercautren -> BGV

Discuss the security of these schemes.

2.2 Considered Implementations
The library used, version, implementaion details, versions, references, modifications required, how-to-installl, how-to-use.Platforms accepted and other depedeices.

2.3 Intial set-up cost(The cost not depending on the actual program)
Can be integrated with subsection 2.1

3. DIDACTIC EXAMPLE : MAXIMUM OF TWO INTEGER (1 PAGE)
3.1 Input Program for Fully Homomorphic Encryption Scheme
Details of the circuit or the program used to calculate the maximum of two bounded integers.

3.2 Theoretical Cost with the Schemes
Analyse the cost of the program wrt SV, BGV.

3.3 Experimental Analysis
Once for all analysis of common operations(KeyGen, Encrypt, Decrypt of 1 bit) varying the algorithmic and security parameters.

Measurements taken are CPU time, Wall Time, Memory Usage by varying the input size and the algorithmic parameters. Noise reduction threshold.

KeyGen

Encryption and Decryption

4. CHOICE OF BENCHMARKS
3 different classes of problems :

- Operations on bits,
- operation on integers (possibility of extension on blocks and comparision with RSA and
- branching

For each problem we propse the program, analyse their cost and eventually on security.

Why certain other programs cannot be executed under homomorphic encryption.

5. EVALUATION ON THE BENCHMARKS (1 PAGE)
Measurements on varying the parameters or the plaintext space. Evaluation of program dependent properties.

6. ANALYSIS OF THE RESULTS
Anlayze the results previously obtained and its impact on security and complexity. Comparisions of security-cost tradeoff with other schemes like RSA.

7. CONCLUSION

Conclusion