People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research

Faculty of Sciences
Department of Computer Science



Ferhat Abbas University - Setif 1

A Thesis Submitted in Fulfillment of the Requirements for the Degree of

Master of Science

Specialty: RSD

Theme

Study and Implementation of Homomorphic Encryption Based Protocols

---

Supervised by:

Samia Kharchi

Prepared by:

Kouadri Hadjer
Khattab Nesrine

2025/2026

Contents

Dedication . . . . . **ii**

Dedication . . . . . **iii**

List of Tables . . . . . **iv**

List of Figures . . . . . **v**

List of Algorithms . . . . . **vii**

List of Abbreviations . . . . . **viii**

List of Terms . . . . . **ix**

General Introduction **1**

Chapter 1: Literature Review on Cryptography **3**

Introduction 3

1.1 Definitions of Cryptography 3

1.1.1 Definition 1 3

1.1.2 Definition 2 4

1.2 History of cryptography 4

1.3 Objectives of cryptography 5

1.4 Cryptography classes 6

1.4.1 classical cryptography 6

1.4.2 Modern cryptography 7

1.4.2.1 •symmetric cryptography 7

1.4.2.2 - Asymmetric Cryptography 8

1.5 Cryptographic Protocols 9

1.6 Applications of Cryptography 10

1.7 Cryptographic Attacks 10

1.8 Limits of Cryptography 11

1.9 Emerging Trends in Cryptography 12

Conclusion 12

Chapter 2: Fundamental Principles of Homomorphic Encryption **13**

Introduction 13

2.1 Origins and Applications of Homomorphism 13

2.2 Definition of Homomorphic Encryption . . . 14
2.3 Objectives of Homomorphic Encryption . . . 14
2.4 Classification of homomorphic encryption schemes . . . 15
2.4.1 Partially Homomorphic Encryption (PHE) . . . 16
2.4.1.1 RSA Cryptosystem . . . 16
2.4.1.1.1 Algorithms . . . 16
2.4.1.1.2 Characteristics . . . 18
2.4.1.2 ElGamal Cryptosystem . . . 18
2.4.1.2.1 Algorithmes . . . 18
2.4.1.2.2 Characteristics . . . 19
2.4.1.3 Paillier Cryptosystem . . . 20
2.4.1.3.1 Algorithmes . . . 20
2.4.1.3.2 Caractéristiques . . . 21
2.4.2 Somewhat Homomorphic Encryption (SHE) . . . 21
2.4.2.1 DGHV (Van Dijk, Gentry, Halevi, Vaikuntanathan) . . . 21
2.4.2.1.1 Mathematical Foundations . . . 21
2.4.2.1.2 Algorithms . . . 22
2.4.2.1.3 Characteristics . . . 23
2.4.2.1.4 Limitations . . . 24
2.4.3 Fully Homomorphic Encryption (FHE) . . . 24
2.4.3.1 The Technological Bottleneck: the Noise Problem . . . 24
2.4.3.2 Main FHE Schemes . . . 24
2.4.3.2.1 BFV: Exact Computation on Integers . . . 25
2.4.3.2.2 BGV: Noise Control via Modulus Switching . . . 27
2.4.3.2.3 CKKS: The Revolution of Approximate Computation . . . 29
2.4.3.3 Comparative Synthesis . . . 32
2.4.3.4 FHE Assessment . . . 33
2.4.4 Comparison between PHE, SHE, and FHE . . . 33
2.4.5 Challenges and Limitations . . . 34
Conclusion . . . 34

Chapter 3:Homomorphic Encryption for Secure Cloud-Based Medical Systems . . . 35

Introduction . . . 35
3.1 Global Scenario Description . . . 35
3.1.1 Mathematical Model of PMI Based on Henssge's Law and Homomorphic Compatibility . . . 36
3.1.2 Principle of Henssge's law . . . 37
3.1.3 Correction factors . . . 37

3.2 Case Study: Secure Estimation of PMI using the Paillier Cryptosystem (PHE) . . . 37
3.2.1 Description of the Method . . . 37
3.2.2 Proposed Algorithm . . . 38
3.2.3 Calculation Procedure . . . 38
3.2.4 Result Analysis . . . 40
3.2.4.1 Execution Time Analysis . . . 40
3.2.4.1.1 a) Cost of homomorphic encryption . . . 40
3.2.4.1.2 b) Modular exponentiation . . . 40
3.2.4.1.3 c) Additional security phases . . . 40
3.2.5 Limitations of the Paillier Cryptosystem . . . 41
3.2.5.1 Limited support for operations . . . 41
3.2.6 Summary . . . 42
3.3 Case Study: Secure Estimation of PMI using the DGHV Scheme (SHE) . . . 42
3.3.1 Description of the Method . . . 42
3.3.2 Algorithme Proposé . . . 43
3.3.3 Detailed Explanation of the DGHV Implementation . . . 43
3.3.3.1 Execution Result . . . 44
3.3.3.2 Analysis of execution results . . . 44
3.3.4 Algorithme Proposé . . . 47
3.3.5 Detailed Explanation of the CKKS Implementation . . . 47
3.3.6 Execution Result . . . 48
3.3.6.1 Results Analysis . . . 48
3.3.6.2 Execution Time Analysis . . . 49
3.3.6.3 Analysis of CKKS Limitations . . . 49
3.3.7 Summary . . . 50
3.4 Comparison of Performance (Execution Time) . . . 53
3.4.1 Analysis of the Obtained Results . . . 53
3.5 Proposed Contribution: Noise Mitigation via a Bootstrapping Inspired Approach . . . 54
3.5.1 Proposed Algorithm . . . 54
3.5.1.1 Parameter Initialization . . . 54
3.5.1.2 Encryption and Thermal Ratio Computation . . . 55
3.5.1.3 PMI Computation under Homomorphic Noise . . . 55
3.5.1.4 Refresh Mechanism . . . 55
3.5.1.5 Results Analysis . . . 55
3.5.2 Algorithm Execution Process . . . 55
Conclusion . . . 59
General Conclusion . . . **61**

Abstract

Homomorphic encryption is a promising solution for ensuring the confidentiality of sensitive data while allowing its processing without prior decryption. This technology is particularly suitable for cloud environments, where medical and forensic data require a high level of protection.

This thesis presents a study of the main homomorphic encryption schemes, namely Paillier (PHE), DGHV (SHE), and CKKS (FHE), along with their characteristics, advantages, and limitations. A case study on secure post-mortem interval (PMI) estimation was conducted based on Henssge's cooling law. Computations were performed on encrypted data to preserve the confidentiality of information extracted from autopsy reports.

Experimental results show that the Paillier scheme ensures good accuracy but has a high computational cost. The DGHV scheme enables homomorphic operations on integers but requires mathematical approximations and remains limited by noise accumulation. The CKKS scheme appears to be the most suitable for medical applications due to its ability to handle real numbers directly with a good trade-off between accuracy, security, and performance.

Finally, a contribution based on a bootstrapping-inspired approach was proposed to mitigate noise accumulation in CKKS. The results show improved computational stability and reduced error in PMI estimation, confirming the relevance of this approach for secure computation over encrypted medical data.

Keywords:

Homomorphic encryption, Paillier, DGHV, CKKS, Post-mortem interval, Henssge's law, Cloud computing, Medical data security, Noise accumulation.

Résumé

Le chiffrement homomorphe constitue une solution prometteuse pour assurer la confidentialité des données sensibles tout en permettant leur traitement sans déchiffrement préalable. Cette technologie est particulièrement adaptée aux environnements cloud, où les données médicales et médico-légales nécessitent un niveau élevé de protection.

Ce mémoire présente une étude des principaux schémas de chiffrement homomorphe, notamment Paillier (PHE), DGHV (SHE) et CKKS (FHE), ainsi que leurs caractéristiques, avantages et limitations. Une étude de cas portant sur l'estimation sécurisée de l'intervalle post-mortem (PMI) a été réalisée à partir de la loi de refroidissement de Henssge. Les calculs ont été effectués sur des données chiffrées afin de préserver la confidentialité des informations issues des rapports d'autopsie.

Les résultats expérimentaux montrent que le schéma Paillier garantit une bonne précision mais présente un coût computationnel élevé. Le schéma DGHV permet l'exécution d'opérations homomorphes sur des entiers, mais nécessite des approximations mathématiques et reste limité par l'accumulation du bruit. Le schéma CKKS apparaît comme la solution la plus adaptée aux applications médicales, grâce à sa capacité à traiter directement des nombres réels avec un bon compromis entre précision, sécurité et performances.

Enfin, une contribution basée sur une approche inspirée du bootstrapping a été proposée afin d'atténuer l'accumulation du bruit dans CKKS. Les résultats obtenus montrent une amélioration de la stabilité des calculs et une réduction de l'erreur lors de l'estimation du PMI, confirmant l'intérêt de cette approche pour les applications de calcul sécurisé sur données médicales chiffrées.

Mots-clés :

Chiffrement homomorphe, Paillier, DGHV, CKKS, Intervalle post-mortem, Loi de Henssge, Cloud computing, Sécurité des données médicales, Accumulation de bruit.

ملخص

يُعدّ التشفير المتماثل شكليًا (Homomorphic Encryption) حلاً واحدًا لضمان سرية البيانات الحساسة مع السماح بمعالجتها دون الحاجة إلى فك تشفيرها مسبقًا. وتُعدّ هذه التقنية مناسبة بشكل خاص لبيئات الحوسبة السحابية، حيث تتطلب البيانات الطبية والطبّية الشرعية مستوىً عاليًا من الحماية.

يقدّم هذا العمل دراسةً لأهم مخططات التشفير المتماثل شكليًا، ولا سيما Paillier (PHE) وDGHV (SHE) وCKKS (FHE)، مع استعراض خصائصها ومزاياها وقيودها. كما تم إجراء دراسة حالة حول التقدير الآمن للفاصل الزمني بعد الوفاة (PMI) اعتمادًا على قانون هينسغه للتبريد (Henssge Cooling Law). وقد أجريت الحسابات على بيانات مشفّرة بهدف الحفاظ على سرية المعلومات المستخرجة من تقارير التشريح.

تُظهر النتائج التجريبية أن مخطط Paillier يوفّر دقة جيدة، إلا أنه يتطلب تكلفة حسابية مرتفعة. أما مخطط DGHV فيتيح تنفيذ العمليات المتماثلة شكليًا على الأعداد الصحيحة، لكنه يتطلب تقريبًا رياضيًا ويظل محدودًا بسبب تراكم الضوضاء. في المقابل، يبرز مخطط CKKSبوصفه الحل الأكثر ملاءمة للتطبيقات الطبية، بفضل قدرته على معالجة الأعداد الحقيقية مباشرةً مع تحقيق توازن جيد بين الدقة والأمان والأداء.

وأخيرًا، تم اقتراح مساهمة تعتمد على مقاربة مستوحاة من تقنية إعادة التهيئة (Bootstrapping)، بهدف التخفيف من تراكم الضوضاء في مخطط CKKS. وقد أظهرت النتائج المتحصل عليها تحسنًا في استقرار العمليات الحسابية وانخفاضا في نسبة الخطأ عند تقدير الفاصل الزمني بعد الوفاة (PMI)، مما يؤكد أهمية هذه المقاربة في تطبيقات الحوسبة الآمنة على البيانات الطبية المشفّرة.

الكلمات المفتاحية: التشفير المتماثل شكليًا، Paillier، DGHV، CKKS، الفاصل الزمني بعد الوفاة (PMI)، قانون هينسغه للتبريد، الحوسبة السحابية، أمن البيانات الطبية، تراكم الضوضاء.