UNIVERSITÉ DE LORRAINE

École doctorale IAEM Lorraine

Programmation DC et DCA pour certaines classes de problèmes en cryptographie

DC Programming and DCA for some classes of problems in cryptography

THÈSE

présentée et soutenue publiquement le 6 décembre 2023

pour l'obtention du

Doctorat de l'Université de Lorraine

(mention informatique)

par

NGUYEN Thi Tuyet Trinh

Composition du jury

Rapporteurs :	Viet Hung NGUYEN	Professeur, Université Clermont Auvergne
	Mounir HADDOU	Professeur, INSA de Rennes
Examinateurs :	Van Tien DO	Professeur, Université de technologie et d'économie de Budapest
	Anass NAGIH	Professeur, Université de Lorraine
	Van Dat CUNG	Professeur, Grenoble INP-UGA
Directrice de thèse :	Hoai An LE THI	Professeur, Université de Lorraine

Laboratoire de Génie Informatique, de Production et de Maintenance — EA 3096

Résumé

La cryptographie, l'art et la science de la communication sécurisée, a une longue et illustre histoire. Elle utilise des algorithmes mathématiques pour convertir des messages en clair en texte chiffré illisible, protégeant ainsi la confidentialité, l'intégrité et l'authenticité des données. Cette thèse vise à déployer des techniques d'optimisation avancées pour résoudre certaines classes de problèmes en cryptographie. Le thème principal de la thèse est d'appliquer des approches efficaces basées sur la programmation DC (Différence de fonctions Convexes) et DCA (algorithme DC) pour résoudre les problèmes de gestion dynamique centralisée des clés de groupe, la construction de l'arbre de Merkle dans les systèmes de transaction blockchain, et l'architecture autoencoder pour le cryptage et le décryptage de texte.

La thèse se compose de cinq chapitres. Le chapitre 1 présente des préliminaires sur la programmation DC et DCA, ainsi que sur la cryptographie. Le chapitre 2 étudie le problème de la mise à jour de la clé de groupe lorsque l'appartenance change dynamiquement dans la gestion centralisée des clés de groupe avec deux techniques : l'insertion par lots et la recomposition par lots. Nous proposons des modèles d'optimisation pour minimiser le coût de la remise en clé et maintenir l'arbre aussi équilibré que possible en même temps. Les deux objectifs importants mentionnés sont combinés dans un modèle d'optimisation unifié dont la fonction objective contient des fonctions discontinues avec des variables binaires, ce qui est connu pour être NP-hard. Nous reformulons le problème comme un programme DC standard qui peut être résolu efficacement par DCA. De plus, les nœuds d'insertion et de suppression doivent être des nœuds feuilles, nous introduisons un algorithme en deux étapes pour réduire la complexité du modèle. Dans le chapitre 3, nous proposons un modèle d'optimisation pour résoudre le problème de la construction d'une structure d'arbre de Merkle basée sur la distribution des transactions Ethereum. L'objectif est de minimiser le nombre de valeurs de hachage nécessaires pour mettre à jour les données de compte associées à chaque transaction et d'assurer l'intégrité des données dans le système Ethereum. En utilisant les techniques de pénalités exactes, nous reformulons ce programme quadratique binaire en un programme DC conventionnel qui peut être résolu efficacement par le DCA. Pour obtenir une meilleure approximation convexe de la fonction objective sans connaître la décomposition DC, nous appliquons DCA-Like, une nouvelle extension de DCA. En outre, nous déployons la DCA accélérée (ADCA) et la DCA-Like accélérée (ADCA-Like) pour améliorer la DCA et la DCA-Like en y incorporant la technique d'accélération de Nesterov. Nous combinons séparément les approches DCA, ADCA, DCA-Like et ADCA-Like avec l'algorithme "diviser pour régner" pour résoudre le problème lorsque le nombre de comptes est élevé. Un autoencodeur efficace et sûr pour le cryptage et le décryptage de texte est examiné au chapitre 4. Il s'agit d'une approche basée sur l'apprentissage profond utilisant des réseaux neuronaux, qui présente un degré élevé de confidentialité et représente le prochain développement de la cryptographie. Nous appliquons un nouvel algorithme stochastique appelé DCA stochastique à chaîne de Markov (MCSDCA) comme optimiseur dans diverses architectures d'autoencodeurs. Enfin, le chapitre 5 conclut la thèse.

Mots-clés: Gestion centralisée des clés de groupe, L'arbre de Merkle, transaction de la blockchain, Autoencoder, Programmation DC et DCA

Abstract

Cryptography, the art and science of secure communication, has a long, illustrious history. It uses mathematical algorithms to convert original messages into unreadable ciphertext, thereby protecting the data's confidentiality, integrity, and authenticity. Cryptography plays a crucial role in securing our information systems in the interconnected world of today, where immense quantities of sensitive data are transmitted and stored electronically. This thesis aims to deploy advanced optimization techniques for solving certain classes of problems in Cryptography. The main theme of the thesis is to propose the optimization model and apply efficient approaches based on DC (Difference of Convex functions) programming and DCA (DC Algorithm) to solve the problems of dynamic centralized group key management, Merkle tree construction in blockchain transaction systems, and autoencoder architecture for text encryption and decryption.

The thesis consists of five chapters. Preliminaries on DC programming and DCA, and cryptography are presented in Chapter 1. Chapter 2 studies the problem of updating the group key when membership changes dynamically in centralized group key management with two techniques: batch insertion and batch rekeying. We propose optimization models for minimizing the rekeying cost and keeping the tree as balanced as possible at the same time. The two mentioned important objectives are combined into a unified (deterministic) optimization model whose objective function contains discontinuous step functions with binary variables, which is known to be NP-hard. We reformulate the problem as a standard DC program that can be solved efficiently by DCA. Moreover, the insertion and deletion nodes must be the leaf nodes, we introduce a two-step algorithm to reduce the model's complexity. In Chapter 3, we propose an optimization model for solving the problem of constructing a Merkle tree structure based on the Ethereum transaction distribution. The objective is to minimize the number of hash values required to update the account data associated with each transaction and to ensure the integrity of data in the Ethereum system. Using the exact penalty techniques, we reformulate this binary quadratic program as a conventional DC program that is efficiently solvable by the DCA. To get better convex approximation of the objective function without knowing a DC decomposition, DCA-Like, a novel extension of DCA, is applied. Furthermore, we deploy Accelerated DCA (ADCA) and Accelerated DCA-Like (ADCA-Like) to improve DCA and DCA-Like by incorporating the Nesterov's acceleration technique into it. We separately combine DCA, ADCA, DCA-Like, and ADCA-Like approaches with the divide-and-conquer algorithm to solve the problem when the number of accounts is large. An efficient and secure autoencoder for text encryption and decryption is discussed in Chapter 4. This is a deep learning-based approach using neural networks, which has a high degree of confidentiality and represents the next development in cryptography. We apply a new stochastic algorithm called Markov chain stochastic DCA (MCSDCA) as the optimizer in various autoencoder architectures. Finally, Chapter 5 brings the thesis to a close.

Keywords: Centralized group key management, Merkle tree, blockchain transaction, Autoencoder, DC (Difference of Convex functions) programming and DCA (DC Algorithms)