COLLEGE ED MATHEMATIQUES
DOCTORAL STIC
PAYS DE LA LOIRE

Nantes Université

THÈSE DE DOCTORAT DE

NANTES UNIVERSITÉ

ÉCOLE DOCTORALE N° 641
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Informatique et Architectures numériques*

Par
Vincent KOWALSKI

Abstractions byzantines utiles au niveau de calculabilité de la mémoire partagée

Thèse présentée et soutenue à Nantes, UFR Sciences et Techniques, le 10 / 12 / 2025
Unité de recherche : LS2N

Rapporteurs avant soutenance :

Vincent GRAMOLI	Full Professor, University of Sydney
Antonio FERNÁNDEZ ANTA	Research Professor, IMDEA Networks

Composition du Jury :

Examinateurs :	Assia MAHBOUBI	Directrice de recherche, Nantes Université
	Sara TUCCI-PIERGIOVANNI	Directrice de laboratoire, Université Paris-Saclay
	Silvia BONOMI	Associate Professor, Sapienza Universitá di Roma
	Emmanuelle ANCEAUME	Directrice de recherche, IRISA
Dir. de thèse :	Achour MOSTÉFAOUI	Professeur, Université de Rennes
Encadrant :	Matthieu PERRIN	Maître de conférance, Nantes Université

COLLEGE ED MATHEMATIQUES
DOCTORAL STIC
PAYS DE LA LOIRE

Nantes Université

Titre : Abstractions byzantines utiles au niveau de calculabilité de la mémoire partagée

Mot clés : Faute Byzantine, Registre, Broadcast primitive, Message ordering, Vie privée.

Résumé : Ces dernières années, les blockchains sont devenues un sujet majeur de recherche, tant dans le milieu académique qu'industriel, avec l'émergence de nombreuses variantes et applications. Cependant, le concept fondamental de blockchain repose sur la création d'un ordre total entre les opérations d'un système, ce qui engendre d'importants défis en termes de performance et de scalabilité dans des contextes soumis à des fautes et attaques Byzantines. Pour répondre à ces problèmes, le projet ByBloS explore l'utilisation de garanties allégées, que de nombreuses applications basées sur la blockchain peuvent adopter, permettant ainsi des solutions plus efficaces et évolutives.

ByBloS se concentre sur trois objectifs principaux : (1) développer des abstractions légères, (2) effectuer la transition des systèmes fermés vers des systèmes ouverts, et (3) garantir la confidentialité dans des systèmes Byzantins. Cette thèse aborde principalement le premier objectif à travers trois contributions : spécifier et comparer la calculabilité de trois abstractions de registres Byzantins, définir une abstraction de diffusion équivalente à un registre Byzantin, et optimiser une abstraction de diffusion pour des instantanés Byzantins. Elle contribue également au troisième objectif en définissant et en implémentant un registre Byzantin qui restreint l'accès aux processus autorisés.

Ce travail s'aligne sur les objectifs de ByBloS, en faisant progresser la conception de mécanismes légers et efficaces pour des systèmes tolérants aux fautes Byzantines.

Title: Useful byzantine abstraction at computability level of shared memory

Keywords: Byzantine fault, Register, Broadcast primitive, Message ordering, Privacy.

Abstract: In recent years, blockchains have become a major focus of academic and industrial research, with numerous variations and applications emerging. However, the core blockchain concept relies on creating a total order among system operations, which poses significant performance and scalability challenges in contexts subject to faults and Byzantine attacks. To address these issues, the ByBloS project explores the use of lighter guarantees that many blockchain-based applications can adopt, enabling more efficient and scalable solutions.

ByBloS focuses on three objectives: (1) developing lightweight abstractions, (2) transitioning from closed to open systems, and (3) ensuring privacy in Byzantine systems. This thesis primarily addresses the first objective through three contributions: specifying and comparing the computability of three Byzantine register abstractions, defining a broadcast abstraction equivalent to a Byzantine register, and optimizing a broadcast abstraction for Byzantine snapshots. Additionally, it contributes to the third objective by defining and implementing a Byzantine register that restricts access to authorized processes.

This work aligns with ByBloS's goals, advancing the design of efficient, lightweight mechanisms for Byzantine-tolerant systems.