## RÉSUMÉ

Cette thèse vise à développer des méthodes efficientes et mathématiquement rigoureuses afin d'améliorer la fiabilité des logiciels en utilisant l'interprétation abstraite, un cadre formel pour approximer les comportements des programmes. Nous développons un cadre quantitatif pour mesurer l'influence des variables d'entrée sur le comportement des programmes, aidant ainsi à certifier les comportements corrects et à identifier les défauts. Le cadre proposé est flexible, permettant différentes mesures d'impact et garantissant des résultats rigoureux, ce qui signifie que l'impact calculé sera toujours une surestimation ou une sous-estimation. Ce cadre est appliqué à la fois aux propriétés extensionnelles, qui mesurent le comportement entrée-sortie, et aux propriétés intentionnelles, qui évaluent des détails computationnels comme les itérations de boucles. Il a été implémenté dans trois outils : IMPATTO, LIBRA et TIMESEC. Ces outils ciblent respectivement la fiabilité générale des logiciels, l'équité dans les réseaux de neurones et les vulnérabilités de canaux auxiliaires. Les évaluations expérimentales ont validé ces outils, démontrant leur efficacité dans divers cas d'utilisation, tels que la détection de biais dans les réseaux de neurones et les vulnérabilités dans les bibliothèques cryptographiques. Dans l'ensemble, ce travail améliore la compréhension de l'utilisation des données d'entrée dans les logiciels, offrant à la fois des perspectives théoriques et des outils pratiques pour améliorer la fiabilité et la sécurité des systèmes.

## MOTS CLÉS

interprétation abstraite ⋆ analyse statique ⋆ méthodes formelles ⋆ vérification quantitative ⋆ réseaux de neurones ⋆ propriétés de sécurité

## ABSTRACT

This thesis aims to develop efficient, mathematically sound methods to improve software reliability using abstract interpretation, a formal framework for approximating program behaviors. We develop a quantitative framework to measure how much input variables affect program behavior, helping to certify correct behaviors and identify flaws. The proposed framework is flexible, allowing different measures of impact and ensuring sound results, meaning the calculated impact will always be an over- or under-approximation. This framework is applied to both extensional properties, which measure input-output behavior, and intensional properties, assessing computational details like loop iterations. It was implemented in three tools: IMPATTO, LIBRA, and TIMESEC. These tools target general software reliability, fairness in neural networks, and side-channel vulnerabilities, respectively. Experimental evaluations validated the tools, showing their effectiveness in various use cases, such as detecting biases in neural networks and vulnerabilities in cryptographic libraries. Overall, this work improves the understanding of input data usage in software, offering both theoretical insights and practical tools for improving system reliability and security.

## KEYWORDS

abstract interpretation ⋆ static analysis ⋆ formal methods ⋆ quantitative verification ⋆ neural networks ⋆ security properties