Prix de thèse Gilles Kahn
Palmarès 2025

La Société Informatique de France (SIF) est ravie d'annoncer les récipiendaires 2025 du prix de thèse Gilles Kahn. Ce prix, placé sous le patronage de l'Académie des Sciences, attribué chaque année depuis 1998, met en lumière de jeunes scientifiques dont les travaux de thèse constituent une avancée remarquable pour la discipline informatique. Le prix 2025 est décerné à **Margot Hérin** pour sa thèse intitulée « *Learning Preference Models: A Marriage between Decision Theory and Machine Learning* » préparée au LIP6, UMR 7606 (CNRS), Sorbonne Université. Les deux accessits sont décernés, par ordre alphabétique, à **Son Ho** pour sa thèse intitulée « *Formal Verification of Rust Programs by Functional Translation* » réalisée à Inria Paris et **Corentin Jeudy** pour sa thèse intitulée « *Design of Advanced Post-Quantum Signature Schemes* » préparée à l'IRISA, UMR 6074 (CNRS), Inria, Université de Rennes et Orange, qui reçoit en outre la mention « thèse à portée industrielle ».

La thèse de **Margot Hérin**, intitulée « *Learning Preference Models: A Marriage between Decision Theory and Machine Learning*», s'inscrit dans le domaine de l'intelligence artificielle, à l'interface de la théorie de la décision, de la recherche opérationnelle et de l'apprentissage automatique. Ses travaux visent à concilier des propriétés jusqu'alors difficiles à réunir, mais essentielles pour de nombreuses applications d'aide à la décision : concevoir des systèmes de recommandation à la fois expressifs, interprétables et multicritères, tout en conservant de bonnes performances calculatoires.

Margot Hérin

Margot Hérin montre qu'il est possible d'apprendre des modèles décisionnels très riches, capables de représenter des interactions complexes entre de nombreux critères, tout en conservant une structure compréhensible. En introduisant des principes de parcimonie et en les déclinant dans des scénarios d'apprentissage variés, ses travaux permettent de traiter des problèmes de bien plus grande dimension que l'état de l'art, ce qui constitue une avancée majeure pour le domaine.

*Le jury a été particulièrement impressionné par la largeur et la profondeur des contributions de **Margot Hérin**, ainsi que par la qualité remarquable de la rédaction du manuscrit, permettant de rendre accessibles des concepts complexes. L'ampleur des résultats théoriques, systématiquement accompagnés de validations expérimentales sur des problèmes réels, ainsi que la reconnaissance internationale de ces travaux à travers des publications dans les meilleures conférences et journaux, font de cette thèse une contribution scientifique de tout premier plan.*

La thèse de **Son Ho**, « *Formal Verification of Rust Programs by Functional Translation*», s'inscrit dans le domaine de la vérification formelle, où l'un des défis majeurs consiste à concilier l'efficacité des programmes bas-niveau avec la capacité à produire des preuves modulaires capables de s'abstraire de ces détails, afin de raisonner plus aisément sur des logiciels de grande ampleur.

Son Ho

Son Ho a contribué à plusieurs avancées dans ce domaine, couvrant un large spectre allant des fondations théoriques aux outils pratiques. Il a d'abord proposé une approche modulaire basée sur l'évaluation partielle pour la vérification d'un langage de protocoles cryptographiques permettant de produire des implémentations efficaces et prouvées de protocoles d'établissement de canaux sécurisés. Il a ensuite développé une méthodologie de preuve modulaire pour les constructions cryptographiques telles que les fonctions de hachage, dont certaines de ses implémentations sont aujourd'hui utilisées dans des environnements industriels comme la bibliothèque standard de Python. Enfin, Son Ho a posé les bases théoriques et conçu les outils pour la vérification formelle de programmes Rust via transformations fonctionnelles, en définissant une sémantique purement fonctionnelle pour la partie sûre du langage, intégrant son modèle d'emprunts. Une traduction fonctionnelle vers un λ-calcul pur permet ensuite l'utilisation d'outils de preuve matures tels que Lean ou Rocq pour raisonner sur des programmes Rust.

Le jury a été impressionné par le large spectre couvert dans cette thèse, des aspects fondationnels aux aspects pratiques, avec un impact avéré dans les différentes communautés scientifiques correspondantes. Il souligne également le souci constant de transférer ces résultats vers des environnements réels, qui confère aux travaux de Son Ho un impact industriel notable.

La thèse de **Corentin Jeudy**, intitulée « *Design of Advanced Post-Quantum Signature Schemes* » s'intéresse à des solutions cryptographiques pour se prémunir de la menace quantique. Les avancées récentes permettent d'augmenter les performances et d'élargir l'utilisation. Notamment, une question d'actualité est celle des accréditations anonymes qui permettent de garder son anonymat lorsqu'on certifie son appartenance à un groupe, comme la vérification de l'âge en ligne.

Corentin Jeudy

La solution qui a reçu la standardisation NIST à l'issue de la compétition Post Quantum est celle des réseaux euclidiens. Les schémas de signature intégrés dans le protocole https sont basés sur des instances structurées des problèmes sous-jacents. Contrairement au instances générales où les clés publiques sont des matrices carrées et demandent un espace de stockage quadratique, les instances structurées demandent un espace linéaire. Les travaux de Corentin Jeudy se distinguent par une meilleur utilisation des distributions gaussiennes, qui a été validé par un très grand nombre de publications.

Lorsqu'il aborde l'accréditation anonyme, Corentin Jeudy propose le premier schéma basé sur les réseaux euclidiens, intitulé Phoenix. Une analyse théorique d'excellence scientifique est prolongée par une implantation rapide en C.

Le jury a été impressionné par l'importance des contributions de la thèse, depuis les principes fondamentaux de la sécurité jusqu'à une implémentation. Il souligne également le caractère novateur des contributions puisqu'il s'agit d'un des premiers schémas sécurisés post-quantiques pour la cryptographie avancée. Le jury a noté l'impact industriel de la thèse, qui s'est déroulée dans le cadre CIFRE entre Orange et un laboratoire de recherche universitaire.

Société informatique de France
Qui sommes-nous ?

Créée en 2012 – Association reconnue d'utilité publique

Société savante d'informatique en France, la SIF a vocation à rassembler toutes celles et ceux pour qui faire progresser l'informatique est un métier ou une passion, qu'ils soient issus du monde académique ou socio-économique. Elle vise en particulier à :

- Animer sa communauté scientifique et technique ;
- Contribuer à la culture des citoyennes et citoyens ;
- Accompagner l'enseignement de la discipline du primaire au supérieur ;
- Participer aux débats de société en lien avec l'informatique.

Contacts presse
Président : Yves Bertrand, president@societe-informatique-de-france.fr,
Coordinatrice communication : Sylvie Alayrangues, sylvie.alayrangues@societe-informatique-de-france.fr

Institut Henri Poincaré
11 rue Pierre et Marie Curie
75231 PARIS CEDEX 05

Socinfo.fr