MCF en Section 27 à l'UNC
Enseignements : Département Sciences et Techniques
Recherche : ISEA (Institut de Sciences Exactes et Appliquées)

Tél. pro. : (+687) 29 02 66
tania.richmond@unc.nc

Tania Richmond

Curriculum Vitae - Synthèse

Parcours professionnel

2023-auj.	**Maîtresse de Conférences** en Informatique à l'Université de la Nouvelle-Calédonie
2020-2023	**Ingénieure** évaluatrice de ressources crypto dans l'équipe d'eXpertise de Composants de Sécurité à DGA-MI
2017-2020	**Post-doctorante** dans l'équipe TAMIS à l'Inria Rennes - Bretagne Atlantique
2016-2017	**ATER** en Informatique à l'Université de Toulon (temps plein)
2015-2016	**ATER** en Informatique à l'Université de Toulon (temps partiel)
2012-2015	**Contrat doctoral élargi** à l'Université Jean Monnet, à Saint-Étienne

Formation

2012-2016	**Doctorat** en Informatique à l'Université Jean Monnet, à Saint-Étienne
2010-2012	**Master** Mathématiques spécialité Cryptologie et Sécurité Informatique à l'Université Bordeaux 1
2007-2010	**Licence** Mathématiques et Informatique à l'Université de la Nouvelle-Calédonie

Activités de recherche

Thèmes — Cryptographie post-quantique, codes correcteurs d'erreurs, attaques par canaux auxiliaires.

Projets
- Étudier les attaques possibles sur les protocoles cryptographiques basés sur les codes correcteurs d'erreurs soumis à la standardisation post-quantique du NIST ;
- Étendre mes travaux aux schémas de signature et à la métrique rang.

Encadrements — Thèse de Jean-François Quinquis à l'ISEA (2024-2029).
Thèse d'Agathe Cheriere à l'IRISA, soutenue le 19 Décembre 2023.

Collaboration — CROWD (Cryptography with Skew Codes) : projet de recherche franco-allemand qui a débuté en Janvier 2023 pour 3 ans, en association avec l'IRISA.

Travaux (récents)

Thèse — *Implantation sécurisée de protocoles cryptographiques basés sur les codes correcteurs d'erreurs*
soutenue le 24 Octobre 2016 devant le jury : Viktor Fischer (directeur de thèse, Pr), Pierre-Louis Cayrel (co-encadrant, MCF), Marine Minier (rapporteuse, Pr), Arnaud Tisserand (rapporteur, DR) et Jean-Claude Bajard (examinateur, Pr).

Publications
Exploiting ROLLO's Constant-Time Implementations with a Single-Trace Analysis (Extended Version) accepté au journal *Designs, Codes and Cryptography 2023*
BIKE Key-Recovery : Combining Power Consumption Analysis and Information-Set Decoding accepté à la conférence *Applied Cryptography and Network Security 2023*
Exploiting ROLLO's Constant-Time Implementations with a Single-Trace Analysis présenté au *Workshop on Coding and Cryptography 2022*
Automatic Ladderisation : Improving Code Security through Rewriting and Dependent Types accepté à la conférence *Partial Evaluation and Program Manipulation 2022*
A Hole in the Ladder : Interleaved Variables in Iterative Conditional Branching.
accepté à la conférence *IEEE International Symposium on Computer Arithmetic 2020*
Improving Side-Channel Analysis through Semi-Supervised Learning
accepté à la conférence *Smart Card Research and Advanced Application Conference 2018*
Statistical Model Checking of Incomplete Stochastic Systems accepté à la conférence *International Symposium On Leveraging Applications of Formal Methods, Verification and Validation 2018*
Survey on cryptanalysis of code-based cryptography : from theoretical to physical attacks
accepté à la conférence *International Conference on Computers Communications and Control 2018*

Pré-publications
A Hole in the Ladder : Interleaved Variables in Iterative Conditional Branching (Extended Version)
soumis dans un journal

Enseignements (récents)

2023 — 148h - Mathématiques pour l'Informatique (L1), Programmation avancée et complexité (L2), Logique et programmation logique (L3), Décidabilité et théorie de la complexité (L3) à l'Université de la Nouvelle-Calédonie.