# Randomisation of NTT to counteract side channel analysis of RLWE cryptosystem

Christophe Negre*[1], Vincent Zucca , and Mbaye Ngom

[1]Equipe DALI (UPVD, LIRMM-UM2) (DALI-LIRMM) – Université de Perpignan, LIRMM – France

**Résumé**

.

*Intervenant