Université de Bretagne Occidentale

Ecole Doctorale

*Mathématiques et Sciences et Technologies de l'Information et de la Communication*

*Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance*

**AVIS DE SOUTENANCE DE THESE**

**Le mardi 25 mai 2021**

à l'Université de Bretagne Occidentale, Brest.

**Monsieur DJATH LIBEY OKONFU**

soutiendra une thèse de doctorat sur le sujet suivant :

" Accélérateurs matériels RNS flexibles pour la cryptographie asymétrique à haute sécurité ".

**Le jury sera ainsi composé :**

**- M. BAJARD JEAN-CLAUDE, Professeur des universités**
Sorbonne Université - PARIS 05EME

**- M. BIGOU KARIM, Maître de conférences**
Univ. de Bretagne Occidentale - BREST

**- MME CHOTIN ROSELYNE, Maître de conférences**
Sorbonne Université - PARIS 05EME

**- M. DIDIER LAURENT-STEPHANE, Professeur des universités**
Université de Toulon - LA GARDE

**- M. NEGRE CHRISTOPHE, Maître de conférences**
Université de Perpignan - PERPIGNAN

**- M. TISSERAND ARNAUD, Directeur de Recherche**
Université Bretagne Sud - LORIENT

**invité(e) :**

**- M. GERARD BENOIT, Expert**
DGA - BRUZ

A BREST, le 12 avril 2021

Le Président de l'Université de Bretagne Occidentale,

UNIVERSITE DE BRETAGNE OCCIDENTALE

**M. GALLOU**

DOCTORAT BRETAGNE LOIRE MATHSTIC

Université de Bretagne Occidentale

**Titre :** Accélérateurs matériels RNS flexibles pour la cryptographie asymétrique à haute sécurité

**Mot clés :** arithmétique des ordinateurs, système modulaire de représentation des nombres, flexibilité, implantation matérielle sur FPGA.

**Résumé :** Les implantations RNS de cryptosystèmes asymétriques actuels utilisent des ressources matérielles correspondant à la taille des opérandes traitées. Dans cette thèse, nous proposons une nouvelle approche dans l'implantation RNS de cryptosystèmes asymétriques qui permet une utilisation flexible de ressources matérielles. Dans un premier temps, un nouvel algorithme d'extension de base est présenté. Les extensions de bases sont, de part leurs coûts, des opérations critiques dans les implantations RNS. Notre nouvel algorithme d'extension de base utilise une approche hiérarchique dans le calcul du théorème chinois des restes. Comparé à l'algorithme d'extension de base de l'état de l'art, il présente un coût théorique réduit, qui se traduit par un gain en surface et en temps dans nos implantations HLS sur FPGA. Ensuite, nous implantons les deux algorithmes d'extension de base à partir de la nouvelle approche d'implantation RNS. Enfin, des multiplications scalaires utilisant chacune des deux extensions de base sont implantées avec la nouvelle approche. Nos implantations HLS sur FPGA utilisent des ressources matérielles en quantité flexible. De plus, quoique comparables en compromis surface/temps à ceux de l'état de l'art, la plupart de nos résultats sont bien plus petits.

**Title:** RNS-Flexible Hardware Accelerators for High-Security Asymmetric Cryptography

**Keywords:** computer arithmetic, residue number system, flexibility, FPGA hardware implementation.

**Abstract:** Asymmetric cryptosystems are implemented in RNS using a quantity of hardware resources corresponding to the size of the cryptographic operands. In this thesis we propose a new approach to perform RNS implementations of asymmetric cryptosystems that leads to a flexible utilization of hardware resources. We start with describing a new method to perform base extensions which are crucial operations in RNS implementations of asymmetric cryptosystems. The proposed base-extension method, based on a hierarchical approach for computing the Chinese remainder theorem, introduces a reduction of the theoretical cost. Our FPGA implementations using HLS show an area and time gain compared with the state-of-the-art method. Then, we demonstrate the practicality of our new RNS-implementation approach on the two base-extension methods. Last, elliptic curve scalar multiplications based on the two base-extension methods are implemented using our RNS-implementation approach. Our FPGA implementations use a flexible quantity of hardware resources. Besides, although comparable with state-of-the-art ones in area *vs.* time trade-offs, most of our solutions are much smaller.