SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Generating Residue Number System Bases

Jean-Claude Bajard * Kazuhide Fukushima † Shinsaku Kiyomoto † Thomas Plantard ‡
Arnaud Sipasseuth † Willy Susilo ‡

Keywords: Residue Number Systems

Abstract

Residue number systems provide efficient techniques for speeding up calculations and/or protecting against side channel attacks when used in the context of cryptographic engineering. One of the interests of such systems is their scalability, as the existence of large bases for some specialized systems is often an open question. In this paper, we present highly optimized methods for generating large bases for residue number systems and, in some cases, the largest possible bases. We show their efficiency by demonstrating their improvement over the state-of-the-art bases reported in the literature. This work make it possible to address the problem of the scalability issue of finding new bases for a specific system that arises whenever a parameter changes, and possibly open new application avenues.

* Sorbonne Université, CNRS, INRIA, Institut de Mathématiques de Jussieu-Paris Rive Gauche, Ouragan, F-75005 Paris, France, (jean.bajard@inria.fr)

† Information Security Laboratory of KDDI Research Inc, 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan, (ka-fukushima@kddi-research.jp, kiyomoto@kddi-research.jp, ar-sipasseuth@kddi-research.jp)

‡ Institute of Cybersecurity and Cryptology, University of Wollongong, Australia, (thomaspl@uow.edu.au, wsusilo@uow.edu.au)