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

高速 RNS モンゴメリ乗算器の小面積化のためのパラメータ選択法
Parameter Selection Method for Small Area of Fast RNS Montgomery Multiplier

芳賀 陸雄 * 森本 康太 * 藤本 大介 * 川村 信一 †
Rikuo Haga Kota Morimoto Daisuke Fujimoto Shinichi Kawamura
林 優一 *
Yuichi Hayashi

キーワード Residue Number System, RNS モンゴメリ乗算器, 小規模回路, 面積時間積

あらまし

近年の IoT(Internet of Things) 機器の急激な増加に伴い、IoT 機器上で公開鍵暗号を扱う需要が高まっている。IoT 機器で公開鍵暗号を扱うためには小規模な回路で高速に剰余乗算を行う必要がある。RNS(Residue Number System) 表現を用いたモンゴメリ乗算器 [1] は回路規模を抑えることができ、さらにその上で高速化を実現する RNS のパラメータの選択方法 [2] も提案されている。しかし、これらの回路規模の評価は、FPGA(Field Programmable Gate Array) に実装した際の DSP(Digital Signal Processor) 数や Slice 数で行われており、全体の回路規模を単純に比較することが困難であり、回路規模を考慮した実装パラメータを選択することが困難であった。そこで、本研究では、RNS モンゴメリ乗算器を構成する大きな要素が乗算器と加算器が支配的であると考え、それらの回路規模を全加算器で換算し、実装パラメータ毎の回路規模を比較する手法を提案する。この手法を用いて、過去の検討でなされた高速な実装パラメータに加えて回路規模を評価し、高速かつ小規模な実装パラメータの選択例を示す。

参考文献

[1] Gavin Xiaoxu Yao,Junfeng Fan, Ray CC Cheung, and Ingrid Verbauwhede,“Faster Pairing Coprocessor Architecture,” In International Conference on Pairing-Based Cryptography，pp.160-176, Springer, 2012

[2] Gavin Xiaoxu Yao,Junfeng Fan, Ray CC Cheung, and Ingrid Verbauwhede. “Novel RNS Parameter Selection for Fast Modular Multiplication,” IEEE Transaction on Computers, Institute of Electrical and Electornics Engineers 63 (8), pp.2099-2105,2014

* 奈良先端科学技術大学院大学,
Nara Institute of Science and Technology,
1916-5 Takayama-cho, Ikoma-shi, Nara, 630-0192, Japan
† 産業技術総合研究所,
National Institute of Advanced Industrial Science and Technology,
2-3-26 Aomi, Koto-ku, Tokyo, 135-0064, Japan