先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	情報セキュリティ工学 （林　優一　（教授））		
学籍番号	2411110	提出日	令和 8年 1月 19日
学生氏名	小泉　理久		
論文題目	CRYSTALS-Kyber向け数論変換器のDSP非依存設計とエネルギー効率化に関する研究		

要旨

量子計算機の実用化に伴い、現行の暗号方式、特に公開鍵暗号の安全性低下が懸念されるため、耐量子計算機暗号（PQC）の標準化が国際的に進められている。こうした背景のもと、米国国立標準技術研究所（NIST）は鍵カプセル化方式としてCRYSTALS-Kyberを標準化した。一方、同方式では数論変換（NTT）における剰余乗算が計算負荷の主要なボトルネックとなっていることから、電力制約下での適用に向けたエネルギー効率の向上が課題である。従来のFPGA実装の多くはDSPを用いた乗算器に依存しており、特定デバイスに依存した評価にとどまるとともに、ASIC等への移植性にも課題があった。本研究では、将来的なASIC実装への移行を見据え、DSPに依存しない論理回路ベースの剰余乗算パイプラインを設計し、エネルギー最適化を行った。DSP不使用条件でFPGA上の評価を実施した結果、既存手法と比較してスループットが向上し、面積・遅延・エネルギーの各指標において総合的な効率改善を達成した。