ISS-P-124

複数アルゴリズムに対応した暗号回路の構成法に関する研究

濱口　朋浩†　　渡邊　誠也†　　名古屋　彰†
†岡山大学大学院自然科学研究科

1. はじめに

近年，暗号化技術は重要なものとなっており，SSL などの暗号通信において，サーバの負荷を軽減するためにSSL アクセラレータなどの暗号処理を行う専用回路が用いられている．しかし，多くのアルゴリズムに対応した暗号回路の実装にはコストがかかる．そこで，本研究では複数の暗号アルゴリズムに対応した回路を実装し，各暗号アルゴリズムの共通部分における回路の共有化を行い回路規模の削減を図った．

2. 実装方法

ハードウェア記述言語 SFL[1]を用いて AES，Camellia，CLEFIA の 3 種類の暗号アルゴリズムに対してマルチサイクル実装およびパイプライン実装を行った．また，共有化の効果を確認するためにサイクル数やステージ数の異なる複数の実装を行った．

3. 共有化方法

本研究では以下の 2 種類の方法で共有化を行った．

(1) S-box の共有化

AES と Camellia の S-box の$GF((2^4)^2)$において共有化を行った．実装した共有化 S-box を図 1 に示す．

(2) パイプラインレジスタの共有化

パイプライン実装は，様々なステージ数による実装を行い，パイプラインレジスタを共有化した.パイプラインレジスタの挿入箇所の例を図 2 に示す．

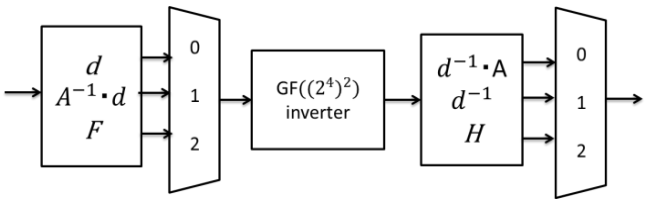

図 1: 共有化 S-box(0:AES 暗号化，1:AES 復号，2:Camellia)

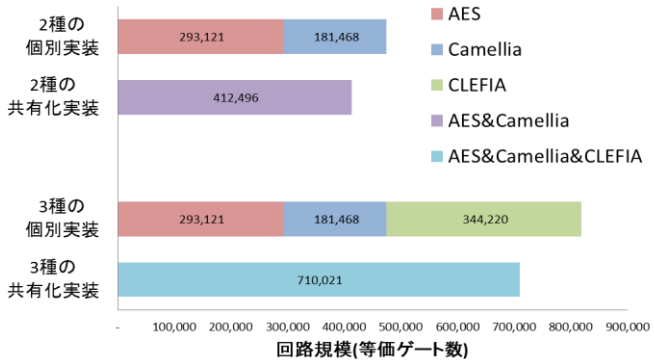

図 3: パイプライン実装の回路規模

4. 評価

PARTHENON[1]により得られた論理合成結果から，例としてパイプライン実装(AES: 10 ステージ，Camellia: 9 ステージ，CLEFIA: 9 ステージ)の回路規模を図 3 に示す．パイプライン実装において，個別にそれぞれ実装した回路と比較すると最大で約 13%のゲート数が削減できており，共有化の効果を確認できた．

上記の各回路を FPGA 向けに論理合成した結果，共有化した回路のスループットは個別実装した回路の約 66.2%になった．

5. 今後の課題

さらに多くの暗号アルゴリズムに対応した回路の実装や，CLEFIA における共有化 S-box の実装が挙げられる．

参考文献

[1] 小栗 清，中村 行宏，野村 亮，名古屋 彰，“主要なハードウェア記述言語の特徴と標準化状況SFL，” 情報処理, vol. 33, no. 11, pp. 1256－1262, 1992.

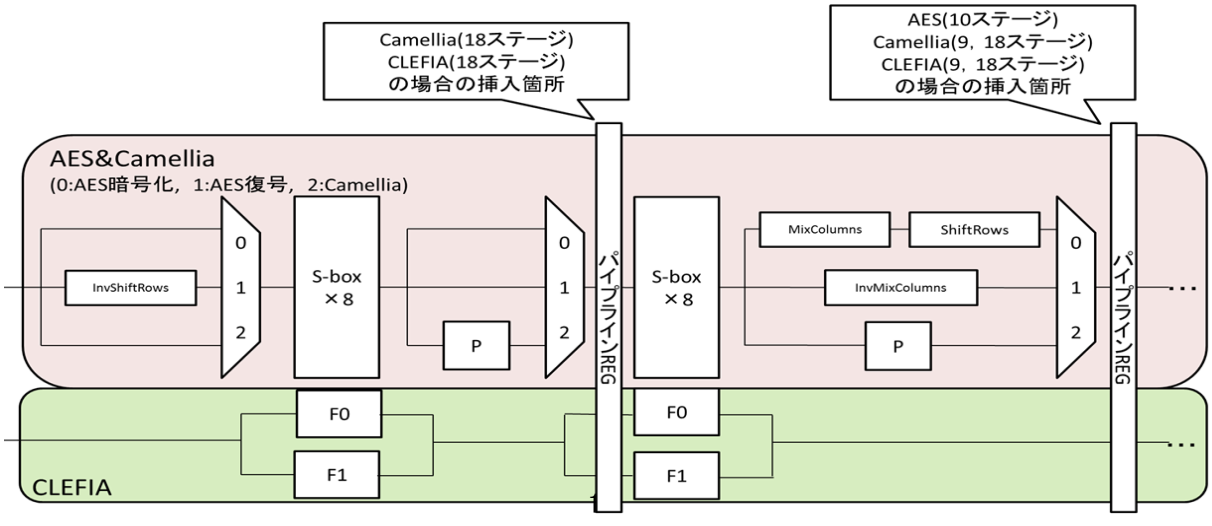

図 2 データ攪拌部の一部におけるパイプラインレジスタの挿入箇所