高位合成を用いた共通鍵ブロック暗号 CLEFIA の FPGA 上への実装と性能評価

情 19-0017　井口　大雅
指導教員　　桑門　秀典

1. はじめに

FPGA は現場で回路構成を書き換えることができるという特性を持ち、処理に応じた専用の回路を書き込むことで、CPU よりも高速な処理を可能にする。従来、回路構成の書き込みにはハードウェア記述言語が用いられてきたが、C 言語などの高級言語での書き込みを可能とする高位合成が登場し、注目されている。

本研究では、より高速で安全な情報セキュリティシステムの構築を目的とし、共通鍵ブロック暗号アルゴリズムの１つである CLEFIA[1]を高位合成によって FPGA 上に実装し、CPU 上での実行速度との比較を行う。

2. 研究方法

本研究では共通鍵ブロック暗号アルゴリズムに CLEFIA を用いる。このプログラムについては、ソニー株式会社が公開している C 言語のリファレンスコード[2]を参考に独自編集したものである。また、FPGA ボードには、内蔵 CPU ブロック（以下、内蔵 CPU ブロックを PS、FPGA ブロックを PL とする）に ARM Cortex-A9 が搭載されている Digilent 社製 PYNQ-Z1 を用いた。
この研究は次の手順でおこなう。

(1) CLEFIA の C 言語プログラムを作成する。
(2) (1)にディレクティブを付与し、高位合成したビットストリーム（回路情報）を PL に書き込み、Python から呼び出して実行する。
(3) (1)をコンパイルして生成した実行ファイルを PS 上で実行する。
(4) (2),(3)について処理時間を測定し比較を行う。

(2)に関して、高位合成には Vitis HLS 2022.1 及び Vivado 2022.1 を使用し、Vivado 2022.1 による回路規模と、消費電力の推定値を調べた。

3. 実験結果

上記手順(2)、(3)においてメッセージ長 16bytes、共通鍵 32bytes のデータ転送と実行をそれぞれ 2 の 17 乗回ずつ行い、処理時間の平均を取った結果を表 1 に示す。

表１を見ると、PL を用いて実行するよりも、PS だけで実行した方が速いことがわかる。ただし、PS のみの実行は、鍵長によって処理時間にばらつきが大きいのに対し、PL を用いた場合、ばらつきがほとんどなくなる結果となった。

	鍵長[bits]	PS	PL
暗号化	128	29901	150582
	196	41087	151675
	256	45070	155807
復号	128	29681	157314
	196	40830	158763
	256	44815	157086

表１　処理時間(ns)の平均の比較

PL を用いて処理を行う際にボトルネックとなり得るのがデータ転送時間である。そこで、(1)のプログラムの暗号化/復号関数内を空にし、引数の受け渡しのみを行なった際にかかる時間の平均をとることで、データ転送にかかる時間を調べた。その結果が表２である。

	PS	PL
データ転送時間	27	149568

表２　データ転送時間(ns)の平均の比較

表１と表２を見比べると、PL を用いた際の処理時間のほとんどをデータ転送時間が占めていることがわかった。

最後に、Vivado 2022.1 の機能によって得た消費電力と回路規模を表３に示す。回路規模については鍵長が大きくなるほど、使用するリソースも多くなっていた。

	鍵長[bits]	消費電力[W]	BRAM[x18KB]	DSP[個]	FF[個]	LUT[個]
暗号化	128	1.593	2.5	0	5734	6388
	196	1.434	3.5	0	7784	8368
	256	1.678	4.5	0	8855	9093
復号	128	1.413	2.5	0	6262	6917
	196	1.675	4.5	0	7859	8507
	256	1.745	4.5	0	9112	9719

表３　消費電力と回路規模

4. まとめ・考察

本研究では、より高速で安全な情報セキュリティシステムを構築するために、CLEFIA を FPGA 上で実行した際の処理時間について調査した。その結果、PL を用いずに PS だけで実行した方が処理時間が短くなる結果となった。ただし、PS だけでの処理は鍵長によって、処理時間にばらつきが生じるのに対し、PL を用いて計算することでばらつきがほとんど生じなくなる結果となった。その理由として、PS のみの場合では処理時間の大半を暗号化/復号の計算が占めているのに対し、PL を用いた場合ではデータ転送時間がその大半を占めていることが考えられる。リソースの観点からは、鍵長が大きくなるほど多くのリソースを使うことがわかった。

今回の実験では、PL を用いる際のデータ転送に MMIO（メモリーマップによるデータ転送）を用いたが、DRAM を介してデータの読み書きをする DMA を用いることで、PS と PL 間のデータ転送時間が短くなるとされている。今後は、DMA を用いたデータ転送時間の評価や CLEFIA 以外の暗号化アルゴリズムを実行した際の評価を行い、FPGA が実生活でより身近なものとして活用される余地があるのか検討することが課題である。

参考文献

[1] CLEFIA　最終閲覧日 2023/1/9
https://www.sony.co.jp/Products/cryptography/clefia/
[2] ソニー株式会社のリファレンスコード　最終閲覧日 2023/1/9
https://www.sony.co.jp/Products/cryptography/clefia/download/data/clefia_ref.c