DES暗号のためのデータ依存回路設計と評価

指導教官 市川周一　　学籍番号 023737　宮本雅人

1　はじめに

DES 暗号は共通鍵暗号アルゴリズムの一つで，米国では政府標準の暗号化手法の 1 つになっている [1].

一般に論理回路の入力が定数であれば，回路規模を削減し，動作速度を向上させることができる．生成された回路は入力データに依存するため “データ依存回路” と呼ばれる．データ依存回路では，入力データ毎に回路を生成する必要がある．そのため，再構成可能な LSI である FPGA を利用して実装することが前提となる．

本研究の目的は DES アルゴリズムのデータ依存回路を設計し，論理規模，動作速度を評価することである．

2　DES アルゴリズム

図 1 に DES アルゴリズムの概要を示す.

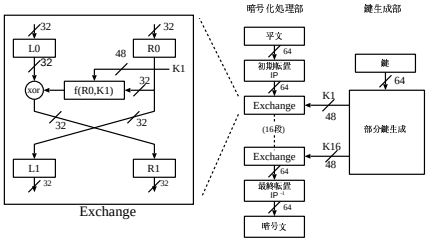

図 1: DES アルゴリズムの概要図

鍵生成部では，入力鍵から 16 個の部分鍵 (subkey) を生成し，暗号処理部へ送る．暗号処理部では，転置と置換を 16 段繰り返す.

3　設計

本研究では，評価の基本として，descracker[2] の DES 処理部 (VHDL ソース) を利用した．以下，これを DESc と呼ぶ (図 2). DESc は初期化を合わせて 17 サイクルで 64 ビットの平文を暗号化する.

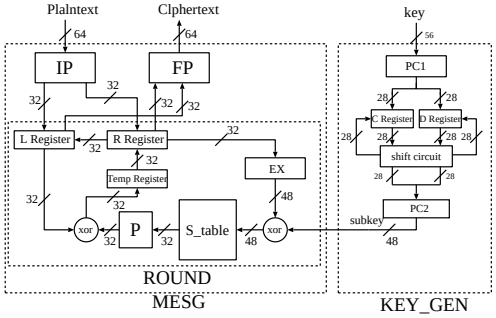

図 2: DESc

DESc を元に以下の回路を作成・評価した.

DESo DESc を FPGA 用に最適化した回路．転置を行う部分は，すべて 1 ビットごとの代入文に書き換えた.

DESd1 DESo の入力鍵を固定し，復号化を行う回路を取り除いた回路 (以降の回路はすべて暗号化のみとする).

DESd2 DESo の 16 段の部分鍵を固定した回路．入力鍵からあらかじめ 16 個の部分鍵を計算して回路記述を生成することにより，KEY_GEN 部分の回路を省略することができる．xor の入力 (subkey) が定まれば，xor を代入文に置き換えることができる．例えば，“y <= x xor 1” を “y <= not x” という記述に置き換える.

DESd3 ROM を用いて DESo の 16 段の部分鍵を固定した回路．EX の出力と subkey の xor 部分が ROM に置き換わる.

DESex DESo の ROUND 部分，KEY_GEN 部分 (PC1 は除く) を 16 段展開した回路．組合せ論理で実現できる.

DESexd DESex の入力鍵を固定した回路 (DESo に対する DESd1 に対応).

4　評価方法

表 1: 評価環境

シミュレーション	Mentor 社 ModelSim
論理合成	Synopsys 社 FPGA Compiler II 3.7.0
マッピング，P&R	Xilinx 社 ISE5.2i

10 個の鍵をランダムに生成し，データ依存回路を生成して結果の平均をとる．論理は VHDL で記述し，論理合成，マッピング，P&R を行って結果を評価する．評価環境を表 1 に示す．暗号化が正しく行われているか，シミュレーションの結果と暗号化ライブラリ libdes の結果を比べて確認する．今回評価に用いたデバイスは，Xilinx 社の Virtex-II，Virtex，Spartan-II の 3 つである.

5　評価

表 2: P&R までの結果：Virtex-II

回路名	スライス数	動作周波数 [MHz]	遅延時間 [ns]	動作速度 [MB/s]	AT 積 [スライス・s]
DESc	592.0	66.68	255.0	31.38	$1.509 * 10^{-4}$
DESo	279.0	130.1	130.5	61.43	$3.640 * 10^{-5}$
DESd1	193.0	127.5	133.3	60.01	$2.573 * 10^{-5}$
DESd2	227.2	196.8	86.40	92.59	$1.963 * 10^{-5}$
DESd3	179.0	97.08	175.1	45.69	$3.130 * 10^{-5}$
DESex	1538	N/A	103.4	77.36	$1.591 * 10^{-4}$
DESexd	1310	N/A	90.66	88.24	$1.188 * 10^{-4}$

表 3: 先行研究 [3] の結果

回路名	CLB 数	動作周波数 [MHz]	遅延時間 [ns]	動作速度 [MB/s]	AT 積 [CLB・s]
Static Design	938	4.90	3265	2.45	$3.063 * 10^{-3}$
Dynamic Design	520	6.60	2424	3.30	$1.261 * 10^{-3}$

Virtex-II の結果を表 2 にまとめる．最も回路規模を削減できたのは DESd3 で，DESo と比べて約 36 %削減された．しかし，動作周波数は約 25 %低下しており，AT 積は高くなった．一方，DESd2 は DESo より約 51 %高速で，AT 積も一番低い．16 段に展開した回路 DESex，DESexd は，動作速度は向上したが，回路規模が大きいため AT 積は高くなった．このような傾向は，デバイスによらずほぼ同じであった．(Virtex と Spartan-II の結果はスペースの関係上省略する．)

先行研究 [3] ではデータ依存回路化によって，回路規模が約 45 %削減されている (表 3)．本研究では，回路規模は最も削減された DESd3 でも約 36 %減であり，先行研究におよばなかった．一方，先行研究では動作速度の向上が約 31 %のところ，本研究では約 51 %向上した (DESd2)．AT 積では，先行研究で 59 %の減少に対し，本研究は DESd2 の 46 %減であった.

6　まとめ

DES アルゴリズムのデータ依存回路を設計した結果，回路規模削減と動作速度向上を確認した．しかし，先行研究ほど回路規模が減らなかったため，さらに改善する方法を検討したい.

また，次世代の暗号標準である AES についても評価を進める予定である.

参考文献

[1] National Bureau of Standards, Data Encryption Standard (DES), FIPS PUB 46 (1977).

[2] Electronic Frontier Foundation, Cracking DES, O’Reilly & Associates (1998).

[3] J. Leonard, W. H. Mangione-Smith, A Case Study of Partially Evaluated Hardware Circuits: Key Specific DES, Proc. FPL’97 (LNCS 1304), Springer, pp. 151–160 (1997).