AES 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 033702　後野遼一郎

1　データ依存回路

一般に回路の入力データの一部を固定することで, 回路規模を縮小し, 動作速度を改善できる. このようにして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.

暗号処理をデータ依存回路で実装すると, 攻撃に対する耐性が向上するなどの利点がある. データ依存回路では暗号鍵は回路に埋め込まれ, さらに回路が最適化されるため, 例えば鍵のすりかえや盗用に対する耐性が高まる.

先行研究 [1][2] では DES 暗号のデータ依存回路を実装しているが, 今日では DES の暗号強度は高いとはいえない.

本研究の目的は AES 暗号のデータ依存回路を実装し, 回路規模と動作速度を定量的に評価することである.

2　AES 回路設計

AES は 2001 年に米国商務省標準技術局 (NIST) により選定された, 米国政府標準の暗号化アルゴリズムである. AES では初期化を含め 11 ラウンドの処理で平文 128bit を暗号化する. 図 1 は AES 暗号処理のフローである. KeyExpansion 部は入力鍵から各ラウンドのラウンド鍵を生成する. AddRoundKey 部では入力データとラウンド鍵の xor 演算が行われる.

本研究では, Usselmann の AES 回路 [3](Verilog HDL 記述) を評価の基本として使用する. 鍵長は 128bit である. これを元に以下の回路を作成した.

original Usselmann の回路の暗号化処理のみを取り出した. ブロック図は図 1 の通りである.

fixed_key 図 1 の key を定数に固定した.

fixed_round_key key が固定されれば, KeyExpansion が生成する round_key は事前に計算できる. そこで KeyExpansion を, ラウンド番号に応じて定数を選択するマルチプレクサに置き換えた.

xor_collapse AddRoundKey は, 入力データと round_key の xor 演算を行う. round_key に応じて xor ゲートを単純結線または not ゲートに置き換え, ラウンド番号に応じてマルチプレクサで配線を切り替えた.

xor_by_ROM AddRoundKey の出力は入力データとラウンド番号によって一意に定まるので, AddRoundKey を ROM(Block SelectRAM, 以下 BlockRAM) で置き換えた. ただしデータフローの簡単化のため, 初期・最終ラウンドは xor_collapse と同等とした.

さらに, 以上の各回路の全ラウンドを展開し, パイプライン化を行った回路も作成した. パイプライン化した回路は接頭辞 “pl_” をつけて区別する. ただし xor_by_ROM については, BlockRAM の不足によりパイプライン化できなかった.

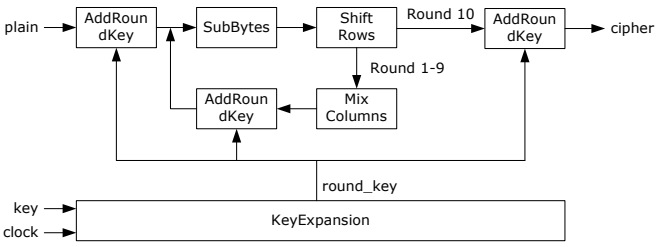

図 1: original のブロック図

3　評価

作成した論理記述に対し, 論理合成, テクノロジマッピング, 配置配線を行って回路を生成した. 評価環境を表 1 に示す. 回路の論理規模は SLICE 数と BlockRAM 数で評価する. 実行時間は平文 128bit の暗号化にかかる時間とする. データ依存回路については, ランダムな鍵で 100 種類の回路を生成し, その平均値を掲載した. 100 種類の鍵は, 全回路で共通とした.

表 1: 評価環境

Device	Virtex2 xc2v4000-ff1152-4 23040 Slices / 120 BlockRAMs
PC	Athlon XP 2400+ / Mem. 1GB WinXP Pro SP1
Synthesis	LeonardoSpectrum Ver.2003b.35
Map, P&R	Xilinx ISE 6.2.02i
Optimize for	auto

作成した回路の SLICE 数と実行時間の比較を図 2 に, BlockRAM 数と実行時間の比較を図 3 に示す.

逐次実行回路では, SLICE 数が 10.7%〜57.7%削減された. 最も SLICE 数が削減できたのは xor_by_ROM であるが, BlockRAM の使用量は 2.7 倍となり, 実行時間も 39.9%増加した. xor_by_ROM 以外では実行時間が 15.8%〜34.1%短縮された. 実行時間が最も短縮されたのは fixed_round_key であった.

全ラウンドを展開しパイプライン化した回路では, SLICE 数が 6.0%〜52.9%減少した. pl_fixed_key 以外では実行時間が 18.3%改善し, BlockRAM が 20.0%削減された. いずれの評価項目でも pl_fixed_round_key と pl_xor_collapse が最良だった.

なお, DES 暗号に関する先行研究 [1] では, 回路規模が最大 45%, 動作速度が最大 31%向上している. 先行研究 [2] では, 回路規模が最大 36%, 動作速度が最大 51%向上している. 本研究の逐次実行回路では両先行研究以上に回路規模が削減され, 動作速度は先行研究 [1] と同程度に向上した。

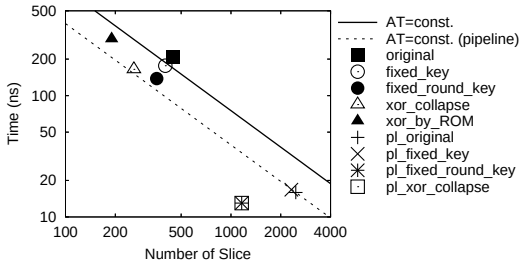

図 2: 作成した回路の SLICE 数と実行時間

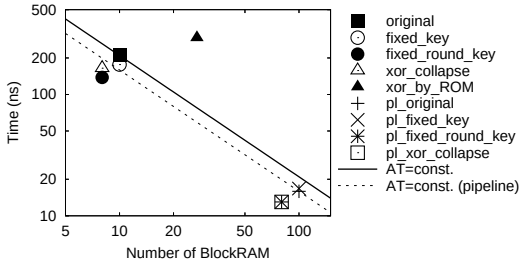

図 3: 作成した回路の BlockRAM 数と実行時間

参考文献

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

[2] 宮本雅人: DES 暗号のためのデータ依存回路設計と評価, 豊橋技術科学大学知識情報工学系特別研究 (2003).

[3] Usselmann, R.: AES(Rijndael) IP Core: Overview, `http://www.opencores.org/projects.cgi/web/aes_core/overview`. (2004/12/8 に参照).