

# MISTY1 H/W 実装評価報告

東芝

2001-01-12

## 目次

1	はじめに	3
2	ハードウェア設計の方針	3
3	回路構成	6
4	実装結果	7
4.1	ハードウェア規模 . . . . .	7
4.2	処理速度 . . . . .	7
5	まとめ	9

## 1 はじめに

本ドキュメントは、ブロック暗号アルゴリズム MISTY1 のハードウェア実装評価について記述したものである。

MISTY1 は、128 ビットの暗号化鍵を持つ 64 ビットブロック暗号であり、評価は、8 段の暗号化回路に対して行った。

評価は、VHDL で設計し、同一の記述に対して合成条件で速度優先の条件と面積優先の条件で合成することにより行った。

## 2 ハードウェア設計の方針

設計方針を以下に示す。

1. ループアーキテクチャを採用する。
2. パイプラインアーキテクチャは採用しない。
3. 置換表はテーブルを用い、論理合成ツールを用いて最適化を行う。
4. コントロール回路は副鍵生成及び暗号化回路の全てのタイミング信号を生成する。

図 1 に評価アルゴリズムを示す。左側が暗号化アルゴリズムで、右側が鍵スケジューアルゴリズムである。図中において、FO は、副関数  $FO$ 、FL は、副関数  $FL$ 、FI は、副関数  $FI$  を表している。

図 1 において、点線は、1 段のループで処理される境界を示している。9 クロックで暗号化処理が完了すし、1 クロックで鍵スケジューが完了する。

各ループでの処理内容を表 1 に示す。

表 1: 各ループにおける処理内容

- 1 FL 関数 + FO 関数
- 2 FO 関数
- 3 FL 関数 + FO 関数
- 4 FO 関数
- 5 FL 関数 + FO 関数
- 6 FO 関数
- 7 FL 関数 + FO 関数
- 8 FO 関数
- 9 FL 関数

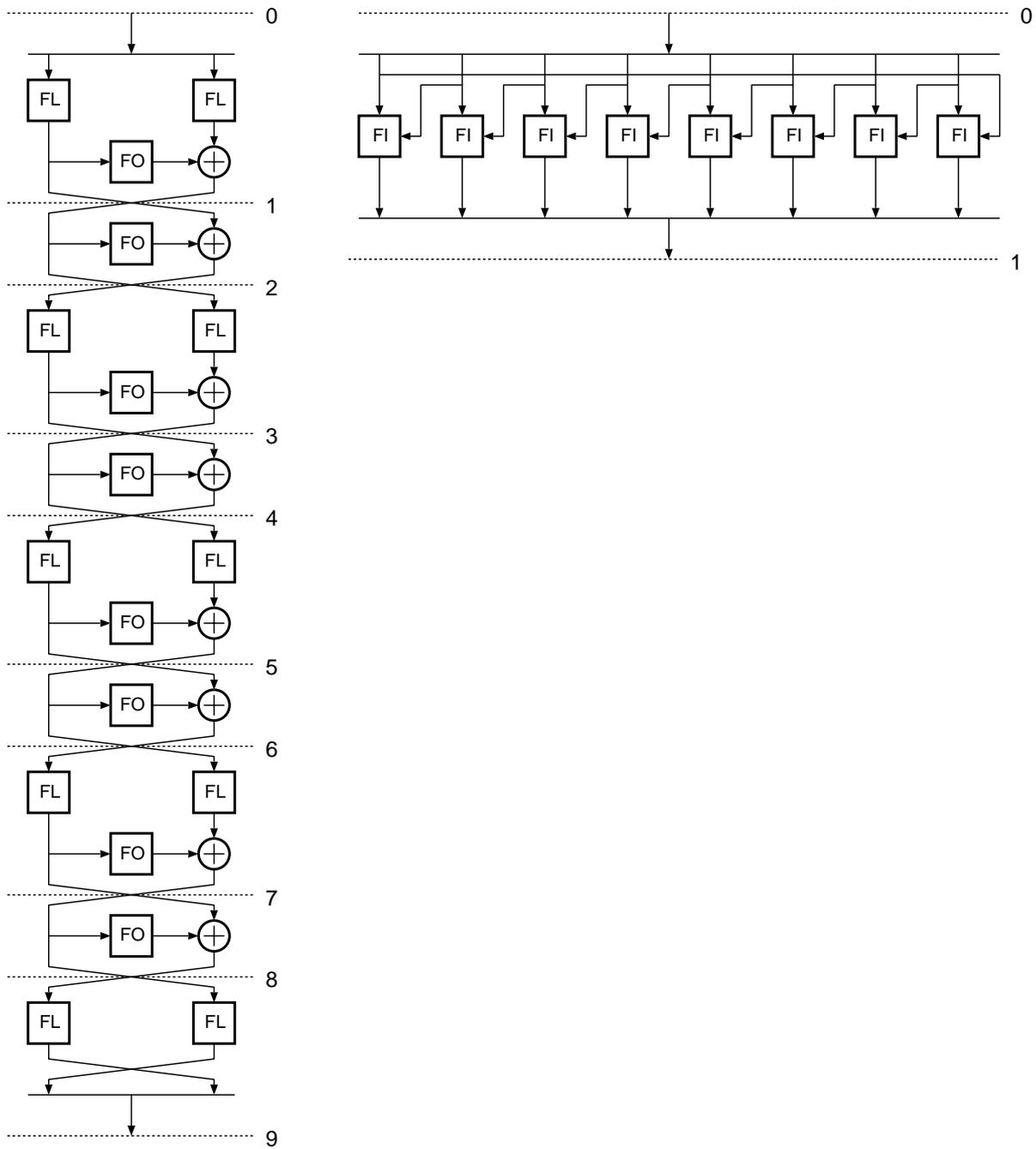


図 1: 評価アルゴリズム

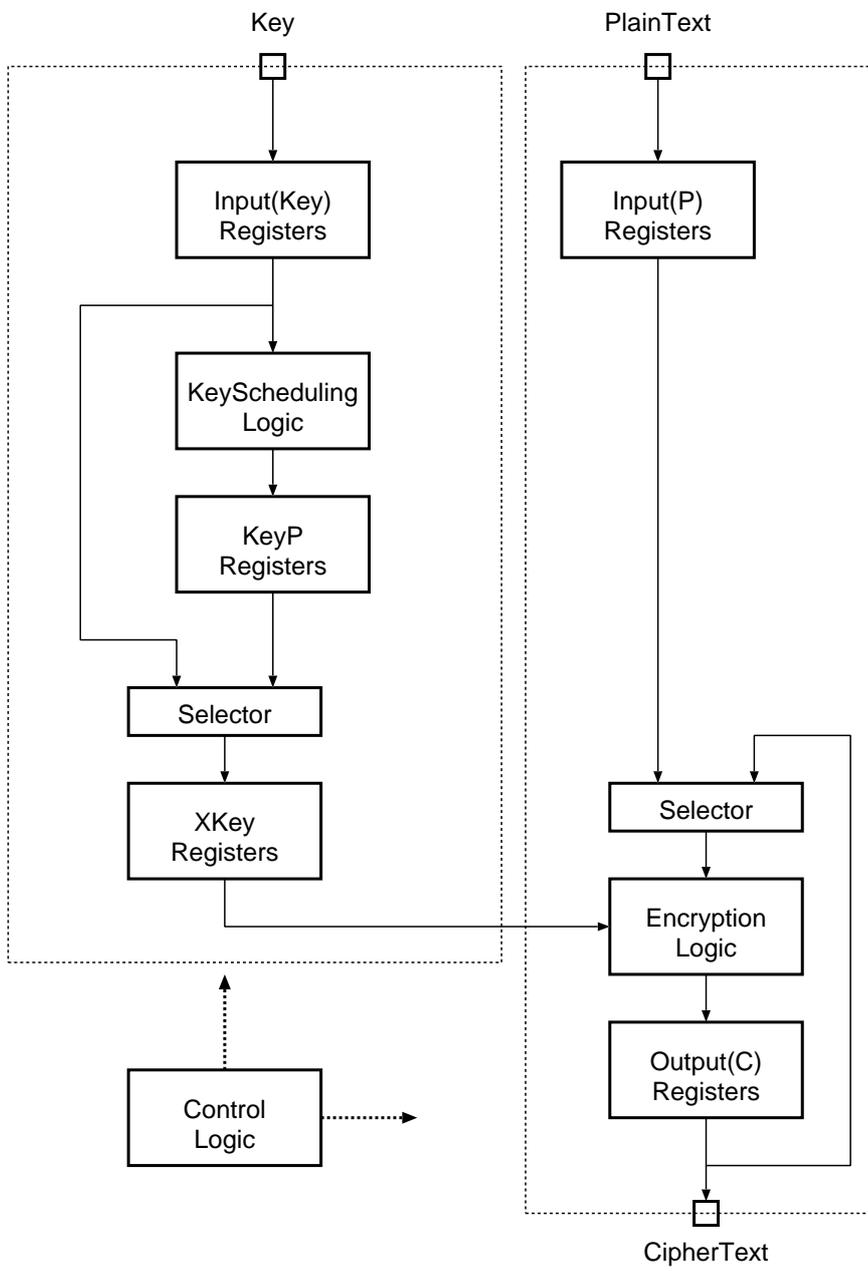


图 2: 評価回路

### 3 回路構成

本評価に使用した評価回路の構成を図 2 に示す。

評価回路は、暗号化回路、鍵スケジュール回路、コントロール回路で構成される。

- 暗号化回路

暗号化回路は、一段分の暗号化のための回路である。

暗号化回路は、入力された平文を保持する入力レジスタ (Input(P) Register), ループの途中結果と暗号化された暗号文を保持する出力レジスタ (Output(C) Register), 暗号化を実現する組み合わせ回路 (Encryption Logic) で構成される。

- 鍵スケジュール回路

コントロール回路からの制御信号に従い副鍵を生成する回路。

鍵スケジュール回路は、入力された鍵を保持する入力レジスタ (Input(Key) Register), 鍵スケジュールの中間結果を保持するレジスタ (KeyP Register), 鍵スケジュールを実現する組み合わせ回路 (KeyScheduling Logic), 拡大鍵を一時的に保持する一時レジスタ (XKey Register) で構成される。

- コントロール回路

鍵生成の制御信号やタイミングの制御信号を生成する。

表 1 に示した動作タイミングを図 3 に示す。

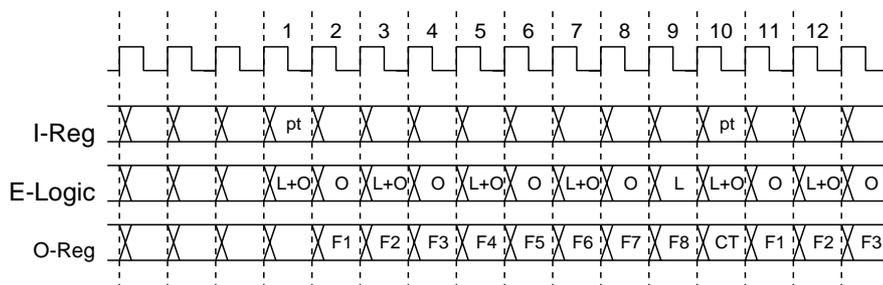


図 3: 評価回路の動作タイミング

図中において、I-Reg は、暗号化回路の入力レジスタの出力、E-Logic は、暗号化回路の暗号化ロジックの処理内容、O-Reg は、暗号化回路の出力レジスタの出力である。

'1' のタイミングで、I-Reg に平文 pt が保持され、その値に L+O (FL 関数 + FO 関数) の処理が行われ、その結果 F1 が次のクロックの立ち上がりで一時レジスタに保持される。'2' のタイミングで、一時レジスタに保持されている値 F1 に対して FO (FO 関数) の処理が行われ、その結果 F2 が次のクロックの立ち上がりで一時レジスタに保持される。同様に処理が進められ、'10' のタイミングで、一時レジスタに保持されている値 F8 に対してその値に FL (FL 関数) の処理が行われ、その結果の暗号文 CT が次のクロックの立ち上がりで出力レジスタに保持される。このような動作によって暗号化処理が行われる。

## 4 実装結果

MISTY1 (128Bit 鍵) のハードウェア実装評価結果を示す。

以上の設計方針のもと、MISTY1 を ASIC に実装した場合について評価検討を行った。評価条件を表 2 に示す。合成は、速度優先の条件と面積優先の条件の 2 つで行った。

表 2: ハードウェア設計及び評価環境

記述言語	VHDL
シミュレータ	ModelSim5.4a
デザインライブラリ	TOSHIBA 0.25 $\mu$ COMS ASIC Design Library
論理合成ツール	Design Compiler . 2000.05-1
動作条件	0 ~ 70 , 3.3V $\pm$ 5 %

### 4.1 ハードウェア規模

ハードウェアの規模の評価結果を以下に示す。

表 3: ハードウェア実装結果 (ハード規模) 単位: Gate

暗号アルゴリズム	暗号回路	鍵スケジュール	コントロール回路	TOTAL
Triple-DES *1	4,218	1,333	151	6,496
Triple-DES *2	2,011	1,088	134	5,111
MISTY1 *1	19,935	44,773	94	64,809
MISTY1 *2	10,609	28,194	68	38,875

\*1 スピード優先にて論理合成

\*2 規模優先にて論理合成

### 4.2 処理速度

スループットの評価結果を以下に示す。

クリティカルパスは、1 クロックサイクルの最大遅延時間を表している。したがって、暗号化に要する処理時間は、クリティカルパス  $\times$  処理クロック数となり、スループットは、暗号化のブロックサイズを処理時間で割った値となる。Triple-DES では、処理に 59 クロック要し、Misty1 では、処理に 9 クロック要する。

数値は全て、ワースト条件での値である。

表 4: ハードウェア実装結果 (スループット)

暗号アルゴリズム	クリティカルパス	暗号化処理時間	スループット
Triple-DES *1	4.44ns	262.0ns	244Mbps
Triple-DES *2	7.10ns	418.9ns	153Mbps
MISTY1 *1	11.86ns	106.7ns	600Mbps
MISTY1 *2	24.70ns	222.3ns	288Mbps

\*1 スピード優先にて論理合成

\*2 規模優先にて論理合成

## 5 まとめ

本稿では, MISTY1 の設計方針, ハードウェア実装に対する解析結果を示した.

ハードウェア規模に関しては, MISTY1 は, Triple-DES に比べ 7.6 倍から 10 倍程度大きくなった. また, データスケジュール部と鍵スケジュール部では, 鍵スケジュール部の方が大きくなる. これは, 鍵スケジュール部が 8 個の FI 関数を持つのに対し, データランダムイズ部が 3 個の FI 関数 (FO 関数に含まれる) を持つためと考えられる.

スループットに関しては, MISTY1 は, Triple-DES に比べ 1.9 倍から 2.5 倍高速になった.