Memoirs of the Faculty of Science
Kochi University (Information Science)
Vol.29 (2008), No.13

暗号化アルゴリズムのハードウェア化手法の性能評価

高知大学理学部情報コース　村岡研究室
松永　惇弥　　村岡　道明

1. まえがき

高度情報化に伴い、暗号化処理技術はますます重要性が高まっている。しかし、ソフトウェア処理では大規模なデータを処理する場合には長時間を必要とする。そこで本研究では、ソフトウェア言語で書かれた DES 暗号アルゴリズムの一部をハードウェア化をすることにより高速化を検討した。

2. 研究内容

2.1 ハードウェア化部分の検討

本研究で用いる DES は､64bit のデータを 56bit の鍵を用いて暗号化を行い 64bit のデータを得る処理である。

DES の暗号化処理のフローを図１に示す。

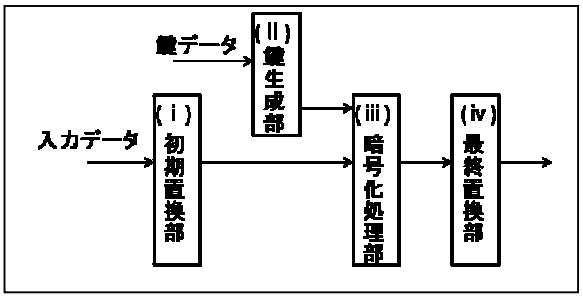

図１．ソフトウェア記述の DES のフロー

図１において各処理の説明［1］を以下に示す。

（ⅰ） 初期置換部は入力されたデータを初期置換表に従い置換を行う。
（ⅱ） 鍵生成部は与えられた鍵データを置換表に従い置換して、それを二等分し決められた回数左シフトをしてラウンド鍵を 16 個作る。
（ⅲ） 暗号化処理部は入力されたデータを二等分し f 関数処理やラウンド鍵と XOR 演算などの処理を 16 回行う。
（ⅳ） 最終置換部は入力されたデータを最終置換表に従い置換を行う。

図１の(ⅰ)～(ⅳ)で時間計測を行い、時間が一番かかる暗号化処理部(上記の(ⅲ))のハードウェア化を検討した。

2.2 暗号化処理部のアルゴリズム

暗号化処理部のハードウェアのアルゴリズムを下に示す。

(1) 鍵生成部で生成されたラウンド鍵を保存しておき、ラウンドに応じて出力する。
(2) 外部から入力されたデータ IP を入力制御部に格納する。
(3) 入力データ制御部から暗号化するデータ P0 を受け取とり、sp を上位 32bitL、下位 32bitR0 に分け出力
(4) F 関数処理は入力された R0 を 48bit に拡大し、そのデータと 48bit の鍵(RK)の XOR 演算で得た結果を 6bit 単位の bit 列に 8 個に分けて、それぞれ S-BOX に入力して得た 32bit のデータを P 置換表に従い置換をして f として出力する。
(5) L を cunt で制御し、L0 を出力する。
(6) f と L0 で XOR 演算を行い R1 を出力する。
(7) R0 を cunt で制御し、L1 を出力する。
(8) R1 と L1 を上位 32bit と下位 32bit を入れ替えて(ⅱ)～(ⅵ)を 16 回行っていないときは L1R1、行っているときは R1L1 をそれぞれ選択して P1 を出力する。
(9) (ⅶ)で L1R1 を選択していれば、P1 を(ⅲ)に送り、P1 を選択して処理を繰り返す。(ⅷ)で R1L1 を選択したならば P1 は次の暗号化データ部に格納され P2 を出力する。
(10) ここで､3 ビットカウンタのカウントアップをいつ始めるかを制御する。
(11) sp 信号が入力されると+1 ずつカウントアップする cunt を出力する。
(12) (ⅷ)で 1 カウントアップする cun を出力する。

このアルゴリズムでは、(ⅳ)の中の S-BOX での処理をソフトウェアのアルゴリズムとは変えて並列にして行った。

上記のブロック図を図 2 に示す。

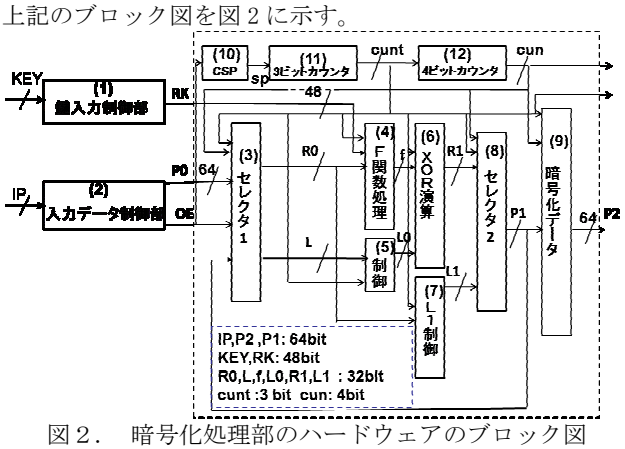

図２．　暗号化処理部のハードウェアのブロック図

3. 暗号化処理部の処理時間の評価

暗号化処理部の評価式を下に示す。

$$Ts = Tb + (\sum_{n=1}^{16} Tn) * X + Ta$$

Ts:暗号化処理部全体の時間
Tb:最初の入録制御部から読み取る時間
Tn:16 回繰り返す処理部分の一回分の時間
X:処理するデータの数
Ta:暗号化されたデータを保存するのにかかる時間

上の評価式を用いて、ファンクションシミュレーション、タイミングシミュレーションで行い評価をした。

4. まとめ

今回は、暗号化アルゴリズムのハードウェア化による高速化の評価を行った。暗号化アルゴリズムの一部をハードウェア化により、評価式から 30 万の入力データのサイクル数を導き出し処理時間を計測すると、約 1/37 に短縮することができた。今後の課題としては、パイプライン化により、さらに高速化を検討していきたい。