SHA256 回路の FPGA 実装の研究

FPGA implementation of SHA-256 function

秋山　拓範†　田中　勇樹†　魏　書剛†
Takunori AKIYAMA†　Yuuki TANAKA†　Shugang WEI†
† 群馬大学大学院　理工学専攻
† Graduate School of Science and Technology, Gunma University

1. はじめに

現在,暗号技術は広く使われており,取り扱うデータ量も増えてきている.そのため,一定時間に暗号化処理を行えるデータ量を増加させるために,高速化をすることは需要がある.本研究では暗号技術の一つであるハッシュ化を行う回路である SHA-256 回路の FPGA 上での実装を行う.また,回路中で最も遅延時間の長い加算部分に SDA,CSA を用いることで高速化を検討する.

2. SHA-256

本研究で使用する SHA-256 回路は FIPS-180-2 のアルゴリズム[1]を使用した回路となっている.本アルゴリズムでは 512bit のメッセージ入力から 256bit のハッシュ値を生成するアルゴリズムである.また,512bit を超えた入力（$\leq 2^{64}-1$）は 512bit ずつのブロックに分割され,順次演算処理される.アルゴリズムは以下の手順からなる.

(1) メッセージパディング処理
入力されたメッセージを 512bit ずつのブロックに分割する.この際に,512bit ブロックに不足がないよう,メッセージの最後に 1bit のデータ'1'を加え桁数に応じた'0'を付け加える。また，最終ブロックには 64bit のメッセージを付け加えることで入力桁数の差別化を行う.

(2) メッセージ拡張処理
512bit のブロックから 32bit のワードを 64 個生成する.まず 512bit のデータは 16 個のワード($M_t^{(i)}$)に分割される.のちに以下の式に則り拡張処理を行う．$\sigma_0^{\{256\}}(x)\sigma_1^{\{256\}}(x)$はシフト演算である.

$$W_t = \begin{cases} M_t^{(i)}\ (0 \leq t \leq 15) \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} (16 \leq t \leq 64) \end{cases} \quad (1)$$

(3) メッセージ圧縮処理
メッセージ拡張処理にて生成したW_tよりハッシュ値を生成する．$a,b,c\ldots,h$はハッシュ値$H_j^{(i)}$を生成するために使用する作業変数である.

for $t = 0$ to 63
{
$T_1 = h + \Sigma_1^{\{256\}}(e) + Ch(e,f,g) + K_t^{\{256\}} + W_t.$
$T_2 = \Sigma_0^{\{256\}}(a) + Maj(a,b,c).$
$h = g, \quad g = f, \quad f = e, \quad e = d + T_1,$
$d = c, \quad c = b, \quad b = a, \quad a = T_1 + T_2.$
}(2)

ハッシュ化処理は 512bit のブロックの数だけ繰り返される．ここでK_tは定数であり，また，$\Sigma_0^{\{256\}}(x), \Sigma_1^{\{256\}}(x)$はシフト演算である．また，$Ch(x,y,z)$は選択演算,$Maj(x,y,z)$は多数決の演算である.

(4) ハッシュ値更新
元のハッシュ値$H_j^{(i-1)}$と$a,b,c\ldots,h$の加算から新しいハッシュ値$H_j^{(i)}$を生成する.

3. 加算手法

SHA-256 のアルゴリズムでは実装の際に式(2)の演算に最も遅延が発生する.そこで,様々な加算方式を利用することで高速化することを考える.本研究は桁上げ伝搬加算器(RCA),桁上げ保存加算器(CSA),SD 数加算器(SDA)の記述を利用した回路を作成した.

4. 性能評価

本研究では Xilinx 社製 Z7020 チップ搭載の FPGA ボード ZedBoard への実装を行った.また,unroll 化処理を行っている他論文[2]との比較も記載する.
ここでは以下の式(3)より$Throughput$を求め比較を行った.

$$Throughput = \frac{最大周波数(MHz) \times ブロック長(bit)}{クロック数(回)} \quad (3)$$

表 1.回路評価

加算手法	最大周波数 (MHz)	クロック数 (回)	$Throughput$ (Mbps)
RCA	125.000	68	941.2
CSA	125.000	68	941.2
SDA	125.000	68	941.2
Unroll[2]	73.975	38	996.7

5. まとめ

性能としては Unroll 処理を行った他論文が最も Throughput が高かった.FPGA ボードの性能により,RCA・CSA・SDA の手法間で差がなかった.

参考文献

[1] Secure Hash Standard(SHS),NIST,2015.
[2] Robert P. McEvoy, Francis M. Crowe, Colin C. Murphy and William P. Marnane, “Optimisation of the SHA-2 Family of Hash Functions on FPGAs”, ISVLSI'06,2006.