ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ

VLSI III PROJECT

Secure Hash Algorithm – 256

SHA-256

ΟΜΑΔΑ 09

ΜΑΪΣ ΜΥΡΙΑΜ 1083745

ΜΠΟΥΡΤΣΟΥΚΛΗΣ ΘΕΟΔΟΣΙΟΣ 1083891

ΠΑΤΡΑ, 25/02/2025

SHA – 256 Αρχές Λειτουργίας (1)

1ο Βήμα (Padding)

Είσοδος : Λέξη (M) μήκους l

Έξοδος : Λέξη k x 512 bits , όπου k = 1,2,3....
l + 1 + n +64 = k x 512 bits , όπου n αριθμός 0 και 64 το μήκος του M δηλαδή το l σε binary μορφή.

2ο Βήμα (Parsing)

Είσοδος : Λέξη μήκους k x 512 bits

Έξοδος : k λέξεις των 512 bits ($M_i^{(n)}$, με i = 0,1,2,...,15)

3ο Βήμα (Message Schedule)

Είσοδος : 16 λέξεις των 32 bit, $M_i^{(n)}$, με i = 0,1,2,...,15

Έξοδος : 64 λέξεις των 32 bit, Wt , με t = 0,1,2,3...63

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 63 \end{cases}$$

SHA – 256 Αρχές Λειτουργίας (2)

4ο Βήμα (Message Schedule)

Είσοδος : 64 λέξεις των 32 bit, Wt , με t = 0,1,2,3...63

Έξοδος : 8 λέξεις των 32 bit, H^i

$$a = H_0^{(i-1)}$$
$$b = H_1^{(i-1)}$$
$$c = H_2^{(i-1)}$$
$$d = H_3^{(i-1)}$$
$$e = H_4^{(i-1)}$$
$$f = H_5^{(i-1)}$$
$$g = H_6^{(i-1)}$$
$$h = H_7^{(i-1)}$$

Αρχικοποίηση

$$T_1 = h + \sum_1^{\{256\}}(e) + Ch(e,f,g) + K_t^{\{256\}} + W_t$$
$$T_2 = \sum_0^{\{256\}}(a) + Maj(a,b,c)$$
$$h = g$$
$$g = f$$
$$f = e$$
$$e = d + T_1$$
$$d = c$$
$$c = b$$
$$b = a$$
$$a = T_1 + T_2$$

Υπολογισμός

$$H_0^{(i)} = a + H_0^{(i-1)}$$
$$H_1^{(i)} = b + H_1^{(i-1)}$$
$$H_2^{(i)} = c + H_2^{(i-1)}$$
$$H_3^{(i)} = d + H_3^{(i-1)}$$
$$H_4^{(i)} = e + H_4^{(i-1)}$$
$$H_5^{(i)} = f + H_5^{(i-1)}$$
$$H_6^{(i)} = g + H_6^{(i-1)}$$
$$H_7^{(i)} = h + H_7^{(i-1)}$$

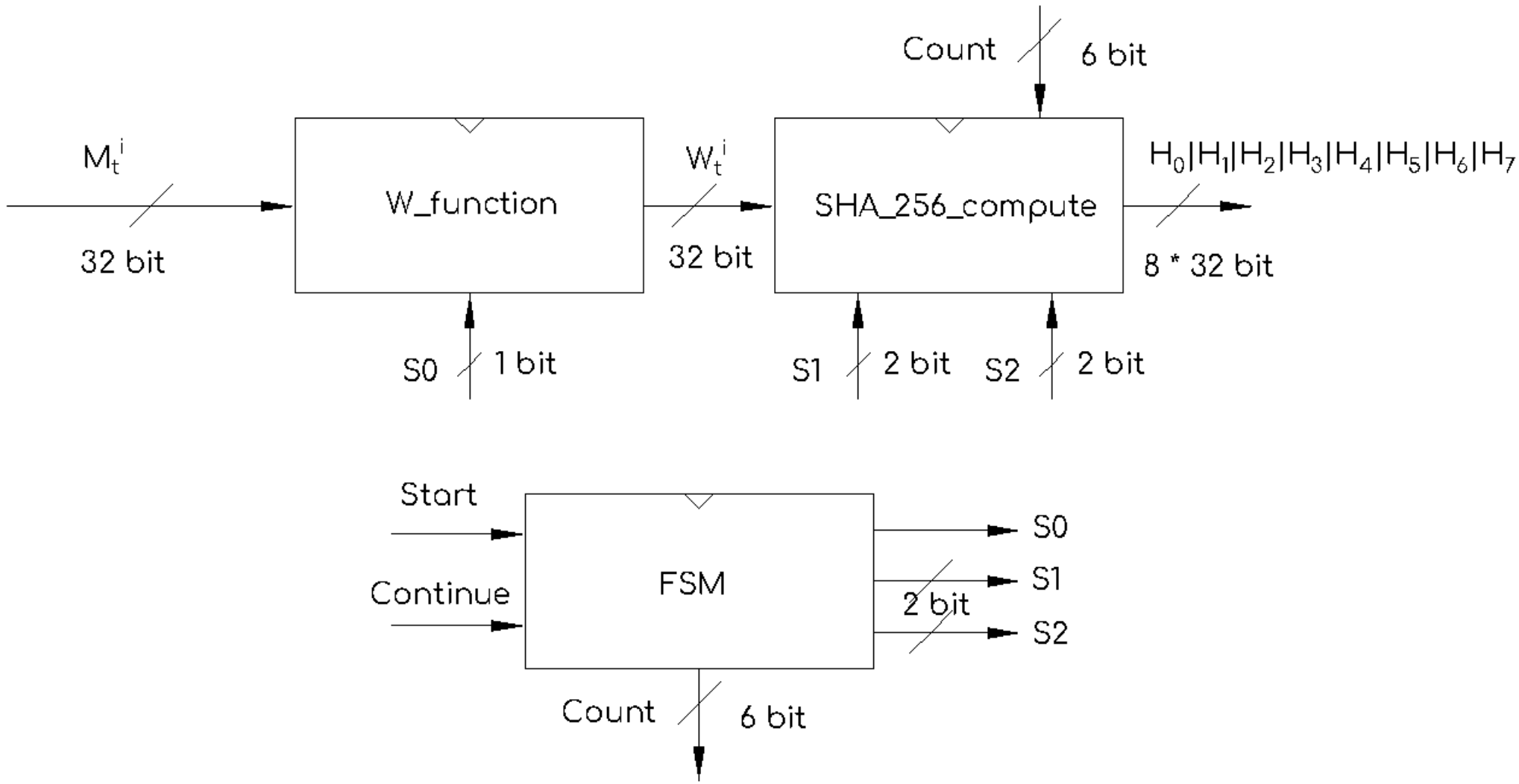
Τελικό αποτέλεσμα

SHA – 256 Αρχές Λειτουργίας (3)

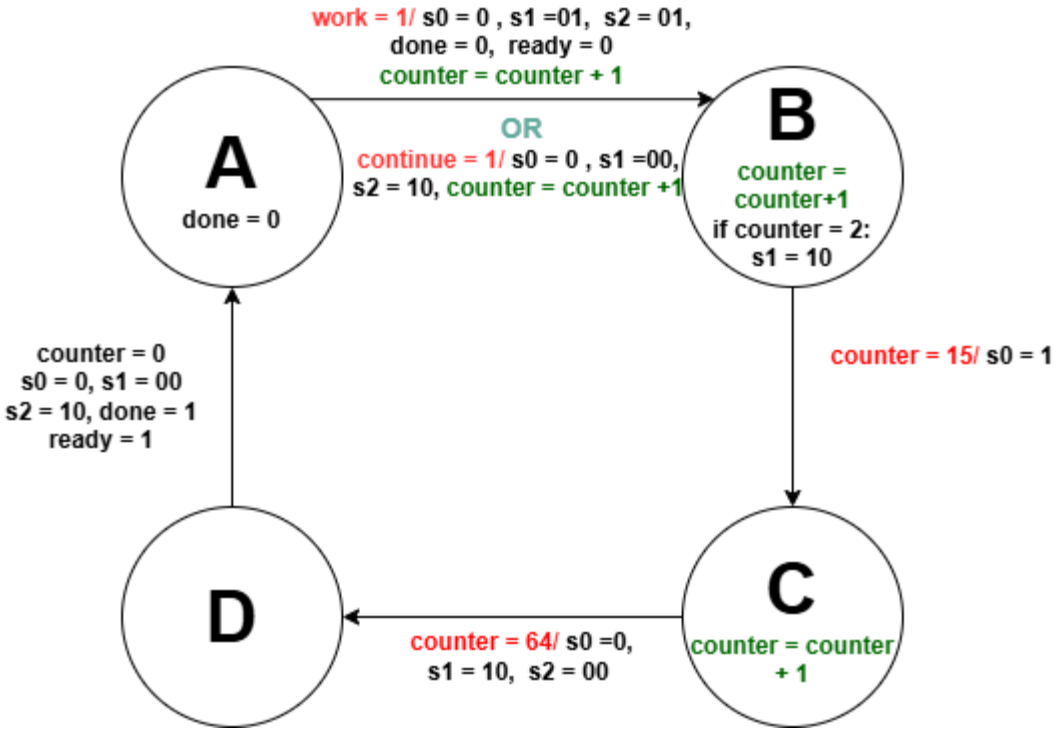
Βασικές Συναρτήσεις αλγορίθμου

- $Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$
- $Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$
- $\sum_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$
- $\sum_1^{\{256\}}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$
- $sigma_0^{\{256\}}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$
- $sigma_1^{\{256\}}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$

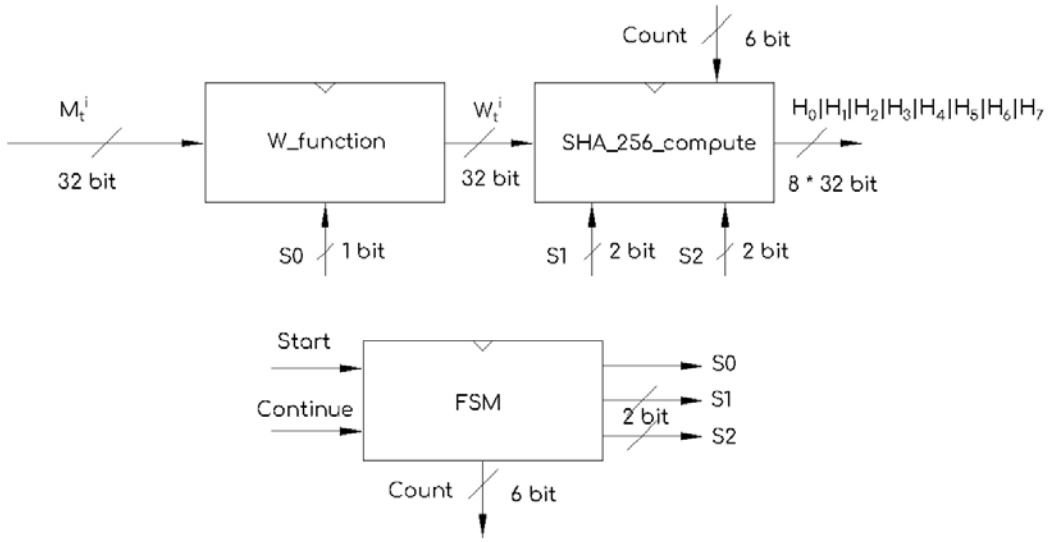
Βασική Αρχιτεκτονική



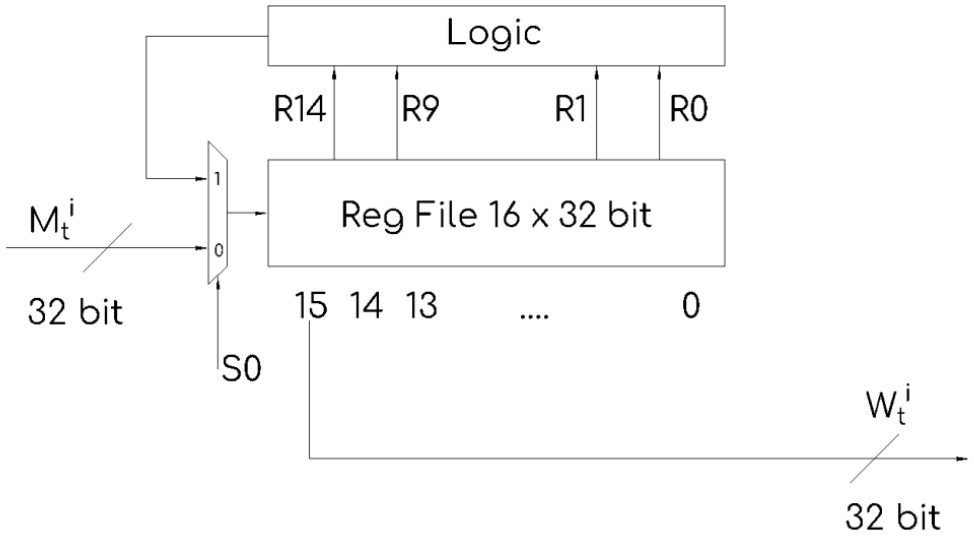
FSM



Κατάσταση	Λειτουργία
A	Αναμονή, το κύκλωμα αρχικοποιημένο και περιμένει σήμα start η Continue
B	Κύκλωμα σε λειτουργία, σειριακή αποστολή εισόδου W στο SHA compute (0≤t≤15)
C	Κύκλωμα σε λειτουργία, σειριακή αποστολή με επεξεργασία W στο SHA compute (16≤t≤63)
D	Έτοιμο hash αποθήκευση και επιστροφή στην αναμονή (κατάσταση A)



MESSAGE SCHEDULER



S0	Στέλνει στην έξοδο του W_function :
0	την είσοδο του Wt
1	επεξεργασμένη τιμή Wt

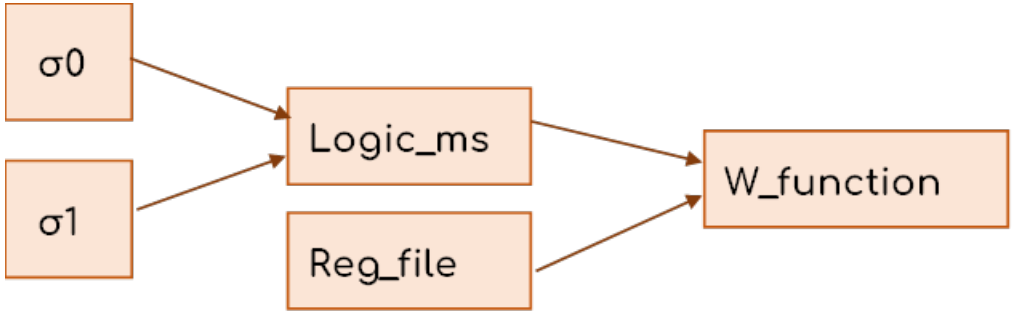
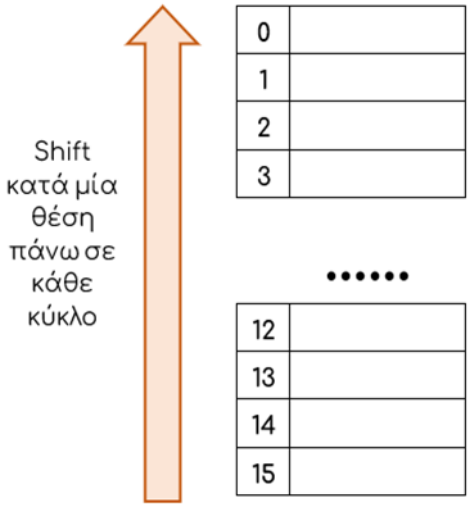
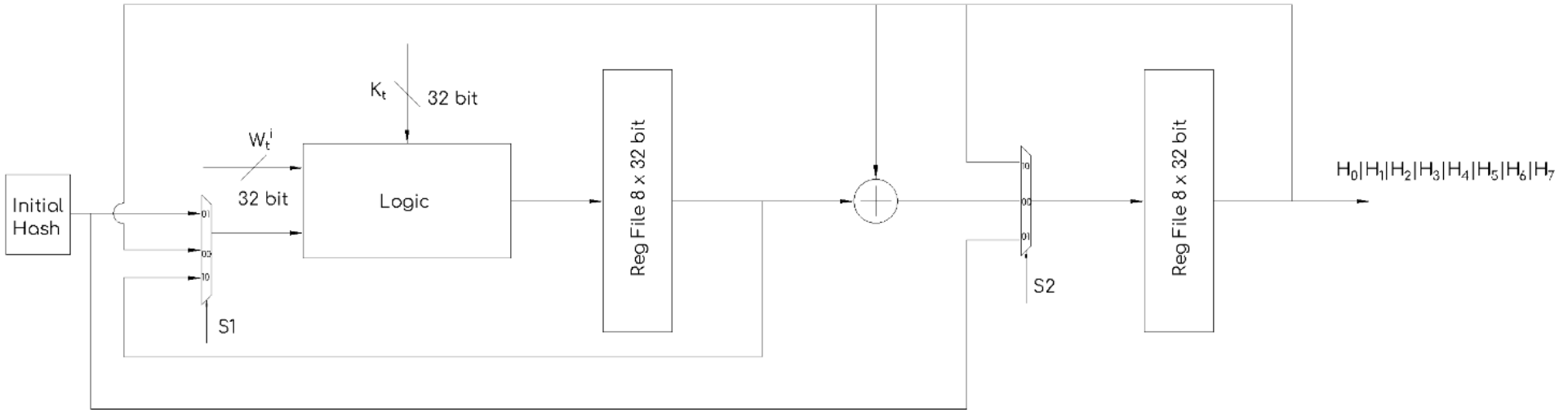


Figure 1 Bottom - up schematic for message scheduler



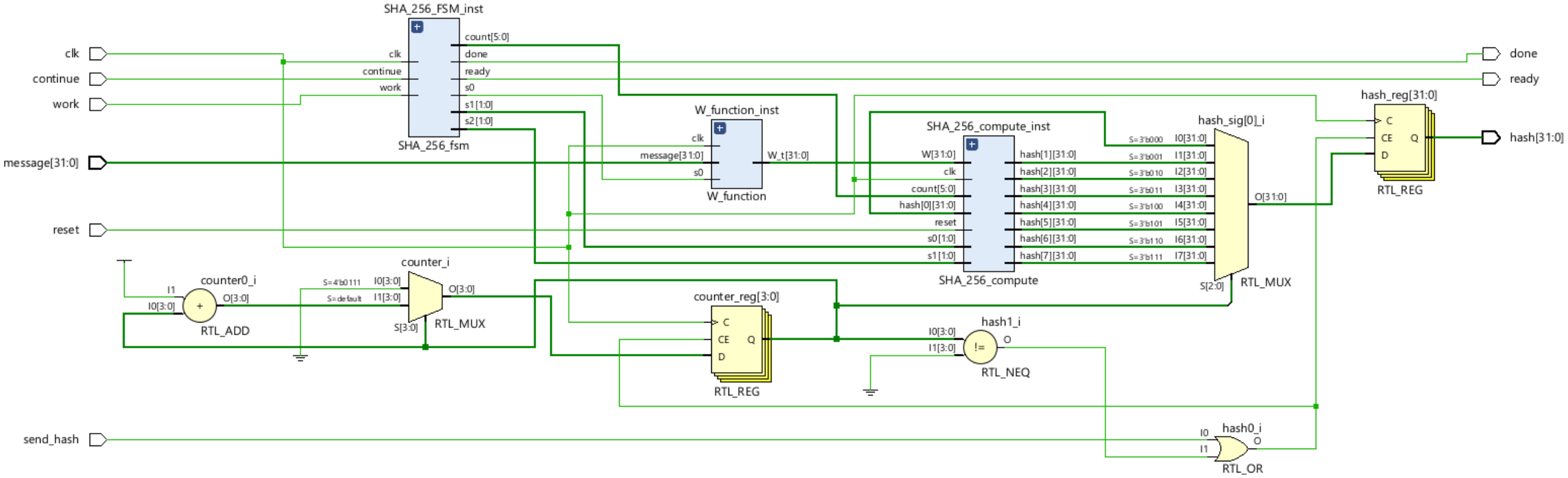
SHA – 256 COMPUTE



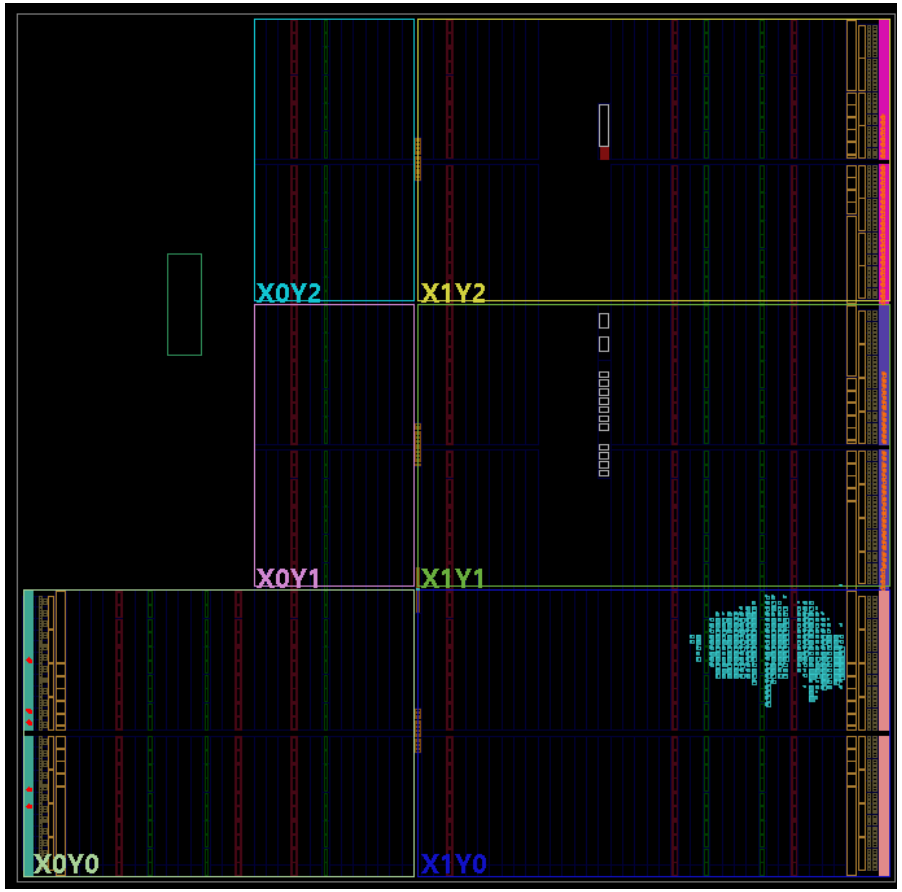
S1	Αρχικοποίηση abcdefgh με :
00	Hash i-1
01	Με το 1ο σετ σταθερών
10	Τα abcdefgh που παράχθηκαν στον προηγούμενο κύκλο

S2	Αρχικοποίηση H^{i-1} με :
00	abcdefgh + H i-1
01	Με το 1ο σετ σταθερών
10	Hold H^{i-1}

ΣΥΝΟΛΙΚΗ ΥΛΟΠΟΙΗΣΗ (1)



ΣΥΝΟΛΙΚΗ ΥΛΟΠΟΙΗΣΗ (2)



Site Type	Used	Fixed	Prohibited	Available	Util%
Slice	280	0	0	13300	2.11
SLICEL	171	0			
SLICEM	109	0			
LUT as Logic	967	0	0	53200	1.82
using O5 output only	0				
using O6 output only	879				
using O5 and O6	88				
LUT as Memory	32	0	0	17400	0.18
LUT as Distributed RAM	0	0			
LUT as Shift Register	32	0			
using O5 output only	0				
using O6 output only	0				
using O5 and O6	32				
Slice Registers	736	0	0	106400	0.69
Register driven from within the Slice	544				
Register driven from outside the Slice	192				
LUT in front of the register is unused	27				
LUT in front of the register is used	165				
Unique Control Sets	13		0	13300	0.10

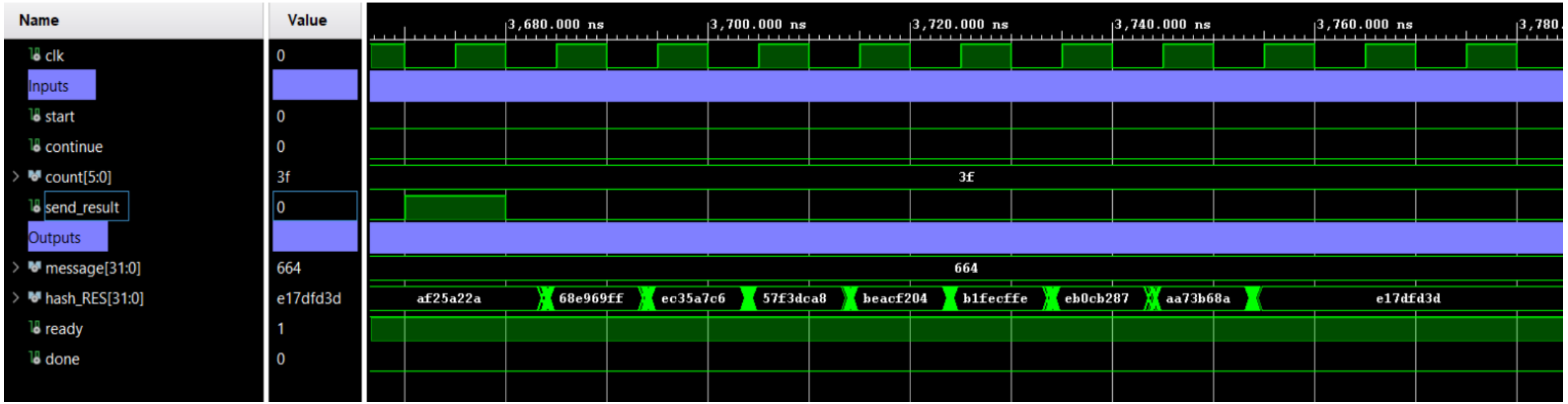
Clock	Waveform(ns)	Period(ns)	Frequency(MHz)
clk	{0.000 5.000}	10.000	100.000

ΣΥΝΟΛΙΚΗ ΥΛΟΠΟΙΗΣΗ (3)

Total On-Chip Power (W)	0.164
Design Power Budget (W)	Unspecified*
Power Budget Margin (W)	NA
Dynamic (W)	0.058
Device Static (W)	0.105
Effective TJA (C/W)	11.5
Max Ambient (C)	83.1
Junction Temperature (C)	26.9
Confidence Level	Low
Setting File	---
Simulation Activity File	---
Design Nets Matched	NA

Input :
theodosissaaefergtrgrtyhtyhytht5t45y56y4rrrrrrr
rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrry

Output :
68e969ff ec35a7c6 57f3dca8 beacf204
b1fecffe eb0cb287 aa73b68a e17dfd3d



Τέλος παρουσίασης

Ακολουθεί κώδικας - προσομοίωση

Σας ευχαριστούμε για την προσοχή σας

ΟΜΑΔΑ 09

ΜΑΪΣ ΜΥΡΙΑΜ 1083745
ΜΠΟΥΡΤΣΟΥΚΛΗΣ ΘΕΟΔΟΣΙΟΣ 1083891