CHIPIONS 21

PHASE 2

PROJECT 1: AES ENCRYPTION
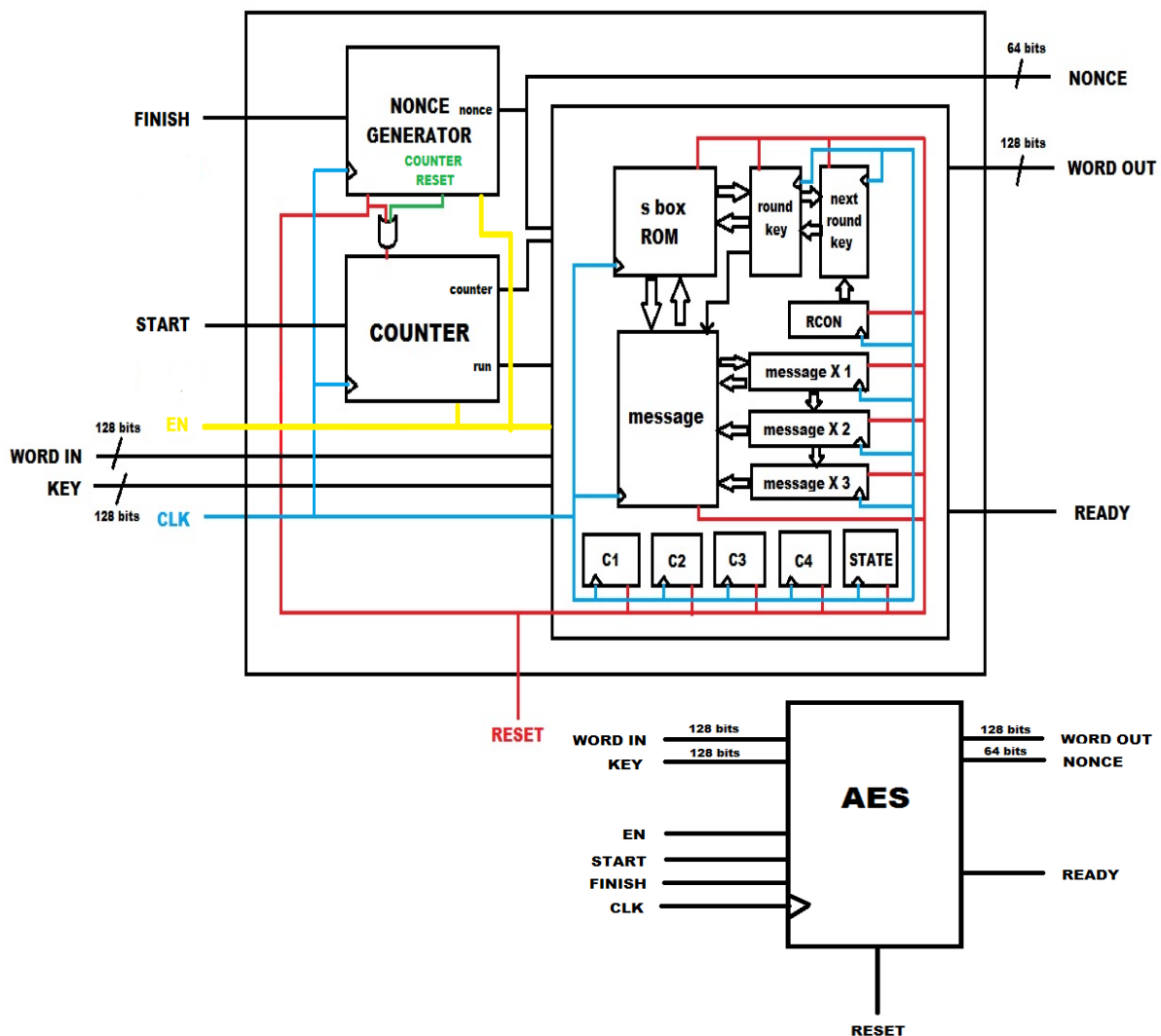
Team 4

Khalid Mahmoud Taher
Omar Nasr Mohamed Younis
Karim Hussein Elbarashy
Noureddine Mohamed
Mohamed El-shazly
Mohamed Fathy
Alaa Elghamry

AES ARCHITECTURE

INPUTS	Input Description	Input Possible Values
CLK	System clock.	Oscillating.
		The rising edge is the point of interest.
rst	System reset.	Binary 0 or binary 1.
en	Enable system.	Binary 0 or binary 1.
start	Start encryption	Binary 0 or binary 1.
finish	Start new message.	Binary 0 or binary 1.
word_in	Plaintext	128-bit word.
key	Cipher key	128-bit word.

OUTPUTS	Input Description	Input Possible Values
ready	Encryption complete.	Binary 0 or binary 1.
word_out	ciphertext	128-bit word.
nonce	Generated nonce	64-bit word.

RESOURCE UTILIZATION

Utilization - Post-Implementation

Resource	Utilization	Available	Utilization %
FF	932	607200	0.15
LUT	1137	303600	0.37
I/O	454	600	75.67
BUFG	1	32	3.12

TESTING AND VERFICATION STRATEGY