

# ECSE 323 — Group 47 Lab 4 Report Permutation

Junyoung Shin id. 260499663  
Timothee Flichy id. 260557686

April 1, 2016

## 1 Permutation

The permutation is used encrypt and revert to the original message. To do so, we were given a table which depicts the character encryption list given in the figure 1. There are 4 configuration we are given to be made. To make the permutation circuit, we need 2 input and 2 outputs. The inputs will receive a 2 bit rotor\_type giving which type of encryption that must be done and the second input inputs a 5 bit input\_code that must be encrypted. The outputs are a 5 bit output\_code which outputs the encrypted version of the input bits determined by the rotory position and the second input is the inv\_output\_code giving out the inverted or decrypted 5 bit code. This is given by the figure 2. We tested out vhdl code on the ModelSim and got what we were expected to get from the permutation graph

INPUT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rotor I	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
Rotor II	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
Rotor III	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
Rotor IV	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B

Figure 1: Permutation graph.

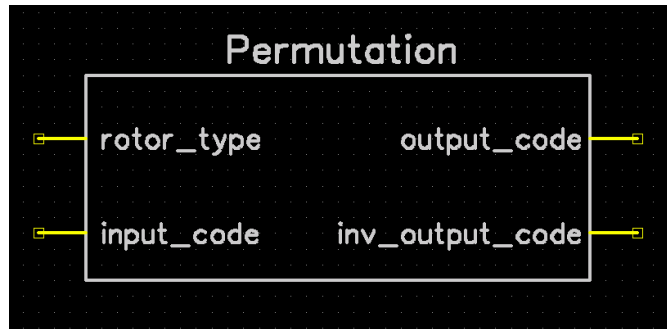


Figure 2: Permutation symbol.

as you can see from the figures 3, 4, 5, 6, and 7.

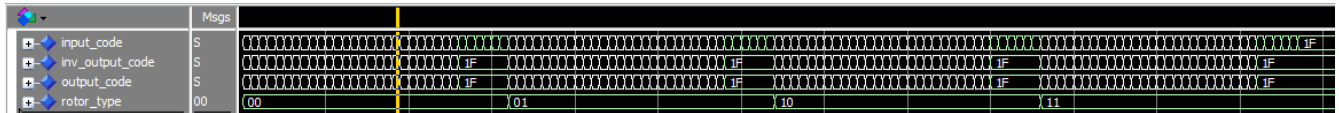


Figure 3: Tested circuit on ModelSim

	Msgs	
input_code	S	(A)(B)(C)(D)(E)(F)(G)(H)(I)(J)(K)(L)(M)(N)(O)(P)(Q)(R)(S)(T)(U)(V)(W)(X)(Y)(Z)(1A)(1B)(1C)(1D)(1E)(1F)
inv_output_code	S	(U)(W)(Y)(G)(A)(D)(F)(P)(V)(Z)(B)(E)(C)(K)(M)(T)(H)(X)(S)(L)(R)(I)(N)(Q)(O)(J)(IF)
output_code	S	(E)(K)(M)(F)(L)(G)(D)(Q)(V)(Z)(N)(T)(O)(W)(Y)(H)(X)(U)(S)(P)(A)(I)(B)(R)(C)(J)(IF)
rotor_type	00	(00)

Figure 4: With rotor I.

	Msgs	
input_code	S	(1F)(1F)(A)(B)(C)(D)(E)(F)(G)(H)(I)(J)(K)(L)(M)(N)(O)(P)(Q)(R)(S)(T)(U)(V)(W)(X)(Y)(Z)(1A)(1B)(1C)(1D)(1E)(1F)
inv_output_code	S	(1F)(A)(J)(P)(C)(Z)(W)(R)(L)(F)(B)(D)(K)(O)(T)(Y)(U)(Q)(G)(E)(N)(H)(X)(M)(I)(V)(S)(1F)
output_code	S	(1F)(A)(J)(D)(K)(S)(I)(R)(U)(X)(B)(L)(H)(W)(T)(M)(C)(Q)(G)(Z)(N)(P)(Y)(F)(V)(O)(E)(1F)
rotor_type	00	(00)(01)

Figure 5: With rotor II.

	Msgs	
input_code	S	(1F)(A)(B)(C)(D)(E)(F)(G)(H)(I)(J)(K)(L)(M)(N)(O)(P)(Q)(R)(S)(T)(U)(V)(W)(X)(Y)(Z)(1A)(1B)(1C)(1D)(1E)(1F)
inv_output_code	S	(1F)(T)(A)(G)(B)(P)(C)(S)(D)(Q)(E)(U)(F)(V)(N)(Z)(H)(Y)(I)(X)(J)(W)(L)(R)(K)(O)(M)(1F)
output_code	S	(1F)(B)(D)(F)(H)(J)(L)(C)(P)(R)(T)(X)(V)(Z)(N)(Y)(E)(I)(W)(G)(A)(K)(M)(U)(S)(Q)(O)(1F)
rotor_type	00	(01)(10)

Figure 6: With rotor III.

	Msgs	
input_code	S	(1F)(1F)(A)(B)(C)(D)(E)(F)(G)(H)(I)(J)(K)(L)(M)(N)(O)(P)(Q)(R)(S)(T)(U)(V)(W)(X)(Y)(Z)(1A)(1B)(1C)(1D)(1E)(1F)
inv_output_code	S	(1F)(H)(Z)(W)(V)(A)(R)(T)(W)(L)(G)(U)(P)(X)(Q)(C)(E)(J)(M)(B)(S)(K)(D)(Y)(O)(I)(F)(1F)
output_code	S	(1F)(E)(S)(O)(V)(P)(Z)(J)(A)(Y)(O)(U)(I)(R)(H)(X)(L)(N)(F)(T)(G)(K)(D)(C)(M)(W)(B)(1F)
rotor_type	00	(10)(11) sim:/g47_permutation_vhd_test/inv_output_code @ 987944 ps

Figure 7: With rotor V.

2 fsm

3 fsm\_testbed