



# MILES USER MANUAL



## Contents

S-Box to DDT .....	2
DDT To Truth Table .....	3
Truth Table Minimization.....	5
Linear Inequalities Generation.....	7
Contact Us.....	8

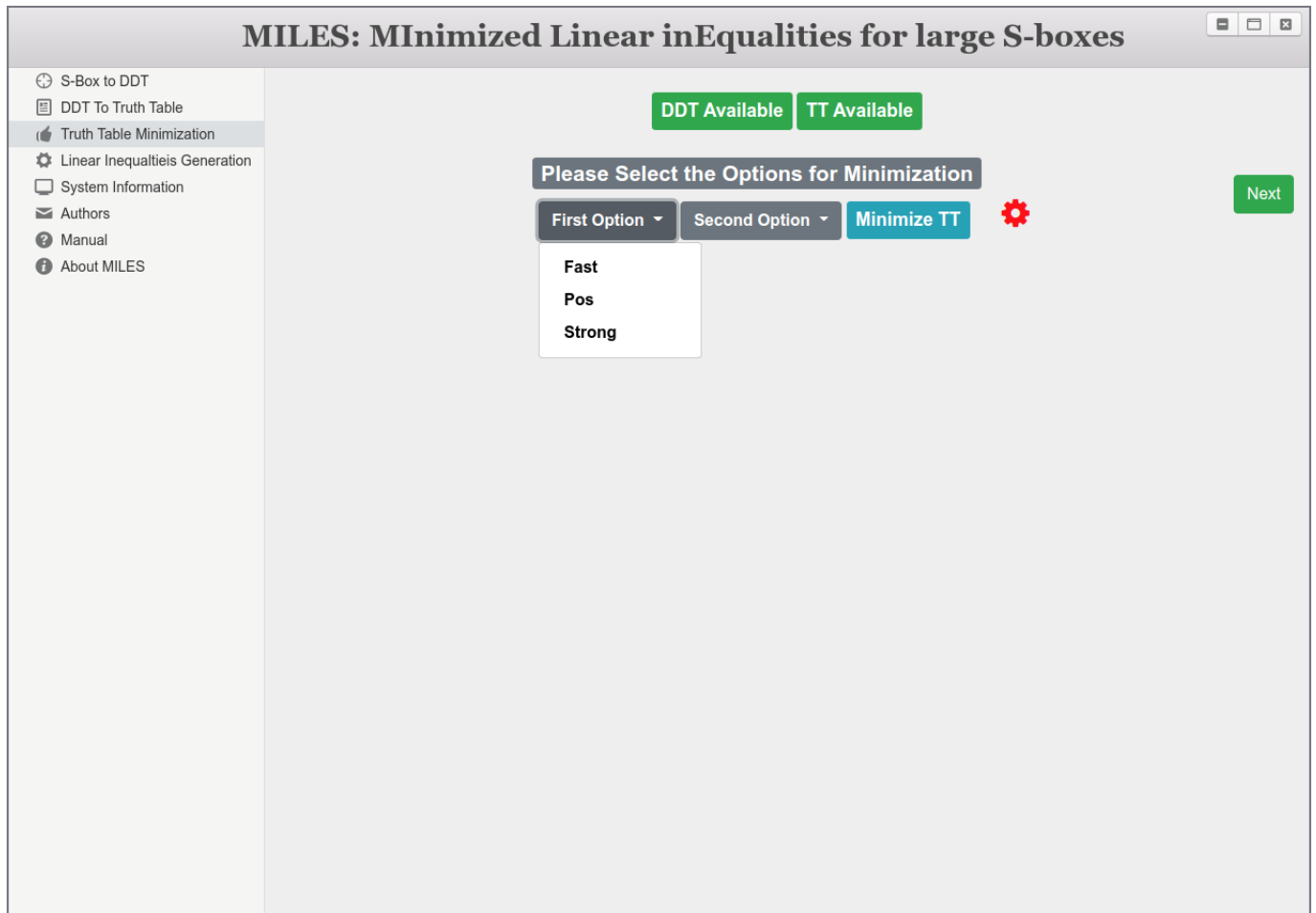


## DDT To Truth Table





## Truth Table Minimization





## Linear Inequalities Generation

S-Box to DDT

DDT To Truth Table

Truth Table Minimization

Linear Inequalities Generation

System Information

Authors

Manual

About MILES

DDT Available

TT Available

Minimized TT Available

Generate Linear Inequalities

Export Linear Inequalities

#	Linear Inequalities
1	$X_0 - X_1 + X_2 + X_3 + X_4 - X_5 - X_6 - X_7 - X_8 + X_9 + X_{10} + 4 \geq 0$
2	$X_0 - X_1 - X_2 + X_3 + X_4 + X_5 - X_6 - X_7 - X_8 + X_9 + X_{10} + 4 \geq 0$
3	$X_0 - X_1 + X_2 + X_3 + X_4 - X_5 + X_6 - X_7 + X_8 - X_9 + X_{10} + 3 \geq 0$
4	$-X_0 - X_1 + X_2 + X_3 + X_4 + X_5 - X_6 + X_7 + X_8 - X_9 + X_{10} + 3 \geq 0$
5	$-X_0 + X_1 + X_2 + X_3 - X_6 - X_7 + X_8 - X_9 + X_{10} + 3 \geq 0$
6	$-X_0 - X_1 + X_4 - X_5 + X_6 + X_7 + X_8 - X_9 + X_{10} + 3 \geq 0$
7	$X_0 - X_1 - X_2 + X_3 + X_4 + X_5 - X_6 + X_7 + X_8 - X_9 + X_{10} + 3 \geq 0$
8	$+X_1 - X_2 + X_3 + X_4 - X_5 - X_6 + X_7 + X_8 - X_9 + X_{10} + 3 \geq 0$
9	$X_0 + X_1 - X_2 + X_3 + X_4 - X_5 + X_6 - X_7 + X_8 - X_9 + X_{10} + 3 \geq 0$
10	$-X_0 - X_2 + X_3 + X_4 + X_5 + X_6 - X_7 + X_8 - X_9 + X_{10} + 3 \geq 0$
11	$X_0 - X_1 + X_2 - X_3 - X_4 - X_5 - X_6 - X_7 + X_8 - X_9 + X_{10} + 6 \geq 0$
12	$X_0 - X_1 - X_2 - X_3 - X_4 + X_5 - X_6 - X_7 + X_8 - X_9 + X_{10} + 6 \geq 0$
13	$X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_7 + X_8 + X_9 + X_{10} + -1 \geq 0$
14	$X_0 - X_1 + X_2 + X_3 + X_4 + X_5 - X_6 - X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$
15	$X_0 - X_1 - X_2 + X_3 + X_4 - X_5 - X_6 - X_7 + X_8 + X_9 - X_{10} + 5 \geq 0$
16	$-X_1 - X_3 + X_4 + X_5 - X_6 + X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$
17	$X_0 - X_1 + X_2 + X_3 - X_4 + X_6 - X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$
18	$+X_1 - X_3 + X_4 - X_5 - X_6 + X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$
19	$X_0 - X_3 + X_4 - X_5 + X_6 - X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$
20	$-X_0 - X_1 + X_2 + X_3 - X_4 + X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$
21	$-X_0 - X_3 + X_4 + X_5 + X_6 - X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$
22	$-X_0 + X_1 - X_3 + X_4 - X_6 - X_7 + X_8 + X_9 - X_{10} + 4 \geq 0$
23	$X_0 - X_2 + X_3 - X_4 - X_6 + X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$
24	$+X_1 - X_2 + X_3 - X_4 + X_6 - X_7 + X_8 + X_9 - X_{10} + 3 \geq 0$

7 | Page



**MILES: MInimized Linear inEqualities for large S-boxes**

[S-Box to DDT](#) | 
 [DDT To Truth Table](#) | 
 [Truth Table Minimization](#) | 
 [Linear Inequalities Generation](#) | 
 [System Information](#) | 
 [Authors](#) | 
 [Manual](#) | 
 [About MILES](#)

[DDT Available](#) | 
 [TT Available](#) | 
 [Minimized TT Available](#)

[Generate Linear Inequalities](#) | 
 [Export Linear Inequalities](#)

#	Linear Inequalities
1	$-X_0 - X_2 - X_3 - X_4 + X_5 - X_6 + X_7 + 4 \geq 0$
2	$-X_0 + X_2 - X_3 - X_4 - X_5 - X_6 + X_7 + 4 \geq 0$
3	$X_0 - X_1 + X_2 - X_3 + X_5 - X_7 + 2 \geq 0$
4	$X_0 - X_1 - X_2 - X_4 - X_5 - X_7 + 4 \geq 0$
5	$-X_0 + X_1 - X_2 - X_3 - X_4 - X_5 - X_6 + 2 \geq 0$
6	
7	
8	
9	
10	
11	$-X_0 - X_1 - X_3 + X_6 + X_7 - X_{10} + 3 \geq 0$
12	$-X_1 + X_4 - X_5 + X_7 - X_{10} + 2 \geq 0$
13	$-X_2 + X_5 + X_6 + X_7 + X_{10} + 0 \geq 0$
14	$+X_1 + X_2 + X_7 - X_9 + 0 \geq 0$
15	$+X_1 - X_3 + X_{10} + 0 \geq 0$
16	$X_0 - X_1 - X_2 + X_4 - X_7 - X_9 + 3 \geq 0$
17	$X_0 - X_1 - X_4 - X_6 - X_7 - X_{10} + 4 \geq 0$
18	$-X_6 + X_8 + X_9 + X_{10} + 0 \geq 0$

Linear Inequalities Saved to File: /home/tarunyadav/-LinearInequalities.txt

OK

## Contact Us

