Logic Design and Design for Security, Fall 2018

Project 2: SAT-based attack

1. Goal

In this project, you are given a SAT-attack program, the encrypted circuits and the corresponding original circuits.

(1) Read the circuit from the encrypted benchmarks

(2) Find out the location of key-gates, try to decide the key bits which contribute to less solving time, that is, the key bits that relatively having lower security level

(3) Reduce the specific key size and maximize the SAT-attack solving time with remaining key

(4) Output the reduced key to a file

(5) Scores are depending on the solving time compared with everybody

2. Input

Each encrypted circuit contains

(1) the correct key on the first line

(2) inputs, outputs and internal gates of the circuit

(3) NOTE: the type of gates only contains buf, not, or, nor, and, nand, xor, xnor, inputs of some gates may be more than two

Code	Explanation
# key=11101001001100110111	Correct key
INPUT(n1)	Primary input
INPUT(n2)	
….	
INPUT(keyinput0)	Key input
INPUT(keyinput1)	
….	
OUTPUT(n144$enc)	Primary output
OUTPUT(n298$enc)	
….	
G298 = buf(n293$enc)	Buffer gate
G4114 = and(n135, n4115)	And gate
G2825 = not(n2824)	Invert gate
….	

3. Output

Write your reduced key into a file

(1) '0' or '1' is the key bit you want to reduce, assign the correct value

(2) 'x' is the key bit you want to reserve

For example, if the correct key is 0101010101 (10 bits), you want to reduce 40% of it (the last four bits are selected here), then you need to output :

Output file
xxxxxx0101

NOTE: You don't need to change the circuit files, just output the reduced key

4. Command line

Your SAT-attack solver should take five arguments:

./solver [Encrypted circuit] [Original circuit] [Output File] [SatAttackExe] [N]

(1) SatAttackExe is the filename of the SAT-attack executable, and

(2) N is the percentage of key bits to be reduced. For example, setting N=20 means we want to reduce 20% of key size

The usage of SatAttackExe with specific key is:

./ SatAttackExe [Encrypted circuit] [Original circuit] –k xxxxxx0101

You can try it to test the reduced key you found

5. Hand in your assignment

Submit the following files in a zip, with student ID specified (e.g., 0456456.zip).

(1) Source codes

(2) A short (1~2 pages) report that introduces your implementation

6. Platform

Linux

7. Q&A

For any questions regarding this homework, please contact 蔡佳旅 (hyalineheaven@gmail.com).