Analysis of Circuit Reverse Engineering Techniques

Osaze Shears
oshears@gmu.edu

Advisor:
Houman Homayoun

Dept. of Electrical and Computer Engineering

I. Introduction

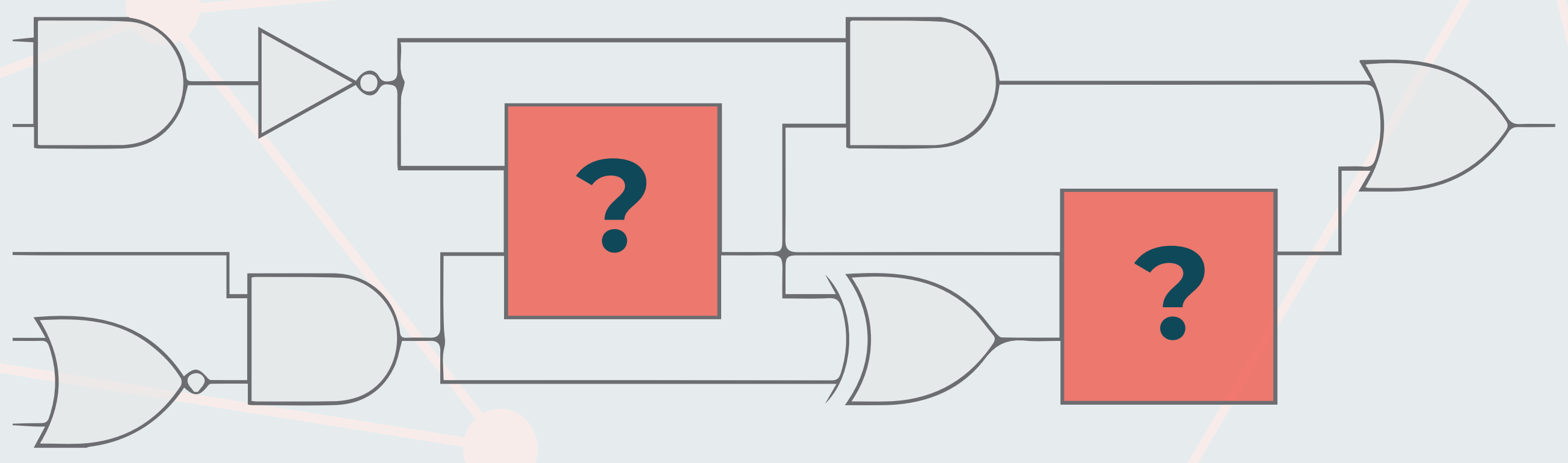
Intellectual property (IP) counterfeiting is the process of deconstructing an integrated circuit (IC) and analyzing its components for the purpose of wide scale redistribution without the original circuit designer's authorization. IP counterfeiting can take revenue away from businesses who produced the original designs, as well as put lives at risk when counterfeit circuits are sold for civilian and defense applications. This is because modifications may be made to counterfeit circuits that could cause them to malfunction, or discretely send information to remote sources. To combat this reverse engineering practice, research has been conducted on the methods used by attackers to reconstruct circuit designs in order to help improve prevention methods.

II. Methods

Two methods of reverse engineering prevention have been considered in order to evaluate the effectiveness of their corresponding reverse engineering methods.

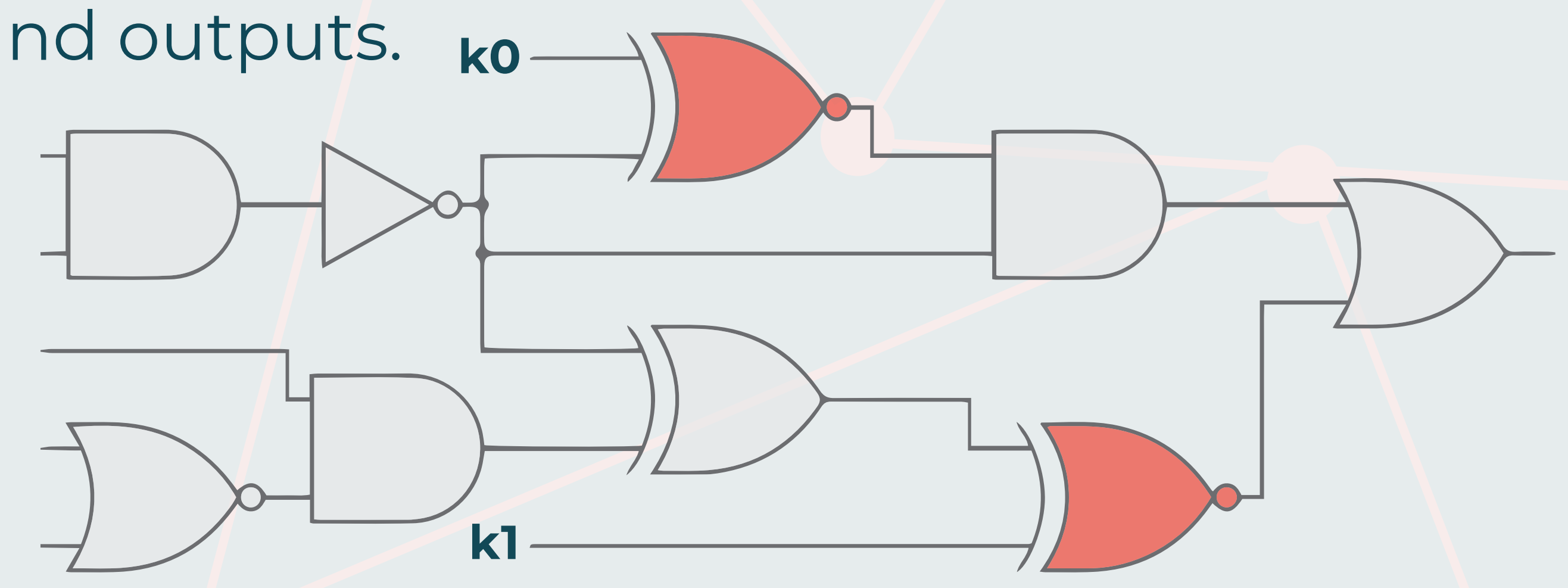
Camouflaging

Involves selecting individual logic gates that make up the IC and prevent them from being detectable via image processing attacks.



Obfuscation

A more intensive approach. It involves selecting individual logic gates on the design and connecting their outputs to XOR and XNOR gates that are interfaced alongside their inputs and outputs.



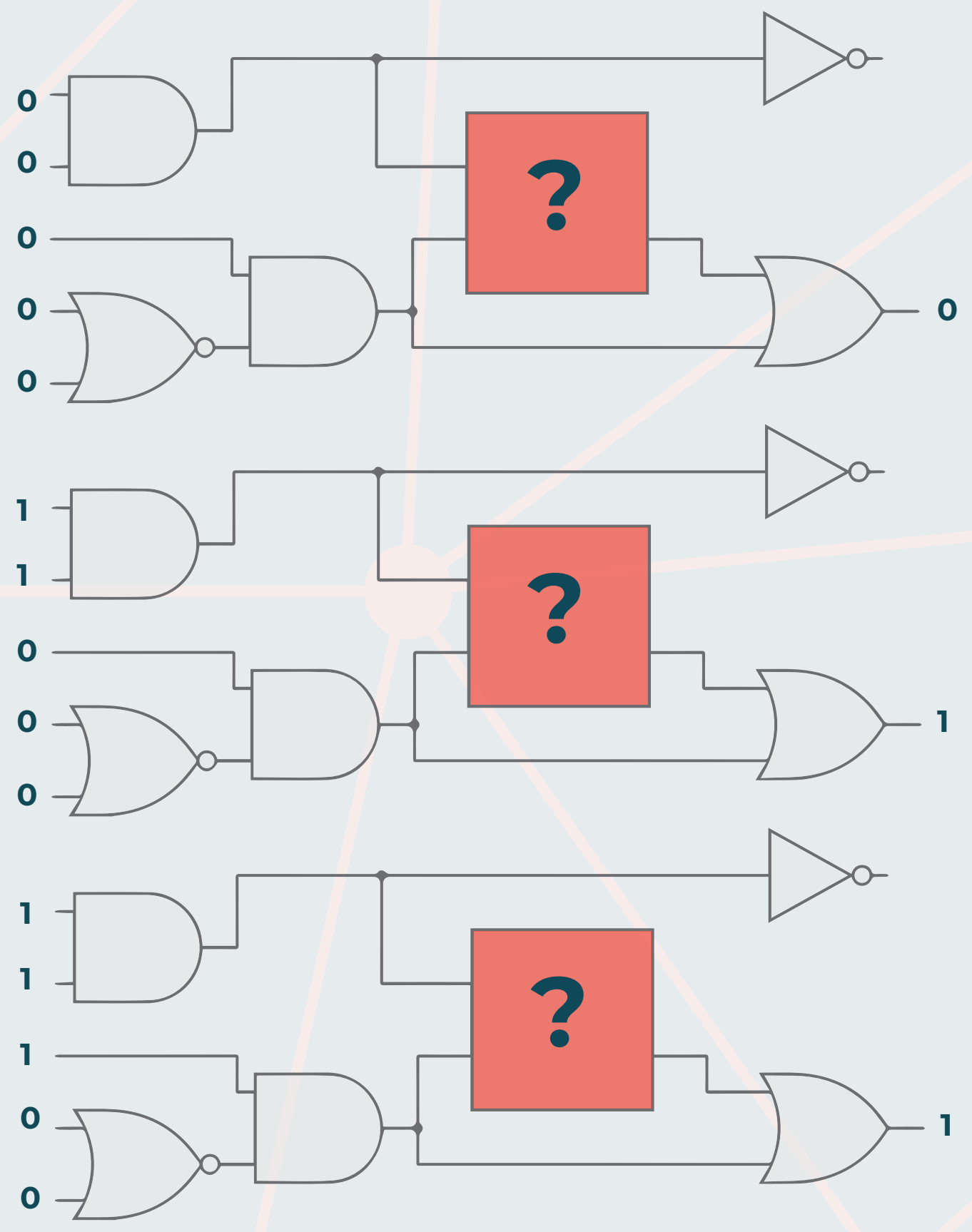
III. Results

For each of the reverse engineering prevention techniques listed in the Section II, an additional attack method was considered in order to evaluate the effectiveness of an attackers ability to identify the design of an IC.

Discriminating Set of Inputs

The first of these methods is a decamouflaging process to counter the first technique in Section II. The purpose of this algorithm is to identify the functions of the camouflaged gates. This process works by applying various combinations of inputs and recording the outputs for each combination. As input-output pairs are recorded, the number of logic gate possibilities that a hidden gate could represent decreases.

Input Gate Options vs Circuit Outputs



Input Combinations	00000	11000	11100
AND	0	0	
NAND	1		
OR*	0	1	1
NOR	1		
XOR	0	1	0
XNOR	1		

Distinguishing Input Pairs

The second method is a process for determining distinguishing input pairs that will counter the second technique in Section II. This algorithm determines the correct key combination for the black box circuit in order to observe the circuit's correction functional outputs, without being obscured by the added XOR and XNOR gates. In order to achieve this, the correct input-output pairs must be attained before the algorithm can determine the correct key.

IV. Discussion

From this research a greater understanding of contemporary reverse engineering attacks has been attained. Future work on this project will include implementing the attacks described in order to evaluate their performance on new defense techniques. The algorithms will operate in conjunction with a logic evaluation tool called MiniSAT.

V. References

[1] El Massad, M., Garg, S., & Tripunitara, M. V. (2015). Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes. In NDSS.

[2] Subramanyan, P., Ray, S., & Malik, S. (2015, May). Evaluating the security of logic encryption algorithms. In Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on (pp. 137-143). IEEE.