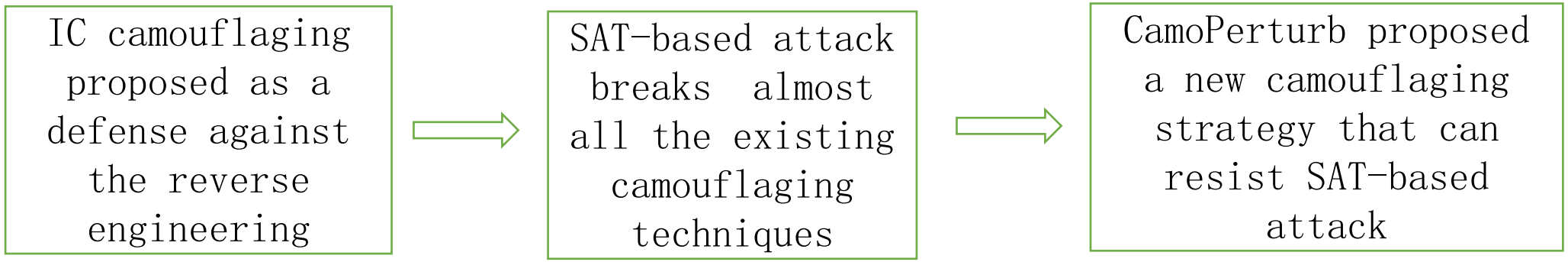
An Efficient Technique to Reverse Engineer Minterm Protection based Camouflaged Circuit

Shan Jiang, Ning Xu, XueYan Wang, Qiang Zhou

Jiang S, Xu N, Wang XY et al. An efficient technique to reverse engineer minterm protection based camouflaged circuit. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 33(5): 998-1006 Sept. 2018. DOI 10.1007/s11390-018-1870-z

1 Research Problem

- Background



- Purpose

✓ Evaluate the security of this minterm protection based camouflaging strategy to enhance its resistance against reverse engineering.

2 Kernel Contributions

1. Demonstrate the mechanism of influence relation between gate functionality and minterm perturbation in a circuit.

2. Propose a novel attack algorithm to reverse engineer the CamoPerturb circuit.

3. Evaluate the security of minterm protection based IC camouflaging strategy and give some suggestions for improvement.

Algorithm 1: Decamouflage CamoPerturb

Input: Camouflaged netlist, Functional IC
Output: perturbed minterm, changed gate

```
Remove CamoFix block;
foreach gate G in Cpert do
    Calculate the SMA{G};
    if |SMA(I)| = 1 then
        Record the minterm and gate in PerturbedList
    end
end
foreach minterm in PerturbedList do
    if the output of Camouflaged netlist and Functional IC
     is different then
        Restore gate functionality, Resolve functionality,
         Break;
    end
end
```

3 Conclusion

- Results
  - ✓ The proposed attack method is able to restore the camouflaged circuits with very little time consumption.
  - ✓ This minterm protection based camouflaging strategy still has some security vulnerabilities and should be improved.

- Future work
  - ➢ Synthesizing the perturbed circuit and camouflaged circuit to defend against removing attack.
  - ➢ Enhance the security of the remaining minterm perturbed block.