Abstract

Hassan Shokry El-Dib

SMT-Based Verification of Software Countermeasures against Side-Channel Attacks

A common strategy for designing countermeasures against side channel attacks is using randomization techniques to remove the statistical dependency between sensitive data and side-channel emissions. However, this process is both labor intensive and error prone, and currently, there is a lack of automated tools to formally access how secure a countermeasure really is. We propose the first SMT solver based method for formally verifying the security of a countermeasures against such attacks. In addition to checking whether the sensitive data are masked, we also check whether they are perfectly masked, i.e., whether the joint distribution of any d intermediate computation results is independent of the secret key. We encode this verification problem into a series of quantifier-free first-order logic formulas, whose satisfiability can be decided by an off-the-shelf SMT solver. We have implemented the new method in a tool based on the LLVM compiler and the Yices SMT solver. Our experiments on recently proposed countermeasures show that the method is both effective and efficient for practical use.