# Pusher: An Augmented Fuzzer based on Connection between Input and Comparison Operand

**Bin ZHANG,**

**Jiaxi YE, Ruilin LI, Chao FENG, Yunfei SU, Chaojing TANG**

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0075-8

# Problems & Ideas

- Problems of coverage based fuzzing for real-world programs when facing complex branch constraints
  - Huge and sizable search space
  - Less feedback from target program
- Ideas: Transform branch constraint bypass problem to a searching problem
  - Collect the connection between input and comparison operands when testing by instrumentation
  - Leverage searching algorithms like GA to quickly generate test cases that satisfies the branch constraint by searching in a limited space

# Main Contributions

- **Branch coverage for four real-world programs in 72 hours testing.**