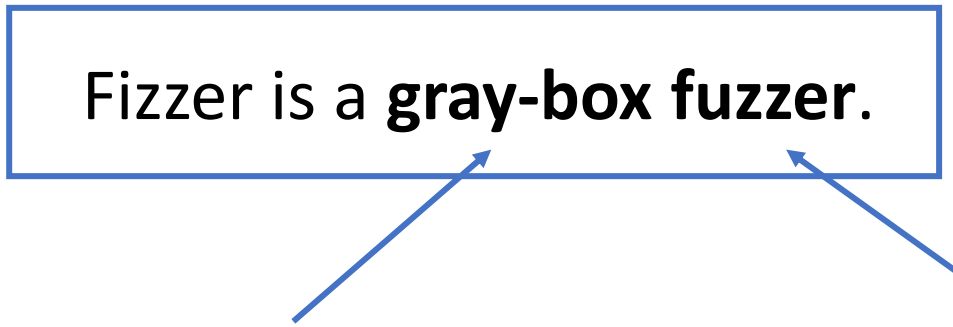
Fizzer: Covering Boolean Expressions

Martin Jonáš, Jan Strejček, Marek Trtík, Lukáš Urban

Tool Classification

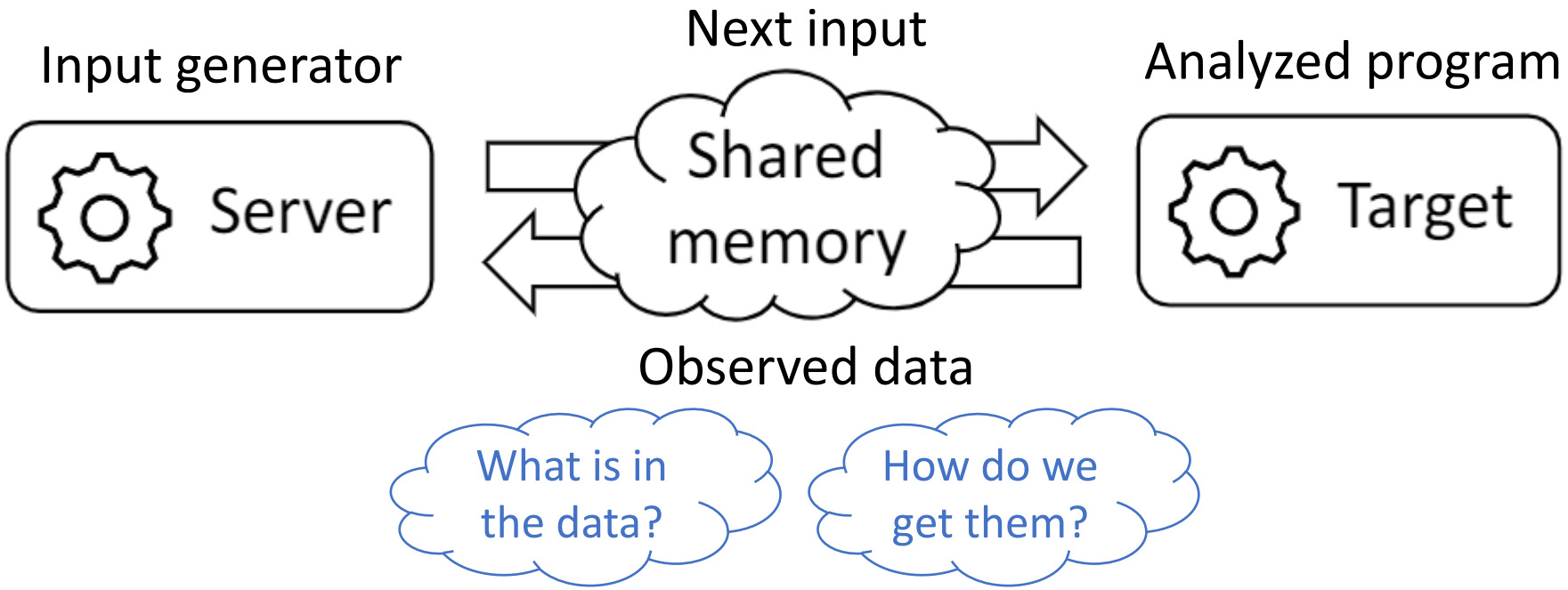


Only a **partial** information about the analyzed program is considered.

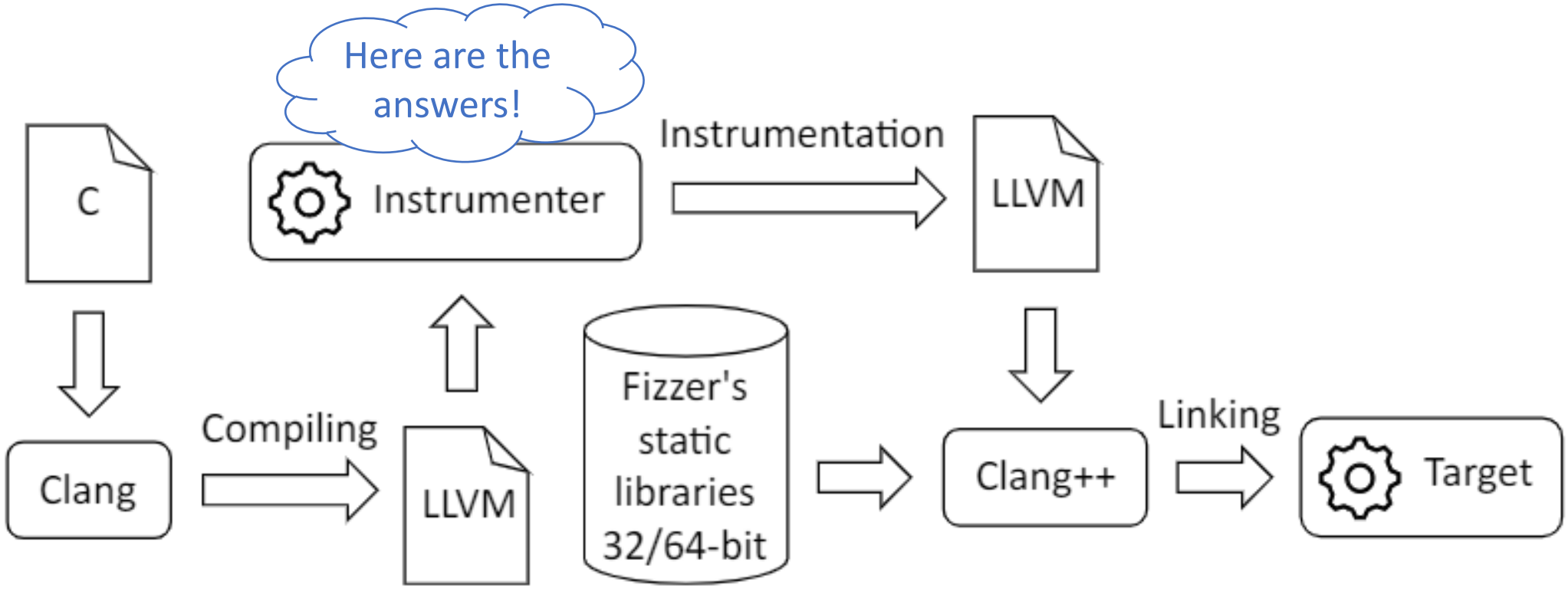
Next input is produced by **mutating** some previous input.

Functionality Overview

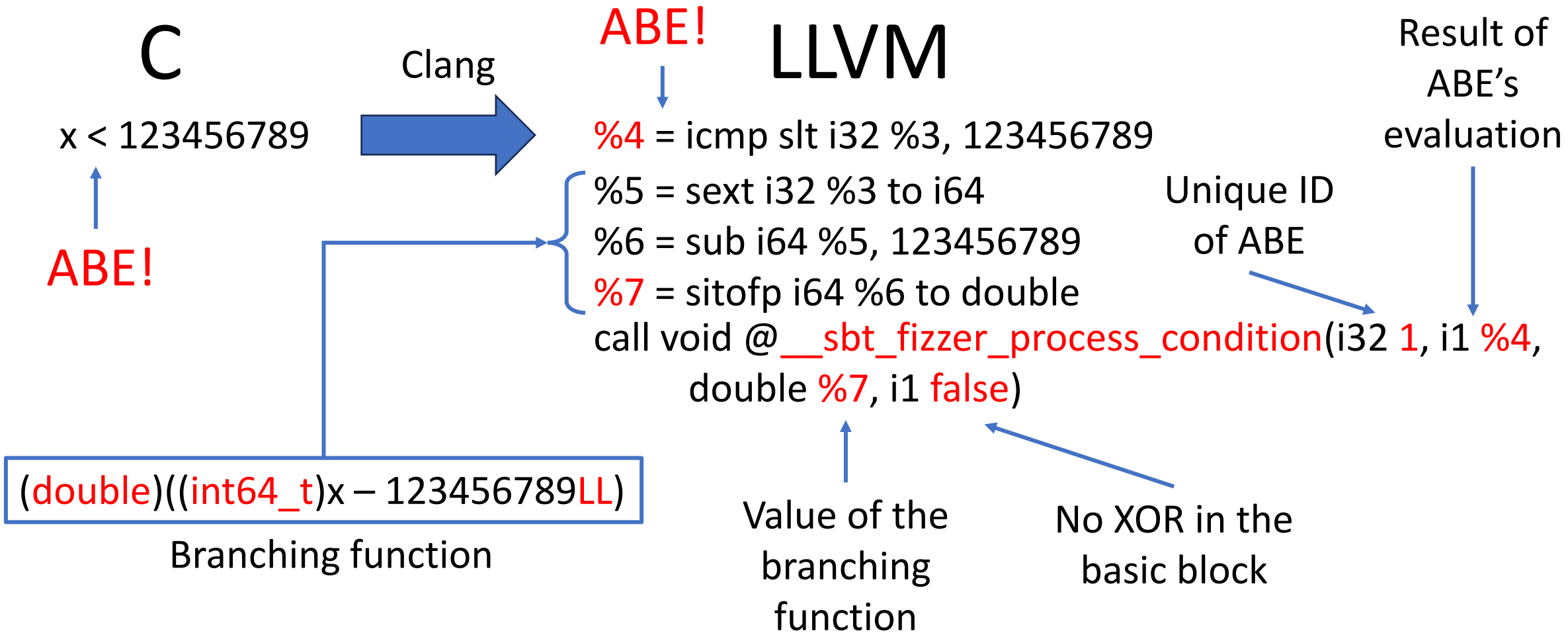
- The analysis proceeds in “rounds/iterations” of this form:



Building the Target Executable



Atomic Boolean Expression (ABE)



ABE Tree

- ABE tree is a **rooted binary tree**.
  - Nodes are ABEs.
    - The root is the first ABE reached during Target's execution.
  - Left outgoing edge – the ABE was evaluated to FALSE.
  - Right outgoing edge – the ABE was evaluated to TRUE.
  - Paths in the tree correspond to executed paths in the Target.
  - Each node also holds:
    - One of the **input**s for which the execution path reaches the node.
    - The value of the **branching function** obtained for that input.
    - Types for parts of the input (where the information is available).
- Input generation is a function defined on the ABE Tree.