**9. Encode Branches results analysis (0-add.c)**

|  |
| --- |
| 1. ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 **--Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis** --Functions=main --out=r1AntiBranchAnalysis.c /home/ubuntu/tigress/example/**0-add.c**  * Replace branches with other constructs.   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r1AntiBranchAnalysis.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r1AntiBranchAnalysis.c) |

|  |
| --- |
| \*\*\*\*\*\*  2. ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 **--Transform=InitBranchFuns** **--InitBranchFunsCount=2**  --Transform=AntiBranchAnalysis --Functions=main --AntiBranchAnalysisKinds=branchFuns --out=r2AntiBranchAnalysisKinds\_branchFuns.c /home/ubuntu/tigress/example/0-add.c  Comma-separated list of the kinds of constructs branches can be replaced with. Default=branchFuns.   * branchFuns = Generate calls to branch functions. --Transform=InitBranchFuns must be given prior to this transform   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r2AntiBranchAnalysisKinds\_branchFuns.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r2AntiBranchAnalysisKinds_branchFuns.c) |

|  |
| --- |
| 3.ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 **--Transform=InitBranchFuns --InitBranchFunsCount=2** --Transform=AntiBranchAnalysis --Functions=main **--AntiBranchAnalysisKinds=goto2call** --out=r3AntiBranchAnalysisKinds\_goto2call.c /home/ubuntu/tigress/example/0-add.c   * goto2call = Replace goto L with push L; call lab; ret; lab: ret   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [**r3AntiBranchAnalysisKinds\_goto2call.c**](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r3AntiBranchAnalysisKinds_goto2call.c) |

|  |
| --- |
| 4.ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main --AntiBranchAnalysisKinds=goto2push --out=r4AntiBranchAnalysisKinds\_goto2push.c /home/ubuntu/tigress/example/0-add.c   * goto2push = Replace goto L with push L; ret   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r4AntiBranchAnalysisKinds\_goto2push.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r4AntiBranchAnalysisKinds_goto2push.c) |

|  |
| --- |
| \*\*\*\*\*\*  5.ubuntu@user:~/tigress/8-Encode\_Branches/10-goto$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main --Transform=InitOpaque --Functions=main **--AntiBranchAnalysisOpaqueStructs=list,array,input** **--AntiBranchAnalysisKinds=goto2nopSled** --out=**r5AntiBranchAnalysisKinds\_goto2nopSled.c** /home/ubuntu/tigress/example/10-goto1.c  Or  ubuntu@user:~/tigress/8-Encode\_Branches/10-goto$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main --Transform=InitOpaque --Functions=main --AntiBranchAnalysisOpaqueStructs=list,array,input --AntiBranchAnalysisKinds=goto2push --AntiBranchAnalysisKinds=goto2nopSled --out=r5AntiBranchAnalysisKinds\_goto2nopSled.c /home/ubuntu/tigress/example/10-goto1.c     * goto2nopSled = Replace goto L with goto \*p where p is the address of a sequence of nop:s that eventually lead to L   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r5AntiBranchAnalysisKinds\_goto2nopSled.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r5AntiBranchAnalysisKinds_goto2nopSled.c) |

|  |
| --- |
| 6. ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main **--AntiBranchAnalysisKinds=\*** --out=r6AntiBranchAnalysisKinds\_star.c /home/ubuntu/tigress/example/0-add.c  \* = Same as branchFuns,goto2call,goto2push  ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r6AntiBranchAnalysisKinds\_star.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r6AntiBranchAnalysisKinds_star.c) |

|  |
| --- |
| 7. ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main **--AntiBranchAnalysisOpaqueStructs=list** --out=r7AntiBranchAnalysisOpaqueStructs-list.c /home/ubuntu/tigress/example/0-add.c  Comma-separated list of the kinds of opaque constructs to use. Default=list,array.   * list = Generate opaque expressions using linked lists   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r7AntiBranchAnalysisOpaqueStructs-list.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r7AntiBranchAnalysisOpaqueStructs-list.c) |

|  |
| --- |
| 8.ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main --AntiBranchAnalysisOpaqueStructs=array --out=r8AntiBranchAnalysisOpaqueStructs-array.c /home/ubuntu/tigress/example/0-add.c   * array = Generate opaque expressions using arrays   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r8AntiBranchAnalysisOpaqueStructs-array.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r8AntiBranchAnalysisOpaqueStructs-array.c) |

|  |
| --- |
| 9. ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main --AntiBranchAnalysisOpaqueStructs=input --out=r9AntiBranchAnalysisOpaqueStructs-input.c /home/ubuntu/tigress/example/0-add.c   * input = Generate opaque expressions that depend on input. Requires --Inputs to set invariants over input.   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r9AntiBranchAnalysisOpaqueStructs-input.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r9AntiBranchAnalysisOpaqueStructs-input.c) |

|  |
| --- |
| 10. ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main **--AntiBranchAnalysisOpaqueStructs=input** --out=r10AntiBranchAnalysisOpaqueStructs-env.c /home/ubuntu/tigress/example/0-add.c   * env = Generate opaque expressions from entropy. Requires --InitEntropy.   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r10AntiBranchAnalysisOpaqueStructs-env.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r10AntiBranchAnalysisOpaqueStructs-env.c) |

|  |
| --- |
| 11. ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main **--AntiBranchAnalysisOpaqueStructs=\*** --out=r11AntiBranchAnalysisOpaqueStructs-star.c /home/ubuntu/tigress/example/0-add.c  ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r11AntiBranchAnalysisOpaqueStructs-star.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r11AntiBranchAnalysisOpaqueStructs-star.c)   * \* = Same as list,array,input,env |

|  |
| --- |
| \*\*\*\*\*\*  12.ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ tigress --Environment=x86\_64:Linux:Gcc:4.6 --Transform=InitBranchFuns --InitBranchFunsCount=2 --Transform=AntiBranchAnalysis --Functions=main **--AntiBranchAnalysisKinds=branchFuns** **--AntiBranchAnalysisObfuscateBranchFunCall=true --AntiBranchAnalysisOpaqueStructs=list,array** --out=r12AntiBranchAnalysisObfuscateBranchFunCall.c /home/ubuntu/tigress/example/0-add.c   * Obfuscate the body of the branch function. Default=false.   ubuntu@user:~/tigress/8-Encode\_Branches/0-add$ gedit [r12AntiBranchAnalysisOpaqueStructs-list\_obfuscateT.c](https://github.com/ajaymas/tigress/blob/master/8-Encode_Branches/10-goto/r12AntiBranchAnalysisOpaqueStructs-list_obfuscateT.c) |

|  |
| --- |
| --AntiBranchAnalysisBranchFunFlatten |

|  |
| --- |
| --AntiBranchAnalysisBranchFunAddressOffset |