Publicationes Mathematicae Debrecen **Year: 2022** **Vol.: 100** **Fasc.: Suppl.**

Title: Control flow obfuscation with irreducible loops and self-modifying code

Author(s): Gregory Morse, Midya Alqaradaghi and Tamás Kozsik

This paper considers an obfuscation scheme designed around runtime generated self-modifying code and irreducible loops, both of which are notoriously difficult to reason about. This leads to a mechanism for both source and binary code that increase resistance to static analysis as well as dynamic analysis. By making use of the fact that static analysis of self-modifying code has limits in decidability as per Rice's theorem, and that transformation of irreducible loops to reducible ones using techniques such as node-splitting or introduction of variables can have a quadratic complexity increase on the size of the control-flow graph. Our construction looks at turning an algorithm into the lowest abstraction level with multi-input logic gates, to evaluate the most generic perspective on the scheme though it is applicable to any control-flow graph. A final benefit is that although complicated and naturally inter-related, the different ideas could be applied separately.