5G-AKA: A Formal Verification

David Clayton and Ira Harmon

December 11, 2018

Abstract: The 5th generation of cell phone technology is scheduled to be deployed by 2021. It will connect more people around the world than any prior generation. The 5G protocol suite includes modifications of proven protocols as well as new protocols. However, the foundation of 5G security rests upon the 5G-AKA protocol. Since inception, 5G-AKA has gone through multiple revisions due to discovered vulnerabilities. In this paper the most recent version of the protocol is tested using the Tamarin Prover and recommendations are made that would improve its overall security.