5G-AKA: A Formal Verification

David Clayton and Ira Harmon

November 29, 2018

Abstract:

1 Introduction

By 2019 over 5 Billion people are expected to own a mobile phone. Currently over 62 percent of the world population uses mobile phones. As cell phones become more pervasive their use touches every aspect of modern life: Facebook updates, news, and banking transactions are all increasingly done via cell. At this critical time in the evolution of cellular technology, 3GPP, the body that standardizes cell phone protocols is preparing to deploy 5G. And while 5G promises to connect more users with better service than previous generations, the unrestrained growth of the technology makes the security implications of 5G critical. 5G-AKA (Authentication and Key Agreement) is the first line of defense in securing mobile users communications. The protocol authenticates the user and distributes information that is used to derive session keys.

References

[1] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1383–1396. ACM, 2018.

[2] Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, and Thyla van der Merwe. A comprehensive symbolic analysis of tls 1.3. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1773–1788. ACM, 2017.

[3] Martin Dehnel-Wild and Cas Cremers. Security vulnerability in 5g-aka draft (3gpp ts 33.501 draft v0.7.0). Available athttps://www.cs.ox.ac.uk/5G-analysis/(2018/02/08).

[4] Anand R Prasad, Sivabalan Arumugam, B Sheeba, and Alf Zugenmaier. 3gpp 5g security. *Journal of ICT Standardization*, 6(1):137–158, 2018.