# 5G-AKA: A Formal Verification

David Clayton and Ira Harmon

November 29, 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 existing protocols as well as new protocols. However, the foundation of 5G security rest 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 through symbolic analysis and recommendations are made that would improve its overall security.

# 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 communications. The protocol authenticates the user and distributes long term keys. The most recent version of the protocol is outlined in 3GPP Publication TS 33.501 V15.2.0. In this paper we validate the most recent version of the protocol through symbolic analysis.

# 2 The 5G-AKA Protocol

5G-AKA is similar to authentication protocols used in previous generations. 5G allows for authentication via 5G-AKA or EAP-AKA. For the purposes of this paper, the focus is 5G-AKA. There are at least 4 actors in the 5G authentication process.

1) **UE** (user equipment) - The UE is a mobile device. It is identified by its SUPI (SUbscription Permanent Identifier). The SUPI serves the same purpose as the IMSI in previous generations.

2) **SEAF** (SEcurity Anchor Function) - The SEAF is co-located with the AMF (core Access Management Function). The SEAF creates a key, $K_{seaf}$, that is used to encrypt all communications during authentication [9]. This key is also used to derive the session key post authentication. The SEAF communicates with the UE via the SUCI (SUbscriper Concealed Identifier). This equivalent to the TMSI in previous generations.

3) **AUSF** (AUthentication Server Function) - The AUSF handles authentication requests for the 3GPP network and non-3GPP network. It informs the UDM of successful and failed authentications.

4) **UDM** (Unified Data Management) - The ARPF (Authentication credential Repository and Processing Function) is co-located with the UDM. The ARPF is located in the home network of the UE. The ARPF stores the long term key of the UE. This is the same key stored on the SIM card of the UE. The ARPF also stores the SUPI associated with each SUCI. It communicates an authentication vector back to the AUSF after receiving an authentication request. Because of its credential store it is the most secured component in the network [3].

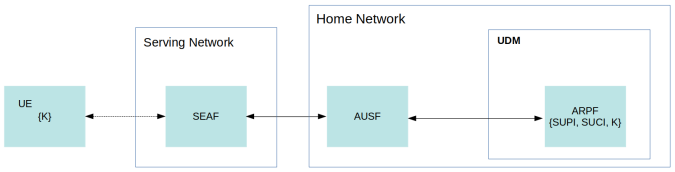


Figure 1: Dashed lines indicate insecure connections.

Figure 2.1 gives a high level overview of the connections between the four components.

## 3 Related Work

The Tamarin-Prover is software for the symbolic analysis and verification of security protocols.

## References


[1] 3rd generation partnership project; technical specification group services and system aspects; security architecture and procedures for 5g system 3gpp ts 33.501. Technical report, 3rd Generation Partnership Project, 650 Route des Lucioles Sophia Antipolis Valbonne France, 9 2018.

[2] 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.

[3] 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.

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

[5] Roger Piqueras Jover and Vuk Marojevic. Security and protocol exploit analysis of the 5g specifications. *arXiv preprint arXiv:1809.06925*, 2018.

[6] Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. The tamarin prover for the symbolic analysis of security protocols. In *International Conference on Computer Aided Verification*, pages 696–701. Springer, 2013.

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

[8] The Tamarin Team. Tamarin prover manual. Available at https://https://tamarin-prover.github.io/manual/tex/tamarin-manual.pdf, note = Online; accessed 27 October 2018.

[9] Xiaowei Zhang, Andreas Kunz, and Stefan Schröder. Overview of 5g security in 3gpp. In *Standards for Communications and Networking (CSCN), 2017 IEEE Conference on*, pages 181–186. IEEE, 2017.