Analysis of Randomness of GAEN keys

April Sheeran, Master of Computer Science

University of Dublin, Trinity College, 2024

Supervisor: Stephen Farrell

Digital contact tracing applications, such as those using the Google/Apple Exposure Notification (GAEN) system, have highlighted the critical role of cryptographic keys, particularly Temporary Exposure Keys (TEKs), in protecting user privacy while enabling contact tracing. This dissertation analyses the randomness of GAEN keys, specifically TEKs, to verify the privacy and security claims of the GAEN applications. This study employs a battery of statistical tests called Dieharder and a number of other statistical tests and visualisations to evaluate the randomness of GAEN keys generated by mobile devices across the world. This study contributes to the broader discourse on cryptographic key randomness and privacy-preserving technologies in the context of digital contact tracing.