Analysis of Randomness of GAEN keys

April Sheeran, MCS

A Dissertation

Presented to the University of Dublin, Trinity College

in partial fulfilment of the requirements for the degree of

Master of Science in Computer Science

Supervisor: Stephen Farrell

April 2024

Analysis of Randomness of GAEN keys

April Sheeran, Master of Science in Computer Science
University of Dublin, Trinity College, 2024

Supervisor: Stephen Farrell

...ABSTRACT...

Acknowledgments

Thank you Mum & Dad.

April Sheeran

University of Dublin, Trinity College

April 2024

Contents

List of Tables

List of Figures

Chapter 1

State of the Art

Give introduction

1.1 Background

introduction

1.1.1 What are GAEN Keys

Google and Apple developed the Google/Apple Exposure Notification (GAEN) system to facilitate contact tracing in response to the Covid-19 Pandemic. (Mention conventional contact tracing). Nations across the world used this technology to create contract tracing apps, for example Covid Tracker in Ireland and SwissCovid in Switzerland (Leith and Farrell (2021)).

The way the contact tracing works, if a user enables it, is as follows: Every 10-20 minutes the user's device will generate a random 128-bit key, referred to as a Temporary Exposure Key (TEK). The user's device will broadcast these keys using Bluetooth Low Energy (BLE). The user's device will listen and store the TEKs being broadcasted from other devices within a certain radius. These TEKs are stored locally on the device. If

a user tests positive for Covid, they can log this into the app. The app will send the user's recent TEKs (around the 14 days) to a central server managed by the local health authority. Every approx. 2 hours, the user's device will download the TEKs from the central server. The app compares these downloaded TEKs to the TEKs stored locally on the device. If there is a match, this means that the user has potentially been exposed to Covid and the app will notify them. CITES

Contact Tracing Apps

Studies on GAEN-based Apps

1.1.2 What is Randomness

1.2 Literature Review

1.2.1 How to Test for Randomness

1.2.2 Studies on Randomness Testing

1.2.3 Examples of Randomness Failures

1.3 Summary

Chapter 2

Design

2.1 Chosen Tests

2.1.1 Test Suites

The NIST and Dieharder test suites were chosen to evaluate the GAEN keys.

(May not be used because it wants streams of random numbers as input) NIST is widely used in industry (Hłobaż (2020)) (Brosas et al. (2020)) (Mohamed et al. (2012)) and is accepted as a standard. It contains tests that are recommended by NIST for the evaluation of PRNGs used in cryptography.

Dieharder is another widely used battery of tests for randomness created by Robert G. Brown. It is an extension of the Diehard suite of tests created by George Marsgalia.

2.1.2 Other Tests

Some tests outside of the test suites were performed. These include chi-squared test, lagplot and hilbert curve. The counts of the numbers of 1s and 0s in each bit position were also recorded and this data was plotted to allow for quick inspection.

This is a non-exhaustive list of possible tests. There are endless tests that can be ran to build confidence that the keys are random, however it is never certain if the data is

Dieharder Test	**Descriptions**
Birthdays Test	Item 1
OPERM5 Test	Item 1
32x32 Binary Rank Test	Item 1
6x8 Binary Rank Test	Item 1
Bitstream Test	Item 1
OPSO	Item 1
DNA Test	Item 1
Count the 1s stream Test	Item 1
Count the 1s byte Test	Item 1
Parking Lot Test	Item 1
Minimum Distance 2d circle Test	Item 1
Minimum Distance 3d sphere Test	Item 1
Squeeze Test	Item 1
Runs Test	Item 1
Craps Test	Item 1
Tang and Marsgalia GCD Test	Item 1
STS Monobit Test	Item 1
STS runs Test	Item 1
STS serial Test	Item 1
RGB Bit Distribution Test	Item 1
RGB Generalised Minimum Distance Test	Item 1
RGB Permutations Test	Item 1
RGB Lagged Sum Test	Item 1
RGB Kolmogorov-Smirnov Test	Item 1
Byte Distribution	Item 1
DAB DCT	Item 1
DAB Fill Tree Test	Item 1
DAB Fill Tree 2 Test	Item 1
DAB Monobit 2 Test	Item 1

Table 2.1: Tests in Dieharder test suite

truly random or not. The tests done here detect deviations from randomness rather than prove randomness.

Lagplot "A lag plot checks whether a data set or time series is random or not. Random data should not exhibit any identifiable structure in the lag plot. Non-random structure in the lag plot indicates that the underlying data are not random" (NIST (2010))

Hilbert Curve why ??

Spectral Test (Discrete FFT) Note that this description is taken from the NIST

documentation http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf . The focus of this test is the peak heights in the Discrete Fourier Transform of the sequence. The purpose of this test is to detect periodic features (i.e., repetitive patterns that are near each other) in the tested sequence that would indicate a deviation from the assumption of randomness. The intention is to detect whether the number of peaks exceeding the 95per cent threshold is significantly different than 5per cent.

Chi-squared A chi-square test checks how many items you observed in a bin vs how many you expected to have in that bin. It does so by summing the squared deviations between observed and expected across all bins (expand)

Plot of Counts Counts number of 0s and 1s in each bit position. Should be 50-50 1s and 0s. A plot of the data quickly shows any potential biases.

2.2 Closely-Related Work

2.2.1 Aspect #1

2.2.2 Aspect #2

2.3 Summary

Summarize the chapter and present a comparison of the projects that you reviewed.

	Aspect #1	**Aspect #2**
Row 1	Item 1	Item 2
Row 2	Item 1	Item 2
Row 3	Item 1	Item 2
Row 4	Item 1	Item 2

Table 2.2: Caption that explains the table to the reader

Bibliography

Brosas, D. G., Sison, A. M., Hernandez, A. A., and Medina, R. P. (2020). Analysis of the randomness performance of the proposed stream cipher based cryptographic algorithm. In 2020 11th IEEE Control and System Graduate Research Colloquium (ICSGRC), pages 76–81.

Hłobaż, A. (2020). Statistical analysis of enhanced sdex encryption method based on sha-512 hash function. In 2020 29th International Conference on Computer Communications and Networks (ICCCN), pages 1–6.

Leith, D. J. and Farrell, S. (2021). Contact tracing app privacy: What data is shared by europe's gaen contact tracing apps. In IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, pages 1–10.

Mohamed, E. M., El-Etriby, S., and Abdul-kader, H. S. (2012). Randomness testing of modern encryption techniques in cloud environment. In 2012 8th International Conference on Informatics and Systems (INFOS), pages CC–1–CC–6.

NIST (2010). Lagplot.