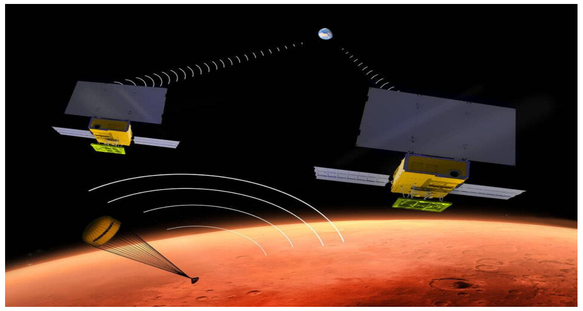
U40

Total Ionizing Dose Degradation of Symmetric Key Infrastructure in Space Telemetry

Augustus Richter*, Dr. Daniel Loveless
dlovele@iu.edu

Introduction

Space mission communication links often require encryption to protect sensitive telemetric and telecommand data [1]



Satellites with Return Space Link to Earth [2]

Total ionizing dose (TID), the dose accumulation from various radiation sources, can degrade electronic circuits on spacecraft [3]

Symmetric key infrastructure (SKI), the hardware, algorithms, and policies that manage keys and execute symmetric encryption, needs to be tested for reliability in radiation environments

Objective

To obtain TID failure threshold for AES coprocessor and compare entropy of random number generators (RNG) on system-on-chip (SoC) device

Methods

Use MSP430FR6989 as SoC in radiation lab with ^{60}Co source

- Apply a common dose rate of 30 Gy/hr over a week to get a total dose of ~ 5 kGy
- Run test operations below each hour

MSP430FR6989 SoC

Accuracy test: encrypt and decrypt table of messages at a 256-bit security level; find the dose threshold at which erroneous results start to occur

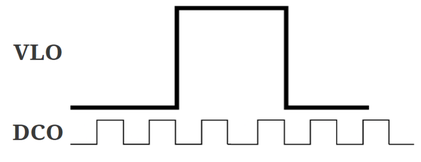
Entropy test: produce > 100-bit numbers using the RNGs and then:

- Conduct null hypothesis tests on the numbers assuming RNG is a Bernoulli variable with $p = 0.5$
- Compute estimators of min-entropy, a bound on randomness of a variable X:

$$H_{min}(X) = -log(max(p(x))$$

Results

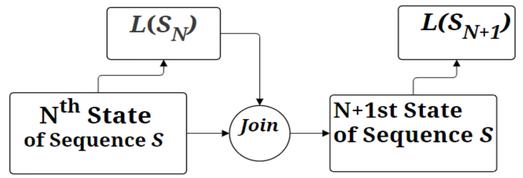
True-RNG has been implemented; it extracts a new bit by computing N mod 2 where N is the number of DCO clock cycles in one VLO clock cycle



Clock-Based Generator

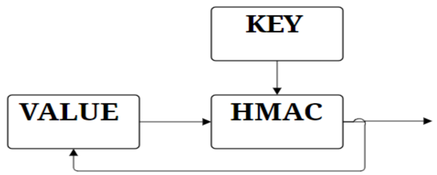
Two pseudo-RNGs have been implemented so far:

- Updates portion of a sequence S with linear function L



Linear-Feedback Shift Register

- Update a sequence through repeated hashing *HMAC(KEY, VALUE)*



HMAC-DRBG Algorithm

Discussion and Future Work

Experiment will be conducted in January or February

Results of experiment will be limited to devices with a similar architecture (e.g. similar clock subsystem)

The statistical tests will help inform engineers on when to factor TID effects into the design of security protocols for SKIs in space missions.

References

[1] CCSDS Cryptographic Algorithms, CCSDS 352.0-B-2 Blue Book, August 2019

[2] "CubeSats." The European Space Agency. https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/CubeSats (accessed Dec. 7, 2023)

[3] CERN-ESA-SSC. (2017). Radiation environment and its effects in EEE components and hardness assurance for space applications [Online]. Available: https://indico.cern.ch/event/635099/contributions/2570674/attachments/1456398/2249969/Radiation_Effects_and_RHA_ESA_Course_9-10_May_2017_TID_MP_FINAL_WIN.pdf

Acknowledgements

This work was supported, in part, by the U.S. Department of Defense under Contract W52P1J-22-9-3009