Paper ID: 53627
interactive
student

IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Advanced Technologies for Space Communications (1)

Author: Mr. Melvin Mathews
University of British Columbia, Canada

USING BIT FLIPS AS A SOURCE OF RANDOMNESS IN CUBESAT COMMUNICATION ENCRYPTION

Abstract

This paper will discuss the use of the randomness of bit flips in memory caused by ionized radiation in space, in conjunction with cryptographically-secure pseudorandom number generators (CSPRNGs) to improve upon CUBESAT communication encryption. CUBESAT encryption is largely unexplored but with their increasing popularity it is becoming vital that secure methods of CUBESAT communication both among CUBESAT constellations as well as to ground stations are established. While other methods of encryption exist and are widely used among CUBESATS and larger satellites alike (AES, blowfish, CubeSat Space Protocol, etc.), the use of bit flip locations in memory are an untapped source of randomness to create more secure cryptographic systems. A bit flip simulator shall be designed and utilized in conjunction with the Command and Data Handling and Communications sub-systems of UBC Orbit, a student-lead satellite design team, to conduct research. The prototyped design will be tested at TRIUMF, a Canadian cyclotron research facility. The results and conclusions drawn from this study will provide a potential benefit to the detriment bit flips present to CUBESAT communication by using them as a source of randomness for encryption.