An investigation of the effects of radiation on current key storage solutions and on Physical Unclonable Functions (PUFs) being used as key storage

Ravi Sarangdhar*, Yufan Fan*, Nikolaos Athanasios Anagnostopoulos*, Udo Gayer†,
Frank Flederer§, Tobias Mikschl§, Tolga Arul*, Philipp R. John†, Kirsten Hierholz‡,
Sergio Montenegro§ and Stefan Katzenbeisser*

* Security Engineering Group, Computer Science Department,
TU Darmstadt, Darmstadt, Germany
† Nuclear Physics Institute, Physics Department, TU Darmstadt, Darmstadt, Germany
‡ Institute for Radiooncology and Radiation Therapy, Klinikum Darmstadt, Darmstadt, Germany
§ Chair of Aerospace Information Technology, Computer Science Department,
Julius Maximilian University of Würzburg, Würzburg, Germany

Security and fault tolerance are two of the most important objectives that electronic device manufacturers have to meet before a product can go into mass production. These two goals either together or separately have the power to put a manufacturer out of business. Moreover, the choice of key storage solutions is very important with respect to the level of security a device manufacturer is willing to provide to the end customer. An ideal key storage would be completely fault-tolerant and would provide a high level of security, while also being cost-efficient.

However, environmental effects, such as ionising radiation, can significantly affect electronics, including key storage components. When exposed to ionising radiation, electronic devices can potentially suffer from threshold shifts, functional failures or leakage currents, which may also lead to temporary malfunctions or even permanent damage. Hence, it is important to investigate the effects of ionising radiation on different key storage solutions, with a particular focus on cost-efficient key storage solutions being used in high-radiation environments, such as Flash memory, and on novel secure key storage, such as Physical Unclonable Functions (PUFs).

Although the effects of radiation on semiconductor devices have been extensively studied in the past [Ba10, Do12, Ge13, Gi01, Go14, Ng98, Sa13, Sn89], to the best of our knowledge, no comprehensive study exists regarding the effects of radiation on cost-efficient contemporary memory components used for secure key storage, such as Flash memory found on commercial off-the-shelf (COTS) devices and SRAM PUFs implemented on such devices. We therefore aim to investigate the advantages and disadvantages of using such cost-efficient devices for secure and fault-tolerant key storage, by examining the effects of radiation on the two aforementioned memory components found on them. In this way, we will be able to determine their suitability for being used as secure key storage in high-radiation environments, such as nuclear plants, power facilities and the outer space, and in applications related to radiation therapy and nuclear weapons deterrence.

To this end, we want to investigate and evaluate the effects of radiation on the Flash memories of two COTS devices that are used in space applications, the STM32F407VG Discovery and the STM32L152RE Nucleo boards, as well as on memory-based PUFs implemented using the start-up values of the SRAMs of these two boards. In particular, we have already started conducting experiments using radioactive sources in order to induce faults on the two memory components of the boards and test their tolerance to such faults. However, current results have been less than promising, because of the low absorbed dose due to the limited period of time that the boards have so far been irradiated. Future experiments with stronger sources and for a longer period of time are planned.

Current and future experiments will be conducted using beta and gamma radiation emitting sources, which emit photons and electrons respectively. In this way, we can test the tolerance of key storage against radiation commonly occuring in high-radiation environments. Additionally, we measure the probability of persistent and non-persistent faults occuring both when the value of the memory cells is 1 and when their value is 0. In relevant literature, it has been noted that Flash memory cells are highly unlikely to be flipped from 1 into 0, due to the way in which they are constructed [Ba10, Sn89]. We therefore expect to observe faults in Flash memory only when the value of its cells is 0. Furthermore, we expect that the SRAM PUF will be able to recover from soft, non-persistent, errors, due to the volatile nature of SRAM, while the non-volatile Flash memory will not be able to do so. Finally, based on the number and nature of faults occuring, we will be able to estimate the probability of faults affecting a key stored in the Flash memory or generated by the SRAM PUF, taking into account existing error correction mechanisms. Therefore, we will be able to assess the fault tolerance of current secure key storage storage solutions in high-radiation environments.

References

[Ba10] M. Bagatin, G. Cellere, S. Gerardin, and A. Paccagnella. Radiation effects on NAND Flash memories, in *Inside NAND Flash Memories*, pp. 537-571. Springer Netherlands, 2010.

[Do12] E. Ć. Dolićanin. Gamma ray effects on Flash memory cell arrays. Nuclear Technology and Radiation Protection, 27(3):284-289. Vinča Institute of Nuclear Sciences, 2012.

[Ge13] S. Gerardin, M. Bagatin, A. Paccagnella, K. Grurmann, F. Gliem, T. R. Oldham, F. Irom, and D. N. Nguyen. Radiation Effects in Flash Memories. Transactions on Nuclear Science, 60(3):1953-1969, IEEE 2013.

[Gi01] A. Giraud, J. P. Le Gac, and J. M. Armani. Characterization of low voltage SRAM response to gamma radiation, in *6th European Conference on Radiation and Its Effects on Components and Systems*, pp. 494-499. IEEE, 2001.

[Go14] Maxim S. Gorbunov, Pavel S. Dolotov, Alexandra I. Shnaider, Gennady I. Zebrev, Andrey A. Antonov, and Anatoly A. Lebedev. Radiation-induced mismatch enhancement in 65nm CMOS SRAM for space applications, in *International Conference on Micro- and Nano-Electronics 2014*, Proceedings of SPIE, 9440(19), 2014.

[Ng98] D. N. Nguyen, C. I. Lee, and A. H. Johnston. Total ionizing dose effects on Flash memories, in *Radiation Effects Data Workshop*, pp.100-103. IEEE,1998.

[Sa13] G. Saxena, R. Agrawal, and S. Sharma. Single Event Upset (SEU) in SRAM. International Journal of Engineering Rearch and Applications (IJERA) 3(4):2171-2175, 2013.

[Sn89] E. S. Snyder, P. J. McWhorter, T. A. Dellin, and J. D. Sweetman. Radiation response of floating gate EEPROM memory cells. Transactions on Nuclear Science, 36(6):21312139. IEEE, 1989.