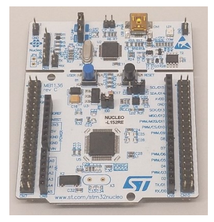
# Low-Temperature Attacks Against Digital Electronics: A Challenge for the Security of Superconducting Modules in High-Speed Magnetic Levitation (MagLev) Trains

**N. A. Anagnostopoulos, Y. Fan, M. Heinrich, N. Matyunin, D. Püllen, P. Muth, C. Hatzfeld, M. Rosenstihl, T. Arul, and S. Katzenbeisser**

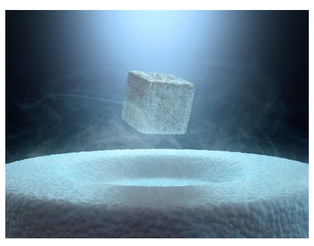
## Introduction and Motivation



- In recent years, Commercial Off-The-Shelf (COTS) devices have started to find application in custom use cases, such as space exploration and smart vehicular applications, where until recently only tailor-made hardware was employed.

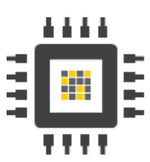
- Additionally, the notion of the Internet of Things (IoT), a network in which devices communicate with each other and take actions based on data acquired by other devices, without human intervention, has been steadily gaining popularity. In this context, the idea of an Internet of Railway Things (IoRT) has also started to gain significance. Furthermore, the IoT has achieved widespread adoption partly due to the low cost of the devices used in it, which are utilising economies of scale during their production.

- Moreover, recent advances in technology have enabled the introduction of high-speed trains, which are based on magnetic levitation. Such trains are commonly being referred to as MagLev trains, and some of the fastest MagLev trains are utilising superconducting magnets in order to achieve electrodynamic suspension. However, these superconducting magnets require extremely low temperatures in order to function properly.

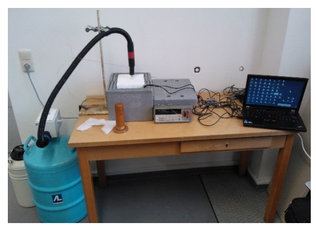


- Although certain materials seem to be able to act as superconducting magnets at *relatively* higher temperatures, usually such temperatures are only as high as 100 Kelvin (-173.15 degrees Celsius). Thus, the identification and examination of materials that can act as *superconducting* magnets at 0 degrees Celsius (273.15 Kelvin), let alone at room temperature (around 20-25 degrees Celsius), are still open research topics, with the relevant scientific field being rather at its infancy.

- We do note that superconducting modules would naturally require protection from physical tampering and other attacks. To this end, an on-site security solution is required. In this regard, we do also note that cryptographic protocols employed in order to secure IoT devices and networks are most often, if not always, based upon the agreement and storage of a secret, e.g. a key, in a secure manner. Additionally, such a security solution should ideally be lightweight and cost-efficient, in order to be used in practice.



## Our Work

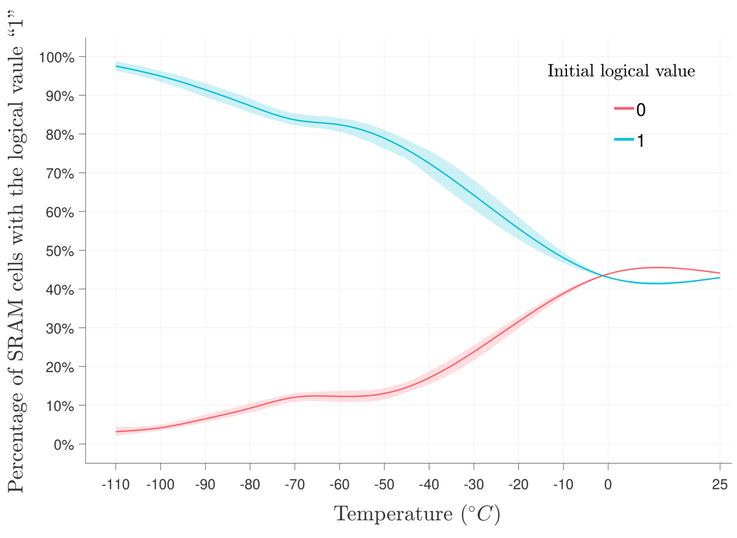


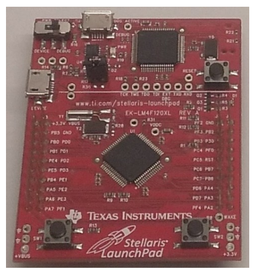
- We, therefore, examine, in this work, the ability of current Commercial Off-The-Shelf (COTS) volatile memory modules to act as secure and cost-efficient key storage, either in the context of their normal operation or while acting as instances of memory-based Physical Unclonable Functions (PUFs).

- In particular, we observe that the most well-known and widely used volatile memory modules, such as Static Random Access Memory (SRAM) and Dynamic Random Access Memory (DRAM) devices, suffer from increasingly higher degrees of data remanence as temperatures become lower, which precludes their usage as secure key storage modules in such conditions, due to cold boot attacks. Thus, we take note of the need for the future introduction of novel solutions in order to address this issue, which is occurring due to the temperature-dependent leakage of the semiconductors and the other electrical components of the examined memory devices.

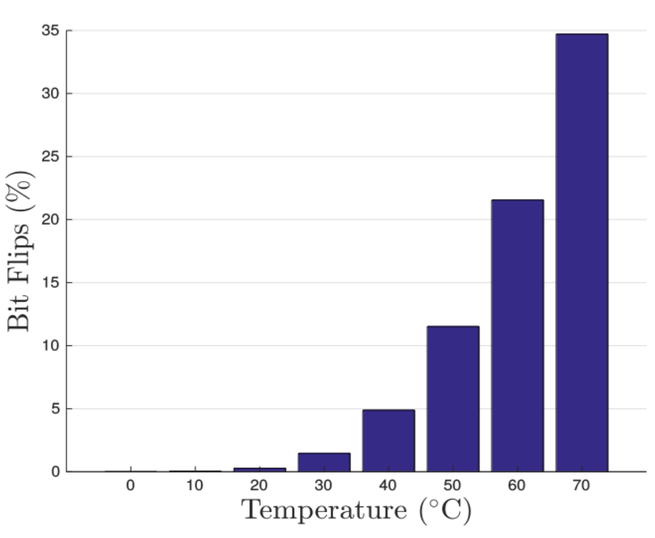
- Nevertheless, our work also demonstrates that contemporary volatile memory modules can successfully be utilised as temperature sensors, even at such a low temperature as -110ºC. Thus, we additionally suggest that the ability of such memory modules to serve as temperature detectors needs to be also tested at even lower temperatures, in the future.

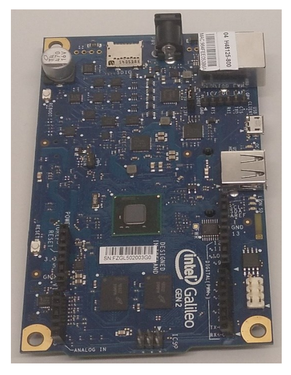
## Experimental Results




Data remanence (left) in the on-chip SRAM module of the LX4F120H5QR MCU of a TI Stellaris board (right), in the temperature range between -110°C and 25°C, as a percentage of SRAM cells with the logical value "1" after 10ms of power-off time, when all the cells initally either had the logical value of "1" (blue) or of "0" (red).




Number of bit flips (left) for a DRAM retention-based PUF implemented on the Micron MT41K128M8 DRAM of the Intel Galileo Gen 2 board (right), in the temperature range between 0°C and 70°C, as a percentage of the DRAM region being employed as a PUF, for a decay time of 300s. As the number of bit flips of the DRAM retention-based PUF is based on the loss of the values stored in the memory, it is essentially inversely proportional to the data remanence.

UNIVERSITÄT PASSAU

TECHNISCHE UNIVERSITÄT DARMSTADT

Funded by DFG Deutsche Forschungsgemeinschaft German Research Foundation

This work has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 236615297; 439892735; 440182124.