Addressing the Effects of Temperature Variations on Intrinsic Memory-Based Physical Uncloneable Functions

Nikolaos Athanasios Anagnostopoulos, Tolga Arul, Yufan Fan, Christian Hatzfeld, Fatemeh Tehranipoor, and Stefan Katzenbeisser

1 Computer Science Department, Technical University of Darmstadt, Germany
2 Department of Electrical Engineering and Information Technology, Technical University of Darmstadt, Germany
3 School of Engineering, San Francisco State University, United States of America

Physical Uncloneable Functions (PUFs) ideally act as functions encoded in hardware, which produce a unique output, being referred to as a response, for a specific input, being called a challenge. PUFs are often implemented using inherent components of a system, such as memory modules, in order to be practical and cost-efficient. Such PUFs are called intrinsic, as they do not require the addition of hardware for their construction and operation. Intrinsic PUFs can be used in low-end resource-constrained devices in order to implement flexible and low-weight cryptographic protocols. Well-known examples of memory-based intrinsic PUFs include SRAM-based and DRAM-based PUFs.

However, recent publications have revealed that temperature can have a dramatic effect on the performance of such intrinsic memory-based PUFs. Low temperatures can lead to data remanence in both DRAM and SRAM modules [HSH+09, AAF+18], significantly affecting their ability to serve as PUFs [AKR+16]. Additionally, high temperatures can speed up the aging of such modules and, therefore, potentially also affect their performance [TKYC17]. Finally, a number of recent works [SXA+17, SXA+18, AKCT18, KPHM18, AAF+18] have proven that DRAM retention-based PUFs, which can be accessed at runtime and provide multiple challenge-response pairs, are significantly affected by common temperature variations, such as those normally occurring through a day.

Our work addresses these issues through the usage of temperature sensors, which are inherent in most contemporary DRAM modules. We combine temperature readings obtained from such a sensor with the responses of the relevant PUF, in order to establish an authentication protocol that can be used at different temperatures, even if the PUF is highly dependent on temperature. Additionally, our protocol also disallows access to the PUF response, if the relevant temperature readings indicate that the performance of the PUF operation may have been afflicted by temperature-related effects, such as data remanence.

References


