An extensive classification and analysis of attacks against Physical Unclonable Functions (PUFs)

Nikolaos Athanasios Anagnostopoulos*, Sebastian Gabmeyer*,
Tolga Arul* and Stefan Katzenbeisser*

* Security Engineering Group, Computer Science Department, TU Darmstadt, Germany

Cryptographic applications usually require the storage of secret keys. Physical Unclonable Functions (PUFs) can provide secure key storage even on low-end hardware [Katz12], such as devices used for the Internet of Things (IoT). PUFs offer lightweight cryptographic solutions by exploiting intrinsic physical properties of hardware. Their security is based on the fact that, for a given input (PUF challenge), the PUF creates a unique output (PUF response).

Usually, PUF responses are afflicted with noise. Several methods, such as error correction and fuzzy commitment schemes, are used as a remedy. In this way, robust responses can be obtained and subsequently employed in a number of cryptographic applications. PUFs can not only serve as secure key storage, enabling device authentication and identification, but also act as security anchors for true random number generation, software attestation, secure boot and other applications.

PUFs have been derived from numerous different physical structures. The high number and diversity of PUF implementations has, so far, prevented a concise assessment of their resilience against attacks. This lack of insight has been further aggreviated by the significant number and diversity of corresponding attacks. The substantial and enduring popularity of research on attacks against PUFs has led to a plethora of publications. The large number of such publications makes it difficult to get a comprehensive overview of the field and therefore, also, a clear understanding of current threats against particular PUF implementations.

Another challenge originates from the fact that some papers may present particular attacks against certain PUF types, while others focus more on remedies for specific attacks. Additionally, an increasing number of publications survey thoroughly a particular PUF type, but only briefly examine relevant attacks and countermeasures. Consequently, although all this information is easily accessible, it is very difficult to use it for a higher order analysis which may consider multiple factors together and, therefore, require tedious processing. As a result, it is almost impossible to efficiently assess the effective security of different PUF implementations.

Our work aims to address the aforementioned shortcomings of publications regarding the security of PUFs. It is, to the best of our knowledge, the first systematic survey concerning attacks against PUFs. We examine the diverse and abundant relevant literature in a comprehensive manner, in order to identify classification categories for attacks against PUFs. We establish a novel classification concept using these categories and use it to classify the relevant literature, in order to provide a clear understanding of the current state of the art regarding threats to PUFs. Using the results of our classification, we can then assess the resilience of particular PUF implementations against different attacks. Consequently, we are also able to provide valuable insights into their security and, therefore, their suitability for different applications.

References

[Katz12] Stefan Katzenbeisser, Ünal Kocabas, Vladimir Rožic, Ahmad-Reza Sadeghi, Ingrid Verbauwhede and Christian Wachsmann. PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon (Extended Version). Cryptology ePrint Archive, Report 2012/557, 2012. https://eprint.iacr.org/2012/557