Fast and Reliable PUF Response Evaluation from Unsettled Bistable Rings

Abstract:
Bistable ring (BR) based strong PUFs are promising candidates for lightweight authentication applications. It has been observed that a good '0'/1'-balance of their responses correlates with longer settling times. This is problematic, since the state-of-the-art evaluation method requires the BR to be settled in order to generate a reliable PUF response. We show that settling times can easily extend beyond 100 milli seconds for 70 percent of the responses in the TBR PUF, which is a BR-based PUF with good '0'/1'-balance characteristics. Hence, it is practically impossible to wait for all BRs to settle, which results in a reliability penalty. In order to solve this problem, we present three new methods, which allow the evaluation of unsettled BRs with increased reliability compared to the state-of-the-art method. We were able to achieve evaluation times down to 1 micro second and improve response reliability from 80 percent to up to 98.5 percent. This enables the fast and reliable use of BR-based PUFs in strong PUFs applications.

Stichworte:
Bistable ring (BR), PUF
Kongress- / Buchtitel:            Euromicro Conference on Digital System Design (DSD 2016)
Kongress / Zusatzinformationen:  Limassol, Cyprus
Jahr:                            2016
Quartal:                         3. Quartal
Jahr / Monat:                    2016-08
Monat:                           Aug
Revied:                          ja
Sprache:                         en
Occurences:
  · Hochschulbibliographie > 2016 > Fakultäten > Elektrotechnik und Informationstechnik > Sicherheit in der Informationstechnik (Prof. Sigl)
  · Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2016
entries: