Ring oscillators (ROs) are a robust way to implement a physical unclonable function (PUF) into ASICs or FPGAs, but claims of predictability arose recently. We describe why this likely results from not using adjacent ROs for pairwise comparison because of spatial patterns in mean frequency and correlation coefficients found by principal component analysis. We show that the covariance is too small for our approach to estimate bits if adjacent ROs are compared. Our assumption of normality for the inter-device distribution passes an Anderson-Darling test and we outline that devices with proximate serial numbers are not more similar than other devices.
Jahr / Monat: 2014-12
Monat: Dec
Revied: ja
Sprache: en
WWW: http://www.isic2014.org/

Occurences:
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2014

Entries: