Abstract:

Recent publications have emphasized the power of high-resolution, low-distance EM measurements for side channel analysis. In this paper, we investigate several aspects of such measurements, e.g. different coil-diameters, probe-to-die distances, bandwidths and measurement resolutions. We use an FPGA-based implementation of an AES s-box as device under test and perform measurements of the magnetic near-field. Using the peak amplitude of the magnetic near-field and the Pearson correlation coefficient as quality measures, we show that the probes with smallest diameters lead to the best results. We propose a suitable trade-off between measurement time and measurement quality by using one fourth of the coil diameter as spatial measurement resolution. We show that the correlation is decreasing significantly if a bandwidth below 300 MHz is used and we recommend a bandwidth of 1 GHz. Additionally we confirm that the maximum value of the measured EM amplitude decreases by $1/r^2$, and the correlation of the measurement by $1/r$ with $r$ being the distance between probe and...
Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften

Kongress-/Buchtitel:
International Symposium on Integrated Circuits (ISIC)

Kongress/Zusatzinformationen:
Singapore

Jahr:
2014

Quartal:
4. Quartal

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: