Ultra-small designs for inversion-based S-Boxes

With RFID-tags becoming a part of our everyday lives, the need for (ultra-)lightweight implementations of cryptographic algorithms are a major challenge for researchers and engineers alike. While purpose-built algorithms offer low hardware-footprint, their usage is often impeded by the need to comply with standards, most notably the Advanced Encryption Standard (AES). We take on this challenge by devising a new way to design inversion based S-Boxes, such as the Rijndael S-Box. The design is based on the observation that inversion in Galois fields can be simulated using Linear Feedback Shift Registers (LFSRs), a fact that has been neglected until recently. Our contribution is threefold: First, we develop a general framework to describe inversion in arbitrary extension fields as linear-feedback structures. Second, we give alternative constructions for inversion circuits based on linear-feedback structures. Third, we leverage our framework to find linear-feedback structures of minimal size for inversion in the Rijndael-field used in AES S-Boxes. Using our framework we are able to fully explore the design space and give the first description of an (unprotected) AES SBox with an area requirement of less than 180
gate equivalents.

Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften

Kongress- / Buchtitel:
EUROMICRO Conference on Digital System Design (DSD) 2014

Kongress / Zusatzinformationen:
Verona, Italien

Jahr:
2014

Quartal:
3. Quartal

Jahr / Monat:
2014-08

Monat:
Aug

Revied:
ja

Sprache:
en

WWW:
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6927285

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

entries: