

# Cryptology ePrint Archive: Report 2011/332

## A depth-16 circuit for the AES S-box

*Joan Boyar and Rene Peralta*

**Abstract:** New techniques for reducing the depth of circuits for cryptographic applications are described and applied to the AES S-box. These techniques also keep the number of gates quite small. The result, when applied to the AES S-box, is a circuit with depth 16 and only 128 gates. For the inverse, it is also depth 16 and has only 127 gates. There is a shared middle part, common to both the S-box and its inverse, consisting of 63 gates.

**Category / Keywords:** implementation / AES; S-box; nite eld inversion; circuit complexity; circuit depth.

**Date:** received 17 Jun 2011

**Contact author:** peralta at nist gov

**Available formats:** [PDF](#) | [BibTeX Citation](#)

**Version:** 20110622:201147 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]