NAU
NORTHERN ARIZONA UNIVERSITY

Department of Mathematics and Statistics
Colloquium
Tuesday November 26
AMB 164 4:00 - 5:00 pm

Involutive S-Boxes over $\mathrm{GF}((2^3)^n)$ for $n \in \{2, 3, 4\}$

Tolga Yalçın

NAU - SICCS

Abstract

S-Boxes are fundamental building blocks for substitution layer in symmetric cryptography. While 4- and 8-bit S-Boxes have been extensively studied, there has been very little research on 3n-bit S-Boxes. In our study, we study a special class of 3n-bit S-Boxes, namely composite field involutive S-Boxes over $\mathrm{GF}((2^3)^n)$ for $n \in \{2, 3, 4\}$. We evaluate all 6, 9 and 12-bit S-Boxes in this class in terms of cryptographic properties as well as their physical implementation, i.e. chip area and present our results.

Refreshments at 3:45