A New Fundamental Structural Property on AES

Navid Ghaedi Bardeh, Sondre Rønjom

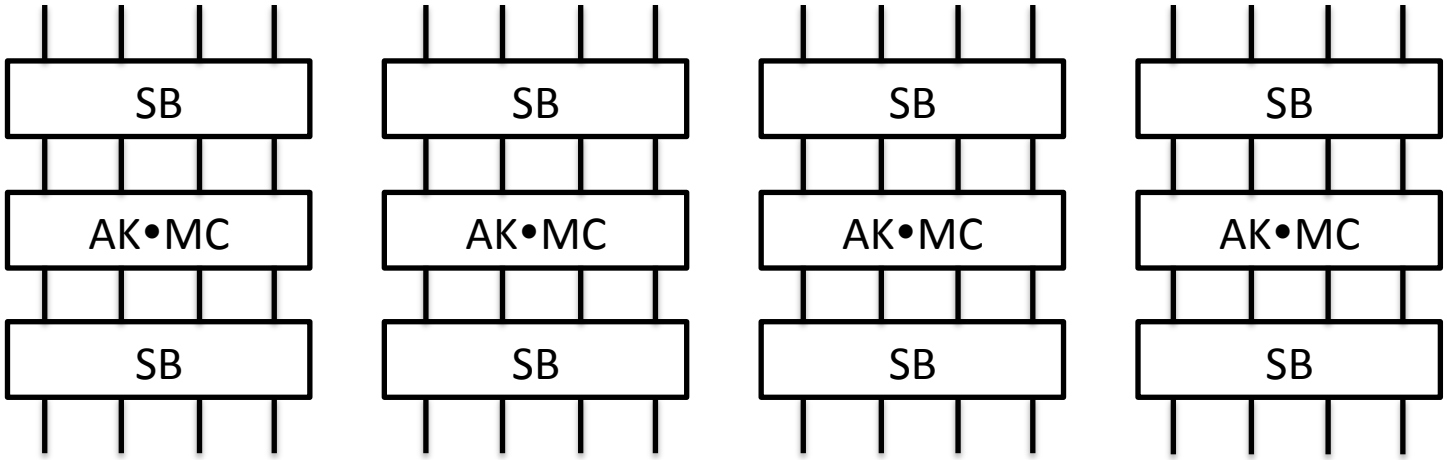
University of Bergen

07.03.2017

The AES Super- box

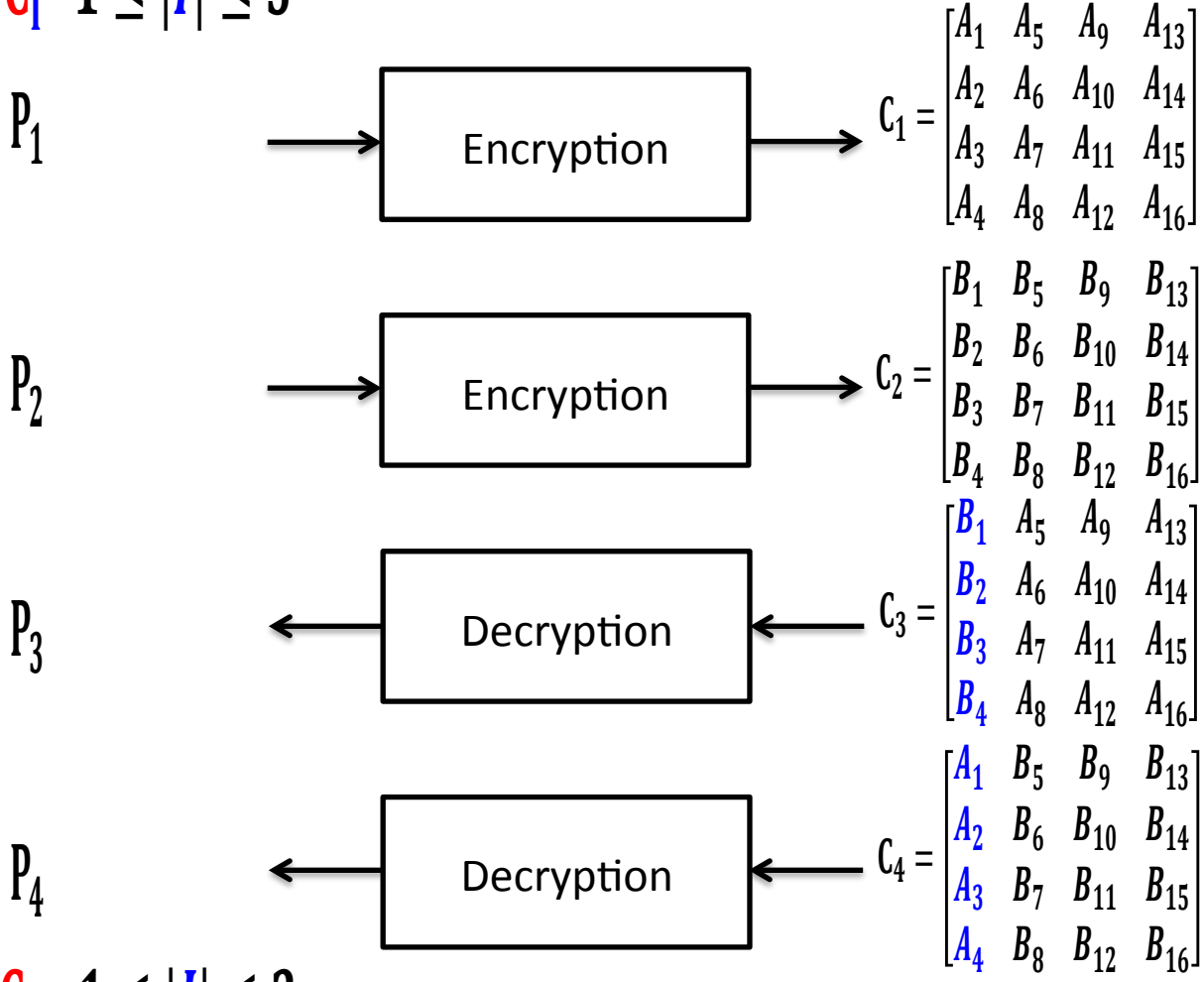
- The super- box representation for two rounds of the AES

SB•AK•MC•SB



A Structural Property on 4-rounds of AES

$P_1 \oplus P_2 \in C_I \quad 1 \le |I| \le 3$



$P_3 \oplus P_4 \in C_I \quad 1 \le |I| \le 3$

4-rounds of AES

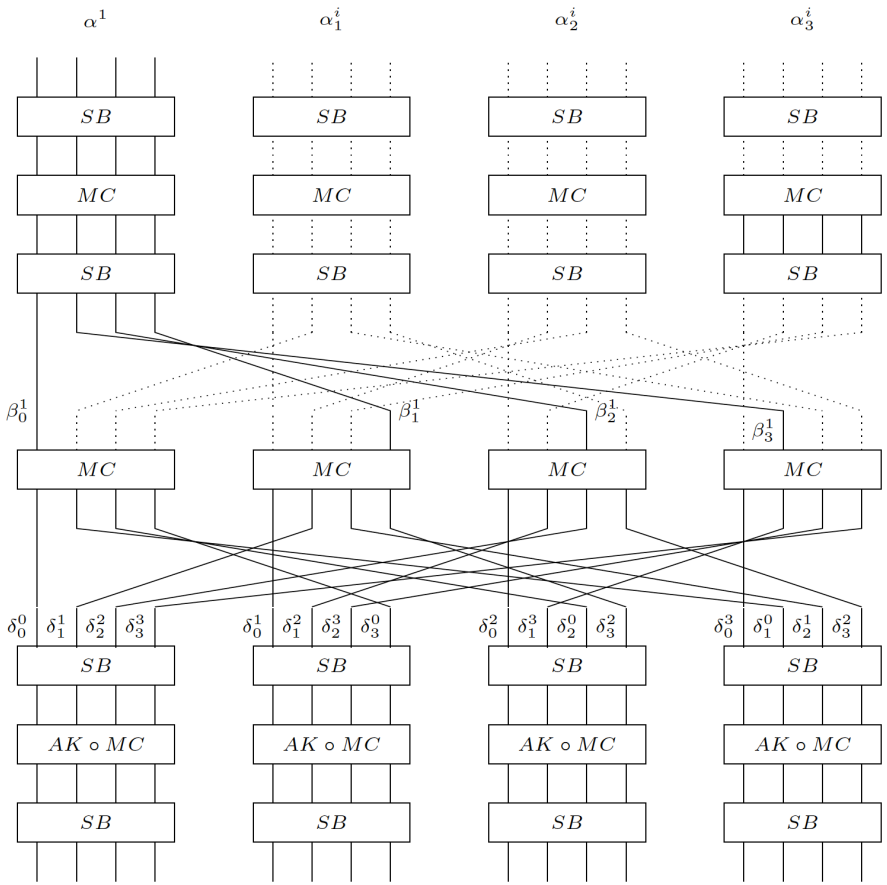


Figure 2: Four Rounds of AES minus final linear layer

6-rounds of AES

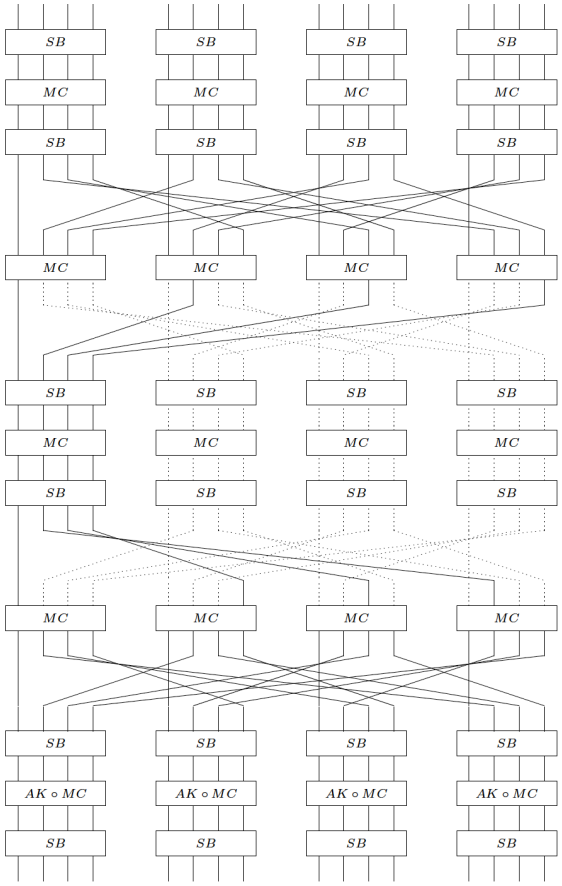


Figure 2: Six Rounds

Our Results

- 4-rounds distinguisher which need only 4 adaptively chosen plaintexts and ciphertexts to work.

- 5-rounds distinguisher that requires $2^{11.3}$ adaptively chosen plaintexts and ciphertexts.