New Results on Zorro

Orr Dunkelman

Computer Science Department
University of Haifa, Israel

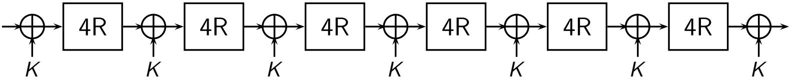
March 4th, 2014

Joint work with Ahiya Bar-On, Itai Dinur, Nathan Keller, Virginie Lallemand, María Naya-Plasencia, Boaz Tsaban, and Adi Shamir

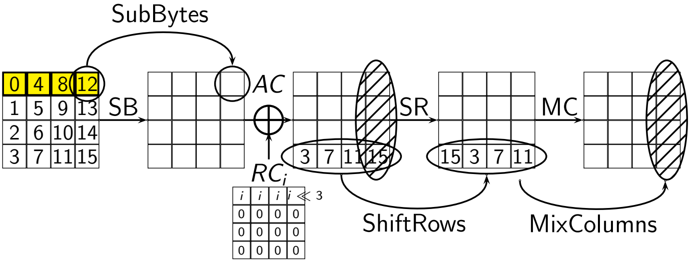
Zorro block cipher [G+13]

- Lightweight block cipher that targets side channel security.
- 128-bit block, 128-bit key.
- Single-key iterated Even-Mansour construction.
- 24 rounds, every four rounds the key is XORed to the state.
- Based on the AES

The ZORRO Block Cipher (cont.)



The ZORRO Round Function



Interesting Properties of Zorro [W+13]

- S-boxes are used only in the first row.

Interesting Properties of Zorro [W+13]

- S-boxes are used only in the first row.
- Circulant matrices have interesting properties when raised to the power. Namely,

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Interesting Properties of Zorro [W+13]

- S-boxes are used only in the first row.
- Circulant matrices have interesting properties when raised to the power. Namely,

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- **So what?**

Differential/Linear Properties of Zorro [W+13]

- Consider differences/masks of the form:

$$\begin{pmatrix} a & a & a & a \\ b & b & b & b \\ c & c & c & c \\ d & d & d & d \end{pmatrix}$$

- The equality of different columns remains, up to the S-boxes.

Differential/Linear Properties of Zorro [W+13]

- Consider differences/masks of the form:

$$\begin{pmatrix} a & a & a & a \\ b & b & b & b \\ c & c & c & c \\ d & d & d & d \end{pmatrix}$$

- The equality of different columns remains, up to the S-boxes.
- Which are applied only to the first row.

Differential/Linear Properties of Zorro [W+13]

- Consider differences/masks of the form:

$$\begin{pmatrix} a & a & a & a \\ b & b & b & b \\ c & c & c & c \\ d & d & d & d \end{pmatrix}$$

- The equality of different columns remains, up to the S-boxes.
- Which are applied only to the first row.
- So let's try to not activate it...

Differential/Linear Properties of Zorro (cont.)

$$\begin{pmatrix} 0 \\ a \\ 0 \\ b \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} 0 \\ a \\ 0 \\ b \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} 0 \\ c \\ d \\ e \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} 0 \\ c \\ d \\ e \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} 0 \\ f \\ 0 \\ g \end{pmatrix} \xrightarrow{SB}$$

$$\begin{pmatrix} 0 \\ f \\ 0 \\ g \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} \mathbf{h} \\ i \\ j \\ k \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} \mathbf{h} \\ i \\ j \\ k \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} 0 \\ a \\ 0 \\ b \end{pmatrix} \xrightarrow{AK} \begin{pmatrix} 0 \\ a \\ 0 \\ b \end{pmatrix}$$

Implications [W+13]

- Using the iterative characteristic it is possible to devise:
  - Differential attack (20-round characteristic, $2^{-108.3}$ probability, 4-R attack, $2^{112.4}$ CPs, $2^{112.4}$ time).
  - Linear distinguisher (24-round characteristic, $2^{-52.62}$ bias, 0-R attack, $2^{105.3}$ KPs).

Our Improvements — Linear Attack

- Distinguisher ⇒ key recovery transformation.
- 20-round linear characteristic
- 4-round attack
- Immediate attack — 2^{90} KPs and time
- With some more improvements can be reduced. . .

A Different Mask

- We can also change the mask a bit, to obtain characteristics with 2 active S-boxes every two rounds:

$$\begin{pmatrix} 0 & 0 \\ x_1 & x_3 \\ x_2 & x_2 \\ x_3 & x_1 \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} 0 & 0 \\ x_1 & x_3 \\ x_2 & x_2 \\ x_3 & x_1 \end{pmatrix} \xrightarrow{SR} \begin{pmatrix} 0 & 0 \\ x_3 & x_1 \\ x_2 & x_2 \\ x_1 & x_3 \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} \mathbf{c}' & 0 \\ a' & a \\ d & d' \\ b' & b \end{pmatrix}$$

$$\xrightarrow{SB} \begin{pmatrix} \mathbf{c}' & 0 \\ a' & a \\ d & d' \\ b' & b \end{pmatrix} \xrightarrow{SR} \begin{pmatrix} c' & 0 \\ a & a' \\ d & d' \\ b & b' \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} 0 & 0 \\ x_1 & x_3 \\ x_2 & x_2 \\ x_3 & x_1 \end{pmatrix}$$

A Different Mask (cont.)

- The different mask has 2 active S-boxes/2 rounds, rather than 4 active S-boxes/4 rounds.

A Different Mask (cont.)

- The different mask has 2 active S-boxes/2 rounds, rather than 4 active S-boxes/4 rounds.
- The gain is not in the probability, but rather in the key recovery phase.

Attack	Complexity		
	Data	Time	Memory
Differential	2^{95} CPs	2^{98}	—
Linear	$2^{83.3}$ KPs	2^{88}	2^{80}

Questions?

Thank you for your attention!