The Additive Differential Probability of ARX

V. Velichkov N. Mouha C. De Cannière B. Preneel

ESAT/COSIC, K.U.Leuven; IBBT

FSE 2011, February 14-16, Lyngby, Denmark

Outline

Introduction

ARX

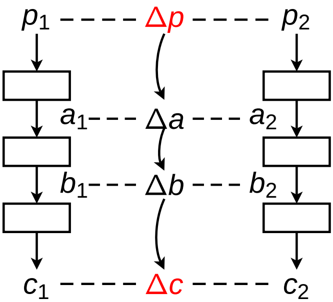
S-functions

adp$^{\mathsf{ARX}}$

Experiments

Outline

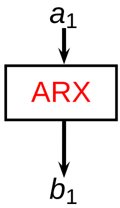
Differential Cryptanalysis



$$P(\Delta p \rightarrow \Delta c) = ?$$

Addition, Rotation, XOR

Combining $\boxplus$, $\lll$, $\oplus$ improves **resistance to differential cryptanalysis**



- Addition ($\boxplus$) : **non-linearity**
- Rotation ($\lll$) : **diffusion** within a single word
- XOR ($\oplus$): **diffusion** between words

Differential Properties of Addition, Rotation, XOR: Previous Work

P	$\boxplus$	$\lll$	$\oplus$	ARX
Δ^{+}	1	$\mathrm{adp}^{\lll}$	$\mathrm{adp}^{\oplus}$	$\mathrm{adp}^{\mathsf{ARX}}$
$\Delta^{\oplus}$	xdp^{+}	1	1	$\mathrm{xdp}^{\mathsf{ARX}} \Leftrightarrow \mathrm{xdp}^{+}$

adp : additive differential probability

xdp : xor differential probability

COSIC

Outline

Introduction

ARX

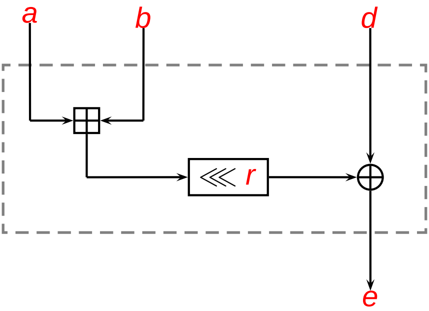
S-functions

adp$^{\text{ARX}}$

Experiments

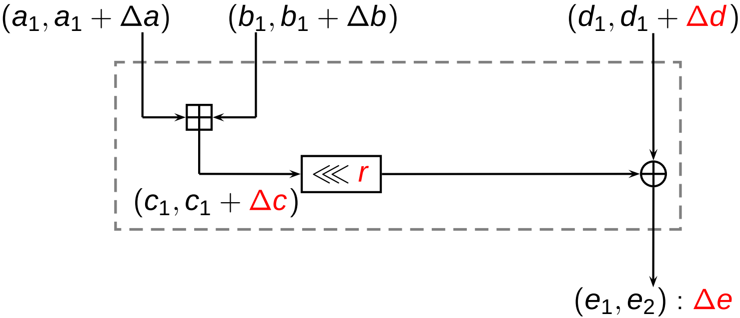
The ARX Operation

$$\mathrm{ARX}(a, b, d, r) = ((a + b) \lll r) \oplus d = e$$



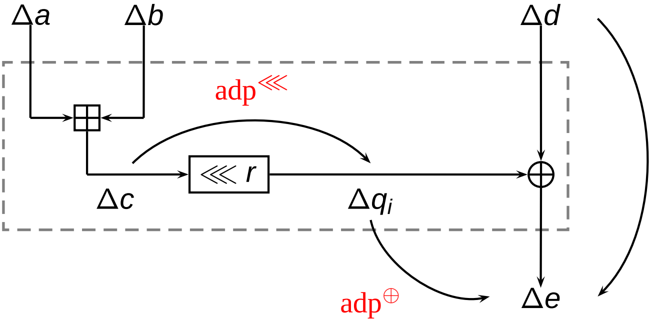
$\mathrm{adp}^{\mathrm{ARX}}$: the Additive Differential Probability of ARX

$$\mathrm{adp}^{\mathrm{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e) \triangleq \frac{|\{(c_1, d_1) : e_2 - e_1 = \Delta e\}|}{|\{(c_1, d_1)\}|}$$

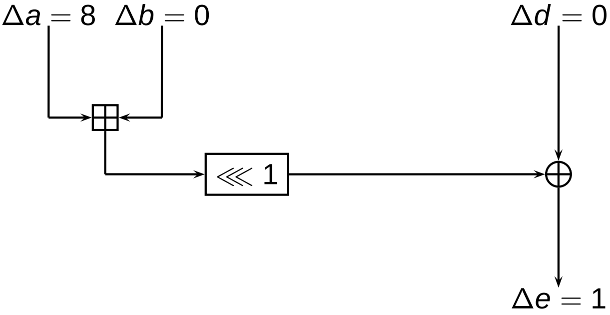


Estimation of $\mathrm{adp}^{\mathrm{ARX}}$ using $\mathrm{adp}^{\lll}$ and $\mathrm{adp}^{\oplus}$

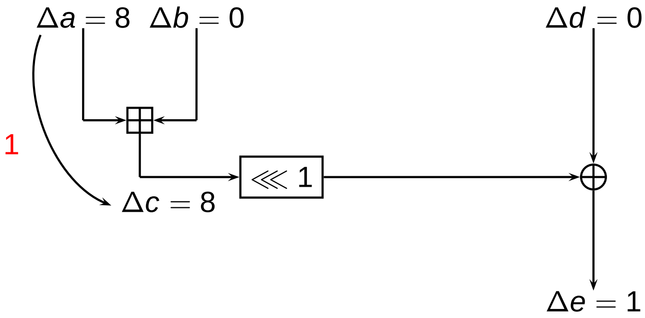
$$\mathrm{adp}^{\mathrm{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e) \approx \sum_i \mathrm{adp}^{\lll}(\Delta c \xrightarrow{r} \Delta q_i) \cdot \mathrm{adp}^{\oplus}(\Delta q_i, \Delta d \rightarrow \Delta e)$$



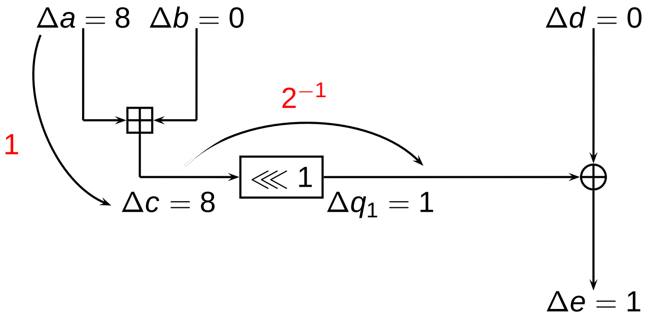
4-bit Example: $\mathrm{adp}^{\mathrm{ARX}} \neq \sum \mathrm{adp}^{\lll} \cdot \mathrm{adp}^{\oplus}$



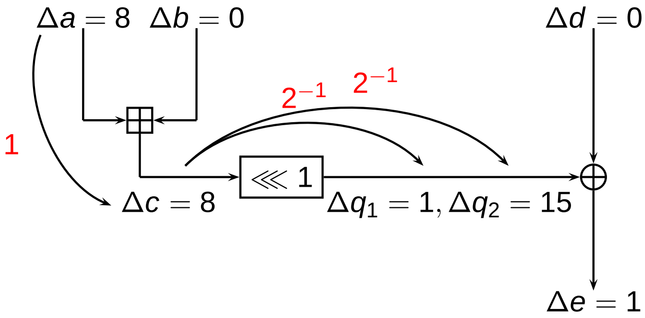
4-bit Example: $\text{adp}^{\text{ARX}} \neq \sum \text{adp}^{\lll} \cdot \text{adp}^{\oplus}$



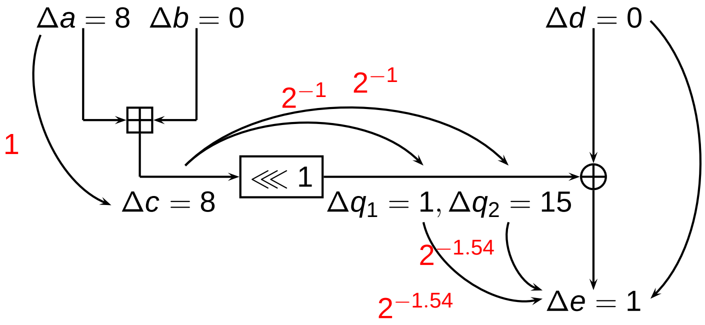
4-bit Example: $\mathrm{adp}^{\mathrm{ARX}} \neq \sum \mathrm{adp}^{\lll} \cdot \mathrm{adp}^{\oplus}$



4-bit Example: $\text{adp}^{\text{ARX}} \neq \sum \text{adp}^{\lll} \cdot \text{adp}^{\oplus}$



4-bit Example: $\mathrm{adp}^{\mathrm{ARX}} \neq \sum \mathrm{adp}^{\lll} \cdot \mathrm{adp}^{\oplus}$



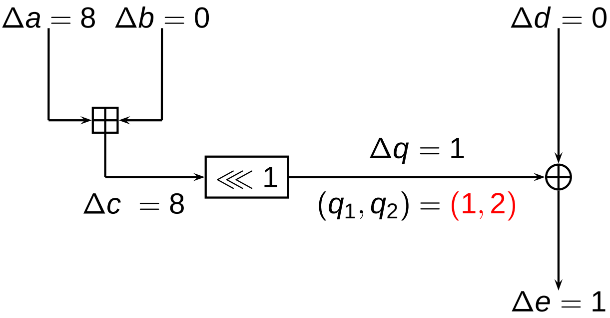
4-bit Example: $\mathrm{adp}^{\mathsf{ARX}} \neq \sum \mathrm{adp}^{\lll} \cdot \mathrm{adp}^{\oplus}$

$$\sum \mathrm{adp}^{\lll} \cdot \mathrm{adp}^{\oplus} = 2^{-1} \cdot 2^{-1.54} + 2^{-1} \cdot 2^{-1.54} = 2^{-1.54}$$

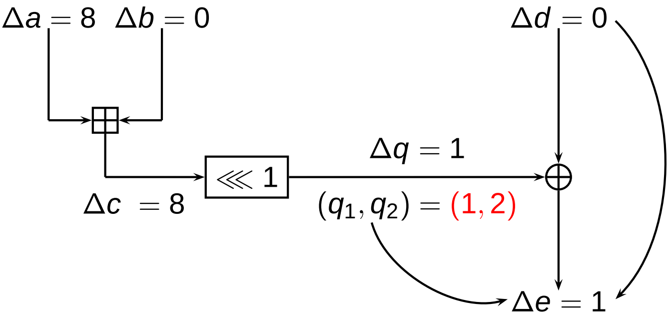
$$\neq$$

$$\mathrm{adp}^{\mathsf{ARX}} = 2^{-1}$$

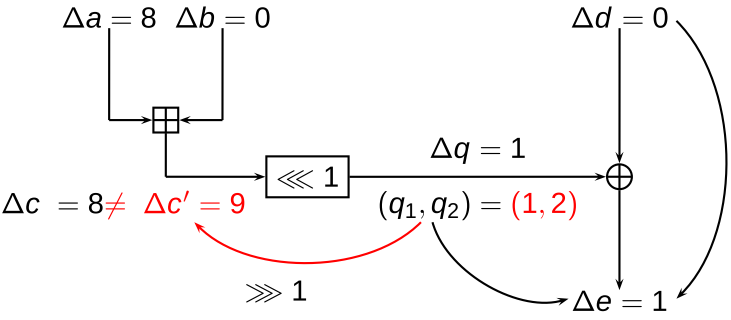
4-bit Example: $\mathrm{adp}^{\mathrm{ARX}} \neq \sum \mathrm{adp}^{\lll} \cdot \mathrm{adp}^{\oplus}$



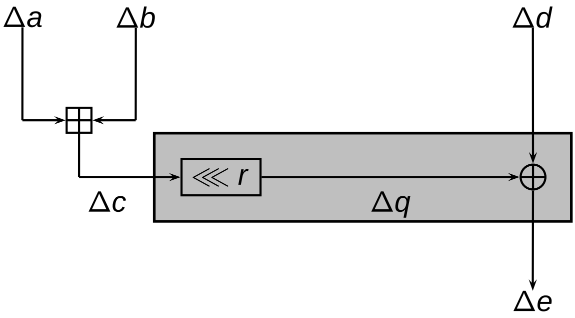
4-bit Example: $\mathrm{adp}^{\mathrm{ARX}} \neq \sum \mathrm{adp}^{\lll} \cdot \mathrm{adp}^{\oplus}$



4-bit Example: $\mathrm{adp}^{\mathrm{ARX}} \neq \sum \mathrm{adp}^{\lll} \cdot \mathrm{adp}^{\oplus}$



ARX as a Single Operation

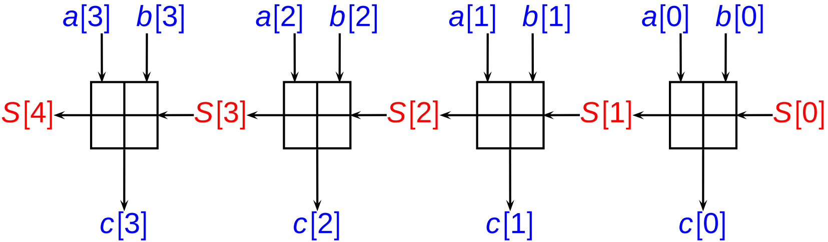


Outline

S-function [Mouha et al.,SAC 2010]

Simple 4-bit example: $a + b = c$

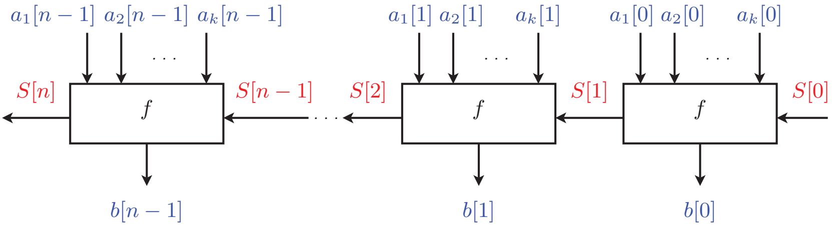
$$(c[i], S[i+1]) = f(a[i], b[i], S[i]), \quad 0 \leq i < 4 \ .$$



S-functions: General Case

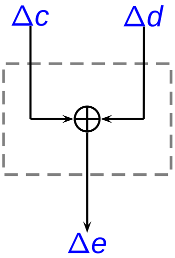
An S-function accepts n-bit words $a_1, a_2, \ldots, a_k$ and an n-digit input state S, and produces an n-bit output word b:

$$(b[i], S[i+1]) = f(a_1[i], a_2[i], \ldots, a_k[i], S[i]), \quad 0 \leq i < n \ .$$



S-function for adp$^{\oplus}$

$$(\Delta e[i], S[i+1]) = f(c_1[i], d_1[i], \Delta c[i], \Delta d[i], S[i]), \qquad 0 \leq i < n$$



$$\begin{cases} c_2 & \leftarrow c_1 + \Delta c \;, \\ d_2 & \leftarrow d_1 + \Delta d \;, \\ e_1 & \leftarrow c_1 \oplus d_1 \;, \\ e_2 & \leftarrow c_2 \oplus d_2 \;, \\ \Delta e & \leftarrow e_2 - e_1 \end{cases}$$

The State S

The state $S[i+1]$ at time $i+1$ is composed of **two carries** and **one borrow**:

$$S[i+1] \leftarrow (s_1[i+1], s_2[i+1], s_3[i+1]) \ ,$$

where

$$s_1[i+1] \leftarrow (c_1[i] + \Delta c[i] + s_1[i]) \gg 1 \ ,$$
$$s_2[i+1] \leftarrow (d_1[i] + \Delta d[i] + s_2[i]) \gg 1 \ ,$$
$$s_3[i+1] \leftarrow (e_2[i] - e_1[i] + s_3[i]) \gg 1 \ .$$

The **initial state** is

$$S[0] = (0, 0, 0)$$

All States

$S[i]$ has **fixed size** of 3 bits. There are 8 states in total:

$S[i]$	0	1	2	3	4	5	6	7
$s_1[i], s_2[i], s_3[i]$	0,0,-1	1,0,-1	0,1,-1	1,1,-1	0,0,0	1,0,0	0,1,0	1,1,0

- **One adjacency matrix** describes
  - all transitions $S[i] \to S[i+1]$ for fixed $(\Delta c[i], \Delta d[i], \Delta e[i])$
- **Eight adjacency matrices** in total
  - one for each 3-tuple $(\Delta c[i], \Delta d[i], \Delta e[i])$
  - computed using the S-function for $\mathrm{adp}^{\oplus}$

The Adjacency Matrices

$$(\Delta c[i], \Delta d[i], \Delta e[i]) = (0, 1, 1)$$

$$S[i+1] \quad \overset{S[i]}{\begin{array}{c|cccccccc} & 0 & 1 & \mathbf{2} & 3 & 4 & 5 & 6 & 7 \\ \hline 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{2} & 0 & 1 & \mathbf{4} & 0 & 1 & 0 & 0 & 1 \\ 3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}}$$

$\mathbf{A_{011}}$

Interpretation:
There are **4** pairs $(c_1[i], d_1[i])$ for which $(\Delta c[i], \Delta d[i] \to \Delta e[i])$, and $S[i] = 2 \to S[i+1] = 2$

Example: $\mathrm{adp}^{\oplus}(\Delta c, \Delta d \rightarrow \Delta e)$

MSB			LSB	
0	0	0	1	Δc
0	0	0	0	Δd
0	0	0	1	Δe

Example: $\mathrm{adp}^{\oplus}(\Delta c, \Delta d \rightarrow \Delta e)$

MSB			LSB	
0	0	0	1	Δc
0	0	0	0	Δd
0	0	0	1	Δe

$$A_{101} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \leftarrow S[0] = (0, 0, 0)$$

Example: $\mathrm{adp}^{\oplus}(\Delta c, \Delta d \rightarrow \Delta e)$

MSB			LSB	
0	0	0	1	Δc
0	0	0	0	Δd
0	0	0	1	Δe

$$A_{000} A_{101} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \leftarrow S[0] = (0, 0, 0)$$

Example: $\mathrm{adp}^{\oplus}(\Delta c, \Delta d \rightarrow \Delta e)$

MSB			LSB	
0	0	0	1	Δc
0	0	0	0	Δd
0	0	0	1	Δe

$$A_{000} A_{000} A_{101} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \leftarrow S[0] = (0, 0, 0)$$

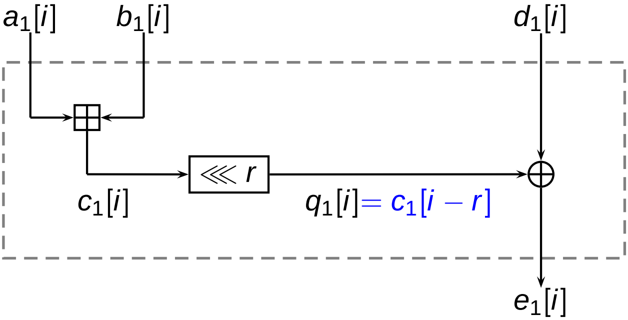
Example: $\mathrm{adp}^{\oplus}(\Delta c, \Delta d \to \Delta e)$

MSB			LSB	
0	0	0	1	Δc
0	0	0	0	Δd
0	0	0	1	Δe

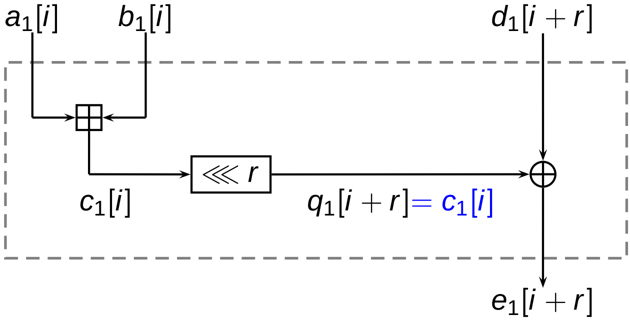
$$2^{-1.54} = \left(\frac{1}{4}\right)^4 \begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\end{bmatrix}^T A_{000} A_{000} A_{000} A_{101} \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix} \leftarrow S[0] = (0,0,0)$$

Outline

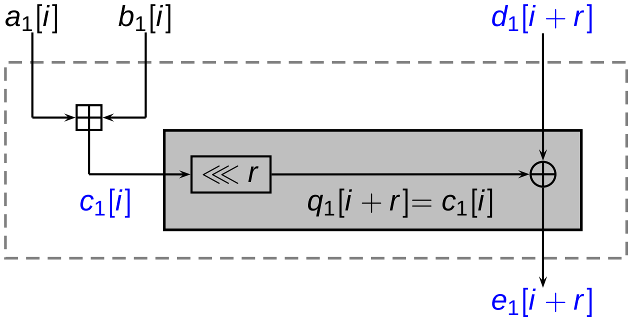
ARX : Circumventing the Intermediate Values



ARX : Circumventing the Intermediate Values

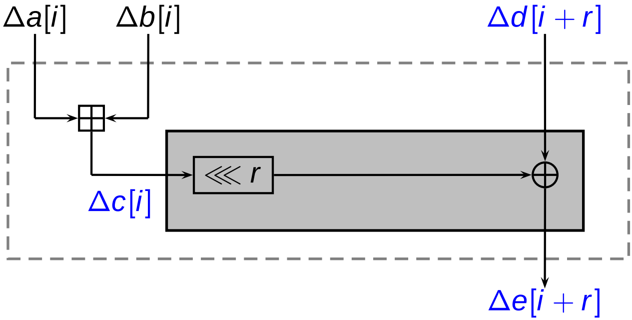


ARX : Circumventing the Intermediate Values



S-function for adp$^{\mathrm{ARX}}$

$$(\Delta e[i+r], S[i+1]) = f(c_1[i], d_1[i+r], \Delta c[i], \Delta d[i+r], S[i]),$$
$$0 \leq i < n$$



Example: $\mathrm{adp}^{\mathrm{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e)$

MSB			LSB	
1	0	0	0	Δc
0	0	0	0	Δd
0	0	0	1	Δe

Example: $\mathrm{adp}^{\mathrm{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e)$

MSB			LSB	
1	0	0	0	Δc
0	0	0	0	Δd
0	0	0	1	Δe

$S[0] = (0, 0, -1)$ $S[0] = (0, 1, -1)$ $S[0] = (0, 0, 0)$ $S[0] = (0, 1, 0)$

$$A_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Example: $\mathrm{adp}^{\mathrm{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e)$

	MSB			LSB	
	1	0	0	0	Δc
	0	0	0	0	Δd
	0	0	0	1	Δe

$S[0] = (0, 0, -1)$ $S[0] = (0, 1, -1)$ $S[0] = (0, 0, 0)$ $S[0] = (0, 1, 0)$

$$A_0 A_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Example: $\text{adp}^{\text{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e)$

	MSB			LSB	
	1	0	0	0	Δc
	0	0	0	0	Δd
	0	0	0	1	Δe

$S[0] = (0, 0, -1)$ $S[0] = (0, 1, -1)$ $S[0] = (0, 0, 0)$ $S[0] = (0, 1, 0)$

$$A_0 A_0 A_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_0 A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Example: $\mathrm{adp}^{\mathrm{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e)$

MSB			LSB	
1	0	0	0	Δc
0	0	0	0	Δd
0	0	0	1	Δe

$S[0] = (0, 0, -1)$ $S[0] = (0, 1, -1)$ $S[0] = (0, 0, 0)$ $S[0] = (0, 1, 0)$

$$\mathbf{R}A_0A_0A_0\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix} \quad \mathbf{R}A_0A_0A_0\begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix} \quad \mathbf{R}A_0A_0A_0\begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix} \quad \mathbf{R}A_0A_0A_0\begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix}$$

Example: $\text{adp}^{\text{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e)$

	MSB			LSB
Δc	1	0	0	0
Δd	0	0	0	0
Δe	0	0	0	1

$S[0] = (0, 0, -1)$ $S[0] = (0, 1, -1)$ $S[0] = (0, 0, 0)$ $S[0] = (0, 1, 0)$

$$A_5 \mathbf{R} A_0 A_0 A_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_5 \mathbf{R} A_0 A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_5 \mathbf{R} A_0 A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad A_5 \mathbf{R} A_0 A_0 A_0 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Example: $\mathrm{adp}^{\mathrm{ARX}}(\Delta c, \Delta d \xrightarrow{r} \Delta e)$

MSB			LSB	
1	0	0	0	Δc
0	0	0	0	Δd
0	0	0	1	Δe

$S[0] = (0,0,-1)$ $S[0] = (0,1,-1)$ $S[0] = (0,0,0)$ $S[0] = (0,1,0)$

$$2^{-1} = \begin{bmatrix}1\\1\\0\\0\\0\\0\\0\\0\end{bmatrix}^T A_5\mathbf{R}A_0A_0A_0\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\1\\1\\0\\0\\0\\0\end{bmatrix}^T A_5\mathbf{R}A_0A_0A_0\begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\0\\1\\1\\0\\0\end{bmatrix}^T A_5\mathbf{R}A_0A_0A_0\begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\1\end{bmatrix}^T A_5\mathbf{R}A_0A_0A_0\begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix}$$

Outline

- Introduction
- ARX
- S-functions
- adp^{ARX}
- Experiments

Experiments on 32-bit Additive Differences

#	Δc	Δd	Δe	r	$P_{\texttt{exper}}$	$P_{\texttt{ARX}}$	$P_{\texttt{rotxor}}$
1	0x80000100	0x00000000	0x0007fc00	11	−2.58	−2.58	−4.17
2	0x40000008	0x00000000	0x000001d0	6	−4.58	−4.58	−5.59
3	0x80000008	0x04000000	0xfc000f00	9	−4.16	−4.16	−5.70
4	0x40010001	0x04000000	0xd3ffc000	30	−5.90	−5.91	−6.60
5	0xa2005800	0x00400000	0xf4000b00	29	−7.53	−7.54	−8.57
6	0x45003700	0x00000000	0xc8ffbb00	16	−8.77	−8.76	−9.37
7	0x4007800d	0x03800300	0x01e803f0	21	−11.1	−11.1	−11.8
8	0xbf006400	0x00900050	0xf37ff9f0	28	−11.8	−11.8	−12.8

$P_{\texttt{exper}}$ was computed over 2^{22} random inputs

COSIC

Conclusions

- Proposed an algorithm for the **exact computation** of $\mathrm{adp}^{\mathrm{ARX}}$
- Allows for **more accurate computation** of the **probabilities of characteristics**
- Improving accuracy of characteristics may eventually lead to **attack**
- Can be easily modified to handle **other variations of ARX** e.g. AXR, RXA, XRA, etc.

Conclusions

- Proposed an algorithm for the **exact computation** of $\mathrm{adp}^{\mathsf{ARX}}$
- Allows for **more accurate computation** of the **probabilities of characteristics**
- Improving accuracy of characteristics may eventually lead to **attack**
- Can be easily modified to handle **other variations of ARX** e.g. AXR, RXA, XRA, etc.

Thank you for your attention!
Questions?