Analysis of Differential Attacks in ARX Constructions

Gaëtan Leurent

UCL Crypto Group & University of Luxembourg

Asiacrypt 2012

ARX Constructions

Two main categories of designs in symmetric cryptography:

ARX designs

- Additions, Rotations, Xors
- Inspired by MD/SHA
- Lots of light rounds

SBox designs

- S-Boxes and Linear Layers
- Inspired by the AES
- Few heavy rounds

The SHA-3 competition

- 51 submissions in 2008; Winner: Keccak in October 2012
- 2 of the 5 finalists are ARX designs

Differential attacks against ARX

- Most of the cryptanalysis of ARX designs is bit-twiddling
  - As opposed to SBox based designs
- Building/Verifying differential trails for ARX designs is hard
  - Many trails built by hand
  - Problems with MD5 and SHA-1 attacks [Manuel, DCC 2011]
  - Problems with differential trails
    - SHACAL [Wang, Keller & Dunkelman, SAC 2007]
  - Problems reported with boomerang attacks (incompatible trails):
    - HAVAL [Sasaki, SAC 2011]
    - SHA-256 [BLMN, Asiacrypt 2011]
- Some tools are described in literature, but most are not available

Outline

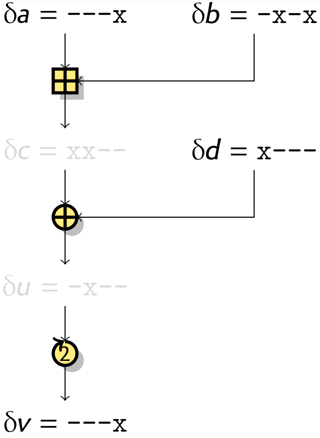
Introduction

Differential characteristics

Multi-bit constraints

Application

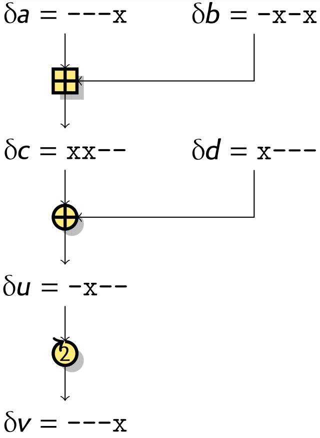
Differential Characteristic



$c = a + b$
$u = c + d$
$v = u \lll 2$

- Choose a difference operation: ⊕
- A differential only specifies the input and output difference
- A differential characteristic specifies the difference of each internal variable
- Compute probability for each operation

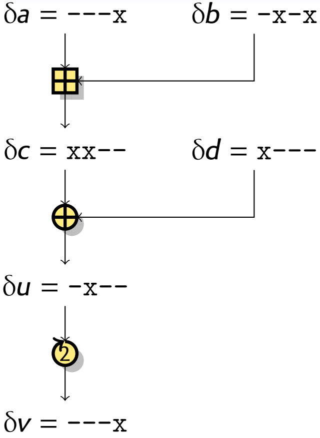
Differential Characteristic



$$c = a + b$$
$$u = c + d$$
$$v = u \lll 2$$

- Choose a difference operation: ⊕
- A differential only specifies the input and output difference
- A differential characteristic specifies the difference of each internal variable
- Compute probability for each operation

Differential Characteristic



$$c = a + b$$
$$u = c + d$$
$$v = u \lll 2$$

- Choose a difference operation: $\oplus$
- A differential only specifies the input and output difference
- A differential characteristic specifies the difference of each internal variable
- Compute probability for each operation

Signed difference

- A trail defines a set of good pairs:
  - $x^{[i]} \oplus x'^{[i]} = 0 \quad \Leftrightarrow \quad \left(x^{[i]}, x'^{[i]}\right) \in \left\{(0,0),(1,1)\right\}$
  - $x^{[i]} \oplus x'^{[i]} = 1 \quad \Leftrightarrow \quad \left(x^{[i]}, x'^{[i]}\right) \in \left\{(0,1),(1,0)\right\}$
- Wang introduced a signed difference:
  - $\delta\left(x^{[i]}, x'^{[i]}\right) = 0 \quad \Leftrightarrow \quad (x^{[i]}, x'^{[i]}) \in \left\{(0,0),(1,1)\right\}$
  - $\delta\left(x^{[i]}, x'^{[i]}\right) = +1 \quad \Leftrightarrow \quad (x^{[i]}, x'^{[i]}) \in \left\{(0,1)\right\}$
  - $\delta\left(x^{[i]}, x'^{[i]}\right) = -1 \quad \Leftrightarrow \quad (x^{[i]}, x'^{[i]}) \in \left\{(1,0)\right\}$
  - Captures both xor difference and modular difference
- Generalized constraints [De Cannière & Rechberger 06]

Generalized constraints [De Cannière & Rechberger 06]

	(x,x'):	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
?	*anything*	✓	✓	✓	✓
-	$x = x'$	✓	-	-	✓
x	$x \neq x'$	-	✓	✓	-
0	$x = x' = 0$	✓	-	-	-
u	$(x,x') = (0,1)$	-	✓	-	-
n	$(x,x') = (1,0)$	-	-	✓	-
1	$x = x' = 0$	-	-	-	✓
#	*incompatible*	-	-	-	-
3	$x = 0$	✓	✓	-	-
5	$x' = 0$	✓	-	✓	-
7		✓	✓	✓	-
A	$x' = 1$	-	✓	-	✓
B		✓	✓	-	✓
C	$x = 1$	-	-	✓	✓
D		✓	-	✓	✓
E		-	✓	✓	✓

Outline

Introduction

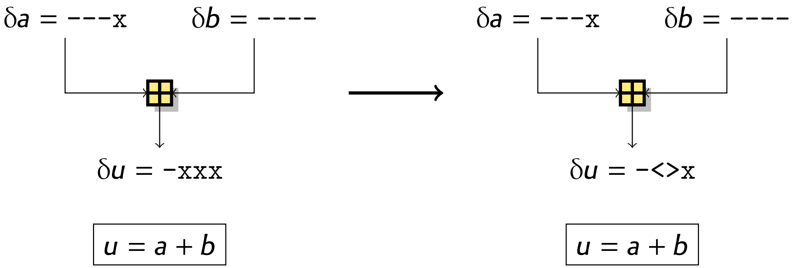
Differential characteristics

Multi-bit constraints

Application

Multi-bit Constraints

- We study carry propagation



- Two possibilities:
  - $\delta a = \texttt{---u}$ and $\delta u = \texttt{-unn}$
  - $\delta a = \texttt{---n}$ and $\delta u = \texttt{-nuu}$
- Active bits signs are linked
- We introduce new constraints
  - $> \equiv \{\texttt{nn}, \texttt{uu}\}$: $x'^{[i]} \neq x^{[i]} = x^{[i-1]}$
  - $< \equiv \{\texttt{nu}, \texttt{un}\}$: $x'^{[i]} \neq x^{[i]} \neq x^{[i-1]}$

Multi-bit Constraints

- Carry propagation leads to constraints of the form $x^{[i]} = x^{[i-1]}$
- We use multi-bit constraints to capture this information
  - We consider subsets of $\left\{(x^{[i]}, x'^{[i]}, x^{[i-1]})\right\}$ (1.5-bit), instead of $\left\{(x^{[i]}, x'^{[i]})\right\}$ (1-bit)
- Captures more accurately the behavior of modular addition
  - Only source of non-linearity in pure ARX designs (Boolean functions in MD/SHA)

Generalization

- 1.5-bit constraints: subsets of $\left\{(x^{[i]}, x'^{[i]}, x^{[i-1]}\right\}$
  - Relations between carry extensions
- 2-bit constraints: subsets of $\left\{(x^{[i]}, x'^{[i]}, x^{[i-1]}, x'^{[i-1]})\right\}$
  - Describe exactly the set $\{x, x' | x' = x \boxplus \Delta\}$ for any Δ
- 2.5-bit constraints: subsets of $\left\{(x^{[i]}, x'^{[i]}, x^{[i-1]}, x'^{[i-1]}, x^{[i-2]}\right\}$
  - Relations between potential carry extensions

See examples

Limitations

- We have to use reduced sets of constraints (full set of 2.5-bit constraints: 2^{32})
- Propagation for 2.5-bit constraints is slow

Comparison

- Experiments with a few rounds of a reduced Skein (4-bit words and 6-bit words)
- We look at the number of accepted input/output differences

	2 rounds (total: 2^{32})		3 rounds (sparse)	
Method	Accepted	Fp.	Accepted	Fp.
Exhaustive search	$2^{25.1}$ (35960536)	0	$2^{18.7}$ (427667)	
2.5-bit constraints	$2^{25.3}$ (40820032)	0.14	$2^{19.5}$ (746742)	0.7
1.5-bit constraints	$2^{25.3}$ (40820032)	0.14	$2^{20.4}$ (1372774)	2.2
1-bit constraints	$2^{25.4}$ (43564288)	0.21	$2^{20.7}$ (1762857)	3.1
Check adds indep.	$2^{25.8}$ (56484732)	0.57		

Outline

Verifying trails

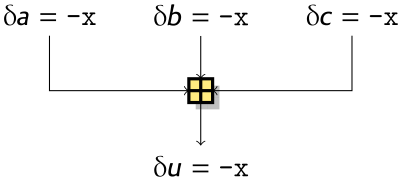
Problem

Most analysis assume that operations are independent
and multiply the probabilities.
But sometimes, operations are not independent...
Known problem in Boomerang attacks. [Murphy, TIT 2011]

- We compute necessary conditions.
- This allows to detect cases of incompatibility
- We have detected problems in several published works
  - Incompatible trails seem to appear quite naturally

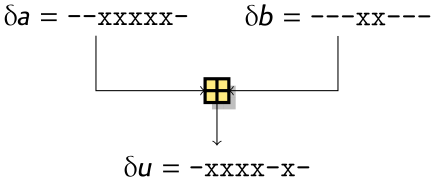
Incompatibility with additions

Some “natural” differentials do not work with additions:



$$u = a + b + c$$

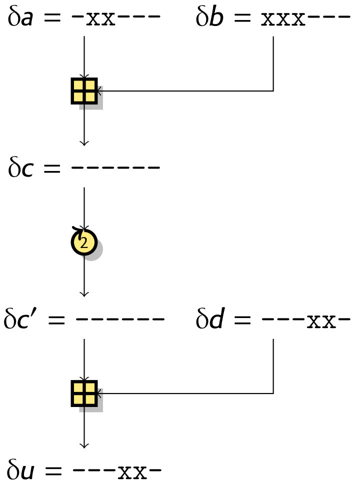
- Linearized trail



$$u = a + b$$

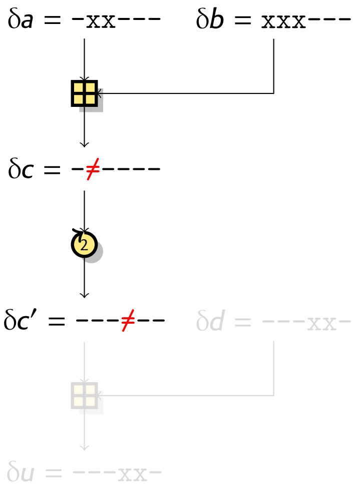
- Seems valid with signed difference
- Found in Skein near-collision [eprint 2011/148]

Carry incompatibility



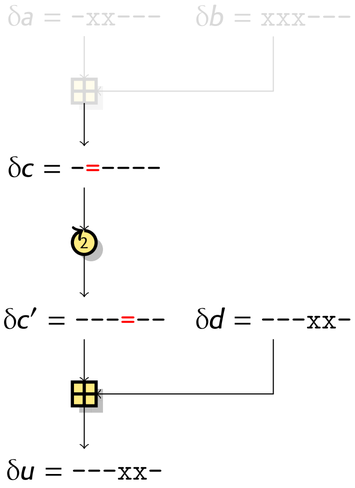
- Each operation has a non-zero probability
- Trail seems valid with signed difference
- Consider the 1st addition
  - Constraint: $c^{[4]} \neq c^{[5]}$
- Consider the 2nd addition
  - Constraint: $c'^{[2]} = c'^{[3]}$
- Incompatible!
  - Detected with the multi-bit constraints

Carry incompatibility



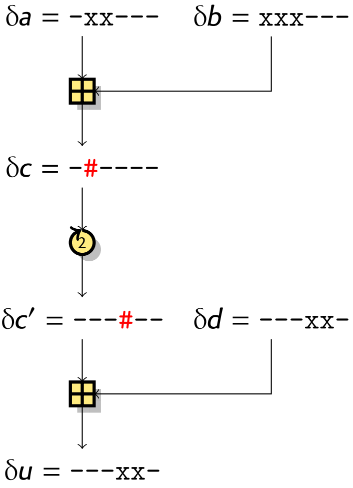
- Each operation has a non-zero probability
- Trail seems valid with signed difference
- Consider the 1st addition
  - Constraint: $c^{[4]} \neq c^{[5]}$
- Consider the 2nd addition
  - Constraint: $c'^{[2]} = c'^{[3]}$
- Incompatible!
  - Detected with the multi-bit constraints

Carry incompatibility



- Each operation has a non-zero probability
- Trail seems valid with signed difference
- Consider the 1st addition
  - Constraint: $c^{[4]} \neq c^{[5]}$
- Consider the 2nd addition
  - Constraint: $c'^{[2]} = c'^{[3]}$
- Incompatible!
  - Detected with the multi-bit constraints

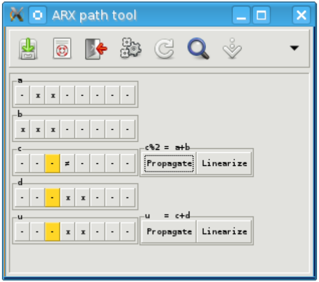
Carry incompatibility



- Each operation has a non-zero probability
- Trail seems valid with signed difference
- Consider the 1st addition
  - Constraint: $c^{[4]} \neq c^{[5]}$
- Consider the 2nd addition
  - Constraint: $c'^{[2]} = c'^{[3]}$
- Incompatible!
  - Detected with the multi-bit constraints

Graphical tool

- To study more complex cases, we have a graphical tool
- We can manually constrain some bits and propagate.



Verifying characteristics

Several published attacks are invalid.

- Boomerang attacks on Blake [Biryukov & *al.*, FSE 2011]
  - Basic linearized trails, with MSB difference
  - Proposed attack on 7/8 round for KP and 6/6.5 for CF do not work
  - 7-round KP attack can be made with the 6-round trail
  - 8-round KP attack and 6/6.5-round CF attack can be fixed using another active bit (non-MSB)
- Boomerang attacks on Skein-512 [Chen & Jia, ISPEC 2010]
  - Basic linearized trails, with MSB difference
  - Proposed attacks do not work on Skein-512
  - Similar trails work on Skein-256 [Leurent & Roy, CT-RSA 2012]
  - Can be fixed using another active bit [Yu, Chen & Wang, SAC 2012]
- Near-collision attack on Skein [eprint 2011/148]
  - Complex rebound-like handcrafted characteristic
  - Path is not satisfiable

Our results

1. New constraints
   - Multi-bit constraints
     - Better targeted to pure ARX designs
   - Boomerang constraints

2. Tools for analysis of differential characteristics
   - Publicly available
   - Code and documentation available at:
     `http://www.di.ens.fr/~leurent/arxtools.html`
     `http://www.cryptolux.org/ARXtools`

3. Problems found in several proposed attacks
   - Incompatible trails seem to appear quite naturally

Thanks

With the support of:

- FNR Luxembourg
- ERC project CRASH

Outline

Extra slides

Multi-bit Constraints as S-systems

We use the theory of S-functions to study multi-bit constraints

[Mouha & *al.*, SAC 2010]

- We can write a bitwise function f so that:

$$(x,x') \text{ is a right pair} \Leftrightarrow f(x,x',x \boxplus x) = 1$$

- We can count the number of solutions efficiently
  - Testing for zero or non-zero very efficient

- We use the same tools to propagate constraints:
  1. Split each subset in two smaller subsets
  2. If one subset gives zero solutions,
     the characteristic can be restricted to the other subset.

? → -/x   - → 0/1, =/!   x → u/n, </>   ...

1.5-bit Constraints Table

	$(x \oplus x', x \oplus 2x, x)$:	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
?	*anything*	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
-	$x = x'$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	-	-	-	-
x	$x \neq x'$	-	-	-	-	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
0	$x = x' = 0$	$\checkmark$	-	$\checkmark$	-	-	-	-	-
u	$(x,x') = (0,1)$	-	-	-	-	$\checkmark$	-	$\checkmark$	-
n	$(x,x') = (1,0)$	-	-	-	-	-	$\checkmark$	-	$\checkmark$
1	$x = x' = 0$	-	$\checkmark$	-	$\checkmark$	-	-	-	-
#	*incompatible*	-	-	-	-	-	-	-	-
3	$x = 0$	$\checkmark$	-	$\checkmark$	-	$\checkmark$	-	$\checkmark$	-
C	$x = 1$	-	$\checkmark$	-	$\checkmark$	-	$\checkmark$	-	$\checkmark$
5	$x' = 0$	$\checkmark$	-	$\checkmark$	-	-	$\checkmark$	-	$\checkmark$
A	$x' = 1$	-	$\checkmark$	-	$\checkmark$	$\checkmark$	-	$\checkmark$	-
=	$\equiv \{00, 11\}$	$\checkmark$	$\checkmark$	-	-	-	-	-	-
!	$\equiv \{01, 10\}$	-	-	$\checkmark$	$\checkmark$	-	-	-	-
>	$\equiv \{nn, uu\}$	-	-	-	-	$\checkmark$	$\checkmark$	-	-
<	$\equiv \{nu, un\}$	-	-	-	-	-	-	$\checkmark$	$\checkmark$

Comparison

Simple situations with a modular difference of ± 1:

Diff, carry	1-bit cstr.	1.5-bit cstr.	2-bit cstr.	2.5-bit cstr.
$+1$, k-bit (2^{n-k})	-unnn (2^{n-k})	-unnn (2^{n-k})	-unnn (2^{n-k})	-unnn (2^{n-k})
± 1, k-bit (2^{n-k+1})	-xxxx (2^{n})	-><<x (2^{n-k+1})	-><<x (2^{n-k+1})	-><<x (2^{n-k+1})
$+1$, any (2^{n})	????x (2^{2n-1})	????x (2^{2n-1})	UUUUx (2^{n})	UUUUx (2^{n})
± 1, any (2^{n+1})	????x (2^{2n-1})	????x (2^{2n-1})	XXXXx ($2^{n} \times n$)	///Xx (2^{n+1})

Back to the talk