杭州電子科技大学
HANGZHOU DIANZI UNIVERSITY

Finding Impossible Differentials in ARX Ciphers under Weak Keys

Tingting Cui
cuitingting@hdu.edu.cn

Joint work with Qing Ling, Hongtao Hu, Sijia Gong, Zijun He, Jiali Huang, Jia Xiao

FSE 2024 @ Leuven, Belgium

Background

Impossible differential (ID) attack is one of the most powerful cryptanalysis method in the field of symmetric ciphers. The methods to find IDs can be summarized in two phases:

- Phase 1: search IDs by treating the S-boxes as ideal ones, such as $\mathcal{U}$-method [KHL10], $\mathcal{UID}$-method [LLW14]
- Phase 2: search IDs by using DDT with automatic tools, such as based on MILP [ST17, CCJ+16], SAT/SMT [AK18, KLT15, MP13, RKJ+20] and CP [SGL+17]

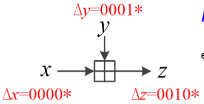
All methods above to find ID are based on two underlying assumptions:

- Markov cipher assumption
- key independence assumption

Motivation — Is Markov cipher assumption true?

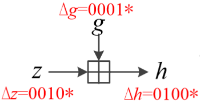
The trend to design ciphers towards lightweight: lighter round function and lighter key schedule. Take an example in ARX cipher as follows:

- Under Markov cipher assumption:



$Pr(\Delta x, \Delta y \rightarrow \Delta z) = p_1 > 0$

e.g. ($\Delta x = 00001$, $\Delta y = 00011$, $\Delta z = 00100$, $x = 00000$ and $y = 00000$)

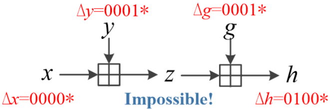


$Pr(\Delta z, \Delta e \rightarrow \Delta h) = p_2 > 0$

e.g. ($\Delta z = 00100$, $\Delta e = 00011$, $\Delta h = 01001$, $z = 00001$ and $e = 00000$)

$$Pr(\Delta x = 0000*, \Delta y = 0001*, \Delta g = 0001* \rightarrow \Delta h = 0100*) = p_1 p_2 > 0.$$

- Without Markov cipher assumption:



$$Pr(\Delta x = 0000*, \Delta y = 0001*, \Delta g = 0001* \rightarrow \Delta h = 0100*) = 0.$$

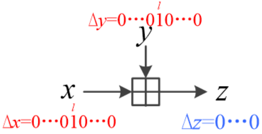
Properties on Single Addition Modulo 2^n

Property 1. [Li+19]

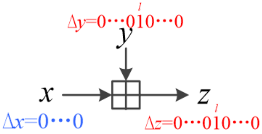
Let $x = z \boxplus y$ and $x' = z' \boxplus y'$, where $x, y, z, x', y', z' \in \mathbb{F}_2^n$. Suppose $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$ and $\Delta z = z \oplus z'$. If $\Delta x = \Delta y = 0 \cdots 0\overset{l}{1}0 \cdots 0$, then $\Delta z = 0 \cdots 0$ if and only if $x[l] \neq y[l]$ or $x'[l] \neq y'[l]$.

Property 2.

Let $x = z \boxminus y$ and $x' = z' \boxminus y'$, where $x, y, z, x', y', z' \in \mathbb{F}_2^n$. Suppose $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$ and $\Delta z = z \oplus z'$. If $\Delta z = \Delta y = \overset{n-1}{0} \cdots 0\overset{l}{1}0 \cdots \overset{0}{0}$, $0 \leq l < n-1$, then $\Delta x = 0 \cdots 0$ if and only if $z[l] = y[l]$ or $z'[l] = y'[l]$.



iff. $x[l] \neq y[l]$ or $x'[l] \neq y'[l]$



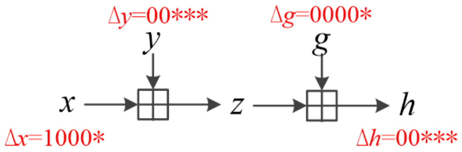
iff. $z[l] = y[l]$ or $z'[l] = y'[l]$

Properties on Two Consecutive Modular Additions

Property 3.

Let $z = x \boxplus y$, $z' = x' \boxplus y'$, $h = z \boxplus g$ and $h' = z' \boxplus g'$, where $x, y, z, g, h, x', y', z', g', h' \in \mathbb{F}_2^5$. Suppose $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$, $\Delta z = z \oplus z'$, $\Delta g = g \oplus g'$ and $\Delta h = h \oplus h'$. If $\Delta z[2:1] \neq 00$, then we have

$$(\Delta x = 1000*, \Delta y = 00***, \Delta g = 0000* \nrightarrow \Delta h = 00***).$$



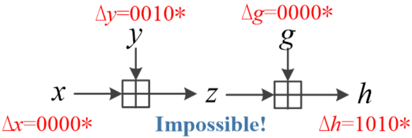
- When $\Delta z[2:1] \neq 00$, the differential will be impossible.
- In practical ciphers, $\Delta z[2:1] \neq 00$ is possible to happen.

Properties on Two Consecutive Modular Additions

Property 4.

Let $z = x \boxplus y$, $z' = x' \boxplus y'$, $h = z \boxplus g$ and $h' = z' \boxplus g'$, where $x, y, z, g, h, x', y', z', g', h' \in \mathbb{F}_2^5$. Suppose that $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$, $\Delta z = z \oplus z'$, $\Delta g = g \oplus g'$ and $\Delta h = h \oplus h'$. Then

$$(\Delta x = 0000*, \Delta y = 0010*, \Delta g = 0000* \nrightarrow \Delta h = 1010*).$$



- The carries brought by lower bits do not make the ID transitions viable.
- The ID can be extended to

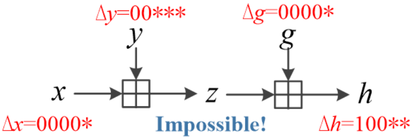
$$(\Delta x = * \cdots * \underbrace{\boxed{0000*}}^{i+4,\cdots,i} * \cdots *, \Delta y = * \cdots * \underbrace{\boxed{0010*}}^{i+4,\cdots,i} * \cdots *, \Delta g = * \cdots * \underbrace{\boxed{0000*}}^{i+4,\cdots,i} \nrightarrow \Delta h = * \cdots * \underbrace{\boxed{1010*}}^{i+4,\cdots,i} * \cdots *).$$

Properties on Two Consecutive Modular Additions

Property 5.

Let $z = x \boxplus y$, $z' = x' \boxplus y'$, $h = z \boxplus g$ and $h' = z' \boxplus g'$, where $x, y, z, g, h, x', y', z', g', h' \in \mathbb{F}_2^5$. Suppose that $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$, $\Delta z = z \oplus z'$, $\Delta g = g \oplus g'$ and $\Delta h = h \oplus h'$. Then

$$(\Delta x = 0000*,\ \Delta y = 00***, \Delta g = 0000* \nrightarrow \Delta h = 100**)$$

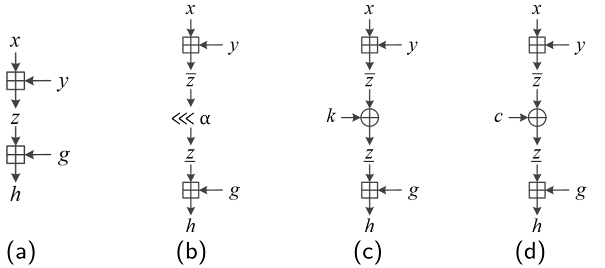


- The carries brought by lower bits do not make the ID transitions viable.
- The ID can be extended to

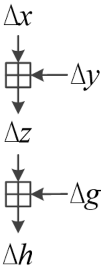
$$(\Delta x = *\cdots*\underbrace{0000*}^{i+4,\cdots,i}*\cdots*,\ \Delta y = *\cdots*\underbrace{00***}^{i+4,\cdots,i}*\cdots*,\ \Delta g = *\cdots*\underbrace{0000*}^{i+4,\cdots,i} \nrightarrow \Delta h = *\cdots*\underbrace{100**}^{i+4,\cdots,i}*\cdots*).$$

Summary on Properties 3 ∼ 5

- The ID patterns in Properties 3∼5 can be extended by adding uncertain bits on higher and lower bit positions.
- Properties 3∼5 represent just a thin selection of thousand ID patterns found experimentally.
- These Properties can be used to find IDs on four local constructions extracted from ARX ciphers.



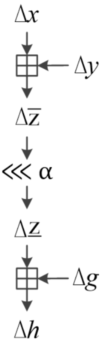
IDs on Local Construction (a)



(a)

Constraints	$\Delta z[i+2:i+1] \neq 00$		
Differentials	$\Delta x = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{1000\ast}}\ \ast\cdots\ast)$ $\Delta y = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{00\ast\ast\ast}}\ \ast\cdots\ast)$ $\Delta z = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{\ast\ast\ast\ast\ast}}\ \ast\cdots\ast)$ $\Delta g = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{0000\ast}}\ \ast\cdots\ast)$ $\Delta h = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{00\ast\ast\ast}}\ \ast\cdots\ast)$	$\Delta x = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{0000\ast}}\ \ast\cdots\ast)$ $\Delta y = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{0010\ast}}\ \ast\cdots\ast)$ $\Delta z = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{\ast\ast\ast\ast\ast}}\ \ast\cdots\ast)$ $\Delta g = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{0000\ast}}\ \ast\cdots\ast)$ $\Delta h = (\ast\cdots\ast\ \overset{i+4,\cdots,i}{\boxed{1010\ast}}\ \ast\cdots\ast)$	$\Delta x = (\ast\cdots\ast\ \overset{i+3,\cdots,i}{\boxed{0000}}\ \ast\cdots\ast)$ $\Delta y = (\ast\cdots\ast\ \overset{i+3,\cdots,i}{\boxed{00\ast\ast}}\ \ast\cdots\ast)$ $\Delta z = (\ast\cdots\ast\ \overset{i+3,\cdots,i}{\boxed{\ast\ast\ast\ast}}\ \ast\cdots\ast)$ $\Delta g = (\ast\cdots\ast\ \overset{i+3,\cdots,i}{\boxed{0000}}\ \ast\cdots\ast)$ $\Delta h = (\ast\cdots\ast\ \overset{i+3,\cdots,i}{\boxed{100\ast}}\ \ast\cdots\ast)$
Result	$(\Delta x,\ \Delta y,\ \Delta g \nrightarrow \Delta h)$ according to Property 3	$(\Delta x,\ \Delta y,\ \Delta g \nrightarrow \Delta h)$ according to Property 4	$(\Delta x,\ \Delta y,\ \Delta g \nrightarrow \Delta h)$ according to Property 5

IDs on Local Construction (b)

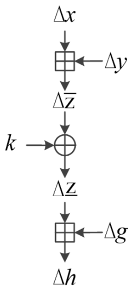


(b)

Constraints	$\Delta\bar{z}[i+2:i+1] \neq 00$		
Differentials	$\Delta x = (*\cdots* \overset{i+4,\cdots,i}{\boxed{1000*}} *\cdots*)$	$\Delta x = (*\cdots* \overset{i+4,\cdots,i}{\boxed{0000*}} *\cdots*)$	$\Delta x = (*\cdots* \overset{i+3,\cdots,i}{\boxed{0000}} *\cdots*)$
	$\Delta y = (*\cdots* \overset{i+4,\cdots,i}{\boxed{00***}} *\cdots*)$	$\Delta y = (*\cdots* \overset{i+4,\cdots,i}{\boxed{0010*}} *\cdots*)$	$\Delta y = (*\cdots* \overset{i+3,\cdots,i}{\boxed{00**}} *\cdots*)$
	$\Delta\bar{z} = (*\cdots* \overset{i+4,\cdots,i}{\boxed{*****}} *\cdots*)$	$\Delta\bar{z} = (*\cdots* \overset{i+4,\cdots,i}{\boxed{*****}} *\cdots*)$	$\Delta\bar{z} = (*\cdots* \overset{i+3,\cdots,i}{\boxed{****}} *\cdots*)$
	$\Delta\underline{z} = (*\cdots* \overset{j+4,\cdots,j}{\boxed{*****}} *\cdots*)$	$\Delta\underline{z} = (*\cdots* \overset{j+4,\cdots,j}{\boxed{*****}} *\cdots*)$	$\Delta\underline{z} = (*\cdots* \overset{j+3,\cdots,j}{\boxed{****}} *\cdots*)$
	$\Delta g = (*\cdots* \overset{j+4,\cdots,j}{\boxed{0000*}} *\cdots*)$	$\Delta g = (*\cdots* \overset{j+4,\cdots,j}{\boxed{0000*}} *\cdots*)$	$\Delta g = (*\cdots* \overset{j+3,\cdots,j}{\boxed{0000}} *\cdots*)$
	$\Delta h = (*\cdots* \overset{j+4,\cdots,j}{\boxed{00***}} *\cdots*)$	$\Delta h = (*\cdots* \overset{j+4,\cdots,j}{\boxed{1010*}} *\cdots*)$	$\Delta h = (*\cdots* \overset{j+3,\cdots,j}{\boxed{100*}} *\cdots*)$
Result	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 3	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 4	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 5

- The i-th bit of $\bar{z}$ is cyclically shifted to the j-th bit of $\underline{z}$.

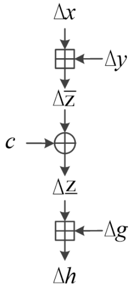
IDs on Local Construction (c)



(c)

Constraints	$k[i+3:i+1] = 000$ or 111; $\Delta\bar{z}[i+2:i+1] \neq 00$	$k[i+3:i+2] = 00$ or 11	$k[i+2:i+1] = 00$ or 11
Differentials	$\Delta x = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{1000*}}\ *\cdots*)$	$\Delta x = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{0000*}}\ *\cdots*)$	$\Delta x = (*\cdots*\ \overset{i+3,\cdots,i}{\boxed{0000}}\ *\cdots*)$
	$\Delta y = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{00***}}\ *\cdots*)$	$\Delta y = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{0010*}}\ *\cdots*)$	$\Delta y = (*\cdots*\ \overset{i+3,\cdots,i}{\boxed{00**}}\ *\cdots*)$
	$\Delta z = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{*****}}\ *\cdots*)$	$\Delta z = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{*****}}\ *\cdots*)$	$\Delta z = (*\cdots*\ \overset{i+3,\cdots,i}{\boxed{****}}\ *\cdots*)$
	$\Delta g = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{0000*}}\ *\cdots*)$	$\Delta g = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{0000*}}\ *\cdots*)$	$\Delta g = (*\cdots*\ \overset{i+3,\cdots,i}{\boxed{0000}}\ *\cdots*)$
	$\Delta h = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{00***}}\ *\cdots*)$	$\Delta h = (*\cdots*\ \overset{i+4,\cdots,i}{\boxed{1010*}}\ *\cdots*)$	$\Delta h = (*\cdots*\ \overset{i+3,\cdots,i}{\boxed{100*}}\ *\cdots*)$
Result	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 3	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 4	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 5

IDs on Local Construction (d)



(d)

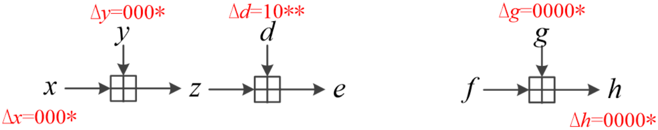
Constraints	$c[i+3:i+1] = 000$ or 111 $\Delta\overline{z}[i+2:i+1] \neq 00$	$c[i+3:i+2] = 00$ or 11	$c[i+2:i+1] = 00$ or 11
Differentials	$\Delta x = (*\cdots* \overset{i+4,\cdots,i}{\boxed{1000*}} *\cdots*)$	$\Delta x = (*\cdots* \overset{i+4,\cdots,i}{\boxed{0000*}} *\cdots*)$	$\Delta x = (*\cdots* \overset{i+3,\cdots,i}{\boxed{0000}} *\cdots*)$
	$\Delta y = (*\cdots* \overset{i+4,\cdots,i}{\boxed{00***}} *\cdots*)$	$\Delta y = (*\cdots* \overset{i+4,\cdots,i}{\boxed{0010*}} *\cdots*)$	$\Delta y = (*\cdots* \overset{i+3,\cdots,i}{\boxed{00**}} *\cdots*)$
	$\Delta z = (*\cdots* \overset{i+4,\cdots,i}{\boxed{*****}} *\cdots*)$	$\Delta z = (*\cdots* \overset{i+4,\cdots,i}{\boxed{*****}} *\cdots*)$	$\Delta z = (*\cdots* \overset{i+3,\cdots,i}{\boxed{****}} *\cdots*)$
	$\Delta g = (*\cdots* \overset{i+4,\cdots,i}{\boxed{0000*}} *\cdots*)$	$\Delta g = (*\cdots* \overset{i+4,\cdots,i}{\boxed{0000*}} *\cdots*)$	$\Delta g = (*\cdots* \overset{i+3,\cdots,i}{\boxed{0000}} *\cdots*)$
	$\Delta h = (*\cdots* \overset{i+4,\cdots,i}{\boxed{00***}} *\cdots*)$	$\Delta h = (*\cdots* \overset{i+4,\cdots,i}{\boxed{1010*}} *\cdots*)$	$\Delta h = (*\cdots* \overset{i+3,\cdots,i}{\boxed{100*}} *\cdots*)$
Result	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 3	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 4	$(\Delta x, \Delta y, \Delta g \nrightarrow \Delta h)$ according to Property 5

Properties on Three Consecutive Modular Additions

Property 6.

$x \boxplus y = z \pmod{2^4}$, $x' \boxplus y' = z' \pmod{2^4}$, $z \boxplus d = e \pmod{2^4}$, $z' \boxplus d' = e' \pmod{2^4}$, $f \boxplus g = h \pmod{2^5}$ and $f' \boxplus g' = h' \pmod{2^5}$. Suppose that $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$, $\Delta z = z \oplus z'$, $\Delta d = d \oplus d'$, $\Delta e = e \oplus e'$, $\Delta f = f \oplus f'$, $\Delta g = g \oplus g'$ and $\Delta h = h \oplus h'$. If $f[4:1] = e$, then

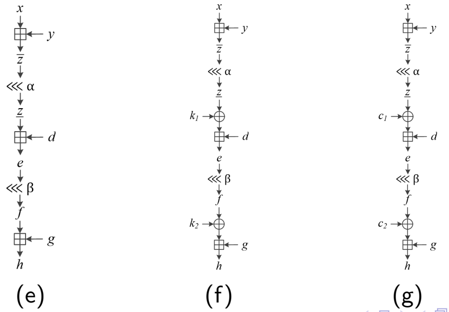
$$(\Delta x = 000*, \Delta y = 000*, \Delta d = 10**, \Delta g = 0000* \nrightarrow \Delta h = 0000*)$$



- When $f = e \| *$, the differential will be impossible.
- In practical ciphers, $f = e \| *$ is possible to happen.

Local Constructions of ARX ciphers

- The ID patterns in Property 6 can be extended by adding uncertain bits on higher and lower bit positions.
- The structures of consecutive three modular additions and its variants are extracted from ARX ciphers.
- These Property 6 can be used to find IDs on these local constructions below. Please refer to the table on the next page.



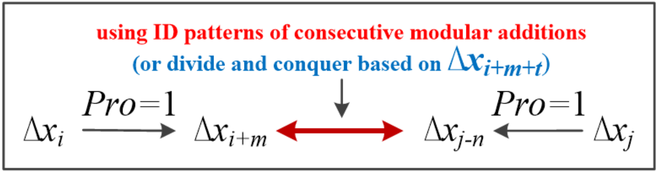
IDs on Local Constructions (e)∼ (g)

Constraints		$k_1[2:1] = 00$ or 11 $k_2[j+3:j+1] = 000$ or 111	$c_1[2:1] = 00$ or 11 $c_2[j+3:j+1] = 000$ or 111
Differentials	$\Delta x = (*\cdots* \overset{i+3,\cdots,i}{\boxed{000*}} *\cdots*)$	$\Delta x = (*\cdots* \overset{i+3,\cdots,i}{\boxed{000*}} *\cdots*)$	$\Delta x = (*\cdots* \overset{i+3,\cdots,i}{\boxed{000*}} *\cdots*)$
	$\Delta y = (*\cdots* \overset{i+3,\cdots,i}{\boxed{000*}} *\cdots*)$	$\Delta y = (*\cdots* \overset{i+3,\cdots,i}{\boxed{000*}} *\cdots*)$	$\Delta y = (*\cdots* \overset{i+3,\cdots,i}{\boxed{000*}} *\cdots*)$
	$\Delta \bar{z} = (*\cdots* \overset{i+3,\ \cdots,\ i}{\boxed{*\ ***}} *\cdots*)$	$\Delta \bar{z} = (*\cdots* \overset{i+3,\ \cdots,\ i}{\boxed{*\ ***}} *\cdots*)$	$\Delta \bar{z} = (*\cdots* \overset{i+3,\ \cdots,\ i}{\boxed{*\ ***}} *\cdots*)$
	$\Delta \underline{z} = (*\cdots* \overset{3,\ \cdots,\ 0}{\boxed{****}})$	$\Delta \underline{z} = (*\cdots* \overset{3,\ \cdots,\ 0}{\boxed{****}})$	$\Delta \underline{z} = (*\cdots* \overset{3,\ \cdots,\ 0}{\boxed{****}})$
	$\Delta d = (*\cdots* \overset{3,\ \cdots,\ 0}{1\boxed{0**}})$	$\Delta d = (*\cdots* \overset{3,\ \cdots,\ 0}{1\boxed{0**}})$	$\Delta d = (*\cdots* \overset{3,\ \cdots,\ 0}{1\boxed{0**}})$
	$\Delta e = (*\cdots* \overset{3,\ \cdots,\ 0}{\boxed{****}})$	$\Delta e = (*\cdots* \overset{3,\ \cdots,\ 0}{\boxed{****}})$	$\Delta e = (*\cdots* \overset{3,\ \cdots,\ 0}{\boxed{****}})$
	$\Delta f = (*\cdots* \overset{j+4,\ \cdots,\ j}{\boxed{*****}} *\cdots*)$	$\Delta f = (*\cdots* \overset{j+4,\ \cdots,\ j}{\boxed{*****}} *\cdots*)$	$\Delta f = (*\cdots* \overset{j+4,\ \cdots,\ j}{\boxed{*****}} *\cdots*)$
	$\Delta g = (*\cdots* \overset{j+4,\cdots,j}{\boxed{0000*}} *\cdots*)$	$\Delta g = (*\cdots* \overset{j+4,\cdots,j}{\boxed{0000*}} *\cdots*)$	$\Delta g = (*\cdots* \overset{j+4,\cdots,j}{\boxed{0000*}} *\cdots*)$
	$\Delta h = (*\cdots* \overset{j+4,\cdots,j}{\boxed{0000*}} *\cdots*)$	$\Delta h = (*\cdots* \overset{j+4,\cdots,j}{\boxed{0000*}} *\cdots*)$	$\Delta h = (*\cdots* \overset{j+4,\cdots,j}{\boxed{0000*}} *\cdots*)$
Result	(Δx, Δy, Δd, $\Delta g \nrightarrow \Delta h$) according to Property 6		

[1] The i-th bit of $\bar{z}$ is cyclically shifted to LSB of $\underline{z}$.

[2] The LSB of e is cyclically shifted to the j-th bit of f.

Framework for Finding IDs in ARXs under weak keys



Step 1. Obtain the differentials $\Delta x_i \rightarrow \Delta x_{i+m}$ and $\Delta x_{j-n} \leftarrow \Delta x_j$ by some tool according to properties of addition modulo 2^n.

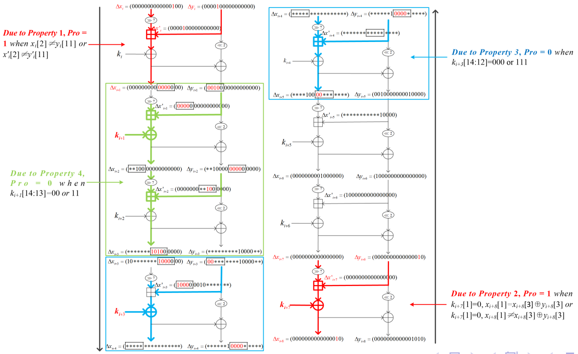
Step 2. Check the possibility of the differential $\Delta x_{i+m} \rightarrow \Delta x_{j-n}$ by using ID patterns of consecutive modular additions.
If $\Delta x_{i+m} \nrightarrow \Delta x_{j-n}$, return $\Delta x_i \nrightarrow \Delta x_j$.

Step 3. Use some tool to obtain possible forms of intermediate difference Δx_{i+m+t} and **divide and conquer** with them. Specially, return to Step 2 to check $\Delta x_{i+m} \rightarrow \Delta x_{i+m+t}$ and $\Delta x_{i+m+t} \rightarrow \Delta x_{j-n}$.
$(i+m < i+m+t < j-n)$

Apply to SPECK32/64

When $k_{i+1}[14:13] = 00$ (or 11), $k_{i+3}[14:12] = 000$ (or 111), $x_i[2] \neq y_i[11]$ or $(x'_i[2] \neq y'_i[11]$, there are two 8-round IDs for SPECK32/64 under 2^{60} weak keys:

- $(\Delta x_i = 0\cdots0100, \Delta y_i = 000010\cdots0) \nrightarrow (\Delta x_{i+8} = 0\cdots010, \Delta y_{i+8} = 0\cdots01010)$ under $k_{i+7}[1] = 0$ if $x_{i+8}[2] = x_{i+8}[4] \oplus y_{i+8}[4]$.
- $(\Delta x_i = 0\cdots0100, \Delta y_i = 000010\cdots0) \nrightarrow (\Delta x_{i+8} = 0\cdots010, \Delta y_{i+8} = 0\cdots01010)$ under $k_{i+7}[1] = 1$ if $x_{i+8}[2] \neq x_{i+8}[4] \oplus y_{i+8}[4]$.



Apply to LEA-k ($k = 128, 192, 256$)

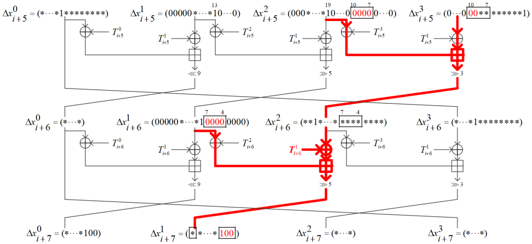
11-round ID for LEA-k under 2^{k-1} weak keys:

- Rounds $i \sim i+5$:

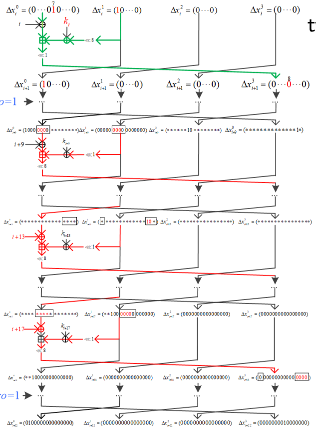
  $(10\cdots0, 10\cdots0, 10\cdots0, 10\cdots0) \rightarrow (*\cdots*\overset{9}{1}*\cdots*, 0\cdots\overset{27}{0}*\cdots*\overset{13}{1}0\cdots0, 000*\cdots*\overset{19}{1}0\cdots0, 0\cdots\overset{9}{0}*\cdots*)$

  with prob. 1
- Rounds $i+7 \sim i+11$:

  $(*\cdots*100, **\cdots*100, *\cdots*, *\cdots*) \rightarrow (0\cdots0, 0\cdots0, 00010\cdots0, 0\cdots0)$ with prob. 1
- Rounds $i+5 \sim i+6$: When $T^1_{i+6}[6:5] = 00$ or 11, the differential of **the red part is impossible according to the Property 5**.



Apply to CHAM64/128



two 22-round IDs for CHAM-64/128 under 2^{127} weak keys:

- $(\Delta x_i^0 = 0\cdots0\overset{7}{1}0\cdots0, \Delta x_i^1 = 10\cdots0, \Delta x_i^2 = 0\cdots0, \Delta x_i^3 = 0\cdots0)$
  $\nrightarrow (\Delta x_{i+22}^0 = 01\cdots0, \Delta x_{i+22}^1 = 0\cdots0, \Delta x_{i+22}^2 = 0\cdots0, \Delta x_{i+22}^3 = 0\cdots0\overset{7}{1}0)$
  under $k_i[7] = 0$ if $x_i^0[7] \neq x_i^1[15]$.
- $(\Delta x_i^0 = 0\cdots0\overset{7}{1}0\cdots0, \Delta x_i^1 = 10\cdots0, \Delta x_i^2 = 0\cdots0, \Delta x_i^3 = 0\cdots0)$
  $\nrightarrow (\Delta x_{i+22}^0 = 01\cdots0, \Delta x_{i+22}^1 = 0\cdots0, \Delta x_{i+22}^2 = 0\cdots0, \Delta x_{i+22}^3 = 0\cdots0\overset{7}{1}0)$
  under $k_i[7] = 1$ if $x_i^0[7] = x_i^1[15]$.
- **According to Property 1**, if $k_i[7] = 0$, $x_i^0[7] \neq x_i^1[15]$ or $k_i[7] = 1$, $x_i^0[7] = x_i^1[15]$, there is the differential $(\Delta x_i \rightarrow \Delta x_{i+1})$**with Probability 1**, refer to the green part.
- When $(i+13)[2:1] = 00$ or 11 and $(i+17)[10:8] = 000$ or 111, the differential $(\Delta x_{i+9} \rightarrow \Delta x_{i+18})$of **the red part is impossible according to the property 6**.

Compare with Previous Results

Cipher	Round	Weak key space	Starting round	Reference
SPECK-32/64	6	2^{64}	any	[Li+18]
	6	2^{64}	any	[XSQ17]
	7	2^{64}	any	[Li+19]
	8	$\mathbf{2^{60}}$	**any**	This work
LEA-k	10	2^{k}	any	[Hon+14]
	10	2^{k}	any	[Cui+16]
	11	$\mathbf{2^{k-1}}$	**any**	This work
CHAM-64/128	18	2^{128}	any	[Koo+17]
	20	2^{128}	$i, i \in A$	[Xu+22]
	22	$\mathbf{2^{127}}$	$\mathbf{i}, \mathbf{i} \in \mathbf{B}$	This work

1 $A = \{3, 5, 11, 13, 19, 21, 27, 29, 35, 37, 43, 45, 51, 53, 59\}$.

2 $B = \{2, 4, 10, 12, 18, 20, 26, 28, 34, 36, 42, 44, 50, 52, 58\}$.

Conclusion

This work

- Some more accurate differentials properties on consecutive addition modulo 2^n.
- A framework to find IDs of ARX ciphers under weak key.
- Apply to SPECK, LEA and CHAM to find longer IDs under weak key.

Future work

- As properties $3 \sim 6$ represent just a thin selection of the ID patterns found experimentally, it is valuable to continue analyzing these ID patterns.
- It is also a meaningful work to try to build an automated search model to find more impossible differentials.
- It is worthwhile to dig deeper for more impossible differentials to get better key recovery attacks for ARX ciphers.

Thanks for your attention!

Q & A