Automatic Search for the Best Trails in ARX: Application to Block Cipher SPECK

A. Biryukov V. Velichkov Y. Le Corre

LACS, SnT
University of Luxembourg

23rd International Conference on Fast Software Encryption
March 22, 2016, Bochum, Germany

OUTLINE

SEARCHING FOR OPTIMAL TRAILS IN ARX

Provable Resistance against LC and DC

1. Minimum number of active S-boxes in any trail: AES.
2. Best linear and differential trail/s: DES.

ARX Ciphers (Addition $\boxplus$/Rotation $\lll$/XOR $\oplus$)

- No S-boxes; rely on $\boxplus$ for non-linearity.
- **Pure** (ARX only) vs. **Augmented** (ARX + Boolean functions, etc.).
- Examples: Salsa20, BLAKE, Skein/Threefish, Simon, Speck, MD- and SHA- incl. SHA-3/Keccak, etc.

SEARCHING FOR OPTIMAL TRAILS IN ARX

Provable Resistance against LC and DC

1. Minimum number of active S-boxes in any trail: AES.
2. Best linear and differential trail/s: DES.

ARX Ciphers (Addition $\boxplus$/Rotation $\lll$/XOR $\oplus$)

- No S-boxes; rely on $\boxplus$ for non-linearity.
- **Pure** (ARX only) vs. **Augmented** (ARX + Boolean functions, etc.).
- Examples: Salsa20, BLAKE, Skein/Threefish, Simon, Speck, MD- and SHA- incl. SHA-3/Keccak, etc.

Problem

Design strategies (1) and (2) – not applicable to ARX.

LUXEMBOURG

TECHNIQUES FOR TRAIL SEARCH IN ARX

Bottom-up

Wang+ 2005 (MD5, SHA-1), De Cannière+ 2006 (SHA-1), Schläffer+ 2006 (MD4), Fouque+ 2007 (MD4), Stevens+ 2007 (MD5), Mendel+ 2011 (SHA-2), Leurent 2013 (Skein), Biryukov+ 2014 (TEA, XTEA, Simon, Speck), Dobraunig+ 2015 (CAESAR), Yao+ 2015 (Speck).

Top-down (SAT, MILP)

Mouha+ 2013 (Salsa20), Sun+ 2014–2015 (Simon), Fu+ 2016 (Speck).

TECHNIQUES FOR BEST TRAIL SEARCH IN ARX

Bottom-up

Wang+ 2005 (MD5, SHA-1), De Cannière+ 2006 (SHA-1), Schläffer+ 2006 (MD4), Fouque+ 2007 (MD4), Stevens+ 2007 (MD5), Mendel+ 2011 (SHA-2), Dobraunig+ 2015 (CAESAR), Leurent 2013 (Skein), Biryukov+ 2014 (TEA, XTEA, Simon, Speck), Yao+ 2015 (Speck).

Top-down (SAT, MILP)

Mouha+ 2013 (Salsa20), Sun+ 2014–2015 (Simon), Fu+ 2016 (Speck).

TECHNIQUES FOR BEST TRAIL SEARCH IN ARX

Bottom-up

Wang+ 2005 (MD5, SHA-1), De Cannière+ 2006 (SHA-1), Schläffer+ 2006 (MD4), Fouque+ 2007 (MD4), Stevens+ 2007 (MD5), Mendel+ 2011 (SHA-2), Dobraunig+ 2015 (CAESAR), Leurent 2013 (Skein), Biryukov+ 2014 (TEA, XTEA, Simon, Speck), Yao+ 2015 (Speck).

Top-down (SAT, MILP)

Mouha+ 2013 (Salsa20), Sun+ 2014–2015 (Simon), Fu+ 2016 (Speck).

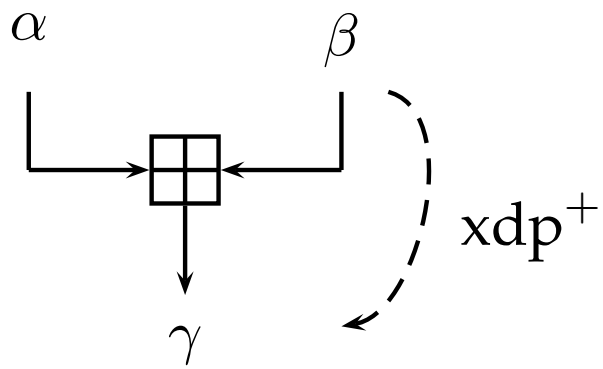
Our Contribution

A new bottom-up approach for best trail search in ARX.

UNIVERSITÉ DU LUXEMBOURG

OUTLINE

THE XOR DIFFERENTIAL PROBABILITY OF $\boxplus$



Definition (xdp$^+$)

$$\mathrm{xdp}^+(\alpha, \beta \to \gamma) = \frac{\#\{(x, y) : ((x \oplus \alpha) + (y \oplus \beta)) \oplus (x + y) = \gamma\}}{2^{2w}} .$$

where α, β, γ are w-bit XOR differences.

MONOTONICITY OF xdp^+

Proposition (Biryukov+, CT-RSA 2014)

xdp^+ *is monotonously decreasing with the word size* w *of the differences in the direction LSB to MSB:*

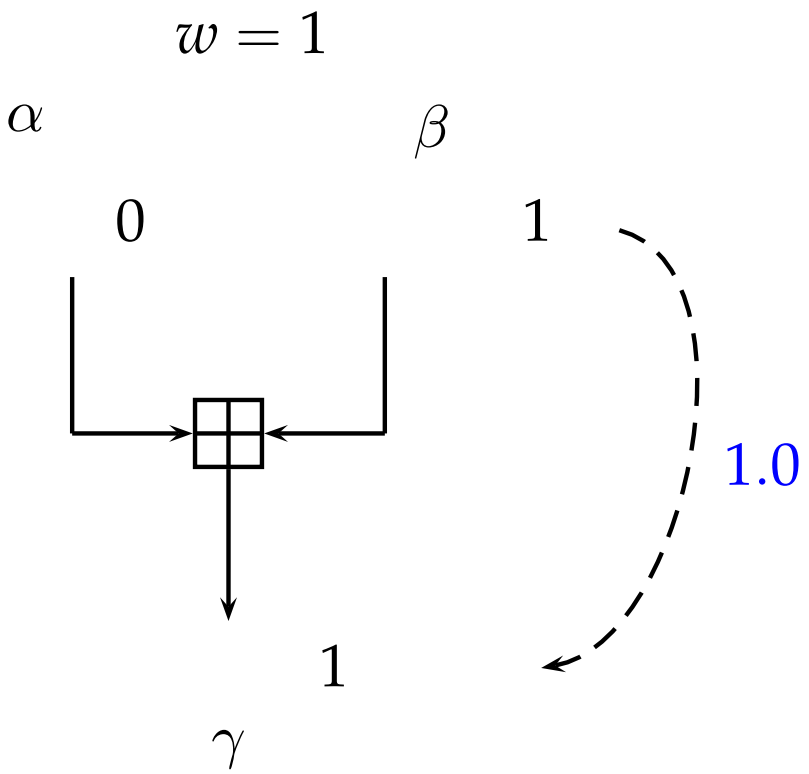
$$\tilde{p}_1 \geq \tilde{p}_2 \ldots \geq \tilde{p}_{w-1} \geq \tilde{p}_w = \mathrm{xdp}^+(\alpha, \beta \rightarrow \gamma) \ ,$$

where

$$\tilde{p}_i = \mathrm{xdp}^+(\alpha[i-1:0], \beta[i-1:0] \rightarrow \gamma[i-1:0]) : \ w \geq i \geq 1 \ ,$$

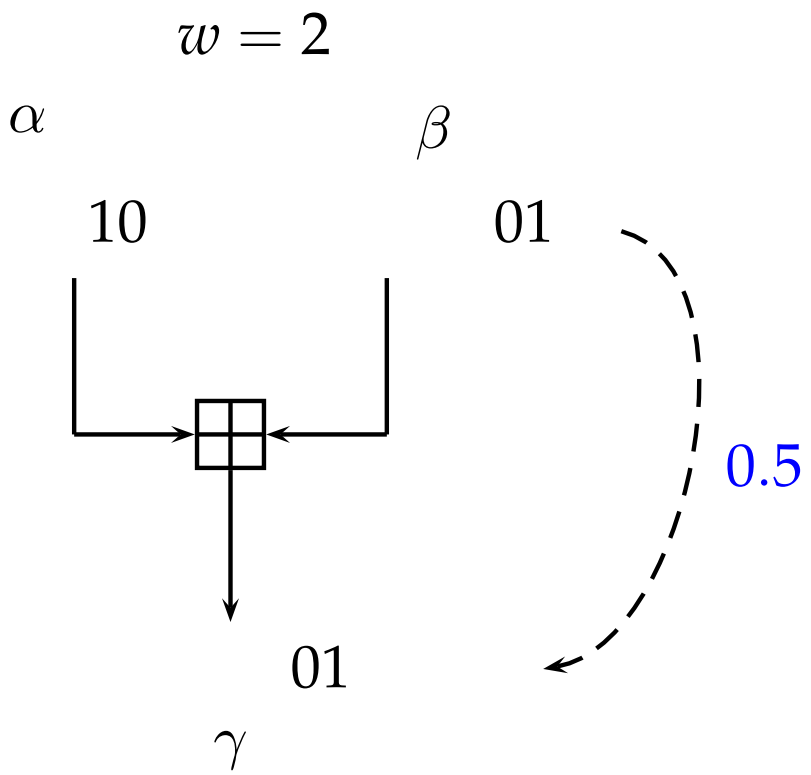
is the probability of the partial differential composed of the i *LS bits of* α, β, γ.

xdp$^+$ IS DECREASING LSB TO MSB



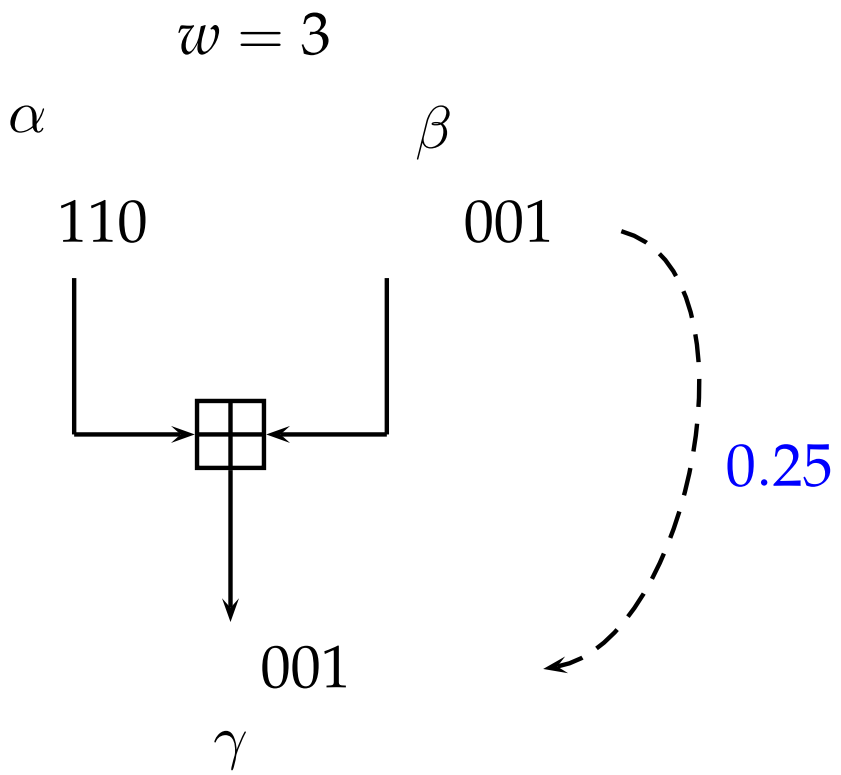
1.0

xdp$^+$ IS DECREASING LSB TO MSB



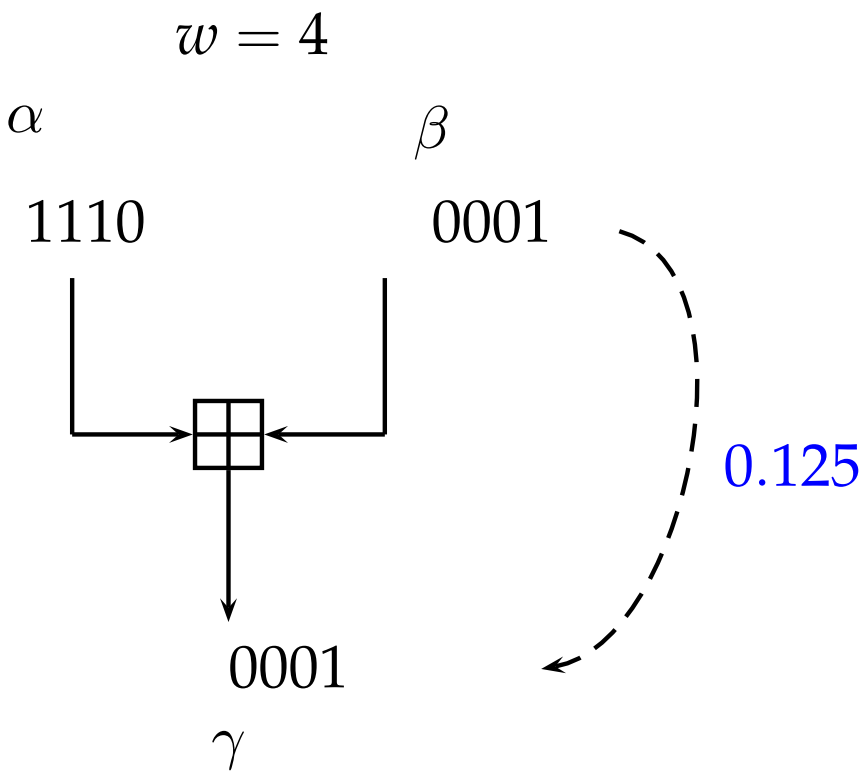
$0.5 \leq 1.0$

xdp$^+$ IS DECREASING LSB TO MSB



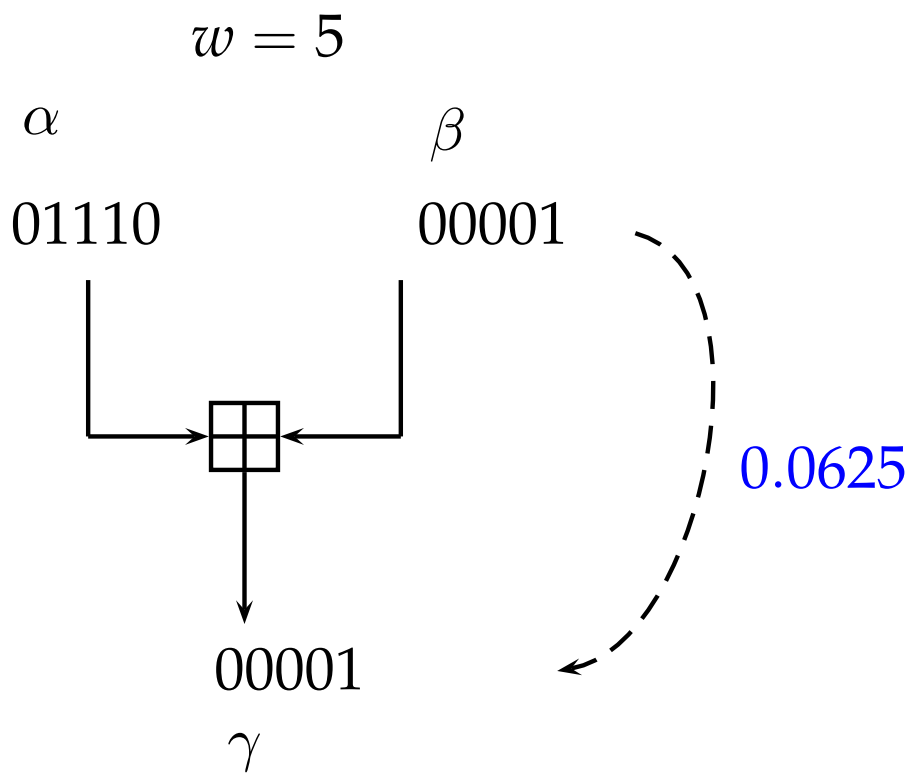
$0.25 \leq 0.5 \leq 1.0$

xdp$^+$ IS DECREASING LSB TO MSB



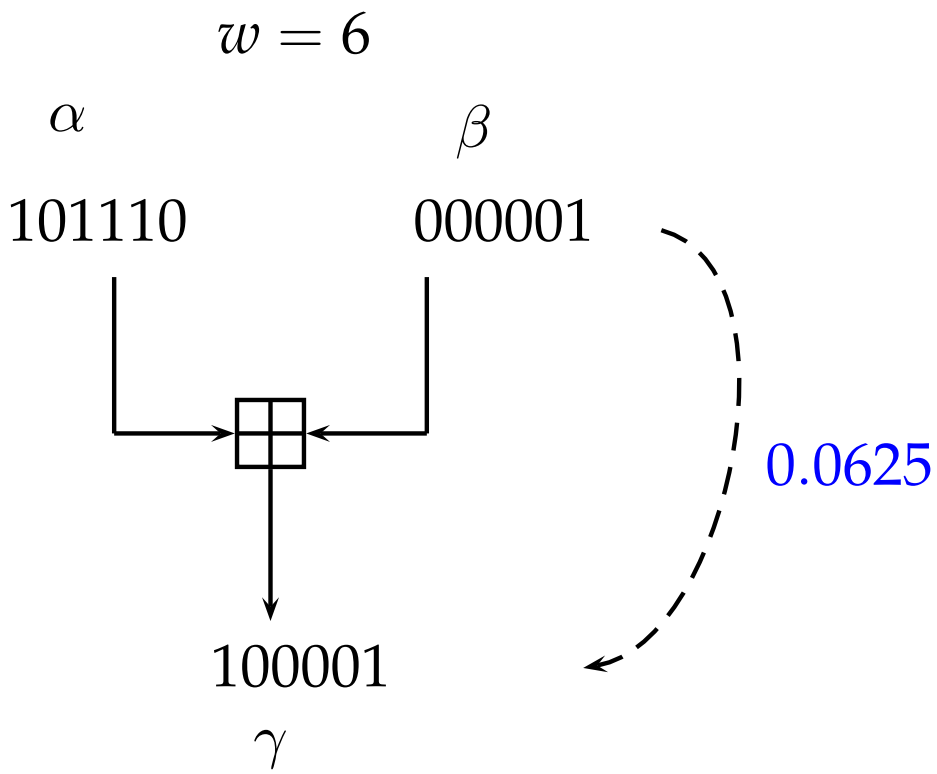
$$0.125 \leq 0.25 \leq 0.5 \leq 1.0$$

xdp$^+$ IS DECREASING LSB TO MSB



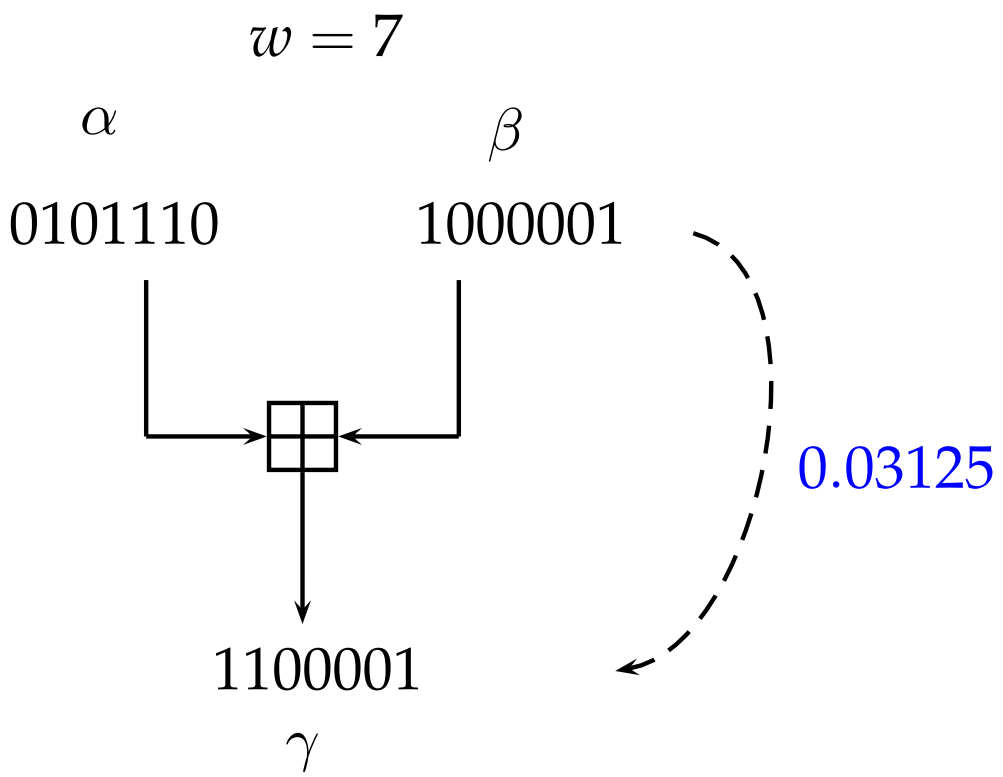
$0.0625 \leq 0.125 \leq 0.25 \leq 0.5 \leq 1.0$

xdp$^+$ IS DECREASING LSB TO MSB



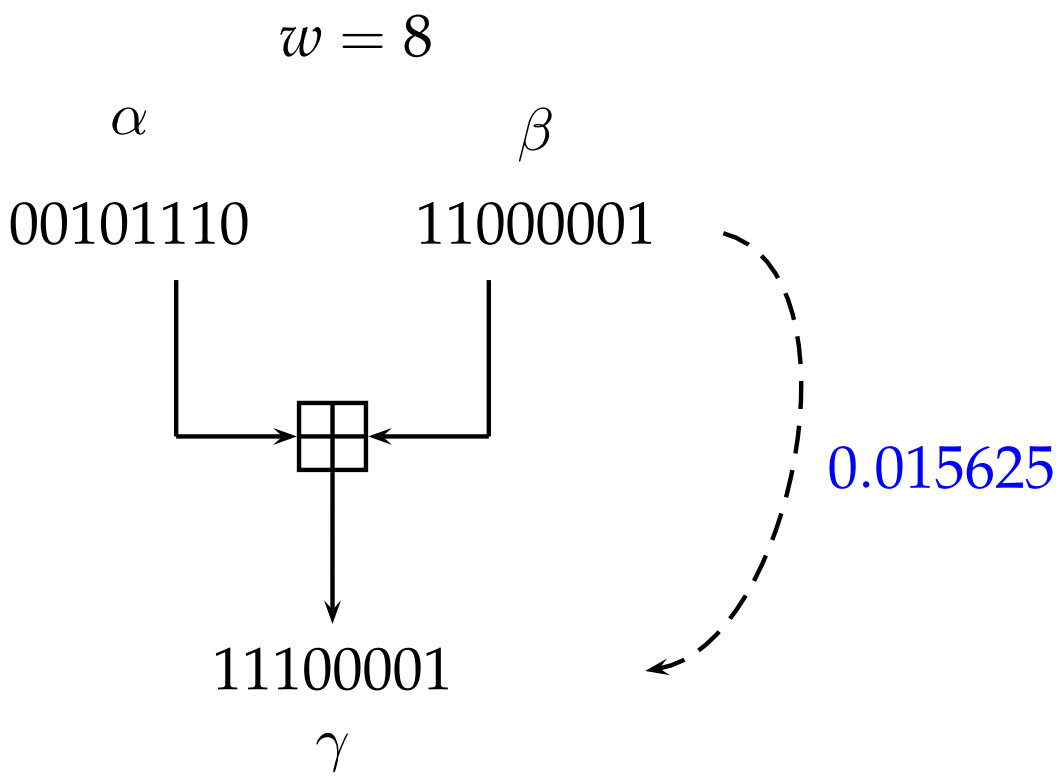
$$0.0625 \leq 0.0625 \leq 0.125 \leq 0.25 \leq 0.5 \leq 1.0$$

xdp$^+$ IS DECREASING LSB TO MSB



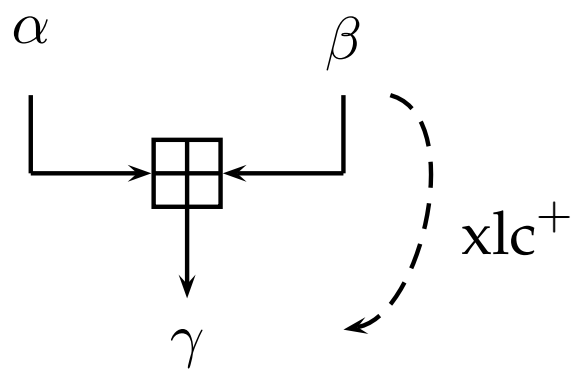
$$0.03125 \leq 0.0625 \leq 0.0625 \leq 0.125 \leq 0.25 \leq 0.5 \leq 1.0$$

xdp$^+$ IS DECREASING LSB TO MSB



$$0.015625 \leq 0.03125 \leq 0.0625 \leq 0.0625 \leq 0.125 \leq 0.25 \leq 0.5 \leq 1.0$$

THE XOR LINEAR CORRELATION OF $\boxplus$



Definition (xlc$^+$)

$$\mathrm{xlc}^+(\alpha, \beta \to \gamma) = 2\,\frac{\#\{(x,y) : (x^T\alpha) \oplus (y^T\beta) = (z^T\gamma)\}}{2^{2w}} - 1\ .$$

where α, β, γ are w-bit linear masks and $a^T b$ denotes dot-product.

MONOTONICITY OF xlc$^+$

Proposition

$|\mathrm{xlc}^+|$ is monotonously decreasing with the word size w of the masks in the direction MSB to LSB:

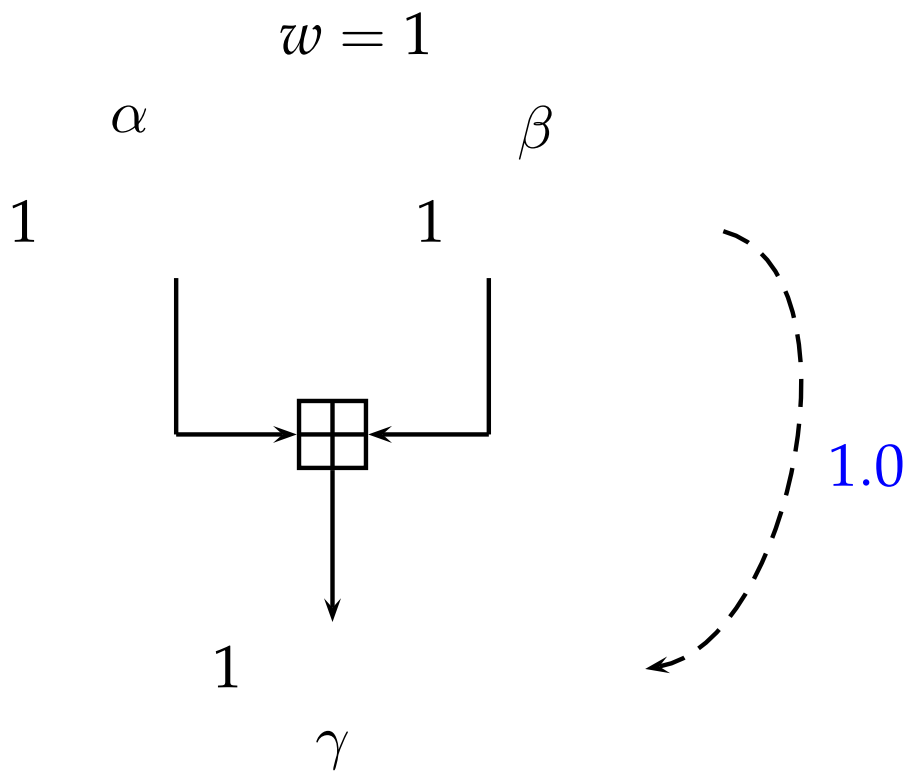
$$\tilde{c}_{w-1} \geq \tilde{c}_{w-2} \ldots \geq \tilde{c}_1 \geq \tilde{c}_0 = |\mathrm{xlc}^+(\alpha, \beta \rightarrow \gamma)| \ ,$$

where

$$\tilde{c}_i = |\mathrm{xlc}^+(\alpha[w-1:i], \beta[w-1:i] \rightarrow \gamma[w-1:i])| : \ w-1 \geq i \geq 0 \ ,$$

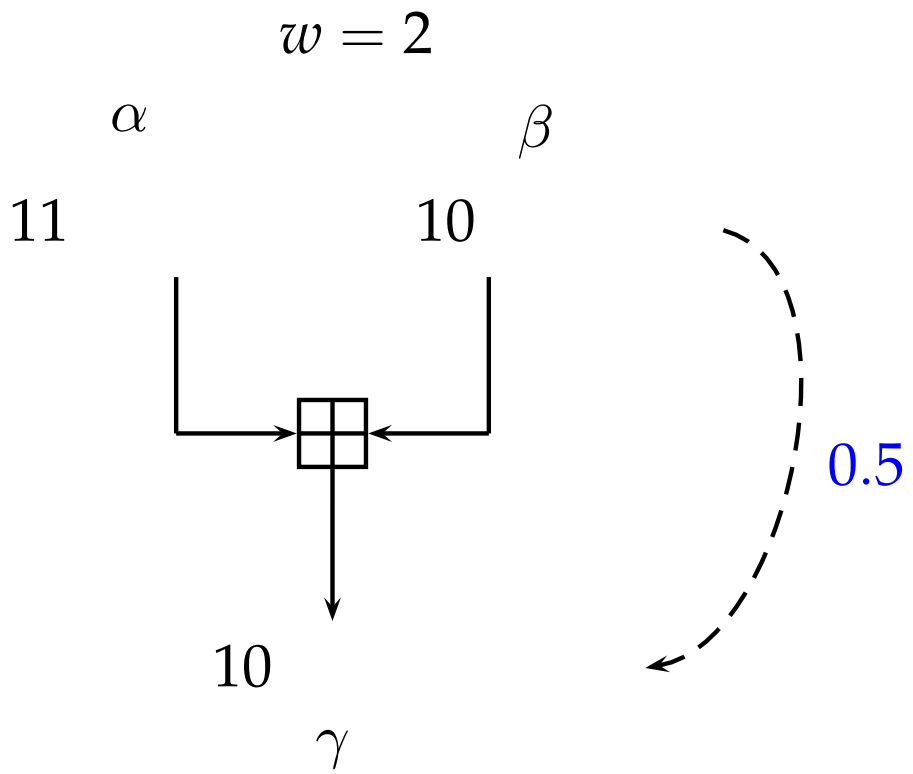
is the absolute value of the correlation of the partial linear approximation composed of the i MS bits of α, β, γ and $|a|$ denotes the absolute value of a.

xlc$^+$ IS DECREASING MSB TO LSB



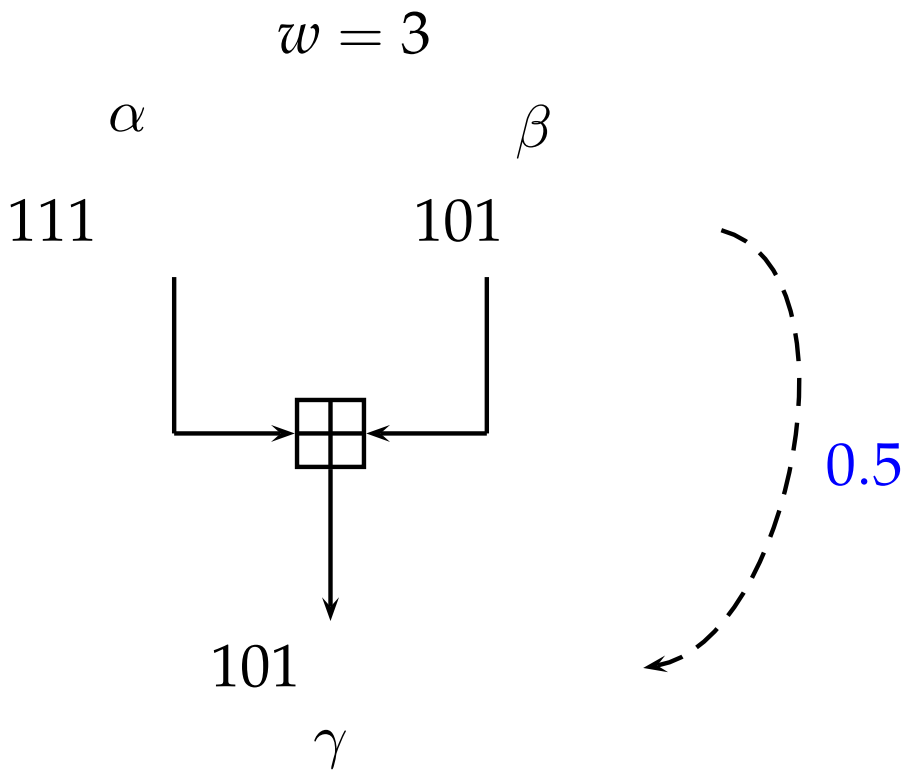
1.0

xlc$^+$ IS DECREASING MSB TO LSB



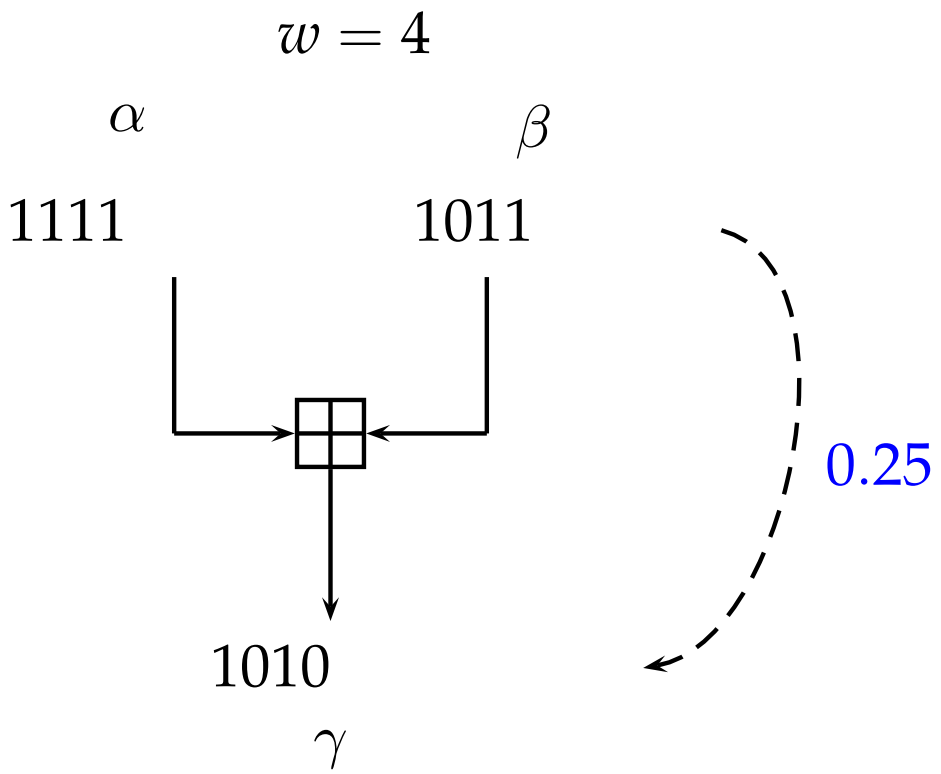
$1.0 \geq 0.5$

xlc$^+$ IS DECREASING MSB TO LSB



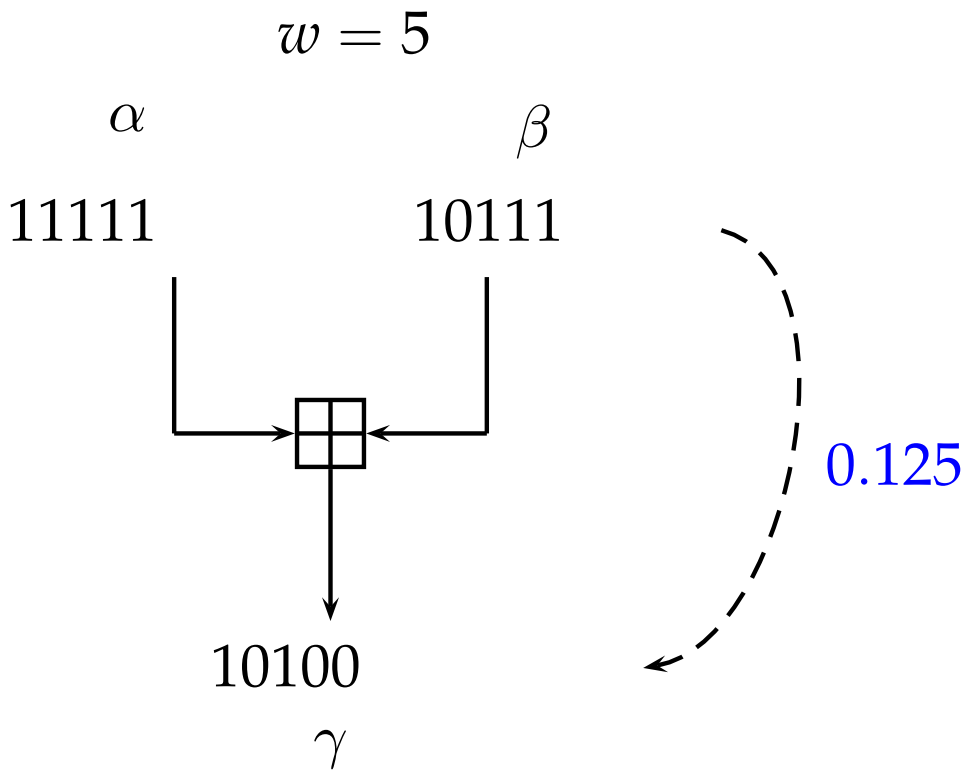
$1.0 \geq 0.5 \geq 0.5$

xlc$^+$ IS DECREASING MSB TO LSB



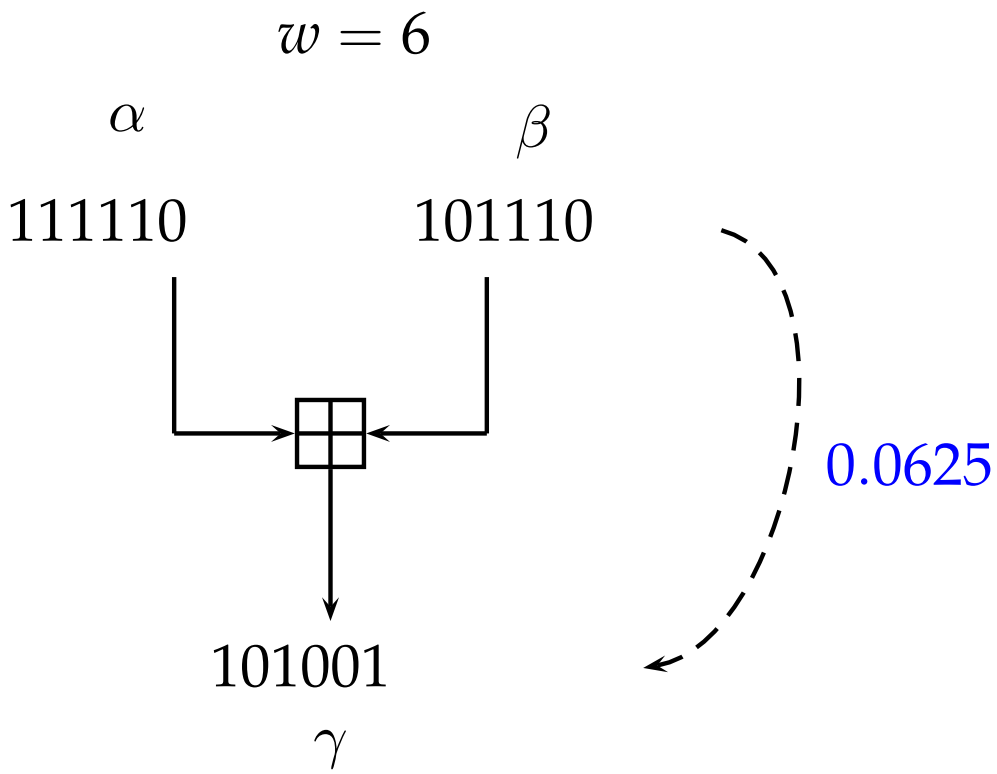
$1.0 \geq 0.5 \geq 0.5 \geq 0.25$

xlc$^+$ IS DECREASING MSB TO LSB



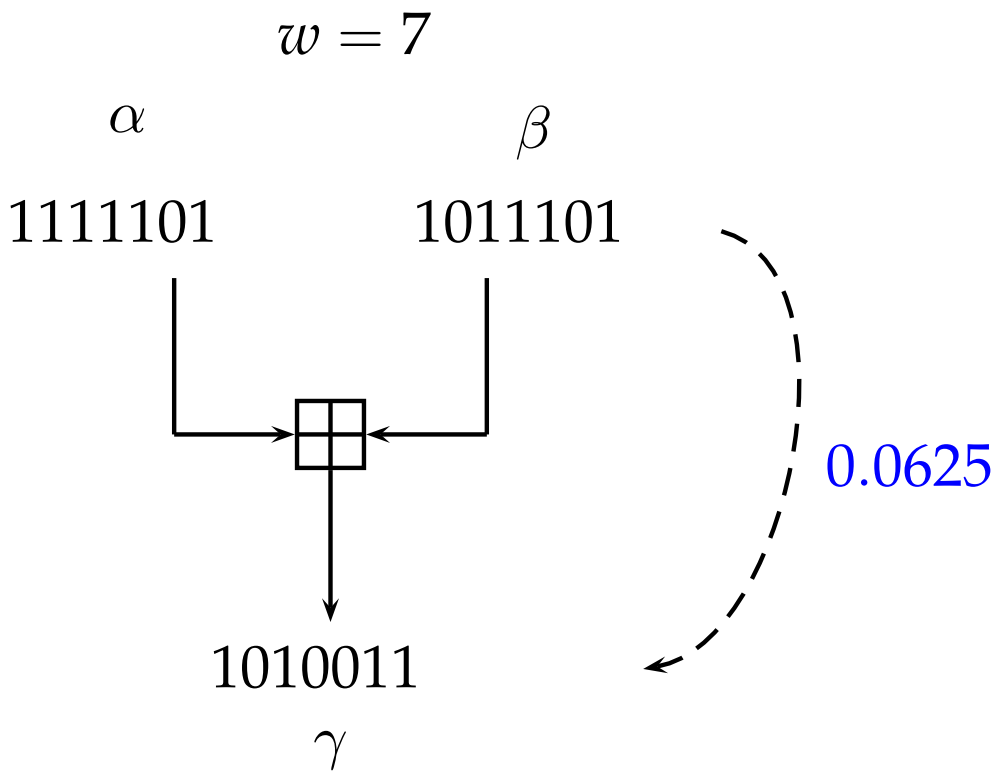
$1.0 \geq 0.5 \geq 0.5 \geq 0.25 \geq 0.125$

xlc$^+$ IS DECREASING MSB TO LSB



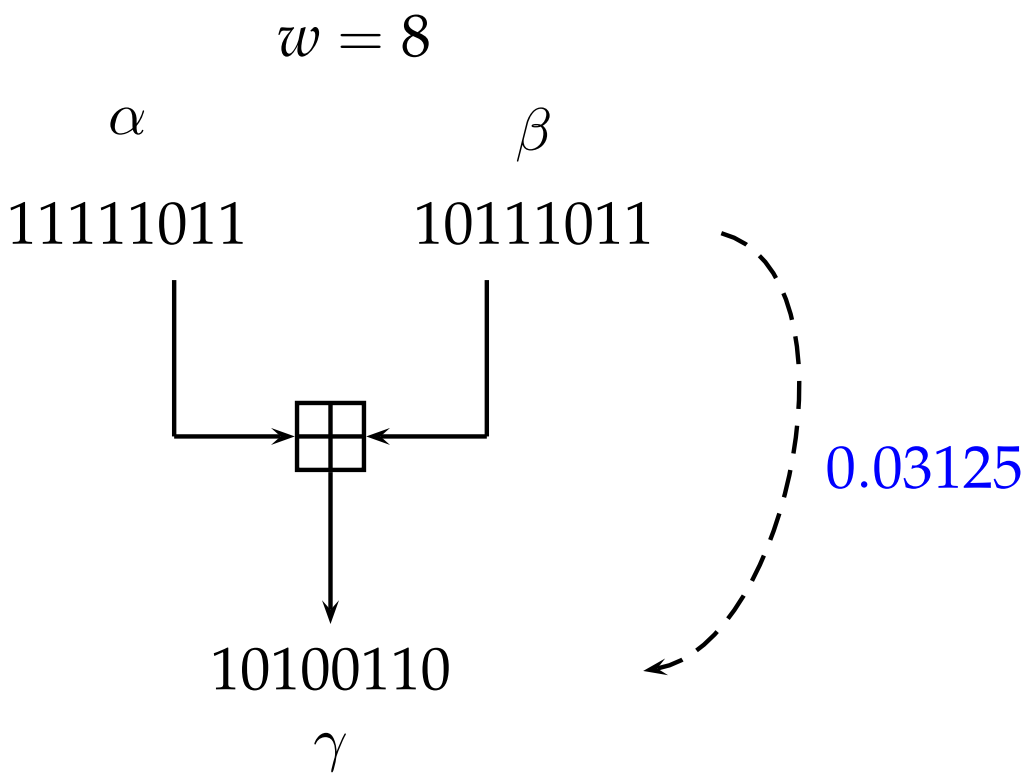
$1.0 \geq 0.5 \geq 0.5 \geq 0.25 \geq 0.125 \geq 0.0625$

xlc$^+$ IS DECREASING MSB TO LSB



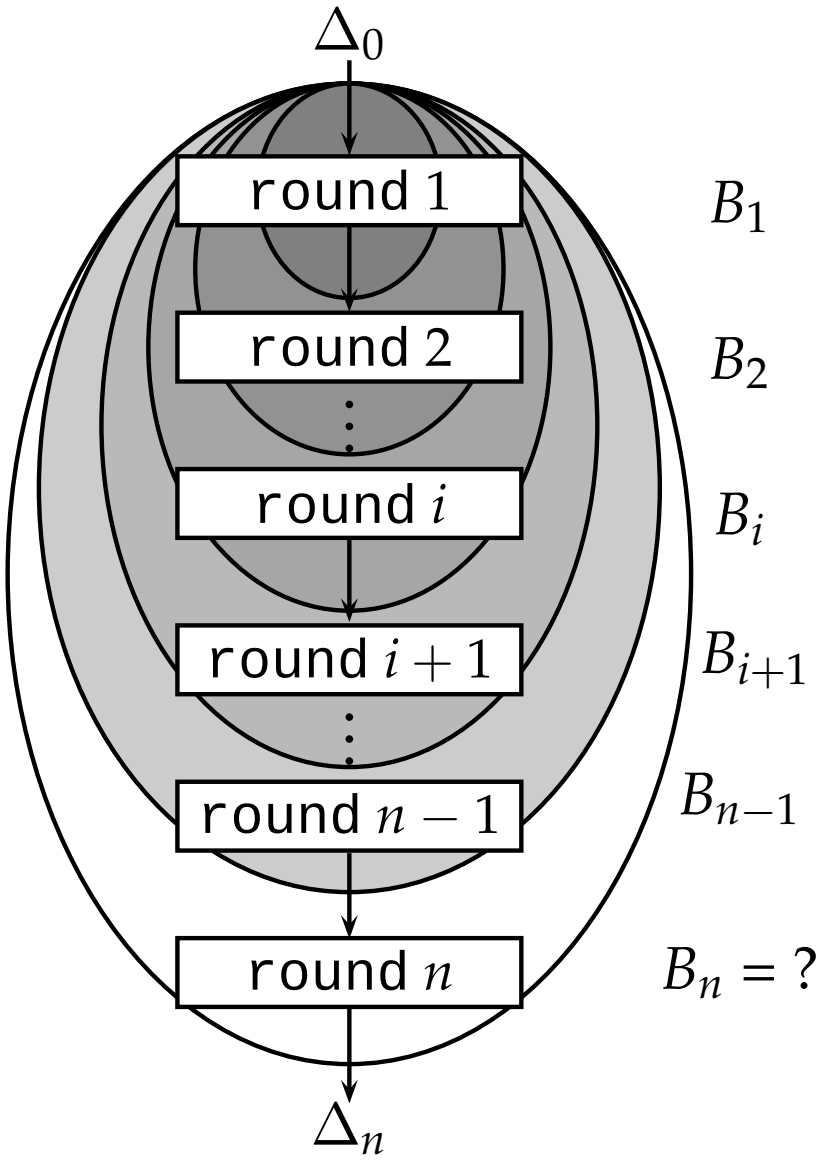
$$1.0 \geq 0.5 \geq 0.5 \geq 0.25 \geq 0.125 \geq 0.0625 \geq 0.0625$$

xlc$^+$ IS DECREASING MSB TO LSB

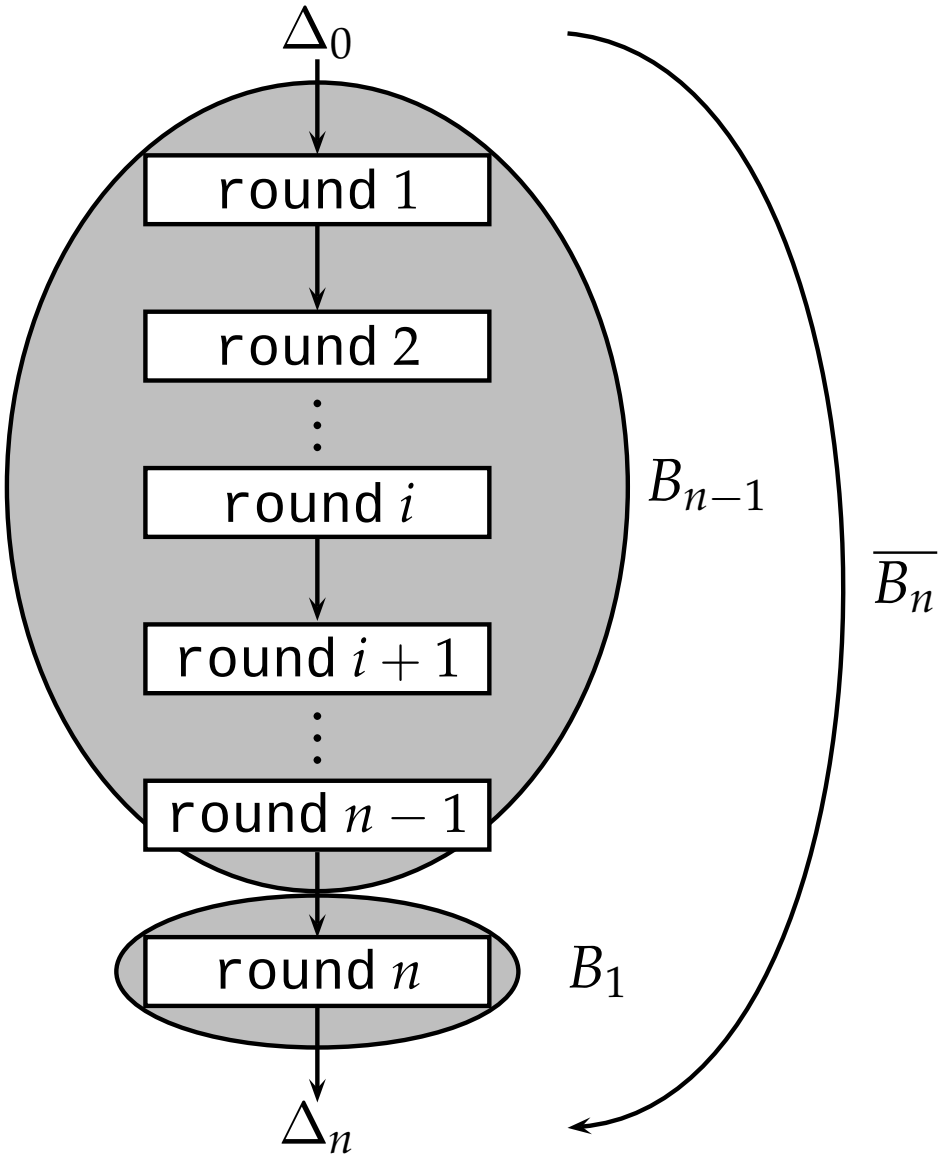


$$1.0 \geq 0.5 \geq 0.5 \geq 0.25 \geq 0.125 \geq 0.0625 \geq 0.0625 \geq 0.03125$$

OUTLINE

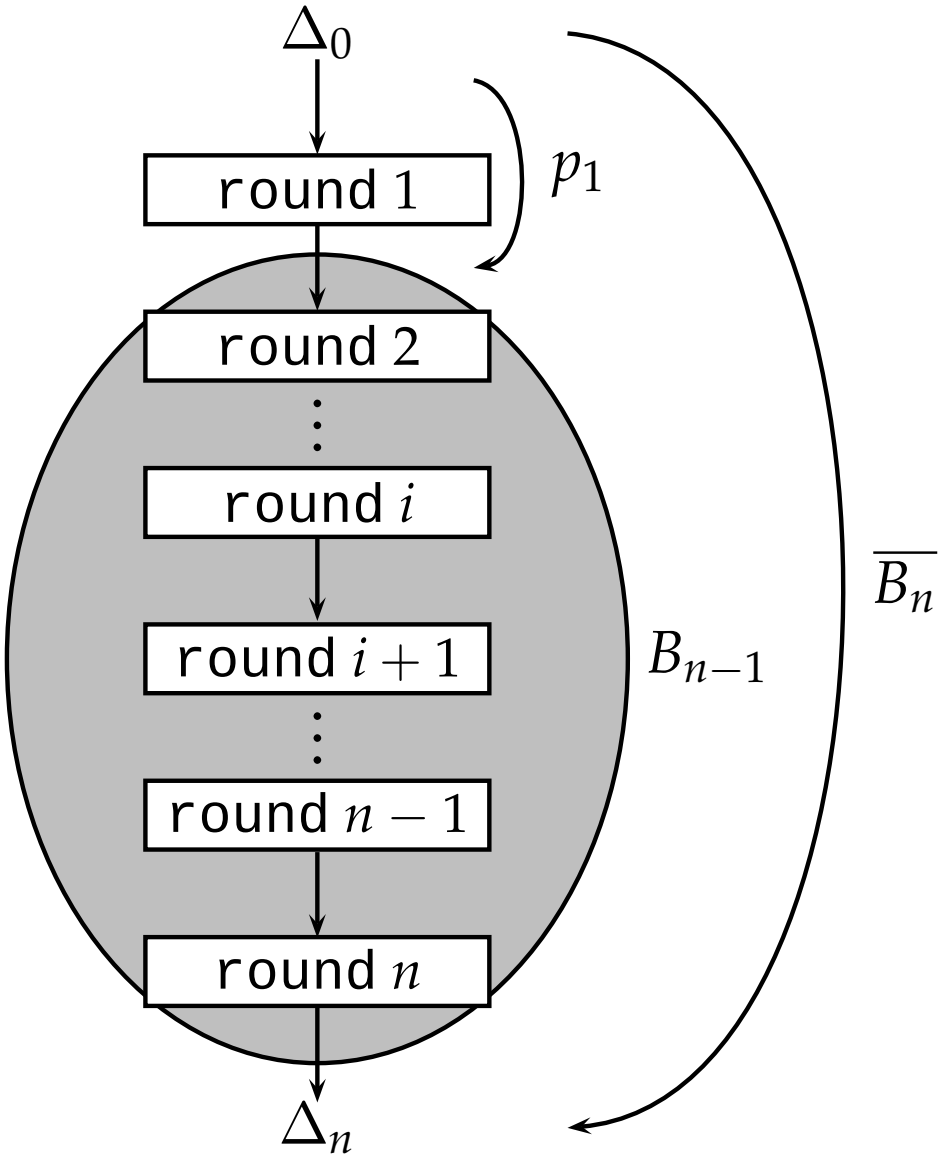


Input: best p for $n-1$ rounds:
$B_1, B_2, \ldots, B_{n-1}$
Output: best p for n rounds:
B_n

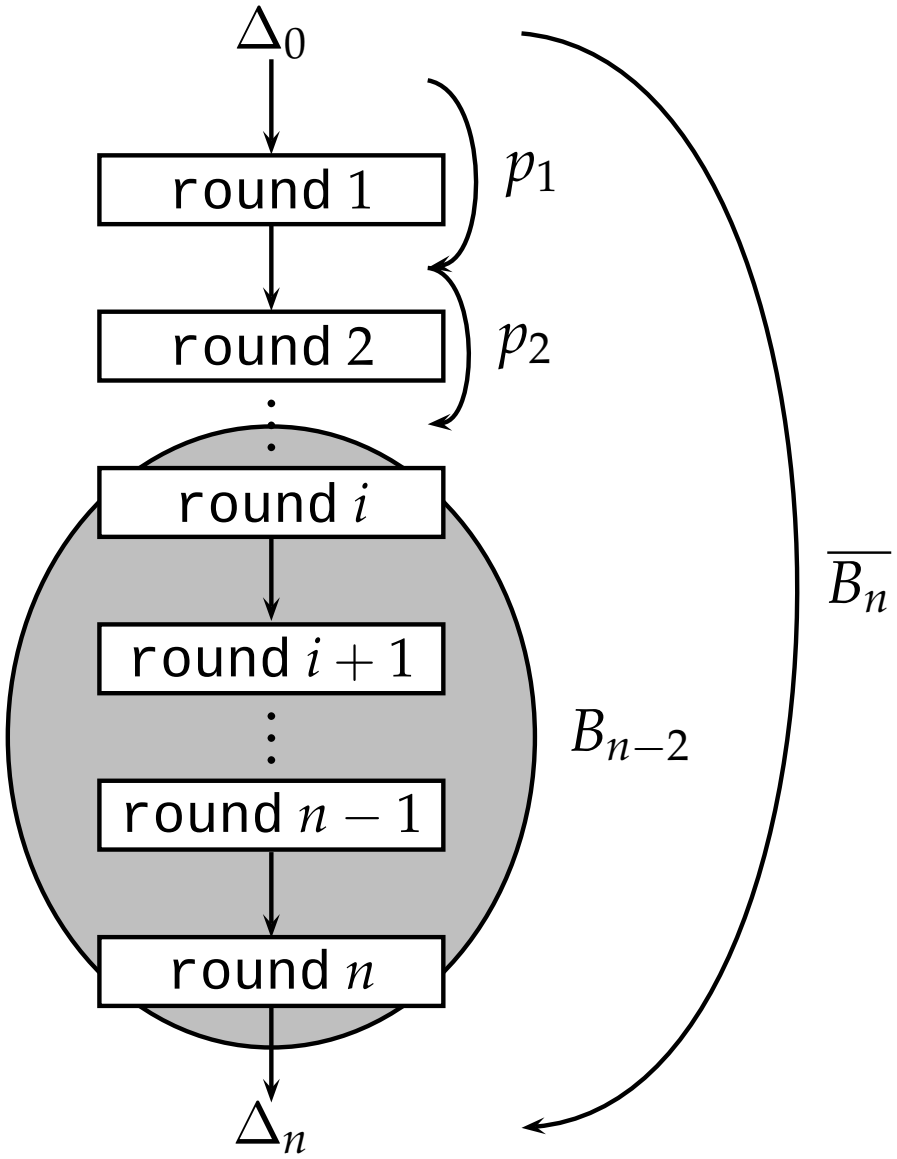


Init bound:

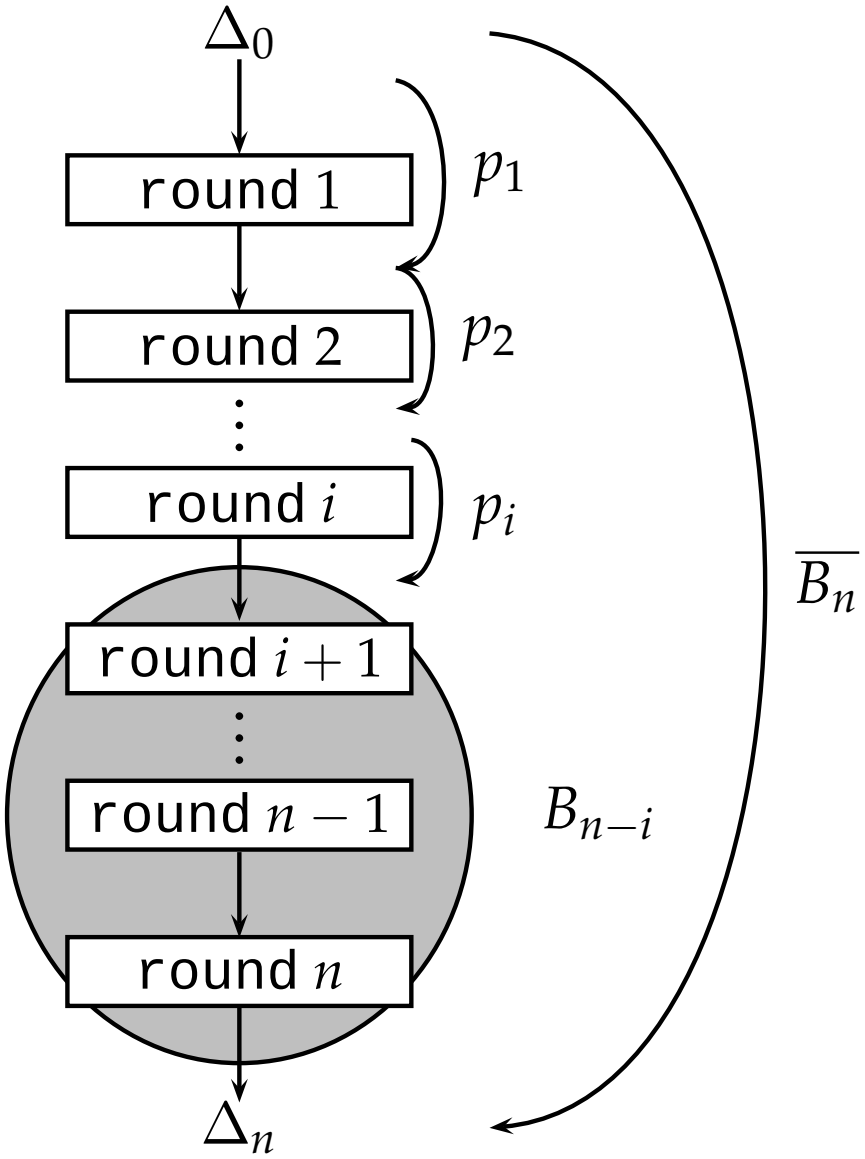
$$\overline{B_n} \leq B_n$$



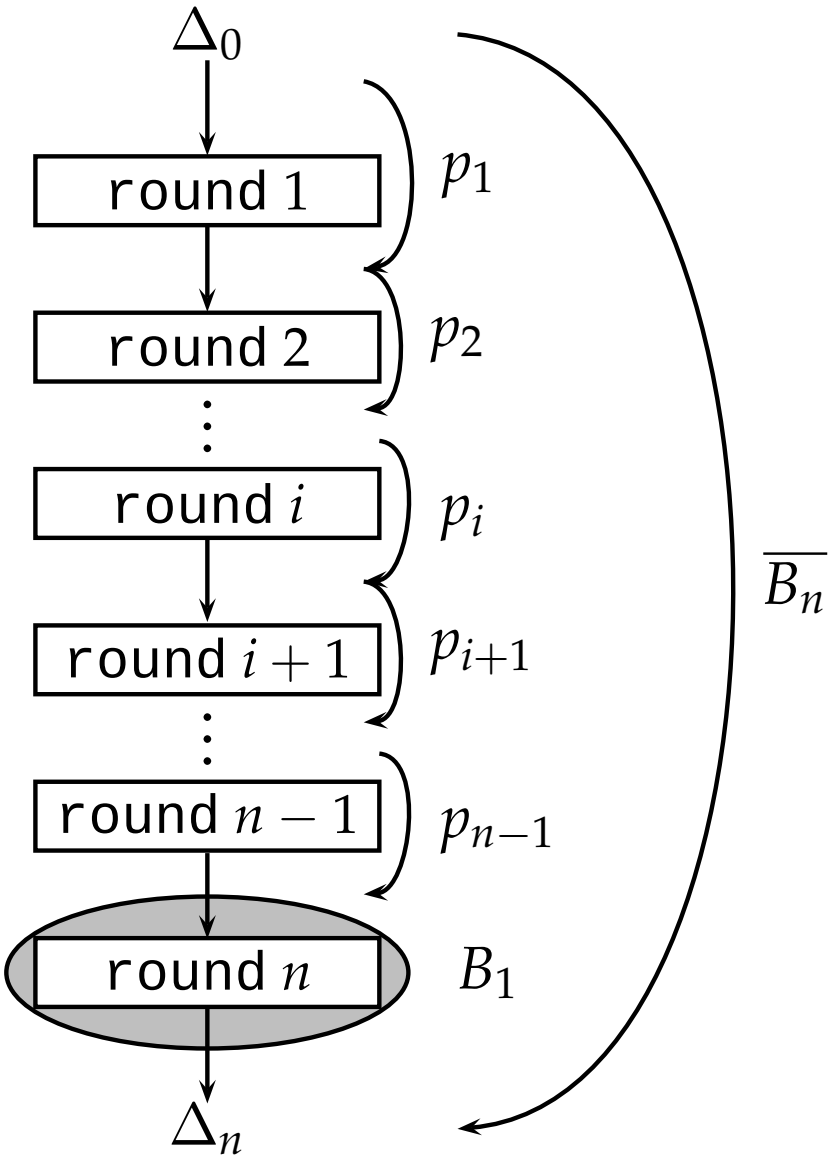
for all (Δ_0, Δ_1) :
if $p_1 B_{n-1} \geq \overline{B_n}$:
call round 2



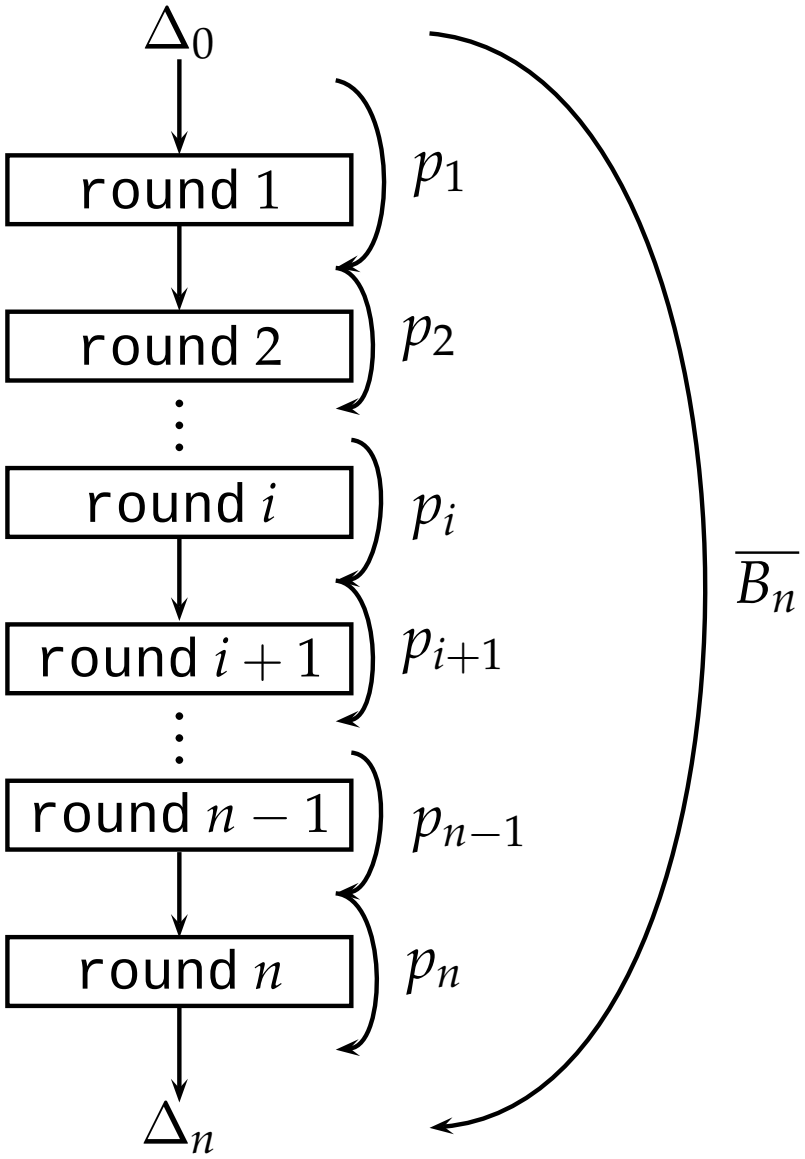
for all Δ_2 :
  if $p_1 p_2 B_{n-2} \geq \overline{B_n}$:
    call round 3



for all Δ_i :
  if $p_1 p_2 \ldots p_i B_{n-i} \geq \overline{B_n}$:
    call round $i+1$



for all Δ_{n-1} :
  if $p_1 p_2 \ldots p_{n-1} B_1 \geq \overline{B_n}$:
    call round n



for all Δ_n :
  if $p = p_1 p_2 \ldots p_{n-1} p_n \geq \overline{B_n}$:
    update bound:
      $\overline{B_n} \leftarrow p$

MATSUI'S ALGORITHM FOR ARX

Matsui's Algorithm

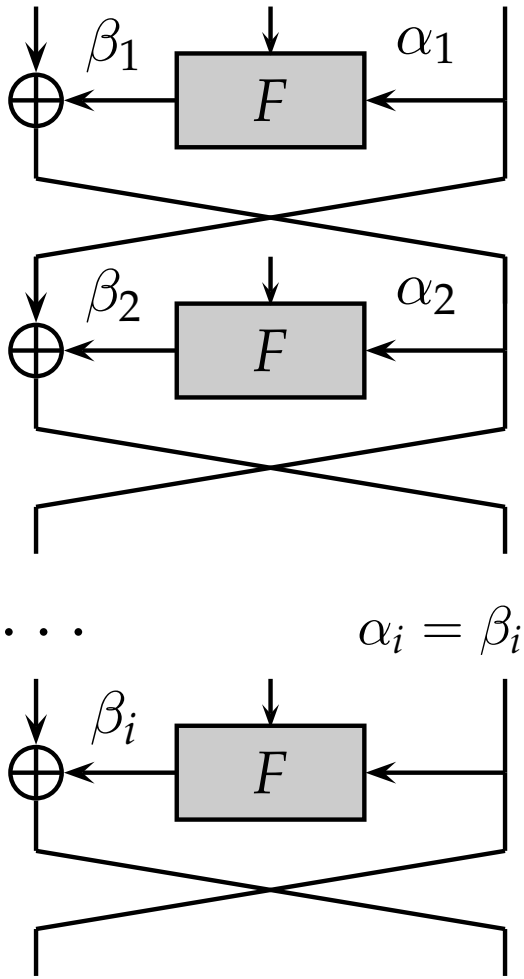
- Returns optimal results if $\overline{B_n} \leq B_n$.
- Applicable to S-box based ciphers.
- Not applicable to ARX.

Main Idea

- Adapt Matsui's algorithm to ARX.
- Inspired by the *threshold search* algorithm by Biryukov+ (CT-RSA 2014).

OUTLINE

MATSUI'S ALGORITHM APPLIED TO DES



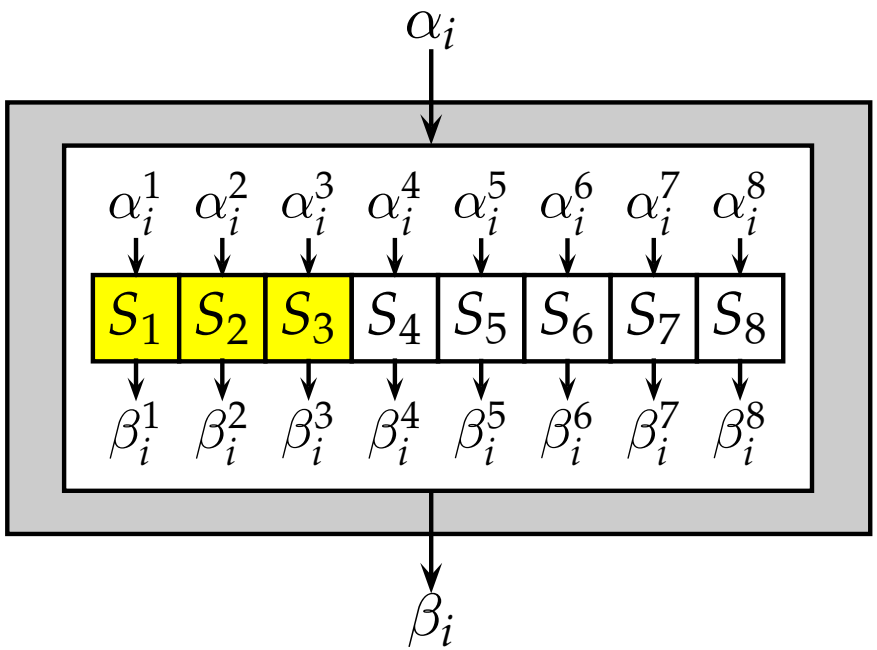
round 1
for all α_1 :
  $\beta_1 : p_1 = \max_\beta p(\alpha_1 \to \beta)$
  if $p_1 B_{n-1} \geq \overline{B_n}$:
    call round 2

round 2
for all α_2, β_2 :
  $p_2 = p(\alpha_2 \to \beta_2)$
  if $p_1 p_2 B_{n-2} \geq \overline{B_n}$
    call round 3

$\cdots$

round i
$\alpha_i = \beta_{i-1} \oplus \alpha_{i-2}$
for all $\beta_i : p_i = p(\alpha_i \to \beta_i)$:
  if $p_1 p_2 \ldots p_i B_{n-i} \geq \overline{B_n}$:
    call round $i+1$

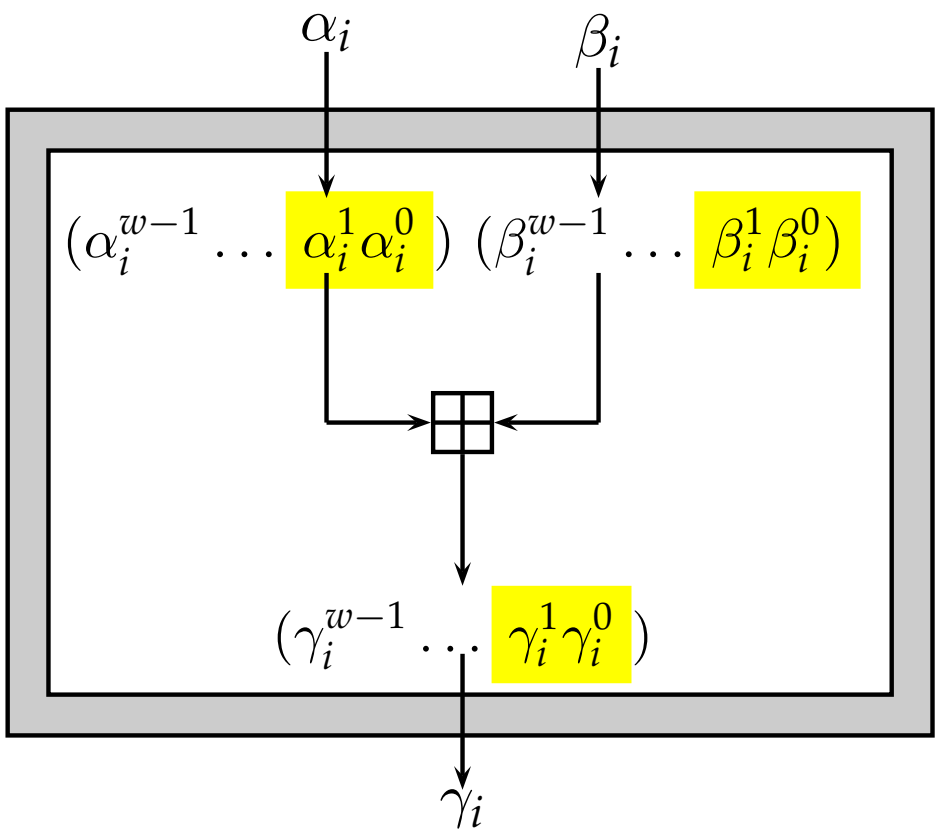
DIVIDE-AND-CONQUER THE S-BOX LAYER



round i
while $j \leq 8$:
  for all α_i^j, β_i^j :
    $p^j = p(\alpha_i^j \rightarrow \beta_i^j)$
    $\tilde{p}_i = p^1 p^2 \ldots p^j$
    if $p_1 p_2 \ldots \tilde{p}_i B_{n-i} \geq \overline{B_n}$
      $j = j + 1$
    if $j = 8$
      call round $i + 1$

Note: p is computed using the DDT of the S-boxes.

DIVIDE-AND-CONQUER THE MODULAR ADDITION



round i

while $j \leq w-1$:

  for all $\alpha_i^j, \beta_i^j, \gamma_i^j \in \{0,1\}$:

    $\tilde{p}_i = \text{xdp}^+(\alpha_i[0:j], \beta_i[0:j] \rightarrow \gamma_i[0:j])$

    if $p_1 p_2 \ldots \tilde{p}_i B_{n-i} \geq \overline{B_n}$

      $j = j + 1$

    if $j = w - 1$

      call round $i+1$

OUTLINE

SPECK FAMILY OF BLOCK CIPHERS

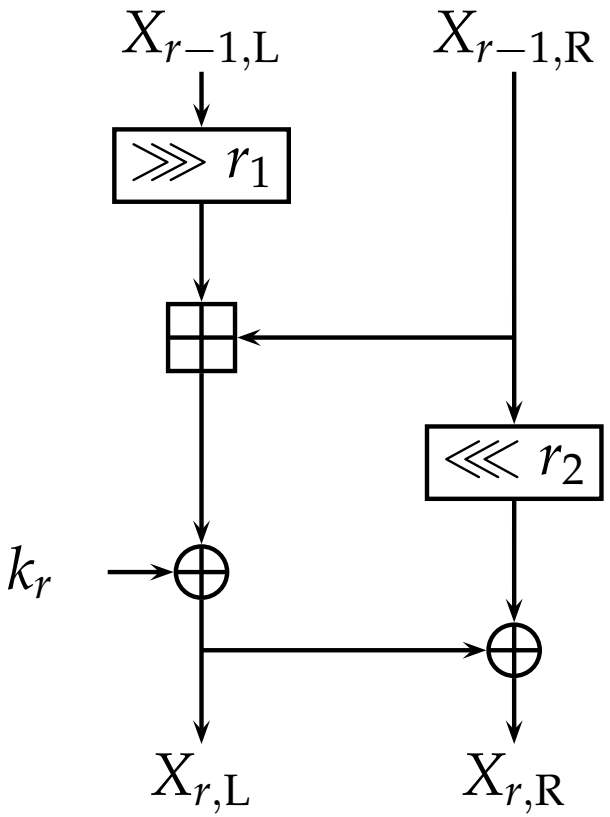


Figure : One round of Speck.

- SpeckN: N-bit block size, w-bit word size ($w = N/2$).
- $N = 32/48/64/96/128$ resp. $w = 16/24/32/48/64$.
- $r_1 = 7, r_2 = 2$ for Speck32; $r_1 = 8, r_2 = 3$ for other versions.
- Key size and number of rounds depend on N (next slide).

SPECKN: KEY SIZES AND NUMBER OF ROUNDS

SPECKN	N	w	Key	R	Key	R	Key	R
SPECK32	32	16	64	22				
SPECK48	48	24	72	22	96	23		
SPECK64	64	32	96	26	144	29		
SPECK96	96	48	96	28	144	29		
SPECK128	128	64	128	32	192	33	256	34

Table : N – block size (bits); $w = N/2$ – word size (bits); Key – key size (bits); R – num. of rounds.

MARKOV ASSUMPTION

Definition

Markov assumption = Markov cipher + Independent round keys.

Definition (Markov Cipher [Lai, Massey, 1991])

An iterated cipher with round function F is Markov if for all choices of α and β: $P_k^F(\beta|\alpha, x) = P_{k,x}^F(\beta|\alpha)$.

Multiplying Probabilities [Theorem 2, Lai, Massey, 1991]

If a cipher is Markov and the round keys are independent and uniformly random, then the probability of a trail is the product of the probabilities of single-round trails.

BEST* DIFFERENTIAL TRAILS FOR SPECK

R \ N	32	t	48	t	64	t	96	t	128	t
1	-0	0s	-0	0s	-0	0s	-0	0s	-0	0s
2	-1	0s	-1	0s	-1	0s	-1	0s	-1	0s
3	-3	0s	-3	0s	-3	0s	-3	0s	-3	0s
4	-5	0s	-6	0s	-6	0s	-6	6s	-6	22s
5	-9	0s	-10	1s	-10	1m	-10	5m	-10	26m
6	-13	1s	-14	3s	-15	26m	-15	5h	-15	2d
7	-18	1m	-19	1m	-21	4h	-21	5d	< -20	1d
8	-24	34m	-26	9m	-27	22h	< -27	3d	< -25	4h
9	-30	12m	-33	7d	< -30	19h				
10	-34	6m								

* Under the Markov assumption.

UPPER BOUNDS* ON THE DP OF SPECK

Instance	Upper Bound	Rounds	Upper Bound	Rounds	Upper Bound	Rounds
SPECK32	-69	22				
SPECK48	-72	22	-76	23		
SPECK64	-91	26	-96	29		
SPECK96	-90	28	-94	29		
SPECK128	-104	32	-104	33	-105	34

* Under the Markov assumption.

LIMITATIONS

Complexity

- Increases with word size and rounds.
- (Currently working on parallelization.)

Linear Trails

- Search for linear trails infeasible for SpeckN for $N > 32$.

Markov Assumption

- The Markov assumption does not hold for Speck (see Appendix).
- The best a cryptanalyst can do even for non-Markov ciphers.
- Experimentally checked that the trails hold for most keys.

UNIVERSITÉ DU LUXEMBOURG

LIMITATIONS

Complexity

- Increases with word size and rounds.
- (Currently working on parallelization.)

Linear Trails

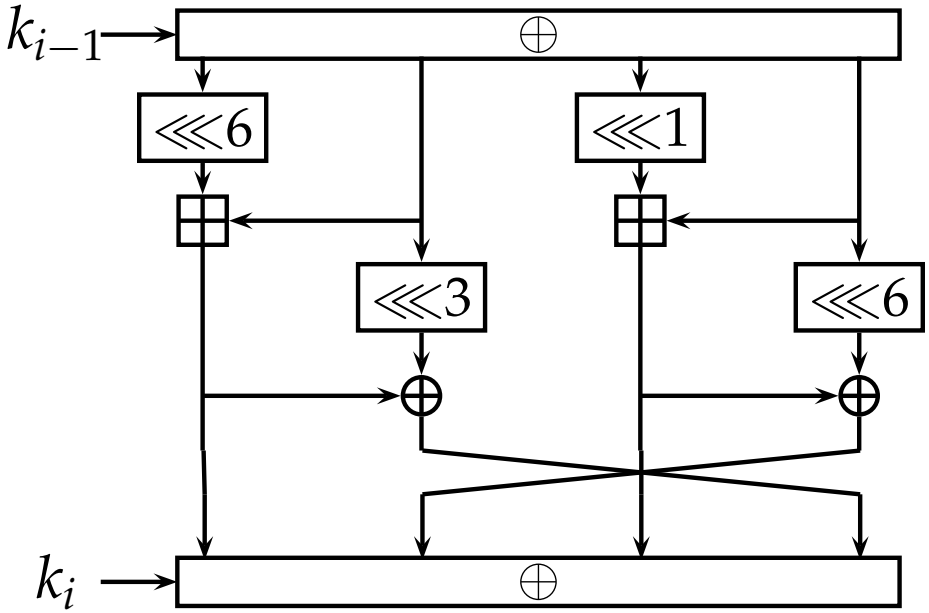
- Search for linear trails infeasible for SpeckN for $N > 32$.

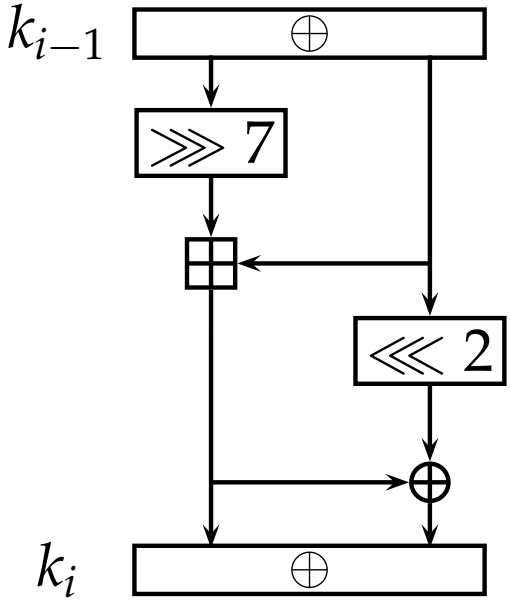
Markov Assumption

- The Markov assumption does not hold for Speck (see Appendix).
- The best a cryptanalyst can do even for non-Markov ciphers.
- Experimentally checked that the trails hold for most keys.

UNIVERSITÉ DU LUXEMBOURG

MARX (MIX+ARX) AND SPECKEY (SPECK32+KEY)





# R	1	2	3	4	5	6	7	8	9	10
DP_{MARX}	-0	-1	-3	-6	-10	-15	-21	-27	-31	-35
LC_{MARX}	-0	-0	-1	-3	-5	-8	-10	-12	-14	-16
$DP_{Speckey}$	-0	-1	-3	-5	-9	-13	-18	-24	-30	-34
$LC_{Speckey}$	-0	-0	-1	-3	-5	-7	-9	-12	-14	-17

OUTLINE

SUMMARY OF RESULTS

Contributions

1. The first adaptation of Matsui's alg. to ARX with optimal results.
2. Best differential trails for up to 10, 9, 8, 7, and 6 rounds of Speck32, Speck48, Speck64, Speck96 and Speck128 resp. + exact number.
3. Bounds on the security of SPECK against DC.
4. MARX and Speckey: ARX components with provable bounds against single-trail DC and LC.
5. Source code will be made public as part of YAARX: `https://github.com/vesselinux/yaarx` .

Thank you for your attention!
Questions?

uni.lu UNIVERSITÉ DU LUXEMBOURG