RadioGatún,
a belt-and-mill hash function

Guido Bertoni, Joan Daemen,

Michaël Peeters[*] and Gilles Van Assche

STMicroelectronics *[*]De Valck Consultants*

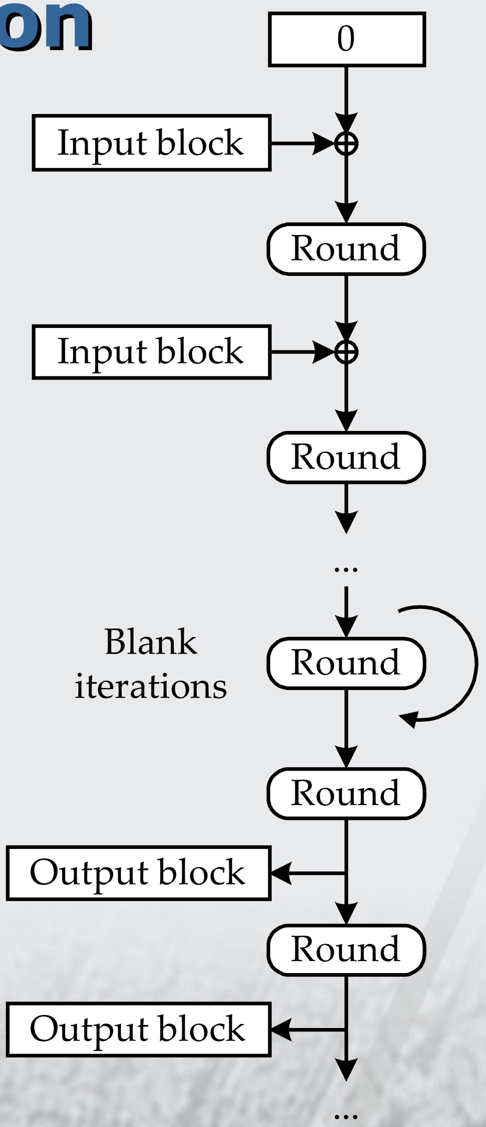
Second Cryptographic Hash Workshop

Introduction

- New hash function (family)
- Alternative design
    - Not based on fixed-length comp. function (Damgård-Merkle)
    - Not based on reduction
    - ⇨ **Variable-length input, variable-length output**
    - Diversity
- Building upon PANAMA
    - Generalizing collision-generating attack [Rijmen et al.]
    - Simplify and strengthen
    - Performance in SW and HW

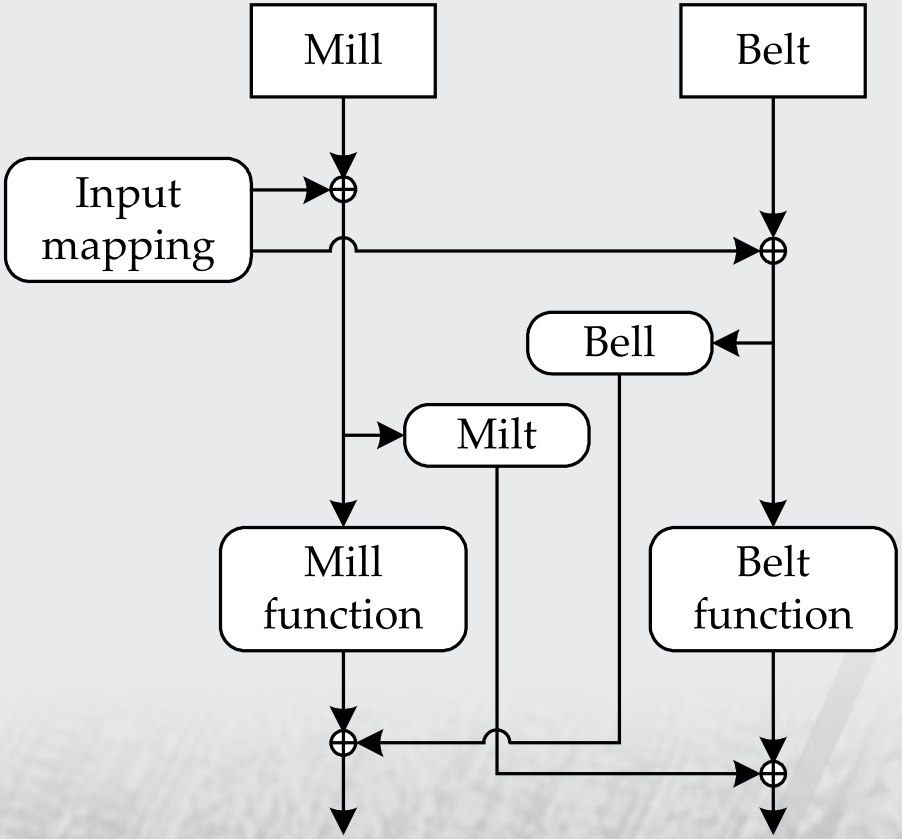
Alternating-input construction

- State
  - Starts from 0
- Iterate with **input** blocks
  - Input mapping
  - State size > input block size (l_i)
- Do **blank iterations**
- Iterate with **output** blocks
  - Output mapping
  - Fixed number for hash function



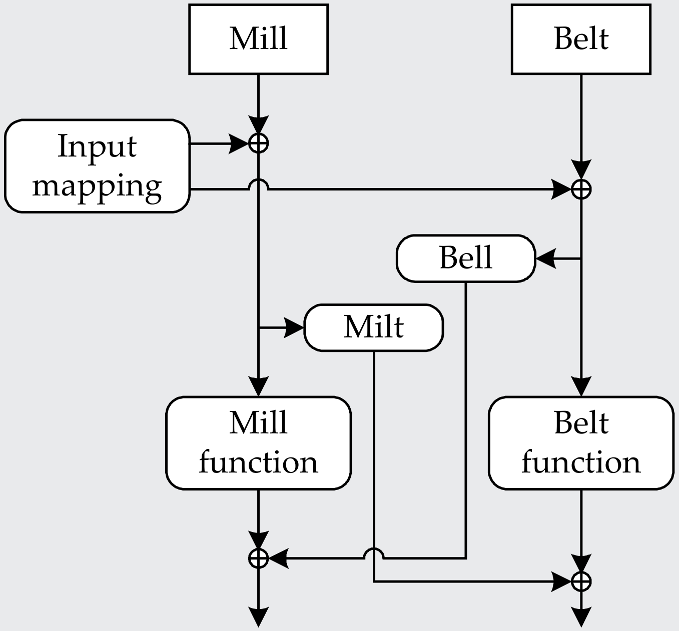
Belt-and-mill structure

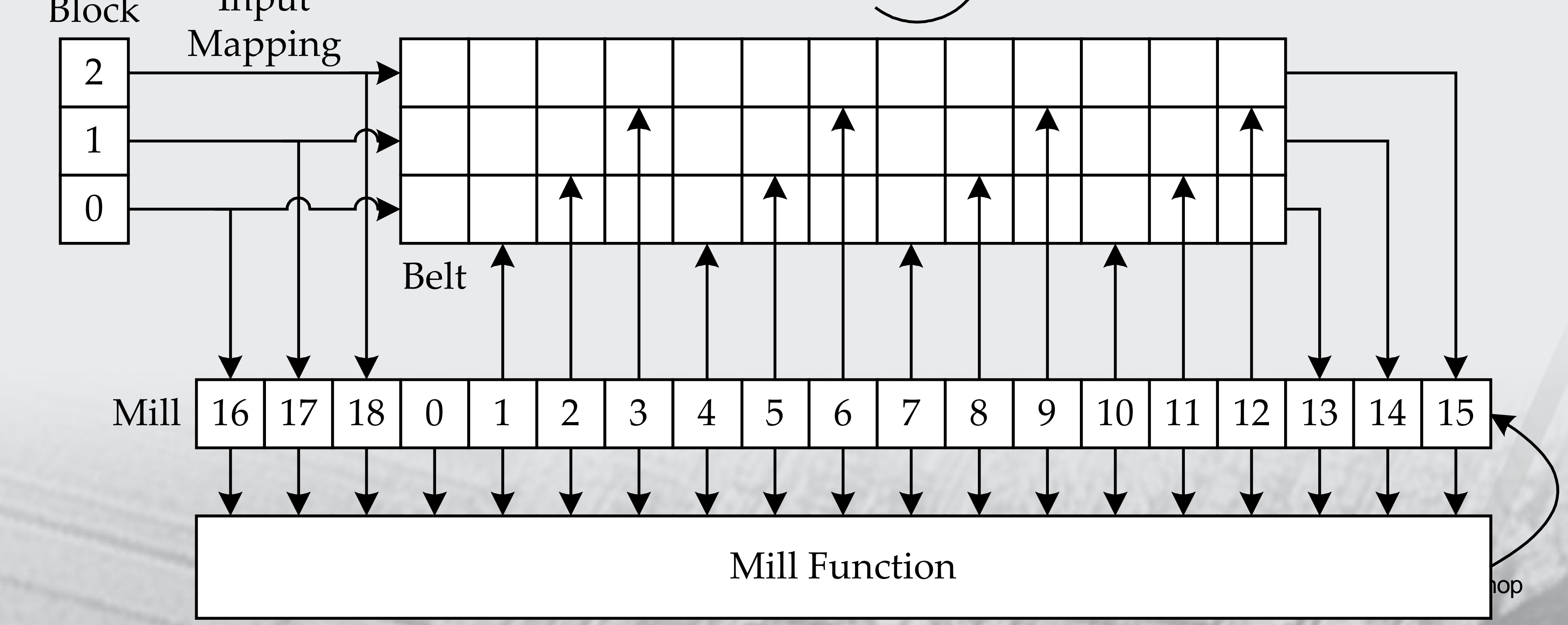
- State = (**mill**, **belt**)
- Mill function
  - **Non-linear** function
  - Diffusion and confusion
- Belt function
  - Linear function
  - **Long-term diffusion**
- Belt-to-mill + mill-to-belt
  - **Bell + milt**
  - Linear mappings



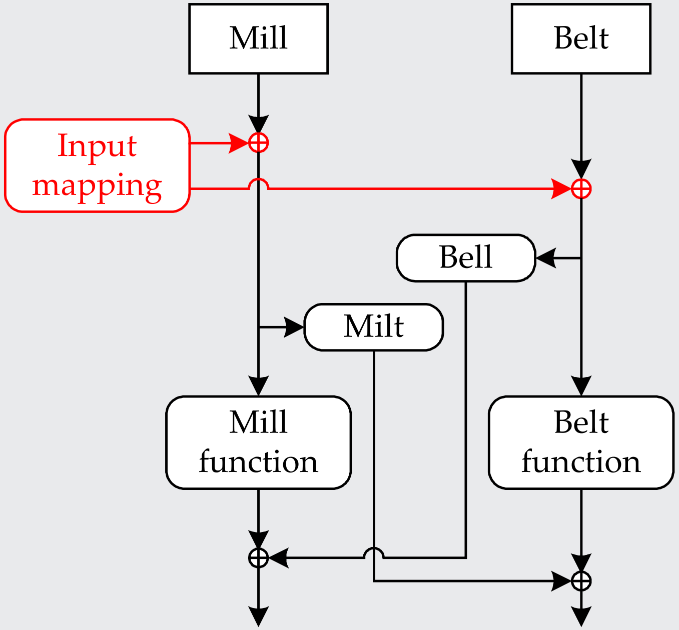
RadioGatún

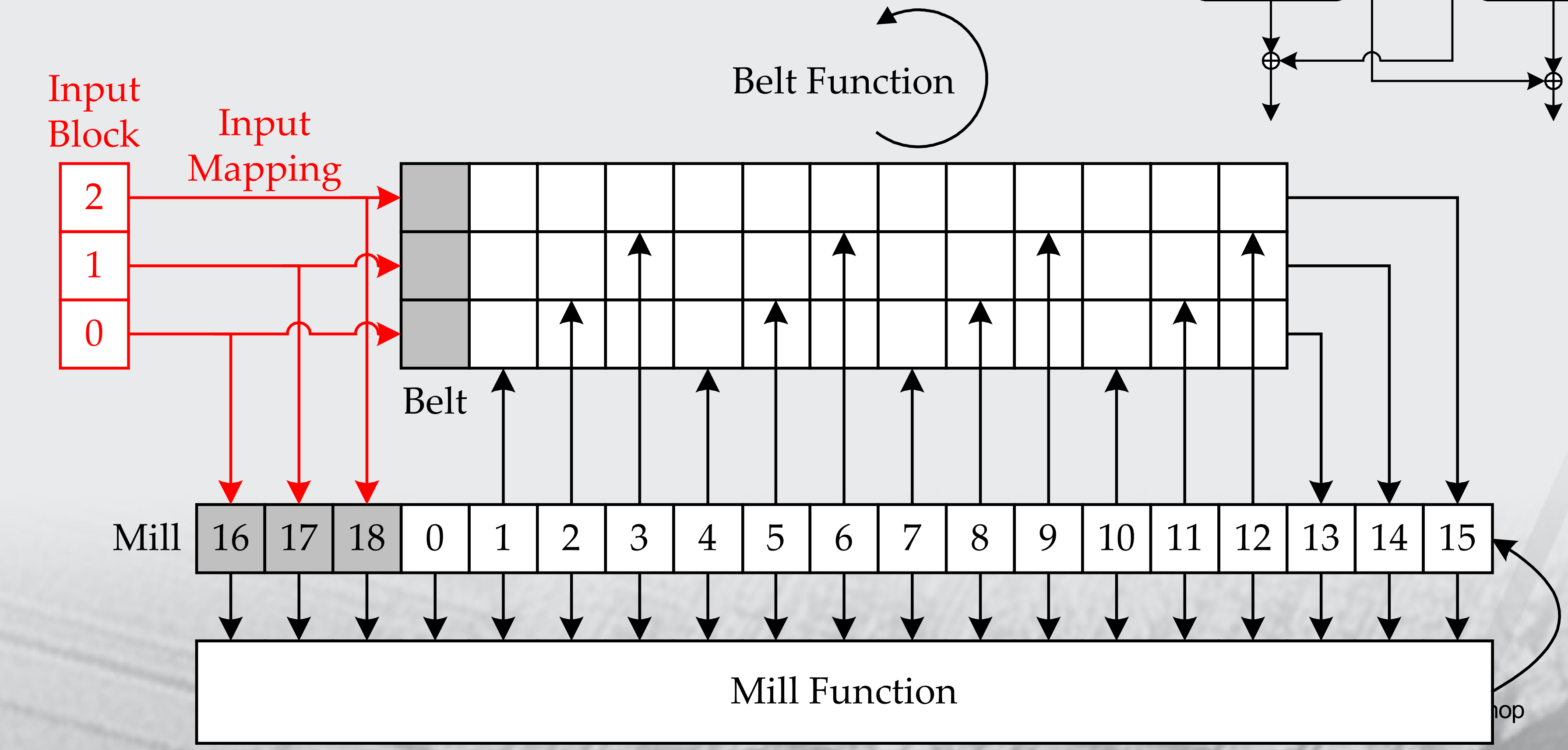
- Parameter: **word size**
  - RadioGatún[32]
  - RadioGatún[64]





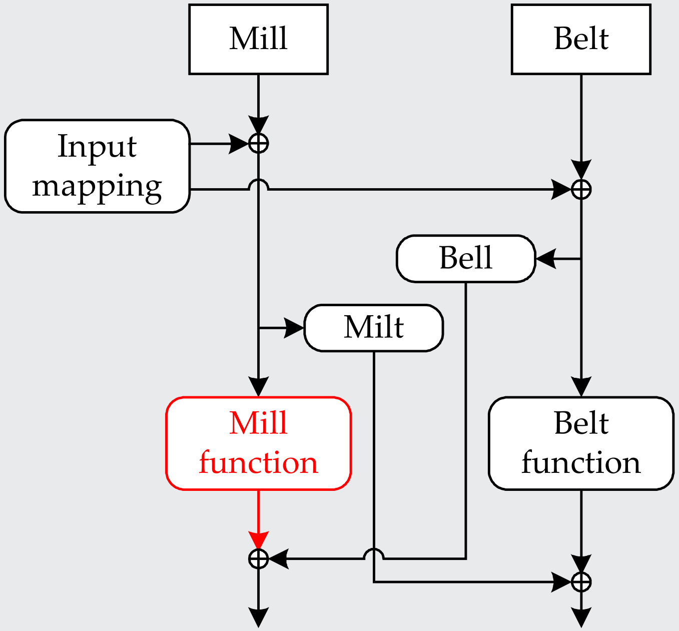
RadioGatún

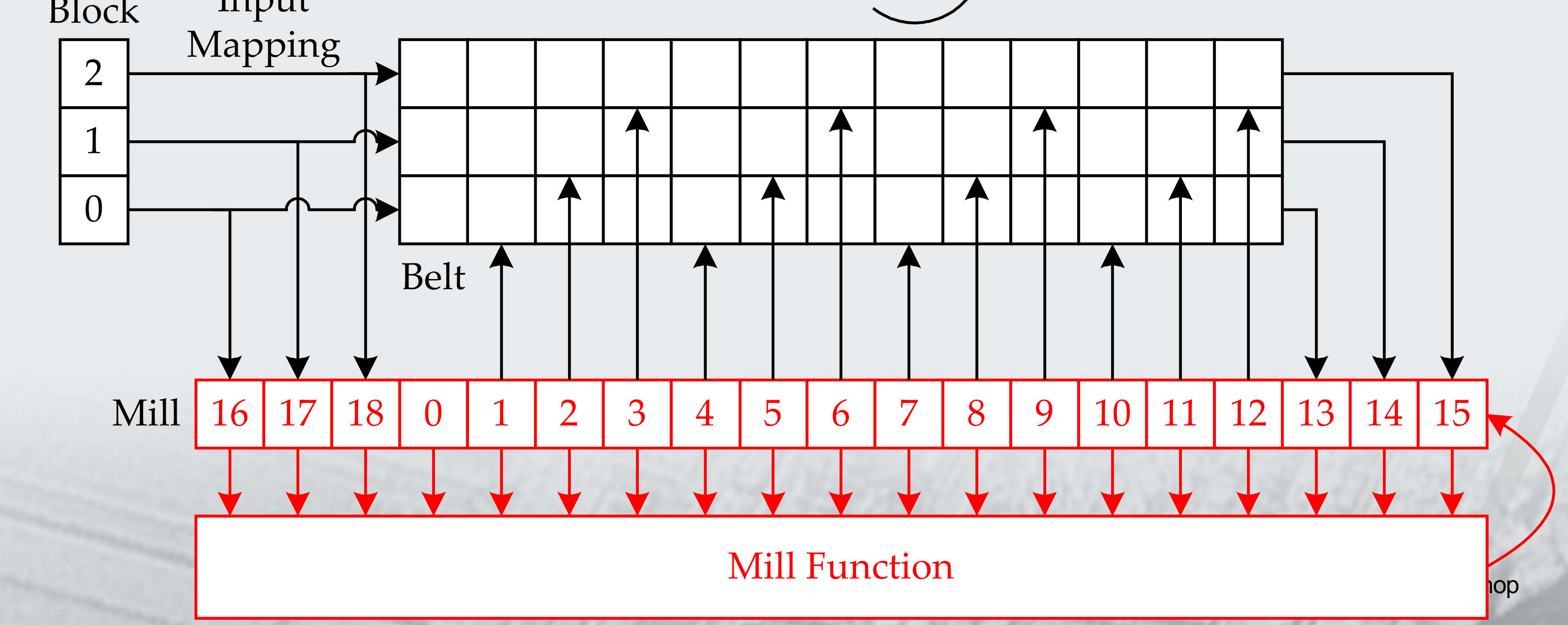

Mill
Belt
Input
mapping
Bell
Milt
Mill
function
Belt
function


Belt Function
Input
Block
Input
Mapping
2
1
0
Belt
Mill
16
17
18
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Mill Function

RadioGatún

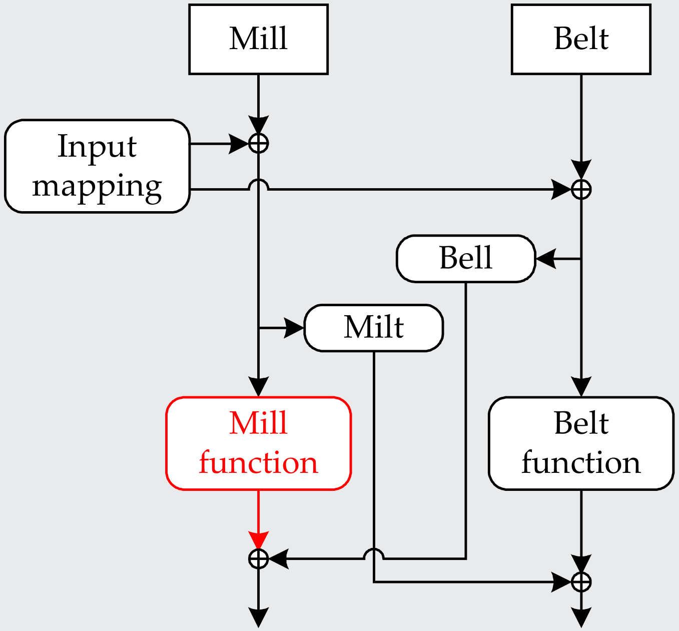
- The mill function contains:
  - Bitwise logical operations (XOR, AND, NOT)
  - Cyclic shifts

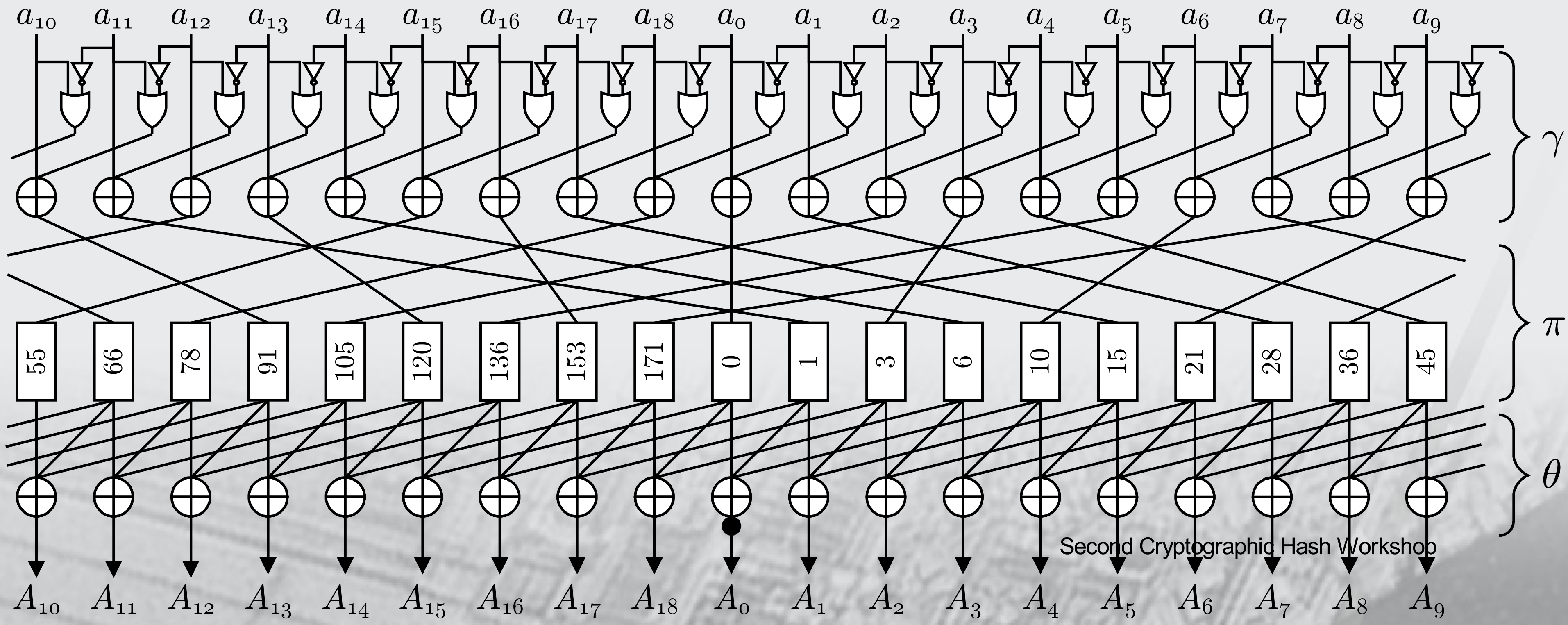




RadioGatún

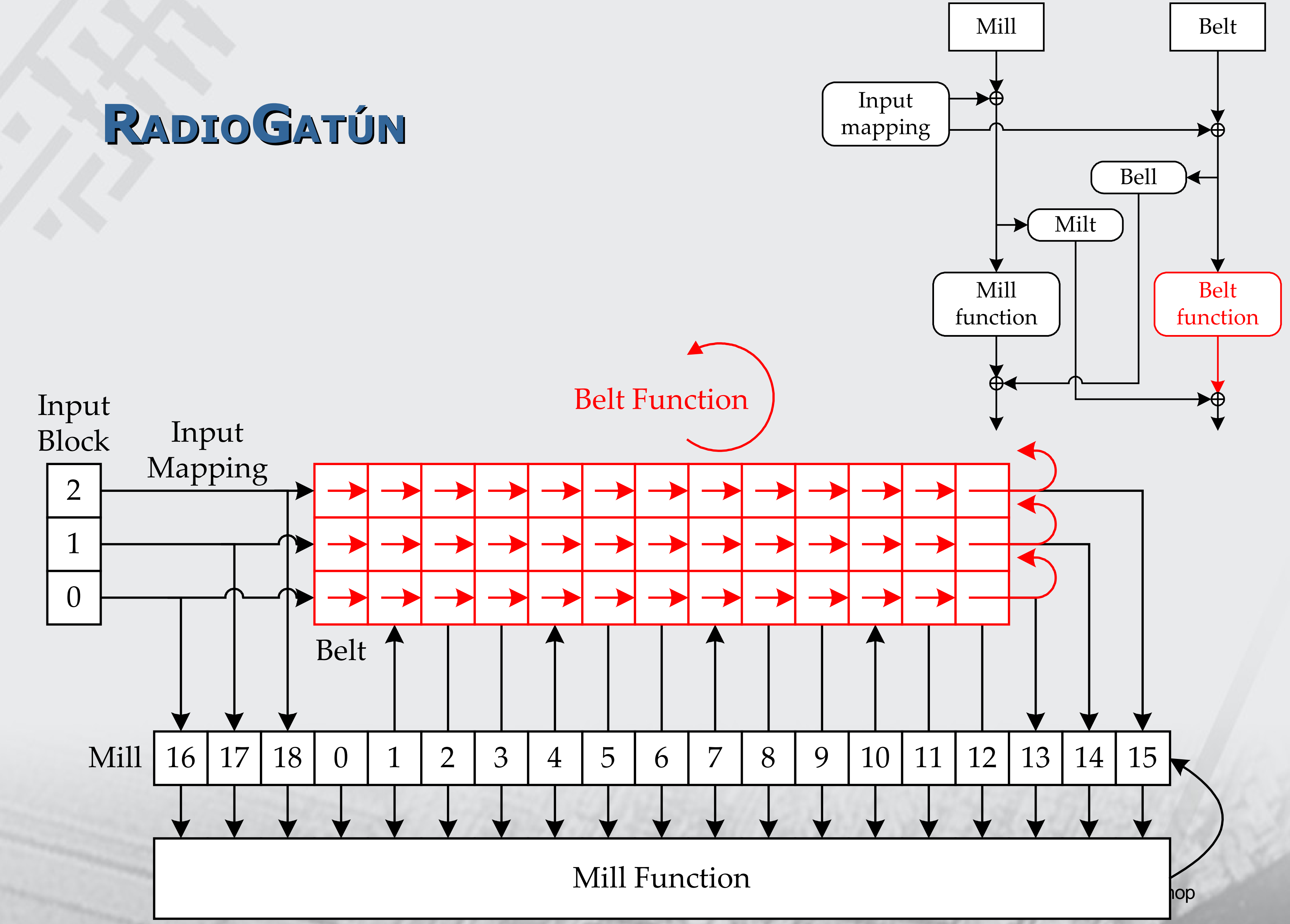
- The mill function contains:
  - Bitwise logical operations (XOR, AND, NOT)
  - Cyclic shifts



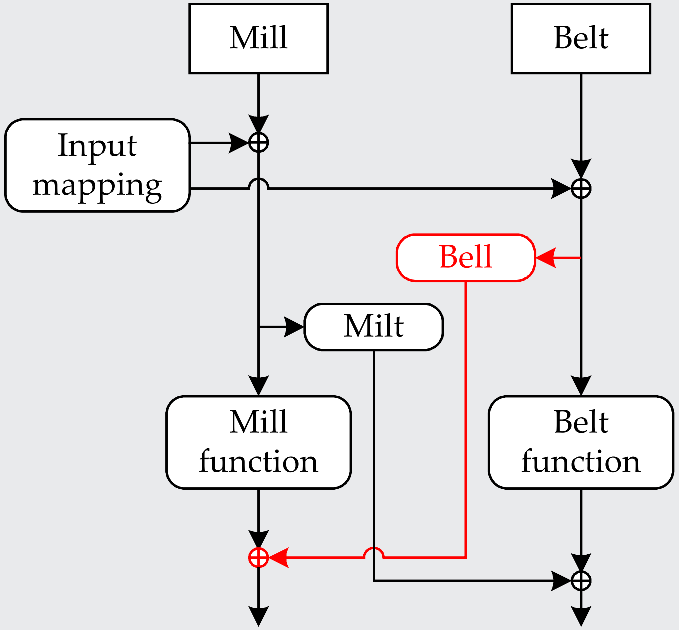


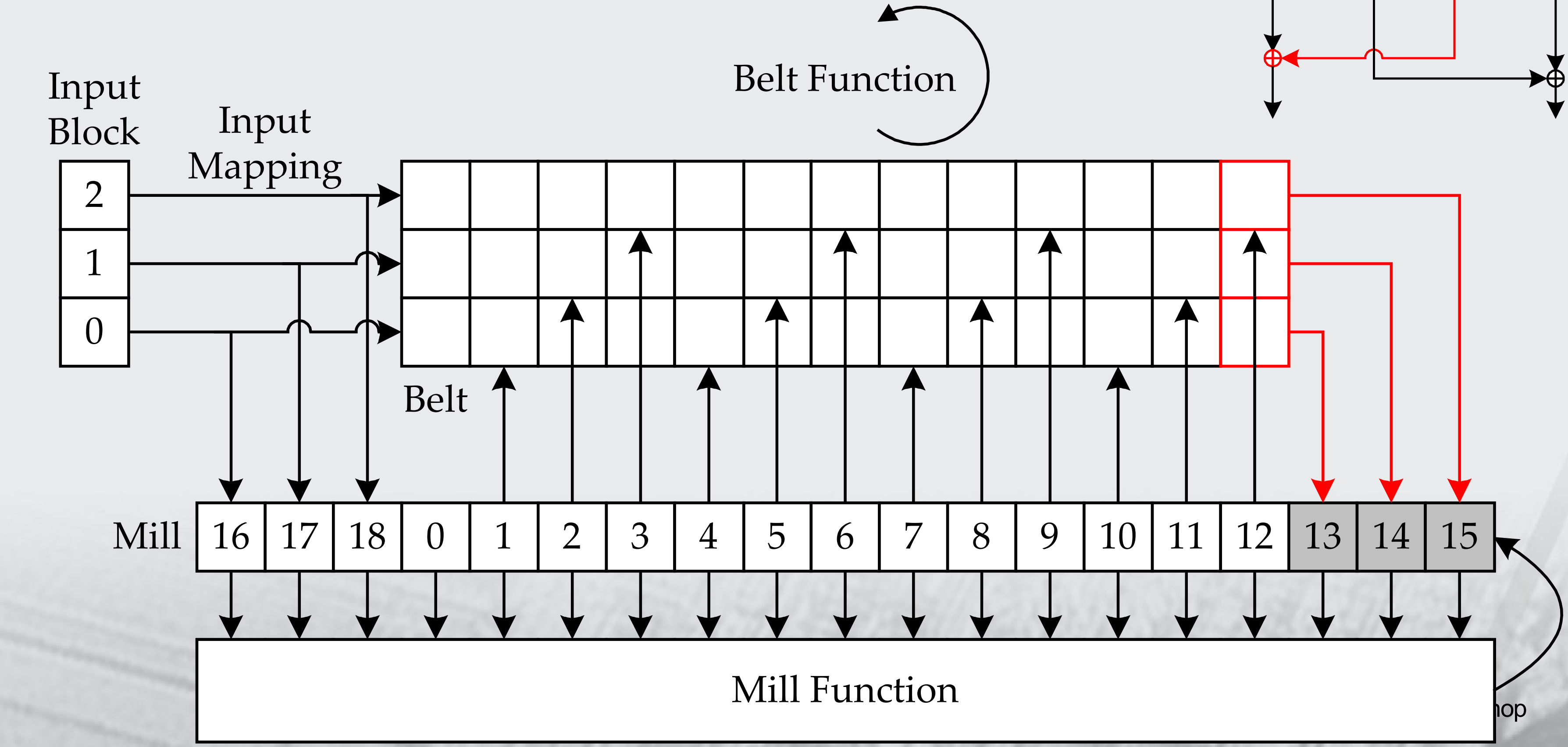
a_{10} a_{11} a_{12} a_{13} a_{14} a_{15} a_{16} a_{17} a_{18} a_0 a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9
γ
π
55 66 78 91 105 120 136 153 171 0 1 3 6 10 15 21 28 36 45
θ
A_{10} A_{11} A_{12} A_{13} A_{14} A_{15} A_{16} A_{17} A_{18} A_0 A_1 A_2 A_3 A_4 A_5 A_6 A_7 A_8 A_9

RadioGatún

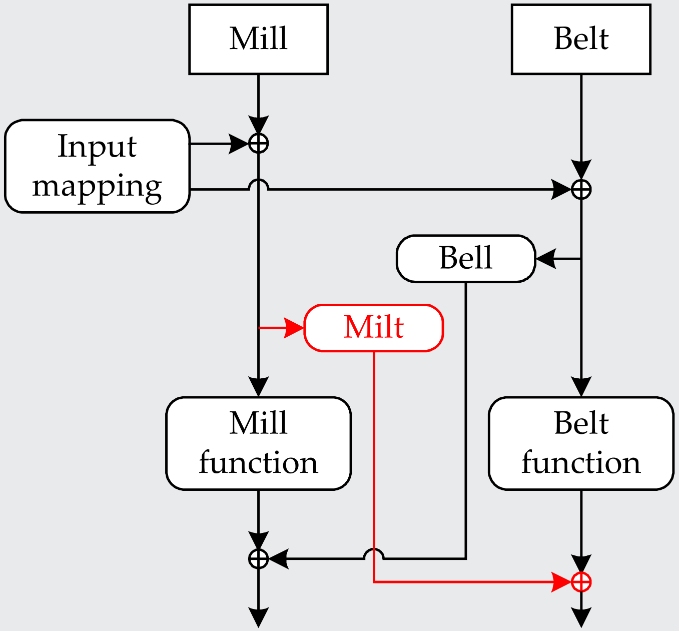

Mill
Belt
Input mapping
Bell
Milt
Mill function
Belt function
Belt Function
Input Block
2
1
0
Input Mapping
Belt
Mill
16
17
18
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Mill Function
hop

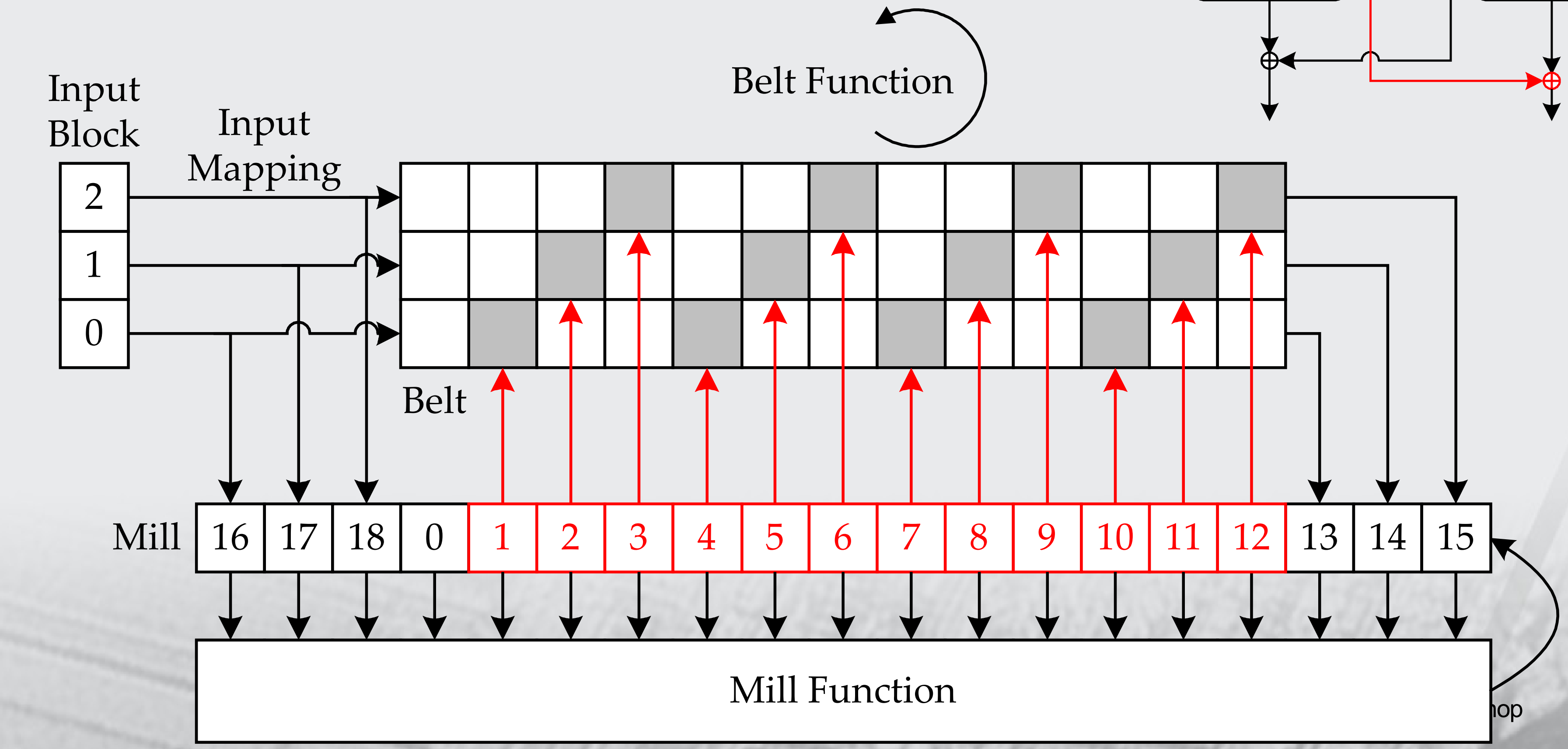
RadioGatún


Mill
Belt
Input mapping
Bell
Milt
Mill function
Belt function


Belt Function
Input Block
2
1
0
Input Mapping
Belt
Mill
16
17
18
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Mill Function
hop

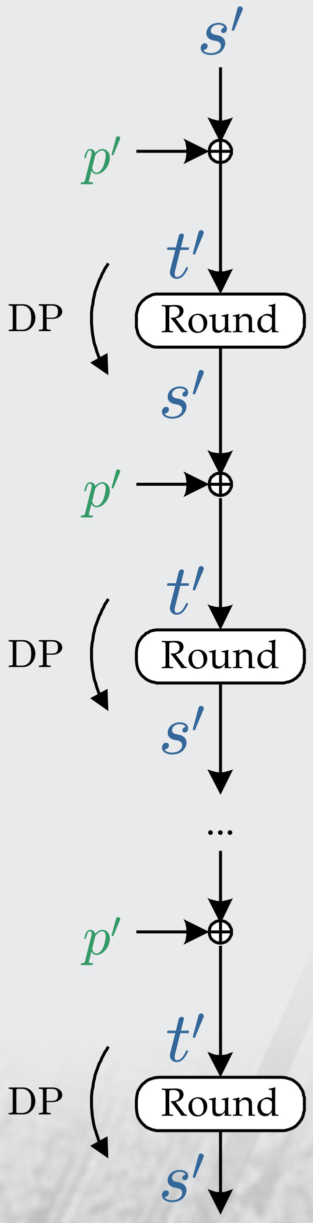
RadioGatún


Mill
Belt
Input mapping
Bell
Milt
Mill function
Belt function


Input Block
2
1
0
Input Mapping
Belt Function
Belt
Mill
16
17
18
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Mill Function
nop

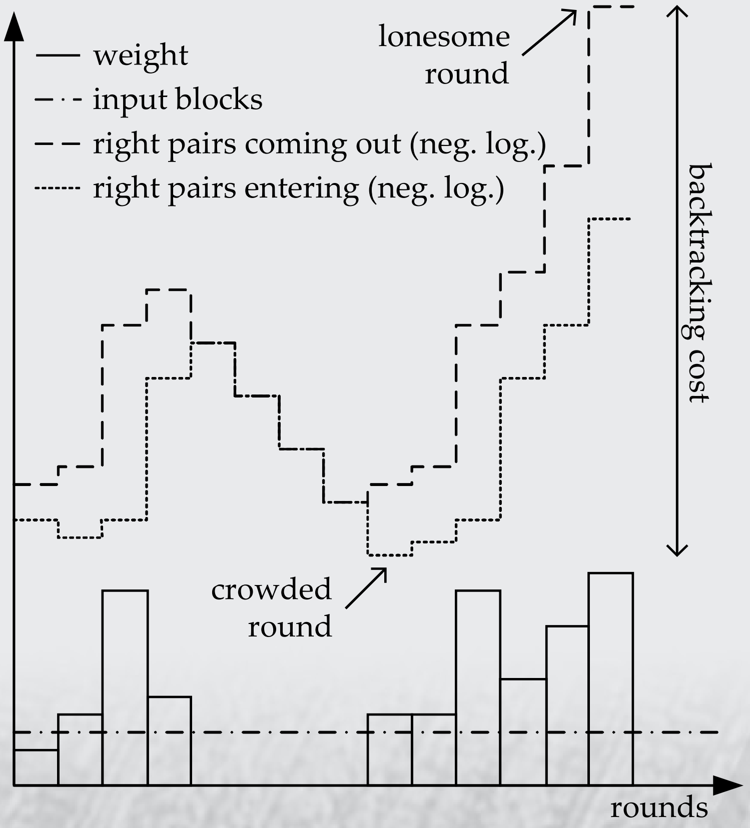
Differential trails

- Differential trail
  - State differences + input differences
  - Used to find an **internal collision**
- Weight
  - Negative (binary) logarithm of probability



Trail backtracking

- Propagate difference
  - Through each round
  - Only if right pair
  - weight > l_i : fraction thru
  - weight ≤ l_i : pair creation
- Complexity
  - Lonesome round
  - Crowded round
  - **Backtracking cost**
    - Also for algebraic attacks



Analysis

- RadioGatún[1, 2, 4, …] useful for analysis
  - **Explicit** search of collisions
  - Differential trails with lowest complexity
    - Trail for RadioGatún[1] extends to RadioGatún[n]
  - Symmetry destroyed in the mill
    - Specific trails for RadioGatún[n] may exist with lower cost
- Other aspects
  - Fixed points
  - Algebraic attacks on RadioGatún[1, 2, 3, 4, …, 64]
- Ongoing
  - Prove bounds

Performance

- Extremely fast in hardware
- Fast in software

Dell Precision 670 with Intel Xeon 3GHz (in Mbyte/sec)	Windows (32 bits) Visual Studio 2005	Linux (x86_64) GCC 3.3.5
SHA-1	90	91
SHA-256	65	80
Panama	480	288
RadioGatún[32]	**120**	175
RadioGatún[64]	55	**270**

Conclusion

- Belt-and-mill structure
  - Simplicity (analysis)
- RadioGatún
  - Performance
  - Existence of toy cipher (analysis)
  - No patent
- Analysis ongoing
- Do not hesitate to attack!
  - See security claims in RadioGatún paper

http://radiogatun.noekeon.org