RadioGatún, a belt-and-mill hash function

Guido Bertoni, Joan Daemen,
Michaël Peeters* and Gilles Van Assche

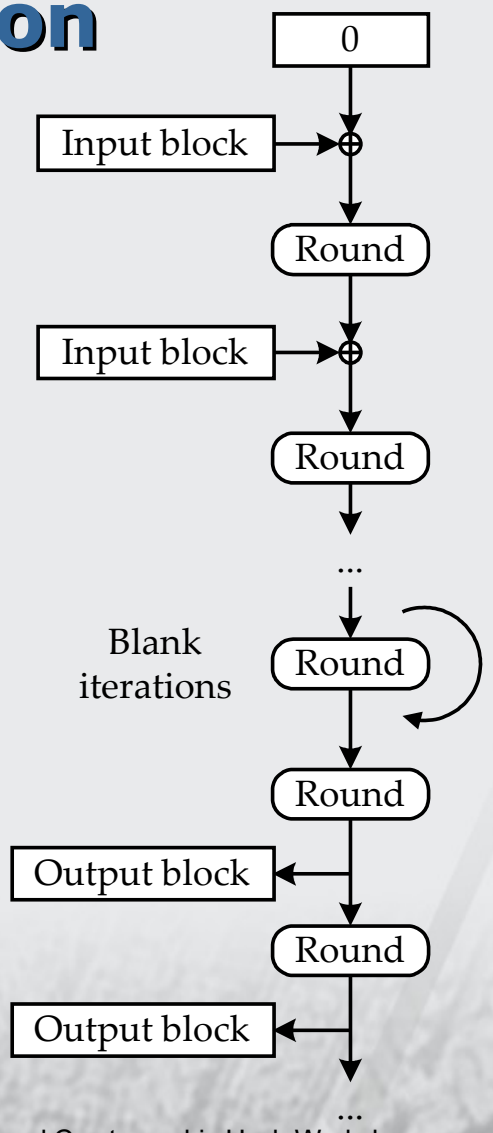
STMicroelectronics **De Valck Consultants*

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

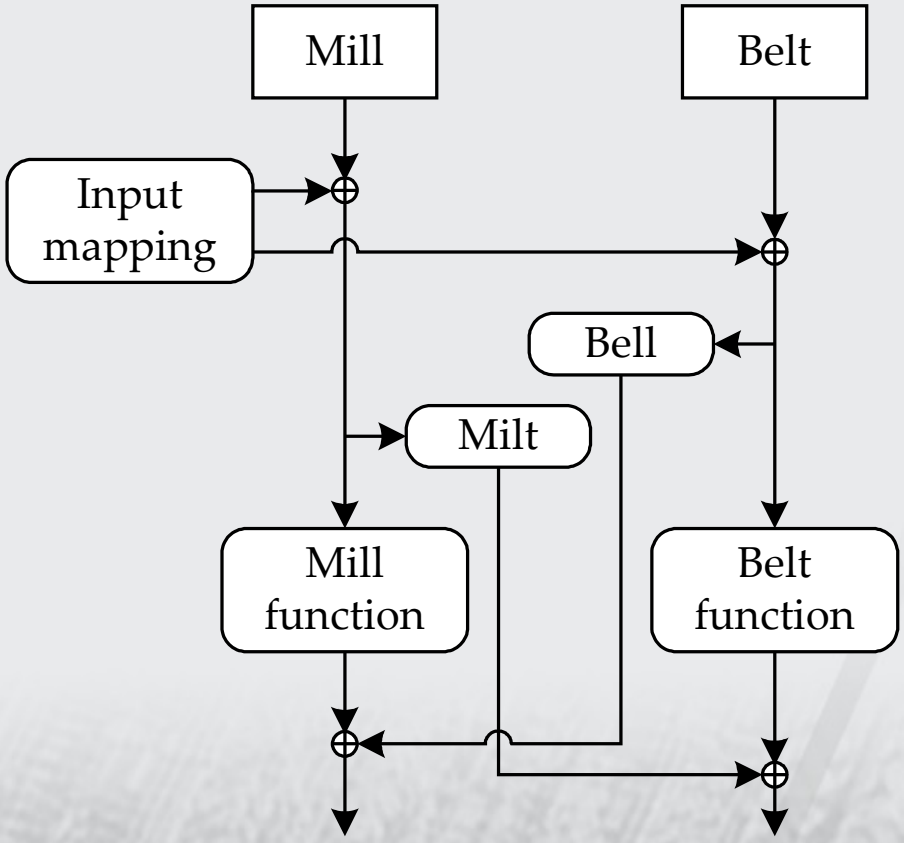
Alternating-input construction

- 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



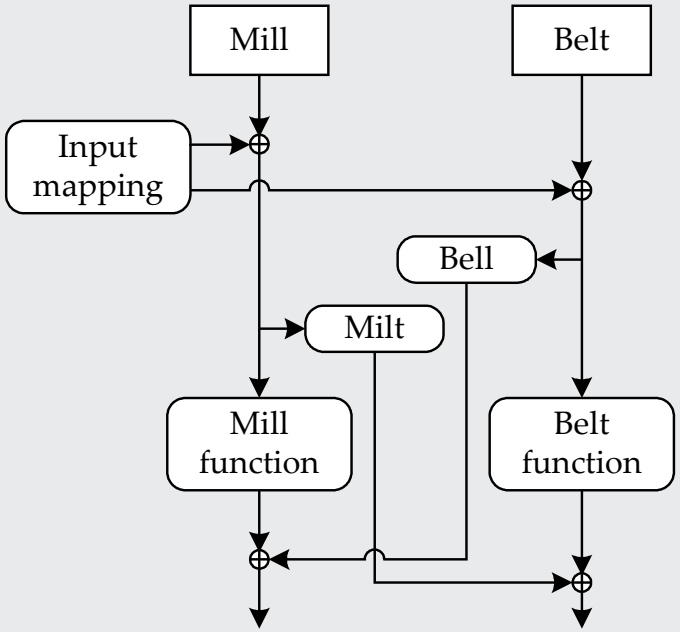
Belt-and-mill structure

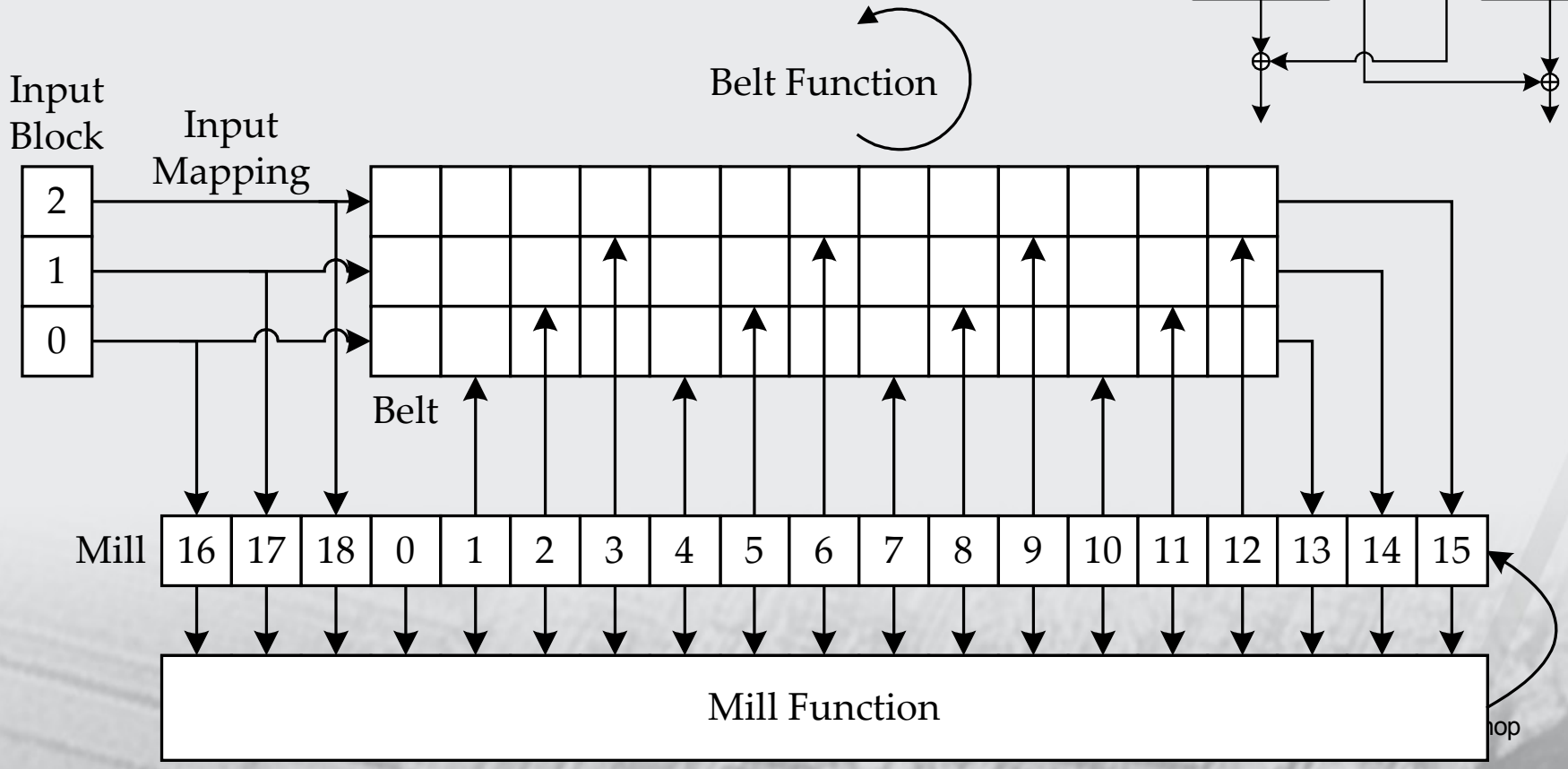
- State = (**mill**, **belt**)
- Mill function
  - **Non-linear** function
  - Diffusion and confusion
- Belt function
  - Linear function
  - **Long-term diffusion**
- Belt-to-mill + mill-to-belt
  - **Bell + milt**
  - Linear mappings



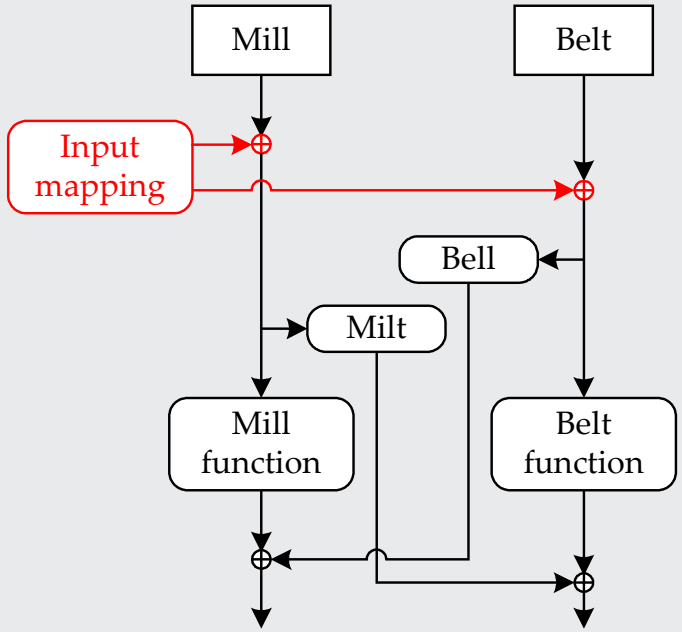
RadioGatún

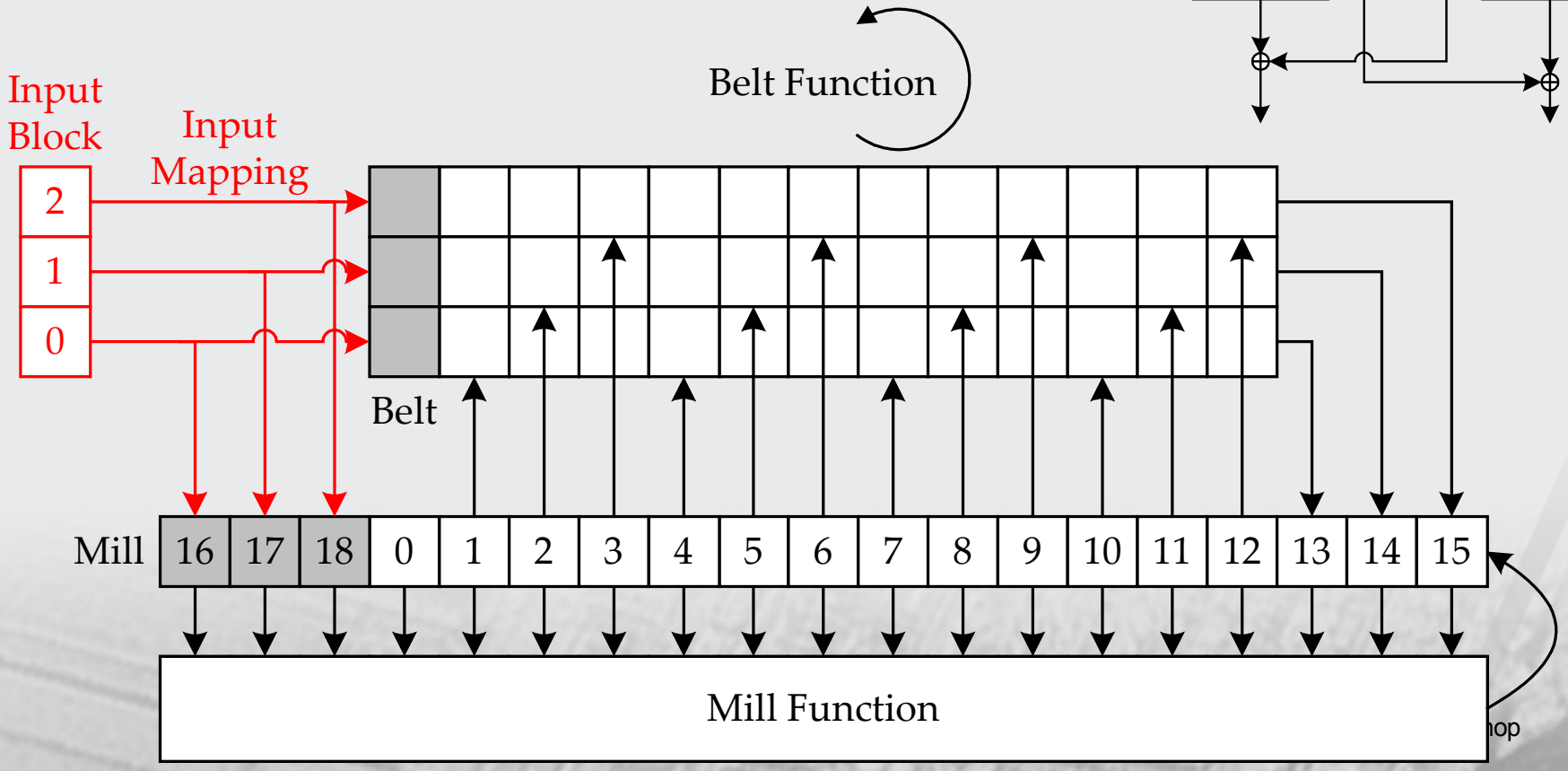
- Parameter: **word size**
  - RadioGatún[32]
  - RadioGatún[64]





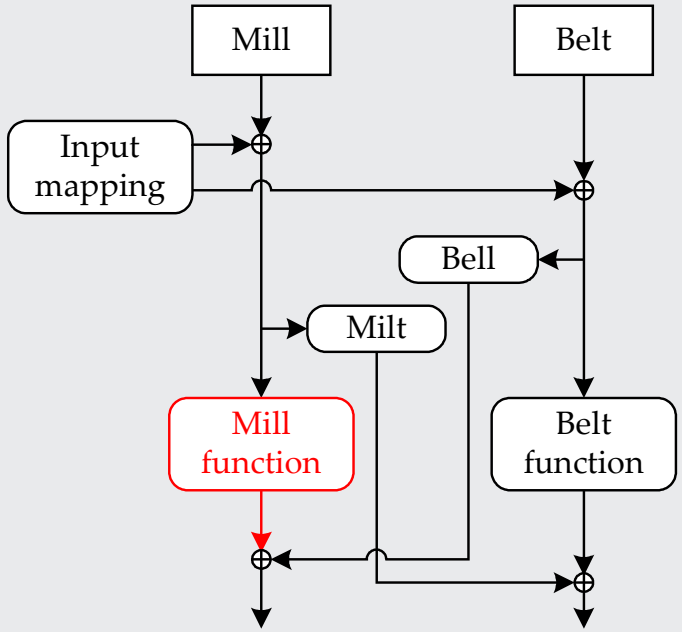
RadioGatún

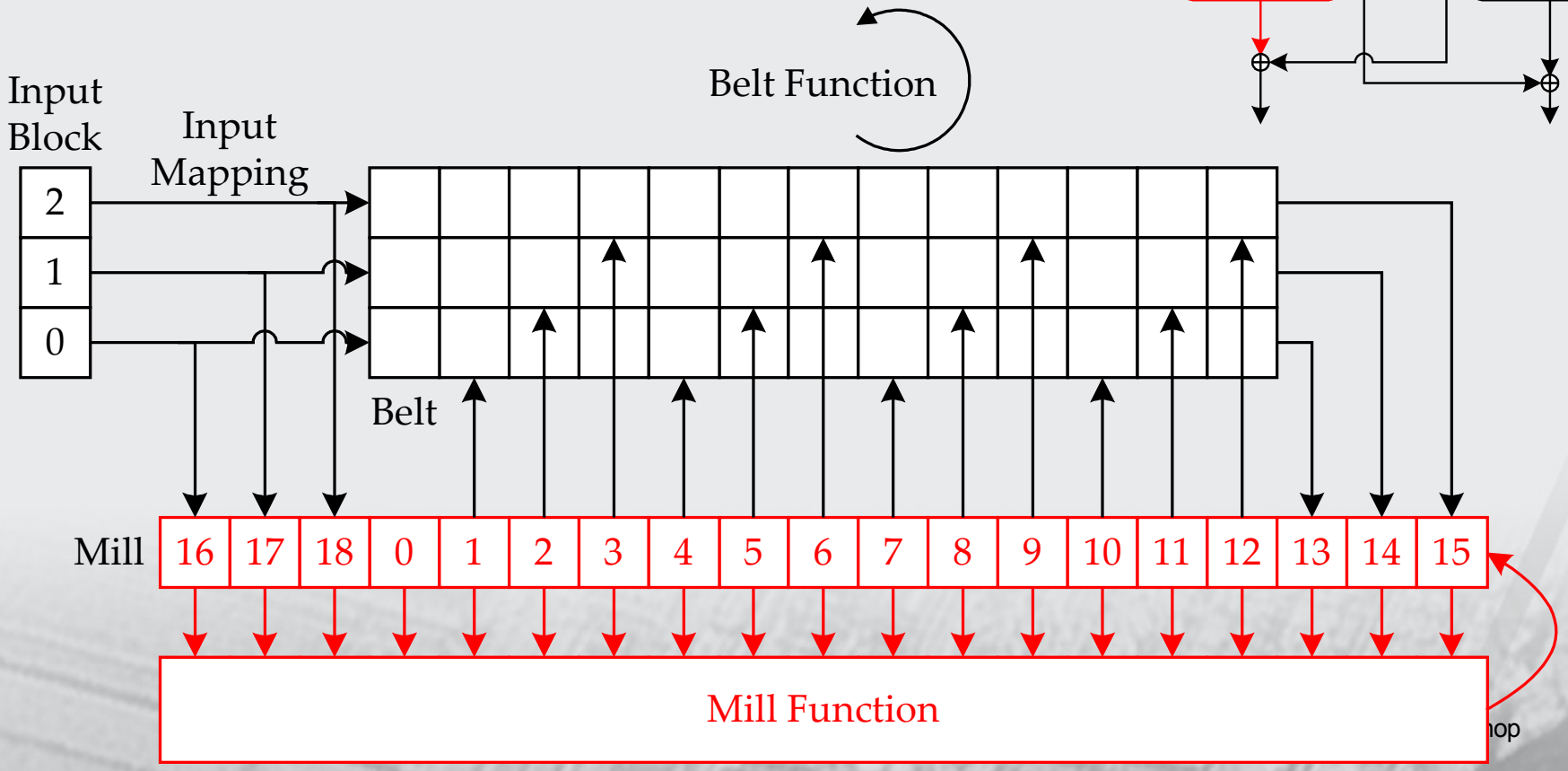

Mill
Belt
Input mapping
Bell
Milt
Mill function
Belt function


Input Block
Input Mapping
Belt Function
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

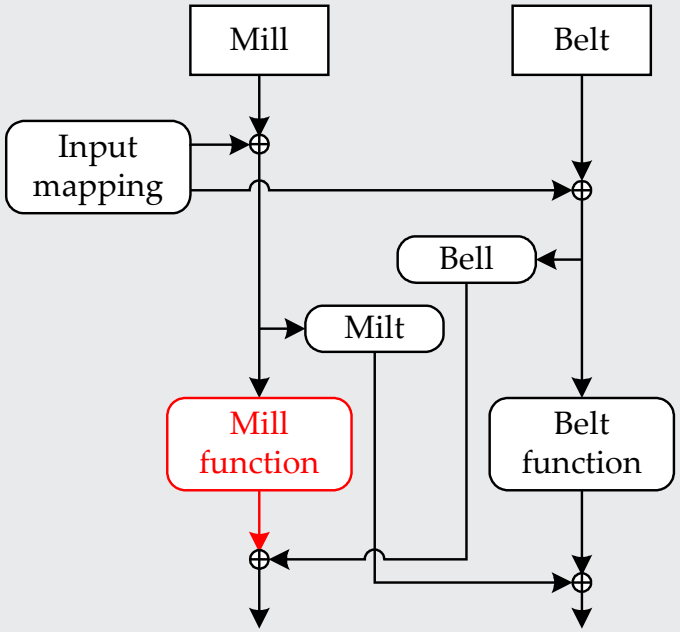
- The mill function contains:
  - Bitwise logical operations (XOR, AND, NOT)
  - Cyclic shifts

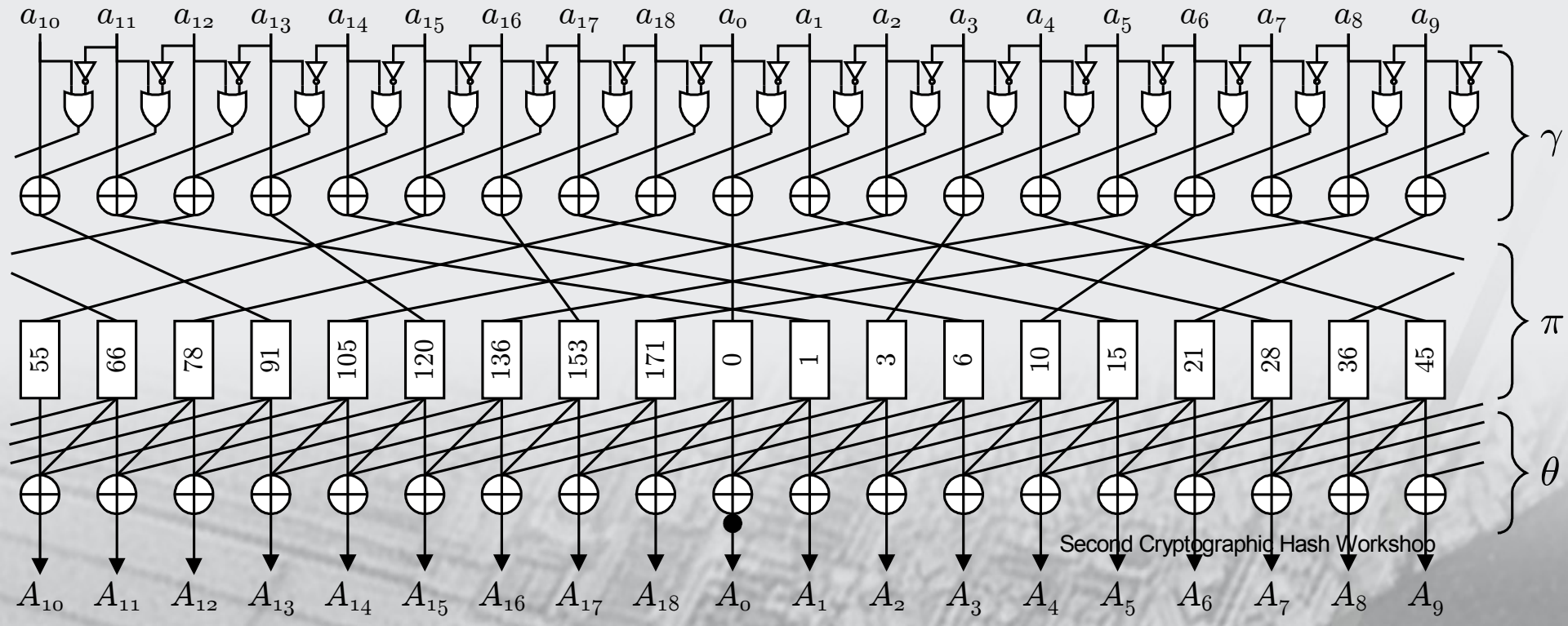




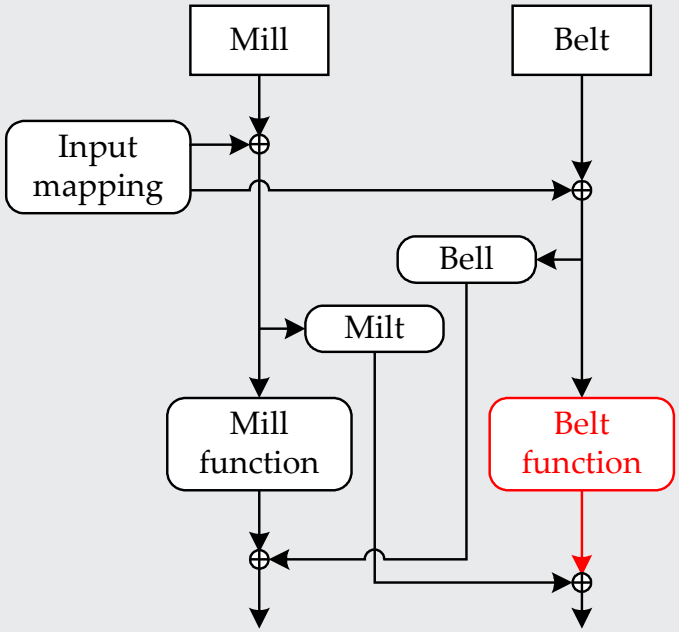
RadioGatún

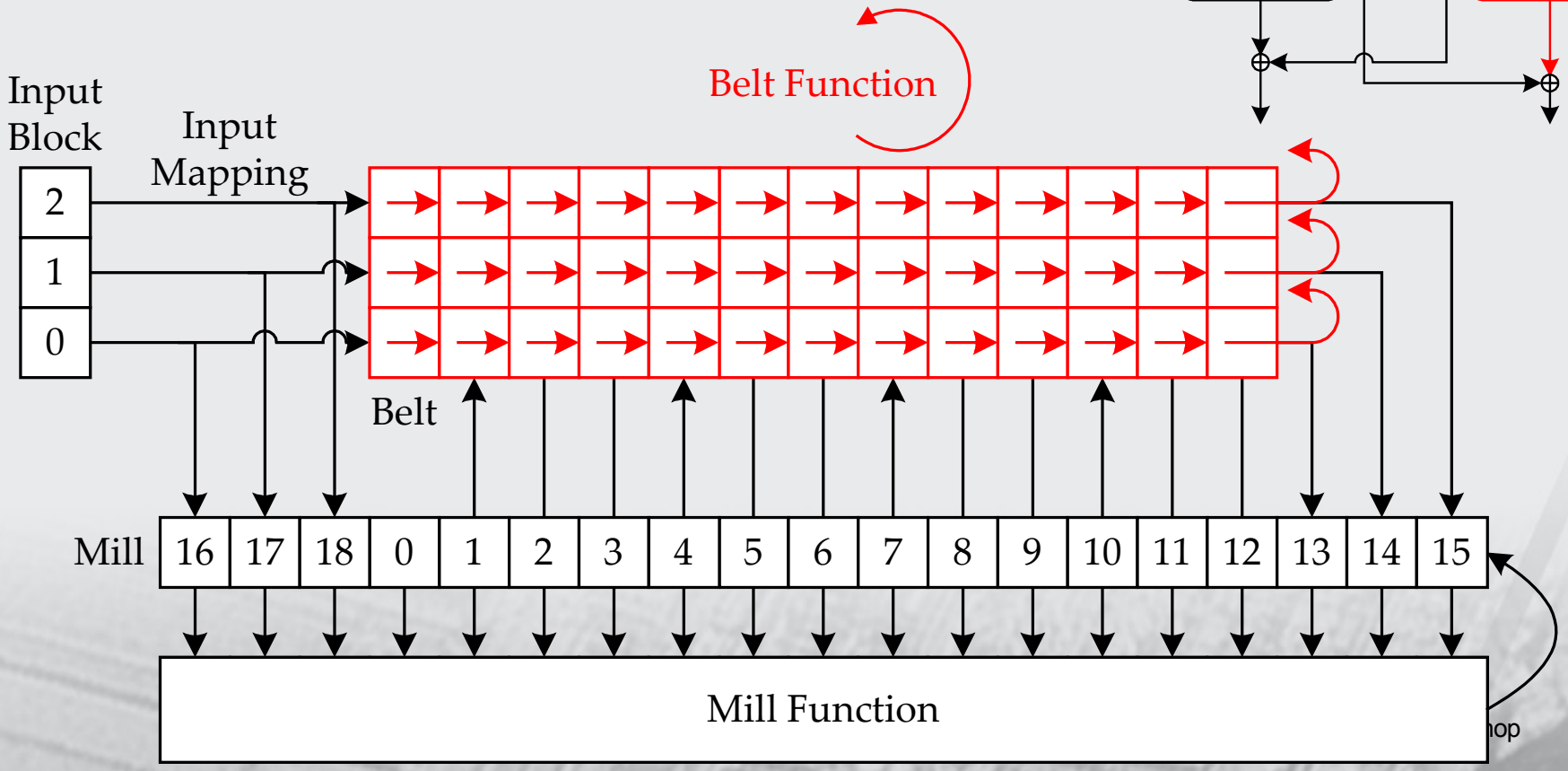
- The mill function contains:
  - Bitwise logical operations (XOR, AND, NOT)
  - Cyclic shifts



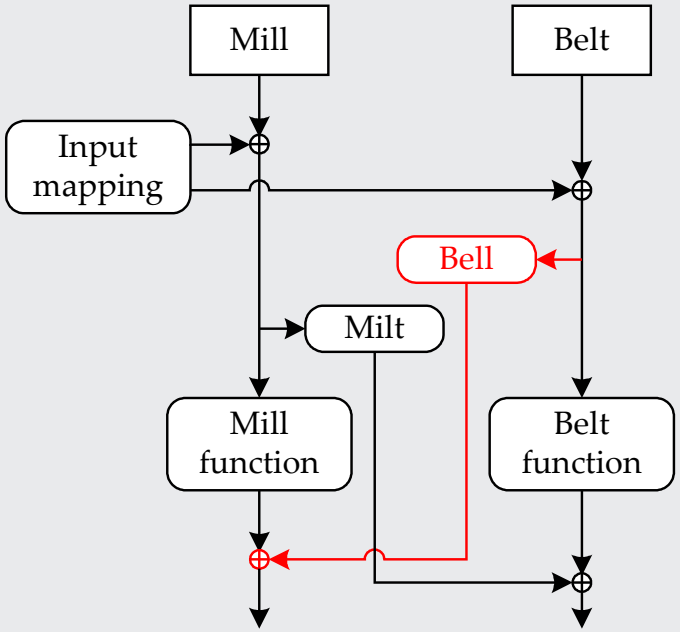


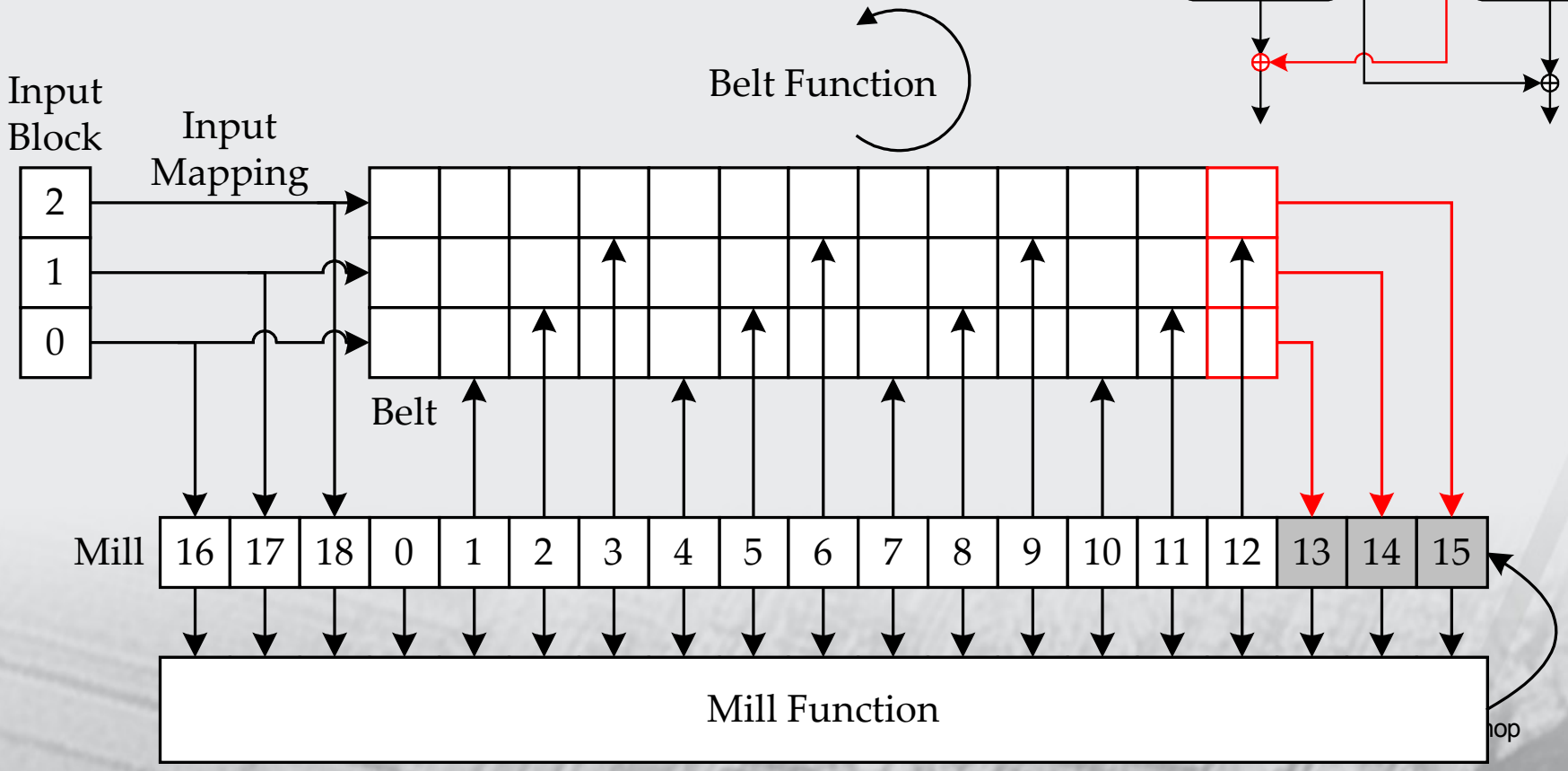
RadioGatún


Mill
Belt
Input mapping
Bell
Milt
Mill function
Belt function

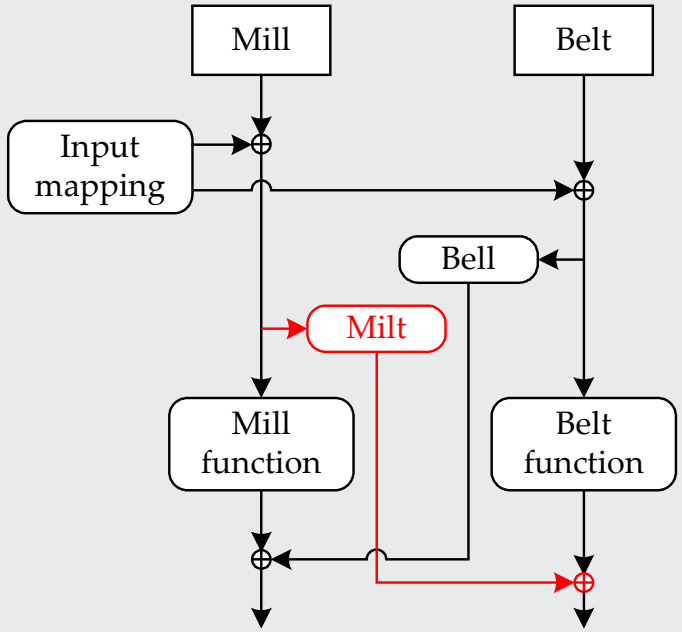

Input Block
Input Mapping
Belt Function
2
1
0
Belt
Mill
16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Mill Function

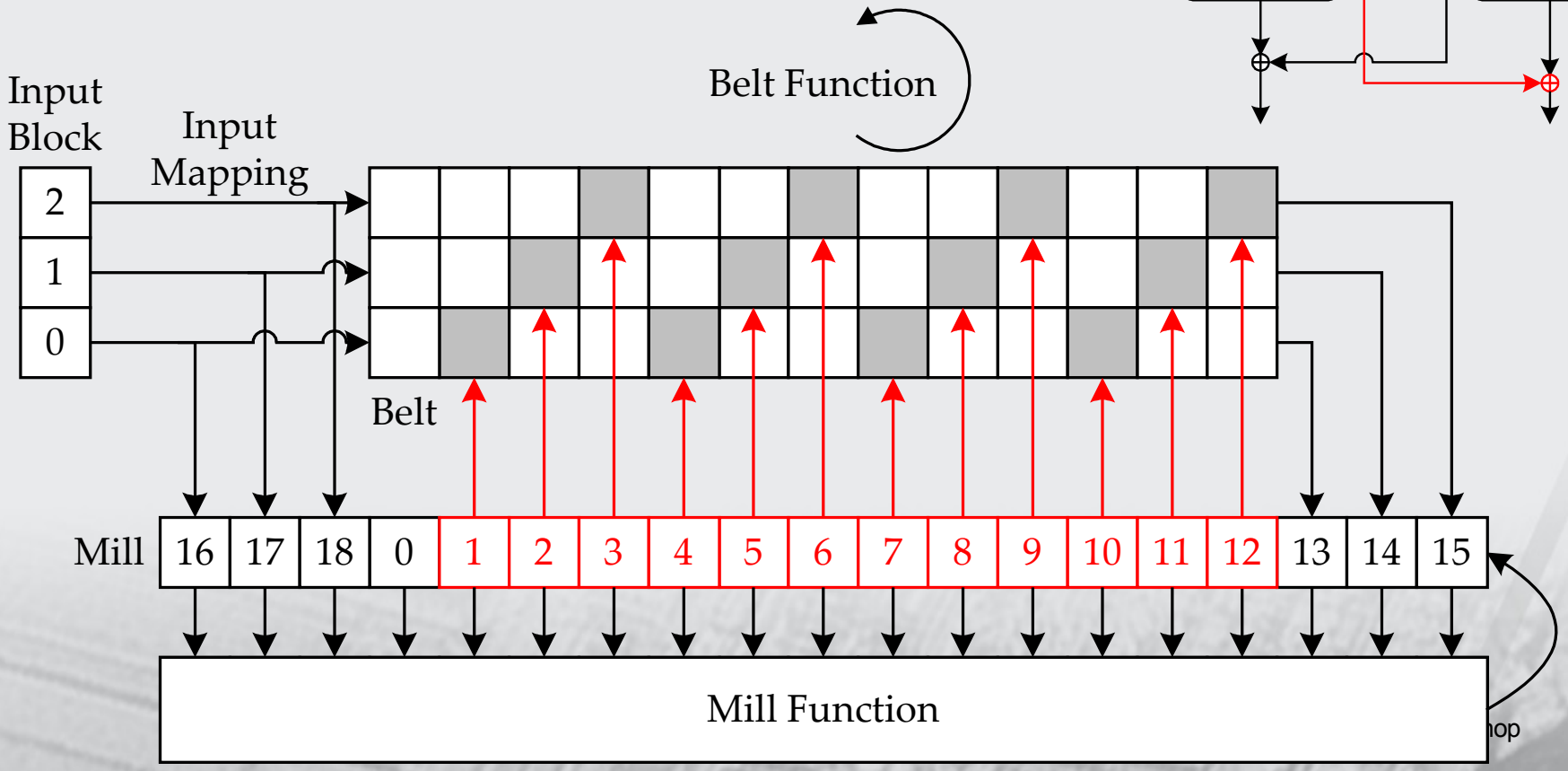
RadioGatún


Mill
Belt
Input mapping
Bell
Milt
Mill function
Belt function


Input Block
Input Mapping
Belt Function
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

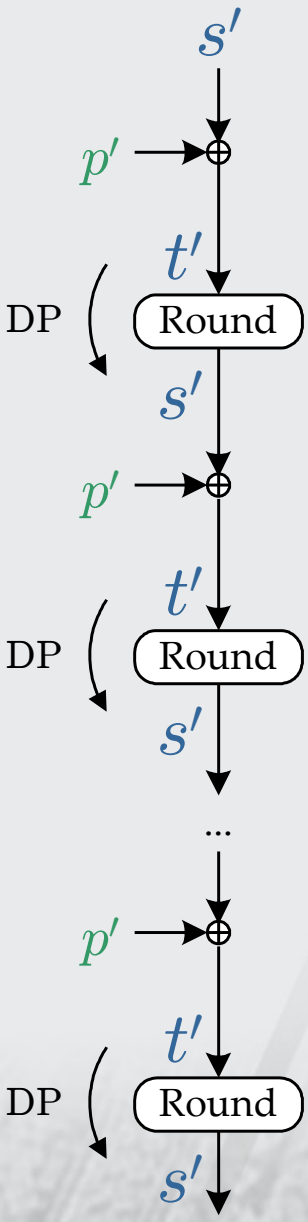
RadioGatún


Mill
Belt
Input mapping
Bell
Milt
Mill function
Belt function


Input Block
Input Mapping
Belt Function
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

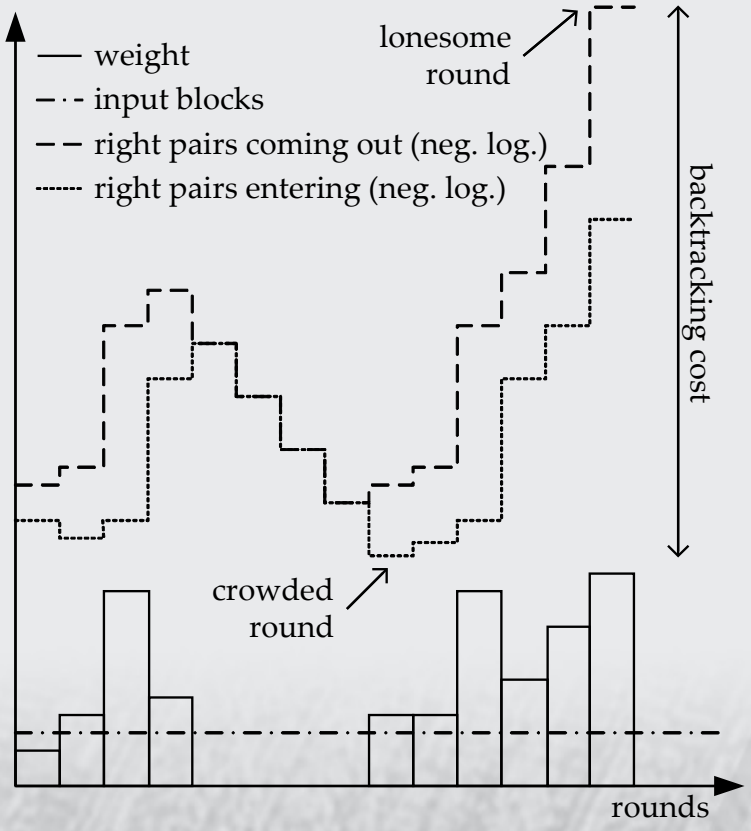
Differential trails

- 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
  - $\mathrm{weight} > l_i$: fraction thru
  - $\mathrm{weight} \leq l_i$: 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