Better than Brute-Force
Optimized Hardware Architecture for Effcient **Biclique Attacks on AES-128**

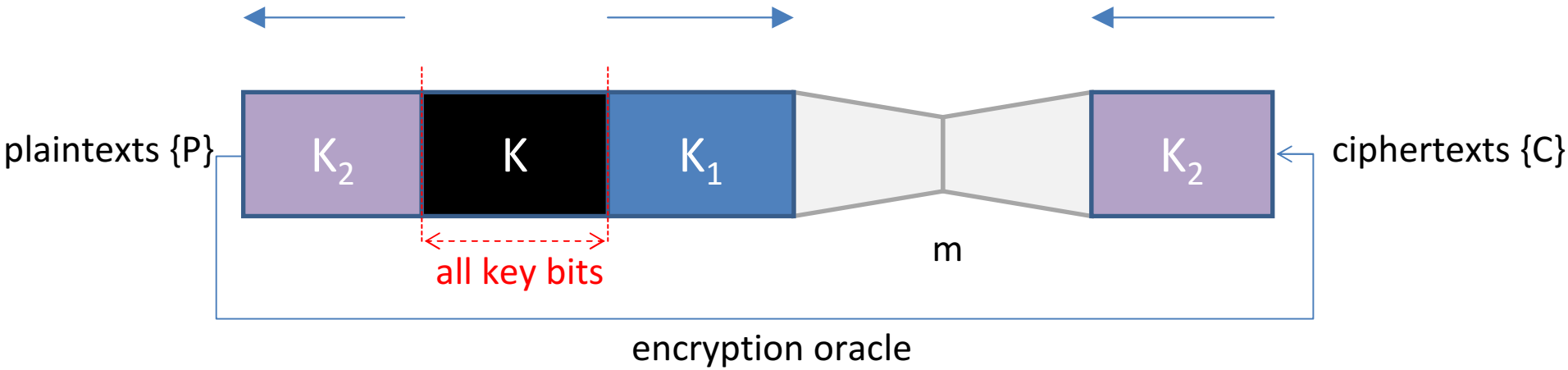
Andrey Bogdanov*, Elif Bilge Kavun**, Christof Paar**,
Christian Rechberger***, Tolga Yalcin**

* KU Leuven, Belgium, ** HGI-RUB, Germany, *** DTU, Denmark

Overview

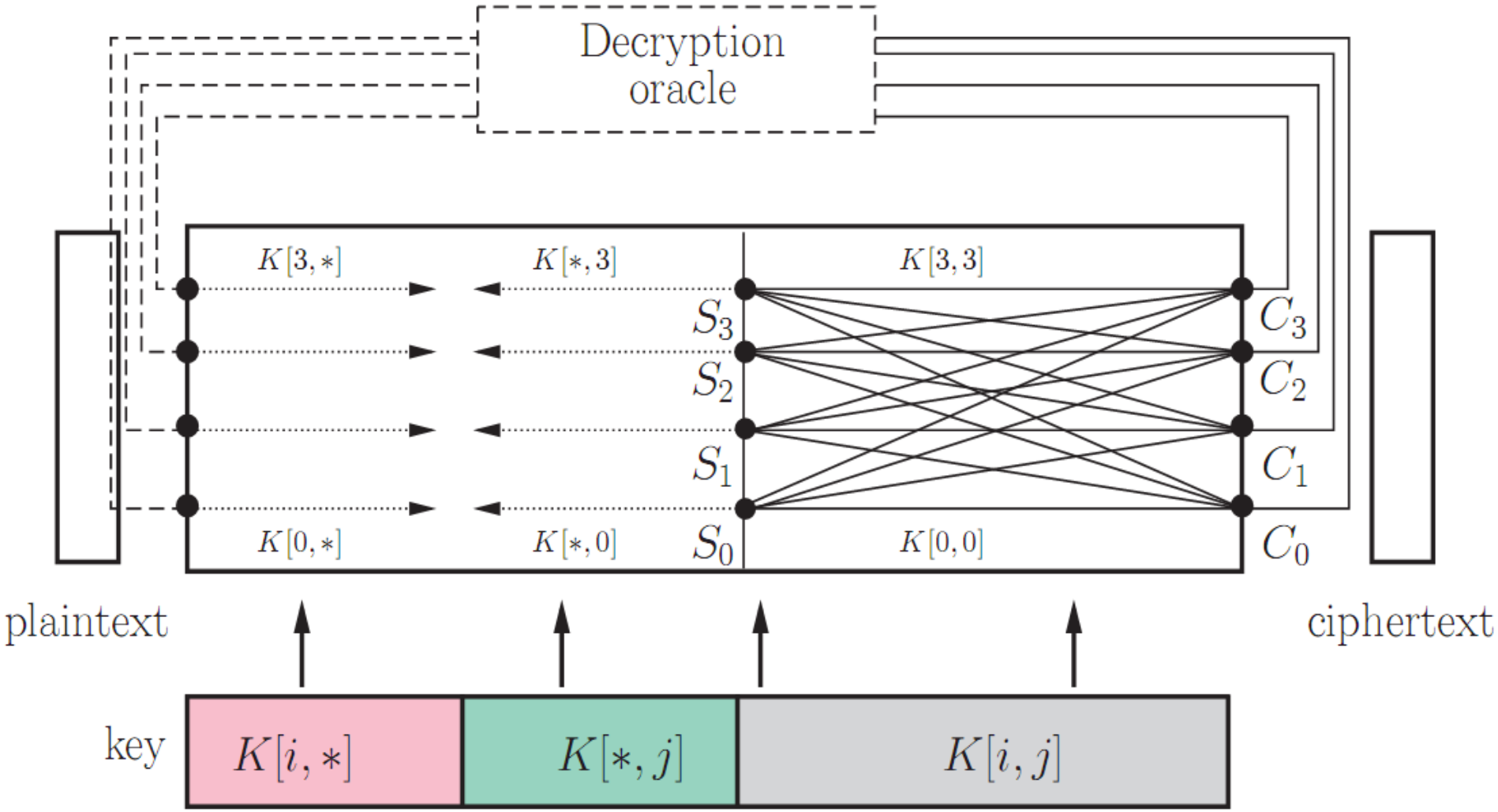
- Meet-in-the-Middle with Bicliques
- Low Data Complexity Biclique Cryptanalysis of AES-128
- Optimized Brute Force Attack on AES-128
  - on FPGA
  - on ASIC
- Biclique Attack on AES-128
  - on FPGA
  - on ASIC
- Conclusion

MITM with Bicliques



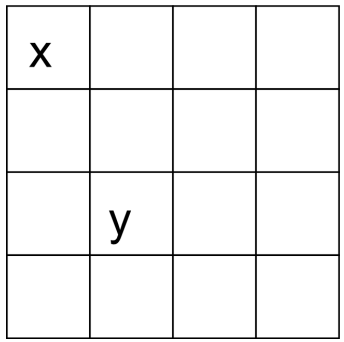
- Allow all key bits affect a part of the cipher
- Stick to a structure to enable efficient enumeration of keys and states in this part
- Structure = **biclique!**

MITM with Bicliques



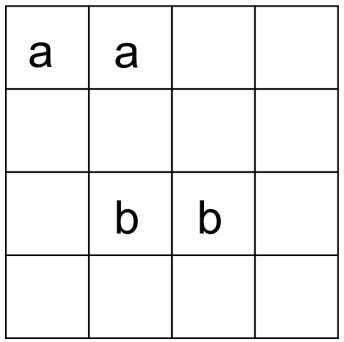
Low Data Complexity Biclique Cryptanalysis of AES-128

- Start modifications in the first round of AES-128
- Divide entire space of 2^{128} keys into of 2^{124} non-overlapping groups of 2^4 keys
- Fix a base key and enumerate all other keys in the key group



$x = (x_0x_1x_2x_3x_4x_500)_2$

$y = (y_0y_1y_2y_3y_4y_500)_2$

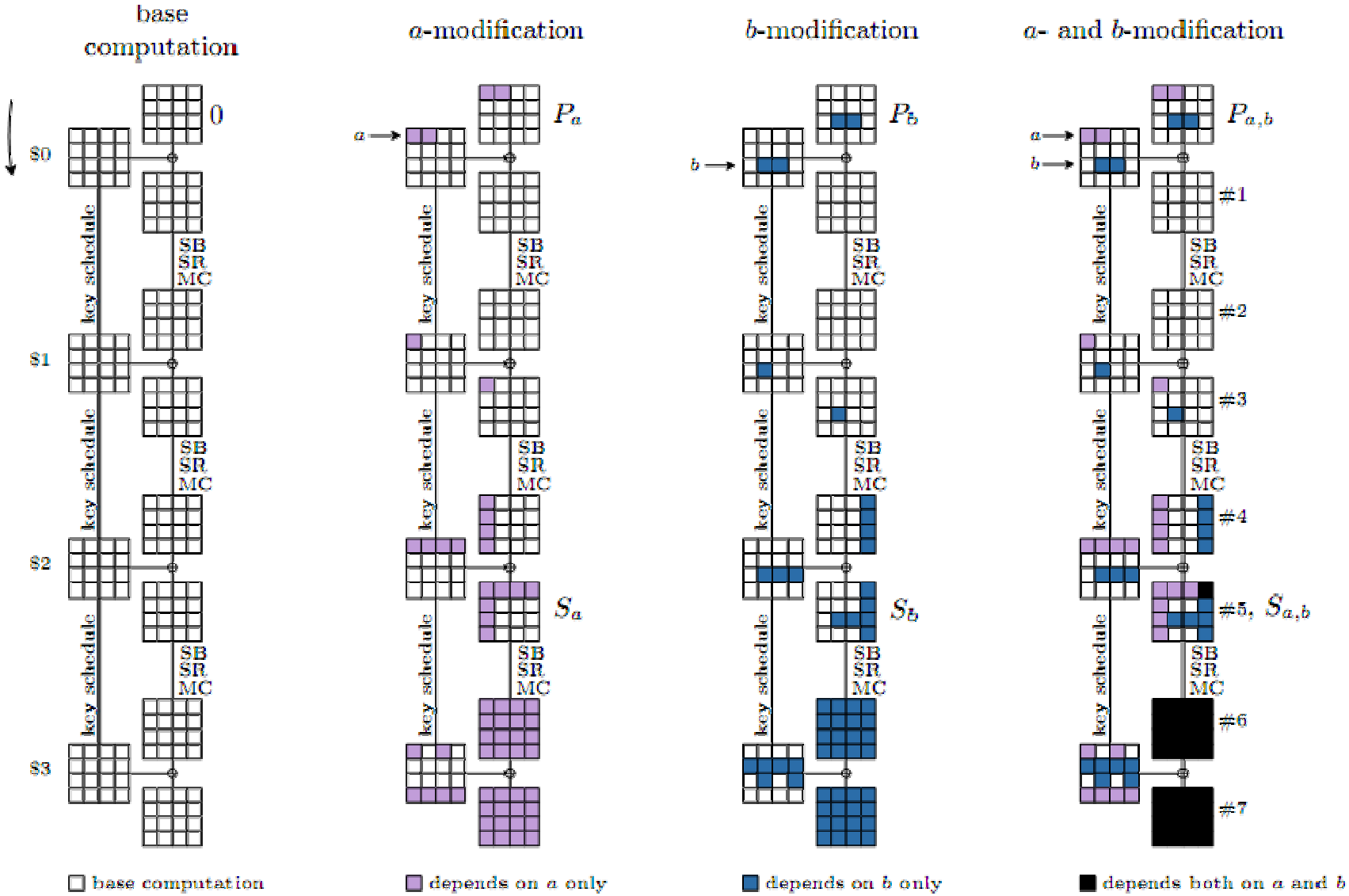


$a = (000000a_1a_0)_2$

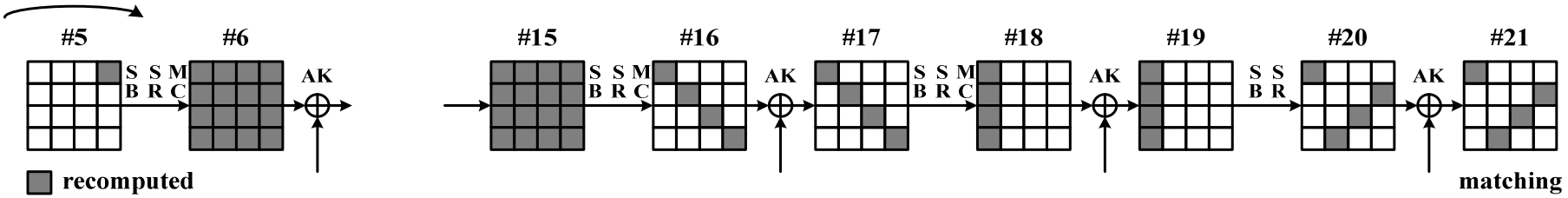
$b = (000000b_1b_0)_2$

- Modify base key at two byte positions independently (in 2^2 ways each)
- Follow propagation of modifications forwards and backwards

Low Data Complexity Biclique Cryptanalysis of AES-128



Low Data Complexity Biclique Cryptanalysis of AES-128



Recomputation at matching

Low Data Complexity Biclique Cryptanalysis of AES-128

Complexities:

- Computational complexity to precompute all states S_a and S_b in each key group: 0.3 AES-128 runs (first step).
- About 7.12 AES-128 runs to test all 16 keys in the key group (second step).
- Negligible computation complexity (2^{-32}) for false positives
- *Overall computation complexity:*

  $2^{124}(0.3 + 7.12) = 2^{126.89}$ AES executions.

- *Data complexity:*

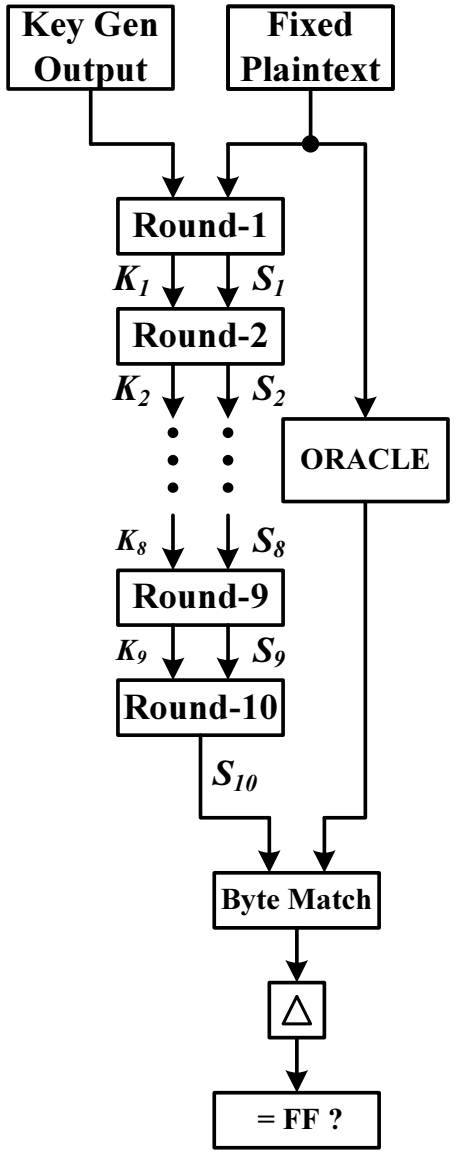
  Only 16 chosen plaintexts!!

Implementation

- FPGA target platform: RIVYERA Computing Cluster
  - 128 Xilinx Spartan3 XC3S500 high performance FPGAs
  - Equivalent computing power of 640 million system gates
- ASIC target technology: NANGATE
  - 45 nm Generic Library

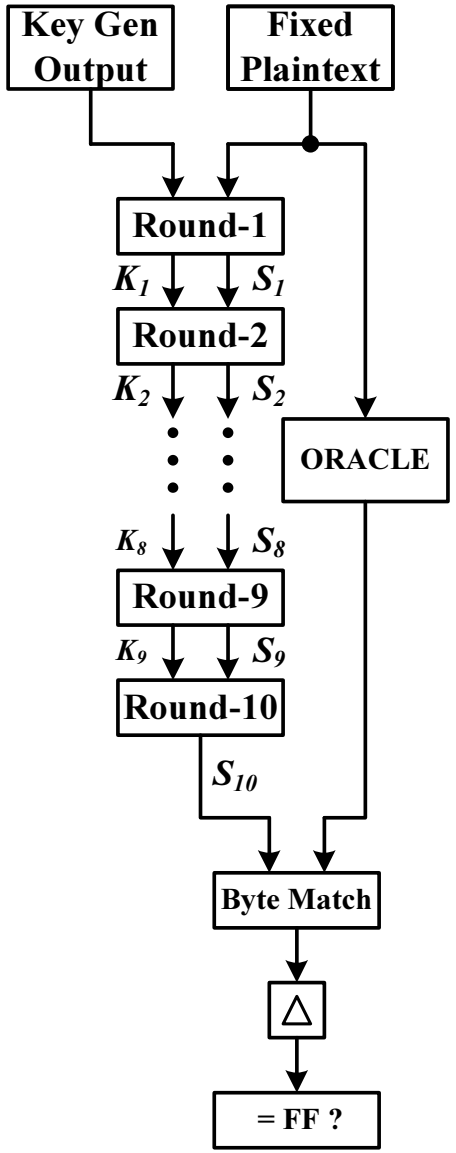
Optimized Brute-Force Attack on AES-128

- Highly pipelined architecture for highest possible speed (11-stage pipeline within each AES round)
- Composite field inverters over GF((2²) ²) ² for s-boxes
- Register based (RAMless) design – suitable for both FPGA and ASIC implementation

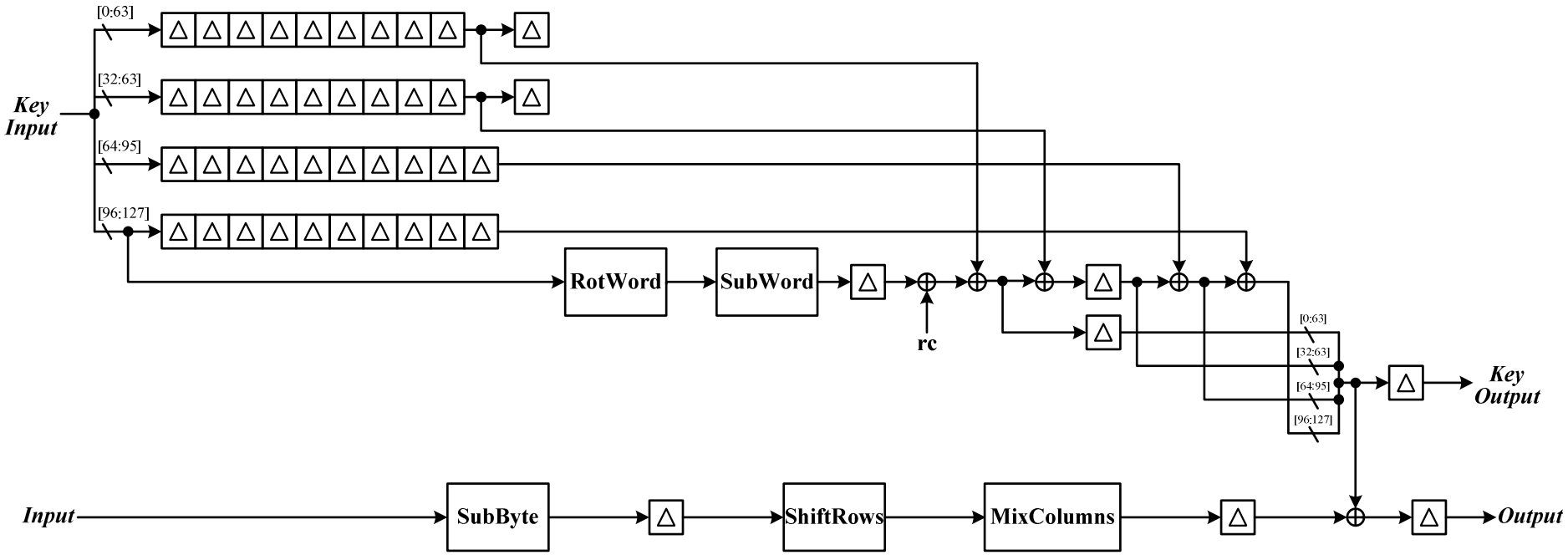


Optimized Brute-Force Attack on AES-128

- Design implemented in two favors:
  - All identical rounds (for a fair comparison with respect to the original biclique advantage figures)
  - Partial matching in the last three rounds (for better area utilization – makes no difference for FPGA)
- Smaller and faster than the reported fastest design (362*KGE* vs 660*KGE* and 2.5*GHz* vs 2*GHz*)

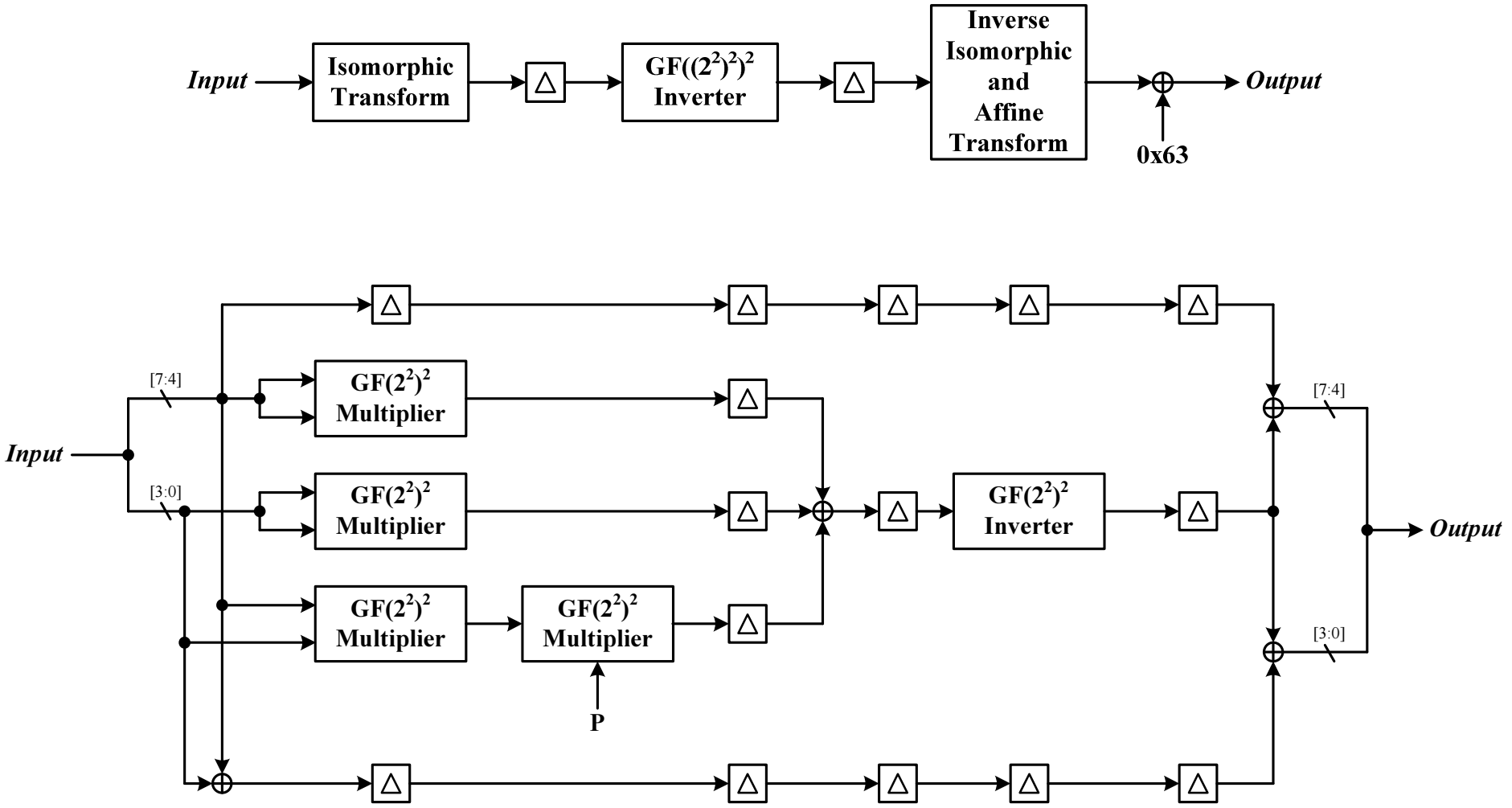


Optimized Brute-Force Attack on AES-128



* Pipeline register cost negligible for FPGA implementation – already part of the slice!

Optimized Brute-Force Attack on AES-128



Optimized Brute-Force Attack on AES-128

FPGA Performance

Slice Utilization	% FPGA Utilization	Maximum Freq (MHz)	Keys tested/sec/FPGA
26949 / 33278	80.98	263.16	526×10^6

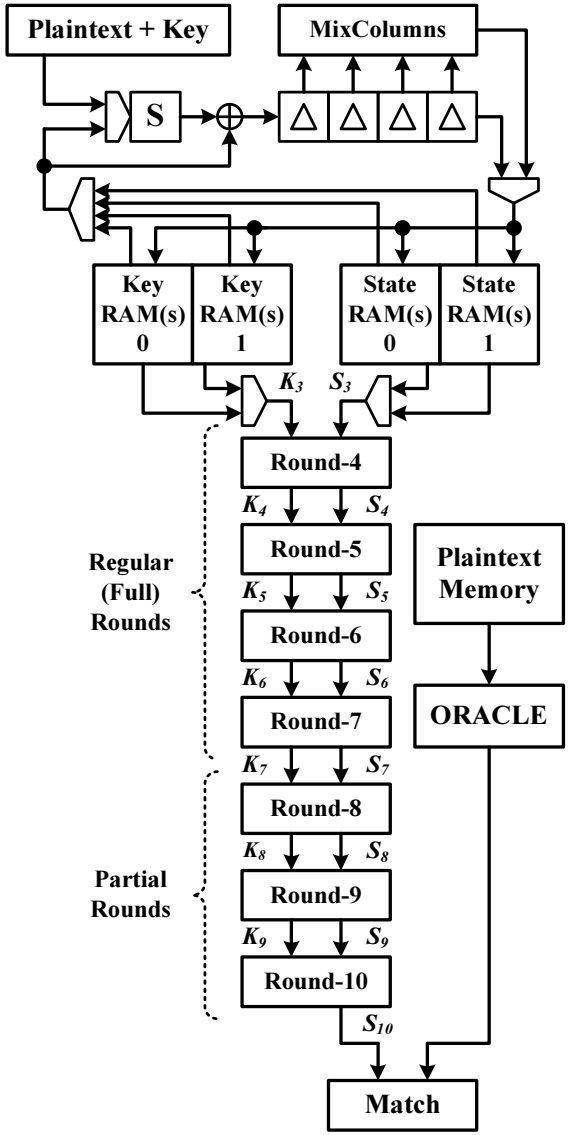
ASIC Performance

Core Area (GE)	Maximum Freq (MHz)	Average Power (mW)	Keys tested/mW
362181	2480	622.937	3.98×10^6

Biclique Attack on AES-128

Starting Point: Conceptual design

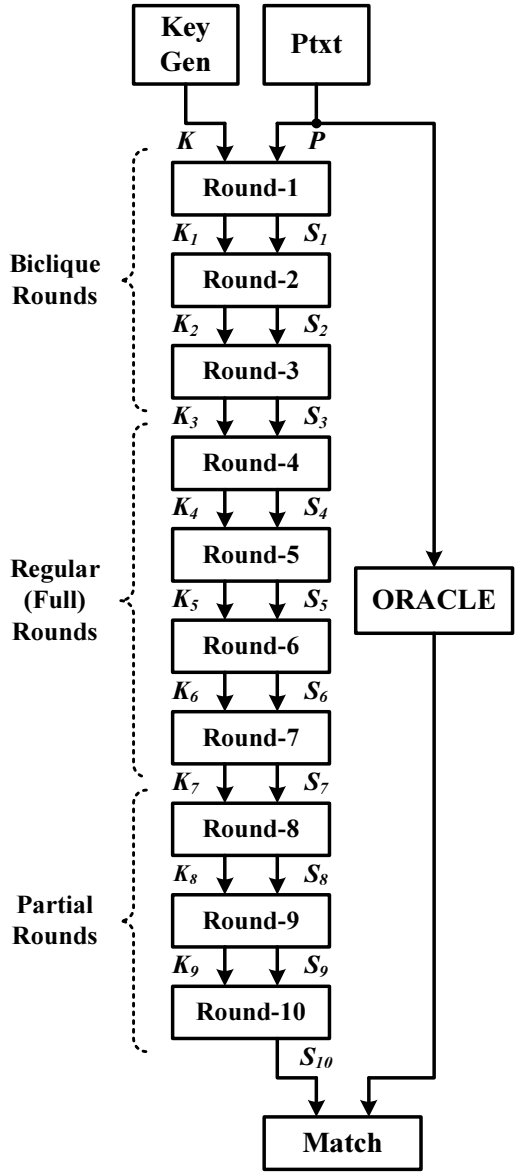
- One-to-one maps theory to implementation
- Based on precomputation of all base and biclique states
- Not feasible for hardware implementation
  - ➢ Requires too many RAMs
  - ➢ Interconnection and control logic too complex to allow an area and speed efficient design



Biclique Attack on AES-128

New Approach: Recomputation

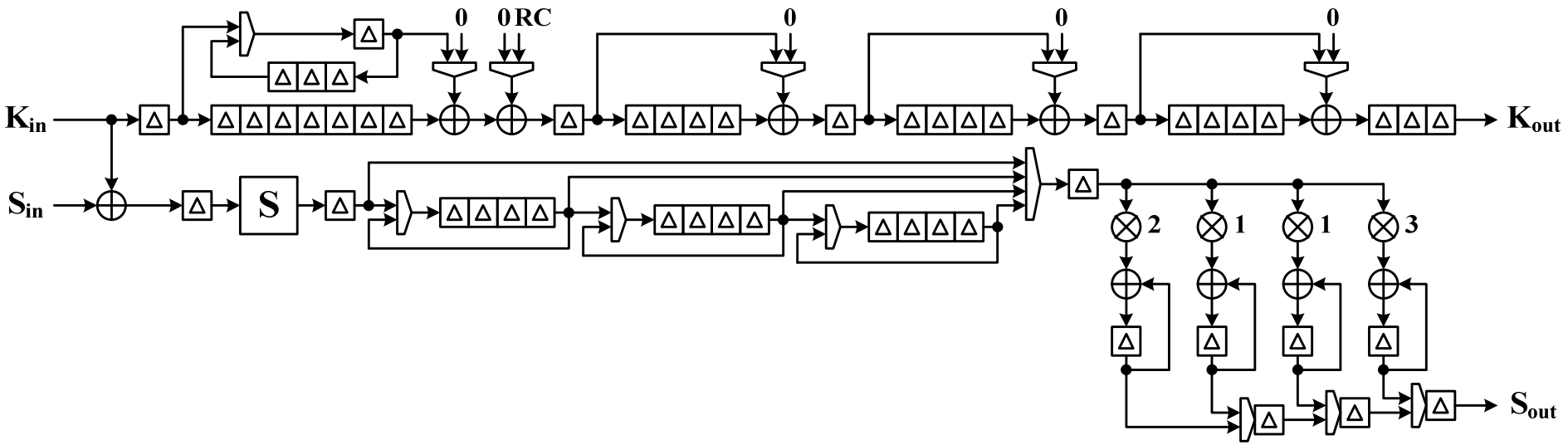
- On the fly calculation of base and biclique states
- Pipeline registers act as state storage media
  - ➢ No additional RAMs/registers required – virtual storage
- Similar to optimized brute force attack in structure
  - ➢ simpler control logic and interconnections



Biclique Attack on AES-128

First “Biclique” Round:

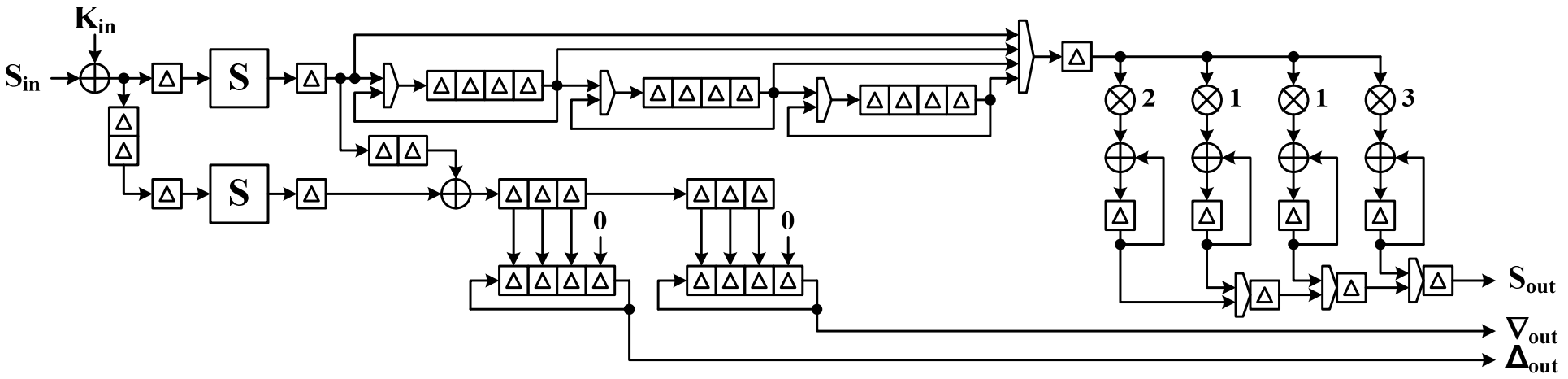
- Serial AES implementation
- 8-bit (!) datapath
- Single S-Box



Biclique Attack on AES-128

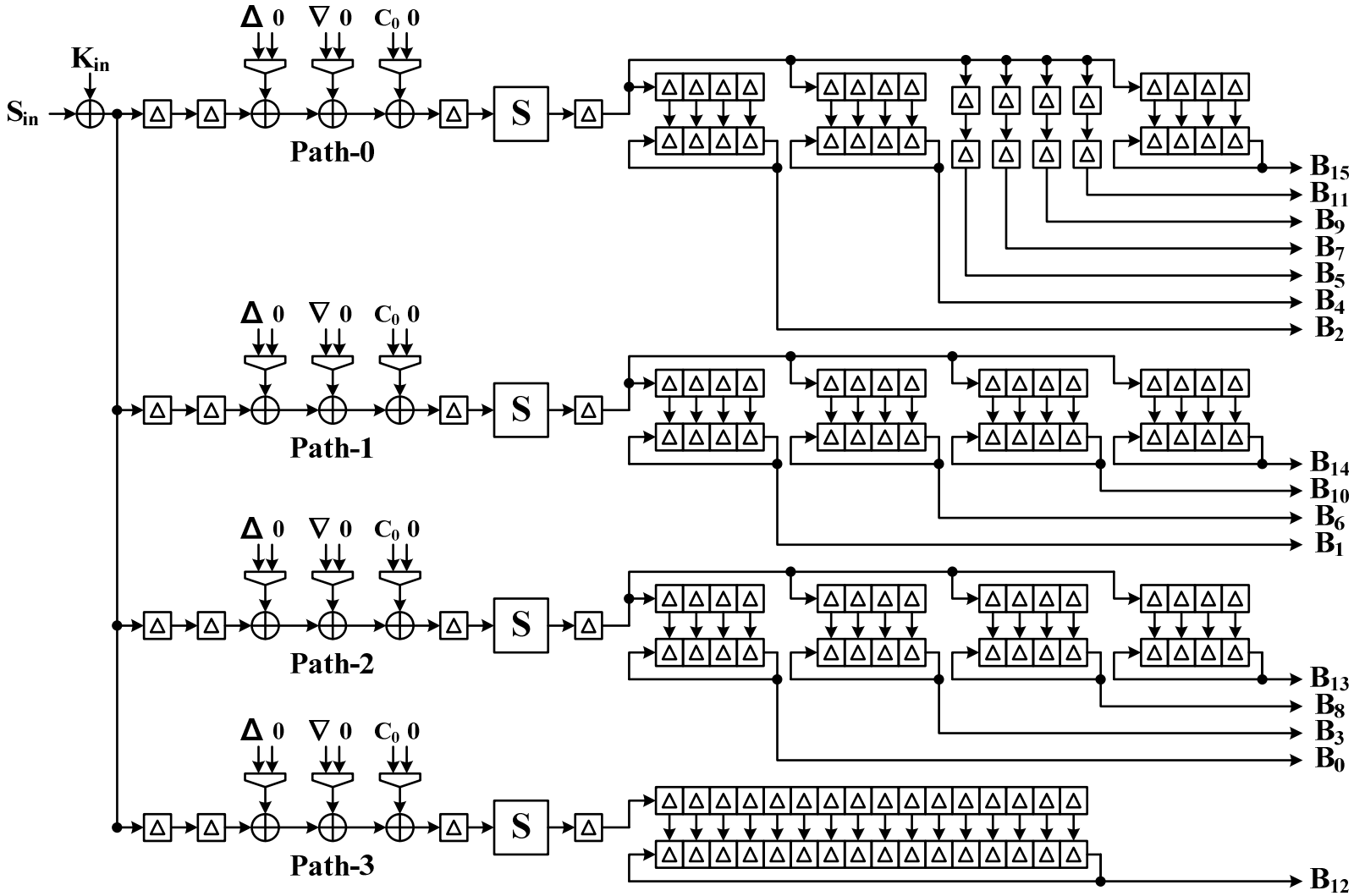
Second “Biclique” Round:

- Slightly modified serial AES implementation
- Still 8-bit (!) datapath
- Two S-Boxes
- Limited additional storage (shift registers) for biclique states



Biclique Attack on AES-128

Third “Biclique” Round:



Biclique Attack on AES-128

Third “Biclique” Round:

- Serial AES implementation on 4 separate paths
- Still 8-bit (!) datapath (on each path)
- Four S-Boxes
- Slightly more complex control logic
- More registers for double-buffering of biclique states (still shift registers with minimal cost
- Only covers the “SubBytes” stage of a full AES round – the rest implemented as in a regular round

Optimized brute-force attack on AES-128

FPGA Performance

Slice Utilization	% FPGA Utilization	Maximum Freq* (MHz)	Keys tested/sec/FPGA
30720 / 33278	92.31	236.22	945×10^6

ASIC Performance

Core Area (GE)	Maximum Freq (MHz)	Average Power (mW)	Keys tested/mW
163912	1548	211.545	7.32×10^6

* Slower than the brute-force attack due to reduced number of pipeline stages

Conclusion

- The ***fastest*** brute-force attack implementation on AES-128
- The ***first*** biclique attack implementation on AES-128
  - Almost a factor of 2 speed and cost gain
  - Only 16 chosen plaintexts (w.r.t. 288 in the original biclique attack paper)
- Suitable for both FPGA and ASIC implementation
- Applicable to AES-192 and AES-256 as well