Efficient AES Implementation for Better Resource Usage and Performance of IoTs

Authors: **Umer Farooq,** Maria Mushtaq, Khurram Bhatti

Contact: ufarooq@du.edu.om

CYBER 2020, NICE, France

Outline

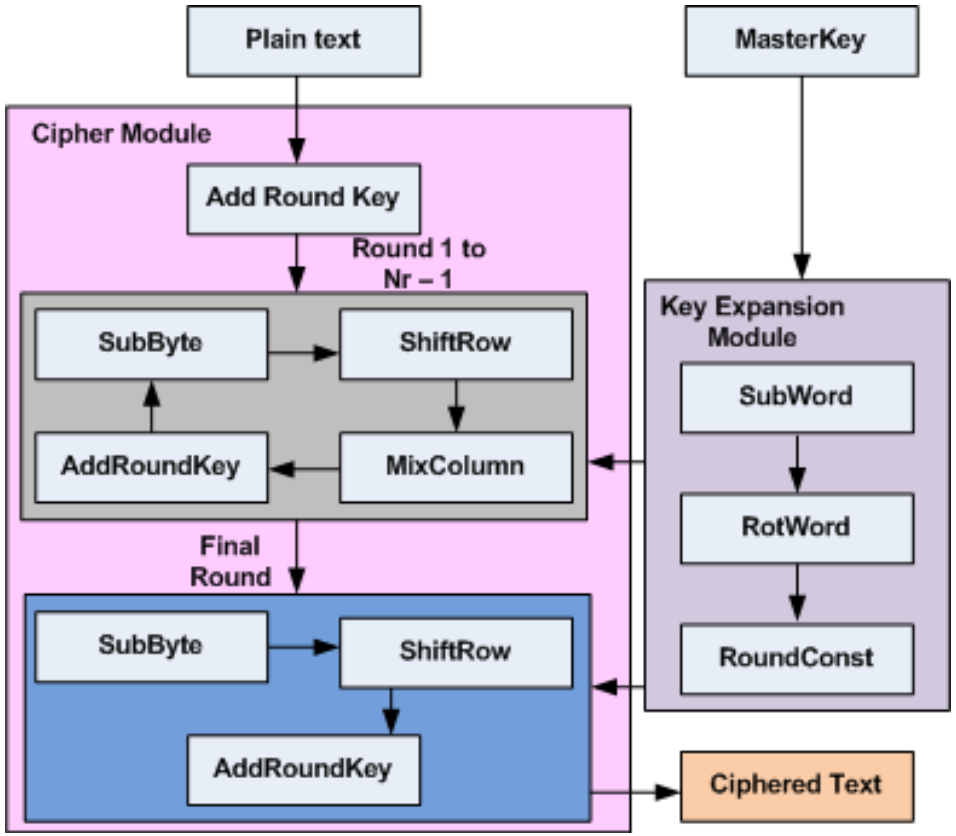
- Introduction
- Overview of AES
- Proposed Techniques
- Results
- Conclusion

Introduction

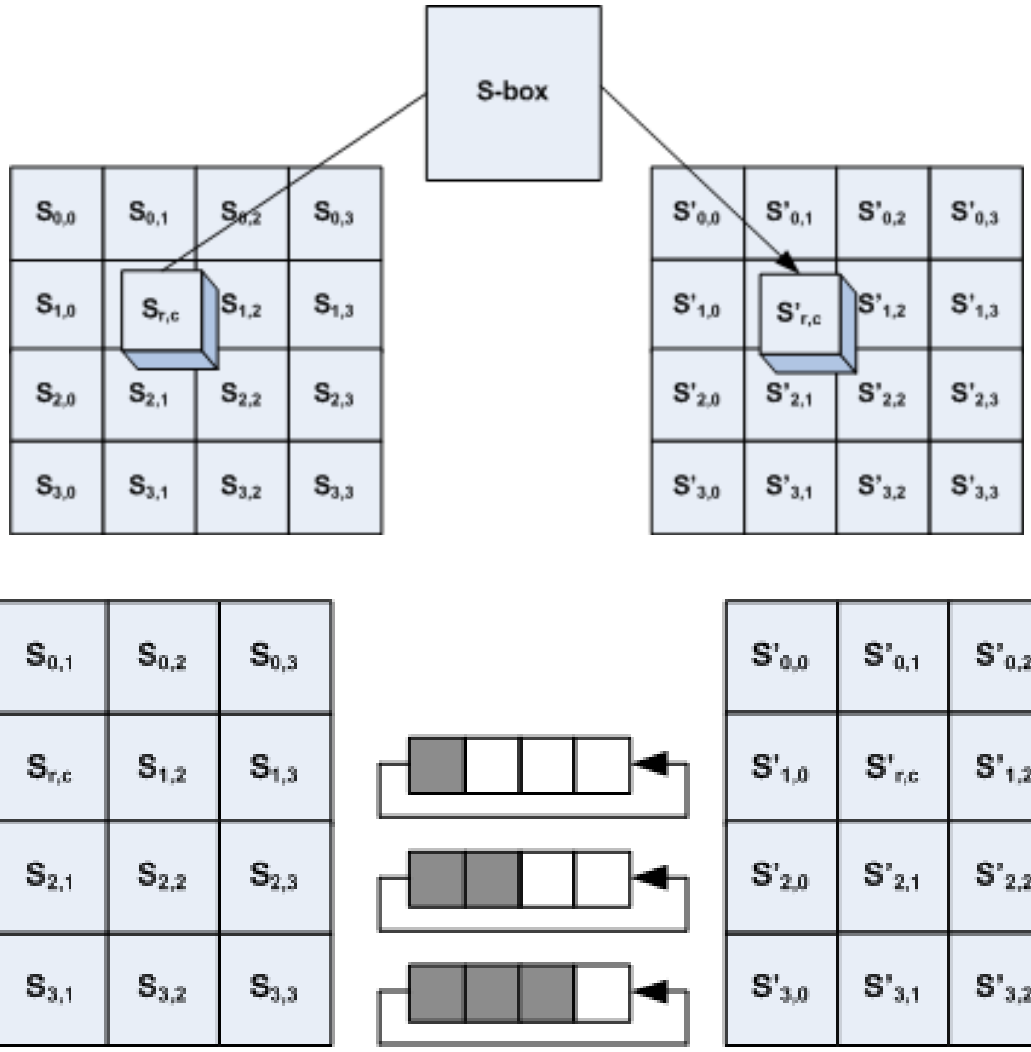
- The Internet of Things (IoTs) devices are prevalent in almost every sphere of human life today.
- The amount and nature of data handled by IoT devices makes them a lucrative target for potential attackers.
- In an IoT-based system, securing an edge side device is a hugely challenging task.
- Among the various countermeasures against security threats, cryptographic algorithms offer an interesting solution.
- Advanced Encryption Standard (AES) is an algorithm that offers robust and hardware independent implementation.

Overview of AES

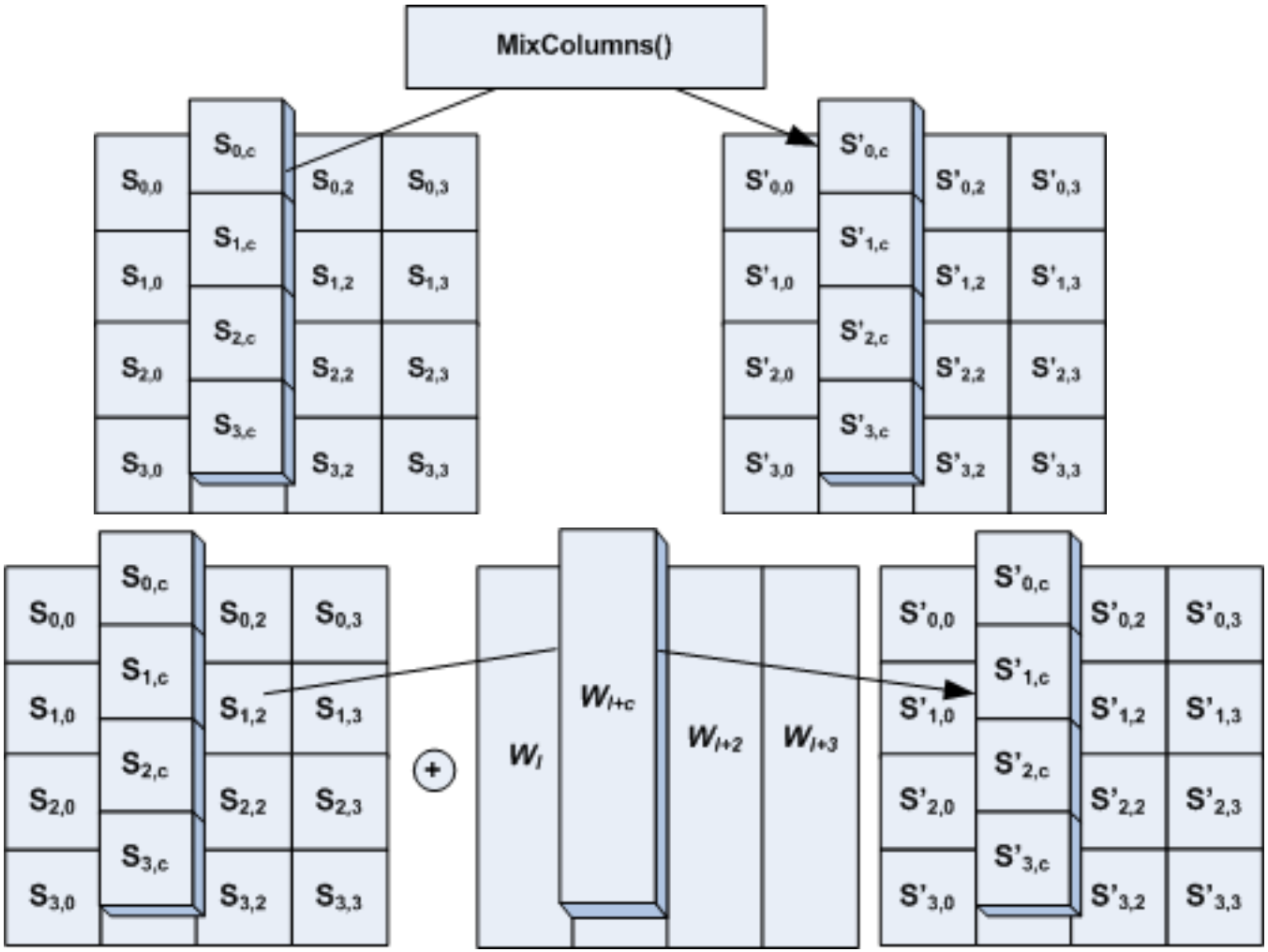
- AES is an iterative algorithm that is implemented over multiple rounds.
- The implementation of AES is mainly divided into two modules:
  - Cipher module
  - Key expansion module
  - Both modules run in parallel



Cipher Module Implementation (1/2)



Cipher Module Implementation (2/2)



Proposed Techniques (1/2)

- Technique 1
  - In this technique, S-box for both cipher module and key expansion module are implemented using BRAMs.
  - It is executed in a serialized manner.
  - First key is expanded and then cipher module is executed.
- Technique 2
  - Both cipher and key expansion module are implemented in BRAMs.
  - Parallelism is achieved through loop unrolling
- Technique 3
  - S-box of cipher module in BRAMs whereas entire key expansion module in CLBs of the FPGA
  - Execution is performed in serialized manner

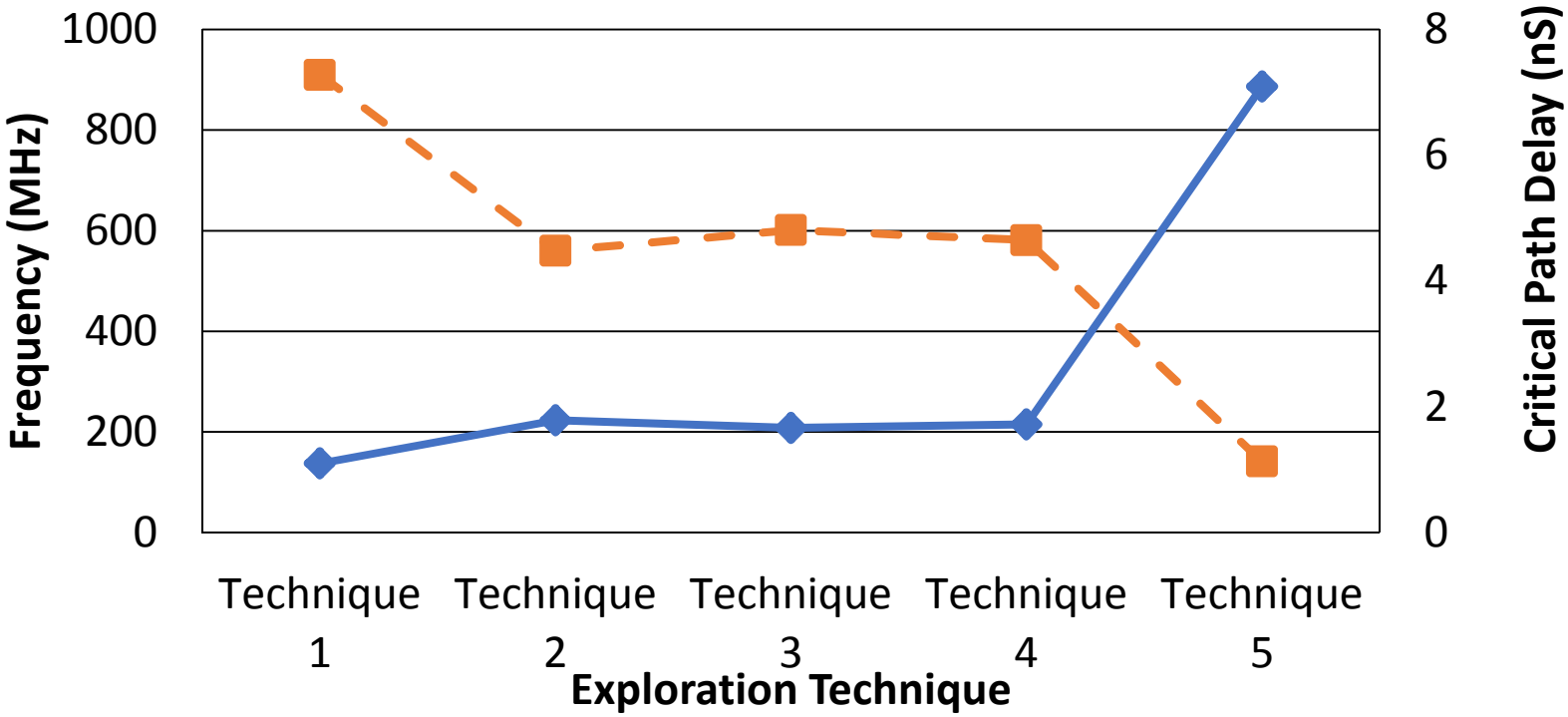
Proposed Techniques (2/2)

- Technique 4
  - S-box of cipher module in BRAMs whereas entire key expansion module in CLBs of the FPGA
  - Parallel execution achieved through loop unrolling and online key generation.
  - Better delay results, but poor area results.
- Technique 5
  - Both cipher module and key expansion module are implemented entirely in CLBs
  - Implementation of S-box in CLBs leads to very good delay results.
  - Very high resources in terms of CLBs are required.

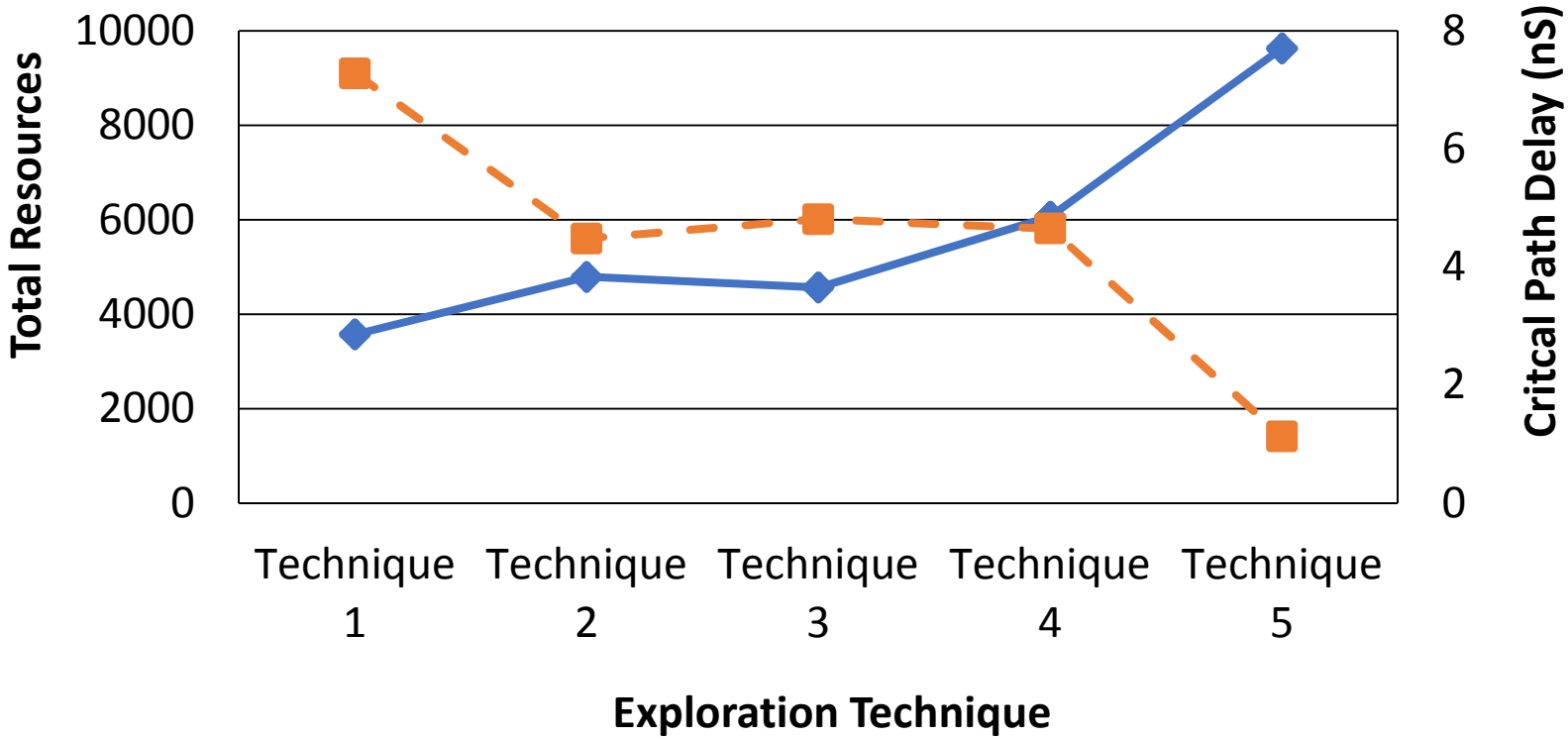
Results

Technique	Number of Slice Registers	Number of Slice LUTs	Frequency (MHz)	Throughput (Gb/S)	Efficiency
Technique 1	278	3315	137.29	17.57	4.85
Technique 2	1547	3253	223.03	28.54	5.89
Technique 3	280	4307	207.74	26.6	5.78
Technique 4	1589	4530	214.96	27.51	4.51
Technique 5	256	9375	886.64	113.49	11.78

Results


1000
800
600
400
200
0
Frequency (MHz)
8
6
4
2
0
Critical Path Delay (nS)
Technique 1
Technique 2
Technique 3
Technique 4
Technique 5
Exploration Technique

Results


Total Resources
10000
8000
6000
4000
2000
0
8
6
4
2
0
Critcal Path Delay (nS)
Technique 1
Technique 2
Technique 3
Technique 4
Technique 5
Exploration Technique

Conclusion

- Modern IoT-based systems are quite heterogeneous in nature and they are subject to all sort of security threats.
- In this work, based on various algorithmic and architecture level optimization, we explore five different implementations of AES.
- Results show that
  - Serialized implementations are good for resource constrained devices
  - Parallel implementations give good frequency results, but they are resource hungry.

Thanks!!!