Design and Analysis of an FPGA-based, Multi-processor HW-SW System for SCC Applications

Andrew Fitzgerald

Department of Computer Engineering
Rochester Institute of Technology

September 3, 2010

Primary Adviser: Dr. Marcin Łukowiak

Committee Members: Dr. Michael Kurdziel, Dr. Pratapa Reddy

Outline

Outline

Motivation

- Embedded systems have advanced remarkably over the last 30 years
- Modern systems require application of high assurance, fail-safe and security design techniques
- New families of devices have been released by the FPGA industry featuring:
  - anti-tamper monitoring
  - bit steam encryption
  - optimized routing architectures
- High assurance and fail-safe systems can now be implemented within the fabric of an FPGA
  - Can meet classified Fail-Safe Design and Analysis (FSDA) requirements [1, 2]

Thesis Objectives

- Design and analyze an FPGA-based system containing two isolated softcore Nios II processors that share data through two crypto engines
  - Resource analysis to quantify costs of red/black separation
- Employ FPGA-based Single Chip Cryptographic (SCC) techniques
- Crypto-engines will be custom implementations of the Advanced Encryption Standard (AES) operating in Galois/Counter mode (GCM)
- Architectures will target high performance, minimal hardware usage or a balance between the two

High-level Design

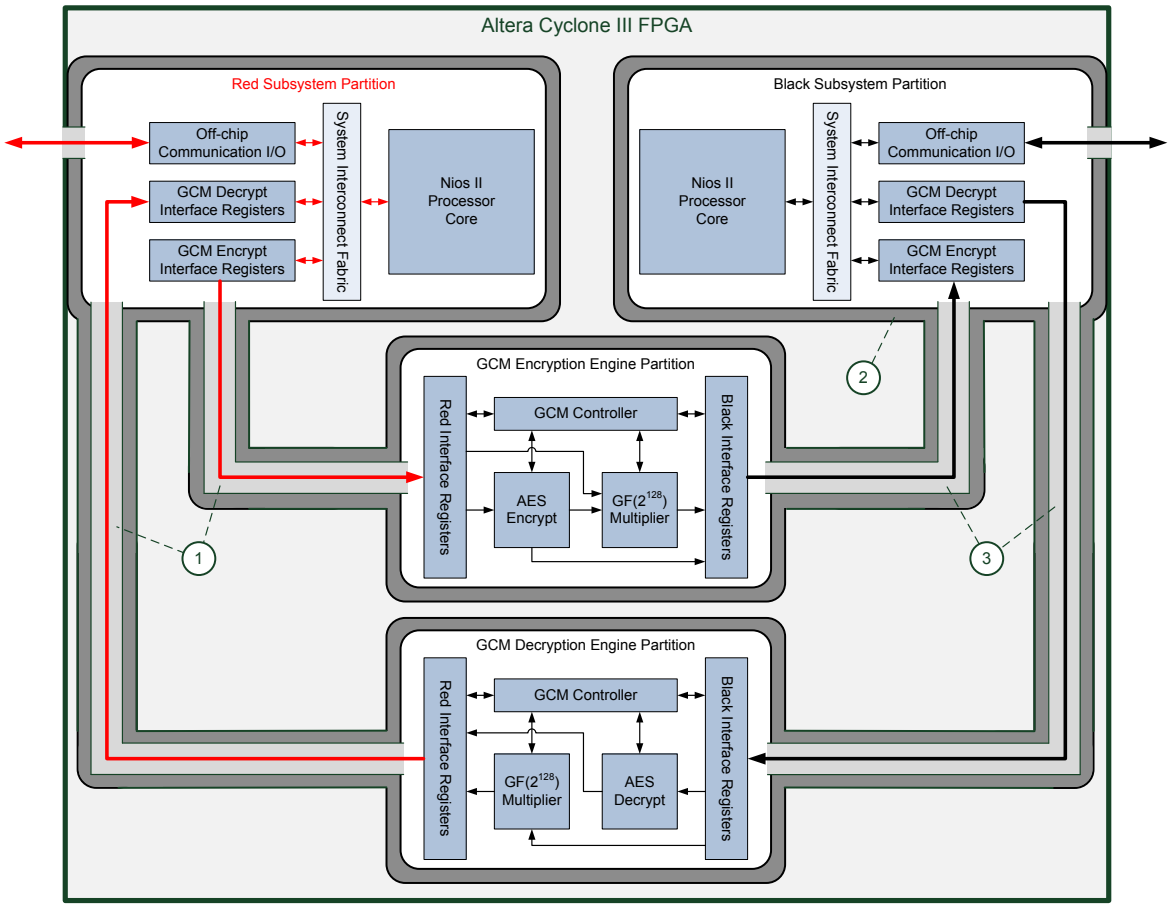


Figure: Dataflow diagram of FPGA-based multiprocessor HW-SW system with AES GCM encryption and decryption engines.

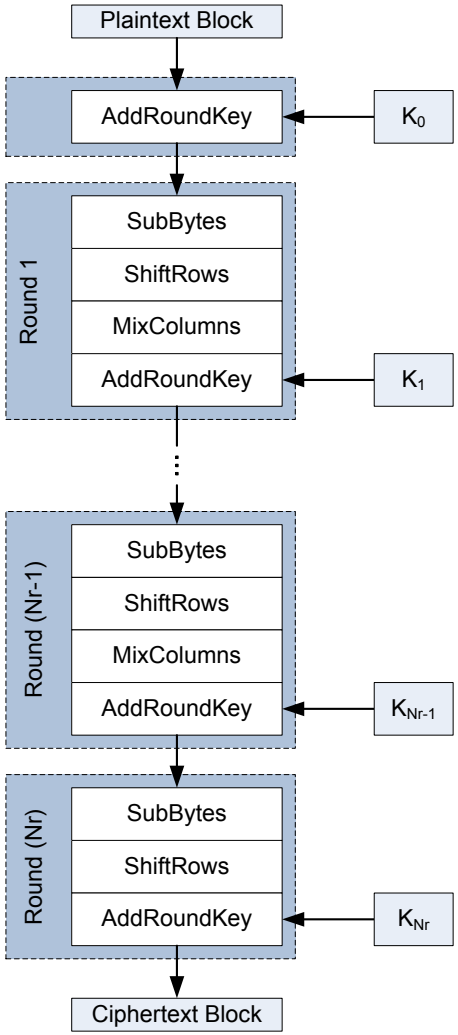
Outline

Outline

The Advanced Encryption Standard

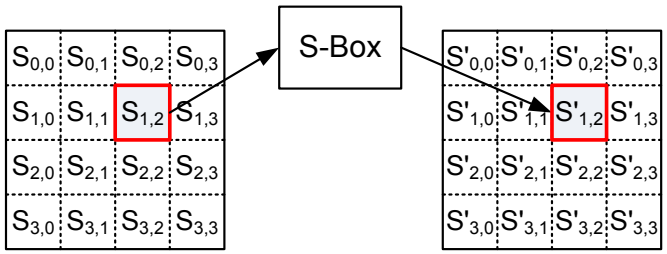
- Standardization of the Rijndael block cipher[3]
- Adopted in November 2001
- Input, output & internal state are 128 bits (block)
- Supports 3 key lengths: 128, 192, 256-bits
- US government approved for use in securing classified material[4]

Encrypt Round Structure

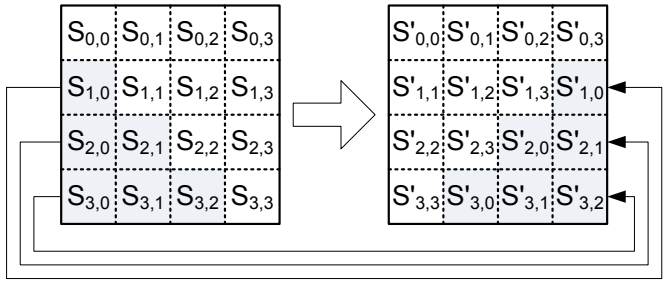


Key length (bits)	Number of Rounds
128	10
192	12
256	14

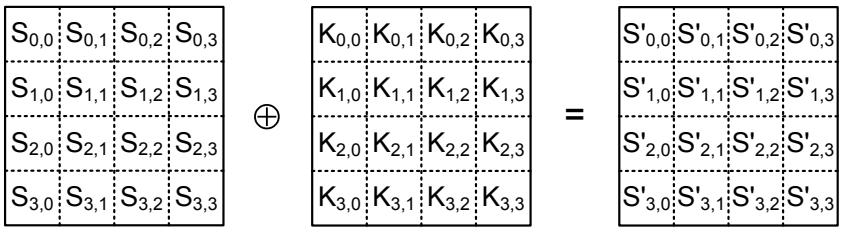
Encrypt Round Operations



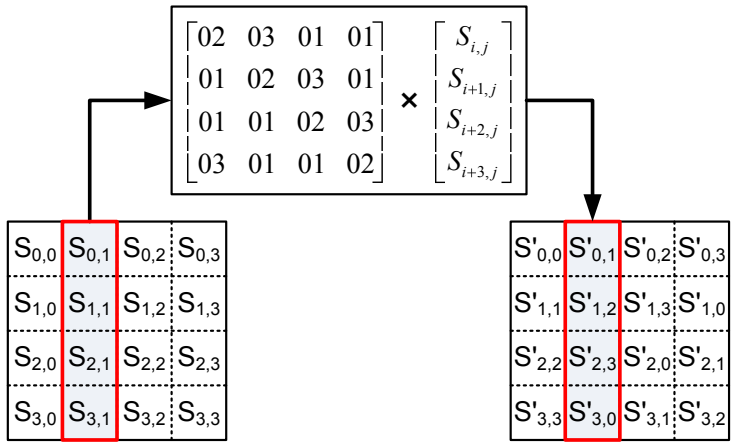
(a) SubBytes



(b) ShiftRows



(c) AddRoundKey



(d) MixColumns

Key Schedule

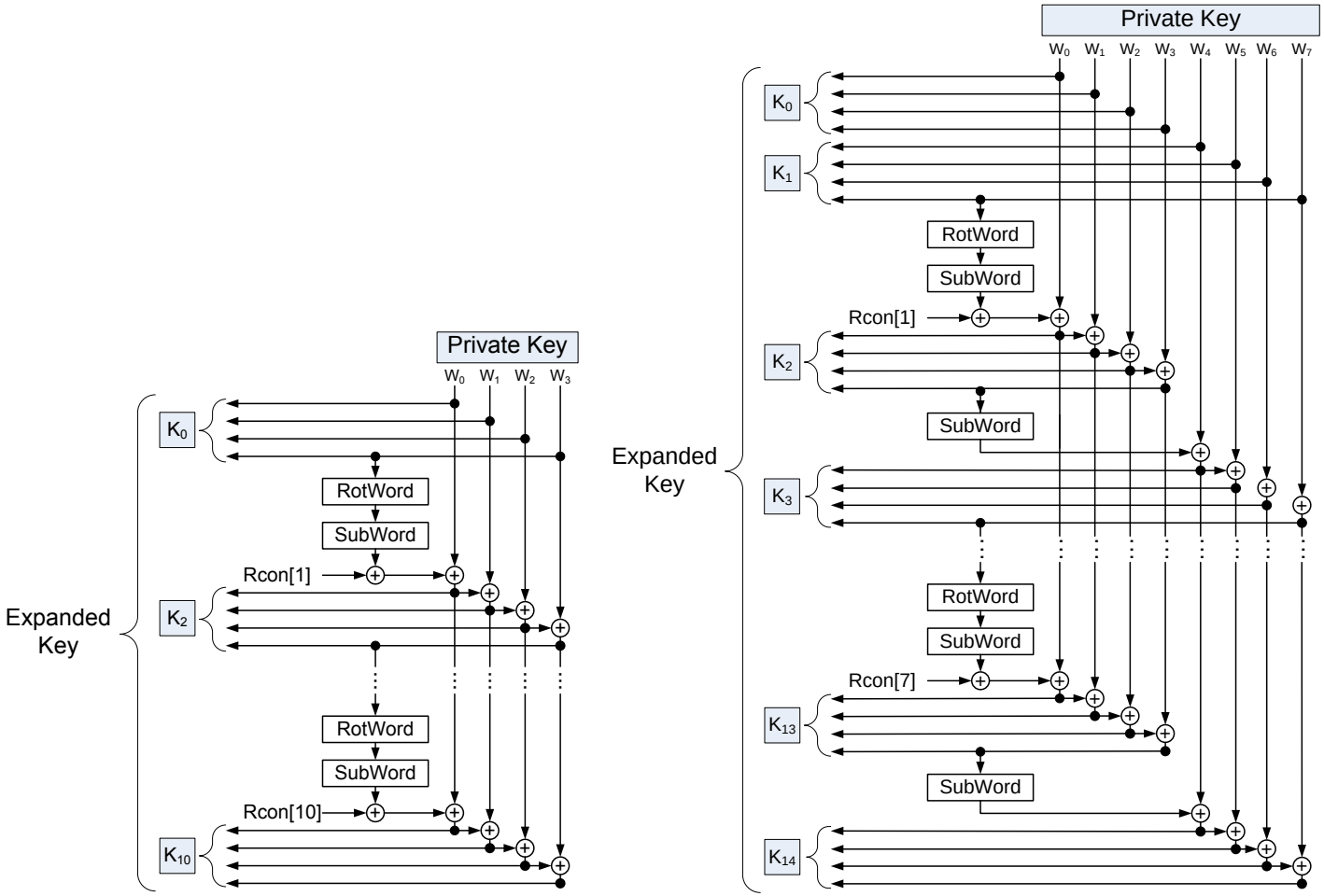


Figure: AES 128 & 256 bit key expansion operations[5].

Outline

Galois/Counter Mode

- Created in 2005 [6] and standardized in 2007 [7]
- Authenticated encryption mode of operation for a block cipher
- Parallelizable and relatively efficient [7]
- Requires a NIST approved block cipher with block size of 128-bits

GCTR Operation

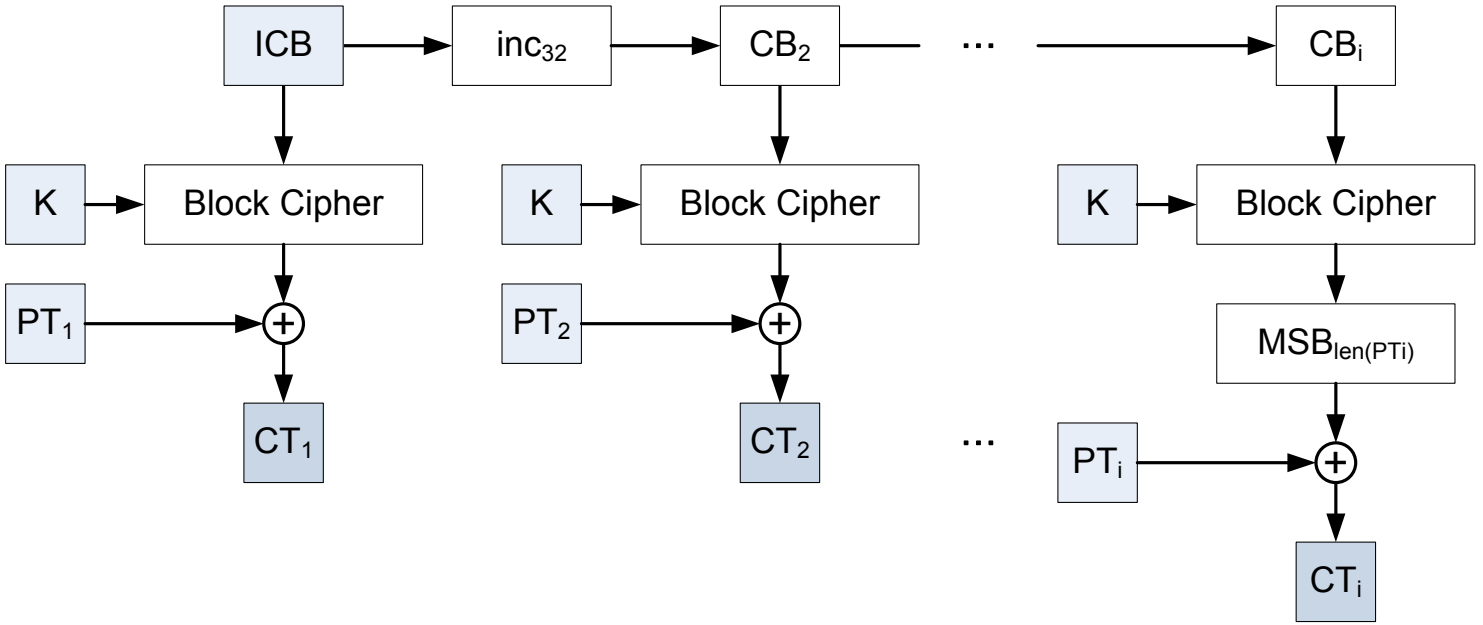


Figure: The GCTR function where the inputs, the ICB, key and plaintext PT_i, are shown in light blue, and the ciphertext CT_i, is shown in dark blue.[7]

GHASH Operation

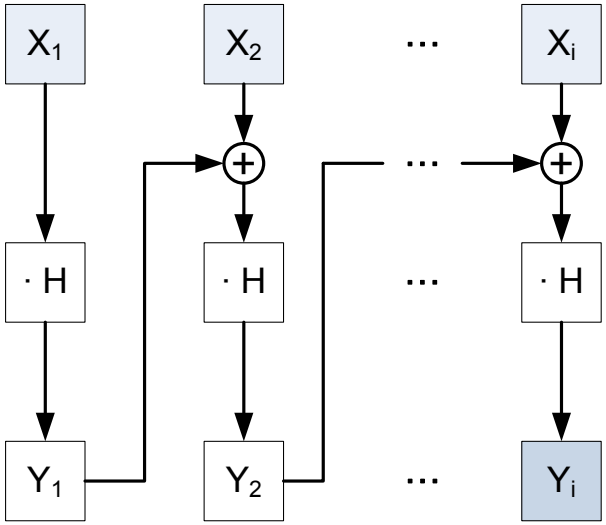


Figure: The GHASH function with inputs X_i and final output hash Y_i.[7]

$$Y_i = X_1 \cdot H^i \oplus X_2 \cdot H^{i-1} \oplus \ldots \oplus X_{i-1} \cdot H^2 \oplus X_i \cdot H^1 \qquad (1)$$

High-level Operation

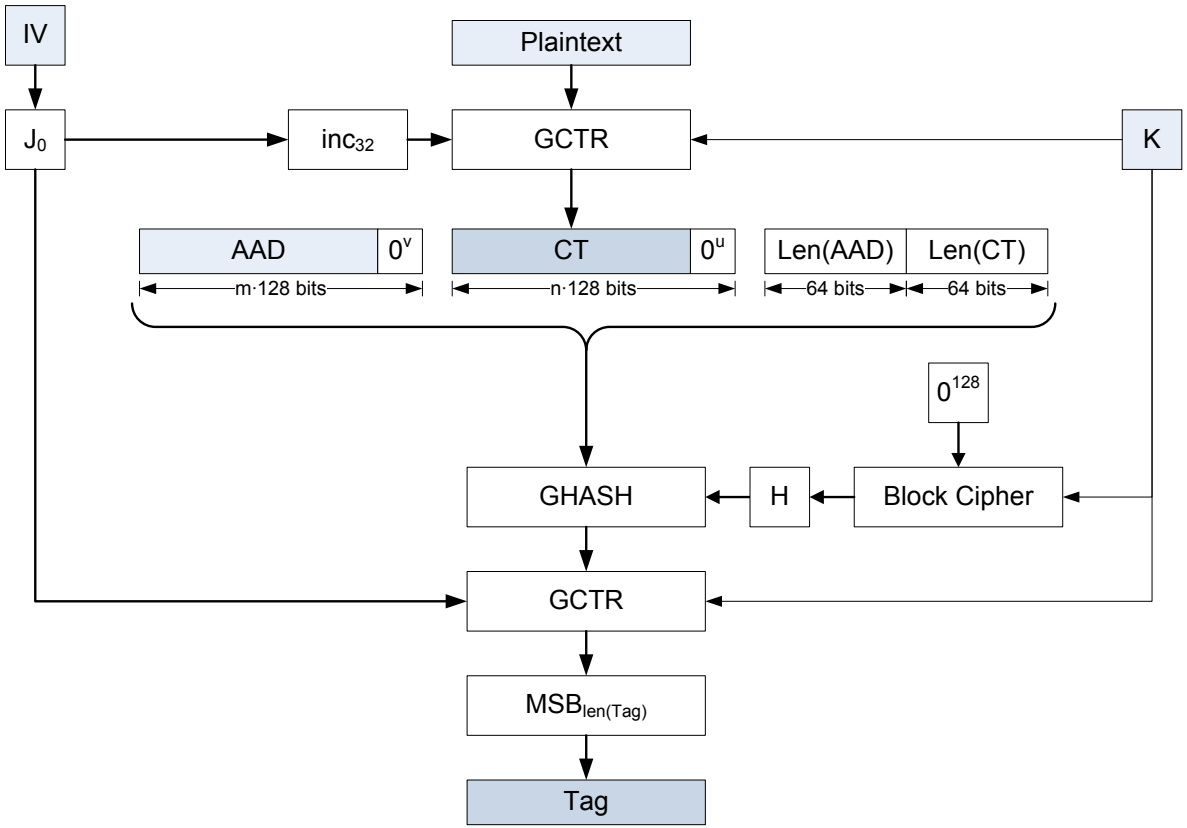


Figure: The operations in GCM from the IV, plaintext, AAD, and key inputs, shown in light blue, to the tag and ciphertext outputs, shown in dark blue[7].

Outline

FPGAs and SCC

- FPGAs are a convenient middle ground between an ASIC and a general purpose processor
- An FPGA is an IC that contains programmable logic blocks that are connected with reconfigurable interconnection structures
- SCC originated from the need to reduce & consolidate components in system design
- FPGA-based SCC for type-1 crypto was not orignally possible
  - Verification was considered intractable [2]
- Modern secued FPGAs have tools to perform this analysis [2, 8]

Red/black separation

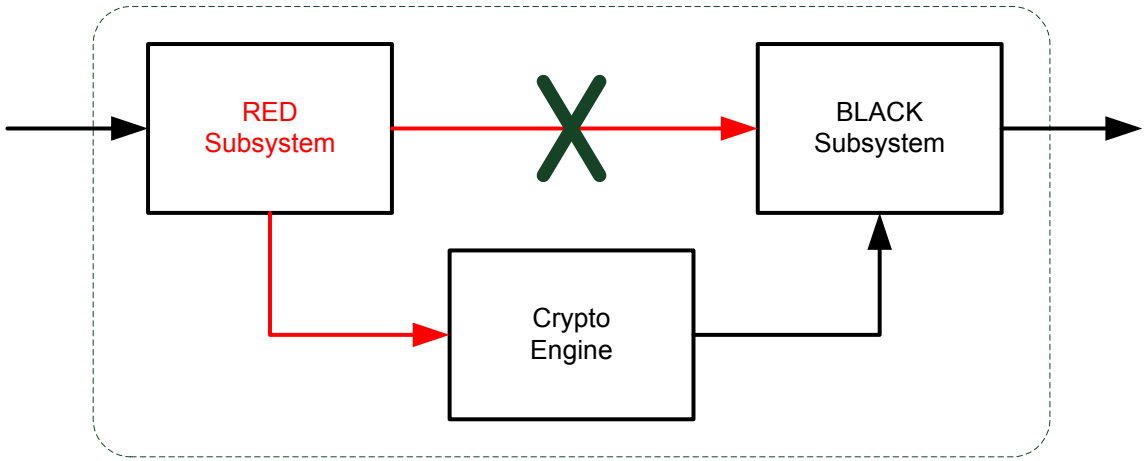


Figure: Physically separated black and red subsystems that exchange data only by means of a cryptographic engine [9].

Outline

Outline

GCM Top Level Design

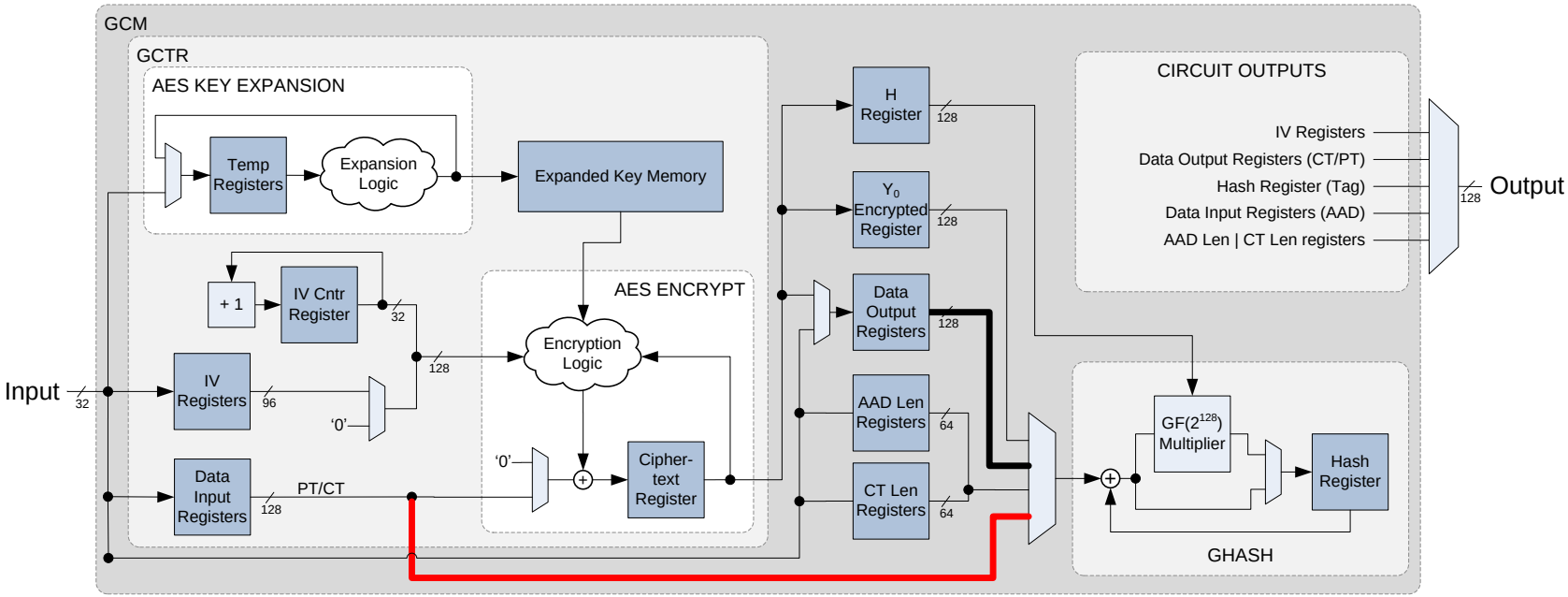


Figure: A high-level diagram illustrating the individual GCM components and their interconnections.

GCM Top Level Design

- 96-bit IV was chosen for the implementation
  - Recommended for the algorithms efficiency at this size [10]
- Supports both encryption and decryption with all three AES key lengths
- Data must be a multiple of the AES block size
  - Padding is handled at the software level
- Operation is controlled through configuration, control and status registers
  - Access to I/O and control signals is restricted based on processor
- Software Library
  - Provides C functions to work with the GCM engine
  - Since the top level architecture was consistent across target implementations, the software library did not need to be changed

Outline

Small Area

- Used a 32-bit AES datapath
  - Encrypt operates on one 32-bit word at a time
  - Key schedule modified from [12]
- Round keys stored in 32-bit addressable on-chip memory
- The GHASH multiplier was implemented as bit-serial
  - Requires 128 clock cycles to complete one multiplication

32-bit Encrypt

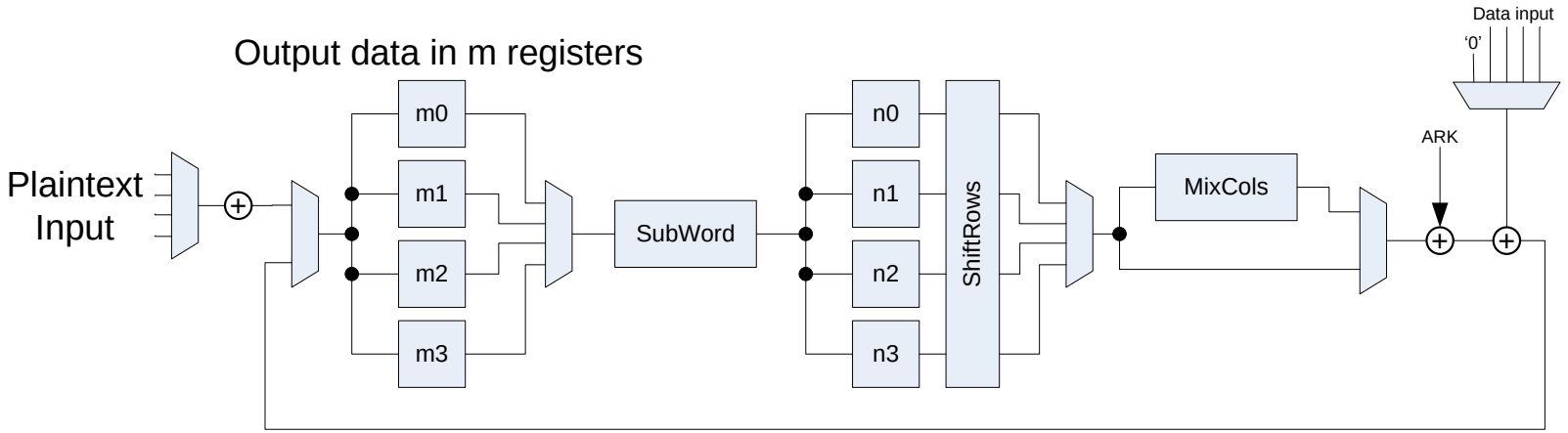


Figure: The 32-bit wide datapath encrypt implementation

32-bit Modified Chodowiec key schedule

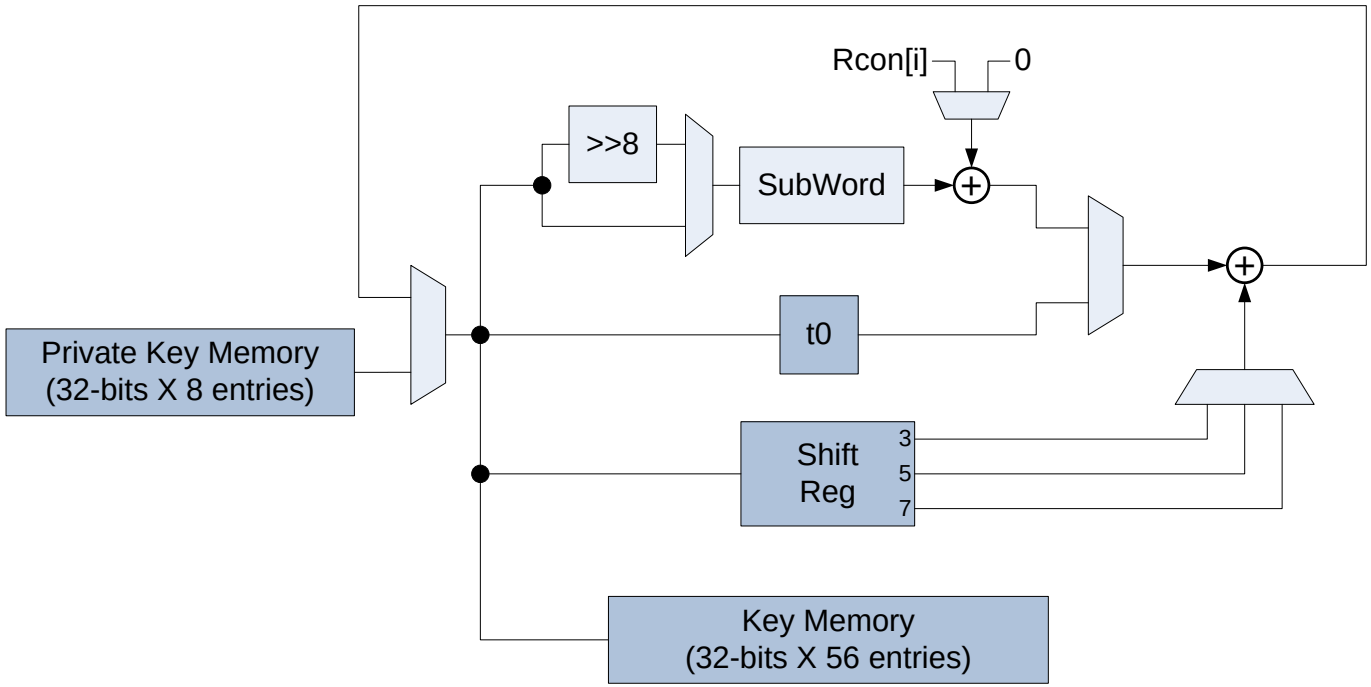


Figure: The 32-bit width datapath key schedule that was modified from [12] to better fit the architecture of the target FPGA.

High Performance

- Used a 128-bit AES datapath
  - Encrypt based on a round iterative design, calculating 1 block per cycle
  - Key schedule modified from [13]
- Round keys stored in 128-bit addressable on-chip memory
- The GHASH multiplier was implemented as full-parallel
  - Computes a result every clock cycle
  - Deep critical path

128-bit Encrypt

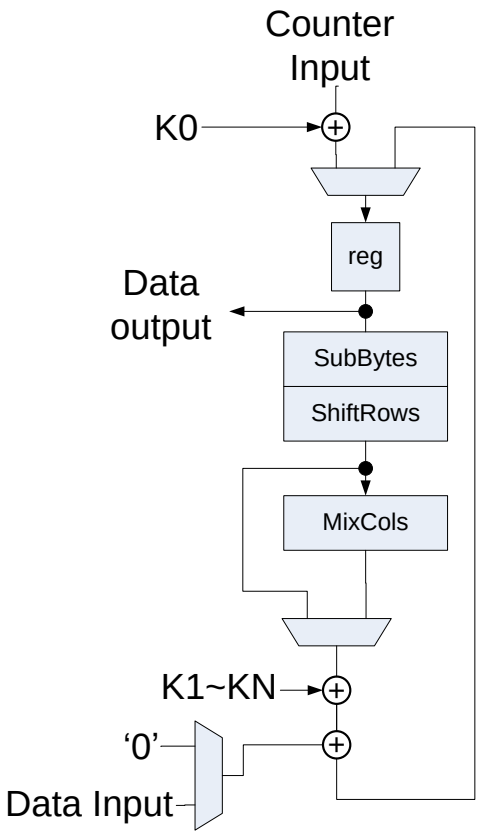


Figure: The 128-bit wide datapath encrypt implementation [13]

128-bit Modified Satoh Key schedule

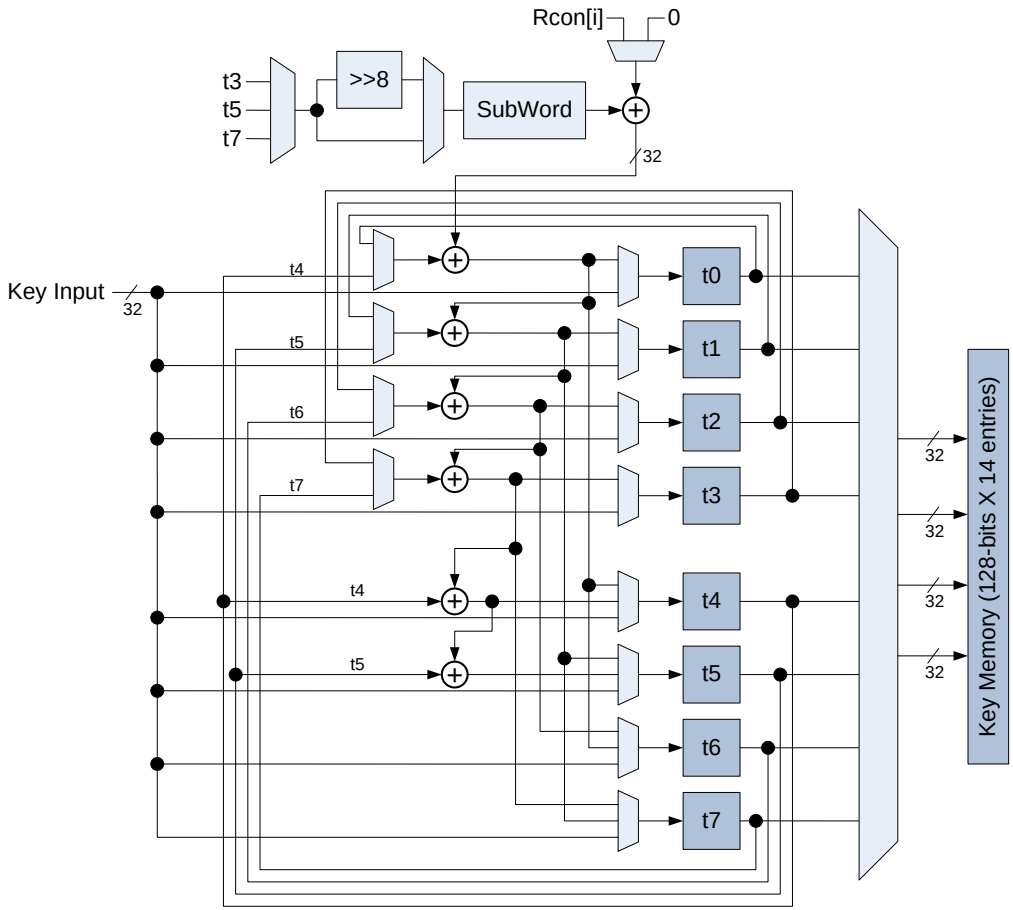


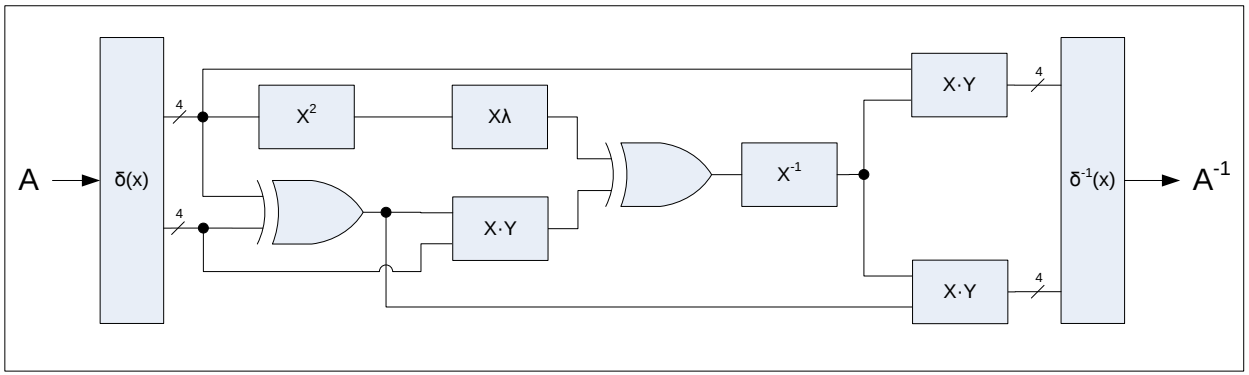
Figure: The 128-bit width datapath key schedule from [13] that was modified to better fit the architecture of the target FPGA.

Balanced Performance

- Used a 128-bit AES datapath
  - Used the same encrypt and key schedule implementations as the high performance design
- Rounds keys stored in 128-bit addressable on-chip memory
- The GHASH multiplier utilizes a sequential multiply and add approach [14]
  - A product is calculated every 16 clock cycles
  - This version was selected to better match the encryption components performance

S-Box Implementation

- Each of the target architectures was designed with an S-Box implemented in 1) combinational logic and 2) M9K memory elements
- The combinational logic based S-Box was based on the composite field technique [11]
  - The S-Box output is found through calculations in lower order Galois fields



Outline

Target Platform

- Functional verification performed on an Altera Cyclone III (EP3C120) FPGA
  - 119,088 logic elements, 432 M9Ks or 3,888 memory kbits
- Final designs synthesized for a Cyclone III LS (EP3CLS70) FPGA
  - 70,208 logic elements, 333 M9Ks or 2,997 memory kbits

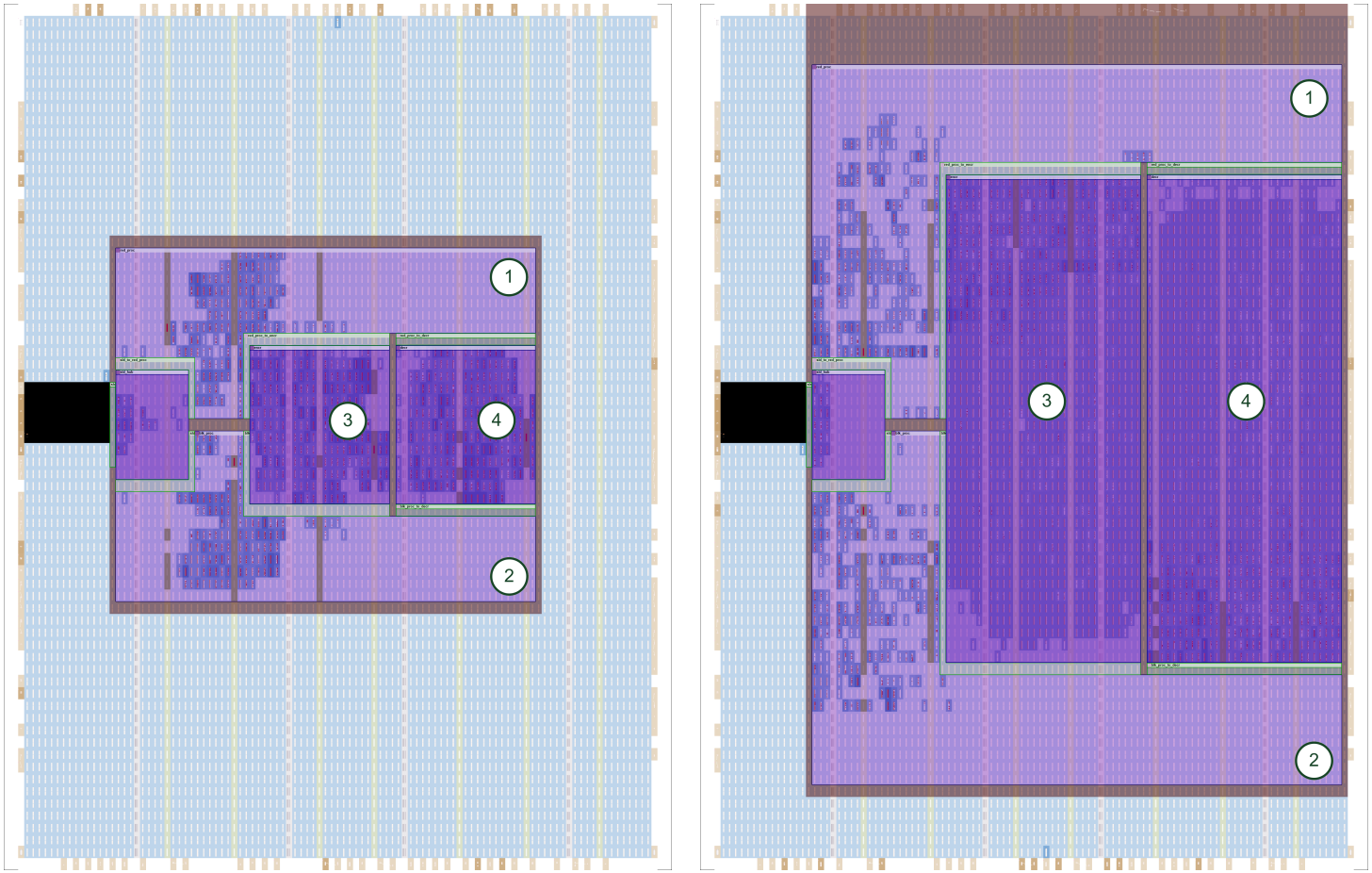
Outline

Single GCM engine performance statistics

Target Application	AES Width (bits)	AES S-Box Arch.	GHASH Arch.	GCM Max Freq. (MHz)	128-bit Packet Throughput (Mbps)	2K-bit Packet Throughput (Mbps)
Small area	32	C-Field	Bit serial	68.7	33.6	63.6
	32	M9K	Bit serial	119	58.1	110
High performance	128	C-Field	Full parallel	71.2	434	528
	128	M9K	Full parallel	79.7	486	591
Bal. performance	128	C-Field	16-Sequen.	64.6	218	430
	128	M9K	16-Sequen.	97.0	327	645

Outline

Sample Implementation Floorplans



(a) Small area

(b) High performance

Table: GCM engine secured region resource utilization statistics

Target App.	AES Width (bits)	AES S-Box Arch	GHASH Arch	GCM Engine Partion: Utilized M9K (#)	Utilized LEs (#)	Allocated M9K (#)	Allocated LEs (#)	Utilization M9K (%)	Utilization LEs (%)
Small area	32	C-Field	Bit serial	3	3696	26	4160	12	89
	32	M9K	Bit serial	7	3170	26	4160	27	76
High perf.	128	C-Field	Full parallel	4	17023	94	21056	4	81
	128	M9K	Full parallel	14	14956	94	21056	15	71
Bal. perf.	128	C-Field	16-Sequen.	4	6122	30	6240	14	99
	128	M9K	16-Sequen.	14	4682	30	6240	47	75

Table: Red/Blk secured region resource utilization statistics

Target App.	AES Width (bits)	AES S-Box Arch	GHASH Arch	Red/Blk Subsystem Partition: Utilized M9K (#)	Utilized LEs (#)	Allocated M9K (#)	Allocated LEs (#)	Utilization M9K (%)	Utilization LEs (%)
Small area	32	C-Field	Bit serial	22	1591	51	7856	43	20
	32	M9K	Bit serial	22	1596	51	7856	43	20
High perf.	128	C-Field	Full parallel	22	1663	99	15760	22	11
	128	M9K	Full parallel	22	1691	99	15760	23	11
Bal. perf.	128	C-Field	16-Sequen.	22	1651	60	9648	37	18
	128	M9K	16-Sequen.	22	1636	60	9488	37	18

Performance and area analysis

- As expected, the deep critical path in the composite field S-Box limited the FMAX of the GCM engine
  - Possible advantage if placed on an FPGA with little memory
- True-dual port memory S-Box designs were more area efficient for this FPGA
- Memory based S-Box designs also had a higher throughput, due to the increase FMAX
- The balanced implementation had the highest throughput for the larger packet size
  - This is because its higher FMAX and the high performance implementation had an equivalent AES encrypt component that continued computation while the GHASH component sat idle

Secure partitioning costs

- For the high performance implementation:
  - Unused resources in fences: 8912 LEs, 36 M9Ks, 20 embedded multipliers
  - Unused resources in SRIs: 3120 LEs, 12 M9Ks, 9 embedded multipliers
  - I/O banks 6 and 7 are not usuable, and banks 5 and 8 are only partially usable
- 186 signals pass between the Altera JTAG hub and the processor partitions
  - Routability constraints required the size of the JTAG hub region be expanded
- The height of the processor secured partitions is 8 LABs to allow routing to all contained LABs
  - Significant contributor to the excessive size of the red and black partitions

Outline

What was accomplished?

- A red/black separated systems were designed with independent encryption and decryption implementations of GCM using AES to pass authenticated and encrypted information between two Nios II processors
- High performance, small area and balanced performance implementations were created
- The costs of secure partitioning were assessed for these systems on the target secured FPGA

Suggested future work

- AES
  - S-box sharing between key schedule and encrypt
  - 32-bit wide datapath key schedule with 128-bit wide datapath encryption
- GCM
  - FIFO to queue up data
  - Register data sizes internally and mask bits as necessary
- System
  - Interrupt interface for processors
  - Direct input to the GCM engines from the I/O pins
    - Processors used to manage the flow of data, instead of passing data through themselves
  - Eliminate redundant registers
    - Might have to sacrafice some modularity

Conference proceedings

Published document:

A. Fitzgerald, M. Łukowiak, M. Kurdziel, C. Mackey, K. Smith Jr, B. Boorman, D. Harris, and W. Skiba

FPGA-Based, Multi-Processor HW-SW System for Single-Chip Crypto Applications

The 2010 Military Communications Conference - Unclassified Program - Cyber Security and Network Management

San Jose, California, October 2010

Questions?

Contact information:

Andy Fitzgerald
afitzy@gmail.com

Harris Corporation,
RF Communications Division
andrew.fitzgerald@harris.com

References I


D. Harris, J. Fitton, and C. Mackey, "High Assurance Multiplexer Techniques for use with Secure Digital Communications," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, (1680 University Avenue, Rochester, NY), p. 1, Harris Corporation, RF Communications Division, November 2008.


P. Quintana, "Fail-Safe FPGA Design Features for High-Reliability Systems," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, (101 Innovation Drive, San Jose, CA), pp. 1–7, Altera Corporation, Oct. 2009.


National Institute of Standards and Technology (NIST), "Specification for the Advanced Encryption Standard (AES)." Federal Information Processing Standards Publication 197, 2001.


L. Hathaway, "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information." Online, June 2003.
CNSS Policy No. 15, Fact Sheet No. 1.


A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," in *Advances in Cryptology ASIACRYPT 2001*, vol. 2248 of *Lecture Notes in Computer Science*, pp. 239–254, Springer Berlin / Heidelberg, 2001.


D. McGrew and J. Viega, "The Galois/Counter Mode of Operation (GCM)," May 2005.


M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," NIST Special Publication 800-38D, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930, USA, November 2007.


M. McLean and J. Moore, "FPGA-based single chip cryptographic solution," *Military Embedded Systems*, March 2007.

References II


P. Quintana, “Fail-Safe FPGA Design Features for High-Reliability Systems,” Tech. Rep. CP-01053-1.0, Altera Corporation, 101 Innovation Drive, San Jose, CA, April 2009.


B. Yang, S. Mishra, and R. Karri, “A High Speed Architecture for Galois/Counter Mode of Operation (GCM).” Cryptology ePrint Archive, Report 2005/146, 2005.


V. Rijmen, “Efficient Implementation of the Rijndael S-box,” 2000.


P. Chodowiec and K. Gaj, “Very Compact FPGA Implementation of the AES Algorithm,” in *Cryptographic Hardware and Embedded Systems - CHES 2003*, vol. 2779 of *Lecture Notes in Computer Science*, pp. 319–333, Springer Berlin / Heidelberg, 2003.


A. Satoh, “High-Speed Hardware Architectures for Authenticated Encryption Mode GCM,” in *Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on*, pp. 4831–4834, May 2006.


A. Satoh, T. Sugawara, and T. Aoki, “High-Speed Pipelined Hardware Architecture for Galois Counter Mode,” in *Information Security*, vol. 4779 of *Lecture Notes in Computer Science*, pp. 118–129, Springer Berlin / Heidelberg, 2007.