REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2004	Final Report (Aug.2001-July.2004)

4. TITLE AND SUBTITLE
High-Speed and Low-Power VLSI Error Control Coders

5. FUNDING NUMBERS
DAAD19-01-1-0705

6. AUTHOR(S)
Keshab K. Parhi

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Minnesota, Department of Electrical & Computer Engineering
200 Union st S. E. Minneapolis, MN 55455

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
42436-EL-CI

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
This final report describes our research results obtained during the period Aug. 1, 2001 to July 31, 2004 by support from the ARO grant "High-Speed and Low-Power VLSI Error Control Coders" (ARO Grant Number: DA/DAAD19-01-1-0705 (42436-CI)). Research results obtained in the areas of architectures for product turbo coders (based on component codes such as BCH codes, extended Hamming codes, and single parity check codes), space-time block codes, low-density parity check (LDPC) and long BCH codes are described. Efficient implementations of AES cryptosystems are described. Architectures for ultra wideband communication systems are summarized. Erasure decoding in Reed-Solomon codes, and some preliminary results on soft-decision Reed-Solomon decoders are outlined.

14. SUBJECT TERMS
Turbo Codes, BCH, LDPC, Soft-Decision Reed-Solomon Code, AES, Ultra wideband

15. NUMBER OF PAGES
8

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Final Report

Title: High-Speed and Low-Power VLSI Error Control Coders

ARO Grant Number: DA/DAAD19-01-1-0705 (42436-CI)

PI: Keshab K. Parhi, Distinguished McKnight University Professor
Department of Electrical & Computer Engineering
University of Minnesota
200 Union Street SE
Minneapolis, MN 55455
Tel: (612) 624-4116
Fax: (612) 625-4583
E-mail: parhi@ece.umn.edu
http://www.ece.umn.edu/users/parhi

This final report describes our research results obtained during the period Aug. 1, 2001 to July 31, 2004 by support from the ARO grant "High-Speed and Low-Power VLSI Error Control Coders" (ARO Grant Number: DA/DAAD19-01-1-0705 (42436-CI)). Research results obtained in the areas of architectures for product turbo coders (based on component codes such as BCH codes, extended Hamming codes, and single parity check codes), space-time block codes, low-density parity check (LDPC) and long BCH codes are described. Efficient implementations of AES cryptosystems are described. Architectures for ultra wideband communication systems are summarized. Erasure decoding in Reed-Solomon codes and some preliminary results on soft-decision Reed-Solomon decoders are outlined.

1. High-Speed BCH Turbo Product Decoder

In this work, a sub-optimal algorithm for decoding BCH (t>=2) turbo codes has been developed. High speed VLSI decoder architectures have been proposed for codes constructed over extended GF(2^5). While the algorithm applies to higher order BCH product codes, it is shown that this particular block turbo code, when decoded using the proposed algorithm, gives the best performance (achieving 10^{-6}} bit error rate at a signal to noise ratio of 2.4 dB) among all two dimensional turbo product codes. Following an analysis of the impact of finite word-length effect on the performance of the SISO decoder, high-level architectures for full parallel decoding have been developed. Lower level high speed implementation strategies such as application of look-ahead technique to reduce the critical path of the merge sort circuit and fast finite field operations have also been developed. Area and timing estimates obtained by logic synthesis (0.18 micron, 1.5V CMOS technology) from VHDL descriptions show that a throughput of >32M bits/s can be achieved.

[1] Z. Chi and K. K. Parhi, "High Speed Algorithm and VLSI Architecture Design for Decoding BCH Product Codes", *Proc. of 2002 IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Orlando, pp. 3089-3092, May 2002

[2] Z. Chi and K.K. Parhi, "High-Speed VLSI Architecture Design for Block Turbo Decoder", *Proc. of 2002 IEEE Int. Symp. on Circuits and Systems*, Vol. 1, pp. 901-904, Scottsdale, AZ, May 2002

2. Extended Hamming Block Turbo Coder

To explore time diversity to combat channel noise, redundancy can be introduced to the transmitted information. Block turbo code introduced in 1994 is one of the most powerful error control codes with performance approaching Shannon limit. Unfortunately, its decoding complexity is very high. A very low complexity block turbo decoder composed of extended Hamming codes has been proposed. New efficient complexity reduction algorithms are proposed including simplifying the extrinsic information computation and soft inputs updating algorithm. For performance evaluation, $[\text{eHamming } (32,26,4)]^2$ and $[\text{eHamming } (64,57,4)]^2$ block turbo code transmitted over AWGN channel using BPSK modulation are considered. Extra 0.3dB to 0.4dB coding gain is obtained when compared with the most recent schemes and the hardware overhead is negligible. The complexity of our new block turbo decoder is about ten times less than that of the near-optimum block turbo decoder with a performance degradation of only 0.5dB. Other schemes such as reduction of test patterns in the Chase algorithm and memory saving techniques have been considered.

[3] Y. Chen and K.K. Parhi, "A Very Low Complexity Block Turbo Decoder Composed of Extended Hamming Codes", *Proc. of 2001 IEEE Globecom Conference*, Vol. 1, pp. 171-175, San Antonio, Texas

3. Turbo Product Codes with Single Parity Check Component Codes

Both complexity and performance aspects of serially concatenated 2-D single parity check turbo product codes were investigated. The extremely simple Max-Log-MAP decoding is alternatively derived with only three additions needed to compute each bit's extrinsic information. A parallel decoding structure has been proposed to increase the decoding throughput while a new helical interleaver is constructed to further improve the coding gain. For performance evaluation, $(16, 14, 2)^2$ single parity check turbo product codes with code rate 0.766 over AWGN channel using QPSK are considered. The simulation results using Max-Log-MAP decoding show that it can achieve BER of 10^{-5} at SNR of 3.8dB with 8 iterations. Compared to the same rate and codeword length turbo product code composed of extended Hamming codes, the proposed scheme can achieve similar performance with much less complexity. Other implementation issues such as the finite precision analysis and efficient sorting circuit design have been addressed.

[4] Y. Chen and K.K. Parhi, "Parallel Decoding of Interleaved Single Parity Check Turbo Product Codes", *Proc. of 2002 IEEE Signal Processing Systems Workshop*, pp. 27-32, San Diego, Oct. 2002

[5] Y. Chen and K.K. Parhi, "On the Performance and Implementation Issues of Interleaved Single Parity Check Turbo Product Codes" *Journal of VLSI Signal Processing Systems*, Vol. 35, No. 1, Jan. 2005

4. Reduced Complexity Space-Time Block Codes

A computationally efficient algorithm has been developed for the soft decoding of space-time block codes. Compared to the original maximum likelihood algorithm, the proposed algorithm saves up to 80% hardware operations. The simulation results using space-time block turbo coded modulation scheme show that the proposed algorithm achieves the same decoding performance as the maximum likelihood decoding with much lower complexity. Two approaches of block turbo code with antenna diversity have been compared in terms of bit error rate (BER) performance under various configurations. One is block turbo code with multiple transmit and receive antennas (BTC-Diversity system), the other is the serial concatenation of block turbo code with space time block code (BTC-STBC system). The latter still achieves better BER performance even with the constraint of same spectral efficiency. The implementation issues such as algorithm complexity reduction scheme without performance loss and corresponding structure, new early stopping criterion and proper interleaver choice for different fading channels have been investigated for the concatenated system.

[6] Y. Chen and K.K. Parhi, "Reduced Complexity Decoding Algorithms for Space-Time Block Turbo Coded System", *EURASIP Journal on Applied Signal Processing*, 2003(13), pp. 1335-1345, 2003

5. Regular LDPC code and decoder design and Architectures

In the past few years, Gallager's Low-Density Parity-Check (LDPC) codes have received a lot of attention and many efforts have been devoted to analyze and improve their error-correcting performance. However, little consideration has been given to the LDPC decoder VLSI implementation. In this work, a joint code and decoder design approach was proposed to construct a class of (3, k)-regular LDPC codes which exactly fit to a partly parallel decoder implementation and have a very good performance. In addition, a high-speed (3, k)-regular LDPC code partly parallel decoder architecture has been developed. Based on this, a 9216-bit, rate-1/2 (3, 6)-regular LDPC code decoder has been implemented on Xilinx FPGA device. When performing maximum 18 iterations for each code block decoding, this partly parallel decoder supports a maximum symbol throughput of 54Mbps and achieves BER 10^{-6} at 2dB over AWGN channel. To the best of our knowledge, this was the first LDPC decoder FPGA implementation reported in the open literature at that time.

Novel overlapped scheduling techniques have been developed for quasi-cyclic LDPC codes which can reduce the number of clock cycles by upto factor of 2. Novel hardware sharing techniques have been developed to reduce the data path hardware complexity of LDPC decoders.

[7] T. Zhang and K. K. Parhi, “A Class of Efficient-Encoding Generalized Low-Density Parity-Check Codes”, *Proc. of 2001 IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, vol. 4, pp. 2477-2480, Salt Lake City, Utah, May 2001

[8] T. Zhang and K. K. Parhi, “VLSI Implementation-Oriented (3, k)-regular Low-Density Parity-Check Codes", *Proc. of the 2001 IEEE Workshop on Signal Processing Systems (SiPS): Design and Implementation*, pp. 25-36, Antwerp, Belgium, Sept. 2001

[9] T. Zhang and K. K. Parhi, “Joint Code and Decoder Design for Implementation-Oriented (3,k)-regular LDPC codes", *Proc. of Asilomar Conference on Signals, Systems and Computers*, Vol. 2, pp. 1232-1236, Nov. 2001

[10] T. Zhang and K. K. Parhi, “High-Performance, Low-Complexity Decoding of Generalized Low-Density Parity-Check Codes", *Proc. Of Globecom'01*, Vol. 1, pp. 181-185, San Antonio, TX, Nov. 2001

[11] T. Zhang and K. K. Parhi, “A 54 Mbps (3,6)-Regular FPGA LDPC Decoder", *IEEE 2002 IEEE Workshop on Signal Processing Systems (SiPS): Design and Implementation*, pp. 127-132, San Diego, Oct. 2002

[12] T. Zhang and K.K. Parhi, "An FPGA Implementation of (3,6) Regular Low-Density Parity-Check Code Decoder", *Eurasip Journal on Applied Signal Processing*, Vol. 2003(6), pp. 530-542, May 2003

[13] T. Zhang and K.K. Parhi, "Joint (3,k)-regular LDPC Code and Decoder/Encoder Design", *IEEE Trans. Signal Processing*, Vol. 52(4), pp. 1065-1079, April 2004

[14] Y. Chen and K.K. Parhi, "High Throughput Overlapped Message Passing for Low Density Parity Check Codes", *Proc. of ACM/IEEE Great Lakes Symp. on VLSI*, pp. 245-248, April 2003

[15] Y. Chen and K.K. Parhi, "Overlapped Message Passing of Quasi-Cyclic Low-Density Parity Check Codes", *IEEE Trans. on Circuits and Systems, Part-I: Regular Papers*, Vol. 51(6), pp. 1106-1113, June 2004

[16] Z. Wang, Y. Chen and K.K. Parhi, "Area-Efficient Decoding of Quasi-Cyclic Low-Density Parity Check Codes," *Proc. of the 2004 IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Vol. V, pp. 49-52, Montreal, May 2004

6. Architectures for Long BCH Encoders

The speed in long BCH encoders is limited by the feedback loop of the linear feedback shift register. Several approaches were developed to circumvent the speed problem and the fanout problem simultaneously in long BCH encoders.

For the case of decoders, novel substructure sharing approaches were developed to reduce the hardware complexity of the Chien search part which is the most computationally complex part of the decoder.

[17] X. Zhang and K.K. Parhi, "High-Speed Architectures for Long BCH Encoders", *Proc. of 2004 Great Lakes Symp. on VLSI*, pp. 1-6, Boston, April 2004

[18] X. Zhang and K.K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm", *IEEE Trans. on VLSI Systems*, **12**(9), pp. 957-967, Sep. 2004

[19] Y. Chen and K.K. Parhi, "Small Area Parallel Chien searchArchitectures for Long BCH Codes", *IEEE Trans. on VLSI Systems*, **12**(5), pp. 545-549, May 2004

[20] Y. Chen and K.K. Parhi, "Area-Efficient Parallel Decoder Architecture for Long BCH Codes", *Proc. of the 2004 IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, **Vol. V**, pp. 73-76, Montreal, May 2004

7. Architectures for AES

Various approaches for efficient hardware implementation of the Advanced Encryption Standard algorithm have been studied. The optimization methods can be divided into two classes: architectural optimization and algorithmic optimization. Architectural optimization exploits the strength of pipelining, loop unrolling and sub-pipelining. Speed is increased by processing multiple rounds simultaneously at the cost of increased area. Architectural optimization is not an effective solution in feedback modes. Loop unrolling is the only architecture that can achieve a slight speedup with significantly increased area. In non-feedback modes, sub-pipelining can achieve maximum speedup and the best speed/area ratio. Algorithmic optimization exploits algorithmic strength inside each round unit. Various methods to reduce the critical path and area of each round unit are exploited. Resource sharing issues between encryptor and decryptor become important when both encryptor and decryptor need to be implemented in a small area.

[21]X. Zhang and K.K. Parhi, "Hardware Implementation of Advanced Encryption Standard Algorithm", *IEEE CAS Magazine*, **2**(4), pp. 24-46, Dec. 2002

[22] X. Zhang and K.K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm", *IEEE Trans. on VLSI Systems*, **12**(9), pp. 957-967, Sep. 2004

[23] X. Zhang and K.K. Parhi, "An Efficient 21.5 Gbps AES Implementation on FPGA", *Proc. of 38th Asilomar Conference on Signals, Systems, and Computers*, Nov. 2004, Pacific Grove (CA)

8. Ultra Wideband Systems

In [24], the power spectrum of fast-frequency hopping (FFH) multi-carrier (MC) ultra wideband (UWB) communication systems was analyzed in detail and compared with single carrier (SC) UWB systems. According to the analysis, the MB UWB system is easier to fit into the power spectrum mask for UWB systems defined by FCC and thus achieves a higher transmitting efficiency. At the same time, based on the analysis, it is possible to design the parameters of a practical MC-UWB system. In [25] and [26], a novel algorithm, SD-KB algorithm, was proposed by combining the sphere decoding and K-best algorithms to solve the maximum likelihood detection (MLD) problem sub-optimally. The new algorithm dramatically reduces the computation complexity compared with the sphere decoding algorithm in low SNR range. Specifically, this new algorithm was applied to the simultaneously operating piconets (SOP) problem in multi-band OFDM (MB-OFDM) systems. Compared with the baseline FFT and equalization detection algorithm, by applying the new algorithm, the performance of the system in SOP can be enhanced up to 4dB. In [26], the algorithm was further improvement by dynamically choosing the division points of the sphere decoding and K-best parts in the SD-KB algorithm. In [27], a new pulsed-OFDM (P-OFDM) system was proposed for the UWB communication based on the baseline MB-OFDM system. The new P-OFDM system can achieve similar or better performance than MB-OFDM system by balancing coding gain and diversity gain. Meanwhile, it requires a lower implementation complexity with a smaller size FFT/IFFT processor, up-sampling, and time-multiplexing of the FFT processor.

[24] J. Tang and K. K. Parhi, “On the power spectrum density and parameter choice of multi-carrier UWB communications”, in *Proc. of 37th Asilomar Conference on Signals, Systems and Computers*, vol. 2, Nov. 2003, pp. 1230-1234.

[25] J. Tang, A. H. Tewfik, and K. K. Parhi, “High performance solution for interfering UWB piconets with reduced complexity sphere decoding”, in *Proc. IEEE International Symposium on Signals and Systems*, vol. 5, May 2004, pp. 377-380.

[26] J. Tang, A. H. Tewfik, and K. K. Parhi, “Reduced complexity sphere decoding and application to interfering IEEE 802.15.3a piconets”, in *International Conference on Communications*, vol. 5, June 2004, pp. 2864-2866.

[27] E. Saberinia, J. Tang, A. H. Tewfik, and K. K. Parhi, “Pulsed OFDM modulation for ultra wideband communications”, in *IEEE International Symposium on Signals and Systems*, 2004, vol. 5, May 2004, pp. 369-372.

9. High-Speed Errors-and-Erasures Correcting Reed-Solomon Decoders VLSI Design

It is well known that RS decoder with the capability of correcting errors as well as erasures will improve performance in various systems. In this work, we reformulated the Berlekamp-Massey (BM) algorithm for errors-and-erasures RS decoding to improve the decoding speed. We developed a semi-systolic architecture which has a critical path of only $T_{mult}+T_{add}$ that is much smaller than that of the previous RS decoder implementations using BM algorithm. Moreover, an operation scheduling scheme has been proposed for the key equation solver (KES) block so that the overall RS decoder hardware complexity can be reduced without loss of throughput. Compared with the errors-alone RS decoder, the proposed errors-and-erasures RS decoder may achieve the same throughput but requires extra d+2floor((d-1)/2)-3 multipliers and d+floor((d-1/2)-3 adders due to the implementation of erasure locator (EL) block and higher possible degree of errata locator polynomial $\Lambda(z)$ in the KES block.

[28] T. Zhang and K.K. Parhi, "On the High-Speed VLSI Implementation of Errors-and-Erasures Correcting Reed-Solomon Decoders", *Proc. of 2002 Great Lakes Symp. on VLSI*, pp. 95-100, Binghamton, NY, April 2002

10. Soft-Decison Reed-Solomon Codes

Reed-Solomon codes are among the most extensively used error-control codes. In 2001, a polynomial complexity soft-decision decoding algorithm was proposed by Koetter and Vardy (KV), which significantly outperforms both the Guruswami-Sudan's list decoding and the Generalized Minimum Distance-based decoding algorithms. However, the high complexity of the KV algorithm makes its applications prohibitive. How to reduce the complexity of the extensively used Hasse derivative computation and root finding of univariant polynomials in the hardware implementations of the KV algorithm are of great interest. Reducing memory requirement is another concern, the number of look-up tables and intermediate values need to be stored grows significantly with the total multiplicity. Reducing the total number of iterations and exploring the parallelism are critical for speeding up the decoding process. Current research is directed towards solving these issues.

[29] X. Zhang and K.K. Parhi, "Fast Factorization Architecture in Soft-Decision Reed-Solomon Decoding", *Proc. of 2004 IEEE Workshop on Signal Processing Systems*, Sept. 2004, Austin (TX)

11. Students Supported:

Mr. Zhipei Chi
Mr. Tong Zhang
Ms. Yanni Chen

Ms. Xinmiao Zhang
Mr. Jun Tang
Mr. Yongru Gu

12. Awards

A paper on High-Speed Long BCH Encoder coauthored by Xinmiao Zhang and Keshab K. Parhi was chosen to be the recipient of the best paper award at the 2004 Great Lakes Symposium on VLSI held in Boston in April-2004. Keshab K. Parhi was awarded the 2003 IEEE Kiyo Tomiyasu Technical Field award and the 2004 F.E. Terman award from the American Society of Engineering Education.