AN OBFUSCATED RADIX-2 REAL FFT ARCHITECTURE

Goutham N. C. Shanmugam, Yingjie Lao and Keshab K. Parhi, Fellow, IEEE

Department of Electrical and Computer Engineering
University of Minnesota, Minneapolis, MN, USA

ABSTRACT

Design of integrated circuits that cannot be reverse engineered is very important for protecting the intellectual property of owners. Integrated circuits can be obfuscated by introducing several modes into the control flow. Only one of the modes is the desired mode and other modes represent either meaningful modes where computations are partially correct or modes where the outputs computed are completely random. This paper presents a novel architecture and implementation of an obfuscated FFT for real input signals. The proposed design can be reconfigured to compute real FFTs of size N or N/4 with 2-parallel or 4-parallel processing, which are considered the 4 meaningful modes in the design. A 4-bit configure data is used to select one of the four meaningful modes. The remaining 12 modes output partially correct results. The meaningful mode with the most number of blocks, i.e., an N-point, 4-parallel real FFT, is designed first and that circuit is then obfuscated with the inclusion of a reconfigurator and an obfuscating FSM. A *novel control flow* approach is introduced for hiding the modes for obfuscation. It is shown that the proposed approach results in minimal area and power overhead compared to the base design.

Index Terms **–** Fast Fourier Transform (FFT), real FFT (RFFT), hardware security, obfuscation, reverse engineering

1. INTRODUCTION

The fast Fourier transform (FFT) is one of the most important and widely used functions in the field of digital signal processing (DSP) and image processing. Pipelined architectures are largely preferred for FFT computations as these provide higher throughput, low latency, low area and decreased power consumption [1-9]. Many physical signals such as electrocardiography (ECG), electroencephalography (EEG), speech, image, radar, audio and biomedical signals are real. To reduce hardware complexity of FFTs for these applications, there has been a growing interest in efficient FFT computation for real samples. When the input samples are real, the frequency spectrum of the FFT is Hermitian symmetric and approximately half of the computations are redundant [10]. This property can be used to lower hardware complexity, thereby reducing the overall area and power consumption. With increasing demand for the electronic devices, hardware security has become one of the most important challenges [11]. Reverse engineering is often used to recreate the design; thus the intellectual property of a designer is no longer protected. Other examples include sale of excess parts by a foundry to someone other than the client. These excess parts bring down the cost of the device leading to loss of revenue for the client [12]. Therefore, it is important to design integrated circuits that are harder to reverse engineer. An approach to obfuscating DSP circuits through high level transformations has been proposed to improve the security of various devices [13] [14] and is shown in Fig. 1. The foundry can no longer sell excess parts to a third party as these excess parts cannot be used without the *key* that is required for correct functionality of the chip. The approach to obfuscation involves embedding many undesired and non-meaningful modes to the design. A two-part key is introduced where the first part, referred to as the *initialization key*, is processed by a finite state machine (FSM) which then triggers a reconfigurator. The second part, referred to as the *configure data*, selects a mode of operation. A wrong configure data triggers an undesired mode leading to undesired outputs. These keys are programmed after the chips have been fabricated with the foundry playing no role in this process.

This research was supported in parts by the National Science Foundation under grant number CNS-1441639 and by the Semiconductor Research Corporation under contract number 2014-TS-2560.

This paper presents a novel architecture to design an obfuscated real FFT (RFFT) with 16 operating modes, out of which 4 modes are meaningful and 12 are non-meaningful. The 4 meaningful modes compute a real FFT of size either N or N/4 with level of parallelism 2 or 4. The meaningful mode with the most number of blocks, i.e., an N-point, 4-parallel real FFT, is designed first and then obfuscated to accommodate the other modes with the help of an obfuscating FSM and a reconfigurator. Additional switches, delay elements and control circuits are needed for obfuscation.

The rest of the paper is organized as follows. Section 2 presents the implementation of the obfuscated design using the N-point, 4-parallel mode as the base architecture. Section 3 presents a discussion on how the non-meaningful modes should be created to increase the level of obfuscation. In Section 4, the synthesis results of the obfuscated design are analyzed and are compared with that of the most complex meaningful mode.

2. OBFUSCATED DESIGN

The N-point, 4-parallel mode is first designed as it has the most number of blocks. The block diagram of 64-point radix-2 decimation-in-frequency (DIF) RFFT 4-parallel and 2-parallel modes are shown in Fig. 2 and Fig. 3, respectively. The architecture used here is similar to the one proposed in [10].

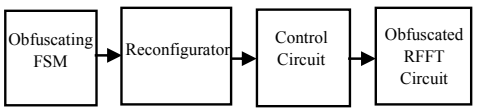


Fig. 1. Block diagram of the Obfuscated Design

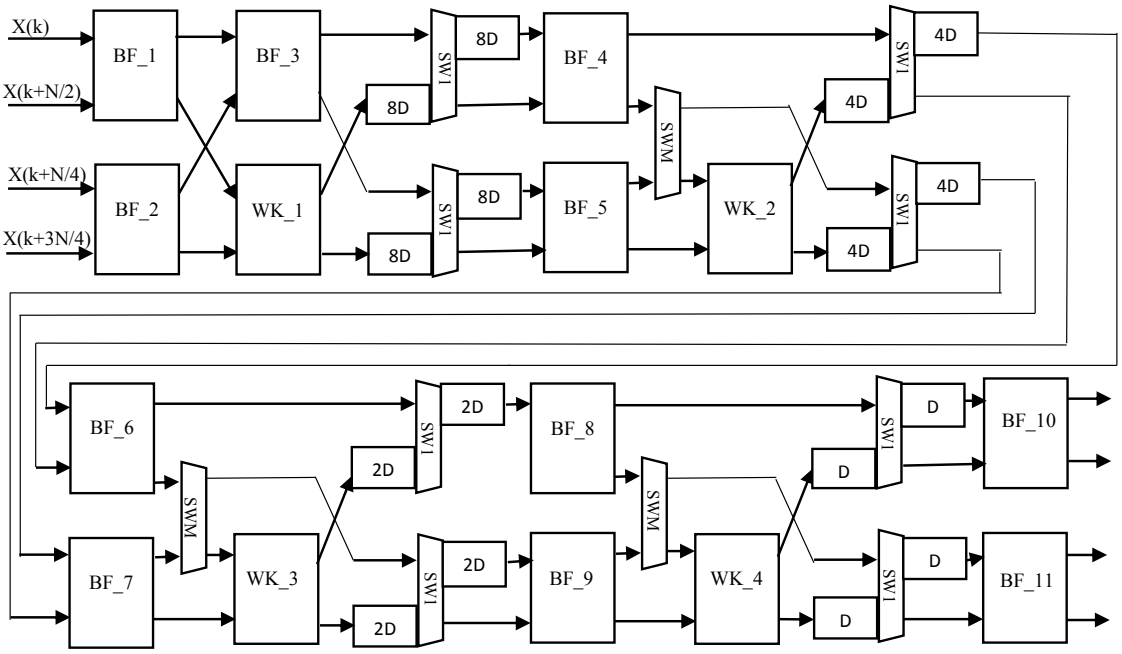


Fig. 2. 64-Point 4-Parallel Radix-2 DIF RFFT

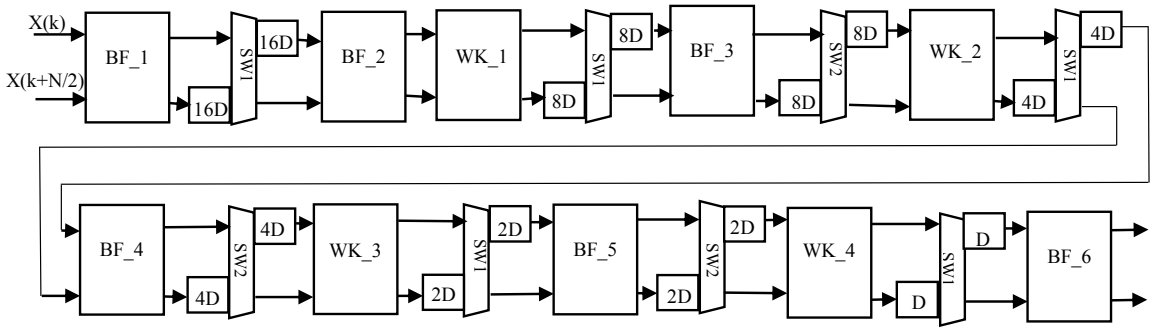


Fig. 3. 64-Point 2-Parallel Radix-2 DIF RFFT

A novel architecture has been designed for the obfuscated real FFT circuit, shown in Fig. 4, with the four following meaning modes: i) 64-point, 4-parallel ii) 16-point, 4-parallel iii) 64-point, 2-parallel iv) 16-point, 2-parallel. Various mode converters (MCs) are introduced for configuring the data flow so that the signals are processed by their respective datapaths when the mode of operation is changed.

2.1. Mode Converters

The mode converter (MC) blocks are included for obfuscation and are shown in red and blue colors in Fig. 4. The mode converters are switches whose control signals vary according to the mode of operation. The functionality of these MCs for different modes of operation is described in Table 1.

2.1.1. 4-Parallel Operation

During 4-parallel operation (Table 1), MC_1 swaps the second and third input signals to the outputs. MC_2 passes all the signals. The middle switches (SWMs) required for the normal 4-parallel circuit (Fig. 2) are placed inside MC_3, MC_4 and MC_5, through which the signals are passed. MC_Ms are switches that swap the signals.

2.1.2. 2-Parallel Operation

During 2-parallel operation (Table 1), the first two input signals are passed to a switch with 16 units of delay before and after it, which is placed inside MC_1. MC_2 sends the first two inputs to the last two outputs which is then input to the twiddle block WK_1. Switch2's (SW2s) used in a normal 2-parallel circuit (Fig. 3) are included within MC_3, MC_4 and MC_5, through which the signals are passed. MC_Ms just let the signals pass through.

2.1.3. N/4-Point Operation

During 16-point operation, the inputs (marked in red) are processed by BF_6 and BF_7. The blocks marked in blue (Fig. 4) are only active during 16-point operation. They operate in the same way as MC_1 and MC_2. During 64-point operation, these blocks just pass the signals. MC_4 just passes the signals during a 16-point operation.

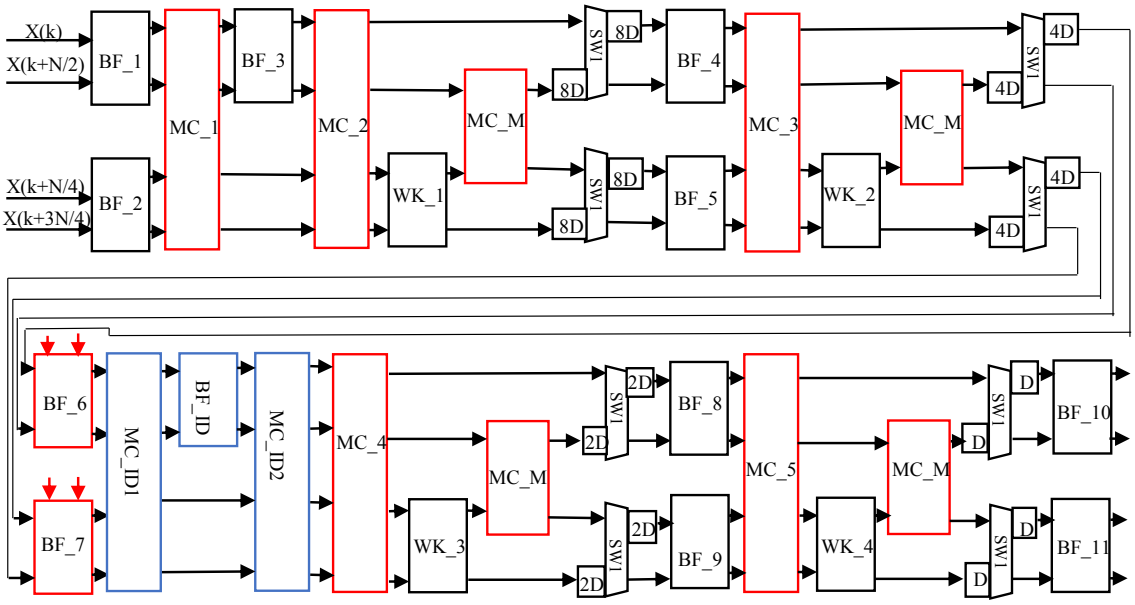


Fig. 4. Architecture of the obfuscated RFFT

2.2. Obfuscating FSM

An example of a 4-bit initialization key (here "0110") input to the obfuscating FSM is shown in Fig. 5. The actual key length can be longer. The correct key activates the state S6 and the reconfigurator is enabled. If the initialization key is incorrect then no output is produced, meaning the circuit is locked. Repeated incorrect attempts can activate a denial-of-service circuit.

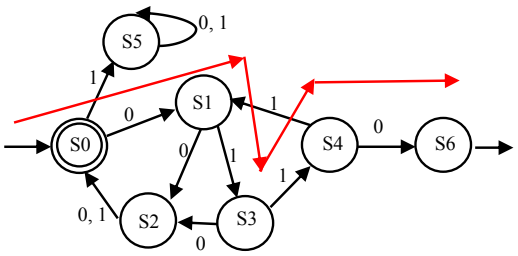


Fig. 5. Obfuscating FSM

2.3. Reconfigurator

A 4-bit configure data is given to the reconfigurator. Only when the control signal from the obfuscating FSM is active, four trigger signals (c1, c2, c3, c4) are produced depending on the configure data, which decide the mode of operation of the system as shown in Table 2.

2.4. Control Circuit

These four trigger signals are input to the control circuit, based on which, the control signals for the butterflies and switches are generated by a 5-bit counter (for N=64). The different meaningful modes are designed just by changing when the counter is reset. The first four meaningful modes from Table 1 are designed by resetting the counter at 01111, 00011, 11111 and 00111, respectively. It is obvious that when the reset value is anything other than these four values, it results in a non-meaningful mode. We are only interested in non-meaningful modes which create enough confusion for the adversary making it more tedious to figure out the functionality of the circuit.

3. NON-MEANINGFUL MODES

When an incorrect configure data key is given to the obfuscating FSM, the circuit will operate in any one of the non-meaningful modes leading to incorrect output values. Although, if the outputs produced by these non-meaningful modes are completely meaningless, it will be easier for the adversary to figure out the non-meaningful modes of the circuit. But when the non-meaningful modes produce outputs that are functionally meaningful, the process of eliminating non-meaningful modes becomes more complex, thus improving the security of the circuit.

For example, a non-meaningful mode can be designed in such a way that the first 25%, 50% or 75% of the outputs produced exactly coincide with that of a meaningful mode and the remaining outputs are incorrect. This will make the adversary check each and every value of the output only to confirm that it is a non-meaningful mode, further enhancing the security of the circuit. This can be achieved by modifying the twiddle blocks such that the signals get multiplied with a wrong twiddle factor after 25%, 50% or 75% of the signals.

4. ANALYSIS AND COMPARISON OF SYNTHESIS RESULTS

The obfuscated circuit was synthesized using 65nm technology and the results are shown in Tables 3 and 4. The clock frequency of the design is 100MHz and is independent of N as the design is pipelined. Of all the meaningful modes, the most complex mode in terms of area and power consumption is the N-point, 2-parallel design as the number of delays are considerably more than that of any other mode. Hence it was designed and synthesized separately and the results are compared with that of the obfuscated design. From Tables 3 and 4, it can

Table 1. Mode converters operations in 2-parallel and 4-parallel modes

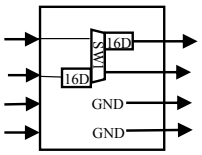
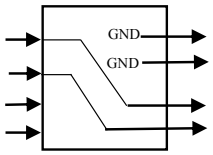
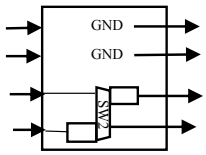
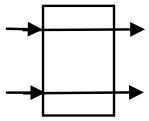
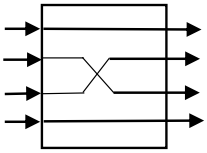
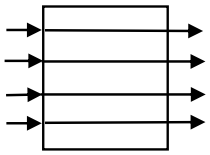
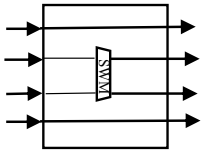
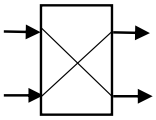
Modes	MC_1	MC_2	MC_3,4,5	MC_M
2-parallel				
4-parallel				

Table 2. Various modes based on configure data (CFD)

CFD	Modes of Operation	Trigger signals (c1, c2, c3, c4)
0000	N-pt, 4-parallel	0, 0, 0, 0
0001	N/4-pt, 4-parallel	0, 0, 0, 1
0010	N-pt, 2-parallel	0, 0, 1, 0
0011	N/4-pt, 2-parallel	0, 0, 1, 1
0100	N-pt, 4-parallel (1st 25% outputs correct)	0 ,1, 0, 0
0101	N/4-pt, 4-parallel (1st 25% outputs correct)	0, 1, 0, 1
0110	N-pt, 2-parallel (1st 25% outputs correct)	0, 1, 1, 0
0111	N/4-pt, 2-parallel (1st 25% outputs correct)	0, 1, 1, 1
1000	N-pt, 4-parallel (1st 50% outputs correct)	1, 0, 0, 0
1001	N/4-pt, 4-parallel (1st 50% outputs correct)	1, 0, 0, 1
1010	N-pt, 2-parallel (1st 50% outputs correct)	1, 0, 1, 0
1011	N/4-pt, 2-parallel (1st 50% outputs correct)	1, 0, 1, 1
1100	N-pt, 4-parallel (1st 75% outputs correct)	1, 1, 0, 0
1101	N/4-pt, 4-parallel (1st 75% outputs correct)	1, 1, 0, 1
1110	N-pt, 2-parallel (1st 75% outputs correct)	1, 1, 1, 0
1111	N/4-pt, 2-parallel (1st 75% outputs correct)	1 ,1, 1, 1

be seen that the area increases by about 24% and dynamic power consumption increases by about 40% due to obfuscation. These overheads represent the cost of obfuscating the design with few meaningful and configurable modes. It may be noted that the power consumption can be lowered using clock gating technique.

Table 3. Effect of obfuscation on area

N	Area of the most complex mode (mm^2)	Area of Obfuscated Design (mm^2)	Area increase factor
16	0.042	0.053	1.25
64	0.173	0.215	1.24
256	0.335	0.412	1.23
1024	0.460	0.568	1.24

Table 4. Effect of obfuscation on power

N	Power of the most complex mode (mW)	Power of Obfuscated Design (mW)	Power increase factor
16	2.408	3.299	1.37
64	5.177	7.455	1.44
256	8.586	11.935	1.39
1024	18.685	26.325	1.40

5. CONCLUSION

This paper presents a novel architecture for an obfuscated radix-2 real FFT with 4 meaningful modes and 12 non-meaningful modes. Obfuscation greatly increases the security of the device. Without the correct initialization key and the configure data, the adversary cannot figure out the functionality of the circuit. The area and power overhead incurred due to obfuscation are minimal when compared to the level of hardware security achieved. Future research will be directed towards quantifying obfuscation metrics and attack modes for these circuits.

6. AKNOWLEDGEMENT

The authors are grateful to Dr. Chris H. Kim and Ms. Sandhya Koteswara for many useful discussions.

6. REFERENCES

[1] L. Yang, K. Zhang, H. Liu, J. Huang, and S. Huang, "An efficient locally pipelined FFT processor," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 53, no. 7, pp. 585–589, Jul. 2006.

[2] S. He and M. Torkelson, "Design and implementation of a 1024-point pipeline FFT processor," in *Proc. Custom Integr. Circuits Conf.*, Santa Clara, CA, May 1998, pp. 131–134.

[3] M. A. Sánchez, M. Garrido, M. L. López, and J. Grajal, "Implementing the FFT algorithm on FPGA platforms: A comparative study of parallel architectures," presented at the *XIX Int. Conf. Design Circuits Integr. Syst. (DCSI 2004)*, Bourdeaux, France, Nov. 2004.

[4] W.-C. Yeh and C.-W. Jen, "High-speed and low-power split-radix FFT," *IEEE Trans. Signal Process.*, vol. 51, no. 3, pp. 864–874, Mar. 2003.

[5] H. Sorensen, D. Jones, M. Heideman, and C. S. Burrus, "Real-valued fast Fourier transform algorithms," *IEEE Trans. Acoust., Speech Signal Process.*, vol. 35, no. 6, pp. 849–863, Jun 1987.

[6] M. Ayinala and K.K. Parhi, "FFT Architectures for Real-valued Signals based on Radix-2^3 and Radix-2^4 algorithms," *IEEE Trans. Circuits and Systems-I: Regular Papers*, 60(9), pp. 2422-2430, Sept. 2013

[7] G. Bi and E. V. Jones, "A pipelined FFT processor for world-sequential data," *IEEE Tran. Acoust., Speech Signal Process.*, vol. 37, no. 12, pp. 1982–1985, Dec. 1989.

[8] M. Ayinala, M.J. Brown and K.K. Parhi, "Pipelined Parallel FFT Architectures via Folding Transformation", *IEEE Trans. VLSI Systems*, pp. 1068-1081, 20(6), June 2012

[9] M. Garrido, K.K. Parhi, and J. Grajal, "A Pipelined FFT Architecture for Real-Valued Signals", *IEEE Trans. Circuits and Systems-I: Regular Papers*, 56(12), pp. 2634-2643, Dec. 2009

[10] S.A. Salehi, R. Amirfattahi, and K.K. Parhi, "Pipelined Architectures for Real-Valued FFT and Hermitian-Symmetric IFFT with Real Datapaths," *IEEE Trans. Circuits and Systems-II: Transactions Briefs*, 60(8), pp. 507-511, Aug. 2013

[11] J. Villasenor and M. Tehranipoor, "Chop Shop Electronics," *IEEE Spectrum, Volume: 50, Issue: 10*, pp 41-45, Oct 2013

[12] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Brand and IP protection with physical unclonable functions," in *Proceedings of IEEE International Symposium on Circuits and Systems, 2008*, pp. 3186–3189.

[13] Y. Lao and K.K. Parhi, "Obfuscating DSP Circuits via High-Level Tansformations," *IEEE Transactions on VLSI Systems,* DOI 10.1109/TVLSI.2014.2323976

[14] K.K. Parhi, "Verifying Functionality of Digital Signal Processing Circuits," *Proc. of 46th Asilomar Conference on Signals, Systems and Computers*, pp. 99-103, Pacific Grove, CA, Nov. 2012